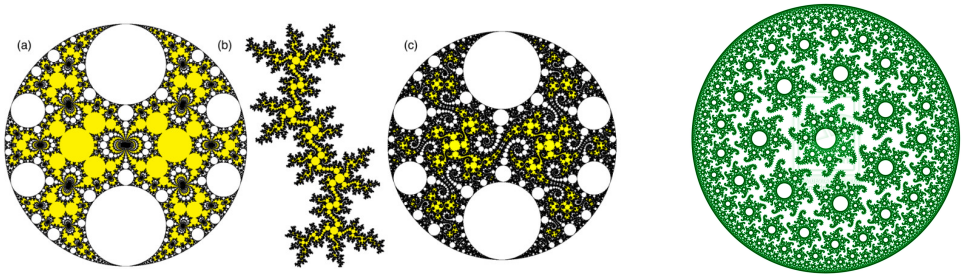
Département de Mathématiques d'Orsay

Groupes, Anneaux, Corps

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

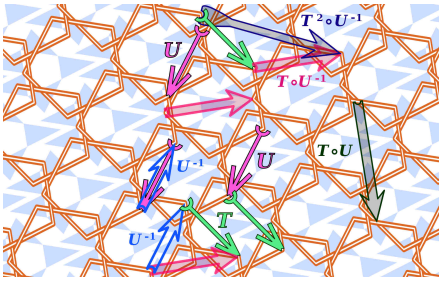
« Le plagiat est nécessaire. Le progrès l'implique. Il serre de près la phrase d'un auteur, se sert de ses expressions, efface une idée fausse, la remplace par l'idée juste. »

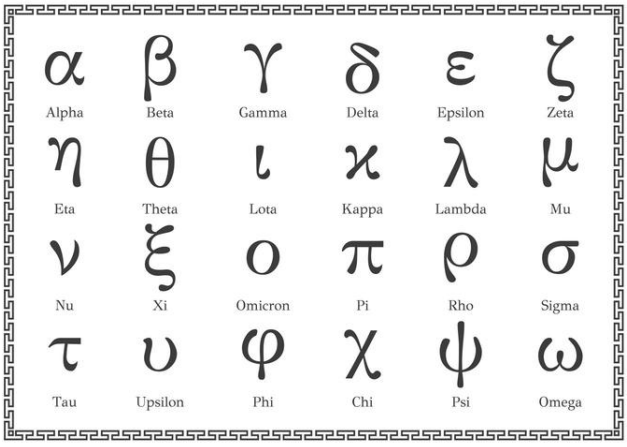
Isidore DUCASSE, dit *Comte de Lautréamont*



« Copier sur un seul, c'est du plagiat. Copier sur deux, c'est de la recherche. »

Alban DU PLESSIS DE LA ROQUENTIÈRE




α Alpha
β Beta
γ Gamma
δ Delta
ε Epsilon
ζ Zeta
η Eta
θ Theta
ι Lota
κ Kappa
λ Lambda
μ Mu
ν Nu
ξ Xi
ο Omicron
π Pi
ρ Rho
σ Sigma
τ Tau
υ Upsilon
φ Phi
χ Chi
ψ Psi
ω Omega

Méthodologie de travail pour le cours « *Structures Algébriques* »
Licence 2 Double Diplôme

Joël MERKER alias François DE MARÇAY
Département de Mathématique d'Orsay
Université Paris-Saclay, France

• **Notes de cours.** Des notes de cours seront régulièrement transmises par courriel sous forme pdf. La référence principale utilisée pour ce cours sera le livre de Grégory BERHUY, *Algèbre, le grand combat*.

• **Modalités de contrôle.** Les **100 %** de la note finale complète comprendront :

□ **15 %** contrôle continu = les **2** devoirs à la maison (DMs) et les **2** interrogations écrites en TD.

□ **35 %** examen partiel.

□ **50 %** examen terminal.

• **Devoirs à la maison.** Deux devoirs à la maison seront à rendre. Ils seront établis et visés par le professeur responsable, Joël Merker.

! Chaque devoir non rendu se verra attribuer une note de $\frac{0}{20}$ qui contribuera à hauteur de **7,5 %** de la note finale **!**

Pour chaque DM, entre 16 et 18 points sur 20 seront facilement accessibles.

• **Méthode classique :** ***Obligation impérative d'écrire à la main !***

□ *Pourquoi ?* Parce qu'un document sur ordinateur peut facilement être échangé par mail entre étudiants et être récopié en entier ou par morceaux via Control-C puis Control-V.

□ *Quel est le but ?* Que les étudiants apprennent et assimilent des mathématiques par la lecture. Mieux vaut un vrai travail personnel formateur qu'une dilapidation de son temps sur internet, ou devant la télévision.

• **Transmission des devoirs à la maison :** *Par mail, sous forme scannée (ou photographiée).* Document pdf unique apprécié.

• **Examens.** Les sujets de l'examen partiel et de l'examen terminal seront établis par le professeur responsable, Joël Merker. Les copies seront intégralement corrigées par ledit professeur.

• **Règle d'or pendant les cours :**

Interdiction absolue d'utiliser et de consulter
smartphones, téléphones et ordinateurs portables
et tous autres gadgets électroniques contraires au travail.

• **Modalités d'application de cette règle d'or.** Les étudiants qui contreviendront à cette règle seront exclus sur le champ de la salle de cours. Le cours ne reprendra que lorsque les étudiants en question seront sortis de la salle de cours.

• **Lecture régulière du cours.** Chaque étudiant s'imposera de lire, relire et étudier régulièrement le cours. Ce travail s'effectuera occasionnellement, même sur des courtes périodes d'une dizaine de minutes, à la maison, à la bibliothèque ou dans les transports en commun. ***C'est en lisant qu'on développe son intelligence***, car on absorbe les intelligences variées d'autres personnes sans rester confiné en soi-même, voire infiniment pire : confiné à l'abrutissement total du tripotage crétinisant de smartphone !

• **Assiduité au cours.** C'est principalement le cours oral au tableau qui permettra de transmettre les idées informelles et les intuitions importantes. Aussi, lecture du cours et présence au cours seront-elles *deux activités complémentaires et indispensables pour une préparation optimale au métier de scientifique*. De plus, *on lit beaucoup plus facilement les notes de cours après avoir écouté le professeur*. ***De toute façon, une bonne prise de notes manuscrites personnelles a plus de valeur que les polycopiés.***

• **Prise de notes pendant les séances de cours.** ***L'existence de documents écrits transmis par les professeurs ne dispense absolument pas de prendre des notes manuscrites complètes et soignées***.

Table des matières

Arithmétique dans $\mathbb{Z}$ et dans $\mathbb{Z}/n\mathbb{Z}$

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Introduction

2. Ensemble $\mathbb{N}$ des entiers positifs

En mathématiques, tout le monde connaît l'ensemble $\mathbb{N}$ des *entiers naturels* 0, 1, 2, 3, 4, 5, 6, 7, $\ldots$ On dit que ces entiers sont « *naturels* », car leur existence semble tout à fait claire sur la Terre (souffrante) qui nous environne — notamment lorsque le professeur compte le nombre (entier) de copies d'examen de ses étudiants. Dans notre atmosphère de plus en plus enrichie en molécules de CO_2, les nombres entiers existent partout, c'est bel et bien certain !

Mais à partir de la fin du XIX$^{\text{ième}}$ siècle, les mathématiciens ont désiré renforcer l'autonomie des mathématiques en créant des théories abstraites qui ne reposeraient ni sur la physique, ni sur la chimie, ni sur la biologie, ou que sais-je encore, sur l'espionnage nanométré de milliards de smartphones.

Et dans les mathématiques contemporaines, ce sont les axiomes dits *de Peano* [1] qui sont actuellement considérés comme un fondement rigoureux pour l'ensemble des nombres entiers, au sein de la branche reine des mathématiques, l'Arithmétique.

1. Giuseppe Peano (1858–1932) était un mathématicien et linguiste italien. Pionnier de l'approche formaliste des mathématiques, il développa, parallèlement à l'Allemand Richard Dedekind, une axiomatisation de l'arithmétique.

Au début de 1889, Giuseppe Peano publie un livret d'à peine 36 pages où il introduit pour la première fois les « axiomes de Peano » sur la construction des nombres entiers naturels. Il l'intitule « *Arithmetices principa nova metodo expositan* », et ses résultats seront, en grande partie, rapidement adoptés par la communauté mathématique.

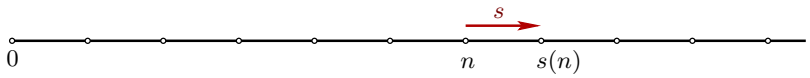
Dans le prolongement de sa contribution à l'axiomatique et à la logique symbolique, Peano formule un projet de langage logique universel grâce auquel il va pouvoir tout, ou presque, écrire et comprendre, avec son *Formulaire de mathématiques*. Les notations des mathématiques d'aujourd'hui doivent beaucoup à cet ambitieux projet de formalisation des mathématiques, écrit en français, que Peano conduit aidé de plusieurs de ses élèves, de 1895 à 1908.

À la fin de sa carrière, Peano finit par passer plus de temps à l'enseignement de ses notations originales, et à établir les définitions et concepts de base, qu'au programme d'enseignement qu'il devait traiter en face de ses étudiants. Convaincu des bénéfices de son formulaire et de ses symboles, Peano en vint même à exiger que les examens soient rédigés dans ce nouveau langage par ses étudiants !

Axiomes 2.1. [de Peano] Il existe un ensemble noté $\mathbb{N}$ contenant un élément distingué $0 \in \mathbb{N}$ appelé *zéro*, tel que $\mathbb{N}$ est muni d'une *application successeur :*

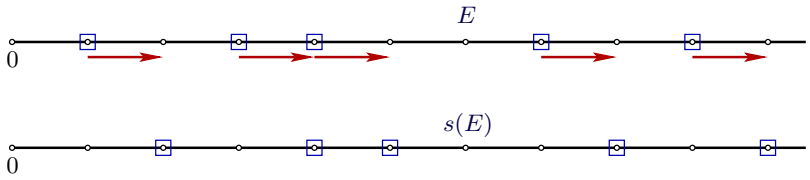
$$s\colon \quad \mathbb{N} \longrightarrow \mathbb{N},$$

laquelle vérifie les trois propriétés fondamentales suivantes.



(A1) 0 n'est le successeur d'aucun élément $n \in \mathbb{N}$, c'est-à-dire que $s(n) \neq 0$ pour tout $n \in \mathbb{N}$.

(A2) Deux nombres entiers m et n qui ont même successeur $s(m) = s(n)$ sont nécessairement égaux $m = n$, c'est-à-dire que l'application s est injective.



(A3) [Principe de récurrence] Si un sous-ensemble $E \subset \mathbb{N}$ contient $0 \in E$, et est *stable par* s, c'est-à-dire vérifie [2] :

$$s(E) \subset E,$$

alors en fait il remplit tout :

$$E = \mathbb{N}.$$

Les éléments de $\mathbb{N}$ sont appelés *entiers naturels* [3].

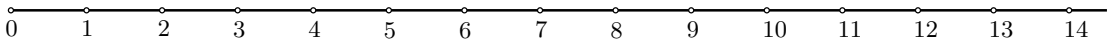
Parmi ces trois propriétés, la plus subtile et la plus importante, c'est **(A3)**, et nous y reviendrons dans quelques instants afin de justifier l'appellation « *Principe de récurrence* ».

Évidemment, il faut avoir à l'esprit que :

$$s(n) := n + 1,$$

et on pose :

$$1 := s(0), \qquad 2 := s(1), \qquad 3 := s(2), \qquad 4 := s(3), \qquad 5 := s(4), \qquad \ldots\ldots$$



Question 2.2. *Pourquoi formuler des axiomes ?*

2. Sur la figure illustrative au-dessus, on n'a *ni* $0 \in E$, *ni* $s(E) \subset E$.

3. On notera que ces axiomes ne disent pas véritablement comment construire $\mathbb{N}$. Heureusement, en théorie des ensembles, il est possible de construire $\mathbb{N}$ uniquement à partir de l'ensemble vide $\emptyset$, de la manière suivante : $0 := \emptyset$, puis $1 := \{\emptyset\}$ (l'ensemble dont l'unique élément est l'ensemble vide), puis :

$$2 := \big\{\emptyset,\, \{\emptyset\}\big\} = \{0, 1\},$$
$$3 := \Big\{\emptyset,\, \{\emptyset\},\, \big\{\emptyset,\, \{\emptyset\}\big\}\Big\} = \{0, 1, 2\}, \qquad \text{et ainsi de suite.}$$

De manière imagée, les axiomes doivent être envisagés comme des « règles du jeu », avant que ne débute le jeu véritable. Ce sont aussi des points de départ, des principes. Or les mathématiciens évoluent dans un monde essentiellement *incorporel*[4], et donc ils doivent impérativement créer et re-créer toutes les conséquences de leurs axiomes et de leurs principes, pour garantir que leur monde idéal existe véritablement.

Autrement dit, les axiomes vont servir de briques élémentaires pour de nombreuses démonstrations mathématiques. Notamment, il s'agira de *raisonner* avec logique, de *déduire* des conséquences, et de *démontrer* des résultats, tout cela, en prenant appui *seulement* sur les axiomes.

Nous pouvons donc commencer à décrire brièvement comment la théorie de Peano déduit *mathématiquement* toutes les propriétés évidentes ou connues des entiers naturels $n \in \mathbb{N}$.

Proposition 2.3. *Tout entier $a \neq 0$ est le successeur $a = s(c)$ d'un unique entier c.*

Démonstration. L'unicité de c est garantie par l'Axiome **(A2)**.

Pour ce qui est de l'existence de c, nous allons nous servir de l'Axiome crucial **(A3)**. Introduisons le sous-ensemble de $\mathbb{N}$:

$$E \,:=\, \{0\} \cup s(\mathbb{N}).$$

Premièrement, on a $0 \in E$. Deuxièmement, $E \subset \mathbb{N}$ implique $s(E) \subset s(\mathbb{N})$, et comme E contient visiblement $s(\mathbb{N})$, il vient :

$$s(E) \,\subset\, s(\mathbb{N}) \,\subset\, E.$$

Par conséquent, l'Axiome **(A3)** s'applique, il donne $E = \mathbb{N}$, et nous en déduisons que :

$$s(\mathbb{N}) \,=\, E \setminus \{0\} \,=\, \mathbb{N} \setminus \{0\}.$$

Si donc $a \in \mathbb{N}\setminus\{0\}$ est quelconque, cette égalité montre qu'il appartient aussi à $s(\mathbb{N})$, donc il existe bien $c \in \mathbb{N}$ tel que $s(c) = a$. □

Maintenant, définissons l'addition.

Proposition-Définition 2.4. [Addition] *Soit $n \in \mathbb{N}$. Il existe une application $m \longmapsto n+m$ de $\mathbb{N}$ dans $\mathbb{N}$ définie en posant :*

- $n + 0 := n$*;*
- $n + s(p) = s(n + p)$*, pour tout $p \in \mathbb{N}$.*

Cette application définit une opération sur $\mathbb{N}$, c'est-à-dire une application de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$ qui, au couple (n, p) associe l'entier $n + p$.

Cette opération est appelée addition*, et l'entier $n + p$ est appelé* somme *de n et de p.*

Preuve résumée. Il s'agit de vérifier que l'ensemble E des entiers m pour lesquels cette application est définie est $\mathbb{N}$ tout entier. Comme E contient 0 et est stable par successeur, cela résulte de l'Axiome **(A3)**, *i.e.* du principe de récurrence. □

4. Les philosophes stoïciens estimaient qu'il y avait une différence entre les *principes* et les *éléments*. Les principes sont incréés et incorruptibles, tandis que les éléments se corrompent dans la conflagration. De plus, les principes sont incorporels et informes, tandis que les éléments sont pourvus d'une forme.

Grâce à cet énoncé, on a, par définition :

$$n+1 \;=\; n+s(0) \;=\; s(n+0) \;=\; s(n),$$

ce qui justifie pleinement notre intuition initiale que l'application de successeur $s(n)$ d'un entier n consiste à lui ajouter 1.

Cette observation permet de reformuler le principe de récurrence sous la forme la plus naturelle et la plus connue.

Théorème 2.5. [Principe de récurrence] *Soit $P(n)$ une propriété définie pour tout entier $n \in \mathbb{N}$. On suppose que :*

(1) Initialisation : *$P(0)$ est vraie ;*

(2) Hérédité : *$P(n)$ implique $P(n+1)$, quel que soit $n \in \mathbb{N}$.*

Alors $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Preuve résumée. Il suffit d'appliquer l'Axiome **(A3)** à l'ensemble E des entiers n qui vérifient la propriété $P(n)$. Les détails sont laissés en exercice (facile). □

À présent, les propriétés bien connues de l'addition peuvent être « dévoilées » comme *conséquences* des Axiomes **(A1)**, **(A2)**, **(A3)** de Peano.

Proposition 2.6. *Les quatre propriétés suivantes sont satisfaites.*

(1) Associativité de l'addition : *Pour tous $a, b, c \in \mathbb{N}$, on a $a+(b+c) = (a+b)+c$.*

(2) Commutativité de l'addition : *Pour tous $a, b \in \mathbb{N}$, on a $a+b = b+a$.*

(3) Règle de simplification : *Pour tous $a, b, c \in \mathbb{N}$, l'égalité $a+b = a+c$ implique $b = c$.*

(4) *Si $a+b=0$ est nul, alors $a=0$ et $b=0$ sont nuls.*

Attention ! En première approche, les étudiants sont invités à « sauter » la lecture de cette démonstration, et à reprendre la lecture à partir de « Sur notre route . . . ».

Démonstration concise. **(1)** On fixe $a, b \in \mathbb{N}$, et on applique le principe de récurrence à c. Soit E l'ensemble des c qui vérifient la propriété. On a $0 \in E$, car par définition $a+(b+0) = a+b$ et $(a+b)+0 = a+b$.

Ensuite, supposons que $c = s(p)$ soit le successeur d'un entier p, et que p vérifie l'associativité, *i.e* que $a+\big(b+p\big) = (a+b)+p$. Alors on calcule en appliquant la définition de l'addition :

$$\begin{aligned} a+(b+c) \;=\; a+\big(b+s(p)\big) \;=\; a+s(b+p) \;&=\; s\big(a+(b+p)\big) \\ \text{[Hypothèse de récurrence]} \qquad\qquad &= s\big((a+b)+p\big) \\ &= (a+b)+s(p) \\ &= (a+b)+c, \end{aligned}$$

pour constater que $c = s(p)$ vérifie encore l'associativité. On voit donc qu'on a bien $c \in E$, de sorte que E est stable par successeur, donc égal à $\mathbb{N}$, d'après l'Axiome **(A3)**.

(2) Commençons par établir deux lemmes.

Lemme 2.7. *Pour tout $a \in \mathbb{N}$, on a $a+0 = a = 0+a$.*

Indication de preuve. En partant de $0+0 = 0 = 0+0$, il suffit de raisonner par récurrence sur $a \in \mathbb{N}$. □

Lemme 2.8. *Pour tous $a, p \in \mathbb{N}$, on a $s(p)+a = s(p+a)$.*

On notera une différence d'ordre des termes à gauche, par rapport à l'identité connue $p + s(a) = s(p + a)$ de la Proposition-Définition 2.4.

Démonstration. On raisonne par récurrence sur $a \in \mathbb{N}$. Précisément, introduisons l'ensemble E des a qui vérifient $s(p) + a = s(p + a)$, pour tout $p \in \mathbb{N}$. Par définition de l'addition, 0 est dans E, c'est-à-dire $s(p) + 0 = s(p) = s(p + 0)$.

Soit $q \in E$. On a donc $s(p) + q = s(p + q)$, pour tout p. Montrons que $a := s(q)$ est aussi dans E, en calculant :

$$\begin{aligned} s(p) + a &= s(p) + s(q) \\ \text{[Définition de l'addition]} \qquad &= s\big(s(p) + q\big) \\ \text{[Hypothèse de récurrence]} \qquad &= s\big(s(p + q)\big) \\ \text{[Définition de l'addition]} \qquad &= s\big(p + s(q)\big) \;=\; s(p + a). \end{aligned}$$

Donc $E = \mathbb{N}$ grâce à l'Axiome **(A3)**. □

Nous pouvons maintenant prouver le point **(2)**. Raisonnons par récurrence sur b en introduisant l'ensemble E des $b \in \mathbb{N}$ qui vérifient la commutativité $a + b = b + a$ pour tout $a \in \mathbb{N}$. Grâce au Lemme 2.7, on a $0 \in E$

Supposons que $p \in E$ c'est-à-dire que $a+p = p+a$, et montrons $s(p) \in E$ en calculant :

$$a + s(p) \;=\; s(a + p) \;=\; s(p + a) \;=\; s(p) + a,$$

successivement : par définition ; par hypothèse de récurrence ; par le Lemme 2.8. Donc $s(p) \in E$, puis $E = \mathbb{N}$ grâce à **(A3)**, et cela termine **(2)**.

(3) Après commutation, ce point se montre par récurrence sur a (exercice).

(4) Ce dernier point est facile en raisonnant par l'absurde. Si, par exemple, b n'était pas égal à 0, par la Proposition 2.3, b serait successeur[5] $s(q) = b$ d'un q, d'où l'on déduirait par définition de l'addition :

$$0 \;=\; a + b \;=\; a + s(q) \;=\; s(a + q),$$

en contradiction avec l'Axiome **(A1)**, d'après lequel 0 n'est successeur de personne. □

Sur notre route, nous avons démontré, pour tout $a \in \mathbb{N}$, que :

$$1 + a \;=\; a + 1.$$

Mais le premier théorème vraiment important de l'arithmétique, que tous les écureuils connaissent, c'est : *deux et deux font quatre*, c'est-à-dire $2 + 2 = 4$. Et grâce à tout ce qui précède, nous pouvons le *démontrer* comme suit :

$$4 \;=\; s(3) \;=\; 3 + 1 \;=\; (2 + 1) + 1 \;=\; 2 + (1 + 1) \;=\; 2 + 2.$$

Parlons maintenant de la multiplication.

Proposition-Définition 2.9. *On définit une loi de multiplication sur $\mathbb{N}$, notée[6] $\cdot$, en posant :*

- $n \cdot 0 = 0$ *pour tout* $n \in \mathbb{N}$ *;*
- $n \cdot s(p) = (n \cdot p) + n$, *pour tout* $n \in \mathbb{N}$ *et tout* $p \in \mathbb{N}$.

Alors les sept propriétés suivantes sont satisfaites.

5. À ne pas confondre avec *cul*cesseur !

6. Parfois notée sans symbole opératoire lorsqu'il n'y a pas de risque de confusion, par exemple $n\,p$ au lieu de $n \cdot p$. La notation $n \times p$ apprise à l'école élémentaire sera très peu souvent utilisée.

(1) Associativité : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, *pour tous* $a, b, c \in \mathbb{N}$.

(2) Commutativité : $a \cdot b = b \cdot a$, *pour tous* $a, b \in \mathbb{N}$.

(3) Distributivité à gauche : $(a + b) \cdot c = a \cdot c + b \cdot c$, *pour tous* $a, b, c \in \mathbb{N}$.

(4) Distributivité à droite : $a \cdot (b + c) = a \cdot b + a \cdot c$, *pour tous* $a, b, c \in \mathbb{N}$.

(5) Élément neutre : $n \cdot 1 = n = 1 \cdot n$, *pour tout* $n \in \mathbb{N}$.

(6) Intégrité : $a \cdot b = 0$ *si et seulement si* $a = 0$ *ou* $b = 0$.

(7) Simplification : $a \cdot b = a \cdot c$ *avec* $a \neq 0$ *implique* $b = c$.

Indication de démonstration. Les preuves s'effectuent essentiellement par récurrence. Pour alléger ce cours polycopié, elles ne seront pas présentées en détail. □

3. Relation d'ordre sur les entiers naturels

Un aspect intuitif extrêmement important des nombres entiers, c'est qu'ils *croissent indéfiniment*, au fur et à mesure qu'on emploie l'application de successeur $s(\bullet)$. Il en découle que les entiers naturels $n \in \mathbb{N}$ peuvent être *ordonnés* d'une manière naturelle. Et la théorie de Peano est capable d'élaborer le concept d'*ordre* à partir des axiomes.

Définition 3.1. Soient deux entiers $p, q \in \mathbb{N}$. On dit que q *est supérieur ou égal à* p, et on écrit $q \geqslant p$, s'il existe $n \in \mathbb{N}$ tel que $q = n + p$.

On dit que q *est strictement supérieur à* p, et on écrit $q > p$, si on a $q \geqslant p$ avec de plus $q \neq p$.

Évidemment, on peut aussi définir les relations d'infériorité $\leqslant$ et d'infériorité stricte $<$, en écrivant $p \leqslant q$ si et seulement si $q \geqslant p$, ainsi que $p < q$ si et seulement si $q > p$.

Proposition 3.2. *La relation* $\geqslant$ *entre les entiers est une relation d'ordre, c'est-à-dire que pour tous* $p, q, r \in \mathbb{N}$, *elle satisfait les propriétés suivantes.*

(1) Réflexivité : *on a* $p \geqslant p$ *pour tout* $p \in \mathbb{N}$.

(2) Antisymétrie : *si* $q \geqslant p$ *et* $p \geqslant q$, *alors* $q = p$.

(3) Transitivité : *si* $r \geqslant q$ *et* $q \geqslant p$, *alors* $r \geqslant p$.

Indication de preuve. Cela résulte aussitôt des propriétés de l'addition (exercice). □

Voici maintenant des propriétés élémentaires connues qui seront extrêmement utiles dans de nombreuses démonstrations ultérieures de ce cours.

Proposition 3.3. **(1)** Ordre total : *Si* p, q *sont deux entiers quelconques, alors on a* $p \geqslant q$ *ou* $q \geqslant p$.

(2) Simplification : *Pour tous* $a, b, c \in \mathbb{N}$, *on a l'équivalence :* $a + b \geqslant a + c \iff b \geqslant c$.

(3) *Il n'existe pas d'entier* $n_* \in \mathbb{N}$ *tel que* $0 < n_* < 1$.

(4) *Il n'existe pas d'entier* $r^* \in \mathbb{N}$ *qui soit supérieur ou égal* $r^* \geqslant m$ *à tous les entiers* $m \in \mathbb{N}$.

(5) *Si* $q \geqslant p$, *alors* $n \cdot q \geqslant n \cdot p$, *pour tout* $n \in \mathbb{N}$.

À nouveau, les étudiants sont invités à « sauter » la lecture de cette démonstration. Mais ils doivent quand même se concentrer avec intensité pour construire leur compréhension intuitive de cette proposition.

Démonstration. **(1)** Pour p fixé, introduisons l'ensemble :

$$E_p := \big\{q \in \mathbb{N} \colon\ q \leqslant p \text{ ou } q \geqslant p\big\},$$

et montrons que cet ensemble E_p est égal à $\mathbb{N}$ tout entier, en utilisant l'Axiome **(A3)**. D'abord, 0 est dans E_p, car on a $0 \leqslant p$, c'est-à-dire $p \geqslant 0$, puisque par la Définition 3.1, on peut écrire $p = p + 0$

Ensuite, si q est dans E_p, deux cas sont à considérer.

Premier cas $q < p$. Autrement dit, $p = n+q$ avec $n \neq 0$, c'est-à-dire $n = s(m) = m+1$ avec $m \in \mathbb{N}$. On a alors $p = m + 1 + q = m + s(q)$, donc encore (par définition) $s(q) \leqslant p$. Ainsi, $s(q) \in E_p$.

Deuxième cas : $q \geqslant p$. Autrement dit $q = n + p$ avec $n \in \mathbb{N}$ par définition, donc $s(q) = q + 1 = n + 1 + p = (n + 1) + p$, et on a donc $s(q) \geqslant p$. Ainsi, $s(q) \in E_p$.

(2) Utiliser la définition de $\geqslant$ et la règle de simplification (laissé au lecteur).

(3) Par l'absurde, supposons qu'il existe un tel entier $0 < n_* < 1$. L'inégalité stricte $n_* < 1$ signifie par définition qu'il existe $p \neq 0$ avec $1 = n_* + p$. Comme p est non nul, il existe q tel que $p = s(q) = q + 1$, et on a donc $1 = n_* + q + 1$. Par simplification, on en déduit $0 = n_* + q$, donc $n_* = 0$ (et aussi $q = 0$) d'après la Proposition 2.6 **(4)**. Ceci contredit $0 < n_*$, et finit l'argumentation.

(4) Ce dernier point est aisé, en considérant r^* et son successeur (exercice).

(5) C'est une conséquence calculatoire (aussi laissée au lecteur) des définitions de $\cdot$ et de $\geqslant$. □

Au-delà de l'ensemble $\mathbb{N}$, on peut introduire le concept abstrait d'*ordre*.

Définition 3.4. Soit F un ensemble quelconque. Un *ordre partiel* sur F est une relation binaire, notée $\leqslant$, qui est réflexive, antisymétrique, et transitive :

(1) Réflexivité : $x \leqslant x$, pour tout $x \in F$;

(2) Antisymétrie : $x \leqslant y$ et $y \leqslant x$ impliquent $x = y$, pour tous $x, y \in F$;

(3) Transitivité : $x \leqslant y$ et $y \leqslant z$ impliquent $x \leqslant z$, pour tous $x, y, z \in F$.

L'ordre partiel $\leqslant$ est dit être un *ordre total* lorsque, de plus :

(4) Totalité : Deux éléments quelconques $x \in F$ et $y \in F$ sont toujours comparables, c'est-à-dire qu'on a $x \leqslant y$ ou $y \leqslant x$.

Il est clair que l'ordre $\leqslant$ sur $\mathbb{N}$ est total, d'après la Proposition 3.3 **(1)**.

Définition 3.5. Sur un ensemble F, un ordre $\leqslant$ est dit être un *bon ordre* si tout sous-ensemble non vide E de F possède un *plus petit élément*, c'est-à-dire un élément $m_* \in E$ tel que :

$$m_* \leqslant n \qquad (\forall\, n \in E).$$

Si $(F, \leqslant)$ est bien ordonné, alors $\leqslant$ est nécessairement un ordre total. En effet, l'ensemble $\{x, y\}$ possède un plus petit élément, donc on a $x \leqslant y$ ou $y \leqslant x$.

4. Élément minimal et élément maximal

Terminons cette présentation de l'ensemble $\mathbb{N}$ des entiers naturels par deux énoncés intuitivement évidents, mais qui possèderont une importance capitale dans les démonstrations ultérieures de la théorie arithmétique. La première assertion exprime que $\leqslant$ est un *bon ordre* sur $\mathbb{N}$.

Théorème 4.1. *Tout sous-ensemble non vide E contenu dans $\mathbb{N}$ possède un plus petit élément, c'est-à-dire un élément $m_* \in E$ tel que :*

$$m_* \leqslant n \qquad (\forall\, n \in E).$$

Il importe de faire remarquer ici que E peut tout à fait incorporer une infinité d'éléments.

Démonstration. Il revient au même de montrer que si E est un sous-ensemble de $\mathbb{N}$ qui n'a pas de plus petit élément, alors $E = \emptyset$ est vide.

Pour cela, introduisons la propriété :

$$P(n)\colon \quad i \notin E, \text{ pour tout } i \leqslant n.$$

Nous affirmons que $P(0)$ est vraie. Sinon, si $P(0)$ était fausse, *i.e.* si $i \in E$ pour au moins un $i \leqslant 0$, c'est-à-dire pour $i = 0$, d'où $0 \in E$, et alors 0 serait le plus petit élément de E, puisque 0 est le plus petit élément de $\mathbb{N}$.

Ensuite, supposons $P(n)$ et montrons $P(n+1)$. On sait qu'aucun des entiers $0, 1, \ldots, n$ n'est dans E, et il s'agit de voir que $n+1$ n'est pas non plus dans E. Mais sinon, si $n+1$ appartenait à E, il serait forcément le plus petit élément de E, contrairement à notre hypothèse.

Donc par récurrence, $P(n)$ est vraie pour tout $n \in \mathbb{N}$, donc $i \notin E$ pour tout $i \in \mathbb{N}$, donc $E = \emptyset$, ce qui termine l'argumentation. □

La deuxième assertion, au contraire, n'accepte pas une infinité d'éléments.

Théorème 4.2. *Tout sous-ensemble* fini *non vide E contenu dans $\mathbb{N}$ possède un plus grand élément, c'est-à-dire un élément $r^* \in E$ tel que :*

$$n \leqslant r^* \qquad (\forall\, n \in E).$$

Quand E possède un nombre *infini* d'éléments, la conclusion est en générale fausse — penser par exemple à $E := \mathbb{N}$, qui n'a *pas* de plus grand élément, d'après la Proposition 3.3 **(4)**.

Démonstration. Raisonnons par récurrence sur le cardinal $n := \mathsf{Card}\, E$ de E. Si $n = 1$, autrement dit s'il n'y a qu'un seul élément dans E, alors cet élément est bel et bien le plus grand !

Supposons que tout sous-ensemble E' de $\mathbb{N}$ de cardinal n possède un plus grand élément, et soit E contenu dans $\mathbb{N}$ de cardinal $n+1$. Grâce au Théorème 4.1, il existe un élément m_* qui est le plus petit parmi les éléments de E. Introduisons $E' := E \backslash \{m_*\}$. Comme $\mathsf{Card}\, E' = n$, l'hypothèse de récurrence s'applique, donc E' possède un plus grand élément, disons r^*, qui est évidemment aussi le plus grand élément de E. □

L'énoncé suivant, intéressant sur le plan logique, peut être laissé de côté en première lecture, car il ne sera pas utilisé dans la suite du cours.

Théorème 4.3. *Le principe de récurrence est équivalent à la propriété de bon ordre, c'est-à-dire qu'on a équivalence entre :*

(i) *$P(0)$ est vraie et $P(n) \Longrightarrow P(n+1)$ quel que soit n entraînent que $P(n)$ est vraie pour tout $n \in \mathbb{N}$;*

(ii) *Tout sous-ensemble E de $\mathbb{N}$ possède un plus petit élément.*

Démonstration. La démonstration du Théorème 4.1 a déjà fait voir l'implication **(i)** $\Longrightarrow$ **(ii)**, comme on peut s'en convaincre en la relisant.

Pour démontrer **(ii)** $\Longrightarrow$ **(i)**, on raisonne par l'absurde en supposant que $P(n)$ n'est pas vraie pour tous les entiers n, et on introduit l'ensemble des contre-exemples :

$$E := \big\{n \in \mathbb{N} \colon\ P(n) \text{ n'est pas vraie}\big\}.$$

Ainsi, E est non vide.

Par conséquent, l'hypothèse **(ii)** garantit que E possède un plus petit élément m_*, qui est donc le contre-exemple minimal. On $m_* \neq 0$, car $P(0)$ est vraie par hypothèse. On considère alors $m_* - 1$, qui est encore dans $\mathbb{N}$, car $m_* > 0$, et qui est $< m_*$, donc n'est plus dans E, puisque m_* est le plus petit élément de E. Il s'ensuit que $P(m_* - 1)$ est vraie. Mais alors, comme on suppose que $P(n) \Longrightarrow P(n+1)$ quel que soit n, on doit forcément avoir que $P(m_*)$ est vraie, ce qui est une contradiction dans notre raisonnement.

En définitive, $E = \emptyset$ doit être vide, ce qui équivaut à **(i)** — terminé ! □

5. Anneau $\mathbb{Z}$ des entiers relatifs

L'ensemble $\mathbb{N}$ des entiers naturels, muni de l'addition, a un défaut : étant donné un entier quelconque $n \in \mathbb{N}$, il n'existe la plupart du temps *aucun* entier $m \in \mathbb{N}$ tel que :

$$n + m \ = \ 0.$$

Autrement dit, il n'existe pas d'opération *inverse* de l'addition.

À la fin du XIX$^{\text{ième}}$ siècle, les mathématiques abstraites et structurales, ont introduit la notion de *groupe commutatif*, que nous étudierons ultérieurement dans ce cours. Donnons-en toutefois la définition.

Définition 5.1. Un *groupe commutatif* est un ensemble G muni d'une relation binaire interne notée $(\bullet) * (\bullet)$ qui satisfait :

Associativité : $x * (y * z) = (x * y) * z$, pour tous $x, y, z \in G$;

Commutativité : $x * y = y * x$, pour tous $x, y \in G$;

Élément neutre : il existe un élément $e \in G$ tel que $e * x = x = x * e$, pour tout $x \in G$;

Existence d'un inverse : pour tout $x \in G$, il existe un unique élément $x' \in G$ tel que $x * x' = e = x' * x$.

Dans $\mathbb{N}$, l'opération $* \ = \ +$ est l'addition (commutative), l'élément neutre est $e = 0$. Mais *aucun* $n \in \mathbb{N}$ avec $n \neq 0$ n'admet un *inverse* n' pour l'addition, à savoir un n' satisfaisant $n + n' = 0 = n' + n$, à cause de la Proposition 2.6 **(4)**. Il s'agit là d'un défaut majeur de $\mathbb{N}$.

On a cependant une soustraction partielle.

Lemme 5.2. *Étant donné deux entiers $m, n \in \mathbb{N}$ avec $n \leqslant m$, il existe un unique entier p tel que $n + p = m$. On note alors $p = m - n$.*

Démonstration. Ceci est une reformulation de la Définition 3.1 même de la relation d'ordre ! □

L'objectif est maintenant de « plonger » $\mathbb{N}$ dans un ensemble plus « gros » $\mathbb{Z}$ pour lequel la soustraction $m - n$ entre deux entiers quelconques aura toujours un sens. La construction la plus naturelle de $\mathbb{Z}$ consiste simplement à adjoindre à tous les éléments $n \in \mathbb{N}$ leurs *opposés* $-n$. Autrement dit, à un entier, on va associer un signe.

On pose :

$$\mathbb{N}^* := \mathbb{N}\backslash\{0\} = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ \dots\},$$

et on définit $\mathbb{Z}$ comme la réunion de $\mathbb{N}$ et d'une copie de $\mathbb{N}^*$, notée $-\mathbb{N}^*$:

$$\mathbb{Z} := -\mathbb{N}^* \cup \mathbb{N}.$$

Les éléments de $-\mathbb{N}^*$ seront notés $-n$, avec $n \in \mathbb{N}^*$. Pour le moment, ce signe $-$ est juste une notation formelle, car on n'a pas encore démontré qu'il correspond à l'opération *inverse* de l'addition.

On parlera des entiers de $\mathbb{N}$ comme des entiers *positifs*, et des entiers de $-\mathbb{N}^*$ comme des entiers *négatifs*.

Définition 5.3. La *valeur absolue* $|\bullet|$ d'un élément de $\mathbb{Z} = -\mathbb{N}^* \cup \mathbb{N}$ est :

- $|-n| := n$ pour tout $-n \in -\mathbb{N}^*$;
- $|n| := n$ pour tout $n \in \mathbb{N}$.

La définition de l'addition est alors bien naturelle et correspond bien à ce qu'on souhaite au final.

Définition 5.4. Sur $\mathbb{Z} = -\mathbb{N}^* \cup \mathbb{N}$, on définit une addition comme suit.

- Pour $m, n \in \mathbb{N}$, la somme $m + n$ est prise au sens de $\mathbb{N}$.
- Pour $-m$ et $-n$ appartenant à $-\mathbb{N}^*$, on pose $(-m) + (-n) := -(m+n)$.
- Pour m dans $\mathbb{N}$ et $-n$ dans $-\mathbb{N}^*$, il y a deux sous-cas :

  ☐ lorsque $m < n$, d'où $n = m+p$ pour un entier unique p de $\mathbb{N}^*$, on pose $m+(-n) := -p = -(n-m)$.

  ☐ lorsque $m \geqslant n$, d'où $m+q = n$ pour un entier unique q de $\mathbb{N}$, on pose $m+(-n) := q$.
- Pour $-m$ dans $-\mathbb{N}^*$ et n dans $\mathbb{N}$, afin de définir $(-m) + n$, on procède de manière symétrique au cas précédent.

En réfléchissant sur ce dernier cas symétrique, on se convainc aisément (exercice de réflexion) que cette définition rend *commutative* l'addition $+$ dans $\mathbb{Z}$.

Théorème 5.5. *Muni de la loi $+$, l'ensemble $\mathbb{Z} = -\mathbb{N}^* \cup \mathbb{N}$ est un groupe commutatif, d'élément neutre $0 \in \mathbb{N}$, et dans lequel l'opposé, pour l'addition, d'un entier $n \in \mathbb{N}$ avec $n \neq 0$ est $-n \in -\mathbb{N}^*$, tandis que l'opposé de $-n$ est n.*

Cet énoncé justifie donc la notation $-n$, comme opposé de n, avec un signe $-$. Observons que $-(-n) = n$. Aux étudiants, il est conseillé de sauter la lecture de la démonstration, un peu aride et ardue.

Indication de démonstration. Seule l'associativité est non évidente, et nécessite de distinguer de nombreux cas. Il s'agit de montrer, pour tous $a, b, c \in \mathbb{Z}$, que l'on a $(a+b)+c = a+(b+c)$. Lorsque $a, b, c \in \mathbb{N}$, c'est l'associativité connue dans $\mathbb{N}$. Mais il y a des cas plus délicats.

Détaillons par exemple un cas « difficile », celui où a et b sont dans $\mathbb{N}$, tandis que $c = -d$ est dans $-\mathbb{N}^*$. Hélas, il faut encore distinguer trois sous-cas de figure.

(1) : $d \leqslant b$. On a donc $b = d+e$ avec $e \in \mathbb{N}$, et donc $e = b-d$, d'où aussi $a+b = d+(a+e)$, ce qui montre $d \leqslant a+b$. Par définition, on a :

$$a + (b+c) \ = \ a + (b-d) \ = \ a+e,$$

et il s'agit de faire voir que ceci est égal à $(a+b)+c=(a+b)-d$, autrment dit qu'on a $d+(a+e)=a+b$. Mais, vu l'égalité $b=d+e$, cela résulte des propriétés de l'addition dans $\mathbb{N}$.

(2) : $b<d\leqslant a+b$. Cette fois, on a $d=b+e$ et $a+b=d+f$, avec $e,f\in\mathbb{N}$. On en déduit $d+f=b+e+f=a+b$, d'où $a=e+f$, ce qui montre $e\leqslant a$. Alors on a $(a+b)+c=(a+b)+(-d)=f$ ainsi que $a+(b+c)=a+\big(b+(-d)\big)=a+(-e)=f$, d'où le résultat.

(3) : $a+b<d$. On a $d=a+b+e$, d'où $d-b=a+e$. On calcule alors $(a+b)+c=(a+b)+(-d)=-e$, puis $a+(b+c)=a+\big(b+(-d)\big)=a+\big(-(a+e)\big)=-e$.

Les autres cas se traitent de manière analogue, et nous nous dispenserons de les détailler. □

Ensuite, il s'agit de donner un sens à la multiplication dans $\mathbb{Z}$, *i.e.* de la *prolonger* de $\mathbb{N}$ à $\mathbb{Z}$.

Définition 5.6. La multiplication $a\cdot b$ entre deux éléments $a,b\in\mathbb{Z}$ est définie comme suit.

- Pour $a,b\in\mathbb{N}$, la multiplication $a\cdot b$ est prise au sens de $\mathbb{N}$.
- Pour $a\in\mathbb{N}$ et $b=-c$ dans $-\mathbb{N}^*$, on pose $a\cdot(-c):=-(a\cdot c)$.
- Symétriquement, pour $a=-c$ dans $-\mathbb{N}^*$ et $b\in\mathbb{N}$, on pose $(-c)\cdot b:=-(c\cdot b)$.
- Enfin, pour $a=-c$ dans $-\mathbb{N}^*$ et $b=-d$ dans $-\mathbb{N}^*$, on pose $(-c)\cdot(-d):=c\cdot d$.

De manière équivalente, la multiplication entre deux entiers est définie par la multiplication entre leurs valeurs absolues, et par la « *règle des signes* » :

□ $+$ fois $+$ égale $+$;

□ $+$ fois $-$ égale $-$;

□ $-$ fois $+$ égale $-$;

□ $-$ fois $-$ égale $+$.

Théorème 5.7. *Sur $\mathbb{Z}$, l'opération de multiplication $(\bullet)\cdot(\bullet)$ est associative, est commutative, a pour élément neutre 1, et est distributive à gauche et à droite par rapport à l'addition $(\bullet)+(\bullet)$.*

Autrement dit, la multiplication de $\mathbb{Z}$ hérite de toutes les propriétés dont elle jouissait sur $\mathbb{N}$, telles qu'énoncées dans la Proposition-Définition 2.9. À nouveau, il est conseillé de sauter la lecture de la démonstration.

Indication de démonstration. Pour toutes ces propriétés, il s'agit simplement d'effectuer une vérification directe, mais qui est parfois technique.

Contentons-nous de détailler un des cas nécessaires concernant la distributivité, en montrant la formule :

$$a\cdot\big(b+(-d)\big)\;=\;(a\cdot b)+\big(a\cdot(-d)\big),$$

où $a,b\in\mathbb{N}$ et $-d\in-\mathbb{N}^*$ sont quelconques. Hélas, il faut distinguer deux sous-cas.

(1) : $b<d$. On a donc $d=b+e$ avec $e\in\mathbb{N}$, d'où $a\cdot\big(b+(-d)\big)=a\cdot(-e)=-a\cdot e$. Mais on a par ailleurs $a\cdot d=a\cdot b+a\cdot e$, d'où le calcul conclusif :

$$a\cdot b+a\cdot(-d)\;=\;a\cdot b+(-a\cdot d)\;=\;-a\cdot e\;=\;a\cdot\big(b+(-d)\big).$$

(2) : $b \geqslant d$. On a donc $b = d + e$ avec $e \in \mathbb{N}$, d'où $b + (-d) = e$. Il s'agit de montrer :

$$a \cdot \big(b + (-d)\big) \;=\; a \cdot e \;\stackrel{?}{=}\; a \cdot b + \big(-(a \cdot d)\big),$$

ce qui revient à $a \cdot e + a \cdot b \stackrel{?}{=} a \cdot b$, et qui n'est autre que la distributivité (connue) dans $\mathbb{N}$. □

Quelle que soit la méthode employée pour construire $\mathbb{Z}$ et pour détailler tous les arguments des démonstrations, on obtient au final le résultat capital suivant.

Théorème 5.8. *Muni de ses deux lois* $(\bullet) + (\bullet)$ *d'addition et* $(\bullet) \cdot (\bullet)$ *de multiplication, l'ensemble* $\mathbb{Z} = -\mathbb{N}^* \cup \mathbb{N}$ *est un anneau commutatif.* □

Mais au fait — qu'entend-on ici par *anneau commutatif ?* Heureusement, les mathématiciens ont inventé la

Définition 5.9. [Anneau] Un *anneau commutatif* est un ensemble $\mathbb{A}$ muni de deux opérations internes, appelées *addition* et *multiplication*, notées en général $+$ et $\cdot$ (ou parfois $\times$), qui se comportent exactement comme celles $+$ et $\cdot$ de l'ensemble $\mathbb{Z}$ des entiers relatifs.

Plus précisément, toutes les conditions suivantes doivent être satisfaites.

Addition :

Associativité de l'addition : $a + (b + c) = (a + b) + c$, quels que soient $a, b, c \in \mathbb{A}$.

Commutativité de l'addition : $a + b = b + a$, quels que soient $a, b \in \mathbb{A}$.

Élément neutre pour l'addition : Il existe un élément spécial noté $0 \in \mathbb{A}$ satisfaisant $0 + a = a = a + 0$, quel que soit $a \in \mathbb{A}$.

Existence d'un inverse pour l'addition : Pour tout $a \in \mathbb{A}$, il existe un élément unique, noté $-a \in \mathbb{A}$, tel que $a + (-a) = 0 = (-a) + a$.

Multiplication :

Associativité de la multiplication : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, quels que soient $a, b, c \in \mathbb{A}$.

Commutativité de la multiplication : $a \cdot b = b \cdot a$, quels que soient $a, b \in \mathbb{A}$.

Élément neutre pour la multiplication : Il existe un élément spécial noté $1 \in \mathbb{A}$ satisfaisant $1 \cdot a = a = a \cdot 1$, quel que soit $a \in \mathbb{A}$.

Distributivité de la multiplication par rapport à l'addition :

Distributivité à gauche : $(a + b) \cdot c = a \cdot c + b \cdot c$, quels que soient $a, b, c \in \mathbb{A}$.

Distributivité à droite : $a \cdot (b + c) = a \cdot b + a \cdot c$, quels que soient $a, b, c \in \mathbb{A}$.

On parle alors de l'anneau commutatif $\big(\mathbb{A}, +, \cdot, 0, 1\big)$.

Il est important de faire observer qu'on ne demande *pas* ici l'existence d'un inverse pour la multiplication. D'ailleurs, dans $\mathbb{Z}$ lui-même, la plupart des nombres n'ont *pas* d'inverse multiplicatif, par exemple :

$$\frac{1}{25} \;=\; 0,04,$$

n'est *pas* un nombre entier !

La notion d'*anneau* est donc moins riche de structure que celle de *corps*.

Définition 5.10. [Corps] Un *corps* commutatif $\mathbb{K}$ est un anneau commutatif satisfaisant la condition supplémentaire suivante.

Existence d'un inverse pour la multiplication : Pour tout $x \in \mathbb{K}$, il existe un élément unique, noté $x^{-1} \in \mathbb{K}$, tel que $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.

Par exemple, l'ensemble $\mathbb{Q} = \left\{ \frac{p}{q} :\ p \in \mathbb{Z},\ q \in \mathbb{N}_{\geqslant 1} \right\}$ des nombres *rationnels* est un corps. Mais dans ce chapitre, nous ne travaillerons qu'avec des *anneaux*, tels que $\mathbb{Z}$, ou $\mathbb{Z}/n\mathbb{Z}$ — à découvrir plus tard.

Il est temps maintenant d'introduire la relation d'ordre naturel sur $\mathbb{Z}$.

Définition 5.11. Étant donné deux entiers $m, n \in \mathbb{Z}$, on dit que $m \leqslant n$ est *inférieur ou égal* à n si $(-m) + n$ appartient à $\mathbb{N}$, et on dit que $m < n$ est strictement inférieur à n si on a de plus, $(-m) + n \geqslant 1$ — dans $\mathbb{N}$.

Comme sur $\mathbb{N}$, on peut aussi définir sur $\mathbb{Z}$ les relations duales de supériorité $\geqslant$ et de supériorité stricte $>$, lesquelles sont bien connues.

Nous ne détaillerons pas la démonstration de la proposition suivante, qui liste plusieurs propriétés de compatibilité entre les opérations algébriques et la relation d'ordre sur $\mathbb{Z}$. Les étudiants doivent vraiment apprendre et maîtriser cette proposition, car elle sera souvent utilisée dans les démonstrations du cours et dans les examens.

Proposition 5.12. [Importante] *Soient des entiers m, n, a, b, c dans $\mathbb{Z}$.*

(1) $m \geqslant 0$ *et* $n \geqslant 0$ *impliquent* $m + n \geqslant 0$ *et* $m \cdot n \geqslant 0$.

(2) $a \leqslant x \leqslant b$ *implique* $-b \leqslant -x \leqslant -a$.

(3) $a \leqslant x \leqslant b$ *et* $c \leqslant y \leqslant d$ *impliquent* $a + c \leqslant x + y \leqslant b + d$.

(4) $a \leqslant b$ *implique* $a + c \leqslant b + c$, *quel que soit le signe de* c.

(5) $0 \leqslant a \leqslant b$ *et* $0 \leqslant c$ *impliquent* $0 \leqslant a\,c \leqslant b\,c$.

(6) $0 \leqslant a \leqslant b$ *et* $c \leqslant 0$ *impliquent* $b\,c \leqslant a\,c \leqslant 0$ — *Attention ! a et b changent de place !*

(7) $a \in \mathbb{Z}$ *avec* $a \neq 0$ *implique* $|a| \geqslant 1$. □

Terminons cette présentation de l'anneau $\mathbb{Z}$ des entiers relatifs par trois énoncés qui sont des conséquences assez directes des Théorèmes 4.1 et 4.2.

Théorème 5.13. **(1)** *Tout sous-ensemble non vide* fini E *contenu dans $\mathbb{Z}$ possède un plus petit élément* et *un plus grand élément, c'est-à-dire deux éléments $m_* \in E$ et $r^* \in E$ avec $m_* \leqslant r^*$ tels que :*

$$m_* \ \leqslant\ n \ \leqslant\ r^* \qquad (\forall\, n \in E).$$

(2) *Tout sous-ensemble non vide* minoré E *de $\mathbb{Z}$, c'est-à-dire tel qu'il existe* $\mathrm{J} \in \mathbb{Z}$ *avec* $\mathrm{J} \leqslant n$ *pour tout $n \in E$, admet un plus petit élément $m_* \in E$, satisfaisant :*

$$m_* \ \leqslant\ n \qquad (\forall\, n \in E).$$

(3) *Tout sous-ensemble* majoré E *de $\mathbb{Z}$, c'est-à-dire tel qu'il existe* $\mathrm{K} \in \mathbb{Z}$ *avec* $n \leqslant \mathrm{K}$ *pour tout $n \in E$, admet un plus grand élément $r^* \in E$, satisfaisant :*

$$n \ \leqslant\ r^* \qquad (\forall\, n \in E).$$

Démonstration. Laissée au lecteur, sachant que le plus important est de se construire des *intuitions mentales et/visuelles* au sujet de **(1)**, **(2)**, **(3)**. □

6. Division à l'École élémentaire

Soit $\mathbb{Z}$ l'anneau des nombres entiers naturels positifs ou négatifs, et soit $\mathbb{N} = \mathbb{Z}_+ \subset \mathbb{Z}$ le sous-ensemble des entiers qui sont positifs.

Diviser *avec reste* un entier $a \geqslant 1$ par un entier $1 \leqslant b \leqslant a$ qui lui est inférieur, cela consiste à trouver un *quotient* entier $q \geqslant 0$ et un *reste* entier $r \geqslant 0$ tels que :

$$a \;=\; q\,b + r,$$

le quotient q étant maximal possible, de telle sorte que dans le reste r, on ne puisse plus extraire « du b » :

$$0 \leqslant r \leqslant b - 1.$$

Il est bien connu que diviser avec reste est toujours possible, le couple $(q, r) \in \mathbb{N} \times \mathbb{N}$ étant alors déterminé de manière unique en partant de $a \geqslant 1$ et de b avec $1 \leqslant b \leqslant a$ quelconques.

Exemple 6.1. Comme à l'école élémentaire, soit à diviser $a = 126$ par $b = 35$:

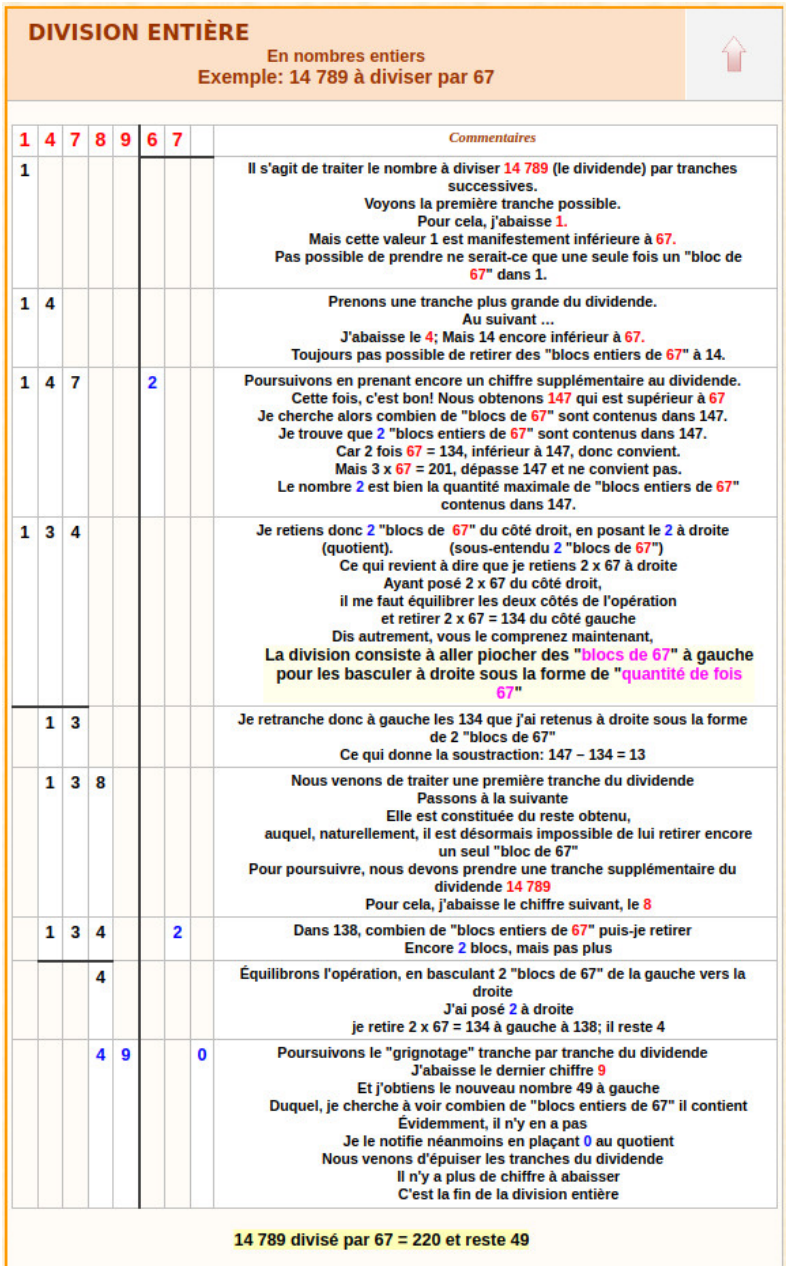
$$\begin{array}{r|l} 126 & 35 \\ \cline{2-2} -\,105 & 3 \\ 21 & \end{array}$$

Mentalement, on essaie de multiplier 35 successivement par 1, 2, 3, 4, et on trouve que $3 \times 35 = 105$ est le résultat maximum qui demeure inférieur à 126. On reporte alors $-\,105$ à gauche, on soustrait $126 - 105 = 21$, et on trouve :

$$\underbrace{126}_{a} \;=\; \underbrace{3}_{q} \cdot \underbrace{35}_{b} + \underbrace{21}_{r}.$$

Cet exemple s'inscrit dans un contexte général, connu depuis la Préhistoire sur Terre, sur Mars, sur Jupiter, sur Vénus, et sans doute aussi sur quelques exoplanètes dotées de mathématiques encore embryonnaires.

Voici un exemple plus élaboré.



DIVISION ENTIÈRE

En nombres entiers

Exemple: 14 789 à diviser par 67

1	4	7	8	9	6	7		*Commentaires*
1								Il s'agit de traiter le nombre à diviser 14 789 (le dividende) par tranches successives. Voyons la première tranche possible. Pour cela, j'abaisse 1. Mais cette valeur 1 est manifestement inférieure à 67. Pas possible de prendre ne serait-ce que une seule fois un "bloc de 67" dans 1.
1	4							Prenons une tranche plus grande du dividende. Au suivant ... J'abaisse le 4; Mais 14 encore inférieur à 67. Toujours pas possible de retirer des "blocs entiers de 67" à 14.
1	4	7			2			Poursuivons en prenant encore un chiffre supplémentaire au dividende. Cette fois, c'est bon! Nous obtenons 147 qui est supérieur à 67 Je cherche alors combien de "blocs de 67" sont contenus dans 147. Je trouve que 2 "blocs entiers de 67" sont contenus dans 147. Car 2 fois 67 = 134, inférieur à 147, donc convient. Mais 3 x 67 = 201, dépasse 147 et ne convient pas. Le nombre 2 est bien la quantité maximale de "blocs entiers de 67" contenus dans 147.
1	3	4						Je retiens donc 2 "blocs de 67" du côté droit, en posant le 2 à droite (quotient). (sous-entendu 2 "blocs de 67") Ce qui revient à dire que je retiens 2 x 67 à droite Ayant posé 2 x 67 du côté droit, il me faut équilibrer les deux côtés de l'opération et retirer 2 x 67 = 134 du côté gauche Dis autrement, vous le comprenez maintenant, La division consiste à aller piocher des "blocs de 67" à gauche pour les basculer à droite sous la forme de "quantité de fois 67"
	1	3						Je retranche donc à gauche les 134 que j'ai retenus à droite sous la forme de 2 "blocs de 67" Ce qui donne la soustraction: 147 – 134 = 13
	1	3	8					Nous venons de traiter une première tranche du dividende Passons à la suivante Elle est constituée du reste obtenu, auquel, naturellement, il est désormais impossible de lui retirer encore un seul "bloc de 67" Pour poursuivre, nous devons prendre une tranche supplémentaire du dividende 14 789 Pour cela, j'abaisse le chiffre suivant, le 8
	1	3	4			2		Dans 138, combien de "blocs entiers de 67" puis-je retirer Encore 2 blocs, mais pas plus
			4					Équilibrons l'opération, en basculant 2 "blocs de 67" de la gauche vers la droite J'ai posé 2 à droite je retire 2 x 67 = 134 à gauche à 138; il reste 4
			4	9			0	Poursuivons le "grignotage" tranche par tranche du dividende J'abaisse le dernier chiffre 9 Et j'obtiens le nouveau nombre 49 à gauche Duquel, je cherche à voir combien de "blocs entiers de 67" il contient Évidemment, il n'y en a pas Je le notifie néanmoins en plaçant 0 au quotient Nous venons d'épuiser les tranches du dividende Il n'y a plus de chiffre à abaisser C'est la fin de la division entière

14 789 divisé par 67 = 220 et reste 49

7. Divisibilité dans $\mathbb{Z}$

On commence par introduire une relation fondamentale entre les nombres entiers, quel que soit leur signe.

Définition 7.1. Soient deux entiers $a, b \in \mathbb{Z}$. On dit que a *divise* b s'il existe $u \in \mathbb{Z}$ tel que :

$$a\,u \;=\; b.$$

Dans ce cas, on dit que a *est un diviseur de* b, ou que b est un multiple de a. Cette propriété sera notée :

$$a \,|\, b.$$

Mais au fait, que se passe-t-il lorsque $a = 0$ ou $b = 0$? On sait qu'avec le nombre 0, il est souvent « aventureux », voire « interdit » de toucher au « bouton rouge » de la division !

En effet, avec $a = 0$ et pour $b \neq 0$, écrire que « 0 divise b », c'est-à-dire précisément que $0\,u = b$, semblerait impliquer que $u = \frac{b}{0}$ — Aïe ! On diviserait par 0 !

Observation 7.2. *Avec $b \in \mathbb{Z}$, la propriété $0 \mid b$ est impossible sauf lorsque $b = 0$.*

Démonstration. Avec $a = 0$, si $a\,u = b$, certainement $0\,u = 0 = b$. On confirme donc bien qu'un entier *non nul* $b \neq 0$ ne peut *jamais* être divisible par 0 — Ouf ! Toutes les mathématiques connues jusqu'à présent restent préservées et cohérentes ! □

Dans l'autre sens, tout se passe bien.

Observation 7.3. *On a toujours $a \mid 0$, quel que soit l'entier $a \in \mathbb{Z}$.*

Démonstration. Avec $b = 0$, il suffit de prendre $u := 0$ pour trouver effectivement $a\,0 = 0$. □

Heureusement, dans toutes les considérations qui suivront, nous n'aurons presque jamais à nous préoccuper de ces subtilités concernant les cas $a = 0$ et $b = 0$ dans le symbole binaire $a \mid b$. Presque toujours, lorsqu'on écrira $a \mid b$, il sera clair en fonction du contexte que $a \neq 0$ et $b \neq 0$.

Quelques exemples numériques simples de $a \mid b$:

$$2 \mid 4, \qquad 5 \mid -625, \qquad 17 \mid 323, \qquad -2 \mid 20,$$

semblent montrer que a est toujours plus petit que b. Mais il faut aussi tenir compte du fait que $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ peuvent être négatifs. La valeur absolue doit intervenir, et pour un nombre réel $x \in \mathbb{R}$ quelconque, rappelons-en la définition :

$$|x| := \mathsf{max}\big\{ -x,\ x \big\}.$$

Par exemple $|-19| = 19$. Intuitivement, la valeur absolue efface le signe $-$ des nombres négatifs.

Lemme 7.4. *Si $a \mid b$ avec $b \neq 0$, alors $|a| \leqslant |b|$.*

Démonstration. En effet, si $a \mid b$, il existe par définition $u \in \mathbb{Z}$ tel que $a\,u = b$. Comme b est non nul, u est non nul aussi — sinon, si $u = 0$ était nul, on aurait $a\,0 = 0 = b$. Comme u est un entier, on a $1 \leqslant |u|$, et donc :

$$\begin{aligned} |a| \;=\; |a| \cdot 1 \;&\leqslant\; |a| \cdot |u| \\ &=\; \big|a \cdot u\big| \\ &=\; |b|. \end{aligned}$$

□

Lemme 7.5. *Si $a \mid b$ et $b \mid a$, alors $b = \pm a$.*

Démonstration. Distinguons deux cas : $b = 0$, puis $b \neq 0$.

Premier cas : $b = 0$. On suppose donc $a \mid 0$ (toujours vrai) et $0 \mid a$. Mais nous venons de voir dans l'Observation 7.2 que cela force $a = 0$. Donc $a = 0 = b$, et on a bien $0 = \pm 0$.

Deuxième cas : $b \neq 0$, en supposant toujours $a \mid b$ et $b \mid a$. Autrement dit, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que :

$$a\,u \;=\; b \qquad\qquad \text{et} \qquad\qquad b\,v \;=\; a.$$

Mais alors, en multipliant la deuxième identité par u (en vert), on peut calculer :

$$\begin{aligned} &\big(b\,v \;=\; a\big)\,u \\ &b\,v\,u \;=\; a\,u \;=\; b, \end{aligned}$$

puis soustraire et factoriser :

$$b\,\big(v\,u-1\big)\;=\;0,$$

pour déduire ensuite, *puisque b est supposé non nul*, que :

$$v\,u\;=\;1.$$

En particulier, on en déduit que u et v sont tous deux non nuls. De plus, u et v doivent être de même signe, car $v\,u>0$.

Assertion 7.6. *On a $u=\pm 1$.*

Démonstration. Premier cas : u et v sont strictement positifs. Alors, comme ce sont des entiers, on a $u\geqslant 1$ et $v\geqslant 1$, d'où :

$$1\;\leqslant\;u\;\leqslant\;v\,u\;=\;1,$$

puis $u=1$ par encadrement entre deux gendarmes n°1.

Deuxième cas : u et v sont strictement négatifs. Alors $-u$ et $-v$ sont strictement positifs, satisfont aussi $(-v)(-u)=1$, donc le premier cas s'applique, et il donne $-u=1$, c'est-à-dire $u=-1$. □

En conclusion, puisque $u=\pm 1$, on a bien $a\,(\pm 1)=b$, ce qui était annoncé. □

Lemme 7.7. *Si $a\,|\,b$, alors pour tous entiers $k\in\mathbb{Z}$ et $\ell\in\mathbb{Z}$, on a aussi :*

$$a\,\Big|\,\big(k\,a+\ell\,b\big)$$

Démonstration. En effet, $a\,u=b$ implique que le nouveau nombre entier $B:=k\,a+\ell\,b$ est aussi multiple de a :

$$\begin{aligned}B\;=\;k\,a+\ell\,b\;&=\;k\,a+\ell\,a\,u\\&=\;a\,\big(\underbrace{k+\ell\,u}_{=:\,U\,\in\,\mathbb{Z}}\big),\end{aligned}$$

et cette égalité $a\,U=B$ exprime précisément que $a\,|\,B$. □

Même si cela paraît un peu stupide, observons que l'on a toujours :

$$a\,|\,a,$$

simplement parce que $a\,1=1$. Ensuite, énonçons la propriété de *transitivité* de la divisibilité.

Lemme 7.8. *Si $a\,|\,b$ et $b\,|\,c$, alors $a\,|\,c$.*

Démonstration. En effet :

$$\begin{array}{l}\big(a\,u\;=b\big)\,v\\\qquad b\,v\;=\;c\end{array}\qquad\text{implique}\qquad a\,\underbrace{u\,v}_{=:\,w}\;=\;b\,v\;=\;c$$

et cette égalité $a\,w=c$ exprime précisément que $a\,|\,c$. □

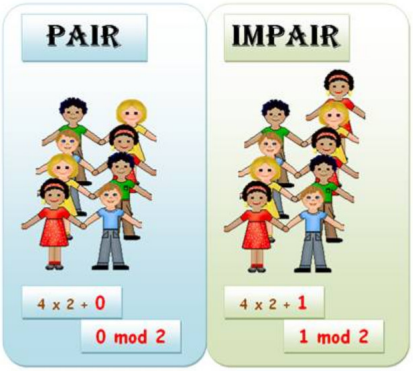
8. Idée de congruence et de périodicité dans le monde réel

Je connais ce domaine sans le savoir

Quand à l'école primaire vous avez fait connaissance avec les nombres pairs et impairs vous faisiez du calcul modulo 2 sans en connaître le nom.

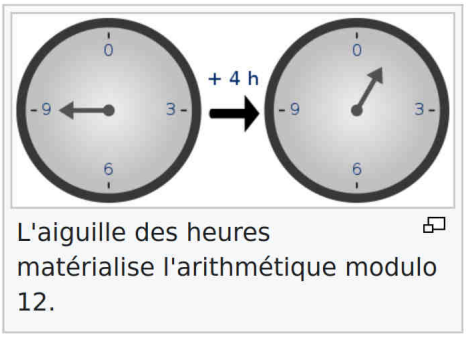
- un nombre pair est un nombre égal 0 modulo 2: divisé par 2 son reste est nul.
- un nombre impair est un nombre égal 1 modulo 2: divisé par 2 son reste est égal à 1.

Modulo est un mot qui signifie que l'on met en rang par 3, 4, ... n ...
En fait, une généralisation des nombres pairs et impairs.



8 est pair et 8 = 0 mod 2
9 est impair et 9 = 1 mod 2

Voici un autre exemple : l'« arithmétique de l'horloge », qui se réfère à l'« addition » des heures indiquées par la petite aiguille d'une horloge.



L'aiguille des heures matérialise l'arithmétique modulo 12.

Concrètement, si nous commençons à 9 heures et travaillons pendant 4 heures, alors plutôt que de terminer à 13 heures (comme dans l'addition normale), nous sommes à 1 heure. De la même manière, si nous commençons à minuit et nous attendons 7 heures trois fois de suite, nous nous retrouvons à 9 heures (au lieu de 21 heures).

Fondamentalement, quand nous atteignons 12, nous recommençons à zéro ; nous travaillons « *modulo 12* ». Pour reprendre l'exemple précédent, on dit que « *9 et 21 sont congrus modulo 12* ».

Les nombres 9, 21, 33, 45, *etc.* sont considérés comme égaux lorsqu'on travaille modulo 12.

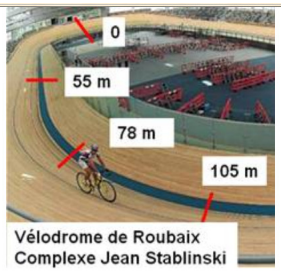
Plus généralement, l'« *arithmétique modulaire* » est un système arithmétique d'entiers modifiés, où les nombres sont « abaissés » lorsqu'ils atteignent une certaine valeur.

Imaginez un vélodrome avec un anneau de 250 m de long. Ce cycliste sait qu'en dix minutes il fait toujours un peu plus de vingt tours, mais il veut comparer ses records. Tous les jours, lorsque le chrono marque 10 minutes, il note de combien il dépasse: 55 m puis 78 m et aujourd'hui, c'est 105 m. Il vient de battre son record!

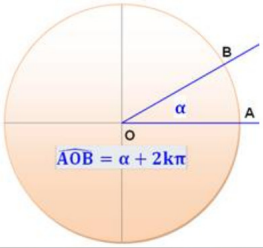
Ce cycliste fait un calcul en modulo sans le savoir.

En trigonométrie, seul l'angle sur le cercle compte. Le nombre tours que pourrait faire cet angle ne nous intéresse pas. Il peut tourner cent fois, mille fois ... on s'en fiche!

On dit que l'angle est connu à $2k\pi$ près; on aurait pu dire: modulo 2π.



Vélodrome de Roubaix
Complexe Jean Stablinski



En arithmétique, la congruence sur les entiers est une relation d'équivalence entre les entiers. Elle fut pour la première fois étudiée en tant que structure mathématique par le mathématicien allemand Carl Friedrich Gauss à la fin du XVIII$^{\text{ième}}$ siècle, dans un traité célèbre publié en 1801 et intitulé *Disquisitiones Arithmeticæ*. La congruence est aujourd'hui couramment utilisée en théorie des nombres, en algèbre générale, et en cryptographie.

C'est une arithmétique où l'on ne raisonne pas directement sur les nombres, mais sur leurs restes respectifs par la division euclidienne par un certain entier : le *module*.

9. Congruence modulo un entier

Définition 9.1. Soit un entier naturel $n \geqslant 1$. Deux entiers $a, b \in \mathbb{Z}$ sont dits *congrus modulo* n si leur différence $a - b$ est un multiple de n :

$$a \equiv b \mod n \quad \overset{\text{def}}{\Longleftrightarrow} \quad \exists\, k \in \mathbb{Z} \qquad a - b = k\,n,$$

ou, de manière équivalente, si $a - b$ est divisible par n.

On notera que le symbole nouveau introduit ici avec trois traits horizontaux :

$$\equiv$$

est distinct du signe d'égalité $=$. Mais du point de vue définitionnel, ce symbole $\equiv$ de congruence repose sur le signe $=$ d'égalité :

$$\begin{array}{rl} \text{lire} & a \equiv b \mod n \\ \text{traduire} & a = b + k\,n \quad (\exists\, k \in \mathbb{Z}). \end{array}$$

Mentalement et intuitivement, il faudra toujours avoir à l'esprit qu'il existe toujours un « entier k caché » derrière le symbole $\equiv$. Et nous verrons bientôt pourquoi ce « k », il est très souvent préférable de le « cacher ».

Question 9.2. *Pourquoi ne pas définir la congruence $a \equiv b \bmod n$ aussi pour des entiers $n \leqslant -1$?*

On pourrait tout à fait définir la congruence avec un $n \leqslant -1$, mais comme :

$$a - b \,=\, k\,n \qquad\qquad \Longleftrightarrow \qquad\qquad a - b \,=\, (-k)\,(-n),$$

on aurait l'équivalence :

$$a \,\equiv\, b \mod n \qquad\qquad \Longleftrightarrow \qquad\qquad a \,\equiv\, b \mod (-n),$$

et donc, la congruence modulo un $n \leqslant -1$ se ramènerait à la congruence modulo $-n \geqslant 1$.

Question 9.3. *Pourquoi ne pas définir aussi la congruence modulo $n = 0$?*

Si, cela aurait du sens ! Mais cela serait inutile, car on retrouverait la notion connue d'égalité :

$$a - b \,=\, k\,0 \,=\, 0 \qquad\qquad \Longleftrightarrow \qquad\qquad a \,=\, b.$$

En définitive, dans la Définition 9.1, il est justifié de prendre des entiers $n \geqslant 1$.

Question 9.4. *À quoi ressemble la congruence modulo un entier n lorsque $n = 1$?*

Avec $n = 1$, par définition, deux entier $a, b \in \mathbb{Z}$ sont congrus modulo 1 s'il existe $k \in \mathbb{Z}$ tel que :

$$a - b \,=\, k \cdot 1.$$

Mais il suffit alors de prendre $k := a - b$ pour satisfaire cette égalité ! Donc deux entiers a et b quelconques sont toujours congrus entre eux modulo 1 ! Incroyable ! En particulier, tout entier a est congru à 0 modulo 1 :

$$a - 0 \,=\, a \cdot 1 \qquad\qquad \text{(prendre } k := a\text{)}.$$

Fait 9.5. [Peu intéressant] *Modulo $n = 1$, tous les entiers $a, b, c, d, e, \cdots \in \mathbb{Z}$ sont congrus entre eux, et congrus à 0.* □

Par conséquent, la notion de congruence modulo un entier n ne commence à être intéressante que pour $n \geqslant 2$.

D'ailleurs pour $n = 2$, par définition, deux entiers $a, b \in \mathbb{Z}$ sont congrus modulo 2 s'il existe $k \in \mathbb{Z}$ tel que :

$$a - b \,=\, k \cdot 2.$$

Et comme $2\,k \,\in\, 2\,\mathbb{Z}$ est un nombre *pair*, a et b sont congrus modulo 2 si et seulement si ils sont tous les deux pairs, ou tous les deux impairs. En base 10, comment fait-on pour différencier les nombres impairs des nombres pairs (de chaussettes) ?

Ensuite, au-delà de $n = 2$, voici deux exemples simples. Modulo 3, on a :

$$35 \equiv 2 \mod 3 \qquad \text{car} \qquad 35 = 2 + 11 \cdot 3.$$

Modulo 7, on a :

$$26 \equiv 12 \mod 7 \qquad \text{car} \qquad 26 - 12 = 2 \cdot 7.$$

Proposition 9.6. *Pour tout entier $n \geqslant 1$, et tout entier relatif $a \in \mathbb{Z}$, on a :*

$$a \equiv 0 \mod n \qquad \Longleftrightarrow \qquad a \text{ est multiple de } n.$$

Démonstration. En effet, $a - 0 = k\,n$ si et seulement si $a = k\,n$. □

La proposition suivante est importante, elle montre que le symbole binaire $\bullet \equiv \bullet \mod n$ se comporte comme l'égalité $\bullet = \bullet$.

Proposition 9.7. *Pour tout entier $n \geqslant 1$, la relation binaire $\bullet \equiv \bullet \mod n$ est une relation d'équivalence.*

(1) Réflexivité : $a \equiv a \mod n$, *quel que soit* $a \in \mathbb{Z}$.

(2) Symétrie : $a \equiv b \mod n$ *équivaut à* $b \equiv a \mod n$, *quels que soient* $a, b \in \mathbb{Z}$.

(3) Transitivité : $a \equiv b \mod n$ *et* $b \equiv c \mod n$ *entraîne* $a \equiv c \mod n$, *quels que soient* $a, b, c \in \mathbb{Z}$.

Démonstration. **(1)** Il est clair que $a - a = 0 = 0\,n$, avec $k = 0$.

(2) On a :

$$a - b = k\,n \qquad \Longleftrightarrow \qquad b - a = (-k)\,n.$$

(3) Effectivement :

$$\begin{aligned} a - b &= k\,n, \\ b - c &= \ell\,n, \end{aligned}$$

impliquent par addition verticale :

$$a - \underline{b}_{\circ} + \underline{b}_{\circ} - c = (k + \ell)\,n, \qquad \text{c'est-à-dire} \qquad a - c = j\,n. \qquad \square$$

On voit bien que l'entier k dans la Définition 9.1 change, puisqu'il devient ici $j := k + \ell$.

Une autre proposition importante garantit une *compatibilité* de la congruence $\bullet \equiv \bullet \mod n$ avec les opérations d'addition et de multiplication, c'est-à-dire de *compatibilité* avec la structure d'*anneau* de $\big(\mathbb{Z}, +, \times\big)$. Juste avant d'exposer de nombreux exemples concrets, intuitifs, et instructifs, cette compatibilité nous permettra de définir les *anneaux quotients* $\mathbb{Z}/n\mathbb{Z}$, qui constituent les domaines fondamentaux de l'*arithmétique modulaire*.

Proposition 9.8. *Pour tout entier $n \geqslant 1$ et tous entiers relatifs $a, b, a', b' \in \mathbb{Z}$ avec :*

$$\begin{aligned} a &\equiv b \mod n, \\ a' &\equiv b' \mod n, \end{aligned}$$

on a :

$$\begin{aligned} a + a' &\equiv b + b' \mod n, \\ a \cdot a' &\equiv b \cdot b' \mod n. \end{aligned}$$

Démonstration. En effet :

$$\begin{aligned} a &= b + k\,n, \\ a' &= b' + k'\,n, \end{aligned}$$

impliquent par addition et par multiplication verticales :

$$\begin{aligned} a + a' &= b + b' + (k + k')\,n, \\ a\,a' &= (b + k\,n)\,(b' + k'\,n) = b\,b' + \big(b\,k' + k\,b' + k\,k'\,n\big)\,n. \end{aligned}$$

À nouveau, l'entier k de la Définition 9.1 *change de visage*, il devient $k+k'$ pour l'addition, et $bk' + kb' + kk'n$ pour la multiplication. □

Et justement nous allons comprendre au fur et à mesure de notre progression que tout l'intérêt du calcul arithmétique modulo n est d'« oublier » volontairement ces entiers k qui peuvent devenir de plus en plus compliqués.

Théoriquement, on devrait employer des notations spécifiques pour l'addition et la multiplication modulo n, par exemple :

$$\overset{\mathsf{mod}}{+} \qquad \text{et} \qquad \overset{\mathsf{mod}}{\times},$$

mais pour des raisons de simplicité, tous les mathématiciens ré-utilisent la même notation $+$ et $-$ que dans $\mathbb{Z}$, en conservant à l'esprit que leur sens devient différent dans $\mathbb{Z}\backslash n\,\mathbb{Z}$, *i.e.* quand on travaille modulo n.

Ainsi en travaillant par exemple modulo 6, on écrira $3 + 2 \equiv 5 \mod 6$, et aussi $4 + 2 \equiv 0 \mod 6$, car la somme de 4 et 2 est égale à $1 \cdot 6$.

Modulo $n = 6$, on peut alors construire les deux tables d'opérations suivantes.

Table d'addition dans $\mathbb{Z}/6\mathbb{Z}$

+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Table de multiplication dans $\mathbb{Z}/6\mathbb{Z}$

×	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

10. Anneaux $\big(\mathbb{Z}/n\mathbb{Z}, +, \times\big)$

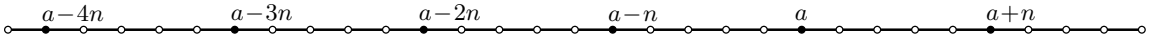
Nous pouvons maintenant introduire les domaines fondamentaux de l'arithmétique modulaire : les anneaux $\big(\mathbb{Z}/n\mathbb{Z}, +, \times\big)$. Quelques préliminaires s'avèrent nécessaires.

Proposition 10.1. *On fixe un entier $n \geqslant 2$. Alors modulo n, pour tout entier $a \in \mathbb{Z}$, il existe un entier a' tel que :*

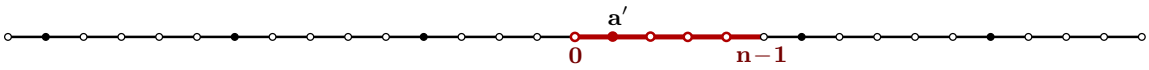
(1) $0 \leqslant a' \leqslant n - 1$*;*

(2) $a' \equiv a \mod$.

Autrement dit, tout entier relatif est toujours congru modulo n à au moins un entier $a' \in \big\{0, 1, 2, \ldots, n-2, n-1\big\}$.



Intuitivement, l'ensemble de tous les entiers $a' = a + k\,n$ congrus à a modulo n se représente comme une suite doublement infinie d'entiers situés à distance n l'un de l'autre.



L'intervalle entier :

$$[\![0,\, n-1]\!] = \{0, 1, 2, \ldots, n-2, n-1\},$$

étant de longueur (entière) égale à n, il existe forcément un nombre $a' = a + k\,n$ qui « tombe » dans cette « marmite » $[\![1, n-1]\!]$.

Démonstration. Donnons des arguments directs, simples, intuitifs. Pour tout entier $\mathrm{M} \in \mathbb{Z}$, l'entier $a + \mathrm{M}\,n$, est congru à a modulo n. En prenant $\mathrm{M} \gg 1$ positif assez grand, on peut garantir que $a + \mathrm{M}\,n \geqslant 0$. Donc on peut supposer depuis le début que $a \geqslant 0$.

Si $0 \leqslant a \leqslant n-1$, alors $a' := a$ convient.

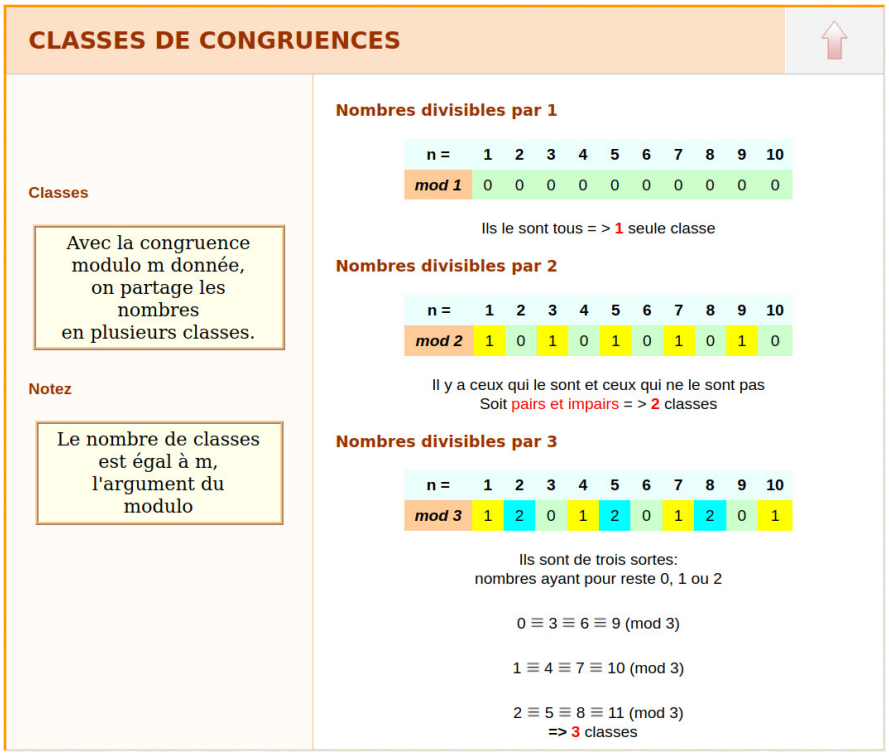
Sinon, $n \leqslant a$. Alors $a_1 := a - n$ est congru à a modulo n, et satisfait $0 \leqslant a_1$. Si $0 \leqslant a_1 \leqslant n-1$, alors $a' := a_1$ convient.

Sinon, $n \leqslant a_1$. Alors $a_2 := a_1 - n = a - 2\,n$ est congru à a modulo n, et satisfait $0 \leqslant a_2$. Si $0 \leqslant a_2 \leqslant n-1$, alors $a' := a_2$ convient.

Et ainsi de suite.

Puisque la suite $a_2 = a - 2\,n$, puis $a_3 = a - 3\,n$, *etc.*, tend vers $-\infty$, on ne peut pas toujours avoir $n \leqslant a_k = a - 2\,k$, et donc, il y a forcément un moment où $a' = a - 2\,k$, avec un certain $k \geqslant 0$, satisfera $0 \leqslant a' \leqslant n-1$. Cela achève la démonstration. □

Cette Proposition 10.1 importante sera aussi une conséquence de la division euclidienne classique, dont nous verrons plus tard une version élaborée dans la Section **17**.



Ensuite, il est intuitivement clair qu'à tout entier $a \in \mathbb{Z}$ est associé un *unique* entier $a' \equiv a \bmod n$ avec $a' \in \{0, 1, 2, \ldots, n-2, n-1\}$.

Proposition 10.2. *On fixe un entier $n \geqslant 2$. Alors modulo n, les entiers :*

$$0, \quad 1, \quad 2, \quad \ldots, \quad n-2, \quad n-1,$$

sont mutuellement distincts, i.e. *aucun n'est congru à un autre.*

Démonstration. Soient donc deux tels entiers a et a' *distincts*, *i.e.* $a \neq a'$, avec :

$$\begin{aligned} 0 \leqslant a \leqslant n-1, \\ 0 \leqslant a' \leqslant n-1. \end{aligned}$$

En multipliant la deuxième ligne par -1, le sens des inégalités s'inverse (ou la gauche s'échange avec la droite) :

$$\begin{aligned} 0 \leqslant \quad a \leqslant n-1, \\ -(n-1) \leqslant \quad -a' \leqslant 0. \end{aligned}$$

Ensuite, par addition verticale, on obtient :

$$-(n-1) \leqslant a - a' \leqslant n-1,$$

et enfin en prenant la valeur absolue :

$$\big|a - a'\big| \leqslant n-1. \tag{10.3}$$

Raisonnons par l'absurde. Si a et a' étaient congrus l'un à l'autre modulo n, c'est-à-dire si on avait :

$$a - a' = k \cdot n,$$

pour un certain entier $k \in \mathbb{Z}$, alors k serait non nul car on suppose $a \neq a'$, donc on aurait $|k| \geqslant 1$, donc en prenant la valeur absolue, on aurait :

$$\begin{aligned} \big|a - a'\big| &= |k| \cdot n \\ &\geqslant 1 \cdot n, \end{aligned}$$

ce qui contredirait (10.3). En conclusion, deux entiers distincts :

$$a, a' \in \{0, 1, 2, \ldots, n-2, n-1\}$$

ne peuvent jamais être congrus l'un à l'autre modulo n. □

Définition 10.4. L'ensemble « quotient [7] » de $\mathbb{Z}$ par la relation d'équivalence :

$$a \sim b \qquad \Longleftrightarrow \qquad a \equiv b \bmod n,$$

sera noté :

$$\mathbb{Z}/n\mathbb{Z}.$$

La *classe d'équivalence* d'un entier $a \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, sera notée :

$$\overline{a} := \{a' \in \mathbb{Z} \colon\ a' \equiv a \bmod n\}.$$

7. Cette notion mathématique quelque peu abstraite sera définie en détail ultérieurement dans un cadre très général.

On peut alors définir l'addition et la multiplication entre classes par :

$$\begin{aligned} \overline{a} + \overline{b} &:= \overline{a+b}, \\ \overline{a} \cdot \overline{b} &:= \overline{a \cdot b}, \end{aligned}$$

puis on peut vérifier, en utilisant la Proposition 9.8, que tout cela a du sens, mais ce point de vue n'est pas très pratique, car avec chaque classe $\overline{a}$, on manipule en fait simultanément une infinité de nombres $a' = a + k\,n$ congrus à a modulo n. Avec un unique symbole tel que $\overline{a}$, on préfèrerait en fait manipuler un seul objet à la fois, simple et concret.

Heureusement, il existe un meilleur point de vue. Grâce à la Proposition 10.1 et à la Proposition 10.2, nous savons qu'il existe une application de « *projection* » :

$$\begin{aligned} \pi\colon \quad \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ a &\longmapsto \text{unique } a' \in \big\{0,\, 1,\, 2,\, \ldots,\, n-2,\, n-1\big\} \\ &\qquad \text{tel que } a' \equiv a \mod n. \end{aligned}$$

On peut donc :

identifier $\quad \mathbb{Z}/n\mathbb{Z} \quad$ à $\quad \big\{0,\, 1,\, 2,\, \ldots,\, n-2,\, n-1\big\} \mod n.$

De plus, grâce à la Proposition 9.8, nous pouvons écrire pour tous $a, b \in \mathbb{Z}$:

$$\begin{aligned} \pi\big(a+b\big) &= \pi\big(\pi(a) + \pi(b)\big), \\ \pi\big(a \cdot b\big) &= \pi\big(\pi(a) \cdot \pi(b)\big), \end{aligned}$$

ce que nous pouvons expliquer concrètement au moyen des deux recettes suivantes concernant l'addition et la multiplication entre deux nombre quelconques :

$$a,\, b \,\in\, [\![0,\, n-1]\!] \,=\, \mathbb{Z}/n\mathbb{Z}.$$

Recette 10.5. [Addition dans $\mathbb{Z}/n\mathbb{Z}$] *Faire l'addition classique $a + b$ dans $\mathbb{Z}$, puis soustraire $a + b - k \cdot n$ avec le bon entier k pour « tomber » dans l'intervalle $[\![0, n-1]\!]$.*

L'opération de projection $\pi(\bullet)$, c'est justement la soustraction du bon multiple $k \cdot n$ de n à chaque étape de calcul. Pour additionner comme nous l'avons écrit plus haut, il faut d'ailleurs soustraire le bon $k \cdot n$ *trois fois*, d'abord pour avoir $\pi(a)$ et $\pi(b)$ dans $[\![0,\, n-1]\!]$, puis surtout, il faut ré-appliquer la projection $\pi\big(\pi(a) + \pi(b)\big)$, car l'addition $\pi(a) + \pi(b)$ peut « faire sortir de la marmite » $[\![0,\, n-1]\!]$.

Par exemple, avec $n := 17$, de telle sorte que :

$$\mathbb{Z}/17\mathbb{Z} \,=\, \big\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16\big\} \mod 17,$$

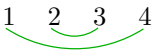
si on veut additionner $7 + 13 = 20$, en soustrayant $1 \cdot 17$ on trouve $20 - 1 \cdot 17 = 3$ qui appartient bien à $[\![0, 16]\!]$, et donc :

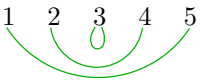
$$7 + 13 \,=\, 3 \qquad (\text{dans } \mathbb{Z}/17\mathbb{Z}).$$

Parfois, on « reste dans la marmite » :

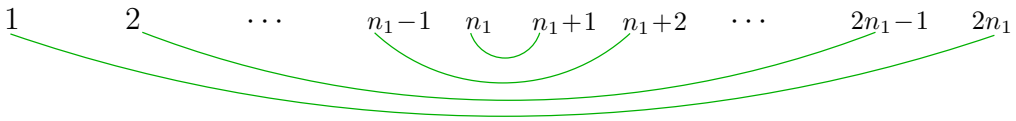
$$2 + 3 \,=\, 5 \qquad (\text{dans } \mathbb{Z}/17\mathbb{Z}).$$

Pour l'addition, chaque élément $a \in \mathbb{Z}/n\mathbb{Z}$ possède l'inverse $a' := n - a$, puisque $a + (n - a) \equiv 0 \mod n$. On peut représenter les paires d'inverses additifs modulo n, d'abord dans $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$, puis dans $\mathbb{Z}/6\,\mathbb{Z}$:

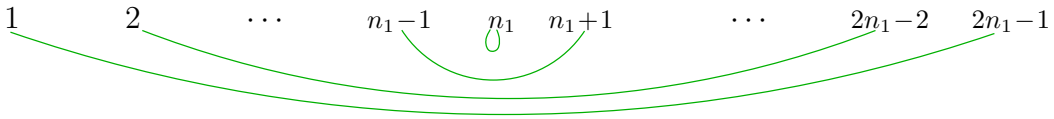




D'ailleurs, cette belle symétrie est valable généralement. Quand $n = 2\,n_1 + 1$ est *impair*, on peut représenter les paires d'inverses additifs comme suit :



et quand $n = 2\,n_1$ est pair, comme suit :



En revanche, pour la multiplication $\times$, il existe en général des éléments $a \in \mathbb{Z}/n\mathbb{Z}$ qui n'ont *pas* d'inverse multiplicatif.

*	**[0]**	**[1]**	**[2]**	**[3]**
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

En effet, la table de multiplication de $\mathbb{Z}/4\mathbb{Z}$ montre par exemple qu'*aucun* nombre $a' \bmod 4$ ne parvient à faire que $2 \times a' \equiv 1 \bmod 4$.

Recette 10.6. [Multiplication dans $\mathbb{Z}/n\mathbb{Z}$] *Faire la multiplication classique $a \cdot b$ dans $\mathbb{Z}$, puis soustraire $a \cdot b - \ell \cdot n$ avec le bon entier ℓ pour « tomber » dans l'intervalle $[\![0, n-1]\!]$.*

La même nécessité d'appliquer plusieurs fois $\pi(\bullet)$ concerne aussi la multiplication. Par exemple, toujours $n := 17$, puique l'on a dans $\mathbb{Z}$:

$$7 \cdot 13 \;=\; 91 \;=\; 6 + 5 \cdot 17,$$

il vient :

$$7 \cdot 13 \;=\; 6 \qquad \text{(dans } \mathbb{Z}/17\mathbb{Z}\text{)}.$$

Afin de différencier les nombres dans $\mathbb{Z}$ des nombres dans $\mathbb{Z}/n\mathbb{Z}$, certains auteurs mettent une barre au-dessus des nombres, par exemple en écrivant :

$$\mathbb{Z}/17\mathbb{Z} \;=\; \big\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6},\ \overline{7},\ \overline{8},\ \overline{9},\ \overline{10},\ \overline{11},\ \overline{12},\ \overline{13},\ \overline{14},\ \overline{15},\ \overline{16}\big\} \bmod 17,$$

de telle sorte :

$$\overline{7} + \overline{13} \;=\; \overline{3},$$
$$\overline{7} \cdot \overline{13} \;=\; \overline{6},$$

mais nous préférons ne mettre aucun signe supplémentaire, tout en précisant bien le domaine, $\mathbb{Z}$, ou $\mathbb{Z}/n\mathbb{Z}$, dans lequel on effectue les calculs.

Corollaire 10.7. *On a :*

$$\mathsf{Card}\,\mathbb{Z}/n\mathbb{Z} \;=\; n.$$

Démonstration. En effet, il y a précisément n nombres dans l'ensemble $\{0,\ 1,\ 2,\ \ldots,\ n-2,\ n-1\}$ de tous les $\pi(\bullet)$ possibles modulo n. □

En résumé, pour tout entier $n \geqslant 1$, le quotient :

$$\begin{aligned}\big(\mathbb{Z}/n\mathbb{Z},\ +,\ \times\big) &= \mathbb{Z} \text{ modulo } n\,\mathbb{Z} \\ &= \big\{0,\ 1,\ 2,\ 3,\ \ldots,\ n-1,\ n-1\big\} \bmod n\end{aligned}$$

représente l'ensemble des nombres entiers $a \in \mathbb{Z}$ identifiés lorsqu'ils diffèrent d'un multiple de n :

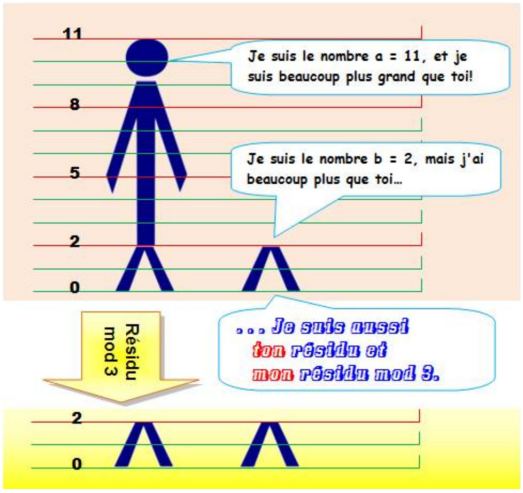
$$a \equiv a' \mod n \iff a - a' \text{ est divisible par } n.$$

Grâce à la Proposition 9.8, nous concluons que $\big(\mathbb{Z}/n\mathbb{Z}, +, \times\big)$ est un *anneau*, au sens abstrait de la Définition 5.9 déjà vue *supra*.

Théorème 10.8. *Pour tout entier (module) fixé $n \geqslant 1$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$, muni de ses deux lois d'addition et de multiplication modulo n :*

$$(\bullet) + (\bullet) \mod n, \qquad \textit{et} \qquad (\bullet) \cdot (\bullet) \mod n,$$

est un anneau commutatif. □



Terminologie 10.9. On fixe un entier $n \geqslant 2$. Pour tout entier $a \in \mathbb{Z}$, le *résidu de a modulo n* est l'entier unique $a' = \pi(a)$ tel que :

(1) $0 \leqslant a' \leqslant n-1$;

(2) $a' \equiv a \mod$.

Pour terminer cette section, donnons un exemple élémentaire d'application du calcul modulaire. Nous savons que modulo n, tout entier $a \in \mathbb{Z}$ est congru à exactement 1 entier parmi $\{0, 1, 2, \ldots, n-2, n-1\}$. Donc dans le cas $n = 3$, tout entier est congru ou bien à 0, ou bien à 1, ou bien à 2.

Proposition 10.10. *Pour tout entier $m \in \mathbb{Z}$, le produit $m(m+1)(m+2)$ est divisible par 3.*

Démonstration. Autrement dit, il s'agit de faire voir que :

$$m\,(m+1)\,(m+2) \equiv 0 \mod 3.$$

• Premier cas : $m \equiv 0 \mod 3$. Alors $m = 3\,m'$ est divisible par 3, avec $m' \in \mathbb{Z}$, donc $m(m+1)(m+2) = 3\,m'(m+1)(m+2)$ aussi.

• Deuxième cas : $m \equiv 1 \mod 3$. Alors $m+2 \equiv 0 \mod 3$, donc $m+2 = 3\,m'$ est divisible par 3, avec $m' \in \mathbb{Z}$, donc $m(m+1)(m+2) = m(m+1)\,3\,m'$ aussi.

• Troisième cas : $m \equiv 2 \mod 3$. Alors $m+1 \equiv 0 \mod 3$, donc $m+1 = 3\,m'$ est divisible par 3, avec $m' \in \mathbb{Z}$, donc $m(m+1)(m+2) = m\,3\,m'\,(m+2)$ aussi. □

D'une manière similaire, $m(m+1)(m+2)(m+3)$ est toujours divisible par 4 (exercice). Au fait, que peut-on dire de $m(m+1)$? Plus généralement, on peut démontrer (exercice) la

Proposition 10.11. *Pour tout entier $n \geqslant 1$, le produit $m(m+1)\cdots(m+n-1)$ est divisible par n.* □

11. Multiplication modulaire et exponentiation modulaire

Avant de présenter de nombreux exemples très instructifs concernant le *calcul modulaire*, énonçons et démontrons deux propositions concernant le comportement de la congruence $\equiv$ modulo n vis-à-vis de la multiplication.

Proposition 11.1. *Pour tout entier $n \geqslant 1$, pour tous entiers relatifs $a, b \in \mathbb{Z}$, et pour tout multiplicateur $c \in \mathbb{Z}$, on a :*

$$a \equiv b \mod n \qquad \Longrightarrow \qquad a\,c \equiv b\,c \mod n.$$

Démonstration. En effet :

$$\big(a = b + k\,n\big)\,c \qquad \text{devient} \qquad a\,c = b\,c + (k\,c)\,n. \qquad \square$$

L'exponentiation est une forme généralisé de multiplication.

Proposition 11.2. *Pour tout entier $n \geqslant 1$, pour tous entiers relatifs $a, b \in \mathbb{Z}$, et pour tout exposant entier $r \geqslant 0$ on a :*

$$a \equiv b \mod n \qquad \Longrightarrow \qquad a^r \equiv b^r \mod n$$

Démonstration. Pour $r = 0$, puisque $a^0 = 1 = b^0$, on a bien, d'une manière tautologique, $1 \equiv 1 \mod n$.

Pour $r \geqslant 1$, la formule du binôme de Newton nous permet de développer la puissance r-ième :

$$\big(a = b + k\,n\big)^r \qquad \text{devient} \qquad \begin{aligned} a^r \;=\; & b^r + \tbinom{r}{1}\, b^{r-1}\,(k\,n)^1 \\ & + \tbinom{r}{2}\, b^{r-2}\,(k\,n)^2 \\ & + \cdots\cdots\cdots\cdots \\ & + \tbinom{r}{r-1}\, b^1\,(k\,n)^{r-1} \\ & + \tbinom{r}{r}\, b^0\,(k\,n)^r, \end{aligned}$$

et comme dans la colonne verticale à droite tous les termes $(k\,n)^*$ sont à une puissance $* \geqslant 1$ au moins égale à 1, on peut factoriser le tout par n pour obtenir :

$$a^r = b^r + \Big\{ \underbrace{\tbinom{r}{1}\, b^{r-1}\,k^1 + \tbinom{r}{2}\, b^{r-2}\,k^2\,n^1 + \cdots + \tbinom{r}{r-1}\, b^1\,k^{r-1}\,n^{r-2} + \tbinom{r}{r}\, b^0\,k^r\,n^{r-1}}_{=:\ \text{nouvel entier } \kappa} \Big\}\, n,$$

ce qui donne une relation :

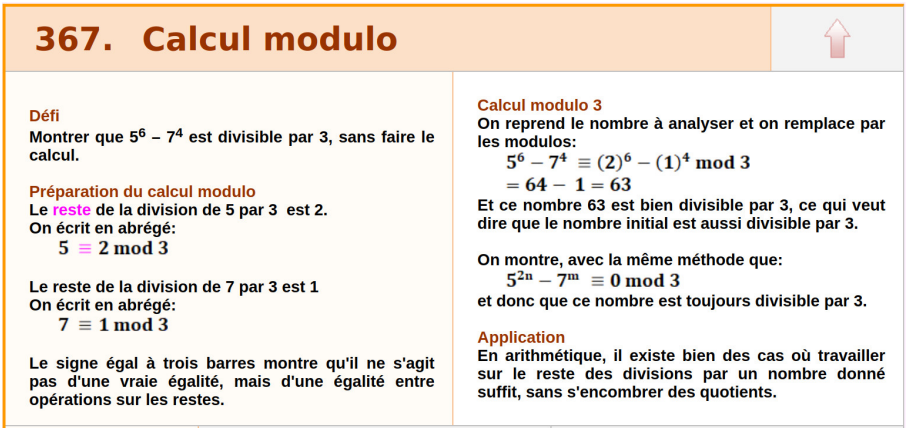
$$a^r \;=\; b^r + \mathrm{K}\, n,$$

exprimant bien que $a^r \equiv b^r \mod n$. □

On constate d'ailleurs manifestement dans ce dernier calcul que le fameux « entier k kaché » dans la relation de congruence peut absorber une complexité considérable de calculs annexes. Au travers de nombreux exemples « magiques » — et promis depuis bien longtemps —, nous allons enfin pouvoir vraiment dévoiler l'intérêt de « cacher » ces k intempestifs qui « explosent », et même mieux encore, nous allons montrer comment toujours s'épargner de nombreux calculs délicats.

« Neuf personnes sur dix aiment les mathématiques sans calculs », dit-on parfois en cours ou sur les bancs des écoles, et « La dizième *ment* », ajoute-t-on. Mais… rien n'est si sûr…, car dans les calculs se lovent toutes sortes de plaisirs gourmands et de découvertes impromptues.

12. Exemples de calculs modulo un entier



367. Calcul modulo

Défi
Montrer que $5^6 - 7^4$ est divisible par 3, sans faire le calcul.

Préparation du calcul modulo
Le reste de la division de 5 par 3 est 2.
On écrit en abrégé:
$5 \equiv 2 \bmod 3$

Le reste de la division de 7 par 3 est 1
On écrit en abrégé:
$7 \equiv 1 \bmod 3$

Le signe égal à trois barres montre qu'il ne s'agit pas d'une vraie égalité, mais d'une égalité entre opérations sur les restes.

Calcul modulo 3
On reprend le nombre à analyser et on remplace par les modulos:
$5^6 - 7^4 \equiv (2)^6 - (1)^4 \bmod 3$
$= 64 - 1 = 63$
Et ce nombre 63 est bien divisible par 3, ce qui veut dire que le nombre initial est aussi divisible par 3.

On montre, avec la même méthode que:
$5^{2n} - 7^m \equiv 0 \bmod 3$
et donc que ce nombre est toujours divisible par 3.

Application
En arithmétique, il existe bien des cas où travailler sur le reste des divisions par un nombre donné suffit, sans s'encombrer des quotients.

Question 12.1. *Étant donné un entier $m \in \mathbb{Z}$, peut-on l'écrire sous la forme $m = a^2 + b^2$, avec deux entiers relatifs a et b ?*

Par exemple, est-ce possible pour $m = 40\,003$? Une idée simple serait de tester toutes les sommes possibles $a^2 + b^2$ avec $a, b \leqslant \sqrt{40\,003}$, ce qui exigerait pas mal de calculs.

Mais une idée [8] plus astucieuse et plus économique consiste à examiner toutes les valeurs de carrés a^2 modulo 4, où $a \in \mathbb{Z}$ est quelconque, puis celles de $a^2 + b^2$ modulo 4.

En effet, tout entier a est congru modulo 4 à l'un des quatre nombres 0, 1, 2, 3. Donc a^2 est congru à 0^2, 1^2, 2^2, 3^3 modulo 4, c'est-à-dire à 0, 1, 0, 1 : il n'y a que deux valeurs possibles !

Par conséquent, une somme a^2+b^2 de deux carrés ne peut être congrue, modulo 4, qu'à :

$$0+0 \;\equiv\; 0, \qquad 0+1 \;\equiv\; 1, \qquad 1+1 \;\equiv\; 2,$$

c'est-à-dire à 0, 1, 2 : il n'y a que trois valeurs possibles !

8. On pourrait se demander : *Pourquoi le nombre 4, ici ?* Et la question est légitime.
En fait, l'Idée générale qui gouverne le calcul modulaire, c'est la possibilité de choisir divers *modules* $n \geqslant 1$, et de calculer modulo n afin de *contracter les calculs*. Si $n = 4$ ne marche pas, on essaie alors d'autres entiers $n = 5$, *etc.*, juste pour « tester », et souvent, cela finit par marcher.

Ainsi, la valeur 3 ne peut *jamais* être atteinte par une somme $a^2 + b^2$ de deux carrés entiers !

Et comme $40\,003 \equiv 3 \bmod 4$, nous concluons qu'il n'est *pas* représentable comme somme de deux carrés.

Nous n'avons pas complètement répondu à la Question 12.1, mais nous avons au moins trouvé une *méthode* pour obtenir un *critère négatif*.

Proposition 12.2. **(1)** *Aucun entier de la forme $3 + 4\,k$ ne peut être représenté comme somme de deux carrés.*
(2) *Aucun entier de la forme $7 + 8\,k$ ne peut être représenté comme somme de trois carrés.*

Démonstration. Il reste à traiter **(2)**. En raisonnant modulo 8, les valeurs des carrés 0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2 sont $0, 1, 4, 1, 0, 1, 4, 1$, c'est-à-dire $0, 1, 4$.

Si un entier $m = a^2 + b^2 + c^2$ est somme de trois carrés, ses valeurs modulo 8 ne peuvent être que :

$$0+0+0 \equiv 0,$$
$$0+0+1 \equiv 1, \qquad 0+0+4 \equiv 4,$$
$$0+1+1 \equiv 2, \qquad 0+4+4 \equiv 0, \qquad 1+1+4 \equiv 6,$$
$$1+1+1 \equiv 3, \qquad 4+4+4 \equiv 4, \qquad 1+4+4 \equiv 1, \qquad 0+1+4 \equiv 5,$$

donc *jamais* 7 modulo 8. En conclusion, aucun entier de la forme $7 + 8\,k$ ne peut être atteint. □

13. Contraction de calculs avec des grands nombres

Grand nombre ...

Démontrez que $N = 10^{1\text{ million}} + 10$ est divisible par 13

Avec 10, il manque 3 pour arriver à 13.	$10 \equiv -3 \bmod 13$
Élévation au carré. **Effectivement 100 = 7x13 + 9**	$100 \equiv 9 \bmod 13$
Poursuivons en prenant le cube.	$1000 \equiv -27 \bmod 13$ $\equiv (-13 - 13 - 1) \bmod 13$ $\equiv -1 \bmod 13$
Super! Car le 1, élevé à une puissance quelconque, donne toujours 1.	$(10^3)^k \equiv (-1)^k \bmod 13$
Pour approcher le million proposé en exposant.	$(10^3)^{333\,333} \equiv (-1)^{333\,333} \bmod 13$
L'exposant est impair, le signe moins est conservé.	$10^{999\,999} \equiv -1 \bmod 13$
En multipliant par 10.	$10^{1\,000\,000} \equiv (-1) \times (-3) \bmod 13$ $\equiv 3 \bmod 13$
Reste à ajouter 10 pour avoir N.	$N = 10^{1\,000\,000} + 10$ $\equiv (3 + 10) \bmod 13$ $\equiv 0 \bmod 13$ ■

Un peu d'astuce avec les grands nombres	
Calculer le reste de la division par 5 de 2009^{2009}	$2^{2009} \equiv x? \bmod 7$
On note que	$2^2 \equiv 4 \bmod 7$ $2^3 = 8 \equiv 1 \bmod 7$
Or, 2009 = 3 x 669 + 2	$2^{2009} = 2^{3\times 669+2} = (2^3)^{669} \times 2^2$ $\equiv 1^{669} \times 4 \equiv 4 \bmod 7$
Calculer le reste de la division par 5 de 2009^{2009}	$2009^{2009} \equiv x? \bmod 5$
On note que 2009 = 2010 – 1 avec 2010 divisible par 5	$2009 \equiv -1 \bmod 5$
Rapidement, on obtient:	$2009^{2009} \equiv (-1)^{2009} = -1 \equiv 4 \bmod 5$
Vérification par logiciel de calcul	$2009^{2009} \bmod 5;$ 4

14. Carrés modulo un entier

Fixons un module $n \geqslant 1$. Rappelons comment nous avons établi que tout entier $a \in \mathbb{Z}$ est congru, modulo n, à exactement un entier parmi $\{0, 1, 2, \ldots, n-2, n-1\}$. L'argument-clé, c'était que les entiers :

$$\ldots,\ a-2\,n,\ a-n,\ a,\ a+n,\ a+2\,n,\ \ldots,$$

se situaient à distance exactement n l'un à la suite de l'autre, et que l'intervalle entier $[\![0, n-1]\!]$ était une « marmite » de même longueur n. En raisonnant de manière similaire, on établit la

Proposition 14.1. *Modulo n, tout entier $a \in \mathbb{Z}$ est congru à un et à un seul entier a' tel que :*

$$-\tfrac{n}{2} < a' \leqslant \tfrac{n}{2}.$$

Démonstration. Observons que l'inégalité à gauche est stricte, et que $\frac{n}{2}$ n'est pas toujours entier. Pour être plus précis, il vaut mieux distinguer deux cas :

• $n = 2\,n_1$ est pair, d'où $\frac{n}{2} = n_1$, puis $-n_1 < a' \leqslant n_1$ désigne l'intervalle entier $[\![-n_1 + 1, n_1]\!]$, de longueur égale à $2\,n_1 = n$;

• $n = 2\,n_1 + 1$ est impair, d'où $\frac{n}{2} = n_1 + \frac{1}{2}$, puis $-n_1 - \frac{1}{2} < a' \leqslant n_1 + \frac{1}{2}$ désigne l'intervalle entier $[\![-n_1, n_1]\!]$, de longueur égale à $2\,n_1 + 1 = n$;

Dans les deux cas, l'intervalle entier $\frac{n}{2} < a' \leqslant \frac{n}{2}$ est de longueur précisément égale à n, donc l'argument-clé déjà vu de la « marmite de longueur n » s'applique. □

Notation 14.2. La *partie entière*, notée $\lfloor x \rfloor$, d'un nombre réel $x \in \mathbb{R}$ est l'unique entier $\lfloor x \rfloor \in \mathbb{Z}$ satisfaisant :

$$\lfloor x \rfloor \leqslant x < 1 + \lfloor x \rfloor,$$

par exemple, $\lfloor \frac{2n_1+1}{2} \rfloor = n_1$.

Par souci de symétrie, nous considérerons l'intervalle entier $[\![-\lfloor \frac{n}{2} \rfloor,\ \lfloor \frac{n}{2} \rfloor]\!]$, sans inégalité stricte à gauche, sachant que pour $n = 2\,n_1$ pair, cet intervalle contient $n + 1$ nombres

entiers au lieu de n attendus (une tomate de plus), et que pour $n = 2\,n_1 + 1$, il en contient n comme voulu.

Proposition 14.3. *Les carrés modulo n sont les résidus modulo n de 0^2, 1^2, 2^2, …, $\lfloor \frac{n}{2} \rfloor^2$.*

Autrment dit, pour connaître les valeurs des carrés modulo n, on peut diviser par 2 le travail.

Démonstration. En effet, soit donc a' avec :

$$-\lfloor \tfrac{n}{2} \rfloor \leqslant a' \leqslant \lfloor \tfrac{n}{2} \rfloor.$$

Pour $a' = 0, 1, 2, \ldots \lfloor \frac{n}{2} \rfloor$, on obtient bien les carrés indiqués. Pour $a' = -1, -2, \ldots, -\lfloor \frac{n}{2} \rfloor$, quand on prend un carré, son signe s'évanouit, car $(-1)^2 \equiv 1 \bmod n$, et donc, on obtient forcément les mêmes carrés. □

Par exemple, modulo 10, il suffit de calculer :

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 \equiv 4, \qquad 3^2 \equiv 9, \qquad 4^2 \equiv 6, \qquad 5^2 \equiv 5.$$

15. Nombres de Fermat

En 1758, Euler a découvert que le cinquième nombre de Fermat :

$$2^{2^5} + 1 \;=\; 4\,294\,967\,297,$$

inférieur, en euros, aux plus grandes fortunes de France protégées de l'impôt avec le consentement des législateurs, n'est *pas* un nombre premier, et qu'il est divisible par :

$$641 \,\Big|\, 2^{2^5} + 1.$$

Pour voir cela de la manière la plus économique qui soit, Euler se propose un petit entraînement (échauffement) qui consiste à calculer — à la main ! — le nombre :

$$7^{160},$$

et Euler commence par calculer, toujours modulo 641, les nombres successifs :

$$7^2,\;\; 7^4,\;\; 7^8,\;\; 7^{16},\;\; 7^{32},\;\; 7^{64},\;\; 7^{128},$$

en prenant les carrés des nombres qui précèdent. Euler récupère le résultat intermédiaire 7^{32} qu'il n'a qu'à relire sur son manuscrit, pour calculer enfin :

$$7^{160} \;=\; 7^{128} \cdot 7^{32},$$

le tout modulo 641 *à chaque étape* [9].

Mais ce ne sont pas les puissances de 7 qui l'intéressent, c'est le cinquième nombre de Fermat.

9. Pour rendre transparente la difficulté, mentionnons que :

$$7^{32} \;=\; 1104427674243920646305299201,$$

et pour faire transpirer un peu plus les électrons-esclaves de notre ordinateur, ajoutons que :

$$7^{128} \;=\; 148781564719761169591031268174127357033235671715479894989849830508638731542330099965475756192863330589703680 1,$$

ce qui, au final, devrait donner quelque chose d'aussi astronomique que :

$$7^{160} \;=\; 164318477493817185791700041055654480634183741959952349706976 467123320756556228789187756432381825444948691083899787146729804736961289600 1.$$

Théorème 15.1. [Euler 1732] *Contrairement à ce que Fermat affirmait, le nombre* $2^{2^5}+1$ *n'est* pas *un nombre premier, et il est divisible par le nombre premier* 641*, à savoir on a :*

$$2^{2^5} \equiv -1 \bmod 641.$$

Démonstration. Il suffit de partir d'un nombre encore trop petit pour que sa réduction modulo 641 commence à prendre effet, par exemple :

$$2^{2^3} = 2^8 = 256 \bmod 641,$$

pour monter ensuite deux crans plus haut tout en réduisant modulo 641 chaque fois que cela est possible :

$$\begin{aligned} 2^{2^5} &\equiv \left(\left(2^{2^3}\right)^2\right)^2 \bmod 641 \\ &\equiv \left(\left(256\right)^2 \bmod 641\right)^2 \bmod 641 \\ &\equiv \left(65536 \bmod 641\right)^2 \bmod 641 \\ &\equiv \left(154\right)^2 \bmod 641 \\ &\equiv 23716 \bmod 641 \\ &\equiv -1 \bmod 641. \end{aligned}$$

□

DIVISIBILITÉ par 641

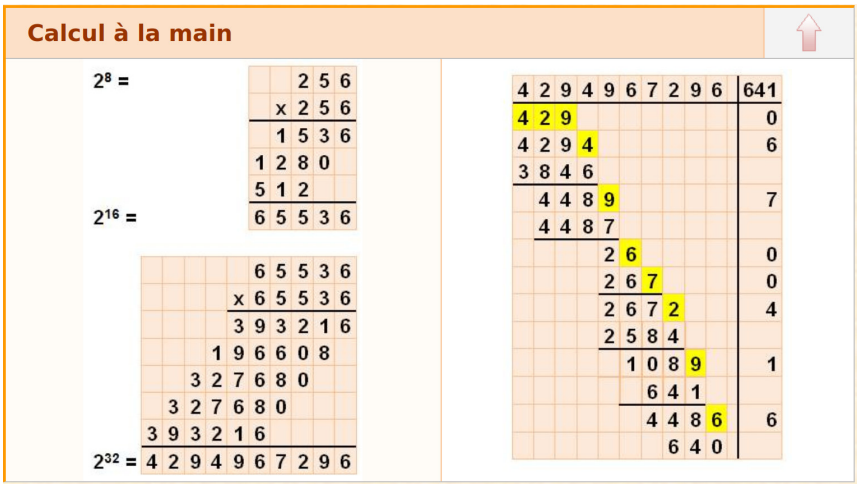
Nombre de Fermat n°5: divisible par 641.

Enjeu historique: on savait que les nombres de Fermat inférieurs à F_5 étaient tous premiers. Fermat, lui-même, conjecturait qu'ils étaient tous premiers. On sait qu'ils sont tous composés à partir de F_5 et jusqu'à F_{31}.

Aujourd'hui: Sachant que ce nombre est divisible par 641, plusieurs méthodes de calcul sont possibles: à la main, calculette ou via les congruences classiquement ou via une astuce. Ne connaissant pas 641, la méthode directe consisterait à écrire un programme pour détecter cette valeur.

Propriétés

Le nombre de Fermat F_5 est composé. Il est divisible par 641.	$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 641\ k$
Autres puissances de 2 mod 641 N = r mod m veut dire que N divisé par m donne un reste r.	$2^{32} \equiv -1 \bmod 641$ $2^{64} \equiv 1 \bmod 641$ $2^{96} \equiv -1 \bmod 641$ etc.



En effet, la découverte d'Euler était fantastique : arrêtons-nous quelques instants pour en dire plus.

Définition 15.2. Pour $n \geqslant 0$ entier, le n-ième *nombre de Fermat* est :

$$F_n := 2^{2^n} + 1.$$

Ces nombres doivent leur nom au mathématicien français Pierre de Fermat (1601–1665) qui émit la conjecture *erronée* que tous ces nombres étaient premiers.

Ironie cinglante : tous les nombres de Fermat connus, depuis F_5, F_6, F_7, …, jusqu'à :

$$F_{32} = 2^{2^{32}} + 1,$$

ne sont *pas* premiers.

Assertion 15.3. *Les seuls nombres de Fermat premiers connus sont donc :*

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65537. \quad \square$$

En 1640, dans une lettre adressée à Bernard Frénicle de Bessy, Pierre de Fermat énonce son petit théorème, puis il commente :

> Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers ; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.

Dans cette même lettre, il émet la conjecture que ces nombres sont tous premiers, quoiqu'il reconnaisse :

> Je n'ai pu encore démontrer nécessairement la vérité de cette proposition.

Mais cette hypothèse le fascine littéralement. Deux mois plus tard en effet, dans une lettre àMarin Mersenne, Pierre de Fermat écrit :

> Si je puis une fois tenir la raison fondamentale que 3, 5, 17, *etc.* sont nombres premiers, il me semble que je trouverai de très belles choses en cette matière, car j'ai déjà trouvé des choses merveilleuses dont je vous ferai part.

Il écrit encore à Blaise Pascal :

> Je ne vous demanderais pas de travailler à cette question si j'avais pu la résoudre moi-même.

Dans une lettre à Kenelm Digby, non datée mais envoyée en copie par Digby à John Wallis le 16 juin 1658, Fermat donne encore sa conjecture comme non démontrée. Toutefois, dans une lettre de 1659 à Pierre de Carcavi, il s'exprime en des termes qui, selon certains commentateurs, impliquent qu'il estime avoir trouvé une démonstration.

Mais en 1732, le jeune Leonhard Euler, à qui Christian Goldbach avait signalé cette conjecture trois ans auparavant, la réfute spectaculairement :

$$F_5 = 2^{2^5} + 1 \textit{ est divisible par } 641.$$

Or la motivation initiale de Fermat était de trouver une formule qui produise une infinité de nombres premiers [10]. Il connaissait la proposition élémentaire suivante.

Lemme 15.4. *Si $k \geqslant 1$ est un entier tel que le nombre $2^k + 1$ est premier, alors k est une puissance de 2.*

Démonstration. En divisant k pas à pas par 2 tant qu'on garde un nombre pair, on peut extraire k une puissance maximale de 2, et donc l'écrire comme $k = 2^b\, k'$, avec un entier $b \geqslant 0$, et avec un entier *impair* k'.

10. Il n'existe aucune formule ayant cette propriété qui soit *intéressante* ou *utile*.

Pour mémoire, on rappelle les factorisations classiques avec des puissances impaires :

$$\begin{aligned} 1+c^3 &= (1+c)\left(1-c+c^2\right), \\ 1+c^5 &= (1+c)\left(1-c+c^2-c^3+c^4\right). \end{aligned}$$

En posant $c := 2^{2^b}$, on dispose alors des égalités suivantes :

$$\begin{aligned} 1+2^k &= 1+2^{k'2^b} \\ &= 1+c^{k'} \\ &= (1+c)\left(1-c+c^2-\cdots-c^{k'-2}+c^{k'-1}\right), \end{aligned}$$

lesquelles montrent que $1+c$ serait un diviseur du nombre premier $1+2^k$ si on avait $k' \geqslant 3$, ce qui est impossible, donc $k'=1$ et enfin $k=2^b$. □

Fermat a conjecturé (erronément, comme on l'a vu) que la réciproque de ce lemme était vraie, après avoir confirmé (aisément) que les cinq (premiers) nombres :

$$\begin{aligned} F_0 &= 3, \\ F_1 &= 5, \\ F_2 &= 17, \\ F_3 &= 257, \\ F_4 &= 65537, \end{aligned}$$

sont tous premiers.

De nos jours encore, on ignore *cruellement* s'il existe d'autres nombres de Fermat qui sont premiers. On sait que F_5, F_6, …, F_{32} sont tous *composés*, mais on ne sait pas si F_{33} est premier ou composé.

Le plus grand nombre de Fermat dont on sait qu'il est composé est :

$$F_{2\,747\,499},$$

et on sait que l'un de ses diviseurs est :

$$57 \cdot 2^{2\,747\,499}+1.$$

En fait, Euler avait démontré le :

Théorème 15.5. *Tout facteur premier p d'un nombre de Fermat F_n est de la forme :*

$$k\,2^{n+1}+1,$$

où k est un entier. □

Ceci permet d'ailleurs à Euler de trouver rapidement par une autre voie que F_5 est divisible par 641.

En effet, on cherche un entier k tel que le nombre :

$$p = k\,2^6+1 = 64\,k+1$$

soit à la fois premier et diviseur strict de F_5. Les premières valeurs de k ne conviennent pas, mais dès $k=10$, on constate que $p=641$ est premier et que modulo 641, on a :

$$5^4 \cdot 2^{32} = \left(5\cdot 2^8\right)^4 = \left(5\cdot 128\cdot 2\right)^4 = \left(640\cdot 2\right)^4 \equiv (-2)^4 \bmod 641 \equiv 16 \bmod 641,$$

et par ailleurs :

$$5^4 \cdot 2^{32} \equiv \left(5^4 \bmod 641\right) \times 2^{32} \equiv \left(625 \bmod 641\right) \times 2^{32} \equiv -16 \times 2^{32} \bmod 641,$$

d'où en comparant ces deux résultats :

$$16 \bmod 641 \equiv -16 \times 2^{32} \bmod 641,$$

et enfin, après division par 16 qui est premier avec 641 :

$$1 \equiv -2^{32} \bmod 641,$$

ce qui montre bien que F_5 est divisible par 641. Plusieurs autres démonstration on déjà été données plus haut.

Le cas général est un problème difficile du fait de la taille des entiers F_n, même pour des valeurs relativement faibles de n.

Aujourd'hui, le plus grand nombre de Fermat dont on connaisse la factorisation complète est F_{11}, et le plus grand de ses cinq diviseurs premiers possède 560 chiffres. Les factorisations complètes des F_n, pour n entre 5 et 10, sont, elles aussi, entièrement connues.

En ce qui concerne F_{12}, on sait qu'il est composé mais c'est le plus petit nombre de Fermat dont on ne connaisse pas la factorisation complète.

Quant à F_{20}, c'est le plus petit nombre de Fermat composé dont on ne connaisse aucun diviseur premier.

16. Exponentiation rapide

Méthode de calcul de restes sur grands nombres

Calcul d'une puissance mod m.
Le calcul est accéléré en profitant de cette relation

$$a^k = \begin{cases} \left(a^{\frac{k}{2}}\right)^2 & \text{pour k pair} \\ a \cdot \left(a^{\frac{k-1}{2}}\right)^2 & \text{pour k impair} \end{cases}$$

Exemple: 3^{1304} **(mod 121)**

Étape 1 – Ligne 1: remplir les cellules de gauche à droite en commençant par l'exposant (1304). Si le nombre est pair, le suivant est sa moitié; sinon soustraire 1.

k	1304	652	326	163	162	81	80	40	20	10	5	4	2	1
3^k [121]	$(3^{652})^2$	$(3^{326})^2$	$(3^{163})^2$	$3 \cdot 3^{162}$	$(3^{81})^2$	$3 \cdot 3^{80}$	$(3^{40})^2$	$(3^{20})^2$	$(3^{10})^2$	$(3^5)^2$	243	81	9	3
	9^2	3^2	27^2	$3 \cdot 9$	3^2	$3 \cdot 1$	1^2	1^2	1^2	1^2				
	81	9	3	27	9	3	1	1	1	1	1	81	9	3

Étape 2 – Lignes 2, 3 et 4: on inscrit dans chaque cellule la valeur de $3^{\text{nombre du haut}}$ mod 121.
Le calcul est simplifié en remplissant les cellules de droite à gauche (donc dans l'autre sens). On profite des résultats précédents. Exemple: $3^{10} = 3^{5x2} = (3^5)^2$ soit $(1)^2$ en mod 121.

Vérification avec logiciel de calcul

$$3^{1304} \bmod 121;$$
$$81$$

Exemple avec l'année 2021

Calculer le reste de la division par 13 de 2021^{2021}		$2021^{2021} \equiv x? \bmod 13$
Premier pas	**Reduire la base 2021**	$2021 = 155 \times 13 + 6$ $2021 \equiv 6 \bmod 13$ $2021^{2021} \equiv 6^{2021} \bmod 13$
Conversion en binaire de 2021. **On se souvient que $2^{10} = 1024$**	N, k^2, k, B 2021 997, 1024, 10, 1 485, 512, 9, 1 229, 256, 8, 1 101, 128, 7, 1 37, 64, 6, 1 5, 32, 5, 1 5, 16, 4, 0 5, 8, 3, 0 1, 4, 2, 1 1, 2, 1, 0 0, 1, 0, 1	**En colonnes centrales toutes les puissances de 2 inférieures à 2021.** **En colonne de gauche, le nombre N puis sa valeur diminuée des valeurs successives de 2^k. Si le résultat reste positif, un 1 est placé en colonne de droite (binaire). Sinon, on conserve la valeur et on place un 0 à droite.** **La colonne de droite (B) indique la conversion en binaire de 2021.** **$2021_{10} = 111\ 1110\ 0101_2$**
Avec les puissances de 2	$2021^{2021} \equiv 6^{2\wedge 10} \times 6^{2\wedge 9} \times \ldots \times 6^{2\wedge 0} \bmod 13$	
Attention *Voir Puissances à étages*	$6^{2\wedge 10} = 6^{2^{10}} = 6^{1024} = 6,7124\ldots 10^{796} \equiv 9\ mod\ 13$ $et\ non\ pas\ (6^2)^{10} = 36^{10} = 3,6561\ldots 10^{15} \equiv 3\ mod\ 13$	

Attention *Voir Puissances à étages*	$6^{2\wedge 10} = 6^{2^{10}} = 6^{1024} = 6,7124\ldots 10^{796} \equiv 9\ mod\ 13$ $et\ non\ pas\ (6^2)^{10} = 36^{10} = 3,6561\ldots 10^{15} \equiv 3\ mod\ 13$	

Calcul des puissances de 6 mod 13	$6^{2^0} = 6^1 \equiv 6 \bmod 13$ $6^{2^1} = 6^2 = 36 \equiv 10 \bmod 13$ $6^{2^2} = 6^2 \times 6^2 = 100 \equiv 9 \bmod 13$ $6^{2^3} = 9 \times 9 = 81 \equiv 3 \bmod 13$ $6^{2^4} = 3 \times 3 = 9 \equiv 3 \bmod 13$ ... ð [6, 10, 9, 3, 9, 3, 9, 3, 9, 3, 9]	**Multiple de 13** **13, 26, 39, 52, 65, 78, 91, 104, 117, 130, ...**
Retour au calcul demandé	$2021^{2021} \equiv 9 \times 3 \times 9 \times 3 \times 9 \times 3 \times 9 \times 6 \bmod 13$ $\equiv 27 \times 27 \times 27 \times 54 \equiv 1 \times 1 \times 1 \times 2 \equiv$ **2 mod 13**	
Année 2021 en modulo	**2021 = [0, 1, 2, 1, 1, 5, 5, 5, 5, 1, 8, 5, 6, 5, 11, 5, 15, 5, 7, 1] mod (1, 2, 3,.., 13, ..., 20)** **2021^{2021} = [0, 1, 2, 1, 1, 5, 3, 5, 2, 1, 8, 5, 2, 3, 11, 5, 2, 11, 11, 1] mod (1, 2, 3,.., 13, ..., 20)**	

17. Division euclidienne générale dans $\mathbb{Z}$

Lorsque $a \geqslant 0$ et $b \geqslant 1$, la division euclidienne de a par b est intuitivement facile à effectuer. Le quotient q est le plus grand entier $q \geqslant 0$ tel que $0 \leqslant q\,b \leqslant a$, et le reste est alors $r := a - q\,b$.

Par exemple, la division euclidienne de 5 par 2 est :

$$5 \;=\; 2 \cdot 2 + 1.$$

Autrement dit, $q = 2$ et $r = 1$

Il faut en revanche faire un peu attention lorsqu'on travaille avec des entiers négatifs. Par exemple, la division euclidienne de -5 par 2 est :

$$-5 \;=\; 2\cdot(-3)+1.$$

Ainsi, dans ce cas, on a $q=-3$ et $r=1$.

Nous sommes maintenant prêts à démontrer un résultat fondamental pour toute l'arithmétique.

Théorème 17.1. [Division euclidienne dans $\mathbb{Z}$] *Soient $a,b\in\mathbb{Z}$ avec $b\neq 0$ non nul. Alors, il existe $q,r\in\mathbb{Z}$ tels que :*

(1) $a=q\,b+r$ *;*

(2) $0\leqslant r<|b|$.

De plus, les entiers q et r sont uniques.

Démonstration. Commençons par établir l'existence de q et de r. Comme $b\neq 0$ est supposé non nul, on peut diviser le travail en deux cas : $b\geqslant 1$, puis $b\leqslant -1$.

Premier cas : $b\geqslant 1$. Introduisons l'ensemble :

$$E \;:=\; \big\{m\in\mathbb{Z}\colon\; m\,b\leqslant a\big\}.$$

Assertion 17.2. *E est non vide et majoré.*

Preuve. Introduisons deux sous-cas : $a\geqslant 0$, puis $a\leqslant -1$.

Premier sous-cas : $a\geqslant 0$. Clairement, $0\in E$ car $0\cdot b=0\leqslant a$, donc $E\neq\emptyset$.

Ensuite, nous affirmons que a est un majorant de E, c'est-à-dire que $m\leqslant a$ pour tout $m\in E$. Pour cela, raisonnons par l'absurde. S'il existait $m_*\in E$ tel que $m_*\geqslant a+1$, alors on aurait $m_*\geqslant 1$ puisque $a\geqslant 0$, d'où nous déduirions les inégalités :

$$\begin{aligned} a+1 \;&\leqslant\; m_* \\ [b\geqslant 1] \qquad &\leqslant\; m_* b \\ [m_*\in E] \qquad &\leqslant\; a, \end{aligned}$$

dont la conséquence $a+1\leqslant a$, équivalente à $1\leqslant 0$, serait une contradiction fatale à toutes les mathématiques ! Donc on a bien $\max\limits_{m\in E} m\leqslant a$.

Deuxième sous-cas : $a\leqslant -1$. Clairement, $a\in E$ car $b\geqslant 1$ implique alors que $a\,b\leqslant a$, donc $E\neq\emptyset$.

Ensuite, nous affirmons que 0 est un majorant de E. Pour cela, raisonnons à nouveau par l'absurde. S'il existait $m_*\in E$ tel que $m_*\geqslant 1$, nous déduirions les inégalités :

$$\begin{aligned} [b\geqslant 1] \qquad 1 \;&\leqslant\; m_*\,b \\ [m_*\in E] \qquad &\leqslant\; a \\ &\leqslant\; -1, \end{aligned}$$

dont le résultat $1\leqslant -1$ serait très faux ! Donc on a bien $\max\limits_{m\in E} m\leqslant 0$. □

Grâce au Théorème 5.13 **(3)** concernant les sous-ensembles de $\mathbb{Z}$ majorés, E possède un plus grand élément, soit q. On a donc $q\in E$ et $q+1\notin E$, ce qui se traduit par :

$$q\,b\;\leqslant\; a\;<\;(q+1)\,b.$$

Posons alors $r:=a-q\,b$. L'encadrement précédent se ré-écrit $0\leqslant r<b=|b|$, d'où l'existence de q et de r dans ce premier cas $b\geqslant 1$.

Deuxième cas : $b \leqslant -1$. Alors $-b \geqslant 1$, et grâce à l'étude du premier cas, il existe $q, r \in \mathbb{Z}$ tels que :

$$\begin{aligned} a &= q\,(-b) + r \\ &= (-q)\,b + r, \end{aligned}$$

avec $0 \leqslant r < -b = |b|$, d'où le résultat.

Établissons maintenant l'unicité de (q, r). Supposons que $q, r, q', r' \in \mathbb{Z}$ vérifient :

$$\begin{aligned} a &= q\,b + r, \\ a &= q'\,b + r', \end{aligned}$$

avec :

$$\begin{aligned} 0 &\leqslant r < |b|, \\ 0 &\leqslant r' < |b|. \end{aligned}$$

Multiplions la deuxième ligne par -1, ce qui demande d'inverser les inégalités et d'échanger la droite avec la gauche :

$$\begin{aligned} 0 &\leqslant \quad r < |b|, \\ -|b| &< -r' \leqslant 0. \end{aligned}$$

Ensuite, par addition verticale, il vient — noter qu'après sommation, les inégalités sont *strictes* des deux côtés ! — :

$$-|b| < r - r' < |b|,$$

puis en prenant la valeur absolue :

$$|r - r'| < |b|. \tag{17.3}$$

Par ailleurs, en soustrayant verticalement les deux représentations de $a = q\,b + r$ et $a = q'\,b + r'$ écrites plus haut, on obtient :

$$0 = q\,b - q'\,b + r - r',$$

c'est-à-dire :

$$-(q - q')\,b = r - r'. \tag{17.4}$$

Nous affirmons que $q - q' = 0$. Sinon, si $q - q' \neq 0$, en prenant la valeur absolue de ce qui précède, on obtiendrait :

$$|q - q'|\,|b| = |r - r'|,$$

d'où à cause de $|q - q'| \geqslant 1$:

$$|b| \leqslant |r - r'|,$$

en contradiction manifeste avec (17.3).

Donc $q = q'$, et enfin en revenant à (17.4), nous concluons que $r = r'$. Cela achève la démonstration. □

Définition 17.5. Les entiers q et r définis par dans le Théorème 17.1 par $a = q\,b + r$ s'appellent respectivement le *quotient* et le *reste* de la division euclidienne de a par b.

Nous pouvons maintenant dévoiler un lien fondamental entre le calcul modulaire et la division euclidienne, dans $\mathbb{Z}$.

Proposition 17.6. *Pour tout entier $n \geqslant 1$, et tous entiers relatifs $a, b \in \mathbb{Z}$, on a équivalence entre :*

(i) $a \equiv b \mod n$ *;*

(ii) a *et* b *ont le même reste dans leur division euclidienne par* n*.*

Démonstration. **(i)** $\Longrightarrow$ **(ii)** Si $a = b + k\,n$ est l'expression de la congruence, et si $b = q\,n + r$ est la division euclidienne de b par n, avec un reste $0 \leqslant r \leqslant n-1$, il en découle que :

$$a \;=\; (q+k)\,n + r,$$

et par unicité dans la division euclidienne, cette relation *est* la division de a par n, donc le reste r de b divisé par n est *aussi* le reste de a divisé par n.

(ii) $\Longrightarrow$ **(i)** Écrivons les deux divisions de a et de b par n avec les deux restes incriminés :

$$\begin{aligned} a \;&=\; p\,n + r && \text{avec} \quad 0 \;\leqslant\; r \;\leqslant\; n-1, \\ b \;&=\; q\,n + s && \text{avec} \quad 0 \;\leqslant\; s \;\leqslant\; n-1, \end{aligned}$$

mutiplions la deuxième ligne par -1, puis additionnons verticalement :

$$\begin{aligned} 0 \;&\leqslant\; && r \;\leqslant\; n-1 \\ -(n-1) \;&\leqslant\; && -s \;\leqslant\; 0 \\ -(n-1) \;&\leqslant\; && r-s \;\leqslant\; (n-1). \end{aligned}$$

Ceci montre que l'entier $r - s$ appartient à l'intervalle entier $[\![-(n-1),\, (n-1)]\!]$.

Fait 17.7. *Aucun entier de l'intervalle $[\![-(n-1),\, (n-1)]\!]$, c'est-à-dire aucun entier parmi :*

$$-(n-1),\; -(n-2),\; \ldots,\; -2,\; -1,\; \mathbf{0},\; 1,\; 2,\; \ldots,\; n-2,\; n-1,$$

ne peut être congru à 0 *modulo* n*, excepté* **0** *au centre.*

Preuve. Soit $e \in [\![-(n-1),\, (n-1)]\!]$ avec $e \equiv 0 \mod n$. Par la Proposition 9.6, $e = k\,n$ est un multiple de n, avec $k \in \mathbb{Z}$. Clairement, $k = 0$ marche et donne $e = \mathbf{0}$.

Pour $k \neq 0$, puisque $|k| \geqslant 1$, on minore $|e| = |k\,n| = |k|\,n \geqslant n$, donc $e = k\,n$ ne peut *pas* appartenir à l'intervalle $[\![-(n-1),\, (n-1)]\!]$. □

Ensuite, soustrayons les deux représentations de a et de b laissées sur le bord du chemin plus haut :

$$\begin{aligned} a - b \;&\equiv\; (p-q)\,n + r - s \\ &\equiv\; r - s \mod n. \end{aligned} \tag{17.8}$$

En définitive :

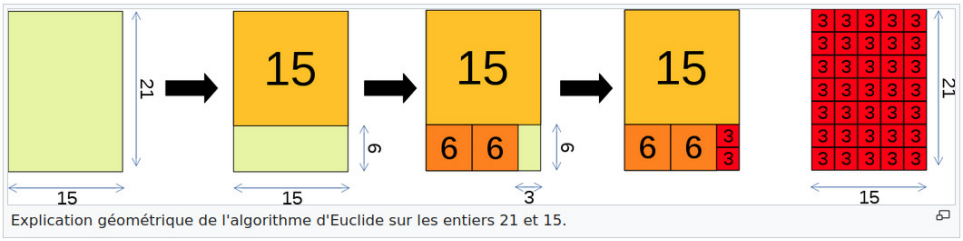
$$\begin{aligned} a \equiv b \mod n \quad &\Longleftrightarrow \quad a - b \equiv 0 \mod n \\ \text{[Équation (17.8)]} \quad &\Longleftrightarrow \quad r - s \equiv 0 \mod n \\ \text{[Fait 17.7]} \quad &\Longleftrightarrow \quad r - s = 0 \\ &\Longleftrightarrow \quad r = s. \end{aligned}$$

□

Observons au passage que la deuxième partie de la démonstration a en fait établi l'équivalence **(ii)** $\Longleftrightarrow$ **(i)** *dans les deux sens*.

18. Algorithme d'Euclide : Histoire et Géométrie

L'algorithme de divisions successives d'Euclide est décrit dans le livre VII, Propositions 1 à 3, des *Éléments* d'Euclide (vers 300 av. J.-C.), sous la forme dite de l'*Anthyphérèse*[11]. Il est aussi décrit dans le livre X, Proposition 2, mais pour un problème de nature géométrique : comment trouver une « unité de mesure » commune pour deux longueurs de segments. L'algorithme procède par soustractions répétées de la longueur du plus court segment sur la longueur du plus long.



Explication géométrique de l'algorithme d'Euclide sur les entiers 21 et 15.

Considérons par exemple le rectangle de longueur $L = 21$ et de largeur $l = 15$, dans n'importe quelle unité de mesure. On peut y glisser un carré de côté 15, mais il reste alors un rectangle de côtés 15 et 6.

11. *Anthyphèrese* provient du grec $\alpha\nu\theta\upsilon\phi\alpha\iota\rho\varepsilon\iota\nu$, qui signifie « soustraire alternativement ». On appelle donc anthyphérèse une méthode qu'Euclide utilisait pour calculer le plus grand commun diviseur de deux nombres ou pour démontrer que deux longueurs sont incommensurables.

Dans le livre VII, Proposition 2, Euclide préconise en effet d'ôter au plus grand nombre le plus petit, autant que faire se pourra, puis d'ôter le reste au plus petit des nombres, et ainsi de suite.

L'Antyphérèse est de nouveau employée dans le livre X, Théorème 24 pour caractériser deux longueurs incommensurables (on parlerait de nos jours de longueurs dont le rapport est irrationnel). Si le processus se poursuit indéfiniment, les longueurs sont incommensurables. Cette méthode aurait pu être employée, par exemple, pour démontrer l'irrationalité de la racine carrée $\sqrt{2}$ de 2.

Qu'à cela ne tienne, glissons-y alors *deux* carrés de côté 6. Carrramba ! Encore rrraté ! Il reste encore un carré de côtés 6 et 3. Sans nous décourager, glissons enfin deux carrés de côté 3 : ouf ! tout est rempli !

Enfin, observons que nos carrés de côté 6 et celui de côté 15 peuvent aussi se carreler en carrés de côté 3. Par conséquent, le rectangle initial tout entier, de côtés 21 et 15, peut se carreler en carrés de côté 3. Et il n'existe pas de carré plus grand permettant un tel carrelage.

Cet algorithme *géométrique* n'a probablement pas été découvert par Euclide lui-même, qui aurait compilé des résultats d'autres mathématiciens dans ses *Éléments*. Pour le mathématicien et historien van der Waerden, le livre VII vient d'un livre de théorie des nombres écrit par un mathématicien de l'école de Pythagore. L'algorithme était probablement connu d'Eudoxe de Cnide (vers 375 av. J.-C.). Il se peut même que l'algorithme ait existé avant Eudoxe, sachant que le terme technique utilisé $\alpha\nu\theta\upsilon\phi\alpha\iota\rho\varepsilon\iota\nu$, soustraction réciproque — apparaît déjà dans les œuvres d'Aristote.

Quelques siècles plus tard, l'algorithme « d'Euclide » est (ré)inventé de manière indépendante à la fois en Inde et en Chine. L'objectif était de résoudre des équations diophantiennes issus de l'astronomie et de faire des calendriers plus précis. Au V$^{\text{ième}}$ siècle, le mathématicien et astronome indien Aryabhata a décrit cet algorithme comme le « *pulvérisateur* », à cause de son efficacité pour résoudre les équations diophantiennes.

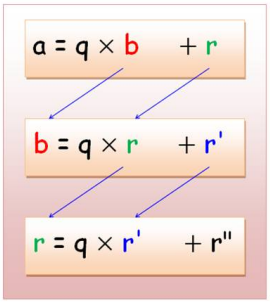
Exemple 18.1. Avant d'aborder l'algorithme général, présentons un autre calcul concret. Il est avisé de représenter synoptiquement la recherche du plus grand commun diviseur entre 126 et 35 :

$$\begin{aligned}
126 &\overset{126\ \geqslant\ 35}{=} 3\cdot 35 + 21\\
35 &\overset{35\ \geqslant\ 21}{=} 1\cdot 21 + 14\\
21 &\overset{21\ \geqslant\ 14}{=} 1\cdot 14 + 7\\
14 &\overset{14\ \geqslant\ 7}{=} 2\cdot \boxed{\mathbf{7}} + \mathbf{0},
\end{aligned}$$

et ici, puisque le dernier reste $\mathbf{0}$ est nul, l'avant-dernier reste $\boxed{\mathbf{7}}$ est le pgcd recherché.

Exemple 18.2. De manière alternative, on peut représenter sous forme d'un tableau un autre calcul qui montre que 315 et 307 n'ont aucun facteur en commun, *i.e.* ont un plus grand commun diviseur égal à 1. En effet, le Théorème 20.2 de Bézout *infra* va nous expliquer dans un instant que cela est *démontré* par le fait que l'*avant-dernier* reste dans l'avant-dernière ligne $3 = 2 \times 1 + 1$ est égal à $\mathbf{1}$.

	Dividende	Diviseur	Reste
315 =1 x 307 + 8	315	307	8
307 = 8 x 38 + 3	307	8	3
8 = 2 x 3 + 2	8	3	2
3 = 2 x 1 + 1	3	2	1
2 = 2 x 1 + 0	2	1	0



Notre « plan T », *i.e.* Théorique, est le suivant.

☐ Décrire précisément l'algorithme d'Euclide

☐ Montrer qu'il permet naturellement de trouver facilement le *plus grand commun diviseur* entre deux entiers donnés.

☐ Montrer qu'il permet aisément de trouver une *relation de Bézout* $a\,u + b\,v = 1$ entre deux entiers a et b qui sont *premiers entre eux*.

Tous ces termes et concepts nouveaux vont être définis rigoureusement dans un instant, mais à travers les exemples qui précèdent, nous avons en fait déjà deviné plus de $50\,\%$ de ce qu'ils sont.

19. Algorithme d'Euclide : Plus Grand Commun Diviseur (PGCD)

Soient deux entiers relatifs quelconques $a, b \in \mathbb{Z}$. Quitte à les multiplier par -1 si besoin est, on peut les supposer positifs pour introduire la

Définition 19.1. Le *plus grand commun diviseur* de deux entiers $a \geqslant 0$ et $b \geqslant 0$, noté $\mathsf{pgcd}\,(a,b)$, est le plus grand entier $d \geqslant 1$ qui les divise tous les deux, à savoir :

$$\mathsf{pgcd}\,(a,b) \;:=\; \mathsf{max}\,\Big\{d \geqslant 1 :\;\; d \,|\, a \text{ et } d \,|\, b\Big\}.$$

Quand $a = 0$ et $b = 0$, on convient que $\mathsf{pgcd}\,(0,0) = 0$. Pour $a, b \in \mathbb{Z}$ éventuellement négatifs, on convient que :

$$\mathsf{pgcd}\,(a,b) \;:=\; \mathsf{pgcd}\,\big(|a|,\,|b|\big).$$

L'ensemble sur lequel on prend un maximum est non vide, car $d = 1$ lui appartient, et il est majoré, car pour des nombres positifs, $d \,|\, a$ implique $d \leqslant a$, d'où :

$$\mathsf{pgcd}\,(a,b) \;\leqslant\; \mathsf{min}\,(a,b).$$

Évidemment, on a :

$$\mathsf{pgcd}\,(b,a) \;=\; \mathsf{pgcd}\,(a,b).$$

Si $a = 0$ et $b \geqslant 1$, il est clair que le plus grand entier $d \geqslant 0$ divisant 0 et b est $d = b$. Par symétrie, on a donc :

$$\mathsf{pgcd}\,(0,b) \;=\; b \qquad\qquad \text{et} \qquad\qquad \mathsf{pgcd}\,(a,0) \;=\; a.$$

La notion de pgcd n'est donc intéressante que lorsque $a \geqslant 1$ et $b \geqslant 1$.

Par exemple, $\mathsf{pgcd}\,(10,30) = 10 = 2 \cdot 5$, parce que $20 = 2^2 \cdot 5$ et $30 = 2 \cdot 3 \cdot 5$, ce que nous comprendrons bientôt dans un contexte très général.

La Définition 19.1 se généralise aisément au $\mathsf{pgcd}\,(a,b,c)$ entre trois entiers quelconques $a, b, c \in \mathbb{N}$. Par exemple, $\mathsf{pgcd}\,(36,48,60) = 12 = 2^2 \cdot 3$, parce que $36 = 2^2 \cdot 3^2$, puis $48 = 2^4 \cdot 3$, et enfin $60 = 2^2 \cdot 3 \cdot 5$. Nous y reviendrons plus tard.

Question 19.2. *Comment déterminer le* pgcd (a, b) *entre deux entiers quelconques* $a \geqslant 1$ *et* $b \geqslant 1$ *?*

Réponse : grâce à l'algorithme d'Euclide !

Ainsi, on peut supposer $a \geqslant 1$ et $b \geqslant 1$. Quitte à les permuter, on peut aussi supposer que $a \geqslant b \geqslant 1$. Alors, *divisons avec reste* a par b :

$$a \;=\; q\,b + r,$$

avec des entiers naturels q et $0 \leqslant r < b$. Mais comme r est (strictement) inférieur à b, on peut spontanément avoir l'idée de re-diviser b par r ! Ce qui donne :

$$b \;=\; u\,r + s,$$

avec un certain reste $0 \leqslant s < r$. Mais alors pour la même raison, on peut donc encore re-diviser r par s :

$$r \;=\; v\,s + t,$$

avec encore un certain reste $0 \leqslant t < s$, et ainsi de suite.

Comme l'alphabet ne contient qu'un nombre limité de lettres, si on veut décrire complètement ce procédé, il est nécessaire d'introduire un formalisme mathématique avec des *indices*. Commençons alors par renommer :

$$r_0 := a, \qquad r_1 := b, \qquad q_1 := q, \qquad r_2 := r,$$

de telle sorte que nos deux premières divisions peuvent s'écrire :

$$\begin{aligned} r_0 &= q_1\,r_1 + r_2, \\ r_1 &= q_2\,r_2 + r_3, \end{aligned}$$

en nommant r_3 le dernier reste qui apparaît.

Alors en poursuivant indéfiniment ces divisions successives, nous aboutissons à un résultat qui peut être représenté au moyen d'un diagramme en forme diagonale descendante :

$$\begin{aligned} r_0 &= q_1\,r_1 + r_2, \\ r_1 &= q_2\,r_2 + r_3, \\ &\ddots \quad \ddots \quad \ddots \\ r_{i-1} &= q_i\,r_i + r_{i+1}, \\ &\ddots \quad \ddots \quad \ddots \\ r_{\ell-2} &= q_{\ell-1}\,r_{\ell-1} + \boxed{r_\ell}, \\ r_{\ell-1} &= q_\ell\,\boxed{r_\ell} + \mathbf{0}, \end{aligned}$$

avec, à chaque étape, un nouveau reste r_{i+1} strictement inférieur au précédent :

$$0 \;\leqslant\; r_{i+1} \;<\; r_i.$$

Assertion 19.3. *À partir d'un certain rang, le dernier reste obtenu devient égal à* $\mathbf{0}$.

Preuve. En partant du premier reste :

$$r \;=\; r_2 \;<\; b,$$

les restes suivants décroissent strictement à chaque étape :

$$0 \;\leqslant\; \cdots\cdots \;<\; r_3 \;<\; r_2 \;<\; b,$$

et comme ils sont tous positifs, ils sont minorés par 0.

Le nombre de restes r_i strictement positifs est donc nécessairement *fini*. Appelons alors ℓ ce nombre, avec $\ell \geqslant 1$ et $r_\ell \neq 0$, exactement comme cela était visible dans l'avant-dernière ligne du diagramme en diagonale descendante.

Par définition de ℓ, le prochain reste $r_{\ell+1} = \mathbf{0}$ est nécessairement nul. C'est bien ce que montre la dernière ligne écrite dans le diagramme. □

Ce dernier reste non nul $r_\ell \neq 0$ joue un rôle capital dans la théorie arithmétique.

Proposition 19.4. *On a* $r_\ell = \mathsf{pgcd}\,(a, b)$.

Démonstration. Notons de manière abrégée $d := \mathsf{pgcd}\,(a, b)$. Ainsi, $d \,|\, r_0$ et $d \,|\, r_1$, avec d maximal, d'ailleurs.

Comme $r_2 = r_0 - q_1\, r_1$, on voit que $d \,|\, r_2$ aussi, puisque r_0, r_1 multiples de d impliquent $r_0 - q_1\, r_1$ multiple de d.

Ensuite, $r_3 = r_1 - q_2\, r_2$ est aussi divisible par d, et ainsi de suite.

À la fin, $d \,|\, r_{\ell-2}$ et $d \,|\, r_{\ell-1}$ impliquent $d \,|\, r_\ell$, car $r_\ell = r_{\ell-2} - q_{\ell-1}\, r_{\ell-1}$. Autrement dit $\mathsf{pgcd}\,(a, b) \,|\, r_\ell$, et donc :

$$\mathsf{pgcd}\,(a, b) \leqslant r_\ell. \tag{19.5}$$

Maintenant, comme des saumons, remontons la cascade diagonale, en partant du bas (droite) vers le haut (gauche). L'égalité $r_{\ell-1} = q_\ell\, r_\ell$ dit que $r_{\ell-1}$ est divisible par r_ℓ.

Puis $r_{\ell-2} = q_{\ell-1}\, r_{\ell-1} + r_\ell$ entraîne que $r_{\ell-2}$ est divisible par r_ℓ.

Puis $r_{\ell-3} = q_{\ell-2}\, r_{\ell-2} + r_{\ell-1}$ entraîne que $r_{\ell-3}$ est divisible par r_ℓ, *et ainsi de suite*.

À la fin, c'est-à-dire en haut (regarder encore le diagramme), à l'avant-dernier étage supérieur, $r_1 = q_2\, r_2 + r_3$ entraîne que $r_1 = b$ est divisible par r_ℓ, puis, à la source du torrent tout en haut, $r_0 = q_1\, r_1 + r_2$ entraîne que $r_0 = a$ est divisible par r_ℓ.

Ainsi, $r_\ell \,|\, a$ et $r_\ell \,|\, b$. Comme le pgcd est le *plus grand* des diviseurs simultanés possibles, il est clair que :

$$r_\ell \leqslant \mathsf{pgcd}\,(a, b),$$

ce qui est l'inégalité *opposée* de celle, (19.5), déjà obtenue. En conclusion, on a bien :

$$\mathsf{pgcd}\,(a, b) = r_\ell.$$ □

Ensuite, on peut se convaincre en y réfléchissant que toutes ces opérations ne dépendent que des deux entiers a et b fournis au départ. En particulier, tous les restes r_i construits pas à pas ne dépendent que de a et de b. Et dans un instant, nous allons dévoiler des *formules* qui expriment les restes r_i comme *combinaison linéaires* de a et de b.

À cette fin, outre la suite connue :

$$r_0 := a, \qquad r_1 := b, \qquad r_{i+1} := r_{i-1} - q_i\, r_i \qquad (1 \leqslant i \leqslant \ell-1),$$

introduisons les *deux* suites auxiliaires assez similaires :

$$u_0 := 1, \qquad u_1 := 0, \qquad u_{i+1} := u_{i-1} - q_i\, u_i \qquad (1 \leqslant i \leqslant \ell-1),$$
$$v_0 := 0, \qquad v_1 := 1, \qquad v_{i+1} := v_{i-1} - q_i\, v_i \qquad (1 \leqslant i \leqslant \ell-1).$$

Lemme 19.6. *Pour tout* $i = 0, 1, 2, \ldots, \ell$*, le reste* r_i *se représente comme la combinaison linéaire suivante de* a *et de* b *:*

$$u_i\, a + v_i\, b = r_i.$$

Démonstration. Pour $i = 0$, vérifions :

$$u_0\, a + v_0\, b \;=\; 1 \cdot a + 0 \cdot b \;\overset{?}{=}\; r_0,$$

ce qui est vrai car $a = r_0$ par définition.

Pour $i = 1$, vérifions :

$$u_1\, a + v_1\, b \;=\; 0 \cdot a + 1 \cdot b \;\overset{?}{=}\; r_1,$$

ce qui est à nouveau vrai car $b = r_1$ par définition.

En raisonnant par récurrence *double*, supposons que pour un certain indice i avec $1 \leqslant i \leqslant \ell - 1$, on ait démontré les *deux* formules :

$$\begin{aligned} u_{i-1}\, a + v_{i-1}\, b \;&=\; r_{i-1}, \\ u_i\, a + v_i\, b \;&=\; r_i, \end{aligned}$$

et demandons-nous si, à l'étage en-dessous, on a encore :

$$u_{i+1}\, a + v_{i+1}\, b \;\overset{?}{=}\; r_{i+1},$$

ou, de manière équivalente, si on a :

$$\big(u_{i-1} - q_i\, u_i\big)\, a + \big(v_{i-1} - q_i\, v_i\big)\, b \;\overset{?}{=}\; r_{i-1} - q_i\, r_i.$$

Mais après réorganisation, et factorisation de deux termes à gauche par q_i, ceci équivaut à l'identité vraie tautologiquement :

$$\underbrace{u_{i-1}\, a + v_{i-1}\, b}_{= r_{i-1}} - q_i \Big(\underbrace{u_i\, a + v_i\, b}_{= r_i} \Big) \;\overset{\text{oui}}{=}\; r_{i-1} - q_i\, r_i. \qquad \square$$

À la fin tout en bas, pour $i = \ell$, on obtient donc une représentation :

$$u_\ell\, a + v_\ell\, b \;=\; \mathsf{pgcd}\,(a, b),$$

du $\mathsf{pgcd}\,(a, b) = r_\ell$ comme combinaison linéaire de a et de b.

Théorème 19.7. *Le* pgcd *entre deux entiers quelconques donnés $a \geqslant b \geqslant 1$ se calcule en effectuant l'algorithme d'Euclide, et en mémorisant les résultats intermédiaires jusqu'à obtenir :*

$$\mathsf{pgcd}\,(a, b) \;=\; u_\ell\, a + v_\ell\, b \qquad (\exists\, u_\ell \in \mathbb{Z},\, \exists\, v_\ell \in \mathbb{Z}). \qquad \square$$

Toutefois, cet énoncé n'est pas assez précis, *techniquement*. Il sous-entend que l'on doit implémenter les trois suites $\{r_i\}_{i=0}^{\ell}$, $\{u_i\}_{i=0}^{\ell}$, $\{v_i\}_{i=0}^{\ell}$, ce qui fonctionne très bien sur ordinateur, mais comme les ordinateurs ne sont pas autorisés lors des examens universitaires, il est tout à fait légitime de se poser la

Question 19.8. *Comment calculer, concrètement et manuellement, une représentation linéaire du* pgcd *entre deux entiers sous la forme :*

$$\mathsf{pgcd}\,(a, b) \;=\; u\, a + v\, b \;\textbf{?}$$

Répondons à cette question en traitant un exemple, qui va nous faire comprendre comment les deux suites auxiliaires $\{u_i\}_{i=0}^{\ell}$, $\{v_i\}_{i=0}^{\ell}$ interviennent naturellement.

Soit, comme précédemment, à déterminer $\mathsf{pgcd}\,(126,\,35)$. Comme nous l'avons déjà vu, l'algorithme d'Euclide donne :

$$\begin{aligned} 126 &= 3\cdot 35 + 21 \\ 35 &= 1\cdot 21 + 14 \\ 21 &= 1\cdot 14 + \mathbf{7} \\ 14 &= 2\cdot \mathbf{7} + \mathbf{0}, \end{aligned}$$

un pgcd égal à $\mathbf{7}$, au bout de $\ell = 4$ lignes. Alors, *comment trouver* u_4 *et* v_4 *satisfaisant* $u_4\,126 + v_4\,35 = \mathbf{7}$? En se ré-incarnant sous la peau d'un saumon !

Partons en effet de l'avant-dernière ligne, en ne conservant que $\mathbf{7}$ à droite — attention ! il faut lire ces calculs du bas-droite vers le haut-gauche ! —, et remplaçons via la commande $\underline{\ }_{\text{rpl}}$:

$$\begin{aligned} 2\cdot 126 - 7\cdot 35 \;=\; -1\cdot 35 + 2\cdot\big(126 - 3\cdot 35\big) \;=\; \\ -1\cdot 35 + 2\cdot \underline{21}_{\text{rpl}} \;=\; 21 - 1\cdot\big(35 - 1\cdot 21\big) \;=\; \\ 21 - 1\cdot \underline{14}_{\text{rpl}} \;=\; \mathbf{7}. \end{aligned}$$

Effectivement, on a bien en haut à gauche $252 - 245 = \mathbf{7}$.

« Pour le fun », et avant de clore cette section, toujours avec $r_0 = a$ et $r_1 = b$, expliquons ce qui se passe généralement lorsqu'on a 4 étages :

$$\begin{aligned} r_0 &= q_1\, r_1 + r_2, \\ r_1 &= q_2\, r_2 + r_3, \\ r_2 &= q_3\, r_3 + \mathbf{r_4}, \\ r_3 &= q_4\, \mathbf{r_4} + \mathbf{0}, \end{aligned}$$

ce qui donne en remontant depuis l'avant-dernière ligne :

$$\begin{aligned} \big(\underbrace{1 + q_3\, q_2}_{=:\,u_4}\big) r_0 + \big(\underbrace{-q_3 - q_1 - q_3\, q_2\, q_1}_{=:\,v_4}\big) r_1 = -\,q_3\, r_1 + \big(1 + q_3\, q_2\big)\big(r_0 - q_1\, r_1\big) = \\ -\,q_3 r_1 + \big(1 + q_3 q_2\big)\,\underline{r_2}_{\text{rpl}} \;=\; r_2 - q_3\big(r_1 - q_2 r_2\big) = \\ r_2 - q_3 \underline{r_3}_{\text{rpl}} \;=\; \mathbf{r_4}. \end{aligned}$$

20. Théorème de Bézout

Cette valeur terminale $r_\ell = \mathsf{pgcd}\,(a, b)$ de l'algorithme d'Euclide vaut parfois $r_\ell = 1$, et parfois, elle satisfait $r_\ell \geqslant 2$. Ces deux cas sont extrêmement différents, et ils motivent une conceptualisation adéquate. Rappelons que pour deux entiers a et b éventuellement négatifs, on a défini :

$$\mathsf{pgcd}\,(a, b) \;:=\; \mathsf{pgcd}\,\big(|a|,\,|b|\big).$$

Définition 20.1. On dit que deux entiers relatifs $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ sont *premiers entre eux* lorsque [12] :

$$1 \;=\; \mathsf{pgcd}\,(a, b),$$

et on note cette propriété [13] :

$$a \wedge b \;=\; 1.$$

On dit parfois aussi que a *est premier à* b, ou que b *est premier à* a.

12. Ceci exclut $(a, b) = (0, 0)$, dont le pgcd vaut 0 par convention
13. Certains auteurs utilisent la notation raccourcie $a \wedge b$ pour désigner $\mathsf{pgcd}\,(a, b)$, ce qui est cohérent.

L'aboutissement ultime de l'algorithme d'Euclide, c'est le résultat hyper-important suivant, ultra présent dans tous les exercices et dans tous les examens de L1, L2, L3, M1, et dont le slogan mnémotechnique [14] pourrait être : « *Bézout partout* ».
i

Théorème 20.2. [Bézout] *Pour toute paire d'entiers $a, b \in \mathbb{Z}$ quelconques avec $(a, b) \neq (0, 0)$, il existe $u, v \in \mathbb{Z}$ tels que :*

$$u\,a + v\,b \;=\; \mathsf{pgcd}\,(a, b).$$

De plus, on a équivalence entre :

(i) *a et b sont premiers entre eux,* i.e. $1 = a \wedge b$*;*

(ii) *il existe $u, v \in \mathbb{Z}$ tels que $1 = u\,a + v\,b$.*

Les entiers u et v ne sont *jamais* uniques, car en prenant $u' := u + \lambda\,b$ et $v' := v - \lambda\,a$, avec $\lambda \in \mathbb{Z}$ quelconque, on a encore :

$$\big(u + \lambda\,b\big)\,a + \big(v - \lambda\,a\big)\,b \;=\; u\,a + v\,b \;=\; \mathsf{pgcd}\,(a, b).$$

Démonstration. On a vu il y a un instant que :

$$u_\ell\,a + v_\ell\,b \;=\; r_\ell \;=\; \mathsf{pgcd}\,(a, b),$$

donc la première affirmation était en fait déjà « okay ».

(i) $\Longrightarrow$ **(ii)** revient alors à la Définition 20.1.

(ii) $\Longrightarrow$ **(i)** Si donc $1 = u\,a + v\,b$, soit $d \in \mathbb{N}$ un diviseur commun à a et à b. Puisque $d \,|\, a$ et $d \,|\, b$, il vient :

$$d \;\Big|\; \big(u\,a + v\,b\big),$$

c'est-à-dire $d \,|\, 1$, ce qui force $d = 1$. Le maximum des d divisant a et b ne peut donc qu'être égal à 1, donc en conclusion $\mathsf{pgcd}\,(a, b) = 1$. □

Étant donné deux entiers relatifs non nuls $a, b \in \mathbb{Z}^*$ premiers entre eux, à savoir avec $1 = \mathsf{pgcd}\,(a, b)$, on peut supposer, quitte à changer leurs signes, que $1 \leqslant a, b$, et alors, ce Théorème 20.2 de Bézout fournit $u, v \in \mathbb{Z}$ satisfaisant, quitte à remplacer $v \longmapsto -v$:

$$u\,a - v\,b \;=\; 1.$$

On peut aussi supposer $1 \leqslant a \leqslant b$. On sait qu'il n'y a pas unicité, puisque, pour tout entier $k \in \mathbb{Z}$, on a encore :

$$\big(u + k\,b\big)\,a - \big(v + k\,a\big)\,b \;=\; 1.$$

14. Certains auteurs appelle ce résultat *Théorème de Bachet-Bézout.*

Mais la préciosité de notre langue nous retient avec pudeur d'oser utiliser une terminologie qui pourrait évoquer ou rappeler l'un des jurons compulsifs et dégueulatoires du Capitaine Haddock.

Question 20.3. *Peut-on restreindre le domaine des valeurs de a et de b, de façon à avoir quand même une certaine forme d'unicité ?*

Le cas $1 = a$ est inintéressant, car alors $1 \wedge b = 1$ est automatique, et en prenant $u := 1$ puis $v := 0$, il est trivial que :

$$1 \cdot 1 - 0 \cdot b \, = \, 1.$$

Donc on peut supposer que $2 \leqslant a \leqslant b$, avec en fait $a < b$ si $1 = a \wedge b$.

Théorème 20.4. *Soient deux entiers $2 \leqslant a \leqslant b$ premiers entre eux. Alors il existe u et v uniques avec :*

$$0 \, \leqslant \, u \, \leqslant \, b-1 \qquad \textit{et} \qquad 0 \, \leqslant \, v \, \leqslant \, a-1,$$

satisfaisant une identité de Bézout :

$$u\,a - v\,b \, = \, 1.$$

Démonstration. Unicité. Supposons qu'il y ait deux identités de Bézout :

$$\begin{aligned} u\,a - v\,b \, &= \, 1, \\ u'\,a - v'\,b \, &= \, 1, \end{aligned}$$

avec $0 \leqslant u, u' \leqslant b-1$, et avec $0 \leqslant v, v' \leqslant a-1$. Alors par soustraction, il vient :

$$\big(u-u'\big)\,a \, = \, \big(v'-v\big)\,b, \tag{20.5}$$

avec, comme nous le savons de Marseille :

$$\big|u-u'\big| \, \leqslant \, b-1 \qquad \text{et} \qquad \big|v'-v\big| \, \leqslant \, a-1.$$

Mais alors, à cause de la primalité relative $1 = a \wedge b$, Gauss force dans l'équation (20.5) :

$$\begin{aligned} a \,\big|\, (v'-v), \qquad & \text{d'où} \qquad v' \, = \, v, \\ b \,\big|\, (u-u'), \qquad & \text{d'où} \qquad u \, = \, u'. \end{aligned}$$

Existence. Répétons que si (u_0, v_0) est une solution quelconque, fournie par le Théorème 20.2 de Bézout :

$$u_0\,a - v_0\,b \, = \, 1,$$

alors pour tout $k \in \mathbb{Z}$, on a encore une solution :

$$\big(\underbrace{u_0 + k\,b}_{=:\,u}\big)\,a - \big(\underbrace{v_0 + k\,a}_{=:\,v}\big)\,b \, = \, 1.$$

Grâce à ce que nous connaissons de la congruence modulo l'entier $a \geqslant 2$, nous pouvons choisir k afin que :

$$0 \, \leqslant \, v_0 + k\,a \, \leqslant \, a-1.$$

Nous avons donc trouvé u et v satisfaisant :

$$u\,a - v\,b \, = \, 1 \qquad \text{avec} \qquad 0 \, \leqslant \, v \, \leqslant \, a-1.$$

Assertion 20.6. *Alors automatiquement, on a $0 \leqslant u \leqslant b-1$.*

Preuve. Écrivons :

$$\begin{aligned} u\,a &= 1 + v\,b && \text{[Implique } u \geqslant 0\text{]} \\ &\leqslant 1 + (a-1)\,b \\ &= a\,b - (b-1) \\ &\leqslant a\,b - 1, && \text{[}2 \leqslant b\text{]} \end{aligned}$$

donc :

$$0 \leqslant u \leqslant b - \tfrac{1}{a},$$

et comme u est entier, on a bien $u \leqslant b-1$. □

En conclusion, nous avons bien $u\,a - v\,b = 1$, avec $0 \leqslant u \leqslant b-1$ et avec $0 \leqslant v \leqslant a-1$ uniques. □

21. Théorème de Gauss et applications

Voici un énoncé extrêmement célèbre et universellement utile en arithmétique.

Théorème 21.1. [Gauss] *Si deux entiers $a, b \in \mathbb{Z}$ sont premiers entre eux $a \wedge b = 1$, alors pour tout $c \in \mathbb{Z}$:*

$$a \;\Big|\; b\,c \qquad\qquad \Longrightarrow \qquad\qquad a \mid c.$$

Informellement : si a est « étranger » à b, il ne peut posséder de « points communs » qu'avec c.

Démonstration. Par le Théorème 20.2 du Bizou, il existe deux entiers $u, v \in \mathbb{Z}$ tels que $u\,a + v\,b = 1$. On a alors $u\,a\,c + v\,b\,c = c$. Comme $a \mid a\,c$ trivialement et comme $a \mid b\,c$ par hypothèse, on obtient :

$$a \;\Big|\; \big(u\,a\,c + v\,b\,c\big),$$

c'est-à-dire $a \mid c$. □

Le Théorème 21.1 de Gauss est très utile, car il permet souvent de simplifier certaines situations. Par exemple si on sait que $3 \mid 2\,n$, alors on peut en conclure que $3 \mid n$. Voici d'autres énoncés parfois bien utiles.

Proposition 21.2. *Soient a, b, c trois entiers quelconques. Si a et b sont tous les deux premiers à c, alors leur produit $a\,b$ est aussi premier à c.*

Démonstration. Il s'agit de faire voir que :

$$d := \mathsf{pgcd}\,\big(ab,\, c\big)$$

est égal à 1.

Comme $d \mid c$, il y a un entier e avec $d\,e = c$. Ensuite, grâce au Théorème 20.2 de Bézout, l'hypothèse $1 = a \wedge c$ s'exprime par une identité :

$$1 \;=\; u\,a + v\,c \;=\; u\,a + (v\,e)\,d,$$

qui montre que a et d sont aussi premiers entre eux.

Par ailleurs, comme $d \mid a\,b$ par définition et comme nous venons de dire $1 = d \wedge a$, le Théorème 21.1 de Gauss force $d \mid b$. Or par hypothèse, $d \mid c$ aussi. Enfin, comme b et c sont premiers entre eux, on a bien $d = 1$. □

Proposition 21.3. *Si a et b sont deux entiers premiers entre eux, et s'ils divisent tous deux un certain entier c, alors leur produit $a\,b$ divise aussi c.*

Démonstration. En effet, on peut écrire $a\,u = c$ avec un entier u.

Ensuite, comme b divise c et que b est premier à a, le Théorème 21.1 de Gauss nous dit que b doit diviser u, c'est-à-dire $b\,v = u$ avec un entier v.

Enfin, on conclut bien que ab divise c grâce à :

$$c \;=\; a\,u \;=\; ab\,v. \qquad \square$$

Encore une fois, ce dernier résultat est très intuitif : si a et b divisent c, une raison pour laquelle $a\,b$ ne doit pas forcément diviser c est que a et b auront peut-être des diviseurs en commun, et le produit $a\,b$ peut être « trop gros » pour diviser c. Par exemple 6 et 3 divisent 12, mais *pas* leur produit $3 \cdot 6 = 18$ [15].

Mais si on suppose a et b premiers entre eux, ils n'ont par définition aucun diviseur en commun, et on s'attend alors bien à ce que $a\,b$ divise c.

On peut aisément généraliser l'énoncé précédent pour obtenir le résultat suivant, très pratique.

Proposition 21.4. *Soient $a_1, \ldots, a_r$ avec $r \geqslant 2$ des entiers premiers entre eux deux à deux, c'est-à-dire satisfaisant :*

$$1 \;=\; \mathsf{pgcd}\left(a_{i_1},\, a_{i_2}\right) \qquad (\forall\, 1 \leqslant i_1 \neq i_2 \leqslant r).$$

S'ils divisent tous $a_1 \,|\, n$, …, $a_r \,|\, n$ un entier n donné, alors leur produit $a_1\, a_2 \cdots a_r$ divise aussi l'entier n.

Indication de preuve. Raisonner par récurrence sur le nombre $r \geqslant 2$ d'entiers a_i, en appliquant à chaque fois la Proposition 21.3. $\square$

Pour terminer cette Section **21**, revenons maintenant au Théorème 20.2 de « *Bézout-partout* [16] », afin de mieux présenter ce qu'il exprime véritablement.

Considérons le cas général où a et b sont deux entiers quelconques, non nécessairement premiers entre eux, et introduisons :

$$d \;:=\; \mathsf{pgcd}\,(a, b).$$

Comme $d \,|\, a$ et $d \,|\, b$ par définition, on peut factoriser :

$$a \;=\; d\,a' \qquad\qquad \text{et} \qquad\qquad b \;=\; d\,b',$$

au moyen de deux entiers uniques a' et b'. *Que dire alors de a' et de b' ?* Attention ! On doit tenir compte du fait que d est *maximal* parmi les diviseurs communs de a et de b !

Souvenons-nous en effet que le pgcd entre deux entiers représente *tout* ce que ces entiers ont en commun d'un point de vue arithmétique. On doit donc s'attendre à ce que a' et b' soient premiers entre eux — et c'est bien le cas !

Proposition 21.5. *Toute paire d'entiers $a, b \in \mathbb{Z}$ avec $(a, b) \neq (0, 0)$ se factorise sous la forme :*

$$a \;=\; a' \cdot \mathsf{pgcd}\,(a, b), \qquad\qquad a \;=\; b' \cdot \mathsf{pgcd}\,(a, b), \qquad\qquad \textit{avec} \qquad\qquad 1 \;=\; a' \wedge b'.$$

15. Tout le monde aura maintenant bien compris l'intérêt incomparable du cours d'arithmétique : deux étudiants ayant obtenu 3 sur 20 et 6 sur 20 à l'examen partiel de chimie des matériaux n'auront qu'à entrer en réaction multiplicative afin d'augmenter superbement leur note !

16. — c'est-à-dire partout dans les exercices de Travaux Dirigés, les Devoirs à la Maison, les Examens Partiels, et les Examens Terminaux —

Preuve. En effet, d'après le Théorème 20.2 de Bézout, $d := \mathsf{pgcd}\,(a, b)$ est combinaison linéaire entière de a et de b :

$$\begin{aligned} d &= u\,a + v\,b \\ &= u\,d\,a' + v\,d\,b', \end{aligned}$$

et après division par d de cette égalité, on voit bien que a' et b' sont premiers entre eux :

$$1 = u\,a' + v\,b'. \qquad \square$$

22. Équations linéaires à coefficients entiers

Grâce à toutes ces études préparatoires basées sur l'Algorithme d'Euclide, nous pouvons maintenant étudier un type de problèmes très anciens, auquel le pgcd est très fortement lié : les *équations linéaires à coefficients entiers*. Il s'agit d'équations de la forme :

$$a\,x + b\,y = c,$$

où a, b, c sont des entiers constants fixés dans $\mathbb{Z}$, et où on cherche des solutions (x, y) telles que $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ soient tous deux entiers.

Exemple 22.1. On dispose de billets de 20 et 50 euros. Combien y a-t-il de façons, et quelles sont-elles, de réunir la somme de 240 euros ?

Après quelques instants de réflexion, on comprend que la question revient précisément à trouver tous les entiers naturels $x \geqslant 0$ et $y \geqslant 0$ tels que :

$$20\,x + 50\,y = 240.$$

Sans s'aider d'un distributeur de billets, le lecteur est invité à résoudre ce petit exercice par lui-même. Mais pour la question mathématique générale, on admet que x et y puissent être négatifs, *i.e.* avoir un compte en banque à découvert.

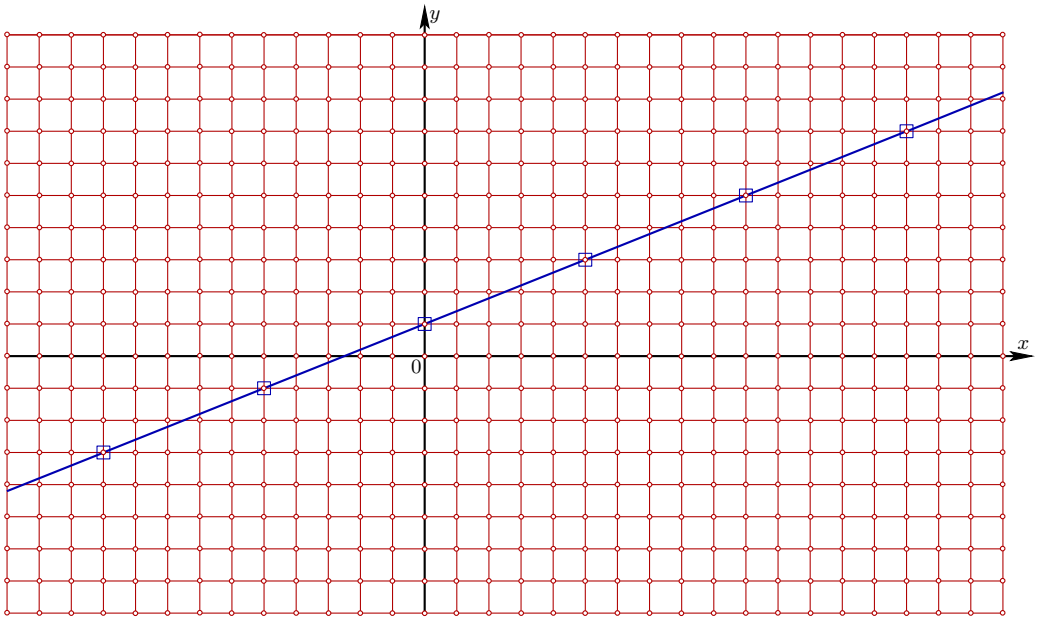
PIÈCES DE MONNAIE

Utilisation des congruences (modulo)
pour résoudre un problème de pièces de monnaie

J'achète 351 euros avec un lot de pièces de 17 et 18 euros.
Combien de pièces de chaque?

On pose l'équation	18 x + 17 y = 351
On cherche une solution simple, en utilisant le fait que 17 et 18 sont deux nombres consécutifs	18 – 17 = 1 18 x 351 – 17 x 351 = 351
Retranchons membre à membre les deux équations	18 x + 17 y = 351 18 x 351 – 17 x 351 = 351
Résultat	18(x - 351) = – 17(y + 351)
Et pour x	x = – 17(y + 351)/18 + 351
Si on divise x par 17, on obtient les restes suivants (x mod 17)	x mod 17 = 0 + 351 mod 17
Or, le reste de 351 par 17 est 11	x mod 17 = 11
Autrement dit x est un multiple de 17 plus 11	x = 17 k + 11
Même chose pour y	y = – 18(x - 351) /17 – 351
En reste par 18	y mod 18 = 9 (ou -9)
Valeur de y	y = – 18 k' + 9
Essayons k= k' = 0	18 x 11 + 17 x 9 = 198 + 153 = 351
Avec d'autres valeurs, on trouve des valeurs trop grandes pour x ou négatives pour y	18 x 28 + 17 x 9 = 657 18 x 11 – 17 x 9 = 45
Seule solution	x = 11 et y = 9

En fait, on sait bien que l'équation $a\,x + b\,y = c$ représente une *droite* dans le plan $\mathbb{R}^2$ muni des coordonnées (x, y). Ce plan est un *continu* 2-*dimensionnel*, c'est-à-dire que partout et à tous les endroits, il y a une infinité de points arbitrairement proches les uns des autres. Et nous savons bien qu'au voisinage de chacun de ses points, une droite dans le plan contient *aussi* une infinité de points arbitrairement proches les uns des autres.



Mais si on ne recherche que les solutions *entières* de $a\,x + b\,y = z$, on voit qu'on ne s'intéresse qu'à l'intersection de cette droite avec le *réseau* des nombres entiers :

$$\mathbb{Z} \times \mathbb{Z} = \big\{(x, y) \in \mathbb{R}^2 \colon\ x \in \mathbb{Z},\ y \in \mathbb{Z}\big\}.$$

Sur la figure, l'équation de la droite est $y = 1 + \frac{2}{5}\,x$, c'est-à-dire $-\,2\,x + 5\,y = 5$, et de cinq en cinq en montant du bas-gauche vers le haut-droite, les petits carrés bleus capturent les points dont les *deux* coordonnées sont entières.

Fixons donc $a, b, c \in \mathbb{Z}$, et examinons tout d'abord, le cas dégénéré où $a = b = 0$ pour lequel l'équation à résoudre :

$$a\,x + b\,y \ =\ 0\,x + 0\,y \ =\ 0 \overset{?}{=} c,$$

n'a de solutions que si $c = 0$, et dans ce cas :

$$0\,x + 0\,y \overset{\text{oui}}{=} 0 \qquad (\forall\, x,\, \forall\, y),$$

est trivialement satisfaite. L'ensemble des solutions est donc (doublement) infini.

On peut donc supposer dorénavant que a et b ne sont pas tous les deux nuls. Alors grâce au Grand Bézout, nous allons pouvoir résoudre totalement cette équation à inconnues entières.

Comme à l'accoutumée, notons $d := \mathsf{pgcd}\,(a, b)$, avec $d \neq 0$ puisque $(a, b) \neq (0, 0)$. Alors $a = d\,a'$ et $b = d\,b'$, avec a' et b' premiers entre eux, comme cela a été vu dans la Proposition 21.5. L'équation à résoudre :

$$a\,x + b\,y \ =\ c \qquad\qquad \Longleftrightarrow \qquad\qquad d\,a'\,x + d\,b'\,y \ =\ c,$$

force visiblement c, à droite, à être multiple de d, à gauche. Donc elle n'a *aucune* solution lorsque c n'est pas divisible par d — *Argl !*

Qu'à cela ne tienne, supposons dorénavant que $c = d\,c'$ est multiple de $d = \mathsf{pgcd}\,(a, b)$. L'équation à résoudre équivaut alors à :

$$d\,a'\,x + d\,b'\,y \ =\ d\,c', \qquad\qquad \Longleftrightarrow \qquad\qquad a'\,x + b'\,y \ =\ c'.$$

Alors le fait que $a' \wedge b' = 1$ *améliore énormément la situation.* Car si jamais on avait $c' = 1$, on reconnaîtrait une relation de Bézout :

$$a'\,x + b'\,y \;=\; 1,$$

dont on sait qu'il existe au moins une solution (x_*, y_*), d'après le Théorème 20.2.

Proposition 22.2. *Soient trois constantes entières quelconques* $a, b, c \in \mathbb{Z}$ *avec* $(a, b) \neq (0, 0)$. *Alors si* $d := \mathsf{pgcd}\,(a, b)$ *divise* c*, l'équation* $a\,x + b\,y = c$ *possède au moins une solution entière* $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$

Démonstration. En multipliant par c' une telle solution « *bézoutique* » (x_*, y_*) :

$$c'\,\big(\,a'\,x_* + b'\,y_* \;=\; 1\,\big) \qquad \text{devient} \qquad a'\,(\underbrace{c'\,x_*}_{=:\,x_0}) + b'\,(\underbrace{c'\,y_*}_{=:\,y_0}) \;=\; c',$$

on trouve au moins une solution (x_0, y_0) de $a'\,x_0 + b'\,y_0 = c'$, et enfin après multiplication par d :

$$d\,\big(\,a'\,x_0 + b'\,y_0 \;=\; c'\,\big) \qquad \text{devient} \qquad d\,a'\,x_0 + d\,b'\,y_0 \;=\; d\,c',$$

on trouve une solution (x_0, y_0) de l'équation proposée au début $a\,x_0 + b\,y_0 = c$. □

Et c'est encore de Bézout (partout) que nous allons nous servir pour établir le

Théorème 22.3. *Soient trois constantes entières quelconques* $a, b, c \in \mathbb{Z}$ *avec* $(a, b) \neq (0, 0)$. *Alors l'équation* $a\,x + b\,y = c$ *possède au moins une solution entière* $(x, y) \in \mathbb{Z} \times \mathbb{Z}$*, si et seulement si* $d := \mathsf{pgcd}\,(a, b)$ *divise* c.

Dans ce cas, en posant $a = d\,a'$, $b = d\,b'$ *avec* $a' \wedge b' = 1$*, et* $c = d\,c'$*, et en partant d'une solution particulière quelconque* $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ *de l'équation* [17] *:*

$$a\,x_0 + b\,y_0 \;=\; c,$$

l'ensemble de toutes *les solutions de* $a\,x + b\,y = c$ *est infini, et est égal précisément à :*

$$\mathsf{Sol} \;:=\; \Big\{\big(x_0 + b'k,\;\; y_0 - a'\,k\big) :\;\; k \in \mathbb{Z}\Big\}.$$

Effectivement, cet ensemble est infini, car il contient autant d'éléments qu'il y a d'entiers quelconques $k \in \mathbb{Z}$. Autrement dit, Sol est *paramétré* par $\mathbb{Z}$.

Démonstration. Quitte à échanger $a \longleftrightarrow b$, on peut supposer que $a \neq 0$. On suppose donc aussi que $c = d\,c'$, sinon, comme nous venons de le constater, il n'y aurait *aucune* solution.

Prenons alors une solution entière quelconque (x, y) de $a\,x + b\,y = c$. L'astuce intersidérale, utilisé dans toutes les galaxies mathématiques autant en Algèbre Linéaire que dans la théorie des Équations Différentielles, consiste à lui *soustraire* une solution particulière :

$$\begin{aligned} a\,x + b\,y \;&=\; c, \\ a\,x_0 + b\,y_0 \;&=\; c \end{aligned} \qquad \Longrightarrow \qquad a\,\big(x - x_0\big) + b\,\big(y - y_0\big) \;=\; 0,$$

afin de se ramener à une équation *plus simple* de second membre égal à 0, et avec *seulement deux termes*.

Dans cette équation, remplaçons $a = d\,a'$ (avec $a' \neq 0$ puisque $a \neq 0$), remplaçons $b = d\,b'$, puis divisons par d (non nul), pour obtenir une égalité :

$$a'\big(x - x_0\big) \;=\; b'\,\big(y_0 - y\big), \tag{22.4}$$

17. — nous venons d'argumenter qu'il en existe au moins une —

qui montre que a' *divise* $b'(y_0 - y)$. Mais comme $a' \wedge b' = 1$, le Théorème 21.1 de Gauss force $y_0 - y$ à être divisible par a'.

Autrement dit, il existe $k \in \mathbb{Z}$ tel que :

$$y_0 - y \;=\; a'\,k,$$

ce qui montre que $y = y_0 - a'k$ est de la forme annoncée dans Sol.

Ensuite, en remplaçant dans (22.4), nous obtenons $a'(x - x_0) = b'a'k$, et après division par a' qui est non nul, nous obtenons aussi l'expression de x annoncée dans Sol :

$$x \;=\; x_0 + b'\,k.$$

En définitive, nous venons d'achever de faire voir que si (x, y) est une solution entière quelconque de $a\,x + b\,y = c$, alors elle est nécessairement de la forme annoncée dans Sol. Yep !

Mais pour terminer rigoureusement la démonstration, il reste encore à vérifier que $x = x_0 + b'k$, $y = y_0 - a'k$ avec $k \in \mathbb{Z}$ *arbitraire* est *effectivement* une solution, ce qui est vrai grâce à une annihilation couplée :

$$\begin{aligned} c &\overset{?}{=} a\,x + b\,y \\ &= d\,a'\,\big(x_0 + b'\,k\big) + d\,b'\,\big(y_0 - a'\,k\big) \\ &= a\,x_0 + \underline{d\,a'\,b'\,k}_{\circ} + b\,y_0 - \underline{d\,b'\,a'\,k}_{\circ} \\ &= c \qquad \text{OUI.} \end{aligned}$$

□

23. Plus Petit Commun Multiple ppcm

La notion de *plus petit commun multiple* est très proche de celle de *plus grand commun diviseur* — elle est en quelque sorte « *duale* ».

Définition 23.1. Le ppcm entre deux entiers positifs $a \geqslant 0$ et $b \geqslant 0$ avec $(a, b) \neq (0, 0)$ est l'entier :

$$\begin{aligned} \mathsf{ppcm}\,(a, b) \;&:=\; \mathsf{min}\,\Big\{n \in \mathbb{N}^* :\;\; n \text{ multiple de } a,\;\; n \text{ multiple de } b\Big\} \\ &=\; \mathsf{min}\,\Big\{n \in \mathbb{N}^* :\;\; a \,|\, n,\;\; b \,|\, n\Big\}. \end{aligned}$$

On convient que $\mathsf{ppcm}\,(0, 0) := 0$, et pour $a, b \in \mathbb{Z}$ de signe quelconque, on pose :

$$\mathsf{ppcm}\,\big(|a|,\, |b|\big) \;:=\; \mathsf{ppcm}\,(a, b).$$

Évidemment, on a pour $a, b \geqslant 0$:

$$\mathsf{ppcm}\,(a, b) \;=\; \mathsf{ppcm}\,(b, a), \qquad\qquad \mathsf{ppcm}\,(a, 0) \;=\; a, \qquad\qquad \mathsf{ppcm}\,(0, b) \;=\; b.$$

Donc puisque le signe ne compte pas, nous pouvons supposer à partir de maintenant que $a \geqslant 1$ et $b \geqslant 1$.

Il existe effectivement un lien fort entre pgcd et ppcm. Déjà, il est clair que $a\,b$ est toujours un multiple commun à a et à b, mais ce n'est cependant pas toujours leur ppcm, car on peut voir qu'il existe souvent des multiples communs à a et à b qui sont plus petits.

Soit en effet $d := \mathsf{pgcd}\,(a, b)$. On peut écrire $a = d\,a'$ et $b = d\,b'$, où a' et b' sont premiers entre eux. Alors $d\,a'\,b'$ est toujours un multiple de a, car il s'agit de $a\,b'$. Mais c'est aussi toujours un multiple de b, puisqu'on peut aussi l'écrire $b\,a'$. C'est donc un multiple commun à a et à b !

Or on voit bien que $d\,a'\,b'$ est en général [18] plus petit que :

$$a\,b \;=\; d^2\,a'\,b'.$$

En fait, nous pouvons démontrer que cet entier $d\,a'\,b'$ *est* le ppcm de a et de b.

Théorème 23.2. *Soient deux entiers $a \geqslant 1$ et $b \geqslant 1$. Soient aussi a', b' avec $1 = a' \wedge b'$ définis par $a = d\,a'$, $b = d\,b'$. Alors :*

$$d \;:=\; \mathsf{pgcd}\,(a,b) \qquad\qquad \textit{et} \qquad\qquad m \;:=\; \mathsf{ppcm}\,(a,b),$$

satisfont :

$$m \;=\; \frac{a\,b}{d} \;=\; d\,a'\,b'.$$

Démonstration. Comme $a \,|\, m$, il existe un entier $k \geqslant 1$ tel que :

$$m \;=\; a\,k \;=\; d\,a'\,k. \tag{23.3}$$

Or $b = d\,b'$ divise aussi m, c'est-à-dire $d\,b' \,\big|\, d\,a'\,k$, d'où $b' \,|\, a'\,k$ après division (simplification) par $d \geqslant 1$. Mais comme b' est premier à a', le Théorème 21.1 de Gauss force $k = b'\,k'$ à être multiple de b', avec $k' \geqslant 1$ entier.

En revenant à (23.3), il vient alors :

$$m \;=\; d\,a'\,b'\,k'.$$

Autrement dit, nous venons de démontrer que tout entier m qui est multiple de a et de b est un multiple, au moyen de $k' \geqslant 1$, de $d\,a'\,b'$.

Mais comme nous avons compris plus haut que $d\,a'\,b'$ *est déjà* multiple de a et de b, et comme m est par définition le *plus petit* multiple commun, il faut choisir $k' := 1$, ce qui conclut l'argumentation. □

Corollaire 23.4. *Avec $a \geqslant 1$ et $b \geqslant 1$ entiers, le produit $a\,b$ coïncide avec* $\mathsf{ppcm}\,(a,b)$ *lorsque, et seulement lorsque* $\mathsf{pgcd}\,(a,b) = 1$. □

24. Décomposition des entiers en facteurs premiers

Introduisons maintenant une notation primordiale, et toujours très riche en mystères mathématiques inexpugnables.

Définition 24.1. Un nombre entier $p \in \mathbb{N}$ est dit *premier* si $p \geqslant 2$ et si ses seuls diviseurs positifs sont $d = 1$ et $d = p$.

Par exemple, 37 est un nombre premier. Il est important de faire remarquer que 1 n'est *pas* considéré comme étant un nombre premier. La plupart du temps, les nombres premiers seront désignés au moyen de la lettre p.

L'ensemble des nombres premiers sera noté :

$$\mathscr{P} \;:=\; \big\{2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ \ldots\ \big\},$$

18. — dès que $d \geqslant 2$, car alors $d^2 > d$, strictement —

Voici d'ailleurs la liste complète de tous ceux qui sont inférieurs à 1 000 :

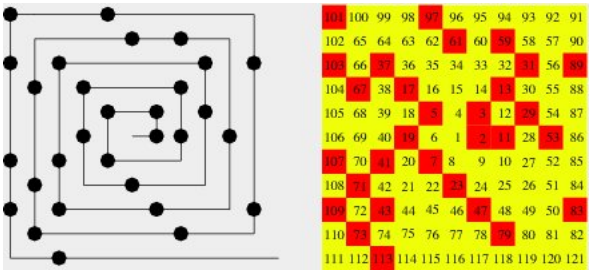
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137,
139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211,
223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283,
293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379,
383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461,
463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563,
569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643,
647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739,
743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829,
839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937,
941, 947, 953, 967, 971, 977, 983, 991, 997.

Certaines représentations imagées sont plus parlantes.

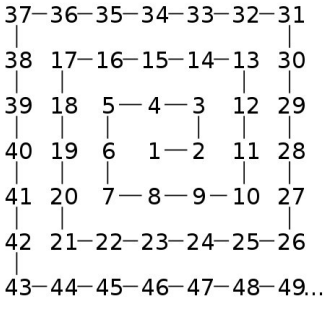
2 3 5 7 11 13 17
19 23 29 31 37 41
43 47 53 59 61 67
71 73 79 83 89 97

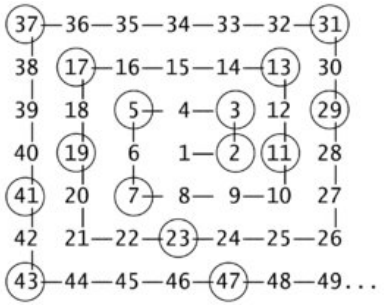
0									
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

En mathématiques, la *spirale d'Ulam*, ou spirale des nombres premiers est une méthode simple pour représenter les nombres premiers qui révèle un motif qui n'a jamais été pleinement expliqué. Elle fut découverte par le mathématicien Stanislaw Ulam, lors d'une conférence scientifique en 1963.

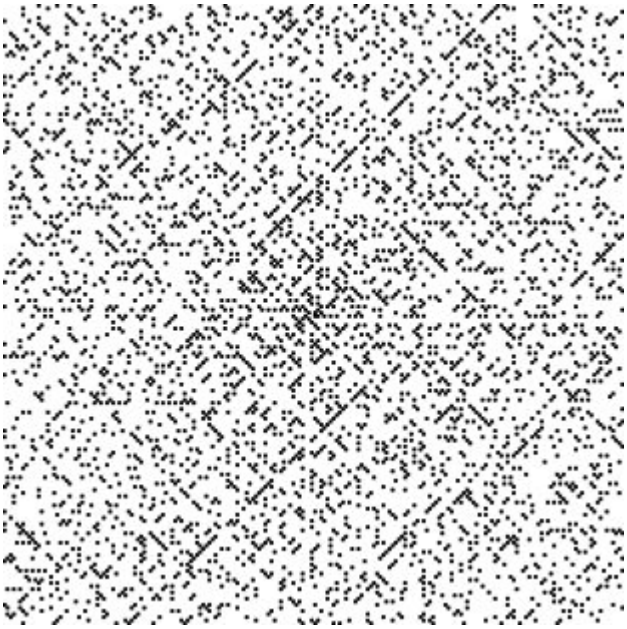


Ulam se trouvait coincé, contraint d'écouter « un exposé très long et très ennuyeux ». Il passa son temps à crayonner et se mit à gribouiller des entiers consécutifs, commençant par 1 au centre, dans une espèce de spirale tournant dans le sens inverse des aiguilles d'une montre. Il obtint une grille régulière de nombres, démarrant par 1 au centre, et spiralant vers l'extérieur, comme ci-dessous. Puis, Ulam entoura tous les nombres premiers, et il obtint alors l'image suivante.





À sa surprise, les nombres entourés tendaient à s'aligner le long de lignes diagonales. L'image suivante illustre ceci. C'est une spirale d'Ulam de 200×200, où les nombres premiers sont des points noirs. Des *diagonales noires* sont clairement visibles.



Il apparaît donc des lignes diagonales comportant une grande quantité de nombres premiers. Ceci semble rester vrai, même si le nombre central au départ est plus grand que 1. On remarque donc qu'il semble exister une infinité d'entiers naturels a, b et c tels que la fonction :

$$f(n) := a\,n^2 + b\,n + c$$

génère un nombre extraordinairement grand de nombres premiers. Néanmoins, aucune démonstration n'est connue sur Terre qu'il existe une *infinité* de nombres premiers de la forme $a\,n^2 + b\,n + c$ pour $a \neq 0$, b, c bien choisis.

Pour les traqueurs de nombres premiers, ces nombres étaient familiers. Au XVIII$^{\text{ième}}$ siècle, Euler avait avancé la formule n^2+n+17 qui, pour des valeurs successives de n, donnait des nombres premiers de $n = 0$ à $n = 15$. En fait, ces seize nombres premiers sont ceux qui apparaissent sur la diagonale principale de la spirale d'Ulam avec 17 comme nombre central de départ : 17, 19, 23, 29, 37, 47, 59, 73, 89, 107, 127, 149, 173, 199, 227 et 257.

Euler proposa une autre formule, $n^2 - n + 41$ qui, pour des valeurs successives de n entre 1 et 40, ne produit que des nombres premiers.

Par calcul sur ordinateur, on montra que la formule d'Euler $n^2 - n + 41$ était étonnamment bonne, puisqu'elle engendre des nombres premiers inférieurs à dix millions dans 47,5% des cas.

Après cette parenthèse culturelle, revenons au cours formel.

Proposition 24.2. *Deux nombres premiers $p \neq p' \in \mathscr{P}$* distincts *sont toujours premiers entre eux $p \wedge p' = 1$.*

Autrement dit, leur pgcd est égal à 1.

Démonstration. Notons donc $d := \mathsf{pgcd}\,(p, p')$. On a $d \,|\, p$ et $d \,|\, p'$, et comme les seuls diviseurs d'un nombre premier sont 1 et lui-même, il vient :

$$\Big(\ d = 1 \quad \text{ou} \quad d = p\ \Big) \qquad \text{et} \qquad \Big(\ d = 1 \quad \text{ou} \quad d = p'\ \Big).$$

La seule possibilité commune — c'est-à-dire satisfaisant ce « et » — est $d = 1$. □

Ensuite, nous pouvons obtenir l'énoncé suivant, dans lequel le symbole $\nmid$ signifie « *ne divise pas* ».

Proposition 24.3. *Soit un nombre premier $p \in \mathscr{P}$. Alors, pour tout $a \in \mathbb{Z}$, on a équivalence entre :*

(i) *p et a sont premiers entre eux ;*

(ii) *$p \nmid a$.* □

Démonstration. L'implication **(i)** $\Longrightarrow$ **(ii)** est évidente, car en partant de $1 = p \wedge a$, si on avait non **(ii)**, c'est-à-dire si p divisait a, alors $\mathsf{pgcd}\,(p, a) = p$ serait > 1 !

Montrons maintenant **(ii)** $\Longrightarrow$ **(i)**. Soit $d := \mathsf{pgcd}\,(p, a)$, d'où $d \,|\, p$, donc $d = 1$ ou $d = p$ car p est premier. Mais $d = p$ est impossible, car $d \,|\, a$ et $p \nmid a$ par l'hypothèse **(ii)**. Donc $d = 1 = p \wedge a$, c'est-à-dire que p et a sont premiers entre eux. □

On en déduit un troisième énoncé, classique et célèbre.

Théorème 24.4. [Euclide] *Soit un nombre premier $p \in \mathscr{P}$. Alors pour tous $a, b \in \mathbb{Z}$, on a :*

$$p \,\big|\, a\,b \qquad \Longrightarrow \qquad \Big(\ p \mid a \quad \textit{ou} \quad p \mid b\ \Big).$$

Si de plus a et b sont premiers, alors $p = a$ ou $p = b$.

Autrement dit, un « atome » donné ne peut se trouver que dans une seule des deux molécules, et si les molécules elles-mêmes sont des atomes, alors l'atome donné est *égal* à l'une des deux.

Démonstration. Soient $a, b \in \mathbb{Z}$ avec $p \,|\, a\,b$. Si $p \,|\, a$, il n'y a rien à faire.

Si $p \nmid a$, alors la Proposition 24.3 précédente montre que a et p sont premiers entre eux. Mais alors le Théorème 21.1 de Gauss garantit que $p \,|\, b$, ce qui était annoncé.

Quand a et b sont premiers, par définition, leurs seuls diviseurs sont 1, a et 1, b. On vient d'obtenir $p \,|\, a$ ou $p \,|\, b$. Si c'est $p \,|\, a$, alors $p = a$. Si c'est $p \,|\, b$, alors $p = b$. □

La généralisation suivante du Théorème 24.4 d'Euclide va s'avérer d'une utilité extrêmement importante sur le plan technique dans ce qui va suivre.

Proposition 24.5. *Soit un nombre premier $p \in \mathscr{P}$. Alors pour tous $a, b, c, \ldots, \ell \in \mathbb{Z}$, on a :*

$$p \,\big|\, a\,b\,c\cdots\ell \qquad \Longrightarrow \qquad \Big(\ p \mid a \quad \textit{ou} \quad p \mid b \quad \textit{ou} \quad p \mid c \quad \textit{ou} \quad \cdots \quad \textit{ou} \quad p \mid \ell\ \Big).$$

Si de plus tous les facteurs $a, b, \ldots, \ell$ sont premiers, alors $p = a$, ou $p = b$, …, ou $p = \ell$.

Démonstration. Il suffit de raisonner par récurrence sur le nombre de facteurs en appliquant successivement le Théorème 24.4 précédent. □

Terminologie 24.6. Étant donné un nombre entier $n \geqslant 2$, on appelle *diviseur* de n tout entier $d \mid n$ qui divise n. On dit que d est un *diviseur strict* lorsqu'on a de plus $1 < d < n$.

Alors on peut écrire $n = d\,m$ avec $m \in \mathbb{N}$. Dans le cas strict $1 < d < m$, observons que l'on a aussi $1 < m < n$. En effet, si on avait $m = 1$, on aurait $n = d$, ce qui n'est pas. Si on avait $m = n$, on aurait $1 = d$, ce qui n'est pas non plus.

Nous pouvons dorénavant énoncer et démontrer le résultat principal de ce chapitre, « découpé » en deux théorèmes, d'existence, puis d'unicité.

Théorème 24.7. *Tout entier $n \geqslant 2$ se décompose comme produit d'un nombre fini $r \geqslant 1$ de puissances de nombres premiers :*

$$n \;=\; p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

avec $2 \leqslant p_1 < \cdots < p_r$ premiers, et avec des exposants $\alpha_1 \geqslant 1$, …, $\alpha_r \geqslant 1$.

Voici trois exemples de telles décompositions :

$$\begin{aligned} 888 &= 2^3 \cdot 3 \cdot 37, \\ 1\,235 &= 5 \cdot 13 \cdot 19, \\ 5\,040 &= 5 \cdot 2^4 \cdot 3^2 \cdot 7. \end{aligned}$$

Il s'agit donc de décompositions « atomiques » de chaque « nombre entier-molécule ». Ce théorème s'appelle *Théorème fondamental de l'arithmétique*, car la structure arithmétique d'un nombre entier dépend uniquement de sa décomposition en produit de nombres premiers. Les nombres premiers sont ainsi les « particules élémentaires » qui constituent l'arithmétique (labyrinthique) des nombres entiers.

Rappelons que l'entier 1 n'est pas un nombre premier. Pourquoi ? Parce que multiplier un entier n par 1 ne le change en rien : $n \cdot 1 = n$, et donc, 1 ne peut en aucun cas être considéré comme une « brique » de construction.

Démonstration. Expliquons donc l'*existence* d'une telle décomposition.

À cet effet, introduisons l'ensemble $\overline{E}$ des entiers naturels $\overline{n} \geqslant 2$ qui ne s'écrivent *pas* comme un produit (fini) $\prod\, p_i^{\alpha_i}$ de nombres premiers, avec certaines puissances lorsqu'il y a des répétitions. Notre but est de montrer que $\overline{E} = \emptyset$.

Supposons alors par l'absurde que $\overline{E} \neq \emptyset$. Grâce au Théorème 4.1, $\overline{E}$ admet alors un *plus petit élément*, disons $\overline{n} \in \overline{E}$.

Clairement, $\overline{n}$ ne peut pas être égal à un nombre premier $p \in \mathscr{P}$. Mais alors, comme $\overline{n}$ n'est *pas* un nombre premier, il existe forcément (et logiquement), d'après la Définition 24.1, un diviseur *strict* d de $\overline{n}$, qui satisfait l'inégalité $1 < d < \overline{n}$. On a ainsi $\overline{n} = d\,m$, avec $m \in \mathbb{N}$ satisfaisant aussi $1 < m < \overline{n}$.

D'après la minimalité de $\overline{n}$, ces deux entiers $d < \overline{n}$ et $m < \overline{n}$ n'appartiennent *pas* à $\overline{E}$, et donc eux, il *peuvent* tous deux s'écrire comme un produit fini de puissances de nombres premiers :

$$d \;=\; p_1^{\gamma_1} \cdots p_i^{\gamma_i} \qquad \text{et} \qquad d \;=\; q_1^{\delta_1} \cdots q_j^{\delta_j}.$$

Mais alors, il clair et évident que leur *produit* $d\,m \;=\; \overline{n}$ devient aussi un produit fini $\prod\, p_i^{\gamma_i} \prod\, q_j^{\delta_j}$ de puissances de nombres premiers — ce qui est une contradiction manifeste. Donc $\overline{E} = \emptyset$, comme voulu. □

Ensuite, traitons de l'*unicité* de la décomposition en nombres premiers.

Théorème 24.8. *La décomposition de tout entier $n \geqslant 2$ en produit de nombres premiers :*

$$n \;=\; p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

avec $2 \leqslant p_1 < \cdots < p_r$ premiers et $\alpha_1, \ldots, \alpha_r \geqslant 1$, est unique*, au sens où si l'on a aussi :*

$$n \;=\; q_1^{\beta_1} \cdots q_s^{\beta_s},$$

avec $2 \leqslant q_1 < \cdots < q_s$ premiers et $\beta_1, \ldots, \beta_s \geqslant 1$, alors en fait, tous ces citoyens entiers sont égaux :

$$s \;=\; r, \qquad q_1 = p_1, \;\ldots\; q_r = p_r, \qquad \beta_1 = \alpha_1, \;\ldots\; \beta_r = \alpha_r.$$

Ce théorème constitue le *fondement absolu* de toute l'arithmétique, mais il cache encore de très grands mystères mathématiques toujours non résolus actuellement.

Démonstration. Ainsi, supposons que :

$$p_1^{\alpha_1} \cdots p_r^{\alpha_r} \;=\; n \;=\; q_1^{\beta_1} \cdots q_s^{\beta_s}.$$

Pour tout indice $i = 1, \ldots, r$, si on écrit $p_i^{\alpha_i} = p_i \, p_i^{\alpha_i - 1}$, alors cette identité :

$$p_i \underbrace{p_1^{\alpha_1} \cdots p_i^{\alpha_i - 1} \cdots p_r^{\alpha_r}}_{=:\, u \text{ nombre entier}} \;=\; q_1^{\beta_1} \cdots q_s^{\beta_s},$$

montre que p_i divise $q_1^{\beta_1} \cdots q_s^{\beta_s}$, qui est un produit de nombres premiers. Et grâce à la Proposition 24.5 — encore elle ! —, nous déduisons que p_i doit être égal à l'un des nombres premiers $q_1, \ldots, q_s$.

En raisonnant de manière symétrique, on déduit aussi que chaque q_j avec $1 \leqslant j \leqslant s$ doit être égal à l'un des p_i. Par conséquent, ces deux ensembles de nombres premiers doivent coïncider :

$$\big\{p_1, \ldots, p_r\big\} \;=\; \big\{q_1, \ldots, q_s\big\}.$$

Or comme ces deux collections de nombres premiers distincts $p_1 < \cdots < p_r$ et $q_1 < \cdots < q_s$ sont ordonnées de manière strictement croissante, cela force $r = s$ ainsi que $p_1 = q_1$, …, $p_r = q_r$.

Nous avons donc obtenu l'identité :

$$p_1^{\alpha_1} \cdots p_i^{\alpha_i} \cdots p_r^{\alpha_r} \;=\; n \;=\; p_1^{\beta_1} \cdots p_i^{\beta_i} \cdots p_r^{\beta_r},$$

et il nous reste encore à montrer l'égalité $\alpha_i \stackrel{?}{=} \beta_i$ des exposants, pour tout $i = 1, \ldots, r$.

Si on avait $\alpha_i > \beta_i$, en divisant cette identité par $p_i^{\beta_i}$, on obtiendrait une égalité :

$$\underbrace{p_1^{\alpha_1} \cdots p_i^{\alpha_i - \beta_i} \cdots p_r^{\alpha_r}}_{= p_i \text{ fois un nombre entier}} \;=\; n \;=\; p_1^{\beta_1} \cdots p_{i-1}^{\beta_{i-1}} \cdot 1 \cdot p_{i+1}^{\beta_{i+1}} \cdots p_r^{\beta_r},$$

qui montrerait que p_i à gauche *divise* le nombre entier à droite, et alors la Proposition 24.5 — encore et toujours elle ! — forcerait p_i à être *égal* à l'un des nombres premiers :

$$p_1, \;\ldots,\; p_{i-1}, \;p_{i+1}, \;\ldots,\; p_r,$$

ce qui n'est pas.

En raisonnant de manière symétrique, on trouve aussi que $\alpha_i < \beta_i$ est absurde. En conclusion, $\alpha_i = \beta_i$, pour tout $i = 1, \ldots, r$. Cela achève la démonstration. □

Question 24.9. *Y a-t-il un nombre fini, ou un nombre infini, de nombres premiers ?*

En explorant les nombres premiers « à la main » — c'est-à-dire sur papier ou sur ordinateur —, on devine qu'il est toujours possible de trouver des nombres premiers de plus en plus grands, toujours nouveaux. Cependant de simples observations expérimentales ne constituent pas une véritable démonstration mathématique. Une argumentation rigoureuse très élégante du fait qu'il existe une infinité de nombres premiers est connue depuis Euclide — la voici.

Théorème 24.10. *Il existe une infinité de nombres premiers.*

Démonstration. Supposons par l'absurde qu'il n'y ait qu'un nombre *fini* $\mathrm{K} < \infty$ de nombres premiers, et notons-les alors :

$$q_1 < \cdots < q_k < \cdots < q_{\mathrm{K}},$$

avec évidemment $q_1 = 2$, $q_2 = 3$, $q_3 = 5$, *etc.*, puisque tout le monde connaît les tous *premiers* nombres premiers !

Par une immense astuce, introduisons alors l'entier :

$$\mathrm{N} := 1 + 2 \cdot 3 \cdot 5 \cdots q_k \cdots q_{\mathrm{K}},$$

qui a la propriété forte d'être congru à 1 modulo *tous* ces nombres premiers :

$$\mathrm{N} \equiv 1 \mod q_k, \qquad \forall\ 1 \leqslant k \leqslant \mathrm{K}. \tag{24.11}$$

Mais alors le Théorème 24.7 fondamental de l'arithmétique s'appliquerait à cet entier N pour le représenter comme un produit fini :

$$\mathrm{N} = q_{i_1}^{\alpha_1} \cdots q_{i_r}^{\alpha_r},$$

de certaines puissances de nombres premiers $q_{i_1} < \cdots < q_{i_r}$ qui *appartiendraient forcément tous* à cette liste finie $\{q_1, \ldots, q_{\mathrm{K}}\}$, ce qui impliquerait par exemple :

$$\mathrm{N} \equiv 0 \mod q_{i_1},$$

en contradiction manifeste avec (24.11) pour $k = i_1$.

Notre hypothèse était donc fausse, ce qui démontre bien qu'il existe une *infinité* de nombres premiers. □

Proposition 24.12. *Soit un nombre premier $p \in \mathscr{P}$. Alors pour tout exposant $\alpha \geqslant 1$, les seuls diviseurs de p^α sont :*

$$1,\ p,\ p^2,\ \ldots,\ p^{\alpha-1},\ p^\alpha.$$

Démonstration. Soit donc un diviseur $d \,|\, p^\alpha$. Grâce au Théorème 24.7, on sait maintenant que d est un produit de nombres premiers. Prenons alors un facteur premier quelconque q de d, d'où $q \,|\, d$. Par transitivité de la relation de divisibilité $q \,|\, d \,|\, p^\alpha$, il vient $q \,|\, p^\alpha$. Autrement dit, q divise $p \cdot p \cdots p$, avec α facteurs identiques.

Mais alors grâce à la Proposition 24.5, q doit être égal à l'un de ces facteurs premiers identiques, donc forcément $q = p$!

Ainsi, tous les diviseurs premiers q de p^α sont égaux à p, donc d est de la forme $d = p^\beta$, avec $\beta \leqslant \alpha$ puisque $d \,|\, p^\alpha$ — c'est-à-dire $d\,u = p^\alpha$ — implique $d \leqslant p^\alpha$ et $p^\beta \leqslant p^\alpha$ implique $\beta \leqslant \alpha$.

Enfin, comme chaque p^β avec $0 \leqslant \beta \leqslant \alpha$ divise manifestement $p^\alpha = p^\beta\, p^{\alpha-\beta}$, le travail est terminé. □

Revenons à la factorisation générale :

$$n \,=\, p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Dans cette factorisation, on peut en fait « faire apparaître » *tous* les nombres premiers $p \in \mathscr{P}$, *y compris* ceux qui sont distincts de $p_1, \ldots, p_r$, simplement en les mettant à la puissance 0, car $p^0 = 1$ — par exemple :

$$10 \,=\, 2 \cdot 5 \,=\, 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdots .$$

Notation 24.13. On note la décomposition d'un entier $n \in \mathbb{Z}$ quelconque :

$$n \,=\, \varepsilon \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(n)},$$

où :

□ $\varepsilon = \pm 1$ est le *signe* de n ;

□ $\mathsf{v}_p(n)$ est un exposant entier, appelé la *valuation p-adique* de n, et qui vaut presque toujours 0, sauf pour un nombre *fini* de nombres premiers $p \in \mathscr{P}$.

Par convention, on pose aussi $\mathsf{v}_p(0) := \infty$.

En effet, dans $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, il y a toujours un nombre *fini* de facteurs premiers. Tous les $p \neq p_1, \ldots, p_r$ sont mis à la puissance 0, ce qui donne la neutralité Suisse $1 = p^0$.

Proposition 24.14. *Soit un nombre premier $p \in \mathscr{P}$. Alors pour tous entiers relatifs $m, n \in \mathbb{Z}$, les trois propriétés suivantes sont satisfaites.*

(1) *On a l'égalité :*

$$\mathsf{v}_p\big(m+n\big) \;\geqslant\; \mathsf{min}\,\big(\mathsf{v}_p(m),\, \mathsf{v}_p(n)\big).$$

(2) *On a :*

$$\mathsf{v}_p\big(m\,n\big) \,=\, \mathsf{v}_p(m)\,\mathsf{v}_p(n).$$

(3) *On a $m \,|\, n$ si et seulement si $\mathsf{v}_p(m) \leqslant \mathsf{v}_p(n)$ pour tout premier $p \in \mathscr{P}$.*

Démonstration. Expliquons seulement **(3)**, laissant **(1)** et **(2)** en exercice.

$\Longrightarrow$ Supposons donc $m \,|\, n$, c'est-à-dire $m\,u = n$, pour un entier $u \in \mathbb{Z}$. Décomposons chacun de ces trois entiers en facteurs premiers :

$$\begin{aligned}
m \,&=\, \varepsilon \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(m)}, & \varepsilon \,&=\, \pm 1,\\
n \,&=\, \delta \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(n)}, & \delta \,&=\, \pm 1,\\
u \,&=\, \gamma \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(u)}, & \gamma \,&=\, \pm 1,
\end{aligned}$$

et écrivons vraiment l'égalité $m\,u = n$:

$$\varepsilon \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(m)} \;\gamma \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(u)} \;=\; \delta \prod_{p \in \mathscr{P}} p^{\mathsf{v}_p(n)}.$$

Les signes doivent s'accorder (diplomatie oblige), c'est-à-dire $\varepsilon\,\gamma = \delta$. Ensuite, par la règle d'additivité des puissances, $p^{\alpha} \cdot p^{\alpha'} = p^{\alpha+\alpha'}$, il vient :

$$\mathsf{v}_p(m) + \mathsf{v}_p(u) \,=\, \mathsf{v}_p(n),$$

donc puisque $\mathsf{v}_p(u) \geqslant 0$ est toujours vrai car $\mathsf{v}_p(u) \in \mathbb{N}$ par définition, on a bien $\mathsf{v}_p(m) \leqslant \mathsf{v}_p(n)$, pour tout premier $p \in \mathscr{P}$.

$\Longleftarrow$ Réciproquement, en supposant que $\mathsf{v}_p(m) \leqslant \mathsf{v}_p(n)$ pour tout $p \in \mathscr{P}$, on trouve facilement le multiplicateur u satisfaisant $m\,u = n$:

$$u \;:=\; \tfrac{\varepsilon}{\delta} \prod_{p\in\mathscr{P}} p^{\mathsf{v}_p(n)-\mathsf{v}_p(m)},$$

avec $\frac{\varepsilon}{\delta} = \frac{\pm 1}{\pm 1} = \pm 1$ (of course !), et avec u entier, puisque tous les exposants sont *entiers*. □

Enfin, énonçons une représentation très naturelle et très intuitive du pgcd et du ppcm, dont la vérification formelle est laissée en exercice d'assimilation du cours.

Théorème 24.15. *Pour $a, b \in \mathbb{Z}$ quelconques non tous les deux nuls, on a :*

$$\mathsf{pgcd}\,(a,b) \;=\; \prod_{p\in\mathscr{P}} p^{\mathsf{min}\,(\mathsf{v}_p(a),\,\mathsf{v}_p(b))},$$

$$\mathsf{ppcm}\,(a,b) \;=\; \prod_{p\in\mathscr{P}} p^{\mathsf{max}\,(\mathsf{v}_p(a),\,\mathsf{v}_p(b))}.$$ □

Les notions de pgcd et de ppcm se généralisent à 3, 4, 5, *etc.* entiers, comme dans les Définitions 19.1 et 23.1.

Grâce à une application directe du Théorème 24.15 qui précède, on vérifie alors que :

$$\mathsf{pgcd}\,\big(a,b,c\big) \;=\; \mathsf{pgcd}\,\big(\mathsf{pgcd}\,(a,b),\,c\big),$$

$$\mathsf{ppcm}\,\big(a,b,c\big) \;=\; \mathsf{ppcm}\,\big(\mathsf{ppcm}\,(a,b),\,c\big),$$

ce qui signifie qu'on peut ramener le calcul du pgcd et/ou du ppcm de *plusieurs* entiers à des calculs successifs de pgcd et/ou de ppcm *classiques* entre *paires* d'entiers.

25. Théorème de Fermat

En mathématiques, le (petit) théorème de Fermat est un résultat de l'arithmétique modulaire, qui peut aussi se démontrer avec les outils de l'arithmétique élémentaire. Il doit son nom à Pierre de Fermat, qui l'énonce pour la première fois [19] en 1640.

19. La première apparition connue de l'énoncé de ce théorème provient d'une lettre de Fermat à Frénicle de Bessy datée de 1640. On peut y lire ceci :

> *Tout nombre premier mesure infailliblement une des puissances -1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné -1 ; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.*

En termes modernes, Fermat exprime que pour tout nombre premier p et tout nombre a premier avec p, il existe un entier t tel que p divise $a^t - 1$, et, t étant le plus petit entier vérifiant ceci, t divise $p-1$, et tous les multiples n de t vérifient que p divise $a^n - 1$.

Comme habituellement dans sa correspondance Fermat ne donne aucune démonstration de ce résultat, ni même, comme il le fait parfois, d'indications à propos de celle-ci, mais il précise :

> *Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers ; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.*

À cette époque, il est d'usage de ne pas publier les preuves des théorèmes. Ainsi Leibniz rédige une démonstration vers 1683 mais ne la publie pas. En 1741, 1750 et 1761, Euler en publie deux qui procèdent par récurrence et utilisent le développement du binôme, et une qui étudie la répartition des restes modulo le nombre premier considéré. On trouve cette dernière en 1801 dans les *Disquisitiones arithmeticae* de Gauss.

Ce théorème dispose de nombreuses applications, à la fois en arithmétique modulaire et en cryptographie.

Théorème 25.1. [de Fermat] *Si p est un nombre premier, alors pour tout entier $a \in \mathbb{Z}$ qui est* non divisible par *p, l'entier a^{p-1} est congru à 1 modulo p :*

$$a^{p-1} \equiv 1 \mod p.$$

Évidemment, il faut exclure $a \equiv 0 \mod p$, car $0^{p-1} \equiv 0 \mod p$ n'est pas congru à 1 !

Mais si on multiplie par a, on obtient un énoncé essentiellement équivalent qui est est vrai sans exception.

Théorème 25.2. [de Fermat-bis] *Si p est un nombre premier, alors pour tout entier $a \in \mathbb{Z}$:*

$$a^p \equiv a \mod p.$$

Voici quelques exemples non triviaux de ce second énoncé.

- Pour $p = 2$, les entiers $a \in \mathbb{Z}$ sont congrus, ou bien à 0, ou bien à 1, modulo 2, et on a $0^2 \equiv 0$ ainsi que $1^2 \equiv 1$ modulo 2 — trivialement.
- $5^3 - 5 = 120$ est bien divisible par 3.
- $2^5 - 2 = 30$ est bien divisible par 5.
- $(-3)^7 + 3 = -2184 - 7 \cdot 312$ est bien divisible par 7.
- Avec le nombre premier $p = 97$ et avec $a = 2$:

$$\begin{aligned} 2^{97} - 2 &= 158\,456\,325\,028\,528\,675\,187\,087\,900\,670 \\ &= 97 \cdot 1\,633\,570\,361\,118\,852\,321\,516\,370\,110, \end{aligned}$$

est bien divisible par 97.

Autre illustration : *Que vaut le reste de la division de 5^{400} par le nombre premier 397 ?* Le Théorème 25.2 de Fermat-bis donne :

$$5^{397} \equiv 5 \mod 397,$$

d'où :

$$5^{400} \equiv 5^{397+3} \equiv 5^{3+1} \equiv 5^4 \equiv 625 \equiv 328 \mod 397.$$

Assertion 25.3. *Les Théorèmes 25.1 de Fermat et 25.2 de Fermat-bis sont équivalents.*

Preuve. Si le premier énoncé est vrai, alors le deuxième aussi, grâce à la factorisation :

$$a^p - a = a\left(a^{p-1} - 1\right) \overset{?}{\equiv} 0 \mod p,$$

car si $a \equiv 0 \mod p$, on a clairement $a^p - a \equiv 0 \mod p$, et si $a \not\equiv 0 \mod p$, c'est le deuxième facteur $a^{p-1} - 1 \equiv 0 \mod p$ qui fait le travail.

Inversement, si le deuxième énoncé est vrai, alors le premier aussi, car avec $a \not\equiv 0 \mod p$, donc avec $1 = p \wedge a$, en partant de la factorisation :

$$\mod p \;\; 0 \equiv a^p - a \equiv \underline{a}_\circ \left(a^{p-1} - 1\right) \text{ est divisible par } p,$$

le Théorème 24.4 d'Euclide force p à devoir diviser $a^{p-1} - 1$. Autrement dit, $a^{p-1} - 1 \equiv 0 \mod p$. □

Concentrons-nous donc sur le deuxième énoncé.

Démonstration du Théorème 25.1 de Fermat. Il s'agit d'arguments dus à Leibniz et à Euler, qui reposent sur une utilisation astucieuse de la formule du binôme de Newton (club des grands).

Tout d'abord, pour $a = 0$, on a bien $0^p \equiv 0 \mod p$. En partant de 0, et en ajoutant $+1$ pas à pas pour couvrir tous les éléments de $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\} \mod p$, nous allons raisonner par récurrence en appliquant le

Lemme 25.4. *Si $p \in \mathscr{P}$ est premier, alors tout entier $a \in \mathbb{Z}$ satisfait :*

$$\big(a+1\big)^p \equiv a^p + 1 \mod p.$$

Démonstration. Développons :

$$\big(a+1\big)^p = a^p + \tbinom{p}{1} a^{p-1}\, 1^1 + \tbinom{p}{2} a^{p-2}\, 1^2 + \cdots + \tbinom{p}{p-2} a^2\, 1^{p-2} + \tbinom{p}{p-1} a^1\, 1^{p-1} + 1^p,$$

avec, pour tout $1 \leqslant k \leqslant p-1$, les coefficients binomiaux :

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!} \in \mathbb{N},$$

dont on sait qu'ils sont *entiers*. Extrayons p via $p! = p \cdot (p-1)!$:

$$\mathbb{N} \ni \frac{p\,(p-1)!}{k!\,(p-k)!} = p\, \underbrace{\frac{(p-1)!}{k!\,(p-k)!}}_{\text{doit être entier}},$$

et observons au dénominateur que :

- aucun facteur premier de $k! = 1 \cdot 2 \cdots k$ ne peut être égal à p, parce que $k \leqslant p-1$;
- aucun facteur premier de $(p-k)! = 1 \cdot 2 \cdots (p-k)$ ne peut être égal à p non plus, parce que $p - k \leqslant p - 1$, vu que $1 \leqslant k$.

Donc le p au numérateur ne peut se simplifier avec *aucun* nombre premier au dénominateur : il reste *intact*, et alors, les facteurs de $k!$ et de $(p-k)!$ ne peuvent se simplifier qu'avec $(p-1)!$. Nous avons en fait démontré le

Lemme 25.5. *Si $p \in \mathscr{P}$ est premier, alors pour tout $1 \leqslant k \leqslant p-1$:*

$$\binom{p}{k} = p\, \frac{(p-1)!}{k!\,(p-k)!} \equiv 0 \mod p.$$

En réduisant modulo p l'équation plus haut, nous obtenons bien :

$$\big(a+1\big)^p \equiv a^p + 0 + 0 + \cdots + 0 + 0 + 1^p \equiv a^p + 1 \mod p. \qquad \square$$

Par récurrence ascendante, en partant de $a = 0$, on peut appliquer ce lemme :

$$\begin{aligned} 1^p &\equiv \big(1+0\big)^p \equiv 1^p + 0^p \equiv 1 \mod p, \\ 2^p &\equiv \big(1+1\big)^p = 1^p + 1 \equiv 1 + 1 \equiv 2 \mod p, \\ 3^p &\equiv \big(2+1\big)^p = 2^p + 1 \equiv 2 + 1 \equiv 3 \mod p, \end{aligned}$$

et ainsi de suite pour obtenir $a^p \equiv a \mod p$, quel que soit l'entier $a \geqslant 0$.

Pour attraper tous les entiers $a \leqslant 0$ négatifs, on raisonne de manière similaire [20] avec :

$$\begin{aligned}\big(a-1\big)^p &= a^p + \tbinom{p}{1}\, a^{p-1}\,(-1)^1 + \cdots + \tbinom{p}{p-1}\, a^1\,(-1)^{p-1} + (-1)^p \\ &\equiv a^p + (-1)^p \mod p.\end{aligned}$$

□

26. Théorème de Wilson

En arithmétique élémentaire, le théorème de Wilson énonce qu'un entier $n \geqslant 2$ est un nombre premier *si et seulement si* la factorielle de $n-1$ est congrue à -1 modulo n. Cette caractérisation des nombres premiers est assez anecdotique et ne constitue pas un test de primalité efficace. Son principal intérêt réside dans son histoire [21], et dans la relative simplicité de son énoncé et de ses preuves.

Rappelons que la *factorielle* d'un entier $m \geqslant 1$ est :

$$m\,! \;=\; 1 \cdot 2 \cdot 3 \cdots (m-1) \cdot m.$$

Théorème 26.1. [de Wilson] *Pour tout entier $n \geqslant 2$, on a équivalence entre :*

(i) *$n = p \in \mathscr{P}$ est premier ;*

(ii) $(n-1)! \equiv -1 \mod n$.

Voici quelques exemples illustrant cet énoncé.

- Si p est égal à 2, alors $(p-1)\,!+1$ est égal à 2, un multiple de 2.
- Si p est égal à 3, alors $(p-1)\,!+1$ est égal à 3, un multiple de 3.
- Si p est égal à 4, alors $(p-1)\,!+1$ est égal à 7, qui n'est *pas* un multiple de 4.
- Si p est égal à 5, alors $(p-1)\,!+1$ est égal à 25, qui *est* un multiple de 5.
- Si p est égal à 6, alors $(p-1)\,!+1$ est égal à 121, qui n'est *pas* un multiple de 6.
- Si p est égal à 17, alors $(p-1)\,!+1$ est égal à $20\,922\,789\,888\,001$, qui *est* un multiple de 17, car :

$$17 \cdot 1\,230\,752\,346\,353 \;=\; 20\,922\,789\,888\,001.$$

Démonstration. Le cas $n = 2$, qui est premier, est clair, car $(2-1)! \equiv -1 \mod 2$. On peut donc supposer que $n \geqslant 3$.

Montrons **(i)** $\Longrightarrow$ **(ii)**. D'après le Théorème 27.5, on sait que $\mathbb{Z}/p\,\mathbb{Z}$ est un corps. Ainsi, tout élément non nul a dans l'ensemble :

$$\big(\mathbb{Z}/p\mathbb{Z}\big)^{\times} \;=\; \big\{1,\, 2,\, \ldots,\, p-2,\, p-1\big\} \mod p,$$

20. Il y a néanmoins une petite subtilité technique : il faut s'arranger à l'avance que $p \geqslant 3$ afin d'avoir $(-1)^p = -1$, donc il faut avoir traité le cas $p = 2$ à part, auparavant, ce que nous avons en fait déjà fait !

Autre moyen de raisonner : comme l'application $a \longmapsto a \mod p$ de $\mathbb{N}$ dans $\mathbb{Z}/p\mathbb{Z}$ est surjective, et comme l'équation de Fermat $a^p \equiv a \mod p$ s'exprime véritablement non pas dans $\mathbb{Z}$, mais dans $\mathbb{Z}/p\mathbb{Z}$, le fait d'avoir traité tous les $a \geqslant 0$ suffit largement.

21. Le premier texte actuellement connu qui fait référence à ce résultat est dû au mathématicien arabe Alhazen (965–1039). Ce théorème est connu à partir du XVII$^{\text{ième}}$ siècle en Europe. Leibniz (1646–1716) fait référence à ce résultat sans le démontrer. John Wilson (1741–1793) redécouvre ce qu'il croit être une conjecture, et en partage la découverte avec son professeur Edward Waring, qui publie cette conjecture en 1770.

En définitive, John Wilson est connu pour avoir énoncé (ou conjecturé) un théorème sur les nombres premiers qui porte son nom, alors qu'il ne l'a pas *du tout* démontré…

Lagrange en présente deux premières démonstrations en 1771, puis Euler une troisième en 1773. Utilisant les notations de l'arithmétique modulaire, Gauss reformule la démonstration d'Euler et donne une quatrième preuve, la plus élégante, celle que nous détaillons.

possède un inverse multiplicatif a', *qui appartient nécessairement au même ensemble*.

Or le cardinal de cet ensemble est égal à $p-1$, car tout nombre premier $p \geqslant 3$ est *impair*. Mais $1 = 1^{-1}$ est son propre inverse, et $(p-1) = (p-1)^{-1}$ aussi, car :

$$1 \cdot 1 \;=\; 1 \mod p, \qquad \text{et} \qquad (p-1)\cdot(p-1) \;=\; p^2 - 2\,p + 1 \;\equiv\; 1 \mod p.$$

Assertion 26.2. *Les éléments* 1 *et* $p-1$ *de* $\mathbb{Z}\big/p\mathbb{Z}$ *sont les seuls* x *satisfaisant :*

$$x^2 \;\equiv\; 1 \mod p.$$

Preuve. Soit un tel x. Certainement, $x \not\equiv 0 \mod p$, car $0^2 \equiv 1 \mod p$ est faux. On factorise :

$$(x-1)\,(x+1) \;\equiv\; 0 \mod p,$$

c'est-à-dire :

$$(x-1)\,\big(x-(p-1)\big) \;\equiv\; 0 \mod p.$$

Alors oui, $x = 1$ et $x = p-1$ satisfont bien cette congruence.

Mais alors, *aucun* $x = a$ parmi les éléments restants $a \in \{2, \ldots, p-2\}$ ne peut satisfaire cette congruence, car les inégalités :

$$\begin{aligned} 2 \;\leqslant\; a \;\leqslant\; p-2 \qquad &\Longrightarrow \qquad 1 \;\leqslant\; a-1 \;\leqslant\; p-3 \\ &\text{et} \qquad -(p-3) \;\leqslant\; a-(p-1) \;\leqslant\; -1, \end{aligned}$$

montrent que les deux entiers $a - 1 \;\not\equiv\; 0 \mod p$, ainsi que $a - (p-1) \;\not\equiv\; 0 \mod p$ ne peuvent *pas* être congrus à 0 modulo p.

Assertion 26.3. [Intégrité de $\mathbb{Z}\big/p\mathbb{Z}$] *Avec* $p \in \mathscr{P}$ *premier, on a toujours, pour* $a, b \in \mathbb{Z}$ *:*

$$\Big(\; a \;\not\equiv\; 0 \mod p \quad \textit{et} \quad b \;\not\equiv\; 0 \mod p \;\Big) \qquad \Longrightarrow \qquad a\,b \;\not\equiv\; 0 \mod p.$$

Preuve. Traitons plutôt l'implication contraposée, qui lui est équivalente :

$$\Big(\; a \;\equiv\; 0 \mod p \quad \text{ou} \quad b \;\equiv\; 0 \mod p \;\Big) \qquad \Longleftarrow \qquad a\,b \;\equiv\; 0 \mod p.$$

Supposons donc qu'il existe $k \in \mathbb{Z}$ tel que :

$$a\,b \;=\; k\,p,$$

de telle sorte que $a\,b$ soit divisible par p. Mais le Théorème 24.4 d'Euclide garantit alors que :

$$\big(p \,|\, a \quad \text{ou} \quad p \,|\, b\big) \qquad \text{c'est-à-dire} \qquad \big(a \;\equiv\; 0 \mod p \quad \text{ou} \quad b \;\equiv\; 0 \mod p\big).$$ □

Enfin, grâce à l'*intégrité* de $\mathbb{Z}\big/p\mathbb{Z}$, nous concluons que le produit de nos deux entiers est *aussi* non congru à zéro modulo p :

$$a^2 - 1 \;\equiv\; (a-1)\,\big(a-(p-1)\big) \;\not\equiv\; 0 \mod p.$$

En conclusion, pour tout $a \;\neq\; 1$ et $\neq\; p-1$, on a bien vérifié que $a^2 \;\not\equiv\; 1 \mod p$. En particulier, a ne peut *pas* être son propre inverse modulo p. □

Par conséquent, dans l'ensemble restant $\big\{2, \ldots, p-2\big\}$ de cardinal égal à $p-3$ *pair*, chaque élément $a \in \big\{2, \ldots, p-2\big\}$ trouve son inverse $a^{-1} \in \{2, \ldots, p-2\big\}$ *qui est différent de* a. Autrement dit, les éléments de $\big\{2, \ldots, p-2\big\}$ s'accouplent par paires annihilatrices — pour la multiplication …

Par exemple, modulo 7 et modulo 11, relions en rouge les paires d'inverses multiplicatifs :

et constatons que la combinatoire semble moins simple que pour les paires d'inverses additifs, qui exhibaient une symétrie très agréable dans la Section **10**. Dans ces deux exemples, les produits complets :

$$\begin{aligned} 2\cdot 3\cdot 4\cdot 5 &\equiv 2\cdot 3\cdot 2^{-1}\cdot 3^{-1} \\ &\equiv 1 \mod 7, \\ 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9 &\equiv 2\cdot 3\cdot 3^{-1}\cdot 5\cdot 2^{-1}\cdot 7\cdot 7^{-1}\cdot 5^{-1} \\ &\equiv 1 \mod 11, \end{aligned}$$

sont congrus à 1, c'est-à-dire généralement :

$$2\cdot 3\cdots(p-3)\cdot(p-2) \equiv 1 \mod p.$$

Enfin, on atteint la propriété **(ii)** :

$$\begin{aligned} (p-1)! &= 1\cdot\big[2\cdot 3\cdots(p-3)\cdot(p-2)\big]\cdot(p-1) \\ &\equiv 1\cdot\big[1\big]\cdot(p-1) \mod p \\ &\equiv p-1 \mod p \\ &\equiv -1 \mod p. \end{aligned}$$

Ensuite, montrons la réciproque **(ii)** $\Longrightarrow$ **(i)**. Par contraposition, cela revient à montrer :

$$\text{non } \textbf{(i)} \quad\Longrightarrow\quad \text{non } \textbf{(ii)}.$$

Supposons donc non **(i)**. Soit donc un entier $n \geqslant 4$ *non premier*, c'est-à-dire décomposé comme produit $n = d\,m$, avec $1 < d < n$ et $1 < m < n$. Clairement [22], l'écriture :

$$(n-1) = 1\cdot 2\cdots d\cdots(n-1),$$

fait voir que $(n-1)!$ est congru à 0 modulo d, donc *pas* congru à -1 :

$$(n-1)! \not\equiv -1 \mod d.$$

Enfin, grâce à la contraposée de la Proposition 33.2, qui a été énoncée comme le Corollaire 33.3, nous attteignons aussitôt non **(ii)** :

$$(n-1)! \not\equiv -1 \mod \underbrace{d m}_{=n}. \qquad \square$$

27. Intégrité et non-intégrité de $\mathbb{Z}/n\mathbb{Z}$

Dans $\mathbb{Z}/4\mathbb{Z} = \big\{0,1,2,3\big\} \mod 4$, les éléments inversibles sont :

$$\begin{aligned} 1 \text{ d'inverse } 1, &\quad \text{car } 1\cdot 1 \equiv 1 \mod 4, \\ 3 \text{ d'inverse } 3, &\quad \text{car } 3\cdot 3 \equiv 1 \mod 4, \end{aligned}$$

tandis que 2 n'a *pas* d'inverse, puisque modulo 4 :

$$0\cdot 2 \equiv 0, \qquad 1\cdot 2 \equiv 2, \qquad 2\cdot 2 \equiv 0, \qquad 3\cdot 2 \equiv 2.$$

Dans $\mathbb{Z}/8\mathbb{Z} = \big\{0,1,2,3,4,5,6,7\big\} \mod 8$, les éléments inversibles sont :

22. L'écriture symétrique $(n-1)! = 1\cdot 2\cdots m\cdots(n-1)$, qui montre que $(n-1)!$ est aussi divisible par m, n'est pas utilisée dans l'argumentation.

$$1 \text{ d'inverse } 1, \quad \text{car} \quad 1 \cdot 1 \equiv 1 \mod 8,$$
$$3 \text{ d'inverse } 3, \quad \text{car} \quad 3 \cdot 3 \equiv 1 \mod 8,$$
$$5 \text{ d'inverse } 5, \quad \text{car} \quad 5 \cdot 5 \equiv 1 \mod 8,$$
$$7 \text{ d'inverse } 7, \quad \text{car} \quad 7 \cdot 7 \equiv 1 \mod 8,$$

tandis que 2, 4, 6 n'ont *pas* d'inverse modulo 8, comme le montre la table de multiplication complète.

*	**[0]**	**[1]**	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**	**[7]**
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[0]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Dans $\mathbb{Z}/11\mathbb{Z}$, *tous* les éléments non nuls 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 sont inversibles, comme on peut le voir en constatant dans la table de multiplication que chaque ligne (ou chaque colonne) concernée contient le nombre 1.

*	**[0]**	**[1]**	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**	**[7]**	**[8]**	**[9]**	**[10]**
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[1]	[3]	[5]	[7]	[9]
[3]	[0]	[3]	[6]	[9]	[1]	[4]	[7]	[10]	[2]	[5]	[8]
[4]	[0]	[4]	[8]	[1]	[5]	[9]	[2]	[6]	[10]	[3]	[7]
[5]	[0]	[5]	[10]	[4]	[9]	[3]	[8]	[2]	[7]	[1]	[6]
[6]	[0]	[6]	[1]	[7]	[2]	[8]	[3]	[9]	[4]	[10]	[5]
[7]	[0]	[7]	[3]	[10]	[6]	[2]	[9]	[5]	[1]	[8]	[4]
[8]	[0]	[8]	[5]	[2]	[10]	[7]	[4]	[1]	[9]	[6]	[3]
[9]	[0]	[9]	[7]	[5]	[3]	[1]	[10]	[8]	[6]	[4]	[2]
[10]	[0]	[10]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Il y a quelques secondes, nous avons « laissé passer[23] » le fait — absolument non-anodin ! — que dans $\mathbb{Z}/4\mathbb{Z}$:

$$2 \cdot 2 \equiv 0 \mod 4.$$

Autrement dit, dans un anneau commutatif $\big(\mathbb{A}, +, \times\big)$ au sens de la Définition 5.9, il peut exister des $a \neq 0$ et des $b \neq 0$ dont le *produit* $a \times b = 0_A$ est *nul ! Aïe !*

Définition 27.1. Un anneau commutatif $\big(\mathbb{A}, +, \times\big)$ est dit *intègre* si, pour tous a et b dans $\mathbb{A}$:

$$a\,b = 0 \qquad \Longrightarrow \qquad \Big(a = 0 \quad \text{ou} \quad b = 0 \Big).$$

De manière équivalente :

$$\Big(a\,b = 0 \quad \text{avec} \quad a \neq 0 \Big) \qquad \Longrightarrow \qquad b = 0.$$

Certainement, les anneaux $\mathbb{A} = \mathbb{Z}/n\mathbb{Z}$ sont commutatifs, *mais pas forcément intègres*.

Proposition 27.2. [Règle de simplification] *Si $a \neq 0$, alors $a\,b = a\,c$ implique $b = c$.*

23. Attention ! À l'aéorort de Sidney en Australie,

Démonstration. Ceci équivaut à $a\big(b-c\big) = 0$, et par intégrité, comme $a \neq 0$, il vient $b-c=0$, c'est-à-dire $b=c$. □

Pire ! Dans $\mathbb{Z}/4\mathbb{Z}$, on a même un élément a, le nombre 2, qui satisfait $a^2 \equiv 0 \bmod 4$.

En tout cas, l'anneau classique $\big(\mathbb{Z},+,\times\big)$ est intègre (et honnête !), c'est bien connu, tandis que l'anneau $\mathscr{M}_{2\times 2}(\mathbb{R})$, tout comme $\mathbb{Z}/4\mathbb{Z}$, n'est *pas* intègre, ce que montre la matrice :

$$M := \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right),$$

qui satisfait :

$$M^2 = M \cdot M = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right).$$

Maintenant, souvenons-nous de la Définition 5.10 de *corps commutatif* $\mathbb{K}$, qui demandait que tout élément non nul $x \in \mathbb{K}\backslash\{0\}$ ait un inverse x' pour la multiplication, c'est-à-dire satisfaisant $x'x=1$. Nous avions dit que $\mathbb{Z}$ n'est *pas* un corps, car aucun élément $a \in \mathbb{Z}$, excepté $a = \pm 1$, n'a d'inverse pour la multiplication, *e.g.* $\frac{1}{137} \notin \mathbb{Z}$.

Question 27.3. *Un anneau $\mathbb{Z}/n\mathbb{Z}$ d'entiers modulo n peut-il être un corps ?*

Avec tous ces $\mathbb{Z}/4\mathbb{Z}$ et autres $\mathbb{Z}/8\mathbb{Z}$ trublionnaires, il semblerait que non. En tout cas, rappelons-nous qu'un corps est toujours un anneau commutatif, et qu'il a de meilleures propriétés. Par exemple, $\mathbb{Q} = \big\{\frac{p}{q} :\ p \in \mathbb{Z},\ q \in \mathbb{N}^*\big\}$, qui est un corps, est aussi un anneau, comme $\mathbb{Z}$, mais il est « mieux » que $\mathbb{Z}$, car l'inverse de $\frac{p}{q}$ est $\frac{q}{p}$, lorsque $p \neq 0$. Or, tous les corps sont intègres !

Proposition 27.4. *Tout corps commutatif $\big(\mathbb{K},+,\times\big)$ est un anneau* intègre.

Démonstration. Étant donné $a, b \in \mathbb{K}$ quelconques avec $a \neq 0$, satisfaisant $a\,b = 0$, il s'agit de montrer que $b=0$.

Comme $\mathbb{K}$ est un corps, un inverse multiplicatif (unique) a^{-1} de a existe, avec $a^{-1}\,a = 1$, et donc, il suffit de l'utiliser :

$$a^{-1}\,\big(\ a\,b \ = \ 0\ \big) \qquad \text{donne} \qquad a^{-1}\,a\,b \ = \ 1\cdot b \ = \ b \ = \ 0. \qquad \square$$

Théorème 27.5. *Pour $n \geqslant 2$ entier, les assertions suivantes sont équivalentes.*

(i) *$n = p \in \mathscr{P}$ est un nombre premier.*

(ii) *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre.*

(iii) *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.*

Observons que $\mathbb{Z}/n\mathbb{Z} = \big\{0,1,\ldots,n-1\big\} \bmod n$ possède au moins les deux éléments $0 \neq 1$, puisque $n \geqslant 2$.

Démonstration. Nous allons démontrer ces équivalences « en yo-yo » :

$$\begin{array}{cc} \textbf{(i)} & \textbf{(i)} \\ \Downarrow & \Uparrow \\ \textbf{(ii)} & \textbf{(ii)} \\ \Downarrow & \Uparrow \\ \textbf{(iii)} & \textbf{(iii)} \end{array}$$

Montrons **(i)** $\Longrightarrow$ **(ii)**. Supposons donc que $n = p$ est premier. Soient deux éléments $x, y \in \mathbb{Z}/p\mathbb{Z}$ satisfaisant $x \cdot y = 0$ dans $\mathbb{Z}/p\mathbb{Z}$. Pour avoir l'*intégrité* de $\mathbb{Z}/p\mathbb{Z}$, il s'agit de faire voir que $x=0$ ou $y=0$, dans $\mathbb{Z}/p\mathbb{Z}$.

Autrement dit, x et y appartiennent à $\{0,1,2,\dots,p-1\}$ $\mathsf{mod}\, p$ et satisfont :

$$x\cdot y \equiv 0 \ \mathsf{mod}\, p \qquad \Longleftrightarrow \qquad x\,y = k\,p \qquad (k\in\mathbb{Z}).$$

Mais alors, ceci montre que p *divise* le produit $x\,y$, et par conséquent, le Théorème 24.4 d'Euclide force p à diviser x ou à diviser y.

Enfin, comme p ne peut aucunement diviser les nombres $1,2,\dots,p-1$ qui lui sont inférieurs [24], et qu'il ne peut donc diviser que 0, on conclut bien que $x=0$ ou $y=0$.

Montrons **(ii)** $\Longrightarrow$ **(iii)**. Supposons donc $\mathbb{Z}/n\mathbb{Z}$ intègre. Prenons $x\in\{1,2,\dots,n-1\}$ quelconque, différent de 0. Pour avoir que $\mathbb{Z}/n\mathbb{Z}$ est un corps, il s'agit de trouver un *inverse multiplicatif* $x'\in\mathbb{Z}/n\mathbb{Z}$ satisfaisant :

$$x\,x' \equiv 1 \ \mathsf{mod}\, n.$$

Certainement, x' doit se trouver parmi $\{1,2,\dots,n-1\}$, car $x'=0$ est exclu. Regardons alors *tous* les produits $x\,k$ modulo n, pour $k=0,1,2,\dots,n-1$, en espérant y trouver x', y compris pour $k=0$.

Assertion 27.6. *Modulo n, les n produits $x\,0$, $x\,1$, $x\,2$, …, $x\,(n-1)$ prennent des valeurs deux à deux distinctes :*

$$x\,k_1 \not\equiv x\,k_2 \qquad (\forall\, 0\leqslant k_1\neq k_2\leqslant n-1).$$

Preuve. Supposons qu'il existe k_1 et k_2 avec $x\,k_1\equiv x\,k_2$ $\mathsf{mod}\, n$, c'est-à-dire :

$$x\,(k_1-k_2) \equiv 0 \ \mathsf{mod}\, n. \tag{27.7}$$

On peut supposer $k_2\leqslant k_1$. Puisqu'on a déjà vu que :

$$0\leqslant k_2\leqslant k_1\leqslant n-1 \qquad \Longrightarrow \qquad 0\leqslant k_1-k_2\leqslant n-1,$$

il est clair que k_1-k_2 est un élément de $\{0,1,\dots,n-1\}$. Mais comme $\mathbb{Z}/n\mathbb{Z}$ est supposé *intègre*, et comme on a pris $x\not\equiv 0$, l'équation (27.7) force $k_1-k_2=0$, c'est-à-dire $k_1=k_2$.

Ainsi, $x\,k_1\equiv x\,k_2$ $\mathsf{mod}\, n$ implique $k_1=k_2$. Par contraposition [25], $k_1\neq k_2$ implique $x\,k_1\not\equiv x\,k_2$ $\mathsf{mod}\, n$. □

Comme les n éléments $x\,0$, $x\,1$, $x\,2$, …, $x\,(n-1)$ sont donc deux à deux distincts, on a égalité entre les deux ensembles :

$$\{x\,0,\ x\,1,\ x\,2,\ \dots,\ x\,(n-1)\} \ \mathsf{mod}\, n \ = \ \{0,\ 1,\ 2,\ \dots,\ n-1\} \ \mathsf{mod}\, n,$$

et par conséquent, parmi tous ces $x\,k$ à gauche, il doit forcément y en avoir un qui est égal au 1 à droite modulo n, et ce k-là, c'est l'inverse x' de x que nous recherchions — nous l'avons trouvé !

La première implication **(iii)** $\Longrightarrow$ **(ii)** du yo-yo qui remonte est évidente, car tout corps est un anneau intègre, comme nous la Proposition 27.4 nous l'a déjà fait voir.

Terminons en établissant **(ii)** $\Longrightarrow$ **(i)**. Par contraposition (notion qui vient d'être rappelée en note de bas de page), cela revient à établir non **(ii)** $\Longleftarrow$ non **(i)**.

24. Rappelons en effet qu'avec deux entiers $a\geqslant 1$ et $b\geqslant 1$, la définition de $a\,|\,b$ s'exprime par $a\,u=b$ avec $u\geqslant 1$ entier, ce qui implique aussitôt $a\leqslant b$.

25. Rappelons l'équivalence logique générale valable pour deux propositions P et Q, appelée *contraposition :*

$$\big(\ \mathsf{P}\ \Longrightarrow\ \mathsf{Q}\ \big) \qquad \Longleftrightarrow \qquad \big(\ \mathsf{non\ P}\ \Longleftarrow\ \mathsf{non\ Q}\ \big)$$

Autrement dit, en partant d'un entier n non premier, c'est-à-dire décomposable en produit $n = d\,m$ avec $1 < d < n$ et $1 < m < n$, il s'agit d'établir que $\mathbb{Z}/n\mathbb{Z}$ n'est *pas* intègre. Et comme nous l'avons déjà vu, cela est clair !

En effet, $d \bmod n$ et $m \bmod n$ sont alors tous deux différents de 0 dans $\mathbb{Z}/n\mathbb{Z}$, puisqu'ils appartiennent d'emblée à l'ensemble $\{2, \ldots, n-1\}$, tandis que leur produit $d\,m = n \equiv 0 \bmod n$ est stupidement nul dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi, d et m détruisent l'intégrité éventuelle de $\mathbb{Z}/n\mathbb{Z}$.

Cela achève complètement la démonstration du Théorème 27.5. □

Quand le module n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ n'est donc *pas* un corps. Toutefois, certains éléments spéciaux peuvent quand même avoir un inverse multiplicatif. Voici une caractérisation générale très claire de ces éléments sympathiques.

Théorème 27.8. *Soit $n \geqslant 2$. Pour tout $a \in \mathbb{Z}$, on a équivalence entre :*

(i) *$a \wedge n$ est premier avec n ;*

(ii) *$a \bmod n$ possède un inverse $a' \bmod n$, avec $a\,a' \equiv 1 \bmod n$.*

Ce théorème est en fait essentiellement équivalent au Grand Théorème 20.2 de Bézout.

Démonstration. En effet :

$$\begin{aligned} a \wedge n = 1 \quad &\overset{\text{Bézout}}{\Longleftrightarrow} \quad u\,a + v\,n = 1 \qquad (\exists\, u \in \mathbb{Z},\ \exists\, v \in \mathbb{Z}) \\ &\Longleftrightarrow \quad u\,a \equiv 1 \bmod n, \end{aligned}$$

ce qui montre que le « u » de Bézout n'est autre que l'inverse a^{-1} de a. □

En principe, donc, c'est l'algorithme d'Euclide [26] qui permet de trouver l'inverse d'un élément a de $\mathbb{Z}/n\mathbb{Z}$, lorsqu'il existe.

Définition 27.9. Pour un entier $n \geqslant 2$, on appelle *groupe multiplicatif* de $\mathbb{Z}/n\mathbb{Z}$ l'ensemble noté :

$$\big(\mathbb{Z}/n\mathbb{Z}\big)^{\times} := \Big\{ a \in \mathbb{Z}/n\mathbb{Z} \colon \text{ il existe } a' \in \mathbb{Z}/n\mathbb{Z} \text{ satisfaisant } a\,a' \equiv 1 \bmod n \Big\}.$$

Autrement dit :

$$\big(\mathbb{Z}/n\mathbb{Z}\big)^{\times} = \big\{ a \in \{0, 1, \ldots, n-1\} \colon\ a \wedge n = 1 \big\}.$$

Définition 27.10. On appelle *fonction indicatrice d'Euler* la fonction notée :

$$\varphi \colon \quad \mathbb{N}^* \longrightarrow \mathbb{N}^*,$$

qui est définie pour tout entier $n \geqslant 2$ par :

$$\begin{aligned} \varphi(n) &:= \mathsf{Card}\,\big\{ 1 \leqslant a \leqslant n \colon\ a \wedge n = 1 \big\} \\ &= \mathsf{Card}\,\big(\mathbb{Z}/n\mathbb{Z}\big)^{\times}, \end{aligned}$$

en posant $\varphi(1) := 1$ par convention.

26. — débouchant sur une relation de Bézout $u\,a + v\,b = \mathsf{pgcd}\,(a, b)$, d'après le Théorème 19.7 —

On voit que $\varphi(2) = 1$. Lorsque $n = p \in \mathscr{P}$ est premier, *tous* les entiers $1 \leqslant a \leqslant p-1$ sont premiers avec p, et donc :

$$\varphi(p) \,=\, p-1 \qquad (p \text{ premier}).$$

Ensuite, voici les valeurs de $\varphi(n)$ pour n *non* premier jusqu'à 10 (doigts ?) :

$$\begin{aligned}
\varphi(4) \,&=\, 2, && \text{car } 1,\, 3 \text{ premiers avec } 4,\\
\varphi(6) \,&=\, 2, && \text{car } 1,\, 5 \text{ premiers avec } 6,\\
\varphi(8) \,&=\, 4, && \text{car } 1,\, 3,\, 5,\, 7 \text{ premiers avec } 8,\\
\varphi(9) \,&=\, 6, && \text{car } 1,\, 2,\, 4,\, 5,\, 7,\, 8 \text{ premiers avec } 9,\\
\varphi(10) \,&=\, 4, && \text{car } 1,\, 3,\, 7,\, 9 \text{ premiers avec } 10.
\end{aligned}$$

Plus tard, dans la Section **33**, nous établirons une propriété fondamentale de *multiplicativité* de cette indicatrice pour des entiers premiers entre eux :

$$\varphi\big(m\,n\big) \,=\, \varphi(m)\,\varphi(n) \qquad (\forall\ m \wedge n = 1).$$

28. Théorème des restes chinois

Sur un exemple très simple, commençons par rappeler l'intérêt du *calcul modulaire*, *i.e.* du calcul modulo un entier $n \geqslant 2$. Imaginons-nous que nous sommes un jeudi, jour du cours en amphithéâtre. *Quel jour serons-nous dans 2 583 jours ?*

Un moyen de répondre joliment à cette question est de numéroter les jours : jeudi $= 1$; vendredi $= 2$, et ainsi de suite. Maintenant, on additionne 2583 jours à 1, puisque jeudi $= 1$, ce qui donne $2\,584$ jours. Comme il n'y a que 7 jours dans la semaine, on peut retrancher autant de fois des multiples de 7 que l'on veut ; autrement dit, on peut retrancher autant de semaines que l'on veut. Par une division, on a donc que $2\,584 = 369 \times 7 + 1$, d'où nous concluons que dans $2\,584$ jours, nous serons encore un jeudi !

Comme le calcul modulo 7 nous semble dorénavant réservé aux « bébés » du Lycée qui n'ont pas encore commencé à apprendre les vraies mathématiques universitaires, voici un autre problème, plus complexe, d'origine chinoise et datant de l'Antiquité.

Problème 28.1. *Mon panier peut contenir au plus cent œufs.*

- *Si je le vide par trois œufs à la fois, il en reste un.*
- *Si je le vide par huit œufs à la fois, il en reste deux.*
- *Si je le vide par sept œufs à la fois, il en reste cinq.*

Combien ai-je d'œufs ?

Grâce aux entiers modulaires, et aux théorèmes arithmétiques que nous avons démontrés, nous pouvons résoudre ce problème. En effet, les informations se traduisent en 3 équations modulaires, avec 3 modules distincts (et premiers entre eux), d'inconnue le nombre x d'œufs :

$$x \,\leqslant\, 100 \qquad \text{et} \qquad x \,\equiv\, \begin{cases} 1 \mod 3,\\ 2 \mod 8,\\ 5 \mod 7. \end{cases}$$

Par la première congruence, on a $x = 1 + 3\,k$, avec $k \in \mathbb{N}$. Pour tenir compte de la deuxième contrainte, $x = 2 + 8\,k'$ avec $k' \in \mathbb{N}$, partons de $x = 1 + 3\,k$ avec l'astuce de

multiplier cette équation par 3, car $3 \cdot 3 = 9 \equiv 1 \mod 8$:

$$\begin{aligned} \big(\, 1+3k \;=\; 2+8k' \,\big) \cdot 3 \mod 8 \quad \text{donne} \quad 3+9k &\equiv 6 \mod 8 \\ k &\equiv 3 \mod 8 \\ k &\equiv 3+8\ell \quad (\text{avec } \ell \in \mathbb{N}), \end{aligned}$$

valeur de k que nous pouvons remplacer dans :

$$\begin{aligned} x &= 1+3\big(3+8\ell\big) \\ &= 10+24\ell. \end{aligned}$$

Ensuite, pour tenir compte de la troisième contrainte $x \equiv 5 \mod 7$:

$$10+24\ell \;=\; 5+7k'' \qquad (\text{avec } k'' \in \mathbb{N}),$$

si on veut raisonner de manière analogue, on doit raisonner modulo 7. Comme $24 \equiv 3 \mod 7$, et comme 5 est l'inverse de 3 dans $\mathbb{Z}/7\mathbb{Z}$, car $5 \cdot 3 = 15 \equiv 1 \mod 7$, on doit multiplier cette équation par 5, puis réduire modulo 7, en utilisant $7 \cdot 19 = 119$:

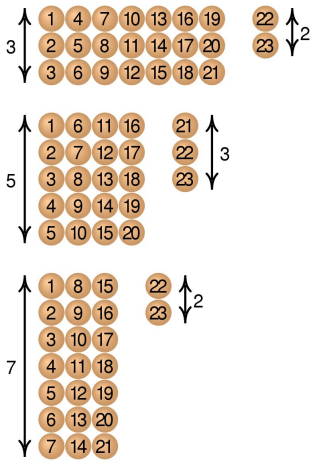
$$\begin{aligned} \big(\, 10+24\ell \;=\; 5+7k'' \,\big) \cdot 5 \mod 7 \quad \text{donne} \quad 50+120\ell &\equiv 25 \mod 7 \\ 1+\ell &\equiv 4 \mod 7 \\ \ell &\equiv 3 \mod 7 \\ \ell &= 3+7m \quad (\text{avec } m \in \mathbb{N}). \end{aligned}$$

Enfin, on remplace cette valeur de ℓ dans :

$$\begin{aligned} x &= 10+24\big(3+7m\big) \qquad 28.2 \\ &= 82+168m \qquad (m \in \mathbb{Z} \text{ quelconque.}) \end{aligned}$$

En conclusion, puisque l'on cherche $x \leqslant 100$, il faut choisir $m = 0$, et il y avait exactement 82 œufs dans le panier de la belle maraîchère.

Voici un autre exemple, dû à Sun Zi. La forme originale du théorème des restes chinois apparaît sous forme de problème dans le livre de Sun Zi, le Sunzi suanjing, datant du III$^{\text{ième}}$ siècle après Jésus-Chirst. Il est repris par le mathématicien chinois Qin Jiushao dans son ouvrage le Shushu Jiuzhang, *Traité mathématique en neuf chapitres*, publié en 1247. Le résultat concerne les systèmes de congruences.



Problème 28.3. *Soient des chevaux ailés en nombre inconnu.*

- *Si on les aligne par* 3 *au-dessus des nuages, il en reste* 2.
- *Si on les aligne par* 5*, il en reste* 3.
- *Si on les range par* 7*, il en reste 2.*

Combien y a-t-il de chevaux dans cet attelage céleste ?.

Cette énigme est parfois associée au général Han Xin comptant son armée (moins poétique). La résolution proposée par Sun Zi est la suivante.

> Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute-lui le produit du reste de la division par 5, c'est-à-dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105.

Cette solution, difficile à comprendre, n'explique qu'imparfaitement la méthode utilisée. Après un moment de concentration, on constate bien que le nombre indiqué par Sun Zi :

$$2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15$$

a effectivement pour restes respectifs 2, 3, 2, dans les divisions par 3, 5, 7. Et comme 105 a pour reste 0 dans les trois types de division, on peut l'ôter ou l'ajouter autant de fois que l'on veut sans changer les valeurs des restes. La plus petite valeur pour le nombre d'objets est alors 23.

Question 28.4. *Mais pourquoi ces trois nombres* 70, 21, 15 *?*

On peut observer, et nous y reviendrons, que :

$$\begin{array}{lll} 70 \equiv 1 \mod 3, & 70 \equiv 0 \mod 5, & 70 \equiv 0 \mod 7, \\ 21 \equiv 0 \mod 3, & 21 \equiv 1 \mod 5, & 21 \equiv 0 \mod 7, \\ 15 \equiv 0 \mod 3, & 15 \equiv 0 \mod 5, & 15 \equiv 1 \mod 7. \end{array}$$

On retrouve ce problème presque à l'identique en 1202 dans le Liber Abbaci de Fibonacci, au sein du chapitre XII qui concerne les problèmes et énigmes où l'on trouve également le problème des lapins de la suite de Fibonacci. Le problème avait aussi été étudié par Ibn al-Haytham (Alhazen), dont Fibonacci a pu lire les œuvres. Euler s'est également intéressé à cette question, ainsi que Gauss.

Enfin, nous ne pouvons pas résister au fait de présenter un problème attrayant concernant des pirates et un trésor.

> Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

La réponse est 785. Les nombres 17, 11 et 6 étant premiers entre eux deux à deux, les solutions sont distantes d'un multiple de $1\,122 = 17 \cdot 11 \cdot 6$; par ailleurs, 785 vérifie bien l'énoncé : $785 = 17 \cdot 46 + 3 = 11 \cdot 71 + 4 = 6 \cdot 130 + 5$. Il s'ensuit que 785 est bien le plus petit des nombres possibles.

Avec son formalisme efficace, l'arithmétique modulaire a rendu ce type de problème plus facile à résoudre.

Théorème 28.5. [des restes chinois] *Soient $n_1, \ldots, n_r$ des entiers premier entre eux deux à deux, c'est-à-dire tels que :*

$$1 \;=\; n_i \wedge n_j \qquad (\forall\, 1 \leqslant i \neq j \leqslant r).$$

Alors pour tous entiers $a_1, \ldots, a_r$ quelconques, il existe un entier x satisfaisant les r équations de congruence :

$$\begin{aligned} x \;&\equiv\; a_1 \mod n_1, \\ &\cdots\cdots\cdots\cdots \\ x \;&\equiv\; a_r \mod n_r. \end{aligned}$$

De plus, toute autre solution x' est congrue $x' \equiv x \mod n_1 \ldots n_r$ à x modulo le produit *des n_i.*

Démonstration. Une solution x, au moins, peut être trouvée comme suit. En notant n le produit complet de tous les n_i :

$$n \;:=\; n_1 \cdots n_{i-1}\, n_i\, n_{i+1} \cdots n_r,$$

pour chaque entier fixé i compris entre 1 et r, les deux entiers :

$$n_i \qquad \text{et} \qquad \widehat{n}_i \;:=\; \frac{n}{n_i} \;=\; n_1 \cdots n_{i-1}\, n_{i+1} \cdots n_r,$$

sont clairement premiers entre eux. Rappelons alors comment, grâce au Théorème 20.2 de Bézout, on peut déterminer l'inverse v_i de $\widehat{n}_i$ modulo n_i.

Pour cela, on applique l'algorithme d'Euclide, jusqu'à obtenir deux entiers u_i et v_i satisfaisant :

$$u_i\, n_i + v_i\, \widehat{n}_i \;=\; 1.$$

Si on pose alors :

$$e_i \;:=\; v_i\, \widehat{n}_i \;=\; v_i\, n_1 \cdots n_{i-1} n_{i+1} \cdots n_r,$$

il vient :

$$e_i \;\equiv\; 1 \mod n_i \qquad \text{ainsi que} \qquad e_i \;\equiv\; 0 \mod n_j \text{ pour tout } j \neq i.$$

Une solution particulière de tout ce système de r équations de congruence s'offre alors tendrement à nous :

$$x \;:=\; a_1\, e_1 + \cdots + a_r\, e_r.$$

Assertion 28.6. *Toute autre solution $x' \equiv a_i \mod n_i$ pour $i = 1, \ldots, r$ satisfait nécessairement :*

$$x' - x \;\equiv\; 0 \mod n_1 \cdots n_r.$$

Preuve. Pour $i = 1, \ldots, r$, soustrayons :

$$x' \;\equiv\; a_i \mod n_i \qquad \text{terme à terme avec} \qquad x \;\equiv\; a_i \mod n_i,$$

pour obtenir :

$$x' - x \;\equiv\; 0 \mod n_i \qquad (i = 1, \ldots, r).$$

Ainsi, $x' - x$ est divisible séparément par les r entiers $n_1, \ldots, n_r$, qui sont premiers entre eux, et donc par conséquent, grâce aux théorèmes que nous avons démontrés [27], $x' - x$ est divisible par leur *produit* $n_1 \cdots n_r$. □

Une fois que notre douce solution particulière $x = a_1\, e_1 + \cdots + a_r\, e_r$ a été trouvée, cette assertion conclut la démonstration d'*unicité*, modulo $n = n_1 \cdots n_r$, des solutions. □

27. Euclide, Gauss, Obélix, et Compagnie …

Devinette – Solution

Problème
Trouver le nombre qui:
- **divisé par 11 a un reste 4,**
- **divisé par 15 a un reste 10, et**
- **divisé par 19 a un reste 16.**

Solution
Avec un tableur, la solution est simple !
- **Colonne 1, les nombres k successifs**
- **Colonne 2, les nombre n = 11k + 4**
- **Colonne 3, valeurs de (n – 10) mod 15**
- **Colonne 4, valeurs de (n – 16) mod 19**
- **Colonne 5, test si mod = 0 en colonne 3 et 4. Si oui, c'est la bonne réponse.**

Le nombre n = 1 555 est la solution.

Extrait tableur

=SI(ET(F142=0;G142=0);"Bingo";"n")

	D	E	F	G	H
		11	15	19	Test
1		15	5	18	n
2		26	1	10	n
3		37	12	2	n
140		1544	4	8	n
141		1555	0	0	Bingo
142		1566	11	11	n

Vérification
11 x 141 + 4 = 1 555
1 555 – 10 est divisible par 15 (= 103)
1 555 – 16 est divisible par 19 (= 81)

29. Anneaux commutatifs

À partir de maintenant, nous allons vouloir présenter et développer des aspects plus abstraits et plus généraux de la théorie mathématique des *structures algébriques*. Souvenons-nous que dans la Section **5**, lorsque nous avons construit $\mathbb{Z}$, nous avons déjà introduit le concept d'*anneau commutatif*, à travers la Définition 5.9, que nous reformulons ici de manière plus concise comme suit [28].

Définition 29.1. Soit $\mathbb{A}$ un ensemble muni de deux *lois de composition internes* $+$ et $\times$, c'est-à-dire $a+b \in \mathbb{A}$ et $a \times b \in \mathbb{A}$ pour tous $a, b \in \mathbb{A}$. On dit que $\mathbb{A}$ est un *anneau commutatif* s'il vérifie les propriétés suivantes.

(1) Le couple $(\mathbb{A}, +)$ est un *groupe commutatif*, au sens de la Définition 5.1 vue au chapitre précédent [29], d'élément neutre $0_{\mathbb{A}}$.

(2) La loi de multiplication $\times$ est associative et commutative d'élément neutre $1_{\mathbb{A}}$.

(3) La loi $\times$ est distributive par rapport à $+$:

$$a \times (b+c) \;=\; a \times b + a \times c \qquad (\forall\, a, b, c \in \mathbb{A}).$$

Le cas d'un anneau dans lequel $0_{\mathbb{A}} = 1_{\mathbb{A}}$ est très dégénéré : l'Exercice 2 propose de vérifier qu'alors tous les éléments $a \in \mathbb{A}$ sont égaux à $0_{\mathbb{A}}$, de telle sorte que $\mathbb{A} = \{0_{\mathbb{A}}\}$. On dit alors que $\mathbb{A}$ est l'*anneau nul*. Mais comme tout ce qui est nul est « *nul* », on supposera toujours à partir de maintenant que $0_{\mathbb{A}} \neq 1_{\mathbb{A}}$.

Clairement :

$$\big(\mathbb{Z}, +, \times\big), \qquad \big(\mathbb{Z}/n\mathbb{Z}, +, \times\big), \qquad \big(\mathbb{Q}, +, \times\big), \qquad \big(\mathbb{R}, +, \times\big), \qquad \big(\mathbb{C}, +, \times\big),$$

sont des anneaux commutatifs. Qui plus est, il y a des inclusions qui respectent les structures respectives.

Définition 29.2. Soit $\big(\mathbb{A}, +_{\mathbb{A}}, \times_{\mathbb{A}}\big)$ un anneau commutatif. On dit qu'un sous-ensemble $\mathbb{B} \subset \mathbb{A}$ est un *sous-anneau* de $\mathbb{A}$ lorsque :

(1) $(\mathbb{B}, +)$ est un *sous-groupe commutatif* de $(\mathbb{A}, +_{\mathbb{A}})$, c'est-à-dire que :

$$b,\, b' \in \mathbb{B} \qquad \Longrightarrow \qquad b +_{\mathbb{A}} b' \in \mathbb{B},$$

28. Plus tard, nous formulerons une définition dans laquelle nous ne demanderons pas forcément que la multiplication $\times$ soit commutative.

29. Rappelons en effet que dans groupe commutatif G, on a $x * (y * z) = (x * y) * z$, puis $x * y = y * x$, et enfin surtout $x * x^{-1} = e = x^{-1} * x$ pour tout $x \neq 0$, où $e \in G$ est l'élément neutre. Ici dans un anneau commutatif, la loi $* := +$ dispose bien de toutes ces bonnes propriétés, mais pas la loi $\times$.

où l'addition est prise dans $\mathbb{A}$, de telle sorte que $(\mathbb{B}, +_{\mathbb{A}})$ est un groupe commutatif en lui-même.

(2) pour tous $b, b' \in \mathbb{B}$, on a $b \times_{\mathbb{A}} b' \in \mathbb{B}$ aussi ;

(3) $1_{\mathbb{A}} \in \mathbb{B}$.

En jouant avec la logique (trop) pure (et peu intéressante), on vérifie que $\big(\mathbb{B}, +, \times_{\mathbb{A}}\big)$ est alors un anneau en lui-même.

Par exemple, les inclusions suivantes sont des inclusions de sous-anneaux :

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

pour l'addition $+$ et la multiplication $\times$ classiques. Enfin, rappelons la Définition 5.10 a déjà introduit le concept de corps commutatif, que nous pouvons reformuler comme suit.

Définition 29.3. [Corps] Un *corps commutatif* $\mathbb{K}$ est un anneau commutatif pour lequel $(\mathbb{K}, \times)$ est un groupe commutatif.

Autrement dit, tout élément non nul $x \in \mathbb{K}\backslash\{0_{\mathbb{K}}\}$ admet un élément inverse $x' \in \mathbb{K}$ satisfaisant $x'x = 1_{\mathbb{K}}$, ce qui garantit que la loi $* := \times$ est une loi de groupe, tout aussi bien que la loi $+$ de l'anneau sous-jacent.

30. Groupe des inversibles d'un anneau commutatif

Soit un anneau commutatif quelconque $\big(\mathbb{A}, +, \times\big)$, par exemple n'importe quel $\mathbb{Z}/n\mathbb{Z}$, ou $\mathbb{Z}$ lui-même. En général, $\mathbb{A}$ n'est *pas* un corps, et on sait d'ailleurs déjà, grâce au Théorème 27.5, que $\mathbb{Z}/n\mathbb{Z}$ n'est *jamais* un corps, dès que l'entier $n = d\,m$ est *composé*, avec $1 < d < n$ et $1 < m < n$.

Autrement dit, il y a certains éléments $a \in \mathbb{A}$ qui n'ont (malheureusement) pas d'*inverse* $a' \in \mathbb{A}$ pour l'opération de multiplication $\times$. Toutefois, on peut décider de sélectionner seulement les éléments de $\mathbb{A}$ qui sont inversibles, pour la multiplication.

Définition 30.1. On appelle *groupe des inversibles* d'un anneau $\big(\mathbb{A}, +, \times\big)$ l'ensemble noté :

$$\mathbb{A}^{\times} := \big\{a \in \mathbb{A} \colon \text{ il existe } a' \in \mathbb{A} \text{ satisfaisant } a\,a' = 1_{\mathbb{A}}\big\}.$$

Par exemple :

$$\mathbb{Z}^{\times} = \big\{-1, +1\big\}.$$

Évidemment, l'inverse d'un élément $a \in \mathbb{A}^{\times}$ est unique, car si a'' est un *autre* inverse, en multipliant à gauche par a' :

$$a' \big(a\,(a' - a'') = 0 \big),$$

on trouve instantanément $a' = a''$.

Alors $A^{\times}$ est un groupe commutatif en lui-même pour l'opération $\times$, au sens de la Définition 5.1, essentiellement parce que :

$$a,\, b \in \mathbb{A}^{\times} \qquad \text{implique} \qquad a \times b \in \mathbb{A}^{\times} \qquad \text{avec} \qquad \big(a \times b\big)' = b' \times a',$$

puisque :

$$\begin{aligned} (a \times b)\,\big(b' \times a'\big) &= a \times \underline{b \times b'}_{\circ} \times a' \\ &= \underline{a \times a'}_{\circ} \\ &= 1. \end{aligned}$$

Mais attention ! On dit bien « *groupe* » (multiplicatif) des inversibles, et non pas « *anneau* » (faux !) des inversibles, car $\mathbb{A}^\times$ n'est jamais invariant pas addition/soustraction, comme le montre l'exemple stupide :

$$1 \in \mathbb{Z}^\times \quad \text{et} \quad -1 \in \mathbb{Z}^\times \qquad \overset{?}{\Longrightarrow} \qquad 1+(-1) = 0 \in \mathbb{Z}^\times \ \text{(ah non !)}.$$

Proposition 30.2. *L'ensemble* $(\mathbb{A}^\times, \times)$ *muni de la multiplication est un groupe commutatif.*

Démonstration. Comme la loi $\times$ est associative sur $\mathbb{A}$, elle l'est également sur $\mathbb{A}^\times$. L'élément neutre $1_\mathbb{A}$ est tautologiquement inversible, donc on a $1_\mathbb{A} \in \mathbb{A}^\times$, et $1_\mathbb{A}$ est élement neutre pour $\times$.

Enfin, tout élément $a \in \mathbb{A}^\times$ admet un inverse *dans* $\mathbb{A}^\times$, car l'existence de $a' \in \mathbb{A}$ avec $a\,a' = a'a = 1_\mathbb{A}$ montre que a' lui-même est inversible, avec a pour inverse, c'est-à-dire appartient aussi à $\mathbb{A}^\times$. □

31. Anneaux commutatifs produits

Dans la Section **33** suivante, nous allons comparer :

$$\mathbb{Z}/mn\mathbb{Z} \overset{?}{\longleftrightarrow} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

où m, n sont deux entiers *premiers entre eux*. À cette occasion, nous aurons besoin du concept de *produit* entre anneaux commutatifs, dont voici une

Définition 31.1. Étant donné deux anneaux commutatifs $\big(\mathbb{A}, +_\mathbb{A}, \times_\mathbb{A}\big)$ et $\big(\mathbb{B}, +_\mathbb{B}, \times_\mathbb{B}\big)$, l'*anneau produit* $\big(\mathbb{A}\times\mathbb{B},\ +,\ \times\big)$ est l'ensemble produit constitué de couples d'éléments :

$$\mathbb{A}\times\mathbb{B} := \big\{(a,b)\colon\ a\in\mathbb{A}\ \text{quelconque},\ b\in\mathbb{B}\ \text{quelconque}\big\},$$

pour lequel les deux lois de compositions interne $+$ et $\times$ sont définies par :

$$\begin{aligned}(a,b)+(a',b') &:= \big(a+_\mathbb{A} a',\ b+_\mathbb{B} b'\big) && \text{d'élément neutre } \big(0_\mathbb{A}, 0_\mathbb{B}\big),\\ (a,b)\times(a',b') &:= \big(a\times_\mathbb{A} a',\ b\times_\mathbb{B} b'\big) && \text{d'élément neutre } \big(1_\mathbb{A}, 1_\mathbb{B}\big).\end{aligned}$$

On vérifie par le raisonnement (tauto)logique que $\big(\mathbb{A}\times\mathbb{B},\ +,\ \times\big)$ est effectivement un anneau commutatif, au sens de la Définition 29.1.

Plus généralement, étant donné un nombre fini $\nu \geqslant 1$ d'anneaux commutatifs $\mathbb{A}_1, \dots, \mathbb{A}_\nu$, on peut construire l'*anneau-produit :*

$$\mathbb{A}_1\times\cdots\times\mathbb{A}_\nu := \big\{\big(a_1,\dots,a_\nu\big)\colon\ a_1\in\mathbb{A}_1\ \text{quelconque},\ \dots,\ a_\nu\in\mathbb{A}_\nu\ \text{quelconque}\big\},$$

muni des opérations :

$$\begin{aligned}\big(a_1,\dots,a_\nu\big)+\big(a'_1,\dots,a'_\nu\big) &:= \big(a_1+_{\mathbb{A}_1} a'_1,\dots,a_\nu+_{\mathbb{A}_\nu} a'_\nu\big),\\ \big(a_1,\dots,a_\nu\big)\times\big(a'_1,\dots,a'_\nu\big) &:= \big(a_1\times_{\mathbb{A}_1} a'_1,\dots,a_\nu\times_{\mathbb{A}_\nu} a'_\nu\big).\end{aligned}$$

Par exemple, avec :

$$\begin{aligned}\mathbb{Z}/2\mathbb{Z} &= \big\{0,\,1\big\}\ \mathsf{mod}\,2,\\ \mathbb{Z}/3\mathbb{Z} &= \big\{0,\,1,\,3\big\}\ \mathsf{mod}\,3,\end{aligned}$$

on a :

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z} = \big\{(0,0),\ (0,1),\ (0,2),\ (1,0)\ (1,1),\ (1,2)\big\}.$$

Proposition 31.2. *Le groupe des inversibles de l'anneau-produit* $\mathbb{A}\times\mathbb{B}$ *est :*

$$\big(\mathbb{A}\times\mathbb{B}\big)^\times = \mathbb{A}^\times\times\mathbb{B}^\times.$$

Preuve. Cela provient directement du fait que la loi de multiplication :

$$\big(a,\, b\big) \times \big(b,\, b'\big) \;=\; \big(aa',\, bb'\big),$$

s'effectue composante par composante. □

32. Isomorphismes entre anneaux commutatifs

Sur le plan didactique général, le terme « *isomorphisme* » désigne une relation entre des corps ou des objets de formes analogues, ou encore, entre des réalisations de même structure sous-jacente.

> La notion d'isomorphisme vient de la constatation qu'un individu tend à reconstruire autour de lui une constellation relationnelle qui reste relativement invariable même quand on le change de milieu.

En cristallographie, les corps dits « *isomorphes* » ont généralement une grande parenté dans leur constitution chimique, et notamment, ils ont la propriété de pouvoir se remplacer mutuellement dans la formation d'un même cristal, appelé parfois « *solution solide* ».

En linguistique aussi, « *isomorphisme* » est un concept avéré : il désigne une relation existant entre deux langues ou deux structures linguistiques, quand elles présentent toutes deux le même type de relations combinatoires.

En mathématiques enfin, un « *isomorphisme* » entre deux ensembles structurés est une application *bijective* qui *préserve* les structures respectives, et dont la réciproque *préserve aussi* ces structures.

> Le lecteur nous accordera que deux édifices mathématiques d'apparences fort dissemblables puissent, quand on examine leurs « secrètes architectures » conduire à des structures identiques, indiscernables. Chacun d'eux est la réalisation concrète d'un même groupe abstrait : on dit qu'ils sont « *en isomorphie* ». François LE LIONNAIS, Les grands courants de la pensée mathématique.

Un *isomorphisme* est donc une bijection pour laquelle les relations « algébriques » entre les éléments de l'ensemble d'arrivée sont les mêmes que celles entre leurs antécédents respectifs : la structure algébrique est préservée. Ce « méta-concept » mathématique admet une définition formelle.

Avec des symboles, soient E et F deux ensembles dont les éléments généraux sont notés e et f, respectivement. De plus, soient $\oplus$ et $\otimes$ leurs lois internes respectives. S'il existe une application bijective $\Phi\colon\, E \longrightarrow F$ satisfaisant :

$$\Phi\big(e_1 \oplus e_2\big) \;=\; \Phi(e_1) \otimes \Phi(e_2) \qquad (\forall\; e_1, e_2 \in E),$$

de telle sorte que la bijection réciproque $E \longleftarrow F \;:\Phi^{-1}$ satisfait de même :

$$\Phi^{-1}(f_1) \oplus \Phi^{-1}(f_2) \;=\; \Phi^{-1}\big(f_1 \otimes f_2\big) \qquad (\forall\; f_1, f_2 \in F),$$

alors on dit que les deux ensembles munis de structures $(E, \oplus)$ et $(F, \otimes)$ sont *isomorphes*. On dit que Φ et son inverse Φ^{-1} sont des *isomorphismes*. Quand $E = F$ et $\oplus = \otimes$, on dit que Φ est un *automorphisme*.

Parce qu'un isomorphisme préserve les aspects structuraux d'un ensemble, d'un groupe, d'un anneau, d'un corps, ou autres, on cherche souvent à *trouver* des isomorphismes qui envoient un objet « compliqué » vers un objet plus « simple » ou mieux connu, afin de comprendre, ou de mieux « pénétrer », ses propriétés mathématiques intimes.

Définition 32.1. Soient $\big(\mathbb{A}, +_{\mathbb{A}}, \times_{\mathbb{A}}\big)$ et $\big(\mathbb{B}, +_{\mathbb{B}}, \times_{\mathbb{B}}\big)$ deux anneaux commutatifs. Un *morphisme d'anneaux* de $\mathbb{A}$ vers $\mathbb{B}$ est une application $f\colon \mathbb{A} \longrightarrow \mathbb{B}$ satisfaisant [30] :

(1) $f\big(a +_{\mathbb{A}} a'\big) = f(a) +_{\mathbb{B}} f(a')$ pour tous $a, a' \in \mathbb{A}$;

(2) $f(0_{\mathbb{A}}) = 0_{\mathbb{B}}$;

(3) $f\big(a \times_{\mathbb{A}} a'\big) = f(a) \times_{\mathbb{B}} f(a')$, pour tous $a, a' \in \mathbb{A}$;

(4) $f(1_{\mathbb{A}}) = 1_{\mathbb{B}}$.

Quand f est bijectif, on dit que f est un *isomorphisme* [31].

> Certains auteurs — français — disent *morphisme*, plutôt que *homomorphisme*. Les anglais/américains disent *homomorphism*, les italiens *omomorfismo*, les espagnols *homomorfismo*, les allemands *Homomorphismus*, ou *Gruppenhomomorphismus*. Depuis quelques années, certains français disent *morphisme* — bon, . . . Thomas Delzant

Lorsque seules les conditions **(1)** et **(2)** sont satisfaites, on parle de morphismes de groupes commutatifs sous-jacents

Par exemple, l'application $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ définie par $x \longmapsto -x$ est un isomorphisme entre les deux groupes commutatifs $(\mathbb{Z}, +)$ et $(\mathbb{Z}, +)$, d'application inverse $-y \longleftarrow y$.

Terminologie 32.2. Quand $\mathbb{A} = \mathbb{B}$, on dit que f est un *endomorphisme* de $\mathbb{A}$. Quand $f\colon \mathbb{A} \longrightarrow \mathbb{A}$ est de plus bijectif, on dit que f est un *automorphisme* de $\mathbb{A}$.

Par (contre-)exemple, avec une constante non nulle $\lambda \in \mathbb{Z}\backslash\{0\}$, l'application $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ définie par $f(x) := \lambda\, x$ est un morphisme de groupes commutatifs $(\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$, mais dès que $\lambda \neq 1$, ce n'est *pas* un morphisme d'anneaux, car :

$$f\big(a\, a'\big) \;=\; \lambda\, a\, a' \;\neq\; (\lambda\, a)\, (\lambda\, a').$$

Définition 32.3. Le *noyau* d'un morphisme d'anneaux commutatifs $f\colon \mathbb{A} \longrightarrow \mathbb{B}$ est l'ensemble :

$$\mathsf{Ker}\, f \;:=\; \big\{a \in \mathbb{A}\colon\;\; f(a) = 0_{\mathbb{B}}\big\}.$$

Son *image* est l'ensemble :

$$\mathsf{Im}\, f \;:=\; \big\{b \in \mathbb{B}\colon\;\; \text{il existe } a \in \mathbb{A} \text{ tel que } f(a) = b\big\}.$$

L'Exercice 3 propose de vérifier que $\mathsf{Im}\, f$ est toujours un sous-anneau de $\mathbb{B}$.

Mais comme $\mathsf{Ker}\, f$ ne contient pas toujours $1_{\mathbb{A}}$, et comme on *demande* dans la Définition 29.1 d'anneau commutatif (unitaire) que la multiplication $\times$ ait un élément neutre 1, le noyau $\mathsf{Ker}\, f$, qui ne contient en général pas $1_{\mathbb{A}}$, n'est pas toujours un sous-anneau de $\mathbb{A}$.

Proposition 32.4. *Tout morphisme d'anneaux commutatifs $f\colon \mathbb{A} \longrightarrow \mathbb{B}$ induit, en restriction au groupe des inversibles $\mathbb{A}^{\times} \subset \mathbb{A}$, un morphisme de groupes commutatifs :*

$$f\colon\quad \mathbb{A}^{\times} \;\longrightarrow\; \mathbb{B}^{\times}.$$

Observons que nous n'avons pas encore formellement défini le concept de *morphisme entre groupes commutatifs*, mais le lecteur-étudiant aura certainement déjà deviné de quoi il s'agit.

30. On peut montrer que **(2)** est conséquence de **(1)**.

31. On peut vérifier que la bijection inverse $\mathbb{A} \longleftarrow \mathbb{B} : f^{-1}$ satisfait quatre axiomes similaires, par exemple $f^{-1}(b) +_{\mathbb{A}} f^{-1}(b') = f^{-1}(b +_{\mathbb{B}} b')$ ainsi que $f^{-1}(b) \times_{\mathbb{A}} f^{-1}(b') = f^{-1}(b \times_{\mathbb{B}} b')$.

Démonstration. Comme f est un morphisme d'anneaux, on sait déjà qu'il transfère (traduit) la multiplication dans $\mathbb{A}$ en la multiplication dans $\mathbb{B}$, et que $f(1_{\mathbb{A}}) = 1_{\mathbb{B}}$. La seule chose qui manque, c'est que f envoie bien les inversibles de $\mathbb{A}$ vers les inversibles de $\mathbb{B}$:

$$f\big(\mathbb{A}^\times\big) \overset{?}{\subset} \mathbb{B}^\times \textbf{ ?}$$

Mais si $a \in \mathbb{A}^\times$ admet l'inverse $a^{-1} \in \mathbb{A}^\times$ avec $a\,a^{-1} = 1_{\mathbb{A}}$, l'égalité suivante, vraie grâce au fait que f est un morphisme :

$$f(a)\,f(a^{-1}) \;=\; f\big(a\,a^{-1}\big) \;=\; f(1_{\mathbb{A}}) \;=\; 1_{\mathbb{B}},$$

montre aussitôt que $f(a^{-1}) := b'$ est un inverse de $f(a) = b$, unique en fait, que l'on peut d'ailleurs noter aussi b^{-1}.

Donc on a bien $f(a)$ inversible, quel que soit $a \in \mathbb{A}^\times$. □

33. Isomorphisme $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ pour $m \wedge n = 1$

Question 33.1. *Comment comparer les divers $\mathbb{Z}/n\mathbb{Z}$, lorsque $n \in \mathbb{Z}$ varie ?*

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x mod 3	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
x mod 5	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4

Par exemple, la première ligne (en caractères gras) du tableau ci-dessus liste les quinze éléments de $\mathbb{Z}/15\mathbb{Z}$, puis la seconde et la troisième ligne représentent tous les couples d'éléments du produit $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. On y constate que chaque paire d'éléments apparaît exactement une seule fois, et donc, que $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ possède *aussi* quinze éléments. Bientôt, nous allons expliquer de manière générale ce phénomène.

Commençons par une observation naturelle, élémentaire, et très utile.

Proposition 33.2. *Étant donné deux entiers $m \geqslant 1$ et $n \geqslant 1$, quels que soient $a, b \in \mathbb{Z}$, on a :*

$$a \;\equiv\; b \mod m\,n \qquad\Longrightarrow\qquad \begin{cases} a \;\equiv\; b \mod m, \\ a \;\equiv\; b \mod n. \end{cases}$$

Preuve. Cela est tout à fait clair :

$$a \;=\; b + m\,n\,k \qquad\Longrightarrow\qquad \begin{cases} a \;=\; b + m\,(n\,k), \\ a \;=\; b + n\,(m\,k). \end{cases}$$ □

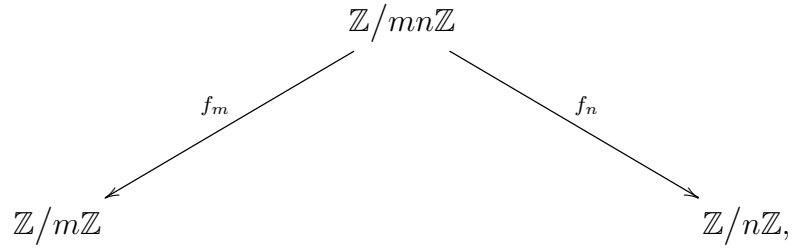
Corollaire 33.3. *Par contraposition de la première ligne :*

$$a \;\not\equiv\; b \mod m\,n \qquad\Longleftarrow\qquad a \;\not\equiv\; b \mod m.$$ □

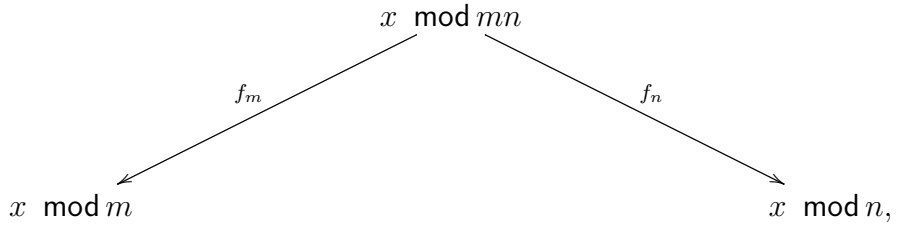
Nous pouvons illustrer cette proposition avec $m := 5$ et $n := 2$, où les $5 \cdot 2 = 10$ éléments de $\mathbb{Z}/10\mathbb{Z}$, sont réduits modulo 5 :

$$\begin{aligned} &\big\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\big\} \mod 10 \\ \text{deviennent}\quad &\big\{0,\ 1,\ 2,\ 3,\ 4,\ 0,\ 1,\ 2,\ 3,\ 4\big\} \mod 5. \end{aligned}$$

Proposition 33.4. *Soient deux entiers arbitraires $m \geqslant 1$ et $n \geqslant 1$. Alors il existe deux applications de réduction :*



définies par :



qui sont de plus des morphismes d'anneaux.

Par symétrie, on peut étudier seulement f_m. Ici, f_m prend un entier modulo $m\,n$ et le « réduit » modulo m, comme dans l'exemple des deux mains à cinq doigts ci-dessus.

D'abord, il faut vérifier que f_m est bien définie, ce que nous allons faire. Ensuite aussi, que l'on a bien, quels que soient $a, b \in \mathbb{Z}/mn\mathbb{Z}$:

$$\begin{aligned} f_m(a+b) \;&=\; f_m(a) + f_m(b), \\ f_m(a \times b) \;&=\; f_m(a) \times f_m(b). \end{aligned}$$

Attention ! Les opérations $+$, $\times$ *à gauche* s'effectuent modulo mn, c'est-à-dire dans $\mathbb{Z}/mn\mathbb{Z}$, tandis que les opérations $+$, $\times$ *à droite* s'effectuent modulo m, dans $\mathbb{Z}/m\mathbb{Z}$, qui comporte *moins* d'éléments — n fois moins, précisément.

Avec $m = 5$, $n = 2$, explicitons concrètement le fait que f_5 est un morphisme d'anneaux, sur deux exemples numériques :

$$\begin{aligned} 7+9 \underset{10}{\equiv} 6 \;\overset{f_5}{\longmapsto}\; \underset{5}{\equiv} 1 \quad &\overset{\text{OUI}}{=} \quad 1 \underset{5}{\equiv} 2+4 \;=\; f_5(7) + f_5(9), \\ 4 \times 7 \underset{10}{\equiv} 8 \;\overset{f_5}{\longmapsto}\; \underset{5}{\equiv} 3 \quad &\overset{\text{OUI}}{=} \quad 3 \underset{5}{\equiv} 4 \times 2 \;=\; f_5(4) \times f_5(7). \end{aligned}$$

Démonstration de la Proposition 33.4. Rappelons que :

$$\mathbb{Z}/mn\mathbb{Z} \;=\; \big\{0,\, 1,\, 2,\, \ldots,\, mn-1\big\} \mod mn.$$

Autrement dit, dans les calculs, tous les entiers de $\mathbb{Z}$ sont considérés modulo mn, et « ramenés dans la marmite », l'ensemble $\{0, 1, \ldots, mn-1\}$.

Un élément $a \in \mathbb{Z}/mn\mathbb{Z}$, c'est un $a \in \big\{0, 1, \ldots, mn-1\big\}$ avec la collection de tous les $a + mn\,k$, où $k \in \mathbb{Z}$ est quelconque. Et l'on identifie $a + mn\,k$ avec $a + mn\,k'$ *parce que* leur différence :

$$a + mn\,k - \big(a + mn\,k'\big) \;=\; m\,n\,\big(k - k'\big),$$

est un multiple de $m\,n$.

Commençons par montrer que l'application :

$$\begin{array}{rccc} f_m\colon & \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ & a \mod mn & \longmapsto & a \mod m, \end{array}$$

est *bien définie*. Il faut vérifier que f_m prend la même valeur sur deux éléments quelconques :

$$a + mn\,k \qquad \text{et} \qquad a + mn\,k',$$

et cela est clair, parce que un multiple de $m\,n$ est toujours un multiple de m :

$$\begin{array}{rc} & a + mn\,k \overset{?}{\equiv} a + mn\,k' \mod m \\ \iff & 0 \overset{\text{OUI}}{\equiv} m\,(n\,k' - n\,k) \mod m. \end{array}$$

Ensuite, montrons que f_m est un morphisme d'anneaux. Soient $a, b \in \mathbb{Z}/mn\mathbb{Z}$ quelconques. Quel que soient les quatre éléments de $\mathbb{Z}$:

$$\begin{array}{ll} a + m\,n\,k, & a + m\,n\,k', \\ b + m\,n\,\ell, & b + m\,n\,\ell', \end{array}$$

il vient par addition verticale :

$$a + \underline{m\,n\,k}_{\circ} + b + \underline{m\,n\,\ell}_{\circ} \mod m \;\equiv\; a + \underline{m\,n\,k'}_{\circ} + b + \underline{m\,n\,\ell'}_{\circ} \mod m,$$

donc on a bien :

$$f_m\big(\underbrace{a+b}_{\substack{\text{addition}\\ \text{modulo } mn}}\big) \;=\; \underbrace{f_m(a) + f_m(b)}_{\substack{\text{addition}\\ \text{modulo } m}}.$$

Pour ce qui est des deux multiplications possibles :

$$\begin{array}{rcl} \big(a + m\,n\,k\big)\,\big(b + m\,n\,\ell\big) & = & a\,b + a\,m\,n\,\ell + m\,n\,k\,b + m\,n\,k\,m\,n\,\ell, \\ \big(a + m\,n\,k'\big)\,\big(b + m\,n\,\ell'\big) & = & a\,b + a\,m\,n\,\ell' + m\,n\,k'\,b + m\,n\,k'\,m\,n\,\ell', \end{array}$$

leur résultat est *identique modulo* m, car les 3 derniers termes de chaque ligne sont visiblement tous multiples de m !

Donc on a bien aussi :

$$f_m\big(\underbrace{a\times b}_{\substack{\text{multiplication}\\ \text{modulo } mn}}\big) \;=\; \underbrace{f_m(a) + f_m(b)}_{\substack{\text{multiplication}\\ \text{modulo } m}}. \qquad \square$$

Répétons que les opérations $+$ et $\times$ ont un sens *différent* de part et d'autre du signe '='. Et dans la Définition 32.1 générale, nous avions bien spécifié que les additions et les multiplications pouvaient être *différentes* dans $\mathbb{A}$ et dans $\mathbb{B}$, lorsque nous avons écrit :

$$\begin{array}{rcl} f\big(a +_{\mathbb{A}} a'\big) & = & f(a) +_{\mathbb{B}} f(a'), \\ f\big(a \times_{\mathbb{A}} a'\big) & = & f(a) \times_{\mathbb{B}} f(a'). \end{array}$$

Nous parvenons enfin à un point de maturité théorique où nous pouvons exprimer une version mathématique abstraite et plus complète du Théorème 28.5 des restes chinois, déjà exposé avec des outils rudimentaires.

Le produit $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ étant encore un anneau, grâce à la Section **31**, nous pouvons « mettre ensemble » nos deux applications f_m et f_n, ce qui nous donne l'application :

$$\begin{aligned} f: \qquad \mathbb{Z}/mn\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x &\longmapsto \big(f_m(x),\, f_n(x)\big). \end{aligned}$$

Théorème 33.5. *Si $m \wedge n = 1$ sont premiers entre eux, alors le morphisme d'anneaux :*

$$\begin{aligned} f: \qquad \mathbb{Z}/mn\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x \bmod mn &\longmapsto \Big(x \bmod m,\ \ x \bmod n\Big), \end{aligned}$$

est un isomorphisme.

Démonstration. Il s'agit de montrer que f est *bijectif*. Mais comme :

$$q \,=\, \mathsf{Card}\,\big\{0,\, 1,\, 2,\, \ldots,\, q-1\big\},$$

tous ces anneaux sont de cardinal fini, *i.e.* ont un nombre fini d'éléments [32] :

$$\begin{aligned} mn \,&=\, \mathsf{Card}\,\mathbb{Z}/mn\mathbb{Z}, \qquad\qquad m \,=\, \mathsf{Card}\,\mathbb{Z}/m\mathbb{Z}, \qquad\qquad n \,=\, \mathsf{Card}\,\mathbb{Z}/n\mathbb{Z} \\ &=\, \mathsf{Card}\,\Big(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\Big), \end{aligned}$$

donc f est un morphisme entre anneaux de cardinaux *égaux*. Super !

Or puisque l'on sait qu'une application entre ensembles de même cardinal est bijective si et seulement si elle est injective, il va nous suffire de démontrer que :

$$f(x) \,=\, f(x') \qquad\qquad \overset{?}{\Longrightarrow} \qquad\qquad x \,=\, x'.$$

Mais comme f respecte l'addition, *i.e.* est un morphisme de groupes pour les lois $+$ respectives, ceci équivaut à [33] :

$$f(x - x') \,=\, (0, 0).$$

Avec $y := x - x'$, montrons donc que :

$$f(y) \,=\, \big(0 \bmod m,\ \ 0 \bmod n\big),$$

implique $y = 0$ dans $\mathbb{Z}/mn\mathbb{Z}$.

Or les deux équations $y \equiv 0 \bmod m$ et $y \equiv 0 \bmod n$ signifient qu'il existe $i \in \mathbb{Z}$ et $j \in \mathbb{Z}$ avec :

$$y \,=\, m\,i \qquad\qquad \text{et} \qquad\qquad y \,=\, n\,j.$$

Mais alors, l'égalité $m\,i = n\,j$ montre que $m\,i$ est divisible par n, et comme par hypothèse n est premier avec m, le Théorème 21.1 de Gauss force n à diviser i, c'est-à-dire $i = n\,k$, avec $k \in \mathbb{Z}$, d'où en remplaçant :

$$y \,=\, m\,n\,k \,=\, 0 \quad \text{ dans } \mathbb{Z}/mn\mathbb{Z}.$$

Donc f est injective, donc f est bijective, donc f établit un isomorphisme d'anneaux. Cela *achève* — à coups de hash ? — la démonstration. □

32. Rappelons en effet que si $E = \{e_1, \ldots, e_m\}$ et $F = \{f_1, \ldots, f_n\}$ sont deux ensembles finis, leur produit $E \times F$ a pour éléments tous les couples (e_i, f_j) avec $i = 1, \ldots, m$ et $j = 1, \ldots, n$, donc $\mathsf{Card}\, E \times F = \mathsf{Card}\, E \cdot \mathsf{Card}\, F$.

33. Oui, il y a bien deux zéros $(0, 0)$ à droite, le 0 de $\mathbb{Z}/m\mathbb{Z}$ et le 0 de $\mathbb{Z}/n\mathbb{Z}$ — pas d'erreur !

La Proposition 31.2 offre alors un corollaire direct de ce Théorème 33.5 chinois *occidentalisé*.

Théorème 33.6. *En restriction aux groupes d'inversibles respectifs, l'isomorphisme d'anneaux du théorème précédent offre un isomorphisme de groupes commutatifs :*

$$\begin{aligned} f\colon \qquad \big(\mathbb{Z}/mn\mathbb{Z}\big)^\times &\longrightarrow \big(\mathbb{Z}/m\mathbb{Z}\big)^\times \times \big(\mathbb{Z}/n\mathbb{Z}\big)^\times \\ x \bmod mn &\longmapsto \Big(x \bmod m,\ x \bmod n\Big). \end{aligned}$$

Enfin, énonçons un résultat général, sans en détailler la démonstration puisqu'une simple récurrence sur le nombre de facteurs fonctionne sans obstacle.

Théorème 33.7. *Étant donné un nombre $r \geqslant 1$ d'entiers $n_1, \dots, n_r$ mutuellement premiers entre eux $n_i \wedge n_j = 1$ pour $i \neq j$, il existe un isomorphisme d'anneaux commutatifs :*

$$\begin{aligned} f\colon \qquad \mathbb{Z}/n_1 \cdots n_r\mathbb{Z} &\longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \\ x \bmod n_1 \cdots n_r &\longmapsto \Big(x \bmod n_1,\ \dots,\ x \bmod n_r\Big), \end{aligned}$$

qui, en restriction aux groupes des inversibles respectifs, fournit aussi un isomorphisme de groupes commutatifs :

$$\begin{aligned} f\colon \qquad \big(\mathbb{Z}/n_1 \cdots n_r\mathbb{Z}\big)^\times &\longrightarrow \big(\mathbb{Z}/n_1\mathbb{Z}\big)^\times \times \cdots \times \big(\mathbb{Z}/n_r\mathbb{Z}\big)^\times \\ x \bmod n_1 \cdots n_r &\longmapsto \Big(x \bmod n_1,\ \dots,\ x \bmod n_r\Big). \end{aligned}$$

□

34. Multiplicativité de la fonction indicatrice φ d'Euler

Rappelons la Définition 27.10 de la fonction indicatrice d'Euler :

$$\begin{aligned} \varphi(n) &:= \mathsf{Card}\,\big\{1 \leqslant a \leqslant n\colon\ a \wedge n = 1\big\} \\ &= \mathsf{Card}\,\big(\mathbb{Z}/n\mathbb{Z}\big)^\times, \end{aligned}$$

Le résultat suivant, qui va découler du (très) beau Théorème 33.7, permet de calculer rapidement $\varphi(n)$ pour un entier n arbitraire.

Théorème 34.1. **(1)** *Si $m \geqslant 1$ et $n \geqslant 1$ sont premiers entre eux,* i.e. *vérifient $m \wedge n = 1$, alors :*

$$\varphi\big(m\,n\big) \,=\, \varphi(m)\,\varphi(n).$$

(2) *Si $p \in \mathscr{P}$ est premier, alors pour tout exposant $\alpha \geqslant 1$, on a :*

$$\varphi\big(p^\alpha\big) \,=\, p^\alpha - p^{\alpha-1}.$$

(3) *Pour un entier n arbitraire décomposé en facteurs premiers :*

$$n \,=\, p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

avec $p_1 < \cdots < p_r$ premiers et avec des exposants $\alpha_1 \geqslant 1$, …, $\alpha_r \geqslant 1$, on a :

$$\begin{aligned} \varphi(n) \,&=\, \varphi\big(p_1^{\alpha_1}\big) \cdots \varphi\big(p_r^{\alpha_r}\big) \\ &=\, \big(p_1^{\alpha_1} - p_1^{\alpha_1-1}\big) \cdots \big(p_r^{\alpha_r} - p_r^{\alpha_r-1}\big). \end{aligned}$$

Par exemple :

$$\begin{aligned}\varphi\big(1\,235\big) &= \varphi(5)\,\varphi(13)\,\varphi(19)\\ &= (5-1)\,(13-1)\,(19-1)\\ &= 4\cdot 12\cdot 18 \;=\; 864.\end{aligned}$$

Autre exemple :

$$\begin{aligned}\varphi\big(22\,500\,000\big) &= \varphi\big(2^5\big)\,\varphi\big(3^2\big)\,\varphi\big(5^7\big)\\ &= \big(2^5-2^4\big)\,\big(3^2-3^1\big)\,\big(5^7-5^6\big)\\ &= 16\cdot 6\cdot 625\,000\\ &= 6\,000\,000 \qquad \text{(d'euromillions).}\end{aligned}$$

Démonstration. Montrons **(1)**, appelée *propriété de multiplicativité* de la fonction indicatrice φ d'Euler.

Grâce à la Proposition 32.4, et à la Proposition 31.2, l'isomorphisme d'anneaux du Théorème 33.5 :

$$f\colon\quad \mathbb{Z}/mn\mathbb{Z} \;\xrightarrow{\sim}\; \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z},$$

induit par restriction aux groupes des inversibles respectifs un isomorphisme de groupes commutatifs :

$$\begin{aligned}\big(\mathbb{Z}/mn\mathbb{Z}\big)^\times \;&\xrightarrow{\sim}\; \big(\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\big)^\times\\ &= \big(\mathbb{Z}/m\mathbb{Z}\big)^\times\times\big(\mathbb{Z}/n\mathbb{Z}\big)^\times,\end{aligned}$$

donc en particulier, une *bijection*. Par conséquent :

$$\mathsf{Card}\,\big(\mathbb{Z}/mn\mathbb{Z}\big)^\times \;=\; \mathsf{Card}\,\big(\mathbb{Z}/m\mathbb{Z}\big)\times\cdot\mathsf{Card}\,\big(\mathbb{Z}/n\mathbb{Z}\big)^\times,$$

c'est-à-dire précisément $\varphi(m\,n)=\varphi(m)\,\varphi(b)$, ce qui offre **(1)**.

Ensuite, montrons **(2)**. Soit donc un nombre premier $p\in\mathscr{P}$, et soit un exposant $\alpha\geqslant 1$. Observons que dans la formule à démontrer :

$$\varphi\big(p^\alpha\big) \;\overset{?}{=}\; p^\alpha - p^{\alpha-1},$$

il y a un signe « $-$ ».

Or rappelons que pour un ensemble *fini* E, et un sous-ensemble quelconque $F\subset E$, on a :

$$\mathsf{Card}\,\big(E\backslash F\big) \;=\; \mathsf{Card}\,E - \mathsf{Card}\,F.$$

Ici, l'ensemble E concerné a pour cardinal :

$$\mathsf{Card}\,\big\{1\leqslant k\leqslant p^\alpha\big\} \;=\; p^\alpha.$$

Alors plutôt que de déterminer directement :

$$\varphi\big(p^\alpha\big) \;=\; \mathsf{Card}\,\big\{1\leqslant k\leqslant p^\alpha\colon\ k \text{ est premier avec } p^\alpha\big\},$$

comptons les *autres* k, c'est-à-dire ceux qui ne sont *pas* premiers avec p^α.

Assertion 34.2. *Toujours avec $\alpha\geqslant 1$, pour un entier $1\leqslant k\leqslant p^\alpha$, on a équivalence entre :*

(i) *k est divisible par p, c'est-à-dire $k=p\,\ell$, avec $\ell\in\mathbb{N}$;*

(ii) *k n'est* pas *premier avec p^α.*

Preuve. L'implication **(i)** $\Longrightarrow$ **(ii)** est claire, puisque p est alors un facteur commun entre $k = p\,\ell$ et p^α car $\alpha \geqslant 1$.

Montrons maintenant **(ii)** $\Longrightarrow$ **(i)**. Par hypothèse, $d := \mathsf{pgcd}\,(k, p^\alpha)$ est > 1. Or d divise p^α. Grâce à la Proposition 24.12, on sait que $d = p^\beta$ pour un exposant $0 \leqslant \beta \leqslant \alpha$. Comme $d > 1$, nécessairement $\beta \geqslant 1$.

Enfin, comme d divise aussi k, c'est-à-dire $k = d\,\ell = p^\beta\,\ell$ avec $\ell \in \mathbb{N}$, nous concluons que k est bien divisible par p :

$$k \;=\; p^\beta\,\ell \;=\; p\,\big(p^{\beta-1}\,\ell\big). \qquad \square$$

Nous obtenons donc bien **(2)** :

$$\begin{aligned}
\varphi\big(p^\alpha\big) \;&=\; p^\alpha - \mathsf{Card}\,\big\{1 \leqslant k \leqslant \alpha\colon\ k \text{ n'est } \textit{pas} \text{ premier avec } p^\alpha\big\} \\
&=\; p^\alpha - \mathsf{Card}\,\big\{1 \leqslant k \leqslant p^\alpha\colon\ k = p\,\ell\big\} \\
&=\; p^\alpha - \mathsf{Card}\,\big\{1 \leqslant \ell \leqslant p^{\alpha-1}\big\} \\
&=\; p^\alpha - p^{\alpha-1}.
\end{aligned}$$

Pour terminer, montrons **(3)** en utilisant **(1)** et **(2)** :

$$\begin{aligned}
\varphi\big(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\big) \;&=\; \varphi\big(p_1^{\alpha_1}\big)\,\varphi\big(p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r}\big) \\
&=\; \big(p_1^{\alpha_1} - p_1^{\alpha_1-1}\big)\,\varphi\big(p_2^{\alpha_2}\big)\,\varphi\big(p_3^{\alpha_3} \cdots p_r^{\alpha_r}\big) \\
&=\; \big(p_1^{\alpha_1} - p_1^{\alpha_1-1}\big)\,\big(p_2^{\alpha_2} - p_2^{\alpha_2-1}\big) \cdots \big(p_r^{\alpha_r} - p_r^{\alpha_r-1}\big). \qquad \square
\end{aligned}$$

35. Théorème d'Euler

Le Théorème d'Euler généralise le Théorème 25.1 de Fermat, qui ne traitait que le cas où $n = p$ était un nombre premier. Ce théorème d'arithmétique modulaire, publié [34] en 1761 par le mathématicien suisse Leonhard Euler, s'énonce comme suit.

Théorème 35.1. [Euler] *Pour tout entier $n \geqslant 1$, et tout entier $a \wedge n = 1$ premier avec n,* i.e. *inversible modulo n, on a :*

$$a^{\varphi(n)} \;\equiv\; 1 \mod n.$$

Par exemple, en base 10, proposons-nous de trouver le chiffre des unités de :

$$7^{\,222},$$

c'est-à-dire de trouver quel nombre (chiffre) entre 0 et 9 est congru à 7^{222} modulo 10. C'est facile ! Il suffit de voir que 7 et 10 sont premiers entre eux, et de savoir que $\varphi(10) = 4$, ce que l'on peut constater à partir de la table de multiplication suivante :

*	**[0]**	**[1]**	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**	**[7]**	**[8]**	**[9]**
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[2]	[0]	[2]	[4]	[6]	[8]	[0]	[2]	[4]	[6]	[8]
[3]	[0]	[3]	[6]	[9]	[2]	[5]	[8]	[1]	[4]	[7]
[4]	[0]	[4]	[8]	[2]	[6]	[0]	[4]	[8]	[2]	[6]
[5]	[0]	[5]	[0]	[5]	[0]	[5]	[0]	[5]	[0]	[5]
[6]	[0]	[6]	[2]	[8]	[4]	[0]	[6]	[2]	[8]	[4]
[7]	[0]	[7]	[4]	[1]	[8]	[5]	[2]	[9]	[6]	[3]
[8]	[0]	[8]	[6]	[4]	[2]	[0]	[8]	[6]	[4]	[2]
[9]	[0]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

34. L. EULER, *Theoremata arithmetica nova methodo demonstrata*, Novi Comment. Acad. Sci. Imp. Petrop., vol. 8, 1763, pp. 74–104.

Le Théorème 35.1 d'Euler nous indique donc que :

$$7^4 \equiv 1 \mod 10,$$

d'où :

$$\begin{aligned} 7^{222} = 7^{4\cdot 55+2} &= \left(7^4\right)^{55} \cdot 7^2 \\ &\equiv 1^{55} \cdot 7^2 \\ &\equiv 49 \equiv 9 \mod 10. \end{aligned}$$

Le chiffre recherché est donc 9.

Démonstration. Les arguments, simples et élégants, sont essentiellement dus à Lagrange. Soit donc $n \geqslant 1$. On fixe $a \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ avec $a \wedge n = 1$, d'où $a \in \left\{2, \ldots, n-1\right\}$.

Assertion 35.2. [Point-clé] *Pour a premier avec n, l'application suivante est une bijection :*

$$\begin{array}{ccc} \left(\mathbb{Z}/n\mathbb{Z}\right)^\times & \longrightarrow & \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \\ x & \longmapsto & a\,x. \end{array}$$

Preuve. Comme $a \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ est inversible, il existe $a^{-1} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ avec $a^{-1}a = 1$, dans $\mathbb{Z}/n\mathbb{Z}$.

Comme l'espace de départ et l'espace d'arrivée sont tous deux égaux — à $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ — et de cardinal fini, il suffit de vérifier que cette application est *injective*.

Si donc $a\,x \equiv a\,x' \mod n$, c'est-à-dire $a\,(x-x') \equiv 0$, utilisons a^{-1} pour déduire la coïncidence $x = x'$ témoignant de l'injectivité :

$$a^{-1}\left(\, a\,(x-x') \equiv 0 \,\right) \qquad \text{donne} \qquad x - x' \equiv 0. \qquad \square$$

Par conséquent, les deux ensembles suivant sont égaux, *i.e.* ont exactement les mêmes éléments :

$$\left\{x\colon\ x \in (\mathbb{Z}/n\mathbb{Z})^\times\right\} = \left\{a\,x\colon\ x \in (\mathbb{Z}/n\mathbb{Z})^\times\right\},$$

dont le nombre total est bien sûr égal à $\varphi(n)$. Très astucieusement, introduisons alors le produit :

$$\begin{aligned} \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x &= \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} a\,x \\ &= a^{\varphi(n)} \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x, \end{aligned}$$

le signe '$=$' étant entendu *dans l'anneau* $\mathbb{Z}/n\mathbb{Z}$, puis multiplions l'égalité obtenue par le produit de tous les inverses x^{-1} possibles :

$$\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x^{-1} \left(\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x = a^{\varphi(n)} \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x \right),$$

ce qui offre la conclusion :

$$1 = a^{\varphi(n)}. \qquad \square$$

36. Appendice : Injections, Surjections, Bijections

Fill ??

37. Exercices

Exercice 1. [Caractérisation linéaire du pgcd] Étant donné deux constantes entières $a, b \in \mathbb{Z}$, on considère l'ensemble de leurs combinaisons linéaires à coefficients entiers :

$$\mathbb{Z}\,a + \mathbb{Z}\,b \;:=\; \big\{u\,a + v\,b\colon\ u \in \mathbb{Z},\ v \in \mathbb{Z}\big\}.$$

(a) Que dire lorsque $a = b = 0$?

(b) On suppose dorénavant $(a, b) \neq (0, 0)$ non tous les deux nuls. Soit $d := \mathsf{pgcd}\,(a, b)$. On introduit aussi :

$$\mathbb{Z}\,d \;:=\; \big\{w\,d\colon\ w \in \mathbb{Z}\big\}.$$

Montrer que $\mathbb{Z}\,d \subset \mathbb{Z}\,a + \mathbb{Z}\,b$.

(c) Inversement, montrer que $\mathbb{Z}\,a + \mathbb{Z}\,b \subset \mathbb{Z}\,d$. Indication: Dieu Bézout, aidez-nous !

(d) Conclure en énonçant un théorème soigné, clair, précis.

Exercice 2. Soit un anneau commutatif $\big(\mathbb{A}, +, \times\big)$ dans lequel $1_{\mathbb{A}} = 0_{\mathbb{A}}$. Montrer que $\mathbb{A} = \{0_{\mathbb{A}}\big\}$. Indication: Utiliser les axiomes.

Exercice 3. Soit un morphisme $f\colon \mathbb{A} \longrightarrow \mathbb{B}$ d'anneaux commutatifs. Montrer que $\mathsf{Im}\ f$ est un sous-anneau de $\mathbb{B}$.

Exercice 4. EE

Groupes abstraits

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Introduction

2. Définition de la structure de groupe, exemples, et conséquences

Dans le chapitre consacré à l'arithmétique sur $\mathbb{Z}$ et sur $\mathbb{Z}/n\mathbb{Z}$, nous avons déjà introduit les axiomes définissant les groupes abstraits, mais en requérant la commutativité de la loi interne. Dévoilons enfin la notion la plus générale possible.

Définition 2.1. Un *groupe* est un couple $(G, *)$, où G est un ensemble non vide, et où $*\colon G \times G \longrightarrow G$ est une *loi interne* vérifiant les trois axiomes suivants.

(A1) La loi $*$ est associative : Pour tous $x, y, z \in G$ on a :

$$x * \big(y * z\big) \;=\; \big(x * y\big) * z.$$

(A2) La loi $*$ possède un élément neutre : Il existe un élément $e \in G$ tel que, pour tout $x \in G$:

$$x * e \;=\; x \;=\; e * x.$$

(A3) Tout élément possède un symétrique : Pour tout $x \in G$, il existe $x' \in G$ tel que :

$$x * x' \;=\; e \;=\; x' * x.$$

Par un simple jeu logique avec ces axiomes, on vérifie alors la

Proposition 2.2. *L'élément neutre e est unique, et le symétrique x' d'un $x \in G$ quelconque est aussi unique.*

Démonstration. Si e' est un autre élément neutre, on a $e' * e = e' = e * e'$ par **(A2)** appliqué à $x := e'$. Mais puisque e' est aussi un élément neutre, on réapplique **(A2')** — écrit avec e' au lieu de e — à $x := e$, ce qui donne $e * e' = e = e' * e$. En comparant, on trouve $e = e'$.

Ensuite, si x'' est un autre inverse de x, c'est-à-dire si $x * x'' = e = x'' * x$, on multiplie cela par x' pour obtenir la coïncidence des deux inverses :

$$\big(\; e \;=\; x'' * x \;\big)\, x' \qquad \text{donne} \qquad \begin{aligned} x' \;&=\; x'' * \underline{x * x'}_{\circ} \\ &=\; x'' * e \\ &=\; x''. \end{aligned}$$

□

Pour n'avoir pas à démontrer cette petite propositionette, nous aurions pu demander directement dans les axiomes que e et x' soient uniques.

Notation 2.3. On note alors x^{-1} l'unique symétrique d'un $x \in G$.

Terminologie 2.4. Un groupe $(G, *)$ est dit *commutatif*, ou *abélien*, si sa loi satisfait :

$$x * y \;=\; y * x \qquad (\forall\, x, y \in G).$$

Voici quelques exemples simples de groupes, en vrac, avec un non-exemple au milieu.

• Un singleton tout bête $\{e\}$ peut être muni de la structure de groupe « triviale » $e * e := e$. Peu intéressant…

• Les couples $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes commutatifs.

• Les couples $\big(\mathbb{R}\backslash\{0\}, \times\big)$, $\big(\mathbb{C}\backslash\{0\}, \times\big)$ sont des groupes commutatifs.

• Plusieurs fois, nous avons fait observer que le couple $\big(\mathbb{Z}\backslash\{0\}, \times\big)$ n'est *pas* un groupe, car par exemple l'entier [1] $1\,729$ n'a pas d'inverse multiplicatif dans $\mathbb{Z}$.

• Si E est un $\mathbb{K}$-espace vectoriel quelconque, $(E, +)$ est un groupe commutatif, par exemple $\big(\mathscr{M}_{n\times n}(\mathbb{R}), +\big)$.

Surtout, voici l'exemple *canonique* de ce qu'est un groupe, exemple que nous étudierons en détail dans ce chapitre.

Exemple 2.5. [Permutations d'un ensemble] Soit E un ensemble. L'ensemble $\mathfrak{S}(E)$ des bijections de E dans lui-même :

$$\sigma \;:\quad E \;\xrightarrow{\sim}\; E,$$

muni de la loi de groupe qui est la *composition* $\tau * \sigma := \tau \circ \sigma$ des bijections :

$$E \xrightarrow{\;\sigma\;} E \xrightarrow{\;\tau\;} E, \qquad \text{(avec } \tau\circ\sigma \text{ en arc au-dessus)}$$

est un groupe, appelé *groupe des permutations de* E, ou *groupe symétrique de* E. En effet, la composition des applications est associative (connu), et l'inverse (pour la structure de groupe) d'une bijection $\sigma\colon E \longrightarrow E$ est tout simplement la bijection inverse $E \longleftarrow E : \sigma^{-1}$, tandis que l'élément neutre est évidemment l'application identité $\mathsf{Id}\colon E \longrightarrow E$.

Rappelons pourquoi, entre le bas et le haut du diagramme ci-dessus, il y a une *inversion* de l'ordre d'apparition des lettres σ et τ. C'est parce que par convention, pour tout $x \in E$, on pose en respectant l'ordre des lettres :

$$\tau \circ \sigma\,(x) \;:=\; \tau\big(\sigma(x)\big),$$

1. En effet, $\frac{1}{1\,729} = 0,00\ldots$. Ce nombre $1\,729$ est également connu sous le nom de « *nombre de Hardy-Ramanujan* » ; il s'agit du plus petit entier naturel s'écrivant de deux manières différentes comme somme de deux cubes :

$$1\,729 \;=\; 12^3 + 1^3 \;=\; 10^3 + 9^3.$$

Bien qu'elle ait été découverte en 1657 par Bernard Frénicle de Bessy, cette propriété de $1\,729$ est lié à une anecdote relatée par le mathématicien britannique Godfrey Harold Hardy après une visite à son collègue indien Srinivasa Ramanujan, hospitalisé en 1917.

> Je me souviens d'une fois où j'arrivai à son chevet à Putney. J'avais été conduit par le taxi numéro $1\,729$; la morosité qui semblait émaner de ce nombre avait attiré mon attention. J'espérais qu'il ne constituait pas un mauvais présage. « Non, me répondit-il, c'est un nombre fort intéressant ; c'est le plus petit que l'on puisse exprimer comme somme de deux cubes de deux manières différentes. » Hardy, *A Mathematician's Apology*, Cambridge, 1940.

et alors, ceci montre bien que l'on commence par appliquer $\sigma(\bullet)$ à x avant d'appliquer $\tau\big(\sigma(\bullet)\big)$, et donc du point de vue de l'*action*, la flèche σ *précède* la flèche τ :

$$\begin{array}{ccccc} E & \xrightarrow{\sigma} & E & \xrightarrow{\tau} & E \\ x & \overset{\sigma}{\longmapsto} & \sigma(x) & \overset{\tau}{\longmapsto} & \tau\big(\sigma(x)\big). \end{array}$$

En général, la composition des applications n'est (absolument) *pas* commutative :

$$x \xrightarrow{\tau} \tau(x) \xrightarrow{\sigma} \sigma\big(\tau(x)\big) \quad \text{(arc } \sigma\circ\tau\text{)} \qquad \text{diffère de} \qquad x \xrightarrow{\sigma} \sigma(x) \xrightarrow{\tau} \tau\big(\sigma(x)\big) \quad \text{(arc } \tau\circ\sigma\text{)}$$

c'est-à-dire :

$$\sigma \circ \tau \neq \tau \circ \sigma \qquad \text{(en général)}.$$

Proposition 2.6. *Le groupe $\mathfrak{S}(E)$ des permutations d'un ensemble E :*

(1) *est commutatif pour* $\mathsf{Card}\, E = 1, 2$*;*

(2) *n'est* jamais *commutatif dès que* $\mathsf{Card}\, E \geqslant 3$ *— c'est-à-dire la plupart du temps !*

Démonstration. **(1)** Soit $\mathsf{Card}\, E = 2$. On peut supposer $E = \{1, 2\}$. Alors $\mathfrak{S}(E)$ ne comporte que deux bijections :

$$\begin{array}{cccc} & 1 & 2 \\ \sigma & \downarrow & \downarrow \\ & 1 & 2 \end{array} \qquad \text{et} \qquad \begin{array}{cccc} & 1 & 2 \\ \tau & \downarrow & \downarrow \\ & 2 & 1 \end{array}$$

Notons que $\sigma = \mathsf{Id}$. Donc σ et τ commutent trivialement, puisque $\mathsf{Id} \circ \tau = \tau = \tau \circ \mathsf{Id}$ est toujours vrai. *Too easy, Daisy !*

(2) Soit maintenant $\mathsf{Card}\, E \geqslant 3$. On peut supposer $E \supset \{1, 2, 3\}$. On va considérer des bijections $\sigma\colon E \longrightarrow E$ qui se restreignent en l'identité sur le complémentaire $E\backslash\{1, 2, 3\}$, c'est-à-dire qui satisfont $\sigma(x) = x$ pour tout $x \neq 1, 2, 3$. On peut même supposer que $E = \{1, 2, 3\}$, puisque aucun élément ne change de place ailleurs.

Soient alors les deux bijections :

$$\begin{array}{cccccc} & 1 & 2 & 3 \\ \sigma & \downarrow & \downarrow & \downarrow \\ & 2 & 1 & 3 \end{array} \qquad \text{et} \qquad \begin{array}{cccccc} & 1 & 2 & 3 \\ \tau & \downarrow & \downarrow & \downarrow \\ & 1 & 3 & 2 \end{array}$$

La première échange $1 \longleftrightarrow 2$ en laissant 3 fixé, et la seconde échange $2 \longleftrightarrow 3$ en laissant 1 fixé. *Quite simple, isn't it ?*

Mais ces deux petites babioles ne commutent pas entre elles ! En effet :

$$\begin{array}{cccccc} & 1 & 2 & 3 \\ \tau & \downarrow & \downarrow & \downarrow \\ & 1 & 3 & 2 \\ \sigma & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 \end{array} \qquad \text{diffère de} \qquad \begin{array}{cccccc} & 1 & 2 & 3 \\ \sigma & \downarrow & \downarrow & \downarrow \\ & 2 & 1 & 3 \\ \tau & \downarrow & \downarrow & \downarrow \\ & 3 & 1 & 2 \end{array},$$

c'est-à-dire :

$$\begin{array}{cccccc} & 1 & 2 & 3 \\ \sigma\circ\tau & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 \end{array} \qquad \text{diffère de} \qquad \begin{array}{cccccc} & 1 & 2 & 3 \\ \tau\circ\sigma & \downarrow & \downarrow & \downarrow \\ & 3 & 1 & 2 \end{array} \qquad \square$$

Dans la suite du cours, nous allons étudier le groupe $\mathfrak{S}(E)$ des permutations d'un ensemble E, principalement dans le cas d'un ensemble *fini*, au sens où $\mathsf{Card}\, E < \infty$.

Exemple 2.7. [Groupe linéaire $\mathsf{GL}_{\mathbb{K}}(E)$] Soit E un espace vectoriel de dimesion finie $n \geqslant 1$ sur un corps commutatif $\mathbb{K}$. Alors l'ensemble des applications linéaires *bijectives* $f\colon E \longrightarrow E$, qu'on appelle *automorphismes linéaires de* E, forme un groupe pour la composition des applications linéaires :

$$E \xrightarrow{f} E \xrightarrow{g} E, \qquad g\circ f$$

groupe que l'on note $\mathsf{GL}_n(E,\mathbb{K})$, ou simplement $\mathsf{GL}(E)$.

Après le choix d'une base $\boldsymbol{B} = \big\{e_1, \ldots, e_n\big\}$ de l'espace vectoriel E, on peut identifier $\mathsf{GL}_n(E,\mathbb{K})$ à l'ensemble $\big(\mathscr{M}_{n\times n}(\mathbb{K}), \cdot\big)$ des matrices de taille $n \times n$ muni de la multiplication matricielle $M \cdot N$, qui correspond à la composition des applications linéaires $f \circ g$, avec bien entendu :

$$M \;:=\; \mathsf{Mat}_{\boldsymbol{B}}\, f \qquad\qquad \text{et} \qquad\qquad N \;:=\; \mathsf{Mat}_{\boldsymbol{B}}\, g.$$

Mais attention ! Rappelons que dès que $\mathsf{dim}_{\mathbb{K}} E \geqslant 2$, la multiplication entre deux matrices quelconques ne commute *pas*, donc $\mathsf{GL}(E)$ n'est *pas* un groupe commutatif, comme le montre la petite bagatelle :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \;=\; \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \;\neq\; \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \;=\; \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Voici encore trois exemples un peu plus « avancés » de groupes, que l'on peut « sauter » en première lecture.

• Si $(G,*)$ est un groupe et si X est un ensemble quelconque, on note G^X l'ensemble des applications $f\colon X \longrightarrow G$. Pour toutes applications $f, g \in G^X$, on définit l'application $f * g\colon X \longrightarrow G$ par :

$$(f * g)(x) \;:=\; f(x) * g(x) \qquad\qquad (x \in X).$$

Alors on vérifie (exercice) que $(G^X, *)$ est un groupe, notamment, on peut déterminer (exercice) l'élément neutre et l'inverse d'un élément quelconque.

• Si $(G,*)$ est un groupe, l'ensemble des suites $\{g_n\}_{n=0}^{\infty}$ d'éléments de G est un groupe. C'est d'ailleurs un cas particulier de l'exemple précédent, puisqu'une suite n'est rien d'autre qu'une application $f\colon \mathbb{N} \longrightarrow G$.

• Si $(G,*)$ et $(G',*')$ sont deux groupes, l'ensemble $G \times G'$, muni de la loi interne :

$$\begin{array}{rcl} (G \times G') \times (G \times G') & \longrightarrow & G \times G' \\ \big((g_1, g_1'),\ (g_2, g_2')\big) & \longmapsto & \big(g_1 * g_2,\ g_1' *' g_2'\big), \end{array}$$

est un groupe, appelé *produit direct (externe)* de G et de G'.

Souvent, dans les énoncés qui suivront, nous omettrons de préciser la loi $*$ du groupe G, et nous parlerons du groupe G, plutôt que du groupe $(G,*)$. Ceci, pour alléger les notations.

Le produit de deux éléments x et y de G sera donc souvent noté simplement $x\,y$, sans aucun symbole, et l'élément neutre 1_G, ou même 1 si aucune confusion n'est à craindre.

Attention ! Néanmoins, cette loi $*$ n'est pas forcément la multiplication au sens usuel ; il s'agit juste d'une notation commode lorsqu'on travaille avec une structure de groupe

générale. Et surtout, comme la plupart des groupes qui existent dans la Nature ne sont *pas* commutatifs, il faudra respecter scrupuleusement l'ordre des termes. Par exemple, $x\,y\,z$ est en général différent de $z\,x\,y$, même si la notation semble indiquer une multiplication commutative.

Parfois, lorsque le groupe considéré G est commutatif, on utilise la notation $+$ pour la loi $*$, qui se comporte donc *comme* l'addition usuelle entre nombres entiers, rationnels, ou réels. Dans ce cas précis, l'élément neutre est noté 0_G ou 0, et l'inverse (le symétrique) d'un élément $x \in G$ est noté $-x$.

Pour $n \geqslant 1$ éléments $x_1, \ldots, x_n \in G$, le produit $x_1 \cdots x_n$, dans cet ordre *non interchangeable*, qui sera parfois noté $\prod_{i=1}^{n} x_i$, est défini par :

- $x_1 \cdots x_n := 1_G$ pour $n = 0$;
- par récurrence $x_1 \cdots x_{n-1} x_n := (x_1 \cdots x_{n-1})\, x_n$ pour $n \geqslant 0$.

En tout cas, remarquons que grâce à l'associativité de la loi de groupe, pour tout $1 \leqslant k \leqslant n$, on a :

$$\big(x_1 \cdots x_k\big)\,\big(x_{k+1} \cdots x_n\big) \;=\; x_1 \cdots x_k \cdots x_n.$$

Ensuite, pour $n \in \mathbb{Z}$ quelconque, on pose :

$$\begin{aligned} x^n \;&:=\; x \cdots x && \text{(pour } n \geqslant 1\text{)},\\ x^0 \;&:=\; 1, \\ x^n \;&:=\; x^{-1} \cdots x^{-1} && \text{(pour } n \leqslant -1\text{)}. \end{aligned}$$

On a alors les propriétés agréables, pour tous $m, n \in \mathbb{Z}$:

$$x^m\,x^n \;=\; x^{m+n} \;=\; x^n\,x^m \qquad \text{et} \qquad \big(x^m\big)^n \;=\; x^{mn} \;=\; \big(x^n\big)^m. \tag{2.8}$$

Ces égalités sont faciles à vérifier, bien qu'il soit un peu fastidieux de les établir dans les moindres détails.

Attention ! 2.9. *En général, deux éléments quelconques $x, y \in G$ satisfont $x\,y \neq y\,x$, ainsi que :*

$$(x\,y)^n \;\neq\; x^n\,y^n \qquad (n \in \mathbb{Z}),$$

sauf si $x\,y = y\,x$ commutent entre eux, par exemple si G est commutatif.

En effet, si on suppose que $x\,y = y\,x$, il vient par exemple pour $n = 2$:

$$\big(x\,y\big)^2 \;=\; x\,y\,x\,y \;=\; x\,x\,y\,y \;=\; x^2\,y^2,$$

et ainsi de suite pour $n = 3, 4, 5, \ldots$.

Proposition 2.10. *Soit G un groupe arbitraire.*

(1) La loi de groupe est simplifiable : *Pour tous $x, y, z \in G$, on a :*

$$x\,z \;=\; y\,z \quad\Longrightarrow\quad x \;=\; y \qquad \textit{et} \qquad z\,x \;=\; z\,y \quad\Longrightarrow\quad x \;=\; y.$$

(2) *Pour tout $x \in G$, on a :*

$$\big(x^{-1}\big)^{-1} \;=\; x.$$

(3) *Pour tous $x_1, x_2, \ldots, x_n$ dans G, on a — noter l'inversion de l'ordre des termes — :*

$$\big(x_1\,x_2 \cdots x_n\big)^{-1} \;=\; x_n^{-1} \cdots x_2^{-1} x_1^{-1}.$$

(4) *Pour tout $a \in G$, les translations l_a à gauche et r_a à droite :*

$$l_a : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & a\,x \end{array} \qquad \textit{et} \qquad r_a : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x\,a \end{array}$$

sont bijectives.

Démonstration. **(1)** On multiplie à droite et à gauche par z^{-1} :

$$\big(\, x\,z \,=\, y\,z \,\big)\, z^{-1} \qquad \text{et} \qquad z^{-1}\,\big(\, z\,x \,=\, z\,y \,\big),$$

ce qui donne :

$$x\,\underline{z\,z^{-1}}_{\circ} \,=\, y\,\underline{z\,z^{-1}}_{\circ} \qquad \text{et} \qquad \underline{z^{-1}\,z}_{\circ}\,x \,=\, \underline{z^{-1}\,z}_{\circ}\,y,$$

c'est-à-dire $x = y$ dans les deux cas.

(2) Puisque x^{-1} est l'inverse de x, c'est-à-dire :

$$x^{-1}\,x \,=\, 1_G \,=\, x\,x^{-1},$$

on voit que ces deux équations montrent aussi que x est l'inverse (unique) de x^{-1}, donc on a bien $\big(x^{-1}\big)^{-1} = x$, de manière essentiellement tautologique.

(3) Traitons le cas $n = 2$, avec les notations x, y au lieu de x_1, x_2. Grâce à l'associativité, on a :

$$\begin{aligned} (x\,y)\,\big(y^{-1}\,x^{-1}\big) \,&=\, x\,\underline{y\,y^{-1}}_{\circ}\,y \\ &=\, x\,1_G\,x^{-1} \\ &=\, \underline{x\,x^{-1}}_{\circ} \\ &=\, 1_G, \end{aligned} \qquad \begin{aligned} \big(y^{-1}\,x^{-1}\big)\,(x\,y) \,&=\, y^{-1}\,\underline{x^{-1}\,x}_{\circ}\,y \\ &=\, y^{-1}\,1_G\,y \\ &=\, \underline{y^{-1}\,y}_{\circ} \\ &=\, 1_G. \end{aligned}$$

Ensuite, une récurrence-express donne aussitôt :

$$\begin{aligned} \big(x_1 \cdots x_{n-1}\,x_n\big)^{-1} \,&=\, x_n^{-1}\,\big(x_1 \cdots x_{n-1}\big)^{-1} \\ &=\, x_n^{-1}\,x_{n-1}^{-1} \cdots x_1^{-1}. \end{aligned}$$

(4) Évidemment, $l_{a^{-1}}$ est la bijection inverse de l_a, car :

$$l_{a^{-1}}\big(l_a(x)\big) \,=\, l_{a^{-1}}\big(a\,x\big) \,=\, \underline{a^{-1}\,a}_{\circ}\,x \,=\, x \,=\, l_a\big(l_{a^{-1}}(x)\big),$$

et de manière analogue, $r_{a^{-1}}$ est la bijection inverse de r_a. □

Les translations $l_a(\bullet)$ et $r_a(\bullet)$ dans un groupe G jouent un rôle théorique capital, non seulement pour les groupes de permutations $\mathfrak{S}(E)$ d'ensembles E finis comme nous le verrons, mais aussi dans la théorie dite des *groupes continus (infinis) de transformations* (niveau Master 1 ou 2), dont nous ne pourrons malheureusement pas parler dans ce cours de niveau Licence 2.

Terminologie 2.11. Si G est un groupe *fini*, c'est-à-dire avec $\mathsf{Card}\,G < \infty$, son nombre d'éléments, noté de manière abrégée :

$$|G| \,:=\, \mathsf{Card}\,G,$$

sera appelé l'*ordre* de G.

Ce terme « *ordre* » pour désigner un simple nombre d'éléments est un peu « bizarre », mais telle est la tradition terminologique ! Pour un ensemble quelconque E de cardinal fini, on notera aussi de manière abrégée :

$$|E| \,:=\, \mathsf{Card}\, E.$$

Alors si E est en ensemble fini et si $n := |E|$ est son nombre d'éléments, après une numérotation quelconque, on peut supposer pour fixer les idées que :

$$E \,=\, \big\{1,\, 2,\, \ldots,\, n-1,\, n\big\}.$$

Théorème 2.12. *Si E est un ensemble fini à $n \geqslant 1$ éléments, alors $\mathfrak{S}(E)$ est un groupe fini d'ordre (de cardinal) égal à la factorielle $n!$*

Démonstration. Donc on suppose $E = \{1, \ldots, n\}$. Il s'agit de compter combien de permutations de cet ensemble $\{1, \ldots, n\}$ sont possibles.

Or se donner une permutation de $\{1, \ldots, n\}$ revient à se donner n entiers $\sigma(1), \ldots, \sigma(n)$ distincts deux à deux et tous contenus dans $\{1, \ldots, n\}$.

Donc au début, il y a n choix possibles pour $\sigma(1)$. Une fois $\sigma(1)$ choisi, il n'y a plus que $n-1$ choix possibles pour $\sigma(2)$, puis $n-2$ choix possibles pour $\sigma(3)$, et ainsi de suite, jusqu'à ce qu'il n'y ait plus qu'un seul choix possible pour $\sigma(n)$.

Au total, il y a donc précisément :

$$n\,(n-1)\,(n-2)\,\cdots\,1 \,=\, n!,$$

permutations possibles de l'ensemble $\{1, \ldots, n\}$. □

Théorème 2.13. *Pour $n \geqslant 1$, le groupe additif (et commutatif) $\mathbb{Z}\big/n\mathbb{Z}$ des entiers modulo n est d'ordre (de cardinal) n.*

Preuve. En effet, on sait bien qu'il y a exactement n entiers distincts modulo n :

$$\mathbb{Z}\big/n\mathbb{Z} \,=\, \big\{0,\ 1,\ \ldots, n-1\big\}\ \mathsf{mod}\, n.$$ □

3. Morphismes et isomorphismes de groupes

Maintenant que les objets à étudier, c'est-à-dire les groupes (abstraits et généraux) ont été définis, il importe de définir les « *flèches* » (ou applications) entre ces objets, qu'on appelle (de manière pédante ?) « *morphismes* ». Évidemment, de telles applications n'ont d'intérêt que si elles respectent les structures algébriques respectives.

Définition 3.1. Une application $f\colon G \longrightarrow G'$ entre deux groupes $(G, *)$ et $(G', *')$ est un *morphisme de groupes* si, pour tous $x, y \in G$, on a :

$$f\big(x * y\big) \,=\, f(x) *' f(y).$$

Attention ! Si on décide de ranger le téléscope et de ne plus voir les étoiles, ce qui conduit à écrire :

$$f(x\,y) \,=\, f(x)\,f(y) \qquad (\forall\ x, y \in G),$$

il faut toutefois bien garder à l'esprit que les lois de groupes à gauche et à droite de cette égalité sont en général *différentes*.

Proposition 3.2. *La composition de deux morphismes de groupes :*

$$G \xrightarrow{f} G' \xrightarrow{f'} G'', \qquad f' \circ f =: f''$$

est encore un morphisme de groupes $f'' : G \longrightarrow G''$.

Preuve. Pour tous $x, y \in G$, on vérifie en effet aisément que :

$$\begin{aligned} f''\big(x\,y\big) &= f'\big(f(x\,y)\big) \\ &= f'\big(f(x)\big)\, f''\big(f(y)\big) \\ &= f''(x)\, f''(y). \end{aligned}$$

□

Par exemple, pour un groupe G quelconque, et pour un élément quelconque $x \in G$ choisi fixé, l'appplication ci-après :

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ m & \longmapsto & x^m \end{array}$$

que nous retrouverons maintes fois sur notre belle route, *est* un morphisme du groupe $\big(\mathbb{Z}, +\big)$ dans le groupe G — *mais pourquoi ?* Parce que nous avons déjà vu dans l'équation (2.8) que $x^m\, x^n = x^{m+n} = x^n\, x^m$, pour tous entiers $m, n \in \mathbb{Z}$.

Les applications concrètes et connues (dans l'Essonne) qui suivent :

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ a & \longmapsto & 91\,a, \end{array} \qquad \begin{array}{ccc} \mathbb{R}^* & \longrightarrow & \mathbb{R}^* \\ x & \longmapsto & x^3, \end{array} \qquad \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}_+^* \\ x & \longmapsto & \mathsf{exp}\,(x), \end{array} \qquad \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \mathsf{log}\,(x), \end{array}$$

sont aussi des morphismes de groupes. L'Exercice 1 montre un autre exemple et exhibe un contre-exemple.

Proposition 3.3. *Soit* $f : G \longrightarrow G'$ *un morphisme de groupes. Alors :*

(1) *on a* $f(1_G) = 1_{G'}$ *;*

(2) *pour tout* $x \in G$*, on a* $f(x^{-1}) = f(x)^{-1}$.

Démonstration. **(1)** En effet, on a :

$$f(1_G) \;=\; f\big(1_G\, 1_G\big) \;=\; f(1_G)\, f(1_G),$$

et une mutiplication par l'inverse $f(1_G)^{-1}$:

$$f(1_G)^{-1} \Big(\; f(1_G) \;=\; f(1_G)\, f(1_G) \;\Big) \qquad \text{donne} \qquad 1_{G'} \;=\; f(1_G).$$

(2) Ensuite, on a :

$$f(x)\, f(x^{-1}) \;=\; f\big(x\, x^{-1}\big) \;=\; f(1_G) \;=\; 1_{G'},$$

et de manière similaire :

$$f(x^{-1})\, f(x) \;=\; f\big(x^{-1}\, x\big) \;=\; f(1_G) \;=\; 1_{G'},$$

ce qui montre bien, en relisant l'Axiome **(A3)**, que $f(x^{-1})$ est l'inverse de $f(x)$, □

Terminologie 3.4. • Un *isomorphisme* de groupes est un morphisme *bijectif*.

• Deux groupes G et G' sont dits *isomorphes* lorsqu'il existe (au moins) un isomorphisme de groupes $f\colon G \longrightarrow G'$. On écrit cela $G \cong G'$.

• Un *automorphisme* d'un groupe G est un isomorphisme de groupes de G sur lui-même. L'ensemble des automorphismes de G est noté $\mathsf{Aut}(G)$.

Évidemment, pour tout groupe G, l'application identité $\mathsf{Id}\colon G \longrightarrow G$ qui, à $x \in G$, associe x, est un isomorphisme. On a donc $G \cong G$ pour tout groupe G.

Proposition 3.5. *Si $f\colon G \longrightarrow G'$ est un isomorphisme, alors la bijection réciproque :*

$$G \longleftarrow G' \quad : f^{-1},$$

est aussi un isomorphisme de groupes.

Démonstration. Il s'agit de vérifier que f^{-1}, qui est d'office bijective, est un morphisme. Pour $x', y' \in G'$ quelconques, le fait que f soit un morphisme donne :

$$f\Big(f^{-1}(x')\, f^{-1}(y')\Big) \;=\; f\big(f^{-1}(x')\big)\; f\big(f^{-1}(y')\big) \;=\; x'\, y'.$$

En appliquant $f^{-1}(\bullet)$ à cela :

$$f^{-1}\left(\; f\Big(f^{-1}(x')\, f^{-1}(y')\Big) \;=\; x'\, y' \;\right),$$

on obtient l'égalité qui prouve que f^{-1} est bien un morphisme :

$$f^{-1}(x')\, f^{-1}(y') \;=\; f^{-1}\big(x'\, y'\big). \qquad \square$$

En conséquence, $G \cong G'$ équivaut à $G' \cong G$: être isomorphe est une relation binaire *symétrique*.

Proposition 3.6. *Dans l'univers des groupes, la relation « être isomorphe à » est une relation d'équivalence.*

Preuve. Il reste à vérifier la transitivité, qui est claire, car « *être bijectif* » est transitif, et nous avons déjà vu dans la Proposition 3.2 qu'une composition de morphismes redonne un morphisme. $\square$

Corollaire 3.7. *L'ensemble* $\mathsf{Aut}\,(G)$ *des automorphismes d'un groupe G est un* groupe *pour la loi de composition des applications.* $\square$

On vérifie (exercice) que les applications vues plus haut :

$$\begin{array}{ccc} \mathbb{R}^* & \longrightarrow & \mathbb{R}^* \\ x & \longmapsto & x^3, \end{array} \qquad \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}_+^* \\ x & \longmapsto & \mathsf{exp}\,(x), \end{array} \qquad \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \mathsf{log}\,(x), \end{array}$$

sont des isomorphismes de groupes.

Autre exemple : si E est un $\mathbb{R}$-espace vectoriel de dimension finie $n \geqslant 1$, le choix d'une base $\boldsymbol{B} = \{e_1, \ldots, e_n\}$ de E induit un isomorphisme de groupes :

$$\begin{array}{ccc} \mathsf{GL}(E) & \xrightarrow{\sim} & \mathsf{GL}_n(\mathbb{R}) \\ u & \longmapsto & \mathsf{Mat}_{\boldsymbol{B}}\, u. \end{array}$$

Alors, est-ce qu'il en existe *toujours*, des isomorphismes ? Autres que l'identité, et pour des groupes abstraits quelconques ?

4. Automorphismes intérieurs et sous-groupes conjugués

L'énoncé suivant fournit toute une famille, paramétrée par G lui-même, d'automorphismes de groupes.

Proposition 4.1. *Dans un groupe arbitraire G, pour tout élément fixé $g \in G$, l'application :*

$$\begin{array}{rccc} \mathsf{Int}_g\colon & G & \longrightarrow & G \\ & x & \longmapsto & g\,x\,g^{-1} \end{array}$$

est un automorphisme de G, c'est-à-dire un morphisme bijectif de G dans lui-même.

On dit alors que Int_g est un *automorphisme intérieur* de G dans lui-même.

Démonstration. Pour tous $x, y \in G$, on calcule en effet :

$$\begin{aligned} \mathsf{Int}_g\,(x\,y) &= g\,x\,y\,g^{-1} \\ &= g\,x\,g^{-1}\ g\,y\,g^{-1} \\ &= \mathsf{Int}_g(x)\ \mathsf{Int}_g(y), \end{aligned}$$

ce qui montre que $\mathsf{Int}_g(\bullet)$ est bien un morphisme du groupe G dans lui-même.

Est-il bijectif ? Oui, car l'application $\mathsf{Int}_{g^{-1}}(\bullet)$ associée à l'élément *inverse* g^{-1} satisfait, pour tout $x \in G$:

$$\begin{aligned} \mathsf{Int}_{g^{-1}}\Big(\mathsf{Int}_g(x)\Big) &= \mathsf{Int}_{g^{-1}}\big(g\,x\,g^{-1}\big) \\ &= \underline{g^{-1}\,g}_{\circ}\ x\ \underline{g^{-1}(g^{-1})^{-1}}_{\circ} \\ &= x, \end{aligned}$$

ainsi que, de manière analogue, $\mathsf{Int}_g \circ \mathsf{Int}_{g^{-1}} = \mathsf{Id}$. En conclusion, $\mathsf{Int}_{g^{-1}}(\bullet)$ est le morphisme inverse de $\mathsf{Int}_g(\bullet)$. □

Cette démonstration suggère alors un énoncé situé à un niveau supérieur d'abstraction.

Proposition 4.2. *L'application :*

$$\begin{array}{rccc} \mathsf{Int}\colon & G & \longrightarrow & \mathsf{Aut}(G) \\ & g & \longmapsto & \mathsf{Int}_g \end{array}$$

est un morphisme de groupes.

Telle quelle et toute nue, cette proposition n'est ni assez claire, ni assez explicite, car rappelons que les lois de groupes doivent en principe être écrites :

$$\begin{array}{rccc} \mathsf{Int}\colon & (G,*) & \longrightarrow & \big(\mathsf{Aut}(G),\circ\big) \\ & g & \longmapsto & \mathsf{Int}_g, \end{array}$$

et même davantage, l'information véritable est donnée par le diagramme complet :

$$\begin{array}{rccc} \mathsf{Int}\colon & (G,*) & \longrightarrow & \big(\mathsf{Aut}(G),\circ\big) \\ & g & \longmapsto & \mathsf{Int}_g\colon \quad G \longrightarrow G \\ & & & \qquad\quad x \longmapsto g\,x\,g^{-1}. \end{array}$$

Démonstration. Il s'agit simplement de vérifier que l'on a bien, pour tous $g, g' \in G$:

$$\mathsf{Int}\big(g * g'\big) \stackrel{?}{=} \mathsf{Int}_g \circ \mathsf{Int}_{g'},$$

ce que l'on effectue en tout $x \in G$ comme suit :

$$\begin{aligned}
\mathsf{Int}_{g\,g'}(x) &= g\,g'\;x\;\big(g\,g'\big)^{-1} \\
&= g\,g'\;x\;g'^{-1}\,g^{-1} \\
&= g\;\mathsf{Int}_{g'}(x)\;g^{-1} \\
&= \mathsf{Int}_g\big(\mathsf{Int}_{g'}(x)\big).
\end{aligned}$$

□

En particulier, grâce à la Proposition 3.3, on a :

$$\begin{aligned}
\mathsf{Int}_{1_G} &= \mathsf{Id}, \\
\big(\mathsf{Int}_g\big)^{-1} &= \mathsf{Int}_{g^{-1}},
\end{aligned}$$

ce qu'on vient d'ailleurs de voir et d'utiliser à la fin de la démonstration de la Proposition 4.1.

Définition 4.3. Un *automorphisme intérieur* d'un groupe G est un automorphisme de la forme $\mathsf{Int}_g(\bullet)$, pour un élément $g \in G$.

D'après ce qui précède, et en anticipant un peut la prochaine Section **5** consacrée aux sous-groupes d'un groupe, la collection des automorphismes intérieurs :

$$\mathsf{Aut}_{\mathsf{Int}}(G) \;\subset\; \mathsf{Aut}(G),$$

forme un *sous-groupe* du groupe complet des automorphismes.

Notation 4.4. Si $P \subset G$ est un sous-ensemble de G, pour tout $g \in G$, on note l'image de P par $\mathsf{Int}_{g^{-1}}(\bullet)$ comme suit :

$$\begin{aligned}
g\,P\,g^{-1} &:= \mathsf{Int}_g(P) \\
&= \big\{g\,x\,g^{-1} \colon\; x \in P\big\}.
\end{aligned}$$

Comme $\mathsf{Int}_g(\bullet)$ est un automorphisme (donc une bijection), cet ensemble $g\,P\,g^{-1}$ est fini si et seulement si P est fini, avec égalité des cardinaux :

$$\big|g\,P\,g^{-1}\big| \;=\; |P|,$$

cela, pour tout $g \in G$.

Définition 4.5. • Deux sous-ensembles $P, P' \subset G$ sont dits *conjugués* lorsqu'il existe $g \in G$ tel que :

$$g\,P\,g^{-1} \;=\; P'.$$

• Deux éléments $x, x' \in G$ sont dits *conjugués* s'il existe $g \in G$, non nécessairement unique, tel que :

$$g\,x\,g^{-1} \;=\; x'.$$

• La *classe de conjugaison dans* G d'un élément $x \in G$ est la collection de tous les éléments qui lui sont conjugués :

$$\mathsf{Conj}_G(x) \;:=\; \big\{g\,x\,g^{-1} \colon\; g \in G\big\}.$$

Proposition 4.6. *La relation « être conjugué dans G » :*

$$x \sim y \qquad \Longleftrightarrow \qquad \Big(\exists\, g \in G, \quad g\,x\,g^{-1} = y \Big),$$

est une relation d'équivalence, dont les classes d'équivalence sont les classes de conjugaison $\mathsf{Conj}_G(x)$*, lorsque* $x \in G$ *varie.*

Démonstration. La réflexivité $x \sim x$ est claire, car $1_G\,x\,1_G^{-1} = x$.

La symétrie est claire aussi, car :

$$\begin{aligned} g^{-1}\,\big(\, g\,x\,g^{-1} = y \,\big)\,g \qquad &\Longrightarrow \qquad \underline{g^{-1}\,g}_{\circ}\; x\; \underline{g^{-1}\,g}_{\circ} = g^{-1}\,y\,g \\ &\Longleftrightarrow \qquad\quad x = g^{-1}\,y\,g. \end{aligned}$$

Enfin, la transitivité est tout aussi '*peanuts*' :

$$\begin{aligned} \Big(g\,x\,g^{-1} = y \quad \text{et} \quad h\,y\,h^{-1} = z \Big) \qquad &\Longrightarrow \qquad h\,g\;x\;g^{-1}\,h^{-1} = z \\ &\Longleftrightarrow \qquad (h\,g)\,x\,\big(h\,g\big)^{-1} = z. \quad \square \end{aligned}$$

Par exemple trivial, un élément $x \in G$ qui commute avec *tous* les éléments $g \in G$:

$$g\,x = x\,g \qquad (\forall\, g \in G),$$

ce qui équivaut à :

$$g\,x\,g^{-1} = g \qquad (\forall\, g \in G),$$

a une classe de conjugaison réduite à lui-même en tant que singleton solitaire :

$$\mathsf{Conj}_G(x) = \big\{ g\,x\,g^{-1} \big\} = \{x\}.$$

Donc dans un groupe *commutatif*, on a :

$$\mathsf{Conj}_G(x) = \{x\} \qquad (\forall\, g \in G).$$

Déterminer toutes les classes de conjugaison d'un groupe est une question importante en théorie des groupes, mais difficile à résoudre. Par exemple, pour le groupe $G := \mathsf{GL}_n(\mathbb{C})$ des matrices inversibles de taille $n \times n$ à coefficients complexes, cela revient à savoir décider si deux matrices données M et N sont ou ne sont pas *semblables*, au sens où il existe une *matrice de passage* inversible P telle que :

$$P^{-1} \cdot M \cdot P \overset{?}{=} N.$$

Autrement dit, cela revient à savoir si deux matrices données correspondent à la *même application linéaire*, à un changement de base près. C'est donc un problème absolument fondamental.

Or dans un cours d'Algèbre Linéaire de niveau Licence 2 ou 3, on expose la théorie de Jordan de la réduction des matrices, à coefficients complexes, puis réels, et qui n'est pas une théorie que l'on peut comprendre complètement en seulement quelques heures. Pour d'autres groupes, la détermination exacte et complète des classes de conjugaison peut devenir une activité d'escalade [2], exposée au danger, de décrocher avant d'avoir achevé l'ascension.

2. Il est de notoriété publique que l'Alpinisme « ne sert à rien », sinon, peut-être, au bien-être psychique de ses pratiquants. Les alpinistes ? On les appelle « *Conquérants de l'Inutile* ». Irions-nous jusqu'à en dire autant des mathématiciens ?

Il y a quand même quelques groupes pour lesquels ce problème peut être résolu complètement, et relativement facilement. C'est le cas du groupe symétrique, comme nous l'exposerons dans une section ultérieure, ou dans le cas du groupe alterné, avec un peu plus d'efforts.

Il y a aussi des cas où il est possible de déterminer facilement les classes de conjugaison de certains éléments, ce qui peut grandement aider dans l'étude d'un groupe donné, comme nous le verrons et le comprendrons, au fur et à mesure de notre progression.

5. Sous-groupes $H \subset G$ d'un groupe G

Introduisons maintenant la notion générale de sous-groupe, déjà implicitement vue[3] dans le chapitre consacré à l'arithmétique sur $\mathbb{Z}$. Ce sera l'occasion pour nous d'en fournir quelques exemples, et de réaliser que les morphismes de groupes « fabriquent gratuitement » de nombreux sous-groupes.

Définition 5.1. Un *sous-groupe* $H \subset G$ d'un groupe G est un sous-ensemble de G vérifiant les propriétés suivantes.

(1) $1_G \in H$.

(2) $x\,y \in H$, pour tous $x, y \in H$.

(3) $x^{-1} \in H$, pour tout $x \in H$.

Évidemment, la multiplication et l'inversion sont celles de G. La logique tautologique — et spleenétique[4] — montre alors qu'avec :

$$*_H := *_G \text{ restreinte à } H,$$
$$1_H := 1_G,$$

l'ensemble $\big(H, *_H\big)$ est un groupe *en lui-même*, au sens de la Définition 2.1 originelle.

Clairement, $\{1_G\}$ et G sont des sous-groupes de G — encore une observation idiote et insipide !

Terminologie 5.2. Un sous-groupe $H \subset G$ d'un groupe G sera dit *trivial* lorsque $H = \{1_G\}$, *strict*[5] si $H \neq G$, et *propre*[6] lorsque :

$$\{1_G\} \subsetneq H \subsetneq G.$$

3. La réminiscence (en grec, anamnésis ; également traduit par ressouvenir) est, dans la pensée de Platon, l'éveil par l'âme des possibilités latentes qu'elle porte en elle-même. L'acquisition de la connaissance doit alors débuter par une re-connaissance.

Cette théorie affirme que notre connaissance de la vérité est le souvenir d'un état ancien où, avant d'être incarnée dans un corps, notre âme vivait au contact immédiat des pures *Idées*, dans le *Monde intelligible*. Ainsi, pour Platon, connaître c'est se souvenir, se remémorer. Chercher et apprendre sont un seul et même acte.

> Ainsi, immortelle, et maintes fois renaissante, l'âme a tout vu, tant ici-bas que dans l'Hadès, et il n'est rien qu'elle n'ait appris ; aussi n'y a-t-il rien d'étonnant à ce que, sur la vertu et sur le reste, elle soit capable de se ressouvenir de ce qu'elle a su antérieurement. Platon, Ménon, 81 b.

Si l'âme détient toutes les vérités, il y a cependant une méthode pour la faire accoucher, pour la faire se remémorer : c'est là qu'intervient la *maïeutique*, la méthode de questionnement socratique, afin de faire se rappeler l'âme.

4. Qui inspire le *spleen*, la mélancolie, l'ennui, le vague à l'âme.

5. En mathématiques, la notion de sous-groupe « *très strict* » n'existe pas — mais celle de professeur, *si !*

6. Pareil : « *sale* » n'est pas mathématique !

Souvent, pour montrer qu'un ensemble muni d'une loi de composition est un groupe, il est plus facile de montrer que c'est un sous-groupe d'un groupe connu, car on s'épargne alors d'avoir à vérifier que l'associativité est satisfaite. En outre, une petite propositionette permet (parfois) de raccourcir encore un peu les calculs ou les raisonnements.

Proposition 5.3. *Pour un sous-ensemble* non vide $H \subset G$ *d'un groupe* G*, on a équivalence entre :*

(i) H *est un sous-groupe de* G*;*

(ii) $x\,y^{-1} \in H$*, pour tous* $x, y \in H$*.*

Démonstration. **(i)** $\Longrightarrow$ **(ii)** est clair.

(ii) $\Longrightarrow$ **(i)**. Il s'agit d'obtenir **(1)**, **(2)**, **(3)** de la Définition 5.1 Puisque H est non vide, il y a un élément $h \in H$. Alors $h\,h^{-1} \in H$ grâce à **(ii)**, c'est-à-dire $1_G \in H$.

Ensuite, pour tout $x \in H$, il vient grâce à **(ii)** :

$$x^{-1} \;=\; 1_G\,x^{-1} \;\in\; H.$$

Enfin, pour $x, y \in H$ quelconques, puisque nous venons d'obtenir $y^{-1} \in H$, il vient grâce à **(ii)** :

$$x\,y \;=\; x\left(y^{-1}\right)^{-1} \;\in\; H. \qquad \square$$

Il se peut fort bien qu'un groupe G n'ait aucun sous-groupe propre, comme c'est le cas (exercice) de $G = \{\pm 1\}$.

L'ensemble des fonctions continues $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ est un sous-groupe propre du groupe des fonctions quelconques $f\colon \mathbb{R} \longrightarrow \mathbb{R}$, pour l'opération interne d'addition des fonctions.

Troisième exemple : l'ensemble des matrices triangulaires supérieures inversibles dans le groupe de toutes les matrices inversibles, c'est-à-dire l'ensemble des matrices :

$$A \;:=\; \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n-1} & a_{1,n} \\ \mathbf{0} & a_{2,2} & a_{2,3} & \cdots & a_{2,n-1} & a_{2,n} \\ \mathbf{0} & \mathbf{0} & a_{3,3} & \cdots & a_{3,n-1} & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & a_{n,n-1} & a_{n,n} \end{pmatrix},$$

dont tous les termes diagonaux sont non nuls :

$$0 \;\neq\; a_{1,1} \cdot a_{2,2} \cdot a_{3,3} \cdots a_{n-1,n-1} \cdot a_{n,n},$$

est un *sous-groupe* de $\mathsf{GL}_n(\mathbb{R})$, car on sait (ou on révise !) que la matrice *inverse* A^{-1} d'une matrice triangulaire supérieure A est encore triangulaire supérieure, et on sait (ou on re-révise !) que la matrice *produit* $A \cdot B$ de deux matrices triangulaires supérieures A et B est encore et toujours triangulaire supérieure.

Proposition 5.4. *Si* $H \subset G$ *est un sous-groupe de* G *et si* $K \subset H$ *est un sous-groupe de* H*, alors* $K \subset G$ *est un sous-groupe de* G*.*

Preuve. Laissée au lecteur désœuvré, glaneur d'arguments ailés et faciles, perdu dans la poudrée lumineuse du groupe G_{547} de comètes fabuleuses [7]. $\square$

7. « Accès de lyrisme fantaisiste », inspiré par le fait que la détermination de *tous* les sous-groupes d'un groupe donné est l'un des problèmes mathématiques les plus difficiles et les plus complexes qui puisse être donné à résoudre.

Proposition 5.5. *Si $H_1 \subset G_1$ est un sous-groupe d'un groupe G_1, et si $H_2 \subset G_2$ est un sous-groupe d'un groupe G_2, alors :*

$$H_1 \times H_2 \text{ est un sous-groupe de } G_1 \times G_2.$$

Preuve. En effet, servons-nous aussitôt du critère énoncé par la Proposition 5.3 :

$$\big(x_1,\, x_2\big) \,*\, \big(y_1,\, y_2\big)^{-1} \;=\; \Big(\underbrace{x_1\, y_1^{-1}}_{\in\, H_1},\; \underbrace{x_2\, y_2^{-1}}_{\in\, H_2}\Big). \qquad \square$$

Décrire tous les sous-groupes, à conjugaison près, d'un groupe donné, est un problème mathématique qui peut se révéler extrêmement ardu. Heureusement, pour les objets de base que nous considérons dans ce cours, tels que le groupe $(\mathbb{Z}, +)$, des descriptions complètes sont accessibles.

Théorème 5.6. *Les sous-groupes de $\big(\mathbb{Z}, +\big)$ sont tous de la forme :*

$$n\,\mathbb{Z} \;=\; \big\{n\,k\colon\;\; k \in \mathbb{Z} \text{ quelconque}\big\},$$

pour un entier $n \in \mathbb{Z}$ fixé.

Plus précisément, si $H \subset \mathbb{Z}$ est un sous-groupe de $\big(\mathbb{Z}, +\big)$ non réduit au singleton $\{0\}$, alors $H = n\,\mathbb{Z}$, avec l'entier :

$$n \;:=\; \mathsf{min}\,\big\{m \in H\colon\;\; m \geqslant 1\big\}.$$

Démonstration. Supposons tout d'abord que $H = n\,\mathbb{Z}$, avec $n \in \mathbb{Z}$ fixé. Clairement, $H \neq \emptyset$ — ce qui est demandé dans la Définition 5.1 d'un sous-groupe —, puisqu'alors $n\,0 = 0 \in H$. Ensuite, le critère de la Proposition 5.3 :

$$\Big(\; n\,k \,\in\, H \quad \text{et} \quad n\,\ell \,\in\, H \;\Big) \qquad\qquad \Longrightarrow \qquad\qquad n\,k + \big(-\,n\,\ell\big) \;=\; n\,(k-\ell) \;\in\; H,$$

est satisfait. Donc $H = n\,\mathbb{Z}$ est bien un sous-groupe de $\big(\mathbb{Z}, +\big)$.

Mais alors, pourquoi tous *les sous-groupes de $\big(\mathbb{Z}, +\big)$ sont-ils de cette forme ?*

Prenons un sous-groupe arbitraire $H \subset \mathbb{Z}$. Si $H = \{0\}$, rien à faire. Supposons donc que H contient au moins un élément $h \in \mathbb{Z}\backslash\{0\}$ non nul. Rappelons que 0 est l'élément neutre du groupe $\big(\mathbb{Z}, +\big)$, et que l'inverse de h, pour la loi de groupe $+$, est l'opposé $-\,h$, qui doit aussi appartenir à H.

Ou bien h, ou bien $-\,h$ est un entier > 0. Ainsi, l'ensemble suivant est *non vide :*

$$\big\{h \in H\colon\;\; h \geqslant 1\big\} \;\subset\; \mathbb{N}.$$

Or un théorème fondamental de l'arithmétique sur $\mathbb{Z}$ garantit que tout sous-ensemble non vide *minoré* de $\mathbb{N}$ contient un plus petit élément. Soit donc :

$$n \;:=\; \mathsf{min}\,\big\{h \in H\colon\;\; h \geqslant 1\big\}.$$

Ensuite, puisque $n \in H$ et puisque H est un sous-groupe de $\big(\mathbb{Z}, +\big)$, les éléments :

$$\ldots, \quad -n-n-n, \quad -n-n, \quad -n, \quad 0, \quad n, \quad n+n, \quad n+n+n, \quad \ldots,$$

c'est-à-dire généralement pour tout $k \in \mathbb{Z}$, les éléments $n\,k \in H$, appartiennent alors *aussi* à H. On a donc prouvé l'inclusion :

$$n\,\mathbb{Z} \;\subset\; H.$$

Pour atteindre l'inclusion inverse, prenons un élément arbitraire $a \in H$. Comme $a \in \mathbb{Z}$, nous pouvons l'euclidiviser — néologisme heureux — par n :

$$a \,=\, q\,n + r,$$

avec $q \in \mathbb{Z}$ et avec un reste $0 \leqslant r \leqslant n-1$. Mais comme $a \in H$, comme $q\,n \in H$, et comme H est un sous-groupe, cela force :

$$H \;\ni\; a - q\,n \;=\; r,$$

le reste $r \in H$ à appartenir *aussi* à H.

Si l'on avait $1 \leqslant r \leqslant n-1$, cela contredirait le choix de n *minimal* dans $\big\{m \in H\colon\; m \geqslant 1\big\}$. Donc $r = 0$ obligatoirement, et enfin :

$$a \,=\, n\,q \;\in\; n\,\mathbb{Z},$$

et comme $a \in H$ était arbitraire, ceci établit l'inclusion inverse $H \subset n\,\mathbb{Z}$.

En conclusion, on a bien démontré que $H = n\,\mathbb{Z}$. □

6. Noyau Ker f et image Im f d'un morphisme de groupes

La proposition suivante est fréquemment utilisée pour construire de nouveaux sous-groupes. Rappelons que pour toute application, pas nécessairement bijective, $f\colon E \longrightarrow F$ entre deux ensembles, et pour tout sous-ensemble $Q \subset F$, l'*image réciproque* de Q par f est le sous-ensemble de E défini comme :

$$f^{-1}(Q) \,:=\, \big\{x \in E\colon\; f(x) \in Q\big\}.$$

Proposition 6.1. *Soit un morphisme de groupes $f\colon G \longrightarrow G'$.*

(1) *Si H est un sous-groupe de G, alors l'image $f(H) =: H'$ est* aussi *un sous-groupe de G'.*

(2) *Si H' est un sous-groupe de G', alors l'image réciproque $f^{-1}(H')$ est* aussi *un sous-groupe de G.*

Démonstration. **(1)** Soit donc $H \subset G$ un sous-groupe, et soit son image :

$$f(H) \,=\, \big\{f(h)\colon\; h \in H\big\},$$

Puisque H est non vide, $f(H)$ l'est aussi. Ensuite, prenons $x, y \in H$ quelconques, d'où $x\,y^{-1} \in H$, utilisons le fait que f est un morphisme, et constatons :

$$f(x)\,f(y)^{-1} \,=\, f(x)\,f(y^{-1}) \,=\, f\big(x\,y^{-1}\big),$$

que $f(x)\,f(y)^{-1}$ appartient à l'image $f(H)$, puisque c'est $f(x\,y^{-1})$.

Autrement dit, pour deux éléments quelconques $x' := f(x)$ et $y' := f(y)$ de $f(H)$, on a obtenu que $f(x)\,f(y)^{-1} \in H$ aussi, donc le critère de la Proposition 5.3 s'applique, et ainsi, $f(H) =: H'$ est bien un sous-groups de G'.

(2) Si maintenant H' est un sous-groupe de G', soit son image inverse :

$$f^{-1}(H') \,=\, \big\{x \in G\colon\; f(x) \in H'\big\}.$$

Puisque $f(1_G) = 1_{G'}$, on a $1_G \in f^{-1}(H')$. En particulier, $f^{-1}(H')$ n'est pas vide.

Soient maintenant $x, y \in f^{-1}(H')$ quelconques. Alors comme $f(x) \in H'$, comme $f(y) \in H'$, et comme H' est un sous-groupe, il vient :

$$H' \;\ni\; f(x)\,f(y)^{-1} \,=\, f\big(x\,y^{-1}\big),$$

ce qui montre que $x\,y^{-1} \in f^{-1}(H')$. En conclusion, H' est bien un sous-groupe de G'. □

Définition 6.2. Soit $f\colon G \longrightarrow G'$ un morphisme de groupes.

• Le *noyau* de f est le sous-groupe de G noté :

$$\begin{aligned}\mathsf{Ker}\, f \;&:=\; \big\{x \in G\colon\;\; f(x) = 1_{G'}\big\}\\ &=\; f^{-1}\big(1_{G'}\big).\end{aligned}$$

• L'*image* de f est le sous-groupe de G' noté :

$$\begin{aligned}\mathsf{Im}\, f \;&:=\; \big\{f(x)\colon\;\; x \in G\big\}\\ &=\; f(G).\end{aligned}$$

Un corollaire immédiat de la Proposition 6.1 est en effet la

Proposition 6.3. *Le noyau* $\mathsf{Ker}\, f = f^{-1}(1_{G'})$ *et l'image* $\mathsf{Im}\, f = f(G)$ *d'un morphisme de groupes* $f\colon G \longrightarrow G'$ *sont toujours des sous-groupes de* G *et de* G'. □

La proposition suivante donne une propriété très utile des morphismes de groupes.

Proposition 6.4. *Soit* $f\colon G \longrightarrow G'$ *un morphisme de groupes. Alors* f *est injectif si et seulement si* $\mathsf{Ker}\, f = \{1_G\}$.

Démonstration. Supposons f injectif, et soit $x \in \mathsf{Ker}\, f$, c'est-à-dire :

$$f(x) \;=\; 1_{G'} \;=\; f(1_G).$$

Grâce à l'injectivité de f, il vient $x = 1_G$. Ainsi, $\mathsf{Ker}\, f = \{1_G\}$.

Inversement, supposons que $\mathsf{Ker}\, f = \{1_G\}$, et soient $x, y \in G$ tels que $f(x) = f(y)$. Alors $f(x)\,f(y)^{-1} = f\big(x\,y^{-1}\big) = 1_{G'}$, et donc $x\,y^{-1} \in \mathsf{Ker}\, f$. Par hypothèse on $x\,y^{-1} = 1_G$, c'est-à-dire $x = y$. Ainsi, f est injectif. □

Nous allons maintenant définir une classe importante de sous-groupes.

Définition 6.5. Soit G un groupe, et soit H un sous-groupe. On dit que H est *distingué dans* G s'il satisfait :

$$g\,h\,g^{-1} \;\in\; H, \qquad\qquad \text{pour tout } h \;\in\; H, \quad \text{et tout } g \;\in\; G,$$

c'est-à-dire si :

$$g\,H\,g^{-1} \;=\; H.$$

Autrement dit, un sous-groupe $H \subset G$ est distingué dans G s'il est stable par tout automorphisme intérieur de G :

$$\mathsf{Int}_g(H) \;=\; H \qquad\qquad (\forall\; g \in G).$$

On note cela :

$$H \triangleleft G.$$

Observation 6.6. *Soit* G *un groupe arbitraire.*

(1) *Si* G *est commutatif, tout sous-groupe* $H \subset G$ *est distingué dans* G.

(2) *Les sous-groupes* $\{1_G\}$ *et* G *sont toujours distingués dans* G.

Preuve. **(1)** Par commutativité, $g\,h\,g^{-1} = g\,g^{-1}\,h = h$ appartient trivialement à H, pour tout $h \in H$ et tout $g \in G$.

(2) Cela découle immédiatement de la Définition 6.5. □

Comme nous le verrons plus tard, les sous-groupes distingués interviendront de façon naturelle dans la construction des groupes quotients.

Définition 6.7. Le *centre* $Z(G)$ d'un groupe G est l'ensemble des éléments qui commutent avec *tous* les éléments de G :

$$Z(G) := \big\{z \in G\colon\ z\,g = g\,z,\ \text{ pour tout } g \in G\big\}.$$

Clairement, on a $Z(G) = G$ si et seulement si G est commutatif.

Observation 6.8. *Le centre $Z(G)$ d'un groupe est toujours un sous-groupe commutatif de G qui est de plus distingué dans G.*

Preuve. En effet, pour tous $z, z' \in Z(G)$, on a $z\,z' = z'\,z$, puisque z commute avec tout élément de G, et en particulier, avec tout élément $z' \in Z(G)$.

Ensuite, pour tout $g \in G$, la distinction de $Z(G)$ est facile :

$$\begin{aligned} g\,Z(G)\,g^{-1} &= \big\{g\,z\,g^{-1}\colon\ z \in Z(G)\big\} \\ &= \big\{z\,g\,g^{-1}\colon\ z \in Z(G)\big\} \\ &= \big\{z\colon\ z \in Z(G)\big\} \\ &= Z(G). \end{aligned}$$

□

La proposition suivante fournit toute une famille d'exemples de sous-groupes distingués.

Proposition 6.9. *Soit $f\colon G \longrightarrow G'$ un morphisme de groupes. Alors* $\mathsf{Ker}\, f$ *est toujours un sous-groupe distingué de G.*

Démonstration. Grâce à la Proposition 6.3, on sait déjà que c'est un sous-groupe de G.

Ensuite, comme on a, pour tout $g \in G$ et tout $x \in \mathsf{Ker}\, f$:

$$\begin{aligned} f\big(g\,x\,g^{-1}\big) &= f(g)\,f(x)\,f(g)^{-1} \\ &= f(g)\,1_{G'}\,f(g)^{-1} \\ &= \underline{f(g)\,f(g)^{-1}}_{\circ} \\ &= 1_{G'}, \end{aligned}$$

il est clair que $g\,x\,g^{-1} \in \mathsf{Ker}\, f$ aussi, ce qui montre bien que $g\,\mathsf{Ker} f\,g^{-1} \subset \mathsf{Ker}\, f$, pour tout $g \in G$. □

D'après cette proposition, pour démontrer qu'une partie $P \subset G$ d'un groupe G est un sous-groupe distingué de G, on peut essayer de l'identifier au *noyau* d'un certain morphisme de groupes, à rechercher, à trouver.

Une notion centrale en théorie des groupes est celle de groupe simple. On peut démontrer que les groupes simples sont en quelque sorte les « briques élémentaires » au moyen desquelles tout groupe peut être « construit », ou « reconstitué ».

Définition 6.10. On dit qu'un groupe G est *simple* si $G \neq \{1_G\}$, et si G n'a pas de sous-groupe propre $\{1_G\} \subsetneqq H \subsetneqq G$ qui soit distingué dans G.

Autrement dit, G est simple si $G \neq \{1_G\}$ et si $\{1_G\}$ et G sont les seuls sous-groupes distingués de G. Nous verrons tantôt des exemples de groupes simples.

Classification des groupes finis simples :

Fill ??

7. Sous-groupes engendrés par une partie

En général, la réunion de deux sous-groupes n'est *pas* un sous-groupe. Par exemple, voici deux sous-groupes du groupe produit $(\mathbb{R},+)\times(\mathbb{R},+)$:

$$H_1 := \big\{(x,0)\colon\ x\in\mathbb{R}\big\} \qquad \text{et} \qquad H_2 := \big\{(0,y)\colon\ y\in\mathbb{R}\big\},$$

dont la réunion $H_1\cup H_2$ n'est *pas* un sous-groupe de $(\mathbb{R},+)\times(\mathbb{R},+)$, car l'addition — qui est la loi de groupe — de deux éléments :

$$(x,0)+(0,y) \;=\; (x,y)$$

ne fournit presque jamais un élément de $H_1\cup H_2$, notamment lorsque $x\neq 0\neq y$.

En revanche, tout se passe bien par intersections quelconques.

Proposition 7.1. *Soit G un groupe, et soit $\big(H_i\big)_{i\in I}$ une famille non vide de sous-groupes de G. Alors l'intersection complète :*

$$H \;:=\; \bigcap_{i\in I} H_i$$

est un sous-groupe de G.

Démonstration. Puisque par définition $1_G\in H_i$ pour tout $i\in I$, il est clair $1_G\in H$. En particulier, H est non vide.

Ensuite, soient deux éléments quelconques $x,y\in H$. Alors $x,y\in H_i$ pour tout $i\in I$. Comme H_i est un sous-groupe, on a $x\,y^{-1}\in H_i$. Ceci était vrai pour tout $i\in I$, l'élément $x\,y^{-1}\in H$ est dans l'intersection.

En conclusion, le critère de la Proposition 5.3 s'applique : H est bien un sous-groupe de G. □

Cette proposition justifie alors le caractère bien fondé de l'objet introduit par la

Définition 7.2. Soit G un groupe et soit $P\subset G$ une partie de G, c'est-à-dire un sous-ensemble (qui peut éventuellement être vide). Le *sous-groupe de G engendré par P*, noté :

$$\langle P\rangle,$$

est le sous-groupe de G qui est l'intersection de *tous* les sous-groupes de G contenant P.

Faisons observer que cette définition a bien un sens, parce qu'on exécute l'intersection sur une famille de sous-groupes $H\supset P$ qui est *non vide* car elle contient $H=G$. De manière équivalente, $\langle P\rangle$ est le plus petit sous-groupe de G contenant P, au sens de l'inclusion ensembliste.

Proposition 7.3. *Dans un groupe G, les cinq propriétés suivantes sont satisfaites.*

(1) *$P\subset\langle P\rangle$ pour toute partie $P\subset G$.*

(2) *Si une partie $P\subset H$ est contenue dans un sous-groupe $H\subset G$, alors $\langle P\rangle\subset H$.*

(3) *On a $\langle P\rangle = P$ si et seulement si $P=H$ est un sous-groupe $H\subset G$.*

(4) *Si $P\subset Q$ pour deux parties, alors $\langle P\rangle\subset\langle Q\rangle$.*

(5) *$\langle\emptyset\rangle=\{1_G\}$.*

Preuve. Élémentaire, et laissée au lecteur-étudiant. □

Plus intéressant que ces énoncés « purement logiques » et essentiellement « évidents », présentons une description précise de $\langle P\rangle$.

Théorème 7.4. *Soit G un groupe et soit une partie $P \subset G$. Avec :*

$$P^{-1} := \big\{x^{-1} :\ x \in P\big\},$$

le sous-groupe engendré par P est :

$$\langle P\rangle := \Big\{x_1 \cdots x_n :\ n \geqslant 0 \text{ } \textit{entier quelconque},\ x_1, \ldots, x_n \in P \cup P^{-1}\Big\}.$$

Autrement dit, le sous-groupe $\langle P\rangle \subset G$ engendré par une partie P est constitué de *tous* les produits possibles d'éléments de P et de leurs inverses, de longueur finie quelconque et non bornée. De tels produits doivent évidemment appartenir au plus petit sous-groupe contenant P, et donc, on les prend *tous*, « brutalement » ! On calcule dans tous les sens !

Évidemment, si $P = H$ était déjà un sous-groupe de G, tous ces produits resteraient dans H, et on verrait à nouveau que $\langle P\rangle = H$ dans ce petit cas idiot, *cf.* la Proposition 7.3 **(3)**. Le théorème est surtout intéressant quand P n'est *pas* un sous-groupe de G.

Démonstration. Posons :

$$H := \Big\{x_1 \cdots x_n :\ n \geqslant 0 \text{ entier quelconque},\ x_1, \ldots, x_n \in P \cup P^{-1}\Big\}.$$

Implicitement, pour $n = 0$, ce produit vaut 1_G.

Assertion 7.5. *On a $H \subset \langle P\rangle$.*

Preuve. Pour un élément quelconque $x_1 \cdots x_n \in H$, on veut faire voir que $x_1 \cdots x_n \in \langle P\rangle$. Soit un facteur x_i d'indice arbitraire $1 \leqslant i \leqslant n$.

Comme $x_i \in P$ ou $x_i^{-1} \in P$, et comme par définition $P \subset \langle P\rangle$, il vient $x_i \in \langle P\rangle$ ou $x_i^{-1} \in \langle P\rangle$. Comme par définition $\langle P\rangle$ est un sous-groupe de G — minimal contenant P, qui plus est —, et comme tout sous-groupe est stable par inversion, il vient $x_i \in \langle P\rangle$ dans les deux cas, ce, quel que soit $1 \leqslant i \leqslant n$.

Enfin, comme $\langle P\rangle$ est un sous-groupe, le produit satisfait bien $x_1 \cdots x_n \in \langle P\rangle$. □

Assertion 7.6. *On a $\langle P\rangle \subset H$.*

Preuve. Il suffit de montrer que H est un sous-groupe de G contenant P, puisque par définition, $\langle P\rangle$ est le *plus petit* sous-groupe vérifiant cette propriété.

En prenant $n = 0$ dans $x_1 \cdots x_n$, on voit que $1_G \in H$, donc H est non vide. En prenant $n = 1$ et $x_1 \in P$, on voit que $P \subset H$.

D'autre part, si $y \in P \cup P^{-1}$, on a trivialement $y^{-1} \in P \cup P^{-1}$ aussi. Par conséquent, si $x = x_1, \ldots, x_m$ appartient à H et si $y = y_1 \cdots y_p$ appartient aussi à H, on en déduit que :

$$x\, y^{-1} \ = \ x_1 \cdots x_n\, y_1^{-1} \cdots y_p^{-1} \ \in \ H,$$

est encore un produit fini du type H. En application du critère connu, ceci montre bien que H est un sous-groupe de G. □

Par inclusion et inclusion inverse, ces deux assertions concluent bien que $\langle P\rangle = H$. □

Notation 7.7. Si $P = \big\{a_1, \ldots, a_r\big\}$ est une partie *finie*, de cardinal $r \geqslant 1$, le sous-groupe $\langle P\rangle$ engendré par P sera noté :

$$\big\langle a_1, \ldots, a_r\big\rangle.$$

Le cas d'un unique élément $a_1 =: x$ est très-très souvent utilisé, en théorie des groupes. Pourquoi ? Parce que, alors, on voit ré-apparaître l'arithmétique dans la théorie des groupes, c'est-à-dire dans les puissances quelconques x^m avec $m \in \mathbb{Z}$. Plus tard, nous verrons d'ailleurs aussi ré-apparaître les anneaux $\mathbb{Z}\big/n\mathbb{Z}$ dans la théorie des troupes [8].

Proposition 7.8. *Soit G un groupe et soit $x \in G$. Alors :*

$$\langle\, x \,\rangle \;=\; \big\{ x^m \colon\; m \in \mathbb{Z} \big\}.$$

Démonstration. En effet, le théorème précédent nous dit que :

$$\langle\, x \,\rangle \;=\; \big\{ x^{\varepsilon_1} \cdots x^{\varepsilon_n} \colon\; n \geqslant 0,\; \varepsilon_1, \ldots, \varepsilon_n = \pm 1 \big\}.$$

Mais on sait que x et x^{-1} commutent entre eux, simplement parce que $x\, x^{-1} = 1_G = x^{-1}\, x$. Donc grâce à cela, la propriété agréable (2.8) nous donne :

$$x^{\varepsilon_1} \cdots x^{\varepsilon_n} \;=\; x^{\varepsilon_1 + \cdots + \varepsilon_n},$$

et comme :

$$\varepsilon_1 + \cdots + \varepsilon_n \;=:\; m,$$

est un entier — d'ailleurs quelconque —, c'est terminé ! □

Insistons sur le fait que le groupe $\langle\, x \,\rangle$ engendré par un élément unique $x \in G$ est *toujours commutatif*, ce qu'avait déjà exprimé la propriété agréable (2.8), et que nous ré-écrivons ici, parce que nous aimons bien ce qui est agréable :

$$x^m\, x^n \;=\; x^{m+n} \;=\; x^n\, x^m \qquad \text{et} \qquad \big(x^m\big)^n \;=\; x^{mn} \;=\; \big(x^n\big)^m.$$

Proposition 7.9. *Si G est commutatif, alors le sous-groupe engendré par un nombre fini $r \geqslant 1$ d'éléments $a_1, \ldots, a_r \in G$ est :*

$$\big\langle a_1, \ldots, a_r \big\rangle \;=\; \big\{ a_1^{k_1} \cdots a_r^{k_r} \colon\; k_1, \ldots, k_r \in \mathbb{Z} \big\}.$$

Démonstration. La loi de groupe étant classiquement notée avec le symbole $+$ quand G est commutatif, on a par définition :

$$\big\langle a_1, \ldots, a_r \big\rangle \;=\; \Big\{ x_1 + \cdots + x_n \colon\; x_i \in \{a_1, \ldots, a_r\} \cup \{-a_1, \ldots, -a_r\} \Big\},$$

et il suffit, puisque l'ordre des termes est intercheangeable [9] de collecter au début, les x_i qui sont égaux à $\pm a_1$, puis ceux qui sont égaux à $\pm a_2$, *etc.*, d'où :

$$\big\langle a_1, \ldots, a_r \big\rangle \;=\; \big\{ k_1 a_1 + \cdots + k_r a_r \colon\; k_1, \ldots, k_r \in \mathbb{Z} \big\}. \qquad \square$$

Définition 7.10. Soit G un groupe, et soit P une partie de G. On dit que P *engendre* G si $G = \langle P \rangle$. On dit aussi que P est une *partie génératrice*, ou est un *système de générateurs* de G.

Par exemple-facile, P engendre $\langle P \rangle$!

La notion de partie génératrice est très utile pour simplifier les calculs. Supposons par exemple que l'on veuille montrer ou vérifier qu'après avoir introduit deux sous-groupes $H, H' \subset G$, on a $H \subset H'$. Si l'on dispose d'une partie génératrice P de G, il suffit de démontrer que $P \subset H'$.

De même, supposons que H soit un sous-groupe de G, et que H soit engendré par une partie P. Alors pour montrer que H est un sous-groupe distingué de G, il faut et il suffit de

8. — jeu de mots sputide, euh, pardon, stupide ! —

9. — ce que l'utilisation du symbole élémentaire $+$ cherche à signifier intuitivement —

montrer que, pour tout $g \in G$, et pour tout $x \in P$, on a encore $g\,x\,g^{-1} \in H$. L'Exercice 2 propose de vérifier cette affirmation.

Ces « astuces » de calcul seront utilisées dans les raisonnements qui suivront et dans les exercices.

Maintenant, revenons aux sous-groupes additifs de $\mathbb{Z}$, qui sont tous de la forme $n\,\mathbb{Z}$ grâce au Théorème 5.6. On devrait alors pouvoir décrire l'intersection de deux ou plusieurs sous-groupes, ainsi que les sous-groupes engendrés par deux ou plusieurs sous-groupes, simplement en fonction d'un unique entier du type n dans $n\,\mathbb{Z}$ — et tel est bien le cas !

Théorème 7.11. *Soient deux entiers quelconques $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. Alors les deux entiers d et m tels que* [10] *:*

$$\big\langle a,\, b\big\rangle \;=\; a\,\mathbb{Z} + b\,\mathbb{Z} \;=\; d\,\mathbb{Z} \qquad \textit{et} \qquad a\,\mathbb{Z} \cap b\,\mathbb{Z} \;=\; m\,\mathbb{Z},$$

ne sont autres que :

$$d \;=\; \mathsf{pgcd}\,(a, b) \qquad \textit{et} \qquad m \;=\; \mathsf{ppcm}\,(a, b).$$

Démonstration. Montrons que $d = \mathsf{pgcd}\,(a, b)$.

Soit donc d l'unique entier tel que $a\,\mathbb{Z} + b\,\mathbb{Z} = d\,\mathbb{Z}$. Comme $a \in \langle a, b\rangle = d\,\mathbb{Z}$, il est clair que a est un multiple de d. Autrement dit, $d \mid a$. Par symétrie, $d \mid b$ aussi. Donc par définition du plus grand commun multiple, $d \mid \mathsf{pgcd}\,(a, b)$.

Par ailleurs, si $c \in \mathbb{Z}$ vérifie $c \mid a$ et $c \mid b$, il est clair que c divise aussi toute combinaison entière $k\,a + \ell\,b$, c'est-à-dire que c divise tout élément de $a\,\mathbb{Z} + b\,\mathbb{Z} = d\,\mathbb{Z}$. En particulier, c divise $d\,1$, c'est-à-dire $c \mid d$. Avec le choix de $c := \mathsf{pgcd}\,(a, b)$, on trouve $\mathsf{pgcd}\,(a, b) \mid d$. Une comparaison avec ce qui précède montre que l'on a bien $d = \mathsf{pgcd}\,(a, b)$.

Ensuite, montrons que $m = \mathsf{ppcm}\,(a, b)$. Soit donc m l'unique entier tel que :

$$a\,\mathbb{Z} \cap b\,\mathbb{Z} \;=\; m\,\mathbb{Z}.$$

On a $m \in m\,\mathbb{Z} = a\,\mathbb{Z} \cap b\,\mathbb{Z}$, donc $m \in a\,\mathbb{Z}$ ainsi que $m \in b\,\mathbb{Z}$. Par conséquent, m est un multiple de a, et aussi un multiple de b, ce qui montre, par définition du plus petit commun multiple, que $\mathsf{ppcm}\,(a, b) \mid m$.

Par ailleurs, si $c \in \mathbb{Z}$ vérifie $a \mid c$ et $b \mid c$, il vient :

$$c \;\in\; a\,\mathbb{Z} \cap b\,\mathbb{Z} \;=\; m\,\mathbb{Z},$$

et donc $m \mid c$. En prenant $c := \mathsf{ppcm}\,(a, b)$, on trouve $m \mid \mathsf{ppcm}\,(a, b)$. Une comparaison avec ce qui précède montre que l'on a bien $m = \mathsf{ppcm}\,(a, b)$. □

Corollaire 7.12. *Pour deux entiers quelconques $a, b \in \mathbb{Z}$, il existe toujours deux entiers $u, v \in \mathbb{Z}$ tels que :*

$$u\,a + v\,b \;=\; \mathsf{pgcd}\,(a, b).$$ □

Cette proposition et sa démonstration se généralisent à une famille quelconque $(a_i)_{i\in I}$ d'entiers pour donner :

$$\big\langle a_i,\, i \in I\big\rangle \;=\; \mathsf{pgcd}\,\big((a_i)_{i\in I}\big),$$

et pour fournir en paquet-cadeau dans le baril de lessive bézoutique une famille d'entiers $(u_i)_{i\in I}$ presque tous égaux à 0, tels que :

$$\sum_{i\in I} a_i\,u_i \;=\; \mathsf{pgcd}\,\big((a_i)_{i\in I}\big).$$

10. Ici, l'égalité $\langle a, b\rangle = a\,\mathbb{Z} + b\,\mathbb{Z}$ est un simple cas particulier de la Proposition 7.9.

Enfin, si l'on pose, lorsque la famille d'entiers $(a_i)_{i\in I}$ n'est pas bornée :

$$\mathsf{ppcm}\,\big((a_i)_{i\in I}\big) \;:=\; 0,$$

on se convainc (exercice) que l'on a l'égalité générale :

$$\bigcap_{i\in I} a_i\,\mathbb{Z} \;=\; \mathsf{ppcm}\,\big((a_i)_{i\in I}\big).$$

8. Relations d'équivalence

Cette section est constituée de rappels qui seront nécessaires pour aborder des résultats plus avancées de la théorie des groupes.

Soit E un ensemble, c'est-à-dire :

$$E \;=\; \big\{a\colon\; a\in E\big\}.$$

Soit aussi $\boldsymbol{R}$ une *relation binaire*[11] sur E, c'est-à-dire une manière de mettre en relation des *paires* d'éléments $(a,b)\in E\times E$, ce que l'on écrit :

$$a\,\boldsymbol{R}\,b.$$

Sur l'ensemble $E=\mathbb{R}$ des nombres réels, des exemples simples de relations binaires sont $=$, $\leqslant$, $<$. Si l'on écoutait les puristes, il faudrait noter :

$$\bullet\,\boldsymbol{R}\,\bullet,$$

afin de bien signifier la présence de *deux* éléments de part et d'autre de la relation en question.

Définition 8.1. On dit qu'une relation binaire $\boldsymbol{R}$ sur un ensemble E est :

- *réflexive* si $a\,\boldsymbol{R}\,a$, pour tout $a\in E$;
- *symétrique* si $a\,\boldsymbol{R}\,b \iff b\,\boldsymbol{R}\,a$, pour tous $a,b\in E$;
- *transitive* si, pour tous $a,b,c\in E$:

$$\Big(\; a\,\boldsymbol{R}\,b \quad\text{et}\quad b\,\boldsymbol{R}\,c\;\Big) \qquad\Longrightarrow\qquad a\,\boldsymbol{R}\,c.$$

Enfin, une relation binaire $\boldsymbol{R}$ sur un ensemble E est dite être une *relation d'équivalence* lorsqu'elle est réflexive, symétrique, transitive[12].

Clairement, la relation d'égalité $x=y$ dans $\mathbb{R}$ est une relation d'équivalence. Autre exemple succulent : avec un entier $n\geqslant 1$ fixé, nous avons vérifié que la relation de congruence modulo n est une relation d'équivalence :

$$a\;\equiv\;b\;\mathsf{mod}\,n \qquad\overset{\text{déf}}{\iff}\qquad \Big(\;\exists\,k\in\mathbb{Z},\quad a\;=\;b+n\,k\;\Big).$$

Nous avons d'ailleurs établi que cette relation d'équivalence est *compatible* avec l'addition et la multiplication.

Dernier exemple basique : la relation « *être parallèle à* » est une relation d'équivalence entre les droites D, D', D'', …, du plan réel standard $\mathbb{R}^2$. Toutefois, la relation « D *est sécante avec* D' » n'est *pas* une relation d'équivalence — pourquoi ?

11. Du bas latin *binarius*, « qui met en jeu deux éléments ». En informatique, se dit d'un processus dont la représentation ne comporte que deux symboles.

12. « *Todas les tres !* ».

Définition 8.2. Étant donné une relation d'équivalence $\boldsymbol{R}$ sur un ensemble E, la *classe d'équivalence* d'un élément quelconque $a \in E$ est la collection de *tous* les éléments qui lui sont équivalents :

$$C\ell_{\boldsymbol{R}}(a) \;:=\; \big\{x \in E\colon\ x\,\boldsymbol{R}\,a\big\}.$$

Par exemple, toujours pour $\bullet \equiv \bullet \mod n$, et pour $a \in \mathbb{Z}$, on a :

$$\begin{aligned} C\ell_{\mathsf{mod}\,n}(a) \;&=\; \big\{x \in \mathbb{Z}\colon\ x \equiv a \mod n\big\} \\ &=\; \big\{x \in \mathbb{Z}\colon\ \text{il existe } k \in \mathbb{Z} \text{ avec } x = a + n\,k\big\} \\ &=\; a + n\,\mathbb{Z}. \end{aligned}$$

Ici, la classe d'équivalence consiste donc en une *infinité* d'éléments. Mais souvent, on note ou on abrège :

$$\overline{a} \;:=\; a + n\,\mathbb{Z},$$

et on travaille avec $\overline{a}$ comme s'il s'agissait d'un « vrai nombre », et non d'un ensemble infini, ce que nous avons déjà fait en effectuant toujours les calculs modulo n.

Proposition 8.3. *Les classes d'équivalence satisfont les quatre propriétés suivantes.*

(1) $a \in C\ell_{\boldsymbol{R}}(a)$*, pour tout* $a \in E$*.*

(2)* *Deux classes d'équivalence qui s'intersectent sont forcément* égales :

$$\emptyset \;\neq\; C\ell_{\boldsymbol{R}}(a) \cap C\ell_{\boldsymbol{R}}(b) \qquad\qquad \Longrightarrow \qquad\qquad C\ell_{\boldsymbol{R}}(a) \;=\; C\ell_{\boldsymbol{R}}(b).$$

(3) *Deux classes d'équivalence sont soit égales, soit disjointes :*

$$C\ell_{\boldsymbol{R}}(a) \;=\; C\ell_{\boldsymbol{R}}(b) \qquad\qquad \textit{ou bien} \qquad\qquad C\ell_{\boldsymbol{R}}(a) \cap C\ell_{\boldsymbol{R}}(b) \;\neq\; \emptyset.$$

(4) *Pour tous* $a, b \in E$ *:*

$$C\ell_{\boldsymbol{R}}(a) \;=\; C\ell_{\boldsymbol{R}}(b) \qquad \Longleftrightarrow \qquad a \;\in\; C\ell_{\boldsymbol{R}}(b) \qquad \Longleftrightarrow \qquad b \;\in\; C\ell_{\boldsymbol{R}}(a).$$

Démonstration. **(1)** Ceci équivaut à la reflexivité $a\,\boldsymbol{R}\,a$.

(2)* En effet, supposons qu'il existe un élément $x \in C\ell_{\boldsymbol{R}}(a) \cap C\ell_{\boldsymbol{R}}(b)$, c'est-à-dire que :

$$a\,\boldsymbol{R}\,x \qquad\qquad \text{et} \qquad\qquad x\,\boldsymbol{R}\,b.$$

On veut montrer qu'un élément arbitraire $y \in C\ell_{\boldsymbol{R}}(a)$ appartient aussi à $C\ell_{\boldsymbol{R}}(b)$. Grâce à la transitivité et par l'entremise de x, c'est facile :

$$\begin{aligned} \Big(\; y\,\boldsymbol{R}\,a \quad \text{et} \quad a\,\boldsymbol{R}\,x \;\Big) \qquad &\Longrightarrow \qquad y\,\boldsymbol{R}\,x \\ &\Longrightarrow \qquad \Big(\; y\,\boldsymbol{R}\,x \quad \text{et} \quad x\,\boldsymbol{R}\,b \;\Big) \qquad \Longrightarrow \qquad y\,\boldsymbol{R}\,b. \end{aligned}$$

Donc $C\ell_{\boldsymbol{R}}(a) \subset C\ell_{\boldsymbol{R}}(b)$. Par symétrie, on montre de même l'inclusion inverse $C\ell_{\boldsymbol{R}}(b) \subset C\ell_{\boldsymbol{R}}(a)$. Ces deux classes sont donc égales.

(3) et **(4)** sont alors conséquences immédiates de **(2)**. □

Ainsi, grâce à **(3)**, la collection de toutes les classes d'équivalence :

$$\bigcup_{a \in E} C\ell_{\boldsymbol{R}}(a) \;=\; E,$$

où on identifie celles qui sont égales, décompose E en sous-ensembles mutuellement sans intersection.

Définition 8.4. On appelle *partition* d'un ensemble E toute famille $\big(A_i\big)_{i\in I}$ de sous-ensembles $A_i \subset E$, indexée par un certain ensemble I, satisfaisant :
(1) $E = \bigcup_{i\in I} A_i$;
(2) $A_i \cap A_j = \emptyset$ pour tous $i, j \in I$ avec $i \neq j$;
(3) $A_i \neq \emptyset$ pour tout $i \in I$.

On note parfois :

$$E \,=\, \coprod_{i\in I} A_i,$$

avec le symbole spécial $\coprod$ de réunion (spéciale ?) — au lieu du symbole classique $\bigcup$ — qui signifie que la réunion est *disjointe*, *i.e.* satisfait **(2)** ci-dessus. Il est clair, alors, qu'une relation d'équivalence $\boldsymbol{R}$ sur un ensemble E le partitionne automatiquement.

Théorème 8.5. *Étant donné une relation d'équivalence $\boldsymbol{R}$ sur un ensemble E, la famille :*

$$\big\{C\ell_{\boldsymbol{R}}(a)\colon\ a\in E\big\}_{a\in E} \,=\, \big\{C\ell_{\boldsymbol{R}}(a_i)\colon\ i\in I\big\},$$

des différentes *classes d'équivalence* distinctes deux à deux *constitue une* partition *de :*

$$E \,=\, \coprod_{i\in I} C\ell_{\boldsymbol{R}}(a_i),$$

où certains $a_i \in E$ sont choisis avec :

$$\emptyset \,=\, C\ell_{\boldsymbol{R}}(a_i) \,\cap\, C\ell_{\boldsymbol{R}}(a_j) \qquad\qquad (\forall\, i\neq j). \quad \square$$

Ici, on a introduit un certain ensemble I d'indices $i \in I$, de telle sorte que toutes les classes d'équivalences soient présentes et soient mutuellement distinces.

9. Classes à gauche et classes à droite, modulo un sous-groupe

Rappelons que tous les sous-groupes de $\mathbb{Z}$ non réduits à $\{0\}$ sont de la forme $n\,\mathbb{Z}$, avec un entier $n \geqslant 1$, et que la notion de *congruence* modulo avait été définie comme :

$$\begin{aligned} x \,\equiv\, y \mod n \qquad &\overset{\text{déf}}{\Longleftrightarrow} \qquad x - y \,\in\, n\,\mathbb{Z} \\ &\Longleftrightarrow \qquad -x + y \,\in\, n\mathbb{Z}. \end{aligned}$$

Mais contrairement à la loi commutative $+$ de $\mathbb{Z}$, la loi d'un groupe quelconque n'est pas en général commutative. Si donc $H \subset G$ est un sous-groupe quelconque d'un groupe arbitraire G, l'analogue direct de l'appartenance de $x - y$ au sous-groupe $n\,\mathbb{Z}$ devrait être dupliqué en deux analogues :

$$\begin{aligned} x\,y^{-1} \,&\in\, H, \\ x^{-1}\,y \,&\in\, H. \end{aligned}$$

Nous allons maintenant introduire *deux* relations d'équivalence associées à un sous-groupe quelconque $H \subset G$, pas forcément distingué, car deux concepts distincts sont donc nécessaires.

Proposition 9.1. *Soit G un groupe, et soit $H \subset G$ un sous-groupe. Si, pour tout $a \in G$, on note :*

$$a\,H \,:=\, \big\{a\,h\colon\ h\in H\big\} \qquad\qquad \textit{et} \qquad\qquad H\,a \,:=\, \big\{h\,a\colon\ h\in H\big\},$$

alors les deux propriétés suivantes sont satisfaites.

(1) *La relation* $\sim_{\mathsf{g}}$ *définie sur* G *par :*

$$x \sim_{\mathsf{g}} y \quad \textit{si} \quad x^{-1}y \in H,$$

est une relation d'équivalence sur G*, dont les classes d'équivalences sont :*

$$\begin{aligned}\overline{x}^{\mathsf{g}} &= \big\{y \in G\colon\ x \sim_{\mathsf{g}} y\big\}\\ &= x\,H.\end{aligned}$$

(2) *La relation* $\sim_{\mathsf{d}}$ *définie sur* G *par :*

$$x \sim_{\mathsf{d}} y \quad \textit{si} \quad y\,x^{-1} \in H,$$

est aussi une relation d'équivalence sur G*, dont les classes d'équivalences sont :*

$$\begin{aligned}\overline{x}^{\mathsf{d}} &= \big\{y \in G\colon\ x \sim_{\mathsf{d}} y\big\}\\ &= H\,x.\end{aligned}$$

Il faut effectivement utiliser deux symboles différents, $\overline{x}^{\mathsf{g}}$ et $\overline{x}^{\mathsf{d}}$, pour ces deux types de classes d'équivalence, qui sont *a priori* distinctes.

Terminologie 9.2. Un ensemble de la forme $x\,H$ avec $x \in G$ est appelé une *classe à gauche modulo* H. L'ensemble des classes à gauche modulo H sera noté :

$$G/H := \big\{\overline{x}^{\mathsf{g}}\colon\ x \in G\big\}.$$

Un ensemble de la forme $H\,x$ avec $x \in G$ est appelé une *classe à droite modulo* H. L'ensemble des classes à droite modulo H sera noté :

$$H\backslash G := \big\{\overline{x}^{\mathsf{d}}\colon\ x \in G\big\}.$$

Toutefois, nous allons souvent noter simplement $\overline{x}$ les classes d'équivalence considérées.

Démonstration. Démontrons seulement **(1)**, puisque **(2)** est complètement similaire.

Pour tout $x \in G$, on a la réflexivité $x \sim_{\mathsf{g}} x$, puisque $x^{-1}x = 1_G \in H$.

Pour tous $x, y \in G$, en partant de $x \sim_{\mathsf{g}} y$, c'est-à-dire de $x^{-1}y \in H$, puisque tout sous-groupe est stable par inversion, il vient aussitôt :

$$\big(x^{-1}\,y\big)^{-1} = y^{-1}\,x \in H,$$

c'est-à-dire $y \sim_{\mathsf{g}} x$, ce qui prouve la symétrie.

Enfin, pour tous $x, y, z \in G$, si $x^{-1}y \in H$ et si $y^{-1}z \in H$, il vient puisque tout sous-groupe est stable par la loi interne :

$$\big(x^{-1}\,y\big)\,\big(y^{-1}\,z\big) = x^{-1}\,z \in H,$$

ce qui prouve la transitivité, et conclut. □

Les classes à gauche et à droite s'échangent l'une avec l'autre par l'opération d'inversion.

Proposition 9.3. *Pour tous* $x, y \in G$*, on a :*

$$x \sim_{\mathsf{g}} y \qquad \Longleftrightarrow \qquad x^{-1} \sim_{\mathsf{d}} y^{-1}.$$

Démonstration. En effet :

$$\begin{aligned} x \sim_{\mathtt{g}} y \quad &\overset{\text{déf}}{\iff} \quad x^{-1}y \in H \\ &\iff \quad \left(x^{-1}\,y\right)^{-1} \in H \\ &\iff \quad y^{-1}\left(x^{-1}\right)^{-1} \in H \quad \overset{\text{déf}}{\iff} \quad x^{-1} \sim_{\mathtt{d}} y^{-1}. \end{aligned}$$ □

Lorsque G est commutatif, comme par exemple $(\mathbb{Z}, +)$, classes à gauche et classes à droite *coïncident*. De plus, en notant la loi de G additivement, la classe à gauche ou à droite d'un élément $x \in G$ est l'ensemble :

$$x + H \,:=\, \big\{x + h\colon\ h \in H\big\}.$$

Comme les classes à gauche (ou à droite) d'un groupe G modulo un sous-groupe H sont des classes d'équivalence pour une certaine relation d'équivalence, le Théorème 8.5 général montre que G se *partitionne* selon ces classes. Les considérations préliminaires de la Section **8** donnent donc immédiatement la

Proposition 9.4. *Les classes à gauche (ou à droite) de G modulo H forment une partition de G.*

De plus, pour tous $x, y \in H$, on a :

$$y \in x\,H \qquad \iff \qquad x\,H \,=\, y\,H \qquad \iff \qquad x^{-1}\,y \in H,$$

ainsi que :

$$y \in H\,x \qquad \iff \qquad H\,x \,=\, H\,y \qquad \iff \qquad y\,x^{-1} \in H.$$ □

En particulier, pour tout $x \in G$, on a les équivalences :

$$x\,H \,=\, H \qquad \iff \qquad H\,x \,=\, H \qquad \iff \qquad x \in H.$$

Proposition 9.5. *L'application d'inversion :*

$$\begin{aligned} (\bullet)^{-1}\colon \quad G\big/H \ &\longrightarrow\ H\big\backslash G \\ x\,H \ &\longmapsto\ H\,x^{-1}, \end{aligned}$$

est bijective.

Preuve. C'est une conséquence logique directe de la Proposition 9.3. □

En particulier, le nombre de classes à gauche modulo H est fini si et seulement si le nombre de classes à droite modulo H l'est, et dans ce cas, ces deux nombres sont égaux.

10. Indice $[G : H]$ d'un sous-groupe $H \subset G$

Le fait que les classes à gauche et à droite soient en bijection justifie d'introduire la

Définition 10.1. Soit G un groupe et soit $H \subset G$ un sous-groupe. Le nombre de classes à gauche modulo H, lorsqu'il est fini, est appelé l'*indice de H dans G*, et il est noté :

$$[G : H].$$

C'est aussi le nombre de classes à droite modulo H.

Lorsque $G\big/H$ est de cardinal infini, on pose :

$$[G : H] \,:=\, \infty.$$

Observons que lorsque G est fini, *i.e.* lorsque $|G| < \infty$, pour tout sous-groupe $H \subset G$, on a la finitude $[G : H] < \infty$, car ce nombre est toujours majoré par le nombre d'éléments de G :

$$\big|[G : H]\big| \leqslant |G|.$$

Pour $H = n\mathbb{Z}$ avec $n \geqslant 1$ dans $G = \mathbb{Z}$, nous avons implicitement déjà compris que les deux relation d'équivalence $\sim_{\mathrm{g}}$ et $\sim_{\mathrm{d}}$, qui coïncident puisque la loi est commutative, s'identifient à la relation de *congruence* modulo n. L'ensemble des classes :

$$G/H \,=\, \mathbb{Z}/n\,\mathbb{Z},$$

nous fait donc retrouver un objet bien connu [13], que nous avons étudié dans le chapitre consacré à $\mathbb{Z}$ et à $\mathbb{Z}/n\mathbb{Z}$.

Pour $n \geqslant 1$, nous savons que :

$$\big|[\mathbb{Z} : n\mathbb{Z}\big| \,=\, \big|\mathbb{Z}/n\mathbb{Z}\big| \,=\, n,$$

puisque la « marmite » $\big\{0, 1, \ldots, n-1\big\}$ contient exactement n (gros) légumes, mais en revanche, pour $n = 0$, on a :

$$\big|[\mathbb{Z} : 0\mathbb{Z}\big| \,=\, |\mathbb{Z}| \,=\, \infty,$$

car la relation de congruence modulo 0 n'est autre que la relation d'égalité.

Les relations de classe à gauche et de classe à droite permettent de donner une autre caractérisation des sous-groupes distingués d'un groupe G.

Proposition 10.2. *Pour un sous-groupe quelconque $H \subset G$ d'un groupe arbitraire G, les trois propriétés suivantes sont équivalentes.*

(i) *Le sous-groupe $H \lhd G$ est distingué dans G.*

(ii) *Pour tout $x \in G$, on a $x\,H = H\,x$.*

(iii) *Pour tout $x \in G$, on a $x\,H\,x^{-1} = H$, où :*

$$x\,H\,x^{-1} \,:=\, \big\{x\,h\,x^{-1} :\;\; h \in H\big\}.$$

Démonstration. **(i)** $\Longrightarrow$ **(ii)**. Supposons que H soit distingué dans G, et soit $x \in G$. Pour tout $h \in H$, on a $x\,h\,x^{-1} \in H$. Il existe donc $h' \in H$ avec $x\,h\,x^{-1} = h'$, d'où $x\,h = h'\,x$. Ainsi, on obtient $x\,h \in H\,x$, ce qui montre une première inclusion $x\,H \subset H\,x$.

De manière similaire, on a aussi :

$$x^{-1}\,h\,\big(x^{-1}\big)^{-1} \,\in\, H,$$

donc il existe $h'' \in H$ avec $x^{-1}\,h\,(x^{-1})^{-1} = h''$, d'où $h\,x = x\,h''$. Ainsi, on obtient $h\,x \in x\,H$, ce qui montre l'inclusion inverse $H\,x \subset x\,H$. En comparant ces deux inclusions, on obtient bien $x\,H = H\,x$.

(ii) $\Longrightarrow$ **(iii)**. Soit $x \in G$. On suppose donc $x\,H = H\,x$. En utilisant les définitions des ensembles concernés, on vérifie aisément les égalités attendues :

$$x\,H\,x^{-1} \,=\, (x\,H)\,x^{-1} \,=\, (H\,x)\,x^{-1} \,=\, H\,(x\,x^{-1}) \,=\, H\,1_G \,=\, H.$$

(iii) $\Longrightarrow$ **(i)** est évident. □

À cette occasion, énonçons et démontrons un résultat classique de théorie élémentaire des groupes.

13. Le lecteur pourra rester pantois et admiratif devant la cohérence des notations ! Que c'est beau, les mathématiques !

Proposition 10.3. *Tout sous-groupe $H \subset G$ d'un groupe G dont l'indice égal à :*

$$2 \,=\, [G : H]$$

est distingué *dans G.*

L'hypothèse est donc qu'il n'y a que *deux* classes de G modulo H, que ce soit à gauche ou à droite, et nous allons les exhiber.

Démonstration. Grâce à la proposition précédente, il suffit de faire voir que $x\,H \,=\, H\,x$, pour tout $x \,\in\, G$. Quand $x \,\in\, H$, c'est clair, puisque H est un sous-groupe, donc on a $x\,H = H = H\,x$ d'après la remarque qui suit la Proposition 9.4.

Supposons donc que $x \,\notin\, H$. Alors $x\,H \,\neq\, H$, car sinon, on aurait $x\,1_G \,=\, x \,\in\, H$, contradiction. Ainsi, H *et* $x\,H$ sont *deux* classes à gauche de G modulo H *distinctes*, donc forcément disjointes, et puisqu'il y a exactement *deux* classes par hypothèse, il vient :

$$G \,=\, H \cup x\,H.$$

Pareillement, H et $H\,x$ sont deux classes à droite de G modulo H *distinctes*, et il vient :

$$G \,=\, H \cup H\,x.$$

Comme ces deux réunions sont disjointes et ont l'ensemble H en commun, nous devons nécessairement recevoir du ciel ce que nous désirions :

$$x\,H \,=\, H\,x. \qquad \square$$

Continuons ce paragraphe en présentant une propriété de multiplicativité de l'indice, très classique et très utilisée.

Théorème 10.4. *Soit G un groupe, soit $H \subset G$ un sous-groupe de G, et soit $K \subset H$ un sous-groupe de G. Alors l'indice $[G : K]$ est fini si et seulement si $[G : H]$ et $[H : K]$ sont tous les deux finis, et dans ce cas, on a :*

$$[G : K] \,=\, [G : H] \cdot [H : K].$$

En fait, cette formule de multiplicativité est vraie généralement, car on peut démontrer, en examinant les arguments qui suivent, que $[G : K] = \infty$ si et seulement si $[G : H] = \infty$ ou $[H : K] = \infty$.

Démonstration. Écrivons :

$$G\big/H \,=\, \big\{g_i H\colon\ i \in I\big\},$$

où les classes à gauche $g_i H$, pour $i \in I$, sont deux à deux distinctes. De même, écrivons :

$$H\big/K \,=\, \big\{h_j K\colon\ j \in J\big\},$$

où les classes à gauche $h_j K$, pour $j \in J$, sont deux à deux distinctes.

Lemme 10.5. *Les classes à gauche de $G\big/K$ sont toutes les classes :*

$$G\big/K \,=\, \big\{g_i h_j\, K\colon\ (i,j) \in I \times J\big\},$$

qui sont deux à deux distinctes.

Démonstration. Soit $g \in G$ arbitraire. Alors il existe $i \in I$ tel que $g \in g_i H$ appartient à l'une des classes à gauche de G modulo H, puisque G est la réunion de ces classes. On a donc $g = g_i h$ pour un certain élément $h \in H$.

Mais alors, il existe aussi un indice $j \in J$ tel que $h \in h_j K$, puisque les classes à gauche de H modulo K remplissent H. Ainsi, il existe $k \in K$ tel que :

$$g \, = \, g_i \, h_j \, k.$$

On en déduit que $g \sim g_i h_j$ modulo K (à gauche), et aussi que $g\,K = g_i h_j\,K$.

Puisque $g \in G$ était arbitraire, nous avons donc démontré que la réunion de toutes les classes de la forme :

$$g_i h_j \, K, \qquad \text{avec } \; i \in I \text{ quelconque, } \; \text{et avec } \; j \in J \text{ quelconque,}$$

couvre toutes les classes possibles de G modulo K. Il ne reste plus qu'à faire voir que ces classes sont mutuellement distinctes.

Supposons donc, pour deux paires d'indices (i, j) et (i', j') de $I \times J$, que l'on ait la coïncidence :

$$g_i h_j \, K \, = \, g_{i'} h_{j'} \, K, \tag{10.6}$$

et cherchons à en déduire que $i = i'$ puis que $j = j'$.

Ainsi, il existe $k \in K$ tel que $g_i h_j = g_{i'} h_{j'} k$, c'est-à-dire — attention à l'ordre des termes, car la loi n'est pas forcément commutative — :

$$g_i \, = \, g_{i'} \, h_{j'} \, k \, h_j^{-1}.$$

Comme $k \in K \subset H$, on obtient $g_i \in g_{i'} H$, et donc $g_i \, H \, = \, g_{i'} \, H$. Par le choix de I au début, on déduit que $i = i'$ nécessairement.

Ensuite, puisque $g_i \, = \, g_{i'}$, après multiplication de (10.6) par g_i^{-1}, on trouve $h_j \, K \, = \, h_{j'} \, K$, et par choix de J au début, on déduit comme annoncé que $j = j'$ nécessairement.

En définitive, les classes $g_i h_j \, K$ pour $i \in I$ et $j \in J$ sont bien deux à deux distinctes. □

De ce lemme, il découle que $G\big/K$ est (de cardinal) fini si et seulement si $I \times J$ est un ensemble fini, c'est-à-dire si et seulement si I *et* J sont tous les deux finis. Dans ce cas, les deux indices :

$$[G : H] \, = \, |I| \qquad\qquad \text{et} \qquad\qquad [H : K] \, = \, |J|,$$

sont finis, et on obtient bien la multiplicativité annoncée :

$$[G : K] \, = \, \big|I \times J\big| \, = \, |I| \cdot |J| \, = \, [G : H] \cdot [H : K]. \qquad \square$$

11. Théorème de Lagrange

Nous pouvons enfin énoncer et démontrer le fameux théorème de Lagrange, utile partout, *urbi et orbe*. Attention ! L'hypothèse $|G| < \infty$ que G est de cardinal fini est essentielle !

Théorème 11.1. [Lagrange] *Soit G un groupe arbitraire de cardinal* fini. *Alors pour tout sous-groupe $H \subset G$, on a :*

$$|G| \, = \, [G : H] \cdot |H|.$$

Notamment, le cardinal de tout sous-groupe H d'un groupe fini G divise toujours le cardinal de G.

Le point crucial dont il faut se souvenir est donc la divisibilité cardinalique :

$$|H| \;\big|\; |G|.$$

On peut aussi écrire :

$$\big|G/H\big| \;=\; \frac{|G|}{|H|}.$$

Démonstration. Posons $r := [G : H]$, entier fini car $[G : H] \leqslant |G| < \infty$. Alors comme les r classes à gauche $x_1H, \dots, x_rH$ de G modulo H forment une *partition* de G, on a la réunion *disjointe :*

$$G \;=\; x_1H \cup \cdots \cup x_rH.$$

Lemme 11.2. *Pour tout* $1 \leqslant i \leqslant r$*, on a* $\big|x_iH\big| = |H|$.

Preuve. En effet, puisque x_i^{-1} existe toujours dans un groupe, il suffit de considérer la bijection :

$$\begin{array}{rccc} \ell_{x_i}\colon & H & \longrightarrow & x_i\,H \\ & h & \longmapsto & x_i\,h \end{array} \qquad \text{d'inverse} \qquad \begin{array}{rccc} & H & \longleftarrow & x_i\,H \\ & x_i^{-1}h' & \longleftarrow & h'. \end{array} \quad :\ell_{x_i^{-1}}$$ □

En conclusion :

$$\begin{aligned} |G| \;&=\; \big|x_1H\big| + \cdots + \big|x_rH\big| \\ &=\; |H| + \cdots + |H| \\ &=\; r \cdot |H| \\ &=\; [G : H] \cdot |H|. \end{aligned}$$ □

12. Concept d'ordre d'un élément d'un groupe

Nous pouvons maintenant définir l'ordre d'un élément d'un groupe arbitraire.

Définition 12.1. [Ordre fini] Soit G un groupe. On dit qu'un élément $x \in G$ est *d'ordre fini* si le sous-groupe qu'il engendre dans G :

$$\langle\, x \,\rangle \;=\; \big\{x^i \in G\colon\ i \in \mathbb{Z}\big\},$$

est de cardinal $|\langle x\rangle| < \infty$ fini. Dans ce cas, l'*ordre* de x est défini comme étant ce cardinal, et il est noté :

$$o(x) \;:=\; \big|\langle\, x \,\rangle\big|.$$

En particulier, $o(x)$ est bien défini, pour tout $x \in G$, lorsque G est de cardinal $|G| < \infty$ fini, puisque $\langle x\rangle \subset G$ implique $|\langle x\rangle| \leqslant |G| < \infty$.

Mais cette définition, qui repose sur l'estimation d'un *cardinal*, n'est pas *a priori* très commode à manipuler — en tout cas, pas aussi bien que les masses (psycho-physiques) en période électorale ! Nous allons présenter un éclairage lumineux qui va nous fournir un moyen très pratique et très intuitif de déterminer l'ordre d'un élément.

En effet, considérons la collection de toutes les puissances possibles de x :

$$\langle\, x \,\rangle \;=\; \big\{\,\dots,\, x^{-3},\, x^{-2},\, x^{-1},\, 1_G,\, x,\, x^2,\, x^3,\, \dots\big\}.$$

Si x est d'ordre fini, c'est-à-dire si cet ensemble est de cardinal fini, il est impossible que toutes ces puissances, en nombre *infini*, soient distinctes deux à deux. Donc il doit exister deux entiers distincts $i < j$ tels que :

$$x^j \,=\, x^i \qquad\qquad \Longleftrightarrow \qquad\qquad x^{j-i} \,=\, 1_G.$$

Grâce à cette observationette, nous pouvons *redéfinir* l'ordre de x de manière plus naturelle comme suit.

Définition 12.2. [Ordre fini bis] Un élément $x \in G$ est dit d'*ordre fini* s'il existe un entier $m \geqslant 1$ tel que :

$$x^m \,=\, 1_G.$$

L'*ordre* de x est alors l'entier :

$$o(x) \,:=\, \mathsf{min}\big\{m \geqslant 1 \colon\ x^m = 1_G\big\}.$$

Mais l'équivalence entre ces deux définitions n'est pas encore complète, des raisonnements supplémentaires sont nécessaires, que nous devons entreprendre.

Tout d'abord, il est clair qu'avec $x^m = 1_G$, la collection des puissances de x se répète de manière périodique, comme dans l'anneau connu $\mathbb{Z}/m\mathbb{Z}$:

$$\begin{aligned} \langle\, x \,\rangle \,&=\, \big\{\, \dots, x^{-m}, x^{-m+1}, \dots, x^{-1}, 1_G, x, \dots, x^{m-1}, x^m, x^{m+1}, \dots, x^{2m-1}, \dots \big\} \\ &=\, \big\{1_G, x, \dots, x^{m-1}\big\}, \end{aligned}$$

donc le cardinal $|\langle x \rangle| < \infty$ est fini car il est $\leqslant m$. Ainsi, nous avons au moins compris et vérifié que :

$$\big|\langle\, x \,\rangle\big| \,<\, \infty \qquad\qquad \Longleftrightarrow \qquad\qquad \exists\, m \,\geqslant\, 1, \quad x^m \,=\, 1_G.$$

Il reste encore à comprendre l'égalité :

$$\big|\langle\, x \,\rangle\big| \,=\, \mathsf{min}\big\{m \geqslant 1 \colon\ x^m = 1_G\big\},$$

et pour cela, tous les arguments vont reposer, *in fine*, sur la division euclidienne.

Commençons par observer que la collection des puissances x^p est dotée d'une structure algébrique naturelle.

Proposition 12.3. *Soit G un groupe arbitraire, et soit $x \in G$ un élément quelconque fixé. Alors l'application :*

$$\begin{aligned} h_x \colon\quad \mathbb{Z} \,&\longrightarrow\, G \\ i \,&\longmapsto\, x^i, \end{aligned}$$

est un morphisme de groupes. De plus, on a équivalence entre :

(i) h_x *n'est* pas *injectif ;*

(ii) $\mathsf{Ker}\, h_x \neq \{0\}$ *;*

(iii) x *est d'ordre fini,* i.e. *il existe* $m \geqslant 1$ *avec* $x^m = 1_G$.

Démonstration. L'équivalence entre **(i)** et **(ii)** est une propriété générale des morphismes de groupes, que la Proposition 6.4 a déjà exprimée et démontrée.

Montrons **(ii)** $\Longleftrightarrow$ **(iii)**. On a $\mathsf{Ker}\, h_x \neq \{0\}$ si et seulement si il existe $m \in \mathbb{Z}\backslash\{0\}$ tel que $x^m = 1_G$, par définition. Quitte à remplacer m par $-m$, on peut supposer que $m \geqslant 1$ car $1_G^{-1} = 1_G$. Donc l'équivalence est « okeille » ! $\square$

Théorème 12.4. *Soit G un groupe arbitraire, et soit $x \in G$ un élément quelconque.*
(1) *x est d'ordre fini,* i.e. *$|\langle x\rangle| < \infty$, si et seulement si il existe un entier $m \geqslant 1$ tel que :*

$$x^m \,=\, 1_G.$$

(2) *Dans ce cas, l'ordre de x est le plus petit entier $m \geqslant 1$ tel que $x^m = 1_G$, c'est-à-dire :*

$$\mathbf{o}(x) \,=\, \mathsf{min}\big\{m \geqslant 1\colon\ x^m = 1_G\big\},$$

et le groupe que x engendre dans G est égal précisément à l'ensemble :

$$\langle\, x\,\rangle \,=\, \big\{1_G,\, x,\, x^2,\, \ldots,\, x^{o(x)-1}\big\},$$

constitué d'éléments distincts deux à deux, dont le cardinal est égal à $\mathbf{o}(x)$.
(3) *De plus, pour tout entier $m \in \mathbb{Z}$, on a :*

$$x^m \,=\, 1_G \qquad\qquad \Longleftrightarrow \qquad\qquad \mathbf{o}(x) \,\big|\, m.$$

(4) *Enfin, si G est un groupe fini, l'ordre de tout élément $x \in G$ divise toujours le cardinal de G :*

$$\mathbf{o}(x) \,\big|\, |G|.$$

Démonstration. **(1)** étant acquis, montrons **(2)**. Grâce au morphisme h_x, et grâce à la Proposition 6.3, le sous-ensemble de $\mathbb{Z}$:

$$\begin{aligned}\big\{m \in \mathbb{Z}\colon\ x^m = 1_G\big\} \,&=\, \mathsf{Ker}\, h_x\\ &\subset\, \mathbb{Z},\end{aligned}$$

est alors un *sous-groupe* de $\mathbb{Z}$. Or le point crucial de l'argumentation, c'est que nous connaissons déjà tous les sous-groupes possibles de $\mathbb{Z}$, grâce au Théorème 5.6.

Ainsi, d'après ce théorème super-clair, il existe un entier $n \geqslant 1$ tel que :

$$\mathsf{Ker}\, h_x \,=\, n\,\mathbb{Z}.$$

On a donc simultanément (relire l'énoncé du Théorème 5.6 en question) :

$$\begin{aligned}x^n \,&=\, 1_G,\\ n \,&=\, \mathsf{min}\big\{m \in \mathbb{Z}\colon\ x^m = 1_G\big\}.\end{aligned}$$

Assertion 12.5. *Les éléments $1_G, x, \ldots, x^{n-1}$ sont distincts deux à deux*[14].

Preuve. Supposons qu'il existe deux exposants i et j avec $0 \leqslant i, j \leqslant n-1$ tels que $x^i = x^j$. Alors $x^{i-j} = 1_G$. Autrement dit :

$$i - j \,\in\, \mathsf{Ker}\, h_x \,=\, n\,\mathbb{Z},$$

c'est-à-dire que $i - j$ est un multiple de n.

Mais comme, grâce à une révision d'un argument souvent utilisé dans le chapitre consacré à l'arithmétique dans $\mathbb{Z}$, on a les inégalités :

$$-\,(n-1) \,\leqslant\, i - j \,\leqslant\, n - 1,$$

il est nécessaire que $i - j = 0$, c'est-à-dire que $i = j$. Autrement dit, $x^i = x^j$ si et seulement si $i = j$.

14. C'est une conséquence logique et théorique de $\mathsf{Ker}\, h_x = n\,\mathbb{Z}$, mais re-démontrons cela « à la main », afin de mieux comprendre ce qui est en jeu : l'intervention naturelle de l'anneau $\mathbb{Z}$ « concret » avec sa structure de groupe arithmétique, lorsqu'on considère toutes les puissances x^i d'un élément x vivant « sur une autre planète », dans un « groupe abstrait » G.

Par contraposition, les puissances x^i avec $0 \leqslant i \leqslant n-1$ sont bien mutuellement distinctes. □

Grâce à tout cela, nous concluons bien que nos deux définitions étaient équivalentes :

$$\begin{aligned} n &= \mathsf{min}\left\{m \in \mathbb{Z}\colon\ x^m = 1_G\right\} \\ &= \mathsf{Card}\left\{1_G, x, \ldots, x^{n-1}\right\} \\ &= \mathsf{Card}\left\{x^i\colon\ i \in \mathbb{Z}\right\} \\ &= \left|\langle\, x\,\rangle\right| \\ &= o(x). \end{aligned}$$

La propriété **(3)** est alors claire grâce à ce qui précède, car $x^m = 1_G$ signifie $m \in \mathsf{Ker}\, h_x = n\,\mathbb{Z}$, c'est-à-dire que m est multiple de $o(x) = n$.

On peut d'ailleurs re-démontrer cela « à la main » en utilisant la division euclidienne. Soit $m \in \mathbb{Z}$ avec $x^m = 1_G$. Euclidivisons $m = q\,n + r$ avec $0 \leqslant r \leqslant n-1$. Comme on a déjà $x^n = 1_G$, il vient :

$$1_G \;=\; x^m \;=\; x^{nq+r} \;=\; \left(x^n\right)^q x^r \;=\; (1_G)^q\, x^r \;=\; x^r.$$

Par minimalité de n, ceci force $r = 0$. Donc on a bien :

$$n \;=\; o(x) \;\Big|\; m.$$

Pour terminer, montrons la propriété **(4)**. Le fait que $o(x)$ divise l'ordre du groupe G est une application directe du Théorème 11.1 de Lagrange au sous-groupe $H := \langle x\rangle$ de G. □

Pour tout diviseur d de $|G|$, il n'existe pas forcément un $x \in G$ tel que $o(x) = d$. Par exemple, le groupe à quatre éléments contenus dans $\mathbb{R}^\times \times \mathbb{R}^\times$:

$$G \;:=\; \Big\{(1,1),\ (1,-1),\ (-1,1),\ (-1,-1)\Big\},$$

est d'ordre (de cardinal) 4, mais ne contient aucun élément x d'ordre $o(x) = 4$ (exercice).

Théorème 12.6. *Soit G un groupe d'ordre (de cardinal) :*

$$|G| \;<\; \infty.$$

Alors tout élément $x \in G$ satisfait :

$$x^{|G|} \;=\; 1_G.$$

De plus, si $H \subset G$ est un sous-groupe, alors tout $y \in H$ satisfait :

$$y^{|H|} \;=\; 1_H \;=\; 1_G.$$

Preuve. Grâce au Théorème 12.4 **(4)** qui précède, on a $o(x) \,|\, |G|$, c'est-à-dire :

$$o(x)\, d \;=\; |G| \qquad \text{(avec } d \in \mathbb{Z}\text{)},$$

et puisque, toujours d'après ce théorème, on a $1_G = x^{\,o(x)}$, il vient effectivement :

$$1_G \;=\; \left(x^{\,o(x)}\right)^d \;=\; x^{\,o(x)\,d} \;=\; x^{|G|}.$$

Quand $H \subset G$ est un sous-groupe, donc un groupe en lui-même, ce qui vient d'être démontré s'applique au groupe $G := H$. □

Théorème 12.7. *Soit G un groupe arbitraire, et soit $x \in G$ un élément d'ordre $o(x) < \infty$ fini. Alors pour tout entier $c \geqslant 1$, l'élément x^c est aussi d'ordre $o(x^c) < \infty$ fini, égal à :*

$$o(x^c) \;=\; \frac{o(x)}{\mathsf{pgcd}\,(c, o(x))}.$$

En particulier :

(1) *si $c \,|\, o(x)$, alors $o(x^c) = \frac{o(x)}{c}$;*

(2) *si $c \wedge o(x) = 1$ est premier avec $o(x)$, alors $o(x^c) = o(x)$.*

Démonstration. Soit donc $x \in G$, et soit $c \geqslant 1$. Posons :

$$d \;:=\; \mathsf{pgcd}\,\big(c,\, o(x)\big),$$

puis, écrivons :

$$c \;=\; d\,r \qquad\qquad o(x) \;=\; d\,s,$$

avec deux entier $r \wedge s = 1$ premiers entre eux. Pour $m \in \mathbb{Z}$ quelconque, on a, grâce au Théorème 12.4 **(3)** :

$$\begin{aligned}
\big(x^c\big)^m \;=\; 1_G \qquad \Longleftrightarrow \qquad x^{c\,m} \;=\; 1_G \qquad &\Longleftrightarrow \qquad o(x) \;\big|\; c\,m \\
&\Longleftrightarrow \qquad d\,s \;\big|\; d\,r\,m \\
&\Longleftrightarrow \qquad s \;\big|\; r\,m \qquad \Longleftrightarrow \qquad s \;\big|\; m,
\end{aligned}$$

la dernière équivalence étant gracieusement offerte par le Théorème de gauss.

Par conséquent, x^c est d'ordre fini, puisqu'avec le choix de $m := s$ qui satisfait trivialement $s \,|\, s$, on obtient $(x^c)^s = 1_G$ en remontant ces équivalences.

De surcroît, puisque que $m := s$ est clairement le plus petit exposant $\geqslant 1$ satisfaisant $s \,|\, m$, nous concluons bien en remontant vers la gauche que :

$$o\big(x^c\big) \;=\; s \;=\; \frac{o(x)}{\mathsf{pgcd}\,(c, o(x))}.$$

Les deux cas particuliers **(1)** et **(2)** sont alors des conséquences immédiates de cette agréable formule générale. □

Proposition 12.8. *Soit G un groupe, et soient $x, y \in G$ deux éléments d'ordres finis qui commutent,* i.e. *satisfont $x\,y = y\,x$. Alors :*

(1) *le produit $x\,y$ est d'ordre fini ;*

(2) *sous l'hypothèse supplémentaire $\langle x\rangle \cap \langle y\rangle = \{1_G\}$, on a :*

$$o\big(x\,y\big) \;=\; \mathsf{ppcm}\,\big(o(x),\, o(y)\big);$$

(3) *si les deux ordres $o(x) \cap o(y) = 1$ sont premiers entre eux, alors l'hypothèse supplémentaire $\langle x\rangle \cap \langle y\rangle = \{1_G\}$ est satisfaite, et l'on a :*

$$o\big(x\,y\big) \;=\; o(x) \cdot o(y).$$

Démonstration. **(1)** Posons $m := \mathsf{ppcm}\,\big(o(x), o(y)\big)$. Alors on peut écrire :

$$m \;=\; r\,o(x) \;=\; s\,o(y) \qquad\qquad \text{(avec } r, s \in \mathbb{Z}\text{)}.$$

Puisque $x\,y = y\,x$, on sait que les puissances se contractent :

$$\big(x\,y\big)^m \;=\; x^m\,y^m \;=\; \big(x^{o(x)}\big)^r\,\big(y^{o(y)}\big)^s \;=\; 1_G^r\,1_G^s \;=\; 1_G,$$

donc ce calcul fait voir que le produit $x\,y$ est bien d'ordre fini — divisant m, d'ailleurs, d'après le Théorème 12.4 **(3)**.

Comme **(2)** l'énonce, hypothésons supplémentairement que $\langle x\rangle \cap \langle y\rangle = \{1_G\}$. Il s'agit de montrer que :

$$o\big(x\,y\big) \overset{?}{=} m \,=\, \mathsf{ppcm}\,\big(o(x),\,o(y)\big).$$

Nous venons de voir que $(x\,y)^m = 1_G$, donc d'après le Théorème 12.4 **(3)** qui précède, il est clair que $o(x\,y) \,\big|\, m$.

Introduisons alors l'entier :

$$\ell \,:=\, o\,\big(x\,y\big) \qquad\qquad \text{avec} \qquad\qquad \ell \,\big|\, m.$$

On a $(x\,y)^\ell = x^\ell\,y^\ell = 1_G$. Ainsi, $x^\ell = y^{-\ell}$, et donc $x^\ell \in \langle x\rangle \cap \langle y\rangle$. Comme par hypothèse $\langle x\rangle \cap \langle y\rangle = \{1_G\}$, il est incontournable que :

$$x^\ell \,=\, 1_G \,=\, y^{-\ell}.$$

On en déduit que $o(x) \,|\, \ell$ et que $o(y) \,|\, \ell$, encore grâce au Théorème 12.4 **(3)**.

Par conséquent, la définition même du plus petit commun multiple (réviser !) force $m \,|\, \ell$. En conclusion, $\ell \,|\, m$ et $m \,|\, \ell$ offrent bien l'égalité souhaitée $\ell = m$.

(3) Pour terminer, montrons le dernier point. Comme $\langle x\rangle \cap \langle y\rangle$ est un sous-groupe de $\langle x\rangle$ et aussi un sous-groupe de $\langle y\rangle$, son ordre (son cardinal) doit diviser à la fois $o(x)$ et $o(y)$, d'après le Théorème 11.1 de Lagrange.

Mais puisque ces deux ordres $o(x)$ et $o(y)$ sont premiers entre eux par hypothèse, on en déduit que $\langle x\rangle \cap \langle y\rangle$ est un groupe d'ordre (de cardinal) égal à 1, ce qui le force à se réduire au singleton $\{1_G\}$!

Donc l'hypothèse supplémentaire du point **(2)** est vérifiée, ce qui nous donne :

$$o\big(x\,y\big) \,=\, \mathsf{ppcm}\,\big(o(x),\,o(y)\big) \,=\, o(x)\cdot o(y),$$

la dernière égalité provenant du fait que $o(x)$ et $o(y)$ sont premiers entre eux. □

13. Formule d'inversion de Möbius

Nous consacrons une section « entre parenthèses » à la démonstration d'une formule importante en théorie des nombres, et qui nous sera utile dans la prochaine Section **14**.

Rappelons que tout nombre entier $n \geqslant 2$ se factorise comme :

$$n \,=\, p_1^{\alpha_1}\cdots p_r^{\alpha_r},$$

avec $2 \leqslant p_1 < \cdots < p_r$ premiers, avec $r \geqslant 1$, et avec des exposants $\alpha_1 \geqslant 1$, …, $\alpha_r \geqslant 1$. Le cas où au moins l'un des exposant α_i est $\geqslant 2$ va être « dégénéré ».

Définition 13.1. La *fonction de Möbius* $\mu\colon \mathbb{N}^* \longrightarrow \mathbb{Z}$ est définie par :

$$\mu(n) \,:=\, \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } n \,=\, p_1\cdots p_r \text{ avec } 2 \leqslant p_1 < \cdots < p_r \text{ premiers}, \\ 0 & \text{s'il existe un nombre premier } p \text{ tel que } p^2 \,|\, n. \end{cases}$$

Autrement dit, $\mu(\bullet)$ s'annule sur tous les entiers $n \,=\, p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ dont au moins un exposant α_i satisfait $\alpha_i \geqslant 2$.

Par exemple :

$$\mu(2) \,=\, \mu(3) \,=\, 1, \qquad \mu(18) \,=\, \mu(2{\cdot}3^2) \,=\, 0, \qquad \mu(30) \,=\, \mu\big(2{\cdot}3{\cdot}5\big) \,=\, (-1)^3 \,=\, -1.$$

Dans cette section, si $n \geqslant 1$ est un entier, les symboles $\sum_{d\,|\,n}$ et $\prod_{d\,|\,n}$ désigneront une somme et un produit sur l'ensemble des diviseurs d de n avec $1 \leqslant d \leqslant n$, c'est-à-dire :

$$\sum_{d\,|\,n}(\bullet) := \sum_{\substack{1\leqslant d\leqslant n\\ d\,|\,n}}(\bullet) \qquad \text{et} \qquad \prod_{d\,|\,n}(\bullet) := \prod_{\substack{1\leqslant d\leqslant n\\ d\,|\,n}}(\bullet).$$

Théorème 13.2. *Pour tout entier $n \geqslant 1$, on a :*

$$\sum_{d\,|\,n}\mu(d) = \begin{cases} 1 & \text{si } n = 1,\\ 0 & \text{pour tout } n \geqslant 2.\end{cases}$$

Démonstration. Si $n = 1$, cette somme se réduit à l'unique terme $\mu(1) = 1$. On peut donc supposer $n \geqslant 2$, que l'on décompose en facteurs premiers :

$$n = p_1^{\alpha_1}\cdots p_r^{\alpha_r},$$

toujours avec $2 \leqslant p_1 < \cdots < p_r$, avec $r \geqslant 1$, et avec $\alpha_1, \ldots, \alpha_r \geqslant 1$.

Clairement, les diviseurs d de n sont tous les :

$$d = p_1^{\beta_1}\cdots p_r^{\beta_r},$$

avec $0 \leqslant \beta_1 \leqslant \alpha_1$, …, $0 \leqslant \beta_r \leqslant \alpha_r$. Or, dès qu'un $\beta_i \geqslant 2$, on a $\mu(d) = 0$. Par conséquent, dans la somme à calculer et à égaler à zéro :

$$\sum_{d\,|\,n}\mu(d) \overset{?}{=} 0,$$

les seuls diviseurs de n qui vont contribuer sont ceux de la forme :

$$d = p_{\mathrm{I}} := p_{i_1}\cdots p_{i_s},$$

où $\mathrm{I} = \{i_1, \ldots, i_s\}$, est une partie quelconque à $0 \leqslant s \leqslant r$ éléments de l'ensemble $\{1, \ldots, r\}$, et on a alors :

$$\sum_{d\,|\,n}\mu(d) = \sum_{\mathrm{I}\subset\{1,\ldots,r\}}(-1)^{|\mathrm{I}|}.$$

Or, pour tout s avec $0 \leqslant s \leqslant r$, il y a exactement $\binom{r}{s}$ parties $\mathrm{I} \subset \{1, \ldots, r\}$ comportant $s = |\mathrm{I}|$ éléments. Ainsi, nous obtenons bien le résultat annoncé :

$$\begin{aligned}\sum_{d\,|\,n}\mu(d) &= \sum_{s=0}^{r}\binom{r}{s}(-1)^s\\ &= \big(1-1\big)^r\\ &= 0.\end{aligned}$$

□

Nous pouvons maintenant énoncer et démontrer le

Théorème 13.3. [Formule d'inversion de Möbius] *Soit G un groupe* commutatif*, et soient $f, g\colon \mathbb{N}^* \longrightarrow G$ deux applications. On suppose que l'on a :*

$$g(n) = \prod_{d\,|\,n} f(d), \qquad \text{pour tout } n \geqslant 1. \tag{13.4}$$

Alors on a l'égalité « réciproque » :

$$\prod_{d\,|\,n} g\big(\tfrac{n}{d}\big)^{\mu(d)} = f(n), \qquad \text{pour tout } n \geqslant 1.$$

Démonstration. Commençons par détailler une

Observation 13.5. *Soit $n \geqslant 1$ fixé. Pour tous $d, d' \geqslant 1$, on a les équivalences :*

$$\Big(\, d \,|\, n \quad \textit{et} \quad d' \,|\, \tfrac{n}{d} \, \Big) \qquad \Longleftrightarrow \qquad \Big(\, d' \,|\, n \quad \textit{et} \quad d \,|\, \tfrac{n}{d'} \, \Big) \qquad \Longleftrightarrow \qquad \Big(\, n \,=\, d\, d'\, s \, \Big).$$

Preuve. En effet, demandons-nous si :

$$\begin{pmatrix} n \,=\, d\, r \\ \frac{n}{d} \,=\, d'\, s \end{pmatrix} \qquad \overset{?}{\Longleftrightarrow} \qquad \begin{pmatrix} n \,=\, d'\, r' \\ \frac{n}{d'} \,=\, d\, s' \end{pmatrix},$$

c'est-à-dire si :

$$\Big(\, n \,=\, d\, d'\, s \, \Big) \qquad \overset{?}{\Longleftrightarrow} \qquad \Big(\, n \,=\, d'\, d\, s' \, \Big)$$

Oui, c'est équivalent, avec $s = s'$, tout simplement ! □

On calcule alors en appliquant l'hypothèse (13.4) et cette observation :

$$\begin{aligned} \prod_{d \,|\, n} g\big(\tfrac{n}{d}\big)^{\mu(d)} \;&=\; \prod_{d \,|\, n} \prod_{d' \,|\, \frac{n}{d}} f(d')^{\mu(d)} \\ &=\; \prod_{d' \,|\, n} \prod_{d \,|\, \frac{n}{d'}} f(d')^{\mu(d)} \\ &=\; \prod_{d' \,|\, n} \Big(f(d') \Big)^{\sum\limits_{d \,|\, \frac{n}{d'}} \mu(d)}, \end{aligned}$$

puisque dans le 2ième produit à la 2ième ligne, le terme $f(d')$ est indépendant de $d \,|\, \frac{n}{d'}$.

Grâce au Théorème 13.2, la somme qui apparaît alors en exposant vaut presque toujours 0, sauf lorsque $\frac{n}{d'} = 1$, c'est-à-dire lorsque $d' = n$, où elle vaut 1. En conclusion, on a donc bien :

$$\prod_{d \,|\, n} g\big(\tfrac{n}{d}\big)^{\mu(d)} \;=\; f(n).$$ □

14. Groupes monogènes et groupes cycliques

Introduisons maintenant deux notions assez élémentaires qui vont faire ré-apparaître les seigneurs $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$, pour notre plus grand honneur.

Définition 14.1. On dit qu'un groupe G est *monogène* s'il peut être engendré par un certain élément $x_0 \in G$, c'est-à-dire si :

$$G \;=\; \big\{ x_0^i \colon \; i \in \mathbb{Z} \big\}.$$

On dit que G est *cyclique* s'il est à la fois monogène et (de cardinal) *fini*.

Deux exemples immédiats descendent des cieux éthérés le long d'une nacelle dorée.

- Le groupe $\big(\mathbb{Z}, +\big)$ est monogène, engendré par 1, mais non cyclique, car infini.
- Pour tout entier $n \geqslant 1$, le groupe $\big(\mathbb{Z}/n\mathbb{Z}, +\big)$ est cyclique, engendré par $1 \bmod n$, et d'ordre :

$$n \;=\; \mathsf{Card} \big\{ 0,\; 1,\; \ldots,\; n-1 \big\} \;\bmod n.$$

Reprenons un groupe monogène arbitraire $G = \big\{ x_0^i \colon \; i \in \mathbb{Z} \big\}$. Dans la Section **12**, nous avons déjà constaté la dichotomie suivante.

(I) Ou bien tous les éléments x_0^i avec $i \in \mathbb{Z}$ sont distincts deux à deux, auquel cas $\{x_0^i\colon\ i \in \mathbb{Z}\}$ est de cardinal *infini*.

(II) Ou bien il existe $m \geqslant 1$ tel que $x_0^m = 1_G$, et alors, si $n \geqslant 1$ est le plus petit de ces entiers, avec $x_0^n = 1_G$, on a :

$$\{x_0^i\colon\ i \in \mathbb{Z}\} \ = \ \{1_G,\, x_0,\, x_0^2,\, \ldots,\, x_0^{n-1}\},$$

tous ces éléments étant deux à deux distincts. On croirait reconnaître $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$, *démasqués !*

L'énoncé suivant confirme cette intuition, et il élucide complètement la structure des groupes monogènes.

Théorème 14.2. *Tout groupe monogène de cardinal infini est isomorphe à* $\mathbb{Z}$.
Tout groupe cyclique — i.e. *monogène fini — d'ordre* $n \geqslant 1$ *est isomorphe à* $\mathbb{Z}/n\mathbb{Z}$.

Comme deux groupes $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/n'\mathbb{Z}$ ne peuvent être isomorphes que pour $n = n'$, puisque leurs cardinaux respectifs sont n et n', on déduit que deux groupes cycliques sont isomorphes si et seulement si ils ont le même ordre (cardinal).

Démonstration. Partons donc de $G = \{x_0^i\colon\ i \in \mathbb{Z}\}$. Dans la Proposition 12.3, nous avons introduit le morphisme de groupes :

$$\begin{array}{rccc} h_{x_0}\colon & \mathbb{Z} & \longrightarrow & G \\ & i & \longmapsto & x_0^i. \end{array}$$

Puisque x_0 engendre G, ce morphisme est surjectif. Revisitons alors un raisonnement déjà présenté.

Assertion 14.3. *Le morphisme* h_{x_0} *est injectif si et seulement si* $|G| = \infty$.

Démonstration. En effet, par contraposition, h_{x_0} n'est *pas* injectif si et seulement si le sous-groupe $\mathsf{Ker}\, h_{x_0}$ de $\mathbb{Z}$ n'est *pas* réduit à $\{0\}$, et donc, $\mathsf{Ker}\, h_{x_0} = n\,\mathbb{Z}$, avec un certain entier $n \geqslant 1$, grâce à la description de *tous* les sous-groupes de $(\mathbb{Z}, +)$ offerte par le Théorème 5.6.

Ainsi, $x_0^n = 1_G$, et on a vérifié plus haut que la périodicité :

$$\cdots \ = \ x_0^{-2n} \ = \ x_0^{-n} \ = \ 1_G \ = \ x_0^n \ = \ x_0^{2n} \ = \ \cdots\,,$$

faisait s'« effondrer » l'ensemble infini des puissances de x_0 en :

$$\{x_0^i\colon\ i \in \mathbb{Z}\} \ = \ \{1_G,\, x_0,\, \ldots,\, x_0^{n-1}\},$$

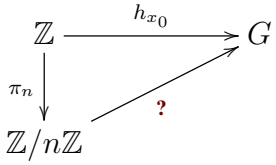
ces n éléments étant deux à deux distincts. □

Si $|G| = \infty$, alors nécessairement, le morphisme surjectif h_{x_0} doit aussi être injectif, et donc dans cette circonstance, h_{x_0} établit par définition un *isomorphisme* $\mathbb{Z} \xrightarrow{\sim} G$.

Si $|G| < \infty$, avec donc $G = \{1_G, x_0, \ldots, x_0^{n-1}\}$, en ré-introduisant la « projection » ou réduction modulo n :

$$\begin{array}{rccc} \pi_n\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & p & \longmapsto & p \ \mathsf{mod}\, n, \end{array}$$

il reste encore à construire un *isomorphisme* $\mathbb{Z}/n\mathbb{Z} \xrightarrow{?} G$:



Or si deux entiers $i \equiv i' \bmod n$ sont congrus entre eux modulo n, c'est-à-dire si $i = i' + n\,k$ avec $k \in \mathbb{Z}$, il est clair que :

$$x_0^i \;=\; x_0^{i'},$$

et donc on peut définir :

$$\begin{aligned} \overline{h}_{x_0} : \qquad \mathbb{Z}/n\mathbb{Z} \;&\longrightarrow\; G \\ i \bmod n \;&\longmapsto\; x_0^i. \end{aligned}$$

On vérifie alors aisément que c'est un morphisme de groupes :

$$\overline{h}_{x_0}\big(i \bmod n + i' \bmod n\big) \;=\; x_0^{i+i'} \;=\; x_0^i\, x_0^{i'} \;=\; \overline{h}_{x_0}\big(i \bmod n\big) + \overline{h}_{x_0}\big(i' \bmod n\big),$$

et comme $\overline{h}_{x_0}$ est bijectif par équicardinalité, c'est lui l'isomorphisme recherché $\xrightarrow{?}$. □

Théorème 14.4. *Tout groupe abstrait fini G de cardinal $|G| = p$ premier est cyclique. De plus :*

$$G \;\cong\; \mathbb{Z}/p\,\mathbb{Z}.$$

Démonstration. Puisque G est d'ordre premier $p \geqslant 2$, il contient un élément $x \neq 1_G$. Soit $\langle x \rangle \subset G$ le sous-groupe de G engendré par x. Alors il est de cardinal :

$$o(x) \;=\; \big|\langle x \rangle\big| \;\geqslant\; 2.$$

Mais par le Théorème 11.1 de Lagrange, $o(x)$ doit diviser $p = |G|$. Comme p est premier, nécessairement :

$$o(x) \;=\; p \;=\; |G|,$$

et par conséquent, ce sous-groupe doit tout remplir :

$$\langle\, x \,\rangle \;=\; \big\{1_G,\, x,\, \ldots,\, x^{p-1}\big\} \;=\; G.$$

Enfin, l'isomorphisme $G \cong \mathbb{Z}/p\mathbb{Z}$ est fourni par le Théorème 14.2 qui précède. □

Intéressons-nous maintenant aux sous-groupes quelconques d'un groupe cyclique, car ils peuvent être tous décrits.

Théorème 14.5. *Soit un groupe cyclique d'ordre $n \geqslant 1$:*

$$G \;=\; \big\{1_G,\, x_0,\, \ldots,\, x_0^{n-1}\big\}, \qquad\qquad \textit{avec } x_0^n \;=\; 1_G.$$

Alors pour tout diviseur $d \,|\, n$, il existe un unique *sous-groupe $H_d \subset G$ d'ordre (de cardinal) d, à savoir :*

$$H_d \;:=\; \Big\{1_G,\, x_0^{\frac{n}{d}},\, \ldots, x_0^{\frac{n}{d}(d-1)}\Big\}.$$

De plus, ce sous-groupe H_d coïncide avec l'ensemble H'_d défini par :

$$H_d \;=\; H'_d \;:=\; \big\{x \in G\colon\; x^d = 1_G\big\}.$$

Démonstration. Clairement, les éléments de H_d sont distincts, car H_d est visiblement un sous-ensemble de G, et car les éléments de G sont déjà distincts. Donc H_d comporte d éléments. De plus, comme :

$$x_0^{\frac{n}{d}(d-1)}\, x_0^{\frac{n}{d}} \;=\; x_0^n \;=\; 1_G,$$

H_d est cyclique.

Ensuite, il s'agit d'établir que $H_d \overset{?}{=} H'_d$.

Assertion 14.6. *On a $H'_d \subset H_d$.*

Preuve. Soit $x \in H'_d$ quelconque, c'est-à-dire avec $x^d = 1_G$. Il s'agit de montrer que $x \in H_d$. Comme $x \in G$, il existe un entier $\nu \in \{0, 1, \ldots, n-1\}$ tel que :

$$x \;=\; x_0^\nu,$$

d'où :

$$1_G \;=\; x^d \;=\; x_0^{d\,\nu},$$

et comme :

$$\big\{m \in \mathbb{Z}\colon\; x_0^m = 1_G\big\} \;=\; n\,\mathbb{Z},$$

nécessairement, on a a $n \,\big|\, d\,\nu$, grâce au Théorème 12.4 **(3)**.

Mais par hypothèse, $d \,|\, n$, donc on en déduit :

$$\tfrac{n}{d} \,\big|\, \nu, \qquad\qquad \text{c'est-à-dire} \qquad\qquad \tfrac{n}{d}\, r \;=\; \nu,$$

avec $r \in \mathbb{N}$, et ainsi nous obtenons bien :

$$x \;=\; x_0^\nu \;=\; \big(x_0^{\frac{n}{d}}\big)^r \;\in\; H_d. \qquad \square$$

Enfin, soit $H \subset G$ un sous-groupe quelconque d'ordre $|H| = d$. Le Théorème 12.6 a montré que :

$$y^d \;=\; 1_H \;=\; 1_G \qquad (\forall\, y \in H),$$

et donc :

$$H \;\subset\; H'_d \;\subset\; H_d.$$

Puisque les termes 1 et 3 sont tous deux de cardinal d, on conclut que :

$$H \;=\; H'_d \;=\; H_d. \qquad \square$$

Maintenant, les apparences sont trompeuses — comme toujours… Car tous les éléments $x \in G$ tels que $x^d = 1_G$, c'est-à-dire tous les éléments $x \in H_d$ avec $x^d = 1_G$, *ne sont pas forcément tous d'ordre d*, parce qu'il peut y avoir une puissance strictement inférieure $e < d$ telle que $x^e = 1_G$, sachant que par définition :

$$\mathsf{o}(x) \;=\; \mathsf{min}\,\big\{m \geqslant 1\colon\; x^m = 1_G\big\}.$$

Parmi les x tel que $x^d = 1_G$, on souhaite *sélectionner* seulement ceux qui sont d'ordre *exactement* égal à d — et mettre tous les autres à la poubelle ?

Théorème 14.7. *Soit G un groupe cyclique quelconque d'ordre $n \geqslant 1$:*

$$G \;=\; \big\{1_G,\, x_0,\, x_0^2,\, \ldots,\, x_0^{n-1}\big\}, \qquad\qquad \textit{avec } x_0^n \;=\; 1_G.$$

*Pour tout diviseur $d \,|\, n$, en particulier pour $d = n$, soit l'*unique *sous-groupe de G d'ordre (de cardinal) d donné par le Théorème 14.5 :*

$$\begin{aligned} H_d \,&=\, \Big\{1_G,\ x_0^{\frac{n}{d}},\ \ldots,\ x_0^{\frac{n}{d}(d-1)}\Big\}, \qquad\qquad \textit{avec } \big(x_0^{\frac{n}{d}}\big)^d \,=\, 1_G, \\ &=\, \big\{x \in G\colon\ x^d = 1_G\big\}. \end{aligned}$$

Alors l'ensemble des éléments $x \in G$ dont l'ordre est exactement égal à d est le sous-ensemble suivant de H_d :

$$\big\{x \in G\colon\ \mathsf{Card}\,\langle\, x\,\rangle = d\big\} \;=\; \Big\{x_0^{\frac{n}{d}c}\colon\ 1 \leqslant c \leqslant d-1 \textit{ avec } c \wedge d = 1\Big\}.$$

Pour $d = 1$, on convient que cet ensemble est réduit à $\{1_G\}$. Parmi les d éléments de H_d, il y a donc autant d'éléments qui sont d'ordre d dans G qu'il y a d'entiers $1 \leqslant c \leqslant d$ premiers avec d.

Intuitivement, pour qui a bien assimilé le cours d'arithmétique, ce théorème semble immédiat, car en posant :

$$x_1 \,:=\, x_0^{\frac{n}{d}},$$

de telle sorte que :

$$H_d \,=\, \big\{1_G,\, x_1,\, x_1^2,\, \ldots,\, x_1^{d-1}\big\}, \qquad\qquad \text{avec } x_1^d \,=\, 1_G,$$

nous pouvons envisager que H_d s'*identifie*[15] au groupe concret bien connu :

$$\big(\mathbb{Z}/n\mathbb{Z},\, +\big) \,=\, \big\{0,\, 1,\, 2,\, \ldots,\, d-1\big\} \ \mathsf{mod}\, d,$$

et alors, pour tout élément $0 \leqslant c \leqslant d-1$ dans ce groupe que l'on itère un nombre quelconque $e \geqslant 1$ de fois :

$$\underbrace{c + \cdots + c}_{e \text{ fois}} \,=\, e\,c,$$

la caractérisation du fait que c est d'ordre exactement égal à d dans $\big(\mathbb{Z}/n\mathbb{Z}, +\big)$ devient transparente grâce aux théorèmes connus d'arithmétique :

$$\Big(\ e\,c \,\equiv\, 0 \ \mathsf{mod}\, d \quad\Longrightarrow\quad e \,\equiv\, 0 \ \mathsf{mod}\, d\ \Big) \qquad\Longleftrightarrow\qquad c \wedge d \,=\, 1.$$

Toutefois, malgré le caractère essentiellement « évident » de ce théorème, nous allons constater que sa démonstration effective va mobiliser simultanément plusieurs théorèmes que nous avons démontrés auparavant.

Démonstration. Soit $x \in G = \langle x_0 \rangle$ d'ordre exactement égal à $d = |\langle x \rangle|$. Avec $H := \langle x \rangle$, rappelons que le Théorème 12.6 a montré que $x^d = 1_G$, et donc :

$$\begin{aligned} x \,&\in\, \big\{x \in G\colon\ x^d = 1_G\big\} \\ &=\, \Big\{1_G,\, x_0^{\frac{n}{d}},\, \ldots,\, x_0^{\frac{n}{d}(d-1)}\Big\}. \end{aligned} \qquad \text{[Théorème 14.5]}$$

Pour $d = 1$, il y a $\varphi(1) = 1$ élément d'ordre 1, à savoir l'élément neutre 1_G. Donc on peut supposer que $d \geqslant 2$ et alors, $x \neq 1_G$. Ainsi, il existe un entier $1 \leqslant c \leqslant d-1$ tel que :

$$x \,=\, x_0^{\frac{n}{d}c}.$$

15. — et d'ailleurs, le Théorème 14.2 a déjà justifié l'existence d'une telle *identification*, qui est même un *isomorphisme* —

Grâce au Théorème 12.7, nous obtenons que :

$$\begin{aligned} \boldsymbol{o}(x) &= \boldsymbol{o}\left(\left(x_0^{\frac{n}{d}}\right)^c\right) \\ &= \frac{\boldsymbol{o}(x_0^{\frac{n}{d}})}{\mathsf{pgcd}\left(c,\, \boldsymbol{o}(x_0^{\frac{n}{d}})\right)} \\ &= \frac{d}{\mathsf{pgcd}\,(c,d)}, \end{aligned}$$

et ainsi, $\boldsymbol{o}(x)$ est égal à d si et seulement si c et d sont premiers entre eux. □

Nous achevons cette section en étudiant à nouveau la fonction indicatrice d'Euler :

$$\varphi(n) \,:=\, \mathsf{Card}\left\{1 \leqslant \nu \leqslant n\colon\ \nu \wedge n = 1\right\}.$$

Théorème 14.8. *Pour tout $n \geqslant 2$, si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ est la décomposition de n en facteurs premiers, alors on a :*

$$\begin{aligned} \varphi(n) &= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ &= \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdots \left(p_r^{\alpha_r} - p_r^{\alpha_r - 1}\right). \end{aligned}$$

Dans le chapitre consacré à l'arithmétique sur $\mathbb{Z}$, nous avons déjà vu cette formule, et ici, nous allons en donner une seconde démonstration, basée sur la très belle formule d'inversion de Möbius.

Démonstration. En regroupant les éléments de G selon leur ordre, on obtient l'égalité :

$$n \,=\, \sum_{d\,|\,n} \varphi(d),$$

et cette égalité est valable pour tout entier $n \geqslant 1$.

Ensuite, grâce à la formule d'inversion de Möbius, *i.e.* grâce au Théorème 13.3, on a alors, pour tout $n \geqslant 1$:

$$\begin{aligned} \varphi(n) &= \sum_{d\,|\,n} \mu(d)\, \frac{n}{d} \\ &= n \sum_{d\,|\,n} \frac{\mu(d)}{d}. \end{aligned}$$

Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ est la décomposition en facteurs premiers de n, et si I décrit la collection de tous les sous-ensembles de $\{1, \ldots, r\}$, il vient donc :

$$\varphi(n) \,=\, n \sum_{\mathrm{I} \subset \{1,\ldots,r\}} \frac{(-1)^{\mathrm{I}}}{p_{\mathrm{I}}},$$

où :

$$p_{\mathrm{I}} \,:=\, \prod_{i \in \mathrm{I}} p_i.$$

Or cette somme $\sum_{\mathrm{I}} \frac{(-1)^{\mathrm{I}}}{p_{\mathrm{I}}}$ n'est rien d'autre que ce que l'on obtient en développant le produit :

$$\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right),$$

car pour écrire un terme quelconque du développement de ce produit, il faut et il suffit de déterminer dans quels facteurs on choisit un terme « $-\frac{1}{p_i}$ », ce qui revient à choisir une partie $\mathrm{I} \subset \{1, \dots, r\}$.

En conclusion, nous obtenons bien la formule annoncée :

$$\varphi(n) \;=\; n\Big(1-\frac{1}{p_1}\Big)\cdots\Big(1-\frac{1}{p_r}\Big) \;=\; \big(p_1^{\alpha_1}-p_1^{\alpha_1-1}\big)\cdots\big(p_r^{\alpha_r}-p_r^{\alpha_r-1}\big). \qquad \square$$

15. Groupes quotients

Soit G un groupe abstrait, et soit $H \subset G$ un sous-groupe. Rappelons que la Proposition 9.1 a défini une relation d'équivalence sur G de la manière suivante, pour $x, y \in G$ quelconques :

$$x \sim y \quad \text{si} \quad x^{-1}y \in H.$$

Les classes d'équivalence pour cette relation sont les *classes à gauche modulo* H.

Autrement dit, pour tout $x \in G$, on a :

$$\overline{x} \;=\; x\,H \;=\; \big\{x\,h\colon\; h \in H\big\}.$$

On note alors G/H l'ensemble de ces classes d'équivalence. Les éléments de l'ensemble G/H sont donc des *parties* — des *sous-ensembles* — de G, ce ne sont *pas* des éléments de G.

On a alors une application surjective canonique :

$$\begin{array}{rccc} \pi\colon & G & \longrightarrow & G/H \\ & x & \longmapsto & \overline{x}. \end{array}$$

Évidemment, on est « tenté » de définir une structure de groupe sur G/H, de manière à ce que cette projection canonique $\pi\colon G \longrightarrow G/H$ soit un morphisme de groupes. La seule façon naturelle de faire cela serait de définir une loi de groupe $*$ sur G/H par :

$$\overline{x} * \overline{y} \;:=\; \overline{x\,y},$$

pour tous $x, y \in G$, ce qui traduirait exactement ce que l'on désire. Et d'ailleurs, immédiatement, on supprimerait le symbole $*$ et on écrirait simplement :

$$\overline{x}\,\overline{y} \;:=\; \overline{x\,y} \qquad (\forall\, x, y \in G).$$

Malheureusement, rien ne nous dit qu'une telle loi soit bien définie…

En fait, la difficulté cachée est que le résultat ne doit pas dépendre des éléments choisis pour représenter les classes d'équivalence de x et de y. Autrement dit, on doit vérifier que si $\overline{x}_1 = \overline{x}_2$ et $\overline{y}_1 = \overline{y}_2$, alors on a $\overline{x_1\,y_1} = \overline{x_2\,y_2}$. Ce n'est pas toujours vrai, comme le montre le contre-exemple suivant.

Exemple 15.1. Soit $G := \mathfrak{S}_3$ le groupe des bijections de $\{1, 2, 3\}$ dans lui-même, qui, d'après le Théorème 2.12, est constitué des $3! = 6$ applications :

$$\begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{array}$$

que l'on écrira dorénavant sans flèches, mais avec des grandes parenthèses.

Introduisons [16] :

$$x_1 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad x_2 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad y_1 := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$y_2 := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = y_1,$$

puis abrégeons :

$$x_1 =: \tau_{1,3}, \qquad x_2 =: \tau_{1,3} \circ \tau_{1,2}, \qquad y_1 =: \tau_{2,3}, \qquad y_2 =: \tau_{2,3} = y_1.$$

Observons que la bijection $\tau_{1,2}$ qui échange $1 \longleftrightarrow 2$ en laissant 3 fixé est sa propre inverse :

$$\tau_{1,2} \circ \tau_{1,2} = 1_G,$$

et donc, le sous-groupe monogène $H \subset G = \mathfrak{S}_3$ qu'elle engendre est réduit à deux éléments :

$$H := \langle \tau_{1,2} \rangle = \{1_G, \tau_{1,2}\}.$$

Avec ces notations, on constate alors que :

$$x_1^{-1} x_2 = \underline{\tau_{1,3}^{-1} \circ \tau_{1,3}} \circ \tau_{1,2} = \tau_{1,2} \in H,$$

ce qui veut dire :

$$x_1 \sim x_2, \qquad \text{d'où} \qquad \overline{x}_1 = \overline{x}_2.$$

Trivialement, puisque $y_1 = y_2$, on a aussi :

$$y_1 \sim y_2, \qquad \text{d'où} \qquad \overline{y}_1 = \overline{y}_2.$$

Mais en revanche, les deux produits (compositions) :

$$x_1\, y_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad x_2\, y_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau_{1,2} \in H,$$

ne sont *pas* égaux modulo H, puisque le premier n'appartient pas à H, tandis que le second est dans H, donc :

$$\big(x_1\, y_1\big)^{-1} x_2\, y_2 \in H$$

serait absurde [17], car ceci impliquerait $x_1\, y_1 \in H$, ce qui n'est pas.

En conclusion, cet exemple assez élémentaire nous a convaincu que l'équivalence $\sim$ à gauche modulo H n'est en général *pas* compatible avec la loi de groupe :

$$\Big(x_1 \sim x_2 \quad \text{et} \quad y_1 \sim y_2 \Big) \qquad \overset{\text{Faux}}{\Longrightarrow} \qquad \Big(x_1\, y_1 \sim x_2\, y_2 \Big).$$

16. L'élément x_2 est une *composition* de deux bijections. Pour lire l'image de 1, on commence à droite, on voit que 1 est envoyé sur 2 par $\tau_{1,2}$, puis à gauche, on voit que 2 est envoyé sur 2 par $\tau_{1,3}$, donc au final 1 est envoyé sur 2 par $\tau_{1,3} \circ \tau_{1,2}$, comme l'exprime la première colonne de la deuxième ligne. Ensuite, $2 \longmapsto 1$, puis $1 \longmapsto 3$, c'est-à-dire $2 \longmapsto 3$, comme l'exprime la deuxième colonne ; et ainsi de suite.

17. En effet, $a^{-1}\, b \in H$ avec $b \in H$ implique :

$$a^{-1}\, b\, b^{-1} \in H\, b^{-1} = H,$$

c'est-à-dire $a^{-1} \in H$, et enfin $a \in H$ puisque H est un groupe, donc est stable par inversion.

Un contre-exemple similaire peut être construit concernant l'équivalence à droite modulo H.

Examinons le problème d'un peu plus près. Supposons que la loi interne :

$$\begin{array}{rcl} G/H \times G/H & \longrightarrow & G/H \\ \big(\overline{x}, \overline{y}\big) & \longmapsto & \overline{x\,y}, \end{array}$$

soit bien définie. Dans ce cas, on a, pour tout $g \in G$:

$$\overline{g} \;=\; \overline{1_G\, g} \;=\; \overline{1}_G\, \overline{g},$$

Mais pour tout $h \in H$, on a $\overline{1}_G = \overline{h}$ par définition de l'ensemble $G\big/H$, et ainsi, on obtient :

$$\overline{g} \;=\; \overline{h}\,\overline{g} \;=\; \overline{h\,g} \qquad (\forall\, g \in G,\, \forall\, h \in H).$$

Par définition de la relation de congruence modulo H, cela revient à dire :

$$g^{-1}\, h\, g \;\in\; H \qquad (\forall\, g \in G,\, \forall\, h \in H).$$

Mais puisque le passage à l'inverse $(\bullet)^{-1}$ induit une bijection de G sur lui-même, en remplaçant alors g par g^{-1} dans ce que nous venons d'obtenir, nous constatons que cela équivaut finalement à :

$$g\, h\, g^{-1} \qquad (\forall\, g \in G,\, \forall\, h \in H).$$

Autrement dit, *le sous-groupe $H \subset G$ est nécessairement distingué dans G.*

Cela explique d'ailleurs l'Exemple 15.1, puisque le groupe $H = \langle \tau_{1,2} \rangle$ engendré par $\tau_{1,2}$ n'était pas distingué dans $\mathfrak{S}_3 = G$, comme nous nous proposons de le vérifier maintenant.

En effet, soient :

$$h \;:=\; \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad\qquad g \;:=\; \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \;=\; g^{-1} \;\notin\; H.$$

Alors on calcule verticalement, du haut vers le bas, sans les grandes parenthèses :

$$\begin{array}{cccc} & 1 & 2 & 3 \\ g^{-1} & 3 & 2 & 1 \\ h & 3 & 1 & 2 \\ g & 1 & 3 & 2 \end{array}$$

ce qui nous donne une permutation qui n'appartient *pas* à H :

$$g\, h\, g^{-1} \;=\; \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \;\notin\; H.$$

L'énoncé suivant montre que, réciproquement, si H est un sous-groupe *distingué* de G, on peut munir G/H d'une structure naturelle de groupe jouissant des propriétés désirées.

Théorème 15.2. *Soit H un sous-groupe* distingué *d'un groupe G. Alors la loi interne sur G/H définie par :*

$$\begin{array}{rcl} G/H \times G/H & \longrightarrow & G/H \\ \big(\overline{x}, \overline{y}\big) & \longmapsto & \overline{x\,y}, \end{array}$$

est bien définie, d'élément neutre $\overline{1}_G$, et elle induit sur G/H une structure de groupe.

De plus, l'application de « projection » :

$$\begin{array}{rccl} \pi\colon & G & \longrightarrow & G/H \\ & x & \longmapsto & \overline{x}, \end{array}$$

est un morphisme de groupes.

Démonstration. Vérifions que si $\overline{x}_1 = \overline{x}_2$ et si $\overline{y}_1 = \overline{y}_2$, alors $\overline{x_1\, y_1} = \overline{x_2\, y_2}$.

Par définition de la relation d'équivalence, il existe $h, h' \in H$ tels que :

$$x_2 \,=\, x_1\, h, \qquad\qquad\qquad y_2 \,=\, y_1\, y',$$

d'où :

$$\begin{aligned} x_2\, y_2 \;&=\; x_1\, h\, y_1\, h' \\ &=\; x_1\, y_1\, \underbrace{\big(y_1^{-1}\, h\, y_1\big)\, h'}_{=:\, h''}. \end{aligned}$$

Ici entre parenthèses, comme H est un sous-groupe *distingué* de G par hypothèse, on a, et c'est crucial :

$$y_1^{-1}\, h\, y_1 \;\in\; H,$$

et donc l'élément h'' souligné ci-dessus appartient à H, c'est-à-dire :

$$x_2\, y_2 \;=\; x_1\, y_1\, h'',$$

et par conséquent on a bien démontré que :

$$\overline{x_2\, y_2} \;=\; \overline{x_1\, y_1}.$$

Ainsi, l'application suivante introduite dans l'énoncé du théorème :

$$\begin{array}{rcl} G/H \times G/H & \longrightarrow & G/H \\ \big(\overline{x}, \overline{y}\big) & \longmapsto & \overline{x\, y}, \end{array}$$

est bien définie, et plus encore, elle permet de *définir une loi de groupe sur* G/H par :

$$\overline{x} * \overline{y} \;:=\; \overline{x\, y}.$$

Dans la suite, cette étoile sera éludée, filante.

Vérifions maintenant que G/H, muni de cette loi, est bien un *groupe*.

Pour tout $\overline{x} \in G/H$, on a :

$$\overline{1}_G\, \overline{x} \;=\; \overline{1_G\, x} \;=\; \overline{x},$$

et de même, $\overline{x}\, \overline{1}_G = \overline{x}$. Donc $\overline{1}_G$ est un élément neutre pour cette loi.

De plus, la loi est associative. En effet, pour tous $\overline{x}, \overline{y}, \overline{z} \in G/H$ on a :

$$\big(\overline{x}\, \overline{y}\big)\, \overline{z} \;=\; \overline{x\, y}\, \overline{z} \;=\; \overline{(x\, y)\, z} \;=\; \overline{x\, (y\, z)} \;=\; \overline{x}\, \overline{y\, z} \;=\; \overline{x}\, \big(\overline{y}\, \overline{z}\big).$$

Enfin, on vérifie facilement que tout $\overline{x} \in G/H$ admet un inverse naturel, la classe à gauche $\overline{x^{-1}}$ de l'inverse de x dans G.

Le fait que π soit un morphisme de groupes provient alors tautologiquement de la définition de la loi de groupe sur G/H. □

Définition 15.3. Soit G un groupe, et soit $H \triangleleft G$ un sous-groupe distingué de G. Le groupe G/H est appelé le *groupe quotient* de G par H.

Une chose importante à retenir de cette définition, outre la définition de la loi de groupe, c'est que pour tout $x \in G$, on a :

$$\overline{x} \;=\; \overline{1}_G \qquad\qquad \Longleftrightarrow \qquad\qquad x \;\in\; H.$$

Si l'indice $[G : H]$ est fini, G/H est d'ordre (de cardinal) $[G : H]$ par définition. En particulier, si G est fini, par le Théorème 11.1 de Lagrange, on a :

$$[G : H] \;=\; \frac{|G|}{|H|}.$$

Si G est commutatif, tout sous-groupe $H \subset G$ est distingué dans G, et l'on peut donc toujours gratuitement former des groupes quotients G/H.

La projection canonique $\pi\colon G \longrightarrow H$ est surjective, de noyau H. Ainsi, tout sous-groupe distingué de G s'identifie-t-il au *noyau* d'un certain morphisme de groupes.

Quel est l'intérêt d'un groupe quotient ? En fait, quotienter G par un sous-groupe distingué H revient à imposer des relations entre les éléments du groupe G, qui n'existent pas forcément. En un sens, on « force » les éléments de H à devenir triviaux.

Par exemple, on a $G/G = \{\overline{1}_G\}$: tout devient trivial ! En effet, tous les éléments sont équivalents dans ce cas. En fait, le groupe G/H est trivial si et seulement si $H = G$.

Autre exemple : on a $G \cong G\big/\{1_G\}$, l'isomorphisme étant donné par la projection canonique. En effet, on a $\overline{x} = \{x\}$, pour tout $x \in G$. La projection canonique est donc bien un isomorphisme. Mais attention ! On a un isomorphisme, pas une égalité.

Enfin le plus bel exemple :

Observation 15.4. *Le groupe $\mathbb{Z}\big/n\mathbb{Z}$ n'est autre que le quotient de $\mathbb{Z}$ par son sous-groupe $n\,\mathbb{Z}$.* □

16. Théorème de factorisation

Soit G un groupe, et soit $H \subset G$ un sous-groupe distingué. Le résultat suivant explique à quoi ressemblent les morphismes de G/H à valeurs dans un autre groupe quelconque G'.

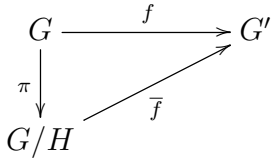
Théorème 16.1. [de factorisation] *Soit G un groupe, et soit H un sous-groupe distingué de G. Soit $f\colon G \longrightarrow G'$ un morphisme de groupes tel que $H \subset \mathsf{Ker}\, f$. Alors il existe un unique morphisme de groupes :*

$$\overline{f}\colon \quad G/H \;\longrightarrow\; G',$$

qui satisfait :

$$f \;=\; \overline{f} \circ \pi,$$

c'est-à-dire qui rend commutatif le diagramme suivant :



De plus, pour tout groupe G', il y a une correspondance bijective :

$$\begin{array}{rcl} \mathsf{Hom}\left(G/H,\, G'\right) & \longrightarrow & \Big\{ f \in \mathsf{Hom}(G, G') \colon\; H \subset \mathsf{Ker}\, f \Big\} \\ \varphi & \longmapsto & \varphi \circ \pi \\ \overline{f} & \longleftarrow\!\shortmid & f \end{array}$$

Démonstration. Remarquons tout d'abord qu'un morphisme $f\colon G \longrightarrow G'$ est constant sur les classes d'équivalence, pour la relation associée à H, si et seulement si $H \subset \mathsf{Ker}\, f$.

En effet, si $H \subset \mathsf{Ker}\, f$, alors pour tout $x \in G$ et tout $h \in H$, on a :

$$f(x\,h) \;=\; f(x)\,f(h) \;=\; f(x).$$

Réciproquement, si le morphisme f est constant sur chaque classe d'équivalence, il est constant sur H. Mais H contient 1_G, et l'on a donc pour tout $h \in H$:

$$f(h) \;=\; f(1_G) \;=\; 1_{G'},$$

c'est-à-dire $H \subset \mathsf{Ker}\, f$.

Comme f est constant sur les classes d'équivalence, un raisonnement ensembliste évident fournit alors l'existence et l'unicité d'une application $\overline{f}$ vérifiant les propriétés voulues. De plus, pour tous $x_1, x_2 \in G$, on a :

$$\overline{f}\big(\overline{x}_1\,\overline{x}_2\big) \;=\; \overline{f}\big(\overline{x_1\,x_2}\big) \;=\; f(x_1\,x_2) \;=\; f(x_1)\,f(x_2) \;=\; \overline{f}(\overline{x}_1)\,\overline{f}(\overline{x}_2),$$

et $\overline{f}$ est donc un morphisme de groupes.

Ensuite, démontrons la seconde partie. Un raisonnement ensembliste évident montre qu'il y a une bijection entre l'ensemble des applications de G/H dans G', et l'ensemble des applications $G \longrightarrow G'$ qui sont constantes sur les classes d'équivalences. Cette bijection est donnée par :

$$\begin{array}{ccc} \varphi & \longmapsto & \varphi \circ \pi \\ \overline{f} & \longleftarrow\!\shortmid & f. \end{array}$$

Si maintenant φ est un morphisme de groupes, alors $\varphi \circ \pi$ est un morphisme dont le noyau contient H. De plus, si f est un morphisme de groupes, alors $\overline{f}$ est un morphisme de groupes.

Ainsi, la correspondance se restreint pour définir une bijection entre les ensembles voulus. Cela achève la démonstration. □

En particulier, on a un énoncé significatif qui est un simple corollaire du théorème précédent.

Théorème 16.2. *Tout morphisme de groupes $f\colon G \longrightarrow G'$ induit un morphisme de groupes :*

$$\overline{f}\colon \quad G\big/\mathsf{Ker}\, f \quad\longrightarrow\quad G'.$$

Preuve. En effet, $H := \mathsf{Ker}\, f$ est un sous-groupe distingué de $G\ldots$ qui contient $\mathsf{Ker}\, f$. □

Au vu de la définition d'un groupe quotient, on peut s'attendre à ce que cette application soit injective, puisque l'on « tue » tous les éléments du noyau. Et c'est bien le cas !

Théorème 16.3. *Soit $f\colon G \longrightarrow G'$ un morphisme de groupes. Alors le morphisme de groupes :*

$$\overline{f}\colon \quad G\big/\mathsf{Ker}\, f \quad\longrightarrow\quad G'$$

est injectif.

Démonstration. Soit $\overline{x} \in G/\mathsf{Ker}\, f$. On a $\overline{f}(\overline{x}) = 1_{G'}$ si et seulement si on a $f(x) = 1_{G'}$, c'est-à-dire si et seulement si $x \in \mathsf{Ker}\, f$, ce qui revient encore à dire que :

$$\overline{x} \;=\; \overline{1}_G \;\in\; G\big/\mathsf{Ker}\, f.$$

Ainsi, $\mathsf{Ker}\,\overline{f}$ est réduit à l'élément neutre, et $\overline{f}$ est bien injective. □

Nous pouvons terminer cette section par un énoncé fondamental.

Théorème 16.4. [d'isomorphisme] *Soient G et G' deux groupes, et soit $f\colon G \longrightarrow G'$ un morphisme de groupes. Alors le morphisme de groupes :*

$$\overline{f}\colon \quad G\big/\mathsf{Ker}\, f \quad \longrightarrow \quad G',$$

induit un isomorphisme de groupes :

$$G\big/\mathsf{Ker}\, f \;\cong\; \mathsf{Im}\, f.$$

Démonstration. D'après le théorème qui précède, $\overline{f}\colon G\big/\mathsf{Ker}\, f \longrightarrow G'$ est un morphisme injectif, qui induit donc un isomorphisme de $G\big/\mathsf{Ker}\, f$ sur son image. Enfin, on a :

$$\begin{aligned}\mathsf{Im}\,\overline{f} \;&=\; \Big\{\overline{f}(\overline{x})\colon\ \overline{x} \in G\big/\mathsf{Ker}\, f\Big\}\\ &=\; \big\{f(x)\colon\ x \in G\big\}\\ &=\; \mathsf{Im}\, f.\end{aligned}$$

□

Ce dernier théorème permet en pratique d'identifier un groupe quotient G/H à un groupe connu de la manière suivante. On essaye d'identifier H au noyau d'un certain morphisme de groupes $f\colon G \longrightarrow G'$ bien choisi, et on calcule l'image de f — en pratique, on essaye même de trouver un f qui soit de plus surjectif.

Exemples 16.5. (1) Identifions le quotient $\mathbb{C}^\times\big/\mathbb{U}$, où :

$$\mathbb{U} \;:=\; \big\{z \in \mathbb{C}^\times\colon\ |z| = 1\big\},$$

est le cercle unité dans $\mathbb{C}$, et considérons l'application :

$$\begin{aligned} f\colon \quad \mathbb{C}^\times \quad &\longrightarrow \quad \mathbb{R}_+^\times\\ z \quad &\longmapsto \quad |z|,\end{aligned}$$

qui est un morphisme de groupes surjectif, de noyau $\mathbb{U}$, donc le Théorème 16.4 nous donne :

$$\mathbb{C}^\times\big/\mathbb{U} \;\cong\; \mathbb{R}_+^\times.$$

(2) Nous pouvons identifier $\mathbb{U}$ à $\mathbb{R}\big/2\pi\mathbb{Z}$ au moyen du morphisme de groupes surjectif :

$$\begin{aligned} f\colon \quad \mathbb{R} \quad &\longrightarrow \quad \mathbb{U}\\ \theta \quad &\longmapsto \quad e^{i\theta},\end{aligned}$$

car le noyau de ce morphisme est égal à $2\pi\,\mathbb{Z}$, donc on obtient bien :

$$\mathbb{R}\big/2\pi\mathbb{Z} \;\cong\; \mathbb{U}.$$

17. Exercices

Exercice 1. (a) Pour un entier $n \geqslant 1$ quelconque, montrer que l'application déterminant :

$$\begin{aligned} \mathsf{GL}_n(\mathbb{R}) \quad &\longrightarrow \quad \mathbb{R}^*\\ M \quad &\longmapsto \quad \det M,\end{aligned}$$

est un morphisme de groupes.

(b) Montrer que son extension à l'ensemble $\mathscr{M}_{n\times n}(\mathbb{R})$ de toutes les matrices — y compris celles qui ne sont pas inversibles — n'est *pas* un morphisme de groupes.

Exercice 2. Soit G un groupe, et soit $H \subset G$ un sous-groupe, qui est engendré par une partie $P \subset G$. Montrer que H est distingué dans G si et seulement si, pour tout $x \in P$ et tout $g \in G$, on a $g\,x\,g^{-1} \in H$ aussi.

Exercice 3. **

Exercice 4. EE

Exercice 5. EE

Groupes symétriques

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Introduction

Ce chapitre est consacré à l'étude de certains groupes *non* commutatifs très naturels, dits *groupes symétriques*, qui interviennent partout dans la vie mathématique, ainsi que dans la vie non mathématique — y compris en physique.

Par exemple, l'adolescent blême qui au petit matin dans les frimas d'un jour brumeux d'automne, secoue le panier des noix sonores et noires qu'il vient de ramasser sous le noyer géant de son enfance, fait agir, sans le savoir, ce fameux *groupe symétrique*.

Car les mathématiques existent partout et depuis toujours, sous le ciel noir constellé d'étoiles et de galaxies, depuis l'enfance de l'univers.

2. Définitions et premières propriétés du groupe symétrique

Soit un ensemble *fini*, c'est-à-dire de cardinal $|E| < \infty$.

Définition 2.1. La collection des *bijections* de E dans lui-même :

$$\mathfrak{S}(E) := \big\{\sigma\colon\ E \longrightarrow E \text{ bijective}\big\},$$

qui est un *groupe* pour la loi de composition $* = \circ$ des applications bijectives, est appelée *groupe des permutations de* E, ou *groupe symétrique sur* E.

Un élément de $\mathfrak{S}(E)$ est appelé une *permutation* de E.

L'exemple canonique d'ensemble de cardinal fini quelconque est l'ensemble :

$$\big\{1,\, 2,\, 3,\, \ldots,\, n\big\},$$

des n premiers entiers naturels. Au lieu de $\mathfrak{S}\big(\{1,\ldots,n\}\big)$, on note alors :

$$\mathfrak{S}_n := \Big\{\sigma\colon\ \{1,\ldots,n\} \longrightarrow \{1,\ldots,n\} \text{ bijective}\Big\}.$$

Une permutation $\sigma \in \mathfrak{S}_n$ sera notée :

$$\sigma \quad \begin{array}{cccc} 1 & 2 & \cdots & n \\ \downarrow & \downarrow & \cdots & \downarrow \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{array} \qquad \text{ou} \qquad \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}.$$

Par exemple :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix}.$$

Tout au long des paragraphes qui suivront, nous continuerons à analyser ce même exemple, dont les caractéristiques heuristiques se dévoileront à nous de manière de plus en plus *séduisante*.

Proposition 2.2. *Si deux ensembles finis $E \overset{\sim}{\longleftrightarrow} E'$ sont en bijection, alors leurs groupes de permutations sont isomorphes :*

$$\mathfrak{S}(E) \;\cong\; \mathfrak{S}(E').$$

Démonstration. Supposons donc l'existence d'une bijection $f\colon E \longrightarrow E'$, de bijection inverse $E \longleftarrow E' : f^{-1}$, et dressons un diagramme de composition :

$$\begin{array}{ccc} E & \xrightarrow{\;\sigma\;} & E \\ {\scriptstyle f^{-1}}\uparrow & & \downarrow{\scriptstyle f} \\ E' & \xrightarrow[f\circ\sigma\circ f^{-1}]{} & E'. \end{array}$$

En s'aidant de ce diagramme, on vérifie alors que l'application :

$$\begin{array}{rcl} \mathfrak{S}(E) & \longrightarrow & \mathfrak{S}(E') \\ \sigma & \longmapsto & f\circ\sigma\circ f^{-1} \;=:\; \sigma', \end{array}$$

est un *isomorphisme* de groupes.

Les détails sont laissés au lecteur-étudiant [1] notamment la vérification du fait que l'isomorphisme inverse s'écrit :

$$f^{-1}\circ\sigma'\circ f \;\longleftarrow\!\shortmid\; \sigma'. \qquad \square$$

Toujours avec E de cardinal fini, considérons le cas particulier simple et concret où $E' := \{1,\dots,n\}$, avec $n := |E|$. Une bijection f^{-1} de $\{1,\dots,n\}$ à valeurs dans E s'identifie alors à une *numérotation* des n éléments de E :

$$\begin{array}{rcll} E & \longleftarrow & \{1,\dots,n\} & : f^{-1} \\ a_i \;:=\; f^{-1}(i) & \longleftarrow\!\shortmid & i, & \end{array}$$

que l'on note alors $\{a_1,\dots,a_n\} = E$.

Par conséquent, l'isomorphisme (inverse) de groupes de la Proposition 2.2 s'écrit :

$$\begin{array}{rcl} \mathfrak{S}(E) & \overset{\sim}{\longleftarrow} & \mathfrak{S}_n \\ f^{-1}\circ\tau\circ f & \longleftarrow\!\shortmid & \tau. \end{array}$$

Enfin, si $\tau \in \mathfrak{S}_n$ est une permutation quelconque, on voit que :

$$f^{-1}\big(\tau(f(a_i))\big) \;=\; f^{-1}\big(\tau(i)\big) \;=\; a_{\tau(i)},$$

ce qui signifie qu'après avoir effectué une numérotation des éléments de E, en éliminant les symboles de numérotation f^{-1} et f, la permutation considérée s'exprime tout simplement au niveau des indices, comme un changement de la place des noix dans notre panier :

$$\big(a_1,\, a_2,\, \dots,\, a_n\big) \;\longmapsto\; \big(a_{\tau(1)},\, a_{\tau(2)},\, \dots,\, a_{\tau(n)}\big).$$

1. En fait, voici « les » détails :

$$\big(f\circ\sigma_1\circ f^{-1}\big)\circ\big(f\circ\sigma_2\circ f^{-1}\big) \;=\; f\circ\sigma_1\circ\sigma_2\circ f^{-1}.$$

Ainsi, l'objectif de ce chapitre est d'étudier les groupes $\mathfrak{S}(E)$, lorsque $|E| < \infty$. Au vu de ces considérations, on peut se restreindre à l'étude du groupe $\mathfrak{S}_n$, ce que nous ferons parfois, mais pas toujours. Rappelons et re-démontrons le

Théorème 2.3. *Si E est un ensemble fini à $n \geqslant 1$ éléments, alors $\mathfrak{S}(E)$ est un groupe fini d'ordre (de cardinal) égal à la factorielle $n!$*

Démonstration. Donc on suppose $E = \{1, \ldots, n\}$. Il s'agit de compter combien de permutations de cet ensemble $\{1, \ldots, n\}$ sont possibles.

Or se donner une permutation de $\{1, \ldots, n\}$ revient à se donner n entiers $\tau(1), \ldots, \tau(n)$ distincts deux à deux et tous contenus dans $\{1, \ldots, n\}$.

Donc au début, il y a n choix possibles pour $\tau(1)$. Une fois $\tau(1)$ choisi, il n'y a plus que $n-1$ choix possibles pour $\tau(2)$, puis $n-2$ choix possibles pour $\tau(3)$, et ainsi de suite, jusqu'à ce qu'il n'y ait plus qu'un seul choix possible pour $\tau(n)$.

Au total, il y a donc précisément :

$$n\,(n-1)\,(n-2)\,\cdots\,1 \;=\; n!,$$

permutations possibles de l'ensemble $\{1, \ldots, n\}$. □

Rappelons aussi que le groupe $\mathfrak{S}_n$ n'est *jamais* commutatif dès que $n \geqslant 3$ — c'est-à-dire la plupart du temps !

En effet, dans le chapitre précédent, nous avons exhibé les deux petites babioles suivantes qui ne commutent pas entre elles :

$$\begin{array}{cccc} & 1 & 2 & 3 \\ \tau & \downarrow & \downarrow & \downarrow \\ & 1 & 3 & 2 \\ \sigma & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 \end{array} \qquad \text{diffère de} \qquad \begin{array}{cccc} & 1 & 2 & 3 \\ \sigma & \downarrow & \downarrow & \downarrow \\ & 2 & 1 & 3 \\ \tau & \downarrow & \downarrow & \downarrow \\ & 3 & 1 & 2 \end{array} .$$

Comme précédemment, on travaille avec un ensemble E fini.

Définition 2.4. L'ensemble des *points fixes* d'une permutation $\sigma \in \mathfrak{S}(E)$ est :

$$\mathsf{Fix}\,\sigma \;:=\; \big\{a \in E\colon\ \sigma(a) = a\big\},$$

tandis que le *support* de σ est l'ensemble des éléments de E qui sont réellement déplacés par σ :

$$\mathsf{Supp}\,\sigma \;:=\; \big\{a \in E\colon\ \sigma(a) \neq a\big\}.$$

Ainsi, l'ensemble total E se décompose comme réunion *disjointe :*

$$E \;=\; \mathsf{Fix}\,\sigma \cup \mathsf{Supp}\,\sigma.$$

Il est clair que $\sigma = \mathsf{Id}$ est l'identité si et seulement si $\mathsf{Fix}\,\sigma = E$, si et seulement si $\mathsf{Supp}\,\sigma = \emptyset$.

Pour la permutation :

$$\sigma \;:=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix},$$

on a :

$$\begin{aligned} \mathsf{Fix}\,\sigma \;&=\; \big\{2,\,6\big\}, \\ \mathsf{Supp}\,\sigma \;&=\; \big\{1,\,3,\,4,\,5,\,7,\,8,\,9\big\}. \end{aligned}$$

L'énoncé technique suivant présente quelques propriétés fondamentales qui seront souvent utilisées ultérieurement.

Proposition 2.5. *Soit E un ensemble fini.*

(1) *Pour toute permutation $\sigma \in \mathfrak{S}(E)$, on a les* égalités :

$$\begin{aligned} \sigma\big(\mathsf{Fix}\,\sigma\big) &= \mathsf{Fix}\,\sigma, \\ \sigma\big(\mathsf{Supp}\,\sigma\big) &= \mathsf{Supp}\,\sigma. \end{aligned}$$

(2) *Pour toute permutation $\sigma \in \mathfrak{S}(E)$, on a les* égalités :

$$\begin{aligned} \mathsf{Fix}\,\sigma &= \mathsf{Fix}\,\sigma^{-1}, \\ \mathsf{Supp}\,\sigma &= \mathsf{Supp}\,\sigma^{-1}. \end{aligned}$$

(3) *Pour toute $\sigma \in \mathfrak{S}(E)$ et tout entier $m \in \mathbb{Z}$, on a les* inclusions :

$$\begin{aligned} \mathsf{Fix}\,\sigma &\subset \mathsf{Fix}\,\sigma^{m}, \\ \mathsf{Supp}\,\sigma &\supset \mathsf{Supp}\,\sigma^{m}. \end{aligned}$$

(4) *Pour $\sigma, \sigma' \in \mathfrak{S}(E)$, on a les* inclusions :

$$\begin{aligned} \mathsf{Fix}\,\sigma \circ \sigma' &\supset \mathsf{Fix}\,\sigma \cap \mathsf{Fix}\,\sigma', \\ \mathsf{Supp}\,\sigma \circ \sigma' &\subset \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma'. \end{aligned}$$

(5) *Si de plus σ et σ' sont à supports disjoints, on a les* égalités :

$$\begin{aligned} \mathsf{Fix}\,\sigma \circ \sigma' &= \mathsf{Fix}\,\sigma \cap \mathsf{Fix}\,\sigma', \\ \mathsf{Supp}\,\sigma \circ \sigma' &= \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma'. \end{aligned}$$

Le point-clé, c'est que les inclusions de $(\mathbf{3})$ et de $(\mathbf{4})$ ne sont pas forcément des égalités. Notamment, avec $G := \mathfrak{S}(E)$, de cardinal $|G| = n!$, le théorème de Lagrange vu au chapitre précédent donne, pour toute permutation $\sigma \in \mathfrak{S}(E)$:

$$\sigma^{|\mathfrak{S}(E)|} = \sigma^{n!} = \mathsf{Id},$$

de telle sorte que :

$$\mathsf{Fix}\big(\sigma^{|E|!}\big) = \mathsf{Fix}\,\mathsf{Id} = E.$$

En première lecture, nous conseillons de « sauter » la

Démonstration. **(1)** Pour tout $a \in E$, en appliquant $\sigma^{-1}(\bullet)$ et $\sigma(\bullet)$, on constate que :

$$\begin{aligned} \sigma\big(\mathsf{Fix}\,\sigma\big) \ni a \quad &\iff \quad \mathsf{Fix}\,\sigma \ni \sigma^{-1}(a) \\ &\iff \quad \sigma\big(\sigma^{-1}(a)\big) = \sigma^{-1}(a) \\ &\iff \quad a = \sigma^{-1}(a) \\ &\iff \quad \sigma(a) = a \\ &\iff \quad \mathsf{Fix}\,\sigma \ni a. \end{aligned}$$

Pareillement :

$$\begin{aligned}\sigma\big(\mathsf{Supp}\,\sigma\big) \ni a \quad &\Longleftrightarrow \quad \mathsf{Supp}\,\sigma \ni \sigma^{-1}(a)\\ &\Longleftrightarrow \quad \sigma\big(\sigma^{-1}(a)\big) \neq \sigma^{-1}(a)\\ &\Longleftrightarrow \quad a \neq \sigma^{-1}(a)\\ &\Longleftrightarrow \quad \sigma(a) \neq a\\ &\Longleftrightarrow \quad \mathsf{Supp}\,\sigma \ni a.\end{aligned}$$

(2) Pour tout $a \in E$, en appliquant aussi $\sigma^{-1}(\bullet)$ et $\sigma(\bullet)$, on constate de même que :

$$\begin{aligned}\sigma(a) = a \quad &\Longleftrightarrow \quad a = \sigma^{-1}(a),\\ \sigma(a) \neq a \quad &\Longleftrightarrow \quad a \neq \sigma^{-1}(a).\end{aligned}$$

(3) Pour tout $a \in E$, on a :

$$\sigma(a) = a \quad \Longrightarrow \quad \sigma\big(\sigma(a)\big) = \sigma(a) = a \quad \Longrightarrow \quad \sigma^3(a) = a \quad \Longrightarrow \quad \cdots,$$

puis par récurrence pour tout entier $m \geqslant 1$:

$$\sigma^m(a) = a,$$

d'où aussi $a = \sigma^{-m}(a)$ en appliquant $\sigma^{-m}(\bullet)$ à cette égalité. Ainsi, on a bien :

$$\mathsf{Fix}\,\sigma \subset \mathsf{Fix}\,\sigma^m \qquad (\forall\, m \in \mathbb{Z}).$$

En passant au complémentaire [2], nous obtenons la deuxième inclusion annoncée :

$$\mathsf{Supp}\,\sigma = E\big\backslash\mathsf{Fix}\,\sigma \supset E\big\backslash\mathsf{Fix}\sigma^m = \mathsf{Supp}\,\sigma^m,$$

(4) Soit $a \in E$ avec $\sigma(a) = a = \sigma'(a)$. Alors :

$$\sigma \circ \sigma'(a) = \sigma\big(\sigma'(a)\big) = \sigma(a) = a,$$

ce qui justifie la première inclusion. La deuxième inclusion s'obtient en passant au complémentaire [3].

(5) Supposons maintenant que $\mathsf{Supp}\,\sigma \cap \mathsf{Supp}\,\sigma' = \emptyset$. Pour un élément dans la réunion de ces deux supports disjoints $a \in \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma'$, on a *ou bien* $a \in \mathsf{Supp}\,\sigma$, *ou bien* $a \in \mathsf{Supp}\,\sigma'$.

Pour fixer les idées, supposons $a \in \mathsf{Supp}\,\sigma$, c'est-à-dire $\sigma(a) \neq a$. Comme $a \notin \mathsf{Supp}\,\sigma'$, c'est-à-dire $\sigma'(a) = a$, il vient :

$$\sigma\big(\sigma'(a)\big) = \sigma(a) \neq a,$$

ce qui montre que $a \in \mathsf{Supp}\,\sigma \circ \sigma'$.

Le cas $a \in \mathsf{Supp}\,\sigma'$ est similaire. Donc on a obtenu l'inclusion :

$$\mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma' \subset \mathsf{Supp}\,\sigma \circ \sigma',$$

qui est *inverse* de **(4)**. En conclusion, on a obtenu la deuxième inclusion **(5)**, tandis que la première s'obtient en passant au complémentaire. □

2. Rappelons que pour tous ensembles $G \subset F \subset E$, on a l'inclusion inversée $E\backslash G \supset E\backslash F$.
3. Rappelons que $F \cap G \subset H \subset E$ implique :

$$E\backslash F \cup E\backslash G = E\big\backslash(F \cap G) \supset E\backslash H.$$

Rendez-vous était donc donné ici à l'étudiant qui aura sagement décidé de sauter la lecture de la démonstration. Bien que $\mathfrak{S}(E)$ ne soit jamais commutatif dès que $|E| \geqslant 3$, on a un résultat très important de commutation entre deux permutations sous hypothèse de support (ou de territoire).

Proposition 2.6. *Deux permutations à supports disjoints commutent toujours.*

Démonstration. Soient donc $\sigma, \sigma' \in \mathfrak{S}(E)$ avec $\emptyset = \mathsf{Supp}\,\sigma \cap \mathsf{Supp}\,\sigma'$, et soit $a \in E$ quelconque. Avec la décomposition en sous-ensembles disjoints :

$$E \;=\; \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma' \cup \big(E \big\backslash \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma'\big),$$

trois cas se présentent.

Si $a \in \mathsf{Supp}\,\sigma$, alors $\sigma(a) \in \mathsf{Supp}\,\sigma$ aussi grâce à la Proposition 2.5 **(1)**. Par hypothèse, $\sigma(a)$ n'est donc *pas* dans le support de σ', et donc $\sigma'\big(\sigma(a)\big) = \sigma(a) = \sigma\big(\sigma'(a)\big)$ car $a = \sigma'(a)$ puisque $a \notin \mathsf{Supp}\,\sigma'$.

Ensuite, si $a \in \mathsf{Supp}\,\sigma'$, d'où $a \notin \mathsf{Supp}\,\sigma$ par hypothèse, on raisonne de manière symétrique pour obtenir encore la commutation annoncée $\sigma'\big(\sigma(a)\big) = \sigma\big(\sigma'(a)\big)$.

Enfin, si $a \notin \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma'$, donc si a est fixé par σ *et* par σ', il vient aisément :

$$\sigma\big(\sigma'(a)\big) \;=\; \sigma(a) \;=\; a \;=\; \sigma'(a) \;=\; \sigma'\big(\sigma(a)\big). \qquad \square$$

3. Orbites d'une permutation $\sigma \in \mathfrak{S}(E)$

Soit toujours un ensemble *fini* E de cardinal $|E| =: n \geqslant 2$. Pour toute permutation $\sigma \in \mathfrak{S}(E)$, c'est-à-dire toute bijection $\sigma\colon E \longrightarrow E$ d'inverse σ^{-1}, rappelons que l'on note $\sigma^0 := \mathsf{Id}$, que l'on note $\sigma^i := \sigma \circ \cdots \circ \sigma$ composée i fois avec elle-même, et enfin, que l'on note aussi $\sigma^{-i} := \sigma^{-1} \circ \cdots \circ \sigma^{-1}$.

Proposition 3.1. *La relation binaire entre éléments $a, b \in E$ définie par :*

$$a \sim b \qquad \overset{\text{déf}}{\Longleftrightarrow} \qquad \exists\, i \in \mathbb{Z} \quad \sigma^i(a) = b,$$

est une relation d'équivalence.

Démonstration. Avec $i := 0$, on a $\sigma^0(a) = a$, d'où la réflexivité $a \sim a$.

La symétrie $b \sim a$ provient de :

$$\sigma^{-i}\big(\; \sigma^i(a) \;=\; b \;\big) \qquad \Longrightarrow \qquad a \;=\; \sigma^{-i}(b).$$

Quant à la transitivité, elle est tout aussi facile :

$$\begin{aligned} \Big(\; a \sim b \quad \text{et} \quad b \sim c \;\Big) \qquad &\Longleftrightarrow \qquad \Big(\; \sigma^i(a) = b \quad \text{et} \quad \sigma^j(b) = c \;\Big) \\ &\Longrightarrow \qquad\quad \sigma^j\big(\sigma^i(a)\big) = c \\ &\Longleftrightarrow \qquad\quad \Big(\; a \sim c \;\Big). \end{aligned} \qquad \square$$

Dans notre exemple continué :

$$\sigma \;=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix},$$

nous avons :

$$\begin{aligned} &1 \sim 4 \sim 5 \sim 8 \sim 1, \\ &2 \sim 2, \\ &3 \sim 7 \sim 9 \sim 3, \\ &6 \sim 6. \end{aligned}$$

D'après les propriétés générales dont jouissent les relations d'équivalence sur des ensembles arbitraires, nous savons que E se partitionne en *classes d'équivalences* associées à une permutation fixée $\sigma \in \mathfrak{S}(E)$. Traditionnellement, on donne un nom à ces classes d'équivalence.

Définition 3.2. Pour $\sigma \in \mathfrak{S}(E)$, la *$\sigma$-orbite* d'un élément quelconque $a \in E$ est la collection de tous les éléments qui sont obtenus en itérant $\sigma(\bullet)$ ainsi que $\sigma^{-1}(\bullet)$ à partir de a :

$$\begin{aligned} \mathsf{Orb}_\sigma(a) &= \big\{b \in E\colon\ b \sim a\big\} \\ &= \big\{\sigma^i(a)\colon\ i \in \mathbb{Z}\big\} \\ &= \Big\{ \ldots,\ \sigma^{-3}(a),\ \sigma^{-2}(a),\ \sigma^{-1}(a),\ a,\ \sigma(a),\ \sigma^2(a),\ \sigma^3(a),\ \ldots \Big\}. \end{aligned}$$

Il est clair qu'une σ-orbite $\mathsf{Orb}_\sigma(a)$ est réduite à un singleton (élément unique) si et seulement si $a = \sigma(a)$ est fixé par σ, car alors $\sigma\big(\sigma(a)\big) = a$, puis $\sigma^3(a) = a$, et ainsi de suite.

Proposition 3.3. *Pour un élément quelconque $a \in E$, on a :*

$$\begin{aligned} a \in \mathsf{Fix}\,\sigma \qquad &\Longleftrightarrow \qquad \big|\mathsf{Orb}_\sigma(a)\big| = 1, \\ a \in \mathsf{Supp}\,\sigma \qquad &\Longleftrightarrow \qquad \big|\mathsf{Orb}_\sigma(a)\big| \geqslant 2. \end{aligned}$$

Démonstration. La première équivalence vient d'être dite. Quant à la seconde, effectivement, elle est équivalente par contraposée à la première. Elle peut aussi être vue directement, car $a \in \mathsf{Supp}\,\sigma$ signifie $a \neq \sigma(a)$, donc $\mathsf{Orb}_\sigma(a)$ contient au moins deux éléments distincts, effectivement. □

Les propriétés générales des classes d'équivalences donnent immédiatement l'énoncé suivant.

Proposition 3.4. *Les orbites d'une permutation $\sigma \in \mathfrak{S}(E)$ satisfont les quatre propriétés suivantes.*

(1) $a \in \mathsf{Orb}_\sigma(a)$, *pour tout* $a \in E$.

(2) *Deux σ-orbites qui s'intersectent sont forcément* égales :

$$\emptyset \neq \mathsf{Orb}_\sigma(a) \cap \mathsf{Orb}_\sigma(b) \qquad \Longrightarrow \qquad \mathsf{Orb}_\sigma(a) = \mathsf{Orb}_\sigma(b).$$

(3) *Deux σ-orbites sont soit égales, soit disjointes :*

$$\mathsf{Orb}_\sigma(a) = \mathsf{Orb}_\sigma(b) \qquad \textit{ou bien} \qquad \mathsf{Orb}_\sigma(a) \cap \mathsf{Orb}_\sigma(b) = \emptyset.$$

(4) *Pour tous $a, b \in E$:*

$$\mathsf{Orb}_\sigma(a) = \mathsf{Orb}_\sigma(b) \qquad \Longleftrightarrow \qquad a \in \mathsf{Orb}_\sigma(b) \qquad \Longleftrightarrow \qquad b \in \mathsf{Orb}_\sigma(a). \qquad \square$$

Maintenant, comment « capturer » une σ-orbite ? C'est tout simple, en faisant défiler de mode tous les éléments :

$$\ldots,\ \sigma^{-5}(a),\ \sigma^{-4}(a),\ \sigma^{-3}(a),\ \sigma^{-2}(a),\ \sigma^{-1}(a),\ a,\ \sigma(a),\ \sigma^2(a),\ \sigma^3(a),\ \sigma^4(a),\ \sigma^5(a),\ \ldots$$

en nombre *infini*, mais tous contenus dans notre ensemble E *fini*.

Or comme E est de cardinal $|E| < \infty$ *fini*, tous ces éléments en nombre *infini* ne peuvent *absolument pas* être *tous* mutuellement distincts — le tapis rouge n'est pas assez long. Donc nécessairement, deux puissances distinctes de σ doivent être égales :

$$\begin{aligned} \exists\, i < j \qquad & \text{avec} \qquad & \sigma^i(a) &= \sigma^j(a), \\ & \text{d'où} \qquad & a &= \sigma^{j-i}(a), \end{aligned}$$

c'est-à-dire que a est *fixé* par une certaine *puissance* de σ.

Pour tout $a \in E$, introduisons alors l'entier :

$$n_a := \min\big\{m \geqslant 1 :\ \sigma^m(a) = a\big\}.$$

Clairement, $\sigma^{k\,n_a}(a) = a$ pour tout entier $k \in \mathbb{Z}$.

Proposition 3.5. *Soit E un ensemble fini, et soit une permutation quelconque $\sigma \in \mathfrak{S}(E)$. Alors pour tout $a \in E$, la σ-orbite de a est :*

$$\mathsf{Orb}_\sigma(a) = \Big\{a,\ \sigma(a),\ \sigma^2(a),\ \ldots,\ \sigma^{n_a-1}(a)\Big\},$$

où ces n_a éléments sont distincts deux à deux.

Preuve. Effectivement, ces éléments doivent être mutuellement distincts, car s'il ne l'étaient pas, à savoir s'il existait deux entiers différents $0 \leqslant i < j \leqslant n_a - 1$ avec $\sigma^i(a) = \sigma^j(a)$, et donc avec :

$$1 \leqslant j - i \leqslant n_a - 1,$$

on déduirait $a = \sigma^{j-i}(a)$, en contradiction flagrante avec la minimalité de $m = n_a$ satisfaisant $a = \sigma^m(a)$. □

L'énoncé suivant était en fait déjà contenu dans la Proposition 3.4 **(4)**, mais nous souhaitons en donner une démonstration explicite.

Proposition 3.6. *Pour tout $b \in \mathsf{Orb}_\sigma(a)$, c'est-à-dire $b = \sigma^\ell(a)$ avec un entier $0 \leqslant \ell \leqslant n_a - 1$, on a aussi :*

$$\begin{aligned} \mathsf{Orb}_\sigma(a) &= \Big\{b,\ \sigma(b),\ \sigma^2(b),\ \ldots,\ \sigma^{n_a-1}(b)\Big\} \\ &= \Big\{b,\ \sigma(b),\ \sigma^2(b),\ \ldots,\ \sigma^{n_b-1}(b)\Big\} = \mathsf{Orb}_\sigma(b). \end{aligned}$$

Autrement dit, pour tout $b \in \mathsf{Orb}_\sigma(a)$, on a :

$$n_a = n_b.$$

Démonstration. Les éléments $\sigma^i(b)$ sont mutuellement distincts, car avec $0 \leqslant i, j \leqslant n_a - 1$, on a :

$$\sigma^i(b) = \sigma^j(b) \qquad \Longleftrightarrow \qquad \sigma^{i+\ell}(a) = \sigma^{j+\ell}(a),$$

d'où en appliquant $\sigma^{-\ell}(\bullet)$:

$$\sigma^i(a) = \sigma^j(a),$$

et enfin, $i = j$ à cause de la Proposition 3.5.

Ainsi, il y a bien $n_a = |\mathsf{Orb}_\sigma(a)|$ éléments distincts parmi b, $\sigma(b)$, …, $\sigma^{n_a-1}(b)$, et donc ces éléments, tous contenus dans $\mathsf{Orb}_\sigma(a)$, « remplissent » bien cette orbite. □

Toujours avec notre exemple récréatif :

$$\sigma \;=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix},$$

puisque :

$$\begin{aligned} 8 \;&=\; \sigma(5) \;=\; \sigma\big(\sigma(4)\big) \;=\; \sigma\big(\sigma\big(\sigma(1)\big)\big), \\ 2 \;&=\; \sigma(2), \\ 9 \;&=\; \sigma(7) \;=\; \sigma\big(\sigma(3)\big), \\ 6 \;&=\; \sigma(6), \end{aligned}$$

nous voyons que :

$$\begin{aligned} \omega_1 \;&:=\; \mathsf{Orb}_\sigma(1) \;=\; \big\{1,\,4,\,5,\,8\big\}, \\ \omega_2 \;&:=\; \mathsf{Orb}_\sigma(2) \;=\; \big\{2\big\}, \\ \omega_3 \;&:=\; \mathsf{Orb}_\sigma(3) \;=\; \big\{3,\,7,\,9\big\}, \\ \omega_4 \;&:=\; \mathsf{Orb}_\sigma(6) \;=\; \big\{6\big\}. \end{aligned}$$

Ensuite, si nous notons $\omega_1, \omega_2, \omega_3, \omega_4$ ces quatre orbites, nous voyons que notre ensemble à neuf éléments en est la réunion *disjointe*, et nous voyons clairement quel est l'ensemble des points fixes de σ, ainsi que son support :

$$\begin{aligned} \big\{1, \ldots, 9\big\} \;&=\; \omega_1 \cup \omega_2 \cup \omega_3 \cup \omega_4, \\ \mathsf{Fix}\,\sigma \;&=\; \omega_2 \cup \omega_4, \\ \mathsf{Supp}\,\sigma \;&=\; \omega_1 \cup \omega_3. \end{aligned}$$

L'énoncé général, dont nous avons déjà compris la démonstration, est le suivant, dans lequel les orbites de σ — qui sont des sous-ensembles de E — sont notées ω_σ.

Proposition 3.7. *Soit E un ensemble fini, et soit une permutation $\sigma \in \mathfrak{S}(E)$. Alors on a les réunions* disjointes :

$$\begin{aligned} E \;&=\; \bigcup_{|\omega_\sigma|=1} \omega_\sigma \;\; \bigcup_{|\omega_\sigma|\geqslant 2} \omega_\sigma, \\ \mathsf{Fix}\,\sigma \;&=\; \bigcup_{|\omega_\sigma|=1} \omega_\sigma, \\ \mathsf{Supp}\,\sigma \;&=\; \bigcup_{|\omega_\sigma|\geqslant 2} \omega_\sigma. \end{aligned}$$

□

Introduisons maintenant la notion de cycle.

Définition 3.8. Une permutation $\sigma \in \mathfrak{S}(E)$ est appelée un *cycle* si σ produit une seule σ-orbite ω_σ non réduite à un singleton, c'est-à-dire avec :

$$p \;:=\; |\omega_\sigma| \;\geqslant\; 2.$$

On dit alors que σ est un *p-cycle*, en sous-entendant que $p \geqslant 2$, et dans ce cas, $\mathsf{Supp}\,\sigma$ est cette unique σ-orbite ω_σ.

Grâce à la description d'une σ-orbite quelconque donnée par la Proposition 3.5, tout p-cycle est de la forme :

$$\Big(a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_{p-1} \longrightarrow a_p \Big)$$

avec $a_1, a_2, \ldots, a_{p-1}, a_p \in E$ distincts, ce qu'on note souvent de manière abrégée sans aucune flèche :

$$\big(a_1 \;\; a_2 \;\; \cdots \;\; a_{p-1} \;\; a_p\big),$$

tandis que les autres éléments sont tous fixés.

Un *cycle*, c'est donc une succession de wagons se poussant les uns les autres sur une ligne de chemin de fer circulaire. Ou encore, un cercle mirifique de clitocybes géotropes.

Par exemple, avec $n = 7$, la permutation :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix},$$

est un 4-cycle. Le cas particulier $p = 2$ mérite attention.

Terminologie 3.9. Un 2-cycle est aussi appelé une *transposition*.

Par exemple, avec $n = 5$:

$$\tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix} = \Big(3 \longrightarrow 5 \Big) = \big(3 \;\; 5\big),$$

Une transposition échange deux éléments distincts, sans toucher aux autres.

Or si deux étudiants échangent puis ré-échangent leurs places, ils reviennent sur leur siège initial, pendant que tous les autres restent à leur place.

Observation 3.10. *Toute transposition $\tau \in \mathfrak{S}(E)$ est sa propre inverse :*

$$\tau \circ \tau = \mathsf{Id} \qquad \Longleftrightarrow \qquad \tau^{-1} = \tau. \qquad \square$$

Bientôt, nous verrons que les transpositions sont les permutations élémentaires, au sens où *toute* permutation $\sigma \in \mathfrak{S}(E)$ peut s'écrire comme composition :

$$\sigma = \tau_1 \circ \cdots \circ \tau_r,$$

de transpositions.

Pour l'instant, souvenons-nous qu'une compagnie $\sigma \in \mathfrak{S}(E)$ construit ses propres lignes de chemin de fer circulaires sans croisements :

$$\sigma \quad \rightsquigarrow \quad \sigma\text{-orbites } \omega_\sigma \text{ disjointes avec } |\omega_\sigma| \geqslant 2,$$

les orbites-fixes $|\omega_\sigma| = 1$ pouvant être vues commes de simples vaches spectatrices immobiles.

Introduisons alors :

$$\Omega_\sigma := \big\{\sigma\text{-orbites } \omega \text{ avec } |\omega| \geqslant 2\big\},$$

d'où :

$$\mathsf{Supp}\,\sigma = \bigcup_{\omega \in \Omega_\sigma} \omega,$$

cette réunion étant disjointe, et extrayons la manière dont σ agit sur une unique ligne circulaire de TGV $\omega \in \Omega_\sigma$ en introduisant la permutation :

$$\sigma_\omega(a) := \begin{cases} a & \text{si } a \notin \omega, \\ \sigma(a) & \text{si } a \in \omega. \end{cases} \tag{3.11}$$

Ainsi, σ_ω exprime l'action de σ sur une de ses orbites, ω, et fixe tous les autres points, c'est-à-dire « *met en grève* » toutes les autres lignes circulaires.

Grâce à la Proposition 3.4 **(3)** et à la Proposition 2.6, on a :

$$\omega \neq \omega' \quad \Longrightarrow \quad \omega \cap \omega' = \emptyset \quad \Longrightarrow \quad \sigma_{\omega'} \circ \sigma_\omega = \sigma_\omega \circ \sigma_{\omega'}.$$

Notons :

$$r := \big|\Omega_\sigma\big|,$$

c'est-à-dire qu'il existe r orbites de longueur $\geqslant 2$, d'où $\mathsf{Supp}\,\sigma = \omega_1 \cup \cdots \cup \omega_r$.

Théorème 3.12. [Décomposition en cycles] *Toute permutation $\sigma \in \mathfrak{S}(E)$ se décompose de manière* unique *comme produit commutatif :*

$$\sigma = \sigma_{\omega_1} \circ \cdots \circ \sigma_{\omega_r},$$

de cycles à supports disjoints.

C'est la carte complète des trajectoires des comètes. Si nous revenons à notre exemple favori :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix},$$

il est clair que sa décomposition est :

$$\sigma = \Big(1 \longrightarrow 4 \longrightarrow 5 \longrightarrow 8 \Big) \circ \Big(3 \longrightarrow 7 \longrightarrow 9 \Big),$$

ce que l'on écrit de manière abrégée :

$$\sigma = \big(1\ 4\ 5\ 8\big)\big(3\ 7\ 9\big).$$

On pourrait même écrire :

$$\sigma = \big(1\ 4\ 5\ 8\big)\big(2\big)\big(3\ 7\ 9\big)\big(6\big),$$

mais il est préférable de ne pas faire apparaître les points fixes, en ayant en tête que les éléments *non écrits* sont fixes.

Démonstration. Montrons que σ est égale à $\sigma_{\omega_1} \circ \cdots \circ \sigma_{\omega_r}$, en faisant agir ces deux permutations sur un élément quelconque a de $E = \mathsf{Fix}\,\sigma \cup \mathsf{Supp}\,\sigma$.

Cas 1 : $a \in \mathsf{Fix}\,\sigma$. Alors $a \notin \omega_1$, …, $a \notin \omega_r$, donc :

$$\sigma_{\omega_1}(a) = a, \ \ldots\ldots\ldots, \ \sigma_{\omega_r}(a) = a,$$

puis :

$$\sigma_{\omega_1}\big(\cdots\big(\sigma_{\omega_r}(a)\big)\cdots\big) = a = \sigma(a).$$

Cas 2 : $a \in \mathsf{Supp}\,\sigma$. Comme $\mathsf{Supp}\,\sigma = \omega_1 \cup \cdots \cup \omega_r$, disjointement, il existe un unique entier $1 \leqslant i \leqslant r$ tel que $a \in \omega_i$, d'où par la définition (3.11) :

$$\begin{aligned} & & \sigma_{\omega_i}(a) &= \sigma(a), \\ j \neq i & \quad\Longrightarrow\quad & \sigma_{\omega_j}(a) &= a, \end{aligned}$$

puis grâce à la commutation :

$$\begin{aligned}\sigma_{\omega_1}\circ\cdots\circ\sigma_{\omega_i}\circ\cdots\circ\sigma_{\omega_r}(a) &= \sigma_{\omega_i}\Big(\sigma_{\omega_1}\circ\cdots\circ\sigma_{\omega_{i-1}}\circ\sigma_{\omega_{i+1}}\circ\cdots\circ\sigma_{\omega_r}(a)\Big)\\ &= \sigma_{\omega_i}(a)\\ &= \sigma(a).\end{aligned}$$

Montrons maintenant l'*unicité* de la décomposition de σ en cycles à supports disjoints. Supposons alors qu'il existe une autre décomposition :

$$\sigma_{\omega_1}\circ\cdots\circ\sigma_{\omega_r} \;=\; \sigma \;=\; \overline{\sigma}_1\circ\cdots\circ\overline{\sigma}_s,$$

en cycles $\overline{\sigma}_\ell$, pour $\ell=1,\ldots,s$, à supports disjoints, donc commutant entre eux, et notons :

$$\varpi_\ell \;:=\; \mathsf{Supp}\,\overline{\sigma}_\ell \qquad (1\leqslant\ell\leqslant s),$$

de telle sorte que :

$$\omega_1\cup\cdots\cup\omega_r \;=\; \mathsf{Supp}\,\sigma \;=\; \varpi_1\cup\cdots\cup\varpi_s. \tag{3.13}$$

Comme $\overline{\sigma}_\ell$ est un cycle, son support ϖ_ℓ est la $\overline{\sigma}_\ell$-orbite d'un de ses points quelconques, d'après la Proposition 3.6.

Assertion 3.14. *Pour $1\leqslant\ell\leqslant s$, chaque $\overline{\sigma}_\ell$-orbite ϖ_ℓ coïncide en fait avec une certaine σ-orbite.*

Par conséquent, ϖ_ℓ ne dépend *que* de σ — c'est un premier pas vers l'unicité.

Preuve. Soit $a\in\varpi_\ell$ quelconque. Nous venons de dire que $\mathsf{Orb}_{\overline{\sigma}_\ell}(a)=\varpi_\ell$.

Pour $m\neq\ell$, on a $\overline{\sigma}_m(a)=a$, d'où :

$$\begin{aligned}\sigma(a) &= \overline{\sigma}_1\circ\cdots\circ\overline{\sigma}_\ell\circ\cdots\circ\overline{\sigma}_s(a)\\ &= \overline{\sigma}_\ell(a).\end{aligned} \tag{3.15}$$

Puisque $\varpi_\ell=\mathsf{Supp}\,\overline{\sigma}_\ell$ satisfait $\overline{\sigma}_\ell\big(\mathsf{Supp}\,\overline{\sigma}_\ell\big)=\mathsf{Supp}\,\overline{\sigma}_\ell$ d'après la Proposition 2.5 **(1)**, nous déduisons pour tout $m\neq\ell$ que :

$$\overline{\sigma}_\ell(a)\;\notin\;\mathsf{Supp}\,\overline{\sigma}_m \qquad\text{d'où}\qquad \overline{\sigma}_m\big(\overline{\sigma}_\ell(a)\big)\;=\;\overline{\sigma}_\ell(a) \qquad (m\neq\ell),$$

puis :

$$\begin{aligned}\sigma\big(\sigma(a)\big) &= \sigma\big(\overline{\sigma}_\ell(a)\big)\\ &= \overline{\sigma}_1\circ\cdots\circ\overline{\sigma}_\ell\circ\cdots\circ\overline{\sigma}_s\big(\overline{\sigma}_\ell(a)\big)\\ &= \overline{\sigma}_\ell\big(\overline{\sigma}_\ell(a)\big).\end{aligned}$$

Ensuite, une récurrence aisée donne :

$$\sigma^i(a) \;=\; \big(\overline{\sigma}_\ell\big)^i(a) \qquad (\forall\, i\in\mathbb{Z}),$$

et ainsi on a bien :

$$\mathsf{Orb}_\sigma(a) \;=\; \big\{\sigma^i(a)\colon\; i\in\mathbb{Z}\big\} \;=\; \big\{\big(\overline{\sigma}_\ell\big)^i(a)\colon\; i\in\mathbb{Z}\big\} \;=\; \mathsf{Orb}_{\overline{\sigma}_\ell}(a) \;=\; \varpi_\ell. \qquad\square$$

Chaque $\overline{\sigma}_\ell$-orbite $\varpi_\ell=\omega_{i(\ell)}$ s'identifie donc à une certaine σ-orbite, au moyen d'une application :

$$\{1,\ldots,s\} \;\ni\; \ell \;\longmapsto\; \ell(i) \;\in\; \{1,\ldots,r\}$$

qui est injective, puisque les deux collections d'orbites (disjointes) sont contenues dans notre ensemble E. De plus, cette application est aussi surjective, car d'après (3.13), les ω_i et les ϖ_ℓ remplissent $\mathrm{Supp}\,\sigma$. Ainsi :

$$r \,=\, s.$$

Assertion 3.16. *On a $\sigma_{\omega_{i(\ell)}} = \overline{\sigma}_\ell$, pour tout $\ell = 1, \ldots, r$.*

Preuve. En effet, ces deux permutations fixent tout élément $a \notin \omega_{i(\ell)} = \varpi_\ell$.

Et en tenant compte de la définition (3.11), le petit calcul (3.15) a déjà montré pour $a \in \omega_{i(\ell)} = \varpi_\ell$ que :

$$\sigma_{\omega_{i(\ell)}}(a) \,=\, \sigma(a) \,=\, \overline{\sigma}_\ell(a). \qquad \square$$

En conclusion, dans les deux décompositions en cycles qui commutent :

$$\sigma_{\omega_1} \circ \cdots \circ \sigma_{\omega_r} \;=\; \sigma \;=\; \overline{\sigma}_1 \circ \cdots \circ \overline{\sigma}_r,$$

il y a les mêmes facteurs, à un simple changement d'ordre près — c'est l'unicité ! $\square$

De manière importante, une permutation quelconque $\sigma \in \mathfrak{S}(E)$ ayant comme orbites $\omega_1, \ldots, \omega_r$ de cardinaux $p_1, \ldots, p_r \geqslant 2$ s'écrit *explicitement :*

$$\Big(a_1 \longrightarrow \sigma(a_1) \longrightarrow \cdots \longrightarrow \sigma^{p_1-1}(a_1) \Big) \circ \cdots \circ \Big(a_r \longrightarrow \sigma(a_r) \longrightarrow \cdots \longrightarrow \sigma^{p_r-1}(a_r) \Big).$$

Quant à notre exemple fétiche :

$$\sigma \,:=\, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix},$$

montrons encore sa décomposition :

$$\sigma \;=\; \Big(\, 1 \longrightarrow 4 \longrightarrow 5 \longrightarrow 8 \, \Big) \circ \Big(\, 3 \longrightarrow 7 \longrightarrow 9 \, \Big).$$

Théorème 3.17. *Le groupe $\mathfrak{S}(E)$ des permutations d'un ensemble fini E est engendré par les cycles.* $\square$

Toutefois, si on nous donne en TD une composition de cycles dont les supports ne sont *pas* disjoints, il faut la re-travailler pour la re-décomposer en cycles à supports *disjoints*.

Exemple 3.18. Soit la permutation de l'ensemble $\{1, 2, 3, 4, 5, 6, 7, 8\}$:

$$\sigma \,:=\, \big(1\ \ 2\ \ 3\ \ 5\big) \circ \big(3\ \ 7\big) \circ \big(7\ \ 4\ \ 8\big),$$

dont les cycles ne sont *pas* disjoints.

Évaluons le devenir de chaque entier, en commençant les compositions par la droite comme il se doit :

$$\begin{array}{ccccccccc} & & (7\ 4\ 8) & & (2\ 7) & & (1\ 2\ 3\ 5) & & \\ 1 & \longrightarrow & 1 & \longrightarrow & 1 & \longrightarrow & 2 \\ 2 & \longrightarrow & 2 & \longrightarrow & 2 & \longrightarrow & 3 \\ 3 & \longrightarrow & 3 & \longrightarrow & 7 & \longrightarrow & 7 \\ 4 & \longrightarrow & 8 & \longrightarrow & 8 & \longrightarrow & 8 \\ 5 & \longrightarrow & 5 & \longrightarrow & 5 & \longrightarrow & 1 \\ 6 & \longrightarrow & 6 & \longrightarrow & 6 & \longrightarrow & 6 \\ 7 & \longrightarrow & 4 & \longrightarrow & 4 & \longrightarrow & 4 \\ 8 & \longrightarrow & 7 & \longrightarrow & 3 & \longrightarrow & 5 \end{array}$$

ce qui nous donne :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 7 & 8 & 1 & 6 & 4 & 5 \end{pmatrix} = \big(1\ 2\ 3\ 7\ 4\ 8\ 5\big).$$

Visiblement, l'ensemble des points fixes est réduit au singleton $\{6\} = \mathsf{Fix}\,\sigma$, et on constate qu'il y a un unique cycle, de longueur 7 :

$$\Big(1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 7 \longrightarrow 4 \longrightarrow 8 \longrightarrow 5 \Big).$$

Théorème 3.19. *Le groupe des permutations $\mathfrak{S}(E)$ d'un ensemble fini E est engendré par les transpositions.*

Démonstration. Soit une permutation arbitraire $\sigma \in \mathfrak{S}(E)$. Comme σ est une composition de cycles, grâce au Théorème 3.12, il suffit de montrer que tout cycle $\big(a_1\ \cdots\ a_p\big)$ est à son tour un produit de transpositions, où les éléments $a_1, \ldots, a_p$ de E sont mutuellement distincts.

Sans difficulté, on vérifie alors que :

$$\Big(a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_p \Big) = \Big(a_1 \longrightarrow a_2 \Big) \circ \Big(a_2 \longrightarrow a_3 \Big) \circ \cdots \circ \Big(a_{p-1} \longrightarrow a_p \Big),$$

par exemple pour $p = 3$, on vérifie que :

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ \downarrow & \downarrow & \downarrow \\ a_2 & a_3 & a_1 \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} a_1 & a_2 & a_3 \\ \downarrow & \downarrow & \downarrow \\ a_2 & a_1 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 \\ \downarrow & \downarrow & \downarrow \\ a_1 & a_3 & a_2 \end{pmatrix},$$

en calculant cette composition depuis la droite :

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ \downarrow & \downarrow & \downarrow \\ a_1 & a_3 & a_2 \\ \downarrow & \downarrow & \downarrow \\ a_2 & a_3 & a_1 \end{pmatrix} \qquad \text{OUI !},$$

le cas général étant similaire. □

Rappelons que dans un groupe abstrait fini G, l'*ordre* d'un élément $x \in G$ est l'entier :

$$\mathsf{o}(x) \,:=\, \mathsf{min}\,\big\{m \geqslant 1 \colon\ x^m = 1_G\big\},$$

et rappelons que pour $G := \mathfrak{S}(E)$, l'élément neutre 1_G est $\mathsf{Id} \colon E \longrightarrow E$.

Théorème 3.20. *L'ordre dans $\mathfrak{S}(E)$ d'un p-cycle :*

$$\sigma \,=\, \Big(a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_{p-1} \longrightarrow a_p \Big),$$

est égal à son nombre d'éléments, ou à sa longueur :

$$p \,=\, \mathsf{o}(\sigma) \,=\, \mathsf{min}\,\big\{m \geqslant 1 \colon\ \sigma^m = \mathsf{Id}\big\}.$$

Il découle alors de la théorie générale des groupes que :

$$\sigma^m \,=\, \mathsf{Id} \qquad\qquad \Longleftrightarrow \qquad\qquad p \,\big|\, m.$$

Démonstration. Comme σ est l'identité sur le complémentaire $E\big\backslash\{a_1, \ldots, a_p\}$, d'où :

$$\sigma^i(a) \,=\, a \qquad\qquad (\forall\, a \neq a_1, \ldots, a_p,\ \forall\, i \in \mathbb{Z}),$$

on peut ignorer purement et simplement tout ce qui se trouve en-dehors du cycle [4].

Tout d'abord, puisque :

$$\begin{aligned}
\sigma(a_1) \,&=\, a_2 \,\neq\, a_1,\\
\sigma^2(a_1) \,&=\, a_3 \,\neq\, a_1,\\
&\cdots\cdots\cdots\cdots\cdots\\
\sigma^{p-1}(a_1) \,&=\, a_p \,\neq\, a_1,
\end{aligned}$$

il est clair que $\sigma, \sigma^2, \ldots, \sigma^{p-1}$ ne sont *pas* l'identité, d'où $\mathsf{o}(\sigma) \geqslant p - 1$.

Mais ensuite, comme :

$$\sigma^p(a_1) \,=\, \sigma\big(\sigma^{p-1}(a_1)\big) \,=\, \sigma(a_p) \,=\, a_1,$$

et comme, pour tout entier $1 \leqslant i \leqslant p$, on a :

$$\sigma^p(a_i) \,=\, \sigma^p\big(\sigma^{i-1}(a_1)\big) \,=\, \sigma^{i-1}\big(\sigma^p(a_1)\big) \,=\, \sigma^{i-1}(a_1) \,=\, a_i,$$

on constate que σ^p *est* l'identité sur son support $\big\{a_1, \ldots, a_p\big\}$, donc partout sur E, ce qui conclut. □

Théorème 3.21. *Si $\sigma_1, \ldots, \sigma_r \in \mathfrak{S}(E)$ sont des permutations à supports disjoints :*

$$\emptyset \,=\, \mathsf{Supp}\,\sigma_i \cap \mathsf{Supp}\,\sigma_j \qquad\qquad (\forall\, 1 \leqslant i \neq j \leqslant r),$$

alors :

$$\mathsf{o}\big(\sigma_1 \circ \cdots \circ \sigma_r\big) \,=\, \mathsf{ppcm}\,\big(\mathsf{o}(\sigma_1),\, \ldots,\, \mathsf{o}(\sigma_r)\big).$$

4. Effectivement, tout ce qui se trouve en dehors du cycle — *magnétique !* — des mathématiques pourrait, et devrait, être ignoré …

En particulier, cette formule arithmétique très élémentaire s'applique à la décompositions de :

$$\sigma \;=\; \sigma_{\omega_1} \circ \cdots \circ \sigma_{\omega_r},$$

en cycles à supports disjoints fournie par le Théorème 3.12, pour donner :

$$\begin{aligned} o(\sigma) \;&=\; \mathsf{ppcm}\,\big\{o(\sigma_1),\,\ldots,\,o(\sigma_r)\big\} \\ &=\; \mathsf{ppcm}\,\big\{\mathsf{longueur}(\sigma_1),\,\ldots,\,\mathsf{longueur}(\sigma_r)\big\}. \end{aligned}$$

Par exemple, l'ordre de notre permutation élue décomposée de l'année 2021 :

$$\sigma \;=\; \big(1\;\;4\;\;5\;\;8\big) \circ \big(3\;\;7\;\;9\big),$$

vaut tout simplement :

$$o(\sigma) \;=\; \mathsf{ppcm}\,(3,4) \;=\; 12.$$

Démonstration. Le cas $r = 1$, où $\sigma = \sigma_1$, est trivial.

Supposons donc $r = 2$, c'est-à-dire $\sigma = \sigma_1 \circ \sigma_2$. Comme les supports de σ_1 et de σ_2 sont par hypothèse disjoints, il est clair que les actions de σ_1 et de σ_2 sur les éléments de E sont totalement indépendantes, et donc :

$$\begin{aligned} \sigma^m \;=\; \sigma_1^m \circ \sigma_2^m \qquad &\Longleftrightarrow \qquad \sigma_1^m \;=\; \mathsf{Id} \qquad \text{et} \qquad \sigma_2^m \;=\; \mathsf{Id}, \\ &\Longleftrightarrow \qquad p_1 \;\Big|\; m \qquad \text{et} \qquad p_2 \;\Big|\; m, \end{aligned}$$

donc par définition du ppcm on a bien :

$$o(\sigma) \;=\; \mathsf{ppcm}\,\big(o(\sigma_1),\,o(\sigma_2)\big).$$

Le cas $r \geqslant 3$ quelconque se déduit du cas $r = 2$ grâce à une récurrence assez immédiate. □

4. Conjugaisons comme changements de coordonnées sur E

Une permutation fixée $\rho \in \mathfrak{S}(E)$ peut être vue comme un « *changement de coordonnées* » sur E, c'est-à-dire un changement de dénomination des éléments de E. Quand on change de « coordonnées », une permutation quelconque $\sigma \in \mathfrak{S}(E)$ est transformée en sa *conjuguée par* ρ :

$$\rho \circ \sigma \circ \rho^{-1} \;=:\; \sigma',$$

comme l'exprime le diagramme suivant :

$$\begin{array}{ccc} E & \xrightarrow{\;\sigma\;} & E \\ {\scriptstyle \rho^{-1}}\uparrow & & \downarrow{\scriptstyle \rho} \\ E' & \xrightarrow[\rho\circ\sigma\circ\rho^{-1}]{\;\sigma'\;} & E'. \end{array}$$

Pour plus de mathématé-clarté, on devrait s'imaginer que l'espace d'arrivé de $\rho\colon E \longrightarrow E'$ est une « *copie* » $E' := E$ de E, que l'on décide néanmoins de considérer comme « différente », au moins au niveau des notations formelles.

Conjugaison = Changement de coordonnées

Dans le cas des permutations qui sont des p-cycles, on a une expression très simple de la conjugaison.

Proposition 4.1. *Le conjugué, par une une permutation fixée $\rho \in \mathfrak{S}(E)$, d'un p-cycle, est le p-cycle de même longueur :*

$$\rho \circ \big(a_1 \ \cdots \ a_p\big) \circ \rho^{-1} \ = \ \big(\rho(a_1) \ \cdots \ \rho(a_p)\big).$$

On voit bien en quoi les noms-coordonnées a_i du p-cycle à gauche se trouvent changés en les noms-coordonnées $\rho(a_i)$ à droite.

Démonstration. La permutation ρ effectue une bijection :

$$E \ \ni \ a \ \longmapsto \ \rho(a) =: b \ \in E.$$

Vérifions que les actions sur n'importe quel élément $b \in E$ sont égales :

$$\rho \circ \big(a_1 \ \cdots \ a_p\big) \circ \rho^{-1}(b) \ \overset{?}{=} \ \big(\rho(a_1) \ \cdots \ \rho(a_p)\big)(b).$$

Cas 1 : $b = \rho(a_i)$ avec $1 \leqslant i \leqslant p-1$. Alors on a bien :

$$\rho \circ (a_1 \ \ldots \ a_p)(a_i) \ = \ \rho(a_{i+1}) \ \overset{\text{OUI}}{=} \ \big(\rho(a_1) \cdots \rho(a_p)\big)\big(\rho(a_i)\big).$$

Cas 2 : $b = \rho(a_p)$. Le même raisonnement fonctionne, avec la convention $a_{p+1} := a_1$.

Cas 3 : $b \neq \rho(a_1), \ldots, \rho(a_p)$. Alors b reste fixé par $\big(\rho(a_1) \ \ldots, \rho(a_p)\big)$ à droite, et de même, son image inverse $a := \rho^{-1}(b)$ est fixée à gauche par $(a_1 \ \ldots \ a_p)$, donc l'égalité $\overset{?}{=}$ est encore vraie, trivialement. □

Ainsi, nous introduisons la copie $E' := E$. Alors la permutation $\rho \colon E \longrightarrow E'$ effectue une « *équivalence* » entre E et E', au sens où l'on a les deux bijections réciproques l'une de l'autre :

$$\begin{aligned} E \ \ni \ a \ &\longmapsto \ \rho(a) := a' \ \in E', \\ E \ \ni \ a := \rho^{-1}(a') \ &\longmapsfrom \ a' \ \in E'. \end{aligned}$$

Une « *équivalence* » échange les deux ensembles fondamentaux en lesquels E et E' se décomposent :

$$\begin{array}{ccccc} & E & = & \mathsf{Fix}\,\sigma & \cup & \mathsf{Supp}\,\sigma \\ \rho & \downarrow & & \downarrow & & \downarrow \\ & E' & = & \mathsf{Fix}\,\sigma' & \cup & \mathsf{Supp}\,\sigma' \end{array}$$

Proposition 4.2. *Une conjugaison $\rho \circ \sigma \circ \rho^{-1} = \sigma'$ induit les deux transferts d'ensembles :*

$$\begin{aligned} \rho\big(\mathsf{Fix}\,\sigma\big) \ &= \ \mathsf{Fix}\,\sigma', \\ \rho\big(\mathsf{Supp}\,\sigma\big) \ &= \ \mathsf{Supp}\,\sigma'. \end{aligned}$$

Démonstration. Montrons que $\rho\big(\mathsf{Fix}\,\sigma\big) \subset \mathsf{Fix}\,\sigma'$. Soit $a \in \mathsf{Fix}\,\sigma$, c'est-à-dire $\sigma(a) = a$. Alors on a bien $\rho(a) \in \mathsf{Fix}\,\sigma'$, car :

$$\sigma'\big(\rho(a)\big) \ = \ \rho \circ \sigma \circ \rho^{-1}\big(\rho(a)\big) \ = \ \rho\big(\sigma(a)\big) \ = \ \rho(a).$$

L'inclusion inverse $\rho\big(\mathsf{Fix}\,\sigma\big) \supset \mathsf{Fix}\,\sigma'$, qui est équivalente à $\rho^{-1}\big(\mathsf{Fix}\,\sigma'\big) \subset \mathsf{Fix}\,\sigma$, se démontre pareillement en intervertissant les rôles de σ et de σ', grâce à $\sigma = \rho^{-1} \circ \sigma' \circ \rho$.

Donc $\rho\big(\mathsf{Fix}\,\sigma\big) = \mathsf{Fix}\,\sigma'$.

Enfin, les supports étant les complémentaires des ensembles de points fixes, et ρ étant une bijection, il vient automatiquement $\rho\big(\mathsf{Supp}\,\sigma\big) = \mathsf{Supp}\,\sigma'$. □

Ensuite, soit un entier $2 \leqslant p \leqslant n = |E|$, et soient deux brochettes de p éléments :

$$\begin{matrix} a_1 \\ \vdots \\ a_p \end{matrix} \quad \text{distincts } \in E \qquad\qquad \begin{matrix} a'_1 \\ \vdots \\ a'_p \end{matrix} \quad \text{distincts } \in E' = E.$$

Alors l'application bijective de morceau d'agneau à morceau de bœuf en passant par les dents de l'ogre gaulois :

$$\begin{matrix} a_1 & \longmapsto & a'_1 \\ \vdots & & \vdots \\ a_p & \longmapsto & a_{p'}, \end{matrix}$$

peut être prolongée en une permutation $\rho \in \mathfrak{S}(E)$, simplement en numérotant les $n-p$ autres éléments $a_{p+1}, \dots, a_n$ de E ainsi que les $n-p$ autres éléments $a'_{p+1}, \dots, a'_n$ de $E' = E$, et en assignant de manière analogue :

$$\rho\big(a_{p+1}\big) := a'_{p+1}, \ \dots\dots, \ \rho\big(a_n\big) := a'_n.$$

Proposition 4.3. *Deux cycles quelconques de même longueur sont toujours conjugués dans* $\mathfrak{S}(E)$.

Démonstration. Soient donc $\big(a_1 \dots, a_p\big)$ et $\big(a'_1 \dots a'_p\big)$ deux cycles, de longueurs égales $p \geqslant 2$. Nous venons de produire $\rho \in \mathfrak{S}(E)$ satisfaisant $\rho(a_i) = a'_i$, pour $i = 1, \dots, n$. Alors la Proposition 4.1 conclut :

$$\rho \circ \big(a_1 \ \cdots \ a_p\big) \circ \rho^{-1} = \big(a'_1 \ \cdots \ a'_p\big). \qquad \square$$

Corollaire 4.4. *Deux transpositions arbitraires sont toujours conjugués dans* $\mathfrak{S}(E)$. $\square$

Exemple 4.5. Maintenant, nous affirmons que les deux éléments de $\mathfrak{S}(E)$ où $E = \{1, \dots, 7\}$:

$$\sigma := (1\ 3\ 5) \circ (2\ 4) \qquad \text{et} \qquad (1\ 2\ 3) \circ (6\ 7),$$

sont *conjugués* dans $\mathfrak{S}_7$. Notons qu'ils ont chacun *deux* cycles de mêmes longueurs $3, 2$.

Clairement :

$$\mathsf{Fix}\,\sigma = \{6, 7\} \qquad \text{et} \qquad \mathsf{Fix}\,\sigma' = \{4, 5\}.$$

D'après la Proposition 4.2, une équivalence ρ satisfaisant $\rho \circ \sigma \circ \rho^{-1} = \sigma'$ doit envoyer $\{6, 7\}$ sur $\{4, 5\}$. De plus, on devine évidemment que ρ doit envoyer les cycles de σ sur les cycles de σ' *de mêmes longueurs* :

$$\begin{matrix} 6 & 7 \\ \downarrow & \downarrow \\ 4 & 5 \end{matrix} \qquad \begin{matrix} 1 & 3 & 5 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{matrix} \qquad \begin{matrix} 2 & 4 \\ \downarrow & \downarrow \\ 6 & 7 \end{matrix}.$$

Si on préfère, pour faciliter les calculs manuels, on peut rajouter les points fixes dans l'écriture, en étendant[5] la notation $(a_1 \cdots a_p)$ au cas $p = 1$, c'est-à-dire $(a_1) = \mathsf{Id}$. Ainsi,

5. Mais attention ! ! ! (a_1) n'est *pas* un cycle, car dans la Définition 3.8, on demande expressément que $p \geqslant 2$! !

on pourra écrire σ et σ' en ordonnant leurs cycles respectifs (qui commutent) par longueur décroissante :

$$\sigma \;=\; \big(1\ 3\ 5\big)\,\big(2\ 4\big)\,(6)\,(7),$$
$$\sigma \;=\; \big(1\ 2\ 3\big)\,\big(6\ 7\big)\,(4)\,(5),$$

afin de faire apparaître des correspondances verticales qui définissent une permutation-candidate :

$$\rho \;:=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 6 & 2 & 7 & 3 & 4 & 5 \end{pmatrix},$$

pour conjuguer σ à $\sigma' = \rho \circ \sigma \circ \rho^{-1}$.

Nous laissons au lecteur-étudiant le soin de vérifier que cette permutation naturelle ρ fonctionne.

Cette vérification est d'ailleurs essentiellement inutile, car nous avons déjà deviné le résultat complètement général.

Théorème 4.6. *Pour deux permutations $\sigma \in \mathfrak{S}(E)$ et $\sigma' \in \mathfrak{S}(E)$, on a équivalence entre :*
(i) *σ et σ' sont* conjuguées, i.e. *il existe une équivalence $\rho \in \mathfrak{S}(E)$ telle que $\rho\circ\sigma\circ\rho^{-1} = \sigma'$;*
(ii) *les listes (avec répétitions) des longueurs décroissantes des cycles (commutant entre eux) à supports disjoints qui les composent :*

$$\sigma \;=\; \big(a_1^1\ \cdots\ a_{p_1}^1\big)\,\big(a_1^2\ \cdots\ a_{p_2}^2\big)\ \cdots\ \big(a_1^i\ \cdots\ a_{p_i}^i\big)\cdots\ \big(a_1^r\ \cdots\ a_{p_r}^r\big),$$
$$\sigma' \;=\; \big(a_1'^1\ \cdots\ a_{p_1'}'^1\big)\,\big(a_1'^2\ \cdots\ a_{p_2'}'^2\big)\ \cdots\ \big(a_1'^i\ \cdots\ a_{p_i'}'^i\big)\cdots\ \big(a_1'^{r'}\ \cdots\ a_{p_{r'}'}'^{r'}\big),$$

avec :

$$p_1 \geqslant p_2 \geqslant \cdots \geqslant p_i \geqslant \cdots \geqslant p_r \geqslant 2,$$
$$p_1' \geqslant p_2' \geqslant \cdots \geqslant p_i' \geqslant \cdots \geqslant p_{r'}' \geqslant 2,$$

sont identiques, *c'est-à-dire que :*

$$r \;=\; r' \qquad\qquad \textit{et} \qquad\qquad p_1 \;=\; p_1',\ \ \ldots\ p_r \;=\; p_r'.$$

Démonstration. **(i)** $\Longrightarrow$ **(ii)**. Supposons donc que $\rho \circ \sigma \circ \rho^{-1} = \sigma'$, avec une $\rho \in \mathfrak{S}(E)$. Décomposons $\sigma = \sigma_1\circ\sigma_2\circ\cdots\circ\sigma_r$ en produit (commutatif) de cycles à supports disjoints, et de longueurs ordonnées de manière croissante, grâce au Théorème 3.12 — en supprimant les lettres ω —, et écrivons :

$$\begin{aligned}\sigma' \;&=\; \rho \circ \sigma \circ \rho^{-1} \\ &=\; \big(\rho \circ \sigma_1 \circ \rho^{-1}\big) \circ \big(\rho \circ \sigma_2 \circ \rho^{-1}\big) \circ \cdots \circ \big(\rho \circ \sigma_r \circ \rho^{-1}\big).\end{aligned}$$

Grâce à la Proposition 4.1, pour tout $1 \leqslant i \leqslant r$, la permutation :

$$\sigma_i' \;:=\; \rho \circ \sigma_i \circ \rho^{-1},$$

est un cycle de même longueur que σ_i, à savoir p_i.

Or d'après la Proposition 4.2, le support de σ' est l'image du support de σ par ρ. De plus, comme ρ est bijective, et comme les supports des σ_i sont disjoints, il en va de même des supports des permutations σ_i', lesquelles commutent, donc.

Par l'*unicité* de la décomposition en cycles donnée par le Théorème 3.12, il est *nécessaire* que :

$$\sigma' \;=\; \sigma_1' \circ \cdots \circ \sigma_i' \circ \cdots \circ \sigma_r',$$

soit la décomposition de σ' en produit de cycles à supports disjoints. Ainsi, on a bien $r = r'$ et $p_i = p'_i$ pour $i = 1, \ldots, r$.

(ii) $\Longrightarrow$ (i). Écrivons alors, en spécifiant le parallèle vertical :

$$\begin{aligned}\sigma \ &= \ \big(a_1^1 \ \cdots \ a_{p_1}^1\big)\,\big(a_1^2 \ \cdots \ a_{p_2}^2\big) \ \cdots \ \big(a_1^i \ \cdots \ a_{p_i}^i\big) \ \cdots \ \big(a_1^r \ \cdots \ a_{p_r}^r\big),\\ \sigma' \ &= \ \big(a_1'^1 \ \cdots \ a_{p_1}'^1\big)\,\big(a_1'^2 \ \cdots \ a_{p_2}'^2\big) \ \cdots \ \big(a_1'^i \ \cdots \ a_{p_i}'^i\big) \ \cdots \ \big(a_1'^r \ \cdots \ a_{p_r}'^r\big),\end{aligned}$$

où nous avons remplacé $r' := r$, et chaque $p'_i := p_i$ aussi. Par définition, les $p_1 + \cdots + p_r$ éléments $a^i_{\ell_i}$ sont distincts entre eux, et de même pour les $a'^i_{\ell_i}$.

Posons :

$$s \ := \ n - \big(p_1 + \cdots + p_r\big),$$

et notons :

$$\begin{aligned}E\big\backslash\big\{a^i_{\ell_i}\big\} \ &= \ \big\{b_1, b_2, \ldots, b_s\big\} \ = \ \mathsf{Fix}\,\sigma,\\ E'\big\backslash\big\{a'^i_{\ell_i}\big\} \ &= \ \big\{b'_1, b'_2, \ldots, b'_s\big\} \ = \ \mathsf{Fix}\,\sigma'.\end{aligned}$$

Assertion 4.7. *La bijection $\rho\colon\ E \longrightarrow E'$ définie par :*

$$\begin{array}{ccccccccccc} a_1^1 & \cdots & a_{p_1}^1 & & & a_1^r & \cdots & a_{p_r}^r & & b_1 \ b_2 & \cdots & b_s \\ \downarrow & \cdots & \downarrow & & \cdots & \downarrow & \cdots & \downarrow & & \downarrow \ \downarrow & \cdots & \downarrow \\ a_1'^1 & \cdots & a_{p_1}'^1, & & & a_1'^r & \cdots & a_{p_r}'^r, & & b'_1 \ b'_2 & \cdots & b'_s, \end{array}$$

conjugue $\sigma' = \rho \circ \sigma \circ \rho^{-1}$.

Preuve. Montrons en effet que $\sigma' \circ \rho\,(c) \overset{?}{=} \rho \circ \sigma\,(c)$ pour tout élément $c \in E$.

Puisqu'un cycle $\big(a_1^i \ \cdots \ a_{p_i}^i\big)$ envoie le dernier élément $a_{p_i}^i$ sur le premier a_1^i, adoptons la convention que $a^i_{p_i+1} := a^i_1$.

Alors premièrement, on a bien :

$$\sigma' \circ \rho\,\big(a^i_{\ell_i}\big) \ = \ \sigma'\big(a'^i_{\ell_i}\big) \ = \ a'^i_{\ell_i+1} \ = \ \rho\big(a^i_{\ell_i+1}\big) \ = \ \rho \circ \sigma\,\big(a^i_{\ell_i}\big).$$

Et deuxièmement, pour $c = b_j$, on a aussi bien :

$$\sigma' \circ \rho\,(b_j) \ = \ \sigma'\big(b'_j\big) \ = \ b'_j \ = \ \rho(b_j) \ = \ \rho \circ \sigma\,(b_j). \qquad \square$$

En conclusion, cette permutation ρ convient. Elle n'est en général pas unique, car par exemple, des numérotations différentes de $\mathsf{Fix}\,\sigma$ et de $\mathsf{Fix}\,\sigma'$ conduisent à des ρ différentes. $\square$

5. Classes de conjugaison de $\mathfrak{S}(E)$ et partitions

Eu égard au Théorème 4.6, nous sommes ramenés à lister toutes les longueurs possibles de cycles disjoints contenus dans E. Nous allons donc maintenant donner un résultat qui permet d'élaborer de telles listes. Commençons par une

Définition 5.1. Une *partition* d'un entier $n \geqslant 1$ est une suite d'entiers :

$$\boldsymbol{p} \ = \ \big\{p_1, \ \ldots, \ p_t\big\},$$

ordonnés de manière décroissante :

$$p_1 \ \geqslant \ p_2 \ \geqslant \ \cdots \ \geqslant \ p_{t-1} \ \geqslant \ p_t \ \geqslant \ 1,$$

dont la somme vaut :

$$n \ = \ p_1 + p_2 + \cdots + p_{t-1} + p_t.$$

L'entier $t \geqslant 1$ est autorisé à varier. Par exemple, voici toutes les partitions des cinq premiers entiers $n = 1, 2, 3, 4, 5$:

$$
\begin{aligned}
&1,\\
&2 = 1+1,\\
&3 = 2+1 = 1+1+1,\\
&4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1,\\
&5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1.
\end{aligned}
$$

Par abus de cervoise, on confondra souvent la suite finie $\boldsymbol{p} = \{p_1, \ldots, p_t\}$ à la somme explicite qui lui est associée.

Notation 5.2. L'ensemble des partitions de n sera noté $\boldsymbol{P}_n$.

Avec $n = 9$, notre exemple-Idéfix :

$$
\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix} = (1\ 4\ 5\ 8)\,(3\ 7\ 9)\,(2)\,(6),
$$

représente la partition :

$$
9 = 4+3+1+1.
$$

Définition 5.3. Le *type* d'une permutation $\sigma \in \mathfrak{S}(E)$ avec $|E| = n \geqslant 2$, est la partition $\boldsymbol{p}(\sigma)$ de n dont les éléments sont les cardinaux des diverses orbites de σ, rangés par ordre décroissant.

En supposant σ décomposée comme produit (commutatif) de cycles à supports disjoints :

$$
\sigma = \big(a_1^1\ \cdots\ a_{p_1}^1\big)\,\big(a_1^2\ \cdots\ a_{p_2}^2\big)\ \cdots\ \big(a_1^r\ \cdots\ a_{p_r}^r\big)\,\big(b_1\big)\,\big(b_2\big)\ \cdots\ \big(b_s\big),
$$

avec :

$$
p_1 \geqslant p_2 \geqslant \cdots \geqslant p_r \geqslant 2,
$$

et avec le nombre suivant de points fixes b_j indiqués en queue de cohorte romaine :

$$
s := n - \big(p_1 + \cdots + p_r\big),
$$

il est clair que le type de σ est :

$$
\boldsymbol{p}(\sigma) := p_1 + \cdots + p_r + 1 + \cdots + 1.
$$

Inversement, en partant d'une énumération quelconque des n éléments de E :

$$
E := \big\{a_1,\, a_2,\, \ldots,\, a_n\big\},
$$

pour n'importe quelle partition $\boldsymbol{p}$ de :

$$
n = p_1 + \cdots + p_r + 1 + \cdots + 1,
$$

la permutation $\sigma_{\boldsymbol{p}} \in \mathfrak{S}(E)$ suivante :

$$
\sigma_{\boldsymbol{p}} := \big(a_1\ \cdots\ a_{p_1}\big)\,\big(a_{p_1+1}\ \cdots\ a_{p_1+p_2}\big)\ \cdots\ \big(a_{p_1+\cdots+p_{r-1}}\ \cdots\ a_{p_1+\cdots+p_{r-1}+p_r}\big),
$$

dans laquelle nous n'écrivons pas à la fin les points fixes sous forme (a_ℓ), a visiblement pour type la partition $\boldsymbol{p}$ dont elle provient.

Si $\sigma \in \mathfrak{S}(E)$ est une permutation arbitraire, notons la *classe de conjugaison* de σ :

$$
\mathsf{Conj}\,\sigma := \big\{\rho \circ \sigma \circ \rho^{-1} :\ \rho \in \mathfrak{S}(E)\big\},
$$

laquelle est une classe d'équivalence pour la relation de conjugaison.

Théorème 5.4. *L'application :*

$$p \longrightarrow \mathsf{Conj}\,\sigma_p$$

est une bijection de l'ensemble $\boldsymbol{P}_n$ des partitions de n sur l'ensemble de toutes les classes de conjugaisons de $\mathfrak{S}(E)$.

Démonstration. En effet, nous avons vu dans ce qui précède que σ_p est un *représentant* de chaque classe de conjugaison. □

6. Systèmes de générateurs

Dans cette section, nous exhibons des systèmes variés de générateurs pour le groupe symétrique $\mathfrak{S}_n$ de l'ensemble $E := \{1, \dots, n\}$.

Rappelons qu'une collection d'éléments $\gamma_1, \dots, \gamma_c \in \mathfrak{S}(E)$ est dite être un *système de générateurs* pour $\mathfrak{S}(E)$ si toute permutation $\sigma \in \mathfrak{S}(E)$ peut s'écrire comme composition finie de $\gamma_1, \dots, \gamma_c$, et de leurs inverses $\gamma_1^{-1}, \dots, \gamma_c^{-1}$. Quand $\gamma_1, \dots, \gamma_c$ sont des transpositions, donc égales à leurs inverses, il suffit de considérer $\gamma_1, \dots, \gamma_c$.

Proposition 6.1. *Le groupe $\mathfrak{S}_n$ est engendré par chacune des deux familles suivantes de transpositions :*

(1) *les transpositions $(1\ i)$ avec $2 \leqslant i \leqslant n$;*

(2) *les transpositions $\big(\ell\ \ \ell+1\big)$ avec $1 \leqslant \ell \leqslant n-1$.*

Démonstration. **(1)** Puisque toute permutation est composition de transpositions grâce au Théorème 3.19, il suffit de faire voir que toute transposition quelconque $(i\ j)$ avec $1 \leqslant i < j \leqslant n$ est une composition (finie) de transpositions de la forme $(1\ i)$ avec $1 \leqslant i \leqslant n$.

Or une vérification aisée, ou une application directe de la Proposition 4.1, montrent que :

$$\big(i\ j\big) \;=\; \big(1\ i\big) \circ \big(1\ j\big) \circ \underbrace{\big(1\ i\big)}_{=\,(1\ i)^{-1}} .$$

(2) De même, il suffit de montrer que toute transposition $(i\ j)$ avec $j - i \geqslant 2$ est composition finie de transpositions de la forme $(\ell\ \ \ell+1)$ avec $1 \leqslant \ell \leqslant n-1$.

Or en introduisant le « changement de coordonnées » :

$$\rho := \big(i\ \ i+1\ \cdots\ j-1\big),$$

la fameuse Proposition 4.1 nous donne :

$$\begin{aligned}\big(i\ \ i+1\ \cdots\ j-1\big) \circ \big(j-1\ \ j\big) \circ \big(i\ \ i+1\ \cdots\ j-1\big)^{-1} &= \rho \circ \big(j-1\ \ j\big) \circ \rho^{-1} \\ &= \big(\rho(j-1)\ \ \rho(j)\big) \\ &= \big(i\ j\big).\end{aligned}$$

Il reste alors seulement à faire observer — par réminiscence de la démonstration du Théorème 3.19 — que cette permutation cyclique :

$$\rho \;=\; \big(i\ \ i+1\ \cdots\ j-1\big) \;=\; \big(i\ \ i+1\big) \circ \cdots \circ \big(j-2\ \ j-1\big),$$

est composition finie de transpositions de la forme $(\ell\ \ \ell+1)$. Son inverse ρ^{-1} jouit alors de la même propriété (exercice mental).

Donc $(i\ j)$ en bas à droite est bien représentée comme composition finie en haut à gauche de transpositions de la forme $(\ell\ \ \ell+1)$. □

Par rapport au Théorème 3.19 qui disait que les $\frac{n(n-1)}{2}$ transpositions $(i\ j)$ engendrent $\mathfrak{S}_n$, cette proposition apporte un certain gain d'économie, en trouvant deux systèmes de $n-1 < \frac{n(n-1)}{2}$ transpositions génératrices. Encore mieux :

Proposition 6.2. *Le groupe $\mathfrak{S}_n$ est engendré par la transposition $(1\ 2)$ et le n-cycle $\big(1\ 2\ \cdots\ n\big)$.*

Démonstration. Grâce à la Proposition 6.1 **(2)** que nous venons d'obtenir, les transpositions $\big(\ell\ \ \ell+1\big)$ avec $1 \leqslant \ell \leqslant n-1$ engendrent $\mathfrak{S}_n$. Il suffit donc de représenter chaque $\big(\ell\ \ \ell+1\big)$ au moyen de $(1\ 2)$ et de $\big(1\ 2\ \cdots\ n\big)$.

Pour $1 \leqslant \ell \leqslant n-1$, la permutation itérée :

$$\rho_\ell \ := \ \big(1\ 2\ \cdots\ n\big)^{\ell-1},$$

envoie 1 sur ℓ, et 2 sur $\ell+1$. Encore grâce à la Proposition-star 4.1, quand on utilise ρ_ℓ pour « changer de coordonnées » :

$$\begin{aligned}\big(\ell\ \ \ell+1\big) \ &= \ \big(\rho_\ell(1)\ \rho_\ell(2)\big) \\ &= \ \big(1\ 2\ \ldots\ n\big)^{\ell-1} \circ \big(1\ 2\big) \circ \big(1\ 2\ \ldots\ n\big)^{-\ell+1},\end{aligned}$$

on constate agréablement que $\big(\ell\ \ \ell+1\big)$ appartient effectivement au sous-groupe engendré par $(1\ 2)$ et $\big(1\ 2\ \cdots\ n\big)$. □

Deux générateurs seulement ! Pour un groupe de cardinal exponentiellement grand, égal à $n!$!

Toutefois, ce résultat devient faux en général si l'on remplace $(1\ 2)$ et $\big(1\ 2\ \cdots\ n\big)$ par une transposition et un n-cycle arbitraires, comme propose d'y réfléchir l'Exercice 1.

7. Groupe alterné

Toujours avec un ensemble fini E de cardinal $|E| = n \geqslant 2$, soit une permutation arbitraire $\sigma \in \mathfrak{S}(E)$. Grâce au Théorème 3.19, nous pouvons représenter :

$$\sigma \ = \ \tau_1 \circ \cdots \circ \tau_r,$$

comme produit (composition) d'un nombre fini $r \geqslant 1$ de transpositions, *mais* une telle représentation n'a absolument rien d'unique, puisqu'on peut insérer partout des couples du type $\tau_* \circ \tau_*^{-1} = \mathsf{Id}$, où τ_* est une transposition quelconque.

Que pourrions-nous dire, alors, lorsque nous avons plusieurs représentations différentes, par exemple deux :

$$\tau_1 \circ \cdots \circ \tau_r \ = \ \sigma \ = \ \tau'_1 \circ \cdots \circ \tau'_{r'} \ \textbf{?}.$$

Théorème 7.1. *La parité du nombre de transpositions nécessaires pour représenter une permutation donnée est un invariant qui ne dépend que de la permutation :*

$$r \ \equiv \ r' \mod 2.$$

Tiens, encore de l'arithmétique qui s'invite ! Pour manger du sanglier rôti !

Démonstration. Après multiplication à gauche :

$$\tau_r \circ \cdots \circ \tau_1 \Big(\ \tau_1 \circ \cdots \circ \tau_r \ = \ \tau'_1 \circ \cdots \circ \tau'_{r'} \ \Big)$$

il vient :

$$\mathsf{Id} \ = \ \tau_1 \circ \cdots \circ \tau_r \circ \tau'_1 \circ \cdots \circ \tau'_{r'},$$

et avec $r + r' =: s$, tout repose sur l'énoncé crucial suivant.

Proposition 7.2. *Si l'identité est représentée comme une composition de s transpositions :*

$$\mathsf{Id} \;=\; \tau_1 \circ \cdots \circ \tau_s,$$

alors $s \in 2\,\mathbb{N}$ est nécessairement pair.

Démonstration. Le cas $n = |E| = 2$ est spécial-facile, car :

$$\mathfrak{S}\big(\{1,2\}\big) \;=\; \big\{\mathsf{Id},\ (1\ 2)\big\},$$

et toute puissance impaire de la transposition $(1\ 2)$ est égale à $(1\ 2)$, tandis que toute puissance paire est égale à Id.

Nous pouvons donc supposer que $n \geqslant 3$, et admettre en raisonnant par récurrence que l'énoncé est vrai pour les permutations de l'ensemble $\{1, \ldots, n-1\}$ à $n-1$ éléments.

Par exemple dans le cas où $E = \{1,2,3,4,5,6,7\}$, c'est-à-dire avec $n = 7$, pour la composition suivante de 5 transpositions :

$$(1\ 7) \circ (2\ 3) \circ (5\ 6) \circ (4\ 7) \circ (4\ 5),$$

l'idée-clé consiste à déplacer vers la droite toutes les transpositions qui incorporent $n = 7$, ce que l'énoncé suivant va nous permettre de faire.

Assertion 7.3. *Pour tous indices distincts deux à deux i, j, k avec $1 \leqslant i, j, k \leqslant n-1$, on a :*

$$\begin{aligned}
(i\ n) \circ (j\ k) &\overset{1}{=} (j\ k) \circ (i\ n),\\
(i\ n) \circ (i\ j) &\overset{2}{=} (i\ j) \circ (j\ n),\\
(i\ n) \circ (j\ n) &\overset{3}{=} (i\ j) \circ (i\ n),\\
(i\ n) \circ (i\ n) &\overset{4}{=} \mathsf{Id}.
\end{aligned}$$

L'exemple en question pourra alors effectivement être soumis à ces procédés :

$$\begin{aligned}
(1\ 7) \circ (2\ 3) \circ (5\ 6) \circ (4\ 7) \circ (4\ 5) &\overset{2}{=} (1\ 7) \circ (2\ 3) \circ (5\ 6) \circ (4\ 5) \circ (5\ 7)\\
&\overset{1}{=} (2\ 3) \circ (5\ 6) \circ (4\ 5) \circ (1\ 7) \circ (5\ 7)\\
&\overset{3}{=} (2\ 3) \circ (5\ 6) \circ (4\ 5) \circ (1\ 5) \circ (1\ 7).
\end{aligned}$$

Preuve. L'égalité de commutation $\overset{1}{=}$ est connue, puisque les supports sont disjoints.

Ensuite, vérifions l'égalité $\overset{2}{=}$ comme suit, sans écrire les éléments non concernés car fixés :

$$\begin{array}{cccc}
 & i & j & n \\
(i\ j) & \downarrow & \downarrow & \downarrow \\
 & j & i & n \\
(i\ n) & \downarrow & \downarrow & \downarrow \\
 & j & n & i
\end{array}
\quad \overset{?}{=} \quad
\begin{array}{cccc}
i & j & n & \\
\downarrow & \downarrow & \downarrow & (j\ n) \\
i & n & j & \\
\downarrow & \downarrow & \downarrow & (i\ j) \\
j & n & i &
\end{array}
\qquad \text{OUI !}$$

Puis, vérifions l'égalité $\overset{3}{=}$ comme suit :

$$\begin{array}{cccc} & i & j & n \\ (j\ n) & \downarrow & \downarrow & \downarrow \\ & i & n & j \\ (i\ n) & \downarrow & \downarrow & \downarrow \\ & n & i & j \end{array} \quad \overset{?}{=} \quad \begin{array}{cccc} i & j & n & \\ \downarrow & \downarrow & \downarrow & (i\ n) \\ n & j & i & \\ \downarrow & \downarrow & \downarrow & (i\ j) \\ n & i & j & \end{array} \qquad \text{OUI !}$$

Enfin, l'égalité $\overset{4}{=}$ est triviale. □

Grâce aux deux relations $\overset{1}{=}$, $\overset{2}{=}$, nous pouvons « repousser » à la fin toutes les transpositions du type $(i\ n)$ avec $1 \leqslant i \leqslant n-1$, ce qui ne change pas le nombre, s, de transpositions dans l'identité $\mathsf{Id} = \tau_1 \circ \cdots \circ \tau_s$.

Ensuite, grâce aux relations $\overset{3}{=}$, $\overset{4}{=}$, nous pouvons contracter toutes les paires successives à la fin $(i\ n) \circ (j\ n)$ de manière à ne conserver qu'au plus une seule occurrence de n. Comme $\overset{3}{=}$, $\overset{4}{=}$ transforment deux transpositions en deux ou en zéro transpositions, à chaque opération $\overset{3}{=}$, $\overset{4}{=}$, la *parité* du nombre de transpositions demeure invariante. Yep !

Une fois ce travail de normalisation achevé, il ne peut rester à la fin qu'*au plus une* transposition du type $(i\ n)$, et donc il y a deux cas à considérer.

Cas 1 :

$$\mathsf{Id} \ = \ \tau'_1 \circ \cdots \circ \tau'_{s'} \circ (i\ n),$$

avec $s' + 1 \equiv s \mod 2$, et avec des transpositions $\tau'_1, \ldots, \tau'_{s'}$ du *sous-ensemble* $\{1, \ldots, n-1\}$. Mais ce cas est impossible ! Car il impliquerait :

$$\tau'_1 \circ \cdots \circ \tau'_{s'} \ = \ (i\ n),$$

c'est-à-dire qu'une permutation de $\{1, \ldots, n-1\}$ serait égalée à une transformation faisant intervenir l'extraterrestre n — contradiction.

Cas 2 :

$$\mathsf{Id} \ = \ \tau'_1 \circ \cdots \circ \tau'_{s'},$$

avec de même $s' \equiv s \mod 2$, où $\tau'_1, \ldots, \tau'_{s'}$ sont à nouveau des permutations de $\{1, \ldots, n-1\}$. Par récurrence évidente sur n, nous concluons :

$$\begin{aligned} 2 \ &\equiv \ s' \mod 2 \\ &\equiv \ s \mod 2. \end{aligned}$$

□

Ainsi, $s = r + r' \in 2\,\mathbb{N}$ est pair, et il est clair que ceci garantit que $r \equiv r' \mod 2$ comme annoncé. □

Ce théorème justifie alors le fait que la définition suivante ait un sens rigoureux.

Définition 7.4. La *signature* d'une permutation arbitraire $\sigma \in \mathfrak{S}(E)$ est l'élément de $\{-1, +1\}$ noté :

$$\varepsilon(\sigma) \ := \ (-1)^r,$$

où $\tau_1 \circ \cdots \circ \tau_r = \sigma$ est une représentation quelconque de σ comme composition de transpositions.

Théorème 7.5. *Soit E un ensemble fini de cardinal $|E| = n \geqslant 2$.*
(1) *La signature de l'identité vaut $1 = \varepsilon(\mathsf{Id})$.*
(2) *La signature d'une transposition τ vaut toujours $-1 = \varepsilon(\tau)$.*
(3) *Pour toutes permutations $\sigma, \sigma' \in \mathfrak{S}(E)$, on a $\varepsilon\big(\sigma \circ \sigma'\big) = \varepsilon(\sigma) \cdot \varepsilon(\sigma')$.*
(4) *Pour toute permutation $\sigma \in \mathfrak{S}(E)$, on a $\varepsilon\big(\sigma^{-1}\big) = \frac{1}{\varepsilon(\sigma)} = \varepsilon(\sigma)$.*

Ces propriétés expriment notamment que l'application de signature :

$$\begin{array}{rccc} \varepsilon\colon & \mathfrak{S}(E) & \longrightarrow & \{-1,+1\} \\ & \sigma & \longmapsto & \varepsilon(\sigma), \end{array}$$

est un morphisme de groupes, où $\{-1,+1\}$ est muni de la loi de multiplication standard.

Démonstration. Nous ne détaillerons que **(3)**, puisque les autres propriétés sont évidentes. Soient deux représentations :

$$\sigma \,=\, \tau_1 \circ \cdots \circ \tau_r \qquad\qquad \text{et} \qquad\qquad \sigma' \,=\, \tau'_1 \circ \cdots \circ \tau'_{r'},$$

comme compositions de transpositions. Alors leur composition possède la représentation suivante :

$$\sigma \circ \sigma' \,=\, \tau_1 \circ \cdots \circ \tau_r \circ \tau'_1 \circ \cdots \circ \tau'_{r'}$$

et donc on a bien :

$$\varepsilon\big(\sigma \circ \sigma'\big) \,=\, (-1)^{r+r'} \,=\, (-1)^r \cdot (-1)^{r'} \,=\, \varepsilon(\sigma) \cdot \varepsilon(\sigma'). \qquad \square$$

Théorème 7.6. *Soit E un ensemble fini de cardinal $|E| = n \geqslant 2$. Alors la signature :*

$$\varepsilon\colon \quad \mathfrak{S}(E) \;\longrightarrow\; \{-1,+1\},$$

*est l'*unique *morphisme non trivial de groupes :*

$$\xi\colon \quad \mathfrak{S}(E) \;\longrightarrow\; \mathbb{C}^\times.$$

Ici, $\mathbb{C}^\times = \big\{z \in \mathbb{C}\colon\ z \neq 0\big\}$ est le groupe multiplicatif des nombres complexes non nuls, pour la multiplication standard. Évidemment, $\{-1,+1\} \subset \mathbb{C}^\times$. En particulier, ce théorème dit que les seules valeurs possibles d'un morphisme de groupes $\mathfrak{S}(E) \longrightarrow \mathbb{C}^\times$ sont -1 et $+1$.

Démonstration. Soit donc $\xi\colon \mathfrak{S}(E) \longrightarrow \mathbb{C}^\times$ un tel morphisme de groupes. À toute permutation $\sigma \in \mathfrak{S}(E)$, ce morphisme associe un nombre réel non nul $\xi(\sigma) \in \mathbb{C}^\times$. Évidemment, $\xi(\mathsf{Id}) = 1$.

Assertion 7.7. *ξ est constant sur les classes de conjugaison de $\mathfrak{S}(E)$.*

Preuve. En effet, si $\sigma' = \rho \circ \sigma \circ \rho^{-1}$ est conjugué à σ via une certaine permutation $\rho \in \mathfrak{S}(E)$, la commutativité de la multiplication dans $\mathbb{C}^\times$ donne :

$$\begin{aligned} \xi(\sigma') \,&=\, \xi\big(\rho \circ \sigma \circ \rho^{-1}\big) \\ &=\, \xi(\rho)\, \xi(\sigma)\, \xi(\rho^{-1}) \\ &=\, \xi(\rho)\, \tfrac{1}{\xi(\rho)}\, \xi(\sigma) \\ &=\, \xi(\sigma). \end{aligned} \qquad \square$$

Assertion 7.8. *Pour toute transposition $\tau \in \mathfrak{S}(E)$, on a $\xi(\tau) = \pm 1$.*

Preuve. Comme $\tau^2 = \mathsf{Id}$, il vient :

$$\xi(\tau)^2 \,=\, \xi(\mathsf{Id}) \,=\, 1. \qquad \square$$

Ensuite, rappelons que d'après le Corollaire 4.4, toutes les transpositions sont conjuguées entre elles, c'est-à-dire forment *une seule* classe de conjugaison.

Assertion 7.9. *$\xi(\tau)$ prend une seule et même valeur sur toutes les transpositions :*

$$\Big(\ \xi(\tau) \,=\, 1 \quad \forall\, \tau \,\in\, \mathfrak{S}(E)\ \Big) \qquad \textit{ou} \qquad \Big(\ \xi(\tau) \,=\, -1 \quad \forall\, \tau \,\in\, \mathfrak{S}(E)\ \Big). \qquad \square$$

La première possibilité $\xi(\tau) = 1$ impliquerait, puisque toute permutation $\sigma = \tau_1 \circ \cdots \circ \tau_r$ s'écrit comme produit de transpositions, que :

$$\xi(\sigma) \,=\, \xi\big(\tau_1 \circ \cdots \circ \tau_r\big) \,=\, \xi(\tau_1) \cdots \xi(\tau_r) \,=\, 1 \cdots 1 \,=\, 1,$$

en contradiction avec l'hypothèse que le morphisme ξ est non trivial.

Donc seule la seconde possibilité est valide, à savoir $\xi(\tau) = -1$ sur toute transposition, et le même calcul conclut la démonstration d'unicité :

$$\begin{aligned} \xi(\sigma) \,&=\, \xi\big(\tau_1 \circ \cdots \circ \tau_r\big) \\ &=\, \xi(\tau_1) \cdots \xi(\tau_r) \\ &=\, (-1) \cdots (-1) \\ &=\, (-1)^r \\ &=\, \varepsilon(\sigma). \end{aligned} \qquad \square$$

Proposition 7.10. *La signature d'un p-cycle $\big(a_1 \ \cdots \ a_p\big)$ avec $p \geqslant 2$ est égale à $(-1)^{p-1}$.*

Démonstration. En effet, on sait qu'un p-cycle est composition de $p - 1$ transpositions :

$$\big(a_1 \ \cdots \ a_p\big) \,=\, \big(a_1 \ a_2\big) \circ \big(a_2 \ a_3\big) \circ \cdots \circ \big(a_{p-2} \ \ a_{p-1}\big) \circ \big(a_{p-1} \ \ a_p\big). \qquad \square$$

Proposition 7.11. *La signature d'une permutation $\sigma \in \mathfrak{S}(E)$ d'un ensemble E à n éléments vaut :*

$$\varepsilon(\sigma) \,=\, (-1)^{n - \mathrm{N}_\sigma},$$

où N_σ est le nombre total de σ-orbites, y compris celles qui sont réduites à un point.

Démonstration. Soit $\sigma_1 \circ \cdots \circ \sigma_r$ la décomposition de σ en produit de cycles à supports disjoints, gratuitement fournie par le Théorème 3.12. Pour $i = 1, \ldots, r$, notons comme d'habitude $p_i \geqslant 2$ la longueur du cycle σ_i. Ainsi, r est le nombre de σ-orbites non réduites à un point.

Alors comme $p_1 + \cdots + p_r$ est le nombre d'éléments de E qui ne sont pas fixés par σ (wagons qui circulent), il reste :

$$n - \big(p_1 + \cdots + p_r\big),$$

éléments de E qui sont fixés par σ (accompagnateurs restés sur les quais), lesquels sont *chacun* des σ-orbites — réduites à un singleton.

Le nombre total de σ-orbites distinctes est donc égal à :

$$\mathrm{N}_\sigma \,:=\, r + n - \big(p_1 + \cdots + p_r\big).$$

Enfin, une application directe de la Proposition 7.10 précédente conclut :

$$\begin{aligned}\varepsilon(\sigma) &= \varepsilon(\sigma_1)\cdots\varepsilon(\sigma_r)\\ &= (-1)^{p_1-1}\cdots(-1)^{p_r-1}\\ &= (-1)^{p_1+\cdots+p_r-r}\\ &= (-1)^{n-\mathrm{N}\sigma}.\end{aligned}$$

□

Nous pouvons maintenant définir le groupe alterné en toute généralité débridée.

Définition 7.12. Le sous-groupe de $\mathfrak{S}(E)$:

$$\begin{aligned}\mathfrak{A}(E) &:= \mathsf{Ker}\,\varepsilon\\ &= \big\{\sigma\in\mathfrak{S}(E)\colon\ \varepsilon(\sigma)=1\big\},\end{aligned}$$

est appelé *groupe alterné de* E.

Alors $\mathfrak{A}(E)$ est un sous-groupe *distingué* de $\mathfrak{S}(E)$, comme l'est tout sous-groupe $H = \mathsf{Ker}\,f$ d'un groupe G qui est noyau d'un morphisme de groupes $f\colon G\longrightarrow G'$.

Maintenant, rappelons que l'*indice* $[G\colon H]$ d'un sous-groupe $H\subset G$ d'un groupe abstrait fini G est le cardinal de l'ensemble des classes à gauche (ou à droite) de G modulo H, comme nous l'avons vu dans le chapitre consacré aux groupes abstraits.

Proposition 7.13. *$\mathfrak{A}(E)$ est un sous-groupe de $\mathfrak{S}(E)$ d'indice :*

$$2 = \big[\mathfrak{S}(E):\mathfrak{A}(E)\big].$$

Démonstration. En effet, si τ est une transposition quelconque fixée avec $-1=\varepsilon(\tau)=\varepsilon(\tau^{-1})$, alors pour toute permutation $\sigma\in\mathfrak{S}(E)$, on a :

$$\text{soit }\ \sigma\in\mathfrak{A}(E),\qquad\qquad \text{soit }\ \tau^{-1}\circ\sigma\in\mathfrak{A}(E),$$

et donc visiblement, $\mathfrak{A}(E)$ et $\tau\,\mathfrak{A}(E)$ sont les deux seules classes à gauche possibles de $\mathfrak{S}(E)$ modulo $\mathfrak{A}(E)$. □

Ensuite, si nous nous remémorons la formule de la Belle Grange :

$$|G| = [G:H]\cdot|H|,$$

toujours avec $|E|=n\geqslant 2$, il vient :

$$\begin{aligned}\big|\mathfrak{A}(E)\big| &= \frac{|\mathfrak{S}(E)|}{[\mathfrak{S}(E):\mathfrak{A}(E)]}\\ &= \frac{n!}{2}.\end{aligned}$$

Pour $n=2$, comme $\frac{2!}{2}=1$, le groupe $\mathfrak{A}_2=\{\mathsf{Id}\}$ est trivial.

Pour $n=3$, l'Exercice 2 propose de démontrer que $\mathfrak{A}_3$ est engendré par n'importe quel 3-cycle.

Le résultat suivant est classique.

Théorème 7.14. *Soit E un ensemble de cardinal $|E|=n\geqslant 2$. Alors le groupe alterné $\mathfrak{A}(E)$ est l'unique sous-groupe d'indice 2 dans $\mathfrak{S}(E)$.*

Rappelons que dans le chapitre consacré aux groupes abstraits, nous avons démontré que tout sous-groupe $H \subset G$ d'indice $2 = [G : H]$ est nécessairement *distingué*, c'est-à-dire que — sans jamais introduire son auriculaire dans l'une de ses narines — il satisfait $g\,H\,g^{-1} = H$ pour tout élément $g \in G$.

Démonstration. Soit donc $H \subset \mathfrak{S}(E)$ un sous-groupe d'indice $2 = [\mathfrak{S}(E) : H]$. On a alors deux classes à gauche, disons H et $\sigma_0 H$, pour une certaine permutation $\sigma_0 \notin H$.

Toute permutation $\sigma \in \mathfrak{S}(E)$ s'écrit donc de manière unique sous la forme :

$$\sigma \,=\, \sigma_0^m\, h, \qquad\qquad \text{avec} \qquad m \,\in\, \{0,\,1\}, \qquad \text{et avec} \qquad h \,\in\, H.$$

Assertion 7.15. *L'application :*

$$f\colon \quad \mathfrak{S}(E) \;\longrightarrow\; \mathbb{C}^\times,$$

définie par :

$$f\big(\sigma_0^m\, h\big) \,:=\, (-1)^m,$$

est un morphisme de groupes.

Cette définition de f et la propriété $H \cap \sigma_0 H \,=\, \emptyset$ des classes à gauche distinctes montrent que :

$$H \,=\, \mathsf{Ker}\, f. \tag{7.16}$$

Preuve. Comme $H \subset \mathfrak{S}(E)$ aux doigts propres est *distingué*, pour tous $m, m' \in \{0, 1\}$ et tous $h, h' \in H$, sans écrire les symboles $\circ$ de composition, nous pouvons faire apparaître dans le produit :

$$\begin{aligned}\big(\sigma_0^m\, h\big)\,\big(\sigma_0^{m'}\, h'\big) \,&=\, \sigma_0^{m+m'}\,\Big(\big(\underbrace{\sigma_0^{-m'}\, h\, \sigma_0^{m'}}_{\in\, H}\big)\, h'\Big)\\ &=:\, \sigma_0^{m+m'}\, h'',\end{aligned}$$

un certain élément $h'' \in H$, et par suite, f est bien un morphisme de groupes :

$$\begin{aligned} f\Big(\big(\sigma_0^m\, h\big)\,\big(\sigma_0^{m'}\, h'\big)\Big) \,&=\, f\big(\sigma_0^{m+m'}\, h''\big)\\ &=\, (-1)^{m+m'}\\ &=\, f\big(\sigma_0^m\, h\big)\cdot f\big(\sigma_0^{m'}\, h'\big).\end{aligned} \tag{7.17}$$

□

Observons que notre morphisme f est non trivial, puisque $f(\sigma_0) = -1 \neq 1 = f(\mathsf{Id})$. Donc grâce au Théorème 7.6 d'unicité, $f = \varepsilon$ est nécessairement le morphisme de signature, d'où :

$$\mathsf{Ker}\, f \,=\, \mathsf{Ker}\, \varepsilon \,=\, \mathfrak{A}(E).$$

En comparant avec (7.16), nous concluons bien que $H = \mathfrak{A}(E)$. □

Terminons ce chapitre en exhibant deux systèmes de générateurs pour le groupe alterné $\mathfrak{A}(E)$.

Théorème 7.18. *Soit E un ensemble fini à n élements. Si $n \geqslant 3$, alors le groupe alterné $\mathfrak{A}(E)$ est engendré par chacune des deux familles suivantes :*

(1) *les produits de deux transpositions (non nécessairement à supports disjoints) ;*

(2) *les 3-cycles.*

Démonstration. **(1)** D'après le Théorème 3.19, le groupe $\mathfrak{S}(E)$ est engendré par les transpositions. Pour tout $\sigma \in \mathfrak{S}(E)$, on peut donc écrire :

$$\sigma \;=\; \tau_1 \circ \cdots \circ \tau_r,$$

où chaque τ_i est une transposition.

Or on sait que que $\varepsilon(\sigma) \;=\; (-1)^r$, et donc on a $\sigma \;\in\; \mathfrak{A}(E)$ si et seulement si $r \;\in\; 2\,\mathbb{N}$ est pair. Autrement dit, les éléments de $\mathfrak{A}(E)$ sont les produits d'un nombre *pair* de transpositions. En particulier, les produits de deux transpositions engendrent $\mathfrak{A}(E)$.

(2) Grâce à **(1)**, il suffit de montrer qu'un produit de deux transpositions est un produit de 3-cycles.

Soient donc $\tau_1, \tau_2 \in \mathfrak{S}(E)$ deux transpositions quelconques. Si elles ont même support, alors $\tau_1 = \tau_2$, d'où $\tau_1 \circ \tau_2 = \mathsf{Id}$, et donc il n'y a rien à démontrer. Yep !

Si les supports de τ_1 et de τ_2 ont exactement un élément en commun, alors on peut supposer que :

$$\tau_1 \;=\; \big(a\ b\big) \qquad\qquad \text{et} \qquad\qquad \tau_2 \;=\; \big(b\ c\big),$$

avec $a, b, c \in E$ distincts deux à deux. Par le calcul, on constate alors que la composition de ces deux transpositions est un 3-cycle :

$$\begin{array}{cccc} & a & b & c \\ \tau_2 & \downarrow & \downarrow & \downarrow \\ & a & c & b \\ \tau_1 & \downarrow & \downarrow & \downarrow \\ & b & c & a \end{array} \qquad\qquad \text{montre que} \qquad\qquad \tau_1 \circ \tau_2 \;=\; \big(a\ b\ c\big).$$

Enfin, si les supports de τ_1 et τ_2 n'ont aucun élément en commun, on peut écrire :

$$\tau_1 \;=\; \big(a\ b\big) \qquad\qquad \text{et} \qquad\qquad \tau_2 \;=\; \big(c\ d\big),$$

avec $a, b, c, d \in E$ distincts deux à deux. Par le calcul, on constate alors que la composition de ces deux transpositions

$$\begin{array}{cccc} & a & b & c & d \\ (c\ d) & \downarrow & \downarrow & \downarrow & \downarrow \\ & a & b & c & d \\ (a\ b) & \downarrow & \downarrow & \downarrow & \downarrow \\ & b & a & d & c \end{array}$$

s'identifie à la composition des deux 3-cycles suivants :

$$\begin{array}{cccc} & a & b & c & d \\ (a\ c\ d) & \downarrow & \downarrow & \downarrow & \downarrow \\ & c & b & d & a \\ (a\ c\ b) & \downarrow & \downarrow & \downarrow & \downarrow \\ & b & a & d & c \end{array}$$

c'est-à-dire :

$$\big(a\ b\big) \circ \big(c\ d\big) \;=\; \big(a\ c\ b\big) \circ \big(a\ c\ d\big). \qquad \square$$

8. Exercices

Exercice 1. Sur l'ensemble $\{1, 2, 3, 4\}$, trouver une transposition et un 4-cycle qui n'engendrent *pas* $\mathfrak{S}_4$.

Exercice 2. Sur l'ensemble $\{1, 2, 3\}$, montrer que le groupe alterné $\mathfrak{A}_3$ est engendré par le 3-cycle $(1\ 2\ 3)$.

Anneaux et corps abstraits

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Introduction

2. Anneaux généraux

Motivés par $\mathbb{Z}$ et ses quotients $\mathbb{Z}/n\mathbb{Z}$, nous avons introduit dans une définition du chapitre précédent la notion d'*anneau commutatif unitaire*. Mais la commutativité de la multiplication n'est pas toujours satisfaite, ou « naturelle ».

Exemple 2.1. Soit l'espace vectoriel des matrices 2×2 :

$$\mathscr{M}_{2\times 2}(\mathbb{R}) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : \ a, b, c, d \in \mathbb{R} \text{ quelconques} \right\},$$

muni de l'addition :

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) + \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) := \left(\begin{smallmatrix} a+a' & b+b' \\ c+c' & d+d' \end{smallmatrix}\right), \qquad \text{d'élément neutre } \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right),$$

et muni de la multiplication dite *matricielle* qui correspond à la *composition* des applications linéaires :

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \times \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) := \left(\begin{smallmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{smallmatrix}\right), \qquad \text{d'élément neutre } I_{2\times 2} := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

Le cours d'Algèbre Linéaire a démontré que $\mathscr{M}_{2\times 2}(\mathbb{R})$, muni de $+$, $\times$, satisfait toutes les propriétés attendues, à l'exception de deux propriétés.

☐ Pour $M \in \mathscr{M}_{2\times 2}$, il n'existe pas toujours $M' \in \mathscr{M}_{2\times 2}$ satisfaisant $M \times M' = I_{2\times 2} = M' \times M$.

☐ Deux matrices quelconques $A, B \in \mathscr{M}_{2\times 2}$ ne satisfont pas toujours :

$$A \times B \overset{?}{=} B \times A \qquad \text{(souvent faux)}.$$

Par exemple :

$$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right) \overset{!}{\neq} \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right).$$

Ceci motive une définition générale d'*anneau* (mathématiques, pas olympique), dans laquelle on ne demande pas forcément que la multiplication $\times$ soit commutative.

Définition 2.2. Soit A un ensemble muni de deux *lois de composition internes* $+$ et $\times$, c'est-à-dire $a+b \in A$ et $a \times b \in A$ pour tous $a, b \in A$. On dit que A est un *anneau* s'il vérifie les propriétés suivantes.

(1) Le couple $\big(A, +\big)$ est un *groupe abélien*, au sens d'une définition vue au chapitre précédent, d'élément neutre 0_A.

(2) La loi de multiplication $\times$ est associative.

(3) La loi $\times$ est distributive, à gauche et à droite, par rapport à $+$:

$$a \times (b+c) \;=\; a \times b + a \times c \qquad (\forall\, a, b, c \in A),$$
$$(a+b) \times c \;=\; a \times c + b \times c \qquad (\forall\, a, b, c \in A).$$

On dit qu'un anneau $\big(A, +, \times\big)$ est *commutatif* lorsque la loi $\times$ satisfait de plus $a \times b = b \times a$, pour tous $a, b \in A$.

Proposition 2.3. *Dans un anneau $\big(A, +, \times\big)$, les trois propriétés suivantes sont satisfaites.*

(1) $a \times 0_A = 0_A = 0_A \times a$, *pour tout* $a \in A$.

(2) $a \times (-b) = -\,a \times b = (-a) \times b$, *pour tous* $a, b \in A$.

(3) $(-a) \times (-b) = a \times b$, *pour tous* $a, b \in A$.

Démonstration. **(1)** Comme 0_A est un élément neutre pour la loi $+$, on a $0_A = 0_A + 0_A$. Ainsi, en multipliant cette égalité par a et en utilisant la distributivité, on a :

$$0_A \times a \;=\; (0_A + 0_A) \times a \;=\; (0_A \times a) + (0_A \times a).$$

Enfin, comme $(A, +)$ est un groupe, on en déduit que $0_A = 0_A \times a$. On montre de manière similaire que $a \times \times 0_A = 0_A$.

(2) Si a et b sont dans A, alors on a :

$$(a \times b) + (a \times (-b)) \;=\; a \times (b-b) \;=\; a \times 0_A \;=\; 0_A,$$

grâce à **(1)** que nous venons de voir. On en déduit que $a \times (-b)$ est l'inverse de $a \times b$ pour la loi $+$, c'est-à-dire :

$$a \times (-b) \;=\; -\,(a \times b).$$

On montre de façon similaire que $(-a) \times b = -\,(a \times b)$.

(3) Si a et b sont dans A, utilisons deux fois la propriété **(2)**, pour conclure :

$$(-a) \times (-b) \;=\; -\,(a \times (-b)) \;=\; -\,\big(-\;(a \times b)\big) \;=\; a \times b. \qquad \square$$

Le cas d'un anneau dans lequel $0_A = 1_A$ est très dégénéré : l'Exercice 1 propose de vérifier qu'alors tous les éléments $a \in A$ sont égaux à 0_A, de telle sorte que $A = \{0_A\}$. On dit alors que A est l'*anneau nul*. Mais comme tout ce qui est nul ne vaut rien, on supposera toujours à partir de maintenant que :

$$0_A \;\neq\; 1_A.$$

Clairement :

$$\big(\mathbb{Z}, +, \times\big), \qquad \big(\mathbb{Z}/n\mathbb{Z}, +, \times\big), \qquad \big(\mathbb{Q}, +, \times\big), \qquad \big(\mathbb{R}, +, \times\big), \qquad \big(\mathbb{C}, +, \times\big),$$

sont des anneaux, commutatifs qui plus est. En fait, il y a des inclusions qui respectent les structures d'anneau.

Définition 2.4. Soit $\big(A, +_A, \times_A\big)$ un anneau. On dit qu'un sous-ensemble $B \subset A$ est un *sous-anneau* de A lorsque :

(1) $\big(B, +_A\big)$ est un *sous-groupe abélien* de $\big(A, +_A\big)$, c'est-à-dire que :

$$b,\, b' \,\in\, B \qquad\qquad \Longrightarrow \qquad\qquad b +_A b' \,\in\, B,$$

où l'addition est prise dans A, de telle sorte que $\big(B, +_A\big)$ est un groupe abélien en lui-même.

(2) pour tous $b, b' \in B$, on a $b \times_A b' \in B$ aussi ;

(3) $1_A \in B$.

On vérifie, en jouant avec la logique, que $\big(B, +, \times\big)$ est alors un anneau en lui-même.

Proposition 2.5. *Si $B \subset A$ est un sous-anneau de $\big(A, +_A, \times_A\big)$, alors le triplet $\big(B, +_A, \times_A\big)$ est un anneau.* □

On notera souvent $+$, $\times$, sans les indices $+_A$, $\times_A$.

Par exemple, les inclusions suivantes sont des inclusions de sous-anneaux :

$$\mathbb{Z} \,\subset\, \mathbb{Q} \,\subset\, \mathbb{R} \,\subset\, \mathbb{C},$$

pour l'addition $+$ et la multiplication $\times$ classiques.

Dans le chapitre précédent, nous avons comparé :

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \overset{?}{=} \mathbb{Z}/mn\mathbb{Z},$$

où m, n sont deux entiers *premiers entre eux*. À cette occasion, nous avons introduit la notion d'*isomorphisme* entre anneaux commutatifs. Voici une définition générale valable dans un anneau quelconque.

Définition 2.6. Étant donné deux anneaux $\big(A, +_A, \times_A\big)$ et $\big(B, +_B, \times_B\big)$, l'*anneau produit* $\big(A \times B, +, \times\big)$ est l'ensemble produit constitué de couples d'éléments :

$$A \times B \,:=\, \big\{(a, b) :\ a \in A \text{ quelconque},\ b \in B \text{ quelconque}\big\},$$

pour lequel les deux lois de compositions internes $+$ et $\times$ sont définies par :

$$\begin{aligned}
(a, b) + (a', b') \,&:=\, \big(a + a',\, b + b'\big) && \text{d'élément neutre } \big(0_A, 0_B\big),\\
(a, b) \times (a', b') \,&:=\, \big(a \times_A a',\, b \times_B b'\big) && \text{d'élément neutre } \big(1_A, 1_B\big).
\end{aligned}$$

On vérifie par le raisonnement (tauto)logique que $\big(A \times B, +, \times\big)$ est effectivement un anneau, au sens de la Définition 2.2. Si A et B sont commutatifs, $A \times B$ l'est également.

Plus généralement, étant donné un nombre $\nu \geqslant 1$ d'anneaux $A_1, \ldots, A_\nu$, on peut construire l'*anneau-produit :*

$$A_1 \times \cdots \times A_\nu \,:=\, \Big\{\big(a_1, \ldots, a_\nu\big) :\ a_1 \in A_1 \text{ quelconque},\ \ldots,\ a_\nu \in A_\nu \text{ quelconque}\Big\},$$

muni des opérations :

$$\begin{aligned}
\big(a_1, \ldots, a_\nu\big) + \big(a'_1, \ldots, a'_\nu\big) \,&:=\, \big(a_1 + a'_1, \ldots, a_\nu + a'_\nu\big),\\
\big(a_1, \ldots, a_\nu\big) \times \big(a'_1, \ldots, a'_\nu\big) \,&:=\, \big(a_1 \times a'_1, \ldots, a_\nu \times a'_\nu\big).
\end{aligned}$$

Par exemple, avec :

$$\begin{aligned}
\mathbb{Z}/2\mathbb{Z} \,&=\, \big\{0,\, 1\big\} \ \mathsf{mod}\, 2,\\
\mathbb{Z}/3\mathbb{Z} \,&=\, \big\{0,\, 1,\, 3\big\} \ \mathsf{mod}\, 3,
\end{aligned}$$

on a :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \,=\, \big\{(0,0),\ (0,1),\ (0,2),\ (1,0)\ (1,1),\ (1,2)\big\}.$$

3. Morphismes d'anneaux et idéaux

Soient deux anneaux quelconques A et B.

Définition 3.1. Un *morphisme d'anneaux* de A vers B est une application $f\colon A \longrightarrow B$ satisfaisant :

(1) $f(a+b) = f(a) + f(b)$, pour tous $a, b \in A$, et $f(0_A) = 0_B$;

(2) $f(a \times b) = f(a) \times f(b)$, pour tous $a, b \in A$, et $f(1_A) = 1_B$.

Par (contre-)exemple, avec un entier fixé $\lambda \in \mathbb{Z}$, l'application $n \longmapsto \lambda\, n$ de $\mathbb{Z}$ dans $\mathbb{Z}$ est un morphisme de groupes $(\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$, mais cependant, dès que $\lambda \neq \lambda^2$, ce n'est pas un morphisme d'anneaux, car :

$$f(m\, n) \,=\, \lambda\, m\, n \,\neq\, \lambda\, m\, \lambda\, n \,=\, f(m)\, f(n) \qquad\qquad (m, n \in \mathbb{Z}).$$

Terminologie 3.2. Un *endomorphisme d'anneau* est un morphisme $A \longrightarrow A$ d'un anneau A vers lui-même.

Un *isomorphisme d'anneaux* est un morphisme $A \longrightarrow B$ d'anneaux qui est *bijectif*, c'est-à-dire simultanément injectif et surjectif.

Un *automorphisme d'anneau* est un isomorphisme d'un anneau A sur lui-même.

Par exemple, l'application de conjugaison complexe :

$$z \,=\, x + i\, y \;\longmapsto\; x - i\, y \,=\, \overline{z},$$

est un automorphisme de l'anneau $\big(\mathbb{C}, +, \times\big)$.

Définition 3.3. Si $f\colon A \longrightarrow B$ est un morphisme d'anneaux, on appelle *noyau* de f l'ensemble :

$$\mathsf{Ker}\, f \,:=\, \big\{a \in A\colon\ f(a) = 0\big\},$$

et on appelle *image* de f l'ensemble :

$$\mathsf{Im}\, f \,:=\, \big\{b \in B\colon\ \exists\, a \in A,\ f(a) = b\big\} \,=\, f(A).$$

Nous laissons en exercice la démonstration de la

Proposition 3.4. *L'image $f(A)$ d'un morphisme d'anneaux $f\colon A \longrightarrow B$ est toujours un sous-anneau de B.* □

Toutefois, le noyau $\mathsf{Ker}\, f$ d'un tel morphisme $f\colon A \longrightarrow B$ n'est en général *pas* un sous-anneau de A, car il ne contient pas toujours 1_A.

Pour terminer cette section, introduisons brièvement une notion qui sera utile ultérieurement, et que nous présentons ici seulement dans le cas où la multiplication $\times$ est commutative.

Définition 3.5. Un sous-ensemble non vide $I \subset A$ d'un anneau commutatif A est appelé un *idéal* s'il vérifie les deux propriétés suivantes :

$$\Big(\ a \in I \quad \text{et} \quad b \in I\ \Big) \qquad\Longrightarrow\qquad a - b \in I,$$

$$\Big(\ a \in I \quad \text{et} \quad p \in A \text{ quelconque}\ \Big) \qquad\Longrightarrow\qquad p\, a \in I.$$

Cette notion absolument fondamentale dans toutes les mathématiques interviendra naturellement lorsque nous étudierons les *polynômes* à une indéterminée x, dans le prochain chapitre.

4. Groupe des inversibles dans un anneau

Si un anneau A n'est *pas* un corps, en général, l'ensemble $A\backslash\{0\}$ de ses éléments non nuls n'est *pas* un groupe pour la loi $\times$ de multiplication. Dans ce cas, on peut introduire un ensemble plus petit, qui lui, est un groupe.

Définition 4.1. Un élément $a \in A$ est dit *inversible* (à gauche et à droite) s'il existe un élément, noté $a^{-1} \in A$, tel que :

$$a^{-1}\, a \;=\; 1_A \;=\; a\, a^{-1}.$$

On note alors $A^\times$ l'ensemble des éléments inversibles de A pour la loi $\times$.

Attention ! Il ne faudra pas confondre $A^\times$ avec $A^* = A\backslash\{0\}$!

Proposition 4.2. *Si $a, b \in A^\times$ sont inversibles, alors leur produit $a\, b \in A^\times$ l'est aussi.*

Preuve. En effet, $b^{-1}\, a^{-1} \in A$ fonctionne :

$$b^{-1}a^{-1}\, a\, b \;=\; b^{-1}\, b \;=\; 1_A \;=\; a\, a^{-1} \;=\; a\, b\, b^{-1}a^{-1}. \qquad \square$$

Théorème 4.3. *Le couple $\big(A^\times, \times\big)$ est un groupe.*

Démonstration. Comme la loi $\times$ est associative sur A, elle l'est également sur $A^\times$. L'élément 1_A est tautologiquement inversible, et donc, on a $1_A \in A^\times$, et 1_A est un élément neutre pour la multiplication $\times$.

Enfin, nous affirmons que tout élément de $A^\times$ est inversible. En effet, il suffit de vérifier que si $a \in A^\times$, alors $a^{-1} \in A^\times$ aussi.

Mais cela est clair, car l'identité *symétrique* qui exprime que a^{-1} est un inverse pour a :

$$a^{-1}\, a \;=\; 1_A \;=\; a\, a^{-1},$$

peut être lue comme une identité qui exprime que a est un inverse pour a^{-1}.

$$a\, a^{-1} \;=\; 1_A \;=\; a^{-1}\, a. \qquad \square$$

Terminologie 4.4. Le groupe $\big(A^\times, \times\big)$ est appelé *groupe des inversibles* de l'anneau A.

Enfin, on vérifie aisément (exercice) la

Proposition 4.5. *Si A et B sont deux anneaux quelconques, alors :*

$$\big(A \times B\big)^\times \;=\; A^\times \times B^\times. \qquad \square$$

5. Intégrité et structure de corps

En supposant que notre anneau A n'est pas commutatif, voici la notion d'intégrité, que nous avons déjà présentée dans le cas commutatif.

Définition 5.1. Un anneau $\big(A, +, \times\big)$ est dit *intègre* si, pour tous $a, b \in A$, la relation $a\, b = 0_A$ implique que $a = 0_A$ ou $b = 0_A$.

Autrement dit, par contraposition, dans un anneau intègre, si $a \neq 0_A$ et si $b \neq 0_A$, alors $a\, b \neq 0_A$ aussi.

Proposition 5.2. *Dans un anneau intègre, les deux règles de simplification suivantes sont vraies.*

(1) *si* $a \neq 0_A$*, alors* $a\,b = a\,c$ *implique* $b = c$*;*

(2) *si* $c \neq 0$*, alors* $a\,c = b\,c$ *implique* $a = b$*.*

Démonstration. Prouvons seulement la règle **(1)**, l'autre étant symétrique.

Supposons donc que $a\,b = a\,c$. Alors comme $(A, +)$ est un groupe (commutatif), on a $a\,b - a\,c = 0$. Comme $-\,a\,c = a\,(-c)$, la distributivité de la multiplication par rapport à l'addition donne :

$$a\,(b - c) \;=\; 0_A.$$

Enfin, comme $a \neq 0_A$ et comme A est par hypothèse intègre, cela force $b - c = 0_A$, donc nous concluons bien que $b = c$. □

L'anneau $\big(\mathbb{Z}, +, \times\big)$ est intègre, c'est bien connu, tandis que l'anneau $\big(\mathscr{M}_{2\times 2}(\mathbb{R}), +, \times\big)$ des matrices carrées de taille 2×2 à coefficients dans $\mathbb{R}$ n'est *pas* intègre, comme le montre la matrice non nulle :

$$M \;:=\; \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

qui satisfait :

$$M \;\neq\; \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{mais} \qquad M \cdot M \;=\; \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0\cdot 0 + 1 \cdot 0 & 0 \cdot 1 + 1 \cdot 0 \\ 0 \cdot 0 + 0 \cdot 0 & 0 \cdot 1 + 0 \cdot 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Voici encore une notion que nous avons déjà introduite, dans un chapitre qui précède, dans le cadre commutatif.

Définition 5.3. Un *corps* $\big(\mathbb{K}, +, \times\big)$ est un anneau $\big(A, +, \times\big)$ avec $1_A \neq 0_A$ tel que $\big(A^*, \times\big)$ est un *groupe*.

Ici, $A^* = A \backslash \{0\}$. De façon équivalente, un corps est un anneau ayant au moins deux éléments tel que tout élément non nul admet un inverse multiplicatif.

Par exemple, les anneaux $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, sont des corps. Par contre, l'anneau $\mathbb{Z}$ n'est pas un corps, car tout entier $n \neq -1, 1$ n'a pas d'inverse multiplicatif dans $\mathbb{Z}$.

Proposition 5.4. *Tout corps est un anneau intègre.*

Démonstration. Soit donc un corps $\mathbb{K}$ — êtes vous d'accorps ? Soient $a, b \in \mathbb{K}$ tels que :

$$a\,b \;=\; 0.$$

Pour satisfaire l'intégrité au sens de la Définition 5.1, nous devons montrer que $a = 0$ ou $b = 0$.

Supposons premièrement que $a \neq 0$ et cherchons à montrer que $b = 0$. Puisque $\mathbb{K}$ est un corps, l'élément $a \in \mathbb{K}^*$ est inversible dans $\mathbb{K}$, c'est-à-dire qu'il existe un élément, noté a^{-1}, tel que $a\,a^{-1} = 1 = a^{-1}\,a$.

Multiplions alors l'égalité $0 = a\,b$ à gauche par a^{-1}, ce qui nous donne :

$$0 \;=\; a^{-1}\,(a\,b) \;=\; a^{-1}\,a\,b \;=\; b,$$

et donc nous obtenons bien $0 = b$.

Deuxièmement, si nous supposons $b \neq 0$, le même argument (symétrisé) donne $a = 0$. □

Y a-t-il une réciproque à cette proposition ? Pas toujours, mais voici au moins une réciproque « partielle », valable avec l'hypothèse supplémentaire de cardinalité finie.

Théorème 5.5. *Pour un anneau A de cardinal fini avec $1_A \neq 0_A$, on a équivalence entre :*

(i) *A est un corps.*

(ii) *A est intègre ;*

Rappelons que la théorie des ensembles élémentaire nous a appris que si E est un ensemble fini et si $f\colon E \longrightarrow E$ est une application quelconque, les trois propriétés suivantes sont équivalentes :

- f est injective ;
- f est surjective ;
- f est bijective.

Démonstration. **(i)** $\Longrightarrow$ **(ii)**. Cette implication est évidente, grâce à la Proposition 5.4.

(ii) $\Longrightarrow$ **(i)** Soit donc $(A, +, \times)$ un anneau intègre de cardinal fini, avec $1_A \neq 0_A$. Il y a donc au moins deux éléments dans A. Notre objectif est d'établir que tout élément non nul fixé $a \in A\backslash\{0\}$ admet un inverse dans A, c'est-à-dire un élément $x \in A$ tel que $a\,x = 1_A = x\,a$, ce qui justifiera que A est un corps.

À cette fin, introduisons l'application de multiplication à gauche par a :

$$\begin{array}{rccc} \varphi\colon & A & \longrightarrow & A \\ & x & \longmapsto & a\,x. \end{array}$$

Cette application φ est un endomorphisme du *groupe* $(A, +)$, car pour $x, y \in A$ quelconques, on a :

$$\varphi(x + y) \,=\, a\,(x + y) \,=\, a\,x + a\,y \,=\, \varphi(x) + \varphi(y).$$

Assertion 5.6. *Le morphisme φ est injectif.*

Preuve. Comme φ est un morphisme de groupes pour l'addition, il suffit de vérifier que son noyau est réduit à $\{0_A\}$. C'est bien le cas, puisque $a \neq 0_A$ dans A intègre donne :

$$\varphi(x) \,=\, 0_A \qquad \Longleftrightarrow \qquad a\,x \,=\, 0_A \qquad \Longleftrightarrow \qquad x \,=\, 0_A. \qquad \square$$

Le point-clé de l'argumentation, c'est que la finitude du cardinal (nombre d'éléments) de A *transmutation de l'injectivité en de la surjectivité*, comme nous l'avons rappelé plus haut.

Par conséquent, φ est surjective !

Cela entraîne que 1_A est dans l'image de A, et fournit donc comme par magie un $x \in A$ tel que $x\,a = 1_A$. Mais attention ! Nous n'avons pas supposé que A était commutatif !

En utilisant l'application $\psi\colon x \longmapsto x\,a$ de multiplication à droite par a, on établit de même qu'il existe un élément $y \in A$ tel que $y\,a = 1_A$.

Pour conclure que a est inversible, il reste encore à vérifier que $x = y$, ce que l'on peut faire en procédant comme suit :

$$y \,=\, y \cdot 1_A \,=\, y\,(a\,x) \,=\, (y\,a)\,x \,=\, 1_A \cdot x \,=\, x. \qquad \square$$

6. Corps des fractions d'un anneau commutatif intègre

Soit un anneau commutatif intègre A. On note $A^* := A\backslash\{0\}$.

Proposition 6.1. *La relation binaire définie sur $A \times A^*$ par :*

$$(a,b) \sim (c,d) \qquad \overset{déf}{\iff} \qquad a\,d = b\,c,$$

est une relation d'équivalence.

Démonstration. Réflexivité. Puisque l'anneau est commutatif, on a $a\,b = b\,a$, ce qui donne $(a,b) \sim (a,b)$.

Symétrie. De nouveau grâce à la commutativité de la loi $\times$:

$$(a,b) \sim (c,d) \quad \iff \quad a\,d = b\,c \quad \iff \quad c\,b = d\,a \quad \iff \quad (c,d) = (a,b).$$

Transitivité. Toujours grâce à la commutativité de la loi $\times$, si :

$$(a,b) \sim (c,d) \qquad \text{et} \qquad (c,d) \sim (e,f),$$

c'est-à-dire si $a\,d = b\,c$ et $c\,f = d\,e$, il vient :

$$a\,d\,f = b\,c\,f = b\,d\,e, \qquad \text{donc} \qquad (a\,f)\,d = (b\,e)\,d,$$

et comme $d \neq 0$ dans A intègre, on peut diviser par d pour obtenir $a\,f = b\,e$, c'est-à-dire $(a,b) \sim (e,f)$. □

Notation 6.2. L'ensemble des classes d'équivalences de $A \times A^*$ pour $(a,b) \sim (c,d)$ sera noté $\mathsf{Frac}\,A$.

La classe d'équivalence d'un élément (a,b) sera noté $\frac{a}{b}$ et appelée *fraction*.

Les raisons de cette notation $\frac{a}{b}$ vont vite devenir très claires.

Ensuite, définissons deux lois naturelles d'addition $+$ et de multiplication $\times$ sur $\mathsf{Frac}\,A$. Pour deux représentants (a,b) et (c,d) de deux fractions $\frac{a}{b}$ et $\frac{c}{d}$, avec $b \neq 0 \neq d$, on pose :

$$\frac{a}{b} + \frac{c}{d} := \frac{a\,d + b\,c}{b\,d},$$

et :

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{a\,c}{b\,d}.$$

Observons qu'en dessous de la barre (de fraction), l'élément $b\,d$ est encore non nul, puisque $b \neq 0 \neq d$ et puisque A est intègre. Notons aussi que cette multiplication entre fractions est commutative, puisque la multiplication dans A est commutative.

Proposition 6.3. *Les deux éléments ainsi définis $\frac{a\,d+b\,c}{b\,d}$ et $\frac{a\,c}{b\,d}$ ne dépendent que des classes de (a,b) et de (c,d).*

Démonstration. Prenons donc deux paires équivalentes $(a,b) \sim (a',b')$ et $(c,d) \sim (c',d')$, et vérifions pour l'addition que l'on a :

$$\big(a\,d + b\,c,\ b\,c\big) \ \sim \ \big(a'\,d' + b'\,c',\ b'\,c'\big).$$

En effet, comme $a\,b' = a'\,b$ et $c\,d' = c'\,d$ par hypothèse, il vient :

$$\begin{aligned}(a\,d + b\,c)\,b'\,c' &= a\,d\,b'\,c' + b\,c\,b'\,c' \\ &= a\,b'\,d\,c' + b'\,c'\,b\,c \\ &= a'\,b\,c\,d' + b'\,c'\,b\,c \\ &= \big(a'\,d' + b'\,c'\big)\,b\,c.\end{aligned}$$

On fait de même pour la loi de multiplication $\times$. □

Théorème 6.4. *Le triplet ainsi défini* $\big(\mathsf{Frac}\, A, +, \times\big)$ *est un corps commutatif d'élément neutre* $\frac{0}{1}$ *pour l'addition et d'élément neutre* $\frac{1}{1}$ *pour la multiplication.*

En particulier, une fraction $\frac{a}{b} \neq 0$ (avec $b \neq 0$) est non nulle dans ce corps si et seulement si $a \neq 0$.

Démonstration. Les arguments détaillés sont laissés en exercice. Le point-clé, c'est qu'une fraction (classe d'équivalence) non nulle $\frac{a}{b}$ avec $a \neq 0 \neq b$ a pour inverse multiplicatif $\frac{b}{a}$, puisque :

$$\frac{a}{b} \cdot \frac{b}{a} \;=\; \frac{a\,b}{b\,a} \;=\; \frac{1}{1},$$

car $a\,b = b\,a$ dans A commutatif. □

Autrement dit, $\mathsf{Frac}\, A$ crée un nouvelle structure algébrique dans laquelle la multiplication devient une loi de *groupe*.

Terminologie 6.5. Le corps $\mathsf{Frac}\, A$ est appelé *corps des fractions* de l'anneau commutatif intègre A.

Enfin, introduisons une application :

$$\begin{array}{rccc} \varphi\colon & A & \longrightarrow & \mathsf{Frac}\, A \\ & a & \longmapsto & \dfrac{a}{1}. \end{array}$$

Proposition 6.6. *L'application* $\varphi(a) := \frac{a}{1}$ *est un morphisme* injectif *de l'anneau* A *dans l'anneau (corps)* $\mathsf{Frac}\, A$.

Démonstration. La vérification du fait que φ est un morphisme d'anneaux (tout corps est un anneau) est laissée en exercice.

Quant à l'injectivité, elle est immédiate :

$$\frac{a}{1} \;=\; \frac{0}{1} \qquad\qquad \Longleftrightarrow \qquad\qquad a \cdot 1 \;=\; 1 \cdot 0 \;=\; 0.$$ □

Grâce à cette application naturelle φ, nous pouvons *identitifier* l'anneau A à son image :

$$A \;\hookrightarrow\; \varphi(A) \;\subset\; \mathsf{Frac}\, A,$$

dans son corps des fractions.

7. Caractéristique d'un anneau intègre

En algèbre, la caractéristique d'un anneau (unitaire) A est par définition l'ordre pour la loi additive de l'élément neutre de la loi multiplicative si cet ordre est fini ; si cet ordre est infini, la caractéristique de l'anneau est par définition 0.

Pour un anneau unitaire $(A, +, \times)$, rappelons que l'on note 0_A l'élément neutre de l'addition $+$, que l'on note 1_A celui de la multiplication $\times$, et que l'on suppose :

$$1_A \;\neq\; 0_A,$$

ce qui exclut le cas extrêmement dégénéré où $A = \{0_A\}$ est l'anneau nul.

Définition 7.1. La *caractéristique* d'un anneau A est le plus petit entier $n \geqslant 1$ tel que :

$$\begin{aligned} n\,1_A &= \underbrace{1_A + 1_A + \cdots + 1_A}_{n \text{ fois}} \\ &= 0_A, \end{aligned}$$

si un tel entier existe. Dans le cas contraire — autrement dit si 1_A est d'ordre infini —, on dit que la caractéristique de A est *nulle*, ou est 0.

Il existe un morphisme naturel d'anneaux unitaires $f\colon \mathbb{Z} \longrightarrow A$, défini, pour un entier $n \geqslant 1$ quelconque, par :

$$f(n) := 1_A + \cdots + 1_A,$$

où 1_A est répété n fois. On sait (ou on vérifie) que le noyau de f est un *idéal* de $\mathbb{Z}$.

Or grâce à la division euclidienne dans $\mathbb{Z}$, tout idéal est principal et donc par définition, la *caractéristique* de A est le générateur positif de $\mathsf{Ker}\, f$, à moins que $\mathsf{Ker}\, f = \{0\}$, auquel cas la caractéristique de A est 0.

Explicitement, la caractéristique de A est l'unique entier naturel $c \geqslant 1$ tel que :

$$\mathsf{Ker}\, f \;=\; c\,\mathbb{Z}.$$

Sans difficulté, on démontre que la caractéristique d'un anneau A est aussi l'unique entier $c \geqslant 0$ tel que $\mathbb{Z}/c\mathbb{Z}$ soit un sous-anneau unitaire de A.

On en déduit en particulier que si B est un sous-anneau unitaire de A, alors A et B ont même caractéristique. Ainsi, les anneaux de caractéristique nulle sont ceux dont $\mathbb{Z}$ est un sous-anneau unitaire. Ils sont donc de cardinal infini.

C'est le cas du corps $\mathbb{C}$ des nombres complexes et de tous ses sous-anneaux unitaires, comme le corps $\mathbb{R}$ des nombres réels ou le corps $\mathbb{Q}$ des nombres rationnels.

Le seul anneau dont la caractéristique vaut 1 est l'anneau nul $A = \{0_A\}$, que nous avons d'ailleurs exclu en supposant $1_A \neq 0_A$.

Proposition 7.2. *La caractéristique d'un anneau intègre est soit égale à 0, soit égale à un nombre premier p.*

Démonstration. En effet, si $\mathbb{Z}/c\mathbb{Z}$ est un sous-anneau unitaire d'un anneau intègre, alors il est lui-même intègre, donc ou bien $c = 0$ est nul, ou bien $c = p$ est un nombre premier. □

Proposition 7.3. *Si A est un anneau commutatif (unitaire), et si sa caractéristique est un nombre premier p, alors pour tous éléments x, y dans A, on a :*

$$(x+y)^p \;=\; x^p + y^p.$$

Démonstration. Le résultat découle de la formule du binôme de Newton et de ce que p divise les coefficients binomiaux apparaissant dans le développement, comme nous l'avons déjà vu dans le chapitre consacré à l'arithmétique sur $\mathbb{Z}$. □

L'application qui $x \longmapsto x^p$ est un endomorphisme de l'anneau A, appelé *endomorphisme de Frobenius*.

Soit maintenant $\mathbb{K}$ un corps commutatif, dans lequel $1 \neq 0$, sinon $\mathbb{K} = \{0\}$ est le corps à un élément seulement. Répétons en partie ce que nous venons de dire au sujet des anneaux, et additionnons 1 plusieurs fois :

$$1, \quad 1+1, \quad 1+1+1, \quad \ldots, \quad \underbrace{1+1+\cdots+1}_{m \text{ fois}}, \quad \ldots.$$

Écrivons alors en abrégé $m\,1$, ou $m \cdot 1$.

Comme $\mathbb{K}$ est un corps, on a ou bien $m \cdot 1 = 0$, ou bien $m \cdot 1 \neq 0$ possède un inverse dans $\mathbb{K}$. Il est possible que $m \cdot 1 \neq 0$ pour tout $m \geqslant 2$. Il est possible, aussi, qu'il existe $m \in \mathbb{N}_{\geqslant 2}$ tel que $m \cdot 1 = 0$.

Lemme 7.4. *S'il existe, l'entier :*

$$p \,:=\, \mathsf{min}\big\{m \in \mathbb{N}_{\geqslant 2} \colon\ m \cdot 1 = 0\big\}$$

est un nombre premier.

Preuve. Sinon, $p = q_1\, q_2$ avec $q_2, q_2 \geqslant 2$ premiers entre eux $1 = q_1 \wedge q_2$.

Mais alors, comme tout corps $\mathbb{K}$ est intègre, cela contredirait la minimalité de p :

$$0 \,=\, q_1\, q_2 \cdot 1 \,=\, q_1 \cdot 1\ q_2 \cdot 1 \qquad \Longrightarrow \qquad \Big(\ q_1 \cdot 1 = 0 \quad \text{ou} \quad q_2 \cdot 1 = 0\ \Big). \qquad \square$$

Théorème 7.5. *Soit $\mathbb{K}$ un corps commutatif quelconque, dans lequel $1 \neq 0$. Alors l'une et l'une seulement des deux circonstances suivantes se produit.*

(1) *Ou bien il existe un entier minimal premier $p \in \mathbb{N}_{\geqslant 2}$ tel que :*

$$p \cdot 1 \,=\, 0 \qquad \Longrightarrow \qquad \Big(\ p \cdot \alpha \,=\, p \cdot 1\, \alpha \,=\, 0 \qquad \forall\, \alpha \,\in\, \mathbb{K}\ \Big).$$

(2) *Ou bien $m \cdot 1 \neq 0$ pour tout entier $m \in \mathbb{N}_{\geqslant 1}$. Dans ce cas, les deux applications :*

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{K} \\ m & \longmapsto & m \cdot 1 \end{array} \qquad \textit{et} \qquad \begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{K} \\ \frac{p}{q} & \longmapsto & p\, q^{-1} \cdot 1 \end{array}$$

sont injectives, et réalisent deux plongements *de $\mathbb{Z}$ et de $\mathbb{Q}$ dans $\mathbb{K}$.*

Par exemple, on sait que pour tout entier premier $p \geqslant 2$, les anneaux quotients $\mathbb{Z}/p\mathbb{Z}$ sont des corps.

Terminologie 7.6. Dans le cas **(1)**, on dit que $\mathbb{K}$ est de *caractéristique zéro*, ou *nulle*.

Dans le cas **(2)**, on dit que $\mathbb{K}$ est de *caractéristique* p.

Démonstration. Le cas **(1)** ayant déjà été expliqué, supposons donc comme en **(2)** que $m \cdot 1 \neq 0$ pour tout entier $m \in \mathbb{N}_{\geqslant 1}$. Alors $-\,m \cdot 1 \neq 0$ aussi, donc $m \cdot 1 \neq 0$ pour tout $m \in \mathbb{Z}^*$.

L'injectivité de l'application $m \longmapsto m \cdot 1$ est alors claire :

$$m \cdot 1 \,=\, m' \cdot 1 \qquad \Longrightarrow \qquad (m - m') \cdot 1 \,=\, 0 \qquad \Longrightarrow \qquad m \,=\, m'.$$

Ensuite, soit une fraction irréductible $\frac{p}{q} \in \mathbb{Q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}_{\geqslant 1}$. Comme $q \cdot 1 \neq 0$ par hypothèse, il en existe un inverse dans le corps $\mathbb{K}$, que l'on note $q^{-1} \cdot 1 \neq 0$. Puis, pour tout $p \in \mathbb{Z}$, on introduit $p \cdot q^{-1} \cdot 1$ la somme de p fois le même terme $q^{-1} \cdot 1$.

Assertion 7.7. *En caractéristique zéro, pour $p \neq 0 \neq q$ entiers, on a $p\, q^{-1} \cdot 1 \neq 0$.*

Preuve. Sinon, si $p\, q^{-1} \cdot 1 = p \cdot q^{-1} \cdot 1 = 0$, en multipliant par q, c'est à dire en additionnant q fois $p\, q^{-1} \cdot 1$, on obtiendrait $p \cdot 1 = 0$, contrairement à l'hypothèse **(2)**. $\square$

Enfin, ceci implique que l'application $\frac{p}{q} \longmapsto p\, q^{-1} \cdot 1$ est injective :

$$\begin{aligned} p\, q^{-1} \cdot 1 \,=\, p'\, q'^{-1} \cdot 1 \qquad &\Longrightarrow \qquad \big(p\, q' - q\, p'\big) \cdot 1 \,=\, 0 \\ &\Longrightarrow \qquad pq' - qp' \,=\, 0 \qquad \Longrightarrow \qquad \frac{p}{q} \,=\, \frac{p'}{q'}. \end{aligned} \qquad \square$$

8. Exercices

Exercice 1. Soit un anneau $\big(A,+,\times\big)$ dans lequel $1_A = 0_A$. Montrer que $A = \{0_A\}$.

Exercice 2. Soit $\big(A,+,\times\big)$ un anneau général, au sens de la Définition 2.2, d'éléments neutres 0_A pour l'addition $+$, et 1_A pour la multiplication $\times$.

(a) Montrer que $a \times 0_A = 0_A = 0_A \times a$, pour tout $a \in A$.

(b) Montrer que $a \times (-b) = -(a \times b) = (-a) \times b$, pour tous $a, b \in A$.

(c) Montrer que $(-a) \times (-b) = a \times b$, pour tous $a, b \in A$.

Exercice 3. On rappelle la formule du binôme, valable pour $x, y \in \mathbb{R}$, et pour un exposant entier $n \in \mathbb{N}$:

$$\big(x+y\big)^n \;=\; \sum_{k=0}^{n} \binom{n}{k} x^k \, y^{n-k},$$

où :

$$\binom{n}{k} \;:=\; \frac{n!}{k!\,(n-k)!} \qquad (0 \leqslant k \leqslant n).$$

L'objectif est de généraliser cette formule à des anneaux quelconques.

(a) Montrer les relations de récurrence :

$$\binom{n+1}{k+1} \;=\; \binom{n}{k} + \binom{n}{k+1}.$$

(b) Soit un anneau $\big(A,+,\times\big)$, pas forcément commutatif. Pour deux éléments $a, b \in A$, est-il légitime d'écrire :

$$\big(a+b\big)^2 \;\stackrel{?}{=}\; a^2 + 2\,ab + b^2 \,?$$

(c) Pour $m \in \mathbb{N}$ et $a \in A$, on pose $m\,a := a + \cdots + a$, avec m termes, ainsi que $a^m := a \times \cdots \times a$, de nouveau avec m termes. Vérifier que :

$$\big(a+b\big)^2 \;=\; a^2 + 2\,ab + b^2 \qquad\qquad \Longleftrightarrow \qquad\qquad a\,b \;=\; b\,a.$$

(d) On suppose dorénavant que deux éléments donnés $a, b \in A$ *commutent*, au sens où $a \times b = b \times a$, c'est-à-dire $a\,b = b\,a$. Montrer que :

$$\begin{aligned}\big(a+b\big)^3 \;&=\; a^3 + 3\,a^2\,b + 3\,a\,b^2 + b^3,\\ \big(a+b\big)^4 \;&=\; a^4 + 4\,a^3\,b + 6\,a^2\,b^2 + 4\,a\,b^3 + b^4.\end{aligned}$$

(e) Montrer, pour $k, \ell \in \mathbb{N}$, que :

$$a^k\,b^\ell\,a \;=\; a^{k+1}\,b^\ell \qquad\qquad \text{et} \qquad\qquad b\,a^k\,b^\ell \;=\; a^k\,b^{\ell+1}.$$

(f) Établir la formule du binôme :

$$\big(a+b\big)^n \;=\; \sum_{k=0}^{n} \binom{n}{k} a^k\,b^{n-k} \qquad (a\,b = b\,a).$$

Exercice 4. EE

Exercice 5. EE

Polynômes

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Introduction

Considérons un anneau commutatif intègre A, c'est-à-dire un anneau dont la multiplication, commutative, satisfait la propriété fondamentale de simplification :

$$a\,b \,=\, 0 \qquad\qquad \Longrightarrow \qquad\qquad \Big(a \,=\, 0 \qquad \text{ou} \qquad b \,=\, 0\Big).$$

Quand nous ne mentionnerons pas que A est intègre, il sera sous-entendu que A est un anneau commutatif général, toujours muni d'un *autre* élément neutre 0 pour l'addition, et d'un élément neutre $1 \neq 0$ pour la multiplication.

Si $n \geqslant 0$ est un entier naturel, et si $a \in A$ est un élément de A, l'application :

$$x \;\longmapsto\; a\,x^n$$

est appelée *fonction-monôme* de A dans A, et elle fait intervenir la multiplication de A.

Au-delà, si on se donne $n+1$ éléments de A :

$$a_0,\; a_1,\; a_2,\; \ldots,\; a_n,$$

alors l'application :

$$x \;\longmapsto\; a_0 + a_1\,x + a_2\,x^2 + \cdots + a_n\,x^n$$

est appelée *fonction-polynôme* de A dans A, et elle fait intervenir les structures additive et multiplicative de A.

En classe de CM2 des années 1970, les polynômes étaient étudiés sous forme de fonctions, comme ci-dessus. Par exemple, on pouvait étudier le polynôme cubique explicite :

$$x \;\longmapsto\; x^3 + 2\,x - 3,$$

de $\mathbb{R}$ dans $\mathbb{R}$, et on travaillait dans le corps $\mathbb{R}$ des nombres réels afin de bénéficier de la notion intuitive de continuité, et afin de faire de l'analyse et de la géométrie.

Dans le chapitre qui commence ici, destiné à des étudiants qui ont réussi à dépasser le niveau CMDD2 haut la main, nous n'allons plus considérer la lettre x comme un élément de l'anneau A, mais comme un *symbole indéterminé*, tellement « indéterminé » d'ailleurs, qu'il pourra être totalement absent au début de la théorie !

L'aspect *fonctionnel* des polynômes sera donc abandonné ! Seul l'aspect *formel abstrait* des polynômes interviendra, primera, et dominera.

Une théorie purement *algébrique* des polynômes formels va donc être développée ici, et finalement, l'indéterminée x apparaîtra comme un polynôme formel particulier, naturel, canonique.

2. Définition abstraite des polynômes formels

Voici donc la terrible notion hyper-abstraite et hyper-formelle qui nous a été promise.

Définition 2.1. On appelle *polynôme à une indéterminé* sur un anneau commutatif intègre A, une suite infinie :

$$\big(a_0,\ a_1,\ a_2,\ \ldots,\ a_n,\ 0,\ 0,\ \ldots\big),$$

d'éléments $a_i \in A$, telle qu'à partir d'un certain rang, tous les termes de la suite sont égaux au zéro $0 = 0_A$ de A.

Les termes a_i de cette suite sont alors appelés *coefficients* du polynôme.

La numérotation commence à partir du rang 0. Les polynômes ainsi définis sont des êtres mathématiques :

$$p \ = \ \big(a_0,\ a_1,\ a_2,\ \ldots,\ a_n,\ 0,\ 0,\ \ldots\big),$$

qui seront notés avec des lettres latines minuscules, telles que p, q, r, *etc.*

Dès que l'on modifie l'un des termes de la suite, on crée un autre polynôme, différent. En effet, d'après les propriétés connues des suites infinies de nombres de A, deux polynômes :

$$\begin{aligned} p \ &= \ \big(a_0,\ a_1,\ \ldots,\ a_i,\ \ldots\big), \\ q \ &= \ \big(b_0,\ b_1,\ \ldots,\ b_i,\ \ldots\big), \end{aligned}$$

sont égaux, ce que l'on note :

$$p \ = \ q,$$

si et seulement si tous leurs coefficients coïncident :

$$a_i \ = \ b_i \qquad (\forall\, i \in \mathbb{N}).$$

Évidemment, le *polynôme nul :*

$$0 \ := \ \big(0,\ 0,\ 0,\ \ldots,\ 0,\ \ldots\big),$$

est celui dont tous les coefficients $a_i = 0$ sont nuls.

Notation 2.2. L'ensemble des polynômes p à une indéterminée sur A sera noté :

$$A[x] \ \ni \ p.$$

La signification de la lettre x ici demeure pour l'instant assez mystérieuse, mais qu'adviendrait-il de la beauté des mathématiques, si elle n'était pas drapée de mystères ?

Définition 2.3. [Degré] Le plus grand entier i tel que $a_i \neq 0$ s'appelle le *degré* du polynôme :

$$p \ = \ \big(a_0,\ a_1,\ \ldots,\ a_n,\ 0,\ \ldots\big),$$

et il est noté :

$$\mathsf{deg}\, p \ := \ \mathsf{max}\ \big\{i \in \mathbb{N}\colon\ a_i \neq 0\big\}.$$

Cette définition a un sens pour tout polynôme $p \in A[x]$ non nul, et on pose par convention :

$$\mathsf{deg}\, 0 \ := \ -\infty.$$

Définition 2.4. [Valuation] Le plus petit entier i tel que $a_i \neq 0$ est appelé la *valuation* du polynôme :

$$p \,=\, \big(0,\ \ldots,\ 0,\ a_m,\ \ldots,\ a_n,\ 0,\ \ldots\big),$$

et il est noté :

$$\begin{aligned}\mathsf{val}(p) \,&:=\, \mathsf{min}\,\big\{i \in \mathbb{N}\colon\ a_i \neq 0\big\}\\ &\leqslant\, \mathsf{deg}\, p.\end{aligned}$$

Cette définition a un sens pour tout polynôme $p \in A[x]$ non nul, et on pose par convention :

$$\mathsf{val}\, 0 \,:=\, \infty.$$

Prenons par exemple l'anneau $A := \mathbb{Z}$ des entiers relatifs, et dans $\mathbb{Z}[x]$, regardons le petit polynôme :

$$p \,:=\, \big(0,\ 0,\ -2,\ 0,\ 1,\ -3,\ 0,\ 0,\ \ldots\big),$$

les points de supension voulant dire, comme nous l'avons déjà compris, que le 0 se répète indéfiniment. Il est alors clair que :

$$\mathsf{val}\, p \,=\, 2 \qquad\qquad \text{et} \qquad\qquad \mathsf{deg}\, p \,=\, 5.$$

Évidemment, deux polynômes $p = q$ égaux satisfont :

$$\mathsf{val}\, p \,=\, \mathsf{val}\, q \qquad\qquad \text{et} \qquad\qquad \mathsf{deg}\, p \,=\, \mathsf{deg}\, q.$$

Comme nous venons de définir, pour le polynôme nul :

$$\mathsf{deg}\, 0 \,=\, -\infty \qquad\qquad \text{et} \qquad\qquad \mathsf{val}\, 0 \,=\, \infty$$

il est nécessaire de prolonger l'arithmétique de $\mathbb{N}$ à l'ensemble $\{-\infty\} \cup \mathbb{N} \cup \{\infty\}$, comme suit.

Convention 2.5. Les symboles $-\infty$, $n \in \mathbb{N}$, ∞ satisfont :

$$\begin{aligned} -\infty + n \,&=\, -\infty, & \qquad \infty + n \,&=\, \infty,\\ -\infty \times n \,&=\, -\infty, & \qquad \infty \times n \,&=\, \infty,\end{aligned}$$

ainsi que :

$$-\infty \,<\, n \qquad\qquad \text{et} \qquad\qquad n \,<\, \infty.$$

3. Addition et multiplication dans $A[x]$

Commençons par l'addition, beaucoup plus simple et intuitive que la multiplication.

Définition 3.1. À tout couple ordonné (p, q) de polynômes de $A[x]$:

$$\begin{aligned} p \,&=\, \big(a_0,\ a_1,\ \ldots,\ a_i,\ \ldots\big),\\ q \,&=\, \big(b_0,\ b_1,\ \ldots,\ b_i,\ \ldots\big),\end{aligned}$$

est associée le *polynôme-somme* de $A[x]$ défini par :

$$p + q \,:=\, \big(a_0 + b_0,\ \ a_1 + b_1,\ \ \ldots,\ \ a_i + b_i,\ \ \ldots\big).$$

Ainsi, pour tout rang i, le coefficient de $p + q$ est égal à la somme des coefficients de rang i de p et de q.

Définition 3.2. Un polynôme :

$$p \,=\, \big(a_0,\ a_1,\ \ldots,\ a_i,\ \ldots\big),$$

a un *opposé :*

$$-\,p \,:=\, \big(-\,a_0,\ -\,a_1,\ \ldots,\ -\,a_i,\ \ldots\big).$$

La structure de groupe additif (commutatif) de A donne immédiatement les propriétés suivantes de l'addition dans $A[x]$.

Proposition 3.3. *L'addition des polynômes dans $A[x] \ni p, q, r$ satisfait :*

(1) $p + q = q + p$*;*

(2) $p + (q + r) = (p + q) + r$*;*

(3) $p + 0 = p$*;*

(4) $p + (-p) = 0$. □

L'addition $p + q$ qui vient d'être définie confère donc à $A[x]$ une structure de *groupe commutatif.*

Proposition 3.4. *Pour tous polynômes $p, q \in A[x]$, on a :*

$$\mathsf{deg}\,\big(p+q\big) \,\leqslant\, \mathsf{max}\,\big\{\mathsf{deg}\,p,\ \mathsf{deg}\,q\big\}.$$

Démonstration. Envisageons deux cas. Cas 1 :

$$n \,:=\, \mathsf{deg}\,p \,>\, \mathsf{deg}\,q \,=:\, m,$$

c'est-à-dire :

$$\begin{aligned} p \,&=\, \big(a_0,\ \ldots,\ a_m,\ a_{m+1},\ \ldots,\ a_n,\ 0,\ \ldots\big),\\ q \,&=\, \big(b_0,\ \ldots,\ b_m,\ 0,\ \ldots\big). \end{aligned}$$

Alors :

$$p+q \,=\, \Big(a_0+b_0,\ \ \ldots,\ \ a_m+b_m,\ \ a_{m+1},\ \ \ldots,\ \ a_n,\ \ 0,\ \ \ldots\Big),$$

est de degré $n = \mathsf{max}\,\{m, n\}$, donc l'inégalité, qui devient une égalité, est bien satisfaite.

Cas 2 :

$$n \,:=\, \mathsf{deg}\,p \,=\, \mathsf{deg}\,q \,=:\, m,$$

c'est-à-dire :

$$\begin{aligned} p \,&=\, \big(a_0,\ \ldots,\ a_{n-1},\ a_n,\ 0,\ \ldots\big),\\ q \,&=\, \big(b_0,\ \ldots,\ b_{n-1},\ b_n,\ 0,\ \ldots\big). \end{aligned}$$

Alors :

$$p+q \,=\, \Big(a_0+b_0,\ \ \ldots,\ \ a_{n-1}+b_{n-1},\ \ a_n+b_n,\ \ 0,\ \ \ldots\Big).$$

Sous-cas 2.1 :

$$0 \,\neq\, a_n + b_n.$$

Alors $p + q$ est de degré $n = \mathsf{max}\,\{n, n\}$, et à nouveau, l'inégalité, qui devient une égalité, est satisfaite.

Sous-cas 2.2 :

$$0 \,=\, a_n + b_n.$$

Alors visiblement :

$$p+q \,=\, \Big(a_0+b_0,\ \ \ldots,\ \ a_{n-1}+b_{n-1},\ \ 0,\ \ 0,\ \ \ldots\Big),$$

est de degré $\leqslant n-1$, et donc, l'inégalité, qui est maintenant une vraie inégalité, est bien satisfaite :

$$\mathsf{deg}\,(p+q) \;\leqslant\; n-1 \;\leqslant\; \mathsf{max}\,\{n,n\} \;=\; \mathsf{max}\,\big\{\mathsf{deg}\,p,\;\mathsf{deg}\,q\big\}.$$

Pour terminer, observons que ces raisonnements sont toujours vrais, même quand $p=0$, ou $q=0$, ou $p+q=0$, car nous avons assigné le degré du polynôme nul comme étant $-\infty$. □

Proposition 3.5. *Pour tous polynômes $p, q \in A[x]$, on a :*

$$\mathsf{val}\,\big(p+q\big) \;\geqslant\; \mathsf{min}\,\big\{\mathsf{val}\,p,\;\mathsf{val}\,q\big\}.$$

Preuve. Les argumens, très analogues à ceux qui précèdent, ne seront pas détaillés. □

Introduisons maintenant la multiplication d'un polynôme par un élément de l'anneau de base A.

Définition 3.6. À tout polynôme dans $A[x]$:

$$p \;=\; \big(a_0,\;\ldots,\;a_i,\;\ldots\big),$$

et à tout élément $h \in A$, est associé le polynôme :

$$h\,p \;:=\; \big(h\,a_0,\;\;\ldots,\;\;h\,a_i,\;\;\ldots\big).$$

Cette définition introduit alors une *loi de composition externe*, c'est-à-dire une application de $A \times A[x]$ dans $A[x]$, qui à (h,p) associe $h\,p$. Et comme A est un anneau commutatif à élément unité $1 = 1_A$, les propriétés suivantes sont évidentes.

Proposition 3.7. *Pour tous polynômes $p, q \in A[x]$ et tous éléments $h, k \in A$ de l'anneau de base, on a :*

(1) $1\,p = p$*;*

(2) $h\,(p+q) = h\,p + h\,q$*;*

(3) $(h+k)\,p = h\,p + k\,p$*;*

(4) $h\,(k\,p) = (h\,k)\,p$*.* □

Nous savons déjà, d'après la Proposition 3.3, que $A[x]$ est un groupe commutatif.

Lorsque $A = \mathbb{K}$ est un *corps*, nous savons que le cours d'Algèbre Linéaire a introduit le concept de $\mathbb{K}$-espace vectoriel — encore une structure algébrique ! —, et toutes ces propriétés montrent la

Proposition 3.8. *Si $\mathbb{K}$ est un corps, $\mathbb{K}[x]$ est un $\mathbb{K}$-espace vectoriel.* □

Dans le cas général où A n'est pas un corps, les mathématiques on introduit une

Terminologie 3.9. On dit que $A[x]$ est un *module* sur l'anneau commutatif A.

Toutefois, la structure algébrique de module sur un anneau n'est étudiée qu'en cours de L3 ou de M1.

Maintenant, voici une conséquence très importante de toutes ces propriétés élémentaires.

Pour tout entier naturel $n \geqslant 0$, si nous introduisons le polynôme-type :

$$u_n \;:=\; \big(0,\;0,\;\ldots,\;0,\;1,\;0,\;\ldots\big), \tag{3.10}$$

dont les composantes sont :

$$u_i := \begin{cases} 1 & \text{pour } i = n, \\ 0 & \text{pour } i \neq n, \end{cases}$$

il est clair que nous pouvons représenter n'importe quel polynôme de $A[x]$:

$$p = \big(a_0,\ a_1,\ \dots,\ a_n,\ \dots\big),$$

avec $a_n \neq 0$, comme la combinaison linéaire :

$$p = a_0\, u_0 + a_1\, u_1 + \cdots + a_n\, u_n.$$

Dans peu de temps, nous reviendrons à cette représentation naturelle.

Passons à la multiplication dans $A[x]$. Étant donné deux fonctions polynomiales $\mathbb{R} \longrightarrow \mathbb{R}$:

$$\begin{aligned} p\colon \quad x &\longmapsto a_0 + a_1\, x + a_2\, x^2 + a_3\, x^3 + \cdots, \\ q\colon \quad x &\longmapsto b_0 + b_1\, x + b_2\, x^2 + b_3\, x^3 + \cdots, \end{aligned}$$

n'ayant qu'un nombre *fini* de monômes dans les points de suspension, il est clair et connu que la fonction-produit s'écrit :

$$\begin{aligned} p\,q\colon \quad x &\longmapsto \Big(a_0 + a_1\, x + a_2\, x^2 + a_3\, x^3 + \cdots\Big) \cdot \Big(b_0 + b_1\, x + b_2\, x^2 + b_3\, x^3 + \cdots\Big) \\ &= a_0\, b_0 + \big(a_0\, b_1 + a_1\, b_0\big)\, x + \big(a_0\, b_2 + a_1\, b_1 + a_2\, b_0\big)\, x^2 \\ &\qquad + \big(a_0\, b_3 + a_1\, b_2 + a_2\, b_1 + a_3\, b_0\big)\, x^3 + \cdots. \end{aligned}$$

En outre, on peut vérifier (exercice-express) qu'il n'y a à nouveau qu'un nombre fini de puissances de x dans les points de suspension. Ce calcul naturel motive et justifie, dans un langage abstrait, la

Proposition-Définition 3.11. *À tout couple ordonné (p, q) de deux polynômes sur l'anneau A :*

$$\begin{aligned} p &= \big(a_0,\ a_1,\ a_2,\ \dots,\ a_i,\ \dots\big), \\ q &= \big(b_0,\ b_1,\ b_2,\ \dots,\ b_i,\ \dots\big), \end{aligned}$$

est associé le polynôme-produit, défini par :

$$p\,q := \Big(a_0\, b_0,\ \ a_0\, b_1 + a_1\, b_0,\ \ a_0\, b_2 + a_1\, b_1 + a_2\, b_0,\ \ \dots\Big),$$

dont le terme de rang i quelconque est :

$$c_i := a_0\, b_i + a_1\, b_{i-1} + \cdots + a_{i-1}\, b_1 + a_i\, b_0 = \sum_{0 \leqslant k \leqslant i} a_i\, b_{k-i}.$$

De plus :

$$\deg p\,q \leqslant \deg p + \deg q.$$

Démonstration. Pour que $p\,q$ soit effectivement un polynôme, il faut encore vérifier (résolution de l'exercice-express ci-dessus) que $c_i = 0$ pour tous les indices $i \gg 1$ assez grands.

Assertion 3.12. *Si $n := \deg p$ et si $m := \deg q$, on a :*

$$0 = c_i, \qquad \text{pour tout } i \geqslant 1 + n + m.$$

Preuve. Soit donc $i \geqslant 1+n+m$ quelconque. Dans la formule qui définit les coefficients du produit $p\,q$:

$$c_i \;=\; \sum_{0 \leqslant k \leqslant i} a_k\, b_{i-k},$$

observons que l'on a toujours :

$$k \;\geqslant\; 1+n \qquad\qquad \text{ou} \qquad\qquad i-k \;\geqslant\; 1+m,$$

car sinon, si on avait au contraire simultanément :

$$k \;\leqslant\; n \qquad\qquad \text{et} \qquad\qquad i-k \;\leqslant\; m,$$

il viendrait par addition :

$$i \;=\; k+i-k \;\leqslant\; n+m,$$

en contradiction avec le choix de $i \geqslant 1+n+m$.

Par conséquent, dans chaque terme-produit $a_k\, b_{i-k}$ qui compose la somme c_i, le premier $a_k = 0$ est nul, ou le second $b_{i-k} = 0$ est nul, et donc nous avons bien :

$$c_i \;=\; \sum_{0 \leqslant k \leqslant i} 0 \;=\; 0 \qquad\qquad (\forall\, i \geqslant 1+n+m).$$ □

Ainsi, nous avons bien vérifié que $p\,q$ est effectivement un polynôme, satisfaisant d'ailleurs $\deg p\,q \leqslant n+m = \deg p + \deg q$. □

Un peu plus tard, *voir* la Proposition 3.16, nous verrons que sur un anneau A qui est *intègre*, on a en fait égalité $\deg p\,q = \deg p + \deg q$.

Voici maintenant les propriétés fondamentales de la multiplication entre polynômes. Auparavant, introduisons le *polynôme-unité :*

$$e \;:=\; \big(1,\; 0,\; 0,\; \ldots\big).$$

Proposition 3.13. *Quels que soient les polynômes $p, q, r \in A[x]$, on a :*

(1) $p\,q = q\,p$*;*

(2) $p\,e = p$*;*

(3) $(p\,q)\,r = p\,(q\,r)$*;*

(4) $(p+q)\,r = p\,q + p\,r$.

Ainsi, la multiplication entre polynômes est commutative, associative, et distributive par rapport à l'addition.

Corollaire 3.14. *Pour tout anneau A, l'ensemble $A[x]$ est aussi un anneau.* □

Démonstration. Nous allons noter :

$$\begin{aligned} p \;&=\; \big(a_0,\; a_1,\; \ldots,\; a_i,\; \ldots\big), \\ q \;&=\; \big(b_0,\; b_1,\; \ldots,\; b_i,\; \ldots\big), \\ r \;&=\; \big(c_0,\; c_1,\; \ldots,\; c_i,\; \ldots\big). \end{aligned}$$

(1) Effectivement, comme la multiplication et l'addition dans A sont commutatives, nous avons bien :

$$\begin{aligned} p\,q &= \Big(a_0\,b_0,\ \ a_0\,b_1+a_1\,b_0,\ \ \ldots,\ \ \sum_{0\leqslant k\leqslant i} a_k\,b_{i-k},\ \ \ldots\Big)\\ &= \Big(b_0\,a_0,\ \ b_0\,a_1+b_1\,a_0,\ \ \ldots,\ \ \sum_{0\leqslant \ell\leqslant i} b_\ell\,a_{i-\ell},\ \ \ldots\Big)\\ &= q\,p. \end{aligned}$$

(2) Effectivement :

$$\begin{aligned} p\,e &= \big(a_0\,1,\ \ a_1\,1,\ \ \ldots,\ \ a_i\,1,\ \ \ldots\big)\\ &= p. \end{aligned}$$

(3) Au lieu de :

$$\sum_{0\leqslant k\leqslant i} a_k\,b_{i-k},$$

écrivons de manière plus symétrique :

$$\sum_{i_1+i_2=i} a_{i_1}\,b_{i_2},$$

de telle sorte que :

$$\begin{aligned} p\,q &= \Big(\sum_{i_1+i_2=i} a_{i_1}\,b_{i_2}\Big)_{i\in\mathbb{N}},\\ q\,r &= \Big(\sum_{i_2+i_3=i} b_{i_2}\,c_{i_3}\Big)_{i\in\mathbb{N}}, \end{aligned}$$

d'où la conclusion par associativité de la multiplication dans A :

$$\begin{aligned} (p\,q)\,r &= \Big(\sum_{i'_2+i_3=i}\Big(\sum_{i_1+i_2=i'_2} a_{i_1}\,b_{i_2}\Big)\,c_{i_3}\Big)_{i\in\mathbb{N}}\\ &= \Big(\sum_{i_1+i_2+i_3=i} a_{i_1}\,b_{i_2}\,c_{i_3}\Big)_{i\in\mathbb{N}}\\ &= \Big(\sum_{i_1+i'_3=i} a_{i_1}\Big(\sum_{i_2+i_3=i'_3} b_{i_2}\,c_{i_3}\Big)\Big)_{i\in\mathbb{N}}\\ &= p\,(q\,r). \end{aligned}$$

(4) Effectivement, par distributivité de la multiplication dans A par rapport à l'addition dans A, nous avons bien :

$$\begin{aligned}(p+q)\,r \;&=\; \Big(\sum_{i_1+i_2=i} \big(a_{i_1}+b_{i_1}\big)\,c_{i_2}\Big)_{i\in\mathbb{N}}\\ &=\; \Big(\sum_{i_1+i_2=i} a_{i_1}\,c_{i_2} + \sum_{i_1+i_2=i} b_{i_1}\,c_{i_2}\Big)_{i\in\mathbb{N}}\\ &=\; \Big(\sum_{i_1+i_2=i} a_{i_1}\,c_{i_2}\Big)_{i\in\mathbb{N}} + \Big(\sum_{i_1+i_2=i} b_{i_1}\,c_{i_2}\Big)_{i\in\mathbb{N}}\\ &=\; p\,r+q\,r.\end{aligned}$$

□

Théorème 3.15. *Sur un anneau* intègre *A, l'anneau $A[x]$ des polynômes à une indéterminée x est aussi* intègre*, c'est-à-dire que pour tous polynômes $p, q \in A[x]$, on a :*

$$p\,q \;=\; 0 \qquad\qquad \Longrightarrow \qquad\qquad \Big(p \;=\; 0 \quad \textit{ou} \quad q \;=\; 0\Big).$$

Démonstration. En supposant, par symétrie, que $p \neq 0$, il s'agit de montrer que $q = 0$ nécessairement.

Si donc $p \neq 0$, sa valuation $\mathsf{val}(p) =: h < \infty$ est finie, c'est-à-dire que :

$$p \;=\; \big(0,\ \ldots,\ 0,\ a_h,\ a_{h+1},\ \ldots\big),$$

avec $a_h \neq 0$.

Le produit de p avec :

$$q \;=\; \big(b_0,\ b_1,\ \ldots,\ b_i,\ \ldots\big),$$

est :

$$p\,q \;=\; \Big(a_h\,b_0,\ \ a_h\,b_1 + a_{h+1}\,b_0,\ \ \ldots,\ \ a_h\,b_i + a_{h+1}\,b_{i-1} + \cdots + a_{h+i}\,b_0,\ \ \ldots\Big),$$

et l'hypothèse $p\,q = 0$ se traduit par le système d'équations :

$$\begin{aligned}0 \;&=\; a_h\,b_0,\\ 0 \;&=\; a_h\,b_1 + a_{h+1}\,b_0,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\ ,\\ 0 \;&=\; a_h\,b_i + a_{h+1}\,b_{i-1} + \cdots + a_{h+i}\,b_0,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\ .\end{aligned}$$

Puisque A est lui-même intègre, et puisque $a_h \neq 0$, nous en déduisons, de proche en proche, les annulations :

$$b_0 \;=\; 0, \qquad b_1 \;=\; 0, \qquad \ldots, \qquad b_i \;=\; 0, \qquad \ldots,$$

et par conséquent, comme attendu :

$$q \;=\; 0.$$

□

Proposition 3.16. *Sur un anneau intègre A, pour tous polynômes $p, q \in A[x]$, on a :*

$$\mathsf{deg}\,p\,q \;=\; \mathsf{deg}\,p + \mathsf{deg}\,q.$$

Démonstration. Écrivons :

$$p = \big(a_0,\ a_1,\ \ldots,\ a_n,\ 0,\ \ldots\big), \qquad \text{avec } a_n \neq 0,$$
$$q = \big(b_0,\ b_1,\ \ldots,\ b_m,\ 0,\ \ldots\big), \qquad \text{avec } b_m \neq 0,$$

c'est-à-dire :

$$n = \deg p \qquad \text{et} \qquad \deg p = m.$$

Nous savons que le terme général c_i de rang i du produit $p\,q$ est :

$$c_i = \sum_{0 \leqslant k \leqslant i} a_k\, b_{i-k}.$$

Calculons alors le terme de rang $i = n + m$, comme suit :

$$k < n \quad \Longrightarrow \quad n + m - k > m \quad \Longrightarrow \quad b_{n+m-k} = 0,$$
$$k > n \quad \Longrightarrow \quad a_k = 0.$$

Dans la sommation, il ne reste donc que le terme correspondant à $k = n$:

$$c_{n+m} = a_n\, b_m \neq 0,$$

qui n'est pas nul, par hypothèse.

Ensuite, prouvons que :

$$i > n + m \qquad \Longrightarrow \qquad c_i = 0.$$

En effet :

$$\Big(i > n + m \quad \text{et} \quad k \leqslant n \Big) \qquad \Longrightarrow \qquad i - k > m \qquad \Longrightarrow \qquad b_{i-k} = 0,$$
$$k > n \qquad \Longrightarrow \qquad a_k = 0.$$

Par conséquent, pour tout $i > n + m$, tous les termes $a_k\, b_{i-k}$ qui apparaissent dans $c_i = \sum_{k=0}^{i} a_k\, b_{i-k}$ sont nuls, et donc, $c_i = 0$. La démonstration est terminée. □

Proposition 3.17. *Sur un anneau intègre A, pour tous polynômes $p, q \in A[x]$, on a :*

$$\mathsf{val}\,\big(p\,q\big) = \mathsf{val}\,p + \mathsf{val}\,q.$$

Démonstration. Les arguments sont en tous points analogues — ou duaux. □

4. Notation définitive pour les polynômes

Nous avons introduit dans l'équation (3.10) les polynômes :

$$u_n = \big(0,\ \ldots,\ 0,\ 1,\ 0,\ \ldots\big),$$

dont le degré coïncide avec la valuation :

$$\mathsf{val}\,u_n = n = \deg u_n.$$

Pour $n = 0$, observons que u_0 est l'élément unité e de la multiplication entre polynômes.

Maintenant, effectuons le produit $u_n\, u_m$. En appliquant la Proposition-Définition 3.11, nous trouvons aisément :

$$u_n\, u_m = u_{n+m} = u_m\, u_n.$$

Pour ce qui est de l'exponentiation, on a immédiatement :

$$\big(u_n\big)^k = u_{n\,k} \qquad (\forall\, n, k \in \mathbb{N}).$$

Notation 4.1. [Monôme fondamental] On notera x le polynôme u_1, c'est-à-dire :

$$x \,:=\, u_1 \,=\, \big(0,\ 1,\ 0,\ \ldots\big).$$

Alors il est clair que :

$$x^k \,=\, \big(u_1\big)^k \,=\, u_k.$$

Ensuite, comme tout polynôme $p = \big(a_0,\, a_1,\, \ldots,\, a_n,\, 0,\, \ldots\big)$ s'écrit :

$$p \,=\, a_0\, u_0 + a_1\, u_1 + \cdots + a_n\, u_n,$$

nous pouvons le ré-écrire au moyen de cette nouvelle indéterminée x :

$$p \,=\, a_0\, e + a_1\, x + a_2\, x^2 + \cdots + a_n\, x^n,$$

où e est l'élément unité de la multiplication de $A[x]$. Par conséquent, tout polynôme p est la somme finie de *monômes* $a_k\, x^k$, où x est le polynôme particulier défini ci-dessus, et où on identifie :

$$e \,\equiv\, x^0.$$

Montrons maintenant comment l'anneau A s'immerge naturellement dans l'anneau $A[x]$, au moyen de l'application :

$$\begin{array}{rccc} \chi\colon & A & \longrightarrow & A[x] \\ & a & \longmapsto & a\, e. \end{array}$$

Tout d'abord, cette application χ est un homomorphisme d'anneaux :

$$\begin{aligned} \chi(a+b) \,&=\, \chi(a) + \chi(b), \\ \chi(a\, b) \,&=\, \chi(a)\, \chi(b). \end{aligned}$$

Ensuite, χ est injectif, car :

$$a\, e \,=\, b\, e \qquad \Longleftrightarrow \qquad \big(a,\ 0,\ \ldots\big) \,=\, \big(b,\ 0,\ \ldots\big) \qquad \Longleftrightarrow \qquad a \,=\, b.$$

Ainsi, χ établit un isomorphisme de A sur son image $\chi(A)$.

Grâce à cette application χ, on *immerge* A dans $A[x]$:

$$A \,\subset\, A[x].$$

Terminologie 4.2. Les éléments de $A \subset A[x]$ sont appelés les *constantes*, ou *polynômes constants*.

En définitive, nous aboutissons à une représentation symbolique tout à fait classique et intuitive de ce que sont les polynômes.

Théorème 4.3. [Fondamental] *Tout polynôme non nul p de $A[x]$ s'écrit sous la forme définitive :*

$$p \,=\, a_0 + a_1\, x + a_2\, x^2 + \cdots + a_n\, x^n,$$

avec avec $a_n \neq 0$ et avec $n = \deg p$. □

Toutefois, il faudra conserver à l'esprit que, d'un point de vue rigoureux et abstrait, la lettre x n'est ni une variable, ni une indéterminée, mais la suite infinie $x = \big(0,\, 1,\, 0, \ldots\big)$. On admettra la coïncidence notationnelle :

$$x^0 \,\equiv\, 1_A.$$

Exemple 4.4. La preuve, donnée par la Proposition 3.16, que $\deg p\,q = \deg p + \deg q$ dans $A[x]$ pour un anneau intègre A, deviendrait complètement fausse si A n'était pas intègre.

En effet, avec :

$$A := \mathbb{Z}/6\mathbb{Z} = \big\{\overline{0},\, \overline{1},\, \overline{2},\, \overline{3},\, \overline{4},\, \overline{5}\big\},$$

où $\overline{\ell} := \ell \bmod 6$, les deux polynômes :

$$\begin{aligned} p &:= \overline{2}\,x + \overline{1}, \\ q &:= \overline{3}\,x^2 + \overline{1}, \end{aligned}$$

ont pour produit :

$$\begin{aligned} p\,q &= \overline{6}\,x^3 + \overline{3}\,x^2 + \overline{2}\,x + \overline{1} \\ &= \overline{0} + \overline{3}\,x^2 + \overline{2}\,x + \overline{1}, \end{aligned}$$

donc on a une inégalité *stricte :*

$$\deg p\,q \;=\; 2 \;<\; 3 \;=\; \deg p + \deg q.$$

Maintenant, rappelons que dans un anneau A, le *groupe des éléments inversibles* est :

$$A^\times := \big\{a \in A\colon\ \exists\, b \in A,\ ab = 1_A\big\}.$$

On sait que b est alors unique, et on le note souvent $b = a^{-1}$.

Proposition 4.5. *Si A est un anneau intègre, les éléments inversibles de $A[x]$ sont exactement les polynômes constants de degré 0 de la forme :*

$$a\,x^0,$$

où $a \in A^\times$.

Démonstration. Si $a \in A^\times$, le polynôme $a\,x^0$ est clairement inversible, d'inverse $a^{-1}x^0$.

Réciproquement, Soit un polynôme inversible $p \in A[x]^\times$, c'est-à-dire tel qu'il existe un autre polynôme $q \in A[x]$ avec :

$$p\,q \;=\; 1_{A[x]} \;=\; 1_A.$$

On a donc :

$$\deg p + \deg q \;=\; \deg 1_A \;=\; 0,$$

ce qui implique :

$$\deg p \;=\; 0 \;=\; \deg q.$$

Par conséquent, il existe $a, b \in A$ tels que :

$$p \;=\; a\,x^0 \qquad\qquad \text{et} \qquad\qquad q \;=\; b\,x^0,$$

et ensuite, $p\,q = 1_A$ donne $a\,b = 1_A$, c'est-à-dire $a \in A^\times$ — et $b \in A^\times$ aussi ! □

Corollaire 4.6. *Si $\mathbb{K}$ est un corps, les éléments de $\mathbb{K}[x]^\times$ sont exactement les polynômes constants non nuls.*

Preuve. C'est une conséquence immédiate de l'énoncé précédent, en tenant compte du fait que les éléments inversibles de $\mathbb{K}$ sont exactement les éléments non nuls de $\mathbb{K}$. □

Nous allons désormais essentiellement considérer des polynômes à coefficients dans des *corps*.

5. Division euclidienne dans $\mathbb{K}[x]$

Dans cette section, nous nous limiterons au cas particulier de l'anneau $\mathbb{K}[x]$ sur un *corps commutatif* $\mathbb{K}$. Certains énoncés seront vrais, plus généralement, dans des anneaux intègres A, pour certains polynômes dont les « *termes de tête* », *i.e.* de plus haut degré, ont des coefficients qui sont des éléments *inversibles* de A, et nous donnerons plus tard les précisions nécessaires à ce sujet.

Dans la pratique, $\mathbb{K}$ sera soit le corps $\mathbb{Q}$ des nombres rationnels, soit le corps $\mathbb{R}$ des nombres réels, soit le corps $\mathbb{C}$ des nombres complexes. Les élément du corps de base $\mathbb{K}$ seront notés par des lettres grecques α, β, γ, *etc.*, tandis que les éléments de l'anneau $\mathbb{K}[x]$ seront notés par des lettres latines, telles que a, b, p, q, r, u, v, *etc.*

Définition 5.1. Étant donné deux polynômes a et b de $\mathbb{K}[x]$, on dit que b *divise* a, ce que l'on note :

$$b \mid a,$$

s'il existe un polynôme $q \in \mathbb{K}[x]$ tel que :

$$b\,q \;=\; a.$$

On dit aussi que a *est un multiple de* b, ou que b *est un diviseur de* a.

Puisque $b\,0 = 0$ quel que soit le polynôme b, on a toujours :

$$b \mid 0.$$

En particulier, $0 \mid 0$. Mais attention ! Pour tout polynôme *non nul* $a \in \mathbb{K}[x]\backslash\{0\}$, il est radicalement impossible que $0 \mid a$, puisque $a = 0\,q = 0$ est contradictoire.

Par exemple, dans l'anneau $\mathbb{R}[x]$, le polynôme $x - 1$ divise $x^2 - 1$, car on peut écrire :

$$(x-1)\,(x+1) \;=\; x^2 - 1.$$

Par contre(-exemple), le polynôme x ne divise *pas* $x + 1$, car on ne peut *pas* trouver (exercice) de polynôme q tel que $x\,q = x + 1$.

Les propriétés élémentaires suivantes résultent immédiatement de la Définition 5.1.

Proposition 5.2. *Pour tous* $a, b, c, d \in \mathbb{K}[x]$*, on a :*

$$\begin{aligned}
& a \mid a && && \text{(\textit{réflexivité})},\\
\big(\, a \mid b \quad \textit{et} \quad b \mid c \,\big) \quad & \Longrightarrow && a \mid c && \text{(\textit{transitivité})},\\
\big(\, a \mid b \quad \textit{et} \quad a \mid c \,\big) \quad & \Longrightarrow && a \mid (b+c), &&\\
\big(\, a \mid b \quad \textit{et} \quad c \mid d \,\big) \quad & \Longrightarrow && a\,c \mid b\,d. && \square
\end{aligned}$$

Toutefois, comme nous l'avons déjà vu dans $\mathbb{Z}$, la relation de divisibilité n'est *pas* symétrique, donc ne définit par une relation d'équivalence.

Soit $b \in \mathbb{K}[x]$ fixé. L'ensemble des polynômes multiples de b :

$$I \;:=\; \big\{ b\,q \colon\; q \in \mathbb{K}[x] \big\} \;=\; b\,\mathbb{K}[x],$$

satisfait les propriétés évidentes suivantes :

$$\begin{aligned}
\Big(\, a \,=\, b\,q \,\in\, I \quad \text{et} \quad a' \,=\, b\,q' \,\in\, I \,\Big) \quad & \Longrightarrow \quad a - a' \,=\, b\,(q - q') \,\in\, I,\\
\Big(\, a \,=\, b\,q \,\in\, I \quad \text{et} \quad p \,\in\, \mathbb{K}[x] \text{ quelconque} \,\Big) \quad & \Longrightarrow \quad p\,a \,=\, b\,(p\,q) \,\in\, I.
\end{aligned}$$

Cet ensemble I contient le polynôme $0 = b\,0$ ainsi que le polynôme $b = b\,1$.

Si l'on écarte le polynôme 0, on a :

$$\begin{aligned} a \in I\backslash\{0\} \quad &\Longrightarrow \quad b \mid a \\ &\Longrightarrow \quad a = b\,q \\ &\Longrightarrow \quad \deg a \geqslant \deg b. \end{aligned}$$

Par conséquent, dans $I\backslash\{0\}$, le polynôme b est un polynôme de *degré minimum*.

De plus, si $a \in I$, par définition, il existe un polynôme q tel que :

$$a - b\,q = 0,$$

tandis que si $a \notin I$ — on dit alors que b ne divise pas a, ce que l'on note $b \nmid a$ —, il n'existe pas de polynôme q vérifiant cette relation $a - b\,q = 0$.

Nous allons donc nous efforcer de trouver un polynôme q tel que la différence $a - b\,q$ ait le plus petit degré possible, lorsque $a \notin I$.

La division euclidienne dans $\mathbb{K}[x]$ fonctionne de manière essentiellement analogue à la division euclidienne dans l'anneau $\mathbb{Z}$ des entiers relatifs, sachant que *plusieurs* opérations de soustractions successives s'avèrent nécessaires. Avant de présenter la division euclidienne générale dans $\mathbb{K}[X]$, traitons un exemple parlant, avec $\mathbb{K} = \mathbb{Q}$.

Exemple 5.3. Soit le polynôme quartique :

$$a := \mathbf{3\,x^4} + 2\,x^3 + x + 5,$$

à *diviser avec reste* par le polynôme quadratique (donc de degré inférieur) :

$$b := \mathbf{x^2} + 2\,x + 3,$$

les deux *monômes de tête* de a et de b étant placés en première position.

On se convainc mentalement que c'est la multiplication par le monôme $3\,x^2$ qui permet de faire monter le monôme de tête de b au niveau de celui de a :

$$\mathbf{3\,x^4} = 3\,x^2 \cdot \mathbf{x^2},$$

et donc, on est conduit à soustraire :

$$a \underbrace{-\,3\,x^2\,b}_{-3x^4-6x^3-9x^2} \quad ,$$

procédé que l'on peut aussi représenter agréablement sous forme d'un tableau incomplet qui commence à se remplir :

$$\begin{array}{rl|l} 3\,x^4 + 2\,x^3 + 0 + x + 5 & & x^2 + 2\,x + 3 \\ \cline{3-3} -\,3\,x^4 - 6\,x^3 - 9\,x^2 & & 3\,x^2 \\ \cline{1-1} -\,4\,x^3 - 9\,x^2 + x + 5 & & \\ 4\,x^3 + 8\,x^2 + 12\,x & & -\,4\,x \\ \cline{1-1} -\,x^2 + 13\,x + 5 & & \\ x^2 + 2\,x + 3 & & -\,1 \\ \cline{1-1} \boxed{\mathbf{15\,x + 8}} & & \\ \cline{3-3} & & \boxed{\mathbf{3\,x^2 - 4\,x - 1}} \end{array}$$

Ce tableau synoptique permet alors de lire instantanément le quotient q et le reste r dans la division du polynôme a par le polynôme b :

$$a \;=\; q\,b + r,$$

équation qui s'écrit donc explicitement :

$$3\,x^4 + 2\,x^3 + x + 5 \;=\; \big(\mathbf{3\,x^2 - 4\,x - 1}\big)\cdot\big(x^2 + 3\,x + 3\big) + \mathbf{15\,x + 8}.$$

Théorème 5.4. *Étant donné deux polynômes a et b dans $\mathbb{K}[x]$ avec $b \neq 0$, il existe un couple* unique *de polynômes (q, r) de $\mathbb{K}[x]$ tels que :*

$$\begin{cases} a \;=\; b\,q + r, \\ \deg r \;<\; \deg b. \end{cases}$$

Pour déterminer ce couple (q, r), nous allons généraliser la division euclidienne que nous connaissons déjà en arithmétique pour les nombres entiers de $\mathbb{Z}$.

Terminologie 5.5. Les polynômes a, b, q, r, sont appelés, respectivement, *dividende*, *diviseur*, *quotient*, *reste*.

Démonstration. Existence. Si $a = 0$, il n'y a rien à faire, puisque $q := 0$ et $r := 0$ conviennent.

Supposons donc $a \neq 0$, écrivons a et b en ordonnant leurs monômes selon les puissances *dé*croissantes :

$$a \;=\; \alpha_n\,x^n + \alpha_{n-1}\,x^{n-1} + \cdots + \alpha_1\,x + \alpha_0 \qquad (\alpha_n \neq 0),$$
$$b \;=\; \beta_m\,x^m + \beta_{m-1}\,x^{m-1} + \cdots + \beta_1\,x + \beta_0 \qquad (\beta_m \neq 0),$$

et proposons-nous d'établir que les deux polynômes q et r existent, en montrant comment les calculer algorithmiquement.

Si $\deg a < \deg b$, alors $q := 0$ et $r := a$ conviennent — aucun travail à faire !

Supposons donc que $\deg a \geqslant \deg b$, c'est-à-dire que $n \geqslant m$.

Puisque les coefficients α_i et β_j appartiennent à un corps $\mathbb{K}$, et puisque $\frac{1}{\beta_m}$ existe dans $\mathbb{K}$, nous pouvons diviser le terme de tête (*i.e.* de plus haut degré) $\alpha_n\,x^n$ de a par celui $\beta_m\,x^m$ de b, ce qui nous donne le joli quotient polynomial :

$$q_1 \;:=\; \tfrac{\alpha_n}{\beta_m}\,x^{n-m}.$$

Ensuite, calculons la différence :

$$\begin{aligned} a - b\,q_1 \;=\; & \underline{\alpha_n\,x^n}_{\circ} + \alpha_{n-1}\,x^{n-1} + \cdots + \alpha_1\,x + \alpha_0 \\ & \underline{-\tfrac{\alpha_n}{\beta_m}\,\beta_m\,x^n}_{\circ} - \tfrac{\alpha_n}{\beta_m}\,\beta_{m-1}\,x^{n-1} - \cdots - \tfrac{\alpha_n}{\beta_m}\,\beta_0\,x^{n-m}, \end{aligned}$$

afin de faire disparaître le monôme de plus haut degré de a, ce qui nous donne un polynôme dont le degré a strictement *baissé :*

$$a - b\,q_1 \;=:\; r_1 \qquad \text{avec} \qquad \deg a \;>\; \deg r_1.$$

Si $\deg r_1 < \deg b$, ce qui inclut le cas $r_1 = 0$ car $\deg 0 = -\infty$ par convention, alors le couple (q_1, r_1) répond à la question — fin du travail en une seule étape !

Supposons donc que $\deg r_1 \geqslant \deg b$, écrivons le polynôme obtenu :

$$r_1 \;=\; \gamma_\ell\,x^\ell + \gamma_{\ell-1}\,x^{\ell-1} + \cdots + \gamma_1\,x + \gamma_0 \qquad (\gamma_\ell \neq 0),$$

qui est de degré $\ell \geqslant m$, divisons à nouveau son terme de tête par celui $\beta_m\, x^m$ de b pour obtenir :

$$q_2 \,:=\, \tfrac{\gamma_\ell}{\beta_m}\, x^{\ell-m},$$

et faisons à nouveau disparaître par soustraction le monôme de plus haut degré de r_1 :

$$\begin{aligned} r_1 - b\, q_2 \,=\, & \underline{\gamma_\ell\, x^\ell}_{\circ} + \gamma_{\ell-1}\, x^{\ell-1} + \cdots + \gamma_1\, x + \gamma_0 \\ & - \underline{\tfrac{\gamma_\ell}{\beta_m}\, \beta_m\, x^\ell}_{\circ} - \tfrac{\gamma_\ell}{\beta_m}\, \beta_{m-1}\, x^{\ell-1} - \cdots - \tfrac{\gamma_\ell}{\beta_m}\, \beta_1\, x^{\ell-m+1} - \tfrac{\gamma_\ell}{\beta_m}\, \beta_0\, x^{\ell-m}, \end{aligned}$$

ce qui nous donne un nouveau polynôme dont le degré a strictement *baissé :*

$$r_1 - b\, q_2 \,=:\, r_2 \qquad\qquad \text{avec} \qquad\qquad \deg r_1 \,>\, \deg r_2.$$

Si $\deg r_2 \,<\, \deg b$, ce qui inclut le cas $r_2 \,=\, 0$ car $\deg 0 \,=\, -\infty$ par convention, alors puisque l'on a :

$$a - b\, q_1 \,=\, r_1 \,=\, b\, q_2 + r_2 \qquad\qquad \Longrightarrow \qquad\qquad a \,=\, b\,(q_1 + q_2) + r_2,$$

le couple $\big(q_1 + q_2, r_2\big)$ répond à la question — fin du travail en deux étapes.

Mais si $\deg r_2 \geqslant \deg b$, nous devons continuer a répéter le même raisonnement, ce qui produit une suite de couples de polynômes (q_i, r_i) satisfaisant :

$$\begin{array}{rcr} r_2 - b\, q_3 \,=:\, r_3 & \text{avec} & \deg r_2 \,>\, \deg r_3, \\ \cdots\cdots\cdots\cdots & \cdots\cdot & \cdots\cdots\cdots\cdots\cdots \\ r_{\nu-1} - b\, q_\nu \,=:\, r_\nu & \text{avec} & \deg r_{\nu-1} \,>\, \deg r_\nu, \end{array}$$

de telle sorte que les *degrés* des restes successifs r_i forment une suite *strictement décroissante* dans $\mathbb{N} \cup \{-\infty\}$:

$$\deg r_1 \,>\, \deg r_2 \,>\, \cdots \,>\, \deg r_\nu \,>\, \cdots\,.$$

Comme $\deg b = m \geqslant 0$ est un entier fini, il est nécessaire qu'à partir d'un certain rang, disons ν comme nous venons de l'écrire à l'instant, on ait :

$$\deg r_{\nu-1} \,\geqslant\, \deg b \,>\, \deg r_\nu,$$

où dans la deuxième inégalité à droite, deux cas peuvent se présenter :

$$\deg r_\nu \,=\, -\infty \qquad\qquad \text{ou} \qquad\qquad \deg r_\nu \,\in\, \mathbb{N}.$$

Dans tous les cas, en additionnant verticalement toutes les égalités obtenues :

$$\begin{aligned} a - b\, q_1 \,&=\, r_1, \\ r_1 - b\, q_2 \,&=\, r_2, \\ r_2 - b\, q_3 \,&=\, r_3, \\ \cdots\cdots\cdots\cdots\cdots & \\ r_{\nu-1} - b\, q_\nu \,&=\, r_\nu, \end{aligned}$$

nous obtenons grâce à des disparitions agréables de termes à gauche et à droite :

$$a - b\,\Big(q_1 + q_2 + \cdots + q_\nu\Big) \,=\, r_\nu,$$

et donc nous concluons la démonstration d'existence en prenant [1] :

$$\begin{aligned} q &:= q_1 + q_2 + \cdots + q_\nu, \\ r &:= r_\nu. \end{aligned}$$

Pour terminer, observons que le premier cas ci-dessus où $\deg r_\nu = -\infty$, c'est-à-dire où $r_\nu = 0$, correspond au cas où $a = b\,q$ est *divisible* par b.

Unicité. Il nous reste à montrer que le couple (q, r) ainsi trouvé est unique. Supposons donc qu'il existe un autre couple (q_1, r_1) répondant à la question, c'est-à-dire qu'on ait à la fois :

$$\begin{cases} a = b\,q + r, \\ \deg r < \deg b, \end{cases} \qquad \text{et} \qquad \begin{cases} a = b\,q_1 + r_1, \\ \deg r_1 < \deg b. \end{cases}$$

Aisément, nous en déduisons :

$$b\,q + r = b\,q_1 + r_1,$$

puis :

$$r - r_1 = b\,\big(q_1 - q\big)$$

ce qui implique :

$$\deg\,(r - r_1) = \deg b + \deg\,(q_1 - q).$$

Par ailleurs, la Proposition 3.4 donne :

$$\begin{aligned} \deg\,(r - r_1) &\leqslant \max\big\{\deg r,\, \deg r_1\big\} \\ &< \deg b. \end{aligned}$$

Ces deux (in)égalités sur $\deg\,(r - r_1)$ sont incompatibles si $\deg\,(q - q_1) \geqslant 0$, c'est-à-dire si $q - q_1 \neq 0$ n'est pas le polynôme nul, car alors tous les degrés impliqués sont des entiers (finis) dans $\mathbb{N}$.

Mais elles sont tout à fait compatibles lorsque :

$$\deg\,(q - q_1) = -\infty \qquad \text{et} \qquad -\infty = \deg\,(r_1 - r),$$

c'est-à-dire lorsque :

$$q = q_1 \qquad \text{et} \qquad r_1 = r. \qquad \square$$

Dans la division euclidienne énoncée par le Théorème 5.4, l'hypothèse $b \neq 0$ est vraiment nécessaire. Le cas particulier où $b = \omega \in \mathbb{K}^*$ est une constante non nulle, c'est-à-dire où $\deg b = 0$, mérite une mention.

Observation 5.6. *Soient un polynôme $a \in \mathbb{K}[x]$ et soit $b \in \mathbb{K}^*$ une constante non nulle. Alors la division euclidienne de a par b est :*

$$a = b\,\big(\tfrac{1}{b}\,a\big) + \mathbf{0}. \qquad \square$$

Autrement dit, le reste $r = 0$ est nul, et la condition $\deg r < \deg b$ est bien satisfaite, car $-\infty < 0$.

1. — et en prononçant à haute voix q_ν ! —

6. Idéaux I dans $\mathbb{K}[x]$ et anneau principal $\mathbb{K}[x]$

Introduisons la notion d'idéal d'un anneau commutatif $\big(A, +, \times, 0, 1\big)$ quelconque.

Définition 6.1. Un sous-ensemble non vide $I \subset A$ est appelé un *idéal* s'il vérifie les deux propriétés suivantes :

$$\Big(\ a \in I \quad \text{et} \quad b \in I \ \Big) \qquad \Longrightarrow \qquad a - b \in I,$$

$$\Big(\ a \in I \quad \text{et} \quad p \in A \text{ quelconque} \ \Big) \qquad \Longrightarrow \qquad p\, a \in I.$$

Un idéal $I \subset A$ est dit *principal* s'il existe $b \in I$ tel que I soit *égal* à l'ensemble de tous les multiples de b :

$$I \ = \ \big\{ b\, q \colon \ q \in A \big\} \ = \ b\, A.$$

Notation 6.2. L'ensemble des multiples d'un élément $b \in I$ sera noté :

$$b\, A \ := \ \big\{ b\, q \colon \ q \in A \big\}.$$

Observation 6.3. *Pour un idéal $I \subset A$, on a équivalence entre :*

(i) $I = A$*;*

(ii) $1 \in A$.

Preuve. **(i)** $\Longrightarrow$ **(ii)** est trivial.

(ii) $\Longrightarrow$ **(i)** Si $1 \in A$, alors $p \cdot 1 \in A$ pour tout $p \in A$ par définition d'un idéal I, c'est-à-dire $A \subset I$, et comme $I \subset A$ de toute façon, c'est que $I = A$. □

Dans cette section, nous considérons l'anneau :

$$A \ := \ \mathbb{K}[x],$$

des polynômes à une indéterminée x et à coefficients dans un corps fixé $\mathbb{K}$.

Souvenons-nous que nous avons démontré que tous les sous-groupes additifs non triviaux [2] de $\mathbb{Z}$ sont de la forme $n\,\mathbb{Z}$ avec $n \geqslant 2$ entier. En particulier, cela implique aussi (exercice) que tous les *idéaux* non triviaux de $\mathbb{Z}$ sont de cette forme $n\,\mathbb{Z}$. Un résultat très analogue et tout aussi étonnant de simplicité est vrai pour $\mathbb{K}[x]$.

Théorème 6.4. *Tout idéal $I \subset \mathbb{K}[x]$ est principal, et plus précisément :*

$$I \ = \ \big\{ d\, q \colon \ q \in \mathbb{K}[x] \ \textit{quelconque} \big\},$$

où $d \in I \backslash \{0\}$ est n'importe quel polynôme non nul de degré minimal.

Démonstration. Si $I = \{0\}$, puisque $\deg 0 = -\infty$, il suffit de prendre $q := 0$.

Nous pouvons donc supposer que $I \neq \{0\}$. Posons alors :

$$I^* \ := \ I \backslash \{0\}.$$

L'ensemble des nombres naturels $\deg a$ lorsque le polynôme a parcourt I^* est donc une partie non vide de $\mathbb{N}$. D'après un théorème connu de l'arithmétique de Peano, cet ensemble admet un certain plus petit élément :

$$m \ := \ \min \big\{ \deg a \colon \ a \in I^* \big\}.$$

2. — c'est-à-dire différents de $\{0\}$ et de $\mathbb{Z}$ lui-même —

Choisissons alors un certain polynôme $d \in I^*$ tel que :

$$\deg d \,=\, m.$$

Un tel polynôme n'est d'ailleurs pas unique, parce que, quelle que soit la constante non nulle $\alpha \in \mathbb{K}^*$, il est clair que $\alpha\, d \in I^*$ a le même degré que d, et donc, $\alpha\, d$ minimise aussi le degré parmi les éléments de I.

Ensuite, puisque d est de degré minimal des éléments de $I\backslash\{0\}$, nous avons l'observation évidente que :

$$\Big(\; r \,\in\, I \qquad \text{et} \qquad \deg r \,<\, \deg d \;\Big) \qquad\qquad \Longrightarrow \qquad\qquad r \,=\, 0.$$

Ceci étant dit, nous affirmons à présent que *tout polynôme appartenant à I est un multiple de d*, ce qui conclura l'argumentation.

En effet, soit $a \in I$ quelconque. Sans aucune retenue, et de manière la plus addictive qui soit, effectuons alors l'euclidivision de a par d :

$$a \,=\, d\,q + r \qquad\qquad \text{avec} \qquad\qquad \deg r \,<\, \deg d,$$

et injectons puissamment cette belle équation dans la définition de l'idéal I :

$$\begin{aligned}
\Big(\; a \,\in\, I, \qquad d \,\in\, I, \qquad q \,\in\, \mathbb{K}[x] \;\Big) \qquad &\Longrightarrow \qquad d\,q \,\in\, I \\
&\Longrightarrow \qquad a - d\,q \,\in\, I, \\
&\Longrightarrow \qquad r \,\in\, I, \\
&\Longrightarrow \qquad r \,=\, 0,
\end{aligned}$$

et souvenons-nous de notre observation évidente, pour conclure que :

$$a \,=\, d\,q \,\in\, d\,\mathbb{K}[x].$$ □

Définition 6.5. Deux polynômes p et q dans $\mathbb{K}[x]$ sont dits *associés* s'il existe une constante non nulle $\lambda \in \mathbb{K}^*$ telle que :

$$\lambda\, p \,=\, q.$$

Il est aisé de vérifier que la relation binaire sur $\mathbb{K}[x]$:

$$p \,\sim\, q \qquad\qquad \overset{\text{déf}}{\Longleftrightarrow} \qquad\qquad \Big(\; \exists\, \lambda \,\in\, \mathbb{K}^* \qquad \lambda\, p \,=\, q \;\Big)$$

est une relation d'équivalence.

Le singleton $\{0\}$ est une classe d'équivalence, tandis que l'ensemble $\mathbb{K}^* = \mathbb{K}\backslash\{0\}$ des constantes non nulles en est une autre.

Définition 6.6. Un polynôme p de degré $n \geqslant 0$ est dit *unitaire* si le coefficient de son monôme de tête est égal à 1 :

$$p \,=\, \mathbf{1} \cdot x^n + \beta_{n-1}\, x^{n-1} + \cdots + \beta_1\, x + \beta_0.$$

Tout polynôme p de degré $n \geqslant 0$ s'écrit :

$$p \,=\, \alpha_n\, x^n + \alpha_{n-1}\, x^{n-1} + \cdots + \alpha_1\, x_1 + \alpha_0 \qquad\qquad (\alpha_n \neq 0),$$

d'où pour $\lambda \in \mathbb{K}^*$ quelconque :

$$\lambda\, p \,=\, \lambda\, \alpha_n\, x^n + \lambda\, \alpha_{n-1}\, x^{n-1} + \cdots + \lambda\, \alpha_1\, x + \lambda\, \alpha_0.$$

Le coefficient de tête $\alpha_n \neq 0$ est transformé en $\lambda\, \alpha_n$. Puisque $\mathbb{K}$ est un corps, avec $\lambda := \frac{1}{\alpha_n} \in \mathbb{K}^*$, on peut rendre le coefficient de tête égal à 1.

Observation 6.7. *Pour tout polynôme non nul $p \in \mathbb{K}[x]\backslash\{0\}$, il existe une unique constante $\lambda \in \mathbb{K}^*$ telle que $\lambda\, p$ est unitaire.* □

En particulier, si $\deg p = n = 0$, d'où $p = \alpha_0 \neq 0$, avec $\lambda := \frac{1}{\alpha_0}$, on fait $\lambda\, p = 1$.

Notation 6.8. L'ensemble des polynômes unitaires sera noté :

$$\mathbb{K}[x]_1 \,:=\, \Big\{x^n + \beta_{n-1}x^{n-1} + \cdots + \beta_1 x + \beta_0 \colon\ n \geqslant 0,\ \beta_{n-1}, \ldots, \beta_1, \beta_0 \in \mathbb{K}\Big\}.$$

Proposition 6.9. *Pour deux polynômes $a, b \in \mathbb{K}[x]$, on a équivalence entre :*

(i) *$a \sim b$ sont associés,* i.e. *il existe $\lambda \in \mathbb{K}^*$ avec $\lambda\, a = b$;*

(ii) *$a \,|\, b$ et $b \,|\, a$;*

(iii) *les idéaux qu'ils engendrent sont égaux :*

$$a\,\mathbb{K}[x] \;=\; b\,\mathbb{K}[x].$$ □

Comme tout idéal non nul de $\mathbb{K}[x]$ est engendré par seulement *un* polynôme, d'après le Théorème 6.4, nous obtenons le

Corollaire 6.10. *Soit I un idéal de $\mathbb{K}[x]$, différent de $\{0\}$. Alors il existe un unique polynôme* unitaire *$d \in \mathbb{K}[x]_1$ tel que :*

$$I \;=\; d\,\mathbb{K}[x].$$ □

7. Plus Grand Commun Diviseur dans $\mathbb{K}[x]$ et théorème de Bézout

Maintenant, nous allons présenter la notion de diviseur commun dans $\mathbb{K}[x]$, ainsi que le concept de plus grand diviseur commun, toujours dans $\mathbb{K}[x]$, en nous souvenant que nous maîtrisons parfaitement ces concepts dans l'anneau $\mathbb{Z}$ depuis que nous avons gaillardement passé l'examen partiel d'arithmétique.

Définition 7.1. Étant donné un polynôme $a \in \mathbb{K}[x]$, on notera $\mathscr{D}(a)$ l'ensemble des diviseurs de a :

$$\begin{aligned}\mathscr{D}(a) \,&:=\, \big\{e \in \mathbb{K}[x] \colon\ e \mid a\big\}\\ &=\, \big\{e \in \mathbb{K}[x] \colon\ \exists\, u \in \mathbb{K}[x],\ e\,u = a\big\}.\end{aligned}$$

Pour $a = 0$, en prenant toujours $u = 0$, nous voyons que $\mathscr{D}(a) = \mathbb{K}[x]$ — cas inintéressant. Nous excluerons dorénavant la plupart du temps le cas dégénéré $a \neq 0$.

Définition 7.2. Étant donné deux polynômes $a \in \mathbb{K}[x]$ et $b \in \mathbb{K}[x]$ avec $(a, b) \neq (0, 0)$ tout polynôme appartenant à l'intersection :

$$\mathscr{D}(a) \cap \mathscr{D}(b) \;=\; \big\{e \in \mathbb{K}[x] \colon\ e \,|\, a \text{ et } e \,|\, b\big\},$$

sera appelé *diviseur commun de a et b.*

Nous voulons comprendre ce que sont les diviseurs communs de a et de b.

Lemme 7.3. *Soit $e \in \mathbb{K}[x]$ tel que $e \,|\, a$ et $e \,|\, b$. Alors :*

$$\mathscr{D}(e) \;\subset\; \mathscr{D}(a) \cap \mathscr{D}(b).$$

Autrement dit, tout diviseur de e divise nécessairement a et b.

Démonstration. Soit donc $f \in \mathscr{D}(e)$, c'est-à-dire $f \mid e$. Ainsi par hypothèse :

$$f \,|\, e \,|\, a \qquad\qquad \text{et} \qquad\qquad f \,|\, e \,|\, b,$$

donc par transitivité de la divisibilité, il vient $f \mid a$ et $f \mid b$, c'est-à-dire $f \in \mathscr{D}(a) \cap \mathscr{D}(b)$. □

Maintenant, comment trouver les diviseurs e communs à a et à b qui sont « *maximaux* », en un certain sens ? Par un détour Eiffel !

Dans cet objectif, étudions en effet l'ensemble :

$$\begin{aligned} I &:= \big\{a\,u + b\,v\colon\ u \in \mathbb{K}[x] \text{ quelconque},\ v \in \mathbb{K}[x] \text{ quelconque}\big\} \\ &= a\,\mathbb{K}[x] + b\,\mathbb{K}[x]. \end{aligned}$$

Il est aisé de vérifier que I est un *idéal* de $K[x]$, comme suit :

$$\begin{aligned} \big(a\,u + b\,v\big) - \big(a\,u' + b\,v'\big) &= a\,\big(u - u'\big) - b\,\big(v - v'\big) \in I, \\ \forall\, p \in \mathbb{K}[x], \qquad p\,\big(a\,u + b\,v\big) &= a\,(p\,u) + b\,(p\,v) \in I. \end{aligned}$$

Or comme tout idéal $I \subset \mathbb{K}[x]$ est principal grâce au Théorème 6.4 — *Deus ex machina !* —, tout polynôme de I est multiple de l'un d'eux, $d \in I$, de degré minimal :

$$\deg d = \min\big\{\deg c\colon\ c \in I\big\}.$$

Quitte à multiplier d par une constante non nulle appropriée, on peut supposer que :

$$d \in \mathbb{K}[x]_1.$$

Ainsi :

$$I = d\,\mathbb{K}[x].$$

Proposition 7.4. *Soient $a, b \in \mathbb{K}[X]$ avec $(a, b) \neq (0, 0)$. Alors l'unique polynôme unitaire $d \in \mathbb{K}[x]_1$ tel que :*

$$a\,\mathbb{K}[x] + b\,\mathbb{K}[x] = d\,\mathbb{K}[x],$$

satisfait :

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(d).$$

Autrement dit, le polynôme d permet donc à lui seul de connaître tous les diviseurs communs à a et à b, puisque ce sont exactement les diviseurs de ce polynôme d !

Démonstration. Pour tous $u, v \in \mathbb{K}[x]$, on vient de dire que :

$$a\,u + b\,v \in I = d\,\mathbb{K}[x],$$

d'où :

$$d \,\Big|\, \big(a\,u + b\,v\big),$$

donc en particulier :

$$\begin{aligned} \text{avec } u := 1 \text{ et } v := 0, \qquad &\text{il vient} \qquad d \mid a, \\ \text{avec } u := 0 \text{ et } v := 1, \qquad &\text{il vient} \qquad d \mid b. \end{aligned}$$

Alors le Lemme 7.3 offre une première inclusion :

$$\mathscr{D}(d) \subset \mathscr{D}(a) \cap \mathscr{D}(b).$$

Pour atteindre l'inclusion inverse $\mathscr{D}(a) \cap \mathscr{D}(b) \subset \mathscr{D}(d)$, prenons un élément quelconque $e \in \mathscr{D}(a) \cap \mathscr{D}(b)$, et cherchons à faire voir que $e \mid d$, c'est-à-dire que $e \in \mathscr{D}(d)$.

Évidemment :

$$\begin{aligned} e \mid a \qquad &\Longrightarrow \qquad e \,\Big|\, a\,u \qquad \forall\, u \in \mathbb{K}[x], \\ e \mid b \qquad &\Longrightarrow \qquad e \,\Big|\, b\,v \qquad \forall\, v \in \mathbb{K}[x], \end{aligned}$$

d'où par la Proposition 5.2 :

$$e \,\Big|\, \big(a\,u + b\,v\big).$$

Or comme $d \in I$, il existe $u_0, v_0 \in \mathbb{K}[x]$ tels que :

$$a\,u_0 + b\,v_0 \;=\; d,$$

donc par conséquent :

$$e \mid d.$$

Ainsi, les deux inclusions inverses l'une de l'autre donnent l'égalité désirée $\mathscr{D}(d) = \mathscr{D}(a) \cap \mathscr{D}(b)$. □

Nous pouvons alors synthétiser et résumer les raisonnements qui précèdent.

Théorème 7.5. *Étant donné deux polynômes quelconques $a, b \in \mathbb{K}[x]$ avec $(a, b) \neq (0, 0)$, il existe toujours un unique polynôme unitaire*[3] *$d \in \mathbb{K}[x]_1$ qui représente l'ensemble de leurs diviseurs communs :*

$$\begin{aligned}\mathscr{D}(a) \cap \mathscr{D}(b) \;&=\; \big\{e \in \mathbb{K}[x] \colon\; e \mid a \text{ et } e \mid b\big\}\\ &=\; \mathscr{D}(d)\\ &=\; \big\{e \in \mathbb{K}[x] \colon\; e \mid d\big\},\end{aligned}$$

comme l'ensemble des diviseurs du seul polynôme d.

De plus, d s'obtient comme l'unique générateur unitaire de l'idéal principal :

$$\begin{aligned}I \;&=\; \big\{u\,a + v\,b \colon\; u \in \mathbb{K}[x],\; v \in \mathbb{K}[x]\big\}\\ &=\; \mathbb{K}[x]\,a + \mathbb{K}[x]\,b\\ &=:\; \mathbb{K}[x]\,d,\end{aligned}$$

et il existe $u_0, v_0 \in \mathbb{K}[x]$ tels que :

$$a\,u_0 + b\,v_0 \;=\; d.$$ □

Évidemment, on s'attend à ce que :

$$d \;\overset{?}{=}\; \mathsf{pgcd}\,(a, b),$$

mais encore faut-il préciser cette notion intuitive.

Définition 7.6. Étant donné deux polynômes quelconques $a, b \in \mathbb{K}[x]$ avec $(a, b) \neq (0, 0)$, un *plus grand commun diviseur de a et de b*, noté :

$$\mathsf{pgcd}\,(a, b),$$

c'est un polynôme $e \in \mathbb{K}[x]$ qui divise $e \mid a$ et $e \mid b$ simultanément, tout en étant de degré *maximal possible*.

Par convention, on assigne $\mathsf{pgcd}\,(0, 0) := 0$. De plus, il est trivial que :

$$\mathsf{pgcd}\,(0, b) \;=\; b \qquad \text{et} \qquad \mathsf{pgcd}\,(a, 0) \;=\; a.$$

Théorème 7.7. *Pour $a, b \in \mathbb{K}[x]$ avec $(a, b) \neq (0, 0)$, il existe un unique* pgcd unitaire *$d \in \mathbb{K}[x]_1$ de a et de b.*

Évidemment, le d en question est celui du Théorème 7.5 précédent.

3. — donc en particulier, $d \neq 0$ ne peut *pas* être le polynôme nul —

Démonstration. Si $e \in \mathbb{K}[x]_1$ est unitaire et divise $e \mid a$ et $e \mid b$, d'où, grâce audit théorème :

$$e \in \mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(d),$$

alors il existe $u \in \mathbb{K}[x]$ tel que :

$$e\,u = d \qquad \Longrightarrow \qquad \deg e + \deg u = \deg d,$$

d'où [4] :

$$\deg e \leqslant \deg d.$$

Ainsi, $e := d$ est bien l'unique diviseur commun à a et à b de degré maximal. □

Définition 7.8. Deux polynômes $a, b \in \mathbb{K}[x]$ avec $(a, b) \neq (0, 0)$ sont dits *premiers entre eux*, ce que l'on note :

$$a \wedge b = 1,$$

si :

$$\mathsf{pgcd}\,(a, b) = d = 1.$$

Nous pouvons maintenant présenter l'énoncé le plus utile de tout ce chapitre.

Théorème 7.9. [Bézout dans $\mathbb{K}[x]$] *Pour toute paire de polynômes $a, b \in \mathbb{K}[x]$ avec $(a, b) \neq (0, 0)$, il existe $u, v \in \mathbb{K}[x]$ tels que :*

$$u\,a + v\,b = \mathsf{pgcd}\,(a, b).$$

De plus, on a équivalence entre :

(i) *a et b sont premiers entre eux, c'est-à-dire que $\mathsf{pgcd}\,(a, b) = 1$ est le polynôme unitaire constant ;*

(ii) *il existe $u, v \in \mathbb{K}[x]$ tels que $u\,a + v\,b = 1$.*

Démonstration. Nous avons déjà vu l'existence de u, v, notés u_0, v_0 plus haut, tels que $u\,a + v\,b = d = \mathsf{pgcd}\,(a, b)$.

(i) $\Longrightarrow$ **(ii)** Découle tautologiquement de tout ce qui vient d'être dit.

(ii) $\Longrightarrow$ **(i)** Si donc $1 = u\,a + v\,b$, comme $\mathbb{K}[x]\,a + \mathbb{K}[x]\,b = \mathbb{K}[x]\,d$ d'après le Théorème 7.5, il existe $w \in \mathbb{K}[x]$ tel que :

$$1 = u\,a + v\,b = w\,d,$$

d'où :

$$0 = \deg w + \deg d \qquad \Longrightarrow \qquad \deg d = 0.$$

Par conséquent, $d \in \mathbb{K}^*$ est une constante, de degré 0, donc $d = 1$, puisque $d \in \mathbb{K}[x]_1$ est unitaire. □

Corollaire 7.10. *Pour deux constantes distinctes $\alpha \neq \alpha' \in \mathbb{K}$, les deux polynômes linéaires $x - \alpha$ et $x - \alpha'$ sont premiers entre eux.*

Preuve. Ligne directe Paris-Bézout en *Economy Class :*

$$1 = \tfrac{1}{\alpha' - \alpha}\big(x - \alpha\big) - \tfrac{1}{\alpha' - \alpha}\big(x - \alpha'\big).$$ □

Une paire de polynômes (u, v) telle que $a\,u + b\,v = d$ n'est *jamais* unique, car quel que soit le polynôme $q \in \mathbb{K}[x]$, on a encore :

$$a\,\big(u - q\,b\big) + b\,\big(v + q\,a\big) = d.$$

4. — comme $d \neq 0$, on a nécessairementt $e \neq 0 \neq u$, donc les trois degrés impliqués sont $\neq -\infty$ —

Théorème 7.11. [Unicité restreinte] *Étant donné deux polynômes quelconques* $a, b \in \mathbb{K}[x]$ *avec* $\deg a \geqslant 1$ *et* $\deg b \geqslant 1$*, qui sont premiers entre eux :*

$$1 \,=\, \mathsf{pgcd}\,(a,b) \,=\, a \wedge b,$$

il existe $u, v \in \mathbb{K}[x]$ uniques *avec :*

$$\deg u \,<\, \deg b \qquad\qquad \textit{et} \qquad\qquad \deg v \,<\, \deg a,$$

satisfaisant :

$$a\,u + b\,v \,=\, 1.$$

Démonstration. Dans l'identité :

$$a\,\big(u - q\,b\big) + b\,\big(v + q\,a\big) \,=\, 1,$$

choisissons $q \in \mathbb{K}[x]$ comme étant le *quotient* de la division euclidienne de u par b, de telle sorte que :

$$u - q\,b \,=\, r, \qquad\qquad \text{avec} \qquad\qquad \deg r \,<\, \deg b.$$

Renotons alors u et v ces deux facteurs satisfaisant :

$$a\,u + b\,v \,=\, 1, \qquad\qquad \text{avec} \qquad\qquad \deg u \,<\, \deg b.$$

Comme ni a ni b ne sont constants, il est impossible que $u = 0$ ou que $v = 0$, car si on avait par exemple $u = 0$, il viendrait $b\,v = 1$, ce qui forcerait $\deg b = 0$, en contradiction avec l'hypothèse $\deg b \geqslant 1$.

Donc $u \neq 0 \neq v$, c'est-à-dire qu'on a $\deg u \geqslant 0$ et $\deg v \geqslant 0$, ce qui permet d'exclure les valeurs « embêtantes » $\deg u = -\infty$ ou $\deg v = -\infty$ dans ce qui suit.

Alors :

$$b\,v \,=\, 1 - a\,u,$$

implique :

$$\begin{aligned} \underline{\deg b}_{\circ} + \deg v \,&=\, \deg a + \deg u \\ &<\, \deg a + \underline{\deg b}_{\circ}, \end{aligned}$$

c'est-à-dire aussi :

$$\deg v \,<\, \deg a. \qquad\qquad \square$$

8. Théorèmes de divisibilité dans $\mathbb{K}[x]$

Nous pouvons maintenant énoncer et démontrer tous les analogues, dans l'anneau $\mathbb{K}[x]$, des grands théorèmes arithmétiques fondamentaux valables dans l'anneau $\mathbb{Z}$ des entiers relatifs.

Théorème 8.1. [Gauss dans $\mathbb{K}[x]$**]** *Si deux polynômes* $a, b \in \mathbb{K}[x]$ *avec* $(a,b) \neq (0,0)$ *sont premiers entre eux* $a \wedge b = 1$*, alors pour tout polynôme* $c \in \mathbb{K}[x]$ *:*

$$a \,\Big|\, b\,c \qquad\qquad \Longrightarrow \qquad\qquad a \mid c.$$

Cet énoncé sera utilisé de manière cruciale dans la Section **11**, lorsque nous démontrerons que tout polynôme se factorise, de manière unique, en produit de polynômes irréductibles.

Démonstration. Par le Théorème 7.9 de Bézout, il existe deux polynômes $u, v \in \mathbb{K}[x]$ tels que $u\,a + v\,b = 1$. On a alors $u\,a\,c + v\,b\,c = c$. Comme $a \,|\, a\,c$ trivialement et comme $a \,|\, b\,c$ par hypothèse, on obtient :

$$a \;\Big|\; \big(u\,a\,c + v\,b\,c\big),$$

c'est-à-dire $a \,|\, c$. □

Proposition 8.2. *Soient a, b, c trois polynômes quelconques. Si a et b sont tous les deux premiers à c, alors leur produit $a\,b$ est aussi premier à c.*

Démonstration. Il s'agit de faire voir que :

$$d \;:=\; \mathsf{pgcd}\,\big(ab,\, c\big)$$

est égal à 1.

Comme $d \,|\, c$, il y a un polynôme e avec $d\,e = c$. Ensuite, grâce au Théorème 7.9 de Bézout, l'hypothèse $1 = a \wedge c$ s'exprime par une identité :

$$1 \;=\; u\,a + v\,c \;=\; u\,a + (v\,e)\,d,$$

qui montre que a et d sont aussi premiers entre eux.

Par ailleurs, comme $d \,|\, a\,b$ par définition et comme nous venons de dire $1 = d \wedge a$, le Théorème 8.1 de Gauss force $d \,|\, b$. Or par hypothèse, $d \,|\, c$ aussi. Enfin, comme b et c sont premiers entre eux, on a bien $d = 1$. □

Proposition 8.3. *Si a et b sont deux polynômes premiers entre eux, et s'ils divisent tous deux un certain polynôme c, alors leur produit $a\,b$ divise aussi c.*

Démonstration. En effet, on peut écrire $a\,u = c$ avec un polynôme u.

Ensuite, comme b divise c et que b est premier à a, le Théorème 8.1 de Gauss nous dit que b doit diviser u, c'est-à-dire $b\,v = u$ avec un polynôme v.

Enfin, on conclut bien que ab divise c grâce à :

$$c \;=\; a\,u \;=\; ab\,v.$$ □

On peut aisément généraliser l'énoncé précédent pour obtenir le résultat suivant.

Proposition 8.4. *Soient $a_1, \ldots, a_r \in \mathbb{K}[x]$ avec $r \geqslant 2$ des polynômes premiers entre eux deux à deux, c'est-à-dire satisfaisant :*

$$1 \;=\; \mathsf{pgcd}\,\big(a_{i_1},\, a_{i_2}\big) \qquad (\forall\, 1 \leqslant i_1 \neq i_2 \leqslant r).$$

S'ils divisent tous $a_1 \,|\, q$, …, $a_r \,|\, q$ un polynôme q donné, alors leur produit $a_1\,a_2 \cdots a_r$ divise aussi q.

Indication de preuve. Raisonner par récurrence sur le nombre $r \geqslant 2$ de polynômes a_i, en appliquant à chaque fois la Proposition 8.3. □

Pour terminer cette Section **8**, revenons maintenant au Théorème 7.9 de Bézout-partout, afin de mieux présenter ce qu'il exprime véritablement.

Considérons le cas général où a et b sont deux polynômes quelconques, non nécessairement premiers entre eux, et introduisons :

$$d \;:=\; \mathsf{pgcd}\,(a, b).$$

Comme $d \,|\, a$ et $d \,|\, b$ par définition, on peut factoriser :

$$a \;=\; d\,a' \qquad\qquad \text{et} \qquad\qquad b \;=\; d\,b',$$

au moyen de deux polynômes uniques a' et b'. *Que dire alors de a' et de b' ?* Attention ! On doit tenir compte du fait que d est de degré *maximal* parmi les diviseurs communs de a et de b !

Proposition 8.5. *Toute paire de polynômes $a, b \in \mathbb{K}[x]$ avec $(a,b) \neq (0,0)$ se factorise sous la forme :*

$$a \,=\, a' \cdot \mathsf{pgcd}\,(a,b), \qquad\qquad a \,=\, b' \cdot \mathsf{pgcd}\,(a,b), \qquad\qquad \textit{avec} \qquad\qquad 1 \,=\, a' \wedge b'.$$

Preuve. En effet, d'après le Théorème 7.9 de Bézout, $d := \mathsf{pgcd}\,(a,b)$ est combinaison linéaire de a et de b :

$$\begin{aligned} d \,&=\, u\,a + v\,b \\ &=\, u\,d\,a' + v\,d\,b', \end{aligned}$$

et après division par d de cette égalité dans $A[x]$ qui est intègre, on voit bien que a' et b' sont premiers entre eux :

$$1 \,=\, u\,a' + v\,b'. \qquad \square$$

9. Algorithme d'Euclide dans $\mathbb{K}[x]$

Comment déterminer le $\mathsf{pgcd}\,(a,b)$ entre deux polynômes quelconques $a, b \in \mathbb{K}[x]$?

Réponse : grâce à l'algorithme d'Euclide !

Par convention, $\mathsf{pgcd}\,(0,0) := 0$. De même, si $a = 0$ ou si $b = 0$, il n'y a rien à faire puisque :

$$\mathsf{pgcd}\,(0,b) \,=\, b \qquad\qquad \text{et} \qquad\qquad \mathsf{pgcd}\,(a,0) \,=\, a.$$

Ainsi, on peut supposer que $a \neq 0 \neq b$, d'où $\deg a \neq -\infty \neq \deg b$, puis par symétrie, que $\deg a \geqslant \deg b \geqslant 0$.

Alors, *divisons avec reste* a par b :

$$a \,=\, q\,b + r,$$

avec des polynômes uniques $q, r \in \mathbb{K}[x]$ et avec $\deg r < \deg b$.

Comme $\deg r$ est (strictement) inférieur à $\deg b$, si $r \neq 0$, c'est-à-dire si $\deg r \neq -\infty$, on peut spontanément avoir l'idée de re-diviser b par r ! Ce qui donne :

$$b \,=\, u\,r + s,$$

avec $\deg s < \deg r$. Mais alors pour la même raison, si $s \neq 0$ n'est pas le polynôme nul, on peut donc encore re-diviser r par s :

$$r \,=\, v\,s + t,$$

avec encore un certain polynôme-reste t de degré $\deg t < \deg s$, et ainsi de suite.

Pour aller plus loin introduisons des indices. Commençons alors par renommer :

$$r_0 := a, \qquad\qquad r_1 := b, \qquad\qquad q_1 := q, \qquad\qquad r_2 := r,$$

de telle sorte que nos deux premières divisions peuvent s'écrire :

$$\begin{aligned} r_0 &= q_1\,r_1 + r_2, \\ r_1 &= q_2\,r_2 + r_3, \end{aligned}$$

en nommant r_3 le dernier reste qui apparaît.

Alors en poursuivant indéfiniment ces divisions successives, nous aboutissons à un résultat qui peut être représenté au moyen d'un diagramme en forme diagonale descendante :

$$\begin{aligned}
r_0 &= q_1\, r_1 + r_2,\\
r_1 &= q_2\, r_2 + r_3,\\
&\ddots\quad\ddots\quad\ddots\\
r_{i-1} &= q_i\, r_i + r_{i+1},\\
r_i &= q_{i+1}\, r_{i+1} + r_{i+2},\\
&\ddots\quad\ddots\quad\ddots
\end{aligned}$$

Tant que le reste apparaissant $r_{i+1} \neq 0$ est non nul, ce qui est une hypothèse nécessaire du Théorème 5.4 de division euclidienne, on peut re-diviser :

$$r_i \;=\; q_{i+1}\, r_{i+1} + r_{i+2},$$

et ainsi de suite.

Assertion 9.1. *À partir d'un certain rang, le dernier reste obtenu devient égal à* $\mathbf{0}$.

Preuve. Par construction, la suite des degrés successifs, à valeurs dans :

$$\{-\infty\} \cup \mathbb{N},$$

est strictement décroissante :

$$\cdots < \deg r_{i+1} < \deg r_i < \cdots < \deg r_3 < \deg r_2 < \deg b.$$

Or on sait que toute suite strictement décroissante dans $\mathbb{N}$ s'arrête en temps fini. Tant que $\deg r_i \in \mathbb{N}$, ce qui implique $r_i \neq 0$ puisque seul le polynôme 0 est de degré égal à $-\infty$, on peut et on doit continuer la division.

Si on rencontre $r_i = \mathbf{0}$, on est obligé de s'arrêter, et $\deg r_i = -\infty$ est vraiment minimal.

Si on rencontre r_i avec $\deg r_i = 0$, d'où $r_i \in \mathbb{K}^*$, on peut encore diviser, et comme l'Observation 5.6 l'a déjà mis en lumière, le reste d'après $r_{i+1} = \mathbf{0}$ est nécessairement nul. □

Ainsi, si nous appelons alors ℓ, avec $\ell \geqslant 1$, l'ultime entier tel que :

$$r_\ell \neq 0 \qquad \text{tandis que} \qquad r_{\ell+1} = \mathbf{0},$$

on peut représenter le processus complet sous forme d'un beau diagramme en diagonale descendante :

$$\begin{aligned}
r_0 &= q_1\, r_1 + r_2,\\
r_1 &= q_2\, r_2 + r_3,\\
&\ddots\quad\ddots\quad\ddots\\
r_{i-1} &= q_i\, r_i + r_{i+1},\\
&\ddots\quad\ddots\quad\ddots\\
r_{\ell-2} &= q_{\ell-1}\, r_{\ell-1} + \boxed{r_\ell},\\
r_{\ell-1} &= q_\ell\, \boxed{r_\ell} + \mathbf{0},
\end{aligned}$$

De même qu'en arithmétique sur $\mathbb{Z}$, ce dernier reste non nul $r_\ell \neq 0$ joue un rôle capital. Sachant que ce polynôme n'est pas forcément unitaire, *i.e.* élément de $\mathbb{K}[x]_1$, on admettra

l'abus de langage de désigner le $\mathsf{pgcd}\,(a,b)$ — qui appartient par définition à $\mathbb{K}[x]_1$ — à multiplication près par une constante non nulle $\lambda \in \mathbb{K}^*$.

Proposition 9.2. *On a* $r_\ell = \mathsf{pgcd}\,(a,b)$.

Autrement dit, le pgcd entre deux polynômes est le dernier reste non nul dans l'algorithme d'Euclide.

Démonstration. Notons de manière abrégée $d := \mathsf{pgcd}\,(a,b)$. Ainsi, $d \,|\, r_0$ et $d \,|\, r_1$, avec $\deg d$ maximal, d'ailleurs.

Comme $r_2 = r_0 - q_1\, r_1$, on voit que $d \,|\, r_2$ aussi, puisque r_0, r_1 multiples de d impliquent $r_0 - q_1\, r_1$ multiple de d.

Ensuite, $r_3 = r_1 - q_2\, r_2$ est aussi divisible par d, et ainsi de suite.

À la fin, $d \,|\, r_{\ell-2}$ et $d \,|\, r_{\ell-1}$ impliquent $d \,|\, r_\ell$, car $r_\ell = r_{\ell-2} - q_{\ell-1}\, r_{\ell-1}$. Autrement dit $\mathsf{pgcd}\,(a,b) \,|\, r_\ell$, et donc :

$$\deg \mathsf{pgcd}\,(a,b) \leqslant \deg r_\ell. \tag{9.3}$$

Maintenant, comme des saumons, remontons la cascade diagonale, en partant du bas (droite) vers le haut (gauche). L'égalité $r_{\ell-1} = q_\ell\, r_\ell$ dit que $r_{\ell-1}$ est divisible par r_ℓ.

Puis $r_{\ell-2} = q_{\ell-1}\, r_{\ell-1} + r_\ell$ entraîne que $r_{\ell-2}$ est divisible par r_ℓ.

Puis $r_{\ell-3} = q_{\ell-2}\, r_{\ell-2} + r_{\ell-1}$ entraîne que $r_{\ell-3}$ est divisible par r_ℓ, *et ainsi de suite*.

À la fin, c'est-à-dire en haut (regarder encore le diagramme), à l'avant-dernier étage supérieur, $r_1 = q_2\, r_2 + r_3$ entraîne que $r_1 = b$ est divisible par r_ℓ, puis, à la source du torrent tout en haut, $r_0 = q_1\, r_1 + r_2$ entraîne que $r_0 = a$ est divisible par r_ℓ.

Ainsi, $r_\ell \,|\, a$ et $r_\ell \,|\, b$. Comme le pgcd est le diviseur simultané ayant le plus grand degré possible, il est clair que :

$$\deg r_\ell \leqslant \deg \mathsf{pgcd}\,(a,b),$$

ce qui est l'inégalité *opposée* de celle, (9.3), déjà obtenue.

En conclusion, on a bien :

$$\deg \mathsf{pgcd}\,(a,b) = \deg r_\ell,$$

et donc forcément — à multiplication par une constante non nulle près — :

$$\mathsf{pgcd}\,(a,b) = r_\ell. \qquad \square$$

Comme dans $\mathbb{Z}$, on peut se convaincre en y réfléchissant que toutes ces opérations ne dépendent que des deux polynômes a et b fournis au départ. En particulier, tous les polynômes-restes r_i construits pas à pas ne dépendent que de a et de b.

Et maintenant, nous allons montrer des *formules* qui expriment les restes r_i comme *combinaison linéaires* de a et de b. À cette fin, outre la suite connue :

$$r_0 := a, \qquad r_1 := b, \qquad r_{i+1} := r_{i-1} - q_i\, r_i \qquad (1 \leqslant i \leqslant \ell-1),$$

introduisons les *deux* suites auxiliaires assez similaires :

$$u_0 := 1, \qquad u_1 := 0, \qquad u_{i+1} := u_{i-1} - q_i\, u_i \qquad (1 \leqslant i \leqslant \ell-1),$$
$$v_0 := 0, \qquad v_1 := 1, \qquad v_{i+1} := v_{i-1} - q_i\, v_i \qquad (1 \leqslant i \leqslant \ell-1).$$

Lemme 9.4. *Pour tout* $i = 0, 1, 2, \ldots, \ell$, *le reste* r_i *se représente comme la combinaison linéaire suivante de* a *et de* b *:*

$$u_i\, a + v_i\, b = r_i.$$

Démonstration. Pour $i = 0$, vérifions :

$$u_0\,a + v_0\,b \;=\; 1 \cdot a + 0 \cdot b \overset{?}{=} r_0,$$

ce qui est vrai car $a = r_0$ par définition.

Pour $i = 1$, vérifions :

$$u_1\,a + v_1\,b \;=\; 0 \cdot a + 1 \cdot b \overset{?}{=} r_1,$$

ce qui est à nouveau vrai car $b = r_1$ par définition.

En raisonnant par récurrence *double*, supposons que pour un certain indice i avec $1 \leqslant i \leqslant \ell - 1$, on ait démontré les *deux* formules :

$$\begin{aligned} u_{i-1}\,a + v_{i-1}\,b \;&=\; r_{i-1}, \\ u_i\,a + v_i\,b \;&=\; r_i, \end{aligned}$$

et demandons-nous si, à l'étage en-dessous, on a encore :

$$u_{i+1}\,a + v_{i+1}\,b \overset{?}{=} r_{i+1},$$

ou, de manière équivalente, si on a :

$$\big(u_{i-1} - q_i\,u_i\big)\,a + \big(v_{i-1} - q_i\,v_i\big)\,b \overset{?}{=} r_{i-1} - q_i\,r_i.$$

Mais après réorganisation, et factorisation de deux termes à gauche par q_i, ceci équivaut à l'identité vraie tautologiquement :

$$\underbrace{u_{i-1}\,a + v_{i-1}\,b}_{=\,r_{i-1}} - q_i\,\big(\underbrace{u_i\,a + v_i\,b}_{=\,r_i}\big) \overset{\text{oui}}{=} r_{i-1} - q_i\,r_i. \qquad \square$$

À la fin tout en bas, pour $i = \ell$, on obtient donc une représentation :

$$u_\ell\,a + v_\ell\,b \;=\; \mathsf{pgcd}\,(a, b),$$

du $\mathsf{pgcd}\,(a, b) = r_\ell$ comme combinaison linéaire de a et de b.

Théorème 9.5. *Le* pgcd *entre deux polynômes quelconques donnés $a \in \mathbb{K}[x]$ et $b \in \mathbb{K}[x]$ avec $a \neq 0 \neq b$ se calcule en effectuant l'algorithme d'Euclide dans $\mathbb{K}[x]$, et en mémorisant les résultats intermédiaires jusqu'à obtenir — à multiplication par une constante non nulle près — :*

$$\mathsf{pgcd}\,(a, b) \;=\; u_\ell\,a + v_\ell\,b \qquad (\exists\, u_\ell \in \mathbb{Z},\, \exists\, v_\ell \in \mathbb{Z}). \quad \square$$

Toutefois, cet énoncé n'est pas assez précis, *techniquement*. Il sous-entend que l'on doit implémenter les trois suites $\{r_i\}_{i=0}^{\ell}$, $\{u_i\}_{i=0}^{\ell}$, $\{v_i\}_{i=0}^{\ell}$, ce qui fonctionne très bien sur ordinateur, mais comme les ordinateurs ne sont pas autorisés lors des examens universitaires, il est tout à fait légitime de se poser la

Question 9.6. *Comment calculer, concrètement et manuellement, une représentation linéaire du* pgcd *entre deux polynômes non nuls sous la forme :*

$$\mathsf{pgcd}\,(a, b) \;=\; u\,a + v\,b \;\textbf{?}$$

10. Exemples de calculs pratiques de pgcd dans $\mathbb{K}[x]$

Répondons à cette question en traitant deux exemples ingrats et pénibles, presque aussi désagréables qu'un sujet d'examen en pleine vague de froid d'un affreux mois de janvier. Travaillons sur le corps $\mathbb{K} := \mathbb{Q}$.

Exemple 10.1. Soient les deux polynômes :

$$a := x^5 - 2x^4 + x^2 - x - 2 = r_0, \qquad b := x^3 - x^2 - x - 2 = r_1.$$

Pour calculer $\mathsf{pgcd}\,(a,b)$, il faut se « taper » l'algorithme d'Euclide, noir de calculs enchevêtrés, semé d'embûches menaçantes, et parsemé d'erreurs potentielles innombrables.

On trouve :

$$\begin{aligned}
\underbrace{x^5 - 2x^4 + x^2 - x - 2}_{r_0} &= (x^2 - x)\,(\underbrace{x^3 - x^2 - x - 2}_{r_1}) + 2x^2 - 3x - 2,\\
\underbrace{x^3 - x^2 - x - 2}_{r_1} &= (\tfrac{1}{2}x + \tfrac{1}{4})\,(\underbrace{2x^2 - 3x - 2}_{r_2}) + \underbrace{\boxed{\tfrac{3}{4}x - \tfrac{3}{2}}}_{r_3},\\
\underbrace{2x^2 - 3x - 2}_{r_2} &= (\tfrac{8}{3}x + \tfrac{4}{3})\,(\tfrac{3}{4}x - \tfrac{3}{2}) + \mathbf{0}.
\end{aligned}$$

D'après la Proposition 9.2, le pgcd est le dernier reste non nul, divisé par le coefficient de son monôme de tête, égal à $\frac{3}{4}$, donc — *as simple as this !* — :

$$\mathsf{pgcd}\,(a,b) = x - 2.$$

Exemple 10.2. Toujours sur $\mathbb{Q}$, proposons-nous de trouver une identité de Bézout $u\,a + v\,b = \mathsf{pgcd}\,(a,b)$ pour :

$$a := x^5 + 3x^4 + 2x^3 - x^2 - 3x - 2, \qquad b := x^4 + 2x^3 + 2x^2 + 7x + 6.$$

Tout d'abord, on effectue patiemment — et sans erreurs, Monsieur le professeur ! — l'algorithme d'Euclide :

$$\begin{aligned}
x^5 + 3x^4 + 2x^3 - x^2 - 3x - 2 &= (x+1)\,(x^4 + 2x^3 + 2x^2 + 7x + 6) - 2x^3 - 10x^2 - 16x - 8,\\
x^4 + 2x^3 + 2x^2 + 7x + 6 &= (-\tfrac{1}{2}x + \tfrac{3}{2})\,(-2x^3 - 10x^2 - 16x - 8) + \boxed{9x^2 + 27x + 18},\\
-2x^3 - 10x^2 - 16x - 8 &= (-\tfrac{2}{9}x - \tfrac{4}{9})\,(9x^2 + 27x + 18) + \mathbf{0},
\end{aligned}$$

d'où :

$$\begin{aligned}
\mathsf{pgcd}\,(a,b) &= \tfrac{1}{9}\,(9x^2 + 27x + 18)\\
&= x^2 + 3x + 2.
\end{aligned}$$

Mais ce n'est pas tout ! Il y a encore des efforts à faire ! En remontant vers le haut, repartons du dernier terme de la deuxième ligne :

$$\begin{aligned}
9\,\mathsf{pgcd}\,(a,b) &= 9x^2 + 27x + 18\\
&= x^4 + 2x^3 + 2x^2 + 7x + 6 - (-\tfrac{1}{2}x + \tfrac{3}{2})\,(\underline{-2x^3 - 10x^2 - 16x - 8}_{\text{rpl}})\\
&= b + (\tfrac{1}{2}x - \tfrac{3}{2})\Big[a - (x+1)\,b\Big]\\
&= (\tfrac{1}{2}x - \tfrac{3}{2})\,a + \Big[1 - \tfrac{1}{2}x^2 - \tfrac{1}{2}x + \tfrac{3}{2}x + \tfrac{3}{2}\Big]\,b,
\end{aligned}$$

d'où :

$$\mathsf{pgcd}\,(a,b) \;=\; \big(\underbrace{\tfrac{1}{18}-\tfrac{1}{6}\,x}_{=:\,u}\big)\,a+\big(\underbrace{\tfrac{5}{18}+\tfrac{1}{9}\,x-\tfrac{1}{18}\,x^2}_{=:\,v}\big)\,b.$$

11. Polynômes irréductibles dans $\mathbb{K}[x]$

Dans cette section terminale, nous développons la théorie des polynômes irréductibles sur un corps commutatif $\mathbb{K}$. Rappelons qu'après division par le coefficient de son monôme de plus haut degré, tout polynôme appartient à l'ensemble, noté $\mathbb{K}[x]_1$, des polynômes *normalisés*, c'est-à-dire dont coefficient de tête égal à 1. Il est facile de vérifier que $\mathbb{K}[x]_1$ est un sous-groupe multiplicatif de $\mathbb{K}[x]$.

Définition 11.1. Dans $\mathbb{K}[x]_1$, on appelle *polynôme irréductible* tout polynôme $p \in \mathbb{K}[x]_1$ de degré $\deg p \geqslant 1$ qui n'est divisible que par 1 et par lui-même :

$$\Big(\; d \in \mathbb{K}[x]_1 \quad \text{et} \quad d \mid p \;\Big) \qquad \Longrightarrow \qquad \Big(\; d = 1 \quad \text{ou} \quad d = p \;\Big).$$

Certains auteurs les appellent *polynômes premiers*, car il y a une analogie profonde avec les *nombres* entiers premiers, mais en hommage à nos ancêtres gaulois, nous choisissons résolument de les appeler « *irréductibles* ».

Il est clair que le polynôme linéaire $x - \alpha$ est irréductible pour tout $\alpha \in \mathbb{K}$. Mais faisons remarquer que la notion d'irréductibilité dépend du corps sur lequel on se situe. En effet, $x^2 + 1$ est irréductible sur $\mathbb{R}$ (exercice), mais ne l'est pas sur $\mathbb{C}$, puisque $x^2 + 1 = (x - i)(x + i)$.

Proposition 11.2. *Deux polynômes irréductibles $p \neq p' \in \mathbb{K}[x]_1$* distincts *sont toujours premiers entre eux $p \wedge p' = 1$.*

Autrement dit, leur pgcd est égal à 1.

Démonstration. Notons donc $d := \mathsf{pgcd}\,(p, p')$. On a $d \mid p$ et $d \mid p'$, et comme les seuls diviseurs d'un polynôme irréductible sont 1 et lui-même, il vient :

$$\Big(\; d = 1 \quad \text{ou} \quad d = p \;\Big) \qquad \text{et} \qquad \Big(\; d = 1 \quad \text{ou} \quad d = p \;\Big).$$

La seule possibilité commune — c'est-à-dire satisfaisant ce « et » — est $d = 1$. □

Ensuite, nous pouvons obtenir l'énoncé suivant, dans lequel le symbole $\nmid$ signifie, comme nous le savons, « *ne divise pas* ».

Proposition 11.3. *Soit un polynôme irréductible $p \in \mathbb{K}[x]_1$. Alors, pour tout polynôme quelconque $a \in \mathbb{K}[x]$, on a équivalence entre :*

(i) *p et a sont premiers entre eux ;*

(ii) *$p \nmid a$.* □

Démonstration. L'implication **(i)** $\Longrightarrow$ **(ii)** est évidente, car en partant de $1 = p \wedge a$, si on avait non **(ii)**, c'est-à-dire si p divisait a, alors $\mathsf{pgcd}\,(p, a) = p$ serait de degré $\deg p \geqslant 1$, donc ne pourrait être égal à la constante 1, qui est de degré 0.

Montrons maintenant **(ii)** $\Longrightarrow$ **(i)**. Soit $d := \mathsf{pgcd}\,(p, a)$, d'où $d \mid p$, donc $d = 1$ ou $d = p$ car p est irréductible. Mais $d = p$ est impossible, car $d \mid a$ et $p \nmid a$ par l'hypothèse **(ii)**. Donc $d = 1 = p \wedge a$, c'est-à-dire que p et a sont premiers entre eux. □

On en déduit un troisième énoncé, important.

Théorème 11.4. [Euclide dans $\mathbb{K}[x]$] *Soit un polynôme irréductible $p \in \mathbb{K}[x]_1$. Alors pour tous polynômes $a, b \in \mathbb{K}[x]$, on a :*

$$p \,\big|\, a\,b \qquad \Longrightarrow \qquad \Big(p \mid a \quad \textit{ou} \quad p \mid b \Big).$$

Si de plus a et b sont irréductibles, alors $p = a$ ou $p = b$.

Démonstration. Soient $a, b \in \mathbb{K}[x]$ avec $p \,|\, a\,b$. Si $p \,|\, a$, il n'y a rien à faire — super !

Si $p \nmid a$, alors la Proposition 11.3 précédente montre que a et p sont premiers entre eux. Mais alors le Théorème 8.1 de Gauss garantit que $p \,|\, b$, ce qui était annoncé.

Quand a et b sont irréductibles, par définition, leurs seuls diviseurs sont 1, a et 1, b. On vient d'obtenir $p \,|\, a$ ou $p \,|\, b$. Si c'est $p \,|\, a$, alors $p = a$. Si c'est $p \,|\, b$, alors $p = b$. □

La généralisation suivante du Théorème 11.4 d'Euclide va s'avérer d'une grande utilité sur le plan technique dans ce qui va suivre.

Proposition 11.5. *Soit un polynôme irréductible $p \in \mathbb{K}[x]_1$. Alors pour tous polynômes $a, b, c, \ldots, \ell \in \mathbb{K}[x]$, on a :*

$$p \,\big|\, a\,b\,c\cdots\ell \qquad \Longrightarrow \qquad \Big(p \mid a \quad \textit{ou} \quad p \mid b \quad \textit{ou} \quad p \mid c \quad \textit{ou} \quad \cdots \quad \textit{ou} \quad p \mid \ell \Big).$$

Si de plus tous les facteurs $a, b, \ldots, \ell$ sont irréductibles, alors $p = a$, ou $p = b$, …, ou $p = \ell$.

Démonstration. Il suffit de raisonner par récurrence sur le nombre de facteurs en appliquant successivement le Théorème 11.4 précédent. □

Terminologie 11.6. Étant donné un polynôme q de degré $\deg q \geqslant 2$, on appelle *diviseur strict* de q tout polynôme $e \,|\, q$ qui divise q est qui est de degré :

$$1 \;\leqslant\; \deg e \;\leqslant\; \deg q - 1.$$

Alors on peut écrire $q = e\,f$ avec $f \in \mathbb{K}[x]$, et on observe que l'on a aussi :

$$1 \;\leqslant\; \deg f \;\leqslant\; \deg q - 1,$$

tout simplement parce que $\deg q = \deg e + \deg f$.

Nous pouvons dorénavant énoncer et démontrer le résultat principal de ce chapitre.

Théorème 11.7. *Tout polynôme $q \in \mathbb{K}[x]$ de degré $\deg q \geqslant 1$ se décompose comme produit d'un nombre fini $r \geqslant 1$ de puissances de nombres premiers :*

$$q \;=\; \alpha\, p_1^{i_1} \cdots p_r^{i_r},$$

où $\alpha \neq 0$ est le coefficient du monôme de plus haut degré de q, avec $p_1, \ldots, p_r \in \mathbb{K}[x]_1$ irréductibles, et avec des exposants entiers $i_1 \geqslant 1$, …, $i_r \geqslant 1$.

De plus, la décomposition est unique*, à l'ordre des facteurs près.*

Naturellement, le « polynôme » constant α n'est pas un polynôme irréductible, car il est de degré 0.

Démonstration. Existence. Travaillons plutôt avec $\frac{1}{\alpha}\,q$, qui appartient à $\mathbb{K}[x]_1$. Si ce polynôme est déjà irréductible, il n'y a rien à faire — après-midi libre !

Sinon, il existe alors deux polynômes unitaires p_1 et p_2 avec $\deg p_1 \geqslant 1$ et $\deg p_2 \geqslant 1$ en lesquels notre polynôme se morcelle :

$$\tfrac{1}{\alpha}\,q \;=\; p_1\,p_2.$$

Si p_1 et p_2 sont premiers, c'est terminé. Sinon, on réitère sur p_1 et sur p_2 ce que l'on vient de faire sur $\frac{1}{\alpha}\,q$.

Le nombre de ces opérations est fini, car il est majoré par $\deg p$, puisque le degré des nouveaux facteurs qui apparaissent à chaque étape baisse d'au moins une unité. On aboutit donc à une décomposition :

$$\tfrac{1}{\alpha}\,q \;=\; p_1\,p_2\,\cdots\,p_h,$$

avec des polynômes irréductibles $p_1,\dots,p_h \in \mathbb{K}[x]_1$ tous de degrés $\geqslant 1$. L'existence est établie !

Unicité. Supposons que l'on ait obtenu deux décompositions :

$$p_1\,p_2\,\cdots\,p_h \;=\; \tfrac{1}{\alpha}\,q \;=\; p'_1\,p'_2\,\cdots\,p'_{h'},$$

et cherchons à prouver que ces deux décompositions sont identiques, à l'ordre près des facteurs irréductibles.

Tout d'abord, en partant de l'égalité :

$$p_1\,p_2\,\cdots\,p_h \;=\; p'_1\,p'_2\,\cdots\,p'_{h'},$$

p_1 divise le premier produit, donc divise le second. Par conséquent, grâce à la Proposition 11.5, il est nécessaire que p_1 soit égal à l'un des facteurs $p'_{i'}$ à droite. En changeant au besoin la numérotation des facteurs du second produit, on a $p_1 = p'_1$.

Mais puisque $\mathbb{K}[x]_1$ est intègre, on peut simplifier par p_1, et obtenir :

$$p_2\,p_3\,\cdots\,p_h \;=\; p'_2\,p'_3\,\cdots\,p'_{h'}.$$

En réitérant ce procédé, on pourra identifier ainsi les h facteurs du premier produit avec autant de facteurs du second. On en déduit que $h \leqslant h'$.

Mais comme les deux décompositions jouent le maisme [5] rôle, en partant inversement du second produit, on identifierait les facteurs de ce produit avec autant de facteurs du premier produit, et on en déduirait de manière parfaitement symétrique que $h \geqslant h'$.

Par conséquent, $h = h'$, ce qui achève l'argumentation d'unicité.

Regroupements. Dans la décomposition obtenue pour $\frac{1}{\alpha}\,q$, il se peut que certains polynômes irréductibles soient égaux. On obtient donc bien une décomposition de la forme annoncée :

$$\tfrac{1}{\alpha}\,q \;=\; p_1^{i_1}\cdots p_r^{i_r}\,, \qquad \square$$

12. Exercices

Exercice 1. EE

Exercice 2. EE

5. — coquille typographique espiègle —

Racines

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Introduction

2. Dérivée d'un polynôme

Commençons par exhiber un exemple « embêtant ». Sur le corps $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, où $p \geqslant 2$ est un nombre premier quelconque, considérons le polynôme :

$$p := x^p + x.$$

Implicitement, les coefficients $1 = \overline{1}$ sont entendus modulo p.

Si on dérive d'une manière naturelle ce polynôme en appliquant les définitions connues, on obtient un polynôme :

$$\begin{aligned} p' &= p\,x^{p-1} + 1 \\ &= 1, \end{aligned}$$

dont le degré n'est *pas* égal à $\deg p - 1$, et même, est de degré beaucoup plus petit, égal à 0 !

Cet exemple « embêtant » ne pourra pas être approfondi en L2. Nous déciderons donc souvent de faire une hypothèse naturelle sur notre corps $\mathbb{K}$ qui va nous éviter d'avoir à tenir compte de phénonènes inhabituels, et nous garantir qu'on a bien $\deg p' = \deg p - 1$ pour tout polynôme $p \in \mathbb{K}[x]$.

Nous travaillons donc dorénavant sur un corps $\mathbb{K}$, qui, dans la pratique, sera $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, rien d'autre qui soit trop exotique. Nous ferons de plus souvent l'hypothèse suivante.

Hypothèse 2.1. L'anneau commutatif A ou le corps commutatif $\mathbb{K}$ seront souvent supposés *de caractéristique nulle*, c'est-à-dire tels que :

$$n \cdot 1_A \neq 0_A, \qquad\qquad n \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}},$$

pour tout entier $n \in \mathbb{Z}\backslash\{0\}$.

Plus précisément, de nombreux énoncés élémentaires qui sont vrais sans cette hypothèse seront développés pour un corps commutatif quelconque, et même, sur un anneau commutatif quelconque. Quand une hypothèse de caractéristique zéro sera « nécessaire » à un énoncé, nous la préciserons expressément. En fait, la caractéristique zéro sera toujours supposée lorsque nous manipulerons des *dérivées* de polynôomes.

Mais en tout cas, au niveau L2, il s'agira surtout de maîtriser les calculs sur les corps standard $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, et parfois, de travailler un peu sur $\mathbb{Z}/p\mathbb{Z}$, pas au-delà.

Soit donc un anneau commutatif quelconque A, sans hypothèse de caractéristique. Soit un polynôme de $A[x]$:

$$p \,:=\, a_0 + a_1\, x + x_2\, x^2 + \cdots + a_n\, x^n.$$

Si nous donnons à l'indéterminée x une *valeur* $\alpha \in A$ de l'anneau de base A, en remplaçant $x := \alpha$ dans p, on obtient alors un élément bien déterminé :

$$p(\alpha) \,:=\, a_0 + a_1\, \alpha + a_2\, \alpha^2 + \cdots + a_n\, \alpha^n.$$

de l'anneau A.

Définition 2.2. L'application :

$$\begin{array}{rccc} p\colon & A & \longrightarrow & A \\ & \alpha & \longmapsto & p(\alpha), \end{array}$$

est appelée *fonction polynomiale* associée au polynôme $p \in A[x]$.

En Analyse Réelle, on définit la dérivée $p'(x)$ d'une fonction polynomiale $p(x) = a_0 + a_1\, x + \cdots + a_n\, x^n$ à coefficients $a_0, a_1, \ldots, a_n \in \mathbb{R}$ en un point $\alpha \in \mathbb{R}$ comme étant la limite :

$$p'(\alpha) \,:=\, \lim_{h \to 0} \frac{p(\alpha + h) - p(\alpha)}{h},$$

et on vérifie aisément que :

$$p'(\alpha) \,=\, a_1 + 2\, a_2\, \alpha + \cdots + n\, a_n\, \alpha^{n-1}.$$

Inspirés par cela, nous pouvons introduire une définition purement formelle de la notion de dérivée d'un polynôme à coefficients dans un anneau A complètement arbitraire, sans utiliser la notion de limite, sans Topologie, sans Analyse, sans Géométrie.

Définition 2.3. On appelle *polynôme dérivé* d'un polynôme de $A[x]$:

$$p \,:=\, a_0 + a_1\, x + a_2\, x^2 + \cdots + a_n\, x^n,$$

le polynôme noté :

$$p' \,:=\, a_1 + 2\, a_2\, x + \cdots + n\, a_n\, x^{n-1}.$$

En particulier, si le polynôme $p = a_0$ est une constante, le polynôme dérivé $p' = 0$ est le polynôme nul 0.

Dans les autres cas, on a $a_n \neq 0$ avec $n \geqslant 1$, d'où lorsque A est intègre et de caractéristique zéro :

$$\deg p' \,=\, \deg p - 1,$$

puisque $n\, a_n \neq 0$. Mais quand A est de caractéristique strictement positive, on a seulement une inégalité :

$$\deg p' \,\leqslant\, \deg p - 1,$$

puisqu'il est possible que $n\, a_n = 0$ lorsque n est un multiple de la caractéristique.

On peut alors noter en abrégé :

$$p \,=\, \sum_{k=0}^{n} a_k\, x^k \qquad\qquad \Longrightarrow \qquad\qquad p' \,=\, \sum_{k=1}^{n} k\, a_k\, x^{k-1}.$$

Proposition 2.4. *Quels que soient les polynômes p et q dans $A[x]$, on a :*

$$\big(p + q\big)' \,=\, p' + q'.$$

Démonstration. Si l'un des deux polynômes est une constante, c'est évident. Sinon, soient :

$$p \,=\, \sum_{k=0}^{n} a_k\, x^k \qquad\qquad \text{et} \qquad\qquad q \,=\, \sum_{k=0}^{m} b_k\, x^k.$$

Par symétrie, on peut supposer $n \geqslant m$. Alors en ajoutant au polynôme q des coefficients $b_k := 0$ tous nuls pour $m < k \leqslant n$, il vient :

$$p + q \,=\, \sum_{k=0}^{n} \big(a_k + b_k\big)\, x^k.$$

Pour les polynômes dérivées, on a par définition :

$$\begin{aligned} p' \,&=\, \sum_{k=1}^{n} k\, a_k\, x^{k-1}, \\ q' \,&=\, \sum_{k=1}^{n} k\, b_k\, x^{k-1}, \\ \big(p+q\big)' \,&=\, \sum_{k=1}^{n} k\, \big(a_k + b_k\big)\, x^{k-1}, \end{aligned}$$

et donc par conséquent, on a bien :

$$\big(p+q\big)' \,=\, p' + q'. \qquad \square$$

Si on introduit l'*application de dérivation :*

$$\begin{aligned} A[x] \;&\longrightarrow\; A[x] \\ p \;&\longmapsto\; p', \end{aligned}$$

cette propriété montre que la dérivation est un endomorphisme du groupe $\big(A[x], +\big)$.

Proposition 2.5. *Quel que soit $\lambda \in A$ et quel que soit $p \in A[x]$, on a :*

$$\big(\lambda\, p\big)' \,=\, \lambda\, p'.$$

Démonstration. En effet :

$$\left(\sum_{k=0}^{n} \lambda\, a_k\, x^k\right)' \,=\, \sum_{k=1}^{n} k\, \lambda\, a_k\, x^{k-1} \,=\, \lambda \left(\sum_{k=0}^{n} a_k\, x^k\right)'. \qquad \square$$

Ces deux propositions montrent alors que la dérivation est un *endomorphisme du A-module $A[x]$*.

Proposition 2.6. *Quels que soient les polynômes $p, q \in A[x]$, on a :*

$$\big(p\, q\big)' \,=\, p'\, q + p\, q'.$$

Démonstration. Vérifions tout d'abord que cette propriété est vraie pour deux monômes quelconques :

$$x^h \qquad\qquad \text{et} \qquad\qquad x^k,$$

de degrés $h \geqslant 0$ et $k \geqslant 0$. Leurs dérivées respectives sont :

$$\big(x^h\big)' \,=\, h\, x^{h-1} \qquad\qquad \text{et} \qquad\qquad \big(x^k\big)' \,=\, k\, x^{k-1},$$

où on observe que pour $h = 0$, on obtient $0\, x^{h-1} = 0$, et de même lorsque $k = 0$.

De plus :

$$x^h\,x^k \;=\; x^{h+k} \qquad\qquad \Longrightarrow \qquad\qquad \big(x^h\,x^k\big)' \;=\; (h+k)\,x^{h+k-1},$$

et donc la propriété est vraie pour les paires de monômes :

$$\big(x^h\,x^k\big)' \;=\; \big(h+k\big)\,x^{h+k-1} \;=\; h\,x^{h-1}\,x^k + x^h\,k\,x^{k-1} \;=\; \big(x^h\big)'\,x^k + x^h\,\big(x^k\big)'.$$

Ensuite, soient deux polynômes quelconques :

$$p \;=\; \sum_{h=0}^{n} a_h\,x^h \qquad\qquad \text{et} \qquad\qquad q \;=\; \sum_{k=0}^{m} b_k\,x^k,$$

dont le produit est :

$$p\,q \;=\; \sum_h \sum_k a_h\,b_k\,x^h\,x^k.$$

Puisque la dérivation est un endomorphisme linéaire de $A[x]$, nous concluons que :

$$\begin{aligned}\big(p\,q\big)' \;&=\; \sum_h \sum_k a_h\,b_k\,\big(x^h\,x^k\big)' \\ &=\; \sum_h a_h\,\big(x^h\big)' \sum_k b_k\,x^k + \sum_h a_h\,x^h \sum_k b_k\,\big(x^k\big)' \\ &=\; p'\,q + p\,q'.\end{aligned}$$

□

3. Dérivées successives

Maintenant, itérons l'opération de dérivation.

Définition 3.1. Pour un entier $\ell \geqslant 1$ quelconque, la dérivée $p^{(\ell)}$ d'ordre ℓ d'un polynôme $p \in A[x]$ est définie par récurrence comme :

$$p^{(\ell)} \;:=\; \big(p^{(\ell-1)}\big)', \quad p^{(\ell-1)} \;:=\; \big(p^{(\ell-2)}\big)', \quad \ldots\ldots, \quad p^{(2)} \;:=\; \big(p'\big)', \quad p^{(1)} \;:=\; \big(p\big)'.$$

Souvent, on écrit les trois premières dérivées :

$$p''', \qquad\qquad p'', \qquad\qquad p'.$$

Par convention, on pose :

$$p^{(0)} \;:=\; 0.$$

Commençons par expliciter la dérivée d'ordre $\ell \geqslant 0$ quelconque d'un monôme x^k.

Proposition 3.2. *Pour deux entiers $k, \ell \geqslant 0$, on a :*

$$\big(x^k\big)^{(\ell)} \;=\; \begin{cases} k(k-1)\cdots(k-\ell+1)\,x^{k-\ell} & \textit{lorsque } \ell \leqslant k, \\ 0 & \textit{lorsque } \ell \geqslant k+1. \end{cases}$$

Dans le premier cas, on peut aussi écrire :

$$\big(x^k\big)^{(\ell)} \;=\; \frac{k!}{(k-\ell)!}\,x^{k-\ell}.$$

Démonstration. Pour $\ell = 0$, la formule est vraie, par convention.

Par récurrence, supposons que la formule est vraie au niveau ℓ. Deux cas sont à considérer.

Si $\ell + 1 \leqslant k$, alors comme $\left(x^{k-\ell}\right)' = (k-\ell)\, x^{k-\ell-1}$, on a bien :

$$\begin{aligned}\left(x^k\right)^{(\ell+1)} &= \Big(k(k-1)\cdots(k-\ell+1)\, x^{k-\ell}\Big)' \\ &= k(k-1)\cdots(k-\ell+1)(k-\ell)\, x^{k-\ell-1},\end{aligned}$$

ce qui établit la formule au niveau $\ell + 1$.

Si $\ell + 1 \geqslant k + 1$, c'est-à-dire si $\ell \geqslant k$, la formule au niveau ℓ est ou bien la constante $k!\, x^0$ lorsque $\ell = k$, ou bien la constante 0 lorsque $\ell \geqslant k + 1$. Quand on dérive une fois de plus, dans ces deux sous-cas, on obtient 0. Donc la formule au niveau $\ell + 1$ est établie dans ce deuxième cas aussi. □

Ensuite, proposons-nous de déterminer la dérivée d'ordre $\ell \geqslant 0$ quelconque d'un polynôme arbitraire :

$$p \,=\, \sum_{k=0}^{n} a_k\, x^k.$$

En dérivant terme à terme et en appliquant ce qui précède à chaque monôme, on obtient immédiatement :

$$\begin{aligned}&\ell \leqslant n \qquad \Longrightarrow \qquad p^{(\ell)} \,=\, \sum_{k=\ell}^{n} a_k\, k\cdots(k-\ell+1)\, x^{k-\ell}, \\ &\ell > n \qquad \Longrightarrow \qquad p^{(\ell)} \,=\, 0.\end{aligned} \tag{3.3}$$

4. Formules de Mac-Laurin et de Taylor

Travaillons dorénavant sur un corps commutatif $\mathbb{K}$, au lieu d'un anneau commutatif A quelconque.

Rappelons que le concept de *caractéristique* d'un anneau commutatif intègre A, en particulier d'un corps commutatif $\mathbb{K}$, a été défini dans le chapitre consacré aux anneaux abstraits, et que cette *caractéristique* est ou bien égale à un nombre premier $p \geqslant 2$, ou bien égale à zéro.

Dans cette Section **4**, nous supposerons que la caractéristique de $\mathbb{K}$ est égale à zéro, ce qui garantit, pour tout entier $m \in \mathbb{Z}\backslash\{0\}$, la non-annulation :

$$0_{\mathbb{K}} \,\neq\, m \cdot 1_{\mathbb{K}}.$$

Nous avons vu alors que le corps $\mathbb{Q}$ des nombres rationnels *s'injecte* dans $\mathbb{K}$, à savoir que tous les quotients $\frac{p\cdot 1_{\mathbb{K}}}{q\cdot 1_{\mathbb{K}}}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}_{\geqslant 1}$ premiers entre eux sont des éléments de $\mathbb{K}$, *mutuellement distincts* $\frac{p\cdot 1_{\mathbb{K}}}{q\cdot 1_{\mathbb{K}}} \neq \frac{p'\cdot 1_{\mathbb{K}}}{q'\cdot 1_{\mathbb{K}}}$ lorsque $(p, q) \neq (p', q')$, toujours avec des couples premiers entre eux.

Considérons maintenant les éléments de $\mathbb{K}[x]$ comme des fonctions polynomiales de $\mathbb{K}$ dans $\mathbb{K}$, l'indéterminée x prenant des valeurs dans l'anneau $\mathbb{K}$.

Si on donne à x la valeur 0 dans la relation (3.3) qui précède, on obtient, pour tout $0 \leqslant \ell \leqslant n$:

$$p^{(\ell)}(0) \,=\, a_\ell\, \ell!,$$

d'où l'on tire puisque $\ell! = \ell! \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ est non nul dans $\mathbb{K}$ donc inversible dans $\mathbb{K}$:

$$p(x) \;=\; \sum_{\ell=0}^{n} \frac{p^{(\ell)}(0)}{\ell!}\, x^{\ell},$$

c'est-à-dire :

$$p(x) \;=\; p(0) + \frac{p'(0)}{1!}\, x^1 + \frac{p''(0)}{2!}\, x^2 + \cdots + \frac{p^{(n)}(0)}{n!}\, x^n.$$

C'est la *formule de Mac-Laurin* pour les polynômes.

Ensuite, soit toujours un polynôme arbitraire à une variable x :

$$\begin{aligned} p(x) \;&=\; a_0 + a_1\, x + a_2\, x^2 + \cdots + a_n\, x^n \\ &=\; \sum_{k=0}^{n} a_k\, x^k. \end{aligned}$$

En remplaçant x par $x + y$, on obtient un polynôme à deux variables x et y :

$$p(x+y) \;=\; \sum_{k=0}^{n} a_k \big(x+y\big)^k. \tag{4.1}$$

Pour chaque rang k avec $0 \leqslant k \leqslant n$, appliquons la formule du binôme de Newton :

$$\big(x+y\big)^k \;=\; x^k + \frac{k}{1!}\, x^{k-1}\, y + \frac{k(k-1)}{2!}\, x^{k-2}\, y^2 + \cdots + \frac{k(k-1)\cdots 2\cdot 1}{k!}\, x^0\, y^k.$$

On peut alors écrire, en reconnaissant les dérivées successives de x^k :

$$\big(x+y\big)^k \;=\; x^k + \frac{(x^k)'}{1!}\, y + \frac{(x^k)''}{2!}\, y^2 + \cdots + \frac{(x^k)^{(k)}}{k!}\, y^k.$$

Or les dérivées de x^k d'ordre $> k$ sont nulles. On peut donc rajouter au second membre de la relation précédente le polynôme nul suivant :

$$\frac{(x^k)^{(k+1)}}{(k+1)!}\, y^{k+1} + \cdots + \frac{(x^k)^{(n)}}{n!}\, y^n \;\equiv\; 0.$$

On obtient alors, pour $0 \leqslant k \leqslant n$:

$$\big(x+y\big)^k \;=\; \sum_{\ell=0}^{n} \frac{(x^k)^{(\ell)}}{\ell!}\, y^{\ell}.$$

En reportant alors ceci dans la relation (4.1), il vient :

$$\begin{aligned} p(x+y) \;&=\; \sum_{k=0}^{n} a_k \sum_{\ell=0}^{n} \frac{(x^k)^{(\ell)}}{\ell!}\, y^{\ell} \\ &=\; \sum_{\ell=0}^{n} \frac{y^{\ell}}{\ell!} \left(\sum_{k=0}^{n} \big(a_k\, x^k\big)^{(\ell)} \right), \end{aligned}$$

la dernière égalité étant justifiée par l'associativité, la commutativité, et la distributivité dans l'anneau A.

Or par définition de la dérivation d'ordre ℓ, on a :

$$\sum_{k=0}^{n} \left(a_k\, x^k\right)^{(\ell)} \;=\; p^{(\ell)}(x),$$

donc on obtient :

$$p(x+y) \;=\; \sum_{\ell=0}^{n} p^{(\ell)}(x)\, \frac{y^\ell}{\ell!},$$

c'est-à-dire sous forme développée :

$$p(x+y) \;=\; p(x) + \frac{p'(x)}{1!}\, y + \frac{p''(x)}{2!}\, y^2 + \cdots + \frac{p^{(n)}(x)}{n!}\, y^n.$$

C'est la *formule de Taylor* pour les polynômes.

Au point $x := 0$, on retrouve la formule de Mac-Laurin.

En remplaçant x par a et $x+y$ par z, on voit que la formule de Taylor s'écrit aussi sous la forme suivante :

$$p(z) \;=\; p(a) + \frac{p'(a)}{1!}\, (z-a) + \frac{p''(a)}{2!}\, (z-a)^2 + \cdots + \frac{p^{(n)}(a)}{n!}\, (z-a)^n.$$

5. Zéros d'un polynôme

Considérons donc maintenant des polynômes de l'anneau $\mathbb{K}[x]$ des polynômes à une indéterminée x et à coefficients dans $\mathbb{K}$.

Définition 5.1. Un élément $a \in \mathbb{K}$ est appelé une *racine* d'un polynôme $p(x) \in \mathbb{K}[x]$ s'il vérifie :

$$0 \;=\; p(a).$$

On dit aussi que a est une *racine* de $p(x)$.

Théorème 5.2. *Pour qu'un élément $a \in \mathbb{K}$ soit une racine de $p(x) \in \mathbb{K}[x]$, il faut et il suffit que $p(x)$ soit divisible par $x-a$, c'est-à-dire qu'il existe un polynôme $q \in \mathbb{K}[x]$ avec $\deg q = \deg p - 1$ tel que :*

$$p(x) \;=\; (x-a)\, q(x).$$

Démonstration. Effectuons une division euclidienne de $p(x)$ par $x-a$:

$$\begin{aligned} p(x) \;&=\; (x-a)\, q(x) + r(x), \\ \deg r(x) \;&\leqslant\; \deg (x-a) \;=\; 1. \end{aligned}$$

La seconde relation prouve que $r(x) =: r \in \mathbb{K}$ est une constante.

Pour calculer cette constante, donnons à x la valeur a dans la première relation, ce qui offre :

$$p(a) \;=\; r,$$

donc par conséquent :

$$p(x) \;=\; (x-a)\, q(x) + p(a).$$

Ainsi, le reste de la division euclidienne de $p(x)$ par $x-a$ est le scalaire $p(a) \in \mathbb{K}$.

Grâce à un théorème vu dans le chapitre précédent, il en résulte que, pour que $p(x)$ soit divisible par $x-a$, il faut et il suffit que $p(a) = 0$, c'est-à-dire que a soit un zéro de $p(x)$. Le théorème est donc démontré, sans transpirer. □

En petits degrés, examinons les liens entre les propriétés d'irréductibilité des polynômes, et la nature de leurs racines.

Nous savons qu'un polynôme de degré 1 :

$$p \,=\, a_1\, x + a_0 \,=\, a_1 \left(x - a_0\, a_1^{-1}\right) \qquad (a_1 \neq 0),$$

est toujours irréductible, car $p = q\, r$ avec :

$$1 \leqslant \deg q, \quad 1 \leqslant \deg r, \qquad \text{mais} \qquad 1 \,=\, \deg p \,=\, \deg q + \deg r,$$

est impossible.

Par ailleurs, $p = a_1\, x + a_0$ a l'unique racine évidente $-\, a_0 a_1^{-1}$.

En degré 2, la réductibilité $p = q\, r$ avec $\deg p = 2$ force :

$$2 \,=\, \deg p \,=\, \deg q + \deg r \,=\, 1 + 1.$$

Théorème 5.3. *Un polynôme de degré* 2 *:*

$$p \,=\, a_2\, x^2 + a_1\, x + a_0 \qquad (a_2 \neq 0),$$

est irréductible si et seulement s'il n'a aucune racine dans $\mathbb{K}$*.*

Démonstration. Montrons plutôt la *contraposée* de cette équivalence :

$$\Big(\; p \,=\, q\, r \quad \text{réductible} \;\Big) \qquad \Longleftrightarrow \qquad \Big(\; \exists\, \alpha \,\in\, \mathbb{K}, \quad 0 \,=\, p(\alpha) \;\Big).$$

$\Longrightarrow$ Puisque $\deg q = 1$, on a $q = b_1\, x + x_0$ avec $b_1 \neq 0$, qui a la racine unique $-\, b_0 b_1^{-1}$ appartenant à $\mathbb{K}$. D'ailleurs, puisque $\deg r = 1$ aussi, on a $r = c_1\, x + c_0$ avec $c_1 \neq 0$ qui a aussi la racine unique $-\, c_0 c_1^{-1}$ appartenant à $\mathbb{K}$.

$\Longleftarrow$ Grâce au Théorème 5.2 vu à l'instant, on a :

$$p(x) \,=\, a_2\, (x - \alpha)\, r(x),$$

avec $r \in \mathbb{K}[x]$ de degré 1, ce qui montre que $p(x)$ est réductible. □

Au-delà d'un simple zéro, on peut faire état de l'*ordre de multiplicité* d'un zéro.

En effet, soit a un zéro d'un polynôme $p(x) \in \mathbb{K}[x]$. Autrement dit, $x - a$ divise $p(x)$, c'est-à-dire qu'il existe un polynôme $p_1(x)$ tel que :

$$p(x) \,=\, (x - a)\, p_1(x).$$

Si $p_1(a) \neq 0$, on dit que a est un *zéro simple* de $p(x)$.

Mais si $p_1(a) \,=\, 0$, alors $p_1(x)$ est lui-même divisible par $x - a$, donc il existe un polynôme $p_2(x)$ tel que :

$$p_1(x) \,=\, (x - a)\, p_2(x).$$

Ainsi :

$$\begin{aligned} p(x) \,&=\, (x - a)\, p_1(x) \\ &=\, (x - a)^2\, p_2(x). \end{aligned}$$

Si $p_2(a) \neq 0$, on dit que a est un *zéro double* (gras double) de $p(x)$.

D'une façon générale, s'il existe un entier naturel $h \geqslant 1$ tel que :

$$p(x) \,=\, (x - a)^h\, p_h(x),$$

avec un polynôme $p_h(x) \in \mathbb{K}[x]$ satisfaisant :

$$\begin{aligned} \deg p_h \,&=\, \deg p - h, \\ p_h(a) \,&\neq\, 0, \end{aligned}$$

alors on dit que a est un *zéro multiple d'ordre h de $p(x)$*, ou que a est un *zéro de multiplicité h de $p(x)$*.

Définition 5.4. On appelle *multiplicité* d'un zéro a d'un polynôme $p(x) \in \mathbb{K}[x]$ le nombre naturel $h \geqslant 1$ tel qu'il existe un polynôme $p_h(x)$ satisfaisant :

$$\begin{aligned} p(x) \;&=\; (x-a)^h\, p_h(x), \\ 0 \;&\neq\; p_h(a). \end{aligned}$$

On a alors la propriété suivante de factorisation.

Théorème 5.5. *Si $a_1, a_2, \ldots, a_r \in \mathbb{K}$ sont des zéros distincts d'un polynôme $p(x) \in \mathbb{K}[x]$ de multiplicités respectives $h_1, h_2, \ldots, h_r \geqslant 1$, alors il existe un polynôme $q(x) \in \mathbb{K}[x]$ avec :*

$$\deg p(x) \;=\; h_1 + h_2 + \cdots + h_r + \deg q(x),$$

tel que :

$$\begin{aligned} p(x) \;&=\; \big(x-a_1\big)^{h_1} \big(x-a_2\big)^{h_2} \cdots \big(x-a_r\big)^{h_r}\, q(x), \\ 0 \;&\neq\; q(a_1),\;\; 0 \;\neq\; q(a_2),\;\; \ldots,\;\; 0 \;\neq\; q(a_r). \end{aligned}$$

En particulier, si :

$$\deg p(x) \;=\; h_1 + h_2 + \cdots + h_r,$$

le polynôme $q(x) \in \mathbb{K}[x]$ est de degré 0, c'est-à-dire est une constante dans $\mathbb{K}$.

Démonstration. Raisonnons par récurrence sur le nombre $r \geqslant 1$ de zéros distincts envisagés.

L'énoncé est vrai pour $r = 1$, car il coïncide alors avec la Définition 5.4.

Supposons maintenant l'énoncé vrai avec $r-1$ racines distinctes $a_1, \ldots, a_{r-1}$, c'est-à-dire, supposons qu'il existe un polynôme $t(x)$ satisfaisant :

$$\begin{aligned} p(x) \;&=\; \big(x-a_1\big)^{h_1} \cdots \big(x-a_{r-1}\big)^{h_{r-1}}\, t(x), \\ 0 \;&\neq\; t(a_1),\;\; \cdots,\;\; 0 \;\neq\; t(a_{r-1}), \end{aligned}$$

et proposons-nous de montrer qu'il existe alors un polynôme $q(x)$ satisfaisant :

$$\begin{aligned} p(x) \;&=\; \big(x-a_1\big)^{h_1} \cdots \big(x-a_{r-1}\big)^{h_{r-1}} \big(x-a_r\big)^{h_r}\, q(x), \\ 0 \;&\neq\; q(a_1),\;\; \ldots,\;\; 0 \;\neq\; q(a_{r-1}),\;\; 0 \;\neq\; q(a_r). \end{aligned}$$

Or puisque a_r est une racine d'ordre h_r de $p(x)$, il existe un polynôme $p_r(x)$ tel que :

$$\begin{aligned} p(x) \;&=\; \big(x-a_r\big)^{h_r}\, p_r(x), \\ 0 \;&\neq\; p_r(a_r). \end{aligned}$$

Rappelons que dans le chapitre précédent, nous avons vérifié que pour deux constantes distinctes $a \neq a' \in \mathbb{K}$, les deux polynômes linéaires $x-a$ et $x-a'$ sont toujours premiers entre eux.

Ainsi, $x - a_r$ est premier avec $x - a_1$, …, $x - a_{r-1}$, puisque $a_r \neq a_1, \ldots, a_{r-1}$. Donc $\big(x-a_r\big)^{h_r}$ est premier avec $\big(x-a_1\big)^{h_1}$, …, $\big(x-a_{r-1}\big)^{h_{r-1}}$.

D'après le théorème de Gauss pour les polynômes vu dans le chapitre précédent, il vient :

$$\begin{aligned}\big(x-a_r\big)^{h_r} \mid p(x) \qquad &\Longleftrightarrow \qquad \big(x-a_r\big)^{h_r} \Big| \big(x-a_1\big)^{h_1} \cdots \big(x-a_{r-1}\big)^{h_{r-1}}\, t(x)\\ &\Longrightarrow \qquad \big(x-a_r\big)^{h_r} \mid t(x).\end{aligned}$$

Il existe donc un polynôme $q(x)$ tel que :

$$t(x) \;=\; \big(x-a_r\big)^{h_r}\, q(x).$$

En outre :

$$\begin{aligned}\Big(t(a_i) \;\neq\; 0 \;\neq\; a_i - a_r \quad \text{pour} \quad 1 \leqslant i \leqslant r-1\Big) \quad &\Longrightarrow\\ \Longrightarrow \quad \Big(q(a_i) \;\neq\; 0 \quad \text{pour} \quad 1 \leqslant i \leqslant r-1\Big)&.\end{aligned}$$

Après remplacement, il en résulte que :

$$p(x) \;=\; \big(x-a_1\big)^{h_1} \cdots \big(x-a_{r-1}\big)^{h_{r-1}} \big(x-a_r\big)^{h_r}\, q(x).$$

On vient de dire que $q(a_i) \neq 0$ pour $i = 1, \ldots, r-1$.

Enfin, par identification des deux représentations de $p(x)$ qui précèdent, on obtient une équation :

$$\big(x-a_r\big)^{h_r}\, p_r(x) \;=\; \big(x-a_1\big)^{h_1} \cdots \big(x-a_{r-1}\big)^{h_{r-1}} \big(x-a_r\big)^{h_r}\, q(x),$$

qui se simplifie en :

$$p_r(x) \;=\; \big(x-a_1\big)^{h_1} \cdots \big(x-a_{r-1}\big)^{h_{r-1}}\, q(x),$$

donc la propriété $0 \neq p_r(a_r)$ se transmet à $q(a_r) \neq 0$, ce qui conclut l'argumentation. □

Dans le cas général, on a toujours l'inégalité :

$$h_1 + h_2 + \cdots + h_r \;\leqslant\; \mathsf{deg}\, p(x),$$

d'où puisque tous les h_i sont $\geqslant 1$:

$$r \;\leqslant\; \mathsf{deg}\, p(x).$$

Comme corollaire du Théorème 5.5, nous avons démontré le

Théorème 5.6. *Tout polynôme $p(x) \in \mathbb{K}[x]$ à coefficients dans un corps commutatif $\mathbb{K}$ admet toujours au plus* $\mathsf{deg}\, p(x)$ *racines dans $\mathbb{K}$.*

Démonstration. Redémontrons ce résultat, d'une manière légèrement différente. Pour $n = 1$, un polynôme de degré 1 :

$$p \;=\; a_1\, x + a_0 \;=\; a_1\, \big(x - (-\, a_0\, a_1^{-1})\big),$$

a la racine évidente $\alpha := -\, a_0 a_1^{-1}$.

Par récurrence, supposons le résultat démontré pour tout polynôme q de degré $n \geqslant 1$. Soit p un polynôme de degré $n+1$.

Si p n'a pas de racine dans $\mathbb{K}$, il n'y a rien à faire, le résultat est vrai.

Si p a une racine $\alpha_1 \in \mathbb{K}$, alors le Théorème 5.2 a montré que $p = (x - \alpha_1)\, q$, avec un certain polynôme q de degré n.

Comme le corps $\mathbb{K}$ est intègre, pour tout $\alpha \in \mathbb{K}$, on a :

$$0 = p(\alpha) \quad \Longleftrightarrow \quad (\alpha - \alpha_1)\, q(\alpha_1) \quad \Longleftrightarrow \quad \Big(\alpha = \alpha_1 \quad \text{ou} \quad q(\alpha) = 0 \Big).$$

Puisque q a au plus n racines par hypothèse de récurrence, p a donc au plus $1 + n$ racines. La récurrence conclut. □

Ensuite, nous allons établir un lien fondamental entre les multiplicités des zéros $a \in \mathbb{K}$ d'un polynôme $p(x) \in \mathbb{K}[x]$, et celles de ses dérivés $p'(x)$, $p''(x)$, ...Ici, nous avons besoin d'une hypothèse sur la caractéristique de $\mathbb{K}$.

Théorème 5.7. *Sur un corps $\mathbb{K}$ de caractéristique nulle, si $a \in \mathbb{K}$ est un zéro d'ordre $h \geqslant 2$ d'un polynôme $p(x) \in \mathbb{K}[x]$, alors a est zéro d'ordre $h - 1$ de $p'(x)$.*

Démonstration. Supposons donc que :

$$p(x) = (x - a)^h\, q(x), \qquad \text{avec} \quad q(a) \neq 0.$$

Dérivons $p(x)$ une fois et factorisons :

$$\begin{aligned} p'(x) &= h\,(x - a)^{h-1}\, q(x) + (x - a)^h\, q'(x) \\ &= (x - a)^{h-1} \big[h\, q(x) + (x - a)\, q'(x) \big]. \end{aligned}$$

Pour $x := a$, le polynôme entre crochets vaut $h\, q(a) + 0$, ce qui est une valeur non nulle par l'Hypothèse 2.1, puisque $q(a) \neq 0$. Par conséquent, a est un zéro de multiplicité exactement égale à $h - 1$, ce qui termine la démonstration. □

Théorème 5.8. *Sur un corps $\mathbb{K}$ de caractéristique nulle, pour qu'un élément $a \in \mathbb{K}$ soit un zéro d'ordre $h \geqslant 1$ d'un polynôme $p(x) \in \mathbb{K}[x]$, il faut et il suffit que :*

$$\begin{aligned} &0 = p(a) = p'(a) = \cdots = p^{(h-1)}(a), \\ &0 \neq p^{(h)}(a). \end{aligned}$$

Démonstration. Supposons que a est un zéro d'ordre $h \geqslant 1$ de $p(x)$. Alors a est un zéro d'ordre $h - 1$ de $p'(x)$, grâce au théorème qui précède.

En appliquant ce même théorème à $p'(x)$, on voit que a est un zéro d'ordre $h - 2$ de $p''(x)$. De proche en proche, on aboutit à ce que a soit un zéro d'ordre 1 (simple !) de $p^{(h-1)}(x)$. Par conséquent, on a bien :

$$0 = p(a) = p'(a) = \cdots = p^{(h-1)}(a) \neq p^{(h)}(a).$$

Inversement, supposons que ces dernières relations sont vérifiées. En appliquant la formule de Taylor au polynôme $p(x)$, nous obtenons :

$$\begin{aligned} p(x) &= (x - a)^h\, \frac{p^{(h)}(a)}{h!} + (x - a)^{h+1}\, \frac{p^{(h+1)}(a)}{(h+1)!} + \cdots + (x - a)^n\, \frac{p^{(n)}(a)}{n!} \\ &= (x - a)^h \Big[\frac{p^{(h)}(a)}{h!} + (x - a)^1\, \frac{p^{(h+1)}(a)}{(h+1)!} + \cdots + (x - a)^{n-h}\, \frac{p^{(n)}(a)}{n!} \Big]. \end{aligned}$$

Le polynôme entre (grands) crochets vaut, pour $x := a$:

$$\frac{p^h(a)}{h!} \neq 0.$$

Par conséquent, a est un zéro d'ordre exactement égal à h de $p(x)$, ce qui conclut. □

6. Polynômes de $\mathbb{C}[x]$ et de $\mathbb{R}[x]$

Rappelons que les corps $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont trivialement de caractéristique nulle.

Nous étudions d'abord les polynômes de $\mathbb{C}[x]$, *i.e.* à coefficients dans le corps $\mathbb{C}$ des nombres complexes. En utilisant des outils d'Analyse plus avancés que ceux de ce cours d'Algèbre, on démontre un énoncé spectaculaire que nous admettrons.

Théorème 6.1. *Tout polynôme de $\mathbb{C}[x]$ de degré $n \geqslant 1$ admet au moins une racine dans $\mathbb{C}$.* □

Grâce à cet énoncé fondamental, nous pouvons déduire le

Théorème 6.2. [D'Alembert-Gauss] *Tout polynôme de degré $n \geqslant 1$ à coefficients complexes :*

$$p(x) \,=\, a_n\, x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_0,$$

admet une factorisation de la forme :

$$p(x) \,=\, \lambda \big(x - \alpha_1\big)\, \big(x - \alpha_2\big)\, \cdots\, \big(x - \alpha_n\big),$$

avec $\lambda = a_n$ et avec n nombres complexes $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$.

En regroupant les α_i qui sont égaux, on en déduit la représentation plus précise :

$$p(x) \,=\, \lambda \big(x - \beta_1\big)^{h_1}\, \big(x - \beta_2\big)^{h_2}\, \cdots \big(x - \beta_r\big)^{h_r},$$

avec des racines β_j distinctes deux à deux, avec des exposants $h_j \geqslant 1$, et avec :

$$n \,=\, h_1 + h_2 + \cdots + h_r.$$

Démonstration. Soit donc $p(x) \in \mathbb{C}[x]$ de degré $\deg p(x) = n \geqslant 1$.

Grâce au Théorème 6.2 de d'Alembert-Gauss, $p(x)$ admet au moins un zéro $\alpha_1 \in \mathbb{C}$. Il existe donc un polynôme $p_1 \in \mathbb{C}[x]$ tel que :

$$p(x) \,=\, (x - \alpha_1)\, p_1(x).$$

Si $n = 1$, on a terminé car $\deg p_1 = 0$, donc $p_1(x) \equiv a_{n=1}$ est une constante, nécessairement égale au coefficient de tête a_1 de $p(x)$.

Si $n \geqslant 2$, on a $\deg p_1 \geqslant 1$. De plus, p_1 est encore à coefficients dans le corps $\mathbb{C}$. Donc on peut appliquer de nouveau le Théorème 6.2 de d'Alembert-Gauss au polynôme $p_1(x)$.

Ainsi, $p_1(x)$ admet au moins un zéro $\alpha_2 \in \mathbb{C}$, et il existe $p_2(x) \in \mathbb{C}[x]$ tel que :

$$p_1(x) \,=\, (x - \alpha_2)\, p_2(x),$$

d'où :

$$p(x) \,=\, \big(x - \alpha_1\big)\, \big(x - \alpha_2\big)\, p_2(x).$$

Si $n = 2$, alors $\deg p_2 = 0$, et $p_2 \equiv a_{n=2}$ est une constante, forcément égale au coefficient de tête a_2 de $p(x)$.

Pour $n \geqslant 2$ quelconque, raisonnons maintenant par récurrence sur le degré n du polynôme $p(x)$. Supposons que :

$$p(x) \,=\, \big(x - \alpha_1\big)\, \big(x - \alpha_2\big)\, \cdots\, \big(x - \alpha_{n-1}\big)\, p_{n-1}(x),$$

avec $\deg p_{n-1} = 1$.

Alors il existe une constante $\lambda \in \mathbb{C}^*$ et un nombre $\alpha_n \in \mathbb{C}$ tels que :

$$p_{n-1}(x) \,=\, \lambda \big(x - \alpha_n\big),$$

et par conséquent :

$$p(x) \,=\, \lambda \big(x-\alpha_1\big)\,\big(x-\alpha_2\big)\,\cdots\,\big(x-\alpha_{n-1}\big)\,\big(x-\alpha_n\big).$$

Pour conclure, il suffit d'identifier les coefficients $a_n = \lambda$ du monôme x^n de plus haut degré de part et d'autre de cette égalité. □

Définition 6.3. Un corps $\mathbb{K}$ dans lequel *tout* polynôme de degré $n \geqslant 1$ arbitraire admet toujours au moins une racine est dit *algébriquement clos.*

Ainsi, $\mathbb{C}$ est algébriquement clos. Par des arguments complètement similaires, on généralise aisément le Théorème 6.2 de d'Alembert-Gauss aux corps algébriquement clos quelconques.

Théorème 6.4. *Sur un corps commutatif $\mathbb{K}$, on a équivalence entre :*
(i) *tout polynôme $p \in \mathbb{K}[x]$ de degré quelconque $n \geqslant 1$ admet au moins une racine dans $\mathbb{K}$;*
(ii) *les polynômes irréductibles de $\mathbb{K}[x]$ sont exactement les polynômes de degré 1 ;*
(iii) *tout polynôme $p \in \mathbb{K}[x]$ de degré quelconque $n \geqslant 1$ est produit de n polynômes de degré 1.* □

Venons-en maintenant aux *relations fondamentales* entre les coefficients d'un polynôme $p(x) \in \mathbb{C}[x]$ et ses racines. Avec $n \geqslant 1$, soit donc :

$$p(x) \,=\, a_n\,x^n + a_{n-1}\,x^{n-1} + \cdots + a_1\,x + a_0.$$

Comme dans le Théorème 6.2, notons $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ ses racines, distinctes ou non, peu importe, de telle sorte que $p(x)$ se décompose en produit de polynômes du premier degré :

$$a_n\,x^n + a_{n-1}\,x^{n-1} + \cdots + a_1\,x + a_0 \,=\, \lambda \big(x-\alpha_1\big)\,\big(x-\alpha_1\big)\,\cdots\,\big(x-\alpha_n\big). \tag{6.5}$$

Maintenant, proposons-nous de *développer courageusement* ce produit de facteurs, même si on avait par exemple $n = 625$!

En identifiant les coefficients du monôme de plus haut degré x^n, nous avons déjà observé que l'on obtient :

$$a_n \,=\, \lambda.$$

Ensuite, pour le coefficient de x^{n-1}, il faut prendre dans le produit à droite $(n-1)$ fois le facteur x, et 1 fois un terme constant $-\alpha_i$ avec $1 \leqslant i \leqslant n$, ce qui donne par identification :

$$a_{n-1} \,=\, -\,\lambda \Big(\alpha_1 + \alpha_2 + \cdots + \alpha_n\Big).$$

On voit ainsi apparaître la *somme* des racines, que l'on note :

$$\sigma_1 \,:=\, \alpha_1 + \alpha_2 + \cdots + \alpha_n.$$

Pour le coefficient de x^{n-2}, il faut prendre dans le produit à droite $(n-2)$ fois le facteur x, et des produits de 2 termes constants $-\,\alpha_{i_1}$ et $-\,\alpha_{i_2}$ avec $1 \leqslant i_1 < i_2 \leqslant n$, ce qui donne par identification :

$$a_{n-2} \,=\, \lambda\,(-1)^2 \sum_{1 \leqslant i_1 < i_2 \leqslant n} \alpha_{i_1}\,\alpha_{i_2}.$$

On voit ainsi apparaître la somme des produits deux à deux des racines :

$$\sigma_2 \,:=\, \sum_{1 \leqslant i_1 < i_2 \leqslant n} \alpha_{i_1}\,\alpha_{i_2}.$$

D'une façon générale, cherchons le coefficient du monôme x^{n-k} avec un entier fixé $1 \leqslant k \leqslant n$. Il faut prendre dans le produit à droite $(n-k)$ fois le facteur x, et des produits de k termes constants $-\alpha_{i_1}, \ldots, -\alpha_{i_k}$ avec $1 \leqslant i_1 < \cdots < i_k \leqslant n$, ce qui donne par identification :

$$a_{n-k} \;=\; \lambda\,(-1)^k \sum_{1\leqslant i_1<\cdots<i_k\leqslant n} \alpha_{i_1}\cdots\alpha_{i_k}.$$

On voit ainsi apparaître :

$$\sigma_k \;:=\; \sum_{1\leqslant i_1<\cdots<i_k\leqslant n} \alpha_{i_1}\cdots\alpha_{i_k} \qquad (1\leqslant k\leqslant n).$$

En particulier :

$$\begin{aligned}\sigma_1 \;&=\; \alpha_1+\alpha_2+\cdots+\alpha_n,\\ \sigma_n \;&=\; \alpha_1\,\alpha_2\,\cdots\,\alpha_n,\end{aligned}$$

sont, respectivement, la somme, et le produit, de toutes les racines.

En définitive, d'après ce qui précède, on aura, puisque $\lambda = a_n$:

$$\frac{a_{n-k}}{a_n} \;=\; (-1)^k\,\sigma_k \qquad (1\leqslant k\leqslant n).$$

Nous obtenons ainsi les n *relations fondamentales* entre les coefficients $a_n, \ldots, a_1, a_0$ d'un polynôme $p(x) \in \mathbb{C}[x]$, et ses zéros $\alpha_1, \ldots, \alpha_n$.

Le polynôme $p(x)$ écrit sous forme d'un produit se développe donc comme suit :

$$\begin{aligned}p(x) \;&=\; \lambda\,\big(x-\alpha_1\big)\,\big(x-\alpha_2\big)\,\cdots\,\big(x-\alpha_n\big)\\ &=\; a_n\Big[x^n-\sigma_1\,x^{n-1}+\cdots+(-1)^k\,\sigma_k\,x^{n-k}+\cdots+(-1)^n\,\sigma_n\Big],\end{aligned}$$

en termes des *fonctions symétriques élémentaires* des racines :

$$\sigma_k \;:=\; \sum_{1\leqslant i_1<\cdots<i_k\leqslant n} \alpha_{i_1}\cdots\alpha_{i_k} \qquad (1\leqslant k\leqslant n).$$

Théorème 6.6. *Pour que $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ soient les zéros d'un polynôme de degré $n \geqslant 1$:*

$$p(x) \;=\; a_n\,x^n+\cdots+a_1\,x+a_0 \qquad (a_n\neq 0),$$

il faut et il suffit que, pour tout $1 \leqslant k \leqslant n$, on ait :

$$\begin{aligned}\frac{a_{n-k}}{a_n} \;&=\; (-1)^k\,\sigma_k\\ &=\; (-1)^k \sum_{1\leqslant i_1<\cdots<i_k\leqslant n} \alpha_{i_1}\cdots\alpha_{i_k}.\end{aligned}$$

□

Afin de mieux appréhender ces formules générales, écrivons-les explicitement en degrés $n = 2$ et $n = 3$.

Pour un polynôme général du second degré :

$$p(x) \;=\; a_2\,x^2+a_1\,x+a_0,$$

un simple développement du produit :

$$a_2\,\big(x-\alpha_1\big)\,\big(x-\alpha_2\big) \;=\; a_2\Big[x^2-\big(\alpha_1+\alpha_2\big)\,x+\alpha_1\,\alpha_2\Big],$$

suivi d'une identification, donnent :

$$\begin{aligned} a_2 &= a_2, \\ a_1 &= -\,a_2\,\big(\alpha_1+\alpha_2\big), \\ a_0 &= a_2\,\alpha_1\,\alpha_2. \end{aligned}$$

Pour un polynôme général du troisième degré :

$$p(x) \;=\; a_3\,x^3 + a_2\,x^2 + a_1\,x + a_0,$$

un simple développement du produit :

$$\begin{aligned} &a_3\,\big(x-\alpha_1\big)\,\big(x-\alpha_2\big)\,\big(x-\alpha_3\big) \;= \\ &\quad= \;a_3\,\Big[x^3 - \big(\alpha_1+\alpha_2+\alpha_3\big)\,x^2 + \big(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3\big)\,x - \alpha_1\,\alpha_2\,\alpha_3\Big], \end{aligned}$$

suivi d'une identification, donnent :

$$\begin{aligned} a_3 &= a_3, \\ a_2 &= -\,a_3\,\big(\alpha_1+\alpha_2+\alpha_3\big), \\ a_1 &= a_3\,\big(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3\big), \\ a_0 &= -\,a_3\,\alpha_1\,\alpha_2\,\alpha_3. \end{aligned}$$

Passons maintenant aux polynômes de $\mathbb{R}[x]$. Comme on a clairement :

$$\mathbb{R} \;\subset\; \mathbb{C} \qquad\qquad \Longrightarrow \qquad\qquad \mathbb{R}[x] \;\subset\; \mathbb{C}[x],$$

ce qui a été dit des polynômes à coefficients complexes s'étend — au moins partiellement — aux polynômes à coefficients réels. Par exemple, tout polynôme à coefficients réels admet au moins une racine dans $\mathbb{C}$, qui, parfois, peut appartenir à $\mathbb{R}$.

Il faut remarquer que les zéros d'un polynôme de $\mathbb{R}[x]$ ne sont pas toujours tous réels. En effet, on sait par exemple que le polynôme général du second degré à coefficients réels :

$$a\,x^2 + b\,x + c \qquad\qquad (a\neq 0),$$

n'a de zéros réels que dans le cas où $b^2 - 4\,ac \geqslant 0$. Mais dans le cas où $b^2 - 4\,ac < 0$, les deux zéros appartiennent à $\mathbb{C}\backslash\mathbb{R}$.

Observation 6.7. *Le corps $\mathbb{R}$ des nombres réels n'est* pas *algébriquement clos.* □

Ainsi, contrairement à ce qui se passe dans $\mathbb{C}[x]$, dans $\mathbb{R}[x]$, les polynômes irréductibles ne sont pas nécessairement tous du premier degré. Nous nous proposons d'établir dans ce qui suit que tout polynôme irréductible de $\mathbb{R}[x]$ est, soit du premier degré, soit du second degré.

Nous allons commencer par établir une propriété importante des polynômes à coefficients réels. Mais auparavant, rappelons que l'involution $\alpha \longmapsto \overline{\alpha}$ de $\mathbb{C}$ dans $\mathbb{C}$, la *conjugaison complexe :*

$$\mathsf{Re}\,\alpha + i\,\mathsf{Im}\,\alpha \;\;\longmapsto\;\; \mathsf{Re}\,\alpha - i\,\mathsf{Im}\,\alpha,$$

est un automorphisme du corps $\big(\mathbb{C},+,\times\big)$, pour l'addition, et pour la multiplication :

$$\begin{aligned} \overline{\alpha+\beta} &= \overline{\alpha}+\overline{\beta}, \\ \overline{\alpha\,\beta} &= \overline{\alpha}\,\overline{\beta}. \end{aligned}$$

Rappelons aussi que le conjugué d'un nombre $\alpha = a \in \mathbb{R}$ de partie imaginaire nulle est $\overline{a} = a$.

Proposition 6.8. *Si $p(x) \in \mathbb{R}[x]$ est un polynôme à coefficients* réels*, alors pour tout $\alpha \in \mathbb{C}$, on a :*

$$\overline{p(\alpha)} \,=\, p\big(\overline{\alpha}\big).$$

Démonstration. Développons :

$$p(x) \,=\, \sum_{k=0}^{n} a_k\, x^k,$$

avec par hypothèse :

$$a_k \,\in\, \mathbb{R} \qquad (\forall\ 0 \leqslant k \leqslant n).$$

Puisque $\alpha \longmapsto \overline{\alpha}$ est un automorphisme de $\mathbb{C}$ pour l'addition et pour la multiplication, et puisque $a_k \in \mathbb{R}$, on a :

$$\overline{a_k\, \alpha^k} \,=\, a_k\, \overline{\alpha}^k \qquad (0 \leqslant k \leqslant n).$$

Ainsi, notre petite annonce publicitaire n'était pas mensongère :

$$\begin{aligned}
\overline{p(\alpha)} \,&=\, \sum_{k=0}^{n} \overline{a_k\, \alpha^k} \\
&=\, \sum_{k=0}^{n} a_k\, \overline{\alpha}^k \\
&=\, p\big(\overline{\alpha}\big).
\end{aligned}$$

□

Il en résulte l'énoncé suivant.

Théorème 6.9. *Si $\alpha \in \mathbb{C}$ est un zéro d'ordre $h \geqslant 1$ d'un polynôme $p(x) \in \mathbb{R}[x]$ à coefficients réels, alors son conjugué $\overline{\alpha}$ est* aussi *un zéro d'ordre h de ce polynôme.*

Démonstration. En effet, en appliquant la caractérisation du Théorème 5.8, on a par hypothèse :

$$p(\alpha) \,=\, p'(\alpha) \,=\, \cdots \,=\, p^{(h-1)}(\alpha) \,=\, 0 \,\neq\, p^{(h)}(\alpha).$$

Par conséquent, puisque les coefficients de p sont tous réels, et puisque $\overline{0} = 0$, la Propostion 6.8 donne aussi :

$$p\big(\overline{\alpha}\big) \,=\, p'\big(\overline{\alpha}\big) \,=\, \cdots \,=\, p^{(h-1)}\big(\overline{\alpha}\big) \,=\, 0 \,\neq\, p^{(h)}\big(\overline{\alpha}\big),$$

ce qui exprime précisément, à nouveau grâce à la caractérisation du Théorème 5.8, que $\overline{\alpha}$ est un zéro d'ordre h de $p(x)$. □

7. Polynômes irréductibles dans $\mathbb{R}[x]$

Soit un polynôme $p(x) \in \mathbb{R}[x]$, de degré $n \geqslant 1$. Il admet n zéros dans $\mathbb{C}$, dont certains peuvent éventuellement être réels.

Pour $k = 1, \ldots, t$, soit $h_k \geqslant 1$ l'ordre de multiplicité d'un zéro $\gamma_k \in \mathbb{C}$, de telle sorte que $p(x)$ se factorise *sur* $\mathbb{C}$ comme :

$$\begin{gathered}
p(x) \,=\, \lambda\, \big(x - \gamma_1\big)^{h_1}\, \big(x - \gamma_2\big)^{h_2} \cdots \big(x - \gamma_t\big)^{h_t}, \\
\lambda \,\in\, \mathbb{C}, \qquad\qquad \gamma_1, \ldots, \gamma_t \in \mathbb{C}, \\
h_1 + h_2 + \cdots + h_t \,=\, n.
\end{gathered}$$

Dans cette décomposition, d'après le Théorème 6.9, à tout zéro $\gamma_k \in \mathbb{C}\backslash\mathbb{R}$ qui n'est *pas* réel, correspond un zéro distinct $\gamma_\ell = \overline{\gamma}_k$, de même multiplicité $h_\ell = h_k$, avec $\ell \neq k$. Pour cette raison, la collection complète des zéros distincts peut être organisée comme :

$$\Big\{\alpha_1, \ldots, \alpha_r,\ \beta_1, \overline{\beta}_1,\ \ldots,\ \beta_s, \overline{\beta}_s\Big\},$$
$$\alpha_i \in \mathbb{R}, \qquad \beta_j \in \mathbb{C}\backslash\mathbb{R},$$

avec des multiplicités respectives :

$$g_1, \ldots, g_r,\ h_1, h_1, \ldots, h_s, h_s,$$

qui satisfont bien sûr :

$$n = g_1 + \cdots + g_r + 2\,h_1 + \cdots + 2\,h_s.$$

Maintenant, portons notre attention sur un doubleton $\big\{\beta_j, \overline{\beta}_j\big\}$ de zéros complexes conjugués *non réels*, avec $1 \leqslant j \leqslant s$. En ce qui les concerne, on a dans la décomposition précédente de $p(x)$ un produit du type :

$$\big(x - \beta_j\big)^{h_j} \big(x - \overline{\beta}_j\big)^{h_j} = \Big[\big(x - \beta_j\big)\big(x - \overline{\beta}_j\big)\Big]^{h_j}.$$

Or com' — que d'la com ! — :

$$\big(x - \beta_j\big)\big(x - \overline{\beta}_j\big) = x^2 - \big(\beta_j + \overline{\beta}_j\big)\,x + \beta_j\,\overline{\beta}_j,$$

et com' :

$$-\beta_j - \overline{\beta}_j =: b_j \in \mathbb{R},$$
$$\beta_j\,\overline{\beta}_j =: c_j \in \mathbb{R},$$

nous pouvons ré-écrire :

$$\big(x - \beta_j\big)^{h_j} \big(x - \overline{\beta}_j\big)^{h_j} = \big(x^2 + b_j\,x + c_j\big)^{h_j} \in \mathbb{R}[x],$$

et constater que nous avons en fait affaire à un polynôme à coefficients *réels*.

Proposition 7.1. *Tout polynôme quadratique $x^2 + b\,x + c$ à coefficients réels $b, c \in \mathbb{R}$ est irréductible dans $\mathbb{R}[x]$ si et seulement si $b^2 - 4\,c < 0$.*

Démonstration. Lorsque $b^2 - 4\,c \geqslant 0$, nous savons qu'il existe deux racines réelles, données par :

$$\frac{-\,b + \sqrt{b^2 - 4\,c}}{2} \qquad \text{et} \qquad \frac{-\,b - \sqrt{b^2 - 4\,c}}{2}.$$

Lorsque $b^2 - 4\,c < 0$, supposons par l'absurde que $x^2 + b\,x + c$ ne soit pas irréductible. Alors puisque son degré est égal à 2, et puisque seule la somme $2 = 1 + 1$ est possible, nécessairement, $x^2 + b\,x + c$ devrait se décomposer :

$$x^2 + b\,x + c \overset{?}{=} \big(x - \delta\big)\big(x - \varepsilon\big),$$

comme produit de deux facteurs unitaires de degré 1, avec $\delta, \varepsilon \in \mathbb{R}$ réels.

Mais alors l'identité :

$$x^2 + b\,x + c = x^2 - (\delta + \varepsilon)\,x + \delta\,\varepsilon,$$

donnerait par identification :

$$b = -\,\delta - \varepsilon, \qquad\qquad c = \delta\,\varepsilon,$$

puis :

$$\begin{aligned} b^2 - 4\,c \;&=\; \big(-\,\delta - \varepsilon\big)^2 - 4\,\delta\,\varepsilon \\ &=\; \delta^2 + \varepsilon^2 - 2\,\delta\,\varepsilon \\ &=\; \big(\delta - \varepsilon\big)^2 \;\geqslant\; 0, \end{aligned}$$

en contradiction avec l'hypothèse $b^2 - 4\,c < 0$ dont nous sommes partis. □

Ici, on vérifie que $b_j^2 - 4\,c_j < 0$ comme suit :

$$\begin{aligned} b_j^2 - 4\,c_j \;&=\; \big(\beta_j + \overline{\beta}_j\big)^2 - 4\,\beta_j\,\overline{\beta}_j \\ &=\; \big(\beta_j - \overline{\beta}_j\big)^2 \\ &=\; \big(2\,i\,\mathsf{Im}\,\beta_j\big)^2 \\ &=\; -\,4\,\big(\mathsf{Im}\,\beta_j\big)^2 \;<\; 0, \end{aligned}$$

puisque par hypothèse $\beta_j \in \mathbb{C}\backslash\mathbb{R}$, donc $x^2 + b_j\,x + c_j$ est irréductible.

Ainsi, le résultat auquel nous sommes parvenus peut s'énoncer sour la forme d'une synthèse conclusive.

Théorème 7.2. *Les polynômes irréductibles (unitaires) de $\mathbb{R}[x]$ sont, soit du premier degré de la forme :*

$$x + a, \qquad \textit{avec} \qquad a \in \mathbb{R},$$

soit du second degré de la forme :

$$x^2 + b\,x + c, \qquad \textit{avec} \qquad b^2 - 4\,c \;<\; 0.$$

De plus, tout polynôme $p(x) \in \mathbb{R}[x]$ de degré $n \geqslant 1$ se factorise comme produit de facteurs irréductibles :

$$\begin{aligned} p(x) \;&=\; \lambda \prod_{i=1}^{r} \big(x + a_i\big)^{g_i} \prod_{j=1}^{s} \big(x^2 + b_j\,x + c_j\big)^{h_j}, \\ n \;&=\; g_1 + \cdots + g_r + 2\,h_1 + \cdots + 2\,h_s, \end{aligned}$$

où $\lambda \in \mathbb{R}$ est le coefficient du monôme de tête x^n dans $p(x)$. □

Exemple 7.3. Proposons-nous de décomposer en produit de facteurs irréductibles dans $\mathbb{R}[x]$ le polynôme dit *cyclotomique :*

$$x^n - 1 \qquad (n \geqslant 1).$$

Dans $\mathbb{C}$, les zéros de $x^n - 1$ sont les racines n-ièmes de l'unité :

$$\begin{aligned} x_n \;&:=\; e^{\frac{2i\pi k}{n}} \\ &=\; \mathsf{cos}\,\tfrac{2k\pi}{n} + i\,\mathsf{sin}\,\tfrac{2k\pi}{n} \qquad (0 \leqslant k \leqslant n-1). \end{aligned}$$

Donc dans $\mathbb{C}[x]$, la décomposition de $x^n - 1$ en produit de facteurs irréductibles — tous de degré 1 — est :

$$x^n - 1 \;=\; \prod_{k=0}^{n-1} \big(x - e^{\frac{2i\pi k}{n}}\big).$$

Ensuite, pour que $x_k = e^{\frac{2i\pi k}{n}}$ et $x_{k'} = e^{\frac{2i\pi k'}{n}}$ soient deux zéros conjugués $x_k = \overline{x_{k'}}$, il faut et il suffit que :

$$\arg x_k \equiv -\arg x_{k'} \mod 2\pi,$$

c'est-à-dire que :

$$k \equiv -k' \mod n.$$

De plus, $x_k = \overline{x_k}$ est une racine réelle si et seulement si :

$$k \equiv -k \mod n.$$

Or cette équation :

$$2\,k \equiv 0 \mod n,$$

a visiblement la solution $k = 0$, qui correspond au zéro évident $x_0 = 1$, et en a éventuellement une autre, $k = n/2$, si $n = 2\,p$ est pair, ce qui donne le zéro réel $x_{n/2} = -1$.

Pour factoriser $x^n - 1$ en produit de facteurs irréductibles sur $\mathbb{R}[x]$, il est donc nécessaire de distinguer deux cas.

Cas 1. $n = 2\,p$ est pair. Il y a alors deux zéros réels, 1 et -1. En outre, comme, pour $1 \leqslant k \leqslant p-1$, on a :

$$\begin{aligned} x_k + \overline{x}_k &= 2\cos\tfrac{2k\pi}{n} = 2\cos\tfrac{k\pi}{p}, \\ x_k\,\overline{x_k} &= 1, \end{aligned}$$

il est clair que :

$$x^{2p} - 1 = (x-1)\,(x+1)\prod_{k=1}^{p-1}\Big(x^2 - 2\cos\tfrac{k\pi}{p}\,x + 1\Big).$$

Ainsi, deux facteurs irréductibles sont de degré 1, et $p-1$ facteurs irréductibles sont de degré 2.

Cas 2. $n = 2\,p+1$ est impair. Il y a alors un seul zéro réel, 1. En outre, comme, pour $1 \leqslant k \leqslant p$, on a :

$$\begin{aligned} x_k + \overline{x}_k &= 2\cos\tfrac{2\,k\pi}{2\,p+1}, \\ x_k\,\overline{x_k} &= 1, \end{aligned}$$

il est clair que :

$$x^{2p+1} - 1 = (x-1)\prod_{k=1}^{p}\Big(x^2 - 2\cos\tfrac{2\,k\pi}{2\,p+1}\,x + 1\Big).$$

Ainsi, un facteur irréductible est de degré 1, et p facteurs irréductibles sont de degré 2.

Les polynômes irréductibles de $\mathbb{Q}[x]$ sont difficiles à classifier. Voici un exemple montrant qu'il existe des polynômes de tous degrés dans $\mathbb{Q}[x]$ qui sont irréductibles.

Proposition 7.4. *Pour un entier arbitraire $n \geqslant 1$, le polynôme $x^n - 2$ est irréductible dans $\mathbb{Q}[x]$.*

Démonstration. Comme $x^1 - 2$ est irréductible, on peut supposer $n \geqslant 2$.

Par l'absurde, supposons au contraire que $x^n - 2$ possède un diviseur unitaire $p \in \mathbb{Q}[x]$ de degré :

$$1 \leqslant \deg p = d \leqslant n-1.$$

Or, comme on connaît la factorisation sur $\mathbb{C}$ de :

$$x^n - 2 \,=\, \prod_{0 \leqslant k \leqslant n-1} \Big(x - \sqrt[n]{2}\, e^{\frac{2i\pi k}{n}} \Big),$$

il doit exister d indices $0 \leqslant k_1 < \cdots < k_d \leqslant n-1$ tels que :

$$p(x) \,=\, \Big(x - \sqrt[n]{2}\, e^{\frac{2i\pi k_1}{n}} \Big) \cdots \Big(x - \sqrt[n]{2}\, e^{\frac{2i\pi k_d}{n}} \Big).$$

Par conséquent, le terme constant de p, *i.e.* de degré 0 — qui appartient à $\mathbb{Q}$ par hypothèse — doit donc s'identifiifier à la valeur à droite pour $x = 0$:

$$\mathbb{Q} \,\ni\, p(0) \,=\, (-1)^d \, \big(\sqrt[n]{2} \big)^d \, e^{\frac{2i\pi (k_1 + \cdots + k_d)}{n}}.$$

Si nous prenons ensuite le module, il vient :

$$\mathbb{Q}_+ \,\ni\, |p(0)| \,=\, 2^{\frac{d}{n}}.$$

Assertion 7.5. *Pour tout entier $n \geqslant 2$ et tout entier $1 \leqslant d \leqslant n-1$, le nombre $2^{\frac{d}{n}} \notin \mathbb{Q}$ n'est par rationnel.*

Preuve. Par l'absurde, s'il existait deux entiers a et b *premiers entre* tels que $2^{\frac{d}{n}} = \frac{a}{b}$, d'où $2^{\frac{d}{n}}\, b = a$, on aurait :

$$2^d \, b^n \,=\, a^n.$$

Comme $d \geqslant 1$, ceci impliquerait $2 \,|\, a$, d'où $a = 2\, a'$ avec a' entier, puis :

$$2^d \, b^n \,=\, 2^n \, a'^n \qquad\qquad \Longrightarrow \qquad\qquad b^n \,=\, 2^{n-d} \, a'^n.$$

Comme $1 \,\leqslant\, n - d$, ceci impliquerait à son tour que $2 \,|\, b$, donc 2 serait un diviseur commun à a et à b, en contradiction manifeste avec notre hypothèse de départ. □

Ainsi, il n'existe pas de polynôme (unitaire) $p \in \mathbb{Q}[x]$ à coefficients rationnels divisant $x^n - 2$ et de degré intermédiaire $1 \leqslant d \leqslant n-1$, ce qui établit bien que $x^n - 2$ est irréductible sur $\mathbb{Q}$. □

8. Résolution des équations de degré 3

Dans cette section, nous allons exposer une *méthode*, qui remonte aux mathématiques italiennes du XVI$^{\text{ième}}$ siècle, de résolution des équations algébriques de degré 3 à coefficients complexes.

L'équation générale du troisième degré est :

$$u^3 + a\, u^2 + b\, u + c \,=\, 0, \tag{8.1}$$

avec des coefficients complexes $a, b, c \in \mathbb{C}$. Posons :

$$u \,=:\, x + h,$$

de telle sorte que la proposée (8.1) devient :

$$x^3 + 3h\, x^2 + 3h^2\, x + h^3 + a \, \big(x^2 + 2\, h\, x + h^2 \big) + b \, \big(x + h \big) + c \,=\, 0,$$

c'est-à-dire :

$$x^3 + (\underline{3\, h + a}_{\circ})\, x^2 + (3\, h^2 + 2\, a\, h + b)\, x + h^3 + a\, h^2 + b\, h + c \,=\, 0.$$

Déterminons alors $h \in \mathbb{C}$ afin que le coefficient de x^2 soit égal à 0. Il est clair que :

$$h \,:=\, -\tfrac{a}{3},$$

est la solution unique. Il en résulte qu'en posant :

$$u \;=:\; x - \tfrac{a}{3},$$

l'équation (8.1) se transforme en une *équation réduite*, de la forme :

$$x^3 + p\,x + q \;=\; 0. \tag{8.2}$$

Ensuite, posons :

$$x \;=:\; y + z, \tag{8.3}$$

c'est-à-dire « cassons » l'inconnue x en deux morceaux, en deux nouvelles inconnues y et z — telle est l'« idée de génie ». En effet, nous allons exprimer entre ces deux nouvelles inconnues y et z une condition de simplification algébrique qui va nous permettre de trouver toutes les racines du polynôme $x^3 + p\,x + q$.

Notre équation (8.2) devient alors :

$$y^3 + 3\,y^2\,z + 3\,y\,z^2 + z^3 + p\,y + p\,z + q \;=\; 0,$$

équation que nous ré-écrivons comme suit :

$$y^3 + z^3 + \big(3\,y\,z + p\big)\,\big(y + z\big) + q \;=\; 0.$$

Choisissons alors la condition de simplification mentionnée de manière à ce que le coefficient de $y + z$ soit nul :

$$3\,y\,z + p \;=\; 0, \tag{8.4}$$

ce qui fait qu'il ne reste plus que :

$$y^3 + z^3 + q \;=\; 0. \tag{8.5}$$

Si (y, z) est une solution du système (8.4), (8.5) alors $y + z$ est évidemment une solution de (8.2).

En prenant le cube de (8.4), nous avons un nouveau système :

$$\begin{aligned} y^3 + z^3 \;&=\; -\,q, \\ y^3\,z^3 \;&=\; -\,\tfrac{1}{27}\,p^3, \end{aligned}$$

qui exprime que nous connaissons la somme $-\,q$, et le produit $-\frac{1}{27}\,p^3$ des cubes de nos deux nouvelles inconnues.

Or le point-clé, et l'éclair de génie, c'est que toute paire de nombres dont on connaît la somme et le produit est automatiquement solution d'une équation du second degré :

$$t^2 + q\,t - \frac{p^3}{27} \;=\; 0, \tag{8.6}$$

et que l'on sait résoudre les équations du second degré !

En effet, cette équation a deux racines dans $\mathbb{C}$:

$$t' \;:=\; \frac{-\,q - \sqrt{q^2 + \frac{4}{27}\,p^3}}{2} \qquad \text{et} \qquad t'' \;:=\; \frac{-\,q + \sqrt{q^2 + \frac{4}{27}\,p^3}}{2},$$

et donc on a :

$$y^3 \;=\; t' \qquad \text{et} \qquad z^3 \;=\; t''.$$

Si α est une racine cubique de t', au moyen de la racine cubique de l'unité :

$$j \;:=\; e^{\frac{2i\pi}{3}},$$

les deux autres racines cubiques sont alors :

$$j\,\alpha, \qquad\qquad j^2\,\alpha.$$

Nous obtenons donc pour y les trois valeurs :

$$y_1 := \alpha, \qquad\qquad y_2 := j\,\alpha, \qquad\qquad y_3 := j^2\,\alpha.$$

Enfin, pour z, les valeurs correspondantes sont données en revenant à (8.2) :

$$z_1 = -\frac{p}{3\,\alpha}, \qquad\qquad z_2 = -\frac{p}{3\,j\,\alpha}, \qquad\qquad z_3 = -\frac{p}{3\,j^2\,\alpha}.$$

On peut d'ailleurs remarquer que z_1, que $z_2 = j^2\,z_1$, que $z_3 = j\,z_1$, sont précisément les trois racines de l'équation $z^3 = t''$.

En définitive, les trois racines complexes de l'équation cubique (8.2) sont :

$$\text{(8.7)} \qquad \begin{cases} x_1 := \alpha - \dfrac{p}{3\,\alpha}, \\ x_2 = j\,\alpha - \dfrac{p}{3\,\alpha}\,j^2, \\ x_3 = j^2\,\alpha - \dfrac{p}{3\,\alpha}\,j, \end{cases}$$

où α est une racine cubique d'une solution de (8.6).

9. Compléments en caractéristique positive

Rappelons que nous avons défini, pour un anneau commutatif intègre A, donc pour un corps $\mathbb{K}$, la *caractéristique*, qui est l'entier minimal m tel que $m \cdot 1 = 0$, un nombre premier p, ou 0.

Rappelons aussi qu'étant donné un polynôme :

$$p(x) = a_n\,x^n + \cdots + a_1\,x + a_0,$$

avec $a_n \neq 0$ si $p \neq 0$, on appelle *fonction polynomiale* associée à p l'application :

$$\begin{array}{rccc} \widetilde{p}\colon & \mathbb{K} & \longrightarrow & \mathbb{K} \\ & \alpha & \longmapsto & a_n\,\alpha^n + \cdots + \alpha_1\,x + \alpha_0. \end{array}$$

Ainsi, $\widetilde{p}(\alpha) \in \mathbb{K}$ est un élément du corps. On démontre aisément la

Proposition 9.1. *Étant donné deux polynômes quelconques $p, q \in \mathbb{K}[x]$, on a pour tout $\alpha \in \mathbb{K}$:*

$$\begin{aligned} \widetilde{p+q}(\alpha) &= \widetilde{p}(\alpha) + \widetilde{q}(\alpha), \\ \widetilde{p\,q}(\alpha) &= \widetilde{p}(\alpha)\,\widetilde{q}(\alpha). \end{aligned}$$

□

Malheureusement, sur un corps $\mathbb{K}$ de caractéristique finie égale à un nombre premier $p \geqslant 2$, certaines choses ne se passent pas bien.

Notamment, à deux polynômes *différents* $p \neq q$ dans $\mathbb{K}[x]$, peuvent être associées deux fonctions polynomiales $\widetilde{p} = \widetilde{q}$ *égales* — chose très surprenante !

Sur le corps $\mathbb{K} := \mathbb{Z}/p\mathbb{Z}$ avec p premier, soient en effet par exemple les deux polynômes *différents* $p := x$ et $q := x^p$. À cause du théorème de Fermat, on a alors, pour tout $\alpha \in \mathbb{K}$ la coïncidence des valeurs :

$$\widetilde{q}(\alpha) = \alpha^p = \alpha = \widetilde{p}(\alpha).$$

Proposition 9.2. *Soient deux polynômes $p, q \in \mathbb{K}[x]$ de degrés $\leqslant n$. S'il existe $n+1$ éléments* deux à deux distincts $x_1, \ldots, x_{n+1} \in \mathbb{K}$ *tels que* $p(x_i) = q(x_i)$ *pour* $i = 1, \ldots, n+1$*, alors* $p = q$*.*

Démonstration. Le polynôme $p - q$ est d'un certain degré $m \leqslant n$.

Si $p - q$ était de degré $1 \leqslant m \leqslant n$ *non nul*, alors le Théorème 5.6 s'appliquerait, et dirait que $p - q$ a au plus $m \leqslant n$ racines, en contradiction totale avec l'hypothèse que $x_1, \ldots, x_{n+1}$ sont $n+1$ racines distinctes.

Donc le polynôme $p-q$ est de degré $\leqslant 0$, c'est-à-dire est une constante, et cette constante doit valoir 0, car elle doit s'annuler aux point x_i. □

Rappelons que d'après un théorème vu dans le chapitre consacré aux anneaux et aux corps abstraits, tout corps de caractéristique zéro est de cardinal infini, puisqu'il contient une copie du corps $\mathbb{Q}$ des nombres rationnels.

Corollaire 9.3. *Sur un corps de cardinal infini, on a équivalence entre :*

(i) $p = q$*;*

(ii) $\widetilde{p} = \widetilde{q}$*.* □

10. Exercices

Exercice 1. EE

Exercice 2. EE

Fractions

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Introduction

Nous savons que l'ensemble $\mathbb{K}[x]$ des polynômes à une indéterminée x sur un corps commutatif $\mathbb{K}$ est un anneau intègre. Mais la multiplication des polynômes n'y définit pas une structure de groupe, parce que la plupart des polynômes dans $\mathbb{K}[x]$ ne possèdent pas un inverse. En fait, aucun polynômes de degré $\geqslant 1$ n'a un inverse polynomial.

Malheureusement, donc, $\mathbb{K}[x]$ n'est *pas* un corps.

Il se pose maintenant, dans $\mathbb{K}[x]$, le même problème que pour la construction du corps $\mathbb{Q}$ des nombres rationnels, à partir de l'anneau $\mathbb{Z}$ des entiers. Il s'agit donc ici de *prolonger* l'anneau intègre $\mathbb{K}[x]$ en un ensemble plus vaste qui soit un corps commutatif. Ainsi, on a affaire au même type de problème général, celui de la construction du *corps des fractions* d'un anneau intègre quelconque.

Ce qui est connu pour la construction du corps $\mathbb{Q}$ à partir de l'anneau $\mathbb{Z}$ peut se répéter pour la solution du problème général en question.

2. Corps $F_{\mathbb{K}}[x]$ des fractions rationnelles

Posons :

$$\mathbb{K}[x]^* \,:=\, \mathbb{K}[x]\backslash\{0\}.$$

Définition 2.1. On appelle *fraction rationnelle* un couple (a, b) de $\mathbb{K}[x] \times \mathbb{K}[x]^*$, que l'on note aussi :

$$\frac{a}{b},$$

où a se nomme *numérateur*, et b *dénominateur*.

Ces fractions rationnelles $\frac{a}{b}$ sont en fait définies modulo une relation d'équivalence naturelle.

Définition 2.2. Deux fractions rationnelles $\frac{a}{b}$ et $\frac{c}{d}$ sont dites *équivalentes*, ce que l'on note :

$$\frac{a}{b} \;\sim\; \frac{c}{d},$$

si :

$$a\,d \,=\, b\,c.$$

On vérifie aisément que c'est bien une relation d'équivalence sur $\mathbb{K}[x] \times \mathbb{K}[x]^*$.

Notation 2.3. Le quotient de $\mathbb{K}[x] \times \mathbb{K}[x]^*$ par la relation d'équivalence $\sim$ sera noté :

$$F_{\mathbb{K}}[x],$$

et appelé *corps des fractions* de $\mathbb{K}[x]$.

Lorsqu'on voudra mettre en évidence un représentant $\frac{a}{b}$ d'une classe appartenant à $F_{\mathbb{K}}[x]$, on notera cette classe :

$$\left[\frac{a}{b}\right].$$

Soit donc une classe :

$$\left[\frac{a}{b}\right] \in F_{\mathbb{K}}[x].$$

Si on note $d := \mathsf{pgcd}(a, b)$, nous savons qu'il existe deux polynômes a_1 et b_1 de $\mathbb{K}[x]$ tels que :

$$a = d\,a_1, \qquad\qquad b = d\,b_1,$$
$$1 = \mathsf{pgcd}\,(a_1, b_1).$$

Puisque :

$$a\,b_1 - b\,a_1 = d\,a_1\,b_1 - d\,b_1\,a_1 = 0,$$

il en résulte que :

$$\frac{a}{b} \sim \frac{a_1}{b_1} \qquad \text{c'est-à-dire} \qquad \left[\frac{a}{b}\right] = \left[\frac{a_1}{b_1}\right].$$

Terminologie 2.4. La fraction $\frac{a_1}{b_1}$, où les deux polynômes a_1 et b_1 de $\mathbb{K}[x]$ sont premiers entre eux, est dite *irréductible.*

C'est un représentant le plus simple de la classe $\left[\frac{a}{b}\right]$.

Proposition 2.5. *Toute fraction rationnelle $\frac{c}{d}$ équivalente à $\frac{a}{b}$ est de la forme :*

$$\frac{p\,a_1}{p\,b_1}, \qquad \textit{avec} \qquad p \in \mathbb{K}[x]^*.$$

Démonstration. En effet, comme :

$$\frac{c}{d} \sim \frac{a_1}{b_1} \qquad \Longleftrightarrow \qquad c\,b_1 = d\,a_1,$$

et comme par le théorème de Gauss on a :

$$a_1 \mid d\,a_1 \qquad \Longrightarrow \qquad a_1 \mid c\,b_1$$
$$[1 = \mathsf{pgcd}\,(a_1, b_1)] \qquad \Longrightarrow \qquad a_1 \mid c,$$

il existe par conséquent $p \in \mathbb{K}[x]^*$ tel que :

$$c = p\,a_1,$$
$$\text{d'où :} \qquad d = p\,b_1. \qquad \square$$

Ensuite, de même que dans l'ensemble $\mathbb{Q}$ des nombres rationnels, on peut définir dans $F_{\mathbb{K}}[x]$ deux lois de composition naturelles.

Addition :

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{a\,d + b\,c}{b\,d}\right].$$

Multiplication :

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] \;=\; \left[\frac{a\,c}{b\,d}\right].$$

Comme pour les fractions rationnelles $\frac{a}{b} \in \mathbb{Q}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, on vérifie aisément les propriétés suivantes.

Proposition 2.6. **(1)** *Les deux lois d'addition et de multiplication dans $F_{\mathbb{K}}[x]$ ne dépendent pas des représentants choisis pour les classes.*

(2) *L'addition et la multiplication dans $F_{\mathbb{K}}[x]$ sont associatives et commutatives.*

(3) *L'addition admet l'élément neutre $\left[\frac{0}{b}\right]$, avec $b \in \mathbb{K}[x]^*$.*

(4) *La multiplication admet l'élément neutre $\left[\frac{b}{b}\right]$, avec $b \in \mathbb{K}[x]^*$.*

(5) *L'addition et la multiplication définissent chacune dans $F_{\mathbb{K}}[x]$ une structure de groupe commutatif.*

(6) *Pour l'addition, l'opposé de $\left[\frac{a}{b}\right]$ est $\left[\frac{-a}{b}\right]$.*

(7) *Pour la multiplication, l'inverse de $\left[\frac{a}{b}\right]$ avec $a, b \neq 0$, est $\left[\frac{b}{a}\right]$.* □

De plus, comme la multiplication est distributive pour l'addition, on a finalement l'énoncé suivant.

Théorème 2.7. *$F_{\mathbb{K}}[x]$ est un corps commutatif.* □

Ensuite, inspiré par l'immersion $\mathbb{Z} \hookrightarrow \mathbb{Q}$, nous allons immerger $\mathbb{K}[x]$ dans $F_{\mathbb{K}}[x]$, grâce à l'application :

$$p \;\longmapsto\; \left[\frac{p}{1}\right],$$

de $\mathbb{K}[x]$ dans $F_{\mathbb{K}}[x]$. On prouve aisément la

Proposition 2.8. *L'application $p \longmapsto \left[\frac{p}{1}\right]$ est un morphisme de groupes commutatifs, pour l'addition, et pour la multiplication.* □

Il est alors naturel d'identifier tout polynôme $p \in \mathbb{K}[x]$ avec son image $\left[\frac{p}{1}\right]$, en posant :

$$\left[\frac{p}{1}\right] \;:=\; p.$$

Ainsi, on *immerge* $\mathbb{K}[x]$ dans $F_{\mathbb{K}}[x]$:

$$\mathbb{K}[x] \;\hookrightarrow\; F_{\mathbb{K}}[x].$$

Tout élément $\left[\frac{a}{b}\right]$ de $F_{\mathbb{K}}[x]$ est alors le quotient exact des deux polynômes a et b. C'est pourquoi on note habituellement $\frac{a}{b}$ au lieu de $\left[\frac{a}{b}\right]$ un élément quelconque de $F_{\mathbb{K}}[x]$.

3. Partie entière d'une fraction rationnelle

Nous considérons toujours l'ensemble $F_{\mathbb{K}}[x]$ des fractions rationnelles sur un corps commutatif $\mathbb{K}$ quelconque.

À tout élément de $F_{\mathbb{K}}[x]$, nous associons son *représentant irréductible* $\frac{a}{b}$, c'est-à-dire avec $\mathsf{pgcd}\,(a, b) = 1$.

Effectuons la division euclidienne de a par b dans $\mathbb{K}[x]$:

$$a \;=\; b\,q + r, \qquad\qquad \mathsf{deg}\, r \;<\; \mathsf{deg}\, b.$$

On obtient alors, dans $F_{\mathbb{K}}[x]$:

$$\frac{a}{b} \;=\; q + \frac{r}{b}, \qquad\qquad \deg r \;<\; \deg b, \tag{3.1}$$

où la fraction $\frac{r}{b}$ est à nouveau irréductible, puisque nous avons déjà vu lors de l'algorithme d'Euclide que :

$$\operatorname{pgcd}(b, r) \;=\; \operatorname{pgcd}(a, b) \;=\; 1.$$

De plus, le degré du numérateur r de la nouvelle fraction $\frac{r}{b}$ est toujours strictement inférieur au degré de son numérateur b.

Terminologie 3.2. Le polynôme q de $\mathbb{K}[x]$ se nomme *partie entière* de la fraction rationnelle $\frac{a}{b}$.

La décomposition (3.1) est évidemment unique, grâce à l'unicité de la division euclidienne dans $\mathbb{K}[x]$.

Théorème 3.3. *Soit une fraction rationnelle $\frac{r}{b} \in F_{\mathbb{K}}[x]$ telle que :*

$$1 \;=\; \operatorname{pgcd}(r, b) \qquad\qquad \textit{et} \qquad\qquad \deg r \;<\; \deg b.$$

Si son dénominateur b est décomposé, d'une manière quelconque :

$$b \;=\; b_1\, b_2 \,\cdots\, b_n,$$

en produit de polynômes premiers entre eux — mais pas forcément irréductibles —, alors il existe n polynômes $r_1, r_2, \ldots, r_n$ de $\mathbb{K}[x]$ avec, pour tout $1 \leqslant i \leqslant n$:

$$\deg r_i \;<\; \deg b_i,$$

et avec :

$$1 \;=\; \operatorname{pgcd}(r_i, b_i) \qquad\qquad (1 \leqslant i \leqslant n),$$

tels que :

$$\frac{r}{b} \;=\; \frac{r_1}{b_1} + \frac{r_2}{b_2} + \cdots + \frac{r_n}{b_n}.$$

De plus, à toute décomposition fixée $b \;=\; b_1\, b_2 \,\cdots\, b_n$ de b en facteurs deux à deux premiers entre eux, il correspond une unique telle décomposition $\frac{r}{b} = \frac{r_1}{b_1} + \frac{r_2}{b_2} + \cdots + \frac{r_n}{b_n}$.

Démonstration. Établissons d'abord le théorème dans le cas déjà difficile et déjà significatif $n = 2$.

Supposons donc que :

$$b \;=\; b_1\, b_2,$$
$$1 \;=\; \operatorname{pgcd}\big(b_1, b_2\big).$$

Grâce au théorème de Bézout, il existe deux polynômes v_1 et v_2 de $\mathbb{K}[x]$ tels que :

$$v_2\, b_1 + v_1\, b_2 \;=\; 1,$$

et on peut multiplier cette identité par n'importe quelle expression.

Par conséquent, quel que soit le polynôme $r \in \mathbb{K}[x]$, il existe deux polynômes $u_1 = v_1\, r$ et $u_2 = v_2\, r$ tels que :

$$u_2\, b_1 + u_1\, b_2 \;=\; r. \tag{3.4}$$

On prend r avec $\deg r < \deg b_1 b_2$ comme dans l'énoncé du théorème.

Effectuons alors deux divisions euclidiennes, de u_1 par b_1, et de u_2 par b_2 :

$$\begin{aligned} u_1 &= b_1\,q_1 + r_1, & \deg r_1 &< \deg b_1, \\ u_2 &= b_2\,q_2 + r_2, & \deg r_2 &< \deg b_2. \end{aligned} \tag{3.5}$$

En remplaçant dans (3.4), il vient :

$$b_1\,b_2\,\big(q_1 + q_2\big) + r_2\,b_1 + r_1\,b_2 \;=\; r.$$

Assertion 3.6. *On a en fait :*

$$q_1 + q_2 \;=\; 0.$$

Preuve. Par l'absurde, si on avait $q_1 + q_2 \neq 0$, le degré du premier membre serait au moins égal à celui de $b_1\,b_2$, parce que :

$$\begin{aligned} \deg\, b_1b_2(q_1+q_2) &\geqslant \deg b_1 + \deg b_2, \\ \deg\big(r_2b_1 + r_1b_2\big) &\leqslant \max\big\{\deg r_2 + \deg b_1,\ \ \deg r_1 + \deg b_2\big\} \\ &< \deg b_1 + \deg b_2, \end{aligned}$$

tandis que le polynôme r du second membre est, par hypothèse, de degré strictement inférieur à celui de $b = b_1\,b_2$.

Donc $q_1 + q_2 \neq 0$ entraînerait une contradiction. □

Ainsi, on a $q_1 + q_2 = 0$, donc l'équation ci-dessus se simplifie en :

$$r_2\,b_1 + r_1\,b_2 \;=\; r,$$

d'où après division :

$$\frac{r}{b_1\,b_2} \;=\; \frac{r_1}{b_1} + \frac{r_2}{b_2},$$

toujours avec :

$$\deg r_1 \;<\; \deg b_1 \qquad \text{et} \qquad \deg r_2 \;<\; \deg b_2.$$

Assertion 3.7. *On a :*

$$\mathsf{pgcd}\,\big(r_1, b_1\big) \;=\; 1 \qquad \textit{et} \qquad 1 \;=\; \mathsf{pgcd}\,\big(r_2, b_2\big).$$

Preuve. Le raisonnement étant le même pour les deux couples, nous le faisons pour le couple (r_1, b_1).

Posons $d := \mathsf{pgcd}\,(r_1, b_1)$. Alors $d \,|\, r_1$ et $d \,|\, b_1$, et comme $b_1\,q_1 + r_1 = u_1$ d'après (3.5), il vient :

$$d \;\mid\; u_1.$$

D'après l'égalité (3.4), et comme $b = b_1\,b_2$, on a :

$$\big(\ d \mid u_1 \quad \text{et} \quad d \mid b_1\ \big) \quad \begin{matrix} \Longrightarrow \\ \Longrightarrow \end{matrix} \quad \left.\begin{matrix} d \mid r \\ d \mid b \end{matrix}\right\} \quad \Longrightarrow \quad d \;\Big|\; \mathsf{pgcd}\,(b, r).$$

Enfin, comme par hypothèse $\mathsf{pgcd}\,(b, r) = 1$, cela force $d = 1$. Ainsi, r_1 et b_1 sont bien premiers entre eux. □

Toujours dans le (long) cas $n = 2$, il reste encore à établir que la décomposition ainsi trouvée $\frac{r}{b} = \frac{r_1}{b_1} + \frac{r_2}{b_2}$ associée à la décomposition $b_1\, b_2$ de b est *unique*.

Supposons donc qu'il existe deux telles décompositions :

$$\frac{r_1}{b_1} + \frac{r_2}{b_2} \;=\; \frac{r}{b_1\, b_2} \;=\; \frac{r'_1}{b_1} + \frac{r'_2}{b_2},$$

d'où en éliminant les dénominateurs :

$$r_1\, b_2 + r_2\, b_1 \;=\; r'_1\, b_2 + r'_2\, b_1,$$

puis :

$$\big(r_1 - r'_1\big)\, b_2 \;=\; \big(r'_2 - r_2\big)\, b_1.$$

On a alors, en appliquant le théorème de Gauss :

$$\left.\begin{array}{l} b_1 \;\big|\; (r_1 - r'_1)\, b_2 \\ 1 \;=\; b_1 \wedge b_2 \end{array}\right. \qquad \Longrightarrow \qquad b_1 \;\big|\; \big(r_1 - r'_1\big).$$

Comme $\deg r_1 < \deg b_1$ et comme $\deg r'_1 < \deg b_1$, il est clair que :

$$\begin{aligned} \deg\big(r_1 - r'_1\big) \;&\leqslant\; \max\big\{\deg r_1,\, \deg r'_1\big\} \\ &<\; \deg b_1. \end{aligned}$$

Par suite :

$$\left.\begin{array}{r} \deg\,(r_1 - r'_1) \;<\; \deg b_1 \\ b_1 \;\big|\; (r_1 - r'_1) \end{array}\right\} \qquad \Longrightarrow \qquad r_1 - r'_1 \;=\; 0.$$

Enfin, l'égalité $r_1 = r'_1$ entraîne $r_2 = r'_2$, et la décomposition est donc bien unique.

Maintenant, raisonnons par récurrence sur le nombre n de facteurs dans :

$$b \;=\; b_1 \,\cdots\, b_{n-1}\, b_n.$$

Supposons donc que pour toute fraction irréductible $\frac{r}{b}$ avec $\deg r \;<\; \deg b$, où $1 \;=\; \mathsf{pgcd}\,(r, b)$, et que pour toute décomposition de $b \;=\; b_1 \,\cdots\, b_{n-1}$ en produit de $n-1$ polynômes $b_1, \ldots, b_{n-1}$ premiers entre eux deux à deux, il existe une décomposition unique :

$$\frac{r}{b} \;=\; \frac{r_1}{b_1} + \cdots + \frac{r_{n-1}}{b_{n-1}},$$

avec, pour tout $1 \leqslant i \leqslant n-1$:

$$\deg r_i \;<\; \deg b_i \qquad\qquad \text{et} \qquad\qquad 1 \;=\; \mathsf{pgcd}\,\big(r_i, b_i\big).$$

Démontrons alors le théorème visé pour toute décomposition de b en un produit $b_1 \,\cdots b_{n-1}\, b_n$ de n polynômes premiers entre eux deux à deux.

Tout d'abord, comme :

$$b \;=\; \big(b_1 \,\cdots\, b_{n-1}\big)\, b_n,$$

et comme b_n est premier avec chacun des b_i pour $1 \leqslant i \leqslant n-1$, il est aussi premier avec leur produit $b_1 \,\cdots\, b_{n-1}$.

Appliquons alors la première partie — cas $n = 2$ — de la démonstration à la décomposition de b en un produit de *deux* facteurs premiers entre eux :

$$\frac{r}{b} \;=\; \frac{c}{b_1 \,\cdots\, b_{n-1}} + \frac{r_n}{b_n},$$

avec :

$$\begin{aligned} \deg c \ &< \ \deg\big(b_1 \cdots b_{n-1}\big), \\ \deg r_n \ &< \ \deg b_n, \\ 1 \ &= \ \mathsf{pgcd}\,\big(c,\, b_1 \cdots b_{n-1}\big) \\ 1 \ &= \ \mathsf{pgcd}\,\big(r_n, b_n\big), \end{aligned}$$

cette décomposition étant unique, d'après ce que nous avons établi dans le long cas $n = 2$.

Sans aucune retenue, appliquons maintenant l'hypothèse de récurrence à la fraction :

$$\frac{c}{b_1 \cdots b_{n-1}}.$$

Grâce à notre hypothèse de récurrence, nous obtenons :

$$\frac{r}{b} \ = \ \frac{r_1}{b_1} + \cdots + \frac{r_{n-1}}{b_{n-1}} + \frac{r_n}{b_n},$$

avec, pour tout $1 \leqslant i \leqslant n$:

$$\begin{aligned} \deg r_i \ &< \ \deg b_i, \\ 1 \ &= \ \mathsf{pgcd}\,\big(r_i, b_i\big), \end{aligned}$$

et cette décomposition est unique. Le Théorème 3.3 est complètement démontré. □

Conséquence importante. Dès lors, appliquons au dénominateur b de la fraction irréductible $\frac{a}{b}$ la décomposition en *facteurs irréductibles* dans $\mathbb{K}[x]$:

$$b \ = \ p_1^{h_1}\, p_2^{h_2} \, \cdots \, p_n^{h_n},$$

avec des polynômes $p_i \in \mathbb{K}[x]$ irréductibles et avec des exposants entiers $h_i \geqslant 1$. Nous savons que cette décomposition est unique, à l'ordre près.

Ensuite, pour tous indices distincts $1 \leqslant i_1 \neq i_2 \leqslant n$, puisque p_{i_1} et p_{i_2} sont irréductibles et distincts, donc premiers entre eux, nous pouvons donc appliquer le Théorème 3.3 à la décomposition :

$$b \ = \ \underbrace{p_1^{h_1}}_{b_1}\, \underbrace{p_2^{h_2}}_{b_2} \, \cdots \, \underbrace{p_n^{h_n}}_{b_n},$$

et obtenir une décomposition unique :

$$\frac{a}{b} \ = \ q + \frac{r_1}{p_1^{h_1}} + \frac{r_2}{p_2^{h_2}} + \cdots + \frac{r_n}{p_n^{h_n}},$$

où q est la partie entière de $\frac{a}{b}$, avec certains polynômes $r_i \in \mathbb{K}[x]$ tels que :

$$\deg r_i \ < \ \deg p_i^{h_i} \qquad (1 \leqslant i \leqslant n).$$

4. Décomposition d'une fraction rationnelle sur un corps commutatif $\mathbb{K}$

Nous allons poursuivre la décomposition sur chacune des fractions du type :

$$\frac{r}{p^h}, \qquad \text{avec} \qquad \deg r \ < \ \deg p^h.$$

Par construction dans les raisonnements qui précèdent, on a $r \wedge p^h = 1$ premiers entre eux. Le point-clé, c'est que les fractions du type $\frac{r}{p^h}$ où p est irréductible peuvent encore être grandement simplifiées. De plus, l'énoncé suivant est plus général, car il ne requiert *pas*, dans ses hypothèses, que $r \wedge p^h = 1$.

Proposition 4.1. *Dans $F_{\mathbb{K}}[x]$, toute fraction rationnelle irréductible $\frac{r}{p^h}$ avec $\deg r < \deg p^h$, et $p \in \mathbb{K}[x]$ irréductible, peut se décomposer de manière unique comme :*

$$\frac{r}{p^h} \;=\; \frac{\tau_h}{p^h} + \frac{\tau_{h-1}}{p^{h-1}} + \cdots + \frac{\tau_1}{p^1},$$

avec des polynômes τ_i satisfaisant :

$$\deg \tau_i \;<\; \deg p \qquad (1 \leqslant i \leqslant h).$$

Contrairement à ce qu'on pourrait imaginer, le numérateur τ_i dans la fraction $\frac{\tau_i}{p^i}$ n'est pas de degré $< \deg p^i$, mais beaucoup mieux, l'énoncé affirme que $\deg \tau_i < \deg p$, indépendamment de l'indice $1 \leqslant i \leqslant h$. En particulier, puisque p est irréductible, cela garantit que :

$$1 \;=\; \tau_i \wedge p \qquad (1 \leqslant i \leqslant h).$$

Démonstration. La propriété est manifeste pour $h = 1$.

Ensuite, raisonnons par récurrence sur $h \geqslant 2$. Supposons la propriété vraie au niveau $h-1$, c'est-à-dire que toute fraction rationnelle irréductible :

$$\frac{q}{p^{h-1}}, \qquad \text{avec} \qquad \deg q \;<\; \deg p^{h-1},$$

se décompose de manière *unique* comme :

$$\frac{q}{p^{h-1}} \;=\; \frac{\tau_{h-1}}{p^{h-1}} + \cdots + \frac{\tau_1}{p},$$

avec des polynômes $\tau_{h-1}, \ldots, \tau_1$ de $\mathbb{K}[x]$ de degrés :

$$\deg \tau_i \;<\; \deg p \qquad (1 \leqslant i \leqslant h-1),$$

et proposons-nous d'établir la même propriété au niveau h, c'est-à-dire pour toute fraction irréductible $\frac{r}{p^h}$.

Effectuons alors la division euclidienne dans $\mathbb{K}[x]$ de r par p :

$$r \;=\; p\,q + \tau_h, \qquad \deg \tau_h \;<\; \deg p,$$

puis, divisons les deux membres de cette équation par p^h, ce qui donne dans $F_{\mathbb{K}}[x]$:

$$\frac{r}{p^h} \;=\; \frac{q}{p^{h-1}} + \frac{\tau_h}{p^h}.$$

Cette décomposition est unique, grâce à l'unicité de la division euclidienne dans $\mathbb{K}[x]$.

Pour terminer, il suffit alors d'appliquer l'hypothèse de récurrence à la fraction :

$$\frac{q}{p^{h-1}} \;=\; \frac{\tau_{h-1}}{p^{h-1}} + \cdots + \frac{\tau_1}{p},$$

et d'additionner pour conclure :

$$\frac{r}{p^h} \;=\; \frac{\tau_{h-1}}{p^{h-1}} + \cdots + \frac{\tau_1}{p} + \frac{\tau_h}{p^h}. \qquad \square$$

Nous pouvons maintenant *enfin* présenter la décomposition générale en éléments simples d'une fraction rationnelle irréductible arbitraire $\frac{a}{b} \in F_{\mathbb{K}}[x]$, en synthétisant le Théorème 3.3 et la Proposition 4.1.

Théorème 4.2. *Toute fraction rationnelle irréductible $\frac{a}{b} \in F_{\mathbb{K}}[x]$ à coefficients dans un corps commutatif $\mathbb{K}$, dont le dénominateur est décomposé en composantes irréductibles :*

$$b = p_1^{h_1}\, p_2^{h_2} \, \cdots \, p_n^{h_n},$$

se décompose de manière unique en une somme de la forme :

$$\begin{aligned} \frac{a}{p_1^{h_1} p_2^{h_2} \cdots p_n^{h_n}} &= q + \frac{\alpha_{h_1}}{p_1^{h_1}} + \frac{\alpha_{h_1-1}}{p_1^{h_1-1}} + \cdots + \frac{\alpha_1}{p_1} && \deg \alpha_i < \deg p_1 \\ &\quad + \frac{\beta_{h_2}}{p_2^{h_2}} + \frac{\beta_{h_2-1}}{p_2^{h_2-1}} + \cdots + \frac{\beta_1}{p_2} && \deg \beta_i < \deg p_2 \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\quad + \frac{\lambda_{h_n}}{p_n^{h_n}} + \frac{\lambda_{h_n-1}}{p_n^{h_n-1}} + \cdots + \frac{\lambda_1}{p_n} && \deg \lambda_i < \deg p_n, \end{aligned}$$

où q est la partie entière. □

Terminologie 4.3. Toute fraction rationnelle $\frac{\tau}{p^h}$ avec $\deg \tau < \deg p$ donc $1 = \tau \wedge p$, et p irréductible dans $\mathbb{K}[x]$, se nomme *élément simple* dans $F_{\mathbb{K}}[x]$.

Lorsqu'on a déterminé une somme du type de celle du Théorème 4.2, on dit que l'on a *décomposé la fraction $\frac{a}{b}$ en éléments simples*.

Exemple 4.4. Soit l'anneau quotient $\mathbb{Z}/5\mathbb{Z}$, qui est un corps car 5 est premier. On écrit :

$$\mathbb{Z}/5\mathbb{Z} = \big\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\big\},$$

où la barre au-dessus d'un entier signifie sa classe résiduelle modulo 5.

Sur ce corps, proposons-nous de décomposer en éléments simples la fraction :

$$\frac{x - \overline{1}}{(x + \overline{1})^2\,(x + \overline{2})}.$$

D'après le Théorème 4.2 que nous venons de démontrer, il doit exister des constantes a, b, c de $\mathbb{Z}/5\mathbb{Z}$ telles que :

$$\frac{x - \overline{1}}{(x + \overline{1})^2\,(x + \overline{2})} = \frac{a}{(x + \overline{1})^2} + \frac{b}{x + \overline{1}} + \frac{c}{x + \overline{2}}.$$

Éliminons le dénominateur pour obtenir l'identité :

$$x - \overline{1} = a\,(x + \overline{2}) + b\,(x + \overline{1})\,(x + \overline{2}) + c\,(x + \overline{1})^2.$$

En faisant $x := -\,\overline{1}$, il vient :

$$-\,\overline{2} = a\,\overline{1} + \overline{0} + \overline{0}, \qquad \text{c'est-à-dire} \qquad a = \overline{3}.$$

En faisant $x := -\,\overline{2}$, il vient :

$$-\,\overline{3} = 0 + 0 + c\,(-\overline{1})^2, \qquad \text{c'est-à-dire} \qquad c = \overline{2}.$$

Remplaçons ces deux valeurs dans notre identité et développons :

$$\begin{aligned} x - \overline{1} &= \overline{3}\,x + \overline{6} + b\,\big(x^2 + \overline{3}\,x + \overline{2}\big) + \overline{2}\,x^2 + \overline{4}\,x + \overline{2} \\ &= x^2\,\big(b + \overline{2}\big) + x\,\big(\overline{3} + \overline{3}\,b + \overline{4}\big) + \overline{1} + \overline{2}\,b + \overline{2}, \end{aligned}$$

donc $b = \overline{3}$ nécessairement pour annuler le coefficient de x^2, et on vérifie alors qu'avec ces trois valeurs trouvées pour a, b, c, cette équation est identiquement satifaite.

En conclusion, nous avons établi la décomposition :

$$\frac{x-\overline{1}}{(x+\overline{1})^2\,(x+\overline{2})} \;=\; \frac{\overline{3}}{(x+\overline{1})^2} + \frac{\overline{3}}{x+\overline{1}} + \frac{\overline{2}}{x+\overline{2}}.$$

5. Décomposition sur le corps des nombres complexes

Nous savons que le corps $\mathbb{C}$ des nombres complexes est algébriquement clos, c'est-à-dire que tout polynôme irréductible dans $\mathbb{C}[x]$ est de degré 1, de la forme $x-\alpha$.

Pour tout polynôme $b \in \mathbb{C}[x]$, nous savons aussi que sa décomposition en facteurs irréductibles est du type :

$$b \;=\; \beta\,\big(x-\alpha_1\big)^{h_1}\,\big(x-\alpha_2\big)^{h_2}\,\cdots\,\big(x-\alpha_n\big)^{h_n},$$

avec $\beta \in \mathbb{C}\backslash\{0\}$ *non nul* égal au coefficient du monôme de tête de b, et avec, pour tout indice $1 \leqslant i \leqslant h$:

$$\alpha_i \in \mathbb{C}, \qquad\qquad h_i \geqslant 1.$$

De plus, soit comme précédemment $a(x) \in \mathbb{C}[x]$.

Terminologie 5.1. Les zéros α_i du dénominateur de la fraction rationnelle :

$$\frac{a}{b} \;=\; \frac{a}{\beta\,(x-\alpha_1)^{h_1}\,(x-\alpha_2)^{h_2}\,\cdots\,(x-\alpha_n)^{h_n}},$$

sont appelés *pôles* de la fraction $\frac{a}{b}$.

L'ordre de multiplicité h_i du zéro α_i de b est appelé *ordre* du pôle α_i de la fraction $\frac{a}{b}$.

Tout *élément simple* dans $F_{\mathbb{C}}[x]$ est donc du type :

$$\frac{\lambda}{(x-\alpha)^k},$$

où $\lambda, \alpha \in \mathbb{C}$ sont des constantes complexes, et où $m \geqslant 1$ est un entier naturel.

D'après le Théorème 4.2, la décomposition en éléments simples d'une fraction rationnelle $\frac{a}{b} \in F_{\mathbb{C}}[x]$ est, en général, le résultat de l'addition de sa partie entière — un polynôme dans $\mathbb{K}[x]$ — et d'un nombre fini de sommes du type :

$$\frac{\lambda_h}{(x-\alpha)^h} + \frac{\lambda_{h-1}}{(x-\alpha)^{h-1}} + \cdots + \frac{\lambda_1}{x-\alpha},$$

où α est un pôle d'ordre h de la fraction $\frac{a}{b}$.

Terminologie 5.2. Une telle somme d'éléments simples se nomme *partie principale relative au pôle* α.

Enfin, voici l'énoncé explicite complet.

Théorème 5.3. *Dans $F_{\mathbb{C}}[x]$, soit une fraction irréductible $\frac{a}{b}$ de partie entière q :*

$$\frac{a}{b} \;=\; q + \frac{r}{b}, \qquad\qquad \deg b \;<\; \deg b,$$

et soit la factorisation du dénominateur en polynômes du premier degré :

$$b \;=\; \lambda\,\big(x-\alpha_1\big)^{h_1}\,\big(x-\alpha_2\big)^{h_2}\,\cdots\,\big(x-\alpha_n\big)^{h_n},$$

avec des $\alpha_i \in \mathbb{C}$ distincts deux à deux et des exposants $h_i \geqslant 1$.

Alors il existe des constantes uniques $\boldsymbol{a}_j^i \in \mathbb{C}$ *telles que :*

$$\begin{aligned}\frac{a}{\lambda\,(x-\alpha_1)^{h_1}\cdots(x-\alpha_n)^{h_n}} \;=\; q &+ \frac{\boldsymbol{a}_1^{h_1}}{(x-\alpha_1)^{h_1}} + \frac{\boldsymbol{a}_1^{h_1-1}}{(x-\alpha_1)^{h_1-1}} + \cdots + \frac{\boldsymbol{a}_1^1}{x-\alpha_1} \\ &+ \frac{\boldsymbol{a}_2^{h_2}}{(x-\alpha_2)^{h_2}} + \frac{\boldsymbol{a}_2^{h_2-1}}{(x-\alpha_2)^{h_2-1}} + \cdots + \frac{\boldsymbol{a}_2^1}{x-\alpha_2} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &+ \frac{\boldsymbol{a}_n^{h_n}}{(x-\alpha_n)^{h_n}} + \frac{\boldsymbol{a}_n^{h_n-1}}{(x-\alpha_n)^{h_n-1}} + \cdots + \frac{\boldsymbol{a}_n^1}{x-\alpha_n}. \qquad \square\end{aligned}$$

Mais alors, comment effectuer la détermination pratique de ces constantes $\boldsymbol{a}_j^i$?

Pour obtenir pratiquement cette partie principale, toujours avec α égal à un α_i parmi $\alpha_1, \alpha_2, \ldots, \alpha_n$, commençons par écrire :

$$\frac{a(x)}{b(x)} \;=\; \frac{a(x)}{(x-\alpha_i)^{h_i}\,\big[\underbrace{(x-\alpha_1)^{h_1}\cdots(x-\alpha_{i-1})^{h_{i-1}}(x-\alpha_{i+1})^{h_{i+1}}\cdots(x-\alpha_n)^{h_n}}_{=:\,c(x)}\big]},$$

c'est-à-dire :

$$\frac{a(x)}{b(x)} \;=\; \frac{a(x)}{(x-\alpha_i)^h\,c_i(x)},$$

où $c_i(x)$ est un polynôme satisfaisant :

$$0 \;\neq\; c_i(\alpha_i).$$

En supprimant l'indice i, notons simplement :

$$\frac{a(x)}{b(x)} \;=\; \frac{a(x)}{(x-\alpha)^h\,c(x)}, \qquad\qquad c(\alpha) \;\neq\; 0.$$

Prenons alors le polynôme $x-\alpha$ comme nouvelle indéterminée y en posant :

$$y \;:=\; x-\alpha.$$

Après cette substitution, $a(x)$ devient un polynôme $\widetilde{a}(y)$, tandis que $c(x)$ devient un polynôme $\widetilde{c}(y)$, et notre fraction $\frac{a}{b}$ devient :

$$\frac{a(x)}{b(x)} \;=\; \frac{\widetilde{a}(y)}{y^h\,\widetilde{c}(y)},$$

avec :

$$0 \;\neq\; c(\alpha) \;=\; \widetilde{c}(0).$$

Maintenant, nous avons besoin d'un énoncé que nous admettrons, mais dont la démonstration est très analogue à la division euclidienne dans $\mathbb{K}[y]$.

Tout d'abord, rappelons que la *valuation* d'un polynôme $c(y) \in \mathbb{K}[y]^*$ non nul écrit comme $c(y) = c_0 + c_1\,y + c_2\,y^2 + \cdots$ — la somme étant bien sûr finie — est l'entier :

$$\mathsf{val}\,c \;:=\; \mathsf{min}\,\big\{i \in \mathbb{N}\colon\; c_i \neq 0\big\}.$$

Si on abrège :

$$\nu \;:=\; \mathsf{val}\,c,$$

il est alors clair que :

$$c(y) \;=\; c_\nu\,y^\nu + c_{\nu+1}\,y^{\nu+1} + \cdots,$$

ce qui montre notamment que $c(y)$ est factorisable par y^ν.

Avant de poursuivre, présentons alors un résultat de *division selon les puissances croissantes*, utile sur le plan théorique, mais dont nous n'aurons quasiment pas besoin dans la pratique des calculs en séance de TD ou en examen.

Théorème 5.4. [Admis] *Soient deux polynômes $a, c \in \mathbb{K}[y]$. On suppose $c(0) \neq 0$, c'est-à-dire que $\mathsf{val}\, c = 0$. Alors étant donné un entier quelconque fixé $k \geqslant 0$, il existe un unique couple de polynômes (q, r) de $\mathbb{K}[y]$ tels que :*

$$\begin{aligned} a &= q\,c + r, \\ \mathsf{deg}\, q &\leqslant k, \\ k &< \mathsf{val}\, r. \end{aligned}$$

□

Exemple 5.5. Divisons jusqu'à l'ordre $k = 3 = \mathsf{deg}\, q$ le polynôme $a(y)$ par le polynôme $c(y)$, où :

$$a(y) := 2 + 4\,y^2 + y^3, \qquad\qquad c(y) := 1 + 2\,y + 3\,y^2,$$

en appliquant une méthode intuitivement claire, ce qui nous donne :

$$\begin{array}{rl|l}
2 + & 4\,y^2 + y^3 & \underline{1 + 2\,y + 3\,y^2} \\
\underline{-\,2 - 4\,y - 6\,y^2} & & 2 \\
-\,4\,y - 2\,y^2 + y^3 & & \\
\underline{4\,y + 8\,y^2 + 12\,y^3} & & -\,4\,y \\
6\,y^2 + 13\,y^3 & & \\
\underline{-\,6\,y^2 - 12\,y^3 - 18\,y^4} & & 6\,y^2 \\
y^3 - 18\,y^4 & & \\
\underline{-\,y^3 - 2\,y^4 - 3\,y^5} & & y^3 \\
\boxed{-\,20\,y^4 - 3\,y^5} & & \\
 & & \hline \\
 & & \boxed{2 - 4\,y + 6\,y^2 + y^3}
\end{array}$$

c'est-à-dire :

$$\overbrace{2 + 4\,y^2 + y^3}^{=\,a} = \big(\overbrace{2 - 4\,y + 6\,y^2 + y^3}^{=:\,q}\big)\big(\overbrace{1 + 2\,y + 3\,y^2}^{=\,c}\big) + \overbrace{-20\,y^4 - 3\,y^5}^{=:\,r}.$$

Revenons à nos considérations, c'est-à-dire à notre fraction :

$$\frac{a(x)}{b(x)} = \frac{\widetilde{a}(y)}{y^h\,\widetilde{c}(y)}, \qquad\qquad \text{avec} \qquad\qquad \widetilde{c}(0) \neq 0.$$

Puisque $\widetilde{c}(0) \neq 0$, nous pouvons alors appliquer le Théorème 5.4 avec l'entier $k := h - 1$, c'est-à-dire, effectuer la division de $\widetilde{a}(y)$ par $\widetilde{c}(y)$ selon les puissances croissantes jusqu'à l'ordre $h - 1$, ce qui nous donne :

$$\widetilde{a}(y) = \big[\lambda_h + y\,\lambda_{h-1} + \cdots + y^{h-1}\,\lambda_1\big]\,\widetilde{c}(y) + y^h\,d(y), \tag{5.6}$$

les nombres λ_i étant les coefficients du quotient $q(y)$, et $y^h\,d(y) = r(y)$ étant le reste, de valuation $\mathsf{val}\, r > h - 1$, c'est-à-dire $\mathsf{val}\, r \geqslant h$, donc factorisable par y^h.

Dans $F_{\mathbb{C}}[y]$, nous obtenons alors :

$$\frac{\widetilde{a}(y)}{y^h\,\widetilde{c}(y)} = \frac{\lambda_h}{y^h} + \frac{\lambda_{h-1}}{y^{h-1}} + \cdots + \frac{\lambda_1}{y} + \frac{d(y)}{\widetilde{c}(y)},$$

et comme $\widetilde{c}(y) \neq 0$, la partie « unicité » du Théorème 4.2 montre que la somme :

$$\frac{\lambda_h}{y^h} + \frac{\lambda_{h-1}}{y^{h-1}} + \cdots + \frac{\lambda_1}{y}$$

est la partie principale relative au pôle zéro d'ordre h de :

$$\frac{\widetilde{a}(y)}{y^h\,\widetilde{c}(y)}.$$

En conclusion, les constantes $\lambda_1, \ldots, \lambda_h$ ainsi déterminées sont les coefficients de la partie principale relative au pôle α de la fraction $\frac{a}{b} \in F_{\mathbb{C}}[x]$.

Dans la relation (5.6), en remplaçant y par 0, il vient :

$$\widetilde{a}(0) \;=\; \lambda_h\,\widetilde{c}(0),$$

d'où :

$$\lambda_h \;=\; \frac{\widetilde{a}(0)}{\widetilde{c}(0)} \;=\; \frac{a(\alpha)}{c(\alpha)},$$

relation qui donne le coefficient de l'élément simple de plus haut degré relatif au pôle α.

Notons que la relation (5.6) est valable en particulier si $h = 1$, c'est-à-dire dans le cas d'un *pôle simple*, de sorte que la formule :

$$\lambda_1 \;=\; \lambda_h \;=\; \frac{\widetilde{a}(\alpha)}{\widetilde{c}(\alpha)},$$

détermine dans ce cas l'unique élément simple de la partie principale relative à un pôle simple.

Toujours dans le cas d'un pôle simple, il existe une formule équivalente et particulièrement pratique.

En effet, si la fraction $\frac{a}{b}$ possède un pôle simple α, avec donc :

$$b(x) \;=\; (x-\alpha)\,c(x), \qquad\qquad 0 \;\neq\; c(\alpha),$$

en prenant les dérivées, on trouve :

$$b'(x) \;=\; c(x) + (x-\alpha)\,c'(x),$$

d'où :

$$b'(\alpha) \;=\; c(\alpha).$$

Pour le coefficient relatif au pôle simple α, on a donc une formule très pratique, que nous mettons en exergue.

Proposition 5.7. *Soient deux polynômes $a \in \mathbb{K}[x]$ quelconque et $b \in \mathbb{K}[x]^*$ non nul. Si $\alpha \in \mathbb{K}$ est un zéro d'ordre 1 de b :*

$$b(\alpha) \;=\; 0 \;\neq\; b'(\alpha),$$

alors l'unique coefficient λ dans la partie concernant α du développement en élément simples :

$$\frac{a(x)}{b(x)} \;=\; \frac{\lambda}{x-\alpha} + \cdots,$$

est donné par la formule :

$$\lambda \;=\; \frac{a(\alpha)}{b'(\alpha)}.$$

□

Exemple 5.8. Dans $F_{\mathbb{C}}[x]$, proposons-nous de décomposer :

$$\frac{1}{x^3-1}.$$

Le degré du numérateur étant strictement inférieur à celui du dénominateur, la partie entière de la décomposition est nulle.

D'autre part, la décomposition en facteurs irréductibles du dénominateur est :

$$x^3-1 \;=\; (x-1)\,(x-j)\,(x-j^2),$$

où $j = e^{2i\pi/3}$.

Comme chacune de ces trois racines 1, j, $j^2 = \overline{j}$, est un pôle simple, on doit avoir une décomposition du type :

$$\frac{1}{x^3-1} \;=\; \frac{\lambda}{x-1} + \frac{\mu}{x-j} + \frac{\nu}{x-\overline{j}}.$$

Or puisque :

$$b(x) \;=\; x^3-1 \qquad\qquad \Longrightarrow \qquad\qquad b'(x) \;=\; 3\,x^2,$$

la Proposition 5.7 donne immédiatement :

$$\lambda \;=\; \frac{1}{3}, \qquad \mu \;=\; \frac{1}{3\,j^2} \;=\; \frac{1}{3}\,j, \qquad \nu \;=\; \frac{1}{3\,\overline{j}^2} \;=\; \frac{1}{3}\,\overline{j},$$

donc la décomposition recherchée est :

$$\frac{1}{x^3-1} \;=\; \frac{1}{3}\left[\frac{1}{x-1} + \frac{j}{x-j} + \frac{\overline{j}}{x-\overline{j}}\right].$$

Exemple 5.9. Proposons-nous de décomposer dans $F_{\mathbb{C}}[x]$ la fraction :

$$\frac{4}{(x^2+1)^2}.$$

La partie entière de la décomposition en éléments simples est nulle.

La décomposition en facteurs irréductibles dans $\mathbb{C}[x]$ du dénominateur est :

$$\big(x^2+1\big)^2 \;=\; (x+i)^2\,(x-i)^2.$$

On doit donc avoir une décomposition en éléments simples du type :

$$\frac{4}{(x^2+1)^2} \;=\; \frac{\lambda_2}{(x-i)^2} + \frac{\lambda_1}{x-i} + \frac{\mu_2}{(x+i)^2} + \frac{\mu_1}{x+i}.$$

Or comme la fraction proposée appartient plus précisément à $F_{\mathbb{R}}[x]$, puisque ses coefficient sont réels, on doit avoir :

$$\mu_2 \;=\; \overline{\lambda}_2, \qquad\qquad \mu_1 \;=\; \overline{\lambda}_1,$$

et donc, il nous suffit de déterminer seulement λ_2, λ_1.

Pour cela, comme nous l'avons exposé dans le cas général, introduisons l'indéterminée nouvelle :

$$y \;:=\; x-i,$$

ce qui transforme la fraction proposée en :

$$\frac{4}{y^2\,(y+2\,i)^2} \;=\; \frac{4}{y^2\,\big(-\,4+4\,i\,y+y^2\big)}.$$

D'après la théorie générale que nous avons développée, nous devons alors diviser $\widetilde{a}(y)$ par $\widetilde{c}(y)$, où :

$$\widetilde{a}(y) \,=\, 4, \qquad\qquad \widetilde{c}(y) \,:=\, -\,4 + 4\,i\,y + y^2,$$

la condition $\widetilde{c}(0) \neq 0$ étant satisfaite, ce qui nous donne :

$$\begin{array}{r|l}
4 & -\,4 + 4\,i\,y + y^2 \\
\cline{1-1}
-\,4 + 4\,i\,y + y^2 & -\,1 \\
\cline{1-1}
4\,i\,y + y^2 & \\
-\,4\,i\,y - 4\,y^2 + i\,y^3 & \quad -\,i\,y \\
\cline{1-1}
\boxed{-\,3\,y^2 + i\,y^3} & \\
 & \cline{2-2} \\
 & \boxed{-\,1 - i\,y}
\end{array}$$

c'est-à-dire :

$$4 \,=\, \big(-\,1 - i\,y\big)\,\big(-\,4 + 4\,i\,y + y^2\big) - 3\,y^2 + i\,y^3,$$

d'où après division :

$$\frac{4}{y^2\,\big(-\,4 + 4\,i\,y + y^2\big)} \,=\, -\,\frac{1}{y^2} - \frac{i}{y} + \underbrace{\frac{-\,3 + i\,y}{-\,4 + 4\,i\,y + y^2}}_{\text{Reste}},$$

ce qui donne les valeurs des deux constantes :

$$\lambda_2 \,=\, -\,1, \qquad\qquad \lambda_1 \,=\, -\,i.$$

En conclusion, la décomposition recherché est :

$$\frac{4}{(x^2+1)^2} \,=\, \frac{-\,1}{(x-i)^2} + \frac{-\,i}{x-i} + \frac{-\,1}{(x+i)^2} + \frac{i}{x+i}.$$

6. Décomposition sur le corps des nombres réels

Nous savons que le corps $\mathbb{R}$ des nombres réels n'est pas algébriquement clos, et que les polynômes irréductibles dans $\mathbb{R}[x]$ sont de deux types.

- Tout polynôme $x + a$ du premier degré.
- Tout polynôme du second degré $x^2 + b\,x + c$ dont le discriminant $b^2 - 4\,c \,<\, 0$ est strictement négatif, de telle sorte qu'aucune de ses racines n'est réelle.

Dans $F_{\mathbb{R}}[x]$, il y a donc deux sortes d'éléments simples.

☐ Les éléments simples dits *de première espèce*, du type :

$$\frac{\tau}{(x+a)^h}$$

$$(\tau \in \mathbb{R},\ a \in \mathbb{R},\ h \geqslant 1).$$

☐ Les éléments simples dits *de deuxième espèce*, du type :

$$\frac{\mu\,x + \nu}{\big(x^2 + b\,x + c\big)^h}$$

$$(\mu \in \mathbb{R},\ \nu \in \mathbb{R},\ b \in \mathbb{R},\ c \in \mathbb{R},\ b^2 - 4\,c < 0,\ h \geqslant 1).$$

Enfin, voici l'énoncé explicite complet.

Théorème 6.1. *Dans $F_{\mathbb{R}}[x]$, soit une fraction irréductible $\frac{a}{b}$ de partie entière q :*

$$\frac{a}{b} \,=\, q + \frac{r}{b}, \qquad\qquad \deg b \,<\, \deg b,$$

et soit la factorisation du dénominateur en puissances de polynômes irréductibles réels du premier degré et du second degrés distincts deux à deux :

$$b \,=\, \lambda \prod_{i=1}^{r} \big(x + a_i\big)^{g_i} \prod_{j=1}^{s} \big(x^2 + b_j\, x + c_j\big)^{h_j},$$

avec des exposants $g_i \geqslant 1$ et $h_j \geqslant 1$.

Alors il existe des constantes uniques $\tau_i^{g_i'} \in \mathbb{R}$ ainsi que $\mu_j^{h_j'} \in \mathbb{R}$ et $\nu_j^{h_j'} \in \mathbb{R}$ telles que :

$$\frac{a}{\lambda \prod_{i=1}^{r} \big(x + a_i\big)^{g_i} \prod_{j=1}^{s} \big(x^2 + b_j\, x + c_j\big)^{h_j}} \,=$$

$$= \, q + \sum_{i=1}^{r} \sum_{1 \leqslant g_i' \leqslant g_i} \frac{\tau_i^{g_i'}}{(x + a_i)^{g_i'}} + \sum_{j=1}^{s} \sum_{1 \leqslant h_j' \leqslant h_j} \frac{\mu_j^{h_j'} + \nu_j^{h_j'}\, x}{\big(x^2 + b_j\, x + c_j\big)^{h_j'}}. \qquad \square$$

Pour commencer, expliquons comment déterminer les éléments de première espèce dans la décomposition en éléments simples d'une fraction rationnelle donnée. En fait, tout ce qui a été dit et développé pour la décomposition dans $F_{\mathbb{C}}[x]$ s'applique *mutatis mutandis*, presque sans modification, aux éléments simples dans $F_{\mathbb{R}}[x]$ qui sont de première espèce. Rien de tel qu'un tout petit exemplounet pour s'en convaincre.

Exemple 6.2. Proposons-nous de décomposer dans $F_{\mathbb{R}}[x]$ la fraction :

$$\frac{4}{(x^2-1)^2}.$$

La partie entière de la décomposition en éléments simples est nulle.

La décomposition en facteurs irréductibles dans $\mathbb{R}[x]$ du dénominateur est :

$$\big(x^2 - 1\big)^2 \,=\, (x-1)^2\,(x+1)^2.$$

On doit donc avoir une décomposition en éléments simples du type :

$$\frac{4}{(x^2-1)^2} \,=\, \frac{\lambda_2}{(x-1)^2} + \frac{\lambda_1}{x-1} + \frac{\mu_2}{(x+1)^2} + \frac{\mu_1}{x+1}.$$

Or comme la fraction proposée à gauche est *paire*, c'est-à-dire qu'elle reste invariante quand on remplace $x \longmapsto -x$, ce qui donne à droite :

$$\frac{4}{(x^2-1)^2} \,=\, \frac{\lambda_2}{(x+1)^2} - \frac{\lambda_1}{x+1} + \frac{\mu_2}{(x-1)^2} - \frac{\mu_1}{x-1},$$

on en déduit par identification et par unicité de la décomposition que :

$$\mu_2 \,=\, \lambda_2, \qquad\qquad \mu_1 \,=\, -\,\lambda_1,$$

et donc, il nous suffit de déterminer seulement λ_2, λ_1.

Pour cela, comme nous l'avons exposé dans le cas général, introduisons l'indéterminée nouvelle :

$$y \,:=\, x - 1,$$

ce qui transforme la fraction proposée en :

$$\frac{4}{y^2\,(y+2)^2} \;=\; \frac{4}{y^2\,\big(4+4\,y+y^2\big)}.$$

D'après la théorie générale que nous avons développée, nous devons alors diviser $\widetilde{a}(y)$ par $\widetilde{c}(y)$, où :

$$\widetilde{a}(y) \;=\; 4, \qquad\qquad \widetilde{c}(y) \;:=\; 4+4\,y+y^2,$$

la condition $\widetilde{c}(0) \neq 0$ étant satisfaite, ce qui nous donne :

$$\begin{array}{r|l}
4 & 4+4\,y+y^2 \\
\cline{2-2}
-\,4-4\,y-y^2 & 1 \\
\cline{1-1}
\quad -\,4\,y-y^2 & \\
\quad\;\; 4\,y+4\,y^2+y^3 & \quad -\,y \\
\cline{1-1}
\quad\;\; \boxed{3\,y^2+y^3} & \\
\cline{2-2}
 & \boxed{1-y}
\end{array}$$

c'est-à-dire :

$$4 \;=\; \big(1-y\big)\,\big(4+4\,y+y^2\big) + 3\,y^2 + y^3,$$

d'où après division :

$$\frac{4}{y^2\,\big(4+4\,y+y^2\big)} \;=\; \frac{1}{y^2} - \frac{1}{y} + \underbrace{\frac{3+y}{4+4\,y+y^2}}_{\text{Reste}},$$

ce qui donne les valeurs des deux constantes :

$$\lambda_2 \;=\; 1, \qquad\qquad \lambda_1 \;=\; -\,1.$$

En conclusion, la décomposition recherché est :

$$\frac{4}{(x^2-1)^2} \;=\; \frac{1}{(x-1)^2} + \frac{-\,1}{x-1} + \frac{1}{(x+1)^2} + \frac{1}{x+1}.$$

Ensuite, expliquons comment déterminer les éléments de *deuxième* espèce dans la décomposition en éléments simples d'une fraction rationnelle donnée. Là, c'est plus « corsé ».

Avant d'essayer d'ingurgiter le cas général, étudions le cas où le dénominateur b de la fraction proposée $\frac{a}{b}$ n'a qu'un seul diviseur irréductible, supposé de degré 2, c'est-à-dire, supposons que :

$$b \;=\; \big(x^2+b\,x+c\big)^h,$$

toujours avec $b^2 - 4\,c \,<\, 0$. Nous pouvons alors appliquer la Proposition 4.1 et effectuer les *divisions euclidiennes successives* qui étaient utilisées dans la démonstration de cette proposition. Encore une fois, rien ne surpassera un exemple parlant.

Exemple 6.3. Proposons-nous de décomposer en éléments simples la fraction :

$$\frac{x^5+2}{(x^2+x+1)^3}.$$

Notons que le degré, 5, du numérateur, est strictement inférieur au degré, 6, du dénominateur. Donc la partie entière est nulle.

Effectuons la division euclidienne du numérateur par le dénominateur x^2+x+1 :

$$x^5+2 \;=\; \big(x^2+x+1\big)\,\big(x^3-x^2+1\big) - x + 1,$$

puis divisons sans vergogne pour obtenir dans $F_{\mathbb{R}}[x]$:

$$\frac{x^5+2}{(x^2+x+1)^3} \;=\; \frac{x^3-x^2+1}{(x^2+x+1)^2} + \frac{-x+1}{(x^2+x+1)^3},$$

la dernière fraction à droite étant un élément de seconde espèce.

Réitérons l'euclidivopération avec la fraction restante, c'est-à-dire, ré-effectuons la division euclidienne du quotient par le même diviseur :

$$x^3-x^2+1 \;=\; \big(x^2+x+1\big)\,(x-2) + x + 3.$$

C'est fini — déjà ? snif ! —, car nous obtenons la décomposition recherchée :

$$\frac{x^5+2}{(x^2+x+1)^3} \;=\; \frac{x-2}{x^2+x+1} + \frac{x+3}{(x^2+x+1)^2} + \frac{-x+1}{(x^2+x+1)^3}.$$

Étudions maintenant le cas général où le dénominateur b de la fraction proposé $\frac{a}{b}$ à coefficients dans $\mathbb{R}$ possède plusieurs diviseurs irréductibles distincts, dont l'un au moins est de degré 2. Supposons donc que :

$$b(x) \;=\; \big[(x-\alpha)^2+\beta^2\big]^h\, c(x),$$

avec $\alpha\in\mathbb{R}$ et $\beta\in\mathbb{R}^*$ ***non nul***, où $c(x)$ n'admet pas le diviseur $(x-\alpha)^2+\beta^2$, irréductible dans $\mathbb{R}[x]$.

D'après la théorie de la décomposition en éléments simples, il existe un polynôme $p(x)\in\mathbb{R}[x]$ et deux nombres réels $\lambda_h,\mu_h\in\mathbb{R}$, tels que :

$$\frac{a(x)}{b(x)} \;=\; \frac{\lambda_h\,x+\mu_h}{\big[(x-\alpha)^2+\beta^2\big]^h} + \frac{p(x)}{\big[(x-\alpha)^2+\beta^2\big]^{h-1}\,c(x)}.$$

En multipliant par $b(x)$ les deux membres de cette égalité, il vient :

$$a(x) \;=\; \big(\lambda_h\,x+\mu_h\big)\,c(x) + \big[(x-\alpha)^2+\beta^2\big]\,p(x).$$

Ensuite, remplaçons x par $\alpha+i\,\beta$, divisons par $c(\alpha+i\,\beta)\neq 0$, abrégeons :

$$\gamma \;:=\; \frac{a(\alpha+i\,\beta)}{c(\alpha+i\,\beta)} \;=\; \lambda_h\,(\alpha+i\,\beta)+\mu_h+0,$$

et écrivons aussi l'équation conjuguée :

$$\begin{aligned}\gamma \;&=\; \lambda_h\,(\alpha+i\,\beta)+\mu_h,\\ \overline{\gamma} \;&=\; \lambda_h\,(\alpha-i\,\beta)+\mu_h,\end{aligned}$$

ce qui donne un système linéaire d'inconnues réelles $\lambda_h,\mu_h\in\mathbb{R}$, dont le déterminant est non nul :

$$\begin{vmatrix} \alpha+i\beta & 1\\ \alpha-i\beta & 1\end{vmatrix} \;=\; 2i\,\beta \;\neq\; 0.$$

On peut donc déterminer de manière unique les deux coefficients inconnus λ_h et μ_h.

Ces nombres étant calculés, on détermine ensuite le polynôme $p(x)$, et on réitère le procédé sur la fraction :

$$\frac{p(x)}{\big[(x-\alpha)^2+\beta^2\big]^{h-1}\,c(x)}.$$

On obtient ainsi successivement les éléments simples concernant le diviseur irréductible $(x-\alpha)^2+\beta^2$.

Exemple 6.4. Proposons-nous de décomposer en éléments simples dans $F_{\mathbb{R}}[x]$:

$$\frac{x+1}{(x^2+1)^2\,(x^2+x+1)^2} \;=\; \frac{a\,x+b}{(x^2+1)^2}+\frac{c\,x+d}{x^2+1}+\frac{e\,x+f}{(x^2+x+1)^2}+\frac{g\,x+h}{x^2+x+1},$$

où $a,b,c,d,e,f,g,h\in\mathbb{R}$ sont des inconnues.

Il existe donc un polynôme $p(x)$ tel que :

$$\frac{x+1}{(x^2+1)^2\,(x^2+x+1)^2} \;=\; \frac{a\,x+b}{(x^2+1)^2}+\frac{p(x)}{(x^2+1)\,(x^2+x+1)^2},$$

ce qui donne en chassant les dénominateurs :

$$x+1 \;=\; (a\,x+b)\,(x^2+x+1)^2+(x^2+1)\,p(x).$$

Remplaçons $x:=i$:

$$i+1 \;=\; (a\,i+b)\,(-1)+0,$$

puis résolvons :

$$a \;=\; -1 \;=\; b.$$

Ensuite, nous devons déterminer le polynôme $p(x)$ satisfaisant :

$$(x+1)-(-x-1)\,(x^2+x+1)^2 \;=\; (x^2+1)\,p(x),$$

où, pour information, avec les inconnues qui précèdent, on doit avoir :

$$p(x) \;=\; (c\,x+d)\,(x^2+x+1)^2+(e\,x+f)\,(x^2+1)+(g\,x+h)\,(x^2+1)\,(x^2+x+1).$$

Toutefois, nous allons plutôt déterminer ce polynôme $p(x)$ en factorisant le membre de gauche. D'ailleurs, le fait que le membre de gauche soit factorisable par x^2+1 devra confirmer que nous ne nous sommes pas trompés dans le calcul des constantes a et b.

Remarquons que ce membre de gauche s'écrit astucieusement :

$$\begin{aligned}(x+1)\,\big[1+(x^2+x+1)^2\big] \;&=\; (x+1)\,\big[(x^2+1)^2+2\,x\,(x^2+1)+x^2+1\big]\\ &=\; (x^2+1)\,(x+1)\,\big[x^2+1+2\,x+1\big],\end{aligned}$$

ce qui donne :

$$p(x) \;=\; (x+1)\,(x^2+2\,x+2).$$

Réitérons ce procédé. Il existe nécessairement un polynôme $q(x)$ tel que :

$$(x+1)\,(x^2+2\,x+2) \;=\; (c\,x+d)\,(x^2+x+1)^2+(x^2+1)\,q(x),$$

qui s'exprime d'ailleurs en fonction des inconnues restantes comme :

$$q(x) \;=\; e\,x+f+(g\,x+h)\,(x^2+x+1).$$

En remplaçant x par i, on obtient :

$$(i+1)\,(2\,i+1) \;=\; (c\,i+d)\,(-1),$$

d'où :

$$c \;=\; -3, \qquad\qquad d \;=\; 1.$$

Ensuite, nous devons déterminer $q(x)$ en factorisant :

$$(x+1)\,(x^2+2\,x+2)+(3\,x-1)\,(x^2+x+1)^2 \;\stackrel{?}{=}\; (x^2+1)\,q(x).$$

Le membre de gauche peut s'écrire, en groupant d'abord les parties contenant x^2+1 en facteur :

$$(x+1)(x^2+1)+(3x-1)\left[(x^2+1)^2+2x(x^2+1)\right] \\ +(x+1)(2x+1)+(3x-1)x^2,$$

et en remarquant que :

$$\begin{aligned}(x+1)(2x+1)+(3x-1)x^2 &= 3x^3+x^2+3x+1\\ &= (3x+1)(x^2+1),\end{aligned}$$

nous obtenons :

$$\begin{aligned}q(x) &= x+1+(3x-1)(x^2+1+2x)+3x+1\\ &= 3x^3+5x^2+5x+1.\end{aligned}$$

En définitive :

$$\frac{x+1}{(x^2+1)^2(x^2+x+1)^2} = \frac{-x-1}{(x^2+1)^2}+\frac{-3x+1}{x^2+1}+\frac{3x^3+5x^2+5x+1}{(x^2+x+1)^2}.$$

Pour décomposer la dernière fraction, il suffit d'effectuer une division euclidienne, car le dénominateur a un seul diviseur irréductible, et donc, la méthode vue plus haut s'applique. On obtient :

$$3x^3+5x^2+5x+1 = (x^2+x+1)(3x-2)-1,$$

d'où la décomposition recherchée :

$$\frac{x+1}{(x^2+1)^2(x^2+x+1)^2} = \frac{-x-1}{(x^2+1)^2}+\frac{-3x+1}{x^2+1}+\frac{-1}{(x^2+x+1)^2}+\frac{3x+2}{x^2+x+1}.$$

7. Méthode par identification

Une autre méthode de décomposition des fractions rationnelles en éléments simples procède par *identification*. C'est la plus simple et la plus directe, à siroter sans modération pendant les examens.

Soit une fraction $\frac{a}{b} \in F_{\mathbb{K}}[x]$ avec $b \neq 0$. On peut supposer que la partie entière a déjà été calculée par division euclidienne, c'est-à-dire, on peut supposer que $\deg a < \deg b$.

La méthode par identification consiste à poser *a priori* la décomposition en éléments simples de $\frac{a}{b}$, et à calculer les coefficients inconnus de cette décomposition, par *identification* des deux polynômes obtenus après avoir multiplié les deux membres par b.

Cette méthode d'identification s'applique de manière efficace notamment quand les diviseurs irréductibles de b sont de seconde espèce, chacun intervenant avec l'exposant 1 dans la décomposition de b.

Exemple 7.1. Proposons-nous de décomposer dans $F_{\mathbb{R}}[x]$ la fraction :

$$\frac{x+1}{x^4+1}.$$

Cherchons d'abord les diviseurs irréductibles de x^4+1 dans $\mathbb{R}[x]$.

À cet effet, remarquons que :

$$x^4+1 = x^4+2x^2+1-2x^2,$$

de telle sorte que notre dénominateur est mis sous la forme d'une différence entre deux carrés :

$$\begin{aligned} x^4+1 &= (x^2+1)^2 - 2\,x^2 \\ &= \big(x^2-\sqrt{2}\,x+1\big)\,\big(x^2+\sqrt{2}\,x+1\big). \end{aligned}$$

Puisque les deux discriminants de ces deux trinômes du second degré sont strictement négatifs :

$$\big(\mp\sqrt{2}\big)^2 - 4\cdot 1 \;=\; -2 \;<\; 0,$$

nous avons trouvé la décomposition du dénominateur en facteurs irréductibles dans $\mathbb{R}[x]$.

Alors posons *a priori* la décomposition en éléments simples de la fraction proposée :

$$\frac{x+1}{x^4+1} \;=\; \frac{a\,x+b}{x^2-\sqrt{2}\,x+1} + \frac{c\,x+d}{x^2+\sqrt{2}\,x+1},$$

et avec l'intention de déterminer les coefficients inconnus $a, b, c, d \in \mathbb{R}$, multiplions les deux membres par x^4+1 :

$$x+1 \;=\; (a\,x+b)\,\big(x^2+\sqrt{2}\,x+1\big) + (c\,x+d)\,\big(x^2-\sqrt{2}\,x+1\big).$$

Ensuite, développons les produits du membre de droite, et identifions les deux polynômes, ce qui nous donne un système linéaire à résoudre :

$$0 \;=\; a+c, \tag{7.2}$$

$$0 \;=\; a\sqrt{2}+b-c\sqrt{2}+d, \tag{7.3}$$

$$1 \;=\; a+b\sqrt{2}+c-d\sqrt{2}, \tag{7.4}$$

$$1 \;=\; b+d. \tag{7.5}$$

En tenant compte de (7.5), les relations (7.2) et (7.3) donnent :

$$\begin{aligned} 0 &= a+c, \\ -\tfrac{1}{\sqrt{2}} &= a-c, \end{aligned}$$

d'où :

$$c \;=\; -a \;=\; \frac{\sqrt{2}}{4}.$$

En tenant compte de (7.2), les relations (7.4) et (7.5) donnent :

$$\begin{aligned} \tfrac{1}{\sqrt{2}} &= b-d, \\ 1 &= b+d, \end{aligned}$$

d'où :

$$b \;=\; \tfrac{1}{4}\,\big(2+\sqrt{2}\big), \qquad\qquad d \;=\; \tfrac{1}{4}\,\big(2-\sqrt{2}\big).$$

Finalement, la décomposition demandée est :

$$\frac{x+1}{x^4+1} \;=\; \frac{1}{4}\;\frac{-\sqrt{2}\,x+2+\sqrt{2}}{x^2-\sqrt{2}\,x+1} + \frac{1}{4}\;\frac{\sqrt{2}\,x+2-\sqrt{2}}{x^2+\sqrt{2}\,x+1}.$$

Pour terminer, détaillons un deuxième exemple qui applique la méthode d'identification.

Exemple 7.6. Dans $F_{\mathbb{R}}[x]$, proposons-nous de déterminer la décomposition en éléments simples de la fraction :

$$\frac{x^2}{(x-1)\,(x^2-x+1)^2}.$$

Le discriminant $(-1)^2-4=-3$ du facteur du second degré au dénominateur étant <0, ce dernier est irréductible.

Par conséquent, il existe *a priori* une décomposition du type :

$$\frac{x^2}{(x-1)\,(x^2-x+1)^2}=\frac{\lambda}{x-1}+\frac{a\,x+b}{(x^2-x+1)^2}+\frac{c\,x+d}{x^2-x+1}.$$

En multipliant cette équation par $x-1$ et en faisant $x:=1$, on voit que $1=\lambda$.

Ensuite, éliminons les dénominateurs :

$$\begin{aligned}x^2 &= (x^2-x+1)^2+(a\,x+b)\,(x-1)+(c\,x+d)\,(x-1)\,(x^2-x+1)\\ &= x^4+x^2+1-2\,x^3+2\,x^2-2\,x+a\,x^2-a\,x+b\,x-b\\ &\qquad\qquad +c\,x^4+(-2\,c+d)\,x^3+(2\,c-2\,d)\,x^2+(-c+2\,d)\,x-d\,x-d\\ &= x^4\,\big[1+c\big]+x^3\,\big[-2-2\,c+d\big]+x^2\,\big[3+a+2\,c-2\,d\big]+x\,\big[b-a-2\,c+2\,d\big]-b-d,\end{aligned}$$

d'où par identification le système linéaire :

$$\begin{aligned}-1 &= c,\\ 2 &= -2\,c+d,\\ -2 &= a+2\,c-2\,d,\\ 2 &= b-a-c+2\,d,\\ -1 &= -b-d.\end{aligned}$$

En résolvant ce petit système linéaire de niveau L1, on trouve successivement :

$$c=-1,\qquad d=0,\qquad a=0,\qquad b=1.$$

En conclusion :

$$\frac{x^2}{(x-1)\,(x^2-x+1)^2}=\frac{1}{x-1}+\frac{1}{(x^2-x+1)^2}+\frac{-x}{x^2-x+1}.$$

8. Exercices

Exercice 1. EE

Exercice 2. EE

Examens corrigés

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Examen 1

Exercice 1. (a) Déterminer le reste dans la division euclidienne de 2^{100} par 63.

Exercice 2. (a) Résoudre complètement l'équation linéaire :

$$1\,665\,x + 1\,035\,y \;=\; 45,$$

d'inconnues $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Indication: Diviser $1\,665$ par 45, puis $1\,035$ par 45 aussi.

(b) Déterminer l'inverse multiplicatif de $23 \mod 37$ dans $\mathbb{Z}/37\mathbb{Z}$.

(c) L'entier $1\,035 \mod 1\,665$ est-il inversible dans $\mathbb{Z}/1\,665\mathbb{Z}$ muni du produit ?

Exercice 3. (a) Montrer que le reste de la division euclidienne par 8 du carré de tout nombre impair vaut 1, et que tout nombre pair $x \in 2\,\mathbb{Z}$ vérifie $x^2 \equiv 0 \mod 8$, ou $x^2 \equiv 4 \mod 8$.

(b) Soient x, y, z trois nombres entiers *impairs*. Montrer que :

$$2\,\big(x^2\,y^2 + x^2\,z^2 + y^2\,z^2\big),$$

ne peut jamais être égal au carré n^2 d'un entier $n \in \mathbb{Z}$.

Exercice 4. (a) Sur l'ensemble $\mathbb{R}$, on définit la loi de composition interne commutative $*$ par :

$$x * y \;:=\; x + y + 1.$$

Est-ce que $\big(\mathbb{R}, *\big)$ est un groupe ?

Exercice 5. Dans le groupe additif des entiers $m \mod 18$, notés $\overline{m}$ pour $m \in \mathbb{Z}$:

$$G \;:=\; \mathbb{Z}/18\mathbb{Z} \;=\; \Big\{\overline{0},\, \overline{1},\, \overline{2},\, \overline{3},\, \overline{4},\, \overline{5},\, \overline{6},\, \overline{7},\, \overline{8},\, \overline{9},\, \overline{10},\, \overline{11},\, \overline{12},\, \overline{13},\, \overline{14},\, \overline{15},\, \overline{16},\, \overline{17}\Big\},$$

on considère le sous-ensemble :

$$H \;:=\; \big\{\overline{m} \in G\colon\; 6\,\overline{m} = \overline{0}\big\}.$$

On rappelle que l'égalité $\overline{0} = 6\,\overline{m} = \overline{6\,m}$ signifie $6\,m \equiv 0 \mod 18$.

(a) Montrer que H est un sous-groupe de G.

(b) Déterminer tous les éléments distincts de H. Par la suite, on notera $d := \mathsf{Card}\,H$ le nombre de ces éléments.

(c) Soit K un sous-groupe de G de même cardinal d. Montrer que $K = H$ nécessairement.

(d) Combien H contient-il d'éléments d'ordre 6 ?

Exercice 6. (a) Décomposer 561 en facteurs premiers. Indication: Cet entier est divisible par 17.

(b) Soit une indéterminée a. Pour tout entier $n \geqslant 1$, justifier la formule :

$$a^n - 1 \,=\, (a-1)\left(a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1\right).$$

(c) Justifier, pour tout entier $\kappa \geqslant 1$ et tout entier $n \geqslant 1$, la formule :

$$a^{\kappa\, n} - 1 \,=\, \left(a^{\kappa} - 1\right)\left(a^{(n-1)\kappa} + a^{(n-2)\kappa} + \cdots + a^{2\kappa} + a^{\kappa} + 1\right).$$

(d) Soit un entier quelconque $a \in \mathbb{Z}$. Justifier que $a^{561} - a = a\left(a^{2\cdot 280} - 1\right) = a\left(a^2 - 1\right)\boldsymbol{k}$ avec un certain entier $\boldsymbol{k} \in \mathbb{Z}$.

(e) Pour $a \in \mathbb{Z}$ quelconque, montrer que $a(a-1)(a+1)$ est toujours divisible par 3.

(f) Montrer que $a^{561} - a$ est multiple de 3.

(g) Montrer que $a^{561} - a$ est multiple de 17. Indication: Observer que $560 = 16 \cdot 35$. Ensuite, penser au théorème de Fermat.

(h) Montrer que $a^{561} - a$ est multiple de 11.

(i) Montrer que $a^{561} \,\equiv\, a \mod 561$, pour tout entier $a \in \mathbb{Z}$.

(j) Interpréter ce résultat.

(k) Que vous inspire le nombre $1\,105$?

Exercice 7. (a)* Déterminer le nombre de diviseurs de $3\,528$.

2. Corrigé de l'examen 1

Exercice 1. **(a)** En calculant les puissances successives de 2 on constate que :

$$2^6 \;=\; 64 \;\equiv\; 1 \mod 63,$$

ce qui donne, puisque $100 = 6 \cdot 16 + 4$:

$$2^{100} \;=\; (2^6)^{16} \cdot 2^4 \;\equiv\; 1^{16} \cdot 16 \;\equiv\; 16 \mod 63.$$

Puisqu'on a $0 \leqslant 16 < 63$, on en déduit que le reste dans la division euclidienne de 2^{100} par 63 est 16.

Exercice 2. **(a)** Effectivement, on constate que :

$$1\,665 \;=\; 45 \cdot 37, \qquad\qquad 1\,035 \;=\; 45 \cdot 23,$$

et donc, l'équation à résoudre est équivalente à :

$$37\,x + 23\,y \;=\; 1.$$

Ici, 37 et 23 sont deux nombres *premiers* distincts, donc premiers entre eux. On reconnaît donc ici une relation de Bézout $a\,u + b\,v = 1$, qui existe toujours lorsque $1 = a \wedge b$. Mais il faut en trouver une !

Pour cela, comme on le sait, on procède avec l'algorithme d'Euclide :

$$\begin{aligned}
37 \;&=\; 1 \cdot 23 \;+\; 14 \\
23 \;&=\; 1 \cdot 14 \;+\; 9 \\
14 \;&=\; 1 \cdot 9 \;+\; 5 \\
9 \;&=\; 1 \cdot 5 \;+\; 4 \\
5 \;&=\; 4 \cdot 1 \;+\; \boxed{\mathbf{1}} \\
1 \;&=\; 1 \cdot 1 \;+\; \mathbf{0},
\end{aligned}$$

puis en remontant depuis l'avant-dernière ligne, on calcule :

$$\begin{aligned}
1 \;&=\; 5 - \underline{4}_{\text{rpl}} \\
&=\; 5 - \big(9 - 5\big) \\
&=\; -\,9 + 2 \cdot \underline{5}_{\text{rpl}} \\
&=\; -\,9 + 2\,\big(14 - 9\big) \\
&=\; 2 \cdot 14 - 3 \cdot \underline{9}_{\text{rpl}} \\
&=\; 2 \cdot 14 - 3\,\big(23 - 14\big) \\
&=\; -\,3 \cdot 23 + 5 \cdot \underline{14}_{\text{rpl}} \\
&=\; -\,3 \cdot 23 + 5\,\big(37 - 23\big) \\
&=\; 5 \cdot 37 - 8 \cdot 23 \\
&=\; \mathbf{185 - 184 \;=\; 1} \quad \text{OUI},
\end{aligned}$$

et donc une solution particulière (x_0, y_0) de notre équation est :

$$1 \;=\; 37\,x_0 + 23\,y_0 \;=\; 37 \cdot 5 + 23 \cdot (-8).$$

D'après un théorème du cours, l'espace des solutions complètes est alors :

$$\mathsf{Sol} \;=\; \Big\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \colon\; x = 5 - 23\,k,\;\; y = -8 + 37\,k \\ \text{avec } k \in \mathbb{Z} \text{ quelconque}\Big\},$$

ce que l'on peut retrouver en soustrayant notre solution particulière à une solution quelconque :

$$\left\{\begin{matrix} 37\,x + 23\,y \;=\; 1 \\ 37\,x_0 + 23\,y_0 \;=\; 1 \end{matrix}\right\} \qquad \text{impliquent} \qquad 37\,\big(x - x_0\big) \;=\; 23\,\big(y - y_0\big) \;=\; 0,$$

d'où, comme $37 \wedge 23 = 1$:

$$x - x_0 \;=\; -\,23\,k, \qquad\qquad y - y_0 \;=\; 37\,k,$$

avec $k \in \mathbb{Z}$ quelconque.

(b) Grâce à la relation de Bézout que nous avons obtenue plus haut :

$$37 \cdot 5 + 23 \cdot (-8) \;=\; 1,$$

qui devient après réduction modulo 37 :

$$23 \cdot (-\,8) \;\equiv\; 1 \mod 37,$$

il est clair que l'inverse de $23 \mod 37$ est $-\,8 \equiv 29 \mod 37$ dans $\mathbb{Z}\big/37\mathbb{Z}$.

(c) Certainement pas ! Car l'existence d'un entier z qui satisferait :

$$1\,035 \cdot z \;\equiv\; 1 \mod 1\,665,$$

ce qui équivaudrait à :

$$1\,305\,z \;=\; 1 + 1\,665\,k,$$

avec un entier k, impliquerait, après réduction modulo 5, l'absurdité fatale :

$$0 \;\equiv\; 1 \mod 5.$$

Exercice 3. (a) Nous allons donc raisonner modulo 8, dans l'anneau additif :

$$\mathbb{Z}\big/8\mathbb{Z} \;=\; \big\{0,\,1,\,2,\,3,\,4,\,5,\,6,\,7\big\} \mod 8,$$

et calculer tous les carrés possibles. Comme 8 est pair, on a :

$$x \;=\; 2\,y \;\in\; 2\,\mathbb{Z} \qquad\Longleftrightarrow\qquad x \;\equiv\; 0,\;2,\;4,\;6 \mod 8,$$
$$x \;=\; 2\,y + 1 \;\in\; 2\,\mathbb{Z} + 1 \qquad\Longleftrightarrow\qquad x \;\equiv\; 1,\;3,\;5,\;7 \mod 8.$$

Ainsi, on calcule les carrés de ces 8 éléments$\big/$représentants, et on les réduit modulo 8 :

x	0	1	2	3	4	5	6	7
x^2	0	1	4	9	16	25	36	49
$x^2 \mod 8$	0	1	4	1	0	1	4	$1.$

Effectivement, il est maintenant transparent que tous les carrés de nombres impairs sont congrus à 1 modulo 8, et que les carrés de nombres pairs peuvent valoir 0 ou 4 modulo 8.

(b) Puisque :

$$x^2 \;\equiv\; 1 \mod 8, \qquad\qquad y^2 \;\equiv\; 1 \mod 8, \qquad\qquad z^2 \;\equiv\; 1 \mod 8,$$

il vient, en prenant les produits deux à deux :

$$x^2\,y^2 \;\equiv\; 1\cdot 1 \mod 8, \qquad x^2\,z^2 \;\equiv\; 1\cdot 1 \mod 8, \qquad y^2\,z^2 \;\equiv\; 1\cdot 1 \mod 8,$$

et donc :

$$\begin{aligned} 2\left(x^2\,y^2 + x^2\,z^2 + y^2\,z^2\right) &\equiv 2\left(1+1+1\right) \mod 8 \\ &\equiv 6 \mod 8. \end{aligned}$$

Or d'après la Question **(a)** qui précède, un carrré quelconque n^2 avec $n \in \mathbb{Z}$ ne peut être congru qu'aux trois valeurs :

$$n^2 \;\equiv\; 0,\; 1,\; 4 \mod 8,$$

toutes distinctes de ce 6 *intempestif!* En conclusion, une égalité du type :

$$2\left(x^2\,y^2 + x^2\,z^2 + y^2\,z^2\right) \;=\; n^2, \qquad \text{avec} \qquad \begin{cases} x,\, y,\, z \;\in\; 2\,\mathbb{Z}+1, \\ n \;\in\; \mathbb{Z}, \end{cases}$$

est *impossible*.

Exercice 4. (a) Tout d'abord, vérifions que cette loi $*$ (un peu spéciale) est associative :

$$\begin{aligned} x * \left(y * z\right) &= x + \left(y * z\right) + 1 \\ &= x + \left(y + z + 1\right) + 1 \\ &= x + y + z + 2 \\ &= \left(x + y + 1\right) + z + 1 \\ &= \left(x * y\right) * z, \end{aligned}$$

ce, pour tous $x, y, z \in \mathbb{R}$. Super, l'associativité passe !

Observons au passage que cette loi est *commutative*, tout autant que l'est l'addition dans $\mathbb{R}$:

$$x * y \;=\; x + y + 1 \;=\; y + x + 1 \;=\; y * x.$$

Ensuite, après une réflexion rapide sur une feuille de brouillon, on devine *qui* doit être l'élément neutre de cette loi :

$$x * (-1) \;=\; x + (-1) + 1 \;=\; x,$$

sachant que $(-1) * x = x$ vient tout seul grâce à la commutativité. Ça commence à se confirmer, que $*$ est une loi de groupe !

Il reste à trouver l'*inverse* d'un élément quelconque $x \in \mathbb{R}$ pour cette loi interne $*$. Après une réflexion personnelle, on le devine aisément, puis on vérifie sur sa copie que :

$$\begin{aligned} x * \left(-\,x - 2\right) &= x + \left(-\,x - 2\right) + 1 \\ &= -\,1, \end{aligned}$$

où on doit retrouver l'élément neutre en question. L'autre égalité, requise pour satisfaire l'axiome d'inverse $(-x-2) * x = -1$, est alors ou bien offerte par la commutativité, ou bien vérifiable de manière analogue (et fort élémentaire).

En conclusion :

$$\left(\mathbb{R},\, *\right)$$

est bien un groupe — il n'y avait pas de piège !

Mais une question subsididaire surgit : ce groupe est-il « équivalent [1] », en un certain sens, au groupe $\big(\mathbb{R},+\big)$. Réponse : oui ! Le lecteur de ce corrigé pourra y réfléchir, en s'inspirant de :

$$x+y+1 \;=\; x+\tfrac{1}{2}+y+\tfrac{1}{2}.$$

Exercice 5. (a) Tout d'abord, on a $\overline{0}\in H$, car $6\cdot 0=0$, d'où $6\cdot\overline{0}=\overline{6\cdot 0}=\overline{0}$.

Ensuite, pour tous $\overline{m},\overline{n}\in H$, comme on sait d'après un théorème du cours que $\overline{m}+\overline{n}=\overline{m+n}$, et comme on sait aussi que :

$$\Big(\;6\,m\;\equiv\;0\;\;\mathsf{mod}\,18\quad\text{et}\quad 6\,n\;\equiv\;0\;\;\mathsf{mod}\,18\;\Big)\qquad\Longrightarrow\qquad 6\,\big(m{+}n\big)\;\equiv\;0\;\;\mathsf{mod}\,18,$$

il est clair que l'on a aussi $\overline{m}+\overline{n}\in H$ aussi.

Enfin, si $\overline{m}$ appartient à H, son élément opposé (pour l'addition) $\overline{-m}$ appartient aussi à H, puisque :

$$6\,m\;\equiv\;0\;\;\mathsf{mod}\,18\qquad\Longrightarrow\qquad 6\,\big(-\,m\big)\;=\;-\,6\,m\;\equiv\;-\,0\;\;\mathsf{mod}\,18.$$

Ces trois vérifications démontrent donc bien que $H\subset G$ est un *sous-groupe* de G.

(b) On a $\overline{m}\in H$ avec $m\in\mathbb{Z}$ si et seulement si :

$$6\,m\;\equiv\;0\;\;\mathsf{mod}\,18.$$

Or, comme $18=6\cdot 3$ (révision de CP), $6\,m$ est multiple de 18 *si et seulement si* m est multiple de 3. Par conséquent, nous obtenons :

$$H\;=\;\Big\{\overline{0},\;\overline{3},\;\overline{6},\;\overline{9},\;\overline{12},\;\overline{15}\Big\}.$$

Visiblement, le cardinal d de H est égal à 6.

(c) Soit donc $K\subset G$ un sous-groupe de cardinal $|K|=6$. Comme K est un groupe en lui-même, un théorème vu en cours qui est une conséquence directe du théorème de Lagrange a montré que *tout* élément $\overline{m}\in K$ a un ordre qui *divise* le cardinal du groupe ambiant :

$$o\big(\overline{m}\big)\;\Big|\;6\;=\;|K|,$$

d'où nous avons déduit que :

$$\overline{m}^{\,6}\;=\;1_K\;=\;1_G,$$

et comme notre groupe $G=\mathbb{Z}\big/18\mathbb{Z}$ est additif-commutatif, d'élément neutre [2] $1_G=\overline{0}$, ceci veut en fait dire que :

$$6\,\overline{m}\;=\;\overline{0},$$

exactement comme dans la définition de H ! Ainsi, $K\subset H$, et comme K et H ont même cardinal $d=6$, ils doivent effectivement coïncider : $K=H$.

(d) D'après un théorème vu en cours, tout élément $\overline{m}\in\mathbb{Z}\big/18\mathbb{Z}$ est d'ordre :

$$o\,\big(\overline{m}\big)\;=\;\frac{18}{\mathsf{pgcd}\,(18,m)}.$$

1. En Théorie des groupes, le *problème d'équivalence* est l'un des problèmes les plus centraux, les plus importants, et les plus difficiles.

2. Aïe ! Éh ! Oh ? Vous êtes sérieux, Messieurs les professeurs ? Vous avez écrit $1=0$? N'avez-vous pas conscience que tout le langage informatique disparaîtrait, englouti à jamais dans un trou noir de contradictions intergalactiques ?

Grâce à cette belle petite formule élémentaire qui nous montre combien le *sang* de l'arithmétique irrigue les canaux fructifères de la théorie des groupes, nous sommes maintenant ramenés à des calculs directs de niveau CE1.

En effet, une petite vérification rapide sur du papier de brouillon nous convainc alors aisément que, parmi les six éléments $\overline{m} = \overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}$ de H, seuls deux ont un représentant $m \in \mathbb{Z}$ qui a un pgcd égal à 3 avec 18, d'où nous concluons qu'il y a exactement *deux* éléments d'ordre 6 dans H :

$$\overline{3} \qquad \text{et} \qquad \overline{15}.$$

Exercice 6. (a) Heureusement qu'il y a une indication ! En divisant 561 par 17, on trouve :

$$561 \;=\; 17 \cdot 33 \;=\; 17 \cdot 11 \cdot 3,$$

ce qui est la décomposition de 561 en ses *trois* facteurs premiers.

(b) Effectivement, quand on développe le produit à droite en disposant le résultat sur deux lignes décalées astucieusement :

$$\begin{aligned} a^n - 1 \overset{?}{=} (a-1)\big(a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1\big) \\ = a^n + a^{n-1} + \cdots + a^3 + a^2 + a \\ \quad - a^{n-1} - a^{n-2} - \cdots - a^2 - a - 1 \\ = a^n + 0 + \cdots\cdots\cdots + 0 + 0 - 1 \quad \text{OUI,} \end{aligned}$$

on constate un grand nombre d'annulations par paires, qui offrent le résultat.

(c) Il suffit de remplacer a par a^κ dans la formule précédente.

(d) En appliquant les questions qui précèdent, on peut effectivement factoriser :

$$\begin{aligned} a^{561} - a \;&=\; a\big(a^{560} - 1\big) \\ &=\; a\big(a^{2\cdot 280} - 1\big) \\ &=\; a\big(a^2 - 1\big)\big(\underbrace{a^{2\cdot 279} + a^{2\cdot 278} + \cdots + a^{2\cdot 2} + a^{2\cdot 1} + 1}_{=:\,k}\big) \\ &=:\; a\big(a^2 - 1\big)\,k. \end{aligned}$$

(e) Modulo 3, trois cas seulement sont possibles :

$$a \equiv 0 \mod 3, \qquad a \equiv 1 \mod 3, \qquad a \equiv 2 \mod 3.$$

Dans chacun de ces trois cas, le produit $a(a-1)(a+1)$:

$$0\cdot(0-1)\cdot(0+1) \equiv 0 \mod 3, \quad 1\cdot(1-1)\cdot(1+1) \equiv 0 \mod 3, \quad 2\cdot(2-1)\cdot(2+1) \equiv 0 \mod 3,$$

est toujours congru à 0 modulo 3, oui.

(f) D'après ce qui précède, on a bien :

$$\begin{aligned} a^{561} - a \;&=\; a\big(a-1\big)\big(a+1\big)\,k \\ &\equiv\; 0 \cdot k \mod 3 \\ &\equiv\; 0 \mod 3. \end{aligned}$$

(g) Grâce à la factorisation indiquée $560 = 16 \cdot 35$ que l'on vérifie aisément en développant ce produit, on peut factoriser de manière analogue :

$$\begin{aligned} a^{561} - a &= a\left(a^{560} - 1\right) \\ &= a\left(a^{16\cdot 35} - 1\right) \\ &= a\left(a^{16} - 1\right)\Big(\underbrace{a^{16\cdot 34} + a^{16\cdot 33} + \cdots + a^{16\cdot 2} + a^{16\cdot 1} + 1}_{=:\, l}\Big) \\ &=: a\left(a^{16} - 1\right) l. \end{aligned}$$

Mais alors, plutôt que de procéder laborieusement comme dans la Question **(e)** plus haut, on redéveloppe ce produit :

$$a^{561} - a = \left(a^{17} - a\right) l,$$

et on reconnaît alors ce dont la deuxième formulation du Théorème de Fermat-bis parlait — tout en vérifiant mentalement que 17 est bien premier !

Ainsi, une simple application dudit Théorème de Fermat-bis offre la réponse :

$$\begin{aligned} a^{561} - a &\equiv 0 \cdot l \mod 17 \\ &= 0 \mod 17. \end{aligned}$$

(h) Évidemment, il faut procéder de manière similaire, mais l'énoncé laissait l'étudiant chercher la factorisation appropriée de 560 :

$$\begin{aligned} a^{561} - a &= a\left(a^{560} - 1\right) \\ &= a\left(a^{10\cdot 56} - 1\right) \\ &= a\left(a^{10} - 1\right)\Big(\underbrace{a^{10\cdot 55} + a^{10\cdot 54} + \cdots + a^{10\cdot 2} + a^{10\cdot 1} + 1}_{=:\, m}\Big) \\ &=: a\left(a^{10} - 1\right) m, \end{aligned}$$

et comme 11 est premier, Fermat vient encore à la rescousse :

$$\begin{aligned} a^{561} - a &= \left(a^{11} - a\right) m \\ &= 0 \cdot m \mod 11 \\ &\equiv 0 \mod 11. \end{aligned}$$

(i) Ah, tiens ? Mais oui ! On re-dirait Fermat, encore . . .

En tout cas, puisque 3, 11, 17 sont premiers entre eux, les trois Questions **(f)**, **(g)**, **(h)**, qui disaient que le nombre $a^{561} - a$ est congru à 0 modulo 3, 11, 17, impliquent, grâce au Théorème de Gauss [3], que ce nombre est *aussi* congru à 0 modulo le *produit* $3 \cdot 11 \cdot 17 = 561$.

Nous avons donc bien démontré, puisque $a \in \mathbb{Z}$ était arbitraire au départ, que l'on a :

$$a^{561} - a \equiv 0 \mod 561 \qquad (\forall\, a \in \mathbb{Z}).$$

(j) Cette conclusion est exactement la même que le Théorème de Fermat-bis — sauf que Fermat, lui, il demandait que le nombre p dans :

$$a^{p} - a \equiv 0 \mod p \qquad (\forall\, a \in \mathbb{Z}),$$

soit un nombre premier, ce qui n'est pas le cas ici, car notre petit Toto $561 = 3 \cdot 11 \cdot 17$ n'est *pas premier*.

3. — argument que l'on a d'ailleurs aussi employé pour démontrer le Théorème des restes chinois —

Ainsi, à cause du *Diable de l'Arithmétique*, les nombres premiers p ne sont pas les seuls nombres n qui vérifient le Théorème de Fermat-bis, énoncé sous la forme :

$$a^n \equiv a \bmod n \qquad (\forall\, a \in \mathbb{Z}).$$

Un nombre $n \geqslant 2$ est appelé *nombre de Carmichael* s'il n'est *pas* premier, *i.e.* s'il est *composé*, et s'il satisfait :

$$a^n \equiv a \bmod n,$$

pour tout entier $0 \leqslant a \leqslant n-1$, donc pour tout entier $a \in \mathbb{Z}$.

Les trois premiers nombres de Carmichael sont :

$$561,$$
$$1105,$$
$$1729.$$

(k) L'idée de le décomposer en facteurs premiers $5 \cdot 13 \cdot 17 = 1\,105$, et de tenter de raisonner avec lui comme nous avons raisonné avec 561. Pas le temps !

Exercice 7. (a)* Commençons par déterminer la *décomposition en facteurs premiers* de ce 'gros' nombre $3\,528$.

Le dernier chiffre est 8, donc 2 est un facteur premier. Mieux : les deux derniers chiffres sont $28 = 4 \cdot 7$, donc 4 divise $3\,528$. Encore mieux : les trois derniers chiffres sont $528 = 400 + 80 + 4$, qui est divisble par 8, donc $3\,528$ est divisible par 8. On fait alors le quotient et on obtient $3\,528 = 8 \cdot 441$.

Ensuite, la somme des chiffres de 441 étant égale à 9, on déduit que 441 est divisible par 9, on fait le quotient et on obtient $441 = 9 \cdot 49$. En définitive :

$$3\,528 = 2^3 \cdot 3^2 \cdot 7^2.$$

Ensuite, un diviseur quelconque de $3\,528$ est de la forme $2^a \cdot 3^b \cdot 7^c$, avec $0 \leqslant a \leqslant 3$, avec $0 \leqslant b \leqslant 2$, et avec $0 \leqslant c \leqslant 2$. Un triplet (a, b, c) satisfaisant ces inégalités détermine de manière unique un diviseur correspondant, et ces trois entiers a, b, c peuvent être choisis indépendamment les uns des autres.

Puisqu'il y a 4 choix possibles pour a, puis 3 choix pour b, puis 3 choix pour c, le nombre $3\,528$ possède au total exactement :

$$4 \cdot 3 \cdot 3 = 36$$

diviseurs mutuellement distincts.

3. Examen 2

Exercice 1. Soient les deux polynômes de $\mathbb{R}[x]$:

$$a := x^3 - 9\,x^2 + 26\,x - 24 \qquad \text{et} \qquad b := x^3 - 7\,x^2 + 7\,x + 15.$$

(a) Trouver pgcd (a, b). Indication: Il est de degré 1, de la forme $x - \alpha$ avec $\alpha \in \mathbb{Z}$, et on doit rencontrer $135 = 3 \cdot 45$ dans les calculs.

(b) Vérifier que le $\alpha \in \mathbb{Z}$ trouvé est bien racine de $a(\alpha) = 0 = b(\alpha)$.

(c) Trouver deux polynômes unitaires $a' \in \mathbb{R}[x]_1$ et $b' \in \mathbb{R}[x]_1$ tels que :

$$a \;=\; (x - \alpha)\,a' \qquad \text{et} \qquad b \;=\; (x - \alpha)\,b'.$$

(d) Décomposer a et b en facteurs irréductibles dans $\mathbb{R}[x]$.

Exercice 2. Soit l'ensemble $E := \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Soient les trois permutations composées de 3-cycles :

$$\begin{aligned} u &:= (1\ 2\ 3) \circ (4\ 5\ 6) \circ (7\ 8\ 9), \\ v &:= (4\ 5\ 6) \circ (7\ 8\ 9), \\ w &:= (1\ 4\ 7) \circ (2\ 5\ 8) \circ (3\ 6\ 9). \end{aligned}$$

(a) Pour trois entiers distincts $1 \leqslant a_1 < a_2 < a_3 \leqslant 9$, montrer que la permutation circulaire :

$$\sigma := \Big(\; a_1 \longrightarrow a_2 \longrightarrow a_3 \; \Big) \;=\; (a_1\ a_2\ a_3)$$

satisfait $\sigma^3 = \mathsf{Id}$, tandis que $\sigma \neq \mathsf{Id} \neq \sigma^2$.

(b) Exprimer σ^{-1} en fonction de σ.

(c) Montrer que l'on a :

$$u^3 \;=\; v^3 \;=\; w^3 \;=\; \mathsf{Id}.$$

(d) Montrer que l'on a :

$$w \circ v \circ w^{-1} \;=\; (1\ 2\ 3) \circ (7\ 8\ 9).$$

Indication: Calculer l'image de chaque élément de $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ par $w \circ v \circ w^{-1}$, en commençant par déterminer w^{-1}.

(e) Avec soin et sans erreur, décomposer $w^{-1} \circ v \circ w$ en composée de cycles à supports disjoints.

(f) En déduire les égalités :

$$\big(w \circ v\big)^2 \circ w \;=\; w \circ v \circ w^{-2} \circ v \circ w \;=\; u^2 \circ v^{-1}.$$

(g) Montrer que u est une puissance négative de $w \circ v$, que l'on déterminera.

Exercice 3. **(a)** Décomposer en éléments simples, dans $F_{\mathbb{R}}[x]$, la fraction :

$$\frac{x}{x^4+x^2+1}.$$

Indication: Au dénominateur, faire apparaître une différence entre deux carrés.

(b) Sur un corps commutatif $\mathbb{K}$, soit un polynôme unitaire du second degré $p := x^2 + \lambda\, x + \mu$. Montrer que p est réductible sur $\mathbb{K}$ si et seulement si il a une racine dans $\mathbb{K}$.

(c) Soit le corps $\mathbb{K} := \mathbb{Z}/5\mathbb{Z}$ des classes résiduelles modulo 5. Décomposer en facteurs irréductibles le polynôme :

$$(x^2+\overline{4})\,(x^2+\overline{3}).$$

(d) Toujours avec $\mathbb{K} = \mathbb{Z}/5\mathbb{Z}$, décomposer en éléments simples dans $F_{\mathbb{K}}[x]$ la fraction :

$$\frac{x-\overline{2}}{(x^2+\overline{4})\,(x^2+\overline{3})}.$$

4. Corrigé de l'examen 2

Exercice 1. (a) Appliquons l'algorithme d'Euclide en divisant a par b avec reste, et en poursuivant les divisions jusqu'à « capturer » le dernier reste non nul :

$$\begin{aligned} x^3 - 9\,x^2 + 26\,x - 24 &= 1 \cdot \big(x^3 - 7\,x^2 + 7\,x + 15\big) - 2\,x^2 + 19\,x - 39, \\ x^3 - 7\,x^2 + 7\,x + 15 &= \big(-\tfrac{1}{2}\,x - \tfrac{5}{4}\big)\,\big(-2\,x^2 + 19\,x - 39\big) + \boxed{\tfrac{45}{4}\,x - \tfrac{135}{4}}, \\ -2\,x^2 + 19\,x - 39 &= \big(-\tfrac{8}{45}\,x + \tfrac{52}{45}\big)\,\big(\boxed{\tfrac{45}{4}\,x - \tfrac{135}{4}}\big) + \mathbf{0}. \end{aligned}$$

Ainsi, pgcd (a, b) est le renormalisé unitaire :

$$\tfrac{4}{45}\,\big(\tfrac{45}{4}\,x - \tfrac{135}{4}\big) = x - 3.$$

et donc, $\alpha = 3$.

(b) Effectivement :

$$\begin{aligned} 3^3 - 9 \cdot 3^2 + 26 \cdot 3 - 24 &= 27 - 81 + 78 - 24 = 0, \\ 3^3 - 7 \cdot 3^2 + 7 \cdot 3 + 15 &= 27 - 63 + 21 + 15 = 0. \end{aligned}$$

(c) Ainsi, a et b sont divisibles par $x - 3$. On divise alors a et b par $x - 3$, et on trouve aisément — avec des restes nuls ! — :

$$a = (x-3)\,(x^2 - 6\,x + 8) \qquad \text{et} \qquad b = (x-3)\,(x^2 - 4\,x - 5).$$

(d) Comme les deux facteurs restants sont de degré 2, on applique la formule connue :

$$\frac{-\,b \pm \sqrt{b^2 - 4\,a\,c}}{2\,a}$$

pour les racines (dans $\mathbb{C}$) d'un trinôme du second degré $a\,x^2 + b\,x + c$ avec $a \neq 0$, ce qui donne les deux couples de racines :

$$\frac{6 \pm \sqrt{6^2 - 4 \cdot 8}}{2} \qquad \text{et} \qquad \frac{4 \pm \sqrt{4^2 + 4 \cdot 5}}{2},$$

c'est-à-dire :

$$\frac{6 \pm \sqrt{4}}{2} = 3 \pm 1 \qquad \text{et} \qquad \frac{4 \pm \sqrt{36}}{2} = 2 \pm 3,$$

d'où en conclusion :

$$a = (x-3)\,(x-4)\,(x-2) \qquad \text{et} \qquad b = (x-3)\,(x-5)\,(x+1).$$

Exercice 2. (a) Cela a été vu en cours, mais re-faisons-le. Pour tout $a \neq a_1, a_2, a_3$, on a $\sigma(a) = a$, c'est-à-dire :

$$\sigma\Big|_{E\setminus\{a_1,a_2,a_3\}} = \mathsf{Id},$$

donc nous pouvons nous restreindre à considérer seulement l'action de σ sur $\{a_1, a_2, a_3\}$.

Alors par définition d'une permutation circulaire, on a :

$$\begin{aligned}\sigma(a_1) &= a_2 \neq a_1,\\ \sigma^2(a_1) &= \sigma(a_2) = a_3 \neq a_1,\end{aligned}$$

donc $\sigma \neq \mathsf{Id} \neq \sigma^2$, tandis que :

$$\begin{aligned}\sigma^3(a_1) &= \sigma(a_3) = a_1,\\ \sigma^3(a_2) &= \sigma^{3+1}(a_1) = \sigma\big(\sigma^3(a_1)\big) = \sigma(a_1) = a_2,\\ \sigma^3(a_3) &= \sigma^{3+2}(a_1) = \sigma^2\big(\sigma^3(a_1)\big) = \sigma^2(a_1) = a_3,\end{aligned}$$

et donc, $\sigma^3 = \mathsf{Id}$, comme demandé. Ainsi, σ est d'ordre 3 dans le groupe $\mathfrak{S}(E)$, lequel est d'ordre — de cardinal — $9! = 362\,880$.

(b) Comme $\mathsf{Id} = \sigma^3 = \sigma^2 \circ \sigma$, il est clair que $\sigma^{-1} = \sigma^2$.

(c) Comme chacune des trois permutations u, v, w est produit de 3-cycles à supports *disjoints :*

$$\begin{aligned}u &= u_1 \circ u_2 \circ u_3,\\ v &= v_1 \circ v_2,\\ w &= w_1 \circ w_2 \circ w_3,\end{aligned}$$

les 3-cycles de chacune de ces trois lignes commutent entre eux, et donc, pour tout entier $m \in \mathbb{Z}$, on a, grâce à une proposition connue démontrée en cours :

$$\begin{aligned}u^m &= u_1^m \circ u_2^m \circ u_3^m,\\ v^m &= v_1^m \circ v_2^m,\\ w^m &= w_1^m \circ w_2^m \circ w_3^m.\end{aligned}$$

Enfin les u_i, v_i, w_i étant *tous* des 3-cycles, la Question **(a)** donne :

$$\begin{aligned}u^3 &= u_1^3 \circ u_2^3 \circ u_3^3 = \mathsf{Id} \circ \mathsf{Id} \circ \mathsf{Id} = \mathsf{Id},\\ v^3 &= v_1^3 \circ v_2^3 = \mathsf{Id} \circ \mathsf{Id} = \mathsf{Id},\\ w^3 &= w_1^3 \circ w_2^3 \circ w_3^3 = \mathsf{Id} \circ \mathsf{Id} \circ \mathsf{Id} = \mathsf{Id}.\end{aligned}$$

(d) En lisant du bas vers le haut la permutation :

$$w = \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\ 4 & 5 & 6 & 7 & 8 & 9 & 1 & 2 & 3 \end{array}$$

on écrit son inverse :

$$w^{-1} = \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\ 7 & 8 & 9 & 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$

Puis, en écrivant :

$$\begin{array}{cccccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ v & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 1 & 2 & 3 & 5 & 6 & 4 & 8 & 9 & 7 \end{array}$$

on peut composer :

$$\begin{array}{cccccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ w^{-1} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 7 & 8 & 9 & 1 & 2 & 3 & 4 & 5 & 6 \\ v & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 8 & 9 & 7 & 1 & 2 & 3 & 5 & 6 & 4 \\ w & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 & 4 & 5 & 6 & 8 & 9 & 7 \end{array}$$

ce qui montre bien que :

$$w \circ v \circ w^{-1} = (1\ 2\ 3) \circ (7\ 8\ 9).$$

(e) Grâce au fait qu'on a déjà fait le travail de détermination de w^{-1}, et qu'on a déjà explicité v, w, il suffit d'élaborer le tableau de composition :

$$\begin{array}{cccccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ w & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 5 & 6 & 7 & 8 & 9 & 1 & 2 & 3 \\ v & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 5 & 6 & 4 & 8 & 9 & 7 & 1 & 2 & 3 \\ w^{-1} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 & 5 & 6 & 4 & 7 & 8 & 9 \end{array}$$

ce qui donne :

$$w^{-1} \circ v \circ w = (1\ 2\ 3) \circ (4\ 5\ 6).$$

(f) L'idée-clé, suggérée ici, était de remplacer w au centre par w^{-2}, ce que la Question **(b)** suggérait à l'avance :

$$\begin{aligned} \big(w \circ v\big)^2 \circ w &= w \circ v \circ \underline{w}_{\text{rpl}} \circ v \circ w \\ &= w \circ v \circ w^{-2} \circ v \circ w \\ &= \big(w \circ v \circ w^{-1}\big) \circ \big(w^{-1} \circ v \circ w\big) \\ \text{[Questions (d) et (e)]} \qquad &= (1\ 2\ 3) \circ (7\ 8\ 9) \circ (1\ 2\ 3) \circ (4\ 5\ 6) \\ \text{[Commutation disjointe]} \qquad &= (1\ 2\ 3)^2 \circ (4\ 5\ 6) \circ (7\ 8\ 9) \\ \text{[Commutation disjointe]} \qquad &= \Big((1\ 2\ 3) \circ (4\ 5\ 6) \circ (7\ 8\ 9)\Big)^2 \circ \Big((4\ 5\ 6) \circ (7\ 8\ 9)\Big)^{-1} \\ \text{[Reconnaître]} \qquad &= u^2 \circ v^{-1} \qquad \text{OUI !} \end{aligned}$$

(g) On déduit de la Question **(f)**, en utilisant $u^2 = u^{-1}$, que :

$$\begin{aligned} \big(w \circ v\big)^3 &= u^2 \\ &= u^{-1}, \end{aligned}$$

donc :

$$\big(w \circ v\big)^{-3} = u.$$

Exercice 3. (a) Écrivons, puis factorisons :

$$\begin{aligned} x^4+x^2+1 &= \big(x^2+1\big)^2-x^2 \\ &= \big(x^2+1-x\big)\,\big(x^2+1+x\big). \end{aligned}$$

Les discriminants de ces deux trinômes du second degré étant < 0, ils sont tous deux irréductibles.

D'après un théorème du cours, il existe des inconnues $a, b, c, d \in \mathbb{R}$, telles que :

$$\frac{x}{(x^2-x+1)\,(x^2+x+1)} = \frac{a\,x+b}{x^2-x+1} + \frac{c\,x+d}{x^2+x+1}.$$

Après élimination des dénominateurs, il vient :

$$\begin{aligned} x &= (a\,x+b)\,(x^2+x+1) + (c\,x+d)\,(x^2-x+1) \\ &= a\,x^3+a\,x^2+a\,x \qquad\quad +c\,x^3-c\,x^2+c\,x \\ &\qquad +b\,x^2+b\,x+b \qquad\quad +d\,x^2-d\,x+d \\ &= (a+c)\,x^3+(a+b-c+d)\,x^2+(a+b+c-d)\,x+b+d. \end{aligned}$$

Il s'agit donc d'un système linéaire :

$$\begin{aligned} 0 &= a+c, \\ 0 &= a+b-c+d, \\ 1 &= a+b+c-d, \\ 0 &= b+d. \end{aligned}$$

Résolvons $a = -\,c$ et $d = -\,b$ depuis les équations 1 et 4, puis, remplaçons ces valeurs dans les équations 2 et 3 :

$$\begin{aligned} 0 &= -\,c+b-c-b = -\,2\,c, \qquad \text{d'où} \quad 0 = c, \quad \text{puis} \quad 0 = a \\ 1 &= -\,c+b+c+b = 2\,b, \qquad \text{d'où} \quad \tfrac{1}{2} = b, \quad \text{puis} \quad -\,\tfrac{1}{2} = d. \end{aligned}$$

En conclusion :

$$\frac{x}{x^4+x^2+1} = \frac{1/2}{x^2-x+1} + \frac{-\,1/2}{x^2+x+1}.$$

(b) Si p est réductible, puisque $2 = 1+1$ est la seule possibilité au niveau des degrés, il se factorise :

$$p(x) = (x-\alpha)\,(x-\beta),$$

en un produit de deux polynômes unitaires de degré 1, à coefficients dans $\mathbb{K}$. Mais alors, α et β sont des racines dans $\mathbb{K}$ de p.

S'il existe $\alpha \in \mathbb{K}$ tel que $p(\alpha) = 0$, on a vu dans le cours que le polynôme se factorise par $(x-\alpha)$:

$$p(x) = (x-\alpha)\,q(x),$$

avec un polynôme $q(x)$ de degré 1, unitaire, à coefficients dans $\mathbb{K}$, donc de la forme $x-\beta$. Ainsi, $p(x) = (x-\alpha)\,(x-\beta)$ se décompose en produit de deux polynômes de degré 1 à coefficients dans $\mathbb{K}$, et on sait que tout polynôme de degré 1 est irréductible.

(c) Comme :

$$x^2+\overline{4} = x^2-\overline{1} = (x+\overline{1})\,(x-\overline{1}),$$

le premier facteur au numérateur est réductible en deux facteurs de degré 1.

Par ailleurs, modulo 5, les carrés des éléments $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$ de $\mathbb{Z}/5\mathbb{Z}$ sont égaux à $\overline{0}$, $\overline{1}$, $\overline{4}$, $\overline{4}$, $\overline{1}$. Aucun n'est égal à $-\overline{3} = \overline{2}$. Donc le polynôme $x^2 + \overline{3}$ n'a pas de racine dans $\mathbb{Z}/5\mathbb{Z}$.

L'équivalence contraposée de la Question **(a)** nous permet de conclure que $p(x)$ est irréductible.

(d) D'après un théorème du cours, comme le degré du numérateur est $<$ le degré du dénominateur, on doit avoir une décomposition en éléments simples du type :

$$\frac{x+\overline{3}}{(x+\overline{1})\,(x+\overline{4})\,(x^2+\overline{3})} = \frac{a\,x+b}{x^2+\overline{3}} + \frac{c}{x+\overline{1}} + \frac{d}{x+\overline{4}},$$

avec certaines constantes inconnues $a, b, c, d \in \mathbb{Z}/5\mathbb{Z}$.

Éliminons les dénominateurs :

$$\begin{aligned} x+\overline{3} &= (a\,x+b)\,(x+\overline{1})\,(x+\overline{4}) + c\,(x^2+\overline{3})\,(x+\overline{4}) + d\,(x^2+\overline{3})\,(x+\overline{1}) \\ &= (a\,x+b)\,(x^2+\overline{4}) + c\,\big(x^3+\overline{4}\,x^2+\overline{3}\,x+\overline{2}\big) + d\,\big(x^3+x^2+\overline{3}\,x+\overline{3}\big) \\ &= (a+c+d)\,x^3 + (b+\overline{4}\,c+d)\,x^2 + (\overline{4}\,a+\overline{3}\,c+\overline{3}\,d)\,x + \overline{4}\,b+\overline{2}\,c+\overline{3}\,d. \end{aligned}$$

Par identification, il s'agit donc de résoudre le système linéaire suivant, à coefficients dans $\mathbb{Z}/5\mathbb{Z}$:

$$\begin{aligned} \overline{0} &= a+c+d, \\ \overline{0} &= b+\overline{4}\,c+d, \\ \overline{1} &= \overline{4}\,a+\overline{3}\,c+\overline{3}\,d, \\ \overline{3} &= \overline{4}\,b+\overline{2}\,c+\overline{3}\,d. \end{aligned}$$

Remplaçons $a = -c-d$ depuis l'équation 1 dans les équations 2, 3, 4 :

$$\begin{aligned} \overline{0} &= b+\overline{4}\,c+d, \\ \overline{1} &= -\overline{4}\,c-\overline{4}\,d+\overline{3}\,c+\overline{3}\,d = \overline{4}\,c+\overline{4}\,d, \\ \overline{3} &= \overline{4}\,d+\overline{2}\,c+\overline{3}\,d. \end{aligned}$$

Remplaçons $d = -b-\overline{4}\,c = \overline{4}\,b+c$:

$$\begin{aligned} \overline{1} &= \overline{4}\,c+\overline{16}\,b+\overline{4}\,c = \overline{3}\,c+b, \\ \overline{3} &= \overline{4}\,b+\overline{2}\,c+\overline{12}\,b+\overline{3}\,c = b, \end{aligned}$$

puis résolvons :

$$b = \overline{3}, \qquad c = \overline{1},$$

et enfin :

$$d = \overline{3}, \qquad a = \overline{1}.$$

En conclusion, nous avons trouvé la décomposition en éléments simples :

$$\frac{x+\overline{3}}{(x+\overline{1})\,(x+\overline{4})\,(x^2+\overline{3})} = \frac{x+\overline{3}}{x^2+\overline{3}} + \frac{\overline{1}}{x+\overline{1}} + \frac{\overline{3}}{x+\overline{4}}.$$

5. Examen 3

Exercice 1. Dans le groupe $\mathfrak{S}_7$ des permutations de l'ensemble $\{1,2,3,4,5,6,7\}$, on considère :

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 6 & 3 & 1 & 2 \end{pmatrix}.$$

(a) Décomposer σ en produit de cycles à supports disjoints.

(b) Déterminer l'ordre de σ.

(c) Calculer $\tau := \sigma^{425}$.

(d) Calculer la signature de σ, puis celle de τ.

Exercice 2. On rappelle que l'on note $\varphi(n)$ le nombre d'entiers $1 \leqslant k \leqslant n$ qui sont premiers avec un entier donné $n \geqslant 1$, où par convention $\varphi(1) = 1$ car 1 est premier avec lui-même.

(a) Calculer $\varphi(135)$.

(b) Déterminer le reste de la division euclidienne de 7^{7202} par 135.

(c) Déterminer le cardinal de l'ensemble $\big(\mathbb{Z}/15\,\mathbb{Z}\big)^\times$ des éléments inversibles pour la multiplication $\times$ de l'anneau $\big(\mathbb{Z}/15\,\mathbb{Z},\ +, \times\big)$.

(d) Déterminer les ordres des deux éléments $\overline{2}$ et $\overline{7}$ dans le groupe abélien $\big((\mathbb{Z}/15\,\mathbb{Z})^\times,\ \times\big)$.

(e) Ce groupe $\big((\mathbb{Z}/15\,\mathbb{Z})^\times,\ \times\big)$ est-il cyclique ?

Exercice 3. Soit $\big(A, +, \times\big)$ un anneau commutatif dans lequel $a+a = 0_A$ pour tout élément $a \in A$.

(a) Montrer que pour tous a et b dans A, on a l'identité $(a+b)^2 = a^2 + b^2$.

(b) Montrer que l'application $\psi\colon A \longrightarrow A$ définie par $\psi(a) := a^2$ est un morphisme d'anneaux.

(c) On suppose dorénavant que A est intègre. Montrer que ψ est une application injective.

(d) En supposant de plus que A est de cardinal fini, montrer que pour tout $a \in A$, il existe $b \in A$ tel que $b^2 = a$.

Exercice 4. **(a)** Calculer le quotient et le reste de la division euclidienne de $X^4 + 5\,X^3 + 12\,X^2 + 20\,X - 6$ par $X^2 + 3\,X - 1$.

(b) Déterminer le pgcd entre $X^4 + 5\,X^3 + 12\,X^2 + 20\,X - 6$ et $X^2 + 3\,X - 1$.

Exercice 5. **(a)** Factoriser le polynôme $X^2 - 1$ en produit de polynômes irréductibles dans $\mathbb{R}[X]$, puis décomposer en éléments simples $\frac{1}{X^2-1}$ sur $\mathsf{Frac}\,\mathbb{R}[X]$.

(b) Factoriser le polynôme $X^4 - 1$ en produit de polynômes irréductibles dans $\mathbb{R}[X]$.

(c) Décomposer en éléments simples $\frac{1}{X^4-1}$ sur $\mathsf{Frac}\,\mathbb{R}[X]$.

(d) Factoriser le polynôme $X^4 + 1$ en produit de polynômes irréductibles dans $\mathbb{R}[X]$.

(e) Décomposer en éléments simples $\frac{1}{X^4+1}$ sur $\mathsf{Frac}\,\mathbb{R}[X]$.

(f) Vérifier que :

$$\frac{1}{X^8-1} = \frac{1/8}{X-1} - \frac{1/8}{X+1} - \frac{1/4}{X^2+1} - \frac{1/2}{X^4+1}.$$

(g) Factoriser le polynôme $X^8 - 1$ en produit de polynômes irréductibles dans $\mathbb{R}[X]$.

(h) Décomposer en éléments simples $\frac{1}{X^8-1}$ sur $\mathsf{Frac}\,\mathbb{R}[X]$.

6. Corrigé de l'examen 3

Exercice 1. (a) Comme on a :

$$\begin{aligned} 1 &\longmapsto 4 \longmapsto 6 \longmapsto 1, \\ 2 &\longmapsto 7 \longmapsto 2, \\ 3 &\longmapsto 5 \longmapsto 3, \end{aligned}$$

la décomposition de Σ en produit de cycles à supports disjoints est :

$$\sigma \,=\, \big(1\ 4\ 6\big)\,\big(2\ 7\big)\,\big(3\ 5\big).$$

(b) Ainsi, la permutation σ est le produit d'un 3-cycle et de deux 2-cycles [4] (transpositions), à supports disjoints. D'après le cours, son ordre vaut donc :

$$o(\sigma) \,=\, \mathsf{ppcm}\,(3,2,2) \,=\, 6.$$

(c) Puisque $\sigma^6 = \mathsf{Id}$, effectuons la division de 425 par 6 :

$$425 \,=\, 6\cdot 70 + 5,$$

d'où :

$$\begin{aligned} \tau \,=\, \sigma^{425} \,=\, \big(\sigma^6\big)^{70}\circ\sigma^5 \,=\, \sigma^5 \,&=\, \sigma^{-1} \\ &=\, \big(1\ 6\ 4\big)\,\big(2\ 7\big)\,\big(3\ 5\big). \end{aligned}$$

(d) Rappelons que la signature $\varepsilon(\bullet)$ est un morphisme de groupes du groupe $\mathfrak{S}_n$ des permutations d'un ensemble à $n \geqslant 1$ éléments à valeurs dans $\big(\{\pm 1\},\times\big)$.

Rappelons aussi que la signature d'un cycle de longueur $p \geqslant 2$ vaut $(-1)^p$. Par conséquent :

$$\begin{aligned} \varepsilon(\sigma) \,&=\, \varepsilon\big((1\,4\,6)\,(2\,7)\,(3\,5)\big) \,=\, (-1)^{3-1}\,(-1)^{2-1}\,(-1)^{2-1} \,=\, 1, \\ \varepsilon(\tau) \,&=\, \varepsilon\big((1\,6\,4)\,(2\,7)\,(3\,5)\big) \,=\, 1. \end{aligned}$$

D'ailleurs, on sait généralement que la multiplicativité $\varepsilon\big(\sigma_1\sigma_2\big) \,=\, \varepsilon(\sigma_1)\,\varepsilon(\sigma_2)$ dans $\mathfrak{S}_n$ implique que $\varepsilon\big(\sigma^{-1}\big) = \frac{1}{\varepsilon(\sigma)}$ pour toute permutation $\sigma \in \mathfrak{S}_n$, et ici, $\frac{1}{1} = 1$.

Exercice 2. (a) D'après un théorème du cours, la fonction indicatrice d'Euler $\varphi(\bullet)$ est multiplicative sur les nombres premiers entre eux, et si un entier $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ est décomposé en facteurs premiers, on a :

$$\begin{aligned} \varphi(n) \,&=\, \varphi\big(p_1^{\alpha_1}\big)\cdots\varphi\big(p_r^{\alpha_r}\big) \\ &=\, \big(p_1^{\alpha_1} - p_1^{\alpha_1-1}\big)\cdots\big(p_r^{\alpha_r} - p_r^{\alpha_r-1}\big). \end{aligned}$$

Ici, comme :

$$135 \,=\, 3^3\cdot 5,$$

il vient :

$$\varphi(135) \,=\, \big(3^3 - 3^2\big)\,\big(5^1 - 5^0\big) \,=\, 18\cdot 4 \,=\, 72.$$

4. — un 2×2 = quadricyle ! ? —

(b) Heureusement que 7 est premier avec $135 = 3^3\,5$, car un théorème d'Euler (qui généralise le Petit Théorème de Fermat) peut être appliqué :

$$7^{\varphi(135)} \equiv 1 \mod 135, \qquad \text{c'est-à-dire :} \qquad 7^{72} \equiv 1 \mod 135.$$

On peut vérifier sur ordinateur que 36 est l'exposant minimal $\geqslant 1$ satisfaisant $7^{36} \equiv 1 \mod 135$, mais cela n'était pas demandé, et d'ailleurs, il vaut mieux faire notre petite affaire légère avec 72, puisque l'observation aisée $7200 = 72 \cdot 100$ nous permet de déterminer le reste de la division euclidienne de $7^{\,7202}$ par 135 :

$$7^{7202} = \big(7^{72}\big)^{100} \cdot 7^2 \equiv 1 \cdot 7^2 \mod 135 \equiv 49 \mod 135.$$

(c) D'après le théorème du cours susmentionné :

$$\mathsf{Card}\,\big(\mathbb{Z}/15\mathbb{Z}\big)^\times = \varphi(15) = \varphi(3^1 \cdot 5^1) = \big(3^1 - 3^0\big)\,\big(5^1 - 5^0\big) = 8.$$

(d) Puisque modulo 15 :

$$\overline{2}^2 \equiv \overline{4} \not\equiv \overline{1}, \qquad \overline{2}^3 \equiv \overline{8} \not\equiv \overline{1}, \qquad \overline{2}^4 \equiv \overline{16} \equiv \overline{1},$$

l'ordre de $\overline{2}$ vaut 4.

De même, puisque modulo 15 :

$$\overline{7}^2 \equiv \overline{49} \equiv \overline{4} \not\equiv \overline{1}, \qquad \overline{7}^3 \equiv \overline{4}\cdot\overline{7} \equiv \overline{28} \equiv -\overline{2} \not\equiv \overline{1}, \qquad \overline{7}^4 \equiv \big(-\overline{2}\big)\cdot\overline{7} = -\overline{14} \equiv \overline{1},$$

l'ordre de $\overline{7}$ vaut 4, aussi !

(e) D'après un théorème du cours, ce groupe $\big(\mathbb{Z}/15\mathbb{Z}\big)^\times$ est cyclique si et seulement si l'un au moins de ses 8 éléments est d'ordre égal à son cardinal, 8.

On vérifie manuellement que les 8 éléments en question de $\big(\mathbb{Z}/15\mathbb{Z}\big)^\times$ sont :

$$\overline{1}, \quad \overline{2}, \quad \overline{4}, \quad \overline{7}, \quad \overline{8}, \quad \overline{11}, \quad \overline{13}, \quad \overline{14},$$

puisque, dans $\mathbb{Z}/15\mathbb{Z}$:

$$\overline{1} = \overline{1}\cdot\overline{1} = \overline{2}\cdot\overline{8} = \overline{4}\cdot\overline{4} = \overline{7}\cdot\overline{13} = \overline{8}\cdot\overline{2} = \overline{11}\cdot\overline{11} = \overline{13}\cdot\overline{7} = \overline{14}\cdot\overline{14}.$$

Parmi ces 8 éléments, on vient de voir que $\overline{2}$ et $\overline{7}$ ne peuvent pas convenir, car il sont tous deux d'ordre $4 < 8$. Évidemment, $\overline{1}$ d'ordre 1 et $\overline{14} = -\overline{1}$ d'ordre 2 ne peuvent pas convenir non plus.

Restent encore $\overline{4}$, $\overline{8}$, $\overline{11}$, $\overline{13}$: l'un d'entre eux est-il d'ordre 8 ? Hélas non, car avec un peu d'astuce pour utiliser la Question **(d)**, on calcule :

$$\begin{aligned}
\overline{4}^4 &= \big(\overline{2}^2\big)^4 = \big(\overline{2}^4\big)^2 = \overline{1},\\
\overline{8}^4 &= \big(\overline{2}^3\big)^4 = \big(\overline{2}^4\big)^3 = \overline{1},\\
\overline{11}^4 &= \big(-\overline{4}\big)^4 = \big(\overline{4}\big)^4 = \overline{1},\\
\overline{13}^4 &= \big(-\overline{2}\big)^4 = \big(\overline{2}\big)^4 = \overline{1}.
\end{aligned}$$

En définitive, *tous* les 8 éléments de $\big(\mathbb{Z}/15\mathbb{Z}\big)^\times$ sont d'ordre égal à 4 ou divisant 4, et donc, aucun ne peut être d'ordre 8. Ceci démontre que $\big(\mathbb{Z}/15\mathbb{Z}\big)^\times$ n'est *pas* cyclique. Quelle déception !

Exercice 3. (a) C'est très simple :

$$\big(a+b\big)^2 \;=\; a^2+ab+ba+b^2 \;=\; a^2+\underline{ab+ab}_{\circ}+b^2 \;=\; a^2+0_A+b^2 \;=\; a^2+b^2.$$

(b) Cela est aisé, avec $a, b \in A$ quelconques :

$$\begin{aligned}\psi(a+b) \;&=\; \big(a+b\big)^2 \;=\; a^2+b^2 \;=\; \psi(a)+\psi(b),\\ \psi\big(a\,b\big) \;&=\; (ab)^2 \;=\; ab\,ab \;=\; aa\,bb \;=\; a^2\,b^2 \;=\; \psi(a)\,\psi(b),\\ \psi(1_A) \;&=\; 1_A^2 \;=\; 1_A.\end{aligned}$$

(c) Avec $a, b \in A$ satisfaisant $\psi(a) = \psi(b)$:

$$a^2 \;=\; b^2 \qquad\qquad \Longleftrightarrow \qquad\qquad (a-b)\,(a+b) \;=\; 0_A,$$

l'hypothèse d'intégrité de A donne $a = b$ — super ! c'est ce qu'on veut pour l'injectivité de ψ ! —, ou $a = -\,b$, mais comme on peut ajouter à droite $0_A = b + b$, il vient aussi dans ce deuxième cas :

$$a \;=\; -\,b \;=\; -\,b+b+b \;=\; b.$$

(d) Notre morphisme ψ est donc une application *injective* de l'anneau *fini* A dans lui-même. D'après la théorie élémentaire des ensembles, ceci implique automatiquement que ψ est surjective (et bijective).

Autrement dit, tout $a \in A$, possède un antécédant $b \in A$ tel que $a = \psi(b) = b^2$.

Exercice 4. (a) On trouve :

$$X^4+5\,X^3+12\,X^2+20\,X-6 \;=\; \big(X^2+3\,X-1\big)\,\big[X^2+2\,X+7\big]+X+1.$$

(b) D'après l'algorithme d'Euclide, il faut continuer à diviser par le reste obtenu :

$$X^3+3\,X-1 \;=\; (X+1)\,[X+2]-3.$$

En une seule étape supplémentaire, nous trouvons alors un reste non nul -3 de degré zéro. Par conséquent, le pgcd recherché vaut 1 : ces deux polynômes sont premiers entre eux.

Exercice 5. (a) Il est clair que $X^2-1 = (X-1)(X+1)$, et on trouve aisément :

$$\frac{1}{X^2-1} \;=\; \frac{1/2}{X-1}-\frac{1/2}{X+1},$$

ce qui se vérifie en réduisant visuellement le membre de droite au même dénominateur.

(b) Dans $\mathbb{R}[x]$, on factorise facilement :

$$X^4-1 \;=\; (X-1)\,(X+1)\,(X^2+1).$$

(c) Ensuite, avec la méthode des coefficients indéterminés :

$$\frac{1}{X^4-1} \;=\; \frac{a}{X-1}+\frac{b}{X+1}+\frac{c\,X+d}{X^2+1},$$

où a, b, c, d sont des inconnues, après multication globale par X^4-1, on obtient un système linéaire que l'on résout, pour trouver :

$$\frac{1}{X^4-1} \;=\; \frac{1/4}{X-1}-\frac{1/4}{X+1}-\frac{1/2}{X^2+1}.$$

(d) Attention ! Ce n'est pas parce que la fonction réelle $x \longmapsto x^4+1$ ne prend que des valeurs $\geqslant 1$ sur $\mathbb{R}$ et donc n'a aucune racine sur $\mathbb{R}$ que le polynôme X^4+1 ne se décompose pas en facteurs irréductibles de degrés <4 !

Et d'ailleurs, on est certain que ce polynôme de degré *doit* se décomposer en facteurs irréductibles non triviaux, car un théorème du cours stipule que dans $\mathbb{R}[X]$, les polynômes irréductibles sont tous de degré égal à $1<4$, ou à $2<4$.

Par une astuce vue dans le polycopié, faisons apparaître une différence entre deux carrés :

$$\begin{aligned} X^4+1 &= (X^2+1)^2 - 2\,X^2 \\ &= \big(X^2+1-\sqrt{2}\,X\big)\,\big(X^2+1+\sqrt{2}\,X\big), \end{aligned}$$

et observons que les discriminants des deux facteurs trouvés :

$$\big(\mp\sqrt{2}\big)^2 - 4 \;=\; -2 \;<\; 0,$$

sont strictement négatifs, ce qui garantit que ces deux facteurs sont irréductibles sur $\mathbb{R}$.

(e) Ensuite, avec la méthode des coefficients indéterminés :

$$\frac{1}{X^4+1} \;=\; \frac{a\,X+b}{X^2-\sqrt{2}\,X+1} + \frac{c\,X+d}{X^2+\sqrt{2}\,X+1},$$

où a, b, c, d sont des inconnues, on trouve :

$$\frac{1}{X^4+1} \;=\; \frac{-\frac{1}{2\sqrt{2}}\,X+\frac{1}{2}}{X^2-\sqrt{2}\,X+1} + \frac{\frac{1}{2\sqrt{2}}\,X+\frac{1}{2}}{X^2+\sqrt{2}\,X+1}.$$

(f) Cela s'effectue par un calcul direct.

(g) Grâce à ce qui précède :

$$\begin{aligned} X^8-1 &= \big(X^4-1\big)\,\big(X^4+1\big) \\ &= (X-1)(X+1)(X^2+1)\,\big(X^2+1-\sqrt{2}\,X\big)\,\big(X^2+1+\sqrt{2}\,X\big). \end{aligned}$$

(h) On procède comme suit :

$$\begin{aligned} \frac{1}{X^8-1} &= \frac{1/8}{X-1} - \frac{1/8}{X+1} - \frac{1/4}{X^2+1} - \frac{1/2}{X^4+1} \\ &= \frac{1/8}{X-1} - \frac{1/8}{X+1} - \frac{1/4}{X^2+1} - \frac{-\frac{1}{4\sqrt{2}}\,X+\frac{1}{4}}{X^2-\sqrt{2}\,X+1} - \frac{\frac{1}{4\sqrt{2}}\,X+\frac{1}{4}}{X^2+\sqrt{2}\,X+1}. \end{aligned}$$

7. Examen 4

Exercice 1. On travaille dans l'anneau commutatif $\big(\mathbb{Z}/p\mathbb{Z}, +, \times\big)$ avec le nombre (magique) $p := 17$.

(a) Calculer le reste de la division euclidienne de $16 \cdot 15 \cdot 14$ par 17.

(b) Dans $\mathbb{Z}\big/17\mathbb{Z}$, calculer $\overline{2}^1$, $\overline{2}^2$, $\overline{2}^3$, $\overline{2}^4$, $\overline{2}^5$, $\overline{2}^6$, $\overline{2}^7$, $\overline{2}^8$.

(c) Déterminer le reste de la division euclidienne du nombre (magique) 2^{2222} par 17.

Exercice 2. On s'intéresse à des systèmes linéaires à coefficients entiers, dont on recherche les solutions entières, exclusivement.

(a) Résoudre dans $\mathbb{Z}^2$ l'équation :

$$-15\,x + 6\,y + 9 \;=\; 0.$$

(b) En déduire les solutions dans $\mathbb{Z}^3$ du système :

$$\begin{cases} 0 \;=\; -3\,x + 8\,y - 2\,z - 11, \\ 0 \;=\; 6\,x + y - z - 10. \end{cases}$$

Exercice 3. Soient deux groupes G et H, et soit $f\colon G \longrightarrow H$ un morphisme de groupes.

(a) Montrer que si un élément $x \in G$ est d'ordre fini égal à un certain entier $1 \leqslant m$, alors son image $f(x) \in H$ est aussi un élément d'ordre fini, que l'on notera $1 \leqslant n$.

(b) Justifier que $n \,|\, m$.

(c) Déterminer tous les morphismes de groupes additifs, de $G := \mathbb{Z}\big/11\mathbb{Z}$ à valeurs dans $H := \mathbb{Z}\big/23\mathbb{Z}$.

Exercice 4. (a) Montrer que le groupe $\big(\mathbb{Z}/14\mathbb{Z}\big)^\times$ des éléments inversibles pour la multiplication $\times$ dans l'anneau $\big(\mathbb{Z}/14\mathbb{Z}, +, \times\big)$ a pour éléments :

$$\big(\mathbb{Z}/14\mathbb{Z}\big)^\times \;=\; \big\{\overline{1},\, \overline{3},\, \overline{5},\, \overline{9},\, \overline{11},\, \overline{13}\big\}.$$

(b) Calculer, dans $\mathbb{Z}/14\mathbb{Z}$:

$$\overline{5}^0, \quad \overline{5}^1, \quad \overline{5}^2, \quad \overline{5}^3, \quad \overline{5}^4, \quad \overline{5}^5, \quad \overline{5}^6.$$

(c) Montrer que l'application :

$$\begin{array}{rccc} \varphi\colon & \big(\mathbb{Z}/6\mathbb{Z}, +\big) & \longrightarrow & \big((\mathbb{Z}/14\mathbb{Z})^\times, \times\big) \\ & \overline{c} \;=\; c \mod 6 & \longmapsto & \overline{5}^c, \end{array}$$

est bien définie, et est un *isomorphisme* de groupes.

(d) Montrer que $(\mathbb{Z}/14\mathbb{Z})^\times$ est un groupe cyclique.

(e) Le groupe $(\mathbb{Z}/12\mathbb{Z})^\times$ est-il cyclique ?

Exercice 5. On fixe un entier premier $p \geqslant 2$, on prend un entier relatif $a \in \mathbb{Z}$ qui n'est *pas* divisible par p, on introduit l'entier :

$$\mathrm{N} \,:=\, 1\,a \cdot 2\,a \cdot 3\,a \cdots (p-1)\,a,$$

et on se propose d'évaluer $\mathrm{N} \bmod p$ de deux manières différentes afin de redémontrer le Petit Théorème de Fermat.

(a) Vérifier que :

$$\mathrm{N} \,\equiv\, (p-1)!\,a^{p-1} \mod p.$$

(b) Pour k entier avec $1 \leqslant k \leqslant p-1$, on note r_k le reste de la division euclidienne de $k\,a$ par p, c'est-à-dire $k\,a = q_k\,p + r_k$ avec $0 \leqslant r_k \leqslant p-1$. Montrer qu'aucun reste r_k ne peut être nul.

(c) Montrer que les deux restes r_{k_1} et r_{k_2} associés à deux entiers quelconques $1 \leqslant k_1, k_2 \leqslant p-1$ satisfont :

$$0 \,\leqslant\, \big|r_{k_1} - r_{k_2}\big| \,\leqslant\, p-1.$$

(d) Établir qu'à deux entiers distincts $1 \leqslant k_1 \neq k_2 \leqslant p-1$ sont associés deux restes $r_{k_1} \neq r_{k_2}$ eux aussi *distincts*.

(e) En déduire que :

$$r_1 \cdots r_{p-1} \,=\, (p-1)!.$$

(f) Établir que :

$$a^{p-1} \,\equiv\, 1 \mod p.$$

Exercice 6. On rappelle que l'on note $\varphi(n)$ le nombre d'entiers $1 \leqslant k \leqslant n$ qui sont premiers avec un entier donné $n \geqslant 1$, où par convention $\varphi(1) = 1$ car 1 est premier avec lui-même.

(a) Avec $p \geqslant 2$ premier, et avec un exposant $r \geqslant 1$, que vaut $\varphi\big(p^r\big)$? Indication: Il suffit d'écrire la réponse sans la justifier, car c'est une question de cours. En cas d'oubli, il est évidemment autorisé de raisonner pour retrouver la valeur de $\varphi\big(p^r\big)$.

(b) Soient trois nombres premiers $2 < p_1 < p_2 < p_3$. On pose $m := p_1^3\,p_2^5$ et $n := p_2^7\,p_3$. Montrer que :

$$\frac{\varphi(m\,n)}{\varphi(m)\,\varphi(n)} \,=\, \frac{p_2}{\varphi(p_2)}.$$

(c) Généralement, soient deux nombres entiers quelconques $m, n \geqslant 1$ écrits sous la forme :

$$m \,=\, \prod_{1 \leqslant i \leqslant r} p_i^{\alpha_i} \prod_{1 \leqslant k \leqslant \mathrm{K}} P_k^{a_k},$$
$$n \,=\, \prod_{1 \leqslant i \leqslant r} p_i^{\beta_i} \prod_{1 \leqslant \ell \leqslant \mathrm{L}} Q_\ell^{b_\ell},$$

avec des nombres premiers deux à deux distincts $p_1, \ldots, p_r$, $P_1, \ldots, P_{\mathrm{K}}$, $Q_1, \ldots, Q_{\mathrm{L}}$, avec des exposants strictement positifs :

$$\alpha_1, \ldots, \alpha_r \,\geqslant\, 1, \qquad\qquad a_1, \ldots, a_{\mathrm{K}} \,\geqslant\, 1,$$
$$\beta_1, \ldots, \beta_r \,\geqslant\, 1, \qquad\qquad b_1, \ldots, b_{\mathrm{L}} \,\geqslant\, 1,$$

de telle sorte que :

$$\mathsf{pgcd}\,(m,\, n) \,=\, \prod_{1 \leqslant i \leqslant r} p_i^{\mathsf{min}(\alpha_i, \beta_i)}.$$

Montrer que :

$$\frac{\varphi(m\,n)}{\varphi(m)\,\varphi(n)} \;=\; \frac{p_1 \cdots p_r}{(p_1-1)\cdots(p_r-1)}.$$

Indication: Chercher à imiter le raisonnement de la question qui précède.

Exercice 7. (a) Soit $n = a\,b$ un entier composé, *i.e.* avec $1 < a < n$ et $1 < b < n$. On exclut $n = 4$, *i.e.* on suppose que $n \geqslant 5$. Montrer que $(n-1)!$ est divisible par n.
Indication: On pourra par exemple observer (et justifier) que $n > a + b$, puis utiliser le fait que $\frac{(a+b)!}{a!\,b!} \in \mathbb{N}$ est entier.

8. Corrigé de l'examen 4

Exercice 1. (a) Il s'agit seulement de lire ce produit modulo 17, et il vaut :

$$16 \cdot 15 \cdot 14 \equiv (-1) \cdot (-2) \cdot (-3) \equiv -6 \equiv 11 \mod 17.$$

(b) Il vient :

$$\begin{aligned}
\overline{2}^1 &= \overline{2}, \\
\overline{2}^2 &= \overline{4}, \\
\overline{2}^3 &= \overline{8}, \\
\overline{2}^4 &= \overline{16} = -\overline{1}, \\
\overline{2}^5 &= -\overline{1} \cdot \overline{2} = -\overline{2} = \overline{15}, \\
\overline{2}^6 &= -\overline{2} \cdot \overline{2} = -\overline{4} = \overline{13}, \\
\overline{2}^7 &= -\overline{4} \cdot \overline{2} = -\overline{8} = \overline{9}, \\
\overline{2}^8 &= -\overline{8} \cdot \overline{2} = -\overline{16} = \overline{1}.
\end{aligned}$$

(c) Ah, super ! On vient de constater que $2^8 \equiv 1 \mod 17$, donc divisons 2222 par 8 :

$$2222 = 277 \cdot 8 + 6,$$

pour engranger rapidement les points :

$$\overline{2}^{2222} = \left(\overline{2}^8\right)^{277} \overline{2}^6 = \overline{1}^{277}\, \overline{13} = \overline{13}.$$

Exercice 2. (a) Après division par 3, cette équation équivaut à :

$$-5\,x + 2\,y + 3 = 0.$$

Comme -5 et 2 sont premiers entre eux, un théorème du cours garantit qu'il existe une infinité de solutions, et d'ailleurs, ledit théorème décrit *toutes* les solutions.

L'idée de la démonstration est de deviner tout d'abord une solution particulière $(x_0, y_0) \in \mathbb{Z}^2$. « *Au doigt et à l'œil* », on trouve :

$$-5 \cdot 1 + 2 \cdot 1 + 3 = 0.$$

Ensuite, on soustrait la solution particulière d'une solution générale éventuelle, afin de faire disparaître la constante 3, ce qui donne :

$$-5\,(x-1) + 2\,(y-1) = 0.$$

Comme $5 \wedge 2 = 1$, et comme ces deux nombres sont premiers, grâce au théorème d'Euclide, on trouve la solution générale :

$$x - 1 = 2\,\boldsymbol{k} \qquad \text{et} \qquad y - 1 = 5\,\boldsymbol{k},$$

avec $\boldsymbol{k} \in \mathbb{Z}$ arbitraire.

Par acquit de conscience, il est avisé de vérifier que la solution trouvée est bien solution de l'équation initiale :

$$\begin{aligned} 0 &\overset{?}{=} -15\big(1+2\boldsymbol{k}\big)+6\big(1+5\boldsymbol{k}\big)+9 \\ &= -15+6+9-15\cdot 2\boldsymbol{k}+6\cdot 5\boldsymbol{k} \qquad\qquad \text{OUI !} \end{aligned}$$

(b) Depuis la deuxième équation, résolvons :

$$z := 6\,x+y-10,$$

puis remplaçons cette valeur de z dans la première équation :

$$\begin{aligned} 0 &= -3\,x+8\,y-12\,x-2\,y+20-11 \\ &= -15\,x+6\,y+9. \end{aligned}$$

Eurêka ! C'est la Question **(a)** !

Ainsi, la solution générale est :

$$\begin{aligned} x &= 1+2\boldsymbol{k}, \\ y &= 1+5\boldsymbol{k}, \\ z &= 6\big(1+2\boldsymbol{k}\big)+1+5\boldsymbol{k}-10 \\ &= -3+17\boldsymbol{k}, \end{aligned}$$

toujours avec $\boldsymbol{k}\in\mathbb{Z}$ arbitraire.

Comme toujours, mieux vaut vérifier tout cela en injectant dans le système initial :

$$0 \overset{?}{=} -3\big(1+2\boldsymbol{k}\big)+8\big(1+5\boldsymbol{k}\big)-2\big(-3+17\boldsymbol{k}\big)-11 \qquad \text{OUI !}$$

$$0 \overset{?}{=} 6\big(1+2\boldsymbol{k}\big)+1\big(1+5\boldsymbol{k}\big)-1\big(-3+17\boldsymbol{k}\big)-10 \qquad \text{OUI !}$$

Exercice 3. (a) Comme $e_G = x^m$, comme le morphisme f envoie l'élément neutre e_G sur l'élément neutre e_H, et comme f respecte les lois de groupes, il est clair que l'on a :

$$e_H \;=\; f(e_G) \;=\; f\big(x^m\big) \;=\; \big(f(x)\big)^m$$

Par définition même, cette identité signifie que l'élément $y := f(x)$ de H est d'ordre fini — mais pas forcément égal à m, éventuellement plus petit que m.

(b) Un théorème du cours a clairement fait voir, grâce à la division euclidienne standard dans $\mathbb{N}_{\geqslant 1}$, que si un élément $y\in H$ satisfait $y^m = e_H$, alors son ordre $o(y)$ — à savoir le plus petit exposant $\ell\geqslant 1$ tel que $y^\ell = e_H$ — *divise* m.

(c) Observons que $11\wedge 23 = 1$ sont premiers entre eux, ne serait-ce que parce que ce sont deux nombres premiers distincts !

Dans $\mathbb{Z}/p\,\mathbb{Z}$ avec p premier, nous savons que l'ordre de tout élément $\overline{a}$ non nul est exactement égal à p (tandis que $\overline{0}$ est trivialement d'ordre 1), parce que $\overline{a}$ additionné $\ell\geqslant 1$ fois avec lui-même donne $\ell\,\overline{a}$, avec $a\in\{1,2,\ldots,p-1\}$ premier avec p, donc $\overline{\ell\,a}$ vaut $\overline{0}$ si et seulement si $\ell\equiv 0 \mod p$.

Attention ! Nous parlons d'un morphisme entre groupes *additifs*. Donc l'hypothèse est que $f(\overline{0}) = \overline{0}$. et nous n'avons pas forcément $f(\overline{1}) = \overline{1}$, puisque nous ne parlons pas de morphismes entre groupes *multiplicatifs*.

Étant donné un morphisme $f\colon \mathbb{Z}/11\mathbb{Z} \longrightarrow \mathbb{Z}/23\mathbb{Z}$, que peut valoir l'image $f(\overline{1})$? L'ordre de $\overline{1}$ vaut 11. Nous venons de dire que l'ordre de $f(\overline{1})$ doit alors diviser 11. Or

à moins que $f(\overline{1})$ ne soit égal à $\overline{0}$ dans $\mathbb{Z}/23\mathbb{Z}$, son ordre doit être égal à 23. Mais 23 ne divise pas 11 ! Donc :

$$f(\overline{1}) \,=\, \overline{0},$$

puis $f\big(\overline{1}+\overline{1}\big) = \overline{0}$, et ainsi de suite, pour conclure que :

$$f\big(\mathbb{Z}/11\mathbb{Z}\big) \,=\, \overline{0}.$$

Le morphisme est obligatoirement trivial !

Exercice 4. **(a)** D'après le cours, un élément non nul $\overline{a}$ de $\mathbb{Z}/14\mathbb{Z}$ avec $a \in \{1, 2, \ldots, 13\}$ est inversible pour la multiplication si et seulement si $a \wedge 14 = 1$. Comme $14 = 2 \cdot 7$, on élimine tous les multiples de 2 et/ou de 7, et il reste six éléments :

$$\mathbb{Z}/14\mathbb{Z} \,=\, \big\{\overline{1},\, \overline{3},\, \overline{5},\, \overline{9},\, \overline{11},\, \overline{13}\big\}.$$

(b) On trouve :

$$\overline{5}^0 \,=\, \overline{1}, \quad \overline{5}^1 \,=\, \overline{5}, \quad \overline{5}^2 \,=\, \overline{11}, \quad \overline{5}^3 \,=\, \overline{13}, \quad \overline{5}^4 \,=\, \overline{9}, \quad \overline{5}^5 \,=\, \overline{3}, \quad \overline{5}^6 \,=\, \overline{1},$$

et on constate qu'à la puissance sixième, on revient au point de départ.

(c) Il est clair que :

$$\overline{5}^0 \,=\, \overline{1},$$
$$\overline{5}^{c \bmod 6} \times \overline{5}^{c' \bmod 6} \,=\, \overline{5}^{c+c' \bmod 6},$$

puisque nous venons de voir que $\overline{5}^6 = \overline{1}$. Cette application φ est donc bien définie, et est un morphisme de groupes.

Qui plus est, φ est surjective grâce à la Question **(b)**. Comme les deux groupes $\mathbb{Z}/6\mathbb{Z}$ et $(\mathbb{Z}/14\mathbb{Z})^\times$ sont tous deux de cardinal égal à 6, ceci implique que φ est *bijective*. Ainsi, φ est bien un *isomorphisme de groupes*.

(d) Nous savons que les groupes additifs $\big(\mathbb{Z}/n\mathbb{Z}, +\big)$ sont cycliques, engendrés par $\overline{1}$, puisque $\overline{1}$ additionné k fois avec lui-même fournit l'élément $\overline{k}$ de $\mathbb{Z}/n\mathbb{Z}$, pour $k = 1, 2, \ldots, n-1$.

En particulier, $\big(\mathbb{Z}/6\mathbb{Z}, +\big)$ est cyclique.

Et comme φ est un *isomorphisme* de groupes, φ transmet instantanément cette propriété d'être cyclique à $(\mathbb{Z}/14\mathbb{Z})^\times$.

(e) Reprenons pas à pas les raisonnements que nous venons d'effectuer pour $(\mathbb{Z}/14\mathbb{Z})^\times$. Tout d'abord :

$$\big(\mathbb{Z}/12\mathbb{Z}\big)^\times \,=\, \big\{\overline{1},\, \overline{5},\, \overline{7},\, \overline{11}\big\}.$$

Ensuite, si $(\mathbb{Z}/12\mathbb{Z})^\times$ était cyclique, il existerait, parmi ses quatre éléments, un certain élément $\overline{a}$ dont les quatre puissances $\overline{a}^0$, $\overline{a}^1$, $\overline{a}^2$, $\overline{a}^3$ serait distinctes et décriraient tous les quatre éléments $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$.

Évidemment, $\overline{a} = \overline{1}$ ne marche pas, et les trois autres non plus, d'ailleurs, puisque :

$$\begin{aligned}
&\overline{5}^0 \,=\, \overline{1}, \qquad \overline{5}^1 \,=\, \overline{5}, \qquad \overline{5}^2 \,=\, \overline{1}, \qquad \overline{5}^3 \,=\, \overline{5},\\
&\overline{7}^0 \,=\, \overline{1}, \qquad \overline{7}^1 \,=\, \overline{7}, \qquad \overline{7}^2 \,=\, \overline{1}, \qquad \overline{7}^3 \,=\, \overline{7},\\
&\overline{11}^0 \,=\, \overline{1}, \qquad \overline{11}^1 \,=\, \overline{11}, \qquad \overline{11}^2 \,=\, \overline{1}, \qquad \overline{11}^3 \,=\, \overline{11}.
\end{aligned}$$

En conclusion, $(\mathbb{Z}/12\mathbb{Z})^\times$ n'est *pas* cyclique — *snif!*

Exercice 5. (a) C'est instantané, grâce à la commutativité de la multiplication dans $\mathbb{Z}$, cette relation étant d'ailleurs une égalité $\mathrm{N} = (p-1)!\, a^{p-1}$, que l'on « projette » ensuite modulo p.

(b) Par l'absurde, si un reste $r_k = 0$ était nul, on aurait $k\, a = q_k\, p + 0$, ce qui impliquerait que p divise $k\, a$. Or comme tous les entiers $k \in \{1, 2, \ldots, p-1\}$ sont premiers avec l'entier premier p car strictement inférieurs à p, le Théorème d'Euclide forcerait alors p à diviser a, ce qui contredirait l'hypothèse que a n'est *pas* divisible par p.

(c) Par définition du reste de la division euclidienne par p, avec deux entiers $k_1, k_2 \in \{1, \ldots, n\}$, nous avons :

$$\begin{aligned} 0 \;&\leqslant\; r_{k_1} \;\leqslant\; p-1, \\ 0 \;&\leqslant\; r_{k_2} \;\leqslant\; p-1, \end{aligned}$$

d'où par soustractions croisées — comme nous l'avons fait plusieurs fois en cours — :

$$0 - (p-1) \;\leqslant\; r_{k_1} - r_{k_2} \;\leqslant\; p - 1 - 0,$$

c'est-à-dire comme indiqué :

$$0 \;\leqslant\; \big|r_{k_1} - r_{k_2}\big| \;\leqslant\; p-1.$$

(d) Avec deux entiers distincts quelconques $1 \leqslant k_1 \neq k_2 \leqslant p-1$, écrivons modulo p :

$$\begin{aligned} k_1\, a \;&\equiv\; r_{k_1}, \\ k_2\, a \;&\equiv\; r_{k_2}, \end{aligned}$$

puis soustrayons :

$$\big(k_1 - k_2\big)\, a \;\equiv\; r_{k_1} - r_{k_2}.$$

Ensuite, observons par soustractions croisées entre :

$$\begin{aligned} 1 \;&\leqslant\; k_1 \;\leqslant\; p-1, \\ 1 \;&\leqslant\; k_2 \;\leqslant\; p-1, \end{aligned}$$

que :

$$1 - (p-1) \;\leqslant\; \underbrace{k_1 - k_2}_{\neq 0} \;\leqslant (p-1) - 1,$$

c'est-à-dire :

$$1 \;\leqslant\; \big|k_1 - k_2\big| \;\leqslant\; p-2,$$

et donc manifestement, $k_1 - k_2$ ne peut pas être divisible par p.

Comme $p \nmid a$ aussi, nous voyons que le membre de gauche ci-dessus $(k_1 - k_2)\, a$ n'est *pas* congru à zéro modulo p.

Donc le membre de droite $r_{k_1} - r_{k_2}$ n'est *pas* non plus congru à zéro modulo p. Autrement dit, $r_{k_1} - r_{k_2} \neq \ell\, p$ pour tout entier $\ell \in \mathbb{Z}$.

Enfin, comme $\big|r_{k_1} - r_{k_2}\big| \leqslant p-1$, nous concluons que $r_{k_1} - r_{k_2} \neq 0$, comme désiré.

(e) Comme les $p-1$ restes $r_1, \ldots, r_{p-1}$, qui appartiennent à l'ensemble $\{1, \ldots, p-1\}$ de cardinal $p-1$, sont mutuellement distincts, il est clair qu'ils décrivent tout cet ensemble :

$$\big\{r_1, r_2, \ldots, r_{p-1}\big\} \;=\; \big\{1, 2, \ldots, p-1\big\},$$

et donc :

$$r_1 \cdot r_2 \cdots r_{p-1} \;=\; 1 \cdot 2 \cdots (p-1).$$

(f) Comme promis, en utilisant $k\,a \equiv r_k \bmod p$, calculons d'une deuxième manière l'entier-produit N modulo p :

$$\begin{aligned} \mathrm{N} \bmod p &\equiv 1\,a \cdot 2\,a \cdots (p-1)\,a \\ &\equiv r_1 \cdot r_2 \cdots r_{p-1} \bmod p \\ &\equiv 1 \cdot 2 \cdots (p-1) \bmod p \\ &\equiv (p-1)! \bmod p. \end{aligned}$$

[Question **(e)**]

Une comparaison avec la Question **(a)** donne alors :

$$(p-1)!\,a^{p-1} \equiv (p-1)! \bmod p,$$

et comme $(p-1)!$ est premier avec p, on peut éliminer $(p-1)!$ dans cette relation de congruence pour atteindre le Petit Théorème de Fermat :

$$a^{p-1} \equiv 1 \bmod p \qquad (p \text{ premier},\ a \wedge p = 1).$$

Exercice 6. (a) D'après le cours :

$$\varphi\big(p^r\big) = p^r - p^{r-1}.$$

(b) Le cours a établi que pour deux entiers $r, s \geqslant 1$ premiers entre eux $1 = r \wedge s$, on a la multiplicativité $\varphi(r\,s) = \varphi(r)\,\varphi(s)$. Toutefois ici, m et n ne sont pas premiers entre eux, puisque $\mathsf{pgcd}(m,n) = p_2^5$.

En tout cas, nous pouvons calculer :

$$\begin{aligned} \varphi(m) &= \varphi\big(p_1^3\,p_2^5\big) = \varphi\big(p_1^3\big)\,\varphi\big(p_2^5\big) = \big(p_1^3 - p_1^2\big)\,\big(p_2^5 - p_2^4\big), \\ \varphi(n) &= \varphi\big(p_2^7\,p_3\big) = \varphi\big(p_2^7\big)\,\varphi\big(p_3\big) = \big(p_2^7 - p_2^6\big)\,\big(p_3 - 1\big), \end{aligned}$$

ainsi que :

$$\varphi\big(m\,n\big) = \varphi\big(p_1^3\,p_2^{12}\,p_3\big) = \big(p_1^3 - p_1^2\big)\,\big(p_2^{12} - p_2^{11}\big)\,\big(p_3 - 1\big).$$

Par conséquent, nous avons bien :

$$\begin{aligned} \frac{\varphi(m\,n)}{\varphi(m)\,\varphi(n)} &= \frac{(p_1^3 - p_1^2)\,(p_2^{12} - p_2^{11})\,(p_3 - 1)}{(p_1^3 - p_1^2)(p_2^5 - p_2^4) \cdot (p_2^7 - p_2^6)\,(p_3 - 1)} \\ &= \frac{p_2^{11}\,(p_2 - 1)}{p_2^4\,(p_2 - 1)\,p_2^6\,(p_2 - 1)} \\ &= \frac{p_2}{(p_2 - 1)} \\ &= \frac{p_2}{\varphi(p_2)}. \end{aligned}$$

(c) La formule connue donne :

$$\begin{aligned} \varphi(m) &= \prod_{1 \leqslant i \leqslant r} p_i^{\alpha_i - 1}\,\big(p_i - 1\big) \prod_{1 \leqslant k \leqslant \mathrm{K}} P_k^{a_k - 1}\,\big(P_k - 1\big), \\ \varphi(n) &= \prod_{1 \leqslant i \leqslant r} p_i^{\beta_i - 1}\,\big(p_i - 1\big) \prod_{1 \leqslant \ell \leqslant \mathrm{L}} Q_\ell^{b_\ell - 1}\,\big(Q_\ell - 1\big), \\ \varphi\big(m\,n\big) &= \prod_{1 \leqslant i \leqslant r} p_i^{\alpha_i + \beta_i - 1}\,\big(p_i - 1\big) \prod_{1 \leqslant k \leqslant \mathrm{K}} P_k^{a_k - 1}\,\big(P_k - 1\big) \prod_{1 \leqslant \ell \leqslant \mathrm{L}} Q_\ell^{b_\ell - 1}\,\big(Q_\ell - 1\big), \end{aligned}$$

d'où le résultat demandé :

$$\begin{aligned}\frac{\varphi(m\,n)}{\varphi(m)\,\varphi(n)} &= \frac{\prod_i p_i^{\alpha_i+\beta_i-1}\,(p_i-1)}{\prod_i p_i^{\alpha_i-1}\,(p_i-1)\ \prod_i p_i^{\beta_i-1}\,(p_i-1)}\\ &= \frac{\prod_{1\leqslant i\leqslant r} p_i}{\prod_{1\leqslant i\leqslant r}(p_i-1)}\\ &= \frac{p_1\cdots p_r}{(p_1-1)\cdots(p_r-1)}.\end{aligned}$$

Exercice 7. (a) On peut supposer $2 \leqslant a \leqslant b$. Comme $n \geqslant 5$, au moins une de ces deux inégalités est stricte, sinon $2 = a = b$ donnerait $n = a\,b = 4$.

On en déduit :

$$n \;=\; a\,b \;\geqslant\; 2\,b \;\geqslant\; a+b,$$

avec à nouveau encore au moins une inégalité stricte, car $a\,b \;=\; 2\,b \;=\; a+b$ forcerait $b = 2 = a$. Donc $n > a+b$, c'est-à-dire $n-1 \geqslant a+b$, et comme le quotient $\frac{(a+b)!}{a!\,b!} \in \mathbb{N}$ est toujours entier puisque c'est un nombre binomial, on conclut grâce à la transitivité de la relation de divisibilité :

$$(n-1)\,!\text{ divisible par }(a+b)\,!\text{ divisible par }a!\,b!\text{ divisible par }a\,b.$$

9. Examen 5

Exercice 1. Soit la permutation suivante d'un ensemble à 13 éléments :

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 8 & 12 & 13 & 1 & 2 & 11 & 7 & 9 & 3 & 5 & 6 & 10 & 4 \end{pmatrix}.$$

(a) Décomposer σ en produit de cycles à supports disjoints.

(b) Déterminer l'ordre $o(\sigma)$ de σ.

(c) Déterminer la décomposition explicite de σ^{2023} en cycles disjoints.

Exercice 2. (a) Déterminer le reste de la division de $X^{96} - X^{25}$ par $X^2 + 1$.

(b) Déterminer les entiers $n \geqslant 1$ tels que :

$$X^3 - X^2 + X - 1 \,\Big|\, \big(X^2 - X + 1\big)^n - X^{2n} + X^n - 1.$$

Indication: On pourra factoriser $X^3 - X^2 + X - 1$ afin d'en déterminer les trois racines complexes.

Exercice 3. Soit un nombre premier $p \geqslant 2$ quelconque. On considère le groupe $\mathfrak{S}_p$ des permutations de l'ensemble $\{1, 2, \ldots, p\}$.

(a) Montrer qu'un élément arbitraire σ du groupe $\mathfrak{S}_p$ est un p-cycle si et seulement si son ordre vaut $p = o(\sigma)$.

(b) Trouver un nombre $n \geqslant 4$ non premier tel que, dans le groupe $\mathfrak{S}_n$ des permutations de $\{1, 2, \ldots, n\}$, il existe un exemple d'élément $\sigma \in \mathfrak{S}_n$ d'ordre égal à n qui n'est *pas* un n-cycle.

Exercice 4. (a) Sur un corps commutatif $\mathbb{K}$, soit un polynôme unitaire du troisième degré $p := x^3 + \lambda\, x^2 + \mu\, x + \nu$. Montrer que p est réductible sur $\mathbb{K}$ si et seulement si il possède une racine dans $\mathbb{K}$.

(b) Soit le corps $\mathbb{K} := \mathbb{Z}/7\mathbb{Z}$ des classes résiduelles modulo 7. Montrer que le polynôme :

$$x^3 + x^2 + \overline{2}\, x + \overline{5}$$

est réductible, en exhibant une factorisation par deux polynômes de degrés 1 et 2.

(c) Montrer que le polynôme $x^2 + \overline{3}\, x + \overline{1}$ est *irréductible* sur $\mathbb{K}[x]$ où $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$.

(d) Dans $\mathbb{K}[x]$ avec $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$, effectuer la division euclidienne de $x^3 + \overline{2}\, x^2 + \overline{3}\, x + \overline{4}$ par $x^3 + x^2 + \overline{2}\, x + \overline{5}$.

(e) Toujours dans $\mathbb{K}[x]$ avec $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$, décomposer en éléments simples la fraction rationnelle :

$$\frac{x^3 + \overline{2}\, x^2 + \overline{3}\, x + \overline{4}}{x^3 + x^2 + \overline{2}\, x + \overline{5}}.$$

Exercice 5. Dans $\mathbb{Q}[x]$, on introduit les trois polynômes :

$$\begin{aligned} D &:= x^2 + 2\,x + 5, \\ Q &:= x^5 + x^4 + 4\,x^3 - 4\,x^2 + 3\,x - 5, \\ P &:= x^6 + 4\,x^5 + 12\,x^4 + 15\,x^3 + 17\,x^2 + 3\,x + 20. \end{aligned}$$

(a) Effectuer la division euclidienne de Q par D, constater que le reste est nul, et enfin, vérifier que le résultat obtenu est correct.

(b) Diviser P par D. Ensuite, vérifier le résultat obtenu.

(c) L'objectif, maintenant, est de déterminer le pgcd entre les deux polynômes de $\mathbb{Q}[x]$:

$$\begin{aligned} B &:= x^3 - x^2 + x - 1, \\ A &:= x^4 + 2\,x^3 + 3\,x^2 - x + 4. \end{aligned}$$

En appliquant l'algorithme d'Euclide sans faire d'erreur de calcul, démontrer que :

$$\mathsf{pgcd}\,\big(A,\,B\big) \;=\; \frac{2925}{256}.$$

(d) Déterminer $\mathsf{pgcd}\,(P, Q)$. Indication: On rappelle que le pgcd est défini à une constante non nulle près.

Exercice 6. Soit $P(X) = a_0 + a_1\,X + \cdots + a_n\,X^n \in \mathbb{R}[X]$ un polynôme à coefficients réels, de degré $n \geqslant 1$, avec $a_n \neq 0$. On suppose qu'il ne prend que des valeurs positives sur $\mathbb{R}$:

$$P(x) \;\geqslant\; 0 \qquad (\forall\, x \in \mathbb{R}).$$

(a) Montrer que $a_n > 0$.

(b) Montrer que $n \in 2\,\mathbb{N}^*$ est pair.

(c) Montrer que les racines réelles $\alpha \in \mathbb{R}$ de $P(X)$ sont de multiplicité paire. Indication: Considérer le comportement de $(x - \alpha)^m$ pour $x \sim \alpha$ proche de α.

(d) Justifier l'écriture :

$$P(X) \;=\; a_n \prod_{i=1}^{s} \big(X - \alpha_i\big)^{2m_i} \prod_{j=1}^{t} \big(X^2 + c_j\,X + d_j\big)^{q_j},$$

et donner des informations sur les c_j, d_j.

(e) Montrer qu'il existe un polynôme $C \in \mathbb{C}[X]$ tel que :

$$P \;=\; C\,\overline{C}.$$

(f) En déduire qu'il existe A et B dans $\mathbb{R}[X]$ tels que :

$$P \;=\; A^2 + B^2.$$

Exercice 7. Soit un polynôme dans $\mathbb{C}[X]$ à coefficients complexes de degré $n \geqslant 1$:

$$P(X) \;:=\; \sum_{k=0}^{n} a_k\,X^k \qquad (a_n \neq 0).$$

L'objectif est de le diviser avec reste par $X^\ell - 1$, où $\ell \geqslant 1$ est un entier fixé quelconque.

(a) Factoriser $X^{q\,\ell} - 1$ par $X^\ell - 1$, où $q \geqslant 0$ est un entier arbitraire. Indication: Factoriser d'abord $Y^q - 1$ par $Y - 1$.

(b) Pour chaque entier $k \in \{0, 1, \dots, n\}$, on note r_k le reste de la division euclidenne de k par ℓ. Montrer que le reste de la division euclidienne de $P(X)$ par $X^\ell - 1$ est le polynôme :

$$R(X) \,:=\, \sum_{k=0}^{n} a_k \, X^{r_k}.$$

Exercice 8. Soit $\mathrm{N} \geqslant 1$, soit $\mathfrak{S}_\mathrm{N}$ le groupe des permutations de $\big\{1, 2, \dots, \mathrm{N}\big\}$, et soit $\sigma \in \mathfrak{S}_\mathrm{N}$ un *cycle*, de longueur n avec $2 \leqslant n \leqslant \mathrm{N}$.

L'objectif est d'établir que pour tout entier $m \geqslant 1$, la permutation :

$$\tau \,:=\, \sigma^m,$$

se décompose en $\mathsf{pgcd}\,(n, m)$ cycles de longueur $\frac{n}{\mathsf{pgcd}(n,m)}$. Par convention dans cet exercice, un *cycle de longueur* 1 dans la décomposition d'une permutation est un *point fixe* sous l'action de cette permutation.

(a) Montrer qu'il suffit d'établir le résultat pour $\mathrm{N} = n$ et pour la permutation circulaire $\sigma = \big(1 \;\, 2 \;\, \cdots \;\, n\big)$.

(b) On suppose donc que σ est le n-cycle $\sigma = \big(1 \;\, 2 \;\, \cdots \;\, n\big)$ appartenant à $\mathfrak{S}_n$, avec $n \geqslant 2$, c'est-à-dire que :

$$\sigma(i) \,:=\, i + 1 \;\; \mathsf{mod}\; n.$$

On écrit $m = d\,m'$, puis $n = d\,n'$, où $d := \mathsf{pgcd}\,(m, n)$, avec bien sûr $1 = m' \wedge n'$.

Pour un élément arbitraire fixé $i \in \big\{1, 2, \dots, n\big\}$, montrer que l'orbite de i par τ :

$$\mathsf{Orb}_\tau(i) \,=\, \big\{\tau^\ell(i) \colon \;\; \ell \in \mathbb{Z}\big\},$$

est constituée des n' éléments *distincts* suivants :

$$\big\{i, \;\, i + m, \;\, i + 2\,m, \;\, \dots, \;\, i + (n' - 1)\,m\big\} \;\; \mathsf{mod}\, n.$$

Indication: En appliquant un résultat du cours, il suffit de déterminer :

$$v \,:=\, \mathsf{min}\,\big\{\ell \in \mathbb{N}_{\geqslant 1} \colon \;\; \tau^\ell(i) = i\big\}.$$

(c) Soient deux orbites avec $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant n$:

$$\begin{aligned}
\mathsf{Orb}_\tau(i) \,&=\, \big\{i, \;\, i + m, \;\, \dots, \;\, i + (n' - 1)\,m\big\} \;\; \mathsf{mod}\, n, \\
\mathsf{Orb}_\tau(j) \,&=\, \big\{j, \;\, j + m, \;\, \dots, \;\, j + (n' - 1)\,m\big\} \;\; \mathsf{mod}\, n.
\end{aligned}$$

Montrer que :

$$\mathsf{Orb}_\tau(i) \,=\, \mathsf{Orb}_\tau(j) \qquad\qquad \Longrightarrow \qquad\qquad i \,\equiv\, j \;\; \mathsf{mod}\; d.$$

Indication: Deux orbites sont égales si et seulement si elles ont un élément en commun.

(d) Montrer qu'on a la réunion disjointe :

$$\big\{1, \;\, 2, \;\, \dots, \;\, n\big\} \,=\, \mathsf{Orb}_\tau(1) \cup \cdots \cup \mathsf{Orb}_\tau(d).$$

(e) Si $\sigma \in \mathfrak{S}_\mathrm{N}$ est un n-cycle, avec $n \geqslant 2$, et si $m \geqslant 1$ est un entier, en déduire les deux cas particuliers suivants :

• lorsque $m \,|\, n$, la permutation $\tau \,=\, \sigma^m$ se décompose en m cycles de longueur $\frac{n}{m}$, à supports disjoints ;

• lorsque $m \wedge n = 1$ sont premiers entre eux, σ^m est aussi un n-cycle de même longueur que σ.

(f) Le résultat subsiste-t-il si l'on remplace $\mathfrak{S}_{\mathrm{N}}$ par $\mathfrak{S}(E)$, où E est un ensemble fini vraiment quelconque à $\mathrm{N} \geqslant 1$ éléments ?

(g) Soit $\sigma \in \mathfrak{S}_{25}$ de type $\big(12, 8, 6, 1\big)$. Calculer le type de σ^4.

10. Corrigé de l'examen 5

Exercice 1. **(a)** Une lecture directe montre que :

$$\begin{aligned}
&1 \longmapsto 8 \longmapsto 9 \longmapsto 3 \longmapsto 13 \longmapsto 4 \longmapsto 1,\\
&2 \longmapsto 12 \longmapsto 10 \longmapsto 5 \longmapsto 2,\\
&6 \longmapsto 11,\\
&7 \longmapsto 7.
\end{aligned}$$

Ainsi, σ se décompose en produit de trois cycles à supports disjoints, plus un point fixe :

$$\begin{aligned}
\sigma &= \big(1\ 8\ 9\ 3\ 13\ 4\big) \circ \big(2\ 12\ 10\ 5\big) \circ \big(6\ 11\big) \circ \big(7\big)\\
&=: c_6 \circ c_4 \circ c_2 \circ c_1.
\end{aligned}$$

(b) Rappelons que, dans le groupe $\mathfrak{S}_n$ des permutations de l'ensemble $\big\{1, 2, \dots, n\big\}$ à $n \geqslant 1$ éléments, l'ordre d'un p-cycle quelconque :

$$c_p = \Big(a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_{p-1} \longrightarrow a_p \Big),$$

avec $a_1, a_2, \dots, a_{p-1}, a_p \in \{1, \dots, n\}$ distincts, vaut :

$$p = \boldsymbol{o}(c_p).$$

Rappelons aussi que les points fixes, tels que (7) ci-dessus, peuvent par léger abus de pensée, être considérés comme des 1-cycles.

Alors d'après un théorème vu en cours :

$$\begin{aligned}
\boldsymbol{o}(\sigma) &= \boldsymbol{o}\big(c_6 \circ c_4 \circ c_2 \circ c_1\big)\\
&= \mathsf{ppcm}\,\Big(\boldsymbol{o}\big(c_6\big), \boldsymbol{o}\big(c_4\big), \boldsymbol{o}\big(c_2\big), \boldsymbol{o}\big(c_1\big), \Big)\\
&= \mathsf{ppcm}\,\big(6,\ 4,\ 2,\ 1\big)\\
&= 12.
\end{aligned}$$

(c) Comme $\sigma^{12} = \mathsf{Id}$, d'où pour tout entier $r \in \mathbb{Z}$:

$$\sigma^r = \sigma^{\,r \bmod 12},$$

il est avisé de diviser 2023 par 12 :

$$2023 = 7 + 168 \cdot 12,$$

d'où puisque les cycles à supports disjoints commutent entre eux et puisque $(c_p)^p = \mathsf{Id}$ pour tout p-cycle c_p :

$$\begin{aligned}\sigma^{2023} &= \sigma^7\\ &= \Big(c_6 \circ c_4 \circ c_2 \circ c_1\Big)^7\\ &= (c_6)^7 \circ (c_4)^7 \circ (c_2)^7 \circ \mathsf{Id}\\ &= c_6 \circ c_4^{-1} \circ c_2.\end{aligned}$$

Mais l'inverse c_4^{-1} de :

$$c_4 = \Big(2 \rightleftarrows 12 \longrightarrow 10 \longrightarrow 5 \Big),$$

se calcule simplement en renversant les flèches :

$$c_4^{-1} = \Big(2 \rightleftarrows 12 \longleftarrow 10 \longleftarrow 5 \Big),$$

c'est-à-dire :

$$c_4^{-1} = \big(2\ \ 5\ \ 10\ \ 12\big).$$

En conclusion :

$$\begin{aligned}\sigma^{2023} &= \big(1\ \ 8\ \ 9\ \ 3\ \ 13\ \ 4\big) \circ \big(2\ \ 5\ \ 10\ \ 12\big) \circ \big(6\ \ 11\big) \circ \big(7\big)\\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13\\ 8 & 5 & 13 & 1 & 10 & 11 & 7 & 9 & 3 & 12 & 6 & 2 & 4 \end{pmatrix}.\end{aligned}$$

Exercice 2. **(a)** Il suffit de raisonner astucieusement modulo X^2+1, sans avoir à calculer le quotient $Q(X)$ dans la division euclidienne :

$$X^{96} - X^{25} = Q(X)\,(X^2+1) + R(X).$$

En effet, modulo X^2+1, on a $X^2 \equiv -1$. Donc modulo X^2+1, il est clair que :

$$X^{96} \equiv (-1)^{48} \equiv 1 \qquad \text{et} \qquad -X^{25} \equiv -X\,X^{24} \equiv -X\,(-1)^{12} \equiv -X,$$

d'où la réponse :

$$R(X) = -X + 1.$$

(b) Factorisons donc :

$$X^3 - X^2 + X - 1 = (X-1)\big(X^2+1\big).$$

Les trois racines, distinctes, sont 1, i, $-i$.

Ensuite, avec $n \geqslant 1$ entier, pour que le polynôme $\big(X^2 - X + 1\big)^n - X^{2n} + X^n - 1$ soit divisible par $(X-1)(X-i)(X+i)$, il faut et il suffit qu'il ait 1, i, $-i$ pour racines.

Clairement, 1 est toujours racine, quel que soit $n \geqslant 1$. De plus, i et $-i$ sont racines si et seulement si :

$$\begin{aligned}0 &= (-i)^n - (-1)^n + i^n - 1,\\ 0 &= i^n - (-1)^n + (-i)^n - 1,\end{aligned}$$

ces deux équations étant identiques, éuivalentes à l'équation factorisée :

$$0 = \big((-1)^n + 1\big)\,\big(i^n - 1\big).$$

On voit aisément que cette équation est satisfaite si et seulement si $n \neq 2 + 4\,m$, avec $m \geqslant 0$ entier.

Exercice 3. (a) Tout d'abord, on sait que l'ordre d'un cycle est égal à sa longueur, donc l'implication $\Longrightarrow$ est immédiate.

Réciproquement, soit $\sigma \in \mathfrak{S}_p$ d'ordre $p = o(\sigma)$, donc d'ordre $\geqslant 2$, car tout nombre premier p est $\geqslant 2$. En particulier, $\sigma \neq \mathsf{Id}$. Nous devons démontrer que σ est un p-cycle.

D'après un théorème du cours, $\sigma \in \mathfrak{S}_p$ se décompose en produit :

$$\sigma \,=\, c_1 \circ \cdots \circ c_k,$$

d'un certain nombre $k \,\geqslant\, 1$ de cycles c_i à supports disjoints ayant une certaine longueur $\ell_i \geqslant 2$, cela, pour $i = 1, \ldots, k$.

D'après un autre théorème du cours, nous savons aussi que :

$$\begin{aligned} p \,=\, o(\sigma) \,&=\, \mathsf{ppcm}\Big(o\big(c_1\big),\, \ldots,\, o\big(c_k\big)\Big) \\ &=\, \mathsf{ppcm}\,\big(\ell_1, \ldots, \ell_k\big). \end{aligned}$$

Comme les cycles sont à supports disjoints dans l'ensemble $\{1, \ldots, p\}$ de longueur p, nous avons l'inégalité :

$$p \,\geqslant\, \ell_1 + \cdots + \ell_k.$$

Si l'une des longueurs ℓ_i était $\leqslant p - 1$, le ppcm à droite ci-dessus serait divisible par ℓ_i, et alors, ℓ_i diviserait p à gauche, en contradiction avec l'hypothèse que p est premier.

Donc $\ell_i = p$ nécessairement, et enfin, $k = 1$ à cause de l'inégalité ci-dessus. En définitive, σ se décompose bien en un unique cycle de longueur p.

(b) Après réflexion au brouillon, on se rend compte que ni $n = 4$ ni $n = 5$ ne peuvent produire d'exemple.

Mais avec :

$$n \,:=\, 6 \,=\, 2 \cdot 3 \,=\, \mathsf{ppcm}\,(2, 3),$$

il suffit de prendre pour σ un produit de deux cycles à supports disjoints de longueurs égales à 2 et à 3, par exemple :

$$\sigma \,:=\, \big(1\ 2\big) \circ \big(4\ 5\ 6\big) \qquad (\sigma(3) = 3).$$

Clairement, σ n'est *pas* un 6-cycle, et son ordre vaut bien :

$$o(\sigma) \,=\, \mathsf{ppcm}\Big(o\big(1\ 2\big),\ o\big(4\ 5\ 6\big)\Big) \,=\, \mathsf{ppcm}\,(2,\ 3) \,=\, 6 \,=\, n.$$

Exercice 4. (a) Si p est réductible, puisque $3 = 1 + 2$ est la seule possibilité au niveau des degrés, il se factorise :

$$p(x) \,=\, (x - \alpha)\,(x^2 + \beta\, x + \gamma),$$

en un produit de deux polynômes unitaires de degré 1, à coefficients dans $\mathbb{K}$. Mais alors, α est une racine de $p(x)$ dans $\mathbb{K}$.

Inversement, s'il existe $\alpha \in \mathbb{K}$ tel que $p(\alpha) = 0$, on a vu dans le cours que le polynôme se factorise par $(x - \alpha)$:

$$p(x) \,=\, (x - \alpha)\, q(x),$$

avec un polynôme $q(x)$ de degré 2, unitaire, à coefficients dans $\mathbb{K}$, donc de la forme $x^2 + \beta\, x + \gamma$. Ainsi, $p(x) = (x - \alpha)\,(x^2 + \beta\, x + \gamma)$ se décompose en produit de deux polynômes de degrés 1 et 2 à coefficients dans $\mathbb{K}$, ce qui montre que p est bien réductible.

(b) Pour $x = \overline{a} \in \mathbb{Z}/7\mathbb{Z}$, calculons les valeurs que prend ce polynôme :

$$\begin{aligned}
\overline{0}^3 + \overline{0}^2 + \overline{2}\cdot\overline{0} + \overline{5} &= \overline{5} = \overline{5}\\
\overline{1}^3 + \overline{1}^2 + \overline{2}\cdot\overline{1} + \overline{5} &= \overline{9} = \overline{2}\\
\overline{2}^3 + \overline{2}^2 + \overline{2}\cdot\overline{2} + \overline{5} &= \overline{21} = \overline{0}\\
\overline{3}^3 + \overline{3}^2 + \overline{2}\cdot\overline{3} + \overline{5} &= \overline{47} = \overline{5}\\
\overline{4}^3 + \overline{4}^2 + \overline{2}\cdot\overline{4} + \overline{5} &= \overline{93} = \overline{2}\\
\overline{5}^3 + \overline{5}^2 + \overline{2}\cdot\overline{5} + \overline{5} &= \overline{165} = \overline{4}\\
\overline{6}^3 + \overline{6}^2 + \overline{2}\cdot\overline{6} + \overline{5} &= \overline{269} = \overline{3}.
\end{aligned}$$

Ainsi, $\overline{2}$ est une racine. Grâce à la Question **(a)** qui précède, notre polynôme cubique est réductible, factorisable par :

$$x - \overline{2} = x + \overline{5}.$$

Une division euclidienne donne alors :

$$x^3 + x^2 + \overline{2}\,x + \overline{5} = \big(x + \overline{5}\big)\big(x^2 + \overline{3}\,x + \overline{1}\big).$$

(c) Un raisonnement tout à fait similaire à celui qui a été conduit en **(a)** montre qu'un polynôme quadratique monique $x^2 + \lambda\,x + \mu$ à coefficients dans un corps $\mathbb{K}$ est irréductible si et seulement si il n'admet aucune racine dans $\mathbb{K}$.

Calculons alors les valeurs que prend la fonction $x \longmapsto x^2 + \overline{3}\,x + \overline{1}$ sur les sept éléments de $\mathbb{Z}/7\mathbb{Z}$:

$$\begin{aligned}
\overline{0}^2 + \overline{3}\cdot\overline{0} + \overline{1} &= \overline{1} = \overline{1},\\
\overline{1}^2 + \overline{3}\cdot\overline{1} + \overline{1} &= \overline{5} = \overline{5},\\
\overline{2}^2 + \overline{3}\cdot\overline{2} + \overline{1} &= \overline{11} = \overline{4},\\
\overline{3}^2 + \overline{3}\cdot\overline{3} + \overline{1} &= \overline{19} = \overline{5},\\
\overline{4}^2 + \overline{3}\cdot\overline{4} + \overline{1} &= \overline{29} = \overline{1},\\
\overline{5}^2 + \overline{3}\cdot\overline{5} + \overline{1} &= \overline{41} = \overline{6},\\
\overline{6}^2 + \overline{3}\cdot\overline{6} + \overline{1} &= \overline{55} = \overline{6}.
\end{aligned}$$

Aucune de ces valeurs n'étant nulle, nous concluons que $x^2 + \overline{3}\,x + \overline{1}$ est bien irréductible.

(d) On trouve :

$$x^3 + \overline{2}\,x^2 + \overline{3}\,x + \overline{4} = \big(x^3 + x^2 + \overline{2}\,x + \overline{5}\big)\cdot\overline{1} + x^2 + x + \overline{6}.$$

(e) Tout d'abord, grâce à la division euclidienne :

$$\frac{x^3 + \overline{2}\,x^2 + \overline{3}\,x + \overline{4}}{x^3 + x^2 + \overline{2}\,x + \overline{5}} = \overline{1} + \frac{x^2 + x + \overline{6}}{x^3 + x^2 + \overline{2}\,x + \overline{5}}.$$

Nous sommes alors dans la situation où le degré du numérateur est strictement inférieur à celui du dénominateur, situation où nous pouvons rechercher une décomposition en éléments simples.

Pour commencer, il faut décomposer en facteurs irréductibles le dénominateur. Mais ce travail a déjà été préparé par les questions qui précèdent :

$$\text{Dénominateur} \;=\; \big(x+\overline{5}\big)\,\big(x^2+\overline{3}\,x+\overline{1}\big).$$

D'après un théorème du cours, il s'agit maintenant de déterminer trois constantes inconnues $\overline{a}$, $\overline{b}$, $\overline{c}$ telles que :

$$\frac{x^2+x+\overline{6}}{(x+\overline{5})\,(x^2+\overline{3}\,x+\overline{1})} \;=\; \frac{\overline{a}}{x+\overline{5}} + \frac{\overline{b}\,x+\overline{c}}{x^2+\overline{3}\,x+\overline{1}}.$$

Après élimination du dénominateur, nous avons :

$$x^2+x+\overline{6} \;=\; \overline{a}\,\big(x^2+\overline{3}\,x+\overline{1}\big) + \big(\overline{b}\,x+\overline{c}\big)\,\big(x+\overline{5}\big).$$

En posant $x := -\,\overline{5} = \overline{2}$, il vient :

$$\begin{aligned} & \overline{2}^2+\overline{2}+\overline{6} \;=\; \overline{a}\,\big(\overline{2}^2+\overline{3}\cdot\overline{2}+\overline{1}\big)+\overline{0} \\ \longleftrightarrow \qquad & \overline{5} \;=\; \overline{a}\cdot\overline{4} \end{aligned}$$

d'où puisque dans le corps $\mathbb{Z}/7\mathbb{Z}$ on a $\overline{4}\cdot\overline{2}=\overline{1}$:

$$\overline{5}\cdot\overline{2} \;=\; \overline{3} \;=\; \overline{a}.$$

Ensuite, après soustraction :

$$\begin{aligned} x^2+x+\overline{6}-\overline{3}\,x^2-\overline{9}\,x-\overline{3} \;&=\; \overline{5}\,x^2+\overline{6}\,x+\overline{3} \\ &=\; \overline{b}\,x^2+\big(\overline{b}\cdot\overline{5}+\overline{c}\big)+\overline{c}\cdot\overline{5}. \end{aligned}$$

Par identification, le système linéaire de trois équations à deux inconnues :

$$\begin{aligned} \overline{5} \;&=\; \overline{b}, \\ \overline{6} \;&=\; \overline{5}\,\overline{b}+\overline{c}, \\ \overline{3} \;&=\; \overline{5}\,\overline{c}, \end{aligned}$$

admet pour solution unique :

$$\overline{b} \;:=\; \overline{5}, \qquad\qquad \overline{c} \;:=\; \overline{2}.$$

En conclusion :

$$\frac{x^3+\overline{2}\,x^2+\overline{3}\,x+\overline{4}}{x^3+x^2+\overline{2}\,x+\overline{5}} \;=\; \overline{1}+\frac{\overline{3}}{x+\overline{5}}+\frac{\overline{5}\,x+\overline{2}}{x^2+\overline{3}\,x+\overline{1}}. \qquad \square$$

Exercice 5. **(a)** On trouve, sans reste :

$$x^5+x^4+4\,x^3-4\,x^2+3\,x-5 \;=\; \big(x^2+2\,x+5\big)\,\big(x^3-x^2+x-1\big).$$

En développant le produit à droite, on retrouve bien le polynôme à gauche.

(b) On trouve, à nouveau sans reste :

$$x^6+4\,x^5+12\,x^4+15\,x^3+17\,x^2+3\,x+20 \;=\; \big(x^2+2\,x+5\big)\,\big(x^4+2\,x^3+3\,x^2-x+4\big).$$

En développant le produit à droite, on retrouve bien le polynôme à gauche.

(c) Divisons avec reste A par B :

$$x^4+2\,x^3+3\,x^2-x+4 \;=\; \big(x^3-x^2+x-1\big)\,(x+3)+5\,x^2-3\,x+7.$$

Ensuite, divisons B par le reste obtenu, ce qui crée des nombres rationnels :

$$x^3 - x^2 + x - 1 \;=\; \big(5\,x^2 - 3\,x + 7\big)\,\big(\tfrac{1}{5}\,x - \tfrac{2}{25}\big) - \tfrac{16}{25}\,x - \tfrac{11}{25}.$$

Enfin, divisons l'avant-dernier reste par le dernier :

$$5\,x^2 - 3\,x + 7 \;=\; \big(-\,\tfrac{16}{25} - \tfrac{11}{25}\big)\,\big(-\,\tfrac{125}{16}\,x + \tfrac{2575}{256}\big) + \tfrac{2925}{256}.$$

Le dernier reste non nul est bien égal à la constante non nulle :

$$\frac{2925}{256} \;=\; \mathsf{pgcd}\,\big(A, B\big),$$

ce qui montre que les deux polynômes A et B sont premiers entre eux.

(d) Après multiplication par une constante, on a :

$$1 \;=\; \mathsf{pgcd}\,\big(A,\,B\big),$$

d'où en conclusion :

$$\begin{aligned}\mathsf{pgcd}\,\big(P,\,Q\big) \;&=\; \mathsf{pgcd}\,\big(D\,A,\;D\,B\big)\\ &=\; D\,\mathsf{pgcd}\,\big(A,\,B\big)\\ &=\; D.\end{aligned}$$

Exercice 6. (a) Lorsque $-\infty \longleftarrow x$, et lorsque $x \longrightarrow \infty$, on sait que le monôme $a_n\,x^n$ domine tous les autres, d'où :

$$\lim_{-\infty\leftarrow x} a_n\,x^n \;=\; \lim_{-\infty\leftarrow x} P(x) \qquad\qquad \text{et} \qquad\qquad \lim_{x\to\infty} P(x) \;=\; \lim_{x\to\infty} a_n\,x^n.$$

Si $a_n < 0$ était (strictement) négatif, cette dernière limite vaudrait $-\infty$, ce qui contredirait l'hypothèse de positivité $P \geqslant 0$ sur $\mathbb{R}$.

(b) Sinon, si $n = 2\,n' + 1$ était *impair*, avec $a_n > 0$ grâce à la Question **(a)**, la limite :

$$-\infty \;=\; \lim_{-\infty\leftarrow x} a_n\,x^{2n'+1} \;=\; \lim_{-\infty\leftarrow x} P(x),$$

contredirait l'hypothèse de positivité $P \geqslant 0$ sur $\mathbb{R}$.

(c) Soit donc $\alpha \in \mathbb{R}$ une racine de $P(X)$, et soit $m \geqslant 1$ sa multiplicité :

$$P(X) \;=\; (X - \alpha)^m\,Q(X),$$

avec $Q(X)$ un polynôme de degré $n - m$ satisfaisant $0 \neq Q(\alpha)$.

Si $m = 2\,m' + 1$ était impair, comme au voisinage de $X = \alpha$ on a l'équivalent :

$$P(X) \;\sim\; \big(X - \alpha\big)^{2m'+1}\,Q(\alpha),$$

et comme la fonction réelle $x \longmapsto (x-\alpha)^{2m'+1}$ change de signe pour $x < \alpha$ et pour $x > \alpha$, ceci contredirait l'hypothèse de positivité $P \geqslant 0$ sur $\mathbb{R}$.

(d) Il s'agit de la décomposition de $P(X)$ en facteurs irréductibles, avec chaque racine réelle α_i de multiplicité *paire* $2\,m_i$, grâce à la Question **(c)**, et avec chaque trinôme du second degré, pour $1 \leqslant j \leqslant t$, n'ayant pas de racine réelle :

$$c_j^2 - 4\,d_j \;<\; 0 \qquad\qquad (1 \leqslant j \leqslant t).$$

Le degré total de $P(X)$ est visiblement *pair :*

$$n \;=\; 2\,m_1 + \cdots + 2\,m_s + 2\,q_1 + \cdots + 2\,q_t.$$

(e) Grâce à cette représentation de $P(X)$, et grâce à la connaissance des racines *complexes :*

$$\begin{aligned}\mu_j^+ &:= \frac{-c_j+\sqrt{-1}\,\sqrt{-c_j^2+4\,d_j}}{2},\\ \mu_j^- &:= \frac{-c_j-\sqrt{-1}\,\sqrt{-c_j^2+4\,d_j}}{2},\end{aligned}$$

qui sont, comme on le sait, manifestement conjuguées par paires :

$$\mu_j := \mu_j^+ = \overline{\mu_j^-} =: \overline{\mu_j} \qquad (1\leqslant j\leqslant t),$$

il vient, sachant que les racines $\overline{\alpha_i}=\alpha_i$ sont réelles :

$$\begin{aligned}P(X) \;=\; & \sqrt{a_n}\prod_{i=1}^{s}\big(X-\alpha_i\big)^{m_i}\;\prod_{j=1}^{t}\big(X-\mu_j\big)^{q_j}\\ & \cdot\;\sqrt{a_n}\prod_{i=1}^{s}\big(X-\alpha_i\big)^{m_i}\;\prod_{j=1}^{t}\big(X-\overline{\mu_j}\big)^{q_j}\\ =:\;& C(X)\\ & \cdot\;\overline{C(X)}.\end{aligned}$$

(f) Il suffit de décomposer $C(X)$ en parties réelle et imaginaire :

$$C(X) \;=\; A(X)+\sqrt{-1}\,B(X) \qquad \text{où} \qquad \begin{aligned}A(X) &:= \frac{C(X)+\overline{C(X)}}{2},\\ B(X) &:= \frac{C(X)-\overline{C(X)}}{2\,\sqrt{-1}},\end{aligned}$$

pour obtenir en conclusion :

$$\begin{aligned}P \;&=\; C\,\overline{C}\\ &=\; \big(A+\sqrt{-1}\,B\big)\,\big(A-\sqrt{-1}\,B\big)\\ &=\; A^2+B^2.\end{aligned}$$

Exercice 7. (a) En posant $Y:=X^\ell$ dans la factorisation connue :

$$Y^q-1 \;=\; (Y-1)\,\big(Y^{q-1}+Y^{q-2}+\cdots+Y+1\big),$$

on trouve :

$$X^{q\,\ell}-1 \;=\; (X^\ell-1)\,\big(X^{(q-1)\,\ell}+X^{(q-2)\,\ell}+\cdots+X^\ell+1\big).$$

(b) Montrons que $X^\ell-1$ divise $P(X)-R(X)$, ce qui conclura, car comme dans chaque division euclidienne sur $\mathbb{Z}$ on a :

$$0 \;\leqslant\; r_k \;\leqslant\; \ell-1 \qquad (0\leqslant k\leqslant n),$$

le degré de $R(X)$ est strictemnt inférieur à ℓ, et donc $R(X)$ sera bien le reste dans la division euclidienne de $P(X)$ par $X^\ell-1$.

Écrivons alors la différence :

$$P(X) - R(X) \;=\; \sum_{k=0}^{n} a_k \left(X^k - X^{r_k}\right).$$

Par linéarité, il suffit de faire voir que $X^\ell - 1$ divise chaque $X^k - X^{r_k}$. À cet effet, écrivons les divisions euclidiennes en question :

$$k \;=\; q_k\,\ell + r_k \qquad (q_k \in \mathbb{N},\, 0 \leqslant r_k \leqslant \ell - 1,\, k=0,1,\ldots,n),$$

et calculons/factorisons :

$$\begin{aligned} X^k - X^{r_k} \;&=\; X^{q_k \ell + r_k} - X^{r_k} \\ &=\; X^{r_k}\left(X^{q_k \ell} - 1\right) \\ &=\; X^{r_k}\left(X^\ell - 1\right)\Big(X^{(q_k-1)\,\ell} + X^{(q_k-2)\,\ell} + \cdots + X^\ell + 1\Big), \end{aligned}$$

ce qui montre bien que $X^\ell - 1$ divise $P(X) - R(X)$.

Exercice 8. (a) Le support $\mathsf{Supp}\,\sigma \;=\; \{a_1, a_2, \ldots, a_n\}$ de σ est constitué de n éléments distincts, qui sont envoyés par σ sur leur voisin situé juste à droite, avec à la fin $\sigma(a_n) := a_1$.

Il est alors clair — ce qui a d'ailleurs été vu en cours — que les autres éléments du complémentaire :

$$\{1, 2, 3, \ldots, \mathrm{N}-1, \mathrm{N}\} \Big\backslash \{a_1, a_2, \ldots, a_n\},$$

restent fixés un à un par σ et par chaque puissance σ^m avec $m \in \mathbb{Z}$. Par conséquent :

$$\mathsf{Supp}\,\sigma^m \;\subset\; \{a_1,\, a_2,\, \ldots,\, a_n\} \qquad (\forall\, m \in \mathbb{Z}),$$

et donc, nous pouvons considérer que σ ainsi que ses puissances σ^m n'agissent que sur ces n éléments $a_1, a_2, \ldots, a_n$.

Autrement dit, c'est seulement la restriction de σ à $\{a_1, a_2, \ldots, a_n\}$ qui nous intéresse, et après une renumérotation éventuelle, nous pouvons supposer que $\{a_1, a_2, \ldots, a_n\} = \{1, 2, \ldots, n\}$.

(b) D'après un résultat du cours, on sait que l'on a en fait :

$$\mathsf{Orb}_\tau(i) \;=\; \{i,\; \tau(i),\; \tau^2(i),\; \ldots,\; \tau^{v-1}(i)\}.$$

Il s'agit donc de déterminer l'entier minimal v tel que $\tau^v(i) = i$, et de démontrer qu'il vaut $v = n'$.

En partant de :

$$\begin{aligned} \tau(i) \;&=\; \underbrace{\sigma \circ \cdots \circ \sigma \circ \sigma}_{m \text{ fois}}(i) \\ &=\; \underbrace{\sigma \circ \cdots \circ \sigma}_{m-1 \text{ fois}}\big(i + 1 \mod n\big) \\ &=\; \cdots\cdots\cdots\cdots\cdots \\ &=\; i + m \mod n, \end{aligned}$$

nous avons :

$$\tau^\ell(i) \;=\; i + \ell\, m \mod n,$$

Ainsi $\tau^\ell(i) = i$ s'exprime par :

$$\begin{aligned}
& i + \ell\, m \;\equiv\; i \mod n \\
\iff \quad & \ell\, m \;\equiv\; 0 \mod n \\
\iff \quad & \ell\, d\, m' \;\equiv\; 0 \mod d\, n' \\
\iff \quad & \exists\, \mathrm{K} \in \mathbb{N}^* \quad \ell\, d\, m' \;=\; d\, n'\, \mathrm{K} \\
\iff \quad & \exists\, \mathrm{K} \in \mathbb{N}^* \quad \ell\, m' \;=\; n'\, \mathrm{K},
\end{aligned}$$

et enfin, le théorème de Gauss avec la primalité relative $1 = n' \wedge m'$ montrent que cela est satisfait si et seulement si ℓ est divisible par n' :

$$\ell \;=\; n' \cdot \ell' \qquad \text{avec } \ell' \geqslant 1 \text{ arbitraire.}$$

En conclusion, la valeur minimale v de tels ℓ est atteinte pour $\ell' := 1$, et elle vaut bien $v = n' \cdot 1 = n'$.

(c) Supposons donc que deux éléments de chacune de ces deux orbites coïncident, et déduisons la conséquence voulue :

$$\begin{aligned}
& i + \ell\, m \;\equiv\; j + h\, m \mod n \\
\iff \quad & i + \ell\, d\, m' \;\equiv\; j + h\, d\, m' \mod d\, n' \\
\iff \quad & i - j \;\equiv\; (-\ell + h)\, d\, m' \mod d\, n' \\
\implies \quad & i - j \;\equiv\; 0 \mod d
\end{aligned}$$

(d) Les entiers $\{1, 2, \ldots, d\}$ sont deux à deux distincts modulo d, et donc, la Question **(c)** qui précède garantit, par contraposition, que ces d orbites sont mutuellement disjointes.

Comme elles sont toutes de même cardinal n', d'après la Question **(b)**, et comme $d\, n' = n$, leur réunion partitionne bien $\{1, 2, \ldots, n\}$.

(e) Ce sont vraiment des corollaires directs et immédiats.

(f) *Oh Yes Elizabeth*, car d'après le cours, toute numérotation des N éléments de E ramène (par isomorphisme) $\mathfrak{S}(E)$ à $\mathfrak{S}_\mathrm{N}$. Encore un demi-point sur 20 qui était « donné » !

(g) Par application du résultat qui vient d'être démontré :

n	12	8	6	1	
$\mathsf{pgcd}(4, n)$	4	4	2	1	nombre de cycles
$\frac{n}{\mathsf{pgcd}(4,n)}$	3	2	3	1	longueurs des cycles

et donc le type de σ^4 est :

$$\Big(3,\, 3,\, 3,\, 3,\quad 2,\, 2,\, 2,\, 2,\quad 3,\, 3,\quad 1\Big) \;=\; \big(3,\, 3,\, 3,\, 3,\, 3,\, 3,\quad 2,\, 2,\, 2,\, 2,\quad 1\big).$$

11. Examen 6

Exercice 1. Dire si les assertions suivantes sont vraies ou fausses. Démontrer celles qui sont vraies et donner un contre-exemple pour celles qui sont fausses.

(a) Soient a et b deux éléments de $\mathbb{Z}$. Si a est divisible par b, alors a^2 est divisible par b^2.

(b) Soient p un nombre premier et a un entier naturel non nul. Si x et y sont deux entiers vérifiant $a\,x \equiv a\,y \bmod p$, alors on a $x \equiv y \bmod p$.

(c) Soit $n \in \mathbb{N}$ un entier naturel au moins égal à 4. Si n n'est pas premier, alors il existe des entiers a, b avec $a \geqslant 2$ et $b \geqslant 2$ tels que $n = a\,b$.

(d) Soit $n \in \mathbb{N}$ un entier naturel au moins égal à 4. Si n n'est pas premier, alors il existe des entiers a, b premiers entre eux avec $a \geqslant 2$ et $b \geqslant 2$ tels que $n = ab$.

Exercice 2. Le but de cet exercice est de trouver l'ensemble des solutions entières n de l'équation

$$\mathsf{pgcd}\big(2n+8,\, 3n+15\big) \;=\; 6.$$

(a) Montrer que si n est une solution, alors $n \equiv 2 \bmod 3$ et $n \equiv 1 \bmod 2$.

(b) Déduire de la question précédente un entier k tel que si n est une solution alors $n \equiv k \bmod 6$.

(c) Montrer que pour tout entier a les nombres $2a+3$ et $3a+5$ sont premiers entre eux (On pourra par exemple trouver une relation de Bézout).

(d) Vérifier que si $n \equiv k \bmod 6$ alors n est une solution.

Exercice 3. Soit G un ensemble muni d'une loi associative notée $*$. On suppose de plus que $(G, *)$ satisfait les deux propriétés suivantes :

(N) $\exists\, e \in G, \forall\, x \in G,\, e * x = x$: Existence d'un « élément neutre à gauche ».

(I) $\forall x \in G, \exists\, y \in G,\, y * x = e$: Tout élément a un « inverse à gauche ».

(a) Montrer qu'un inverse à gauche est aussi un inverse à droite, *i.e.* :

$$\forall\, x, y \in G \qquad y * x \;=\; e \;\Longrightarrow\; x * y \;=\; e.$$

Indication: On pourra considérer un inverse à gauche z de y et calculer $e * (x * y) \;=\; (z * y) * (x * y)$.

(b) Montrer que e est aussi un élément neutre à droite, *i.e.* :

$$\forall\, x \in G \qquad x * e \;=\; x.$$

Indication: On pourra calculer de deux manières $x * (y * x)$, où y est un inverse à gauche de x.

(c) Montrer que $(G, *)$ est un groupe.

Exercice 4. Soit la permutation suivante d'un ensemble à 12 éléments :

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 1 & 5 & 12 & 6 & 3 & 9 & 4 & 2 & 11 & 8 & 10 \end{pmatrix}.$$

(a) Décomposer σ en produit de cycles à supports deux à deux disjoints.

(b) Déterminer l'ordre $o(\sigma)$ de σ.

(c) Décomposer σ^{6666} en produit explicite de cycles à supports disjoints.

(d) Rappeler comment on décompose, dans le groupe $\mathfrak{S}_n$ des permutations de $\{1, 2, 3, \ldots, n\}$, un p-cycle $(a_1\ a_2\ \cdots\ a_p)$ quelconque en un produit de transpositions (*i.e.* de 2-cycles).

(e) Décomposer σ en produit de transpositions.

(f) Déterminer la signature de σ.

(g) Déterminer la signature de σ^{6666}.

Exercice 5. (a) Décomposer en éléments simples dans $F_{\mathbb{R}}[x]$ la fraction réelle :

$$\frac{x^2 + x + 1}{(x^2 - 1)(x^2 + 1)}.$$

(b) Sur $\mathbb{K} := \mathbb{Z}/5\mathbb{Z}$, décomposer en éléments simples dans $F_{\mathbb{K}}[x]$ la fraction :

$$\frac{x - \overline{1}}{(x + \overline{1})^2 (x + \overline{2})}.$$

Exercice 6. (a) Dans $(\mathbb{Z}/9\mathbb{Z}, +)$, déterminer les ordres des éléments suivants, et dire lesquels sont des générateurs : $\overline{5}$, $\overline{6}$, $\overline{7}$.

Exercice 7. En justifiant votre réponse, donner la liste des sous-groupes de G dans chacun des trois cas suivants :

(a) $G = \mathbb{Z}/4\mathbb{Z}$.

(b) $G = \mathbb{Z}/6\mathbb{Z}$.

(c) (Question subsidiaire, à aborder seulement si vous pensez avoir correctement traité tout le reste du sujet.) $G = \mathbb{Z}/n\mathbb{Z}$ avec $n \geqslant 2$.

12. Corrigé de l'examen 6

Exercice 1. **(a)** Vrai ! En effet, a divisible pas b signifie qu'il existe $c \in \mathbb{Z}$ tel que $a = b\,c$, ce qui entraîne que $a^2 = b^2\,c^2$, et donc que b^2 divise a^2.

(b) Faux ! Il ne faut pas se laisser prendre par $a \neq 0$ qui n'est pas suffisant. La bonne hypothèse pour rendre vraie cette affirmation serait a premier à p.

En effet, pour tout $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ et tout $k \in \mathbb{Z}$, on a :

$$k\,p\,x \;\equiv\; k\,p\,y \mod p.$$

Plus concrètement encore, 1 et 2 ne sont par congrus modulo 2, tandis que $2 \cdot 1$ et $2 \cdot 3$ le sont.

(c) Vrai ! Et c'est quasiment la définition !

(d) Faux, Toto ! Un contre-exemple hyper-simple est $n = 4 = 2 \cdot 2$, avec $2 = a = b$.

Exercice 2. Le but de cet exercice est de trouver l'ensemble des solutions entières n de l'équation

$$\mathsf{pgcd}\big(2n + 8,\, 3n + 15\big) \;=\; 6.$$

(a) Si $n \in \mathbb{N}$ est solution de l'équation ci-dessus, on a la suite d'implications :

$$\begin{cases} 6 \,\big|\, 2n + 8 \\ 6 \,\big|\, 3n + 15 \end{cases} \implies \begin{cases} 3 \,\big|\, n + 4 \\ 2 \,\big|\, n + 5 \end{cases} \implies \begin{cases} n + 4 \;\equiv\; 0 \mod 3 \\ n + 5 \;\equiv\; 0 \mod 2 \end{cases} \implies \begin{cases} n \;\equiv\; 2 \mod 3 \\ n \;\equiv\; 1 \mod 2. \end{cases}$$

(b) On sait, d'après le théorème chinois des restes, que l'ensemble des solutions du système de congruences :

$$\begin{aligned} n \;&\equiv\; 2 \mod 3, \\ n \;&\equiv\; 1 \mod 2, \end{aligned}$$

est une classe d'entiers modulo $2 \cdot 3 = 6$, puisque 2 et 3 sont premiers entre eux. On constate alors que $k = 5$ convient.

(c) On constate immédiatement que

$$2 \cdot (3a + 5) - 3 \cdot (2a + 3) \;=\; 6a + 10 - 6a - 9 \;=\; 1\,;$$

si bien que, d'après le théorème de Bézout, $2a + 3$ et $3a + 5$ sont premiers entre eux.

(d) Pour $n \in \mathbb{N}$ supposons que $n \equiv k \mod 6$, il existe $a \in \mathbb{N}$ tel que $n = 6a + k$.

Cherchons alors à déterminer le pgcd de $2n + 8$ et $3n + 15$, *i.e.* le pgcd de :

$$2(6a + k) + 8 \quad \text{et} \quad 3(6a + k) + 15,$$

i.e. puisqu'on peut prendre $k = 5$, le pgcd de :

$$12a + 18 \quad \text{et} \quad 18a + 30.$$

Ce dernier est 6 fois le pgcd de $2a + 3$ et $3a + 5$ dont on a montré dans la Question **(c)** qu'il vaut 1, ce qui répond à la question.

Exercice 3. (a) Pour tout $x \in G$ il existe $y \in G$ tel que $y * x = e$ et $z \in G$ tel que $z * y = e$. Alors :

$$\begin{aligned} x * y &= e * (x * y) \\ &= (z * y) * (x * y) \\ &= ((z * y) * x) * y \\ &= (z * (y * x)) * y \\ &= (z * e) * y \\ &= z * (e * y) \\ &= z * y \\ &= e. \end{aligned}$$

(b) Pour tout $x \in G$, il existe $y \in G$ tel que $y * x = e$. Mais, d'après la Question **(a)**, on a aussi $x * y = e$. Alors :

$$\begin{aligned} x * e &= x * (y * x) \\ &= (x * y) * x \\ &= e * x \\ &= x. \end{aligned}$$

(c) Grâce aux Questions **(a)** et **(b)**, les axiomes de la définition de groupe sont satisfaits.

Exercice 4. (a) On trouve :

$$\sigma = (3\,5\,6)\,(1\,7\,9\,2)\,(4\,12\,10\,11\,8).$$

(b) Lorsque σ est décomposé en produit de cycles à supports deux à deux disjoints comme ci-dessus, l'ordre de σ est le ppcm des ordres de ces cycles. L'ordre d'un cycle est aussi la longueur du cycle. Ainsi :

$$o(\sigma) = 3 \cdot 4 \cdot 5 = 60.$$

(c) Écrivons $6666 = 60 * 111 + 6$, c'est-à-dire faisons la division euclidienne de 6666 par 60. Il vient alors :

$$\sigma^{6666} = \sigma^{60 \cdot 111 + 6} = (\sigma^{60})^{111}\sigma^6 = \mathsf{Id}^{111}\sigma^6 = \sigma^6,$$

puisque l'on vient de voir que $\sigma^{60} = \mathsf{Id}$.

Notons :

$$\gamma_3 := (3\,5\,6), \qquad \gamma_4 := (1\,7\,9\,2), \qquad \gamma_5 := (4\,12\,10\,11\,8),$$

les cycles qui décomposent σ et sont d'ordres respectifs 3, 4, 5. Par ailleurs, comme ces cycles sont à supports deux à deux disjoints, ils commutent :

$$\forall\, i, j \in \{3, 4, 5\}, \qquad \gamma_i\gamma_j = \gamma_j\gamma_i.$$

Il en résulte que :

$$\begin{aligned} \sigma^{6666} &= \sigma^6 \\ &= \gamma_3^6\gamma_4^6\gamma_5^6 \\ &= \gamma_4^2\gamma_5 \\ &= (1\,9)(7\,2)(4\,12\,10\,11\,8). \end{aligned}$$

(d) On a :

$$\big(a_1 \;\; a_2 \;\; \cdots \;\; a_p\big) \;=\; (a_1\, a_2)\,(a_2\, a_3)\cdots(a_{p-1}\, a_p),$$

ce qui correspond à un produit de $p-1$ transpositions.

(e) D'après les Questions **(a)** et **(d)**, on a :

$$\begin{aligned}\sigma &= (3\,5\,6)\,(1\,7\,9\,2)\,(4\,12\,10\,11\,8)\\ &= (3\,5)(5\,6)(1\,7)(7\,9)(9\,2)(4\,12)(12\,10)(10\,11)(11\,8).\end{aligned}$$

Noter que, contrairement à la décomposition en cycles donnée à la Question **(a)**, cette décomposition en produit de transpositions n'est pas unique.

(f) La signature d'une transposition vaut -1. De plus, la signature est multiplicative (autrement dit c'est un morphisme de groupes). Ainsi si σ est un produit de r transpositions, la signature de σ est $(-1)^r$. À la Question **(e)**, on a trouvé $r = 9$; si bien que la signature de σ vaut $(-1)^9 = -1$.

(g) La propriété de multiplicativité de la signature permet de déterminer

$$\varepsilon(\sigma^{6666}) \;=\; \varepsilon(\sigma)^{6666} \;=\; (-1)^{6666} \;=\; 1.$$

On pourrait aussi appliquer les arguments des Questions **(d)** et **(e)** à la décomposition de σ^{6666} trouvée en **(c)**.

Exercice 5. (a) Cherchons $a, b, c, d \in \mathbb{R}$ tels que :

$$\frac{x^2+x+1}{(x^2-1)\,(x^2+1)} \;=\; \frac{a}{x-1} + \frac{b}{x+1} + \frac{cx+d}{x^2+1}.$$

Cette équation donne lieu à la suite d'équivalences :

$$\begin{aligned}&\frac{x^2+x+1}{(x^2-1)\,(x^2+1)} = \frac{a}{x-1} + \frac{b}{x+1} + \frac{cx+d}{x^2+1}\\ \iff\quad & x^2+x+1 = a(x+1)(x^2+1) + b(x-1)(x^2+1) + (cx+d)(x^2-1)\\ \iff\quad & x^2+x+1 = (a+b+c)x^3 + (a-b+d)x^2 + (a+b-c)x + (a-b-d).\end{aligned}$$

Cette dernière égalité équivaut aux systèmes linéaires équivalents suivants :

$$\left\{\begin{array}{rcl} a+b+c &=& 0\\ a-b+d &=& 1\\ a+b-c &=& 1\\ a-b-d &=& 1 \end{array}\right\}$$
$$\Leftrightarrow \quad \left\{\begin{array}{rcl} a+b+c &=& 0\\ a-b+d &=& 1\\ 2a+2b &=& 1\\ 2a-2b &=& 2 \end{array}\right\}$$
$$\Leftrightarrow \quad \left\{\begin{array}{rcl} a+b+c &=& 0\\ a-b+d &=& 1\\ 2a+2b &=& 1\\ 4a &=& 3 \end{array}\right\}$$
$$\Leftrightarrow \quad \left\{\begin{array}{rcl} a &=& \frac{3}{4}\\ b &=& -\frac{1}{4}\\ c &=& -\frac{1}{2}\\ d &=& 0 \end{array}\right\},$$

si bien que :

$$\frac{x^2+x+1}{(x^2-1)\,(x^2+1)} \;=\; \frac{3}{4(x-1)} \;-\; \frac{1}{4(x+1)} \;-\; \frac{x}{2(x^2+1)}.$$

(b) Pour $a, b, c \in \mathbb{K}$ on a (en omettant les barres pour alléger les notations) :

$$\begin{array}{rcl} \dfrac{x-1}{(x+1)^2(x+2)} &=& \dfrac{ax+b}{(x+1)^2}+\dfrac{c}{x+2}\\ \Longleftrightarrow \qquad x-1 &=& (ax+b)(x+2)+c(x+1)^2\\ \Longleftrightarrow \qquad x-1 &=& (a+c)x^2+(2a+b+2c)x+2b+c. \end{array}$$

D'où le système linéaire :

$$\Longleftrightarrow \quad \left\{\begin{array}{rcl} a+c &=& 0\\ 2a+b+2c &=& 1\\ 2b+c &=& -1 \end{array}\right\}$$
$$\Longleftrightarrow \quad \left\{\begin{array}{rcl} a+c &=& 0\\ b &=& 1\\ 2b+c &=& -1 \end{array}\right\}$$
$$\Longleftrightarrow \quad \left\{\begin{array}{rcl} a &=& 3\\ b &=& 1\\ c &=& -3 \end{array}\right\}$$

On a donc dans $\mathbb{Z}/5\mathbb{Z}$ la décomposition :

$$\frac{x-1}{(x+1)^2(x+2)} \;=\; \frac{3x+1}{(x+1)^2}+\frac{-3}{x+2}.$$

Exercice 6. (a) Pour tout $a \in \mathbb{Z}$, l'ordre de $\overline{a}$ dans $\mathbb{Z}/9\mathbb{Z}$ est $\frac{9}{\mathsf{pgcd}\,(9,a)}$. Cela montre que $\overline{5}$ et $\overline{7}$ sont d'ordre 9, c'est-à-dire sont des générateurs de $\mathbb{Z}/9\mathbb{Z}$, et que $\overline{6}$ est d'ordre 3.

Plutôt que d'utiliser que l'ordre vaut $\frac{9}{\mathsf{pgcd}\,(9,a)}$, on pouvait aussi faire la liste des restes dans la division euclidienne par 9 des multiples de a, jusqu'à tomber sur 0. L'ordre de $\overline{a}$ est alors le nombre d'éléments de cette liste. Par exemple pour $a = 6$ on obtient $\overline{a} = \overline{6}$, $2\overline{a} = \overline{12} = \overline{3}$ et $3\overline{a} = \overline{18} = \overline{0}$, donc l'ordre de $\overline{a}$ est 3.

Exercice 7. (a) Il est clair que $\{\overline{0}\}$, $\{\overline{0}, \overline{2}\}$ et $\mathbb{Z}/4\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}/4\mathbb{Z}$: montrons que ce sont les seuls. Soit H un sous-groupe de $\mathbb{Z}/4\mathbb{Z}$. Alors son cardinal divise 4 donc c'est 1, 2 ou 4. Si c'est 1 ou 4 alors H est égal à $\{\overline{0}\}$ ou à $\mathbb{Z}/4\mathbb{Z}$. Supposons désormais que H est de cardinal 2, c'est-à-dire de la forme $\{\overline{0}, \overline{a}\}$ avec $\overline{a} \neq \overline{0}$. Si $\overline{a}$ est égal à $\overline{1}$ ou à $\overline{3}$ alors $2\overline{a} = \overline{2} \in H$ ce qui est contradictoire. Donc $\overline{a} = \overline{2}$ et $H = \{\overline{0}, \overline{2}\}$.

(b) Clairement $\{\overline{0}\}$, $\{\overline{0}, \overline{3}\}$, $\{\overline{0}, \overline{2}, \overline{4}\}$ et $\mathbb{Z}/6\mathbb{Z}$ conviennent. Si H est un sous-groupe de $\mathbb{Z}/6\mathbb{Z}$, son cardinal est 2, 3, 6 ou 1. Les deux derniers cas se traitent comme en **(a)**. Si H est de cardinal 2 alors $H = \{\overline{0}, \overline{a}\}$ avec $\overline{a} \neq \overline{0}$ et $2\overline{a} \in H$. Comme $2\overline{a} = \overline{a}$ imposerait $\overline{a} = \overline{0}$, on a donc $2\overline{a} = \overline{0}$ d'où $\overline{a} = \overline{3}$. Reste à traiter le cas où H est de cardinal 3. Il existe alors $a \in \mathbb{Z}$ tel que $\overline{a} \neq \overline{0}$ et $\overline{a} \in H$. L'ordre de $\overline{a}$ divise 3 et n'est pas 1 donc c'est 3, et $H = \{\overline{0}, \overline{a}, 2\overline{a}\}$ avec $\overline{a} = \overline{2}$ ou $\overline{a} = \overline{4}$ (qui conduisent au même sous-groupe).

(c) Toute partie de la forme $\left\{\overline{d}, 2\overline{d}, \ldots, \frac{n}{d}\overline{d} = \overline{n} = \overline{0}\right\}$, où $d \geqslant 1$ divise n, est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ noté H_d (en effet c'est le sous-groupe engendré par $\overline{d}$). Soit H un sous-groupe quelconque de $\mathbb{Z}/n\mathbb{Z}$; notons δ son cardinal. Alors δ divise n ; posons $d = n/\delta$. Soit $a \in \mathbb{Z}$ tel que $\overline{a} \in H$. L'ordre de $\overline{a}$ divise celui de H donc $\delta\overline{a} = \overline{0}$, c'est-à-dire $n|\delta a$. Comme $n = \delta d$ cela donne $d|a$ d'où $\overline{a} \in H_d$. On a donc $H \subset H_d$; comme ces deux ensembles ont même cardinal, ils sont égaux.