

M1 2023-2024 : GROUPES

David Harari

Table des matières

1. Quelques rappels	1
1.1. Notations, premières propriétés	2
1.2. Générateurs d'un groupe	2
1.3. Sous-groupes distingués, groupes quotients.	3
1.4. Centre et sous-groupe dérivé	6
2. Groupes finis	7
2.1. Opérations de groupes, formule des classes	7
2.2. p -groupes ; théorèmes de Sylow	9
2.3. Compléments sur $\mathbf{Z}/n\mathbf{Z}$	13
3. Groupes simples, exemple du groupe alterné	16
4. Groupes résolubles et nilpotents	20

1. Quelques rappels

Il s'agit principalement ici de rappels de L3, on ira donc assez vite et sans détailler la plupart des démonstrations. On suppose déjà connues les notions suivantes : groupe, sous-groupe, morphisme (et isomorphisme) de groupes, noyau et image d'un morphisme de groupes, ordre d'un élément dans un groupe, théorème de Lagrange, sous-groupe distingué, groupe quotient. On utilisera fréquemment les exemples classiques : groupes cycliques (isomorphes à $\mathbf{Z}/n\mathbf{Z}$ pour un entier $n > 0$), groupe des permutations \mathcal{S}_n , groupe des matrices inversibles $GL_n(K)$ (où K est un corps ; par convention, tous les corps seront supposés commutatifs).

1.1. Notations, premières propriétés

Les lois de groupes seront en général notées multiplicativement. En particulier, l'élément neutre d'un groupe G sera le plus souvent noté 1 et le symétrique d'un élément x sera noté x^{-1} . Pour $n > 0$, on pose $x^n = x.x\dots x$ (n termes), avec les conventions $x^0 = 1$ et $x^{-n} = (x^n)^{-1}$. Si le groupe G est abélien (c'est-à-dire commutatif), on notera parfois $+$ la loi, 0 le neutre, et $-x$ le symétrique de x qu'on appelle alors l'*opposé* de x . On pourra aussi alors noter $x - y$ pour $x + (-y)$, et nx pour $x + x + \dots + x$ (n termes) quand n est un entier > 0 , avec les conventions $0.x = 0$ et $(-n)x = n(-x)$.

Remarque 1.1 On se gardera bien d'utiliser une notation du genre " x/y " si G n'est pas abélien car on ne saurait pas si cela signifie xy^{-1} ou $y^{-1}x$.

Définition 1.2 Un isomorphisme d'un groupe G sur lui-même s'appelle un *automorphisme* de G . On note $\text{Aut}(G)$ l'ensemble des automorphismes de G , c'est un sous-groupe pour la loi \circ du groupe $\mathcal{S}(G)$ des permutations de G . Noter que le groupe $\text{Aut}(G)$ peut être non commutatif même si G l'est (ex. $G = \mathbf{Z}/2 \times \mathbf{Z}/2$, le vérifier en observant que $\text{Aut } G$ est isomorphe à $GL_2(\mathbf{Z}/2)$, lui-même isomorphe à \mathcal{S}_3).

Exemple 1.3 Voici quelques exemples de sous-groupes et de morphismes de groupes :

a) L'application $z \mapsto \exp z$ est un morphisme, surjectif mais non injectif, de $(\mathbf{C}, +)$ dans (\mathbf{C}^*, \times) .

b) Si E est fini de cardinal n , on a $\mathcal{S}(E) \simeq \mathcal{S}_n$. Pour $n \geq 2$, il existe un unique morphisme non trivial ε de \mathcal{S}_n vers $\{\pm 1\}$, la *signature*. En particulier la signature de toute transposition est -1 . Le noyau de la signature est un sous-groupe de \mathcal{S}_n , le *groupe alterné* \mathcal{A}_n .

c) Soit K un corps. Le déterminant est un morphisme de $GL_n(K)$ dans K^* . Si E est un K -ev de dimension n , alors $GL_n(K)$ est isomorphe au groupe $(GL(E), \circ)$ des applications linéaires bijectives de E dans E . Le noyau du déterminant est un sous-groupe de $GL_n(K)$, appelé *groupe spécial linéaire*. On le note $SL_n(K)$.

d) Les sous-groupes de \mathbf{Z} sont les $n\mathbf{Z}$ avec $n \in \mathbf{N}$.

1.2. Générateurs d'un groupe

Proposition 1.4 Soient G un groupe et A une partie de G . Alors il existe un plus petit sous-groupe H de G contenant A . On l'appelle sous-groupe engendré par A et on le note $\langle A \rangle$.

Démonstration : Il suffit de prendre pour $\langle A \rangle$ l'intersection de tous les sous-groupes de G contenant A . On peut aussi décrire $\langle A \rangle$ comme l'ensemble des produits $x_1 \dots x_n$, où chaque x_i vérifie : $x_i \in A$ ou $x_i^{-1} \in A$ (si A est vide on prend $\langle A \rangle = \{1\}$).

□

Remarque 1.5 Si G est un groupe abélien (noté additivement), la description de $\langle A \rangle$ est plus simple : c'est l'ensemble des $\sum_{i=1}^m n_i a_i$ avec $n_i \in \mathbf{Z}$ et $a_i \in A$ (l'entier m pouvant être quelconque), autrement dit l'ensemble des $\sum_{a \in A} n_a a$, où $(n_a)_{a \in A}$ est une famille presque nulle d'entiers. Attention, ceci ne s'étend pas au cas où A n'est pas abélien (par exemple on ne peut pas simplifier une expression du genre xyx dans un groupe non abélien).

Rappelons qu'un groupe est *monogène* si on peut l'engendrer par un seul de ses éléments, *cyclique* s'il est de plus fini (auquel cas il est isomorphe à $\mathbf{Z}/n\mathbf{Z}$, tandis que les groupes monogènes infinis sont isomorphes à \mathbf{Z}). Si $d \in \mathbf{N}^*$ est un diviseur de n , alors le groupe $\mathbf{Z}/n\mathbf{Z}$ possède un et un seul sous-groupe d'ordre d , qui est lui-même cyclique (c'est le groupe $(n/d)\mathbf{Z}/n\mathbf{Z}$, qui est aussi le sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ constitué des x tels que $dx = 0$).

Exemple 1.6 a) Le groupe $(\mathbf{Z}^n, +)$ est engendré par la famille

$$(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, \dots, 0, 1).$$

b) Le groupe symétrique \mathcal{S}_n est engendré par les transpositions.

c) Le groupe $SL_n(K)$ est engendré par les transvections. Si $n \geq 2$, le groupe orthogonal $O_n(\mathbf{R})$ est engendré par les réflexions.

1.3. Sous-groupes distingués, groupes quotients.

Rappelons qu'un sous-groupe H d'un groupe G est *distingué* (et on note alors $H \triangleleft G$) si pour tout $g \in G$ et tout $x \in H$, on a $g x g^{-1} \in H$. On a alors dans ce cas plus précisément $g H g^{-1} = H$ (changer g en g^{-1} dans la définition). Voici quelques exemples :

Exemple 1.7 a) Si $f : G \rightarrow G'$ est un morphisme de groupes et si $H' \triangleleft G'$, alors $f^{-1}(H')$ est distingué dans G . En particulier $\ker f$ est distingué dans G . Si $H \triangleleft G$, alors $f(H)$ est distingué dans $f(G)$ (mais pas dans G' en général). L'intersection de deux sous-groupes distingués dans G est un sous-groupe distingué de G .

b) Soit $n \geq 2$. Alors \mathcal{A}_n est distingué dans \mathcal{S}_n en tant que noyau de la signature.

c) Si K est un corps commutatif, alors $SL_n(K)$ est distingué dans $GL_n(K)$ en tant que noyau du déterminant.

d) Soient $n \geq 3$ et H le sous-groupe de \mathcal{S}_n constitué de l'identité et d'une transposition $\tau = (a, b)$. Alors si $\sigma \in \mathcal{S}_n$, on a $\sigma\tau\sigma^{-1} = (\sigma(a), \sigma(b))$ donc H n'est pas distingué dans \mathcal{S}_n (choisir σ tel que $\sigma(a) = c$ avec c distinct de a et b).

Définition 1.8 Un sous-groupe H de G est dit *caractéristique* si pour tout $\varphi \in \text{Aut } G$, on a $\varphi(H) \subset H$ (dans ce cas on a en particulier $H \triangleleft G$).

Par exemple, le groupe \mathcal{A}_3 est caractéristique dans \mathcal{S}_3 car tout automorphisme de \mathcal{S}_3 doit envoyer un 3-cycle sur un élément d'ordre 3, donc sur un autre 3-cycle. On verra un peu plus loin deux exemples généraux de sous-groupes caractéristiques d'un groupe G , son centre et son sous-groupe dérivé.

Remarque 1.9 Si K est caractéristique dans H et H est caractéristique dans G , on vérifie facilement que K est caractéristique dans G . Par contre, la même propriété ne marche pas avec "distingué" (exercice...).

Voici une notion souvent utile en théorie des groupes, étroitement liée à celle de sous-groupe distingué.

Définition 1.10 Soit G un groupe. Soit H un sous-groupe de G . Le *normalisateur* de H dans G est le sous-groupe $N_G(H)$ de G constitué des $g \in G$ vérifiant $gHg^{-1} = H$.

Il est facile de vérifier que $N_G(H)$ est bien un sous-groupe de G et qu'il contient H . C'est le plus grand sous-groupe de G dans lequel H est distingué, et par définition on a $N_G(H) = G$ si et seulement si H est distingué dans G .

Rappelons que si H est un sous-groupe distingué d'un groupe G , on dispose d'un *groupe quotient* G/H tel que la surjection canonique $\pi : G \rightarrow G/H$ soit un morphisme de groupes. Cela ne marche pas si H n'est pas distingué (vu que le noyau de p doit être H), dans ce cas on doit faire la différence entre l'ensemble des classes à gauche G/H (quotient de G par la relation d'équivalence $x \sim y$ ssi $x^{-1}y \in H$; c'est aussi l'ensemble des aH avec $a \in G$) et celui des classes à droite $H \backslash G$ (quotient de G par la relation d'équivalence $x \sim y$ ssi $xy^{-1} \in H$, qui est aussi l'ensemble des Ha avec $a \in G$).

Remarque 1.11 En général, si H est un sous-groupe d'un groupe G , l'ensemble G/H est en bijection avec l'ensemble $H \backslash G$ via $aH \mapsto Ha^{-1}$. Quand leur cardinal est fini, on dit que H est un sous-groupe *d'indice fini* de G , et on note $[G : H]$ ce cardinal, qu'on appelle *l'indice* de H dans G ; c'est simplement $\#G/\#H$ si G est fini.

Rappelons l'important

Theorème 1.12 (Th. de factorisation) Soit $f : G \rightarrow G'$ un morphisme de groupes. Alors il existe un unique morphisme de groupes $\tilde{f} : G/\ker f \rightarrow G'$ tel que $f = \tilde{f} \circ \pi$. De plus \tilde{f} est injectif d'image $\text{Im } f$, i.e. $G/\ker f \simeq \text{Im } f$ ("premier théorème d'isomorphisme"). En particulier, quand G est fini, on a

$$\#G = \#\ker f \# \text{Im } f.$$

Remarque 1.13 Si N est un sous-groupe distingué de G inclus dans $\ker f$, alors f se factorise encore par un morphisme $\tilde{f} : G/N \rightarrow G'$ d'image $\text{Im } f$, mais on perd alors l'injectivité de \tilde{f} .

Theorème 1.14 ("Théorèmes d'isomorphisme, II et III")

Soit G un groupe. Soit H un sous-groupe distingué de G , on note $\pi : G \rightarrow G/H$ la surjection canonique. Alors :

a) Les sous-groupes de G/H sont exactement les N/H , où N est un sous-groupe de G contenant H . De plus $N/H \triangleleft G/H$ si et seulement si $N \triangleleft G$.

b) Soit K un sous-groupe de G . Posons $KH = \{kh, k \in K, h \in H\}$ (avec une notation similaire pour HK). Alors on a $KH = HK$, et cet ensemble est un sous-groupe de G qui contient H .

c) Pour tout sous-groupe K de G , le sous-groupe $\pi(K)$ de G/H est aussi le sous-groupe KH/H . Ce dernier est isomorphe à $K/K \cap H$ ("deuxième théorème d'isomorphisme").

d) Soit N un sous-groupe distingué de G contenant H . Alors le groupe $(G/H)/(N/H)$ est isomorphe au groupe quotient G/N ("troisième théorème d'isomorphisme").

Ainsi, dans G/H "on obtient un sous-groupe si on diminue G et un quotient si on augmente H ."

Démonstration : a) On vérifie immédiatement que si N est un sous-groupe de G contenant H , alors H (qui est distingué dans G) est a fortiori distingué dans N , et qu'alors N/H est un sous-groupe de G/H . Réciproquement si A est un sous-groupe de G/H , alors $N := \pi^{-1}(A)$ est un sous-groupe de G contenant H (car A contient le neutre de G/H), et on a bien $A = \pi(N) = N/H$ car π est surjective. Si $A \triangleleft G/H$, son image réciproque N est un sous-groupe distingué de G , et si $N \triangleleft G$, alors $A = \pi(N)$ est bien distingué dans $\pi(G) = G/H$.

b) L'égalité $KH = HK$ résulte des identités (valables pour $k \in K, h \in H$) : $kh = (khk^{-1})k$ et $hk = k(k^{-1}hk)$ avec $khk^{-1} \in H, k^{-1}hk \in H$ vu

que $H \triangleleft G$. On a alors $1 = 1.1 \in HK$; si $u_1, u_2 \in KH$, on peut écrire $u_1 = k_1 h_1$ et $u_2 = h_2 k_2$ avec $h_1, h_2 \in H$ et $k_1, k_2 \in K$. Alors $u_1 u_2 = k_1 h_3 k_2$ avec $h_3 = h_1 h_2 \in H$; comme $h_3 k_2 \in HK = KH$, on peut écrire $h_3 k_2 = k_3 h_4$ avec $k_3 \in K$ et $h_4 \in H$, ce qui donne que $u_1 u_2 = (k_1 k_3) h_4 \in KH$. Finalement si $u = kh \in KH$, alors $u^{-1} = h^{-1} k^{-1} \in HK = KH$. Ainsi KH est bien un sous-groupe de G .

c) Soit $u = kh \in KH$. Alors on a $\pi(u) = \pi(k) \in \pi(K)$ car $\pi(h)$ est le neutre de G/H , d'où $KH/H \subset \pi(K)$. Réciproquement, tout élément de $\pi(K)$ est de la forme \bar{k} avec $k \in K \subset KH$, il est donc a fortiori dans KH/H . Soit alors $\varphi : K \rightarrow KH/H$ le morphisme de groupes défini par $\varphi(k) = \bar{k} = \pi(k)$. Son noyau est clairement $K \cap H$ car $\ker \pi = H$. Comme $\pi(K) = KH/H$, on voit que φ est surjectif, et le théorème de factorisation donne alors $K/K \cap H \simeq KH/H$.

d) Soit $\psi : G/H \rightarrow G/N$ le morphisme de groupes défini par $\psi(\bar{g}) = \tilde{g}$, où \tilde{g} désigne l'image de g dans G/N . Cette définition a un sens car si g, g' sont des éléments de G avec $\bar{g} = \bar{g}'$, alors $g^{-1} g' \in H \subset N$ donc $\tilde{g} = \tilde{g}'$. On voit immédiatement que ψ est surjectif de noyau N/H , d'où le résultat avec le théorème de factorisation.

□

Remarque 1.15 Le cas particulier d'un groupe abélien $(A, +)$ est déjà intéressant : si B est un sous-groupe de A , alors les sous-groupes de A/B sont les C/B , où C est un sous-groupe de A contenant B . Plus généralement, l'image dans A/B d'un sous-groupe D de A est $(D + B)/B \simeq D/(B \cap D)$.

1.4. Centre et sous-groupe dérivé

Définition 1.16 Soient G un groupe. Le *centre* Z de G est l'ensemble des x de G qui vérifient $xy = yx$ pour tout y de G .

Exemple 1.17 a) Si K est un corps, le centre de $GL_n(K)$ est le sous groupe des $\lambda I_n, \lambda \in K^*$.

b) Pour $n \geq 3$, le centre de \mathcal{S}_n est réduit à l'élément neutre, comme il résulte facilement du fait que si $\tau = (a, b)$ est une transposition et $\sigma \in \mathcal{S}_n$, alors $\sigma \tau \sigma^{-1} = (\sigma(a), \sigma(b))$, donc σ ne commute pas avec τ dès qu'on choisit a avec $\sigma(a) := c$ distinct de a , puis b distinct de a et c (ce qui est possible pour tout σ distinct de l'identité, dès que $n \geq 3$).

Par définition Z est le noyau du morphisme $\text{int} : G \rightarrow \text{Aut } G$ qui envoie tout $g \in G$ sur l'*automorphisme intérieur* $x \mapsto gxg^{-1}$, donc $Z \triangleleft G$. On vérifie même immédiatement que Z est caractéristique dans G .

Définition 1.18 Soit G un groupe, et x, y deux éléments de G . On appelle *commutateur* de x et y l'élément $[x, y] := xyx^{-1}y^{-1}$. Le sous-groupe *dérivé* de G est par définition le sous-groupe **engendré** par les commutateurs.¹ On le note $D(G)$.

L'intérêt de $D(G)$ réside dans la proposition suivante :

Proposition 1.19 *Le sous-groupe $D(G)$ est caractéristique (en particulier distingué) dans G . Le quotient $G/D(G)$ est abélien, et $D(G)$ est le plus petit sous-groupe de G qui a cette propriété. On note $G^{\text{ab}} := G/D(G)$ ("abélianisé" de G).*

L'abélianisé de G est donc le plus "grand quotient abélien" de G , au sens suivant : si G/H est un autre quotient abélien, alors G/H est un quotient de G^{ab} (via le troisième théorème d'isomorphisme).

Démonstration : Si φ est un automorphisme de G , alors on a $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ d'où $\varphi(D(G)) \subset D(G)$ et $D(G)$ est caractéristique. Par définition du quotient, tout commutateur de $G/D(G)$ est trivial, donc $G/D(G)$ est abélien. Enfin, si $H \triangleleft G$ est un sous-groupe tel que G/H soit abélien, alors on a $xyx^{-1}y^{-1} = \bar{e}$ dans G/H pour tous x, y de G , donc $[x, y] \in H$; ainsi H contient $D(G)$ puisqu'il contient tous les commutateurs.²

□

Par exemple $D(G) = \{1\}$ si et seulement si G est abélien et $D(\mathcal{S}_3) = \mathcal{A}_3$: en effet on voit tout de suite que la signature d'un commutateur est 1, donc $D(\mathcal{S}_3) \subset \mathcal{A}_3$; mais \mathcal{S}_3 n'est pas commutatif donc $D(\mathcal{S}_3)$ n'est pas trivial, donc $D(\mathcal{S}_3) = \mathcal{A}_3$ est la seule possibilité via le théorème de Lagrange, vu que \mathcal{A}_3 est de cardinal 3.

On verra plus tard que pour $n \geq 2$, on a $D(\mathcal{S}_n) = \mathcal{A}_n$ donc $\mathcal{S}_n^{\text{ab}} \simeq \mathbf{Z}/2\mathbf{Z}$.

2. Groupes finis

2.1. Opérations de groupes, formule des classes

Rappelons la définition classique suivante :

1. Attention l'ensemble des commutateurs ne forme en général pas un sous-groupe, bien qu'il soit assez difficile de construire un contre-exemple.

2. Réciproquement, si H est un sous-groupe qui contient $D(G)$, alors H est automatiquement distingué car si $h \in H$ et $g \in G$, alors $(ghg^{-1})h^{-1} \in D(G) \subset H$, d'où $ghg^{-1} \in H$; il est immédiat que G/H est alors abélien.

Définition 2.1 Soit G un groupe et X un ensemble. On dit que G opère (ou agit) sur X si on s'est donné une application $G \times X \rightarrow X$, $(g, x) \mapsto g.x$, vérifiant

- Pour tous g, g' de G et tout x de X , on a $g.(g'.x) = (gg').x$
- Pour tout x de X , on a $1.x = x$

Remarque 2.2 Une définition équivalente consiste à se donner un morphisme $\Phi : G \rightarrow (\mathcal{S}(X), \circ)$, en posant $g.x = (\Phi(g))(x)$.

Exemple 2.3 a) Tout sous-groupe H de G opère sur G par *translations à gauche* via $h.x := hx$ pour tout $h \in H$ et tout $x \in G$.

b) G opère sur lui-même par conjugaison : $g.x := gxg^{-1}$. Ici l'image de G dans $\mathcal{S}(G)$ est de plus contenue dans $\text{Aut } G$ (ce qui n'était pas le cas dans l'exemple précédent). On dit alors que G opère par *automorphismes*.

c) Le groupe \mathcal{S}_n opère naturellement sur l'ensemble $\{1, \dots, n\}$.

Définition 2.4 Étant donnée une opération d'un groupe G sur un ensemble X , on appelle :

- *orbite* d'un élément x de X l'ensemble des $g.x$, $g \in G$. Les orbites sont les classes d'équivalence sur X pour la relation : $x \sim y$ si et seulement s'il existe $g \in G$ tel que $y = g.x$. S'il n'y a qu'une orbite, on dit que G opère *transitivement* sur X .
- *stabilisateur* d'un élément x de X le sous-groupe Stab_x des g de G qui vérifient $g.x = x$. Il n'est pas distingué dans G en général. On dit que l'action est *fidèle* si le seul élément de G qui stabilise tous les éléments de X est 1, *libre* si tous les stabilisateurs sont réduits à $\{1\}$ (c'est beaucoup plus fort). Autrement dit, une opération fidèle correspond à un morphisme $G \rightarrow \mathcal{S}(E)$ injectif.

Exemple 2.5 a) Si H est un sous-groupe de G , l'action de H sur G par translation à gauche est libre, et les orbites ne sont autre que les classes à **droite** suivant H . Si G est fini d'ordre n , on obtient en particulier qu'il existe un morphisme injectif (l'opération de G sur lui-même) de G dans $\mathcal{S}(G) \simeq \mathcal{S}_n$ (théorème de Cayley).

b) L'action de \mathcal{S}_n sur $\{1, \dots, n\}$ est transitive, et tous les stabilisateurs sont isomorphes à \mathcal{S}_{n-1} .

On vérifie immédiatement

Proposition 2.6 Étant donnée une opération d'un groupe G sur un ensemble X et $x \in X$, on définit une bijection de l'ensemble des classes à gauche G/Stab_x sur l'orbite $\omega(x)$ de x via : $\bar{g} \mapsto g.x$. En particulier si G est fini on a $\#\omega(x) = \#G/\#\text{Stab}_x$ (donc le cardinal de $\omega(x)$ divise celui de G).

□

Corollaire 2.7 (Équation aux classes) *Soit G un groupe fini opérant sur un ensemble fini X . Soit Ω l'ensemble des orbites, notons $\#\text{Stab}_\omega$ le cardinal du stabilisateur de x pour x dans l'orbite ω (indépendant du choix de x dans Ω d'après la proposition précédente). Alors*

$$\#X = \sum_{\omega \in \Omega} \frac{\#G}{\#\text{Stab}_\omega}$$

Démonstration : Comme les orbites forment une partition de X , c'est immédiat d'après la proposition précédente. Il y a néanmoins (comme on le verra plus tard) des conséquences tout à fait non triviales!

□

Theorème 2.8 (Formule de Burnside) *Soit G un groupe fini opérant sur un ensemble fini X . Pour tout $g \in G$, notons $\text{Fix } g$ le sous-ensemble de X constitué des points fixes de g . Alors*

$$\sum_{x \in X} \frac{1}{\#\omega(x)} = \frac{1}{\#G} \sum_{g \in G} \#(\text{Fix } g)$$

De plus ce nombre est égal au nombre d'orbites.

Démonstration : Soit E l'ensemble des couples (g, x) de $G \times X$ qui vérifient $g.x = x$. Alors son cardinal est $\sum_{g \in G} \#(\text{Fix } g)$, car pour chaque g de G on a $\text{Fix } g$ éléments x de X tels que $(g, x) \in E$. Mais ce cardinal est aussi $\sum_{x \in X} \#\text{Stab}_x = \sum_{x \in X} \frac{\#G}{\#\omega(x)}$ puisque pour chaque $x \in X$, on a $\#\text{Stab}_x = \frac{\#G}{\#\omega(x)}$ éléments g de G tels que $(g, x) \in E$. La formule en résulte. D'autre part, si Ω est l'ensemble des orbites, on a

$$\sum_{x \in X} \frac{1}{\#\omega(x)} = \sum_{\omega \in \Omega} \sum_{x \in \omega} \frac{1}{\#\omega} = \sum_{\omega \in \Omega} 1 = \#\Omega$$

□

2.2. p -groupes ; théorèmes de Sylow

Définition 2.9 Soit p un nombre premier. On appelle p -groupe un groupe de cardinal p^n , où n est un entier³.

3. Certains auteurs considèrent que le groupe trivial n'est pas un p -groupe, nous préférons la convention contraire qui permet en particulier de dire qu'un sous-groupe d'un p -groupe est toujours un p -groupe.

Proposition 2.10 *Soit G un p -groupe non trivial. Alors :*

- a) *Le centre Z de G n'est pas trivial.*
- b) *Si G est de cardinal p , il est cyclique. Si G est de cardinal p^2 , il est abélien.*

Démonstration : a) On fait opérer G sur lui-même par conjugaison. Il y a $\#Z$ orbites réduites à un élément, et le cardinal des autres orbites est un diviseur de $p^n := \#G$ autre que 1, donc est divisible par p . Ainsi p^n (avec $n > 0$) est la somme du cardinal de Z et d'un multiple de p , donc p divise $\#Z$.

b) Si G est de cardinal p , alors tout élément non trivial de G est d'ordre divisant p , donc d'ordre p , et G est cyclique. Supposons que G soit de cardinal p^2 . Si G n'était pas abélien, le cardinal de Z serait p d'après a), donc G/Z serait cyclique (car de cardinal p). Mais on obtient une contradiction via le lemme suivant :

Lemme 2.11 *Soit G un groupe de centre Z avec G/Z monogène. Alors G est abélien.*

Le lemme se démontre en prenant un générateur \bar{a} de G/Z . Alors tout élément g de G s'écrit $g = a^m z$ avec $z \in Z$, et il est alors immédiat que deux éléments de G commutent.

□

On passe maintenant aux théorèmes de Sylow, qui proviennent de la question suivante : étant donnés un groupe fini G et un entier n divisant son cardinal, peut-on trouver un sous-groupe d'ordre n ? En général la réponse est non (\mathcal{A}_4 est de cardinal 12, mais n'a pas de sous-groupe d'ordre 6, exercice...), mais dans le cas particulier des p -sous-groupes de Sylow, on va voir qu'on a une réponse positive.

Définition 2.12 *Soit p un nombre premier. Soit G un groupe de cardinal $n = p^\alpha m$ avec $\alpha \in \mathbf{N}$, $m \in \mathbf{N}^*$ et p ne divisant pas m . On appelle p -sous-groupe de Sylow (ou p -Sylow en abrégé) un sous-groupe H de cardinal p^α .*

Autrement dit, un p -Sylow est un p -sous groupe de G dont l'indice est premier à p (la notion est intéressante si p divise l'ordre de G , sinon un p -Sylow est juste le groupe trivial).

Théorème 2.13 (Premier théorème de Sylow) *Soit G un groupe fini et p un nombre premier. Alors G contient au moins un p -sous-groupe de Sylow.*

La preuve repose sur deux lemmes, qui ont un intérêt propre.

Lemme 2.14 *Soit H un sous-groupe de G . Si G contient un p -Sylow S , alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p -Sylow de H .*

(Ce lemme permet de se ramener à un "sur-groupe" pour prouver le théorème).

Lemme 2.15 *Soit $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ (corps à p éléments) et $G_p := \text{GL}_n(\mathbf{F}_p)$ avec $n \in \mathbf{N}^*$. Alors G_p possède un p -Sylow.*

Le premier théorème de Sylow résulte facilement de ces deux lemmes. En effet, il ne reste plus qu'à prouver que G est isomorphe à un sous-groupe de G_p . Or G est isomorphe à un sous-groupe de \mathcal{S}_n par le théorème de Cayley, et \mathcal{S}_n se plonge dans G_p en envoyant la permutation σ sur la matrice M_σ qui envoie le vecteur e_i sur $e_{\sigma(i)}$, où (e_1, \dots, e_n) est la base canonique de \mathbf{F}_p^n . Il reste à prouver les deux lemmes.

Preuve du lemme 2.14 : Le groupe H opère sur l'ensemble G/S des classes à gauche via $(h, aS) \mapsto (ha)S$. On voit tout de suite que le stabilisateur $\text{Stab}_H(aS)$ de aS pour cette action est $aSa^{-1} \cap H$. Chacun de ces $\text{Stab}_H(aS)$ est un p -groupe comme sous-groupe de aSa^{-1} , donc il suffit de montrer que l'un d'entre eux a un indice dans H non divisible par p . Or, cet indice $\frac{\#H}{\#\text{Stab}_H(aS)}$ est aussi le cardinal de l'orbite $\omega_H(aS)$. Comme p ne divise pas le cardinal de l'ensemble G/S (puisque S est un p -Sylow de G), le résultat vient de ce que les orbites forment une partition de G/S . □

Preuve du lemme 2.15 : On calcule d'abord le cardinal de G_p . C'est celui du nombre de bases du \mathbf{F}_p -espace vectoriel \mathbf{F}_p^n (en effet si \mathcal{B} est une telle base, il y a un et un seul élément de G_p qui envoie la base canonique sur \mathcal{B}), soit

$$(p^n - 1)(p^n - p) \dots (p^n - p^{n-1}).$$

On a en effet $p^n - 1$ choix pour le premier vecteur de la base (tout vecteur e_1 non nul), puis $p^n - p$ choix pour le deuxième (tout vecteur non multiple de e_1) etc. Il en ressort qu'un p -Sylow de G_p est de cardinal $p^{1+2+\dots+n-1} = p^{n(n-1)/2}$. Or l'ensemble des matrices triangulaires supérieures dont la diagonale n'a que des 1 est un sous-groupe de G_p qui possède ce cardinal. □

Le théorème suivant étudie la conjugaison des p -Sylow.

Theorème 2.16 (Deuxième théorème de Sylow) Soit G un groupe fini de cardinal $n = p^\alpha m$ avec p ne divisant pas m . Alors :

- a) Si $H \subset G$ est un p -groupe, il existe un p -Sylow de G qui le contient.
- b) Les p -Sylow de G sont tous conjugués, et leur nombre k divise n .
- c) k est congru à 1 mod. p (donc k divise m).

Démonstration : a) D'après le premier théorème de Sylow, il existe au moins un p -Sylow S de G . Le lemme 2.14 dit alors qu'il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p -Sylow de H , i.e. $aSa^{-1} \cap H = H$ puisque H est un p -groupe. Ainsi H est inclus dans aSa^{-1} qui est un p -Sylow de G .

b) Si H est un p -Sylow de G , on a de plus $H = aSa^{-1}$ par cardinalité, donc tout p -Sylow de G est conjugué de S . Faisons alors opérer G par conjugaison sur l'ensemble X des p -Sylow. Comme il n'y a qu'une seule orbite, son cardinal k (qui divise celui de G via la proposition 2.6) est celui de X , i.e. le nombre de p -Sylow.

c) Soit S un p -Sylow de G , on fait opérer S sur X par conjugaison. Soient X^S l'ensemble des points fixes pour cette action (i.e. les orbites réduites à un élément) et Ω' l'ensemble des autres orbites. L'équation aux classes s'écrit

$$k = \#X^S + \sum_{\omega \in \Omega'} \#\omega$$

Le cardinal des orbites qui sont dans Ω' divise celui de S (qui est une puissance de p) et n'est pas 1, donc est divisible par p . Pour conclure il suffit donc de montrer qu'il n'y a qu'une seule orbite réduite à un point (celle de S). i.e. : si T est un p -Sylow de G tel que $sTs^{-1} = T$ pour tout s de S , alors $S = T$.

Pour cela, on introduit le sous-groupe N de G engendré par S et T . A fortiori S et T sont des p -Sylow de N , donc sont conjugués par un élément de N via b). Mais T est distingué dans N via le fait que $sTs^{-1} = T$ pour tout s de S : en effet, le normalisateur $N_G(T)$ contient T et S , donc aussi le sous-groupe N qu'ils engendrent. Finalement $T = S$.⁴

□

Un cas particulier important est celui où m n'a aucun diviseur $\neq 1$ qui est congru à 1 modulo p . Alors G possède un p -Sylow unique, qui est donc distingué. Par exemple un groupe d'ordre 63 n'est pas *simple*, i.e. il possède un sous-groupe distingué autre que lui-même et le groupe trivial : en effet son nombre k de 7-Sylow doit diviser 9 et être congru à 1 modulo 7, donc $k = 1$, ce qui implique que l'unique 7-Sylow est distingué. Le même argument fonctionne pour un groupe d'ordre 255.

4. Ce raisonnement s'appelle "l'argument de Frattini".

2.3. Compléments sur $\mathbf{Z}/n\mathbf{Z}$

Rappelons que les générateurs du groupe additif $\mathbf{Z}/n\mathbf{Z}$ sont les \bar{s} , où s est un entier premier à n , il y en a donc $\varphi(n)$ (*indicatrice d'Euler* de n , i.e. le nombre d'entiers x de $[1, n]$ qui sont premiers avec n). Ce sont aussi les éléments du groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$ des inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$. Par exemple pour p premier on a $\varphi(p) = p - 1$, et plus généralement $\varphi(p^\alpha) = p^{\alpha-1}(p - 1)$ si $\alpha \geq 1$. De plus, on a un isomorphisme d'anneaux ("lemme chinois")

$$\mathbf{Z}/n\mathbf{Z} \simeq \prod_{i=1}^r \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}$$

et un isomorphisme de groupes

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq \prod_{i=1}^r (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^*.$$

On pourra aussi vérifier que le groupe des automorphismes du groupe additif $\mathbf{Z}/n\mathbf{Z}$ est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$ (tout élément de $(\mathbf{Z}/n\mathbf{Z})^*$ agissant par multiplication sur $\mathbf{Z}/n\mathbf{Z}$).

Pour aller plus loin, on voudrait maintenant déterminer la structure de $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ pour p premier et $\alpha \in \mathbf{N}^*$. On commence par le cas $\alpha = 1$.

Theorème 2.17 *Soient K un corps⁵ et G un sous-groupe fini du groupe multiplicatif K^* . Alors G est cyclique.*

Démonstration : On utilise le lemme suivant :

Lemme 2.18 *Soit $n \in \mathbf{N}^*$, alors*

$$n = \sum_{d|n} \varphi(d).$$

Le lemme est une conséquence immédiate du fait que les éléments d'ordre d dans $\mathbf{Z}/n\mathbf{Z}$ sont forcément dans l'unique sous-groupe C_d de $\mathbf{Z}/n\mathbf{Z}$ qui est de cardinal d ; or, comme C_d est isomorphe à $\mathbf{Z}/d\mathbf{Z}$, il contient $\varphi(d)$ éléments d'ordre d , donc finalement $\mathbf{Z}/n\mathbf{Z}$ contient $\varphi(d)$ éléments d'ordre d ; d'où le lemme en triant les éléments de $\mathbf{Z}/n\mathbf{Z}$ suivant leur ordre.

5. Rappelons qu'on impose que la multiplication de K soit commutative; sinon la proposition est fautive, l'algèbre \mathbf{H} des quaternions sur \mathbf{C} contenant par exemple un sous-groupe non-abélien de \mathbf{H}^* d'ordre 8.

Revenons à la preuve du théorème 2.17. Soit n le cardinal de G et supposons que G contienne un élément x d'ordre d . Alors le sous-groupe G_d engendré par x est de cardinal d , et tous ses éléments g vérifient $g^d = 1$. Mais dans le corps K l'équation polynomiale $X^d - 1 = 0$ a au plus d solutions, donc nécessairement G_d est l'ensemble de ces solutions. Comme il est cyclique d'ordre d , il contient $\varphi(d)$ éléments d'ordre d qui sont exactement les éléments d'ordre d de G (un élément d'ordre d de G vérifie l'équation $X^d - 1 = 0$, i.e. appartient à G_d). On a ainsi montré que pour tout d divisant n , G possède 0 ou $\varphi(d)$ éléments d'ordre d , c'est-à-dire en tout cas au plus $\varphi(d)$ éléments d'ordre d . D'après le lemme, on a $n > \sum_{d|n, d \neq n} \varphi(d)$, donc on obtiendrait une contradiction si G n'avait pas d'éléments d'ordre n . Ceci montre que G est cyclique. □

Remarque 2.19 Une autre méthode consiste à observer que dans un groupe abélien G fini, il existe un élément a dont l'ordre est le ppcm m des ordres de tous les éléments de G (utiliser le lemme 2.23 ci-dessous). Ensuite, si G est d'ordre n et est un sous-groupe de K^* , alors on ne peut avoir $m < n$, sinon tous les éléments de G vérifieraient $x^m = 1$, alors que cette équation a au plus m solutions dans K . Ainsi la seule possibilité est $m = n$.

Corollaire 2.20 *Pour p premier, le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique (donc isomorphe à $\mathbf{Z}/(p-1)\mathbf{Z}$).*

En effet dans ce cas $\mathbf{Z}/p\mathbf{Z}$ est un corps. Notons que déterminer explicitement un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$ est un problème algorithmique en général difficile.

On passe maintenant au cas général.

Théorème 2.21 *Soient p un nombre premier différent de 2 et $\alpha \in \mathbf{N}^*$. Alors le groupe $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ est cyclique (donc isomorphe au groupe additif $\mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z}$).*

Comme on le verra plus loin, ce résultat est faux si $p = 2$ et $\alpha \geq 3$.

Pour montrer le théorème, on commence par exhiber un élément d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ à l'aide du lemme suivant :

Lemme 2.22 *Soient p premier $\neq 2$ et $k \in \mathbf{N}^*$, alors*

$$(1+p)^{p^k} = 1 + \lambda p^{k+1}$$

avec λ entier non divisible par p .

Démonstration : On procède par récurrence sur k . Pour $k = 1$, on écrit

$$(1 + p)^p = 1 + pC_p^1 + p^2C_p^2 + \dots + p^p = 1 + p^2(1 + C_p^2 + \dots + p^{p-2})$$

et on utilise le fait que p divise C_p^k pour $1 \leq k \leq p-1$ (noter que pour $p = 2$ cette étape ne marche pas car p ne divise pas p^{p-2}), ce qui implique que

$$1 + C_p^2 + \dots + p^{p-2}$$

n'est pas divisible par p .

Supposons le résultat vrai pour k , alors

$$(1 + p)^{p^{k+1}} = (1 + \lambda p^{k+1})^p = 1 + \lambda p^{k+2} + p^{k+2} \sum_{i=2}^p C_p^i \lambda^i p^{i(k+1)-(k+2)}$$

et comme p divise $\sum_{i=2}^p C_p^i \lambda^i p^{i(k+1)-(k+2)}$ (il divise C_p^i pour $2 \leq i \leq p-1$, et $p^{p(k+1)-(k+2)}$), on obtient que

$$\lambda' := \lambda + \sum_{i=2}^p C_p^i \lambda^i p^{i(k+1)-(k+2)}$$

n'est pas divisible par p par hypothèse de récurrence, ce qui montre le lemme. \square

On aura besoin aussi d'un lemme classique sur les groupes abéliens :

Lemme 2.23 *Soit G un groupe abélien, noté multiplicativement. Soit $x \in G$ un élément d'ordre a et $y \in G$ un élément d'ordre b . Si a et b sont premiers entre eux, alors l'ordre de xy est ab .*

Noter que le résultat est faux si on ne suppose pas a et b premiers entre eux (prendre $y = x^{-1}$) et il est également faux dans un groupe non abélien si x et y ne commutent pas (prendre une transposition et un 3-cycle dans \mathcal{S}_3).

Preuve du lemme 2.23 : Soit $n \in \mathbf{N}^*$ tel que $(xy)^n = 1$, alors $x^n = y^{-n}$, d'où $y^{-na} = 1$ et b divise na . Comme b est premier avec a , on obtient que b divise n et de même a divise n , d'où ab divise n (toujours parce que $(a, b) = 1$). Comme par ailleurs $(xy)^{ab} = 1$, on voit que l'ordre de xy est bien ab . \square

Preuve du théorème 2.21 : D'après le lemme 2.22, l'élément $s = \overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$. Cherchons maintenant un élément d'ordre $p-1$. On a un morphisme surjectif $\pi : (\mathbf{Z}/p^\alpha\mathbf{Z})^* \rightarrow (\mathbf{Z}/p\mathbf{Z})^*$ obtenu en envoyant \bar{x} sur la classe de x modulo p (en effet x est inversible modulo p^α si et seulement s'il est inversible modulo p). Soient u un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$ (qui est cyclique d'après le corollaire 2.20) et $v \in (\mathbf{Z}/p^\alpha\mathbf{Z})^*$ tel que $\pi(v) = u$. Soit m l'ordre de v , alors $v^m = \bar{1}$ donc $u^m = \pi(v^m) = \bar{1}$ et $p-1$ (qui est l'ordre de u) divise m . Posons $r = v^{m/(p-1)}$, alors r est d'ordre $p-1$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$. Maintenant rs est d'ordre $(p-1)p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ par le lemme 2.23. \square

Le cas $p = 2$ est exceptionnel et fait l'objet du théorème suivant :

Théorème 2.24 *Pour tout entier $\alpha \geq 3$, le groupe multiplicatif $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ est isomorphe au groupe additif $\mathbf{Z}/2\mathbf{Z} \times (\mathbf{Z}/2^{\alpha-2}\mathbf{Z})$.*

Ainsi pour $\alpha \geq 3$ le groupe $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ n'est pas cyclique (l'ordre de tout élément divise $2^{\alpha-2}$). Les cas $\alpha = 1$ et $\alpha = 2$ sont triviaux, $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ étant alors respectivement isomorphe à $\{0\}$ et à $\mathbf{Z}/2\mathbf{Z}$.

Démonstration : On montre aisément par récurrence sur $k \geq 1$ qu'on a : $5^{2^k} = 1 + \lambda 2^{k+2}$ avec λ entier impair. Il en résulte que l'ordre de $\bar{5}$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ est exactement $2^{\alpha-2}$, autrement dit le sous-groupe N engendré par $\bar{5}$ est de cardinal $2^{\alpha-2}$. Son intersection avec le sous-groupe $C = \{\pm 1\}$ est $\bar{1}$, car toute puissance de 5 (contrairement à -1) est congrue à 1 modulo 4 . Il en résulte que $(n, c) \mapsto nc$ est un morphisme injectif de $N \times C$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$, et c'est donc un isomorphisme par cardinalité. On conclut en observant que N est isomorphe au groupe additif $\mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ et C au groupe additif $\mathbf{Z}/2\mathbf{Z}$. \square

3. Groupes simples, exemple du groupe alterné

Définition 3.1 Un groupe est *simple* s'il n'est pas réduit à $\{1\}$ et ses seuls sous-groupes distingués sont lui-même et $\{1\}$.

Par exemple, les groupes simples abéliens sont les $\mathbf{Z}/p\mathbf{Z}$ avec p premier (on voit en effet tout de suite qu'un tel groupe G est engendré par a pour tout $a \neq 1$ dans G , mais parmi les groupes monogènes \mathbf{Z} et $\mathbf{Z}/n\mathbf{Z}$ avec n non premier ont des sous-groupes non triviaux). Il n'est pas a priori facile de trouver d'autres exemples de groupes simples (voir [2], IV.4 pour l'exemple du groupe $\mathrm{PSL}_n(K)$, quotient de $SL_n(K)$ par les matrices scalaires de déterminant 1 ,

quand $n \geq 3$ ou le corps K possède au moins quatre éléments). Le but de ce paragraphe est de démontrer :

Theorème 3.2 *Pour $n \geq 5$, le groupe alterné \mathcal{A}_n est simple.*

Notons que le résultat est encore vrai (trivialement) pour $n = 2$ et $n = 3$, mais pas pour $n = 4$, le groupe constitué des doubles transpositions dans \mathcal{A}_4 étant un sous-groupe distingué non trivial.

Corollaire 3.3 *Pour $n \geq 5$, on a $D(\mathcal{A}_n) = \mathcal{A}_n$ et $D(\mathcal{S}_n) = \mathcal{A}_n$.*

On notera que la deuxième assertion est vraie pour tout $n \geq 2$ (seul le cas $n = 4$ est à vérifier séparément ; voir TD).

Démonstration : On a $D(\mathcal{S}_n) \subset \mathcal{A}_n$ vu que tout commutateur est de signature 1, et $D(\mathcal{S}_n)$ est distingué dans \mathcal{A}_n (il est déjà distingué dans \mathcal{S}_n), d'où $D(\mathcal{S}_n) = \mathcal{A}_n$ avec le théorème, vu que $D(\mathcal{S}_n)$ n'est pas réduit au neutre (en effet \mathcal{S}_n n'est pas abélien). On a de même $D(\mathcal{A}_n)$ distingué dans \mathcal{A}_n et non trivial (deux 3-cycles dont les supports ont un ou deux éléments en commun ne commutent pas), d'où $D(\mathcal{A}_n) = \mathcal{A}_n$.

□

Corollaire 3.4 *Si $n \geq 5$, \mathcal{S}_n a trois sous-groupes distingués : $\{\text{Id}\}$, \mathcal{A}_n et \mathcal{S}_n .*

Démonstration : Soit H un sous-groupe distingué de \mathcal{S}_n . Alors $H \cap \mathcal{A}_n$ est distingué dans \mathcal{A}_n , donc par le théorème $H \cap \mathcal{A}_n$ est égal à \mathcal{A}_n ou bien réduit à $\{\text{Id}\}$. Dans le premier cas, $H \supset \mathcal{A}_n$, donc $H = \mathcal{A}_n$ ou $H = \mathcal{S}_n$ car \mathcal{A}_n est d'indice 2 dans \mathcal{S}_n . Supposons donc $H \cap \mathcal{A}_n = \{\text{Id}\}$ et montrons que H est le groupe trivial. Si τ et σ sont deux éléments non triviaux de H , alors $\tau\sigma$ est de signature $(-1)(-1) = 1$, donc $\tau = \sigma^{-1}$. De ce fait $H = \{\text{Id}, \sigma, \sigma^{-1}\}$, mais alors H se surjecte sur $\{\pm 1\}$ par la signature, ce qui n'est pas possible si $\sigma \neq \sigma^{-1}$ parce qu'alors H est de cardinal 3, et 2 ne divise pas 3. Finalement H est de cardinal 1 ou 2 ; mais un sous-groupe de cardinal 2 de \mathcal{S}_n est de la forme $\{\text{Id}, \tau\}$ où τ est un produit de transpositions dont les supports sont disjoints, donc un tel sous-groupe ne peut pas être distingué si $n \geq 3$ par un calcul facile (conjuguer par un 3-cycle bien choisi).

□

Il est également vrai que tous les sous-groupes d'indice n de \mathcal{S}_n sont isomorphes à \mathcal{S}_{n-1} pour $n \geq 2$ ([2], corollaire 8.6).

Preuve de la simplicité de \mathcal{A}_n pour $n \geq 5$. Toutes les méthodes passent par deux lemmes assez simples :

Lemme 3.5 *Pour $n \geq 3$, les 3-cycles engendrent \mathcal{A}_n .*

Démonstration : Comme \mathcal{S}_n est engendré par les transpositions, \mathcal{A}_n est engendré par les produits de deux transpositions. Or, si a, b, c, d sont des éléments deux à deux distincts de $[1, n]$, on a $(a, b)(b, c) = (a, b, c)$, et $(a, b)(c, d) = (a, b)(a, c)(a, c)(c, d) = (a, c, b)(a, c, d)$, donc un produit de deux transpositions est un 3-cycle ou un produit de deux 3-cycle. □

Lemme 3.6 *Pour $n \geq 5$, les 3-cycles sont conjugués dans \mathcal{A}_n .*

Démonstration : Soient $\tau = (a_1, a_2, a_3)$ et $\tau' = (b_1, b_2, b_3)$ deux 3-cycles. Alors il existe $\sigma \in \mathcal{S}_n$ telle que $\sigma(a_i) = b_i$ pour $i = 1, 2, 3$, d'où $\sigma\tau\sigma^{-1} = \tau'$. Si $\varepsilon(\sigma) = 1$, c'est fini. Sinon on remplace σ par $\sigma' = \sigma(c, d)$, où c et d sont deux éléments de $[1, n]$, distincts, et distincts de a_1, a_2, a_3 (c'est ici que l'hypothèse $n \geq 5$ est utilisée). □

Il résulte des deux lemmes que tout sous-groupe distingué de \mathcal{A}_n contenant un 3-cycle est égal à \mathcal{A}_n si $n \geq 5$.

On montre maintenant le résultat pour $n = 5$:

Proposition 3.7 *Le groupe \mathcal{A}_5 est simple.*

Démonstration : Le cardinal de \mathcal{A}_5 est 60. On commence par trier ses éléments par leur ordre, en utilisant leur décomposition en cycles.

Les éléments d'ordre 2 sont les produits de deux transpositions à supports disjoints, il y en a $5 \times 3 = 15$ (5 choix pour le point fixe, et 3 doubles transpositions dans \mathcal{S}_4).

Les éléments d'ordre 3 sont les 3-cycles, il y en a $C_5^3 \times 2 = 20$ (C_5^3 choix pour les éléments permutés, et deux 3-cycles dans \mathcal{S}_3).

Il n'y a pas d'élément d'ordre 4 (les 4-cycles sont de signature -1).

Les éléments d'ordre 5 sont les 5-cycles, il y en a $4! = 24$, car se donner un 5-cycle c revient à se donner $c(1)$ (4 choix), puis $c^2(1)$ (3 choix) etc.

Soit maintenant H un sous-groupe distingué de \mathcal{A}_5 . Montrons que si H contient un élément d'ordre ω , avec $\omega \in \{2, 3, 5\}$, alors il contient tous les éléments d'ordre ω . Si $\omega = 3$, cela résulte du lemme 1. Si $\omega = 2$, il suffit de voir que les éléments d'ordre 2 sont conjugués dans \mathcal{A}_5 ; or si

$\tau = (a_1, a_2)(a_3, a_4)(a_5)$ et $\tau' = (b_1, b_2)(b_3, b_4)(b_5)$ sont deux tels éléments, il existe un élément σ de \mathcal{S}_5 tel que $\sigma(a_i) = b_i$ pour $i = 1, \dots, 5$, d'où $\sigma\tau\sigma^{-1} = \tau'$. Si σ est de signature -1, on la remplace par $\sigma(a_2, a_1)$. Enfin, bien que les 5-cycles ne soient pas tous conjugués dans \mathcal{A}_5 ⁶, les sous-groupes d'ordre 5 le sont car ce sont les 5-Sylow de \mathcal{A}_5 ; alors si H contient un élément d'ordre 5, il contient le sous-groupe qu'il engendre, donc tous les sous-groupes d'ordre 5, donc tous les éléments d'ordre 5.

Supposons maintenant $H \neq \{\text{Id}\}$. Alors il ne peut exister $\omega \in \{2, 3, 5\}$ tel que tout élément non trivial de H soit d'ordre ω , sinon d'après ce qui précède H serait de cardinal $15 + 1$, $20 + 1$, ou $24 + 1$, et aucun de ces nombres ne divise 60. Il existe donc au moins deux nombres ω, ω' parmi 2, 3, 5 tels que H contienne tous les éléments d'ordre ω et ω' , mais alors le cardinal de H dépasse strictement $60/2$, et $H = \mathcal{A}_5$ vu que son cardinal doit diviser 60. \square

En fait \mathcal{A}_5 est le le plus petit groupe simple autre que les $\mathbf{Z}/p\mathbf{Z}$ pour p premier (exercice, pas facile...).

Preuve du théorème dans le cas général. Soit $E = [1, n]$, H un sous-groupe de \mathcal{A}_n non réduit à l'identité. On choisit σ non trivial dans H . On va se ramener au cas $n = 5$ en fabriquant un élément de H qui agit sur un sous-ensemble de cardinal au plus 5 de E . Pour cela, on va considérer non pas un conjugué de σ (qui aurait le même nombre de points fixes que σ), mais un commutateur $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$ (qui a une chance d'en avoir davantage). On choisit τ de la manière suivante : soit a dans E tel que $b := \sigma(a)$ soit distinct de a , puis c dans E distinct de a, b , et $\sigma(b)$. On pose alors $\tau = (a, c, b)$, ce qui fait que $\rho = (\tau\sigma\tau^{-1})\sigma^{-1}$ est bien dans H . Alors $\tau^{-1} = (a, b, c)$ d'où $\rho = (a, c, b)(\sigma\tau^{-1}\sigma^{-1}) = (a, c, b)(\sigma.a, \sigma.b, \sigma.c)$. Comme $\sigma.a = b$, on voit qu'il existe un sous-ensemble F de E qui a au plus 5 éléments (et on peut le prendre de cardinal exactement 5) tel que ρ opère trivialement en dehors de F , et F contienne $\{a, b, c, \sigma(b), \sigma(c)\}$. On note aussi que ρ opère non trivialement sur F car $\rho(b) = \tau\sigma(b) \neq b$ (vu que $\sigma(b) \neq c = \tau^{-1}(b)$).

On obtient un morphisme injectif i de $\mathcal{A}(F)$ dans \mathcal{A}_n en prolongeant une permutation de F par l'identité en dehors de F . Posons $H_0 = i^{-1}(H)$, c'est un sous-groupe distingué de $\mathcal{A}(F) \simeq \mathcal{A}_5$. Mais H_0 n'est pas trivial car il contient la restriction de ρ à F . Ainsi $H_0 = \mathcal{A}(F)$ d'après le cas $n = 5$. En particulier H_0 contient un 3-cycle, donc H aussi, donc $H = \mathcal{A}_n$ avec les deux lemmes.

6. En fait si c et c' sont deux 5-cycles, c est conjugué de c' ou c'^2 , ce qui suffit à faire l'argument.

□

4. Groupes résolubles et nilpotents

On se contentera ici des définitions et des premières propriétés. On pourra se reporter au livre de Hall [1] pour plus de détails.

Définition 4.1 Soit G un groupe.⁷ On dit que G est *résoluble* s'il existe une suite finie

$$\{1\} = G_0 \subset G_1 \subset \dots \subset G_n = G$$

avec pour tout $i \in [1, n]$, $G_{i-1} \triangleleft G_i$ et G_i/G_{i-1} abélien.

Il est commode d'avoir la caractérisation suivante :

Proposition 4.2 Soit G un groupe, on pose $D^0(G) = G$, $D^1(G) = D(G)$, et $D^i(G) = D(D^{i-1}(G))$ pour tout $i \geq 2$. Alors G est résoluble si et seulement s'il existe un entier n tel que $D^n(G) = \{1\}$.

Démonstration : S'il existe n tel que $D^n(G) = \{1\}$, alors chaque quotient $D^{i-1}(G)/D^i(G)$ est un groupe abélien par définition du sous-groupe dérivé donc G est résoluble via la suite des $D^i(G)$. Notons que chaque $D^i(G)$ est distingué dans G tout entier parce que le sous-groupe dérivé d'un groupe H est caractéristique dans H , et cette propriété est transitive.

En sens inverse si G est résoluble, soit $(G_i)_{1 \leq i \leq n}$ une suite comme dans la définition 4.1. Alors G/G_{n-1} est abélien donc $G_{n-1} \supset D(G)$. Par récurrence sur i , on a $G_{n-i} \supset D^i(G)$ (si $G_{n-i+1} \supset D^{i-1}(G)$, alors comme G_{n-i+1}/G_{n-i} est abélien, on a $G_{n-i} \supset D(G_{n-i+1}) \supset D(D^{i-1}(G)) = D^i(G)$). Pour $i = n$ cela donne $D^n(G) = \{1\}$.

□

Définition 4.3 Un groupe G est une *extension* d'un groupe H par un groupe N s'il existe une suite exacte courte

$$1 \rightarrow N \rightarrow G \rightarrow H \rightarrow 1,$$

autrement dit si H est isomorphe au quotient de G par un sous-groupe isomorphe à N (qu'on notera souvent aussi N).

⁷. La notion est surtout intéressante pour les groupes finis, mais ce n'est pas indispensable de le supposer.

Remarque 4.4 a) La proposition 4.2 donne qu'on peut demander en plus que chaque G_i soit distingué dans G tout entier (en utilisant la suite $D^i(G)$ des sous-groupes dérivés successifs). Ainsi G résoluble signifie que G se déduit de $\{1\}$ par une suite finie d'*extensions à noyaux abéliens* :

$$1 \rightarrow G_i/G_{i-1} \rightarrow G/G_{i-1} \rightarrow G/G_i \rightarrow 1.$$

b) Si G est fini et qu'on n'impose pas $G_i \triangleleft G$, on peut demander G_i/G_{i-1} cyclique d'ordre premier au lieu d'abélien : en effet tout groupe abélien fini H admet une suite $H \supset \dots \supset \{1\}$ avec tous les H_i/H_{i-1} simples (donc cycliques d'ordre premier car abéliens), par récurrence sur $\#H$. Par contre demander G_i/G_{i-1} cyclique et $G_i \triangleleft G$ pour tout i est plus fort (on parle alors de groupe *hyper-résoluble*).

c) Le terme résoluble vient de la théorie de Galois, comme on le verra dans la partie du cours consacrée à la résolubilité par radicaux des équations algébriques.

Définition 4.5 On dit qu'un groupe G est *nilpotent* s'il existe une suite finie

$$\{1\} = G_0 \subset G_1 \subset \dots \subset G_n = G$$

tel que pour tout $i \in [1, n]$: $G_i \triangleleft G$ et l'extension

$$1 \rightarrow G_i/G_{i-1} \rightarrow G/G_{i-1} \rightarrow G/G_i \rightarrow 1$$

est *centrale*, i.e. G_i/G_{i-1} est inclus dans le centre de G/G_{i-1} .

Cela signifie donc que G se déduit de $\{1\}$ par une suite finie d'extensions centrales (ainsi nilpotent implique résoluble).

Exemple 4.6 a) Un groupe abélien est nilpotent.

b) Un p -groupe G est nilpotent : c'est immédiat par récurrence sur son cardinal, vu que son centre est non trivial si G est non trivial, et le quotient de G par son centre est encore un p -groupe.

c) \mathcal{S}_n et \mathcal{A}_n ne sont pas résolubles pour $n \geq 5$. Cela résulte de ce que $D(\mathcal{S}_n) = D(\mathcal{A}_n) = \mathcal{A}_n$, et de la proposition 4.2.

d) \mathcal{S}_4 est résoluble, via la suite $\mathcal{S}_4 \supset \mathcal{A}_4 \supset V_4 \supset \{1\}$, où V_4 est le sous-groupe constitué de l'identité et des doubles transpositions, mais il ne peut pas être nilpotent car son centre est trivial. Les mêmes conclusions valent pour \mathcal{A}_4 et \mathcal{S}_3

e) \mathcal{S}_3 est hyper-résoluble mais pas \mathcal{A}_4 .

f) Un sous-groupe et un quotient d'un groupe résoluble sont résolubles, ainsi qu'une extension d'un groupe résoluble par un groupe résoluble (voir TD). De même pour nilpotent (à condition pour le dernier énoncé de supposer que l'extension est centrale).

Références

- [1] M. Hall Jr : *The theory of groups*, The Macmillan Co., New York, N.Y. 1959.
- [2] D. Perrin : *Cours d'algèbre*, Ellipses 1996.