Arithmétique et groupes

D. Harari

L2-Maths 209

1. Nombres premiers, congruences

1.1. Nombres entiers, divisibilité

Rappel des notations $\mathbf{N}$, $\mathbf{N}^*$, $\mathbf{Z}$ (on évitera $\mathbf{Z}^*$).

Définition de a *divise* b pour a, b dans $\mathbf{Z}$ (ou encore a est un diviseur de b, b est un multiple de a), notation $a \mid b$. Exemples.

On remarquera qu'on obtient ainsi une relation d'*ordre partiel* sur $\mathbf{N}$ ou $\mathbf{N}^*$ (rappeler la notion).

1.2. Nombres premiers

Définition, exemples. Existence et unicité (admises) de la décomposition en facteurs premiers d'un entier $n \geq 2$ (pour l'existence, on esquissera le principe de la preuve par récurrence, que l'on fera en détails en TD).

Notion d'entiers relatifs *premiers entre eux* (sans parler encore de pgcd en général), caractérisation en termes de leur décomposition en facteurs premiers.

1.3. Division euclidienne

Définition, exemples. Illustration avec un dessin. Démonstration détaillée (en particulier : raisonnement par récurrence sur a pour l'existence de la division de $a \geq 0$ par $b > 0$).

1.4. Congruences

Définition, notation $a \equiv b \quad [n]$. La relation de congruence (pour n fixé) est une *relation d'équivalence* (on en profitera pour rappeler cette notion). On fera remarquer qu'il y a n classes d'équivalence via la division euclidienne (sans parler encore de $\mathbf{Z}/n\mathbf{Z}$). Calcul avec les congruences : on peut additionner ou multiplier des congruences modulo n. Critères de divisibilité (par 3, par 4, par 9, par 11...).

2. Notion de groupe; premières applications en arithmétique

2.1. Définition, premiers exemples

Notion de *loi de composition interne* (notée par exemple T ou encore $*$ pour les questions abstraites) sur un ensemble E : à deux éléments a et b de E, on associe aTb. Définition d'une loi associative, d'un élément neutre (il est unique s'il existe) et d'un symétrique (unique s'il existe quand la loi est associative). Définition d'un *groupe*, d'un groupe commutatif (ou *abélien*). Exemples et contre-exemples avec $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{R}$, $\mathbf{R}^*$ pour l'addition et la multiplication.

Un exemple de groupe non commutatif : les bijections de $\mathbf{R}$ dans $\mathbf{R}$ pour la loi $\circ$. Généralisation : si E est un ensemble, les bijections de E dans E forment un groupe $\mathcal{S}(E)$ (non commutatif en général), qu'on appelle $\mathcal{S}_n$ si $E = \{1, ..., n\}$. Le groupe $\mathcal{S}_n$ est de cardinal $n!$. Un autre exemple consiste à prendre les matrices $(2,2)$ de déterminant non nul, avec comme loi le produit usuel des matrices (qui correspond d'ailleurs à la composition des applications linéaires).

2.2. Sous-groupes

Définition d'un sous-groupe; on fera remarquer que le moyen le plus simple pour montrer qu'un ensemble muni d'une loi est un groupe consiste à le voir comme sous-groupe d'un groupe déjà connu. Exemple de $\mathbf{Z}$ vu comme sous-groupe additif de $\mathbf{R}$ ou $\mathbf{C}$, contre-exemple de $\mathbf{N}$. Exemples multiplicatifs : les complexes de module 1 comme sous-groupe de $\mathbf{C}^*$. Un sous-groupe d'un groupe abélien est abélien, mais pas de réciproque (contre-exemple avec $\mathcal{S}_3$). On observera que tout groupe G admet les sous-groupes triviaux G et $\{e\}$. L'intersection de deux sous-groupes est un sous-groupe, mais pas la réunion en général (voir TD).

2.3. Groupes abéliens-compléments de notations

On peut les noter additivement (mais ce n'est pas toujours le cas, comme on l'a vu avec les groupes multiplicatifs comme $\mathbf{R}^*$). Dans ce cas, on note

$-x$ l'opposé de x et nx l'élément $x + x + ... + x$ quand $n > 0$ (avec la convention $nx = -(-nx)$ si $n < 0$ et $0x = 0$). On insistera bien sur le fait que c'est une *convention* valable dans n'importe quel groupe abélien "abstrait". Exemples : $\mathbf{Z}$, $\mathbf{R}^n$, le groupe additif des matrices carrées. On observera qu'avec ces conventions, les règles de calcul habituel sont valables pour $n(x + y)$, $(m + n)x$, ou encore $(mn)x$.

Remarque : Pour les questions abstraites sur les groupes, il est souvent d'usage de noter la loi multiplicativement *même si elle n'est pas commutative* (on pensera aux matrices); le symétrique de x est alors noté x^{-1}, et x^n désigne le produit $x.x...x$ avec n facteurs si $n \in \mathbf{N}^*$. On fera attention au fait que par exemple $(xy)^{-1} = y^{-1}x^{-1}$ (l'ordre est important) et $(xy)^2 = xyxy$ (ça ne se simplifie pas !). On a bien par contre $x^{mn} = (x^m)^n$ et $x^{m+n} = x^m.x^n$. Nous emploierons plus tard assez systématiquement cette notation multiplicative pour les groupes "abstraits" qui ne sont pas supposés commutatifs.

2.4. Sous-groupes de Z

Pour tout $n \geq 0$, l'ensemble $n\mathbf{Z}$ des nombres divisibles par n est un sous-groupe additif de $\mathbf{Z}$. Réciproquement, tous les sous-groupes de $\mathbf{Z}$ sont de cette forme (et le $n \geq 0$ associé est unique). Preuve via la division euclidienne. On remarque que $m\mathbf{Z} \subset n\mathbf{Z}$ ssi n divise m.

2.5. pgcd

Définition de $a \wedge b$: c'est l'entier $n \geq 0$ tel que le sous-groupe des $ax + by$ (pour x, y dans $\mathbf{Z}$) soit égal à $n\mathbf{Z}$. Caractérisation comme plus grand commun diviseur *pour la relation d'ordre partiel de divisibilité* (c'est aussi le plus grand au sens usuel sauf s'il est nul, ce qui n'arrive que pour $a = b = 0$). Exemples (notamment $a \wedge b =\mid a \mid$ si a divise b, cas de a premier).

Nombres premiers entre eux (=leur pgcd est 1). Théorème de Bezout. Algorithme d'Euclide pour calculer le pgcd. Recherche explicite de u, v tels que $au + bv = a \wedge b$.

Si a divise bc et est premier avec b, alors il divise c (lemme de Gauss, preuve via Bezout). Cela implique l'unicité de la décomposition en facteurs premiers (qu'on avait admise jusque-là), via la cas particulier où a est premier.

Caractérisation du pgcd via la décomposition en facteurs premiers.

pgcd de r entiers; ppcm.

2.6. Application : l'équation $ax + by = c$

On donne la méthode en cinq étapes :

-Si $a \wedge b$ ne divise pas c, pas de solution.

-Sinon on se ramène à a et b premiers entre eux en divisant par $a \wedge b$.

-On cherche alors u et v tels que $au + bv = 1$.

-On trouve une solution particulière (uc, vc).

-On est ramené à $aX + bY = 0$ via un changement de variable, dont les solutions sont $(bn, -an), n \in \mathbf{Z}$ par le lemme de Gauss.

Exemple : $16x + 30y = 10$

3. Le groupe abélien $(\mathbf{Z}/n\mathbf{Z}, +)$

3.1. Définition, premières propriétés

Définition comme les classes d'équivalence pour la relation de congruence mod n. On verra différents systèmes de représentants. Notation $\bar{x}$ pour la classe de $x \in \mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ (ou x mod. n si n n'est pas sous-entendu). On prendra garde que $\mathbf{Z}/n\mathbf{Z}$ n'est pas un sous-groupe de $\mathbf{Z}$, autrement dit ses éléments ne sont pas des nombres au sens usuel.

Structure de groupe abélien (la difficulté est de comprendre qu'il y a quelque chose à vérifier pour définir la loi par la formule $\bar{x} + \bar{y} = \overline{x + y}$). Loi multiplicative (qui ne fait pas de $\mathbf{Z}/n\mathbf{Z}$ un groupe en général, même si on enlève 0). Notion d'anneau, structure d'anneau commutatif sur $\mathbf{Z}/n\mathbf{Z}$.

3.2. Groupe cyclique

Notion de *groupe engendré par un élément* dans un groupe abélien. Le groupe $\mathbf{Z}/n\mathbf{Z}$ est engendré par $\bar{1}$, il est *cyclique* de cardinal n. On observera que par exemple le groupe multiplicatif des racines n-ièmes de l'unité dans $\mathbf{C}$ a la même propriété. Exemple : $n = 12$ (l'aiguille des heures d'une horloge).

3.3. Générateurs de $\mathbf{Z}/n\mathbf{Z}$

Trois propriétés équivalentes. Cas particulier de $n = p$ premier ($\mathbf{Z}/p\mathbf{Z}$ est un *corps*, et ce n'est vrai que si p est premier). Notation $(\mathbf{Z}/n\mathbf{Z})^*$, cardinal de $(\mathbf{Z}/n\mathbf{Z})^*$ (sans pour l'instant les propriétés de $\varphi(n)$). Exemples explicites (n premier, $n = 4$, $n = 6$).

3.4. Lemme chinois

Preuve avec Bezout, ou en utilisant l'application

$$x \,\mathrm{mod.}\, mn \mapsto (x \,\mathrm{mod.}\, m, x \,\mathrm{mod.} n)$$

qui est injective de $\mathbf{Z}/mn\mathbf{Z}$ dans $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$, donc surjective pour raison de cardinalité. Généralisation à r entiers *deux à deux* premiers entre eux.

4. Groupes-théorie générale

4.1. Quelques rappels et exemples

On notera désormais les groupes "abstraits" multiplicativement (attention aux erreurs habituelles avec les règles de calcul !). Rappel des exemples non commutatifs : $\mathcal{S}_n$, groupes de matrices, groupes d'isométries en géométrie plane.

4.2. Morphismes, noyau, image

Définition, propriétés élémentaires, exemples (on fera attention au fait que les lois peuvent être notées différemment au départ et à l'arrivée). Le noyau d'un morphisme $f : G \to G'$ est un sous-groupe de G, et il est réduit au neutre ssi f est injectif. Image d'un morphisme de groupes, isomorphisme de groupes.

Notion de groupes *isomorphes*, exemple des racines n-èmes de l'unité et de $\mathbf{Z}/n\mathbf{Z}$, de $(\mathbf{R}_+^*, \times)$ et $(\mathbf{R}, +)$; on insistera sur le fait que quand deux groupes sont isomorphes, toute "formule" vraie dans l'un est vraie dans l'autre : par exemple $\mathbf{Z}/4\mathbf{Z}$ n'est pas isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

4.3. Retour sur les groupes cycliques

Rappel sur la notion de groupe engendré par un élément (notamment en notation multiplicative). Tout groupe cyclique est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ (et un groupe monogène infini est isomorphe à $\mathbf{Z}$). Notion d'*ordre* d'un élément dans un groupe, exemples avec $\mathbf{Z}/n\mathbf{Z}$, $\mathcal{S}_3$, les matrices.

4.4. Cardinal d'un sous-groupe; théorème de Lagrange

Le cardinal d'un sous-groupe d'un groupe fini divise le cardinal du groupe (admis en cours, voir DM pour une preuve). Application à l'ordre d'un élément (attention : pas de réciproque). Exemple d'un groupe de cardinal premier (forcément cyclique).

5. Le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$

5.1. Structure de groupe multiplicatif de $(\mathbf{Z}/n\mathbf{Z})^*$

Attention aux confusions habituelles entre les loi $+$ et $\times$, et à la définition correcte de $(\mathbf{Z}/n\mathbf{Z})^*$, qui est un groupe commutatif de cardinal $\varphi(n)$ pour la multiplication.

5.2. Théorème d'Euler

Preuve via le théorème de Lagrange, cas particulier du petit théorème de Fermat.

5.3. Calcul de $\varphi(n)$

Retour sur le lemme chinois : formule $\varphi(mn) = \varphi(m)\varphi(n)$ quand m et n sont premiers entre eux. Application au calcul de $\varphi(n)$ pour n quelconque. Exemples. On remarquera au passage que $(\mathbf{Z}/n\mathbf{Z})^*$ n'est pas toujours cyclique, par exemple pour $n = 8$ (attention aux erreurs habituelles : l'ordre de tout élément de $(\mathbf{Z}/n\mathbf{Z})^*$ dans le groupe *additif* $(\mathbf{Z}/n\mathbf{Z})$ est n, mais ça ne dit rien sur son ordre dans le groupe *multiplicatif* $(\mathbf{Z}/n\mathbf{Z})^*$).

5.4. Quelques calculs dans $(\mathbf{Z}/n\mathbf{Z})^*$

Si m et n sont premiers entre eux, les groupes multiplicatifs $(\mathbf{Z}/mn\mathbf{Z})^*$ et $(\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*$ sont isomorphes. Exemples : $(\mathbf{Z}/10\mathbf{Z})^*$ est cyclique, $(\mathbf{Z}/15\mathbf{Z})^*$ ne l'est pas (il est isomorphe au groupe additif $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$).

Si p est premier, $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique (admis). Calcul de l'ordre de $\overline{1+p}$ dans $(\mathbf{Z}/p^k\mathbf{Z})^*$ pour p premier ≥ 3.