M1 2021-2022 : GROUPES

David Harari

Table des matières

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

On commence par la proposition élémentaire suivante, que nous rappelons sans démonstration :

Proposition 2.1 *Soit $n \in \mathbf{N}^*$, $s \in \mathbf{Z}$. Alors les propriétés suivantes sont équivalentes :*

i) $(s, n) = 1$.

ii) $\bar{s}$ *engendre le groupe additif* $\mathbf{Z}/n\mathbf{Z}$.

iii) $\bar{s}$ *appartient au groupe des inversibles* $(\mathbf{Z}/n\mathbf{Z})^*$ *de l'anneau* $\mathbf{Z}/n\mathbf{Z}$.

On note $\varphi(n)$ l'*indicatrice d'Euler* de n, i.e. le nombre d'entiers x de $[1, n]$ qui sont premiers avec n. Ainsi $\varphi(n)$ est le cardinal de $(\mathbf{Z}/n\mathbf{Z})^*$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ si $\alpha \geq 1$ et p est premier.

Proposition 2.2 *Soit $n \in \mathbf{N}^*$, on écrit $n = \prod_{i=1}^r p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts. Alors :*

a) L'application $a \mapsto (x \mapsto ax)$ est un isomorphisme du groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$ sur le groupe $\mathtt{Aut}(\mathbf{Z}/n\mathbf{Z})$ des automorphismes du groupe additif $\mathbf{Z}/n\mathbf{Z}$.

b) (lemme chinois) On a un isomorphisme d'anneaux

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

obtenu en envoyant $\bar{x}$ sur (x_i), où x_i est la classe de x modulo $p_i^{\alpha_i}$. On a un isomorphisme de groupes

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

c) On a $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r}(1 - \frac{1}{p_i})$.

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 2.3 *Soient K un corps*[1] *et G un sous-groupe fini du groupe multiplicatif K^*. Alors G est cyclique.*

Démonstration : On utilise le lemme suivant :

Lemme 2.4 *Soit $n \in \mathbf{N}^*$, alors*

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

Le lemme est une conséquence immédiate de l'existence (pour d divisant n) d'un unique sous groupe d'ordre d dans $\mathbf{Z}/n\mathbf{Z}$ qui implique en particulier que le groupe $\mathbf{Z}/n\mathbf{Z}$ possède $\varphi(d)$ éléments d'ordre exactement d.

Revenons à la preuve du théorème 2.3. 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.

□

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

Corollaire 2.5 *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 (cas particulier de la proposition 2.1). 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.

Theorème 2.6 *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 2.7 *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

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

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

$$1 + C_p^2 + ... + p^{p-2}$$

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.

□

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

Lemme 2.8 *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 théorème 2.6 : D'après le lemme 2.7, 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 $\pi : (\mathbf{Z}/p^\alpha\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*$ 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 2.5) 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 2.8.

□

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

Theorème 2.9 *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 $C = \{\pm\bar{1}\}$ 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 $\mathbf{Z}/2\mathbf{Z}$.

□

Rappelons enfin que tout groupe abélien de type fini est isomorphe à un produit direct $\mathbf{Z}^r \times \mathbf{Z}/d_1 \times ... \times \mathbf{Z}/d_m$, avec $r \in \mathbf{N}$ et les entiers $d_1, ..., d_m$ au moins égaux à 2, et qu'il existe une unique telle décomposition avec $d_1|d_2|...|d_m$.

3. Quelques notions supplémentaires liées aux sous-groupes distingués

3.1. Suites exactes

On commence par la très utile notion de suite exacte, qu'on peut d'ailleurs étendre aux espaces vectoriels (et, comme on le verra plus tard, aux modules).

Définition 3.1 On dit qu'une suite (finie ou infinie)

$$... \to G_i \stackrel{f_i}{\to} G_{i+1} \stackrel{f_{i+1}}{\to} G_{i+2} \to ...$$

est *exacte* (les G_i étant des groupes et les f_i des morphismes) si pour tout i, on a $\mathrm{Im}\, f_i = \ker f_{i+1}$. En particulier

$$1 \to N \stackrel{i}{\to} G \stackrel{p}{\to} H \to 1$$

est une suite exacte (dite courte) si et seulement si on a les trois propriétés : i injective, p surjective, $\mathrm{Im}\, i = \ker p$. Dans ce cas, on a $G/N \simeq H$ (en identifiant N à $i(N)$) via le théorème de factorisation, et on dit que G est une *extension* de H par N.[2]

Remarque 3.2 a) De même qu'on ne confondra pas sous-groupe et quotient, on ne confondra pas "sur-groupe" et extension.

b) Quand tous les groupes sont abéliens et notés additivement, on écrira souvent 0 au lieu de 1 dans une suite exacte courte.

Exemple 3.3 a) Si K est un corps, alors la suite

$$1 \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \stackrel{\det}{\to} K^* \to 1$$

est exacte.

b) Si $n \geq 2$, la suite

$$1 \to \mathcal{A}_n \to \mathcal{S}_n \stackrel{\varepsilon}{\to} \{\pm 1\} \to 1$$

est exacte.

c) Le groupe $\mathbf{Z}/4$ peut se voir comme une extension de $\mathbf{Z}/2$ par $\mathbf{Z}/2$, via la suite exacte

$$0 \to \mathbf{Z}/2 \to \mathbf{Z}/4 \to \mathbf{Z}/2 \to 0, \tag{1}$$

où la flèche $\mathbf{Z}/4 \to \mathbf{Z}/2$ envoie chaque $\bar{x} \in \mathbf{Z}/4$ sur la classe de x dans $\mathbf{Z}/2$, et la flèche $\mathbf{Z}/2 \to \mathbf{Z}/4$ envoie chaque $\bar{y} \in \mathbf{Z}/2$ sur la classe de $2y$ dans $\mathbf{Z}/4$. Noter que $\mathbf{Z}/4$ n'est pas pour autant isomorphe au produit de $\mathbf{Z}/2$ par $\mathbf{Z}/2$.

2. Certains auteurs, par exemple D. Perrin, disent plutôt extension de N par H.

3.2. Produit semi-direct de deux groupes

Attention à cette notion, qui est en général la source de nombreuses erreurs, notamment à l'oral de l'agrégation...

Rappelons que quand G_1 et G_2 sont deux groupes, on dispose du produit direct $G_1 \times G_2$ qui correspond à mettre la loi $(g_1, g_2)(h_1, h_2) = (g_1 g_2, h_1 h_2)$ sur l'ensemble produit.

Le produit semi-direct est une généralisation de cette notion. Soient N et H deux groupes et $\varphi : H \to \mathtt{Aut}N$ un morphisme de groupes, qui définit en particulier une action $h.n := \varphi(h)(n)$ de H sur N (mais on demande en plus ici que l'action soit par automorphismes, i.e. l'image de φ doit être incluse dans $\mathtt{Aut}N$, et pas seulement dans $\mathcal{S}(N)$).

Theorème 3.4 *On définit une loi de groupes sur l'ensemble produit $N \times H$ en posant*

$$(n, h).(n', h') := (n(h.n'), hh')$$

Ce groupe s'appelle le produit semi-direct de N par H relativement à l'action φ ; on le note $N \rtimes_\varphi H$ (ou simplement $N \rtimes H$ si l'action φ est sous-entendue).

Remarque 3.5 a) Parler "du" produit semi-direct de N par H n'a de sens que si on précise l'action, il peut exister plusieurs actions de H sur N, donc plusieurs produits semi-directs. On fera aussi attention au fait que H et N ne jouent pas des rôles symétriques.

b) L'action triviale correspond au produit direct.

Proposition 3.6 *Avec les notations ci-dessus, soit $G = N \rtimes H$. Alors :*

a) On a une suite exacte

$$1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$$

avec $i(n) = (n, 1)$ et $p(n, h) = h$. En particulier N s'identifie à un sous-groupe distingué (noté encore N)[3] *dans G.*

b) La suite exacte est scindée, i.e. il existe un morphisme $s : H \to G$ ("section") vérifiant $p \circ s = \mathrm{Id}_H$. Ainsi H s'identifie à un sous-groupe (encore noté H) de G.

3. N comme "normal" ; le symbole $\rtimes$ ressemble à $\lhd$ et permet de se rappeler le "sens" dans lequel on effectue le produit semi-direct.

Démonstration : a) i et p sont des morphismes via

$$(n,1)(n',1) = (n(1.n'),1) = (nn',1)$$

et

$$(n,h)(n',h') = (n(h.n'),hh').$$

Le fait que la suite soit exacte est immédiat.

b) Il suffit de poser $s(h) = (1,h)$.

□

Noter que dans $N \rtimes_\varphi H$, on a alors $N \cap H = \{1\}$ et $NH = G$, et réciproquement si deux sous-groupes d'un groupe G vérifient ces propriétés avec $N \lhd G$, alors $G \simeq N \rtimes H$ pour l'opération $h.n = hnh^{-1}$. On vérifiera aussi que H n'est distingué dans $N \rtimes_\varphi H$ que si l'opération de H sur N est triviale.

Proposition 3.7 *Soit*

$$1 \to N \to G \to H \to 1$$

une suite exacte admettant une section $s : H \to G$. Alors $G \simeq N \rtimes H$ pour l'opération $h.n = s(h)ns(h)^{-1}$.

Démonstration : Posons $H_1 = s(H)$. Comme s est injective vu que $p \circ s = \mathrm{id}_H$, H_1 est un sous-groupe de G isomorphe à H et il suffit de montrer : $N \cap H_1 = \{1\}$ et $NH_1 = G$ (on a identifié N à son image dans G). Si $h_1 \in N \cap H_1$, alors $p(h_1) = 1$ mais $h_1 = s(h)$ avec $h \in H$, d'où $1 = p(s(h)) = h$ et $h_1 = 1$. Si maintenant $g \in G$, alors g et $s(p(g))$ ont même image par p, donc ils diffèrent d'un élément du noyau N, i.e. $g = nh_1$ avec $h_1 := s(p(g))$, et $g \in NH_1$.

□

C'est en général ce critère qui est le plus utile pour obtenir des décompositions en produit semi-direct, mais on gardera bien à l'esprit la façon de déterminer l'opération de H sur N associée en fonction de la suite exacte et de la section.

Exemple 3.8 a) Pour $n \geq 2$, la suite exacte

$$1 \to \mathcal{A}_n \to \mathcal{S}_n \xrightarrow{\varepsilon} \mathbf{Z}/2\mathbf{Z} \to 1$$

est scindée via la section s qui envoie $\bar{0}$ sur Id et $\bar{1}$ sur une transposition (arbitraire) τ. On en déduit une décomposition $\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \mathbf{Z}/2\mathbf{Z}$.

b) Soient K un corps et $n \in \mathbf{N}^*$. La suite exacte

$$1 \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \stackrel{\det}{\to} K^* \to 1$$

est scindée (envoyer $\lambda \in K^*$ sur la matrice $\mathrm{Diag}(\lambda, 1, ..., 1)$). Ainsi $\mathrm{GL}_n(K) \simeq \mathrm{SL}_n(K) \rtimes K^*$.

c) Le groupe $\mathbf{Z}/4\mathbf{Z}$ n'est *pas* produit semi-direct de $\mathbf{Z}/2\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$. En effet, ce serait alors un produit direct vu que $\mathbf{Z}/4\mathbf{Z}$ est abélien. Or $\mathbf{Z}/4\mathbf{Z}$ n'est pas isomorphe au produit direct $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (le premier groupe a des éléments d'ordre 4 et pas le deuxième). En particulier la suite exacte (1) de l'exemple 3.3 n'est pas scindée. [4]

d) On peut définir le groupe *groupe diédral* D_n comme $D_n \simeq \mathbf{Z}/n\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$ pour l'opération de $\mathbf{Z}/2\mathbf{Z}$ sur $\mathbf{Z}/n\mathbf{Z}$ donnée par $\varepsilon.x = -x$, où ε est l'élément non trivial de $\mathbf{Z}/2\mathbf{Z}$.

4. On voit donc que même dans des cas très élémentaires, on ne peut pas toujours "reconstituer" un groupe à partir de ses sous-groupes. En particulier, la connaissance des groupes finis simples ne suffit absolument pas à connaître tous les groupes finis, contrairement à une croyance populaire assez répandue (notamment chez les agrégatifs !).