AIX-MARSEILLE UNIVERSITÉ

Algèbre 2

Le groupe $\mathbb{Z}_n^\times$

L'exposant d'un groupe. Ordre d'un produit : Soit G un groupe, et $a \in G$. Si a est d'ordre infini, alors toutes les puissances de a sont aussi d'ordre infini. Si a est d'ordre fini, nous avons la formule suivante pour l'ordre des puissances de a :

$$\mathrm{ord}(a^k) = \mathrm{ord}(a)/\mathrm{pgcd}(\mathrm{ord}(a), k)$$

pour chaque entier k. En particulier, les entiers k tels que $a^k = e$ sont les multiples de l'ordre de a (ce qui caractérise l'ordre de a), et l'inverse de a est de même ordre que a.

Il n'y a pas de formule générale reliant l'ordre d'un produit ab aux ordres de a et b. En fait, il est possible que a et b soient tous deux d'ordre finis tandis que ab est d'ordre infini, ou que a et b soit tous deux d'ordre infini tandis que ab est d'ordre fini.

Si $ab = ba$, on peut au moins affirmer que l'ordre de ab divise le $\mathrm{ppcm}(a, b)$, et que, si $\mathrm{ord}(a)$ et $\mathrm{ord}(b)$ sont premiers entre eux, il est même égal au produit $\mathrm{ord}(a)\mathrm{ord}(b)$.

Ceci permet de construire, pour deux éléments a et b vérifiant $ab = ba$, un élément dont l'ordre est le ppcm des ordres de a et b (le produit de deux élévations à une puissance idoine de a et de b), et donc de prouver que l'ensemble des ordres des éléments d'un groupe abélien est stable par ppcm. Une conséquence est que

Proposition 1 *Si l'exposant d'un groupe abélien est fini alors il est égal à l'ordre de l'un des éléments du groupe.*

Dans cette définition on a utilisé la définition :

Définition 2 *Soit G un groupe, d'élément neutre noté e. On appelle exposant de G le plus petit entier strictement positif n, s'il existe, tel que $\forall g \in G,\ g^n = e$. S'il n'en existe pas, on dit que G est d'exposant infini.*

Cette définition équivaut à : l'exposant de G est le plus petit commun multiple des ordres des éléments du groupe si tous ces ordres sont finis et admettent un majorant commun, et l'infini sinon.

Une condition nécessaire (mais pas suffisante) pour que l'exposant d'un groupe soit fini est donc que ce groupe soit de torsion.

Remarque 3 *Soit toujours G un groupe, d'élément neutre noté e. Les entiers relatifs n tels que $x^n = e$ pour tout élément x de G forment un sous-groupe de $(\mathbb{Z}, +)$, qui, comme tout sous-groupe de $(\mathbb{Z}, +)$, admet un unique générateur naturel (éventuellement nul). Si ce générateur est non nul, il est égal à l'exposant de G tel que défini ci-dessus. Si le générateur est nul, l'exposant de G tel que défini ci-dessus est égal à l'infini. Certains auteurs définissent l'exposant de G comme le générateur naturel en question. Cette définition ne diffère de la précédente que dans le cas où l'exposant au premier sens est infini ; dans ce cas, l'exposant au second sens est nul. Avec la seconde définition, la caractéristique d'un corps est l'exposant de son groupe additif.*

Propriétés

1. L'exposant d'un groupe fini est nécessairement fini : c'est même un diviseur de l'ordre du groupe. En effet, dans un groupe fini, l'ordre de chaque élément divise l'ordre du groupe d'après le théorème de Lagrange.
2. Tout groupe abélien d'exposant fini contient au moins un élément dont l'ordre est égal à l'exposant du groupe. En effet, dans un groupe abélien, l'ensemble des ordres des éléments est stable par ppcm, donc si cet ensemble possède un maximum, cet ordre est multiple de tous les autres.

Le groupe $\mathbb{Z}_n^\times$. Dans le cas où n est premier c'est-à-dire si l'anneau est un corps, la structure est la suivante :

Proposition 4 *Si p est un nombre premier, le groupe des unités (des éléments inversibles) $\mathbb{Z}_p^\times$ du corps $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ est un groupe cyclique d'ordre $p - 1$.*

Démonstration: Dans $\mathbb{Z}_p$ (pour p premier), tout élément non nul est inversible. L'ordre du groupe multiplicatif est donc $p - 1$. Ce groupe admet donc un exposant e, qui est un diviseur de $p - 1$ (cf. le paragraphe précédent). Considérons le polynôme $X^e - 1$ de $\mathbb{Z}_p[X]$. Il admet pour racines tous les éléments du groupe multiplicatif $\mathbb{Z}_p^\times = \mathbb{Z}_p^*$, donc $p - 1$ racines différentes. Or tout polynôme à coefficients dans un corps commutatif possède un degré supérieur ou égal à son nombre de racines. On en déduit que e est supérieur ou égal à $p - 1$, si bien que finalement $e = p - 1$.

Pour conclure il suffit d'utiliser le fait que tout groupe abélien fini possède un élément d'ordre l'exposant (cf. le paragraphe précédent). Le groupe multiplicatif possède un élément d'ordre l'ordre du groupe. Cet élément est donc générateur, ce qui montre que le groupe est cyclique. ■

Remarque 5 *Un raisonnement identique montre que le groupe multiplicatif de tout corps fini est aussi cyclique.*

Cas où n n'est pas premier : Étudions d'abord le cas où n est de la forme p^r, pour un nombre premier p et un entier $r \geq 2$ (le cas $r = 1$ vient d'être étudié). Deux configurations se présentent :

Proposition 6 *Si $p = 2$ (et $r \geq 2$), le groupe $\mathbb{Z}_{p^r}^\times$ est le produit direct interne du sous-groupe d'ordre 2 engendré par la classe de -1 et du sous-groupe d'ordre 2^{r-2} engendré par la classe de 5. Si $p \neq 2$, le groupe $\mathbb{Z}_{p^r}^\times$ est cyclique.*

A remarquer que pour $r = 2$ le sous-groupe $\langle [5]_{2^r} \rangle$ est trivial, donc dans ce cas $\mathbb{Z}_{p^r}^\times = \mathbb{Z}_4^\times$ sera cyclique engendré par la classe $[-1]_4 = [3]_4$.

Démonstration: Démonstration Si $p = 2$ et $r \geq 2$, le groupe des unités est le produit direct interne du sous-groupe d'ordre 2 engendré par la classe de -1 et du sous-groupe d'ordre 2^{r-2} engendré par la classe de 5.

La classe de 5 est un élément d'ordre 2^{r-2}. En effet $\mathrm{ord}([5]_{2^r})$ est un diviseur de 2^r, donc est de la forme 2^s où $s \in \{0, \ldots, r\}$ est minimal tel que $[5]^{2^s} = [1]$. L'égalité $s = r - 2$ résulte de l'égalité suivante, que l'on démontre par récurrence sur k :

$$\forall k \in \mathbb{N} \quad \exists \lambda \in \mathbb{N} \quad 5^{2^k} = 1 + 2^{k+2}\lambda \quad \text{avec} \quad \lambda \quad \text{impair}.$$

Pour $k = 0$, l'égalité est vraie avec $\lambda = 1$. Supposons le résultat vrai pour k et montrons-le pour $k + 1$

$$5^{2^{k+1}} = \left(5^{2^k}\right)^2 = \left(1 + 2^{k+2}\lambda\right)^2 = 1 + 2^{k+3}(\lambda + 2^{k+1}\lambda^2).$$

Nous affirmons que $\mathbb{Z}_{2^r}^\times$ est le produit direct interne des deux sous-groupes engendrés par $[5]_{2^r}$ et $[-1]_{2^r}$. En effet, modulo 4, toutes les puissances de 5 sont congrues à 1 donc pas à -1. A fortiori, modulo 2^r pour $r \geq 2$, la classe de -1 n'est pas une puissance de celle de 5. L'intersection des sous-groupes $\langle [-1]_{2^r} \rangle$, $\langle [5]_{2^r} \rangle$ engendrés par ces deux classes est donc réduite au singleton $\{[1]_{2^r}\}$. Le produit de leurs ordres est égal à $2^{r-1} = \varphi(2^r)$, qui est l'ordre du groupe. Ce groupe est donc leur produit direct interne.

Si $p \neq 2$, le groupe des unités est cyclique. La démonstration est en partie analogue à la précédente. Nous affirmons que la classe $[1 + p] \in \mathbb{Z}/p^r\mathbb{Z}$ est un élément d'ordre p^{r-1}. En effet $\mathrm{ord}([1 + p])$ est un diviseur de p^r, donc est de la forme p^s où $s \in \{0, \ldots, r\}$ est minimal tel que $[1+p]^{p^s} = [1]$. L'égalité $s = r-1$ résulte de la formule suivante, que l'on démontre par récurrence sur k :

$$\forall k \in \mathbb{N} \quad \exists \lambda \in \mathbb{N} \quad (1+p)^{p^k} = 1 + p^{k+1}\lambda \quad \text{avec} \quad \lambda \equiv 1 \bmod p. \tag{1}$$

Cette égalité montre que $(1+p)^{p^k} \equiv 1+p^{k+1} \bmod p^{k+2}$, en particulier $(1+p)^{p^{r-2}} \equiv 1+p^{r-1} \bmod p^r$, et $(1+p)^{p^{r-1}} \equiv 1+p^r \bmod p^{r+1}$. La 1ère congruence montre que $[1+p]^{p^{r-2}} \neq [1]$, et la 2ème congruence montre que $[1+p]^{p^{r-1}} = [1]$ dans $\mathbb{Z}/p^r\mathbb{Z}$.

Pour $k = 0$, l'égalité (1) est vraie avec $\lambda = 1$. Supposons la propriété vraie à l'ordre k et montrons-la à l'ordre $k + 1$. La formule du binôme de Newton montre qu'il existe un entier m tel que

$$(1+p)^{p^{k+1}} = \left((1+p)^{p^k}\right)^p = \left(1 + p^{k+1}\lambda\right)^p = 1 + p^{k+2}(\lambda + pm).$$

Maintenant on va montrer que le groupe des unités contient un élément d'ordre $p - 1$:

Le groupe $\mathbb{Z}_p^\times$ est cyclique d'ordre $p - 1$. Il existe donc un entier dont l'ordre multiplicatif modulo p est égal à $p - 1$. Sa classe a modulo p^r est alors un élément de $\mathbb{Z}_{p^r}^\times$ d'ordre multiple de $p-1$, donc a possède une puissance b d'ordre $p-1$.

Le groupe des unités est cyclique : Comme les éléments b et $[p + 1]$ commutent et sont d'ordres premiers entre eux, l'ordre du produit $c = b[p + 1]$ est égal aux produit des ordres, $(p-1)p^{r-1} = \varphi(p^r)$, qui est l'ordre du groupe. Ce groupe est donc engendré par c. ■

Pour p premier et r entier naturel, le groupe des unités de $\mathbb{Z}_{p^r}$ est donc toujours cyclique, sauf si $p = 2$ et $r \geq 3$.

Le cas général se ramène aux précédents grâce au théorème fondamental de l'arithmétique. En effet, d'après le théorème des restes chinois :

Proposition 7 *Soient n et m deux entiers premiers entre eux non nuls. Le groupe des unités de $\mathbb{Z}_{nm}$ est isomorphe au produit direct des groupes des unités de $\mathbb{Z}_n$ et de $\mathbb{Z}_m$. En particulier, $\mathbb{Z}_n^\times$ est cyclique si et seulement si $n = 4$, ou une puissance d'un premier impair, ou le double d'une telle puissance.*