

Structures algébriques

ENTRAÎNEMENT 19

♣ **Exercice 1** — Soient G un groupe et $x, y \in G$. On suppose que xy est d'ordre fini n dans G . Prouver que yx est également d'ordre fini n .

Correction — D'après l'énoncé, $xyxy \cdots xy = e$, c'est-à-dire $x(yx)^{n-1}y = e$. De ce fait, $yx(yx)^{n-1}y = y$, soit $(yx)^n = e$. De plus, si l'ordre de yx était strictement inférieur à n , on aurait $x(yx)^{n-1}y = xy = e$. D'où le résultat.

♣ **Exercice 2** — *Théorème de Fermat*
Soient p un entier premier.

1. Soit $k \in \llbracket 1, p-1 \rrbracket$. Montrer que p divise $\binom{p}{k}$.
2. En déduire que pour tous $x, y \in \mathbb{Z}$,

$$(x + y)^p \equiv x^p + y^p \pmod{p}$$
3. En déduire que pour tout $a \in \mathbb{N}$, $a^p \equiv a \pmod{p}$.
Que dire dans le cas où p ne divise pas a ?

Correction —

1. Soit $k \in \llbracket 1, p-1 \rrbracket$. $k \binom{p}{k} = p \binom{p-1}{k-1}$. p étant premier et $k < p$, $p \wedge k = 1$ donc d'après le lemme de Gauss, $p \mid \binom{p}{k}$.
2. Pour tous $x, y \in \mathbb{Z}$, d'après la formule du binôme et la question précédente,

$$(x + y)^p = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} \equiv x^p + y^p \pmod{p}$$
3. Il s'agit d'une simple récurrence sur l'entier a , l'hérédité se justifiant par le fait que $(a + 1)^p \equiv a^p + 1^p \equiv a + 1 \pmod{p}$. Lorsque $p \nmid a$, on retrouve l'identité $a^{p-1} \equiv 1 \pmod{p}$.

♣ **Exercice 3** — Soit p un nombre premier.

1. Déterminer les carrés de $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/11\mathbb{Z}$.
2. Déterminer le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$.

Indication — On pourra résoudre $x^2 = a^2$ dans $\mathbb{Z}/p\mathbb{Z}$.

Correction —

1. Les carrés se lisent dans les tableaux suivants :

$$p = 7 \quad \begin{array}{c|c|c|c|c|c|c|c} \bar{k} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \hline \bar{k}^2 & \bar{0} & \bar{1} & \bar{4} & \bar{2} & \bar{2} & \bar{4} & \bar{1} \end{array}$$

$$p = 11 \quad \begin{array}{c|c|c|c|c|c|c|c|c|c|c} \bar{k} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} & \bar{7} & \bar{8} & \bar{9} & \bar{10} \\ \hline \bar{k}^2 & \bar{0} & \bar{1} & \bar{4} & \bar{9} & \bar{5} & \bar{3} & \bar{3} & \bar{5} & \bar{9} & \bar{4} & \bar{1} \end{array}$$

2. Mettons de côté le cas où $p = 2$, $\mathbb{Z}/2\mathbb{Z}$ admettant deux carrés. Soit p premier impair. Il semblerait, par symétrie des tableaux précédents, qu'il y ait $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$. Chaque élément donne en fait naissance à un carré mais il y a des doublons... que nous allons éliminer ! Notons que :

$$\bar{x}^2 = \bar{a}^2 \iff (\bar{x} - \bar{a})(\bar{x} + \bar{a}) = \bar{0}$$

$\mathbb{Z}/p\mathbb{Z}$ étant un anneau intègre, $\bar{x}^2 = \bar{a}^2$ ssi $\bar{x} = \pm \bar{a}$. Chaque carré, à l'exception de 0, possède donc exactement 2 antécédents par l'application $\bar{x} \mapsto \bar{x}^2$. Il y a $\frac{p-1}{2}$ carrés non nuls, soit un total de $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.

♣♣ **Exercice 4** — *Équation du second degré dans \mathbb{F}_p*

Soit p un entier premier impair. Montrer que l'équation $x^2 + ax + b = 0$ admet des racines dans $\mathbb{Z}/p\mathbb{Z}$ ssi $a^2 - 4b$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Indications — On pensera à revenir à la forme canonique. Quel est l'inverse de -2 dans $\mathbb{Z}/p\mathbb{Z}$?

Correction — Notons que $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est ici un corps. Pour $x, a, b \in \mathbb{R}$, on écrirait :

$$x^2 + ax + b = \left(x + \frac{a}{2}\right)^2 - \frac{a^2 - 4b}{4} = 0 \quad (*)$$

$\bar{-2}$ étant d'inverse $\bar{\frac{p-1}{2}}$, l'équation (*) se réécrit dans $\mathbb{Z}/p\mathbb{Z}$, en allégeant les notations,

$$\left(x - a \cdot \frac{p-1}{2}\right)^2 = (a^2 - 4b) \cdot \left(\frac{p-1}{2}\right)^2$$

L'équation admet donc des racines dans $\mathbb{Z}/p\mathbb{Z}$ ssi $a^2 - 4b$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

♣♣♣ **Exercice 5** — *Produit de deux groupes cycliques*

Soient G_1 et G_2 deux groupes cycliques d'ordres respectifs n_1 et n_2 .

1. Montrer que si $x \in G_1$ est d'ordre p et $y \in G_2$ est d'ordre q , alors (x, y) est d'ordre $p \vee q$ dans $G_1 \times G_2$.
2. À quelle condition nécessaire et suffisante sur n_1 et n_2 , le groupe produit $G_1 \times G_2$ est-il cyclique ?

Correction —

- Pour tout $k \in \mathbb{Z}$,

$$(x, y)^k = (x^k, y^k) = (e_1, e_2) \iff \begin{cases} p \mid k \text{ et } q \mid k \\ p \vee q \mid k \end{cases}$$

Ainsi, (x, y) est d'ordre $p \vee q$.

- Montrons que $G_1 \times G_2$ est cyclique ssi $n_1 \wedge n_2 = 1$.

\implies Supposons $G_1 \times G_2$ cyclique. Si (x, y) engendre $G_1 \times G_2$, $G_1 = \langle x \rangle$ et $G_2 = \langle y \rangle$. (x, y) est d'ordre $\text{card}(G_1 \times G_2) = n_1 n_2$ mais aussi, d'après ce qui précède, d'ordre $n_1 \vee n_2$. Ainsi, $n_1 \wedge n_2 = 1$.

◀ Supposons que $n_1 \wedge n_2 = 1$. Soient $(x, y) \in G_1 \times G_2$ tels que $G_1 = \langle x \rangle$ et $G_2 = \langle y \rangle$. D'après ce qui précède, (x, y) est d'ordre $n_1 \vee n_2 = n_1 n_2$ dans $G_1 \times G_2$. Par égalité des cardinaux, $G_1 \times G_2 = \langle (x, y) \rangle$.

♣♣ **Exercice 6** — *Radical (ou racine) d'un idéal*
Soit I un idéal d'un anneau commutatif A . On appelle radical de I l'ensemble :

$$\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N}, x^n \in I\}$$

1. Montrer que \sqrt{I} est un idéal de A contenant I .
2. Soient I et J deux idéaux de A .
 - (a) Montrer que si $I \subset J$, alors $\sqrt{I} \subset \sqrt{J}$.
 - (b) Montrer que $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
3. Trouver le radical des idéaux de \mathbb{Z} .

Indications — 1. Ne pas oublier de montrer que $(\sqrt{I}, +)$ est un sous-groupe. 3. On prouvera que pour tout $n \geq 2$, $\sqrt{n\mathbb{Z}} = p_1 \cdots p_r \mathbb{Z}$, où les p_i sont les facteurs premiers de n .

Correction —

1. Il est clair que $I \subset \sqrt{I}$. Il s'agit ensuite de montrer que \sqrt{I} est absorbant pour la loi \times puis que $(\sqrt{I}, +)$ est un sous-groupe.

- Soit $x \in \sqrt{I}$ tel que $x^n \in I$. Alors par commutativité, pour tout $y \in A$, $(xy)^n = y^n x^n$. $x^n \in I$ et I est un idéal donc $xy = xy \in \sqrt{I}$.
- Soient $x, y \in \sqrt{I}$ et $p, q \in \mathbb{N}$ tels que $x^p \in I$ et $y^q \in I$. Par commutativité,

$$(x + y)^{p+q+1} = \sum_{k=0}^{p+q+1} \binom{p+q+1}{k} x^k y^{p+q+1-k}$$

Pour tout $k \geq p$, $x^k \in I$ donc $\binom{p+q+1}{k} x^k y^{p+q+1-k} \in I$. De même, pour tout $k < p$, $p + q + 1 - k \geq q$, donc $y^{p+q+1-k} \in I$ et $\binom{p+q+1}{k} x^k y^{p+q+1-k} \in I$. $(I, +)$ étant un sous-groupe, $(x + y)^{p+q+1} \in I$ et de ce fait, $x + y \in \sqrt{I}$.

2. Soient I et J deux idéaux de A .
 - (a) Soient $x \in \sqrt{I}$. Il existe $n \in \mathbb{N}$ tel que $x^n \in I \subset J$. De façon immédiate, $x \in \sqrt{J}$.
 - (b) Montrons que $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

\subset Soient $x \in \sqrt{I \cap J}$ et $n \in \mathbb{N}$ tel que $x^n \in I \cap J$. Très clairement, $x \in \sqrt{I} \cap \sqrt{J}$.

\supset Soient $x \in \sqrt{I} \cap \sqrt{J}$ et $p, q \in \mathbb{N}$ tels que $x^p \in I$ et $x^q \in J$. $x^{\max(p,q)} \in I \cap J$ donc $x \in \sqrt{I \cap J}$.

3. Les idéaux de \mathbb{Z} sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.
 - Si $n \in \{0, 1\}$, $\sqrt{n\mathbb{Z}} = n\mathbb{Z}$.
 - Supposons maintenant que $n = 2$ et écrivons la décomposition première de n sous la forme $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et montrons que $\sqrt{n\mathbb{Z}} = p_1 \cdots p_r \mathbb{Z}$. Soient $x \in \sqrt{n\mathbb{Z}}$ et $k \in \mathbb{N}$ tel que $x^k \in n\mathbb{Z}$. Il est clair que p_1, \dots, p_n divisent x^k donc divisent x par primalité (lemme de Gauss). Ainsi, $x \in p_1 \cdots p_r \mathbb{Z}$. Réciproquement, en considérant $\alpha = \max(\alpha_1, \dots, \alpha_r)$, $n \mid x^\alpha$ donc $x^\alpha \in n\mathbb{Z}$ et alors, $x \in \sqrt{I}$. D'où $\sqrt{n\mathbb{Z}} = p_1 \cdots p_r \mathbb{Z}$.

♣♣♣ **Exercice 7** — *Cyclicité de \mathbb{F}_p^**
Soit p un entier premier impair.

1. Soit G un groupe abélien cyclique. Montrer que si $x, y \in G$ sont d'ordres respectifs p et q , alors il existe un élément de G d'ordre $p \vee q$.
2. Montrer que $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est un groupe cyclique.

Indication — 1. On pourra dans un premier temps prouver la propriété lorsque $p \wedge q = 1$. 2. Montrer que le ppcm de tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ est $p - 1$.

Correction —

1. (i) Supposons $p \wedge q = 1$. Si $(xy)^k = e$, alors $(xy)^{pk} = y^{pk} = e$ et $(xy)^{qk} = x^{qk} = e$ donc $p \mid qk$ et $q \mid pk$. D'après le lemme de Gauss, $pq = p \vee q \mid k$. Donc xy est d'ordre $p \vee q$.
 - (ii) Pour tout diviseur d de p , on montre facilement que $x^{p/d}$ est d'ordre d . Il en va de même pour un diviseur de q .
 - (iii) Écrivons les décompositions premières de p et q sous la forme $p = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et $q = p_1^{\beta_1} \cdots p_r^{\beta_r}$. Alors, $p \vee q = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ où $\gamma_i = \max(\alpha_i, \beta_i)$. $p_i^{\gamma_i}$ divisant soit p , soit q , le point (ii) prouve qu'il existe un élément g_i de G d'ordre $p_i^{\gamma_i}$. Les $p_i^{\gamma_i}$ étant deux à deux premiers entre eux, le point (i) permet de prouver par récurrence que $g_1 \cdots g_r$ est un élément de G d'ordre $p \vee q$.
2. Revenons maintenant au groupe (abélien) $G = (\mathbb{Z}/p\mathbb{Z})^*$.
 - D'après le cours, l'ordre de chacun de ses éléments divise $\text{card}((\mathbb{Z}/p\mathbb{Z})^*) = p - 1$. Le ppcm de tous ces ordres, notons-le d , divise donc $p - 1$.
 - En outre, chaque élément \bar{k} de $(\mathbb{Z}/p\mathbb{Z})^*$ vérifie $\bar{k}^{-d} = \bar{1}$ donc est racine du polynôme $X^d - 1$. Mais ce polynôme admet dans le corps $\mathbb{Z}/p\mathbb{Z}$ au plus d racines distinctes. De ce fait, $d = p - 1$.
 - D'après le résultat de la question précédente, il existe nécessairement $\bar{k} \in \mathbb{Z}/p\mathbb{Z}$ d'ordre $p - 1$. Pour des raisons de cardinalité, $(\mathbb{Z}/p\mathbb{Z})^* = \langle \bar{k} \rangle$.