TD2 : Groupes abéliens finis

Exercice 1.

Montrer que les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ et $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ sont isomorphes.

Solution
On utilise le lemme chinois pour voir que les deux groupes sont isomorphes au groupe

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times /Z/9\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z})\,.$$

Cette écriture est la décomposition en composantes p-primaire. On peut aussi écrire la décomposition en facteurs invariants de ces deux groupes, et l'on trouve :

$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/900\mathbb{Z}\,.$$

Exercice 2.

Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Solution
Le théorème du cours assure qu'un tel groupe G est isomorphe à un produit $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$, avec $d_i \geq 2$ et $d_i | d_{i+1}$. Comme G n'est pas cyclique, on a $r \geq 2$. Il existe un facteur premier p de d_1, alors p divise tous les d_i, et $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à un sous-groupe de chacun des $\mathbb{Z}/d_i\mathbb{Z}$ (c'est le sous-groupe de p-torsion). Alors le sous-groupe de p-torsion de G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^r$, qui contient clairement un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 3.

1. Combien y a-t-il de groupes abéliens de cardinal 360 ? Faire la liste complète de ces groupes.
2. Plus généralement, pour tout entier n, combien y a-t-il de groupes abéliens de cardinal n ?

Solution

1. On écrit la décomposition en facteurs premiers de $360 = 2^3.3^2.5$. Alors si G est un groupe de cardinal 360, $T_2(G)$ est un groupe abélien de cardinal 2^3, il y a donc 3 classes d'isomorphisme de tels groupes, à savoir $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^3$. De même, il y a exactement deux classes d'isomorphisme possibles pour $T_3(G)$, à savoir $\mathbb{Z}/9\mathbb{Z}$ et $(\mathbb{Z}/3\mathbb{Z})^2$, et $T_5(G)$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Par conséquent, il y a exactement $3.2 = 6$ classes d'isomorphisme de groupes abéliens d'ordre 360, dont les décompositions p-primaires et en facteurs invariants sont les suivantes :

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/360\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$$

$$\mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}\,.$$

2. On utilise la classification des classes d'isomorphisme de groupes abéliens finis. Notons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers. Alors on sait que la classe d'isomorphisme d'un groupe abélien d'ordre n est caractérisée par ses facteurs invariants $(d_1, \dots, d_s)$ qui sont des entiers > 1 tels que $d_i | d_{i+1}$ et $d_1 \dots d_s = n$. Par conséquent, chaque d_i se décompose $d_i = p_1^{\alpha_{i,1}} \dots p_1^{\alpha_{i,r}}$, avec les contraintes suivantes : pour tout j, $\alpha_{i,j} \leq \alpha_{i+1,j}$ (pour tout i) et $\sum_{i=1}^{s} \alpha_{i,j} = \alpha_j$. Par conséquent, le nombre de choix possibles pour les a_i est exactement $\prod_{j=1}^{r} p(\alpha_j)$, où $p(\alpha)$ désigne le nombre de partitions de α, i.e. le nombre de façons d'écrire l'entier α comme une somme croissante d'entiers strictement positifs.

Exercice 4.

1. Le nombre de classes de conjugaison dans $\mathfrak{S}_5$ est le même que le nombre de groupes abéliens de cardinal 32 à isomorphisme près. Pourquoi ?
2. Généraliser au nombre de classes de conjugaison dans $\mathfrak{S}_n$.

Solution

1. Les deux ensembles en question sont naturellement en bijection avec l'ensemble des partitions de 5.
2. Soit p un nombre premier. Notons G_n l'ensemble des classes d'isomorphisme de groupes abéliens de cardinal p^n, P_n l'ensemble des partitions de l'entier n et C_n l'ensemble des classes de conjugaison dans $\mathfrak{S}_n$. On dispose des applications suivantes
$$\varphi : P_n \to G_n$$
et
$$\psi : P_n \to C_n$$
où pour toute partition $(n_1, \dots, n_r)$ de n, $\varphi((n_1, \dots, n_r))$ est la classe d'isomorphisme de $\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ et $\psi((n_1, \dots, n_r))$ est la classe de conjugaison de la permutation $(1, 2, \dots, n_1)(n_1+1, \dots, n_1+n_2)\dots(n_1+\dots+n_{r-1}+1, \dots, n)$. On voit alors facilement que φ et ψ sont des bijections, donc $|C_n| = |G_n|$, i.e. il y a autant de classes de conjugaison dans $\mathfrak{S}_n$ que de classes d'isomorphisme de groupes abéliens d'ordre p^n.

Exercice 5.

Soit G un groupe abélien fini. Montrer qu'il existe dans G un élément d'ordre égal à l'*exposant de G* (c'est-à-dire au ppcm des ordres des éléments de G).

Solution

— On commence par une preuve "élémentaire" : montrons d'abord que pour tous $x, y \in G$ d'ordres respectifs m et n premiers entre eux, le produit xy est d'ordre $m.n$. Il est clair que $(xy)^{mn} = 1$ donc l'ordre de xy divise mn. Soit maintenant $k \geq 1$ tel que $(xy)^k = 1$. En élevant à la puissance n, on obtient $x^{kn} = 1$, donc m divise kn. Or m et n sont premiers entre eux, donc m divise k. Par symétrie, on a aussi que n divise k, donc mn divise k, donc xy est d'ordre mn.
On décompose l'exposant de G en facteurs premiers : $\exp(G) = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, avec les p_i premiers distincts. Par définition de l'exposant de G, pour tout $1 \leq i \leq r$, il existe $g_i \in G$ dont l'ordre est divisible par $p_i^{\alpha_i}$, disons égal à $p_i^{\alpha_i}.m_i$. Alors $g_i^{m_i}$ est d'ordre $p_i^{\alpha_i}$, et on a vu qu'alors l'élément $g := g_1^{m_1} \dots g_r^{m_r} \in G$ est d'ordre exactement $p_1^{\alpha_1} \dots p_r^{\alpha_r} = \exp(G)$.
— Une preuve moins élémentaire : le théorème de classification des groupes abéliens finis assure qu'il existe des entiers $2 \leq d_1 | \dots | d_s$ tels que G soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$. Il est alors clair que $\exp(G) = d_r$ et que l'élément $(0, \dots, 0, 1) \in \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$ est d'ordre d_r.

Exercice 6.

Soit G un groupe et soient H et K des sous-groupes de G. On suppose que :

1. $H \triangleleft G$ et $K \triangleleft G$;
2. $HK = G$;
3. $H \cap K = e$.

Montrer que G est isomorphe à $H \times K$.

Solution
Montrons d'abord que H et K commutent. Soient $h \in H$ et $k \in K$. Comme H est distingué dans G, on a $kh^{-1}k^{-1} \in H$, donc $hkh^{-1}k^{-1} \in H$. De même, K est distingué dans G, donc $hkh^{-1} \in K$, donc $hkh^{-1}k^{-1} \in K$. Donc $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, donc $hk = kh$.
Montrons maintenant que pour tout $g \in G$, il existe un unique couple $(h, k) \in H \times K$ tel que $g = hk$. L'existence est assurée par l'hypothèse b). Pour l'unicité, soient $h, h' \in H$ et $k, k' \in K$ tels que $hk = h'k'$. Alors $kk'^{-1} = h^{-1}h'$ est dans $H \cap K$, donc l'hypothèse c) assure que $kk'^{-1} = h^{-1}h' = e$, donc $h = h'$ et $k = k'$, d'où l'unicité.
On considère alors l'application $\varphi : H \times K \to G$ définie par $\varphi(h, k) := hk$. Le fait que H et K commutent assure que φ est un morphisme de groupes. L'existence et l'unicité prouvée plus haut assurent que φ est une bijection. Donc G est bien isomorphe au groupe $H \times K$.

Exercice 7.

Soit K un corps et soit $G \subset K^*$ un sous-groupe fini d'ordre n. On va montrer que G est un groupe cyclique.

1. Montrer que l'ordre de tout élément de G divise n.

2. Soit d un diviseur de n et $x \in G$ d'ordre d. Soit H le sous-groupe cyclique de G engendré par x. Montrer que tout élément d'ordre d est dans H.
3. On note $N(d)$ le nombre d'éléments de G d'ordre d. Montrer que $N(d) = 0$ ou $\varphi(d)$, et que $\sum_{d|n,\ d>0} N(d) = n$.
4. Conclure.

En particulier, si p est un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, et si K est un corps fini, K^* est un groupe cyclique.

Solution

1. C'est le théorème de Lagrange.
2. Considérons le polynôme $P = X^d - 1 \in K[X]$. Comme K est un corps, le polynôme P a au plus d racines dans K. Or tout élément du groupe H est d'ordre divisant d, donc tous les éléments de H sont des racines de P. Or le cardinal de H est égal à l'ordre de x, c'est-à-dire à d. Donc H contient toutes les racines de P dans K.

   Soit maintenant $y \in G$ d'ordre d. Alors y est racine de P, donc y est dans H.
3. Supposons $N(d) \neq 0$. Alors il existe $x \in G$ d'ordre d. La question b) assure que tout les éléments d'ordre d dans G sont exactement les éléments d'ordre d dans $\langle x \rangle$ qui est un groupe cyclique d'ordre d. Or un groupe cyclique d'ordre d a exactement $\varphi(d)$ éléments d'ordre d, donc $N(d) = \varphi(d)$.

   En outre, on peut partitionner G selon l'ordre des éléments, i.e. G est la réunion disjointe, pour d divisant n (par la question a)), des ensembles G_d formés des éléments d'ordre d. En calculant les cardinaux, on trouve donc $|G| = \sum_{d|n} |G_g|$, i.e. $n = \sum_{d|n} N(d)$.
4. La question c) assure que $n = \sum_{d|n} N(d)$. Or on sait que $n = \sum_{d|n} \varphi(d)$. Donc $\sum_{d|n} N(d) = \sum_{d|n} \varphi(d)$. Or pour tout $d|n$, $N(d) \leq \varphi(d)$, donc on a bien pour tout $d|n$, $N(d) = \varphi(d)$. En particulier, $N(n) = \varphi(n) > 0$, donc il existe un élément d'ordre n dans G, i.e. G est cyclique.

Exercice 8.

Si A est un anneau, on note $A^\times$ le groupe (multiplicatif) des éléments inversibles de A.

1. Soit G un groupe monogène. Montrer que le groupe des automorphismes de G est en bijection avec l'ensemble des générateurs de G.
2. Montrer que pour tout $n \in \mathbb{N}$, on a un isomorphisme de groupes $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
3. Soit p un nombre premier impair et soit $\alpha \geq 1$. Quel est l'ordre de $1+p$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$? En déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.
4. Expliciter $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ pour $\alpha \geq 1$.
5. En déduire $(\mathbb{Z}/n\mathbb{Z})^\times$ pour $n \in \mathbb{N}$.

Solution

1. Soit G_0 l'ensemble des générateurs de G et soit g_0 un élément de G_0. Alors si φ est un automorphisme de G, l'image de φ est engendrée par $\varphi(g_0)$; ce qui veut dire que $\varphi(g_0)$ est un générateur de G. On définit alors une application $\varphi \mapsto \varphi(g_0)$ de $\mathrm{Aut}(G)$ vers G_0. Comme g_0 est générateur, l'application est bijective.
2. Dans $\mathbb{Z}$, montrons par récurrence sur $k \geq 1$ qu'il existe λ_k premier à p vérifiant $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$. L'étape d'initialisation pour $k = 1$ est claire via la formule du binôme, puisque p divise $\binom{p}{2}$. Montrons l'hérédité : soit $k \geq 1$, on a $(1+p)^{p^k} = 1+\lambda_k p^{k+1}$ par hypothèse de récurrence, donc on obtient $(1+p)^{p^{k+1}} = 1+p^{k+2}(\lambda_k + \sum_{i=2}^{p} \binom{p}{i} \lambda_k^i p^{(i-1)(k+1)-1})$ et le résultat est montré par récurrence.

   En particulier, $1+p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

   En utilisant l'exercice , on sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, d'ordre $p-1$. Notons x_0 un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ et prenons un relèvement x_1 de x_0 dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. L'ordre de x_1 est le la forme $(p-1)p^s$ pour un certain $s \leq \alpha$, de sorte que $x := x_1^{p^s}$ est d'ordre $p-1$. Comme x et $1+p$ ont des ordres premiers entre eux et comme le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est abélien, on a vu que $x(1+p)$ est donc d'ordre $p^{\alpha-1}(p-1) = \varphi(p)$ et $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est donc cyclique.
3. Remarquons d'abord que $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ et $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$. Supposons maintenant $\alpha \geq 2$. Par une récurrence semblable à celle effectuée au b), on montre que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. Observons maintenant le morphisme surjectif $\pi : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$: son noyau est exactement $\langle 5 \rangle$, et $\pi(-1) = -1$. Par conséquent, les sous-groupes $\langle 5 \rangle$ et $\langle -1 \rangle$ vérifient les hypothèses de l'exercice , donc $\langle 5 \rangle \times \langle -1 \rangle \cong (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. On obtient donc finalement $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.
4. Si $n = \prod_p p^{\alpha_p}$ est la décomposition en facteurs premiers de n, alors le lemme chinois nous donne

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/2^{\alpha_2}\mathbb{Z})^\times \times \prod_{p \neq 2,\ \alpha_p \geq 1} \big(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{\alpha_p - 1}\mathbb{Z}\big).$$

Exercice 9.

Déterminer les entiers $n \in \mathbb{Z}$ pour lesquels $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

Solution
Si $n = \prod_p p^{\alpha_p}$ est la décomposition en facteurs premiers de n, la question d) de l'exercice assure que

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/2^{\alpha_2}\mathbb{Z})^\times \times \prod_{p\neq 2,\, \alpha_p \geq 1} \big(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{\alpha_p - 1}\mathbb{Z}\big).$$

En remarquant qu'un groupe cyclique ne peut pas contenir plus d'un élément d'ordre 2, on conclut que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = p^\alpha$ ou $2p^\alpha$ avec p un nombre premier impair et $\alpha \geq 0$ ou $n = 4$.

Exercice 10.

Décomposer le groupe $G = (\mathbb{Z}/187\mathbb{Z})^\times$ sous la forme donnée par le théorème de structure des groupes abéliens finis.

Solution
Comme $187 = 11.17$, l'exercice assure que

$$G \cong (\mathbb{Z}/11\mathbb{Z})^\times \times (\mathbb{Z}/17\mathbb{Z})^\times \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/80\mathbb{Z}\,.$$

Les facteurs invariants de G sont donc 2 et 80.