Théorie des groupes

corrigé feuille 12

Exercice 1 Soient $e_1 = (1, -1, 0)$ et $e_2 = (1, 0, -1)$ dans H.

e_1 et e_2 sont bien indépendants.

Si $x = (a, b, c) \in H$, alors $x = -be_1 - ce_2$. Donc $H \subset < e_1, e_2 >$ et $H = < e_1, e_2 >$.

(e_1, e_2) est une $\mathbb{Z}$-base de H.

Exercice 2 Soit G un groupe abélien d'ordre $360 = 2^3.3^2.5$.

Par théorème de structure des groupes abéliens finis, tout groupe abélien d'ordre 360 est isomorphe à un produit de groupes cycliques de la forme :

$$\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$$

Où les d_i sont des entiers ≥ 2 tels que pour tout i, $d_i \mid d_{i+1}$.

Raisonnons sur les valeurs possibles de k.

$k = 1$: Alors $d_1 = 360$ et $G \simeq \mathbb{Z}/360\mathbb{Z}$.

$k = 2$. Il s'agit de répartir les 6 facteurs premiers de 360 dans d_1 et d_2 de manière à ce que $d_1 \mid d_2$. On doit forcément avoir dans d_2 au moins un exemplaire de chacun des facteurs, et au moins 2 exemplaires de 2. (Sinon, $4 \mid d_1$ et $4 \nmid d_2$, absurde). Les possibilités pour d_2 sont donc :

— $d_2 = 5.3.2^2$ et $d_1 = 3.2$. Alors $G \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$.

— $d_2 = 5.3.2^3$ et $d_1 = 3$.Alors $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$.

— $d_2 = 5.3^2.2^2$ et $d_1 = 2$.Alors $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$.

$k = 3$. Comme chaque d_1 doit diviser le suivant, tous les facteurs premiers de d_1 doivent être des facteurs premiers de d_2 et d_3 également. Donc $d_1 = 2$ et $2 \mid d_2$. Comme on a toujours que $2.3.5 \mid d_3$, les possibilités sont :

— $d_3 = 5.3.2$, $d_2 = 2.3$ et $d_1 = 2$. Alors $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$.

— $d_3 = 5.3^2.2$, $d_2 = 2$ et $d_1 = 2$. Alors $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$.

$k \geq 4$ est impossible car aucun facteurs premiers de la décomposition de 360 n'est à puissance supérieure ou égale à 4.

Donc les groupes abéliens d'ordre 360 sont les groupes isomorphes à un groupe parmi : $\mathbb{Z}/360\mathbb{Z}$; $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$; $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$.

Exercice 3 (*p*-groupes abéliens)

On note $\mathcal{G}$ l'ensemble des groupes abéliens d'ordre p^n et $\mathcal{P}$ l'ensemble des partitions n. Par théorème de structure des groupes abéliens finis,

$$\mathcal{G} = \left\{ \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \quad | \quad k \in \mathbb{N}^*; \prod_{i=1}^{k} n_i = p^n; \forall i \;\; n_i \mid n_{i+1} \right\}$$

Soit $A \in \mathcal{P}$ une partition de n. $A = (x_1, \ldots, x_k)$, et on peut supposer les x_i ordonnés par ordre croissant : $x_1 \leq x_1 \leq \cdots \leq x_k$.

On pose $G_A = \mathbb{Z}/p^{x_1}\mathbb{Z} \times \mathbb{Z}/p^{x_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{x_k}\mathbb{Z}$.

On a bien que pour tout i, $p^{x_i} \mid p^{x_{i+1}}$ et que $\prod_{i=1}^{k} p^{x_i} = p^n$. Donc $G_A \in \mathcal{G}$.

Réciproquement : Soit $G \in \mathcal{G}$. Alors, par théorème de structure, G s'écrit de manière unique comme $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \quad | \quad k \in \mathbb{N}^*; \prod_{i=1}^{k} n_i = p^n; \forall i n_i \mid n_{i+1}$.

$\prod_{i=1}^{k} n_i = p^n$ donc pour tout i, $n_i = p^{x_i}$ avec $x_i \in \mathbb{N}^*$.

$\prod_{i=1}^{k} n_i = p^{\sum x_i} = p^n$, donc $\sum_{i=1}^{k} x_i = n$.

Donc $A_G = (x_1, \ldots, x_k) \in \mathcal{P}$.

Ainsi, on a bien défini $\phi : G \mapsto A_G$ et $\psi : A \mapsto G_A$, et il est immédiat que $\phi \circ \psi = Id$ et $\psi \circ \phi = Id$.

D'où la bijection.

Malheureusement, cela reste d'une utilité limitée, le nombre de partitions d'un entier grand étant difficile à obtenir. Cependant, cela donne une idée de l'explosion du nombre de groupes abéliens d'ordre p^n quand n est grand. Par exemple, il y a environ 2.10^8 partitions de 100 et environ 2.10^{31} partitions de 1000.

Exercice 4 (Sous-groupes de p-groupes abéliens)

G est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension n. Un sous-espace vectoriel de dimension k est un sous-groupe de dimension p^k de G, et réciproquement, tout sous-groupe de G peut-être muni d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.

Nous cherchons donc le nombre de sous-espaces-vectoriels de G de dimension k.

Calcul du nombre de familles $\mathbb{Z}/p\mathbb{Z}$-libres à k éléments dans G : $(p^n-1)(p^n-p)(p^n-p^2)\dots(p^n-p^{k-1})$.

Cependant, un même espace vectoriel peut être engendré par plusieurs bases. Le nombre de bases d'un $\mathbb{Z}/p\mathbb{Z}$-ev de dimension k est : $(p^k-1)\dots(p^k-p^{k-1})$.

D'où le nombre de sous-groupes de cardinal p^k de G :

$$\begin{aligned}&\frac{\prod_{i=0}^{k-1}(p^n-p^i)}{\prod_{i=0}^{k-1}(p^k-p^i)}\\ =\ &\frac{\prod_{i=0}^{k-1}p^i\cdot\prod_{i=0}^{k-1}(p^{n-i}-1)}{\prod_{i=0}^{k-1}p^i\cdot\prod_{i=0}^{k-1}(p^{k-i}-1)}\\ =\ &\prod_{i=0}^{k-1}\frac{(p^{n-i}-1)}{(p^{k-i}-1)}\end{aligned}$$

Exercice 5

1. Soit $(x_1,x_2,\dots,x_n)$ une famille finie de générateurs de G. Par le théorème de structure des groupes abéliens de type fini, G est dénombrable. Soit $\varphi \in Aut(G)$. Alors φ est entièrement déterminée par l'image des n générateurs. Pour chaque x_i, il y a au plus une quantité dénombrable d'images possibles, donc une quantité dénombrables d'images possibles pour $(x_1,x_2,\dots,x_n)$, donc pour φ.
2. Par théorème de structure des groupes abéliens de type fini, G est isomorphe à :

$$\mathbb{Z}^r\times\mathbb{Z}/n_1\mathbb{Z}\times\dots\times\mathbb{Z}/n_k\mathbb{Z} \quad | \quad k\in\mathbb{N}; r\in\mathbb{N}; \forall i\ \ n_i \mid n_{i+1}$$

Si $r=0$: Alors G est fini et donc $Aut(G)\subset\mathfrak{S}(G)$ qui est fini.

Si $r=1$: $G\simeq\mathbb{Z}\times H$ avec H abélien fini. Soit $(h_2,\dots h_t)$ une famille génératrice de H. Alors, en posant $g_1=(1,0)$ et $g_i=(0,h_i)$ pour i de 2 à t, on a que (g_i) est une famille génératrice finie de G.

Soit $\varphi\in Aut(G)$. Alors φ préserve l'ordre des éléments donc tous les g_i $(i>2)$ sont envoyés sur un éléments d'ordre fini. Les éléments d'ordre fini de G sont exactement les éléments de $\{0\}\times H$. Donc il y a un nombre fini d'images possibles pour chaque g_i. $\varphi(g_1)$ doit être d'ordre infini, donc dans $\mathbb{Z}^*\times H$. Si $\varphi(g_1)=(a,h\in H)$, alors $\varphi(G)\subset(a\mathbb{Z}\times H)$. Donc $a=\pm1$ et $\varphi(g_1)\in\{-1,1\}\times H$, qui est fini. φ est donc entièrement déterminée par un nombre fini de choix pour un nombre fini d'éléments. Donc $\mathrm{Aut}(G)$ est fini.

On a montré un sens de l'équivalence. Montrons la contraposée de la réciproque :

Si $r\geq 2$: Alors $G\simeq\mathbb{Z}^2\times H$ avec H abélien de type fini. Pour tout a dans $\mathbb{Z}$, on pose :

$\psi_a : \begin{array}{ccc}\mathbb{Z}^2 & \to & \mathbb{Z}^2\\ (x,y) & \mapsto & (x+ay,y)\end{array}$. ψ_a est une application linéaire qui envoie la $\mathbb{Z}$-base $((1,0),(0,1))$ sur la $\mathbb{Z}$-base $((1,0)(a,1))$, donc est un automorphisme.

On pose alors, pour tout $a\in\mathbb{Z}$, $\phi_a\in\mathrm{Aut}(\mathbb{Z}^2)\times\mathrm{Aut}(H)\subset\mathrm{Aut}(G)$ comme $\phi_a=\psi_a\times Id_H$.

$\{\phi_a \mid a\in\mathbb{Z}\}$est infini et inclus dans $\mathrm{Aut}(G)$, donc $\mathrm{Aut}(G)$ est infini.

Exercice 6 (Groupe libre)

1. Soit $u\in\Sigma$, non-nul.

   Si le mot est de la forme $u=g^{\alpha_1}h^{\beta_1}g^{\alpha_2}h^{\beta_2}\dots g^{\alpha_n}$, avec $\alpha_i\neq0\neq\beta_j$ pour tout i,j. Pour $x\in E_1, u(x)\in E_2$, donc $u\neq e$.

   Symétriquement, si $u=h^{\beta_1}g^{\alpha_2}h^{\beta_2}\dots g^{\alpha_n}h^{\beta_n}$ avec $\alpha_i\neq0\neq\beta_j$ pour tout i,j, pour $x\in E_2, u(x)\in E_1$, donc $u\neq e$.

Si $v = g^{\alpha_1}h^{\beta_1}g^{\alpha_2}h^{\beta_2}\dots g^{\alpha_n}h^{\beta_n}$, Alors $u = g^{\alpha_1}vg^{-\alpha_1}$ est de la première forme donc $u \neq e$. Comme u et v sont conjugués, $v \neq e$.

Donc tous les mots non-triviaux ne correspondent pas à e.

2. Pour tout $i \in \mathbb{Z}*$, $A^i = \begin{pmatrix} 1 & sgn(i).2^i \\ 0 & 1 \end{pmatrix}$ et $B^i = \begin{pmatrix} 1 & 0 \\ sgn(i).2^i & 1 \end{pmatrix}$.

On pose $E_1 = \{(x,y) \in \mathbb{R}^2; \quad |x| < |y|\}$ et $E_2 = \{(x,y) \in \mathbb{R}^2; \quad |x| > |y|\}$.

Pour $(x,y) \in E_1$, $A^i(x,y) = (x + sgn(i).2^i y, y)$.

On a : $|x + sgn(i).2^i y| > |sgn(i).2^i y| - |x| > 2^i |y| - |x| > |y|$, donc $A^i(x,y) \in E_2$.

Pour $(x,y) \in E_1$, $A^i(x,y) = (x, y + sgn(i).2^i x)$.

On a : $|y + sgn(i).2^i x| > |sgn(i).2^i x| - |y| > 2^i |x| - |y| > |x|$, donc $A^i(x,y) \in E_1$.

Donc Γ est libre par la question 1.

Exercice 7 (Automorphismes de D_n) 1. Soit $\psi \in \mathrm{Aut}(D_n)$. Alors ψ est entièrement déterminée par l'image de r et s (car générateurs).

Si $\psi \in \mathrm{Stab}_{\mathrm{Aut}(D_n)}(s)$, $\psi(s) = s$. r est envoyé sur un élément d'ordre n. Les éléments d'ordre n dans D_n sont les r^i où i est premier avec n (car $n \geq 3$). Cela donne donc au plus $\varphi(n)$ possibilités pour ψ.

Réciproquement, chacune de ces possibilités donne un automorphisme différent. (Et c'est bien un automorphisme).

2. Si $\psi \in \mathrm{Stab}_{\mathrm{Aut}(D_n)}(r)$, $\psi(r) = r$. s est envoyé sur un élément d'ordre 2. Les éléments d'ordre 2 dans D_n sont toutes les symétries $r^i s$ où i est dans $[\![1, n]\!]$ ($n \geq 3$) ainsi que $r^{n/2}$ si n est pair.

Si $\psi(s) = r^{n/2}$, alors $\psi(D_n) \subset < r >$, ce qui est absurde.

Cela donne donc au plus n possibilités pour ψ.

Réciproquement, chacune de ces possibilités donne un automorphisme différent. (Et c'est bien un automorphisme).

3. Soit $\psi \in \mathrm{Stab}_{\mathrm{Aut}(D_n)}(r)$ et $\alpha \in \mathrm{Aut}(D_n)$.

$\alpha^{-1}(r)$ doit être un élément d'ordre n donc est un r^i avec i premier à n.

$\alpha \circ \psi \circ \alpha^{-1}(r) = \alpha(\psi(r^i)) = \alpha(\psi(r)^i) = \alpha(r^i) = \alpha(\alpha^{-1}(r)) = r$.

Donc $\alpha \circ \psi \circ \alpha^{-1} \in \mathrm{Stab}_{\mathrm{Aut}(D_n)}(r)$.

On a bien montré que $\mathrm{Stab}_{\mathrm{Aut}(D_n)}(r) \lhd \mathrm{Aut}(D_n)$.

4. On note $R = \mathrm{Stab}_{\mathrm{Aut}(D_n)}(r)$ et $S = \mathrm{Stab}_{\mathrm{Aut}(D_n)}(s)$.

Par la question précédente, $R \lhd \mathrm{Aut}(D_n)$.

Si $\psi \in R \cap S$, alors ψ fixe r et s, c'est à dire fixe tous les générateurs de D_n. Donc $\psi = Id$. D'où $R \cap S = \{Id\}$.

Soit $f \in \mathrm{Aut}(D_n)$. On pose $\beta \in \mathrm{Stab}(r)$ définie par $\beta(r) = r$ et $\beta(s) = f(s)$. On pose $\alpha \in \mathrm{Stab}(s)$ définie par $\alpha(s) = s$ et $\alpha(r) = \beta^{-1}(f(r))$. Il est alors facile de vérifier que $f = \beta \circ \alpha \in RS$. Donc $\mathrm{Aut}(D_n) = RS$.

Par théorème de produit semi-direct : $\mathrm{Aut}(D_n) = \mathrm{Stab}_{\mathrm{Aut}(D_n)}(r) \rtimes \mathrm{Stab}_{\mathrm{Aut}(D_n)}(s)$.

5. $Card(\mathrm{Aut}(D_n)) = n\varphi(n)$.

6. On note $\gamma : \begin{array}{ccc} G & \to & \mathrm{Int}(G) \\ g & \mapsto & \delta_g \end{array}$ où $\delta_g : x \mapsto gxg^{-1}$.

γ est bien un morphisme et est surjectif.

$\ker \gamma = Z(G)$, donc par théorème d'isomorphisme, $\mathrm{Int}(G) \simeq G/Z(G)$.

7. **Cas n=3**. $Card(\mathrm{Aut}(D_3)) = 3\varphi(3) = 6$.

$Z(D_3) = \{e\}$ donc $\mathrm{Int}(D_3) \simeq D_3$ et $Card(\mathrm{Int}(D_3) = 6$.

Comme $\mathrm{Int}(D_3) \subset \mathrm{Aut}(D_3)$, on a que $\mathrm{Aut}(D_3) \simeq D_3$.

Exercice 8 1. C'est essentiellement un rappel : On a déjà vu que $\mathfrak{A}_n =< (1ij) >$, que les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$ (On l'a vu dans $\mathfrak{A}_5$, c'est pareil dans $\mathfrak{A}_n$ pour $n \geq 5$). Donc, si $H \lhd \mathfrak{A}_n$ contient un 3-cycle, il les contient tous parce qu'il est stable par conjugaison, et contient donc le groupe engendré par ces 3-cycles, c'est à dire $\mathfrak{A}_n$.

2. $\tau\sigma\tau^{-1} = (12)(45)\dots$ donc est différent de σ. D'où $\rho_1 \neq Id$.
   H stable par conjugaison donc $\tau\sigma\tau^{-1} \in H$ et donc $\rho_1 \in H$.
   Calculons les points fixes de ρ_1 et de σ. Soit x un point fixe de σ supérieur ou égal à 6. $\rho_1(x) = x$, car x n'est dans le support d'aucune permutation parmi $\tau, \tau^{-1}, \sigma, \sigma^{-1}$.
   σ ne fixe pas 1,2,3 ou 4, mais fixe éventuellement 5.
   $\rho_1(x) = \tau\sigma\tau^{-1}\sigma^{-1}(1) = \tau\sigma\tau^{-1}(2) = \tau\sigma(2) = \tau(1) = 1$. Donc 1 est un point fixe de ρ_1. La même chose se produit pour 2.
   Donc ρ_1 a au moins un point fixe de plus que σ.
3. $\tau\sigma\tau^{-1} = (124\dots)\tau\gamma_2\tau^{-1}\dots\tau\gamma_k\tau^{-1}$ donc est différent de σ. D'où $\rho_2 \neq Id$.
   H stable par conjugaison donc $\tau\sigma\tau^{-1} \in H$ et donc $\rho_2 \in H$.
   Calculons les points fixes de ρ_2 et de σ. Soit x un point fixe de σ supérieur ou égal à 6. $\rho_2(x) = x$, car x n'est dans le support d'aucune permutation parmi $\tau, \tau^{-1}, \sigma, \sigma^{-1}$.
   σ ne fixe pas 1,2,3,4 ou 5.
   $\rho_2(2) = \tau\sigma\tau^{-1}\sigma^{-1}(2) = \tau\sigma\tau^{-1}(1) = \tau\sigma(1) = \tau(2) = 2$. Donc 2 est un point fixe de ρ_2.
   Donc ρ_2 a au moins un point fixe de plus que σ.
4. Si σ n'est pas un trois cycle, σ est d'une des formes étudiées ci-dessus. Or dans les deux cas, on a trouvé un élément non-trivial de H ayant plus de points fixes que σ, ce qui contredit la maximalité de N.
   Donc H contient un 3-cycle, donc est $\mathfrak{A}_n$ par la question 1.