

Théorie des groupes

Corrigé Feuille 3

Exercice 1 Notons K ce produit restreint

K est non-vide car $(e_i)_{i \in G_i} \in K$.

Soient $g, h \in K$. On note I_g la partie finie de I contenant les indices i tels que $g_i \neq e_i$. Alors, on pose $g' = (g'_i)_I$ avec pour tout i dans I_g , $g'_i = g_i^{-1}$ et pour tout i dans $I \setminus I_g$, $g'_i = e_i$. g' est alors l'inverse de g et $I_g = I_{g'}$ donc $g^{-1} \in K$.

$gh = (g_i h_i)_I$ donc $I_{gh} = I_g \cup I_h$ et $gh \in K$.

K est donc un sous-groupe du produit direct.

Exercice 2 Soit G un groupe.

Si G fini, alors l'ensemble de ses sous-groupes est inclus dans l'ensemble des parties de G , qui est un ensemble fini. Donc G a un nombre fini de sous-groupes.

Si G a un nombre fini de sous-groupes: Alors pour tout $x \in G$, $\langle x \rangle$ est fini. Sinon, $\langle x \rangle \cong \mathbb{Z}$ et a une infinité de sous-groupes, ce qui serait absurde. $G = \bigcup_{x \in G} \langle x \rangle$, donc G est fini.

Exercice 3 1. On note $\varphi : \begin{array}{ccc} G_1 \times G_2 & \rightarrow & G_2 \times G_1 \\ (x, y) & \mapsto & (y, x) \end{array}$

φ est bien un morphisme.

$\ker \varphi = \{(x, y), (y, x) = (e_{G_2}, e_{G_1})\} = \{(e_{G_1}, e_{G_2})\}$ et φ est surjective, donc est un isomorphisme.

2. Soient $(x_1, x_2), (y_1, y_2)$ dans $H_1 \times H_2$. Alors $(y_1^{-1}, y_2^{-1}) \in H_1 \times H_2$ est l'inverse de (y_1, y_2) . $x_1 y_1^{-1} \in H_1$ et $x_2 y_2^{-1} \in H_2$. D'où $(x_1, x_2) \cdot (y_1, y_2)^{-1} = (x_1 y_1^{-1}, x_2 y_2^{-1}) \in H_1 \times H_2$, qui est donc bien un sous-groupe de $G_1 \times G_2$.

3. Non. Contre-exemple: $\{(0, 0), (1, 1)\}$ est un sous-groupe de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 4 Supposons $H_1 \times H_2$ isomorphe à $\mathfrak{S}_3$.

$|H_1| |H_2| = |\mathfrak{S}_3| = 6$. Or les deux sous-groupes étant non-triviaux, il ne sont pas de cardinal 1. Donc l'un est de cardinal 2 et l'autre 3. Ils sont donc tous les deux abéliens, et leur produit direct est alors abélien. Or $\mathfrak{S}_3$ n'est pas abélien (exemple: $(12)(123) = (32) \neq (13) = (123)(12)$).

Exercice 5 (Classification des groupes d'ordre 4) Soit G un groupe d'ordre 4.

Il ne contient pas d'élément d'ordre 3. Soit par théorème de Lagrange, soit parce que si c'est le cas (pour un certain g), $G = \{e, g, g^2, h\}$. Et alors:

$gh = e \Rightarrow h = g^2$ Absurde.

$gh = g \Rightarrow h = e$ Absurde.

$gh = g^2 \Rightarrow h = g$ Absurde.

$gh = h \Rightarrow g = e$ Absurde. Donc le produit $gh \notin G$. Absurde.

Si G contient un élément d'ordre 4, alors il est cyclique engendré par cet élément et donc est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Sinon, tous ses éléments non-triviaux sont d'ordre 2. Soient g et h d'ordre 2 et distincts.

$ghgh=e$ donc $gh = hg$.

$\langle g \rangle \cap \langle h \rangle = \{e\}$.

$\langle g \rangle \langle h \rangle = G$ car gh ne peut pas être égal à e, g ou h , donc gh est le dernier élément.

par théorème de produit direct, $G \cong \langle g \rangle \times \langle h \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 6 (Représentation linéaires des groupes)

Pour un groupe G , un entier $n \in \mathbb{N}$ et un corps K , on appelle *représentation de matricielle de G de degré n sur K* tout morphisme $\rho \in \text{Hom}(G, \text{GL}(n, K))$. Si de plus ρ est injective, la représentation est dite *fidèle*.

1. On note P_σ la matrice de permutation de dimension 3, 3 associée à une permutation σ de $\mathfrak{S}_3$.

$$\text{Soit } \rho_1 : \begin{array}{ccc} \mathfrak{S}_3 & \rightarrow & \text{GL}_3(\mathbb{Q}) \\ \sigma & \mapsto & P_\sigma \end{array} .$$

$P_\sigma P_{\sigma'} = P_{\sigma\sigma'}$ donc ρ_1 est un morphisme.

$\ker(\rho_1) = \{\sigma, P_\sigma = Id\} = \{Id\}$. Donc ρ_1 est fidèle.

Soit $T = 123$ un triangle équilatéral centré en 0 dont les sommets sont notés 1, 2, 3. On note D_3 l'ensemble des isométries de $\mathbb{R}^2$ préservant ce triangle. D_3 est le 3ème groupe diédral, qui est d'ordre 6, et constitué au moins de: $Id, r_{0,2\pi/3}, r_{0,4\pi/3}, s_{01}, s_{02}, s_{03}$. Si f est une isométrie de $\mathbb{R}^2$ préservant un triangle équilatéral centré en 0, on note σ_f la permutation des sommets induite par f . On a donc $\sigma_f \in \mathfrak{S}_3$. En effet, une isométrie préservant les distances, un coté du triangle ne peut être envoyé que sur un coté, et donc un sommet sur un sommet.

$$\text{Soit alors } \psi : \begin{array}{ccc} D_3 & \rightarrow & \mathfrak{S}_3 \\ f & \mapsto & \sigma_f \end{array} .$$

On peut facilement voir que ψ est un morphisme.

ψ est injective car si $\psi(f) = Id$, alors $f(1) = 1$ et $f(2) = (2)$, donc f est une application linéaire préservant la base $(O1, O2)$ du plan, donc est l'identité.

ψ est surjective car on peut remarquer que les 6 éléments donnés plus haut réalisent toutes les permutations de $\mathfrak{S}_3$. Donc ψ est un isomorphisme, et $\rho_2 = \psi^{-1}$ est une représentation fidèle de degré 2 de $/Sym_3$ sur $\mathbb{R}$.

2. On note $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. On a que $J^2 = -Id$.

$$\text{Soit } \rho_3 : \begin{array}{ccc} \mathbb{C}^* & \rightarrow & \text{GL}_2 \mathbb{R} \\ a + ib & \mapsto & aId + bJ = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{array}$$

$\rho_3(a + ib)\rho_3(c + id) = (aId + bJ)(cId + dJ) = acId + bcJ + adJ - bdId = (ac - bd)Id + (bc + ad)J = \rho_3((a + ib)(c + id))$. Donc ρ_3 est un morphisme. ρ_3 est évidemment injectif, donc est bien une représentation fidèle de degré 2 de $\mathbb{C}^*$ sur $\mathbb{R}$.

3. Soit G fini de cardinal n . Par le théorème de Cayley, il existe $\varphi : G \rightarrow \mathfrak{S}_n$ injectif.

De la même manière qu'à la première question, on note P_σ la matrice de permutation de dimension n, n associée à une permutation σ de $\mathfrak{S}_n$. $\theta : \begin{array}{ccc} \mathfrak{S}_n & \rightarrow & \text{GL}_n(\mathbb{Q}) \\ \sigma & \mapsto & P_\sigma \end{array}$ est un morphisme injectif.

Donc $\rho_4 = \theta \circ \varphi$ est un morphisme injectif de G dans $\text{GL}_n(\mathbb{Q})$. C'est donc bien une représentation fidèle de degré n de G sur $\mathbb{Q}$.

Exercice 7 Soit $\psi : G_1 \rightarrow G_2$ un isomorphisme.

$$1. \text{ Soit } f : \begin{array}{ccc} \text{Aut}(G_1) & \rightarrow & \text{Aut}(G_2) \\ \phi & \mapsto & \psi \circ \phi \circ \psi^{-1} \end{array} .$$

$f(\phi_1 \circ \phi_2) = f(\phi_1) \circ f(\phi_2)$ donc f est un morphisme.

Si on pose $g : \begin{array}{ccc} \text{Aut}(G_2) & \rightarrow & \text{Aut}(G_1) \\ \phi & \mapsto & \psi^{-1} \circ \phi \circ \psi \end{array}$, alors $f \circ g = Id$ et $g \circ f = Id$. Donc f est bijective et est donc un isomorphisme.

2. On note σ_g la conjugaison par g dans G_1 .

Alors $f(\sigma_g) = \sigma_{\psi(g)} \in \text{Int}(G_2)$. Donc $f' = f$ restreinte à $\text{Int}(G_1)$ définit bien un morphisme vers $\text{Int}(G_2)$.

En notant $h : \begin{array}{ccc} \text{Int}(G_2) & \rightarrow & \text{Int}(G_1) \\ \sigma_g & \mapsto & \sigma_{\psi^{-1}(g)} \end{array}$, on a $f' \circ h = Id$ et $h \circ f' = Id$, donc f' est bien un isomorphisme entre $\text{Int}(G_1)$ et $\text{Int}(G_2)$

Exercice 8 (Homographies de la sphère de Riemann)

1. Si $c = 0$, $f|_{\mathbb{C}}$ est une application linéaire sur $\mathbb{C}$ non constante en dimension 1, donc est une permutation de $\mathbb{C}$. Comme $f(\infty) = \infty$, f est une permutation de $\mathbb{P}$.

Si $c \neq 0$, on a, en posant $g : z \mapsto \frac{-dz+b}{cz-a}$, un calcul permet de vérifier que $f \circ g = Id_{\mathbb{P}}$ et donc que f est une permutation de $\mathbb{P}$.

2. On vient de voir que $\mathcal{H}$ est stable par inverse. Reste à montrer qu'il est stable par composition.

Si $f : z \mapsto \frac{az+b}{cz+d}$ et $g : z \mapsto \frac{a'z+b'}{c'z+d'}$, alors $f \circ g = z \mapsto \frac{(aa+bb')'z+(ac'+bd')}{(ac'+b'd)z+(cc'+dd')}$.

Donc $\mathcal{H}$ est un sous-groupe de $\mathfrak{S}_{\mathbb{P}}$.

3. On note K cet ensemble $f_i \circ f_i = Id$ pour tout i , donc K est stable par inversion. f_1 est l'identité, donc les produits par f_1 sont stables.

$$f_2 \circ f_3 = f_3 \circ f_2 = f_4$$

$$f_2 \circ f_4 = f_4 \circ f_2 = f_3$$

$$f_4 \circ f_3 = f_3 \circ f_4 = f_2.$$

K est donc stable par produit donc est un sous-groupe de H . Il est d'ordre 4 mais ne contient pas d'élément d'ordre 4, donc est isomorphe au groupe de Klein.

$$4. \varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) = z \mapsto \frac{(aa+bb')'z+(ac'+bd')}{(ac'+b'd)z+(cc'+dd')} = z \mapsto \frac{az+b}{cz+d} \circ z \mapsto \frac{a'z+b'}{c'z+d'} = \varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)\varphi\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right).$$

Donc φ est un morphisme. On a trivialement que $Im(\varphi) = \mathcal{H}$.

$$\ker \varphi = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad z \mapsto \frac{az+b}{cz+d} = Id \right\} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad b = c = 0; a = d \right\} = \{\lambda Id, \lambda \in \mathbb{C}^*\}.$$

Donc $\ker \varphi = Z(GL_2(\mathbb{C}))$.

Exercice 9 Notons H_1 et H_2 les deux sous-groupes propres de G

1. Pour tout x dans G , $ordre(x)$ est fini. Sinon, $\langle x \rangle$ serait isomorphe à $\mathbb{Z}$ et admettrait une infinité de sous-groupes disjoints. Ce qui est absurde.

On a que $G = \cup_{x \in G} \langle x \rangle$. Comme G a exactement 4 sous-groupes, il s'agit d'une union d'au plus 4 ensembles finis, donc G est fini.

2. On note $r = \min \{i \mid \exists (x_1, x_2, \dots, x_i) \in G^i, G = \langle x_1, x_2, \dots, x_i \rangle\}$. r est donc le cardinal minimal d'une famille génératrice, et existe bien car G est fini.

Montrons que $r = 1$.

On suppose que $r \geq 2$:

Soit $X = \{x_1, x_2, \dots, x_r\}$ un ensemble générateur minimal. Pour tout i , $\langle x_i \rangle$ est propre. En effet, si $\langle x_i \rangle = G$, alors $r = 1$, ce qui est absurde. Si $\langle x_i \rangle = \{e\}$, alors $X \setminus \{x_i\}$ est un ensemble générateur de G , ce qui est absurde par minimalité de r .

- Si $r \geq 3$, tous les $\langle x_i \rangle$ étant propres, ils sont soit H_1 soit H_2 . Donc au moins 2 d'entre eux sont les mêmes. Donc au moins un des x_i est une puissance d'un x_j avec $j \neq i$. Donc $X \setminus \{x_i\}$ est un ensemble générateur de G , ce qui est absurde par minimalité de r .

- Donc $r = 2$. On alors que $\langle x_1 \rangle \neq \langle x_2 \rangle$. On pose $y = x_1 x_2$. $\langle y \rangle$ est propre (sinon on contredit la minimalité de r). Donc $\langle y \rangle = \langle x_1 \rangle$ ou $\langle y \rangle = \langle x_2 \rangle$.

Si $\langle y \rangle = \langle x_1 \rangle$, on a $x_1 x_2 = x_1^k$ avec $k \neq 0$, et $x_2 = x_1^{k-1} \in \langle x_1 \rangle$, ce qui est absurde. De même, si $\langle y \rangle = \langle x_2 \rangle$, on a $x_1 \in \langle x_2 \rangle$, ce qui est absurde.

Notre hypothèse est donc fautive, d'où $r = 1$, ce qui signifie que G est monogène.

3. Soit g tel que $G = \langle g \rangle$. On note n l'ordre de G . Soit $n = \prod_{i=1}^s p_i^{\alpha_i}$ une décomposition de n en facteurs premiers. (avec les $\alpha_i \geq 1$)

- Si $s \geq 3$, alors les sous-groupes $\langle g^{n/p_1} \rangle$, $\langle g^{n/p_2} \rangle$, $\langle g^{n/p_3} \rangle$ sont trois sous-groupes propres d'ordre distincts (respectivement d'ordres p_1 , p_2 et p_3), donc sont distincts. Absurde. Donc $s < 3$.
- Si $s = 2$, alors $n = p^{\alpha_1} q^{\alpha_2}$. Supposons que $\alpha_1 \geq 2$. Alors $\langle g^p \rangle$, $\langle g^{p^2} \rangle$ et $\langle g^q \rangle$ sont trois sous-groupes propres d'ordre distincts (respectivement d'ordres p , p^2 et q). Absurde. Donc $\alpha_1 = 1$. Par symétrie, on a aussi $\alpha_2 = 1$, et donc $n = pq$.
- Si $s = 1$, $n = p^\alpha$.

On ne peut pas avoir $\alpha = 1$, car $\mathbb{Z}/p\mathbb{Z}$ n'a pas de sous-groupe propre.

Si $\alpha = 2$, G ne contient qu'un sous-groupe propre, qui est $\langle g^p \rangle$. En effet, si H est un sous-groupe propre, il ne peut contenir un élément g^k avec k premier avec p^2 car ce sont des générateurs de G . Donc H contient un élément g^{kp} avec $k \neq 0$, donc contient tout $\langle g^p \rangle$.

Si $\alpha > 3$, alors $\langle g^p \rangle$, $\langle g^{p^2} \rangle$ et $\langle g^{p^3} \rangle$ sont trois sous-groupes propres distincts.

D'où $n = p^3$.

On a donc bien montré que les seules possibilités pour G sont d'être cycliques d'ordre pq ou p^3 avec p et q des nombres premiers distincts.