CHAPITRE 10 - GROUPES

Exercice 10.1

Soient $f : G \to G'$ un isomorphisme de groupes et a un élément de G d'ordre n. Comme $e' = f(e) = f(a^n) = (f(a))^n$, on en déduit que $f(a)$ est d'ordre fini, divisant n. Si $f(a)^k = e'$, alors $f(a^k) = e'$ donc $a^k = e$ car f injective, d'où n divise k. Il en résulte que $f(a)$ est d'ordre n.

Exercice 10.2

Dans $\mathbb{Z}/8\mathbb{Z}$, $\bar{1}$ est d'ordre 8, alors qu'aucun élément de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ n'est d'ordre 8, car $4(x, y) = (\bar{0}, \bar{0})$ pour tout $(x, y) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Un isomorphisme conservant l'ordre, les deux groupes ne sont pas isomorphes.

Exercice 10.3

1. On vérifie par calcul $\det(A(\theta)) = \det(B(\theta)) = 1$ ainsi G et H sont inclus dans $GL_2\mathbb{R})$. La matrice I_2 est $A(0) = B(0)$. Par calcul, on vérfie que $A(\theta)A(\theta') = A(\theta + \theta') \in G$ et $A(\theta)^{-1} = A(-\theta) \in G$ (et de même pour $B(\theta)^{-1}$)). On en déduit que G et H sont deux sous-groupes de $GL_2(\mathbb{R})$.
2. Soit $A \in G$. Il existe $\theta \in \mathbb{R}$ tel que $A = A(\theta)$. On a alors $A^2 = A(2\theta)$ et $A^2 = I_2$ si et seulement si $\cos(2\theta) = 1$ et $\sin(2\theta) = 0$ soit $\theta \in \pi\mathbb{Z}$. Il y a donc deux matrices de G qui vérifient $X^2 = I_2$: la matrice $A(0) = I_2$ et $A(\pi) = -I_2$. En revanche dans H, on ne trouve que I_2. S'il existait un isomorphisme φ entre G et H. On a, pour $X \in G$, $\varphi(X^2) = \varphi(X)^2$. Si $X^2 = I_2$ alors $\varphi(X)^2 = \varphi(I_2) = I_2$. Or I_2 et $-I_2$ sont deux matrices de G qui vérifient cela. Si φ est bijective, $\varphi(I_2)$ et $\varphi(-I_2)$ seraient deux matrices distinctes qui vérifient $(\varphi(X))^2 = I_2$ dans H d'où une contradiction.

Exercice 10.4

Pour tout $(x, y) \in G^2$, $f(xy) = f(x)f(y)$ car G est abélien, donc f est un morphisme. Par le théorème de Bézout, il existe deux entiers u et v tels que $uk + vn = 1$, d'où $\forall x \in G$, $(x^k)^u = x^{1-kn} = x$ car tout élément de G élevé à la puissance n est égal à e. Par suite, l'application $g : x \mapsto x^u$ vérifie $f \circ g = g \circ f = \mathrm{Id}$, donc f est bijective, et g est sa réciproque.

Exercice 10.5

On a $(xy)^{pq} = x^{pq}y^{pq} = e$. Donc l'ordre de xy est un diviseur de pq. On note d l'ordre de xy. On a $(xy)^d = e$ et $(xy)^{dp} = e = x^{dp}y^{dp} = y^{dp}$. Ainsi $y^{dp} = e$ et $q|(dp)$. Puisque p et q sont premiers entre eux alors $q|d$. De même $p|d$. Puisque $p \wedge q = 1$, on en déduit que $pq|d$. Finalement $d = pq$.

Exercice 10.6

A partir de la décomposition en facteurs premiers, on peut écrire p et q sous la forme suivante :

$$p = p_1^{u_1} \cdots p_r^{u_r} p_1^{\alpha_1} \cdots p_j^{\alpha_j} p' \text{ et } q = p_1^{u_1} \cdots p_r^{u_r} p_{j+1}^{\alpha_{j+1}} \cdots p_r^{\alpha_r} q',$$

où $p_1, \dots p_r$ sont des nombres premiers distincts, $j \leqslant r$, p' et q' ne sont divisibles par aucun des p_i et sont premiers entre eux. Soit m le PPCM de p et q. Grâce à la décomposition précédente, on a

$$m = \underbrace{p_1^{u_1+\alpha_1} \cdots p_j^{u_j+\alpha_j} p'}_{=a} \underbrace{p_{j+1}^{u_{j+1}+\alpha_{j+1}} \cdots p_r^{u_r+\alpha_r} q'}_{=b},$$

donc m s'écrit ab, avec $a \mid p$, $b \mid q$ et $a \wedge b = 1$. Or $x^{p/a}$ est d'ordre a et $y^{q/b}$ est d'ordre b, et comme a et b sont premiers entre eux, leur produit est d'ordre $m = ab$.

Exercice 10.7

On note a un générateur de G et n son ordre. On a $G = \{e, a, a^2, \dots, a^{n-1}\}$. Soit H un sous-groupe de G. On note $p = \min\{k \in [\![1 ; n-1]\!], a^k \in H\}$. On vérifie alors que H est le sous-groupe cyclique engendré par a^p. On a déjà $a^p \in H$ et $< a^p > \subset H$. Soit $m \in \mathbb{N}$ tel que $a^m \in H$. On effectue la division euclidienne par p : $m = qp + r$. Or $a^r = a^m(a^p)^{-q} \in H$ et $r = 0$ par définition de p. On a donc $H \subset < a^p >$ et finalement l'égalité.

Exercice 10.8

Soit $x \in G$. Le sous-groupe engendré par x est d'ordre fini, sinon il serait isomorphe à $(\mathbb{Z}, +)$ et contiendrait un nombre infini de sous-groupe (et G également).
Tout sous-groupe $< x >$ avec $x \in G$ est cyclique. Le nombre de sous-groupes cycliques de G est donc fini par hypothèse. On suppose que l'ensemble de ces sous-groupes est $< x_1 >, \dots, < x_p >$. Si $x \in G$ alors $< x >$ est l'un de ces sous-groupes donc x appartient à l'un des $< x_i >$. Ainsi G est la réunion (pas disjointe) de ces p sous-groupes finis donc G est fini.

Exercice 10.9

1. On vérifie tout d'abord qu'on a bien défini une relation d'équivalence : on a évidemment $x\mathcal{R}x$ et si $x\mathcal{R}y$ alors $y\mathcal{R}x$. De même la transitivité est immédiate. Deux éléments d'une même classe d'équivalence ont même image. Cela permet de définir une application $\tilde{f}$. On pourrait montrer que c'est même un morphisme de groupes (en commençant à montrer que $G/\mathcal{R}$ a une structure de groupe mais on déborde pas mal). L'application est surjective : si $z \in \text{Im } f$, il existe $x \in G$ tel que $z = f(x)$ et alors $\tilde{f}(\bar{x}) = z$. Elle est injective car si $f(\bar{x}) = f(\bar{y})$ alors $f(x) = f(y)$ et x et y sont dans la même classe d'équivalence. L'application est bijective. On vérifie enfin que chaque classe d'équivalence comporte exactement $|\ker f|$ éléments. Si $f(y) = f(x)$ alors $f(y * x^{-1}) = e_H$ et $y * x^{-1} \in \ker f$ d'ou il existe $g \in \ker f$ tel que $y = x * g$. Réciproquement si $y = x * g$ alors $f(x) = f(y)$. Les éléments $x * g$ lorsque g décrit $\ker f$ sont deux à deux distincts. Ainsi $\bar{x}$ comporte autant d'élément que $\ker f$.
2. On a une partition de G par les classes d'équivalences. Il y en a $|\text{Im } f$ et chacune comporte $|\ker f|$ éléments ce qui donne la formule.
3. Si $f(x) = e$ alors $f^2(x) = f(e) = e$ donc $\ker f \subset \ker f^2$. De même si $y \in \text{Im } f^2$ alors $y \in \text{Im } f$ et $\text{Im } f^2 \subset \text{Im } f$. On alors les équivalences $\ker f = \ker f^2$ si et seulement si les deux sont de même cardinal et de même pour les images. En utilisant alors $|G| = |Imf|.|\ker f| = |Imf^2|.|\ker f^2|$ (puisque f^2 est aussi un automorphisme de G), on a

$$\ker f = \ker f^2 \Leftrightarrow |\ker f| = |\ker f^2| \Leftrightarrow |\text{Im } f| = |\text{Im } f^2| \Longleftrightarrow \text{Im } f = \text{Im } f^2.$$

Exercice 10.10

1. Soit $g = x + \sqrt{2}y \in G$. On a $x^2 - 2y^2 = 1 = (x + \sqrt{2}y)(x - \sqrt{2}y)$ et $x^2 > 2y^2$. Ainsi $x > \sqrt{2}|y| \geqslant -\sqrt{2}y$. On en déduit que $x + \sqrt{2}y > 0$ (et aussi $x - \sqrt{2}y$).
2. on vérifie différente propriété :
   → G est non vide car $1 = 1 + \sqrt{2}.0 \in G$.
   → le produit est interne : on prend $g = x + \sqrt{2}y$ et $g' = x' + \sqrt{2}y'$ dans G et on veut montrer que $h = gg'$ l'est encore. Pour commencer $h = (xx' + 2yy') + (xy' + yx')\sqrt{2}$. On doit montrer que $xx' + 2yy'$ est dans $\mathbb{N}^*$. Il est évidemment dans $\mathbb{Z}$. Comme au début, on a $x > \sqrt{2}|y| \geqslant 0$ et $x' > \sqrt{2}|y'| \geqslant 0$ donc $xx' > 2|yy'| \geqslant -2yy'$. Finalement $xx' + 2yy' > 0$. L'élément est bien sous la forme $a + \sqrt{2}b$ avec $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$. Il reste à prouver que $h = a + \sqrt{2}b$ vérifie $a^2 - 2b^2 = 1$. On peut le faire par calcul compliqué ou simplement remarquer que $x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y)$. Si $g = x + \sqrt{2}y$, on note $\bar{g} = x - \sqrt{2}y$ et on remarque que $g\bar{g} = x^2 - 2y^2 = 1$ soit $\bar{g} = 1/g$. On a alors $(gg')\overline{gg'} = gg'\bar{g}\bar{g}'$ (on vérifie que $\overline{gg'} = \overline{g}\,\overline{g'}$) et en commutant et associant on trouve 1. Ainsi gg' est dans G.
   → On a au passage montré que le symétrique de g est $\overline{g} = \dfrac{1}{g}$ et qu'il est aussi dans G.

   Finalement G est un sous-groupe de $(\mathbb{R}_+^*, \times)$.
3. On a $(x + \sqrt{2}y)(x - \sqrt{2}y) = 1$. Puisque $x + \sqrt{2}y \geqslant 1 + \sqrt{2} > 1$, on a $x - \sqrt{2}y \in]0, 1[$.
4. Les éléments de $G \cap]1, +\infty[$ sont ceux qui s'écrivent $x + \sqrt{2}y$ avec $x, y \in \mathbb{N}^*$ et $x^2 - 2y^2 = 1$. On détermine les premiers éléments qu'on trouve :
   → $x = 1$, le seul élément dans G est $1 + 0\sqrt{2} = 1$,
   → $x = 2$, pas de solution puisqu'on doit avoir $2y^2 = 3$. Plus généralement, si x est pair $x^2 - 2y^2$ l'est aussi donc ne peut être 1.
   → $x = 3$, on a $y^2 = 4$ et $3 \pm 2\sqrt{2}$ sont dans G avec $3 + 2\sqrt{2} > 1$,
   → si $x \geqslant 5$ et $y \geqslant 1$ alors $x + \sqrt{2}y \geqslant 5 + \sqrt{2} > 3 + 2\sqrt{2}$.

   Le plus petit élément strictement supérieur à 1 dans G est $g_0 = 3 + 2\sqrt{2}$.
5. Considérons $H =< g_0 >= \{g_0^n, n \in \mathbb{Z}\}$. C'est un sous-groupe monogène de G. Soit $g > 1$ dans G. Puisque $g_0 > 1$, il existe $n \in \mathbb{Z}$ tel que $g_0^n \leqslant g < g_0^{n+1}$. On a alors $g_0^{-n} g \in G$ et $1 \leqslant g_0^{-n} g < g_0$. Par définition de g_0, on a $g_0^{-n} g = 1$ et $g = g_0^n$. En conclusion $G = H =< g_0 >= \{g_0^n, n \in \mathbb{Z}\}$. On a en fait déterminer toutes les solutions entières de l'équation $x^2 - 2y^2 = 1$ (avec $x \in \mathbb{N}$, mais on peut prendre les mêmes en changeant le signe de x) : elles sont toutes obtenues à partir des puissances g_0^n pour $n \in \mathbb{N}$ (celles avec $n \in \mathbb{Z}$ donnent les couples (x, y) avec $y < 0$).

Exercice 10.11

1. Soient x, y dans G. On a $(xy)^2 = xyxy = e$. En multipliant à gauche par x et à droite par y, on a $xxyxyy = xy$ soit $yx = xy$. Le groupe G est donc commutatif.
2. Puisque $a^2 = e$ et $a \neq e$, $\{e, a\} =< a >$ sous-groupe engendré par a. Par le théorème de Lagrange, l'ordre de ce sous-groupe divise l'ordre de G. Ainsi G est d'ordre pair.
3. On commence par vérifier que $H \cap aH$ est vide : si $x \in H \cap aH = \tilde{H}$ alors, il existe h_1, h_2 dans H tels que $x = h_1 = ah_2$. On en déduit que $a = h_1 h_2^{-1}$ et, puisque H est un sous-groupe de G, $x \in H$ d'où une contradiction. On a déja card $(\tilde{H}) = 2\text{card } H$. Montrons que c'est un sous groupe de G. Soit x, y dans $\tilde{H}$: on a $x = a^{\varepsilon_1} h_1$ et $y = a^{\varepsilon_2} h_2$ avec $h_1, h_2 \in H$ et ε_1 et ε_2 égaux à 0 (si dans H) ou 1 (si dans aH). On a alors, puisque G est commutatif et que $a^{-1} = a$, $xy^{-1} = a^{\varepsilon_1 - \varepsilon_2} h_1 h_2^{-1}$. Puisque $\varepsilon_1 - \varepsilon_2$ vaut 0, 1 ou -1, on a bien xy^{-1} dans $\tilde{H}$. On a montré que $\tilde{H}$ est un sous-groupe de G.
4. On part de $a \neq e$ et $H_1 = \{e, a\}$. Soit $H_1 = G$ et c'est fini, soit ce n'est pas le cas. Il existe $a_2 \in G$ mais pas dans H_1. On construit alors le sous-groupe $H_2 = H_1 \cup a_2 H_1$. On procède de proche en proche : une fois construit H_p sous-groupe de cardinal 2^p de G, soit $H_p = G$ soit ce n'est pas le cas et on construit alors de même un sous-groupe de G, $H_{p+1} = H_p + a_{p+1} H_p$ de cardinal 2^{p+1}. Puisque G est de cardinal fini, on finit par tomber sur G.
   Si on veut une version « plus propre », on peut $\mathscr{A}$ l'ensemble des sous-groupes d'ordre une puissance de 2 de G. On considère un sous-groupe de cardinal maximal dans $\mathscr{A}$. Si ce n'est pas G, on peut alors en construire un autre de cardinal double d'où une contradiction.
   Pour les plus motivés, on peut mettre une structure de $\mathbb{Z}/2\mathbb{Z}$espace vectoriel sur G (réfléchir comment...), utiliser une base $e_1, \ldots, e_k$ de G

pour obtenir que card G est 2^k.

5. Un élément de G est d'ordre 1 (le seul est e), 2, p ou $2p$. Si aucun élément est d'ordre p, tous les éléments de G différents de e sont d'ordre 2 ou $2p$. Si x est d'ordre $2p$ alors x^2 est d'ordre p ce qu'on a exclut. Finalement tous les éléments sont d'ordre 2 (sauf e) et G est de cardinal une puissance de 2. Si p est différent de 2 alors on a une contradiction. Il ne reste plus qu'à regarder le cas où $p = 2$ et G d'ordre 4. L'ordre d'un élément x différent de e est 2 (c'est fini, $p = 2$) ou 4 et dans ce dernier cas x^2 est d'ordre $p = 2$.

Exercice 10.12

1. → si $KH = HK$. Soit $hk, h'k' \in HK$: $(hk)(h'k')^{-}1 = h(kk'^{-1})h'^{-1}$. On a $kk'^{-1} \in H$ et h'^{-1} in K donc $(kk'^{-1})h'^{-1} \in HK = KH$. On peut le réécrire sous la forme $h''k''$ et enfin $(hk)(h'k')^{-}1 = hh''k'' \in HK$ donc HK sous-groupe de G.
   → si HK groupe. Soit $x \in KH$. Il existe $k \in K$ et $h \in H$ tel que $x = kh$. On a alors $h^{-1}k^{-1} \in HK$ et l'inverse, $kh = x$, est encore dans HK puisque HK est un groupe. On a donc $KH \subset HK$. Réciproquement si $x = hk \in HK$ alors c'est l'inverse d'un élément de HK : $x = (x^{-1})^{-1}$. Puisque $x^{-1} \in HK$, on peut l'écrire $x^{-1} = h'k'$ et alors $x = hk = (h'k')^{-1} = k'^{-1}h'^{-1} \in KH$. D'où $HK \subset KH$. Finalement $HK = KH$.
2. Tout d'abord il faut que $H \times K$ et HK soient des groupes. Le premier a une structure naturelle de groupe, le second est un sous-groupe de G si et seulement si $HK = KH$. Supposons avoir cette condition. Si $x = (h_1, k_1)$ et $y = (h_2, k_2)$ sont deux éléments de $H \times K$, on a $xy = (h_1h_2, k_1k_2)$ et on veut $f(xy) = f(x)f(y)$ soit $h_1h_2k_1k_2 = h_1k_1h_2k2$. Par simplification il faut et il suffit d'avoir $h_2k_1 = k_1h_2$ et ce pour tout $h_1 \in H$ et $k_2 \in K$. Une condition nécessaire et suffisante est donc $hk = kh$ pour tout $(h, k) \in H \times K$ (ce qui est a priori plus restrictif que $HK = KH$ mais qui entraîne cette condition).
   Soit $(h, k) \in H \times K$. On a $(h, k) \in \ker f$ si $hk = e$ donc $k = h^{-1}$ est dans H et K. Réciproquement tout élément (h, h^{-1}) avec $h \in H \cap K$ est dans le noyau. On en déduit que $\ker f = \{(h, h^{-1}), h \in H \cap K\}$. L'application est injective si et seulement si $H \cap K = \{e\}$. Elle est immédiatement surjective par définition de HK et dans ce cas elle est bijective.

Exercice 10.13

1. Soit H un sous-groupe de G, distinct de $\{e\}$. On note m le plus petit entier naturel non nul tel que $a^m \in H$. Comme H est un sous-groupe, le sous-groupe engendré par a^m est inclus dans H. Soit $x \in H$. Il existe un entier naturel k tel que $x = a^k$. Par division euclidienne de k par m, il existe deux entiers naturels j et r tels que $k = mj + r$ et $r \leqslant m - 1$. Comme H est un groupe et que $x \in H$, $x(a^m)^{-j} \in H$, c'est-à-dire $a^r \in H$, d'où $r = 0$ par minimalité de m, d'où $x = a^m j$ et $x \in H$. On a montré que H est cyclique engendré par a^m. Par division euclidienne de n par m, il existe deux entiers naturels q et s tels que $n = mq + s$ et $s \leqslant m - 1$. Comme $a^n = e$, on obtient $a^s = (a^m)^{-q}$, donc $a^s \in H$, d'où $s = 0$ par minimalité de m, donc m divise n.
2. Comme d divise n, il existe $m \in \mathbb{N}$ tel que $n = dm$. Montrons que le sous-groupe engendré par a^m est d'ordre d. On a $(a^m)^d = e$. S'il existe deux entiers k et j tels que $0 \leq j < k < d$ et $a^{km} = a^{jm}$, alors $(k - j)m \geqslant n$, ce qui est absurde car $k - j \leqslant d - 1$. Le sous-groupe engendré par a^m est donc formé des d éléments distincts a^{km} pour $0 \leqslant k \leqslant d - 1$. Inversement, si H est un sous-groupe de G de cardinal d, l'étude menée à la première question montre que H est engendré par $a^{n/d}$.
3. Nous sommes ici en notation additive. Soit $x \in [\![0; n-1]\!]$, l'élément $\overline{x}$ est d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si $\overline{dx} = \overline{0}$ et $\forall k \in [\![1; d-1]\!]$, $\overline{kx} \neq \overline{0}$. Cela équivaut à l'existence de $u \in [\![1; d-1]\!]$ premier avec d tel que $x = \frac{n}{d}u$. Par conséquent, $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(d)$ éléments d'ordre d. En partitionnant les éléments de $\mathbb{Z}/n\mathbb{Z}$ suivant leur ordre (qui doit diviser n), on en déduit que $n = \sum_{d|n} \varphi(d)$.

Exercice 10.14

1. Soient z et $z' \in G_p$; il existe deux entiers j et k tels que $z^{p^j} = 1$ et $z'^{p^k} = 1$, d'où $(zz')^{p^{\max(j,k)}} = 1$ et $(z^{-1})^{p^j} = 1$ donc zz' et $z^{-1} \in G_p$. Comme $1 \in G_p$, il en résulte que G_p est un sous-groupe de $\mathbb{C}^*$.
2. On note U_k le groupe multiplicatif des racines p^kièmes de l'unité dans $\mathbb{C}$. On rappelle que U_k est cyclique et que z est un générateur de U_k si, et seulement si z est de la forme $e^{2i\pi u/p^k}$ avec u premier avec p, autrement dit si, et seulement si $z \in U_k \setminus U_{k-1}$. On a $G_p = \bigcup_{k\in\mathbb{N}} U_k$, la suite d'ensembles (U_k) étant croissante pour l'inclusion. Soit G un sous-groupe propre de G_p. Si G contient un élément de $U_k \setminus U_{k-1}$, alors G contient U_k, donc tous les U_j pour $j \leqslant k$. Comme G n'est pas égal à G_p, l'ensemble des entiers k tels que G contienne un élément de $U_k \setminus U_{k-1}$ est majoré, donc possède un plus grand élément r. Cet élément engendre U_r, donc $G \supset U_r$. Mais par définition de r, $G \subset U_r$. Finalement, les sous-groupes propres de G_p sont les sous-groupes U_k ; ils sont tous cycliques, emboîtés les uns dans les autres, donc aucun n'est maximal.
3. Supposons que la famille $(z_1, \ldots, z_n)$ engendre G_p. Chaque élément z_k est d'ordre p^{α_k} où α_k est un entier naturel. En notant $\alpha = \max_{1\leqslant k\leqslant n} \alpha_k$, on a $z_k^{p^\alpha} = 1$ pour tout k, or tout élément z de G_p est un produit d'éléments de la forme z_i, donc on a également $z^{p^\alpha} = 1$, d'où $G_p \subset U_\alpha$, ce qui est absurde.

Exercice 10.17

Si A est un sous-groupe de G et B un sous-groupe de H, alors $A \times B$ est un sous-groupe de $G \times H$ Réciproquement montrons que tout sous-groupe T de $G \times H$ est de cette forme. Comme $p_1 : G \times H \to G, (x, y) \mapsto x$ et $p_2 : G \times H \to G, (x, y) \mapsto y$ sont des morphismes de groupes, $p_1(T) = A$ est un sous-groupe de G et $p_2(T) = B$ un sous-groupe de H. Évidemment $T \subseteq A \times B$ Comme A et B sont images de T par des morphismes surjectifs,

leurs cardinaux divisent $|T|$. Or $|A|$ et $|B|$ sont premiers entre eux, donc $|A| \times |B|$ divise $|T|$ et ainsi, $T = A \times B$. En conclusion, les sous-groupes de $G \times H$ sont les $A \times B$, où A est un sous-groupe de G et B un sous-groupe de H, d'où le résultat demandé.