

Correction des exercices - Chapitre II

Exercice 1

- 1) Soient x et y des éléments de G . On a $(xy)^2 = e$, d'où $xy = y^{-1}x^{-1} = yx$.
- 2) Supposons que G ne possède pas d'élément d'ordre 2. Soit A l'ensemble des éléments x de G qui sont distincts de x^{-1} . On a alors $G = A \cup \{e\}$, où e est l'élément neutre de G . Le cardinal de A est nécessairement pair, ce qui conduit à une contradiction, car e n'est pas dans A .
- 3) Soit y un élément de G . On les égalités

$$(y^{-1}xy)(y^{-1}xy) = y^{-1}x^2y = e.$$

Il en résulte que l'on a $y^{-1}xy = e$ ou bien $y^{-1}xy = x$ i.e. $xy = yx$. Le premier cas ne convient pas car x est distinct de e , d'où le résultat.

Exercice 2

Notons la loi interne de G additivement. Soient H et K des sous-groupes de G . Supposons H non contenu dans K , et K non contenu dans H . Il existe alors $x \in H \setminus K$ et y dans $K \setminus H$. L'élément $x + y$ n'est pas dans $H \cup K$, qui n'est donc pas un sous-groupe de G . Inversement, si l'un des sous-groupes est contenu dans l'autre, alors $H \cup K$ est H ou K , d'où l'assertion.

Exercice 3

- 1) L'ordre de $\bar{3}$ est $\frac{12}{\text{pgcd}(3,12)} = 4$ (cor. 2.2 du cours ; on peut aussi remarquer directement que $\bar{3}$ et $2\bar{3}$ sont non nuls et que l'on a $4\bar{3} = \bar{0}$).
- 2) Le sous-groupe de G engendré par $\bar{3}$ est $\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$.
- 3) Parce que G est cyclique d'ordre 12, l'ensemble des diviseurs positifs de 12 est en bijection avec l'ensemble des sous-groupes de G . Plus précisément, si d divise 12, il existe un unique sous-groupe H_d de G d'ordre d , et il est formé des éléments $x \in G$ tel que $dx = \bar{0}$ (cf. th. 2.4 du cours). On vérifie que l'on a

$$H_1 = \{\bar{0}\}, \quad H_2 = \{\bar{0}, \bar{6}\}, \quad H_3 = \{\bar{0}, \bar{4}, \bar{8}\}, \quad H_4 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\},$$

$$H_6 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}, \quad H_{12} = G.$$

- 4) Les générateurs de G sont les classes d'entiers $a + 12\mathbb{Z}$ avec $1 \leq a \leq 12$ et a premier avec 12 (cor. 2.4). Il y a quatre telles classes, qui sont $\bar{1}, \bar{5}, \bar{7}, \bar{11}$.

Exercice 4

- 1) Posons $G = \{x_1, \dots, x_n\}$. L'application de G dans G qui à x associe son opposé $-x$ est une bijection. Le groupe G étant abélien, on a donc

$$2S = S + S = (x_1 + \dots + x_n) + (-x_1 - \dots - x_n) = 0.$$

- 2) D'après le théorème de Lagrange, il n'existe pas d'éléments d'ordre 2 dans G . Parce que $2S = 0$, et que S n'est pas d'ordre 2, on obtient $S = 0$.
- 3) On a

$$\sum_{k=0}^{n-1} k = \frac{n(n-1)}{2}.$$

Par suite, S est la classe de $\frac{n(n-1)}{2}$ modulo n . Si n est impair, $\frac{n-1}{2}$ est un entier, d'où $S = 0$ (on pouvait aussi utiliser directement la question précédente dans ce cas). Supposons n pair. On a $n-1 \equiv -1 \pmod{n}$ et $-\frac{n}{2} \equiv \frac{n}{2} \pmod{n}$, d'où

$$S = \frac{n}{2} + n\mathbb{Z}.$$

Exercice 5

Si $H = \{0\}$ l'entier $n = 0$ convient. Supposons $H \neq \{0\}$. L'ensemble $A = H \cap \mathbb{N}^*$ n'est pas vide, car si n est dans H , alors $-n$ l'est aussi. Toute partie non vide de \mathbb{N} possède un plus petit élément. Soit n le plus petit élément de A . Vérifions que l'on a $H = n\mathbb{Z}$. Tout d'abord, H étant un sous-groupe de \mathbb{Z} , et n étant dans H , $n\mathbb{Z}$ est contenu dans H . Inversement, soit x un élément de H . On a $n \neq 0$. Il existe donc q et r dans \mathbb{Z} tels que $x = nq + r$ avec $0 \leq r < n$ (division euclidienne, th. 1.1). Parce que x et nq appartiennent à H , il en est de même de r . Le caractère minimal de n entraîne $r = 0$, donc x appartient à $n\mathbb{Z}$, d'où l'assertion. Par ailleurs, si l'on a $n\mathbb{Z} = m\mathbb{Z}$ avec m et n dans \mathbb{N} , alors m divise n et n divise m , d'où $m = n$.

Exercice 6

Soit n l'ordre de G . Pour tout $z \in G$, on a $z^n = 1$ (th. 2.3). Il en résulte que G est contenu dans le sous-groupe de \mathbb{C}^*

$$H = \left\{ \exp\left(\frac{2k\pi i}{n}\right) \mid k = 0, \dots, n-1 \right\}.$$

Parce que G et H ont le même ordre, on a donc $G = H$. Par ailleurs, H est cyclique engendré par $\exp\left(\frac{2\pi i}{n}\right)$, d'où l'assertion.

Exercice 7

- 1) Notons r (resp. s) l'ordre de x (resp. y), d l'ordre de (x, y) et posons $m = \text{ppcm}(r, s)$. On a $(x, y)^m = (x^m, y^m) = (e_1, e_2)$, où e_i est l'élément neutre de G_i , donc d divise m . Par ailleurs, on a $(x^d, y^d) = (x, y)^d = (e_1, e_2)$, donc r et s divisent d . Par suite, m divise d , d'où $m = d$.
- 2) L'ordre de $\bar{3}$ dans G_1 est $\frac{1200}{\text{pgcd}(3, 1200)} = 400$. L'ordre de $\bar{5}$ dans G_2 est $\frac{350}{\text{pgcd}(5, 350)} = 70$. On a $400 = 2^4 \times 5^2$ et $70 = 2 \times 5 \times 7$, d'où $\text{ppcm}(70, 400) = 2800$, qui est donc l'ordre cherché.

Exercice 8

- 1) Soit G un groupe fini d'ordre $2n - 1$. Pour tout $x \in G$, on a $x^{2n-1} = e$, où e est l'élément neutre de G , d'où les égalités $x = x^{2n} = (x^n)^2$.
- 2) Soit $f : G \rightarrow G$ l'application définie par $f(x) = x^2$. C'est un homomorphisme de groupes. Parce que G est cyclique d'ordre pair, G a un unique élément d'ordre 2 (th. 2.4). Le noyau de f est donc d'ordre 2. L'image de f est l'ensemble G^2 des carrés de G , donc G^2 est d'ordre $\frac{n}{2}$ (th. 2.7).
- 3) Soit H le sous-groupe de G formé des éléments x tels que $x^{\frac{n}{2}} = e$. Puisque G est cyclique, H est l'unique sous-groupe d'ordre $\frac{n}{2}$ de G (th. 2.4). D'après la question précédente, on a donc $G^2 = H$, d'où l'équivalence annoncée.
- 4) Supposons $n = 2^t$ avec $t \geq 1$. Le groupe G^2 est de cardinal 2^{t-1} et son complémentaire H dans G aussi. Par ailleurs, il y a exactement $\varphi(2^t) = 2^{t-1}$ générateurs dans G , où φ est la fonction indicatrice d'Euler (th. 2.5). L'ensemble des générateurs de G est contenu dans H , car l'ordre d'un carré divise $\frac{n}{2}$, ce qui entraîne le résultat.

On peut aussi procéder comme suit : soit x un élément de G qui n'est pas dans G^2 . Si y est un générateur de G , il existe m tel que $x = y^m$. L'entier m est impair, donc x est un générateur, car les générateurs de G sont les éléments de la forme y^k avec k premier avec l'ordre de G (th. 2.5). Inversement, un générateur de G n'étant pas un carré, on obtient l'assertion.

Exercice 9

- 1) Supposons que HK soit un sous-groupe de G . Soit hk un élément de HK . Cet élément possède un inverse uv dans HK . On a donc $hk = (uv)^{-1} = v^{-1}u^{-1}$ qui est donc dans KH . Cela montre que HK est contenu dans KH . Par ailleurs, soit kh un élément de KH . L'inverse de kh , qui est $h^{-1}k^{-1}$, appartient à HK . Puisque HK est un sous-groupe de G , kh est donc aussi dans HK . Ainsi KH est contenu dans HK , d'où l'égalité $HK = KH$.

Inversement, supposons $HK = KH$. L'élément neutre e est dans HK et si x est dans HK , il en est de même de x^{-1} . Considérons alors des éléments $u = ab$ et $v = cd$

dans HK . D'après l'hypothèse faite, on a $bc = fg$, où $f \in H$ et $g \in K$. On obtient $uv = (af)(gd) \in HK$. Cela prouve que HK est un sous-groupe de G .

2.1) Soit I la matrice identité de G . On vérifie que l'on a $M^2 \neq I$, ainsi que les égalités $M^4 = I$ et $N^3 = I$. Par suite, l'ordre de M est 4 et celui de N est 3.

2.2) On vérifie par récurrence que pour tout $n \in \mathbb{N}$, on a les égalités

$$(MN)^{2n} = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix},$$

$$(MN)^{2n+1} = \begin{pmatrix} -1 & -1 - 2n \\ 0 & -1 \end{pmatrix}.$$

Pour tout $n \geq 1$, on a donc $(MN)^n \neq I$, d'où le résultat.

2.3) Supposons que HK soit un sous-groupe de G . Les groupes H et K sont finis, donc tel est le cas de $H \times K$. Par ailleurs, l'application $H \times K \rightarrow HK$ qui au couple (h, k) associe hk est surjective. On en déduit que HK est un groupe fini. Cela conduit à une contradiction, car MN appartient à HK et MN est d'ordre infini.

Exercice 10

1) Notons

$$n = \prod_{i=1}^t p_i^{n_i},$$

la décomposition de n en produit de facteurs premiers. Le nombre de diviseurs de $p_i^{n_i}$ est $n_i + 1$. Il en résulte que l'on a

$$d(n) = \prod_{i=1}^t (n_i + 1).$$

2) L'entier n est un carré si et seulement si tous les exposants n_i sont pairs, ce qui signifie que $d(n)$ est impair (question 1).

3) On vérifie que l'ensemble des entiers $n \leq 30$ vérifiant l'égalité $d(n) = \varphi(n)$ est

$$\{1, 3, 8, 10, 18, 24, 30\}.$$

Exercice 11

On constate que $x_0 = \overline{10}$ est une solution particulière de l'équation proposée. On a $\text{pgcd}(5, 1000) = 5$. L'ensemble des solutions est donc (prop. 2.10)

$$S = \{x_0 + z \mid z \in \mathbb{Z}/1000\mathbb{Z} \text{ et } 5z = \overline{0}\}.$$

On vérifie alors que l'on a

$$S = \{\overline{10}, \overline{210}, \overline{410}, \overline{610}, \overline{810}\}.$$

Exercice 12

- 1) Soient a et b des éléments de G . Par hypothèse, on a $(ab)^{-1} = a^{-1}b^{-1}$. Par ailleurs, on a $(ab)^{-1} = b^{-1}a^{-1}$. Cela entraîne l'égalité $ab = ba$.
- 2) Soient a et b des éléments de G tels que l'on ait $f(a) = f(b)$. On a alors $ab^{-1} = \sigma(ab^{-1})$, ce qui, d'après l'hypothèse faite, implique $a = b$.
- 3) Puisque G est fini, l'application f est aussi surjective. Considérons x un élément de G . Il existe a dans G tel que $f(a) = x$, i.e. $\sigma(a^{-1})a = x$. En prenant l'image par σ des deux membres de cette égalité, on obtient $a^{-1}\sigma(a) = \sigma(x)$, d'où l'on déduit que $\sigma(x) = x^{-1}$. L'application $x \mapsto x^{-1}$ est donc un homomorphisme de groupes. D'après la première question, G est abélien.

Supposons que G soit d'ordre pair. Il existe un élément x d'ordre 2 dans G (exercice 1, question 2). On a alors $x^{-1} = x$ d'où $\sigma(x) = x$. Cela contredit le fait que e soit le seul point fixe de σ , donc G est d'ordre impair.

Exercice 13

- 1) Soit $f : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ un homomorphisme de groupes. On a les égalités

$$0 = f(\overline{m}) = f(m\overline{1}) = mf(\overline{1}).$$

Les entiers m et n étant premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $mu + nv = 1$. On a $umf(\overline{1}) = 0$. Par ailleurs, on a $vnf(\overline{1}) = 0$, d'où $f(\overline{1}) = 0$. Pour tout $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$, on a $\overline{a} = a\overline{1}$, d'où $f(\overline{a}) = af(\overline{1}) = 0$, et f est donc nul.

- 2) L'élément neutre appartient à H . Soient x, y des éléments de H . Parce que G est abélien, on a $m(x + y) = mx + my = 0$, donc $x + y$ est dans H . Par ailleurs, on a $m(-x) = -mx$, donc $-x$ est dans H . Ainsi H est un sous-groupe de G .
- 3) On a $mf(\overline{1}) = 0$, donc $f(\overline{1})$ est dans H , autrement dit, ψ est bien définie. On déduit directement de la définition de la structure de groupe sur $\text{Hom}(\mathbb{Z}/m\mathbb{Z}, G)$, que ψ est un homomorphisme de groupes. Si $f \in \text{Hom}(\mathbb{Z}/m\mathbb{Z}, G)$ vérifie la condition $f(\overline{1}) = 0$, alors pour tout $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$, on a $f(\overline{a}) = 0$ i.e. f est nul, donc ψ est injectif. Vérifions que ψ est surjectif. Soit x un élément de H . Pour tout $\overline{k} \in \mathbb{Z}/m\mathbb{Z}$, posons $f(\overline{k}) = kx$. On obtient ainsi une application de $\mathbb{Z}/m\mathbb{Z}$ à valeurs dans G : en effet, si $\overline{k'} = \overline{k}$, il existe $t \in \mathbb{Z}$ tel que $k' = k + mt$, d'où $k'x = kx$ car x est dans H . L'application f est un homomorphisme de groupes et l'on a $\psi(f) = x$, d'où notre assertion.
- 4) Montrons que l'on a

$$H = \{x \in \mathbb{Z}/n\mathbb{Z} \mid dx = 0\}.$$

Soit x un élément de H . On a $mx = nx = 0$. Il existe $u, v \in \mathbb{Z}$ tels que $um + vn = d$, d'où $dx = 0$. Inversement, soit x un élément de G tel que $dx = 0$. Il existe $k \in \mathbb{Z}$ tel que $m = kd$. On obtient $mx = 0$ et x est dans H , d'où l'égalité annoncée. On a $n \neq 0$, donc $\mathbb{Z}/n\mathbb{Z}$ est fini cyclique, ce qui implique le résultat (th. 2.4).

- 5) C'est une conséquence des deux questions précédentes.
- 6) Le groupe $\text{Hom}(\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/6\mathbb{Z})$ est d'ordre 2. On a ici $H = \{0, \bar{3}\}$. Si f est l'homomorphisme non nul, on en déduit que $f(\bar{1}) = \bar{3}$ (car $f(\bar{1})$ est dans H). Il s'agit donc de l'application définie par

$$f(k + 8\mathbb{Z}) = 3k + 6\mathbb{Z}.$$

Indépendamment de ce qui précède, on peut aussi procéder directement : soit f un homomorphisme de $\mathbb{Z}/8\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$. On a $8f(\bar{1}) = 6f(\bar{1}) = 0$, d'où $2f(\bar{1}) = 0$. Si $f(\bar{1}) = 0$, f est nul, sinon $f(\bar{1}) = \bar{3}$ et on retrouve le résultat.
