Planche n° 1. Structures. Corrigé

Exercice n° 1

Soit $x \in G$. Pour $y \in G$, posons $\sigma_x(y) = xy$. σ_x est une application de G dans lui-même. Ensuite, pour tout $y \in G$, $\sigma_x \circ \sigma_{x^{-1}}(y) = xx^{-1}y = y$ et $\sigma_{x^{-1}} \circ \sigma_x(y) = x^{-1}xy = y$. Donc, $\sigma_x \circ \sigma_{x^{-1}} = \sigma_{x^{-1}} \circ \sigma_x = Id_G$. On sait alors que σ_x est une bijection de G sur lui-même ou encore une permutation de G (et de plus, $(\sigma_x)^{-1} = \sigma_{x^{-1}}$).

Soit $\varphi : \begin{array}{ccc} G & \rightarrow & S(G) \\ x & \mapsto & \sigma_x \end{array}$. D'après ce qui précède, φ est une application de G vers $S(G)$.

Vérifions que φ est un morphisme de groupes, du groupe $(G, \times)$ vers le groupe $(S(G), \circ)$. Soit $(x, x') \in G^2$. Pour tout $y \in G$,

$$(\varphi(x \times x'))(y) = \sigma_{xx'}(y) = xx'y = \sigma_x \circ \sigma_{x'}(y) = (\varphi(x) \circ \varphi(x'))(y)$$

et donc $\varphi(x \times x') = \varphi(x) \circ \varphi(x')$. On a montré que φ est un morphisme du groupe $(G, \times)$ vers le groupe $(S(G), \circ)$.

Montrons que φ est injectif. On note e l'élément neutre de G. Soit $x \in G$.

$$\begin{aligned} x \in \text{Ker}(\varphi) &\Rightarrow \varphi(x) = Id_G \Rightarrow \forall y \in G,\ xy = y \Rightarrow xe = e \\ &\Rightarrow x = e. \end{aligned}$$

Donc, $\text{Ker}(\varphi) = \{e\}$ puis φ est injectif.

On sait alors que $\varphi(G)$ est un sous-groupe de $(S(g), \circ)$. De plus, puisque φ est un morphisme injectif, φ réalise un isomorphisme du groupe $(G, \times)$ sur le groupe $(\varphi(G), \circ)$.

Exercice n° 2

1) $0 = 0 + 0i \in \mathbb{Z}[i]$. Soit $(z, z') \in (\mathbb{Z}[i])^2$. Posons $z = a + ib$ et $z' = a' + ib'$ où $(a, b, a', b') \in \mathbb{Z}^4$.
Alors, $z - z' = (a - a') + i(b - b') \in \mathbb{Z}[i]$ et $z \times z' = (aa' - bb') + i(ab' + ba') \in \mathbb{Z}[i]$. Enfin, $1 = 1 + 0i \in \mathbb{Z}[i]$.
Donc, $\mathbb{Z}[i]$ est un sous-anneau de l'anneau $(\mathbb{C}, +, \times)$.

2) Pour $x \in \mathbb{R}$, on pose $\nu(x) = \lfloor x \rfloor$ si $\lfloor x \rfloor \leqslant x \leqslant \lfloor x \rfloor + \dfrac{1}{2}$ et $\nu(x) = \lfloor x \rfloor + 1$ si $\lfloor x \rfloor + \dfrac{1}{2} < x < \lfloor x \rfloor + 1$ (où $\lfloor x \rfloor$ est la partie entière du réel x). Pour tout réel x, $\nu(x)$ est un entier relatif tel que $|x - \nu(x)| \leqslant \dfrac{1}{2}$.

Soit $(z, z') \in \mathbb{Z}[i] \times (\mathbb{Z}[i] \setminus \{0\})$. Soient $a = \nu\left(\text{Re}\left(\dfrac{z}{z'}\right)\right)$ et $b = \nu\left(\text{Im}\left(\dfrac{z}{z'}\right)\right)$. Soient $q = a + ib$ puis $r = z - qz'$. Alors, $q \in \mathbb{Z}[i]$ puis $r = z - qz' \in \mathbb{Z}[i]$ puis $z = qz' + r$.

Il reste à vérifier que $|r| < |z'|$ ou encore que $\left|\dfrac{r}{z'}\right| < 1$.

$$\begin{aligned} \left|\frac{r}{z'}\right| &= \left|\left(\text{Re}\left(\frac{z}{z'}\right) - a\right) + i\left(\text{Im}\left(\frac{z}{z'}\right) - b\right)\right| = \sqrt{\left(\text{Re}\left(\frac{z}{z'}\right) - a\right)^2 + \left(\text{Im}\left(\frac{z}{z'}\right) - b\right)^2} \\ &\leqslant \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \frac{1}{\sqrt{2}} < 1. \end{aligned}$$

On a montré que pour tout $(z, z') \in \mathbb{Z}[i] \times (\mathbb{Z}[i] \setminus \{0\})$, il existe $(q, r) \in (\mathbb{Z}[i])^2$ tel que $z = qz' + r$ et $|r| < |z'|$ (division euclidienne dans l'anneau des entiers de Gauss).

3) Soit $z_0 \in \mathbb{Z}[I]$. Soit $I = z_0\mathbb{Z}[i] = \{z_0 z,\ z \in \mathbb{Z}[i]\}$. Redémontrons que I est un idéal de l'anneau $(\mathbb{Z}[i], +, \times)$ (idéal principal engendré par z_0).

$0 = z_0 \times (0 + 0i) \in I$. Soit $(z, z') \in (\mathbb{Z}[i])^2$. $z_0 z - z_0 z' = z_0(z - z') \in I$ car $z - z' \in \mathbb{Z}[i]$. Enfin, pour $(z, z') \in \mathbb{Z}[i])^2$, $(z_0 z)\, z' = z_0(zz') \in I$ car $zz' \in \mathbb{Z}[i]$.

Vérifions que maintenant que tout idéal de l'anneau $(\mathbb{Z}[i], +, \times)$ est principal. Si $I = \{0\}$, alors $I = 0 \times \mathbb{Z}[i]$ est principal.

Dorénavant, I est un idéal non réduit à $\{0\}$ de l'anneau $(\mathbb{Z}[i], +, \times)$. Soit $z \in I \setminus \{0\}$. Posons $z = a + ib$ où $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. L'ensemble $\mathscr{D} = \left\{a' + ib' \in I /\ 0 < \sqrt{a'^2 + b'^2} \leqslant \sqrt{a^2 + b^2}\right\}$ est non vide et fini (de cardinal inférieur ou égal à $(2|a| + 1) \times (2|b| + 1)$). Il existe donc un élément z_0 de $\mathscr{D}$ de plus petit module. Par construction, $z_0 \neq 0$, $z_0 \in I$ et le module de z_0 est inférieur ou égal au module de tout élément de I (que ce module soit inférieur ou égal ou strictement supérieur à $\sqrt{a^2+b^2}$).

Montrons que $I = z_0\mathbb{Z}[i]$. D'une part, pour tout $z \in \mathbb{Z}[i]$, $z_0 z \in I$ puisque $z_0 \in I$ et par définition d'un idéal. Donc, $z_0\mathbb{Z}[i] \subset I$.
Inversement, soit $z \in I$. D'après la question 2), puisque $z_0 \neq 0$, il existe $(q,r) \in (\mathbb{Z}[i])^2$ tel que $z = qz_0 + r$ et $|r| < |z_0|$. Mais $r = z - qz_0$ est dans I et donc $r = 0$ par définition de z_0. Par suite, $z = qz_0 \in z_0\mathbb{Z}[i]$. Ceci montre que $I \subset z_0\mathbb{Z}[i]$ et finalement que $I = z_0\mathbb{Z}[i]$.

On a montré que tout idéal de l'anneau $(\mathbb{Z}[i], +, \times)$ est principal et donc que l'anneau $(\mathbb{Z}[i], +, \times)$ est principal.

Exercice nº 3

1) Soit $z \in \mathbb{C}$. z est un élément d'ordre fini du groupe $(\mathbb{C}, +)$ si et seulement si il existe $n \in \mathbb{N}^*$ tel que $nz = 0$. Ceci équivaut à $z = 0$.

2) Soit $z \in \mathbb{C}$. z est un élément d'ordre fini du groupe $(\mathbb{C}^*, \times)$ si et seulement si il existe $n \in \mathbb{N}^*$ tel que $z^n = 1$. Les éléments d'ordre fini du groupe $(\mathbb{C}^*, \times)$ sont les racines n-èmes de l'unité pour $n \in \mathbb{N}^*$.
L'ensemble de ces nombres est $\displaystyle\bigcup_{n\in\mathbb{N}^*} U_n$ (et n'est pas U).

Exercice nº 4

On note e l'élément neutre de G. Soit $x \in G$. On sait que l'ordre de x divise le cardinal de G. Puisque $\text{card}(G)$ est un nombre impair, l'ordre de x est un nombre impair. Notons donc $2p+1$, $p \in \mathbb{N}$, l'ordre de x. Alors, $x^{2p+1} = e$ puis $x^{2p+2} = x$ ou encore $x = \left(x^{p+1}\right)^2 = f\left(x^{p+1}\right)$.

Ainsi, pour tout $x \in G$, il existe $x' \in G$ tel que $f(x') = x$. Donc, f est surjective. f est surjective de l'ensemble fini G sur lui-même et donc f est bijective.

Ainsi, par exemple, si $G = U_{2p+1}$ est le groupe des racines $2p+1$-èmes de l'unité dans $\mathbb{C}$, si deux racines $2p+1$-èmes de l'unité ont le même carré, alors elles sont égales (ce n'est par exemple par le cas dans U_4 puisque $(-i)^2 = i^2 = -1$) et toute racine $2p+1$-ème de l'unité est le carré d'une racine $2p+1$-ème de l'unité.

Exercice nº 5

1) Soient $(x,y) \in A^2$ et $(\lambda,\mu) \in \mathbb{R}^2$. $f_a(\lambda x + \mu y) = a(\lambda x + \mu y) = \lambda a x + \mu a y = \lambda f_a(x) + \mu f_a(y)$. Donc, $f_a \in \mathscr{L}(A)$. Soit $a \in A \setminus \{0\}$. Pour $x \in A$,

$$x \in \text{Ker}\,(f_a) \Rightarrow ax = 0 \Rightarrow x = 0 \text{ (car l'algèbre } (A, +, ., \times) \text{ est intègre).}$$

Donc, $\text{Ker}\,(f_a) = \{0\}$ puis $f_a \in GL(A)$ car $\dim(A) < +\infty$. En particulier, il existe $a' \in A$ tel que $aa' = f_a(a') = 1$. a est donc inversible à droite dans l'algèbre $(A, +, ., \times)$. De même, a est inversible à gauche. Soit a'' son inverse à gauche. Alors, $a'' = a''aa' = a'$ et donc a est inversible pour $\times$.

D'autre part, si $a = 0$, a n'est pas inversible pour $\times$ (car 0 est absorbant pour $\times$ et donc, pour tout $x \in A$, $0 \times x \neq 1$). On a montré que : $\forall a \in A$, a inversible pour $\times$ si et seulement si $a \neq 0$. Mais alors, $(A, +, \times)$ est un corps.

2) a) Soit $n = \dim_{\mathbb{R}}(A)$ ($n \in \mathbb{N} \setminus \{0,1\}$). La famille $\left(a^k\right)_{0\leqslant k\leqslant n}$ est de cardinal $n+1 > n = \dim(A)$. Donc, la famille $\left(a^k\right)_{0\leqslant k\leqslant n}$ est liée. On en déduit qu'il existe $(\lambda_0, \ldots, \lambda_n) \in \mathbb{R}^{n+1}$ tel que $(\lambda_0, \ldots, \lambda_n) \neq (0, \ldots, 0)$ et $\lambda_n a^n + \ldots + \lambda_1 a + \lambda_0 = 0$. Le polynôme $P_0 = \displaystyle\sum_{k=0}^{n} \lambda_k X^k$ est un polynôme non nul tel que $P_0(a) = 0$.

b) Soit $I = \{P \in \mathbb{K}[X]/\ P(a) = 0\}$. Montrons que I est un idéal de l'anneau $(\mathbb{R}[X], +\infty)$. $0 \in I$ puis si $(P,Q) \in I^2$, $(P-Q)(a) = P(a) - Q(a) = 0$ et donc $P - Q \in I$. Soit $(P,Q) \in \mathbb{R}[X] \times I$. $(PQ)(a) = P(a) \times Q(a) = P(a) \times 0 = 0$ et donc $PQ \in I^2$. I est donc un idéal de l'anneau $(\mathbb{R}[X], +, \times)$.

Puisque l'anneau $(\mathbb{R}[X], +, \times)$ est un anneau principal, I est un idéal principal de cet anneau. Plus précisément, puisque $I \neq \{0\}$ d'après la question a), on sait qu'il existe un polynôme unitaire μ_a et un seul tel que $I = \mu_a\mathbb{R}[X]$. μ_a est le polynôme minimal de a.

c) Soit $(P,Q) \in (\mathbb{R}[X])^2$ tel que $\mu_a = P \times Q$. Alors $P(a)Q(a) = \mu_a(a) = 0$ et donc $P(a) = 0$ ou $Q(a) = 0$ car l'anneau $(A, +, \times)$ est intègre. Donc, $P \in I \setminus \{0\}$ ou $Q \in I \setminus \{0\}$ (car $P \times Q = \mu_a \neq 0$). Mais alors, $\deg(P) \geqslant \deg(\mu_a)$ ou $\deg(Q) \geqslant \deg(\mu_a)$. Ceci montre que μ_a est irréductible sur $\mathbb{R}[X]$.

3) Soit $a \in A \setminus (\text{Vect}(1))$ (a existe car $\dim(A) \geqslant 2$). μ_a est irréductible sur $\mathbb{R}[X]$. Donc, μ_a est de degré 1 ou 2. $\deg(\mu_a) = 1$ fournit $\mu_a = X - a$ et en particulier $a \in \mathbb{R} = \text{Vect}(1)$ ce qui est faux. Donc, $\deg(\mu_a) = 2$ puis il existe $(\alpha,\beta) \in \mathbb{R}^2$ tel que $\mu_a = X^2 + \alpha X + \beta$ avec $\alpha^2 - 4\beta < 0$. Ceci fournit en particulier $a^2 + \alpha a + \beta = 0$ puis $\left(a + \dfrac{\alpha}{2}\right)^2 = -\dfrac{4\beta - \alpha^2}{4}$ puis

$\left(\dfrac{2a+\alpha}{\sqrt{4\beta-\alpha^2}}\right)^2=-1$. Soit $a_0=\dfrac{2a+\alpha}{\sqrt{4\beta-\alpha^2}}$. a_0 est un élément de A tel que $a_0^2=-1$. De plus, $a_0\notin \text{Vect}(1)$ car aucun élément de $\text{Vect}(1)$ n'a un carré égal à -1 et donc la famille $(1,a_0)$ est libre.

Soit $b\in A$. Si $b\in\text{Vect}(1)$, alors $b\in\text{Vect}\,(1,a_0)$. Sinon $b\in A\setminus\text{Vect}(1)$. Comme précédemment, il existe $(\alpha',\beta')\in\mathbb{R}^2$ tel que on construit $\alpha'^2-4\beta'<0$ et $b^2+\alpha'b+\beta'=0$ puis $b_0=\dfrac{2b+\alpha'}{\sqrt{4\beta'-\alpha'^2}}$ est un élément de A tel que $b_0^2=-1$. Mais alors, $a_0^2=b_0^2$ puis $(b_0+a_0)(b_0-a_0)=0$ et donc $b_0=a_0$ ou $b_0=-a_0$ car l'anneau $(A,+,\times)$ est intègre. Dans, tous les cas, $b_0\in\text{Vect}\,(1,a_0)$ puis $b=\dfrac{1}{2}\left(-\alpha'+\sqrt{4\beta'-\alpha'^2}b_0\right)\in\text{Vect}\,(1,b_0)\subset\text{Vect}\,(1,a_0)$.

Ceci montre que $A=\text{Vect}\,(1,a_0)=\left\{x+a_oy,\ (x,y)\in\mathbb{R}^2\right\}$ puis que $\dim(A)=2$ car $(1,a_0)$ est une base de A. Puisque $a_0^2=-1$, il est immédiat que l'application $\begin{array}{cccc}\varphi: & \mathbb{C} & \rightarrow & A\\ & x+iy & \mapsto & x+a_0y\end{array}$ est un isomorphisme d'algèbres.

Exercice n° 6 On note e l'élément neutre du groupe $(G,\times)$.

$(1)\Rightarrow(4)$. Supposons que HK soit un sous-groupe de $(G,\times)$.
Soit $(h,k)\in H\times K$. On a $kh=\left(h^{-1}k^{-1}\right)^{-1}$. Mais $h^{-1}\in H$ et $k^{-1}\in K$ puis $h^{-1}k^{-1}\in HK$ puis $\left(h^{-1}k^{-1}\right)^{-1}\in HK$ car HK est un sous-groupe. Ainsi, pour tout $(h,k)\in H\times K$, $kh\in HK$. Ceci montre que $KH\subset HK$.

$(4)\Rightarrow(1)$. Supposons que $KH\subset HK$. e est dans H et e est dans K et donc $e=e\times e\in HK$. Soit $(h,k,h',k')\in H\times K\times H\times K$. $(hk)\times(h'k')^{-1}=hkk'^{-1}h'^{-1}$. Ensuite, k'^{-1} est dans K et h'^{-1} est dans H. Donc, $kk'^{-1}h'^{-1}$ est dans $KH\subset HK$ puis il existe $(h'',k'')\in H\times K$ tel que $kk'^{-1}h'^{-1}=h''k''$. Mais alors,

$$(hk)\times(h'k')^{-1}=(hh'')k''\in HK.$$

Ceci montre que HK est un sous-groupe de $(G,\times)$.

On a montré que $(1)\Leftrightarrow(4)$. En échangeant les rôles de H et K, on a aussi $(2)\Leftrightarrow(3)$.

$(3)\Rightarrow(4)$. Supposons $HK\subset KH$. Soit $(h,k)\in H\times K$. $(kh)^{-1}=h^{-1}k^{-1}$ est dans HK et donc dans KH. Mais alors, $kh=\left((kh)^{-1}\right)^{-1}$ est dans HK. Ceci montre que $KH\subset HK$. En échangeant les rôles H et K, on a aussi $(4)\Rightarrow(3)$ et finalement, $(3)\Leftrightarrow(4)$.

On a montré que $(1)\Leftrightarrow(2)\Leftrightarrow(3)\Leftrightarrow(4)$.

Exercice n° 7

Par hypothèse, il existe $n\in\mathbb{N}^*$ tel que $(xy)^n=0$. Mais alors, $(yx)^{n+1}=y(xy)^nx=0$ et donc yx est nilpotent.

Exercice n° 8

Si $I=A$, alors $1\in I$. Inversement, si $1\in I$, alors pour tout $a\in A$, $a=1\times a\in I$ et donc $A\subset I$ puis $A=I$.

Exercice n° 9

Exercice n° 10

Exercice n° 11

Exercice n° 12