Feuille n°1.

Corrigé de l'exercice 6.

On cherche les morphismes de groupes $\varphi : \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$. Soit $d := \text{pgcd}(m, n)$. Puisque $\varphi(\overline{1}+\overline{1}) = \varphi(\overline{1}) + \varphi(\overline{1})$, le morphisme φ est caractérisé par l'image $\varphi(\overline{1})$. En particulier, on a $\varphi(\overline{m}) = m\varphi(\overline{1})$ et comme $\overline{m} = \overline{0}$ dans $\mathbf{Z}/m\mathbf{Z}$, on doit avoir $\overline{(m\varphi(\overline{1}))} = \overline{0}$ dans $\mathbf{Z}/n\mathbf{Z}$. En d'autres termes on veut n divise $m\varphi(\overline{1})$ et c'est le cas si et seulement si $\frac{n}{d}$ divise $\varphi(1)$. On voit donc qu'il existe exactement d morphismes de groupes $\varphi : \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$, ils sont donnés par $\varphi_\lambda : x \mapsto \lambda \cdot x$ pour $\lambda \in \{0, \frac{n}{d}, \dots, (d-1)\frac{n}{d}\}$.

Morphismes injectifs. Parmi ces morphismes φ_λ, déterminons ceux qui sont injectifs. Si m ne divise par n, alors l'élément non nul $\overline{n}$ de $\mathbf{Z}/m\mathbf{Z}$ s'envoie sur $\lambda \cdot \overline{n} = \lambda \cdot \overline{0} = \overline{0}$ dans $\mathbf{Z}/n\mathbf{Z}$ et aucun morphisme φ_λ n'est injectif. Si m divise n, alors $d = m$ et on cherche les éléments λ de $\{0, \frac{n}{m}, \dots, (m-1)\frac{n}{m}\}$ tels que

$$\{k \in \mathbf{Z} \mid \lambda \cdot k = 0 \bmod n\} = m\mathbf{Z}. \tag{1}$$

Si k est dans $m\mathbf{Z}$, on a toujours $\lambda \cdot k = 0 \bmod n$ car λ est de la forme $i\frac{n}{m}$ pour $i \in [|0, m-1|]$. Quelque soit λ, on a donc toujours $m\mathbf{Z} \subset \{k \in \mathbf{Z} \mid \lambda \cdot k = 0 \bmod n\}$ et on cherche à quelles conditions sur λ l'inclusion inverse reste vraie. On a les cas suivants :

- Supposons i est dans $(\mathbf{Z}/m\mathbf{Z})^\times$. Si $i \cdot \frac{n}{m} \cdot k = 0 \bmod n$, alors il existe un entier q tel que $nmq = ink$ donc $mq = ik$ et puisque i est premier à m, on obtient que m divise k. Donc si i est dans $(\mathbf{Z}/m\mathbf{Z})^\times$ et $\lambda = i\frac{n}{m}$ on a l'égalité (1).
- Si $d_0 := \text{pgcd}(i, m) \neq 1$ alors on peut écrire $m = d_0 \cdot m'$ et $i = d_0 \cdot i'$ avec m' et i' premiers entre eux. Si on considère l'élément $k := m'$, cet élément n'est pas dans $m\mathbf{Z}$ mais on vérifie que k est dans $\{k \in \mathbf{Z} \mid i \cdot \frac{n}{m} \cdot k = 0 \bmod n\}$: on a en effet

$$i \cdot \frac{n}{m} \cdot k = d_0 i' \cdot \frac{n}{m} \cdot m' = i' \cdot n \cdot \frac{d_0 m'}{m} = i' \cdot n = 0 \bmod n.$$

  On a donc montré que si i n'est pas dans $(\mathbf{Z}/m\mathbf{Z})^\times$ et $\lambda = i\frac{n}{m}$, alors l'inclusion $m\mathbf{Z} \subset \{k \in \mathbf{Z} \mid \lambda \cdot k = 0 \bmod n\}$ est strict.

En conclusion, on a obtenu que l'égalité (1) est vraie si et seulement si $\lambda = i\frac{n}{m}$ avec i dans $(\mathbf{Z}/m\mathbf{Z})^\times$. On a donc finalement $\varphi(m)$ morphismes injectifs de $\mathbf{Z}/m\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ si m divise n et aucun morphisme injectif de $\mathbf{Z}/m\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ sinon.

Morphismes surjectifs. Si $\varphi_\lambda : \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ est surjectif alors on doit avoir $\frac{m}{|\text{Ker}(\varphi)|} = n$ et donc n divise m. Dans ce cas on a $d = n$ et on cherche les éléments λ de $\{0, \frac{n}{m}, \dots, (n-1)\frac{n}{m}\}$ tels que tout élément y de $\mathbf{Z}/n\mathbf{Z}$ s'écrit $\lambda \cdot x$ avec x dans $\mathbf{Z}/n\mathbf{Z}$. Il suffit donc que λ soit un générateur de $\mathbf{Z}/n\mathbf{Z}$ i.e. λ est dans $(\mathbf{Z}/n\mathbf{Z})^\times$. On obtient donc $\varphi(n)$ morphismes surjectifs de $\mathbf{Z}/m\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ si n divise m et aucun morphisme surjectif de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{Z}/m\mathbf{Z}$ sinon.

Feuille n°2.

Corrigé de l'exercice 5.

(1) On peut supposer $|\alpha| > 1$ (sinon, c'est immédiat). Notons $M := \max_{i=0}^{n} \left(\left| \frac{a_i}{a_n} \right| \right)$. Partons de la relation $\alpha^n = \sum_{i=0}^{n-1} \frac{a_i}{a_n} \alpha^i$. Alors

$$|\alpha|^n \leq M \sum_{i=0}^{n-1} |\alpha|^i = M \frac{1-|\alpha|^n}{1-|\alpha|} \leq M \frac{|\alpha|^n}{|\alpha|-1} \ .$$

On simplifie par $|\alpha|^n$ pour obtenir $1 \leq \frac{M}{|\alpha|-1}$, d'où le résultat.

(2) De l'inégalité $|x-\alpha| < 1$, il vient $|x| < 1 + |\alpha| \leq M + 2$. Alors $|P'(x)| = |na_n x^{n-1} + \cdots + a_1| \leq n|a_n|(M+2)^{n-1} + \cdots + |a_1| =: C$.

(3) On suppose $\alpha \notin \mathbf{Q}$, donc P est de degré $n > 1$. On en déduit que $P(\frac{p}{q})$ est non nul, sinon on aurait que $(X - \frac{p}{q})$ divise P dans $\mathbf{Q}[X]$ et on a supposé P irréductible. On obtient que $q^n P(\frac{p}{q})$ est un entier non nul et donc $|q^n P(\frac{p}{q})| \geq 1$. On applique ensuite le théorème des accroissements finis : il existe c compris entre α et $\frac{p}{q}$ tel que $|P(\frac{p}{q})| = |P(\frac{p}{q}) - P(\alpha)| = |P'(c)| \cdot |\alpha - \frac{p}{q}|$. Comme on a supposé que $\frac{p}{q}$ est dans $]\alpha - 1, \alpha + 1[$, on voit que c est aussi dans $]\alpha - 1, \alpha + 1[$ et on peut donc appliquer la question précédente à $|P'(c)|$. On obtient les inégalités

$$\frac{1}{q^n} \leq |P(\frac{p}{q})| \leq C \cdot |\alpha - \frac{p}{q}|,$$

ce qui termine la preuve.

(4) À noter que α est bien défini (la série converge dans R). On rappelle qu'un nombre réel est rationnel si et seulement si, son développement décimal est périodique à partir d'un certain rang. Ce qui n'est pas le cas pour $\alpha = \sum_{k \geq 1} \frac{1}{10^{k!}}$.

(5) Supposons alors α algébrique sur $\mathbf{Q}$ et considérons le polynôme minimal $P := \mathrm{Irr}(\alpha, \mathbf{Q})$ de α sur $\mathbf{Q}$. Notons $\alpha_m := \sum_{k=1}^{m} \frac{1}{10^{k!}}$. On peut écrire $\alpha_m = \frac{p_m}{q_m}$ avec $q_m = 10^{m!}$. Puisque α n'est pas dans $\mathbf{Q}$, par les questions précédentes, il existe C, ne dépendant que de P, tel que pour $m \geq 1$, $|\alpha - \alpha_m| \geq 1/(C10^{nm!})$. On obtient ainsi, pour tout entier $m \geq 1$

$$\frac{2}{10^{(m+1)!}} \geq \frac{1}{C10^{nm!}} \quad \text{c'est-à-dire} \quad 2C \geq \frac{10^{(m+1)!}}{10^{nm!}},$$

et le terme de droite tend vers $+\infty$ quand m tend vers $+\infty$, d'où une contradiction.

Feuille n°3.

Corrigé de l'exercice 9.

(1) On note b_q la forme bilinéaire symétrique associée à q. On a alors

$$q(x+y) = q(x) + q(y) + 2b_q(x,y) \quad \text{ et } q(x-y) = q(x) + q(y) - 2b_q(x,y).$$

En faisant la somme, on obtient

$$q(x+y) + q(x-y) = 2(q(x) + q(y)).$$

(2) Si le corps de base est $\mathbf{C}$, on peut considérer par exemple le produit scalaire hermitien sur l'espace vectoriel $\mathbf{C}^n$ et l'application $q : \mathbf{C}^n \to \mathbf{C}$ associée :

$$\langle x, y\rangle = \sum_{i=1}^{n} \overline{x}_i y_i \quad \text{ et } \quad q(x) = \sum_{i=1}^{n} |x_i|^2.$$

Cette application n'est pas une forme quadratique sur $\mathbf{C}$ car on a $q(\lambda \cdot x) = |\lambda|^2 x$ pour tout λ dans $\mathbf{C}$ et x dans $\mathbf{C}^n$, mais elle vérifie bien l'égalité du parallélogramme.

(3) On se place sur R et on considère $q : V \to \mathrm{R}$ qui satisfait l'égalité du parallélogramme. On veut calculer $b(x+y, z)$ en fonction de $b(x,z)$ et $b(y,z)$ et on a

$$\begin{aligned} 2b(x+y,z) &= q(x+y+z) - q(x+y) - q(z) \\ 2b(x,z) &= q(x+z) - q(x) - q(z) \\ 2b(y,z) &= q(y+z) - q(y) - q(z). \end{aligned} \tag{2}$$

On cherche donc à écrire $q(x+y+z)$ en fonction de $q(x+y), q(x+z), q(y+z), q(x), q(y), q(z)$. Pour cela on considère les égalités suivantes :

$$\begin{aligned} q(x+y+z) + q(x-y+z) &= 2(q(x+z) + q(y)) \\ q(x+y+z) + q(-x+y+z) &= 2(q(y+z) + q(x)) \\ q(x-y+z) + q(-x+y+z) &= 2(q(x-y) + q(z)). \end{aligned}$$

On fait ensuite $L_1 + L_2 - L3$, on divise par 2 et on obtient

$$q(x+y+z) = q(x+z) + q(y+z) - q(x-y) + q(y) + q(x) - q(z).$$

Mais on a aussi

$$q(x-y) = 2(q(x) + q(y)) - q(x+y),$$

donc on obtient finalement :

$$q(x+y+z) = q(x+z) + q(y+z) + q(x+y) - q(y) - q(x) - q(z). \tag{3}$$

En remplaçant $q(x+y+z)$ dans la première ligne de (2) par la formule (3), on obtient bien

$$b(x+y,z) = b(x,z) + b(y,z).$$

On vient de montrer que b est additive à gauche. On vérifie facilement que b est symétrique et on en déduit l'additivité à droite. Il reste à voir que b est R-bilinéaire.

Puisque b est additive on a pour tout n de $\mathbf{Z}$, $b(n \cdot x, y) = n \cdot b(x, y)$. On en déduit que si n est non nul,

$$n \cdot b(\frac{x}{n}, y) = b(x, y) \quad \text{ i.e. } b(\frac{x}{n}, y) = \frac{1}{n} b(x, y).$$

Et, en utilisant une nouvelle fois l'additivité, on obtient pour tout rationnel $\frac{p}{q}$ dans $\mathbf{Q}$,

$$b(\frac{p}{q}x, y) = \frac{p}{q} b(x, y). \tag{4}$$

On a de plus supposé que q est continue : $b(-, y)$ est donc elle aussi continue de V dans R. Soit λ dans R. Puisque $\mathbf{Q}$ est dense dans R, il existe une suite de rationnels $(r_n)_{n\geq 1}$ qui tend vers λ. On a donc

$$\begin{aligned} b(\lambda \cdot x, y) &= b((\lim_n r_n) \cdot x, y)) \\ &= b(\lim_n (r_n \cdot x), y) \\ &= \lim_n b(r_n \cdot x, y) \\ &= \lim_n \big(r_n \cdot b(x, y)\big) \\ &= (\lim_n r_n) \cdot b(x, y) \\ &= \lambda \cdot b(x, y), \end{aligned}$$

où la troisième égalité utilise le fait que $b(-, y)$ est continue et la quatrième égalité utilise (4).

On obtient finalement que $b(-, y)$ est R-linéaire et par symétrie, on en déduit que $b(x, -)$ est elle aussi R-linéaire. On a donc montré que b est une forme bilinéaire symétrique et donc q est une forme quadratique.

Corrigé de la question (3) de l'exercice 10.

Existence : Si $d = b^2 - 4pc$ avec b et c entiers alors si $q = (p, b, c)$, on a $p = q(1, 0)$.

Unicité : Soit q une forme quadratique binaire qui représente p. Il existe donc (x, y) non nul tel que $q(x, y) = p$. De plus, x et y sont premiers entre eux (puisque $(\gcd(x, y))^2$ divise p). Soient u et v tels que $xv - yu = 1$. Via la matrice $\begin{pmatrix} x & y \\ u & v \end{pmatrix}$, la forme q est équivalente à une forme q' telle que $q'(1, 0) = q(x, y) = p$ et en particulier, q' s'écrit sous la forme (p, b, c) pour des entiers b et c. En utilisant les relations

$$(p, b, c) \overset{+}{\sim} (p, b + 2p, p + b + c) \text{ and } (p, b, c) \overset{+}{\sim} (p, b - 2p, p - b + c)$$

on peut supposer $-p \leq b \leq p$. Puis, en utilisant $(p, b, c) \sim (p, -b, c)$, on peut de plus supposer $b \geq 0$. Remarquons aussi que c est complètement déterminé par b (puisque $c = \frac{b^2 - d}{4p}$). Ainsi pour prouver l'unicité modulo équivalence, il suffit de montrer qu'il existe un unique b tel que $0 \leq b \leq p$ et $d = b^2 \pmod{4p}$.

Soient b et b' dans $\{0,\dots,p\}$ tels que $b^2 = b'^2 = d \pmod{4p}$ et $b' \leq b$. Alors $4p$ divise $(b^2 - b'^2) = (b-b')(b+b')$. On a aussi $0 \leq b-b' \leq p$ et $0 \leq b+b' \leq 2p$. Puisque 4 divise $b-b'$ et $b+b'$ et que les deux termes ont même parité, $b-b'$ et $b+b'$ sont nécessairement pairs.

Supposons que $p \neq 2$, on a donc $0 \leq b-b' < p$ et en particulier, soit $b = b'$, soit $b-b'$ et p sont premiers entre eux. Dans le premier cas, on a fini ; dans le deuxième, on obtient que p divise $b+b'$ donc $b+b'$ est dans $\{0,p,2p\}$. Si $b+b' = 0$ alors $b = -b' = 0$. Si $b+b' = p$ alors $b' = 0$ et $b = p$ mais alors $b-b' = p$, ce qui contredit la parité. Si $b+b' = 2p$ alors $b = b' = p$. Dans tous les cas, on obtient $b = b'$.

Si $p = 2$, on a $b-b' \in \{0,2\}$ et $b+b' \in \{0,2,4\}$ et 8 divise le produit, donc les seules possibilités sont $b-b' = 0$ (dans ce cas, on a fini) ou $b+b' = 0$ (dans ce cas aussi, on a fini) ou $b-b' = 2$ et $b+b' = 4$, ce qui donne $b' = 1$ et $b = 3$: contradiction avec l'hypothèse $b \in \{0,1,2\}$.

Feuille n°3.

Corrigé de l'exercice 7.

(1) Le nombre n_5 de 5-Sylow de G divise 60 (l'ordre de G) et est congru à 1 modulo 5. Les seules possibilités pour n_5 sont donc 1 et 6. Si $n_5 = 1$ alors l'unique 5-Sylow serait distingué, mais on a supposé G simple. Donc $n_5 = 6$. Remarquons au passage que G ne peut pas être abélien car dans ce cas on aurait $n_5 = 1$.

(2) Si on note $E := \{S_1,\dots,S_6\}$ l'ensemble des 5-Sylow de G, on a une action de G sur E donnée par $g \mapsto gS_ig^{-1}$. Cette action permute les S_i : pour tout g, il existe une permutation σ_g de $\mathfrak{S}_6$ telle que $g \cdot S_i = S_{\sigma_g(i)}$ pour tout i. En envoyant g sur σ_g, on obtient un morphisme $\varphi : G \to \mathfrak{S}_6$. Montrons que ce morphisme est injectif. Son noyau $\mathrm{Ker}(\varphi)$ est un sous-groupe distingué de G, c'est donc $\{1\}$ ou G. Si c'est G, alors pour tout g de G, on aurait $gS_ig^{-1} = S_i$, contradiction. Le morphisme φ est donc bien injectif.

Montrons que $H := \varphi(G)$ est inclus dans $\mathfrak{A}_6$. Puisque φ est injectif, il induit un isomorphisme $G \xrightarrow{\sim} H$ et donc H est un groupe simple d'ordre 60. Rappelons que le groupe dérivé $D(H)$ de H est un sous-groupe distingué et donc $D(H)$ est soit réduit à 1, soit égal à H tout entier. S'il est réduit à 1 alors H (et donc G) serait abélien : ceci contredit la remarque faite ci-dessus en question (1). Donc $D(H) = H$. Mais l'inclusion $H \subset \mathfrak{S}_6$ implique $D(H) \subset D(\mathfrak{S}_6)$. Or pour tout élément $[x,y] = x^{-1}y^{-1}xy$ de $D(\mathfrak{S}_6)$, on a $\mathrm{sgn}([x,y]) = 1$ et donc $D(\mathfrak{S}_6) \subset \mathfrak{A}_6$. En conclusion $H = D(H) \subset D(\mathfrak{S}_6) \subset \mathfrak{A}_6$.

H est bien un sous-groupe de $\mathfrak{A}_6$. Comme il est isomorphe à G, il est d'ordre 60 et $\mathfrak{A}_6$ est d'ordre $\frac{6!}{2} = 360$ donc H est d'indice 6 dans $\mathfrak{A}_6$.

(3) Le morphisme $\psi : \mathfrak{A}_6 \to \mathrm{Bij}(\mathfrak{A}_6/H)$ est donné par $\tau \mapsto (gH \mapsto \tau gH)$. On a $\mathrm{Ker}(\psi)$ distingué dans $\mathfrak{A}_6$ et on sait que $\mathfrak{A}_6$ est simple donc $\mathrm{Ker}(\psi)$ est soit $\{1\}$ soit $\mathfrak{A}_6$. Ça ne peut pas être $\mathfrak{A}_6$ car l'action par multiplication à gauche sur les classes est transitive. Donc ψ est injectif. Il induit alors un isomorphisme $\mathrm{Im}(\psi) \simeq \mathfrak{A}_6$ et il suit que $\mathrm{Im}(\psi)$ est d'ordre 360.

L'ensemble $\mathfrak{A}_6/H$ est de cardinal 6 : on a donc $\mathrm{Bij}(\mathfrak{A}_6/H) \simeq \mathfrak{S}_6$ et on obtient que $\mathrm{Im}(\psi)$ est isomorphe à un sous-groupe de $\mathfrak{S}_6$. Comme $\mathfrak{S}_6$ est d'ordre 720 et $\mathrm{Im}(\psi)$ est d'ordre 360, on voit que l'indice de $\mathrm{Im}(\psi)$ dans $\mathfrak{S}_6$ est égal à 2. On a montré en cours que tout sous-groupe d'indice 2 est distingué et on a vu dans l'exercice 8 de la feuille d'exercices n°1 que les seuls sous-groupes distingués de $\mathfrak{S}_6$ sont $\mathfrak{A}_6$ et $\mathfrak{S}_6$. Donc $\mathrm{Im}(\psi)$ est isomorphe à $\mathfrak{A}_6$.

(4) On a $|\psi(H)| = |H| = 60$ car ψ est injectif. Mais $\psi(H)$ est un sous-groupe de $\mathrm{Im}(\psi) \subset \mathrm{Bij}(\mathfrak{A}_6/H) \simeq \mathfrak{S}_6$ et il fixe un élément : la classe $1 \cdot H \in \mathfrak{A}_6/H$. On a donc $\psi(H) \subset \mathfrak{S}_5$ et on a vu qu'il était en fait contenu dans $\mathfrak{A}_6$ donc $\psi(H) \subset \mathfrak{S}_5 \cap \mathfrak{A}_6 = \mathfrak{A}_5$. Enfin, puisque $\psi(H)$ et $\mathfrak{A}_5$ sont tous les deux d'ordre 60, ils sont égaux.