Mathématiques spéciales

Corrigé de la feuille d'exercices n°5 prime - Révisions d'algèbre de Sup' : congruences, groupes, anneaux

Exercices obligatoires : 1 ; 4 ; 8 ; 12 ; 21 ; 29 ; 37.

1. Exercices basiques

a. Congruences

Exercice 1.

1. Déterminer, suivant les puissances de $n \in \mathbb{N}$, le reste de la division euclidienne de 2^n par 5.
2. Quel est le reste de la division par 5 de 1357^{2013} ?

Correction.

1. La méthode pour ce type d'exercice est toujours la même et est très importante à savoir. On commence par rechercher le premier entier $k \geq 1$ tel que $2^k \equiv 1\ [5]$. On va ensuite raisonner modulo k. On trouve successivement :

$$2^1 \equiv 2\ [5], \quad 2^2 \equiv 4\ [5], \quad 2^3 \equiv 3\ [5], \quad 2^4 \equiv 1\ [5].$$

On va donc classer les entiers n modulo 4. En effet, si $n = 4q + r$, alors sachant que $2^{4q} \equiv 1^q\ [5]$ soit $2^{4q} \equiv 1\ [5]$, on trouve que

$$2^n \equiv 2^r\ [5].$$

Ainsi, on obtient

— Si $n \equiv 0\ [4]$, alors $2^n \equiv 1\ [5]$;
— Si $n \equiv 1\ [4]$, alors $2^n \equiv 2\ [5]$;
— Si $n \equiv 2\ [4]$, alors $2^n \equiv 4\ [5]$;
— Si $n \equiv 3\ [4]$, alors $2^n \equiv 3\ [5]$;

2. On commence par effectuer la division euclidienne de 1357 par 5, et on trouve que $1357 \equiv 2\ [5]$, d'où $1357^{2013} \equiv 2^{2013}\ [5]$. De plus, $2013 \equiv 1\ [4]$. On en déduit que $1357^{2013} \equiv 2^1 \equiv 2\ [5]$.

Exercice 2.

Démontrer que la somme de trois cubes consécutifs est toujours divisible par 9.

Correction.

On développe $n^3 + (n+1)^3 + (n+2)^3$:

$$n^3 + (n+1)^3 + (n+2)^3 = 3n^3 + 9n^2 + 15n + 9 = 9(n^2+1) + 3n(n^2+5).$$

Il suffit donc de démontrer que $9|3n(n^2+5)$ ou encore que $3|n(n^2+5)$. Si $n \equiv 0$ [3], c'est bien sûr vrai. Si $n \equiv 1$ [3], on a $n^2 \equiv 1$ [3] et donc $n^2 + 5 \equiv 6 \equiv 0$ [3]. Si $n \equiv 2$ [3], alors $n^2 + 5 \equiv 4 + 5 \equiv 9 \equiv 0$ [3]. Dans tous les cas, $3n(n^2+5)$ est divisible par 9.

Exercice 3.

1. Déterminer les entiers naturels n tels que $5^n \equiv -1$ [13].
2. Déterminer les entiers naturels n tels que 13 divise $5^{2n} + 5^n$.

Correction.

1. On calcule les premiers termes et on trouve $5^0 \equiv 1$ [13], $5^1 \equiv 5$ [13], $5^2 \equiv -1$ [13], $5^3 \equiv -5$ [13], $5^4 \equiv 1$ [13], $5^5 \equiv 5$ [13], $5^6 \equiv -1$ [13],... On voit clairement apparaître le cycle $1, 5, -1, -5, 1, 5, -1$, ce qui nous incite à démontrer par récurrence sur $\surd \in \mathbb{N}$ la propriété $\mathcal{P}(p)$ suivante :

   $$\mathcal{P}(p) = \text{"}5^{4p} \equiv 1 \text{ [13]}, \ 5^{4p+1} \equiv 5 \text{ [13]}, \ 5^{4p+2} \equiv -1 \text{ [13]}, \ 5^{4p+3} \equiv -5 \text{ [13]"}.$$

   La propriété $\mathcal{P}(0)$ est vraie comme le montre le calcul précédent. Soit $p \in \mathbb{N}$ tel que $\mathcal{P}(p)$ est vraie, et prouvons $\mathcal{P}(p+1)$. Alors on a

   $$5^{4(p+1)} = 5^{4p}5^4 \equiv 1 \times 1 \equiv 1 \text{ [13]}.$$

   La démonstration pour les trois autres cas est exactement similaire. Donc $\mathcal{P}(p+1)$ est vraie. Ainsi, les entiers naturels solutions de $5^n \equiv -1$ [13] sont exactement les entiers de la forme $4p+2$, avec $p \in \mathbb{N}$.
2. Écrivons $5^{2n} + 5^n = 5^n(5^n+1)$. Si $13|5^{2n} + 5^n$, puisque $5 \wedge 13 = 1$, le théorème de Gauss assure que $13|5^n + 1$, autrement dit que $5^n \equiv -1$ [13]. D'après la question précédente, ceci est équivalent à dire que $n = 4p+2$, avec $p \in \mathbb{N}$. Réciproquement, si $n = 4p+2$ pour un certain $p \in \mathbb{N}$, on sait que $13|5^n + 1$ et donc $13|5^n(5^n+1) = 5^{2n} + 5^n$. Les entiers n solutions sont donc exactement ceux qui s'écrivent $4p+2$ avec $p \in \mathbb{N}$.

Exercice 4.

Démontrer que 13 divise $3^{126} + 5^{126}$.

Correction.

On va commencer par étudier les puissances de 3 modulo 13. On commence par remarquer que

$$3^1 \equiv 3 \text{ [13]}, \quad 3^2 \equiv 9 \text{ [13]}, \ 3^3 \equiv 1 \text{ [13]}.$$

On sait donc que, puisque $126 = 3 * 42$, $3^{126} \equiv (3^3)^{42}$ [13], et donc $3^{126} \equiv 1$ [13]. De même, on a

$$5^1 \equiv 5 \text{ [13]}, \quad 5^2 \equiv 12 \text{ [13]}, \quad 5^3 \equiv 8 \text{ [13]}, \quad 5^4 \equiv 1 \text{[13]}.$$

Par un raisonnement similaire, et utilisant que $126 = 31 * 4 + 2$, on trouve

$$5^{126} \equiv 5^2 \text{ [13] soit } 5^{126} \equiv 12 \text{ [13]}.$$

On en déduit que

$$3^{126} + 5^{126} \equiv 0 \text{ [13]},$$

ce qui signifie bien que 13 divise $3^{126} + 5^{126}$.

Exercice 5.

Démontrer que, pour tout entier naturel n, $3^{2n+1} + 2^{4n+2}$ est divisible par 7.

Correction.

Notons, pour $n \in \mathbb{N}$, la propriété $\mathcal{P}(n)$ ="$3^{2n+1} + 2^{4n+2}$ est divisible par 7". Prouvons par récurrence que pour tout $n \in \mathbb{N}$, $\mathcal{P}(n)$ est vérifiée. Initialisation : On a $3^1 + 2^2 = 7$ qui est bien divisible par 7. Hérédité : Soit $n \in \mathbb{N}$ tel que $\mathcal{P}(n)$ est vraie. Remarquons que $3^2 \equiv 2$ [7] et que $2^4 \equiv 2$ [7]. Alors, on écrit (modulo 7) :

$$\begin{aligned} 3^{2n+3} + 2^{4n+6} &\equiv 3^2 3^{2n+1} + 2^4 2^{4n+2} \text{ [7]} \\ &\equiv 2 \times 3^{2n+1} + 2 \times 2^{4n+2} \text{ [7]} \\ &\equiv 2 \times (3^{2n+1} + 2^{4n+2}) \text{ [7]} \\ &\equiv 2 \times 0 \text{ [7]} \\ &\equiv 0 \text{ [7]}. \end{aligned}$$

Ainsi, 7 divise $3^{2n+3} + 2^{4n+6}$ et donc $\mathcal{P}(n+1)$ est vraie. En conclusion, par le principe de récurrence, $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$.

Exercice 6.

On considère la suite (u_n) d'entiers naturels définie par $u_0 = 14$ et $u_{n+1} = 5u_n - 6$.

1. Quelle conjecture peut-on émettre sur les deux derniers chiffres de (u_n) ?
2. Montrer que pour tout entier naturel n, $u_{n+2} \equiv u_n$ [4]. En déduire que pour tout entier naturel k, on a $u_{2k} \equiv 2$ [4] et $u_{2k+1} \equiv 0$ [4].
3. (a) Montrer que pour tout entier naturel n, on a $2u_n = 5^{n+2} + 3$.
   (b) En déduire que pour tout entier naturel n, on a $2u_n \equiv 28$ [100].
4. Valider la conjecture émise à la première question.

Correction.

1. En utilisant un tableur, on peut conjecturer que les deux derniers chiffres de u_n sont 14 si n est pair et 64 si n est impair.
2. On a $u_{n+2} = 5u_{n+1} - 6 = 5(5u_n - 6) - 6 = 25u_n - 36$. Écrivons cette égalité modulo 4. On trouve :
$$u_{n+2} \equiv u_n \ [4]$$
puisque $25 \equiv 1$ [4] et $-36 \equiv 0$ [4]. Le reste de la question se déduit par une récurrence assez élémentaire.
3. (a) On va prouver ce résultat par récurrence sur n. La propriété est vraie au rang 0. Si elle est vérifiée au rang n, alors
$$2u_{n+1} = 2(5u_n - 6) = 5(5^{n+2} + 3) - 12 = 5^{n+3} + 3.$$
On aurait pu aussi utiliser la forme générale du terme d'une suite arithmético-géométrique.

   (b) On commence par remarquer que, pour tout $p \geq 1$, alors $5^p = 25$ [100]. C'est en effet vrai pour $p = 1$, et si c'est vrai au rang p, alors
$$5^p \equiv 25 \ [100] \implies 5^{p+1} \equiv 125 \equiv 25 \ [100].$$
Ainsi, pour tout entier naturel n,
$$2u_n \equiv 5^{n+2} + 3 \equiv 25 + 3 \equiv 28 \ [100].$$
4. D'après la question précédente, on sait que pour tout entier naturel k, on a $2u_{2k} = 28+100u$ soit $u_{2k} = 14+50p$. Si $p = 2m$ est pair, alors $u_{2k} = 14+100m$ et $u_{2k} \equiv 14$ [100]. Si $p = 2m+1$ est impair, alors
$$u_{2k} = 14 + 50 + 100m = 64 + 100m = (8 + 25m) \times 4 \implies u_{2k} = 0 \ [4]$$
et ceci contredit le résultat de la question 2. Ce n'est donc pas possible et on a bien $u_{2k} \equiv 14$ [100]. Pour les termes u_{2k+1}, la preuve de la conjecture est identique.

Exercice 7.

Soit a et b deux entiers tels que $a^2 + b^2$ soit divisible par 7. Démontrer que a et b sont divisibles par 7.

Correction.

Commençons par écrire un tableau décrivant les carrés modulo 7.

x (mod 7)	0	1	2	3	4	5	6
x^2 (mod 7)	0	1	4	2	2	4	1

On distingue alors 4 cas :

— Si $a^2 = 0$ modulo 7, alors $a^2 + b^2 = 0$ modulo 7 si et seulement si $b = 0$ modulo 7 : c'est le cas où a et b sont tous les deux divisibles par 7.

— Si $a^2 = 1$ modulo 7, pour que $7|a^2+b^2$, il faudrait que $b^2 = 6$ modulo 7, ce qui est impossible.

— Si $a^2 = 2$ modulo 7, pour que $7|a^2+b^2$, il faudrait que $b^2 = 5$ modulo 7, ce qui est impossible.
— Si $a^2 = 4$ modulo 7, pour que $7|a^2+b^2$, il faudrait que $b^2 = 3$ modulo 7, ce qui est impossible.

Ainsi la seule possibilité est bien que a et b soient divisibles par 7.

b. Groupes

Exercice 8.

Dans les questions suivantes, déterminer si la partie H est un sous-groupe du groupe G.

1. $G = (\mathbb{Z}, +)$; $H = \{\text{nombres pairs}\}$.
2. $G = (\mathbb{Z}, +)$; $H = \{\text{nombres impairs}\}$.
3. $G = (\mathbb{R}, +)$; $H = [-1, +\infty[$.
4. $G = (\mathbb{R}^*, \times)$; $H = \mathbb{Q}^*$.
5. $G = (\mathbb{R}^*, \times)$; $H = \{a + b\sqrt{2};\ a, b \in \mathbb{Q},\ (a, b) \neq (0, 0)\}$.
6. $G = (\{\text{bijections de } E \text{ dans } E\}, \circ)$; $H = \{f \in G;\ f(x) = x\}$ où E est un ensemble et $x \in E$.
7. $G = (\{\text{bijections de } E \text{ dans } E\}, \circ)$; $H = \{f \in G;\ f(x) = y\}$ où E est un ensemble et $x, y \in E$ avec $x \neq y$.

Correction.

1. H est un sous-groupe de G. En effet, $0 \in H$, si $x, y \in H$, alors $-x$ et $x+y$ sont deux entiers pairs et donc $-x \in H$, $x + y \in H$. Le théorème de caractérisation des sous-groupes nous dit que H est un sous-groupe de G.
2. $0 \notin H$ et donc H n'est pas un sous-groupe de G.
3. $2 \in H$ et $-2 \notin H$: H n'est pas un sous-groupe de G.
4. $1 \in H$. Si $x = p/q$ et $y = p'/q'$ sont deux rationnels non-nuls, alors $1/x = q/p$ et $x \times y = \frac{p \times p'}{q \times q'}$ sont deux rationnels non nuls. H est un sous-groupe de G.
5. $1 = 1 + 0\sqrt{2} \in H$. Si $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ sont éléments de H, alors
$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$
est lui aussi un élément de H. De même, $xy \in H$ puisque
$$xy = (ac + 2bd) + (ad + bc)\sqrt{2}$$
est un élément de H. Remarquons que l'on ne peut pas avoir $ac + 2bd = 0$ et $ad + bc = 0$, sinon on aurait $xy = 0$ et donc ou bien $x = 0$ ou bien $y = 0$ ce qui n'est pas le cas. Ainsi H est un sous-groupe de G.
6. Id_E, l'élément neutre de G, est élément de H. De plus, si $f, g \in H$, alors
$$f(x) = x \implies f^{-1}(f(x)) = f^{-1}(x) \implies f^{-1}(x) = x$$
et
$$f \circ g(x) = f(g(x)) = f(x) = x.$$
Ainsi, f^{-1} et $f \circ g$ sont éléments de H, et H est un sous-groupe de G.

7. L'élément neutre de G, Id_E, n'est pas élément de H qui n'est donc pas un sous-groupe de G.

Exercice 9.

Dire si les parties suivantes de $GL_n(\mathbb{R})$ sont des sous-groupes de $GL_n(\mathbb{R})$.

1. $H_1 = \{A \in GL_n(\mathbb{R});\ A \text{ diagonale avec tous ses coefficients diagonaux non-nuls}\}$.
2. $H_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix};\ a > 0,\ b \in \mathbb{R} \right\}$ (ici, $n = 2$).
3. $H_3 = \left\{ \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix};\ a > 0,\ b \in \mathbb{R} \right\}$ (ici, $n = 2$).

Correction.

Remarquons pour commencer que nous avons bien affaire à des parties de $GL_n(\mathbb{R})$. On va appliquer le théorème de caractérisation des sous-groupes pour vérifier si ce sont, ou non, des sous-groupes.

1. Notons $D(\lambda_1, \dots, \lambda_n)$ la matrice diagonale dont les coefficients diagonaux sont $\lambda_1, \dots, \lambda_n$. Les éléments de H_1 sont les matrices $D(\lambda_1, \dots, \lambda_n)$ avec tous les λ_i non nuls. Alors on remarque que $I_n = D(1, \dots, 1) \in H_1$, que si $D(\lambda_1, \dots, \lambda_n)$, $D(\mu_1, \dots, \mu_n) \in H_1$, alors

$$D(\lambda_1, \dots, \lambda_n) \cdot D(\mu_1, \dots, \mu_n) = D(\lambda_1\mu_1, \dots, \lambda_n\mu_n) \in H_1$$

$$D(\lambda_1, \dots, \lambda_n)^{-1} = D(1/\lambda_1, \dots, 1/\lambda_n) \in H_1.$$

   Ainsi, H_1 est bien un sous-groupe de $GL_n(\mathbb{R})$.
2. Notons $M(a, b)$ la matrice $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ de sorte que H_2 est l'ensemble des matrices $M(a, b)$ avec $a > 0$ et $b \in \mathbb{R}$. Alors on a $M(a, b)M(c, d) = M(ac, ad + b)$. Ainsi, on remarque que $I_2 = M(1, 0) \in H_2$, que si $M(a, b)$ et $M(c, d)$ sont dans H_2, alors leur produit est dans H_2 (car $ac > 0$). De plus, calculant l'inverse de la matrice $M(a, b)$, on trouve

$$M(a, b)^{-1} = M\left(\frac{1}{a}, \frac{-b}{a}\right) \in H_2.$$

   On en déduit que H_2 est un sous-groupe de $GL_2(\mathbb{R})$.
3. Remarquons que $I_2 \notin H_3$. Ainsi, H_3 n'est pas un sous-groupe de $GL_2(\mathbb{R})$.

Exercice 10.

Les applications $\phi : G \to H$ définies ci-dessous sont-elles des morphismes de groupes ?

1. $G = (GL_n(\mathbb{R}), \times)$, $H = (\mathbb{R}, +)$, $\phi(A) = \mathrm{tr}(A)$.
2. $G = (M_n(\mathbb{R}), +)$, $H = (\mathbb{R}, +)$, $\phi(A) = \mathrm{tr}(A)$.
3. $G = (\mathbb{R}^*, \times)$, $H = (\mathbb{R}^*, \times)$, $\phi(x) = |x|$.
4. $G = (\mathbb{R}^*, \times)$, $H = (\mathbb{R}^*, \times)$, $\phi(x) = 2x$.

5. $G = (\mathbb{R}, +)$, $H = (GL_2(\mathbb{R}), \times)$, $\phi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.

Correction.

1. Si ϕ était un morphisme de groupe, on aurait, puisque I_n est l'élément neutre du groupe $(GL_n(\mathbb{R}), \times)$ et 0 celui de $\mathbb{R}_+$, $\phi(I_n) = 0$. Ce n'est pas le cas, car $\phi(I_n) = n$. On peut aussi trouver deux exemple de matrices A et B pour lesquelles on n'a pas $\phi(AB) = \phi(A) + \phi(B)$ (ici aussi, $A = B = I_n$ conviennent).
2. Dans ce cas, ϕ est bien un morphisme de groupe car on a bien $\mathrm{Tr}(A+B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$. La morale des deux premières questions est qu'il faut vraiment faire très attention aux groupes en jeu, pas seulement à l'application.
3. Ici aussi, ϕ est un morphisme de groupes car pour tous $x, y \neq 0$, on a
$$\phi(xy) = |xy| = |x| \times |y| = \phi(x) \times \phi(y).$$
4. Si ϕ était un morphisme de groupes, on aurait $\phi(1) = 1$ puisque 1 est l'élément neutre de $(\mathbb{R}^*, \times)$. Ce n'est pas le cas puisque $\phi(1) = 2$.
5. On va revenir à la définition. Soit $x, y \in \mathbb{R}$. On a
$$\phi(x+y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$$
tandis que par les règles du produit matriciel
$$\phi(x) \times \phi(y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}.$$
Les deux résultats coïncident : ϕ est bien un morphisme de groupes.

Exercice 11.

Justifier que exp est un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \cdot)$. Quel est son image ? Son noyau ?

Correction.

On sait que, pour tous $z, w \in \mathbb{C}$, on a
$$\exp(z+w) = \exp(z)\exp(w).$$
Ceci signifie exactement que exp est un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \cdot)$ (la fonction exponentielle ne prend jamais la valeur zéro). De plus, soit $w \in \mathbb{C}^*, w = re^{i\theta}$ avec $r > 0$. Soit $a = \ln r$ et posons $z = a + i\theta$. Alors
$$\exp(z) = \exp(a)\exp(i\theta) = re^{i\theta} = w.$$
L'exponentielle est un morphisme surjectif de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, +)$. Déterminons son noyau. Si $\exp(z) = 1$, posons $z = x + iy$. Alors
$$\exp(z) = \exp(x)\exp(iy) = 1 = 1\exp(i0).$$

Ceci est équivalent à $x = 0$ et il existe $k \in \mathbb{Z}$ tel que $y = k2\pi$. On a donc

$$\ker(\exp) = \{2ik\pi;\ k \in \mathbb{Z}\}.$$

Exercice 12.

Déterminer tous les morphismes de groupes que $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Correction.

Soit f un tel morphisme de groupe. On va commencer par démontrer que pour p et q des entiers naturels, on a $f(p) = pf(1)$ et $f\left(\frac{1}{q}\right) = \frac{1}{q}f(1)$. La première des deux propriétés se démontre aisément par récurrence. Pour la deuxième, on écrit que

$$f(1) = f\left(\frac{1}{q} + \cdots + \frac{1}{q}\right) = qf\left(\frac{1}{q}\right).$$

Notons ensuite $a = f(1)$. Alors a/q est un entier pour tout entier q, et donc $a = 0$. On en déduit que $f(p) = f(1/q) = 0$ pour tous les entiers p et q, puis que $f(p/q) = pf(1/q) = 0$. Finalement, on trouve que f est l'endomorphisme nul.

Exercice 13.

Les ensembles suivants munis des lois considérées sont-ils des groupes ?

1. G est l'ensemble des fonctions de $\mathbb{R} \to \mathbb{R}$ définies par $x \mapsto ax + b$, avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$, muni de la composition ;
2. G est l'ensemble des fonctions croissantes de $\mathbb{R}$ dans $\mathbb{R}$, muni de l'addition ;
3. $G = \{f_1, f_2, f_3, f_4\}$, où

$$f_1(x) = x,\ f_2(x) = -x,\ f_3(x) = \frac{1}{x},\ f_4(x) = -\frac{1}{x},$$

muni de la composition.

Correction.

1. On remarque d'abord que la composition est une loi de composition interne pour G. En effet,
$$(ax + b) \circ (cx + d) = acx + (ad + b).$$
La loi $\circ$ est clairement associative (pour toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$, on a effectivement $f \circ (g \circ h) = (f \circ g) \circ h$). La fonction $x \mapsto x$ est un élément neutre, et l'inverse de $x \mapsto ax + b$ est donné par $x \mapsto \frac{1}{a}x - \frac{b}{a}$ - on trouve cet élément en résolvant le système (d'inconnues c et d)
$$\begin{cases} ac &= 1 \\ ad + b &= 0. \end{cases}$$
On aurait aussi pu démontrer que G est un sous-groupe du groupe des permutations de $\mathbb{R}$.

2. Imaginons que G soit un groupe. Son élément neutre est alors forcément la fonction identiquement nulle. Mais prenons la fonction $f(x) = x$ (qui est bien croissante). Son inverse serait la fonction $f(x) = -x$, qui n'est pas croissante ! Donc $(G, +)$ n'est pas un groupe.
3. Calculons d'abord le résultat des différentes compositions :

$$f_1 \circ f_1 = f_1,\ f_1 \circ f_2 = f_2 \circ f_1 = f_2,\ f_1 \circ f_3 = f_3 \circ f_1 = f_3,\ f_1 \circ f_4 = f_4 \circ f_1 = f_4$$

$$f_2 \circ f_2 = f_1,\ f_2 \circ f_3 = f_3 \circ f_2 = f_4,\ f_2 \circ f_4 = f_4 \circ f_2 = f_3$$

$$f_3 \circ f_3 = f_1,\ f_3 \circ f_4 = f_4 \circ f_3 = f_2$$

$$f_4 \circ f_4 = f_1.$$

De ces calculs, on tire que :

(a) $\circ$ est bien une loi de composition interne pour G. Elle est de plus clairement associative.

(b) f_1 est élément neutre pour cette loi.

(c) Chaque élément admet un inverse : lui-même !

$(G, \circ)$ est bien un groupe. On pourrait démontrer, toujours à partir du résultat des différentes compositions, qu'il est isomorphe au groupe classique $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 14.

Montrer que $H = \{x + y\sqrt{3};\ x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - 3y^2 = 1\}$ est un sous-groupe de $(\mathbb{R}_+^*, \times)$.

Correction.

La première chose à remarquer est que $H \subset \mathbb{R}_+^*$. Pour $x + y\sqrt{3} \in H$, puisque $x^2 - 3y^2 > 0$ et $x \in \mathbb{N}$, on a $x > \sqrt{3}|y|$ et donc $x + y\sqrt{3} > 0$. On remarque ensuite que $1 = 1 + 0\sqrt{3}$ est bien un élément de H. Soient $a = x + y\sqrt{3}$ et $b = u + v\sqrt{3}$ deux éléments de H. Alors :

$$(x + y\sqrt{3})(u + v\sqrt{3}) = (xu + 3yv) + \sqrt{3}(xv + yu).$$

On remarque ensuite que

$$\begin{aligned}(xu + 3yv)^2 - 3(xv + yu)^2 &= x^2u^2 + 9y^2v^2 - 3x^2v^2 - 3y^2u^2 \\ &= x^2(u^2 - 3v^2) + 3y^2(3v^2 - u^2) \\ &= x^2 - 3y^2 \\ &= 1.\end{aligned}$$

De plus, il est clair que $xu + 3yv$ et $xv + yu$ sont éléments de $\mathbb{Z}$. Il reste à voir que $xu + 3yv$ est élément de $\mathbb{N}$. Mais c'est clair car $x \geq \sqrt{3}|y|$ et $u \geq \sqrt{3}|v|$. Ainsi, $ab \in H$. Démontrons finalement que H est bien stable par passage à l'inverse. On a

$$\frac{1}{a} = \frac{1}{x + y\sqrt{3}} = \frac{x - y\sqrt{3}}{x^2 - 3y^2} = x - y\sqrt{3} \in H$$

puisque $x^2 + 3(-y)^2 = 1$. Ainsi, H est bien un sous-groupe de $(\mathbb{R}_+^*, \times)$.

Exercice 15.

Traduire en termes de morphismes de groupes les propriétés bien connues suivantes (dont le domaine de validité a volontairement été omis) :

1. $\ln(xy) = \ln(x) + \ln(y)$;
2. $|zz'| = |z||z'|$;
3. $\sqrt{xy} = \sqrt{x}\sqrt{y}$;
4. $e^{x+y} = e^x e^y$;
5. $\det(MM') = \det(M)\det(M')$.

Correction.

1. La fonction ln est un morphisme du groupe $(\mathbb{R}_+^*, \cdot)$ dans le groupe $(\mathbb{R}, +)$.
2. La fonction $|\cdot|$ est un morphisme de groupes de $(\mathbb{C}^*, \cdot)$ dans lui-même. Attention, même si la propriété est vraie pour $z = 0$, il faut exclure 0 du groupe !
3. La fonction $\sqrt{\ }$ est un morphisme du groupe $(\mathbb{R}_+^*, \cdot)$ dans lui-même.
4. La fonction exp est un morphisme de groupe de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \cdot)$.
5. La fonction det est un morphisme de groupe de $GL_n(\mathbb{R})$ dans $(\mathbb{R}^*, \times)$. Là aussi, il faut se restreindre aux éléments inversibles pour bien avoir affaire à un groupe.

Exercice 16.

Montrer que les lois suivantes munissent l'ensemble G indiqué d'une structure de groupe, et préciser s'il est abélien :

1. $x \star y = \frac{x+y}{1+xy}$ sur $G =]-1, 1[$;
2. $(x, y) \star (x', y') = (x + x', ye^{x'} + y'e^{-x})$ sur $G = \mathbb{R}^2$;

Correction.

1. $(G, \star)$ est un groupe car
   — $\star$ est une loi de composition interne sur G : en effet, si $x, y \in G$, alors $x \star y \in G$. Pour prouver cela, étudions la fonction définie sur $[-1, 1]$ par
   $$f(t) = \frac{t+y}{1+ty}.$$
   Elle est dérivable sur $[-1, 1]$, et sa dérivée vérifie
   $$f'(t) = \frac{1-y^2}{(1+ty)^2} > 0 \text{ sur }]-1, 1[.$$
   f est donc strictement croissante sur $[-1, 1]$ et on a
   $$f(-1) < x \star y = f(x) < f(1).$$
   Comme $f(-1) = (-1+y)/(1-y) = -1$ et $f(1) = (1+y)/(1+y) = 1$, on obtient bien que $x \star y \in G$.

— la loi est associative : pour tout $(x, y, z) \in G^3$,

$$\begin{aligned} x \star (y \star z) &= \frac{x + (y \star z)}{1 + x(y \star z)} \\ &= \frac{x + \frac{y+z}{1+yz}}{1 + x\frac{y+z}{1+yz}} \\ &= \frac{x + y + z + xyz}{1 + xy + xz + yz}, \end{aligned}$$

et un calcul similaire donne le même résultat pour $(x \star y) \star z$.

— 0 est un élément neutre pour la loi $\star$. En effet,

$$x \star 0 = 0 \star x = \frac{x + 0}{1 + 0} = x.$$

— Tout élément $x \in G$ est inversible, d'inverse $-x$. En effet, on a

$$x \star (-x) = (-x) \star x = \frac{x - x}{1 - x^2} = 0.$$

De plus, le groupe est clairement abélien.

2. Il est clair que $\star$ est une loi de composition interne sur $\mathbb{R}^2$. De plus,

— cette loi est associative :

$$\begin{aligned} (x, y) \star \big((x', y') \star (x'', y'')\big) &= (x, y) \star (x' + x'', y'e^{x''} + y''e^{-x'}) \\ &= (x + x' + x'', ye^{x'+x''} + y'e^{x''}e^{-x} + y''e^{-x'}e^{-x}) \\ &= (x + x' + x'', ye^{x'+x''} + y'e^{-x+x''} + y''e^{-x-x'}). \end{aligned}$$

De même,

$$\begin{aligned} \big((x, y) \star (x', y')\big) \star (x'', y'') &= (x + x', ye^{x'} + y'e^{-x}) \star (x'', y'') \\ &= (x + x' + x'', (ye^{x'} + y'e^{-x})e^{x''} + y''e^{-x-x'}) \\ &= (x + x' + x'', ye^{x'+x''} + y'e^{-x+x''} + y''e^{-x-x'}) \end{aligned}$$

et donc on a bien $(x, y) \star \big((x', y') \star (x'', y'')\big) = \big((x, y) \star (x', y')\big) \star (x'', y'')$.

— $(0, 0)$ est un élément neutre de G :

$$(x, y) \star (0, 0) = (x + 0, ye^0 + 0e^{-x}) = (x, y)$$

$$(0, 0) \star (x, y) = (0 + x, 0e^x + ye^{-0}) = (x, y).$$

— Tout élément $(x, y) \in G$ admet un inverse donnée par $(-x, -y)$. En effet,

$$(x, y) \star (-x, -y) = (x - x, ye^{-x} - ye^{-x}) = (0, 0),$$

$$(-x, -y) \star (x, y) = (-x + x, -ye^x + ye^x) = (0, 0).$$

De plus, le groupe n'est pas abélien, car

$$(1, 0) \star (0, 1) = (1, e^{-1}) \text{ tandis que } (0, 1) \star (1, 0) = (1, e^1).$$

Exercice 17.

Soit $(G, \cdot)$ un groupe. Démontrer que les parties suivantes sont des sous-groupes de G :

1. $C(G) = \{x \in G;\ \forall y \in G, xy = yx\}$ ($C(G)$ s'appelle le centre de G) ;
2. $aHa^{-1} = \{aha^{-1};\ h \in H\}$ où $a \in G$ et H est un sous-groupe de G.
3. On suppose de plus que G est abélien. On dit que x est un élément de torsion de G s'il existe $n \in \mathbb{N}$ tel que $x^n = e$. Démontrer que l'ensemble des éléments de torsion de G est un sous-groupe de G.

Correction.

Il suffit, pour chaque cas, d'appliquer le théorème de caractérisation des sous-groupes.

1. e est élément de $C(G)$ car $ey = ye = y$ pour tout $y \in G$. Soient $x_1, x_2 \in C(G)$. Alors, pour tout $y \in G$, on a
$$x_1x_2y = x_1(x_2y) = (x_1y)x_2 = yx_1x_2$$
et donc $x_1x_2 \in C(G)$. Enfin, si $x \in C(G)$, alors pour tout $y \in G$,
$$xy = yx \implies xyx^{-1} = yxx^{-1} = y \implies x^{-1}xyx^{-1} = x^{-1}y \implies yx^{-1} = x^{-1}y$$
où on a multiplié à droite puis à gauche par x^{-1}. On en déduit que $x^{-1} \in C(G)$ qui est donc un sous-groupe de G.
2. Puisque H est un sous-groupe de G, $e \in H$ et donc $aea^{-1} \in G$. Mais $aea^{-1} = e$ et donc $e \in aHa^{-1}$. Soient $x = aha^{-1}$ et $y = ah'a^{-1}$ deux éléments de aHa^{-1} avec donc $h, h' \in H$. On a
$$xy = aha^{-1}ah'a^{-1} = ahh'a^{-1} \in aHa^{-1}$$
puisque $hh' \in H$ (H est un sous-groupe de G). Enfin, on a
$$x^{-1} = (aha^{-1})^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$$
puisque $h^{-1} \in H$. aHa^{-1} est donc bien un sous-groupe de G.
3. Notons T l'ensemble des éléments de torsion de G. On a $e^1 = e$, donc $e \in T$. De plus, si $x, y \in T$, avec respectivement $x^n = e$ et $y^m = e$, il suffit de remarquer que
$$(y^{-1})^m = (y^m)^{-1} = e^{-1} = e$$
puis d'utiliser le fait que x et y^{-1} commutent pour prouver que
$$(xy^{-1})^{nm} = (x^n)^m((y^{-1})^m)^n = e.$$
Ainsi, xy^{-1} est élément de T, et T est bien un sous-groupe de G.

Exercice 18.

Un sous-groupe d'un groupe produit est-il nécessairement produit de deux sous-groupes ?

Correction.

Non, ce n'est pas le cas. Prenons $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ et $H = \{(x, x);\ x \in \mathbb{Z}\}$. H est clairement un sous-groupe de $\mathbb{Z}^2$, et H ne s'écrit pas $H = A \times B$, sinon on aurait $A = B = \mathbb{Z}$ ce qui n'est pas le cas.

Exercice 19.

Soit G un groupe et H, K deux sous-groupes de G. Démontrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

Correction.

Si $H \subset K$, alors $H \cup K = K$ qui est un sous-groupe de G. De même, si $K \subset H$, $H \cup K = H$ qui est un sous-groupe de G. Supposons maintenant que $H \cup K$ est un sous-groupe de G et que ni $H \subset K$, ni $K \subset H$. Alors on peut trouver $x \in H \backslash K$ et $y \in K \backslash H$. Puisque $H \cup K$ est un groupe et que $x, y \in H \cup K$, on a $xy \in H \cup K$. Mais si $xy \in H$, alors $y = x^{-1}(xy)$ est le produit de deux éléments de H, qui est un sous-groupe de G, et donc $y \in H$ ce qui est une contradiction. On obtient de même une contradiction dans l'autre cas possible $xy \in K$. L'hypothèse de départ est donc fausse, et on a bien $H \subset K$ ou $K \subset H$.

Exercice 20.

Déterminer tous les morphismes de $(\mathbb{Z}, +)$ dans lui-même. Lesquels sont injectifs ? surjectifs ?

Correction.

Soit f un morphisme de $(\mathbb{Z}, +)$. Prouvons par récurrence que pour tout $n \geq 1$, on a $f(n) = nf(1)$. C'est vrai pour $n = 1$, et si c'est vrai pour n, alors

$$f(n+1) = f(n) + f(1) = nf(1) + f(1) = (n+1)f(1).$$

De plus, pour $n \leq 0$, on a $-n \geq 0$ et donc $f(-n) = -nf(1)$. On en déduit :

$$0 = f(0) = f(n + (-n)) = f(n) + f(-n) = f(n) - nf(1).$$

Ainsi, on a toujours $f(n) = nf(1)$, quel que soit $n \in \mathbb{Z}$. Caractérisons maintenant les morphismes surjectifs. Supposons donc que f est surjectif. Tout élément de $\mathbb{Z} = f(\mathbb{Z})$ est un multiple de $f(1)$. Or, les seuls éléments de $\mathbb{Z}$ qui divisent tous les autres entiers sont 1 et -1. On en déduit que $f(1) = 1$ ou $f(1) = -1$, et donc que $f(n) = n$ ou $f(n) = -n$. Réciproquement, ces deux applications sont clairement des morphismes surjectifs de $(\mathbb{Z}, +)$. Déterminons enfin les morphismes injectifs. Soit f un morphisme et $n \in \ker(f)$. Alors $f(n) = nf(1) = 0$. Si $f(1) \neq 0$, alors $f(n) = 0 \iff n = 0$ et f est injectif, et si $f(1) = 0$, alors f n'est pas injectif. Donc tous les morphismes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$ sont injectifs sauf l'application identiquement nulle.

c. Anneaux, sous-anneaux

Exercice 21.

Un élément x d'un anneau A est dit nilpotent s'il existe un entier $n \geq 1$ tel que $x^n = 0$. On suppose que A est commutatif, et on fixe x, y deux éléments nilpotents.

1. Montrer que xy est nilpotent.
2. Montrer que $x + y$ est nilpotent.
3. Montrer que $1_A - x$ est inversible.
4. Dans cette question, on ne suppose plus que A est commutatif. Soit $u, v \in A$ tels que uv est nilpotent. Montrer que vu est nilpotent.

Correction.

Soient n, m tels que $x^n = 0$ et $y^m = 0$.

1. Puisque x et y commutent, on a $(xy)^n = x^n y^n = 0 \times y^n = 0$.
2. Remarquons d'abord que pour $p \geq n$, on a $x^p = x^{p-n}x^n = 0$. D'après la formule du binôme, $(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}$. Mais, pour $k \geq n$, $x^k = 0 \implies x^k y^{n+m-k} = 0$. D'autre part, pour $k < n$, on a $n + m - k \geq m$ et donc $y^{n+m-k} = 0 \implies x^k y^{n+m-k} = 0$. Ainsi, $(x+y)^{n+m} = 0$. On pourrait même se contenter de prendre la puissance $n + m - 1$.
3. L'idée est d'utiliser l'identité remarquable (toujours valable dans un anneau)

$$1 - x^p = (1 - x)(1 + x + \cdots + x^{p-1}).$$

   Si on l'applique pour $p = n$, alors on obtient

$$1 = (1 - x)(1 + x + \cdots + x^{n-1})$$

   ce qui implique que $1 - x$ est inversible d'inverse $1 + x + \cdots + x^{n-1}$.
4. Soit $n \geq 1$ tel que $(uv)^n = 0$. Alors

$$(vu)^{n+1} = v(uv)^n u = v \times 0 \times u = 0.$$

   Ainsi, vu est nilpotent.

Exercice 22.

On dit qu'un anneau A est un anneau de Boole si, pour tout $x \in A$, $x^2 = x$. On fixe A un tel anneau.

1. Démontrer que, pour tout $x \in A$, $x = -x$.
2. Montrer que A est commutatif.

Correction.

1. On applique la propriété à l'élément $x + x$. Il vient

$$x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x.$$

   Après simplification, on trouve $x + x = 0$, soit $x = -x$.

2. Soient $x, y \in A$. On doit prouver $xy = yx$. Appliquons la propriété à l'élément $x + y$. On a

$$(x + y) = (x + y)^2 = x^2 + y^2 + xy + yx = x + y + xy + yx.$$

Après simplification, on trouve $xy + yx = 0$ soit $xy = -yx$, soit $xy = yx$ en appliquant le résultat de la question précédente.

Exercice 23.

Soit $(G, +)$ un groupe commutatif. On note $\mathrm{End}(G)$ l'ensemble des endomorphismes de G sur lequel on définit la loi $+$ par $f + g : G \to G,\ x \mapsto f(x) + g(x)$. Démontrer que $(\mathrm{End}(G), +, \circ)$ est un anneau.

Correction.

On remarque d'abord que $+$ et $\circ$ sont bien des lois de composition interne sur $\mathrm{End}(G)$. Ensuite, on vérifie tous les points de la définition d'un anneau.

1. $(\mathrm{End}(G), +)$ est un groupe commutatif. En effet, la loi $+$ est associative, l'application $0_G : G \to G,\ g \mapsto 0$ est un élément neutre pour la loi $+$, et tout élément $f \in \mathrm{End}(G)$ admet un inverse $-f : G \to G,\ x \mapsto -f(x)$.
2. La loi $\circ$ est associative.
3. La loi $\circ$ est distributive par rapport à la loi $+$: pour tous $f, g, h \in \mathrm{End}(G)$ et tout $x \in G$,

$$((f + g) \circ h)(x) = (f + g)(h(x)) = f(h(x)) + g(h(x)) = (f \circ h + g \circ h)(x).$$

Ainsi, $(\mathrm{End}(G), +, \circ)$ est un anneau.

Exercice 24.

Soit $A = \left\{ \frac{m}{n};\ m \in \mathbb{Z},\ n \in 2\mathbb{N} + 1 \right\}$ (c'est-à-dire que A est l'ensemble des rationnels à dénominateur impair). Démontrer que $(A, +, \times)$ est un anneau. Quels sont ses éléments inversibles ?

Correction.

On va démontrer que A est un sous-anneau de $(\mathbb{Q}, +, \times)$. Pour cela, soient $x = \frac{m}{n}$ et $y = \frac{m'}{n'} \in A$. Alors :

$$x - y = \frac{mn' - m'n}{nn'} \text{ et } xy = \frac{mm'}{nn'}.$$

Comme nn', produit de deux nombres impairs, est impair, et que A est non vide puisqu'il contient 1, on en déduit que A est bien un sous-anneau de $(\mathbb{Q}, +, \times)$. Déterminons ensuite les inversibles de A. Soit $x = \frac{m}{n} \in A$ inversible, et soit $y = \frac{m'}{n'} \in A$ tel que $xy = 1$. On en déduit que $mm' = nn'$. En particulier, m est nécessairement impair. Réciproquement, si $x = \frac{m}{n}$ avec m impair, alors $y = \frac{n}{m}$ est dans A (si jamais $m < 0$, il suffit d'écrire $y = \frac{-n}{-m}$ pour vérifier qu'il est bien dans A), et $xy = 1$. Ainsi, les inversibles de A sont les éléments $\frac{m}{n}$ avec $m \in \mathbb{Z}$, $n \in \mathbb{N}^*$, et m, n impairs.

Exercice 25.

Pour $d \in \mathbb{N}$, on note $A_d = \{(x,y) \in \mathbb{Z}^2;\ y - x \in d\mathbb{Z}\}$.

1. Démontrer que, pour tout $d \in \mathbb{N}$, A_d est un sous-anneau de $\mathbb{Z}^2$.
2. Réciproquement, soit A un sous-anneau de $\mathbb{Z}^2$. Démontrer que $H = \{x \in \mathbb{Z};\ (x,0) \in A\}$ est un sous-groupe de $\mathbb{Z}$.
3. En déduire qu'il existe $d \in \mathbb{N}$ tel que $A = A_d$.

Correction.

1. Il est clair que $0_{\mathbb{Z}^2}$ et $1_{\mathbb{Z}^2}$ sont éléments de A_d. Considérons ensuite $(x,y),(x',y') \in A_d$. Que $(x+x', y+y')$ reste élément de A_d ne pose pas de problèmes. Pour le produit, on a
$$(x,y) \times (x',y') = (xx', yy')$$
et on a $yy' - xx' = (y-x)y' + x(y'-x')$ d'où $d | yy' - xx'$.
2. $0 \in H$ et si $x, x' \in H$, alors $(x-x', 0) = (x,0) - (x',0) \in H$ et donc $x - x' \in H$. H est un sous-groupe de $\mathbb{Z}$.
3. Puisque $\mathbb{Z}$ est principal, il existe $d \in \mathbb{N}$ tel que $H = d\mathbb{Z}$. Démontrons que $A = A_d$. D'une part, si $(x,y) \in A$, alors
$$(x-y, 0) = (x,y) - y(1,1) \in A$$
et donc $d | x-y$, c'est-à-dire $(x,y) \in A_d$. Réciproquement, si $(x,y) \in A_d$, alors $x - y \in d\mathbb{Z} = H$, ce qui signifie que $(x-y,0) \in A$. On termine presque comme précédemment en écrivant que
$$(x,y) = (x-y,0) + y(1,1) \in A.$$
Les sous-anneaux de $\mathbb{Z}^2$ sont donc tous de la forme A_d.

2. Exercices d'entraînement

a. Congruences

Exercice 26.

1. Soit $n \geq 1$. Montrer que $(n+1) | \binom{2n}{n}$.
2. Soit $p \geq 2$ premier. Montrer que $p | \binom{p}{k}$ pour $k \in \{1, \ldots, p-1\}$.
3. En déduire une preuve du petit théorème de Fermat : si $n \geq 1$ et p est premier, $n^p \equiv n\ [p]$.
4. (Plus difficile). Déduire de 2. que, pour tout $N \in \mathbb{N}^*$, pour tout $j \in \mathbb{N}^*$, pour tous $(x_1, \ldots, x_N) \in \mathbb{Z}^N$, on a
$$\left(\sum_{i=1}^{N} x_i\right)^{p^j} \equiv \sum_{i=1}^{N} x_i^{p^j}\ [p].$$

Correction.

1. Il est clair que $(n+1)\binom{2n}{n+1} = n\binom{2n}{n}$. Maintenant, comme $(n+1)\wedge n = 1$, on en déduit que $(n+1)|\binom{2n}{n}$.

2. Puisque $\binom{p}{k}$ est entier, on sait que $k!(p-k)!|p! = p\times(p-1)!$. Maintenant, puisque p est premier, on sait aussi que $k!\wedge p = 1$ et $(p-k)!\wedge p = 1$. Par le théorème de Gauss, $k!(p-k)!|(p-1)!$ et donc $\frac{(p-1)!}{k!(p-k)!}$ est un entier. Autrement dit, $p|\binom{p}{k}$.

3. Si $n = 1$, le résultat est trivial. Supposons le résultat établi au rang n et prouvons le au rang $n+1$. On a
$$(n+1)^p = n^p + 1 + \sum_{k=1}^{p-1}\binom{p}{k}n^k \equiv n^p + 1\ [p]$$
d'après la question précédente. Par hypothèse de récurrence,
$$(n+1)^p \equiv n+1\ [p].$$

4. On traite d'abord le cas $j = 1$, et on procède par récurrence sur N. Le cas $N = 1$ est trivial. Pour $N = 2$, on a
$$(x_1+x_2)^p = x_1^p + x_2^p + \sum_{k=1}^{p-1}\binom{p}{k}x_1^k x_2^{p-k} \equiv x_1^p + x_2^p\ [p]$$
d'après la question précédente. Si on suppose l'identité démontrée au rang N et qu'on souhaite la prouver au rang $N+1$, on écrit
$$\begin{aligned}\left(\sum_{i=1}^{N+1}x_i\right)^p &= \left(\sum_{i=1}^{N}x_i + x_{N+1}\right)^p \\ &\equiv \left(\sum_{i=1}^{N}x_i\right)^p + x_{N+1}^p\ [p] \text{ d'après le cas } N=2 \\ &\equiv \sum_{i=1}^{N}x_i^p + x_{N+1}^p\ [p] \text{ (par hypothèse de récurrence).}\end{aligned}$$
Ainsi, l'hypothèse de récurrence est démontrée. On démontre alors la formule générale par récurrence sur j. Le cas $j = 1$ vient d'être abordé. Si la relation est vraie au rang j, alors
$$\begin{aligned}\left(\sum_{i=1}^{N}x_i\right)^{p^{j+1}} &= \left(\left(\sum_{i=1}^{N}x_i\right)^{p^j}\right)^p \\ &\equiv \left(\sum_{i=1}^{N}x_i^{p^j}\right)^p\ [p] \text{ (par H.R.)} \\ &\equiv \sum_{i=1}^{N}x_i^{p^j\times p}\ [p] \text{ (cas } j=1).\end{aligned}$$
Ceci prouve le résultat par récurrence.

Exercice 27.

On note $\mathcal{A} = \{A, B, C, \ldots, Z\}$ l'alphabet, $\mathcal{E} = \{0, 1, 2, \ldots, 25\}$ l'ensemble des 26 premiers entiers naturels, et g la bijection naturelle de $\mathcal{A}$ sur $\mathcal{E}$ consistant à numéroter les lettres :

$$g(A) = 0,\ g(B) = 1,\ g(C) = 2, \ldots, g(Z) = 25.$$

1. Pour tout entier x de $\mathcal{E}$, on note $f(x)$ le reste de la division euclidienne de $35x$ par 26.
   (a) Montrer que l'on définit ainsi une bijection de $\mathcal{E}$ sur $\mathcal{E}$.
   (b) On convient de coder un mot quelconque de la façon suivante : on remplace chaque lettre α du mot par la lettre β dont le numéro $g(\beta)$ est tel que $g(\beta) = f(x)$, où $x = g(\alpha)$. Comment se code le mot OUI ? Montrer que cette méthode de codage est sans ambigüité (deux mots sont distincts ont des codages différents). Quel est le mot dont la codage est NWN ?
   (c) On veut généraliser en remplaçant $35x$ par $ax+b$, avec a et b entiers naturels et $a \neq 0$. Quelle(s) hypothèse(s) doit-on faire sur a et b pour que la même méthode s'applique ?
2. Pour tout couple d'entiers (x, y) de $\mathcal{E} \times \mathcal{E}$, on note $f(x, y)$ et $h(x, y)$ les uniques entiers de $\mathcal{E}$ tels que
   $$f(x, y) \equiv 5x + 17y\ [26] \text{ et } h(x, y) \equiv 4x + 15y\ [26].$$
   (a) Justifier que l'application $f \times h$ est une bijection de $\mathcal{E} \times \mathcal{E}$ sur $\mathcal{E} \times \mathcal{E}$.
   (b) On convient de coder tout mot contenant un nombre *pair* de lettres de la façon suivante : en partant de la gauche vers la droite, on remplace chaque couple de lettres successives (α, β) par le couple (γ, δ) dont les numéros $s = g(\gamma)$, $t = g(\delta)$ sont donnés par
   $$s = f(x, y) \text{ et } t = h(x, y),\ \text{où } x = g(\alpha) \text{ et } y = g(\beta) \text{ sont les numéros de } \alpha \text{ et } \beta.$$
   Comment se code le mot ENFANT ? Le codage d'une lettre dépend-il de la place de cette lettre dans le mot ? Démontrer que le principe de codage est sans ambigüité, et que tout mot d'un nombre pair de lettres est le codage d'un et d'un seul mot. Quel est le mot dont le codage est XMEO ?
   (c) On voudrait généraliser cette méthode de codage à un alphabet comprenant m lettres, en considérant les fonctions
   $$f(x, y) \equiv ax + by\ [m] \text{ et } h(x, y) \equiv cx + dy\ [m],$$
   avec a, b, c, d des entiers naturels. Donner une condition sur a, b, c, d et m assurant que la méthode de codage fonctionne encore.

Correction.

1. (a) Il suffit de remarquer que 35 est inversible modulo 26. En effet, il est premier avec 26, et l'utilisation de l'algorithme d'Euclide conduit à la relation
   $$1 = 3 \times 35 - 4 \times 26.$$
   Son inverse modulo 26 est donc 3, et pour tout a dans $\mathcal{E}$, l'équation $f(x) = a$ a pour seule solution le nombre de $\mathcal{E}$ congru à $3a$ modulo 26. En effet, si $35x \equiv a\ [26]$, alors $3 \times 35x \equiv 3a\ [26]$ et donc $x \equiv 3a\ [26]$.
   (b) Le principe est le suivant. On remplace une lettre par le nombre correspondant. On

code ce nombre en utilisant f. On transcrit le nombre obtenu par la lettre correspondante. Ainsi, à O est associé 14, transformé par f en 22, qui donne W. De même, U est transformé en 20, lui-même transformé en 24, à qui est associé Y, et I est transformé en U. Ainsi, le mot OUI se code WYU. Pour prouver que le codage est sans ambigüité, il suffit de prouver que l'application qui à une lettre associe son codage est injective. Mais cette application s'écrit $g^{-1} \circ f \circ g$. C'est une composée d'applications bijectives, elle est elle-même bijecive, donc injective. Pour trouver le mot dont le codage est NWN, il faut inverser l'application précédente. Mais on a déjà observé à la première question qu'on inversait f en considérant l'application qui à x de $\mathcal{E}$ associe le reste dans la division euclidienne de $3x$ par 26. En procédant comme ci-dessus, on trouve que le mot initial est NON.

(c) Tout fonctionne exactement de la même façon, pourvu que l'application qui à x associe le reste de $ax + b$ soit inversible modulo 26. Ceci est possible si et seulement si a est inversible modulo 26, c'est-à-dire si et seulement si a est premier avec 26.

2. (a) Puisque $\mathcal{E} \times \mathcal{E}$ est un ensemble fini, il suffit de prouver que $f \times h$ est une injection pour prouver que c'est une bijection. Autrement dit, pour tous couples (x, y) et (x', y') de $\mathcal{E} \times \mathcal{E}$ vérifiant

$$\begin{cases} 5x + 17y & \equiv & 5x' + 17y' \ [26] \\ 4x + 15y & \equiv & 4x' + 15y' \ [26] \end{cases}$$

on veut prouver que $x = x'$ et $y = y'$. Mais, si on fait $4(L1) - 5(L2)$, on trouve :

$$-7y = -7y' \ [26].$$

De même, si on fait $15(L1) - 17(L2)$, on trouve

$$7x \equiv 7x' \ [26].$$

Comme 7 est inversible modulo 26 (il est premier avec 26), ceci entraîne que $x = x'$ et $y = y'$, et donc que $f \times h$ est injective.

(b) On découpe le mot par couple de deux lettres. On commence par coder EN. On a $x = 4$ et $y = 13$, d'où $f(x, y) = 7$ et $h(x, y) = 3$. Ainsi, EN se code en HD. De même, FA se code en ZU et NT se code en YZ. Le codage du mot ENFANT est donc HDZUYZ. Le codage d'une lettre dépend de sa place dans le mot, puisqu'on code des binômes de deux lettres ensemble. Pour prouver que le codage est sans ambigüité et que tout mot d'un nombre pair de lettres est le codage d'un mot, il suffit de vérifier que le codage de deux lettres est sans ambigüité et que tout mot de deux lettres est le codage d'un autre mot de deux lettres. Mais c'est exactement le sens de la question précédente. Pour trouver le mot dont le codage est XMEO, il faut déjà inverser l'application $f \times g$. Autrement dit, étant donné $(a, b) \in \mathcal{E} \times \mathcal{E}$, on veut trouver $(x, y) \in \mathcal{E} \times \mathcal{E}$ tel que

$$\begin{cases} 5x + 17y & \equiv & a \ [26] \\ 4x + 15y & \equiv & b \ [26] \end{cases}$$

En effectuant les mêmes opérations que ci-dessus, on trouve

$$-7y \equiv 4a - 5b \ [26] \text{ et } 7x = 15a - 17b \ [26].$$

On inverse maintenant -7 (c'est-à-dire encore 19) modulo 26, et l'algorithme d'Euclide donne

$$1 = -8 \times 26 + 11 \times 19.$$

Ainsi, on obtient

$$y \equiv 44a - 55b \equiv 18a - 3b \equiv 18a + 23b \ [26].$$

On fait de même avec 7, dont un inverse est 15, et on trouve

$$x \equiv 17a + 5b \ [26].$$

On décode ensuite par bloc de 2. Pour XM, on a $a = 23$, $b = 12$, et donc $x = 9$, $y = 14$, on trouve JO, et pour EO, on trouve IE. Le mot décodé est donc JOIE.

(c) On veut trouver une condition portant sur a, b, c, d et m pour que le système

$$\begin{cases} ax + by & \equiv & s \ [m] \\ cx + dy & \equiv & t \ [m] \end{cases}$$

admette toujours au plus une solution. Mais, si on raisonne comme ci-dessus, ce système entraîne

$$(ad - bc)x \equiv bs - dt \ [m] \text{ et } (ad - bc)y \equiv at - cs \ [m].$$

On voit que si $ad - bc$ est inversible modulo m, autrement dit si $ad - bc$ et m sont premiers entre eux, alors on a toujours au plus une solution (et donc en fait exactement une solution, car on travaille avec une application allant d'un ensemble fini dans lui-même). Donc si $ad - bc$ est premier avec m, cette méthode de codage continue de fonctionner.

Exercice 28.

Résoudre, dans $\mathbb{Z}^2$, les équations diophantiennes suivantes :

1. $xy = 2x + 3y$.
2. $x^2 - y^2 - x + 3y = 30$.
3. $x^2 - 5y^2 = 3$.

Correction.

1. On remarque que $xy = 2x + 3y \iff (x - 3)(y - 2) = 6$. Ainsi, $x - 3 | 6$, ce qui impose $x - 3 \in \{-6, -3, -2, -1, 0, 1, 2, 3, 6\}$ soit encore $x \in \{-3, 0, 1, 2, 3, 4, 5, 6, 9\}$. Pour $x = 0$, on obtient $y - 2 = -2$, ie $y = 0$. Pour $x = 3$, l'équation devient $0 = 6$ et n'a pas de solutions. Pour $x = 6$, on trouve $y - 2 = 2$ soit $y = 4$. Pour $x = 9$, on obtient $y = 3$, pour $x = -3$, $y = 1$ et ainsi de suite. L'ensemble des solutions est donc $\{(-3, 1); (0, 0); (1, -1); (2, -4); (4, 8); (5, 5); (6, 4); (9, 3)\}$.
2. On factorise de la même façon en mettant sous forme canonique :

$$x^2 - y^2 - x + 3y = 30 \iff \left(x - \frac{1}{2}\right)^2 - \left(y - \frac{3}{2}\right)^2 = 28 \iff (x + y - 2)(x - y + 1) = 28.$$

On a donc $x + y - 2 | 28$ et $x + y - 2 \neq 0$ soit $x + y - 2 \in \{-28, -14, -7, -4, -2, -1, 1, 2, 4, 7, 14, 28\}$. Si $x + y - 2 = -28$, alors $x - y + 1 = -1$, et

donc le couple (x, y) correspondant est solution du système

$$\begin{cases} x+y &= -26 \\ x-y &= -2. \end{cases}$$

On résoud ce système et on trouve $x = -14$, $y = -12$. On fait de même pour les autres cas, et on trouve, sauf erreur, que l'ensemble des solutions est

$$\{(-14,-12);(-5,0);(-5,3);(-14,-15);(15,-12);(6,0);(6,3);(15,15)\}.$$

3. On écrit l'équations modulo 5, et on trouve que $x^2 \equiv 3\ [5]$. Or, si $x \equiv \pm 1\ [5]$, alors $x^2 \equiv 1\ [5]$ et si $x \equiv \pm 2\ [5]$, alors $x^2 \equiv 4\ [5]$ et donc l'équation $x^2 = 3\ [5]$ n'a pas de solutions. Ainsi, l'équation de départ n'a pas de solutions dans $\mathbb{Z}^2$.

b. Groupes

Exercice 29.

On note $GL_n(\mathbb{Z})$ l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$, à coefficients dans $\mathbb{Z}$, qui sont inversibles et dont l'inverse est à coefficients dans $\mathbb{Z}$.

1. Démontrer que si M est à coefficients dans $\mathbb{Z}$, alors $M \in GL_n(\mathbb{Z})$ si et seulement si $\det(M) = \pm 1$.
2. En déduire que $GL_n(\mathbb{Z})$ est un sous-groupe de $GL_n(\mathbb{R})$.

Correction.

1. Prenons d'abord $M \in GL_n(\mathbb{Z})$. Alors on a

$$\det(M) \times \det(M^{-1}) = \det(MM^{-1}) = \det(I_n) = 1$$

et de plus $\det(M)$ et $\det(M^{-1})$ sont des éléments de $\mathbb{Z}$. Ceci n'est possible que si $\det(M)$ et $\det(M^{-1})$ sont égaux à 1 ou -1. Réciproquement, si $\det(M) = \pm 1$, alors les formules de Cramer nous disent que

$$M^{-1} = \frac{1}{\det M}(\text{comat } M)^T.$$

La comatrice d'une matrice à coefficients dans $\mathbb{Z}$ étant à coefficients dans $\mathbb{Z}$ et $\det(M)$ valant ± 1, on a bien que M^{-1} est une matrice à coefficients entiers.

2. On remarque d'abord que $I_n \in GL_n(\mathbb{Z})$. Ensuite, si $A, B \in GL_n(\mathbb{Z})$, des formules

$$\det(A^{-1}) = \frac{1}{\det(A)}$$

et

$$\det(AB) = \det(A)\det(B)$$

on déduit facilement que $\det(A^{-1})$ et $\det(AB)$ sont éléments de $\{-1, 1\}$ et donc A^{-1}, AB sont éléments de $GL_n(\mathbb{Z})$.

Exercice 30.

Soit $(G, \cdot)$ un groupe. Pour $a \in G$, on note $\tau_a : G \to G$ défini par $\tau_a(x) = axa^{-1}$.

1. Démontrer que τ_a est un endomorphisme de G.
2. Vérifier que, pour tous $a, b \in G$, $\tau_a \circ \tau_b = \tau_{ab}$.
3. Montrer que τ_a est bijective et déterminer son inverse.
4. En déduire que $\Theta = \{\tau_a;\ a \in G\}$ muni du produit de composition est un groupe.

Correction.

1. Il suffit d'appliquer la définition : pour tous $x, y \in G$, on a
$$\tau_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \tau_a(x)\tau_a(y).$$
2. Soit $x \in G$. On a
$$\tau_a \circ \tau_b(x) = \tau_a(bxb^{-1}) = abxb^{-1}a^{-1}$$
tandis que
$$\tau_{ab}(x) = abx(ab)^{-1} = abxb^{-1}a^{-1}.$$
On a donc $\tau_a \circ \tau_b = \tau_{ab}$.
3. Soit $a \in G$. On pourrait prouver que τ_a est injectif en calculant son noyau, puisqu'il est surjectif, mais c'est plus facile d'appliquer la question précédente. Avec $b = a^{-1}$, elle donne
$$\tau_a \circ \tau_{a^{-1}} = \tau_{aa^{-1}} = \tau_e = Id_G$$
et en inversant le rôle joué par a et b, on a aussi
$$\tau_{a^{-1}} \circ \tau_a = Id_G.$$
Ainsi, τ_a est inversible d'inverse $\tau_{a^{-1}}$.
4. On va prouver que $\Theta = \{\tau_a;\ a \in G\}$ est un sous-groupe de $(S_G, \circ)$. Il est non-vide parce qu'il contient τ_e. Si $\tau_a, \tau_b \in \Theta$, alors
$$(\tau_a)^{-1} = \tau_{a^{-1}} \in \Theta$$
et
$$\tau_a \circ \tau_b = \tau_{ab} \in \Theta.$$
Ainsi, $(\Theta, \circ)$ est bien un sous-groupe de $(S_G, \circ)$.

Exercice 31.

Soit G un groupe fini d'élément neutre e. On suppose que le cardinal de G est pair. Démontrer qu'il existe $x \in G$ avec $x \neq e$ tel que $x = x^{-1}$.

Correction.

Notons, pour $x \in G$, $F_x = \{x, x^{-1}\}$. Alors il est facile de voir que l'on a ou bien $F_x = F_y$, ou bien $F_x \cap F_y = \varnothing$ pour tout $x, y \in G$. En effet, si $x = y^{-1}$, alors $x^{-1} = y$ et on a bien $F_x = F_y$. G s'écrit alors comme la réunion disjointe de tous les F_x différents. Au moins l'un parmi ces F_x est de cardinal 1 : il s'agit de F_e. Si tous les autres étaient de cardinal 2, alors le groupe serait de cardinal impair, ce qui n'est pas le cas. Il existe donc $x \neq e$ tel que le cardinal de F_x soit égal à 1, c'est-à-dire tel que $x = x^{-1}$.

Exercice 32.

Soit G un ensemble fini muni d'une loi de composition interne $\star$ associative. On dit qu'un élément a de G est régulier si les deux conditions suivantes sont réalisées :

— l'égalité $a \star x = a \star y$ entraine $x = y$;

— l'égalité $x \star a = y \star a$ entraine $x = y$.

On suppose que tous les éléments de G sont réguliers, et on fixe $a \in G$.

1. Démontrer qu'il existe $e \in G$ tel que $a \star e = a$.
2. Démontrer que, pour tout $x \in G$, on a $e \star x = x$.
3. Démontrer que, pour tout $x \in G$, on a $x \star e = x$.
4. Démontrer que $(G, \star)$ est un groupe.
5. Le résultat subsiste-t-il si G n'est pas fini ?

Correction.

1. Considérons l'application $\phi : G \to G,\ x \mapsto a \star x$. L'hypothèse nous dit que ϕ est injective. Puisque G est fini, elle est aussi surjective, et donc il existe $e \in G$ tel que $a \star e = \phi(e) = a$.
2. On a $a \star e \star x = a \star x$ (car la loi est associative) et donc, puisque a est régulier, on a $e \star x = x$.
3. On a $x \star e \star a = x \star a$ d'après la question précédente, et donc puisque a est régulier, on a $x \star e = x$.
4. Il suffit désormais de prouver que tout élément est inversible. Soit $b \in G$. Puisque $x \mapsto b \star x$ est injective, donc surjective, il existe $c \in G$ tel que $b \star c = e$. De plus, on a $c \star b \star c = c \star e = c$, et donc puisque c est régulier, on en déduit que $c \star b = e$. Ainsi, c est un inverse de b.
5. Non, ce n'est pas vrai, car $(\mathbb{N}, +)$ vérifie que tout élément est régulier, mais ce n'est pas un groupe.

Exercice 33.

Soit $(G, \cdot)$ un groupe fini et A, B deux sous-groupes de G. On note $AB = \{ab;\ a \in A,\ b \in B\}$. Montrer que AB est un sous-groupe de G si et seulement si $AB = BA$.

Correction.

Supposons d'abord que $AB = BA$. Alors AB est un sous-groupe de G car :

1. $e \in AB$, car $e = ee$ avec $e \in A$ et $e \in B$ (ce sont des sous-groupes) ;

2. AB est stable par passage au produit. En effet, si $x = ab \in AB$ et $y = a'b' \in AB$, alors $xy = aba'b'$. Or, ba' est un élément de BA, c'est donc aussi un élément de AB et donc $ba' = a''b''$ avec $a'' \in A$ et $b'' \in B$. On en déduit que

$$xy = aa''b''b \in AB$$

puisque $aa'' \in A$ et $bb'' \in B$.

3. AB est stable par passage à l'inverse. En effet, si $x = ab \in AB$, alors $x^{-1} = b^{-1}a^{-1}$ est élément de BA et $BA = AB$.

Réciproquement, supposons que AB est un sous-groupe de G et prouvons que $AB = BA$. Soit d'abord $x = ab \in AB$. Alors $x^{-1} = b^{-1}a^{-1} \in AB$ et donc $b^{-1}a^{-1} = a'b'$ avec $a' \in A$ et $b' \in B$. On passe à l'inverse :

$$ab = b'^{-1}a'^{-1} \in BA.$$

De même, si $y = ba \in BA$, alors $y^{-1} = a^{-1}b^{-1} \in AB$, et donc $y = (y^{-1})^{-1} \in AB$.

Exercice 34.

Démontrer que les groupes multiplicatifs $(\mathbb{R}^*, \cdot)$ et $(\mathbb{C}^*, \cdot)$ ne sont pas isomorphes.

Correction.

Supposons que ces deux groupes soient isomorphes et soit f un isomorphisme de $(\mathbb{C}^*, \cdot)$ dans $(\mathbb{R}^*, \cdot)$. Posons $a = f(i)$. Alors

$$f(i^4) = a^4 = 1$$

et donc $a^2 = 1$ puisque $a^2 > 0$. D'où $1 = a^2 = f(i^2) = f(-1)$ et $1 = f(1)$. f ne peut pas être injectif, on a obtenu une contradiction.

Exercice 35.

Un groupe $(G, \cdot)$ est dit divisible si, pour tout $g \in G$ et tout $n \in \mathbb{N}^*$, il existe $u \in G$ tel que $u^n = g$.

1. Le groupe $(\mathbb{Q}, +)$ est-il divisible ?
2. Montrer que $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \cdot)$ ne sont pas isomorphes.

Correction.

1. Soit $x \in \mathbb{Q}$, et $n \in \mathbb{N}^*$. Alors, si on pose $y = x/n$, c'est un élément de $\mathbb{Q}$ et $ny = x$: le groupe $(\mathbb{Q}, +)$ est divisible.
2. Procédons en deux temps. On commence par montrer que si G et H sont deux groupes isomorphes et si G est divisible, alors H est divisible. En effet, soit $\phi : G \to H$ un isomorphisme. Soit $h \in H$. Il existe $g \in G$ tel que $h = \phi(g)$. Puisque G est divisible, pour tout $n \geq 1$, il existe $u \in G$ tel que $u^n = g$. Posons $v = \phi(u)$. Alors puisque ϕ est un morphisme, on a $v^n = h$ et h est divisible. Pour conclure, il suffit donc de prouver que $(\mathbb{Q}_+^*, \cdot)$ n'est pas divisible. Mais par exemple, pour $g = 2$ et $n = 2$, il n'existe par de rationnel u tel que

$u^2 = 2$ (car $\sqrt{2}$ est irrationnel). Les deux groupes ne sont donc pas isomorphes.

Exercice 36. *Théorème de Lagrange*

Soit $(G, \cdot)$ un groupe fini et H un sous-groupe de G.

1. Montrer que pour tout $a \in G$, H et $aH = \{ah;\ h \in H\}$ ont le même nombre d'éléments.
2. Soient $a, b \in G$. Démontrer que $aH = bH$ ou $aH \cap bH = \varnothing$.
3. En déduire que le cardinal de H divise le cardinal de G.

Correction.

1. Soit $f : H \to aH$ définie par $f(h) = ah$. Il s'agit clairement d'une surjection de H sur aH. De plus, si $ah_1 = ah_2$, alors $h_1 = h_2$ car a est inversible, et donc f est aussi injective. f est donc une bijection de H sur aH ; ces deux ensembles ont le même nombre d'éléments.
2. Supposons que $aH \cap bH \neq \varnothing$ et prouvons que $aH = bH$. Par symétrie, il suffit de prouver que $aH \subset bH$. Soit $x \in aH \cap bH$, $x = ah_1 = bh_2$. Prenons $y = ah \in aH$. Alors $a = bh_2h_1^{-1}$ et donc $y = bh_2h_1^{-1}h \in bH$.
3. La réunion des ensembles aH est clairement égale à G (si $x \in G$, il est dans xH). On ne garde que les aH deux à deux disjoints et par les deux questions précédentes, on réalise ainsi une partition de G avec des ensembles qui ont tous le même cardinal, à savoir le cardinal de H. Si k est le nombre d'ensembles nécessaires pour réaliser cette partition, on a
$$k\text{card}(H) = \text{card}(G)$$
et donc le cardinal de H divise celui de G.

c. Anneaux, sous-anneaux

Exercice 37.

Soit $\mathbb{D}$ l'ensemble des nombres décimaux,
$$\mathbb{D} = \left\{ \frac{n}{10^k};\ n \in \mathbb{Z}, k \in \mathbb{N} \right\}.$$
Démontrer que $(\mathbb{D}, +, \times)$ est un anneau. Quels sont ses éléments inversibles ?

Correction.

On va prouver que $(\mathbb{D}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$. On remarque d'abord que $\mathbb{D} \subset \mathbb{Q}$, puis que $1 \in \mathbb{D}$. De plus, soient $x = \frac{n}{10^k}$ et $y = \frac{m}{10^l}$ deux éléments de $\mathbb{D}$. Alors
$$x - y = \frac{n10^l - m10^k}{10^{k+l}} \text{ et } xy = \frac{nm}{10^{k+l}}$$
sont clairement des éléments de $\mathbb{D}$, et $(\mathbb{D}, +, \times)$ est bien un sous-anneau de $(\mathbb{Q}, +, \times)$. Déterminons

ensuite les inversibles de $(\mathbb{D},+,\times)$. Soit $x=\frac{n}{10^k}$ inversible, d'inverse $y=\frac{m}{10^l}$. Alors

$$xy=1 \iff nm=10^{k+l}.$$

On en déduit que les seuls diviseurs premiers de n sont 2 et 5, autrement dit que n s'écrit $\pm 2^p5^q$ pour $p,q\in\mathbb{N}$. Réciproquement, soit $x=\frac{\pm 2^p5^q}{10^k}$ et montrons que x est inversible dans $\mathbb{D}$. Posons $y=\frac{\pm 10^k}{2^p5^q}$. Il suffit de vérifier que y est élément de $\mathbb{D}$. Mais on peut aussi écrire

$$y=\frac{\pm 10^k 2^q 5^p}{2^{p+q}5^{p+q}}=\frac{\pm 10^k 2^q 5^p}{10^{p+q}}\in\mathbb{D}.$$

Ainsi, les inversibles de $(\mathbb{D},+,\times)$ sont les éléments $\frac{\pm 2^p5^q}{10^k}$, avec $p,q,k\in\mathbb{N}$.

Exercice 38.

On considère $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2};\ a,b\in\mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}],+,\times)$ est un anneau.
2. On note $N(a+b\sqrt{2})=a^2-2b^2$. Montrer que, pour tous x,y de $\mathbb{Z}[\sqrt{2}]$, on a $N(xy)=N(x)N(y)$.
3. En déduire que les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont ceux s'écrivant $a+b\sqrt{2}$ avec $a^2-2b^2=\pm 1$.

Correction.

1. Il suffit de prouver que c'est un sous-anneau de $(\mathbb{R},+,\times)$. Mais $\mathbb{Z}[\sqrt{2}]$ est
   — stable par la loi $+$: $(a+b\sqrt{2})+(a'+b'\sqrt{2})=(a+a')+(b+b')\sqrt{2}$.
   — stable par la loi $\times$:
   $$(a+b\sqrt{2})\times(a'+b'\sqrt{2})=(aa'+2bb')+(ab'+a'b)\sqrt{2}$$
   .
   — stable par passage à l'opposé $-(a+b\sqrt{2})=-a+(-b)\sqrt{2}$.
   De plus, $1\in\mathbb{Z}[\sqrt{2}]$, ce qui achève la preuve du fait que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.
2. Posons $x=a+b\sqrt{2}$ et $y=a'+b'\sqrt{2}$. En tenant compte de la formule pour le produit obtenue à la question précédente, on a
   $$\begin{aligned} N(xy) &= (aa'+2bb')^2-2(ab'+a'b)^2 \\ &= (aa')^2-2(ab')^2-2(a'b)^2+4(bb')^2. \end{aligned}$$
   D'autre part,
   $$\begin{aligned} N(x)\times N(y) &= (a^2-2b^2)(a'^2-2b'^2) \\ &= (aa')^2-2(ab')^2-2(a'b)^2+4(bb')^2. \end{aligned}$$
3. Soit $x=a+b\sqrt{2}$. Supposons d'abord que x est inversible, d'inverse y. Alors $N(xy)=N(1)=1$, et donc $N(x)N(y)=1$. Puisque $N(x)$ et $N(y)$ sont tous les deux des entiers, on

a nécessairement $N(x) = \pm 1$. Réciproquement, si $N(x) = \pm 1$, alors, en utilisant la quantité conjuguée :

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \pm(a-b\sqrt{2})$$

ce qui montre que $a+b\sqrt{2}$ est inversible, d'inverse $\pm(a-b\sqrt{2})$.

Exercice 39.

Soit A un anneau. On appelle caractéristique de A l'ordre de 1_A dans le groupe additif $(A,+)$. Dans la suite, on supposera que A est de caractéristique finie n.

1. Démontrer que, pour tout $x \in A$, $nx = 0$.
2. Démontrer que si A est intègre, n est un nombre premier.
3. Démontrer que si A est intègre et commutatif, alors $x \mapsto x^n$ est un morphisme d'anneaux.

Correction.

1. Il s'agit juste d'un jeu d'écriture ! On écrit en effet :

$$nx = n(1_A x) = (n1_A)x = 0_A x = 0_A.$$

2. Raisonnons par contraposée. Supposons que $n = pq$ avec $1 < p, q < n$. Alors posons $x = p1_A$ et $y = q1_A$. Ni x ni y ne sont nuls puisque 1_A est d'ordre exactement n. Pourtant, leur produit $xy = (pq)1_A$ est nul et A n'est pas intègre. On vient de démontrer que si n n'est pas premier, alors A n'est pas intègre. Donc A intègre entraîne n premier.
3. On va noter $n = p$ pour souligner que n est un nombre premier, et $f(x) = x^p$. Il n'y a pas de difficultés à vérifier que $f(1_A) = 1_A$ et $f(xy) = f(x)f(y)$ (par la commutativité de A) pour tous $x, y \in A$. D'autre part, on a

$$f(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{n-k} = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{n-k}.$$

D'après le résultat de la première question, il suffit de vérifier que $p|\binom{p}{k}$ pour tout $k = 1, \ldots, p-1$. Mais on a

$$p! = \binom{p}{k} \times k! \times (p-k)!.$$

On a donc

$$p|\binom{p}{k} \times k! \times (p-k)!.$$

Mais comme p est premier et que les décompositions en produits de facteurs premiers de $k!$ et de $(p-k)!$ ne font intervenir que des nombres premiers strictement inférieurs à p, p est premier avec le produit $k! \times (p-k)!$. Ainsi, $p|\binom{p}{k}$, et on a bien $f(x+y) = f(x) + f(y)$. f est bien un morphisme d'anneaux.

3. Exercices d'approfondissement

a. Groupes

Exercice 40.

Soit H un sous-groupe strict d'un groupe $(G, \cdot)$. Déterminer le sous-groupe engendré par le complémentaire de H.

Correction.

Notons K le complémentaire de H et fixons a un élément de K (rappelons que H est strictement inclus dans G). Nous allons prouver que le sous-groupe engendré par K, que nous allons noter L, est égal à G tout entier. Puisque ce sous-groupe contient déjà K, il suffit de prouver qu'il contient également son complémentaire, à savoir H. Soit donc $x \in H$. Alors ax ne peut pas être un élément de H, sinon $a = axx^{-1}$ serait élément de H lui aussi. Donc ax est élément de K. Mais alors, $x = a^{-1}ax$ est un élément de L puisque a et ax sont tous deux éléments de K, donc de L, et que L est un sous-groupe (ce qui entraîne que $a^{-1} \in L$ et que le produit $a^{-1}ax$ est aussi dans L).

Exercice 41.

Soit f un morphisme non constant d'un groupe fini $(G, \cdot)$ dans $(\mathbb{C}^*, \cdot)$. Calculer $\sum_{x \in G} f(x)$.

Correction.

Puisque f n'est pas constante, il existe $a \in G$ tel que $f(a) \neq 1$. Maintenant, l'application $x \mapsto ax$ est une permutation de G : en effet, pour tout $y \in G$, il existe un unique $x \in G$ tel que $y = ax$ (x est égal à $a^{-1}y$). On en déduit que

$$\sum_{x \in G} f(ax) = \sum_{x \in G} f(x).$$

Mais d'autre part, puisque f est un morphisme de groupes, on a aussi

$$\sum_{x \in G} f(ax) = \sum_{x \in G} f(a)f(x) = f(a) \sum_{x \in G} f(x).$$

Ainsi, il vient

$$\big(f(a) - 1\big) \times \sum_{x \in G} f(x) = 0.$$

Puisque $f(a) \neq 1$, on en déduit que $\sum_{x \in G} f(x) = 0$.

b. Anneaux, sous-anneaux

Exercice 42.

Soit A un anneau intègre commutatif fini. Démontrer que A est un corps.

Correction.

Fixons $a \in A$ et considérons le morphisme d'anneaux $A \to A,\ x \mapsto ax$. Alors ce morphisme d'anneaux est injectif, car son noyau est réduit à $\{0_A\}$ puisque A est intègre. Puisque A est fini, ce morphisme est nécessairement bijectif, et donc il existe $x \in A$ tel que $ax = 1_A$. Par commutativité de A, on a aussi $xa = 1_A$ et donc a admet un inverse : A est un corps. Remarquons que l'on peut se passer de l'hypothèse que A est commutatif, par exemple en faisant le même raisonnement avec $x \mapsto xa$, et en prouvant que l'inverse à droite et l'inverse à gauche coïncident.