4MA235
Master de mathématiques
Année académique 2025-2026

SCIENCES SORBONNE UNIVERSITÉ

Feuille d'exercices 1

Solutions

Exercice 1 (Applications de l'écriture en base b)

1. Soit $f \in \mathbb{Z}[X]$ un polynôme tel que ses coefficients soient tous des entiers naturels. Montrer que la connaissance de $f(1)$ et $f(m)$, avec $m > f(1)$ permet de déterminer (les coefficients de) f. Déterminer explicitement f lorsque $f(1) = 10$ et $f(15) = 2026$.

   Posons $f = a_0 + a_1X + \cdots + a_nX^n$. On a les relations $f(1) = a_1 + \cdots + a_n \geq \max_i\{a_i\}$ (car $a_i \geq 0$ pour tout i), d'où l'identité $f(m) = a_0 + a_1m + \cdots + a_nm^n$, avec

   $$0 \leq a_i \leq \max_i\{a_i\} \leq f(1) < m,$$

   ce qui implique que $a_0 + a_1m + \cdots + a_nm^n$ est l'écriture de $f(m)$ en base m. Connaissant les entiers m et $f(m)$, il suffit donc de déterminer explicitement cette écriture. En particulier, pour $f(1) = 10$ et $f(15) = 2026$, on a $15 > f(1)$ et les relations

   $$2026 = 1 + 2025 = 1 + 45^2 = 1 + 9 \cdot 15^2,$$

   amènent alors à l'identité $f = 9X^2 + 1$.

2. Notons $\mathcal{P}_0(\mathbb{N})$ l'ensemble des parties finies de $\mathbb{N}$. Montrer que l'application $f : \mathcal{P}_0(\mathbb{N}) \to \mathbb{N}$ définie par

   $$f(X) = \sum_{n \in X} 2^n$$

   est bijective. Vérifier que pour $X \subset Y$, on a $f(X) \leq f(Y)$. La réciproque est-elle vraie ?

Étant donné un sous-ensemble X de $\mathbb{N}$, notons $\chi_X : X \to \{0,1\}$ sa ***fonction caractéristique***, définie par

$$\chi_X(n) = \begin{cases} 1 \text{ si } n \in X, \\ \\ 0 \text{ sinon.} \end{cases}$$

Si Y est un second sous-ensemble de $\mathbb{N}$, on a alors l'identité $X = Y$ si et seulement si $\chi_X = \chi_Y$. Par définition, pour $X \in \mathcal{P}_0(\mathbb{N})$, on a l'identité

$$f(X) = \sum_{n\in\mathbb{N}} \chi_X(n)2^n,$$

ce qui implique que $\sum_{n\in\mathbb{N}} \chi_X(n)2^n$ est l'écriture de $f(X)$ en base 2. L'injectivité de f découle alors de l'unicité d'une telle écriture et la surjectivité de son existence. Étant donné $Y \subset X$, on a $\chi_Y(n) \leq \chi_X(n)$ pour tout $n \in \mathbb{N}$, d'où les relations

$$f(Y) = \sum_{n\in\mathbb{N}} \chi_Y(n)2^n \leq \sum_{n\in\mathbb{N}} \chi_X(n)2^n = f(X).$$

Étant donné $X \in \mathcal{P}_0(\mathbb{N})$ non vide, posons $m = \max(X) + 1$ et $Y = \{m\}$, on a alors $X \not\subset Y$ et

$$f(X) = \sum_{n\in X} 2^n \leq \sum_{0\leq n<m} 2^n = 2^m - 1 < 2^m = f(Y),$$

ce qui montre que la réciproque est fausse.

Exercice 2 (Applications de la factorisation unique) – L'ensemble $\mathbb{Z}^{\mathbb{N}}$ des applications $f : \mathbb{N} \to \mathbb{Z}$ est muni d'une structure naturelle de groupe abélien : étant données $f, g \in \mathbb{Z}^{\mathbb{N}}$, on pose

$$(f + g)(n) = f(n) + g(n)$$

pour tout $n \in \mathbb{N}$. Le ***support*** de $f \in \mathbb{Z}^{\mathbb{N}}$ est l'ensemble

$$\mathrm{Supp}(f) = \{n \in \mathbb{N} \mid f(n) \neq 0\}.$$

Nous dirons que f est ***à support fini*** si $\mathrm{Supp}(f)$ est un ensemble fini. Notons $\mathbb{Z}_0^{\mathbb{N}}$ le sous-ensemble de $\mathbb{Z}^{\mathbb{N}}$ des applications à support fini. Vérifier que $\mathbb{Z}_0^{\mathbb{N}}$ est un sous-groupe de $\mathbb{Z}^{\mathbb{N}}$ et montrer qu'il est isomorphe au groupe (multiplicatif) $\mathbb{Q}_{>0}^{\times}$ des rationnels strictement positifs.

La première assertion découle de l'inclusion

$$\mathrm{Supp}(f + g) \subset \mathrm{Supp}(f) \cup \mathrm{Supp}(g)$$

et de l'identité $\mathrm{Supp}(-f) = \mathrm{Supp}(f)$. Soit $s : \mathbb{N} \to \mathbb{N}$ l'application qui associe à un entier naturel n le plus petit nombre premier strictement supérieur à n et considérons l'application $p : \mathbb{N} \to \mathbb{N}$ définie par $p(0) = 2$ et $p(n + 1) = s(p(n))$. L'image de p coïncide alors avec l'ensemble des nombres premiers. Étant donnée une application $f \in \mathbb{Z}_0^{\mathbb{N}}$, posons

$$\varphi(f) = \prod_{n\in\mathrm{Supp}(f)} p(n)^{f(n)}.$$

On définit ainsi une application $\varphi : \mathbb{Z}_0^{\mathbb{N}} \to \mathbb{Q}_{>0}^{\times}$. La bijectivité de φ découle de la factorisation unique dans $\mathbb{Q}^{\times}$ et du fait que tout nombre premier appartient à l'image de p. Finalement, étant données deux applications à support fini $f, g \in \mathbb{Z}_0^{\mathbb{N}}$, en posant $X = \mathrm{Supp}(f) \cup \mathrm{Supp}(g)$, on a les identités

$$\varphi(f+g) = \prod_{n\in \mathrm{Supp}(f+g)} p(n)^{f(n)+g(n)} = \prod_{n\in X} p(n)^{f(n)+g(n)} = \prod_{n\in X} p(n)^{f(n)} p(n)^{g(n)} =$$
$$= \prod_{n\in X} p(n)^{f(n)} \prod_{n\in X} p(n)^{g(n)} = \prod_{n\in \mathrm{Supp}(f)} p(n)^{f(n)} \prod_{n\in \mathrm{Supp}(g)} p(n)^{g(n)} = \varphi(f)\varphi(g),$$

ce qui montre que φ est un homomorphisme de groupes.

Exercice 3 (Écriture en base $-b$) – Considérons un entier naturel $b > 1$.

1. Montrer qu'un entier $n \in \mathbb{Z}$ s'écrit de manière unique comme

$$n = \sum_{k\geq 0} a_k(-b)^k,$$

où les entiers $a_0, \ldots, a_k \in \{0, \ldots, n-1\}$ sont presque tous nuls, i.e. nuls à partir d'un certain rang. Une telle expression est ***l'écriture de n en base $-b$***. On écrira alors $n = (a_k \cdots a_0)_{-b}$.

On commence en montrant l'existence d'une telle écriture. On procède par récurrence sur l'entier naturel $|n|$. L'assertion est vérifiée pour $|n| = 0$, auquel cas il suffit de poser $a_k = 0$ pour tout $k \in \mathbb{N}$. Pour $n = 1$, il suffit de poser $a_0 = 1$ et $a_k = 0$ pour tout $k > 0$. De même, pour $n = -1$, on pose $a_0 = b - 1, a_1 = 1$ et $a_k = 0$ pour tout $k > 1$. La propriété est donc vérifiée pour $|n| \leq 1$. Soit $n \neq 0$ un entier avec $|n| > 1$ et supposons la propriété vérifiée pour tout entier m tell que $|m| < |n|$. Notons a_0 le reste de la division euclidienne de n par b. Les identités $n = qb + a_0 = (-q)(-b) + a_0$ combinée avec l'unicité du quotient et du reste de la division euclidienne impliquent que a_0 est également le reste de la division euclidienne de n par $-b$. Considérons l'entier $m = \frac{a_0 - n}{b}$. Pour $n \geq 0$, on a les relations

$$|m| = \frac{|a_0 - n|}{b} = \frac{n - a_0}{b} \leq \frac{n}{b} < n = |n|.$$

Pour $n < 0$, on obtient les relations

$$|m| = \frac{a_0 - n}{b} = \frac{a_0 + |n|}{b} \leq \frac{b - 1 + |n|}{b} = \frac{|n| - 1}{b} + 1.$$

On a $\frac{|n|-1}{b} + 1 \geq |n|$ si et seulement si $|n| \leq 1$, ce qui est exclu. Dans les deux cas, on a donc l'inégalité $|m| < |n|$. En appliquant l'hypothèse de récurrence, on a alors l'identité $m = a_1 - a_2 b + \cdots + a_{k+1}(-b)^k$, d'où l'expression $n = a_0 - a_1 b + \cdots + (-1)^k a_k$, ce qui montre l'existence de l'écriture en base $-b$ pour n. Par le principe de récurrence, la propriété est donc vraie pour tout entier. Concernant l'unicité, considérons deux écritures $n = \sum_k a_k(-b)^k = \sum_k c_k(-b)^k$. Supposons qu'il existe un entier k tel que $a_k \neq c_k$ et notons m le plus petit d'entre eux. On a alors $a_k = b_k$ pour tout $k < m$ et $a_m \neq b_m$, d'où l'es identités

$$(a_m - c_m)(-b)^m = \sum_{k>m} (c_m - a_m)(-b)^k = (-b)^{m+1} \sum_{k>m} (c_m - a_m)(-b)^{k-m-1}.$$

On en déduit que b^{m+1} divise $(a_m - c_m)b^m$, ou encore que b divise $a_m - c_m$. Ayant les inégalités $0 \leq a_m, c_m < b$, on a alors nécessairement $a_m = c_m$, ce qui est exclu. L'écriture est donc unique.

2. Décrire un algorithme permettant de déterminer l'écriture en base $-b$ d'un entier.

Notons $r(n)$ le reste de la division euclidienne d'un entier n par b. Ayant fixé n, considérons la suite (m_i) définie par $m_0 = n$

$$m_{k+1} = \begin{cases} \dfrac{r(m_k) - m_k}{b} \text{ si } m_k \neq 0, \\ \\ 0 \text{ sinon.} \end{cases}$$

D'après la démonstration du point 2, pour $|m_k| > 1$, on a $m_{k+1} < m_k$. Il existe alors un entier k tel que $|m_k| \leq 1$. Pour $m_k = 1$, on obtient $m_{k+1} = 0$. De même, pour $m_k = -1$, on a $m_{k+1} = 1$, d'où $m_{k+2} = 0$. On en déduit qu'il existe un entier k tel que $m_k = 0$, auquel cas on a $m_i = 0$ pour tout $i \geq k$. En posant $a_i = r(m_i)$ pour tout entier naturel i, on démontre alors par récurrence l'identité

$$n = a_0 - a_1 b + \cdots + a_i(-b)^i + (-b)^{i+1} m_{i+1}.$$

En particulier, pour $i = k$, on obtient l'expression

$$n = a_0 - a_1 b + \cdots + a_k(-b)^k,$$

qui est donc l'écriture en base $-b$ de n.

3. Déterminer l'écriture de 2026 en base -10.

En appliquant l'algorithme décrit dans le point précédent, on obtient l'écriture

$$2026 = 6 \cdot 1 - 8 \cdot 10 + 1 \cdot 10^2 - 8 \cdot 10^3 + 1 \cdot 10^4 = (18186)_{-10}.$$

4. Soit n un entier non nul et considérons son écriture $n = \sum_k a_k(-b)^k$ en base $-b$. Notons k le plus grand entier naturel tel que $a_k \neq 0$. Vérifier que l'on a l'inégalité

$$k \leq \log_b(|n|) + 2.$$

Pour $n > 0$, l'entier k est nécessairement pair. En effet, dans le cas contraire, on aurait les relations

$$n = \sum_{i=0}^{k} a_i(-b)^i = -b^k + \sum_{i=0}^{k-1} a_i(-b)^i \leq -b^k + (b-1)\sum_{i=0}^{k-1} b^i = -1,$$

ce qui est exclu. L'inégalité de l'énoncé est directement pour $0 < n < b$ (qui correspondent au cas $k = 0$), on peut supposer $k > 0$. En posant $k = 2m$, on a alors $m \geq 1$ et les relations

$$|n| = n = \sum_{i=0}^{2m} a_i(-b)^i \geq a_{2m} b^{2m} - \sum_{i=0}^{m-1} a_{2i+1} b^{2i+1} \geq b^{2m} - (b-1)\sum_{i=0}^{m-1} b^{2i+1} =$$

$$= b^{2m} - b(b-1)\sum_{i=0}^{m-1} b^{2i} = b^k - b\frac{b^k - 1}{b+1} = \frac{b^k + b}{b+1}.$$

De manière générale, étant donné un entier naturel u, la relation $\frac{b^2u+b}{b+1} < u$ est équivalente à $u < \frac{b}{b^2-b-1}$. L'inégalité $b^2 - b - 1 < b$ est équivalente à $b(b-2) \leq 0$. En particulier, pour $b > 2$, on obtient $\frac{b}{b^2-b-1} < 1$. Pour $b = 2$, on a $\frac{b}{b^2-b-1} = 1$. Dans tout les cas, on en déduit l'inégalit'e $\frac{b^2u+b}{b+1} \geq u$ pour tout $u \geq 1$. Par hypothèse, on a $k = 2m \geq 2$, d'où $b^k = b^2 u$, avec $u = b^{k-2} \geq 1$. D'après ce qui précède, on en déduit les relations

$$|n| \geq \frac{b^k + b}{b+1} = \frac{b^2 u + b}{b+1} \geq u = b^{k-2},$$

d'où l'inégalité $k \leq \log_b(|n|) + 2$. Supposons maintenant n négatif. Comme précédemment, on montre que l'entier k est nécessairement impair, soit $k = 2m+1$, avec $m \geq 0$. On obtient alors les relations

$$|n| = -n = -\sum_{i=0}^{2m+1} a_i(-b)^i \geq a_{2m+1}b^{2m+1} - \sum_{i=0}^{m} a_{2i}b^{2i} \geq b^{2m+1} - (b-1)\sum_{i=0}^{m} b^{2i} =$$
$$= b^k - \frac{b^k - 1}{b+1} = \frac{b^{k+1} - b^k + 1}{b+1}.$$

Étant donné un entier u, l'inégalité $\frac{b^2u - bu + 1}{b+1} \geq \frac{u}{b}$ est équivalente à $(b^3 - b^2 - b)u \geq -b$. Ayant $b \geq 2$, on en déduit les relations $b^3 - b^2 - b = b^2(b-1) - b \geq b(b-1)^2 - b = b(b-2) \geq 0$. En particulier, pour tout $u \geq 0$, on a $\frac{b^2u - bu + 1}{b+1} \geq \mathfrak{u}b$. En posant $u = b^{k-1}$, on obtient alors les relations

$$|n| \geq \frac{b^2u - bu + 1}{b+1} \geq \frac{u}{b} = b^{k-2},$$

ce qui amène une fois encore à l'inégalité $k \leq \log_b(|n|) + 2$.

5. Étant donné un entier $n = \sum_k a_k(-b)^k$, posons $f(n) = \sum_n a_k b^k$. On définit ainsi une application $f : \mathbb{Z} \to \mathbb{N}$. Déduire des questions précédentes que f est bijective.

L'injectivité de f découle de l'unicité de l'écriture d'un entier relatif en base $-b$, sa surjectivité est conséquence de l'existence de l'écriture d'un entier naturel en base b.

Exercice 4 – Déterminer tous les entiers n tels que

$$(n^3 + 3) \wedge (n^2 + n + 2) = 16.$$

On rappelle quétant donnés trois entiers a, b et c, on a la relation $(a + bc) \wedge b = a \wedge b$. Dans le cas présent, on obtient les identités

$$(n^3 + 3) \wedge (n^2 + n + 2) = (n^3 + 3 - n(n^2 + n + 2)) \wedge (n^2 + n + 2) =$$
$$= (n^2 + 2n - 3) \wedge (n^2 + n + 2) = (n - 5) \wedge (n^2 + n + 2) =$$
$$= (n - 5) \wedge (6n + 2) = (n - 5) \wedge 32.$$

On est donc réduit à résoudre l'équation $(n-5) \wedge 32 = 16$. L'entier $n-5$ est alors divisible par 16, soit $n = 16m+5$, ce qui donne $16m \wedge 32 = 16$, ou encore $m \wedge 2 = 1$. En posant $m = 2k+1$, on obtient finalement l'expression $n = 32k + 21$, avec $k \in \mathbb{Z}$.

Exercice 5 (Produit fibré et théorème des restes chinois) – Ce long exercice consititue une bonne révision des notions d'algèbre qui seront utilisées dans le cours. Son objectif est de fournir une démonstration du célèbre ***théorème des restes chinois*** dans une formulation générale.

Considérons trois ensembles X, Y et S ainsi que deux applications $f : X \to S$ et $g : Y \to S$. L'ensemble

$$X \times_S Y = \{(x, y) \in X \times Y \mid f(x) = g(y)\}$$

est le ***produit fibré*** de X et Y au dessus de S. Dans la suite, nous supposerons X, Y et S non vides.

1. Montrer que $X \times_S Y = \emptyset$ si et seulement si $\mathrm{Im}(f) \cap \mathrm{Im}(g) = \emptyset$ et que $X \times_S Y = X \times Y$ si et seulement si $\mathrm{Im}(f) = \mathrm{Im}(g)$ est un singleton.

Si l'ensemble $X \times_S Y$ est non vide alors il existe $(x, y) \in X \times Y$, tel que $f(x) = g(y)$. Dans ce cas, on a $f(x) \in \mathrm{Im}(f) \cap \mathrm{Im}(g)$, d'où $\mathrm{Im}(f) \cap \mathrm{Im}(g) \neq \emptyset$. Réciproquement, si $\mathrm{Im}(f) \cap \mathrm{Im}(g)$ est non vide, il contient un élément s. Par définition, il existe alors $x \in X$ tel que $f(x) = s$. De mêne, il existe $y \in Y$ tel que $g(y) = s$, ce qui implique que le couple (x, y) appartient à $X \times_S Y$, qui est donc non vide. Supposons maintenant que $X \times_S Y$ coïncide avec $X \times Y$. Les ensembles X, Y et S étant supposés non vides, le produit cartésien $X \times Y$ est non vide. D'après ce qui précède, $\mathrm{Im}(f) \cap \mathrm{Im}(g)$ est non vide. Supposons qu'il possède deux éléments distincts s et t. Fixons $x \in X$ tel que $f(x) = s$ et $y \in Y$ tel que $g(x) = t$. Dans ce cas, on a $(x, y) \in X \times Y$ et $(x, y) \notin X \times_S Y$, ce qui est exclu. L'ensemble $\mathrm{Im}(f) \cap \mathrm{Im}(g) = \{s\}$ est donc un singleton. Fixons $y \in Y$. Pour tout $x \in X$, on a alors $(x, y) \in X \times Y = X \times_S Y$, d'où $f(x) = g(y) = s$, ce qui implique que $\mathrm{Im}(f)$ est inclus dans $\mathrm{Im}(f) \cap \mathrm{Im}(g)$, auquel cas ils coïncident. De même, on obtient $\mathrm{Im}(g) = \{s\}$. Réciproquement, si $S = \{s\}$ est un singleton, pour tout $(x, y) \in X \times Y$, on a $f(x) = g(y) = s$, d'où l'identité $X \times_S Y = X \times Y$.

2. Considérons les applications $\pi_1 : X \times_S Y \to X$ et $\pi_2 : X \times_S Y \to Y$ définies par $\pi_1(x, y) = x$ et $\pi_2(x, y) = y$. Montrer que π_1 est surjective si et seulement si $\mathrm{Im}(f) \subset \mathrm{Im}(g)$. De même π_2 est surjective si et seulement si $\mathrm{Im}(g) \subset \mathrm{Im}(f)$. En particulier π_1 et π_2 sont toutes deux surjectives si et seulement si $\mathrm{Im}(f) = \mathrm{Im}(g)$.

L'application π_1 est surjective si et seulement si, pour tout $x \in X$, il existe $(x, y) \in X \times Y$ tel que $f(x) = g(y)$, ce qui traduit le fait que pour tout $x \in X$ on a $f(x) \in \mathrm{Im}(g)$, cette dernière condition étant équivalente à $\mathrm{Im}(f) \subset \mathrm{Im}(g)$.

On suppose désormais que X, Y et S sont des groupes et que les applications f et g sont des homomorphismes surjectifs de groupes. Dans la suite, on se restreint au cas où f et g sont surjectifs. Dans cette situation, les applications π_1 et π_2 sont surjectives (cf. le point ci-dessus).

3. Vérifier que $X \times_S Y$ est un sous-groupe de $X \times Y$, qu'il contient $\ker(f) \times \ker(g)$, que les applications π_1 et π_2 sont des homomorphismes de groupes et que l'on a les identités $\ker(\pi_1) = 1 \times \ker(g)$ et $\ker(\pi_2) = \ker(f) \times 1$.

Tout d'abord, $X \times_S Y$ est non vide, car il contient l'élément $(1, 1)$. Étant donnés deux éléments $g = (x, y)$ et $h = (u, v)$ de $X \times_S Y$, on a les identités $gh^{-1} = (xu^{-1}, yv^{-1})$ et

$$f(xu^{-1}) = f(x)f(u)^{-1} = g(y)g(v)^{-1} = g(yv^{-1}),$$

d'où $gh^{-1} \in X \times_S Y$, ce qui implique que $X \times_S Y$ est un sous-groupe de $X \times Y$. Étant donné $(x, y) \in \ker(f) \times \ker(g)$, on a $f(x) = 1 = f(y)$, d'où $(x, y) \in X \times_S Y$ et, par, suite, l'inclusion $\ker(f) \times \ker(g) \subset X \times_S Y$. L'application f est un homomorphisme de groupes, car restriction de la projection $X \times Y \to X$, qui est un homomorphisme. Finalement, on a $\pi_1(x, y) = 1$ si et seulement si $x = 1$, auquel cas $g(y) = f(x) = 1$, ou encore $y \in \ker(g)$, ce qui donne l'inclusion $\ker(\pi_1) \subset 1 \times \ker(g)$. Réciproquement, on a l'inclusion $f(1 \times \ker(g)) = \{1\}$, d'où l'inclusion $1 \times \ker(g) \subset \ker(\pi_1)$, qui est alors une égalité.

4. On suppose X et Y finis. Justifier le fait que S et $X \times_S Y$ sont finis et montrer que l'on a l'indentité

$$|S| \cdot |X \times_S Y| = |X| \cdot |Y|.$$

Si X et Y sont finis, alors S est fini (car les homomorphismes f et g sont surjectifs) et $X \times_S Y$ est fini, car sous-ensemble de $X \times Y$, qui est fini. L'homomorphisme π_1 étant surjectif, le théorème d'isomorphisme pour les groupes affirme que X est isomorphe au quotient de $X \times_S Y$ par $\ker(\pi_1)$, d'où l'identité $|X \times_S Y| = |X| \cdot |\ker(\pi_1)|$. D'après le point précédent, on a $\ker(\pi_1) = 1 \times \ker(g)$, d'où $|\ker(\pi_1)| = |\ker(g)|$. Finalement, l'homomorphisme $Y \to S$ étant surjectif, on obtient l'identité $|Y| = |\ker(g)| \cdot |S|$, ce qui permet de conclure.

5. Soient H et K deux sous-groupes distingués d'un groupe G. Dans la suite, on pose $X = G/H$ et $Y = G/K$. On a alors des homomorphismes surjectifs canoniques $u : G \to X$ et $v : G \to Y$.

   (a) Vérifier que l'ensemble
   $$HK = \{hk \mid h \in H, k \in K\}$$
   est un sous-groupe distingué de G et que c'est le plus petit sous-groupe contenant $H \cup K$. En posant $S = G/HK$, on obtient alors des homomorphismes canoniques surjectifs de groupes $f : X \to S$ et $g : Y \to S$ et l'on peut donc considérer le produit fibré $X \times_S Y$.

   Soient $x = ab$ et $y = cd$ deux éléments de HK, avec $a, c \in H$ et $b, d \in K$. Le sous-groupe K étant distingué, on a $dbb^{-1} = e \in H$, d'où l'identité $ed^{-1} = d^{-1}e$ et, par suite, les relations
   $$xy^{-1} = ab(cd)^{-1} = abd^{-1}c^{-1} = ad^{-1}ec^{-1},$$
   avec $ad^{-1} \in H$ et $ec^{-1} \in K$ (car H et K sont des sous-groupes de G), d'où $xy^{-1} \in HK$, ce qui montre que HK est un sous-groupe de G. Finalement, étant donné $x = hk \in HK$ et $g \in G$, on a l'identité $g^{-1}hkg = (g^{-1}hg)(g^{-1}kg)$. Les sous-groupes H et K étant distingués, on a $g^{-1}hg \in H$ et $g^{-1}kg \in K$, d'où $g^{-1}xg \in HK$, ce qui montre que HK est distingué. Finalement, si F est un sous-groupe de G contenant H et K, il contient hk pour tout $h \in H$ et tout $k \in K$, d'où l'nclusion $HK \subset F$, ce qui implique que HK est le plus petit sous-groupe de G contenant H et K.

   (b) Considérons l'homomorphisme de groupes $h : G \to X \times Y$ défini par $h(x) = (u(x), v(x))$. décrire son noyau et montrer que son image coïncide avec $X \times_S Y$. En déduire le ***théorème des restes chinois pour les groupes***, qui affirme que les groupes $X \times_S Y$ et $G/H \cap K$ sont isomorphes. En particulier, pour $G = HK$, on en déduit un isomorphisme entre $X \times Y$ et $G/H \cap K$.

   Par définition, on a $u(x) = Hx$, d'où $\ker(u) = H$. De même, on a $\ker(v) = K$. La relation $x \in \ker(h)$ se traduit par $u(x) = 1$ et $v(x) = 1$, ou encore $x \in \ker(u) \cap \ker v = H \cap K$. Étant donné $x \in G$, on a
   $$f(u(x)) = f(Hx) = HKx = g(Kx) = g(v(x)),$$
   d'où $h(x) = (u(x), v(x)) \in X \times_S Y$. Réciproquement, étant donné $(a, b) \in X \times_S Y$, on a $a = Hx$ et $b = Ky$, avec $x, y \in G$. On a alors l'identité $HKx = HKy$, ce qui se traduit par l'existence de $h \in H$ et $k \in K$ tels que $x = hky$. En posant $z = h^{-1}x = ky$, on a les identités $Hz = Hx$ et $Kz = Ky$, ou encore $u(z) = a$ et $v(z) = b$, d'où $(a, b) \in \mathrm{Im}(h)$. On a donc l'inclusion $X \times_S Y \subset \mathrm{Im}(h)$, qui est alors une égalité. Le théorème d'isomorphisme pour les groupes affirme alors que les groupes $G/H \cap K$ et $X \times_S Y$ sont isomorphes.

   (c) Nous dirons que deux éléments $x, y \in G$ sont ***congrus modulo*** H si $xy^{-1} \in H$, ce qui revient à affirmer que x et y définissent le même élément de X. On écrit alors $x \equiv y \pmod{H}$. Étant donnés $a, b \in G$, on s'intéresse à l'existence d'un élément $x \in G$ tel que
   $$\begin{cases} x \equiv a \pmod{H}, \\ x \equiv b \pmod{K}. \end{cases}$$
   Déduire du point précédent qu'un tel élément existe si et seulement si a et b sont congrus modulo HK et qu'il est alors unique modulo $H \cap K$. En particulier, pour $G = HK$, une solution existe toujours.

Considérons les éléments $Ha \in X$ et $Kb \in Y$. L'existence d'une solution x du système de congruences se traduit alors par les relations $Hx = Ha$ et $Kx = Kb$, qui sont équivalentes à $h(x) = (Ha, Hb)$. D'après le point précédent, un tel élément existe si et seulement si on a l'identité $HKa = HKb$, ou encore $ab^{-1} \in HK$. Si deux éléments $x, y \in G$ sont solution du système, on a alors $h(x) = h(y)$, ou encore $xy^{-1} \in \ker(h) = H \cap K$, ce qui permet de conclure.

On suppose finalement que X, Y et S sont des anneaux et que les applications f er g sont des homomorphismes d'anneaux.

8. Vérifier que $X \times_S Y$ est un sous-anneau de $X \times Y$.

Le point 3 affirme que $X \times_S Y$ est un sous-groupe de $X \times Y$. On a $f(1) = g(1) = 1$, d'où $(1, 1) \in X \times_S Y$. Étant donnés $x = (a, b), y = (c, d) \in X \times_S Y$, on a les identités

$$f(ac) = f(a)f(c) = g(b)g(d) = g(bd),$$

d'où $xy = (ac, bd) \in X \times_S Y$, ce qui montre que $X \times_S Y$ est un sous-anneau de $X \times Y$.

9. Considérons deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ d'un anneau A. Posons $X = A/\mathfrak{a}, Y = A/\mathfrak{b}$ et $S = A/(\mathfrak{a} + \mathfrak{b})$. On a alors des homomorphismes canoniques $f : X \to S$ et $g : Y \to S$. Montrer le ***théorème des restes chinois pour les anneaux***, qui affirme que les anneaux $X \times_S Y$ et $A/\mathfrak{a} \cap \mathfrak{b}$ sont isomorphes.

Le théorème des restes chinois pour les groupes, démontré dans le point (5b), affirme que les groupes $X \times_S Y$ et $A/\mathfrak{a} \cap \mathfrak{b}$ sont isomorphes. Les homomorphismes f et g étant des homomorphismes d'anneaux, cet isomorphisme est automatiquesment un isomorphisme d'anneaux.

10. Avec les hypothèses et notations du point précédent, étant donnés $a, b \in A$, montrer que le système de congruences

$$\begin{cases} x \equiv a \pmod{\mathfrak{a}}, \\ \\ x \equiv b \pmod{\mathfrak{b}} \end{cases}$$

admet une solution si et seulement si a est congru à b modulo $\mathfrak{a} + \mathfrak{b}$, auquel cas la solution est unique modulo $\mathfrak{a} \cap \mathfrak{b}$.

Ce n'est qu'une reformulation du point (5c) dans le contexte des anneaux.

11. Deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de A sont ***étrangers*** si $\mathfrak{a} + \mathfrak{b} = A$, ce qui se traduit par l'existence de deux éléments $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ vérifiant la relation $a + b = 1$, appelée ***identité de Bézout***. Montrer que dans ce cas, on a l'identité $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

Ayant toujours l'inclusion $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$, considérons un élément $x \in \mathfrak{a} \cap \mathfrak{b}$. Les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ étant étrangers, on a une identité de Bézout $a + b = 1$, avec $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$, d'où $x = x(a + b) = xa + xb$. On a $a \in \mathfrak{a}$ et $x \in \mathfrak{a} \cap \mathfrak{b}$, ce qui donne $ax \in \mathfrak{ab}$. De même, on obtient $bx \in \mathfrak{ab}$, d'où $x = ax + bx \in \mathfrak{ab}$, ce qui amène à l'inclusion $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{ab}$, qui est alors une égalité.

12. Montrer que si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux étrangers d'un anneau A alors les anneaux $A/\mathfrak{a} \times A/\mathfrak{b}$ et $A/\mathfrak{ab}$ sont isomorphes. Dans ce cas, le système de congruences du point 10 admet toujours une solution, qui est unique modulo $\mathfrak{ab}$. C'est sous cette forme qu'est généralement énoncé le théorème des restes chinois.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont étrangers, le quotient $A/(\mathfrak{a} + \mathfrak{b})$ est un singleton. Le point 1 affirme alors que $X \times_S Y$ et $X \times Y$ coïncident. Compte tenu du dernier point, il suffit alors d'appliquer le théorème des restes chinois pour les anneaux.