TD1 : Arithmétique des entiers

Exercice 1. Combien de diviseurs le nombre $1\,000\,000$ possède-t-il ?

Exercice 2. Échauffements.

a) Quel est le dernier chiffre de 7777^{7777} ?

b) Quel est le reste de la division euclidienne de 900^{200} par 13 ?

c) Déterminer $101^{102^{103}} \bmod 13$, $31^{32^{33}} \bmod 7$, et $100^{100^{100}} \bmod 12$.

Exercice 3. Résoudre les équations diophantiennes suivantes.

a) $3x + 7y = 4$;

b) $189x + 255y = 3$;

c) $12x + 51y = 7$;

d) $43x - 11y = 10$;

e) $xy = 2x + 3y$;

f) $x^2 - y^2 - x + 3y = 30$;

g) $x^2 - 5y^2 = 3$.

Exercice 4. Résoudre les congruences suivantes :

a) $2x \equiv 1 \pmod 7$;

b) $5x \equiv -1 \pmod 8$;

c) $171x \equiv 7 \pmod{212}$;

d) $68x \equiv 100 \pmod{120}$.

Exercice 5. Résoudre les systèmes de congruences suivants :

$$\text{a)} \begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod{11} \end{cases}, \quad \text{b)} \begin{cases} x \equiv 4 \pmod{21} \\ x \equiv 10 \pmod{33} \end{cases}, \quad \text{c)} \begin{cases} x \equiv 3 \pmod{17} \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod 6 \end{cases}.$$

Exercice 6. Déterminer la périodicité de la fonction g définie par $g : \mathbb{Z} \to \mathbb{Z}/7\mathbb{Z},\ g(n) \coloneqq 5^n + n$.

Trouver toutes les solutions de l'équation $g(n) = 0$. Une solution sans calcul fastidieux sera appréciée !

Exercice 7. Démontrer que pour tout $n \in \mathbb{N}$, $2^{3n+5} + 3^{n+1}$ est un multiple de 5.

Exercice 8. Démontrer que pour tout $n \in \mathbb{Z}$, $n^5 - n$ est un multiple de 30.

Exercice 9. Soit n un entier fixé. Démontrer que $\forall a \in \mathbb{N},\ a^n - a \equiv 0 \pmod n$ si et seulement si n est sans facteur carré et si $p - 1$ divise $n - 1$ pour tout facteur premier p de n.

Exercice 10. Déterminer les $n \in \mathbb{N}$ tels que $n + 1$ divise $n^2 + 1$.

Exercice 11. Soient $a, b \in \mathbb{N}$ premiers entre eux. Démontrer que ab est un carré parfait si et seulement si a et b le sont. Si $n \in \mathbb{N}$, quand est-ce que $n(n+1)$ est un carré parfait ?

Exercice 12. Soit $n \geq 1$ un entier. Démontrer que $a \wedge b = 1$ si et seulement si $a^n \wedge b^n = 1$.

Exercice 13. Démontrer que $a \wedge b = 1$ si et seulement si $(a + b) \wedge (ab) = 1$.

Exercice 14. (Équation diophantienne.) On considère l'équation $y(y-1) = x^2$, avec $x, y \in \mathbb{Z}$.

a) Démontrer que si l'équation est vérifiée alors y et $y - 1$ sont des carrés parfaits (à inversibles près).

b) En déduire que l'équation n'admet que deux solutions que l'on déterminera.

Exercice 15. Démontrer qu'il existe des suites d'entiers consécutifs non premiers de longueur arbitraire. (Indication : $n! + 2, n! + 3, n! + 4$, etc.)

Exercice 16. Soit $n \geq 2$ un entier.

a) Si n n'est pas premier, démontrer que n possède un facteur premier $\leq \sqrt{n}$.

b) En déduire que si $10 \leq n \leq 100$, alors n est premier si et seulement s'il est premier avec 210.

Exercice 17. (Crible d'Ératosthène.) Pour déterminer les nombres premiers inférieurs ou égaux à un entier $n \geq 2$ fixé, on applique l'algorithme suivant. On liste tous les entiers compris entre 2 et n. Tant qu'il reste dans cette liste qui ne sont ni barrés, ni entourés, on applique l'opération suivante : on entoure le premier entier qui reste, puis on barre tous ses multiples dans la liste.

a) Appliquer l'algorithme pour $n = 20$ et vérifier qu'on retrouve bien les nombres premiers ≤ 20.

b) Démontrer que l'algorithme produit bien la liste des nombres premiers $\leq n$.

c) Démontrer qu'on ne barre plus d'entiers si ceux qui restent sont $> \sqrt{n}$.

d) En déduire un algorithme de complexité temporelle $O(n)$ pour lister les premiers $\leq n$.

Exercice 18. Nombres de Mersenne.

a) Soient $a \geq 2$ et $n \geq 2$ des entiers. Démontrer que si $a^n - 1$ est premier, alors $a = 2$ et n est premier.

Les nombres de cette forme sont appelés les nombres de Mersenne et sont notés $M_n = 2^n - 1$.

b) Est-ce que M_2, M_3, M_5, M_7 et M_{11} sont premiers ?

c) Soit p premier, $p \equiv 3 \pmod 4$. Démontrer que $2p+1$ est premier si et seulement si $2^p \equiv 1 \pmod{2p+1}$.

d) En déduire que M_{11}, M_{23}, M_{83} et M_{131} ne sont pas premiers.

Exercice 19. Soit $a \geq 2$ un entier.

a) Démontrer que pour tout $n \geq 2$, $a-1$ divise $a^n - 1$.

b) Démontrer que si $(a^n-1)/(a-1)$ est premier, alors n est premier.

c) La réciproque est-elle vraie ?

Exercice 20. (Théorème de Wilson.) Démontrer que $p \geq 2$ est premier si et seulement si $(p-1)! \equiv -1 \pmod p$.

Exercice 21. En quoi l'indicatrice d'Euler φ permet-elle de généraliser le petit théorème de Fermat ?

Exercice 22. (Chiffrement RSA.) Alice veut envoyer à Bob un message privé sur un réseau public. Bob choisit deux nombres premiers $p \neq q$ et note $n = pq$, $\lambda = (p-1) \vee (q-1)$. Il détermine un entier e premier avec λ. Il calcule un entier d tel que $de \equiv 1 \pmod \lambda$. Il dévoile sa clé publique (n, e) et garde secrète sa clé privée d.

Le message d'Alice pour Bob est une suite d'entiers naturels $M < n$. Elle calcule le message chiffré $M' = M^e \pmod n$ qu'elle envoie à Bob. Pour déchiffrer le message, Bob calcule $M'' = (M')^d \pmod n$.

a) Est-ce que Bob a correctement déchiffré le message d'Alice ?

Ève a écouté l'échange ! Elle sait que la clé publique de Bob est $(n, e) = (851, 5)$ et qu'Alice a envoyé le message chiffré suivant à Bob : $(2, 333, 739, 797, 333, 561, 206)$.

b) Est-ce qu'Ève est en mesure de déchiffrer le message ? Que lui manque-t-il ?

c) D'où vient la difficulté de reconstituer la clé privée à partir de la clé publique ?

Exercice 23. Calculer les symboles de Legendre suivants :

a) $\left(\frac{-1}{17}\right)$, c) $\left(\frac{13}{17}\right)$, e) $\left(\frac{-8}{23}\right)$.

b) $\left(\frac{2}{29}\right)$, d) $\left(\frac{7}{19}\right)$,

Exercice 24.

a) Est-ce que 1475 est un résidu quadratique modulo 2389 (qui est premier) ?

b) Soit $n \in \mathbb{N}$ tel que $p = 4n+3$ et $q = 2n+1$ sont premiers. Quand est-ce que 3 est une racine primitive de l'unité modulo p ?

Exercice 25. Déterminer les nombres premiers p tels que 6 soit un résidu quadratique mod p.

Exercice 26. Étant donné un premier p, on s'intéresse au cardinal N_p de la courbe $\mathcal{C} = \{ (x, y) \in \mathbb{Z}/p\mathbb{Z} \mid y^2 = x^3 - x \}$.

a) Démontrer que l'on a la formule :

$$N_p = p + \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x^3 - x}{p}\right).$$

b) Calculer N_7. Généraliser le calcul aux nombres premiers p tels que $p \equiv 3 \pmod 4$.

Exercice 27. Soit p un nombre premier impair.

a) Démontrer que la fonction suivante est une bijection :

$$\mathbb{Z}/p\mathbb{Z} \setminus \{1\} \to \mathbb{Z}/p\mathbb{Z} \setminus \{-1\}, \qquad x \mapsto \frac{1+x}{1-x}.$$

b) En déduire que l'égalité suivante est vraie :

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{1-x^2}{p}\right) = (-1)^{(p+1)/2}.$$

c) Quel est le nombre de points du cercle unité ($x^2 + y^2 = 1$) modulo p ?

Exercice 28. (Test de Solovay–Strassen) Soit $n \geq 3$ un entier impair. On définit :

$$G_n = \left\{ a \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; 0 \neq \left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod n \right\}.$$

a) Démontrer que G_n est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$.

b) Si n est premier, quel est ce sous-groupe ?

c) Démontrer que la réciproque est vraie.

d) Lorsque n n'est pas premier, démontrer que $|G_n| < (n-1)/2$.

Exercice 29. Calculer le symbole de Jacobi $\left(\frac{610}{983}\right)$. Sachant que $610^{491} \equiv 1 \pmod{983}$, est-ce que le test de Solovay–Strassen pour le témoin 610 permet de dire si 983 est premier ?

TD2 : Théorie des anneaux

Exercice 1. Décrire le plus petit sous-anneau de $\mathbb{C}$ contenant $i \in \mathbb{C}$.

Exercice 2. Soit A un anneau et $I, J \subset A$ des idéaux.

a) Démontrer que les sous-ensembles suivants sont des idéaux de A :

$$I \cap J, \qquad I + J = \{ x + y \mid x \in I,\ y \in J \}, \qquad IJ = \{ x_1 y_1 + \cdots + x_n y_n \mid x_i, y_i \in I \}.$$

b) Quelles relations d'inclusions existent entre $I, J, I \cap J, I + J$ et IJ ?

c) Dans le cas où $A = \mathbb{Z}$, $I = m\mathbb{Z}$ et $J = n\mathbb{Z}$ (avec $m, n \in \mathbb{Z}$), décrire ces idéaux.

Exercice 3. Soit A un anneau et $a \in A$. Démontrer que l'unique morphisme $\mathbb{Z}[X] \to A$ tel que $X \mapsto a$ est donné par $P \mapsto P(a)$.

Exercice 4. Soit A un anneau et $I_1, \dots, I_n \subset A$ des idéaux non-triviaux tels que si $i \neq j$ alors $I_i + I_j = A$.

a) Donner un exemple pour $A = \mathbb{Z}$ et $n = 3$.

b) Démontrer que pour tous $x_1, \dots, x_n \in A$, il existe $x \in A$ tel que $x \equiv x_i \pmod{I_i}$ pour tout i.

c) Démontrer que $A/(I_1 \cap \dots \cap I_n) \cong (A/I_1) \times \dots \times (A/I_n)$.

Exercice 5. Soit A un anneau et $I \subset A$ un idéal.

a) Démontrer que les idéaux de A/I sont de la forme J/I avec $I \subset J \subset A$ un idéal, et que l'on a $(A/I)/(J/I) \cong A/J$.

b) Soit $B \subset A$ un sous-anneau de A. Démontrer que $B + I$ est un sous-anneau de A et que I est un idéal de $B + I$.

c) Démontrer que $B \cap I$ est un idéal de A et que $(B + I)/I \cong B/(B \cap I)$.

Exercice 6. Démontrer que les applications suivantes sont des morphismes d'anneaux et déterminer des générateurs de leurs noyaux respectifs :

a) $f : \mathbb{K}[X] \to \mathbb{K},\ f(P) \coloneqq P(a)$, où $\mathbb{K}$ est un corps et $a \in \mathbb{K}$.

b) $g : \mathbb{R}[X] \to \mathbb{C},\ g(P) \coloneqq P(i)$.

c) $h : \mathbb{Z}[X] \to (\mathbb{Z}/n\mathbb{Z})[X],\ h(P) \coloneqq P$, où $n \in \mathbb{Z}$.

d) $j : \mathbb{Q}[X, Y] \to \mathbb{Q},\ j(P) \coloneqq P(0, 1)$.

e) $k : \mathbb{R}[X, Y] \to \mathbb{R}[X],\ k(P) \coloneqq P(X, X^2)$.

Exercice 7. Soit $\mathbb{K}$ un corps.

a) Démontrer que $\mathbb{K}[X, Y]/(X^2 + Y^2 - 1)$ est intègre lorsque $\mathrm{car}(\mathbb{K}) \neq 2$. Est-ce un corps ?

b) Démontrer que $\mathbb{Z}[X]/(2, X^4 + X + 1)$ est un corps.

c) Démontrer que $\mathbb{K}[X, Y]/(Y - X^2)$ est principal.

d) Démontrer que $\mathbb{K}[X, X^{-1}] \coloneqq \mathbb{K}[X, Y]/(XY - 1)$ est principal.

Exercice 8. Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme non nul. Démontrer que $\mathbb{K}[X]/(P)$ est un $\mathbb{K}$-espace vectoriel de dimension $\deg(P)$.

Exercice 9. Soit $f : \mathbb{Z} \to \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ le morphisme canonique. Quel est le noyau et l'image de f ? Expliciter l'isomorphisme inverse $\mathrm{im}(f) \to \mathbb{Z}/\ker(f)$. Faire de même pour $\mathbb{Q}[X] \to \mathbb{Q}[X]/(X^3 - 2) \times \mathbb{Q}[X]/(X^2 + 1)$.

Exercice 10. Soit V un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathrm{End}(V)$, de polynôme minimal $\mu \in \mathbb{K}[X]$.

a) Décrire $\mathbb{K}[X]/(\mu)$ en termes d'endomorphismes de V.

b) Démontrer que l'anneau $\mathbb{K}[X]/(\mu)$ est principal.

Exercice 11. On pose $j \coloneqq \exp(2i\pi/3) \in \mathbb{C}$ et on note $\mathbb{Z}[j]$ (resp., $\mathbb{Q}[j]$) le sous-anneau (resp., sous-corps) de $\mathbb{C}$ contenant j.

a) Décrire les éléments de $\mathbb{Z}[j]$ et $\mathbb{Q}[j]$.

b) Démontrer que pour tout $z \in \mathbb{C}$, il existe $w \in \mathbb{Z}[j]$ tel que $|z - w| < 1$.

c) Démontrer que $\mathbb{Z}[j]$ est euclidien.

Exercice 12. Soit $\mathbb{K}$ un corps et $A = \mathbb{K}[X, Y]/(X^2, Y^2, XY)$.

a) Déterminer les éléments inversibles de A.

b) Déterminer les idéaux principaux de A.

c) Déterminer tous les idéaux de A.

Exercice 13. On considère la courbe $\mathcal{C} = \{ (x, y) \in \mathbb{C}^2 \mid y^2 = x^3 \}$. On dit qu'une fonction $f : \mathcal{C} \to \mathbb{C}$ est polynômiale si c'est la restriction à $\mathcal{C}$ d'une fonction polynômiale $\mathbb{C}^2 \to \mathbb{C}$.

a) Démontrer que l'ensemble A des fonctions polynômiales sur $\mathcal{C}$ forme un anneau.

b) Démontrer que A est isomorphe à l'anneau :

$$\mathbb{C}[T^2, T^3] \coloneqq \{ P(T^2, T^3) \mid P \in \mathbb{C}[X, Y] \} \subset \mathbb{C}[T].$$

On pourra utiliser la paramétrisation $\mathcal{C} = \{ (t^2, t^3) \mid t \in \mathbb{C} \}$. Décrire les éléments de $\mathbb{C}[T^2, T^3]$.

c) Démontrer que A est intègre.

d) Démontrer que les fonctions $\alpha, \beta \in A$ sont des éléments irréductibles de A :

$$\alpha(x, y) \coloneqq x, \qquad \beta(x, y) \coloneqq y.$$

e) Soit $J = \{ f \in A \mid f(0, 0) = 0 \}$. Démontrer que J est un idéal de A et déterminer une famille génératrice. Démontrer que A n'est pas principal.

f) Démontrer que $A/J \cong \mathbb{C}$.

g) Démontrer que $A \cong \mathbb{C}[X, Y]/(Y^2 - X^3)$. Est-ce que cet anneau quotient est principal, euclidien ?

h) Est-ce que A est factoriel ?

Exercice 14. Soit $A = \left\{ x + iy\sqrt{5} \mid x, y \in \mathbb{Z} \right\}$. Étant donné $z \in A$, on note sa norme $N(z) \coloneqq z\bar{z}$.

a) Démontrer que les éléments inversibles de A sont exactement les éléments de norme 1.

b) Démontrer que tous les éléments de norme 9 sont irréductibles.

c) Démontrer que A n'est pas factoriel. Indication : considérer des produits d'éléments de norme 9 bien choisis.

Exercice 15. On note $\xi = \left(1 + i\sqrt{19}\right)/2$ et on note $\mathbb{Z}[\xi]$ le sous-anneau de $\mathbb{C}$ engendré par ξ.

a) Démontrer que tout élément de $\mathbb{Z}[\xi]$ s'écrit de manière unique sous la forme $x + y\xi$ avec $x, y \in \mathbb{Z}$.

b) Démontrer que pour tout $z \in \mathbb{Z}[\xi]$, le conjugué $\bar{z}$ appartient à $\mathbb{Z}[X]$ et que la norme $z\bar{z}$ est un entier.

c) Démontrer que $\mathbb{Z}[\xi]$ est intègre.

d) Démontrer que $z \in \mathbb{Z}[\xi]$ est inversible si et seulement si $z\bar{z} = 1$.

e) Étant donnés $x, y \in \mathbb{Z}$, démontrer que $x^2 + xy + 5y^2 \geq 4y^2$. En déduire que $\mathbb{Z}[\xi]^\times = \{\pm 1\}$.

f) Démontrer que $\mathbb{Z}[\xi]$ est isomorphe à $\mathbb{Z}[X]/(X^2 - X + 5)$.

Exercice 16. Soit $d \in \mathbb{Z}$ un entier sans facteur carré.

a) Démontrer que $\mathbb{Z}[\sqrt{d}]$ est un sous-anneau de $\mathbb{C}$. À quelle condition est-ce un réseau de $\mathbb{C}$?

b) On suppose désormais que $d < 0$. Démontrer que $v(z) \coloneqq z\bar{z}$ est multiplicative et à valeurs dans $\mathbb{N}$.

c) Démontrer que v est un stathme euclidien si et seulement si pour tout $z \in \mathbb{Q}[\sqrt{d}]$, la boule unité centrée en z rencontre un point de $\mathbb{Z}[\sqrt{d}]$.

d) Démontrer que cela n'est le cas que si $d = -1$ ou $d = -2$.

Exercice 17. Soit p un nombre premier impair. On rappelle que $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ est un anneau euclidien.

a) Démontrer que s'il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$, alors $p \equiv 1 \pmod 4$.

b) On suppose désormais que $p \equiv 1 \pmod 4$. Démontrer qu'il existe $\alpha \in \mathbb{Z}$ tel que $\alpha^2 \equiv -1 \pmod p$.

c) Démontrer que la fonction suivante définit un morphisme d'anneaux :

$$\mathbb{Z}[i] \to (\mathbb{Z}/p\mathbb{Z})^2, \qquad a + bi \mapsto (a + \alpha b, a - \alpha b).$$

Déterminer son noyau et son image.

d) En déduire que p est réductible dans $\mathbb{Z}[i]$ et qu'il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.

Exercice 18. (Anneau des entiers de Gauss.)

a) Démontrer que $1 + i$ est irréductible dans $\mathbb{Z}[i]$. Factoriser $2 \in \mathbb{Z}[i]$. Est-ce que les irréductibles qui apparaissent sont associés ?

b) Soit $p \equiv 3 \pmod 4$ un nombre premier. Démontrer que p est irréductible dans $\mathbb{Z}[i]$.

c) Soit $p \equiv 1 \pmod 1$ un nombre premier. Démontrer que $p = \alpha\bar{\alpha}$ avec $\alpha \in \mathbb{Z}[i]$ irréductible et que α et $\bar{\alpha}$ ne sont pas associés.

d) Soit $\alpha \in \mathbb{Z}[i]$ irréductible et $(\alpha) \subset \mathbb{Z}[i]$ l'idéal engendré par α. Démontrer que $\mathbb{Z} \cap (\alpha) = p\mathbb{Z}$ pour un nombre premier p, et que p est le seul nombre premier divisible par α dans $\mathbb{Z}[i]$.

e) En déduire que les irréductibles de $\mathbb{Z}[i]$ sont les nombres premiers p congrus à 3 mod 4 et les entiers de Gauss de la forme $\alpha = x + iy$ avec $x^2 + y^2$ premier.

f) Factoriser $-3 + 15i$ dans $\mathbb{Z}[i]$.

Exercice 19. Soit $p \in \mathbb{Z}$ un nombre premier. Combien existe-t-il de couples $(a, b) \in \mathbb{Z}^2$ tels que $p = a^2 + b^2$?

Exercice 20. (Évaluation 2020) Soit $A = \mathbb{Z}[i]$ l'anneau des entiers de Gauss.

a) Faire la division euclidienne de $6 + 8i$ par $1 + 5i$.

b) En déduire le PGCD de $6 + 8i$ et $1 + 5i$.

c) Proposer une autre méthode pour calculer ce PGCD.

Exercice 21. (Évaluation 2020) Soit $A = \{ P \in \mathbb{R}[X] \mid P'(0) = 0 \}$.

a) Démontrer que A est un anneau intègre.

b) Quels sont les éléments inversibles de A ?

c) Démontrer que X^2 et X^3 appartiennent à A. Est-ce que X^2 divise X^3 dans A ?

d) Démontrer que X^2 et X^3 sont irréductibles dans A.

e) Démontrer que A n'est pas factoriel.

f) L'idéal de A engendré par X^2 est-il premier ?

Exercice 22. (Évaluation 2021) Soit A un anneau commutatif. Le nilradical de A, noté $\mathrm{Nil}(A)$, est l'ensemble des éléments nilpotents $\{ a \in A \mid \exists m \in \mathbb{N},\ a^m = 0 \}$.

a) Que vaut $\mathrm{Nil}(A)$ lorsque A est intègre ?

b) Démontrer que $\mathrm{Nil}(A)$ est un idéal de A.

c) Démontrer que pour tout $a \in A, k \in \mathbb{N}$, $1 - a$ divise $1 - a^k$.

d) Soit $a \in \mathrm{Nil}(A)$. Démontrer que $1 - a \in A^\times$ et en déduire que pour tout $u \in A^\times$, $u + a \in A^\times$.

e) Démontrer que $\mathrm{Nil}(A) \subset \mathrm{Nil}(A[X])$.

f) Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ un polynôme. Démontrer que $P \in \mathrm{Nil}(A[X])$ si et seulement si $a_0, a_1, \ldots, a_n \in \mathrm{Nil}(A)$.

g) Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ un polynôme. Démontrer que $P \in A[X]^\times$ si et seulement si $a_0 \in A^\times$ et $a_1, \ldots, a_n \in \mathrm{Nil}(A)$.

Exercice 23. Soit A un anneau, que l'on ne suppose pas nécessairement commutatif. On dit que $a \in A$ est idempotent si $a^2 = a$. On suppose que tous les éléments de A sont idempotents.

a) Démontrer que A est commutatif et que sa caractéristique vaut 2.

b) Donner un exemple d'un tel anneau A.

c) Dans quel cas A est-il intègre ?

d) Démontrer qu'on peut munir A d'une structure d'espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$. En déduire que si A est fini, alors il existe $n \in \mathbb{N}$ tel que $|A| = 2^n$.

e) On suppose maintenant que A est un anneau commutatif quelconque, et que $A = A_1 \times A_2$ pour des anneaux $A_1, A_2 \neq \{0\}$. Démontrer que A possède au moins quatre éléments idempotents.

TD 3 : Polynômes irréductibles

Exercice 1. Soit $\mathbb{K}$ un corps.

a) Quels sont les polynômes irréductibles de degré ≤ 1 ?

b) Pour $P \in \mathbb{K}[X]$ de degré 2 ou 3, démontrer que P est irréductible dans $\mathbb{K}[X]$ si et seulement si P n'a pas de racine dans $\mathbb{K}$.

c) Pour $P \in \mathbb{K}[X]$ de degré ≥ 4, y a-t-il un lien entre l'irréductibilité de P et l'absence de racine de P dans $\mathbb{K}$?

Exercice 2. Quels sont les polynômes irréductibles unitaires de degré ≤ 3 sur $\mathbb{F}_2$? Sur $\mathbb{F}_3$?

Exercice 3. Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme non constant. Démontrer que $\mathbb{K}[X]/(P)$ est un corps si et seulement si P est irréductible.

Exercice 4. Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ de degré $n \geq 2$.

a) Démontrer que P est irréductible sur $\mathbb{K}$ si, et seulement si, $\mathbb{K}$ n'a pas de racines dans les extensions $\mathbb{L}$ de $\mathbb{K}$ telles que $[\mathbb{L}: \mathbb{K}] \leq n/2$.

b) Application : Démontrer que $P(X) = X^4 + 1$ est irréductible sur $\mathbb{Z}$ mais est réductible sur $\mathbb{F}_p$ pour tout p premier.

Exercice 5. Soient $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ irréductible de degré $n \geq 2$ et $\mathbb{L}$ une extension de degré m avec $m \wedge n = 1$. Démontrer qu'alors P est encore irréductible sur $\mathbb{L}$.

Exercice 6. (Description du corps à 16 éléments).

a) Déterminer tous les polynômes irréductibles de degré 4 sur $\mathbb{F}_2$.

b) Pourquoi les anneaux $\mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$ et $\mathbb{F}_2[X]/(X^4 + X + 1)$ sont-ils isomorphes ?

c) Calculer l'ordre multiplicatif de la classe de X dans chacun de ces quotients.

d) Construire un isomorphisme explicite.

Exercice 7. On considère le polynôme $P = X^4 - 2X^2 + 9$. Déterminer les racines complexes de P et une factorisation de P en polynômes irréductibles dans $\mathbb{C}[X]$. En déduire une factorisation en irréductibles dans $\mathbb{R}[X]$. Le polynôme P est-il irréductible dans $\mathbb{Q}[X]$?

Exercice 8. Factoriser en irréductibles le polynôme $1 + X^2 + X^4$ dans $\mathbb{C}[X]$. Idem dans $\mathbb{R}[X]$ puis dans $\mathbb{Q}[X]$.

Exercice 9. Démontrer que $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$. En déduire que $X^3 + 24X^2 - X + 5$ est irréductible dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$.

Exercice 10. Étudier l'irréductibilité des polynômes suivants dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$:

a) $P_a = X^3 + 4X^2 - 5X + 7$;

b) $P_b = X^3 - 6X^2 - 4X + 13$;

c) $P_c = X^4 + 5X^3 - 3X^2 - X + 7$;

d) $P_d = X^6 + X^3 + 1$;

e) $P_e = X^7 + X + 1$;

f) $P_f = X^5 - 7$.

Exercice 11.

a) Démontrer que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ est une base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

b) Quel est le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$?

c) En déduire que $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

d) Déterminer le groupe des automorphismes (de corps) de $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Exercice 12. On considère le polynôme $\Phi_5 := 1 + X + X^2 + X^3 + X^4 \in \mathbb{Z}[X]$.

a) Décomposer Φ_5 en irréductibles dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.

b) Démontrer que Φ_5 est irréductible dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$. En déduire que $\cos(2\pi/5)$ est irrationnel.

c) Généraliser le raisonnement précédent pour démontrer que pour tout nombre premier $p \geq 5$, $\cos(2\pi/p)$ est irrationnel.

Exercice 13. Soit p un nombre premier et $a \in \mathbb{F}_p^*$. On veut démontrer que le polynôme $P = X^p - X - a$ est irréductible sur $\mathbb{F}_p$ et sur $\mathbb{Q}$.

a) Soit $\mathbb{K}$ une extension de $\mathbb{F}_p$ dans laquelle P possède une racine notée α. Démontrer que les racines de P dans $\mathbb{K}$ sont $\alpha, \alpha+1, \dots, \alpha+p-1$.

b) Soit $U \in \mathbb{F}_p[X]$ un polynôme unitaire de degré $d \geq 1$ qui divise P. En examinant le coefficient du terme $X^d - 1$ de U, démontrer que $P = U$.

c) En déduire que P est irréductible sur $\mathbb{F}_p$, puis sur $\mathbb{Q}$.

Exercice 14.

a) Le nombre 2 est-il un carré dans $\mathbb{F}_5$?

b) Démontrer que $P = X^2 + X + 1$ est irréductible dans $\mathbb{F}_5[X]$.

c) Quelle est la caractéristique de $\mathbb{F}_{25}$?

d) Démontrer que le quotient $\mathbb{F}_5[X]/(P)$ est isomorphe à $\mathbb{F}_{25}$ et que P a deux racines dans $\mathbb{F}_{25}$.

e) On note α une racine de P dans $\mathbb{F}_{25}$. Démontrer que tout $\beta \in \mathbb{F}_{25}$ peut s'écrire de manière unique sous la forme $\beta = x + \alpha y$ avec $x, y \in \mathbb{F}_5$.

f) Soit $Q = X^5 - X + 1$. Déterminer $c, d \in \mathbb{F}_5$ tels que $Q(\alpha) = c + d\alpha$.

g) En utilisant le résultat de la question d, démontrer que pour tout $\beta \in \mathbb{F}_{25}$, on a $Q(\beta) \neq 0$.

h) En déduire que Q est irréductible dans $\mathbb{F}_5[X]$. Le polynôme Q est-il irréductible dans $\mathbb{Q}[X]$?

i) Le polynôme Q est-il irréductible dans $\mathbb{F}_{25}[X]$?

Exercice 15. Soit $n \geq 1$ un entier et p un nombre premier.

a) Soit P un polynôme irréductible de degré d dans $\mathbb{F}_p[X]$. Démontrer que le quotient $\mathbb{K} := \mathbb{F}_p[X]/\big(P(X)\big)$ est un corps. Quel est l'ordre du groupe multiplicatif $\mathbb{K}^\times$? En déduire que tout élément $x \in \mathbb{K}$ vérifie $x^{p^d} = x$.

b) Démontrer ensuite que P divise $X^{p^n} - X$ si et seulement si d divise n. On redémontrera un résultat du cours si nécessaire.

c) Soit $Q_n := X^{p^n} - X$. Calculer Q_n', le polynôme dérivé de Q_n. En déduire que Q_n n'est divisible par aucun carré de polynôme de degré ≥ 1.

d) Démontrer que, dans $\mathbb{F}_p[X]$, le polynôme Q_n est le produit de tous les polynômes unitaires irréductibles dont le degré divise n.

e) On prend $n = 4$ et $p = 2$. Retrouver l'ensemble des polynômes irréductibles de degré 2 puis 4 dans $\mathbb{F}_2[X]$.

f) Soit P un polynôme de degré n dans $\mathbb{F}_p[X]$. Démontrer que P est irréductible si, et seulement si, les deux assertions suivantes sont vérifiées :

i) Le polynôme P divise Q_n.

ii) Pour tout diviseur premier q de n, le polynôme P est premier avec le polynôme $Q_{n/q}$.

Exercice 16. (Évaluation 2020)

a) Questions préliminaires

i) Soit $\mathbb{K}$ un corps, P un polynôme de $\mathbb{K}[X]$ de degré $n \geq 2$. Démontrer que P est irréductible si et seulement si P n'a pas de racine dans toute extension $\mathbb{L} \supset \mathbb{K}$ de degré $\leq n/2$.

ii) Soit $\mathbb{K}$ un corps à p éléments avec p premier. Soit P un polynôme irréductible de $\mathbb{K}[X]$. Soit $\mathbb{L}$ le corps de décomposition de P sur $\mathbb{K}$. On note $\Phi_p : L \to L$ l'application $x \mapsto x^p$ et on rappelle que c'est un automorphisme de corps. Démontrer que si $x \in L$ est une racine de P alors $\Phi_p(x)$ est une racine de P.

b) On considère le polynôme $P = X^3 - X - 1$ sur $\mathbb{F}_3[X]$.

i) Démontrer que $\mathbb{F}_{27} \cong \mathbb{F}_3[X]/(P)$. On note α la classe de X dans $\mathbb{F}_{27}$.

ii) Factoriser P dans $\mathbb{F}_{27}$ en produit de polynômes irréductibles, chacun exprimé en fonction de α.

iii) Est-ce que α est un générateur du groupe $\mathbb{F}_{27}^{\times}$?

c) On considère le polynôme $Q = X^9 - X + 1$ sur $\mathbb{F}_3$. On note $\mathbb{L}$ son corps de décomposition.

i) Démontrer que le polynôme Q n'a de racines ni dans $\mathbb{F}_3$ ni dans $\mathbb{F}_9$.

ii) Démontrer que les racines de Q dans $\mathbb{L}$ sont simples.

iii) Démontrer que $\beta \in \mathbb{F}_{27}$ est racine de Q si et seulement si β est racine de $P = X^3 - X - 1$.

iv) Démontrer que sur $\mathbb{F}_3$, le polynôme Q se factorise en $Q = PR$ où R est un polynôme de degré 6 que l'on déterminera.

v) Démontrer que R est irréductible sur $\mathbb{F}_3$.

vi) En déduire $[L : \mathbb{F}_3]$ et déterminer les sous-corps de L.

vii) Déterminer les groupes de Galois suivants : $\mathrm{Gal}(L/\mathbb{F}_3)$, $\mathrm{Gal}(L/\mathbb{F}_{27})$.

Exercice 17. (Évaluation 2021)

a) Énoncer la division euclidienne dans $\mathbb{R}[X]$. Démontrer qu'il y a unicité des polynômes intervenant dans l'écriture de la division euclidienne.

b) Soient $P_1 = X^3 - 2X^2 - 2X - 3$ et $P_2 = X^2 - 2X - 3$ des polynômes de $\mathbb{R}[X]$. En appliquant l'algorithme d'Euclide, déterminer le PGCD de P_1 et P_2.

c) Décomposer en produits d'irréductibles P_1 et P_2 dans $\mathbb{R}[X]$. En déduire une autre méthode pour déterminer leur PGCD.

Exercice 18. (Évaluation 2021) On considère trois polynômes de $\mathbb{Z}[X]$:

$$P_1 = X^6 - 5X + 20, \qquad P_2 = X^4 + 4X^3 - 6X^2 + 5X + 1, \qquad P_3 = X^3 - 3X^2 - X + 1.$$

a) Étudier l'irréductibilité des polynômes P_1, P_2, P_3 dans $\mathbb{Q}[X]$.

b) Est-ce que P_3 est irréductible dans $\mathbb{R}[X]$?

TD 4 : Extensions de corps, corps finis, théorie de Galois

Exercice 1. Quels sont les idéaux d'un corps ? Montrer qu'un morphisme d'anneaux entre deux corps est toujours injectif.

Exercice 2. Les réels e et π sont transcendants. Que peut-on en déduire de l'extension $\mathbb{Q} \subset \mathbb{R}$?

Exercice 3. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de degré impair. Démontrer que si $a \in \mathbb{K}$ est un carré dans $\mathbb{L}$, alors c'est un carré dans $\mathbb{K}$.

Exercice 4. Calculer les corps de rupture et de décomposition des polynômes suivants, et donner les degrés des extensions correspondantes :

a) $P_1 = X^2 + 7$.
b) $P_2 = X^3 - 2$.
c) $P_3 = X^3 - 11$.
d) $P_4 = X^4 + 1$.
e) $P_5 = X^4 - 1$.
f) $P_6 = X^4 + 2$.
g) $P_7 = X^4 - 2$.
h) $P_8 = X^4 + X^2 + 1$.
i) $P_9 = X^4 - 5X^2 + 6$.
j) $P_{10} = X^p - 1$ (où p est premier).

Exercice 5. Les assertions suivantes sont-elles vraies ou fausses ? Justifier la réponse par une démonstration ou un contre-exemple.

a) Deux corps de rupture d'un polynôme sont isomorphes.
b) Deux corps de rupture d'un polynôme irréductible sont isomorphes à unique isomorphisme près.
c) Deux corps de décomposition d'un polynôme sont isomorphes.
d) Deux corps de décomposition d'un polynôme sont isomorphes à unique isomorphisme près.
e) Le corps de rupture d'un polynôme irréductible est isomorphe à son corps de décomposition.
f) Il existe une fonction $f : \mathbb{N} \to \mathbb{N}$ telle que pour tout corps $\mathbb{K}$, pour tout polynôme $P \in \mathbb{K}[X]$, le degré du corps de décomposition de P sur $\mathbb{K}$ est majoré par $\deg\big(f(P)\big)$.

Exercice 6. Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$. À quel condition l'anneau quotient $\mathbb{K}[X]/(P)$ est-il un corps ? Dans ce cas, quel est le degré de l'extension $\mathbb{K} \subset \mathbb{K}[X]/(P)$?

Exercice 7. Existe-t-il un corps à 8 éléments ? 9 éléments ? 12 éléments ?

Exercice 8. Soit q, q' deux puissances de nombres premiers. À quelle condition le corps $\mathbb{F}_{q'}$ est-il une extension de $\mathbb{F}_q$?

Exercice 9. Déterminer les degrés des extensions suivantes :

a) $\mathbb{Q} \subset \mathbb{Q}\big(\sqrt{5}\big)$.
b) $\mathbb{Q} \subset \mathbb{Q}\big(\sqrt[n]{5}\big)$.
c) $\mathbb{Q} \subset \mathbb{Q}\big(\sqrt{2} + \sqrt{5}\big)$.
d) $\mathbb{Q} \subset \mathbb{Q}\big(i + \sqrt{5}\big)$.

Exercice 10. Quels sont les sous-corps de $\mathbb{F}_{64}$? Combien existe-t-il de générateurs de l'extension $\mathbb{F}_2 \subset \mathbb{F}_{64}$, c'est-à-dire d'éléments $x \in \mathbb{F}_{64}$ tels que $\mathbb{F}_{64} = \mathbb{F}_2(x)$? Combien le groupe $\mathbb{F}_{64}^\times$ a-t-il de générateurs ? Est-ce qu'il y a un lien entre ces deux notions ?

Exercice 11. Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie de corps.

a) Si $[\mathbb{L}:\mathbb{K}]$ est un nombre premier, démontrer que l'extension est monogène.

b) Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Démontrer que si $\deg(P)$ et $[\mathbb{L}:\mathbb{K}]$ sont premiers entre eux, alors P est irréductible sur $\mathbb{L}$.

c) Soit $\alpha \in \mathbb{K}$ un élément algébrique de degré impair. Démontrer que $\mathbb{K}(\alpha) = \mathbb{K}(\alpha^2)$.

Exercice 12. Corps à huit, neuf et seize éléments.

a) Dresser une liste de tous les polynômes irréductibles de degré ≤ 4 sur les corps $\mathbb{F}_2$ et $\mathbb{F}_3$.

b) Parmi les polynômes précédents, lesquels ont pour corps de rupture $\mathbb{F}_9$ et $\mathbb{F}_8$? Écrire la table de multiplication du corps correspondant dans ces cas.

c) Donner des isomorphismes explicites entre les corps ainsi obtenus.

d) Dans chacun des cas, est-ce que l'élément primitif canonique (la classe de X dans le quotient $\mathbb{K}[X]/(P)$) est-il un générateur de $\mathbb{K}^\times$?

e) Démontrer que $\mathbb{F}_8^\times$ est cyclique.

f) Démontrer que tous les éléments de $\mathbb{F}_8$ sont algébriques sur $\mathbb{F}_2$ est donner leurs polynômes minimaux.

g) Reprendre les trois dernières questions en remplaçant $\mathbb{F}_8$ par $\mathbb{F}_{16}$.

Exercice 13. Démontrer que les extensions suivantes sont galoisiennes, déterminer leur degré et leur groupe de Galois :

a) $\mathbb{R} \subset \mathbb{C}$.

b) $\mathbb{F}_q \subset \mathbb{F}_{q^n}$.

c) $\mathbb{Q} \subset \mathbb{Q}(\exp(2i\pi/n))$ (où $n \geq 2$).

Exercice 14. On considère l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Quel est son degré ? Démontrer que c'est une extension galoisienne. Déterminer ses sous-corps. Déterminer un élément primitif.

Exercice 15. On note $\alpha = \sqrt[4]{2}$ et $\beta = \sqrt[5]{2}$ et on pose $\mathbb{K} = \mathbb{Q}(\alpha) \subset \mathbb{L} = \mathbb{Q}(\alpha, \beta)$.

a) Déterminer les polynômes minimaux P et Q de α et β sur $\mathbb{Q}$. Quelles sont les racines (complexes) de ces polynômes ?

b) On note $\mathbb{L}' \subset \mathbb{C}$ le sous-corps engendré par les racines de P et Q. Combien y-a-t-il de morphismes $\mathbb{L} \to \mathbb{L}'$? Décrire les.

c) Déterminer le polynôme minimal de β sur $\mathbb{Q}(\alpha)$.

d) Que vaut $[\mathbb{L}:\mathbb{Q}]$?

e) Déterminer $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ et $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$.

f) Les extensions $\mathbb{Q} \subset \mathbb{K}$ et $\mathbb{Q} \subset \mathbb{L}$ sont-elles galoisiennes ?

TD 5 : Formes normales

Exercice 1. Faire le lien entre la multiplication par l'une des matrices qui suivent avec les opérations élémentaires :

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\quad \begin{pmatrix}1 & 0\\ a & 1\end{pmatrix},\quad \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ b & a & 1\end{pmatrix},\quad \begin{pmatrix}1 & a & 0\\ 0 & 1 & 0\\ 0 & b & 1\end{pmatrix},\quad \begin{pmatrix}0 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 0\end{pmatrix},\quad \begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix}.$$

a) $L_1 \leftrightarrow L_2$

b) $L_1 \leftarrow L_1 + \alpha L_2$

c) $L_2 \leftarrow L_2 + \alpha L_1$

d) $L_1 \leftarrow L_2, L_2 \leftarrow L_3$, et $L_3 \leftarrow L_1$

e) $L_1 \leftarrow L_1 + \alpha L_2$ et $L_3 \leftarrow L_3 + \beta L_2$

f) $L_3 \leftarrow L_3 + \alpha L_1 + \beta L_2$

g) $C_1 \leftrightarrow C_2$

h) $C_1 \leftarrow C_1 + \alpha C_2$

i) $C_2 \leftarrow C_2 + \alpha C_1$

j) $C_1 \leftarrow C_2, C_2 \leftarrow C_3$, et $C_3 \leftarrow C_1$

k) $C_1 \leftarrow C_1 + \alpha C_2$ et $C_3 \leftarrow C_3 + \beta C_2$

l) $C_3 \leftarrow C_3 + \alpha C_1 + \beta C_2$

Exercice 2. À quelle matrice correspond l'opération $C_i \leftarrow \sum_{j=1}^{n} a_j C_j$? L'opération $L_i \leftarrow \sum_{j=1}^{n} a_j L_j$?

Exercice 3.

a) Est-ce que l'ensemble des matrices inversibles à coefficients entiers forme un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$?

b) Calculer le produit $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}$ et en déduire que si $a, b, c, d \in \mathbb{Z}$, alors l'inverse de $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ est à coefficients entiers si et seulement si $ad - bc = \pm 1$.

c) En déduire que $\mathrm{GL}_2(\mathbb{Z}) = \{ A \in \mathcal{M}_2(\mathbb{R}) \mid \det(A) = \pm 1 \}$.

d) Vérifier que les matrices du premier exercice sont unimodulaires (de déterminant ± 1).

Exercice 4. À l'aide d'opérations élémentaires, sur les lignes et les colonnes, déterminer les formes normales de Smith des matrices suivantes :

a) $A = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$

b) $B = \begin{pmatrix}2 & 3\\ 4 & 1\end{pmatrix}$

c) $C = \begin{pmatrix}2 & 3\\ 4 & 5\end{pmatrix}$

d) $D = \begin{pmatrix}2 & 3\\ 4 & 6\end{pmatrix}$

e) $E = \begin{pmatrix}1 & 2 & 2\\ -3 & 3 & 6\\ 5 & -2 & -8\end{pmatrix}$

Exercice 5. Soit $A = \langle v_1, \dots, v_r \rangle \leq \mathbb{Z}^p$ un sous-groupe de $\mathbb{Z}^p$ engendré par une famille $(v_1, \dots, v_r)$ de vecteurs (colonnes) $v_i \in \mathbb{Z}^p$. Pour déterminer une base de A, il suffit de considérer la matrice $M \in \mathcal{M}_{p,r}(\mathbb{Z})$ dont les colonnes sont les v_i, d'échelonner cette matrice **en effectuant des opérations sur les colonnes uniquement** et de garder les colonnes non nulles. Appliquer cette procédure aux deux sous-groupes suivants :

a) Le sous-groupe $A_1 \leq \mathbb{Z}^3$ engendré par $v_1 = (1, 0, -1)$, $v_2 = (4, 3, -1)$, $v_3 = (0, 9, 3)$, et $v_4 = (3, 12, 3)$.

b) Le sous-groupe $A_2 \leq \mathbb{Z}^4$ engendré par $w_1 = (9, 1, 4, 7)$, $w_2 = (6, 2, 5, 8)$ et $w_3 = (12, 4, 8, 10)$.

Exercice 6. Soit $A = \langle v_1, \dots, v_r \rangle \leq \mathbb{Z}^p$ et M comme dans l'exercice précédent. Pour obtenir la structure de groupe abélien de $\mathbb{Z}^p/A$, il suffit de : (i) calculer la forme normale de Smith $UMV = D$ de la matrice M ; (ii)

les coefficients diagonaux de D sont notés $d_1 \mid d_2 \mid \cdots \mid d_s$, où $s = \min(r, p)$; (iii) le quotient est isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z}^{p-s}$ (avec $\mathbb{Z}/1\mathbb{Z} = 0$ et $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$).

Reprendre les sous-groupes A_1 et A_2 de l'exercice précédent et déterminer la structure des quotients.

Exercice 7. Soit $A = \langle v_1, \ldots, v_r \rangle \leq \mathbb{Z}^p$ et M comme dans l'exercice précédent. On dit qu'une base $(e_1, \ldots, e_p)$ de $\mathbb{Z}^p$ est une *base adaptée à* A si A est engendrée par la famille $(d_1 e_1, \ldots, d_p e_p)$ où les d_i sont les facteurs invariants (on omet $d_i e_i$ si $d_i = 0$, et on note $d_i = 0$ si $i > r$).

On en détermine une de la façon suivante : (i) on calcule la forme normale de Smith $UMV = D$; (ii) la matrice $U \in \mathrm{GL}_p(\mathbb{Z})$ représente les opérations effectuées sur les lignes, que l'on garde en mémoire ; (iii) les colonnes de U^{-1} forment alors une base de $\mathbb{Z}^p$ adaptée à A.

Reprendre les sous-groupes A_1 et A_2 de l'exercice précédent et déterminer une base adaptée de $\mathbb{Z}^p$ dans chacun des cas.

Exercice 8. Déterminer tous les groupes abéliens (à isomorphisme près) d'ordre 72.