Exercices

1. Soit A un anneau (pas nécessairement commutatif). On rappelle que $a \in A$ est un diviseur de zéro à gauche, si $a \neq 0$ et s'il existe $b \in A$ avec $b \neq 0$ et vérifiant $ab = 0$. De même, on dit que a est un diviseur à droite, si $a \neq 0$ et s'il existe $b \in A$ avec $b \neq 0$ et vérifiant $ba = 0$.

   (a) On considère l'anneau $A = \mathrm{Mat}_n(k)$ des matrices carrés de taille $n \geq 2$ à coefficients dans un corps k. Montrer qu'une matrice non-nulle $M \in A$ est un diviseur de zéro à gauche (à droite) si est seulement si M n'est pas inversible.

   (b) Soit k un corps. On note $k[T]$ l'espace vectoriel des polynômes à coefficients dans k en une variable T et $A = (\mathrm{End}(k[T]), +, \circ)$ l'anneau des endomorphismes (= applications k-linéaires) de $k[T]$ dans lui-même.
   — On considère la dérivation $\partial \in A$ définie par $\partial(P) = P'$. Montrer que ∂ est un diviseur de zéro à gauche, mais pas à droite.
   — Trouver un élément $f \in A$ qui est un diviseur à droite, mais pas à gauche.

2. Soit A un anneau unitaire. On dit qu'un élément $a \in A$ est inversible s'il existe un élément $b \in A$ tel que $ab = ba = 1$. Si A n'est pas commutatif, on définit aussi les notions d'inverse à gauche et inverse à droite : un élément $a \in A$ est inversible à gauche (resp. à droite) s'il existe un élément $b_g \in A$ (resp. $b_d \in A$) tel que $b_g a = 1$ (resp. $ab_d = 1$).

   (a) Montrer que si un élément a admet un inverse à gauche b_g et un inverse à droite b_d, alors $b_g = b_d$.

   (b) Soit k un corps de caractéristique 0. On note $k[T]$ l'espace vectoriel des polynômes à coefficients dans k en une variable T et $A = (\mathrm{End}(k[T]), +, \circ)$ l'anneau des endomorphismes (= applications k-linéaires) de $k[T]$ dans lui-même.
   — On considère la dérivation $\partial \in A$ définie par $\partial(P) = P'$. Montrer que ∂ admet un inverse à droite (en le donnant explicitement), mais n'admet pas d'inverse à gauche.
   — Trouver un élément $f \in A$ admettant un inverse à gauche, mais pas d'inverse à droite.
   — Qu'est-ce qui change quand k est de caractéristique $p > 0$?

3. Soit V un k-espace vectoriel de dimension quelconque et $A = (\mathrm{End}(V), +, \circ)$ l'anneau des endomorphismes (= applications k-linéaires) de V dans V.
   — Montrer que $f \in A$ est inversible à gauche si et seulement si f est une application injective.
   — Montrer que $f \in A$ est inversible à droite si et seulement si f est une application surjective.
   — On suppose que V est de dimension finie. Montrer que $f \in A$ est inversible à gauche si et seulement si f est inversible à droite.

4. Soit A un anneau unitaire. On note 1 l'unité de A et 0_A le neutre (pour $+$) de A. On rappelle la définition d'un module (à gauche) M sur l'anneau A.

   (a) $(M, +)$ est un groupe abélien. On note 0_M le neutre.

   (b) M est muni d'une opération de A, c'est-à-dire on a une application

   $$A \times M \to M, \quad (a, m) \mapsto a.m$$

   qui vérifie
   — $1.m = m, \quad \forall m \in M$

— $(a+b).m = a.m + b.m, \quad \forall m \in M \quad \forall a,b \in A$
— $a.(m+n) = a.m + a.n, \quad \forall m,n \in M \quad \forall a \in A$
— $(ab).m = a.(b.m), \quad \forall m \in M \quad \forall a,b \in A$

Montrer que $0_A.m = 0_M$ et que $(-1).m = -m \quad \forall m \in M$.

5. Soit M un sous-$\mathbb{Z}$-module de $\mathbb{Z}$. Montrer qu'il existe un entier $n \in \mathbb{Z}$ tel que $M = n\mathbb{Z} \subset \mathbb{Z}$.
6. On considère les anneaux $A = \mathbb{Z}/5\mathbb{Z}$ et $B = \mathbb{Z}/30\mathbb{Z}$.
   (a) Est-ce que A est un B-module ?
   (b) Est-ce que B est un A-module ?
7. On considère l nombres rationnels $r_1, \ldots, r_l \in \mathbb{Q}$ et l'application
$$\phi : \mathbb{Z}^l \longrightarrow \mathbb{Q}, \quad (a_1, \ldots, a_l) \mapsto \sum_{i=1}^{l} a_i r_i.$$
   (a) Montrer que ϕ est une application $\mathbb{Z}$-linéaire.
   (b) Exemple : on prend $l = 2$ et $r_1 = \frac{1}{2}, r_2 = \frac{1}{13}$. Déterminer l'image $\mathrm{im}(\phi)$ de l'application ϕ comme sous-$\mathbb{Z}$-module de $\mathbb{Q}$.
   (c) Montrer que ϕ ne peut pas être surjectif en construisant de façon explicite un nombre rationnel à partir des nombres $r_1, \ldots, r_l$ qui n'est pas dans $\mathrm{im}(\phi)$.
   (d) Montrer qu'il existe un nombre rationnel $r \in \mathbb{Q}$ tel que $\mathrm{im}(\phi) = r\mathbb{Z} \subset \mathbb{Q}$.
8. Soit A un anneau unitaire. On considère l'anneau $B = A[T]$ des polynômes à coefficients dans A en une variable T et les applications
$$\partial : B \to B,\ \partial(P) = P', \quad \mathrm{ev}_0 : B \to A,\ \mathrm{ev}_0(P) = P(0).$$
données par la dérivation des polynômes et l'évaluation en $T = 0$ respectivement.
   (a) Est-ce que ∂ et ev_0 sont des applications A-linéaires ? B-linéaires ?
   (b) Est-ce que ∂ et ev_0 sont des homomorphismes de groupes ? homomorphismes d'anneaux ?
9. On considère l'anneau de Gauss
$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}, \quad \text{avec } i^2 = -1.$$
   (a) Montrer que $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[i]$.
   (b) Est-ce que $\mathbb{Z}[i]$ est un $\mathbb{Z}$-module ?
   (c) Est-ce que $\mathbb{Z}$ est un $\mathbb{Z}[i]$-module ?
   (d) Déterminer tous les $\mathbb{Z}$-modules M vérifiant $\mathbb{Z} \subset M \subset \mathbb{Z}[i]$.
   (e) Parmi ces $\mathbb{Z}$-modules lesquels sont des $\mathbb{Z}[i]$-modules ?
   (f) Parmi ces $\mathbb{Z}$-modules lesquels sont des sous-anneaux de $\mathbb{Z}$?
10. On considère deux idéaux $I_1 = n_1\mathbb{Z}$ et $I_2 = n_2\mathbb{Z}$ de $\mathbb{Z}$. Montrer les égalités suivantes.
   (a) $I_1 + I_2 = \mathrm{PGCD}(n_1, n_2)\mathbb{Z}$.
   (b) $I_1 \cdot I_2 = n_1 n_2 \mathbb{Z}$.
   (c) $I_1 \cap I_2 = \mathrm{PPCM}(n_1, n_2)\mathbb{Z}$.
11. On considère deux idéaux I_1 et I_2 d'un anneau A. Montrer que si $I_1 + I_2 = A$, alors $I_1 \cdot I_2 = I_1 \cap I_2$.
12. Montrer que l'anneau de Gauss $\mathbb{Z}[i]$ est un anneau intègre.
13. Montrer que si K est un corps, alors l'anneau des polynômes $K[X]$ est un anneau intègre.

14. On considère des A-modules N_1, N_2 et M qui vérifient $N_1 \subset N_2 \subset M$. Montrer qu'il existe un isomorphisme
$$M/N_2 \longrightarrow (M/N_1)/(N_2/N_1).$$

15. On considère deux A-modules M et L et une application A-linéaire $f : M \to L$. Soit $N \subset M$ un sous-A-module tel que $N \subset \ker(f)$.

    (a) Montrer qu'il existe une application A-linéaire $\overline{f} : M/N \to L$, qui factorise à travers f, c'est-à-dire qu'on a la relation $\overline{f} \circ \pi = f$, où $\pi : M \to M/N$ est l'application naturelle de passage au quotient.

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"] & L \\ M/N \arrow[ur, "\overline{f}"] & \end{tikzcd}$$

    (b) Montrer que $\overline{f}$ est injectif si et seulement si $N = \ker(f)$.

    (c) Montrer que $\overline{f}$ est un isomorphisme si et seulement si $N = \ker(f)$ et f est surjectif.

    (d) Application : On considère l'application $\mathbb{R}$-linéaire d'évaluation en i d'un polynôme à coefficients réels
$$f : \mathbb{R}[X] \to \mathbb{C}, \quad P \mapsto P(i).$$
    Montrer que f induit un isomorphisme d'anneaux $\overline{f} : \mathbb{R}[X]/(X^2+1) \to \mathbb{C}$.

16. Soit A un anneau commutatif unitaire et soit $a \in A$. On note (a) l'idéal de A engendré par a. Montrer que $(a) = A$ si et seulement si a est inversible dans A.

17. Montrer qu'un idéal maximal est premier.

18. Déterminer tous les idéaux premiers (resp. maximaux) de l'anneau $\mathbb{Z}$.

19. Déterminer tous les idéaux de l'anneau $\mathbb{R}[X]$. Parmi ces idéaux lesquels sont premiers ? maximaux ?

20. Déterminer tous les idéaux de l'anneau $\mathbb{C}[X]$. Parmi ces idéaux lesquels sont premiers ? maximaux ?

21. Déterminer si les idéaux suivants sont premiers/maximaux

    (a) $I = (X^2 - 2X + 1) \subset \mathbb{R}[X]$,

    (b) $I = (17, X - 2) \subset \mathbb{Z}[X]$,

    (c) $I = (X - Y) \subset \mathbb{R}[X, Y]$.

22. (a) Montrer que l'idéal $(X^2+1) \subset \mathbb{Z}[X]$ engendré par le polynôme $X^2+1 \in \mathbb{Z}[X]$ est premier, mais pas maximal.

    (b) Montrer que l'idéal $(2, X^2+1) \subset \mathbb{Z}[X]$ engendré par 2 et X^2+1 n'est pas maximal. Trouver un idéal I vérifiant
$$(2, X^2+1) \subsetneq I \subsetneq \mathbb{Z}[X].$$

    (c) Montrer que l'idéal $(3, X^2+1) \subset \mathbb{Z}[X]$ engendré par 3 et X^2+1 est maximal. Décrire l'anneau quotient $\mathbb{Z}[X]/(3, X^2+1)$.

23. Soit p un nombre premier et $P \in \mathbb{Z}/p\mathbb{Z}[X]$ un polynôme de degré n à coefficients dans le corps $\mathbb{Z}/p\mathbb{Z}$.

    (a) Montrer que l'anneau quotient $A = \mathbb{Z}/p\mathbb{Z}[X]/(P)$ est un anneau fini de cardinal p^n.

(b) Montrer que A est un corps si et seulement si P est un polynôme irréductible.

24. Soit $I = (2, X^2+1) \subset \mathbb{Z}[X]$ l'idéal engendré par 2 et X^2+1. Montrer que I n'est pas principal, c'est-à-dire que I ne peut pas être engendré par un seul polynôme $P \in \mathbb{Z}[X]$.

25. Soit $P = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]$ un polynôme non nul à coefficients entiers $a_i \in \mathbb{Z}$. On considère le contenu de P noté $c(P)$ et défini comme
$$c(P) = \mathrm{PGCD}(a_0, a_1, \ldots, a_d).$$
    (a) Montrer que $c(aP) = ac(P)$ pour tout $a \in \mathbb{Z}$ et $P \in \mathbb{Z}[X]$.
    (b) Montrer que $c(PQ) = c(P)c(Q)$ pour tout $P, Q \in \mathbb{Z}[X]$. (Indication : se ramener au cas $c(P) = c(Q) = 1$, ensuite par l'absurde supposer qu'il existe un nombre premier p qui divise $c(PQ)$ et réduire modulo p, c'est-à-dire utiliser l'homomorphisme d'anneaux $\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$.)
    (c) Application : Soit $P \in \mathbb{Z}[X]$ un polynôme avec $\deg(P) \geq 2$. On suppose qu'il existe une factorisation $P = A \cdot B$ dans $\mathbb{Q}[X]$, c'est-à-dire $A, B \in \mathbb{Q}[X]$ vérifiant $0 < \deg(A) < \deg(P)$ et $0 < \deg(B) < \deg(P)$, alors il existe une factorisation de P dans $\mathbb{Z}[X]$. (Attention : la factorisation dans $\mathbb{Z}[X]$ n'est pas nécessairement donnée par $P = A \cdot B$.)
    (d) Application : Soient $a, b \in \mathbb{Z}$ deux entiers premiers entre eux avec $a \neq 0$. On note $(aX+b) \subset \mathbb{Z}[X]$ l'idéal engendré par le polynôme $aX+b$ dans $\mathbb{Z}[X]$. Montrer que $P \in (aX+b)$ si et seulement si $P(-\frac{b}{a}) = 0$.

26. On considère les deux anneaux $A = K[X]$ et $B = K[X^n]$, où K est un corps et $n \in \mathbb{N}^*$. Montrer que A est un B-module libre de rang n. Montrer que $\{1, X, X^2, \ldots, X^{n-1}\}$ est une B-base de A.

27. On considère le sous-ensemble M de $\mathbb{Q}$ donné par
$$M = \{\frac{a}{2^n} \mid a \in \mathbb{Z} \text{ et } n \in \mathbb{N}\}.$$
    (a) Montrer que M est un sous-Z-module de $\mathbb{Q}$.
    (b) On condidère l'application $f : \mathbb{Z}[X] \to \mathbb{Q}$ donné par $P \mapsto P(\frac{1}{2})$.
        i. Montrer que f est $\mathbb{Z}$-linéaire.
        ii. Montrer que $\mathrm{im}(f) = M$.
        iii. Montrer que $\ker(f) = (2X-1)$.
        iv. En déduire qu'il existe un isomorphisme $\mathbb{Z}$-linéaire
$$\overline{f} : \mathbb{Z}[X]/(2X-1) \to M.$$
    (c) Est-ce que M est un $\mathbb{Z}$-module de type fini ?

28. On considère l'application $f : \mathbb{Z}[X] \to \mathbb{R}$ définie par $f(P) = P(\sqrt{2})$.
    (a) Montrer que $\mathrm{im}(f)$ est un $\mathbb{Z}$-module libre et en donner une base.
    (b) Déterminer $\ker(f)$.
    (c) Mêmes questions pour l'application f définie par $f(P) = P(\pi)$.

29. Montrer que l'anneau de Gauss $\mathbb{Z}[i]$ est euclidien pour la norme complexe.

30. Montrer que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est euclidien pour la norme complexe.

31. Montrer que $\mathbb{Z}[X]$ n'est pas un anneau principal.

32. Montrer que $\mathbb{R}[X, Y]$ n'est pas un anneau principal en montrant que l'idéal (X, Y) n'est pas principal.

33. On considère l'anneau de Gauss $\mathbb{Z}[i]$.
   (a) Déterminer les inversibles de $\mathbb{Z}[i]$.
   (b) Soit $p \in \mathbb{N}$ un nombre premier. Montrer qu'il y a une équivalence entre les deux propriétés suivantes
      i. Il existe $a, b \in \mathbb{Z}$ tel que $p = a^2 + b^2$.
      ii. Il existe des éléments non-inversibles $u, v \in \mathbb{Z}[i]$ tel que $p = uv$.
34. En faisant des opérations sur les lignes et les colonnes, calculer les facteurs invariants des matrices à coefficients entiers suivantes

$$\begin{pmatrix} 1 & 2 \\ 6 & 17 \\ -3 & -6 \end{pmatrix}, \qquad \begin{pmatrix} 1 & -2 & 1 \\ 2 & 2 & 8 \\ 5 & -10 & 5 \end{pmatrix}.$$

   En déduire les classes d'isomorphisme des noyaux et conoyaux des applications $\mathbb{Z}$-linéaires de $\mathbb{Z}^n$ dans $\mathbb{Z}^m$ déterminées par ces deux matrices.
35. On considère l'application

$$f : \mathbb{Z}[i] \to \mathbb{Z}/5\mathbb{Z}, \qquad a + ib \mapsto a + 3b \bmod 5.$$

   (a) Est-ce que f est un homomorphisme d'anneaux ?
   (b) Montrer que $\ker(f) = (2 + i)$.
   (c) En déduire qu'on a un isomorphisme d'anneaux $\overline{f} : \mathbb{Z}[i]/(2 + i) \to \mathbb{Z}/5\mathbb{Z}$.
36. Soit $z = u + iv \in \mathbb{Z}[i]$ avec $\mathrm{PGCD}(u, v) = 1$. On pose $n = u^2 + v^2$.
   (a) Montrer qu'il existe un entier $c \in \{0, \ldots, n-1\}$ vérifiant $u + cv \equiv 0 \;\; [n]$. (Indication : Si $v \neq 0$, montrer que v est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et prendre $\overline{c} = -uv^{-1} \in \mathbb{Z}/n\mathbb{Z}$)
   (b) Montrer que l'entier c vérifie la congruence $c^2 + 1 \equiv 0 \;\; [n]$.
   (c) Montrer que l'application

$$f : \mathbb{Z}[i] \to \mathbb{Z}/n\mathbb{Z}, \qquad a + ib \mapsto a + cb \bmod n$$

   est un homomorphisme d'anneaux qui induit un isomorphisme

$$\overline{f} : \mathbb{Z}[i]/(u + iv) \to \mathbb{Z}/n\mathbb{Z}.$$

37. (a) Calculer $\mathrm{PGCD}(3, 2 + i)$ et $\mathrm{PGCD}(6 + 3i, 1 + 3i)$ dans l'anneau de Gauss $\mathbb{Z}[i]$.
   (b) Déterminer le conoyau de l'application

$$\mathbb{Z}[i] \to \mathbb{Z}[i] \times \mathbb{Z}[i], \qquad z \mapsto (3z, (2 + i)z).$$

   (c) Montrer que le conoyau de l'application

$$\mathbb{Z}[i] \to \mathbb{Z}[i] \times \mathbb{Z}[i], \qquad z \mapsto ((6 + 3i)z, (1 + 3i)z).$$

   est donnée par l'application

$$\mathbb{Z}[i] \times \mathbb{Z}[i] \to \mathbb{Z}[i] \times \mathbb{Z}/5\mathbb{Z}, \qquad (z_1, z_2) \mapsto ((1 + i)z_1 - 3z_2, \overline{f}(z_1)),$$

   où $\overline{f}$ est défini dans l'exercice précédent.

38. Soit p un nombre premier $\neq 2$. On considère les deux applications $f, g : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ définies par
$$f(x) = x^2 \quad \text{et} \quad g(x) = x^{\frac{p-1}{2}} \quad \forall x \in (\mathbb{Z}/p\mathbb{Z})^*.$$
   (a) Montrer que $\ker(g) = \mathrm{im}(f)$.
   (b) En déduire que les 3 propositions suivantes sont équivalentes :
      i. $p \equiv 1 \bmod 4$
      ii. $\overline{-1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$
      iii. $X^2 + \overline{1} \in \mathbb{Z}/p\mathbb{Z}[X]$ n'est pas un polynôme irréductible
39. On considère deux entiers $a, b \in \mathbb{N}^*$ et on note $d = \mathrm{PGCD}(a, b)$ et $m = \mathrm{PPCM}(a, b)$.
   (a) Montrer qu'on a une suite exacte de groupes
$$0 \to \mathbb{Z}/m\mathbb{Z} \xrightarrow{i} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \xrightarrow{p} \mathbb{Z}/d\mathbb{Z} \to 0,$$
   où les homomorphismes i et p sont définis par
$$i(x[m]) = (x[a], x[b]) \ \text{ et } \ p(x_1[a], x_2[b]) = x_1[d] - x_2[d].$$
   (b) On note $u, v \in \mathbb{Z}$ les entiers apparaissant dans l'identité de Bézout $au + bv = d$ et on note $\alpha = \frac{a}{d}$ et $\beta = \frac{b}{d}$. On définit les homomorphismes p' et i'
$$p' : \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, \quad p'(x[d]) = (x\alpha u[a], -x\beta v[b])$$
$$i' : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad i'(x_1[a], x_2[b]) = \beta v x_1 + \alpha u x_2[m].$$
   Montrer que p' et i' sont des scindages de la suite exacte précédente, c'est-à-dire que
$$i' \circ i = \mathrm{Id} \quad \text{et} \quad p \circ p' = \mathrm{Id}.$$
   (c) En déduire un isomorphisme
$$\Phi : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z},$$
   qu'on donnera de manière explicite.
40. Déterminer les facteurs invariants des groupes abéliens suivants
   (a) $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
   (b) $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$
   (c) $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
41. Soit p un nombre premier. Parmi les groupes d'ordre p^4 suivants, trouver ceux qui sont isomorphes
   (a) $(\mathbb{Z}/p\mathbb{Z})^4$
   (b) $(\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})$
   (c) $(\mathbb{Z}/p^3\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$
   (d) $(\mathbb{Z}/p^4\mathbb{Z})$
   (e) $\ker(f)$, $f : (\mathbb{Z}/p\mathbb{Z})^5 \to \mathbb{Z}/p\mathbb{Z}$, $\ (x_1, \ldots, x_5) \mapsto x_1 + \ldots + x_5$
   (f) $\ker(g)$, $g : (\mathbb{Z}/p^5\mathbb{Z}) \to \mathbb{Z}/p^5\mathbb{Z}$, $\ x \mapsto px$

42. On considère les deux matrices

$$M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

   (a) Calculer les invariants de similitude, ainsi que les polynômes minimaux et caractéristiques de M_1 et M_2.
   (b) Est-ce que M_1 et M_2 sont semblables ?
43. Déterminer les invariants de similitude des matrices

$$A = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 1 & 1 \\ 2 & -2 & -2 \end{pmatrix}, \qquad B = \begin{pmatrix} 3 & 2 & -5 \\ 2 & 6 & -10 \\ 1 & 2 & -3 \end{pmatrix}.$$

44. On considère la matrice de Jordan d'ordre r

$$J_r(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & 0 & \lambda & 1 \\ 0 & \dots & 0 & 0 & \lambda \end{pmatrix}$$

avec $\lambda \in K$ sur la diagonale et 1 au-dessus. Calculer par récurrence sur r les invariants de similitude de la matrice $J_r(\lambda)$.
45. Déterminer à similitude près toutes les matrices M carrées d'ordre 4 nilpotentes, c'est-à-dire vérifiant $M^4 = 0$. Donner pour chaque classe de similitude un représentant.
46. Déterminer le corps de fractions $\mathrm{Fr}(\mathbb{Z}[i])$ de l'anneau de Gauss $\mathbb{Z}[i]$.
47. Donner le degré des extensions de corps de $\mathbb{Q}$ suivantes :

$$\mathbb{Q}(\sqrt{2}), \qquad \mathbb{Q}(\sqrt{3}), \qquad \mathbb{Q}(\sqrt{2}, \sqrt{3}), \qquad \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

48. (a) Donner le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$, ainsi que sur $\mathbb{Q}(\sqrt{3})$.
   (b) Donner le polynôme minimal de $\sqrt{2} - \sqrt{3}$ sur $\mathbb{Q}$.
49. Donner le degré de l'extension $\mathbb{Q}(\sqrt{2}, \sqrt[3]{7})$ de $\mathbb{Q}$.
50. On considère l'extension de corps $L = \mathbb{Q}[X]/(X^3 - 2)$ de $\mathbb{Q}$ et on note $\omega_1, \omega_2, \omega_3$ les trois racines complexes du polynôme $X^3 - 2$.
   (a) Donner le degré $[L : \mathbb{Q}]$.
   (b) Pour chacune des trois racines complexes on note L_i l'image de l'application

$$\phi_i : L \to \mathbb{C}, \qquad \overline{X} \mapsto \omega_i.$$

   Donner une base de chaque $\mathbb{Q}$-espace vectoriel L_i.
   (c) Déterminer les intersections $L_i \cap L_j$ pour $i \neq j$.
51. On considère le corps fini $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$.
   (a) Donner une base de $\mathbb{F}_4$ comme $\mathbb{F}_2$-espace vectoriel.
   (b) Etablir la table de multiplication de $\mathbb{F}_4$.

52. On considère les deux polynômes dans $\mathbb{F}_2[X]$

$$P_1 = X^3 + X^2 + 1 \quad \text{et} \quad P_2 = X^3 + X + 1.$$

   (a) Montrer que P_1 et P_2 sont les seuls polynômes irréductibles de degré 3 dans $\mathbb{F}_2[X]$.
   (b) On note L_i le corps fini $\mathbb{F}_2[X]/(P_i)$. On considère le morphisme de $\mathbb{F}_2$-algèbres

$$\Phi : \mathbb{F}_2[X] \to \mathbb{F}_2[X], \quad X \mapsto X + 1.$$

   Montrer que Φ est un isomorphisme.
   (c) Montrer que Φ induit un isormorphisme de corps de L_1 avec L_2.

53. Pour chacune des extensions suivantes $K \subset L$ déterminer le groupe $\mathrm{Aut}_K(L)$ des automorphismes de L sur K
   (a) $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{2})$
   (b) $K = \mathbb{Q}(\sqrt{2})$ et $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$
   (c) $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$
   (d) $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$
   (e) $K = \mathbb{F}_2$ et $L = \mathbb{F}_4$
   (f) $K = \mathbb{F}_2$ et $L = \mathbb{F}_8$

54. On considère l'extension L de $\mathbb{Q}$ engendré par $\sqrt[3]{2}$ et $\omega = e^{\frac{2i\pi}{3}}$ dans $\mathbb{C}$

$$L = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

   (a) Déterminer le degré $[L : \mathbb{Q}]$.
   (b) Déterminer le groupe des automorphismes $\mathrm{Aut}_{\mathbb{Q}}(L)$.
   (c) Donner un élément primitif ainsi que son polynôme minimal.

55. Soit K un corps. On note $K(X)$ le corps de fractions rationnelles en X et à coefficients dans K. Est-ce que les extensions suivantes sont algébriques ? finies ? Si oui, donner leur degré.
   (a) $K \subset K(X)$
   (b) $K(X^2) \subset K(X)$
   (c) $K(\frac{1}{X^3+X}) \subset K(X)$
   (d) $K(\frac{X-1}{X+1}) \subset K(X)$

56. Soit K un corps et $\alpha \in L$, où L est une extension de K. Montrer que α est algébrique sur K si et seulement si $K(\alpha)$ est une extension finie de K.

57. On considère le sous-ensemble $\overline{\mathbb{Q}}$ de $\mathbb{C}$ défini par

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algébrique sur } \mathbb{Q}\}.$$

   Montrer que $\overline{\mathbb{Q}}$ est un corps algébriquement clos. On pourra utiliser le fait que $\mathbb{C}$ est algébriquement clos.

58. Soit K un corps fini d'ordre p^n avec p un nombre premier. En utilisant la correspondance de Galois déterminer tous les sous-corps de K. Exemple : donner la liste de tous les sous-corps de $\mathbb{F}_{64}$.

59. Soit K un corps de caractéristique $p > 0$. On note $K(X)$ le corps de fractions rationnelles en X et à coefficients dans K.

(a) Montrer que l'extension $K(X^p) \subset K(X)$ est non-séparable de degré p et que

$$\mathrm{Aut}_{K(X^p)}(K(X)) = \{\mathrm{id}\}.$$

(b) Montrer que l'extension $K(X^p - X) \subset K(X)$ est séparable de degré p et que

$$\mathrm{Aut}_{K(X^p - X)}(K(X)) = \mathbb{Z}/p\mathbb{Z} = \langle \sigma \rangle,$$

où σ est l'automorphisme de $K(X)$ défini par $\sigma(X) = X + 1$.

60. On considère le polynôme $P = X^3 + 3 \in \mathbb{Q}[X]$. Soit L le corps de décomposition de P dans $\mathbb{C}$. On note $\omega = e^{\frac{2i\pi}{6}} \in \mathbb{C}$.
    (a) Ecrire les racines de P en fonction de $\sqrt[3]{3}$ et ω.
    (b) Déduire que P est irréductible sur $\mathbb{Q}$.
    (c) Montrer que $\omega \in L$.
    (d) Déterminer le polynôme minimal de ω sur $\mathbb{Q}$ ainsi que sur $\mathbb{Q}(\sqrt[3]{3})$.
    (e) Déduire que $[L : \mathbb{Q}] = 6$ et que $\mathrm{Gal}_{\mathbb{Q}}(L) = \mathcal{S}_3$.
    (f) Donner la liste des sous-corps de L contenant $\mathbb{Q}$. Donner un générateur pour chaque sous-corps.
    (g) On considère le polynôme $Q = X^6 - 9$. Montrer que L est le corps de décomposition de Q. On identifie $\mathrm{Gal}_{\mathbb{Q}}(L)$ à un sous-groupe du groupe symétrique $\mathcal{S}_6$ via son action sur les racines de Q. Donner la liste des éléments de $\mathrm{Gal}_{\mathbb{Q}}(L)$ comme sous-groupe de $\mathcal{S}_6$.
61. On considère le polynôme $P = X^6 - 3 \in \mathbb{Q}[X]$. Soit L le corps de décomposition de P dans $\mathbb{C}$. On note $\omega = e^{\frac{2i\pi}{6}} \in \mathbb{C}$.
    (a) Montrer que $L = \mathbb{Q}(\sqrt[6]{3}, \omega)$.
    (b) Montrer qu'on a des inclusions de corps

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt[6]{3}) \qquad \text{et} \qquad \mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{Q}(\sqrt[6]{3}).$$

    (c) Justifier que $\sqrt[6]{3} \notin \mathbb{Q}(\sqrt{3})$.
    (d) Montrer que $[L : \mathbb{Q}(\sqrt{3})] = 6$ et que $[L : \mathbb{Q}] = 12$.
    (e) En identifiant $\mathrm{Gal}_{\mathbb{Q}}(L)$ à un sous-groupe de $\mathcal{S}_6$ donner la liste des éléments de $\mathrm{Gal}_{\mathbb{Q}}(L)$.
    (f) Donner la liste des sous-corps M de L contenant $\mathbb{Q}$. Pour chaque M dire si M est une extension galoisienne sur $\mathbb{Q}$ et donner un système de générateurs.
62. Pour $n \in \mathbb{N}^*$ soit $\Phi_n \in \mathbb{C}[X]$ le polynôme unitaire dont les racines sont simples, égales aux racines primitives n-ièmes de l'unité dans $\mathbb{C}$. Le polynôme Φ_n est appelé le n-ième polynôme cyclotomique.
    (a) Montrer que $\prod_{d|n} \Phi_d = X^n - 1$. En déduire par récurrence que pour tout $n \geq 1$ $\Phi_n \in \mathbb{Z}[X]$. (Indication : utiliser la multiplicativité du contenu d'un polynôme à coefficients entiers).
    (b) Montrer que le corps de décomposition du polynôme $X^n - 1$ est égal à l'extension $L = \mathbb{Q}(\zeta)$, où $\zeta = e^{\frac{2i\pi}{n}} \in \mathbb{C}$.
    (c) Montrer que l'extension $\mathbb{Q} \subset L$ est galoisienne.
    (d) Soit $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(L)$. Montrer qu'il existe un entier l premier à n tel que $\sigma(\zeta) = \zeta^l$.
    (e) Construire un homomorphisme de groupes injectif

$$\iota : \mathrm{Gal}_{\mathbb{Q}}(L) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*.$$

    (Remarque : Cet homomorphisme ι est en fait un isomorphisme, ce qui implique Φ_n est le polynôme minimal de ζ. La démonstration de ce résultat est plus difficile).

63. Suite de l'exercice précédent. On admet que $\mathrm{Gal}_{\mathbb{Q}}(L) = (\mathbb{Z}/n\mathbb{Z})^*$. On suppose dans ce exercice que $n = 11$.
   (a) Justifier que $\mathrm{Gal}_{\mathbb{Q}}(L) = \mathbb{Z}/10\mathbb{Z}$.
   (b) Soit c la conjugaison complexe. Justifier que $c \neq \mathrm{Id}$ dans $\mathrm{Gal}_{\mathbb{Q}}(L)$.
   (c) On pose $H = \langle c \rangle \subset \mathrm{Gal}_{\mathbb{Q}}(L)$. Montrer que $\zeta + \overline{\zeta}$ est un générateur du sous-corps L^H de L fixé par H. (Indication : Calculer le polynôme minimal de ζ sur $\mathbb{Q}(\zeta + \overline{\zeta})$)
   (d) Montrer que l'extension $\mathbb{Q} \subset L^H$ est galoisienne et que $\mathrm{Gal}_{\mathbb{Q}}(L^H) = \mathbb{Z}/5\mathbb{Z}$.
   (e) En déduire le polynôme minimal de $\zeta + \overline{\zeta}$ sur $\mathbb{Q}$. (Réponse : $X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$)
   (f) On considère le sous-groupe $H' \subset \mathrm{Gal}_{\mathbb{Q}}(L)$ d'ordre 5. Montrer que H' est engendré par l'automorphisme $\zeta \mapsto \zeta^4$. Trouver un générateur de l'extension $\mathbb{Q} \subset L^{H'}$ ainsi que son polynôme minimal. (Réponse : générateur $\zeta + \zeta^4 + \zeta^5 + \zeta^9 + \zeta^3$, polynôme minimal $X^2 + X + 3$).
64. Soient P, Q deux polynômes séparables dans $K[X]$ sans racine commune dans une clôture algébrique de K. On note L_P,L_Q et L_{PQ} les corps de décomposition des polynômes P,Q et PQ.
   (a) Montrer que l'extension $K \subset L_{PQ}$ est galoisiennne.
   (b) Montrer qu'on a un homomorphisme de groupes
   $$\mathrm{Gal}_K(L_{PQ}) \hookrightarrow \mathrm{Gal}_K(L_P) \times \mathrm{Gal}_K(L_Q)$$
   injectif.
   (c) Etudier le cas particulier $K = \mathbb{Q}$, $P = X^2 + 1$ et $Q = X^4 + 1$.