Exercice* 1. Soit A un anneau commutatif.

(1) Montrer que $(A[X],+,\cdot)$ est un anneau commutatif.

(2) Montrer que l'application

$$\begin{array}{ccc} A & \to & A[X] \\ a & \mapsto & a = aX^0 \end{array}$$

est un homomorphisme d'anneaux injectif.

Exercice 2. Montrer que $\mathbb{Z}[\sqrt{2}]$ est formé des nombres de la forme $a+b\sqrt{2}$ où $a,b \in \mathbb{Z}$.

Exercice 3. Soient A un anneau intègre et $f,g \in A[X]$. Montrer que

$$\deg(f+g) \leq \max\{\deg f, \deg g\}, \quad \deg(fg) = \deg f + \deg g.$$

En déduire que $A[X]$ est aussi intègre. Donner un contre-exemple à la seconde égalité avec A pas intègre.

Exercice 4. Soit A un anneau unitaire.

(1) Montrer que, pour tout a,b qui commutent dans A, on a la formule de Newton

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

(2) Dire si le résultat est encore valable lorsque a,b ne commutent pas.

Exercice 5. Soit K un corps. Montrer que l'ensemble des unités (les éléments inversibles) de $K[X]$ noté $\mathscr{U}(K[X])$ est un groupe égal à K^*.

Exercice* 6. Soit K un corps infini.

(1) Soient $T \subset K$ une partie infinie et $f \in K[X]$. Montrer que $f = 0$ si $f_K(b) = 0$ pour tout $b \in T$.

(2) Soient $T_1,\ldots,T_n$ des parties infinies de K et $f \in K[X_1,\ldots,X_n]$. Montrer que $f = 0$ si $f(b_1,\ldots,b_n) = 0$ pour tout $(b_1,\ldots,b_n) \in T_1 \times \cdots \times T_n$.

(3) Notons $A(K^n,K)$ l'anneau des application de K^n dans K. Montrer que l'application $\varphi : K[X_1,\ldots,,X_n] \to A(K^n,K)$ qui envoie $f \in K[X_1,\ldots,X_n]$ sur son application polynomiale associée, est un homomorphisme d'anneaux injectif.

Exercice 7.** Montrer que $\mathbb{Z}[X]$ et $K[X,Y] = K[X][Y]$ ne sont pas principaux.

Exercice 8. Soit K un corps.

(1) Montrer que $\mu_n(K)$ l'ensemble des racines n-ième de l'unité de K est un sous groupe multiplicatif fini de K^* d'ordre $\leq n$.

(2) Montrer que $\mu(K)$ l'ensemble des racines de l'unité de K^* est un sous groupe multiplicatif de K.

Exercice* 9. Soit E un ensemble non vide et A l'ensemble des parties de E. Montrer que A est un anneau commutatif pour les opérations de différence symétrique et d'intersection. Quels sont l'élément neutre et l'unité de A ? Est-ce que A est intègre ?

Exercice 10. Soient K un corps et $P,Q \in K[X]$ tels que $\text{pgcd}(P,Q) = 1$. Utiliser l'algorithme d'Euclide étendu pour montrer qu'il existe $U,V \in K[X]$ tels que $UP+VQ = 1$, $\deg U < \deg Q$ et $\deg V < \deg P$.

Exercice* 11.** Trouver tous les automorphismes de l'anneau $K[X]$, où K est un corps.

Exercice 1. Soit A un anneau commutatif intègre. Rappelons qu'un élément non nul p de A est *premier* s'il n'est pas une unité et si, lorsque p divise un produit d'éléments de A, il divise l'un des termes.

(1) Montrer qu'un élément p est premier si et seulement si $A/(p)$ est intègre.

(2) Montrer que tout élément premier de A est irréductible.

(3) Supposons que A est factoriel. Montrer qu'un élément de A est premier si, et seulement si, il est irréductible.

Exercice 2. Soit $A = \mathbb{Z}[i]$ l'anneau des entiers de Gauss, i. e. les nombres complexes de la forme $z = a + ib$ avec $a, b \in \mathbb{Z}$. Posons $\varphi(z) = a^2 + b^2$.

(1) Montrer que, pour tout z, z' dans A, $z' \neq 0$ on a $\varphi(zz') = \varphi(z)\varphi(z')$, puis que $\varphi(z) \leq \varphi(zz')$.

(2) Déterminer le groupe $U = \mathscr{U}(A)$ des éléments inversibles de A.

Rappelons qu'un stathme euclidien sur un anneau intègre B est $\psi : B^* = B \setminus \{0\} \to \mathbb{N}$ telle que :
— pour tout x, y dans B^*, $x \mid y$ implique $\psi(x) \leq \psi(y)$;
— pour tout $(x, y) \in B \times B^*$, il existe $(q, r) \in B \times B$ tel que $x = qy + r$ avec $r = 0$ ou $\psi(r) < \psi(y)$.

(3) Se convaincre que, si $B = \mathbb{Z}$ alors $\psi(x) = |x|$ définit un stathme euclidien, puis que $\psi(p) = \deg(p)$ définit un stathme euclidien sur l'anneau de polynômes $\mathbb{K}[X]$, lorsque $\mathbb{K}$ est un corps.

(4) Soit $w = u + iv \in \mathbb{Q}[i]$, donc avec $u, v \in \mathbb{Q}$. Montrer qu'il existe $n, m \in \mathbb{Z}$ tels que :

$$|u - m| \leq 1/2, \qquad |v - n| \leq 1/2.$$

(5) Déduire de la question précédente que φ est un stathme euclidien sur A.

(6) Soit p un premier naturel. Montrer l'équivalence des conditions suivantes :

a) p n'est pas irréductible dans A ;

b) il existe $z \in A$ tel que $p = \varphi(z)$;

c) il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.

(7) Dire si 2, 3, 5 sont irréductibles dans A. Déterminer le pgcd dans A de $15 + 12i$ et $3 - 9i$.

Exercice* 3. Soit A un anneau intègre. Montrer qu'il existe un corps $\mathbb{K}$, unique à isomorphisme près, tel que A s'identifie à un sous anneau de $\mathbb{K}$ et tel que pour tout $x \in \mathbb{K}$ il existe $a \in A \setminus \{0\}$ tel que $ax \in A$.

Exercice 4. Soit $n \in \mathbb{N}_{\geq 2}$ et $x \in \mathbb{N}$ compris entre 1 et n.

(1) Montrer que $\bar{x} \in A = \mathbb{Z}/n\mathbb{Z}$ engendre A comme groupe additif si et seulement si $\bar{x} \in A$ est inversible dans A et que ceci arrive précisément lorsque $\text{pgcd}(x, n) = 1$.

Définissions l'indicatrice d'Euler $\varphi(n)$ comme le nombre de premiers à n dans $[1, n]$.

(2) Soit $U = \mathscr{U}(A)$ le groupe des unités de A. Montrer que si $n \geq 2$ on a $\varphi(n) = |U|$.

(3) Calculer $\varphi(p)$ pour p premier puis $\varphi(p^\alpha)$ pour $\alpha \in \mathbb{N}$.

(4) Montrer le théorème des restes chinois. En déduire que, si $n, m \geq 2$ sont premiers entre eux alors $\varphi(nm) = \varphi(n)\varphi(m)$.

(5) Pour un entier n décomposé en nombres premiers sous la forme $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec p_i et p_j distincts pour $i \neq j$ et $\alpha_i \in \mathbb{N}_{>0}$, calculer $\varphi(n)$.

Exercice 5. Soient A un anneau intègre et $c : \mathbb{Z} \to A$ l'homomorphisme qui envoie m sur $m \cdot 1_A$.

(1) Montrer qu'il existe $p \in \mathbb{N}$, premier ou nul, tel que $\ker(c) = (p)$.

On appelle p la *caractéristique* de A. Supposons désormais que A soit un corps.

(2) Montrer que A contient un sous corps isomorphe à $\mathbb{Q}$ s'il est de caractéristique 0.

(3) Montrer que A contient un sous corps isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ s'il est de caractéristique $p > 0$.

Exercice* 6. Soient p un nombre premier et $\mathbb{K}$ un corps de caractéristique p. Montrer que l'application (dite de Frobenius) :

$$\begin{array}{rccc} \varphi : & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & x^p \end{array}$$

est un endomorphisme. Montrer que φ est injectif. Montrer que φ est un isomorphisme si $\mathbb{K}$ est fini. Trouver un exemple où φ n'est pas surjectif.

Exercice 7. Montrer que tout homomorphisme injectif $A \to B$ entre anneaux intègres induit un homomorphisme (injectif) entre les corps de fractions associés.

Exercice* 8. Soit A un anneau intègre.

(1) Montrer que, si $A[X]$ est principal, A est principal.

Le *lemme de Krull* affirme que dans un anneau (unitaire) commutatif A, pour tout idéal $I \subsetneq A$ il existe un maximal $M \subsetneq A$ contenant I. On peut le montrer facilement en s'appuyant sur le lemme de Zorn appliqué à l'ensemble des idéaux propres de A contenant I.

(2) Utiliser le lemme de Krull pour montrer que, si $A[X]$ est principal et A n'est pas un corps, alors il existe un corps $\mathbb{K}$ tel que $\mathbb{K}[X]$ soit un corps.

(3) En déduire que $A[X]$ est principal si et seulement si A est un corps.

Exercice** 9. Montrer qu'un anneau principal est factoriel.

Exercice 10. Démontrer que tout automorphisme φ du corps $\mathbb{R}$ est l'identité. Pour le faire :

(1) montrer que φ se restreint à l'identité sur $\mathbb{Q}$;

(2) montrer que, si $a > 0$, alors $\varphi(a) > 0$;

(3) en déduire que φ est strictement croissante ;

(4) montrer que, pour tout $a \in \mathbb{R}$, on a $\{x \in \mathbb{Q} \mid x < a\} = \{x \in \mathbb{Q} \mid x < \varphi(a)\}$. Conclure.

Exercice 1. Soient A un anneau factoriel et K le corps des fractions de A. Soit

$$f = a_0 + a_1X + \cdots + a_nX^n, \quad a_n \neq 0$$

un polynôme à coéfficients dans A. Soit $\alpha = \frac{b}{d} \in K$ une racine de f, où $b, d \in A$ sont premiers entre eux. Montrer que b divise a_0 et d divise a_n.

Exercice 2. Dire quels sont les irréductibles de $\mathbb{C}[X]$ puis de $\mathbb{R}[X]$.

Exercice* 3. Soit $A = \mathbb{Z}[i\sqrt{5}]$.

1. Montrer que A est intègre.
2. Montrer que 9 admet deux factorisations non equivalentes en irréductibles.
3. Montrer que 3 et $2+i\sqrt{5}$ n'ont pas de ppcm et que 9 et $6+3i\sqrt{5}$ n'ont pas de pgcd.

Que peut-on dire de la factorialité de A ?

Exercice* 4. Soit A un anneau commutatif. On dit que $S \subset A$ est une *partie multiplicative* de A si $S \neq \emptyset$ et si pour tous $x, y \in S$, on a $xy \in S$.

1. On définit une relation sur $A \times S$ par $(a,s) \sim (a',s') \Leftrightarrow \exists\, t \in S$ tel que $as't = a'st$. Montrer que $\sim$ est une relation d'équivalence. On note la classe d'équivalence de (a,s) par $\frac{a}{s}$ et l'ensemble des classes d'équivalences par A_S (ou $S^{-1}A$). Montrer que A_S est un anneau (définir la somme et le produit). On l'appelle l'*anneau des fractions* de A, ou la *localisation* de A en S.
2. Supposons S l'ensemble des éléments non nuls de A. Si A est intègre, montrer que A_S est un corps, au fait le corps des fractions de A.
3. Supposons que I est un idéal de A. Montrer que $I_S = \{\frac{a}{s} \mid a \in I, s \in S\}$ est un idéal de A_S.
4. Montrer que $\varphi_S : A \to A_S$ définie par $\varphi_S(a) = \frac{as}{s}$ (pour tout $s \in S$) est un morphisme d'anneaux. Montrer que $\varphi_S(s) \in \mathscr{U}(A_S)$, $\forall s \in S$.
5. Montrer que tout idéal de A_S est de la forme I_S avec I un idéal de A.
6. Soit A un anneau Noethérien. Montrer que A_S est Noethérien.

Exercice 5. On travaille sur $\mathbb{Q}[X]$.

1. Montrer que les polynômes $2X^5 - 15$ et $2X^{10} - 21$ sont irréductibles.
2. Soient $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ sans facteur carré et $n \geq 1$. Montrer que $X^n - a$ est irreductible.
3. Soit p un nombre premier. Montrer que le polynôme $1 + X + X^2 + \cdots + X^{p-1}$ est irreductible.

Exercice 6. Soient L un corps et t un élément d'un corps contenant L. On suppose que t est transcendant sur L et on note K le corps de fractions de $L[t]$. Soit $n \geq 1$. Montrer que le polynôme $X^n - t$ est irreductible dans $K[X]$.

Exercice 7. Montrer que le polynôme $X^5 - 5X^4 - 6X - 1$ est irreductible dans $\mathbb{Q}[X]$.

Exercice 8. Soit K un corps.

1. Montrer que $f \in K[X]$ avec $2 \leq \deg(f) \leq 3$ est irréductible si et seulement si f n'a pas de zéro dans K.
2. Décomposer les polynômes suivants en facteurs irreductibles dans $\mathbb{F}_3[X]$.

$$X^2 + X + 1, \quad X^3 + X + 2, \quad X^4 + X^3 + X + 1.$$

Exercice 9.** Soient A un anneau commutatif.

1. Soit $I \subset A$ un idéal propre. Montrer que $I[X]$ est un idéal de $A[X]$. Montrer que $A[X]/I[X] \simeq (A/I)[X]$. Montrer que, si I est premier, alors $I[X]$ est premier.
2. Soit p un nombre premier. Montrer que $\mathbb{Z}[X]/(p) \simeq \mathbb{F}_p[X]$.
3. Montrer que les idéaux premiers non nuls de $\mathbb{Z}[X]$ sont :
   (a) (p), où $p \in \mathbb{N}$ est un nombre premier ;
   (b) (f), où $f \in \mathbb{Z}[X]$ est un polynôme primitif et irreductible dans $\mathbb{Q}[X]$;
   (c) (p, f), où $p \in \mathbb{N}$ est un nombre premier, $f \in \mathbb{Z}[X]$ et la réduction de f modulo p est un polynôme irreductible de $\mathbb{F}_p[X]$.

Exercice 10. Soient $A = \mathbb{Z}[i\sqrt{3}]$ et K son corps de fractions. Montrer que $X^2 - X + 1$ est primitif et irreductible dans $A[X]$ sans pour autant être irréductible dans $K[X]$. Est-ce que ceci contredit un théorème du cours ?

Exercice* 11. On travaille sur $\mathbb{Q}$.

1. Soit $P \in \mathbb{Q}[X]$ irréductible. Montrer que P n'a que des racines simples sur $\mathbb{C}$.
2. Soit $P \in \mathbb{Q}[X]$ un polynôme ayant une racine $\alpha \in \mathbb{C}$ de multiplicité $> \frac{\deg(P)}{2}$. Montrer que $\alpha \in \mathbb{Q}$.
3. Soit $P \in \mathbb{Q}[X]$, $\deg(P) = 2n+1$ avec $n \geq 2$, tel que P admette une racine d'ordre n. Montrer que P admet une racine dans $\mathbb{Q}$.

Exercice 12. Soient $a_1, \ldots, a_n$, n entiers distincts.

1. Prouver que $P(X) = \prod_{i=1}^{n}(X - a_i) - 1$ est irréductible dans $\mathbb{Z}[X]$.
2. Prouver que $P(X) = \prod_{i=1}^{n}(X - a_i)^2 + 1$ est irréductible dans $\mathbb{Z}[X]$.

Exercice 13. Soient K un corps, $\mathscr{P}$ l'ensemble des polynômes unitaires et irréductibles de $K[X]$. Soit $f \in K(X)$. Montrer que f s'écrit de façon unique sous la forme

$$f = g + \sum_{P \in \mathscr{P}} \frac{f_P}{P^{j(P)}}, \qquad \text{avec :}$$

— $g \in K[X]$, $f_P \in K[X]$ pour tout $P \in \mathscr{P}$ et $j(P) = 0$ pour presque tout $P \in \mathscr{P}$,
— $f_P = 0$ si $j(P) = 0$ et f_P et P sont premiers entre eux si $j(P) > 0$,
— $\deg f_P < \deg P^{j(P)}$ si $j(P) > 0$.

Exercice 14. Décomposer en éléments simples les fractions rationnelles suivantes.

(a) $\frac{3}{X^3+1}$ sur $\mathbb{C}$ puis sur $\mathbb{R}$.

(b) $\frac{X^3}{X^3-1}$ sur $\mathbb{R}$.

(c) $\frac{X^2+X+1}{(X-1)^2(X+1)^2}$ sur $\mathbb{R}$.

(d) $\frac{X^7+1}{(X^2+1)(X^2+X+1)}$ sur $\mathbb{R}$.

(e) $\frac{3X^5+2X^4+X^2+3X+2}{X^4+1}$ sur $\mathbb{R}$.

Exercice 15. Soient a et b deux réels distincts et n, m deux entiers strictement positifs. Posons $F = \frac{1}{(X-a)^n(X-b)^m}$. Décomposer F en éléments simples sur $\mathbb{R}$.

Exercice* 16.** Montrer qu'un idéal premier de $\mathbb{C}[X,Y]$ est soit (0), soit (f) avec f polynôme irréductible, soit un maximal de la forme $(X-a, Y-b)$.

Exercice 1. Soient A un anneau et $t_1,\dots,t_n$ des indéterminées en A. Montrer que, pour $1 \le i \le n$, le i-ème polynôme symétrique élémentaire est homogène de degré i en $t_1,\dots,t_n$.

Exercice 2. Exprimer les polynômes suivants comme polynômes en les polynômes symétriques élémentaires :

(a) $(x_1-x_2)^2$;
(b) $x_1^2+x_2^2+x_3^2$;
(c) $x_1^2x_2^2+x_1^2x_3^2+x_2^2x_3^2$;
(d) $(x_1+x_2-x_3-x_4)(x_1+x_3-x_2-x_4)(x_1+x_4-x_2-x_3)$;
(e) $\sum_{i,j,k \text{ distincts}} x_i^2 x_j x_k$.

Exercice 3. Soient $\mathbb{K}$ un corps et $a_0,\dots,a_n$ et $b_0,\dots,b_m$ des indéterminées sur $\mathbb{K}$. Posons :

$$\begin{aligned} A &= \mathbb{K}[a_0,a_1,\dots,a_n,b_0,b_1,\dots,b_m], \\ f &= a_0X^n + a_1X^{n-1} + \cdots + a_n, \\ g &= b_0X^m + b_1X^{m-1} + \cdots + b_m. \end{aligned}$$

Montrer que $\mathrm{Res}(f,g)$ est un polynôme homogène de degré $n+m$ en $a_0,\dots,a_n,b_0,\dots,b_m$.

Exercice 4. Soit $n \ge 1$. Pour $1 \le d \le n$ on pose $S_d = x_1^d + x_2^d + \cdots + x_n^d$. On notera $s_1,\dots,s_n$ les polynômes symétriques élémentaires en $x_1,\dots,x_n$.

(1) Montrer les égalités suivantes (formules de Newton) :

$$\begin{aligned} 0 &= S_1 - s_1 \\ 0 &= S_2 - s_1S_1 + 2s_2 \\ 0 &= S_3 - s_1S_2 + s_2S_1 - 3s_3 \\ &\cdots \\ 0 &= S_d - s_1S_{d-1} + s_2S_{d-2} - \cdots + (-1)^{d-1}s_{d-1}S_1 + (-1)^d d s_d \end{aligned}$$

(2) En déduire que, si $\mathbb{K}$ est un corps de caractéristique 0, tout polynôme symétrique à coefficients dans $\mathbb{K}$ s'écrit de façon unique comme un polynôme en les polynômes de Newton.

Exercice 5. On suppose $x+y+z=1$, $x^2+y^2+z^2=2$ et $x^3+y^3+z^3=3$. Calculer $x^4+y^4+z^4$.

Exercice 6. Montrer que les polynômes $f = XY-1$ et $g = X^2+Y^2-4$ sont premiers entre eux dans $\mathbb{Q}[X,Y]$.

Exercice 7. Soient $\mathbb{K}$ un corps, $M \in \mathrm{GL}_n(\mathbb{K})$ une matrice inversible, et $V \in \mathbb{K}^n$ un vecteur. Montrer que l'unique solution $X = {}^t(x_1,\dots,x_n)$ de l'équation $MX = V$ est donnée par

$$x_i = \frac{\det(M_i)}{\det(M)}, \quad 1 \le i \le n,$$

où M_i est la matrice obtenue à partir de M en remplaçant la i-ème colonne par V.

Exercice 8. On se donne des indéterminées $\alpha_1,\dots,\alpha_n$, $\beta_1,\dots,\beta_m$, u_0,v_0 sur $\mathbb{Z}$, et on pose :

$$\begin{aligned} A &= \mathbb{Z}[\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_m,u_0,v_0] \ ; \\ f &= u_0(X-\alpha_1)\cdots(X-\alpha_n) \in A[X] \ ; \\ g &= v_0(X-\beta_1)\cdots(X-\beta_m) \in A[X]. \end{aligned}$$

Montrer que la partie homogène de plus haut degré en les $\beta_1,\dots,\beta_m$ de $\mathrm{Res}(f,g)$ vaut :

$$u_0^m v_0^n (-1)^{nm} (\beta_1\beta_2\cdots\beta_m)^n.$$

Exercice 9. Soient A un anneau et $f,g \in A[X]$ de degré $n \geq 1$ et $m \geq 1$, respectivement.

(1) Supposons que
$$f = a_0 \prod_{i=1}^{n} (X - \lambda_i).$$
Montrer que
$$\mathrm{Res}(f,g) = a_0^m \prod_{i=1}^{n} g(\lambda_i).$$

(2) Supposons que
$$f = a_0 \prod_{i=1}^{n} (X - \lambda_i) \quad \text{et} \quad g = b_0 \prod_{j=1}^{m} (X - \mu_j).$$
Montrer que
$$\mathrm{Res}(f,g) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\lambda_i - \mu_j).$$

Exercice 10. Soit A un anneau.

(1) Soient $f,g \in A[X]$ des polynômes de degré $n \geq 1$ et $m \geq 1$ respectivement. Montrer que
$$\mathrm{Res}(f,g) = (-1)^{nm} \mathrm{Res}(g,f).$$

(2) Soient $f,g_1,g_2 \in A[X]$ des polynômes non constants. Montrer que
$$\mathrm{Res}(f,g_1 g_2) = \mathrm{Res}(f,g_1)\,\mathrm{Res}(f,g_2).$$

Exercice 11. On identifie l'ensemble des polynômes unitaires de degré n à coefficients dans $\mathbb{R}$ à l'espace $\mathbb{R}^n$ au moyen de la bijection $X^n + a_1 X^{n-1} + \cdots + a_n \mapsto (a_1, \ldots, a_n)$. Moyennant cette identification, on note $\mu : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^{n+m}$ l'application qui aux polynômes unitaires f et g de degrés respectivement n et m fait correspondre leur produit fg. Comparer le déterminant jacobien de μ au point (f,g) avec le résultant $\mathrm{Res}(f,g)$. En déduire le résultat suivant : si f et g sont premiers entre eux, il existe des voisinages U de f dans $\mathbb{R}^n$, V de g dans $\mathbb{R}^m$ et W de fg dans $\mathbb{R}^{n+m}$ tels que μ induise un difféomorphisme de $U \times V$ sur W. En particulier, pour tout h dans W il existe un unique couple (f,g) dans $U \times V$ tel que $h = fg$.

Exercice 12. (1) Calculer le discriminant de $f = X^3 + aX + b$.

(2) Soit f un polynôme unitaire à coefficients réels de degré n. Montrer que, si $\mathrm{Discr}(f) > 0$, alors le nombre de racines réels de f est congru à n modulo 4, et que, si $\mathrm{Discr}(f) < 0$, alors le nombre de racines réelles de f est congru à $n-2$ modulo 4.

(3) Discuter le nombre de racines réelles de $f = X^3 + aX + b$ selon les valeurs de a et b.

Exercice 13. On considère $P(X) = X^4 + 1$

(1) Montrer que P est irréductible sur $\mathbb{Z}$.

(2) Montrer que P est réductible sur un corps de caractéristique 2.

(3) Soit K un corps et $P \in K[X]$ un polynôme de degré $n > 0$. Montrer que P est irréductible sur K SSI P n'a pas de racine dans une extension $\mathscr{K}$ de K de degré au plus $\frac{n}{2}$.

(4) En déduire que P est réductible sur un corps de caractéristique $p > 2$. (On pourra utiliser l'identité suivante : $X^8 - 1 = (X^4 - 1)(X^4 + 1)$.)

Exercice 1. Soient $K \subset L$ une extension de corps et $\alpha \in L$. Montrer que $K(\alpha)$ est l'ensemble des fractions :

$$\frac{f(\alpha)}{g(\alpha)},$$

avec $f, g \in K[X]$ et $g(\alpha) \neq 0$.

Exercice 2. Soit K un corps.

1. Montrer que toute extension de degré fini de K est de type fini.
2. Montrer qu'il existe des extensions de type fini de K qui ne sont pas de degré fini.

Exercice 3. Soient K, E, L trois corps tels que $K \subset E \subset L$.

1. Montrer que $K \subset L$ est une extension de degré fini si et seulement si $K \subset E$ et $E \subset L$ sont des extensions de degré fini.
2. Soit de plus F un corps tel que $K \subset F \subset L$. Montrer que, si $K \subset F$ est une extension de degré fini, alors $E \subset EF$ est une extension de degré fini.
3. Montrer que, si $K \subset E$ et $K \subset F$ sont de degré fini, alors $K \subset EF$ est une extension de degré fini.

Exercice 4. Soit M un corps et K, E, F des sous corps de M tels que $K \subset E \cap F$. Soit $[E : K] = m$ et $[F : K] = n$. Posons $L = EF$.

1. Montrer que $[L : E] \leq n$, $[L : F] \leq m$, $[L : K] \leq mn$.
2. Caractériser le cas $[L : K] = mn$ à l'aide d'une propriété de E par rapport à F.

Exercice 5. Soient E, F, L des corps tels que $E \subset L$ et $F \subset L$. On note $E[F] = F[E]$ le sous anneau de L engendré par $E \cup F$.

1. Montrer que $E[F] = F[E]$ est formé des éléments de L de la forme

   $$a_1 b_1 + \cdots + a_n b_n$$

   avec $a_1, \ldots, a_n \in E$ et $b_1, \ldots, b_n \in F$.
2. Montrer que EF est le corps des fractions de $E[F] = F[E]$.

Exercice 6. Soit $E = \mathbb{Q}(\alpha)$ où α satisfait l'équation

$$\alpha^3 + \alpha^2 + \alpha + 2 = 0.$$

Exprimer $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ et $(\alpha - 1)^{-1}$ sous la forme

$$a\alpha^2 + b\alpha + c$$

avec $a, b, c \in \mathbb{Q}$.

Exercice 7. Soient α, β deux éléments algébriques sur un corps F. Soient f, g les polynômes minimaux de α, β sur F, respectivement. On suppose que les degrés de f et g sont premiers entre eux. Montrer que g est un polynôme irréductible dans $F(\alpha)[X]$.

Exercice 8. Donner les polynômes minimaux sur $\mathbb{Q}$ des éléments de $\mathbb{C}$ suivants : $j\sqrt{2}$, $i + j$, $j + \sqrt{3}$.

Exercice 9. Soit L un corps algébriquement clos.

1. Soit $f \in L[X]$ un polynôme de degré $d \geq 1$. Montrer qu'il existe $\alpha_1, \ldots, \alpha_d \in L$ et $c \in L^*$ tels que

   $$f = c(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_d).$$

2. Montrer que tout polynôme irréductible dans $L[X]$ est de la forme $c(X-\alpha)$ avec $\alpha \in L$ et $c \in L^*$.

Exercice 10. Soient K un corps et $\mathscr{F} = \{f_i\}_{i\in I}$ une famille de polynômes dans $K[X]$.

1. Soient L_1, L_2 deux corps de décomposition de $\mathscr{F}$. Montrer qu'il existe un K-isomorphisme $\sigma : L_1 \to L_2$.
2. Soit K^a une clôture algébrique de K. Montrer qu'il existe un unique corps de décomposition L de $\mathscr{F}$, tel que $L \subset K^a$.

Exercice 11. Montrer qu'un corps fini n'est jamais algébriquement clos.

Exercice 12. Soient K un corps et $\overline{K}$ la clôture algébrique de K. Soient $a, b \in \overline{K} \setminus K$. Établir l'équivalence des deux conditions suivantes :

i) il existe un K-automorphisme φ de $\overline{K}$ tel que $\varphi(a) = b$;

ii) a et b ont le même polynôme minimal $f \in K[X]$.

Exercice 13. Soit $P \in K[X]$ un polynôme de degré $n \geq 1$ et $L \supset K$ son corps de décomposition. Montrer que $[L : K]$ divise $n!$.

Exercice 14. Soit α un nombre réel tel que $\alpha^4 = 5$.

1. Montrer que $\mathbb{Q}(i\alpha^2)$ est une extension normale de $\mathbb{Q}$.
2. Montrer que $\mathbb{Q}(\alpha + i\alpha)$ est une extension normale de $\mathbb{Q}(i\alpha^2)$.
3. Montrer que $\mathbb{Q}(\alpha + i\alpha)$ n'est pas une extension normale de $\mathbb{Q}$.

Exercice 15. Décrire les corps de décomposition des polynômes suivants sur $\mathbb{Q}$ et donner leur degrés.

a) $X^2 - 2$;

b) $X^3 - 2$;

c) $X^2 + X + 1$;

d) $X^6 + X^3 + 1$.

Exercice 16. Déterminer le corps de décomposition de $X^3 + 2X + 1$ sur $\mathbb{F}_3$.

Exercice 17. Soient p un nombre premier, $L = \mathbb{F}_p(Y, Z)$ et $K = \mathbb{F}_p(Y^p, Z^p)$.

1. Montrer que le polynôme $P(X) = (X^p - Y^p)(X^p - Z^p)$ est scindé sur L.
2. En déduire que L est le corps de décomposition de P sur K.
3. On suppose que Q est un polynôme irréductible sur K et que L est un corps de décomposition de Q. Soit $\alpha \in L$ une racine de Q, montrer que $\alpha^p \in K$ et que α est racine de $X^p - \alpha^p$;
4. Déduire que $[L : K] \leq p$.
5. Montrer que $[K(Y) : K] = p$ et $[L : K] = p^2$.
6. Conclure que que L n'est le corps de décomposition d'aucun polynôme irréductible sur K.