Université de Strasbourg
U.F.R. de Mathématiques

Algèbre S6 - 2024/2025

FEUILLE 1

Exercice 1

Soit A un anneau commutatif et soient $a, b \in A$ et $n > 0$ un entier. Montrer

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

Exercice 2

Considérons le groupe additif $(\mathbb{Z}/4\mathbb{Z}, +)$. On suppose que $\cdot$ est une multiplication sur ce groupe qui est commutative, associative, et distributive sur l'addition.

(a) L'élément 2 peut-il être élément neutre de $\cdot$?

(b) Déterminer toutes les structures d'anneau sur $\mathbb{Z}/4\mathbb{Z}$.

Exercice 3

Soit X un ensemble. Soit $\mathbb{R}^X$ l'ensemble de toutes les applications de X dans $\mathbb{R}$, muni des lois $+$ et $\cdot$ induites par celles de $\mathbb{R}$.

(a) Vérifier que $(\mathbb{R}^X, +, \cdot)$ est un anneau.

(b) À quelle condition sur X est-il intègre?

Exercice 4

(a) Montrer que $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{R}$.

(b) Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.

(c) Montrer que $S = \{A \in M_2(\mathbb{Z}) \mid a_{21} = 0\}$ est un sous anneau de $M_2(\mathbb{Z})$.

Exercice 5

On dit qu'un anneau A est un **anneau de Boole** si, pour tout $x \in A$, on a $x^2 = x$. On ne suppose pas ici à priori que A est commutatif, ni qu'il est unitaire.

(a) Vérifier que $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ est un anneau de Boole.

(b) Soit E un ensemble. On note $\mathcal{P}(E)$ l'ensemble des parties de E. Pour $A, B \in \mathcal{P}(E)$ posons

$$A \Delta B := (A \cup B) \setminus (A \cap B) \ .$$

Vérifier que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau unitaire de Boole.

(c) Soit A un anneau de Boole. Montrer que l'on a $x + x = 0$ pour tout $x \in A$.

(d) Montrer que tout anneau de Boole est commutatif.

(e) Soit A un anneau de Boole. Soient x et y des éléments de A. Calculer $xy(x+y)$. En déduire qu'un anneau de Boole ayant au moins trois éléments ne peut pas être intègre.

(f) Soit $P_b(\mathbb{R})$ l'ensemble des parties bornées de $\mathbb{R}$. Montrer que $(P_b(\mathbb{R}), \Delta, \cap)$ est un anneau de Boole non-unitaire.

Exercice 6

Soit A l'ensemble de toutes les matrices de $M_2(\mathbb{Z})$ de la forme

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}.$$

Montrer que A est un sous-anneau de $M_2(\mathbb{Z})$ et que l'application $\varphi : \mathbb{Z}[\sqrt{2}] \to A$ définie par

$$\varphi(a + b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$$

est un isomorphisme.

Exercice 7

Soit $\varphi : A \to A'$ un morphisme d'anneaux commutatifs et soit J un idéal de A.
(a) Montrer que $\varphi(A)$ est un anneau et que $\varphi(J)$ est un idéal de $\varphi(A)$.
(b) Donner un exemple qui montre que $\varphi(J)$ n'est pas nécessairement un idéal de A'.
(c) Montrer que si I est un idéal de A' alors $\varphi^{-1}(I)$ est un idéal de A.

Exercice 8

Soit A un anneau commutatif et $a \in A$. Montrer que $I_a = \{x \in A \mid ax = 0\}$ est un idéal de A.

Exercice 9

Soit A un anneau commutatif et J un idéal de A. Montrer que

$$\sqrt{J} = \{a \in A \mid \exists n \in \mathbb{N} \text{ tel que } a^n \in J\}$$

est un idéal de A.

Exercice 10

Soit A un anneau commutatif.
(a) Un élément a d'un anneau A est appelé nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$. Montrer que l'ensemble $\sqrt{(0)}$ (voir l'exercice 9) des éléments nilpotents est un idéal de A. Cet idéal est appelé le nilradical de A.
(b) Montrer que le nilradical de $A/\sqrt{(0)}$ est trivial (c.-à.-d. il est l'idéal trivial $(\overline{0})$).

Exercice 11

Soit A un anneau commutatif et $a \in A$.
(a) **(Idéal engendré par un élément - idéal principal)** Montrer que

$$(a) := \{ar \mid r \in A\}$$

est un idéal de A. Cet idéal est appelé l'idéal (principal) engendré par a.
(b) Montrer que l'application

$$\varphi : A[X] \to A,\ P \mapsto P(0)$$

est un morphisme surjectif d'anneaux.
(c) Montrer que $Ker(\varphi) = (X)$.

Université de Strasbourg
U.F.R. de Mathématiques

Algèbre S6 - 2024/2025

FEUILLE 2

Exercice 1

Soit B un anneau de Boole unitaire.

(a) Montrer qu'un idéal $I \subset B$ est premier si et seulement si $B/I \cong \mathbb{Z}/2\mathbb{Z}$.

(b) En déduire qu'un idéal $I \subset B$ est premier si et seulement si I est maximal.

(c) Soit S un ensemble. Montrer que l'ensemble $(\mathbb{Z}/2\mathbb{Z})^S := \{f : S \to \mathbb{Z}/2\mathbb{Z}\}$ munis des lois $+$ et $\cdot$ induit par celles de $\mathbb{Z}/2\mathbb{Z}$ est un anneau de Boole unitaire.

(d) Soit S l'ensemble des idéaux premiers de B et soient $P, P' \in S$. Montrer que si $P \neq P'$ alors $P + P' = B$.

(e) Supposons que B est de cardinal fini. En déduire un isomorphisme d'anneaux entre B et $(\mathbb{Z}/2\mathbb{Z})^S$.

Exercice 2

On considère le groupe additif $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Supposons qu'on a une multiplication $\cdot$ sur $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ tel que $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +, \cdot)$ est un anneau commutatif et unitaire A. On nomme ses élements $0, 1, a, b$ (0 est l'élément neutre pour $+$ et 1 est l'élément neutre pour la multiplication).

(a) Montrer que $a + b = 1$.

(b) Supposons que $a^2 = 0$. Montrer qu'alors $ab = a$ et $b^2 = 1$.

(c) Supposons que $a^2 \neq 0 \neq b^2$ mais $ab = 0$. Montrer qu'alors $a^2 = a$ et $b^2 = b$. Montrer que l'anneau obtenue est isomorphe à l'anneau produit $(\mathbb{Z}/2\mathbb{Z}, +, \cdot) \times (\mathbb{Z}/2\mathbb{Z}, +, \cdot)$.

(d) Supposons maintenant que a^2, b^2 et ab sont non-nul. Montrer que $a^2 = b$, $b^2 = a$ et $ab = 1$.

(e) En déduire qu'il existe, à isomorphisme près, (au plus) un corps avec 4 éléments.

Exercice 3 (Morphisme de Frobenius): Soit p un nombre premier.

Montrer que $\varphi : \mathbb{Z}/p\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X],\ P \mapsto P^p$ est un (homo)morphisme d'anneaux.

Exercice 4

Soit $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

(a) Montrer que $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ est un sous-anneau de $\mathbb{R}$.

(b) Considérons l'application

$$N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}\ , \quad a + b\sqrt{2} \mapsto a^2 - 2b^2\ .$$

Montrer que pour tous $x, y \in \mathbb{Z}[\sqrt{2}]$ on a $N(xy) = N(x)N(y)$ et $N(1) = 1$.

(c) En déduire que $x \in \mathbb{Z}[\sqrt{2}]$ est inversible si et seulement si $N(x) = \pm 1$.

(d) Donner un exemple d'un élément inversible qui est différent de ± 1. En déduire que $\mathbb{Z}[\sqrt{2}]^\times$ est un groupe infini.

Exercice 5

(a) Considérons l'anneau $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ et l'application

$$N : \mathbb{Z}[i] \to \mathbb{Z}\ , \quad a + bi \mapsto a^2 + b^2\ .$$

Montrer que pour tous $x, y \in \mathbb{Z}[i]$ on a $N(xy) = N(x)N(y)$ et $N(1) = 1$.

(b) En deduire que $x \in \mathbb{Z}[i]$ est inversible si et seulement si $N(x) = 1$.

(c) Montrer que le groupe $\mathbb{Z}[i]^\times$ est cyclique d'ordre 4.

Exercice 6

Soit A un anneau (commutatif mais pas nécessairement unitaire). On munit $B = A \times \mathbb{Z}$ des lois $(a, m) + (b, n) = (a + b, m + n)$ et $(a, m) \cdot (b, n) = (mb + na + ab, mn)$.

Montrer que B est un anneau commutatif et unitaire.

Exercice 7

Soit $A = \mathbb{Z}/16\mathbb{Z}$.

(a) Montrer que $|A^\times| = 8$.

(b) Montrer que le groupe $A^\times$ est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 8

Dans l'anneau $A = \mathbb{Z}[\sqrt{2}]$ montrer l'égalité des idéaux suivants:

(a) $(3 + \sqrt{2}, 3 - \sqrt{2}) = A$

(b) $(2 + \sqrt{2}, 2 - \sqrt{2}) = (\sqrt{2})$.

Exercice 9

Soit A un anneaux commutatif unitaire et soient I, J deux idéaux de A tel que $I \subset J$.

(a) Montrer que J/I est un idéal de l'anneau A/I.

(b) Montrer que les anneaux A/J et $(A/I)/(J/I)$ sont isomorphes.

Exercice 10

Montrer que l'anneau quotient $\mathbb{Z}[i]/(1 + 3i)$ est isomorphe à $\mathbb{Z}/10\mathbb{Z}$.

Exercice 11

Montrer qu'un anneau intègre qui a une nombre fini d'éléments est un corps.

Exercice 12

Soit K un corps et A un anneau commutative unitaire avec $1 \neq 0$.

(a) Soit $\varphi : K \to A$ un homomorphisme d'anneaux. Montrer que φ est injective.

(b) Montrer que l'application $K \times A \to A, (\lambda, a) \mapsto \varphi(\lambda)a$ et l'addition de A munissent A d'une structure de K-espace vectoriel.

(c) Supposons de plus que A est intègre et de dimension finie en tant que K-espace vectoriel. Montrer que A est un corps.

Université de Strasbourg
U.F.R. de Mathématiques

Algèbre S6 - 2024/2025

FEUILLE 3

Exercice 1

Soit A un anneau commutatif unitaire et soit $I \subset A$ un idéal. Montrer qu'il existe une bijection entre l'ensemble des idéaux de A contenant I et l'ensemble des idéaux de A/I.

Exercice 2

Soit $d \in \mathbb{Z}$ tel que $\sqrt{d} \in \mathbb{C} - \mathbb{Z}$.

(a) Montrer que $\mathbb{Z}[\sqrt{d}] = \{n + \sqrt{d}m \mid n, m \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$.

(b) On définit la conjugaison par

$$\mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}],\ z = n + \sqrt{d}m \mapsto \overline{z} = n - \sqrt{d}m$$

et la <u>norme</u> par

$$N_d : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z},\ z \mapsto z\overline{z}$$

(On utilise la convention que pour $d < 0$ on pose $\sqrt{d} := i\sqrt{-d}$ si $\sqrt{-d}$ est la racine positive de l'entier positive $-d$.)

Montrer que ces deux applications sont multiplicatives:

$$\overline{z_1.z_2} = \overline{z_1}.\overline{z_2}, \quad N_d(z_1 z_2) = N_d(z_1)N_d(z_2)$$

(c) Montrer que $z \in \mathbb{Z}[\sqrt{d}]$ est inversible si et seulement si $N_d(z) = \pm 1$. Déterminer les éléments inversibles de $\mathbb{Z}[\sqrt{-5}]$.

d) Montrer que si $N_d(z) = \pm p$, où p est un nombre premier, alors z est irréductible dans $\mathbb{Z}[\sqrt{d}]$. Donner quelques exemples d'éléments irréductibles dans $\mathbb{Z}[\sqrt{d}]$ pour $d = -1, 2, -6, p$ où p est un nombre premier.

Exercice 3

Soit $A = \mathbb{Z}[i]$.

(a) Soit $z \in \mathbb{C}$. Montrer qu'il existe $q \in A$ tel que $|z - q|^2 \leq \frac{1}{2}$.

(b) Soient $a, b \in A$ et $b \neq 0$, considérons le nombre complexe $\frac{a}{b}$ et choissisons $q \in A$ tel que $|z - q|^2 \leq \frac{1}{2}$. Montrer que $|a - bq|^2 < |b|^2$.

(c) En déduire que l'application

$$N : \mathbb{Z}[i] - \{0\} \to \mathbb{N}, \quad a + bi \mapsto a^2 + b^2$$

muni $\mathbb{Z}[i]$ avec la structure d'un annéau euclidien.

Exercice 4

(a) Rappeler de l'exercice 3 que $\mathbb{Z}[i]$ est euclidien.

(b) Décomposer les deux éléments $11 + 7i$ et $18 - i$ de $\mathbb{Z}[i]$ en facteurs irréductibles et déterminer leur pgcd.

(c) Montrer que si $a, b \in \mathbb{Z}$ sont des entiers tels que a divise b dans $\mathbb{Z}[i]$, alors a divise b déjà dans l'anneau $\mathbb{Z}$.

(d) Déterminer tous les $a + bi \in \mathbb{Z}[i]$ tel que $(a + bi) = (a - bi)$.

Exercice 5

a) Rappeler de l'exercice 3 que $\mathbb{Z}[i]$ est euclidien et factoriel.

b) Expliquer pourquoi les égalités $(2+i)(2-i) = 5 = (-1-2i)(-1+2i)$ ne sont pas en contradiction avec l'unicité de la décomposition en élḿents irréductibles.

c) Calculer le pgcd de $1 - 13i$ et de $4 + i$ et celui de $1 + 7i$ et de $-8 - i$.

Exercice 6

Montrer que $\mathbb{Z}[\sqrt{-2}]$ et $\mathbb{Z}[\rho]$ sont des anneaux euclidiens, où ρ est une sixième racine primitive de l'unité : $\rho^3 = -1$.

Exercice 7

(a) Soit K un corps fini et $K^\times = K - \{0\}$. Montrer

$$\prod_{x \in K^\times} x = -1$$

(b) En déduire le théorème de Wilson: pour tout nombre premier p,

$$(p-1)! \equiv -1 \mod (p) \ .$$

(c) Soit p un nombre premier de la forme $p = 4n + 1$. En déduire que $(\mathbb{Z}/p)^\times$ contient un élément d'ordre 4. En fait

$$(2n)!(2n)! \equiv -1 \mod (p) \ .$$

Université de Strasbourg
U.F.R. de Mathématiques

Algèbre S6 - 2024/2025

FEUILLE 4

Exercice 1 (Les éléments irreductibles dans $\mathbb{Z}[i]$) et les nombres premiers qui sont des sommes de carées)

Rappellons que deux éléments irréductibles a, b dans un anneau commutatif unitaires sont associés s'il existe $u \in A^\times$ tel que $a = bu$. Rapellons encore que $\mathbb{Z}[i]$ et $K[X]$, K un corps, sont des anneaux euclidiens, donc principaux et même factoriels.

Dans cet exercice p est toujours un mombre premier.

(a) Montrer que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si $X^2+\overline{1}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

(b) Utiliser le théorème de Wilson et ses conséquences (voir l'exercice 7 de la feuille 3) pour montrer que $X^2 + \overline{1} \in \mathbb{Z}/p\mathbb{Z}[X]$ n'est pas irréductible si $p \equiv 1 \mod (4)$.

(c) Utiliser le cardinal de $(\mathbb{Z}/p)^\times$ pour montrer que $X^2 + \overline{1}$ est irréductible si $p \equiv 3 \mod (4)$.

(d) En déduire que $p \in \mathbb{Z}[i]$ est irréductible si et seulement si $p \equiv 3 \mod (4)$.

(e) Soit $z \in \mathbb{Z}[i]$. Rappeler que si $N(z)$ est un nombre premier alors z est irréductible. Montrer qu'il existe $a, b \in \mathbb{Z}$ tel que $p = a^2 + b^2$ si et seulement si $p = 2$ ou $p \equiv 1 \mod (4)$.

(f) En déduire: Les éléments irréductibles de $\mathbb{Z}[i]$ sont les éléments $\pm 1 \pm i$, les éléments εp avec p un nombre premier de la forme $4n + 3$ et $\varepsilon \in \{\pm 1, \pm i\}$, et les éléments $\varepsilon(a \pm bi)$ tels que $a^2 + b^2$ est un nombre premier de la forme $4n + 1$.

Exercice 2

Soit A un anneau euclidien qui n'est pas un corps et $s : A - \{0\} \to \mathbb{N}$ sa fonction euclidienne.

(a) Montrer que la fonction s restreint à $A - (A^\times \cup \{0\})$ admet un minimum.

(b) Soit $0 \neq a \in A - A^\times$ tel que $s(a) \leq s(b)$ pour tout $b \in A - (A^\times \cup \{0\})$. Montrer que la restriction de l'application canonique $\pi_{(a)} : A \to A/(a)$ à l'ensemble $A^\times \cup \{0\}$ est surjective.

Exercice 3

Soit α la racine complexe du polynôme $X^2 - X + 5$ de partie imaginaire positive et soit $A \subset \mathbb{C}$ le plus petit sous-anneau de $\mathbb{C}$ qui contient α.

a) Montrer que $A = \{m + n\alpha \mid m, n \in Z\}$.

b) Montrer que les seules unités dans A sont les éléments ± 1.

c) En déduire (en utilisant l'exercice 2) que A n'est pas un anneau euclidien.

d*) Montrer que pour tout $a \in A$ et tout $b \in A - \{0\}$ il existe $q \in A$ et $r \in A$ tel que $|r| < |b|$ ou $r = 0$, et soit $a = bq + r$ soit $2a = bq + r$.

e) Montrer que $(2) \subset A$ est un idéal maximal.

f) Soit I un idéal propre de A et soit $b \in I - \{0\}$ tel que $|b|$ soit minimal. Montrer que $I = (b)$ (et donc que l'anneau A est principal).

Exercice 4

On continue à utiliser les conventions sur les anneaux $\mathbb{Z}[\sqrt{d}]$ de l'exercice 2 de la feuille 3.

a) Montrer que les éléments suivants de l'anneau $\mathbb{Z}[\sqrt{-5}]$ sont irréductibles:

$$3, 2, 1+\sqrt{-5}, 1-\sqrt{-5}\ .$$

b) En déduire que l'anneau $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

c) Répéter les parties a) et b) avec l'anneau $\mathbb{Z}[\sqrt{5}]$ avec les éléments $2, 3+\sqrt{5}, 3-\sqrt{5}$.

Exercice 5

Soit $A = \mathbb{Q}[X]$. Déterminer le pgcd dans A des polynômes suivants:

a) $X^2 - 1$ et $X^3 + 3X^2 + 3X + 1$

b) $X^5 + X^3 + 5X^2 + 5$ et $2X^4 + X^3 + 5X^2 + 5$.

Exercice 6

Soit K un corps et $A = K[X]$.

Décider lesquelles d'anneaux quotients B suivantes de A sont des corps:

a) $K = \mathbb{Q}$ et $B = A/(X^2 + 3)$

b) $K = \mathbb{Q}$ et $B = A/(X^2 - 4)$

c) $K = \mathbb{R}$ et $B = A/(X^2 + 3)$

d) $K = \mathbb{Z}/5\mathbb{Z}$ et $B = A/(X^2 + 3)$

e) $K = \mathbb{Z}/7\mathbb{Z}$ et $B = A/(X^2 + 3)$

f) $K = \mathbb{Z}/3\mathbb{Z}$ et $B = A/(X^3 + X^2 + X + 2)$

g) $K = \mathbb{R}$ et $B = A/(X^3 + X^2 + X + 1)$

h) $K = \mathbb{Q}$ et $B = A/(X^3 + X^2 + X + 1)$

Exercice 7

Rappelons les inclusions

$$\begin{aligned}\{\text{anneaux euclidiens}\} &\subset \{\text{anneaux principaux}\}\\ &\subset \{\text{anneaux factoriels}\} \subset \{\text{anneaux commutatifs unitaires et intègres}\}\ .\end{aligned}$$

Montrer par des exemples que toutes ces inclusions sont strictes.

Université de Strasbourg
U.F.R. de Mathématiques

Algèbre S6 - 2024/2025

FEUILLE 5

Exercice 1
Soit A un anneau commutatif et unitaire et $S \subset A$ une partie multiplicative. Identifier l'anneau quotient $S^{-1}A$ dans les cas suivants:
a) $A = \mathbb{Z}/4\mathbb{Z}$ et $S = \{\overline{2}^n \mid n \in \mathbb{N}\}$
b) $A = \mathbb{Z} \times \mathbb{Z}$ et $S = \{(0,1)^n \mid n \in \mathbb{N}\}$
c) $A = \mathbb{C}[X]$ et $S = \mathbb{C}[X] - \{0\}$

Exercice 2
Soit A un anneau intègre et soit $P \subset A$ un idéal premier.
a) Montrer que $A - P$ est une partie multiplicative de A.
b) Montrer que l'application $\iota_S : A \mapsto S^{-1}A, a \mapsto \frac{a}{1}$ est injective.
c) Montrer que $\{\frac{a}{s} \in S^{-1}A \mid a \in P\}$ est un idéal maximal de $S^{-1}A$.
d) Montrer que l'anneau $S^{-1}A$ ne contient pas d'autres idéaux maximaux.

Exercice 3
Soit p un nombre premier et $(p) \subset \mathbb{Z}$ l'idéal engendré par p, soit $S_1 = \{p^n \mid n \in \mathbb{N}\}$ et $S_2 = \mathbb{Z} - (p)$. L'anneau $S_1^{-1}A$ est souvent désigné $\mathbb{Z}[\frac{1}{p}]$ et l'anneau $S_2^{-1}\mathbb{Z}$ souvent $\mathbb{Z}_{(p)}$.
a) Identifier $\mathbb{Z}[\frac{1}{p}]$ et $\mathbb{Z}_{(p)}$ avec des sous-anneaux concrets de $\mathbb{Q}$.
b) Quels sont les éléments inversibles dans ces deux sous-anneaux?

Exercice 4
Soit $P = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ un polynôme à coefficients dans $\mathbb{Z}$.
a) Supposons que P admet une racine dans $\mathbb{Q}$. Montrer que cette racine est un entier qui divise a_0.
b) Trouver les racines rationnelles des polynômes suivants
i) $X^5 - 2X^4 - 6X^2 + 2X - 4$
ii) $3X^3 - 2X^2 + 6X - 4$
iii) $\frac{16}{3}X^5 - X^3 + X^2 + 2X - 7$

Exercice 5

Soit K un corps et $P \in K[X]$ de degré 3.

a) Montrer: P est irréductible sur K si et sulement si P n'admet pas de racine sur K.

b) En déduire que $X^3 - 5X^2 - 1$ est irréductible sur $\mathbb{Q}$ mais il n'est pas irréductible sur $\mathbb{R}$.

Exercice 6

Déterminer lequels des polynômes suivants sont irréductibles sur $\mathbb{Z}$ resp. $\mathbb{Q}$:

a) $7X^5 + 2X^4 + 4x^3 - 6X^2 + 2$

b) $X^n - p$ si p est un nombre premier

c) $2X^2 + 6X + 2$

d) $X^4 + 1$

e) $X^6 + X^3 + 1$

f) $X^4 + 2X^3 + X^2 + 2X + 1$

Exercice 7

a) Soit K un corps. Montrer que $X^2 + Y^2 - 1$ est irréductible dans $K[X, Y]$ si et seulement si K n'est pas de caractéristique 2

b) Montrer que $X^n + (Y^n - Z^n)$ est irréductible dans $A[X]$ si $A = \mathbb{Z}[Y, Z]$

Exercice 8

Soit $\rho = \frac{1}{2}(1 + \sqrt{3}i)$, soit A le plus petit sous-anneau de $\mathbb{C}$ qui contient ρ et B le plus petit sous-anneau de $\mathbb{C}$ qui contient $\sqrt{3}i$.

a) Montrer que $\{q_1 + q_2\sqrt{3}i \mid q_1, q_2 \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$.

b) Montrer que le corps de fractions de A et de B sont isomorphes à ce sous-corps.

Exercice 9

Soit $\mathbb{C}(X)$ le corps de fractions de $\mathbb{C}[X]$ et soit

$$G = \{f : \mathbb{C} \to \mathbb{Z} \mid f(z) = 0 \text{ sauf pour un nombre fini des nombres complexes}\} .$$

Montrer que G est un groupe abélien et construire un isomorphisme des groupe entre $\mathbb{C}^\times \times G$ et $\mathbb{C}(X)^\times$.

Exercice 10

Soit p un nombre premier impair et soit $x \in \mathbb{F}_p^\times$.

a) Montrer que x est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.

b) En déduire (voir l'exercice 1 de la feuille 4): -1 est un carré modulo p si est seulement si p est congrue à 1 modulo 4.

Université de Strasbourg
U.F.R. de Mathématiques

Algèbre S6 - 2024/2025

FEUILLE 6

Exercice 1
Calculer le polynômes minimaux des nombres complexes suivants par rapport à l'extension $\mathbb{Q} \subset \mathbb{C}$ et dans les cas b) et c) aussi par rapport à l'extension $\mathbb{Q}[i] \subset \mathbb{C}$.
a) $\sqrt{2} + \sqrt{7}$
b) $i + \sqrt{5}$
c) $i + \sqrt{3} + \sqrt{7}$

Exercice 2
Déterminer $[K : \mathbb{Q}]$ si K est le corps de décomposition des polynômes suivants:
a) $X^2 + X + 1$
b) $X^3 - 1$
c) $X^4 + 1$
d) $X^4 + 4$
e) $X^3 + 7$
f) $X^3 - 7$

Exercice 3
Soit $\alpha \in \mathbb{R} - \mathbb{Q}$ une racine du polynôme $P = X^3 - 5 \in \mathbb{Z}[X]$.
a) Montrer que P est irréductible.
b) Soit $\alpha \in \mathbb{C}$ une racine quelconque de P. Montrer que $i \notin \mathbb{Q}(\alpha)$ quelque soit α.
c) Déterminer $[\mathbb{Q}(\alpha)(i) : \mathbb{Q}]$ et $[\mathbb{Q}(\alpha + i) : \mathbb{Q}]$.
d) En déduire $(\mathbb{Q}(\alpha))(i) = \mathbb{Q}(\alpha + i)$.

Exercice 4
Soit K le corps de décomposition de $X^3 - 3 \in \mathbb{Q}[X]$.
a) Déterminer $[K : \mathbb{Q}]$.

b) Déterminer le cardinal du groupe des automorphisme du corps K et identifier la structure de ce groupe.

Exercice 5

Soit K une extension algébrique de $\mathbb{R}$.

a) Supposons que $[K : \mathbb{R}]$ est impair. Si $a \in K$, montrer que l'application

$$m_a : K \to K,\ x \mapsto ax$$

admet une valeur propre réelle. En déduire que $a \in \mathbb{R}$. Conclure que $K = \mathbb{R}$.

b) Montrer que si $[K : \mathbb{R}]$ est un nombre pair, alors $n = 2$ et K est isomorphe au corps $\mathbb{C}$.

c) Conclure que $K = \mathbb{R}$ ou $K = \mathbb{C}$.

Exercice 6

a) Montrer que les polynômes irréductibles de degré 2 de $\mathbb{F}_3[X]$ sont exactement les polynômes $X^2 + 1$, $X^2 + X - 1$ et $X^2 - X - 1$.

b) Construire des isomorphismes entre les corps $\mathbb{F}_3[X]/(X^2+1)$, $\mathbb{F}_3[X]/(X^2+X-1$ et $\mathbb{F}_3[X]/(X^2-X-1)$.

Exercice 7

Soit p un nombre premier impair, soit K le corps de rupture du polynôme $X^4 + 1 \in \mathbb{F}_p[X]$ et soit $a \in K$ tel que $a^4 = -1$.

a) Soit $b = a + a^{-1}$. Montrer que $b^2 = 2$.

b) Montrer que $b \in \mathbb{F}_p$ si et seulement si $b^p = b$.

c) En déduire que 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod (8)$.

Exercice 8*

Soient p un nombre premier, $n > 0$ un entier et soit K_n un corps fini avec $[K_n : \mathbb{F}_p] = n!$.

a) Montrer que pour tout n il existe un homomorphisme injective de corps $i_n : K_n \to K_{n+1}$.

b) Posons $E_n = K_n - i_{n-1}(K_{n-1})$ et $L_n = \mathbb{F}_p \bigcup (\bigcup_{i=2}^{n} E_n)$. Montrer que L_n admet une structure de corps et que L_n est isomorphe à K_n.

c) Montrer que $L := \mathbb{F}_p \cup (\bigcup_{i\geq 2} E_n)$ admet la structure d'un corps et que ce corps est une clôture algébrique de $\mathbb{F}_p$.

Exercice 9

a) Trouver des polynômes $P_i \in \mathbb{F}_2[X]$ de degré i qui sont irréductibles pour $i = 4, 5$.

b) Déterminer un générateur du groupe $(\mathbb{F}_2[X]/(P_i))^\times$.

Exercice 10

Determiner les polynômes cyclotomiques Φ_4, Φ_6, Φ_8.

Exercice 11

Soit p un nombre premier et Φ_n le n-ième polynôme cyclotomique.

a) Trouver n minimal et un p telle que la réduction modulo p de Φ_n n'est pas irréductible.

b*) Montrer que la réduction de Φ_8 n'est pas irréductible modulo tout premier p.