Feuille de TD n° 2
Corps, extensions de corps, corps finis

Extensions de corps, éléments algébriques

Exercice 1

(1) Montrer que les nombres suivants sont algébriques sur $\mathbb{Q}$ et donner leur polynôme minimal :

$$\sqrt{2}, \qquad \sqrt{4+2\sqrt{2}}, \qquad \sqrt[3]{2}$$

(2) Même question sur $\mathbb{Q}(\sqrt{2})$.

(3) On note $j = e^{\frac{2i\pi}{3}}$. Montrer que les nombres suivants sont algébriques sur $\mathbb{Q}$ et donner leur polynôme minimal :

$$j\sqrt{2}, \qquad \sqrt{2}+\sqrt{3}, \qquad i+\sqrt{2}, \qquad j+\sqrt{3}, \qquad i+j.$$

Exercice 2

Un corps fini peut-il être algébriquement clos ?

Exercice 3

Le corps des fractions $\mathbb{R}(t)$ de $\mathbb{R}[t]$ est une extension (infinie) de $\mathbb{Q}$.

(1) Donner un élément algébrique sur $\mathbb{Q}$ dans $\mathbb{R}(t) \setminus \mathbb{Q}$.

(2) Donner un élément non algébrique sur $\mathbb{Q}$ de $\mathbb{R}(t)$.

Exercice 4

Le corps $\mathbb{C}(X)$ est-il algébriquement clos ?

Exercice 5

Théorème fondamental de l'algèbre (d'Alembert-Gauss) : $\mathbb{C}$ est algébriquement clos.

(1) Montrer qu'il suffit de démontrer que tout polynôme de degré supérieur à 1 à coefficients *réels* admet une racine dans $\mathbb{C}$.

(2) Soit $f = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{R}[x]$ un polynôme de degré $n = 2^k m$ où $k \in \mathbb{N}$ et $m \in \mathbb{Z}$ est impair. Dans la suite, on va montrer par récurrence sur k que f a une racine dans $\mathbb{C}$.

(3) Si $k = 0$, montrer que f a une racine dans $\mathbb{R}$. À partir de maintenant, on suppose que $k \geq 1$.

(4) Supposons que tout polynôme à coefficients réels de degré $2^r \cdot m$ avec m un entier impair et $r \in \{0, 1, \ldots, k-1\}$ admet une racine dans $\mathbb{C}$. Soit F un corps de décomposition de f sur $\mathbb{C}$, alors f se décompose comme $f = a(x-z_1)\cdot\cdots\cdot(x-z_n)$ avec $a = a_n$ et $z_i \in F$. On veut montrer que un des z_i est dans $\mathbb{C}$.

(5) Pour tout nombre réel $t \in \mathbb{R}$, on considère le polynôme $q_t(x) = \prod_{1\leq i<j\leq n}(x - z_i - z_j - t z_i z_j) \in F[x]$. Montrer que les coefficients de $q_t(x)$ sont des polynômes réels symétriques en $z_1, \ldots z_n$ (autrement dit ils sont fixés par l'action naturelle du groupe symétrique S_n sur les variables). En déduire que les coefficients sont réels.

(6) Montrer que $deg(q_t(x)) = 2^{k-1}m(n-1)$. En déduire que $q_t(x)$ admet une racine dans $\mathbb{C}$, autrement dit $z_i + z_j + tz_iz_j \in \mathbb{C}$ pour un certain couple (i,j) avec $i < j$.

(7) Montrer qu'il existe deux nombres réels $t \neq s$ tels que $z_i + z_j + tz_iz_j \in \mathbb{C}$ et $z_i + z_j + sz_iz_j \in \mathbb{C}$ pour un même couple (i,j). En déduire que $z_i + z_j$ et z_iz_j sont dans $\mathbb{C}$.

(8) Conclure que $z_i \in \mathbb{C}$.

Exercice 6

(1) Montrer que $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

(2) Montrer que les seules extensions finies du corps $\mathbb{R}$ sont $\mathbb{R}$ et $\mathbb{C}$ (à isomorphisme près).

(3) Montrer que le corps $\mathbb{C}$ n'a pas d'extension finie non triviale.

(4) Montrer que $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$.

Corps de rupture, corps de décomposition

Exercice 7

Trouver un corps de rupture et un corps de décomposition de chacun des polynômes suivants.

$$x^2 - 3 \in \mathbb{Q}[x];\ x^3 - 2 \in \mathbb{Q}[x];\ x^4 + x + 1 \in \mathbb{F}_2[x];\ x^p - t \in \mathbb{F}_p(t)[x].$$

Exercice 8

Soient p un nombre premier et m un nombre entier premier avec p. On considère le polynôme $P = X^p - X + m$.

(1) Montrer que P n'a pas de racines dans $\mathbb{F}_p$.

(2) Soit α une racine de P dans une clôture algébrique de $\mathbb{F}_p$.

(a) Montrer que pour tout $k \in \mathbb{F}_p$, $\alpha + k$ est une racine de P.

(b) En déduire que $L = \mathbb{F}_p(\alpha)$ est un corps de décomposition de P.

(c) Montrer que P est irréductible sur $\mathbb{F}_p$.

(3) Montrer que $X^p - X + m$ est irréductible sur $\mathbb{Z}$.

Corps finis

Exercice 9

Montrer que les anneaux $\mathbb{Z}/p^r\mathbb{Z}$ et $\mathbb{F}_{p^r}$ ne sont pas isomorphes si $r > 1$.

Exercice 10

Soit $K = \mathbb{F}_{p^r}$ un corps fini. Montrer que pour tout élément $\beta \in K$, il existe un unique élément $\alpha \in K$ tel que $\alpha^p = \beta$.

Exercice 11

Soit $a \in \mathbb{F}_p$. En comptant $\{x^2 | x \in \mathbb{F}_p\}$ et $\{a - y^2 | y \in \mathbb{F}_p\}$, montrer que on peut toujours écrire a comme une somme de deux carrés dans $\mathbb{F}_p$.

Exercice 12

(1) Donner les tables d'addition et de multiplication de $\mathbb{F}_4$.

(2) Donner les tables d'addition et de multiplication de $\mathbb{F}_9$.

Exercice 13

(1) Donner la liste de tous les polynômes irréductibles de $\mathbb{F}_2[x]$ de degré 1,2,3 et 4.

(2) Donner la liste de tous les polynômes irréductibles de $\mathbb{F}_3[x]$ de degré 1,2 et 3.

(3) Factoriser sur $\mathbb{F}_2$ les polynômes suivants :

$$x^5 + x^3 + x + 1; \quad x^6 + x^5 + x^4 + x^3 + 1; \quad x^{10} + x^2 + 1.$$

(4) Factoriser sur $\mathbb{F}_3$ les polynômes suivants :

$$x^3 + x - 2; \quad x^5 - x^4 + 5x^3 + x + 1.$$

(5) Montrer que les polynômes $x^5 + 4x^3 - 7x^2 + 9$ et $9x^4 + 10x^3 + 2x^2 + 17x + 15$ sont irréductibles sur $\mathbb{Z}$.

Exercice 14

Dans cet exercice, on va étudier le corps $\mathbb{F}_{16}$ explicitement.

1. Montrer que $f = X^4 + X + 1 \in \mathbb{F}_2[X]$ est un polynôme irréductible. En déduire que $K = \mathbb{F}_2[X]/(f)$ est une extension de degré 4 de $\mathbb{F}_2$. K^* est alors un groupe abélien d'ordre 15, vérifier que la classe de X dans K, notée par α, est un générateur du groupe K^*. Donner une base de K vu comme un espace vectoriel sur $\mathbb{F}_2$. Exprimer α^8 comme une combinaison linéaire de cette base.
2. Soit ϕ un automorphisme (de corps) de K. Vérifier que $\phi_{|\mathbb{F}_2} = \mathrm{id}_{\mathbb{F}_2}$, que ϕ est une bijection $\mathbb{F}_2$-linéaire, et que ϕ induit un automorphisme du groupe K^*. Montrer que ϕ est déterminé par l'image de α et que ϕ est de la forme $x \mapsto x^s$ avec s un certain entier strictement positif.
3. Montrer que $\phi(\alpha) \in K$ est une racine de f. En déduire que $\alpha, \alpha^2, \alpha^4, \alpha^8$ sont les quatre racines distinctes de f.
4. Montrer que $g = X^4 + X^3 + 1 \in \mathbb{F}_2[X]$ est aussi irréductible. Noter par β la classe de X dans $L = \mathbb{F}_2[X]/(g)$, montrer que $\beta^{-1} \in L$ est une racine de f. Expliciter un isomorphisme ψ de $K = \mathbb{F}_2(\alpha)$ vers L.
5. Montrer que $h = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$ est aussi irréductible. Noter par γ la classe de X dans $M = \mathbb{F}_2[X]/(h)$. Est-ce que γ est un générateur du groupe cyclique M^* ? Calculer l'ordre de $\gamma \in M^*$. Montrer que $\gamma \mapsto \alpha^3$ induit un morphisme de corps $M \to K$, montrer que c'est un isomorphisme.
6. Trouver tous les polynômes irréductibles unitaires de degré 4 dans $\mathbb{F}_2[X]$. En déduire que tout corps fini ayant 16 éléments est isomorphe à K.

Exercice 15

Automorphismes de $\mathbb{F}_q$ ($q = p^r$ avec p un nombre entier).

1. Montrer que tout automorphisme de $\mathbb{F}_q$ fixe le sous-corps $\mathbb{F}_p$.
2. Soit $g \in \mathbb{F}_p[X]$ un polynôme, soit $\gamma \in \mathbb{F}_q$ une racine de g. Montrer que pour tout $\phi \in \mathrm{Aut}(\mathbb{F}_q)$, $\phi(\gamma)$ est encore une racine de g.
3. On sait que le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique engendré par un certain $\alpha \in \mathbb{F}_q^*$, montrer que $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, en déduire que ϕ est déterminé par $\phi(\alpha)$. En déduire que $|\mathrm{Aut}(\mathbb{F}_q)| \leq r$.
4. Considérons $f = X^q - X \in \mathbb{F}_p[X] \subset \mathbb{F}_q[X]$, montrer que les éléments de $\mathbb{F}_q$ sont les racines de f.
5. Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique engendré par $\alpha \in \mathbb{F}_q^*$, en étudiant l'image de α montrer que tout $\phi \in Aut(\mathbb{F}_q)$ est de la forme $x \mapsto x^s$.
6. Montrer que $\phi \mapsto s$ définit bien un homomorphisme injectif de groupes $\mathrm{Aut}(\mathbb{F}_q) \to (\mathbb{Z}/(q-1)\mathbb{Z})^\times$.
7. Vérifier que l'application de Frobenius définie par $Fr : x \mapsto x^p$ est un élément de $\mathrm{Aut}(\mathbb{F}_q)$. Montrer que le sous-groupe de $\mathrm{Aut}(\mathbb{F}_q)$ engendré par Fr est d'ordre r. En déduire que $\mathrm{Aut}(\mathbb{F}_q) \simeq \mathbb{Z}/r\mathbb{Z}$.