Feuille de TD 4
Corps de décomposition, clôtures algébriques et corps finis

Exercice 1
Soient K un corps et $P \in K[X]$ un polynôme irréductible de degré n. Soit L une extension finie de K de degré m premier avec n. Montrer que P est irréductible dans $L[X]$.

Exercice 2 (∗)
Soit $P \in K[X]$ un polynôme de degré $n \in \mathbb{N}^*$ et L un corps de décomposition de P. Montrer que $[L : K]$ divise $n!$.
Indication : procéder par récurrence forte, en distinguant selon que P est irréductible ou non.

Exercice 3
Soient K un corps et $K(T)$ son corps des fractions rationnelles.

1. Montrer que pour tout $n \in \mathbb{N}^*$, le polynôme $X^n - T \in K(T)[X]$ est irréductible.
2. Montrer que $K(T)$ n'est pas algébriquement clos.
3. Soit L une clôture algébrique de $K(T)$. L'extension $L \supseteq K(T)$ peut-elle être finie ?

Exercice 4

1. Soit $L \supseteq K$ une extension algébrique. Montrer que toute clôture algébrique de L est aussi une clôture algébrique de K.
2. Soit $L \supseteq K$ une extension algébrique telle que tout $P \in K[X] \setminus K$ est scindé dans L. Montrer que L est une clôture algébrique de K.

Exercice 5

1. (∗)Montrer que tout corps algébriquement clos est de cardinalité infinie.
2. Soit K un corps fini. Montrer que l'ensemble des polynômes irréductibles de $K[X]$ est infini.
3. Soit Ω un corps algébriquement clos et K un sous-corps de Ω. Montrer que l'ensemble $E = \{x \in \Omega \mid x \text{ est algébrique sur } K\}$ est un corps et est une clôture algébrique de K.
4. Soit K un corps de cardinalité au plus dénombrable et L une clôture algébrique de K. Montrer que L est dénombrable.
5. Le corps $\bar{\mathbb{Q}}$ est-il algébriquement clos ?
6. Soit $\overline{\mathbb{Q}(T)}$ une clôture algébrique du corps des fractions rationnelles $\mathbb{Q}(T)$. Montrer que $\mathbb{C}$ contient un sous-corps isomorphe à $\overline{\mathbb{Q}(T)}$. Montrer que $\overline{\mathbb{Q}(T)}$ n'est isomorphe ni à $\bar{\mathbb{Q}}$, ni à $\mathbb{C}$.

Exercice 6
Soient K un corps, Ω un corps algébriquement clos, et $\varphi : K \to \Omega$ un morphisme de corps.

1. Soit $L \supseteq K$ une extension finie. Montrer qu'il existe un morphisme de corps $\psi : L \to \Omega$ tel que $\psi|_K = \varphi$.
   Indication : commencer par traiter le cas où l'extension est monogène, *i.e.* il existe $\theta \in L$ tel que $L = K(\theta)$.
2. (∗) Même question dans le cas où l'extension $L \supseteq K$ est algébrique.
   Indication : utiliser l'exercice 2 avec le théorème de Steinitz.

Exercice 7 (Extensions normales)
On considère un corps K, un polynôme $P \in K[X]$ et L un corps de décomposition de P.

1. Soit Ω une clôture algébrique de L. Montrer que pour tout K-morphisme de corps $\varphi : L \to \Omega$, on a $\varphi(L) = L$.

2. On se propose de montrer la propriété suivante : quelque soit $Q \in K[X]$ irréductible, si Q a une racine dans L, alors Q est scindé dans L. On dit dans ce cas que L est une extension *normale* de K.

   (i) Soit $Q \in K[X]$ un polynôme irréductible, ayant une racine β dans L. Soit $\gamma \in \Omega$ une autre racine de Q. Montrer que $K(\beta)$ et $K(\gamma)$ sont isomorphes.

   (ii) Montrer qu'il existe un sous-corps L' de Ω contenant $K(\gamma)$ ainsi qu'un isomorphisme $\psi : L \to L'$ prolongeant l'isomorphisme entre $K(\beta)$ et $K(\gamma)$.
   Indication : utiliser l'exercice précédent.

   (iii) Montrer que $L = L'$. Conclure.

3. Réciproquement, soit L une extension algébrique finie et normale de K.

   (i) Justifier qu'il existe $a_1, \ldots, a_m \in L$ tels que $L = K(a_1, \ldots, a_m)$.

   (ii) Montrer que L est le corps de décomposition du polynôme $\prod_{i=1}^{m} \mathrm{Irr}(a_i, K)$.

Exercice 8
Soient p un nombre premier positif et $P = X^4 + pX - p \in \mathbb{Q}[X]$.

1. Montrer que P est irréductible sur $\mathbb{Q}$.
2. Montrer que P a exactement deux racines simples dans $\mathbb{R}$.
3. Soit $\alpha \in \mathbb{C}$ une racine de P et $L = \mathbb{Q}(\alpha)$ un corps de rupture de P, de sorte que $[L : \mathbb{Q}] = 4$. On se propose de montrer par l'absurde que L n'a pas de sous-corps non triviaux. On suppose qu'il existe un corps K tel que $L \subsetneq K \supsetneq \mathbb{Q}$. Montrer que dans $K[X]$ on a $P = (X^2 + aX + b)(X^2 + cX + d)$, où $a, b, c, d \in K$.
4. Établir que a^2 est racine du polynôme $Q = X^3 + 4pX - p^2 \in \mathbb{Q}[X]$.
5. Montrer que Q n'a pas de racines dans $\mathbb{Q}$.
6. En étudiant les degrés possibles de $\mathrm{Irr}(a^2, \mathbb{Q})$, montrer que Q admet une racine dans $\mathbb{Q}$. Conclure.
7. On se propose maintenant de déterminer le degré $[E : \mathbb{Q}]$ où $E \subseteq \mathbb{C}$ est le corps de décomposition de P. Soient $\alpha_1 \in \mathbb{C}$ et $\alpha_2 \in \mathbb{C}$ deux racines différentes de P et $a = -(\alpha_1 + \alpha_2)$. En reprenant l'argumentation ci-dessus, montrer que a^2 est racine du polynôme $Q = X^3 + 4pX - p^2$.
8. Montrer que $[\mathbb{Q}(a^2) : \mathbb{Q}] = 3$ et $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 4$. En déduire que $[E : \mathbb{Q}] = 24$.

Exercice 9 (*)
Soit K une extension finie de $\mathbb{Q}$. Montrer qu'il n'y a qu'un nombre fini de racines de l'unité dans K.

Exercice 10
Soient $\mathbb{F}_q$ un corps à q éléments et $\mathbb{F}_{q^n}$ une extension de degré n de $\mathbb{F}_q$. Montrer qu'il existe $\alpha \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$.

Exercice 11

1. Déterminer tous les polynômes irréductibles unitaires de degré 2 de $\mathbb{F}_3[X]$.
2. Montrer que $\mathbb{F}_3[X]/(X^2 - X - 1)$ et $\mathbb{F}_3[Y]/(Y^2 + 1)$ sont deux corps isomorphes.
3. On note α, resp. β, la classe de X, resp. Y , dans le quotient. Déterminer l'ordre de α et β dans le groupe multiplicatif $\mathbb{F}_{3^2}^*$.
4. Expliciter un isomorphisme et sa réciproque entre $\mathbb{F}_3(\alpha) \simeq \mathbb{F}_3[X]/(X^2 - X - 1)$ et $\mathbb{F}_3(\beta) \simeq \mathbb{F}_3[Y]/(Y^2 + 1)$.
5. Déterminer tous les générateurs de $\mathbb{F}_3(\alpha)^*$ et de $\mathbb{F}_3(\beta)^*$.

Exercice 12

1. Donner un exemple de construction d'un corps k à 4 éléments, d'un corps K à 8 éléments, d'un corps L à 16 éléments.
2. Existe-t-il un plongement du corps k dans le corps L? Si oui, en donner un.
3. Existe-t-il un plongement du corps K dans le corps L? Si oui, en donner un.

4. Combien existe-il de tels plongements?
5. Combien le corps L contient-il de sous-corps à 4 éléments?
6. Soit γ le morphisme d'anneaux de $\mathbb{Z}[X]$ dans $\mathbb{F}_2[X]$ défini par

$$\gamma\Big(\sum_{i=0}^{m} a_i X^i\Big) = \sum_{i=0}^{m} \bar{a}_i X^i.$$

   (i) Quelle est la décomposition de $\gamma(\Phi_{15})$ en produit d'éléments irréductibles de $\mathbb{F}_2[X]$?
   (ii) Combien le polynôme $\gamma(\Phi_{15})$ possède-t-il de racines dans L?
   (iii) Montrer que les générateurs du groupe L^* sont exactement les racines de $\gamma(\Phi_{15})$ dans L.

Exercice 13

1. Quel est le nombre de polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_7$? de degré 4 sur $\mathbb{F}_3$?
2. Donner une construction du corps $\mathbb{F}_{5^2}$.
3. Donner un élément d'ordre 8 dans $\mathbb{F}_{5^2}^*$.
4. Quel est le corps de décomposition de X^4+1 sur $\mathbb{F}_5$?
5. Quel est le corps de décomposition de X^3-2 sur $\mathbb{F}_5$? $\mathbb{F}_7$?
6. Le polynôme X^4-2 est-il irréductible sur $\mathbb{F}_5$? sur $\mathbb{F}_{5^2}$?

Exercice 14
Soit p un nombre premier et soit $m, n \in \mathbb{N}^*$. On note $q = p^m$.

1. Montrer que $p^m - 1$ divise $p^{mn} - 1$. En déduire que $X^{p^m-1} - 1$ divise $X^{p^{mn}-1} - 1$.
2. En déduire que le corps fini $\mathbb{F}_{p^{mn}}$ admet un unique sous-corps à p^m éléments et que $[\mathbb{F}_{p^{mn}} : \mathbb{F}_{p^m}] = n$.
3. En déduire que tout corps intermédiaire $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$ est un corps à q^d éléments où d est un diviseur de n et que, pour chaque diviseur d de n, il existe un unique corps intermédiaire de cardinal q^d.
4. Donner tous les sous-corps de $\mathbb{F}_{2^3}$ et $\mathbb{F}_{2^6}$.

Exercice 15
Soit $\mathbb{F}_q$ un corps fini de caractéristique p. On considère un polynôme irréductible $P \in \mathbb{F}_q[X]$ de degré e.

1. Montrer qu'un corps de rupture de P sur $\mathbb{F}_q$ est aussi un corps de décomposition de P sur $\mathbb{F}_q$.
2. Soit $N \in \mathbb{N}^*$. Démontrer que $P | (X^{q^N} - X)$ dans $\mathbb{F}_q$ si et seulement si $e | N$.
3. Soit $\alpha \in \bar{\mathbb{F}}_p$ une racine de P. Montrer que l'ensemble de racines de P est $\{\alpha^{q^\ell} : \ell \in \{0, \dots, e-1\}\}$, de cardinalité e. Retrouver le résultat du premier item.

Exercice 16
Soit $p \in \mathbb{N}^*$ premier et $n \in \mathbb{N}^*$.

1. Démontrer que l'ordre du morphisme de Frobenius σ de $\mathbb{F}_{p^n}$ est n.
2. En utilisant que l'extension $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ est monogène, montrer que son degré est majoré par n.
3. En déduire que le groupe des automorphismes de $\mathbb{F}_{p^n}$ est cyclique d'ordre n, engendré par le morphisme de Frobenius σ.

Exercice 17
Soient p un nombre premier et $n, m \in \mathbb{N}^*$. On note $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ l'automorphisme de Frobenius $x \mapsto x^p$.

1. Montrer que tout polynôme irréductible de $\mathbb{F}_{p^n}[X]$ est à racines simples dans son corps de décomposition.
2. Montrer qu'il y a soit zéro, soit n morphismes de corps de $\mathbb{F}_{p^n}$ dans $\mathbb{F}_{p^m}$.
3. Montrer que l'ensemble des éléments de $\mathbb{F}_{p^n}$ laissés fixes par l'automorphisme σ^ℓ (avec $\ell \in \mathbb{N}^*$) est le sous-corps de $\mathbb{F}_{p^n}$ à p^d éléments avec $d = \mathrm{PGCD}(n, \ell)$.

Exercice 18
Soit $\mathbb{F}_q$ un corps fini de caractéristique p. On considère un polynôme irréductible $P \in \mathbb{F}_q[X]$ de degré $n > 1$.

1. Soit $d > 1$ un diviseur de n. Montrer que $\mathbb{F}_{q^n}$ est un corps de décomposition de P sur $\mathbb{F}_{q^d}$. En déduire que P n'est pas irréductible sur $\mathbb{F}_{q^d}$.

2. Soit Q un facteur irréductible de P dans $\mathbb{F}_{q^d}[X]$. Montrer qu'un corps de rupture de Q sur $\mathbb{F}_{q^d}$ est un corps de décomposition de P sur $\mathbb{F}_q$. En déduire que P est un produit de d facteurs irréductibles de degré n/d dans $\mathbb{F}_{q^d}[X]$.

3. Soit $\ell \in \mathbb{N}^*$. Montrer que P est irréductible sur $\mathbb{F}_{q^\ell}$ si et seulement si ℓ et n sont premiers entre eux.

Exercice 19
Soit $p \in \mathbb{N}^*$ un nombre premier. Pour tout $i \in \mathbb{N}^*$, on choisit un morphisme de corps $f_i : \mathbb{F}_{p^{i!}} \to \mathbb{F}_{p^{(i+1)!}}$. On pose alors $K = \cup_{i\in\mathbb{N}^*}\mathbb{F}_{p^{i!}}$ où chaque $\mathbb{F}_{p^{i!}}$ s'identifie à son image par $f_{j-1} \circ \cdots \circ f_i$ dans $\mathbb{F}_{p^{j!}}$ pour tout $j > i$. Montrer que K est une clôture algébrique de $\mathbb{F}_p$.

Exercice 20 (*)
On note $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ la fonction de Möbius, définie de la façon suivante :

(i) $\mu(n) = 0$ s'il existe un premier $p \in \mathbb{N}^*$ tel que $p^2|n$,

(ii) $\mu(n) = (-1)^\ell$ si $n = \prod_{i=1}^{\ell} p_i$, avec $\ell \in \mathbb{N}$ et premiers $p_i \in \mathbb{N}^*$ tels que $p_i \neq p_j$ si $i \neq j$.

Noter que $\mu(1) = 1$.

Soit $M(\mathbb{N}^*, \mathbb{C})$ l'ensemble des applications de $\mathbb{N}^*$ dans $\mathbb{C}$. On définit la somme $(f + g)(n) = f(n) + g(n)$ et le produit

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d),$$

pour tout $n \in \mathbb{N}^*$. Vérifier que $M(\mathbb{N}^*, \mathbb{C})$ est une anneau commutatif dont l'unité est l'application $\delta : \mathbb{N}^* \to \mathbb{C}$ donnée par $\delta(n) = 0$ si $n \neq 1$ et $\delta(1) = 1$. On admettra l'identité suivante, appelée **formule d'inversion de Möbius**: $\mu * \phi_1 = \delta$, où $\phi_1 \in M(\mathbb{N}^*, \mathbb{C})$ est l'application constante de valeur 1.

1. Soit $\exp_q \in M(\mathbb{N}^*, \mathbb{C})$ l'application $n \mapsto q^n$. Montrer que le nombre de polynômes irréductibles unitaires de degré n dans $\mathbb{F}_q[X]$ est égal à $(\mu * \exp_q)(n)/n$

2. Retrouver ainsi le nombre de polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_7$ et de degré 4 sur $\mathbb{F}_3$.

Exercice 21

1. Calculer les polynômes cyclotomiques Φ_{14} et Φ_{15}.

2. Soient p un nombre premier et α un entier naturel non nul. Calculer Φ_p et montrer que $\Phi_{p^\alpha}(X) = \Phi_p(X^{p^{\alpha-1}})$.

Exercice 22 (*)
Soit p la caractéristique du corps fini $\mathbb{F}_q$.

1. Soit $n \in \mathbb{N}^*$ tel que $\mathrm{PGCD}(q, n) = 1$. Montrer que le polynôme cyclotomique Φ_n est irréductible sur $\mathbb{F}_q$ si et seulement si q est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

2. Pour les entiers $n \in \{3, 4, 5, 6, 7, 8, 12\}$, discuter selon les valeurs de q de l'irréductibilité sur $\mathbb{F}_q$ de la réduction modulo p du polynôme cyclotomique Φ_n.

3. Factoriser Φ_{14} sur $\mathbb{F}_2$.

Exercice 23 (*)
Soient p un nombre premier et $n \in \mathbb{N}^*$ tel que $n = p^\alpha m$ avec $\alpha \in \mathbb{N}^*$ et $p \nmid m$. Soit Φ_n le n-ème polynôme cyclotomique.

1. Montrer que dans $\mathbb{F}_p[X]$, on a $\Phi_n = (\Phi_m)^{p^\alpha - 1}$.

2. Montrer que Φ_n est réductible sur $\mathbb{F}_p$ sauf éventuellement si $(p, \alpha) = (2, 1)$.