TD12 : Corps finis, extensions normales

Diego Izquierdo

Les exercices 8 et 12 sont à préparer avant la séance de TD. Nous traiterons les exercices dans l'ordre suivant : 8, 12, 9, 15, 17.

Exercice 0 : Critère d'Eisenstein
Soient A un anneau intègre et $\mathfrak{p}$ un idéal premier de A. Soit $f = X^n + a_{n-1}X^{n-1} + ... + a_0 \in A[X]$ un polynôme unitaire tel que $a_i \in \mathfrak{p}$ pour tout i et $a_0 \notin \mathfrak{p}^2$. Montrer que f est irréductible dans $A[X]$. Dans le cas où A est un anneau factoriel et K le corps des fractions de A, cela montre que f est irréductible dans $K[X]$. En déduire que, si $g \in \mathbb{C}[Y]$ possède une racine simple, alors $X^n + g(Y)$ est irréductible dans $\mathbb{C}[X, Y]$.

Exercice 1 : Groupe additif d'un corps fini
Soient $n \in \mathbb{N}^*$ et p un nombre premier. Quel est le groupe additif $(\mathbb{F}_{p^n}, +)$?

Exercice 2 : Intersections de corps finis
Soient p un nombre premier et n, s, t trois entiers avec $s|n$ et $t|n$. Soient K et L les sous-corps de $\mathbb{F}_{p^n}$ de cardinaux respectifs p^s et p^t. Quel est le cardinal de $K \cap L$?

Exercice 3 : Un isomorphisme
Montrer que les anneaux $\mathbb{F}_3[X]/(X^2 + X + 2)$ et $\mathbb{F}_3[X]/(X^2 + 2X + 2)$ sont isomorphes. Exhiber un isomorphisme explicite.

Exercice 4 : Rattrapage 2014
Pour tout entier $n > 0$, on note P_n l'ensemble des polynômes irréductibles de degré n à coefficients dans $\mathbb{F}_q$.

1. Montrer que $X^{q^n} - X = \prod_{m|n} \prod_{f \in P_m} f$. En déduire que $q^n = \sum_{m|n} m|P_m|$.

Dans la suite de l'exercice, on choisit $q = 2$.

2. Montrer que $\prod_{f \in P_4} f = \frac{X^{16} - X}{X^4 - X} \in \mathbb{F}_2[X]$.

3. Expliciter tous les éléments de P_4.

4. Déterminer $|P_6|$.

Exercice 5 : Dénombrement de polynômes irréductibles
On définit la fonction $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ par $\mu(1) = 1$, $\mu(p_1...p_r) = (-1)^r$ si $p_1, ..., p_r$ sont des nombres premiers distincts et $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier.

1. Soient f et g deux fonctions de $\mathbb{N}^*$ vers $\mathbb{C}$ telles que :

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} f(d).$$

Montrer la formule d'inversion de Möbius :

$$\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right).$$

2. Soient $m \in \mathbb{N}^*$ et $q \in \mathbb{N}^*$ une puissance d'un nombre premier. Déduire de la question précédente une formule explicite pour le nombre de polynômes irréductibles de degré m à coefficients dans $\mathbb{F}_q$.

Exercice 6 : Partiel 2013

Soient p et q deux nombres premiers distincts, avec p impair. Soit K un corps de décomposition du polynôme séparable $X^p - 1 \in \mathbb{F}_q[X]$ et soit ω une racine primitive p-ième de l'unité dans K. Pour toute partie Z de $\mathbb{Z}/p\mathbb{Z}$, on pose $P_Z(X) = \prod_{i \in Z}(X - \omega^i) \in K[X]$. Pour tout entier r premier à p, on note aussi $rZ \subseteq \mathbb{Z}/p\mathbb{Z}$ l'image de Z par la bijection $z \mapsto rz$ de $\mathbb{Z}/p\mathbb{Z}$.

1. Montrer que $P_Z \in \mathbb{F}_q[X]$ si, et seulement si, $qZ = Z$.

2. Quels sont les degrés des facteurs irréductibles de $X^7 - 1$ dans $\mathbb{F}_2[X]$? Dans $\mathbb{F}_3[X]$? De $X^{17} - 1$ dans $\mathbb{F}_2[X]$?

On pose $Z_p^+ = \{x \in (\mathbb{Z}/p\mathbb{Z})^\times | \exists y \in (\mathbb{Z}/p\mathbb{Z})^\times, x = y^2\}$ et $Z_p^- = (\mathbb{Z}/p\mathbb{Z})^\times \setminus Z_p^+$ et on suppose à partir de maintenant que la classe de q modulo p est dans Z_p^+.

3. Quels sont les cardinaux de Z_p^+ et Z_p^- ?

4. Montrer que $P_{Z_p^\pm} \in \mathbb{F}_q[X]$. En déduire que le polynôme cyclotomique $\phi_p = \frac{X^p-1}{X-1}$ n'est pas irréductible dans $\mathbb{F}_q[X]$.

On suppose à partir de maintenant $q = 2$ et p tel que $2 \in Z_p^+$.

5. On pose $Q^\pm = \sum_{i \in Z_p^\pm} X^i \in \mathbb{F}_2[X]$. Calculer $Q^+(X)^2$ et en déduire $\{Q^+(\omega), Q^-(\omega)\} = \{0, 1\}$.

On suppose à partir de maintenant $Q^+(\omega) = 0$ et $Q^-(\omega) = 1$, ce qu'on peut toujours faire quitte à changer de racine primitive ω.

6. Montrer que $P_{Z_p^\pm} = \phi_p \wedge Q^\pm$.

7. Décomposer le polynôme $X^7 - 1$ en produit de facteurs irréductibles dans $\mathbb{F}_2[X]$. Même question avec le polynôme $X^{17} - 1$.

Exercice 7 : Quand 5 est un carré modulo p ?

Soit p un nombre premier différent de 5. Soit L un corps de décomposition du polynôme $\phi_5 = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_p[X]$.

1. Montrer que L est engendré par une racine de ϕ_5.

2. Montrer que $[L : \mathbb{F}_p]$ est égal à 1 si $p \equiv 1 \mod 5$, 2 si $p \equiv -1 \mod 5$, 4 si $p \equiv \pm 2 \mod 5$.
3. Soient $\zeta \in L$ une racine de ϕ_5 et $\beta = \zeta + \zeta^{-1}$. Montrer que $(2\beta+1)^2 = 5$.
4. Déduire des questions précédentes que 5 est un carré dans $\mathbb{F}_p$ si, et seulement si, $p \equiv \pm 1 \mod 5$.

Exercice 8 : Partiel 2011
Soit K un corps de caractéristique $p > 0$. Soit $a \in K$. Considérons le polynôme $P = X^p - X - a$. Soit L un corps de décomposition.

1. Soit $x \in L$ une racine de P. Montrer que les racines de P sont $x, x + 1, ..., x + p - 1$.
2. Montrer que P est soit scindé soit irréductible.
3. Montrer que, si P n'a pas de racines dans K, alors $[L : K] = p$.

Exercice 9 : Polynômes de la forme $X^{p^k} - X - a$
Soient F un corps de caractéristique $p > 0$ et $k \geq 1$ un entier. On rappelle que, pour tout $a \in F$, le polynôme $X^p - X - a$ est soit irréductible, soit scindé sur F (exercice précédent).

1. Soit $x \in F$ tel que $x^{p^k} - x \in \mathbb{F}_p$. Montrer que F contient un sous-corps contenant x isomorphe à un sous-corps de $\mathbb{F}_{p^{kp}}$.
2. Soient $a \in \mathbb{F}_p$ et $P = X^{p^k} - X - a$. Montrer que, si P est irréductible, alors $p^k | pk$. En déduire pour quelles valeurs de p, k et a le polynôme P est irréductible.
3. Supposons que $k > 1$ et soit $a \in \mathbb{F}_{p^k}$. Montrer que le polynôme $X^{p^k} - X - a \in \mathbb{F}_{p^k}[X]$ n'est pas irréductible.

Exercice 10 : Théorème de Chevalley-Warning
Soit $P \in \mathbb{F}_q[X_1, ..., X_n]$ homogène de degré d avec $0 < d < n$. Soit $V = \{(x_1, ..., x_n) \in \mathbb{F}_q^n | P(x_1, ..., x_n) = 0\}$.

1. Soient $Q = 1 - P^{q-1} \in \mathbb{F}_q$ et $S = \sum_{x \in \mathbb{F}_q^n} Q(x)$. Montrer que $S = |V|$ dans $\mathbb{F}_q$.
2. Montrer que $S = 0$.
3. Déduire de ce qui précède que P admet un zéro non trivial dans $\mathbb{F}_q^n$.
4. Par contre, il existe un polynôme $P \in \mathbb{F}_q[X_1, ..., X_n]$ homogène de degré n dont l'unique zéro dans $\mathbb{F}_q^n$ est $(0, ..., 0)$. Pouvez-vous exhiber un tel polynôme ? Vous pourrez vous aider de la fonction norme $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$.

Exercice 11 : Clôture algébrique d'un corps fini
Soit p un nombre premier. Montrer que $\bigcup_{n=0}^{\infty} \mathbb{F}_{p^{n!}}$ est une clôture algébrique de $\mathbb{F}_p$.

Exercice 12 : Corps de décomposition
Déterminer les corps de décomposition des polynômes suivants de $\mathbb{Q}[X]$, ainsi que leur dimension sur $\mathbb{Q}$:

$$X^2-3, \quad X^3-2, \quad (X^3-2)(X^2-2), \quad X^5-7, \quad X^4+4, \quad X^6+3, \quad X^8+16.$$

Exercice 13 : Sous-corps de $K = \mathbb{Q}(2^{1/3}, \rho)$
Soient $\rho = e^{2i\pi/3} \in \mathbb{C}$ et $K = \mathbb{Q}(2^{1/3}, \rho)$.

1. Déterminer le degré de K sur $\mathbb{Q}$, et exprimer K comme le corps de décomposition d'un polynôme bien choisi.
2. Déterminer tous les sous-corps de K ainsi que leur degré.

Exercice 14 : Degré du corps de décomposition d'un polynôme de degré 3
Soit K un corps. Considérons P un polynôme de degré 3 sur K et L son corps de décomposition.

1. Montrer que $[L : K] \in \{1, 2, 3, 6\}$.
2. Montrer que P est irréductible si, et seulement si, $[L : K] \in \{3, 6\}$.
3. On suppose que K n'est pas de caractéristique 3.
   (a) Exhiber un polynôme $Q \in K[X]$ de la forme $X^3 + pX + q$ dont le corps de décomposition est L.
   (b) Supposons P irréductible. Notons x, y, z les racines de Q dans L, et considérons :
   $$\delta = (x - y)(y - z)(z - x) \in L.$$
   Montrer que $\delta^2 = -4p^3 - 27q^2$. En particulier, $\delta^2 \in K$: on dit que δ^2 est le discriminant de P.
   (c) Montrer que $[L : K] = 3$ si, et seulement si, $\delta \in K$.
4. Calculer $[L : K]$ dans les cas suivants :
   (a) $K = \mathbb{Q}$, $P = X^3 - 3X^2 - 6X - 20$;
   (b) $K = \mathbb{Q}$, $P = X^3 + 3X^2 - 3X - 4$;
   (c) $K = \mathbb{Q}(i)$, $P = X^3 - 6iX^2 - 9X + 3i$;
   (d) $K = \mathbb{R}(T)$, $P = X^3 + (T^2 - 1)X + T^3 - 1$.

Exercice 15 : Extensions normales
Soient $K = \mathbb{Q}(\sqrt{5})$ et $L = \mathbb{Q}(\sqrt{1 + \sqrt{5}})$. Montrer que les extensions $\mathbb{Q} \subseteq K$ et $K \subseteq L$ sont normales, mais que $\mathbb{Q} \subseteq L$ ne l'est pas. Quelle est sa clôture normale dans $\overline{\mathbb{Q}}$?

Exercice 16 : Partiel 2011
Soient K et K' deux sous-corps d'un corps L tels que l'extension $L/K \cap K'$ est algébrique. On suppose que L/K et L/K' sont normales. Montrer que $L/K \cap K'$ est normale.

Exercice 17 : Automorphismes de corps
Déterminer les groupes d'automorphismes suivants :

$$\mathrm{Aut}(\mathbb{C}/\mathbb{R}),\ \mathrm{Aut}(\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}),\ \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}),\ \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{3},j)/\mathbb{Q}),$$

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt[3]{3})/\mathbb{Q}),\ \mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt[3]{3},j)/\mathbb{Q}),\ \mathrm{Aut}(\mathbb{R}/\mathbb{Q}).$$

Exercice 18 : Non fonctorialité de la clôture algébrique
On va considérer les sous-corps suivants de $\mathbb{C}$: $K = \mathbb{Q}(i)$, $L = K(\sqrt{2})$, $M = K(2^{1/4})$ et $\overline{\mathbb{Q}}$ le corps des nombres algébriques sur $\mathbb{Q}$. Soit $f \in \mathrm{Aut}_K(L)$ l'automorphisme qui envoie $\sqrt{2}$ sur son opposé.

1. Montrer qu'il existe un automorphisme de M qui prolonge f, mais qu'il n'existe pas d'automorphisme involutif de M qui prolonge f.

2. Montrer que tout automorphisme de $\overline{\mathbb{Q}}$ laisse M stable.

3. En déduire qu'il n'existe pas d'automorphisme involutif de $\overline{\mathbb{Q}}$ qui prolonge f.

4. Montrer qu'il n'existe pas d'application $\bar{\cdot}$ vérifiant :

(i) à tout corps k est associé un corps $\overline{k}$, algébriquement clos et extension algébrique de k, et un morphisme de corps $k \to \overline{k}$;

(ii) à tout morphisme de corps $f : k \to k'$ est associé un morphisme $\overline{f} : \overline{k} \to \overline{k'}$ tel que le diagramme

$$\begin{array}{ccc} \overline{k} & \xrightarrow{\overline{f}} & \overline{k'} \\ \uparrow & & \uparrow \\ k & \xrightarrow{f} & k' \end{array}$$

commute et tel que, pour tous f, g on ait $\overline{f \circ g} = \overline{f} \circ \overline{g}$.

On dira qu'il n'existe pas de foncteur « clôture algébrique ».

Exercice 19 : Théorème de Lüroth
Soit K un corps.

1. Soit $F \in K(X)\backslash K$. Soient P et Q deux polynômes dans $K[X]$ premiers entre eux tels que $F = P/Q$. Montrer que l'extension $K(X)/K(F)$ est finie. Quel est son degré ?

2. Montrer qu'il existe un isomorphisme entre $\mathrm{Gal}(K(X)/K)$ et $PGL_2(K)$.

Soit maintenant L une extension de K contenue dans $K(X)$. On suppose que $K \neq L$.

3. Montrer que X est algébrique sur L.

4. On note $P = T^n + F_{n-1}T^{n-1} + ... + F_0 \in L[T]$ le polynôme minimal de X sur L. Montrer qu'il existe i tel que $F_i \notin K$.

5. *(Difficile)* Montrer que $L = K(F_i)$.

6. Quelles sont les fractions rationnelles $F \in K(X)$ telles que $F \circ F \circ ... \circ F = X$?

Exercice 20 : Fonctions zêta

Soit A une $\mathbb{Z}$-algèbre de type fini.

1. Soit $\mathfrak{m}$ un idéal maximal de A. Rappeler pourquoi $A/\mathfrak{m}$ est un corps fini.

La fonction zêta de A est alors définie par :

$$\zeta(A, s) = \prod_{\mathfrak{m} \in \mathrm{Max}(A)} \left(1 - \frac{1}{N(\mathfrak{m})}\right)^{-1}$$

où $N(\mathfrak{m}) = |A/\mathfrak{m}|$.

2. Montrer que la fonction zêta de $\mathbb{Z}$ est la fonction zêta de Riemann.

3. Soit $\mathbb{P}$ l'ensemble des nombres premiers. Montrer que :

$$\zeta(A, s) = \prod_{p \in \mathbb{P}} \zeta(A/pA, s).$$

4. Soient $f_1, ..., f_m \in \mathbb{Z}[X_1, ..., X_n]$ et considérons la $\mathbb{Z}$-algèbre :

$$A = \mathbb{Z}[X_1, ..., X_n]/(f_1, ..., f_m).$$

Si $\mathbb{F}$ est un corps fini, on note $V(\mathbb{F})$ l'ensemble des solutions dans $\mathbb{F}^n$ du système $f_1 = ... = f_m = 0$. Montrer que :

$$\zeta(A/pA, s) = \sum_{k \geq 1} |V(\mathbb{F}_{p^k})| \frac{(p^{-s})^k}{k}.$$

5. Calculer la fonction zêta de $\mathbb{Z}[X_1, ..., X_n]$.

6. Prenons $A = \mathbb{Z}[X, Y]/(X^2+Y^2-1)$. Exhiber des fractions rationnelles $F_p \in \mathbb{Q}[X]$ telles que : $\zeta(A, s) = \prod_{p \text{ premier}} F_p(p^{-s})$. En déduire que :

$$\zeta(A, s) = \zeta(s-1) \left(\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{(2n-1)^s} \right).$$