

# 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  $f = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in A[X]$  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  $(\mathbb{F}_{p^n}, +)$  ?

**Indications :** Comme  $\mathbb{F}_{p^n}$  est un  $\mathbb{F}_p$ -espace vectoriel de dimension  $n$ , c'est  $(\mathbb{Z}/p\mathbb{Z})^n$ .

### 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  $K \cap L$  ?

**Indications :** Notons  $\varphi_p : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}, x \mapsto x^p$  le Frobenius. Soit  $G$  le sous-groupe de  $\text{Aut}(\mathbb{F}_{p^n})$  engendré par  $\varphi_p$ . C'est un groupe cyclique d'ordre  $n$ . On remarque que  $K = \mathbb{F}_{p^n}^{\varphi_p^s}$  et  $L = \mathbb{F}_{p^n}^{\varphi_p^t}$ . Donc  $K \cap L = \mathbb{F}_{p^n}^H$  où  $H$  est le sous-groupe de  $G$  engendré par  $\varphi_p^s$  et  $\varphi_p^t$ . On reconnaît immédiatement que  $H$  est engendré par  $\varphi_p^{s \wedge t}$ . Donc  $K \cap L = \mathbb{F}_{p^n}^{\varphi_p^{s \wedge t}}$  est d'ordre  $p^{s \wedge t}$ .

### 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.

**Indications :** Comme les polynômes  $X^2 + X + 2$  et  $X^2 + 2X + 2$  sont irréductibles sur  $\mathbb{F}_3$ , les deux anneaux proposés sont des extensions de degré 2 sur  $\mathbb{F}_3$  : ils sont donc isomorphes à  $\mathbb{F}_9$ . On définit un isomorphisme par :

$$\begin{aligned} \mathbb{F}_3[X]/(X^2 + X + 2) &\rightarrow \mathbb{F}_3[X]/(X^2 + 2X + 2) \\ X &\mapsto -X. \end{aligned}$$

**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  $q^n = \sum_{m|n} m |P_m|$ .

**Indications :** Voir le corollaire 4.5 de la partie III du polycopié d'algèbre 2 de Jan Nekovář : <https://webusers.imj-prg.fr/~jan.nekovar/co/ens/>.

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

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

**Indications :** On sait que  $\prod_{f \in P_1 \cup P_2 \cup P_4} f = X^{16} - X \in \mathbb{F}_2[X]$  et que  $\prod_{f \in P_1 \cup P_2} f = X^4 - X \in \mathbb{F}_2[X]$ . Donc  $\prod_{f \in P_4} f = \frac{X^{16} - X}{X^4 - X} \in \mathbb{F}_2[X]$ .

3. Expliciter tous les éléments de  $P_4$ .

**Indications :** D'après la question précédente,  $|P_4| = 3$ . Soit  $Q \in P_4$  et écrivons  $Q = X^4 + q_3 X^3 + q_2 X^2 + q_1 X + q_0$ . Comme  $Q$  n'a pas de racines, on a forcément  $q_0 = 1$  et  $(q_3, q_2, q_1) \in \{(1, 1, 1), (1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ . Parmi les quatre polynômes ainsi obtenus, on a  $X^4 + X^2 + 1 = (X^2 + X + 1)^2$ . Donc  $P_4$  est constitué des polynômes  $X^4 + X^3 + X^2 + X + 1$ ,  $X^4 + X^3 + 1$  et  $X^4 + X + 1$ .

4. Déterminer  $|P_6|$ .

**Indications :** Comme à la question 1, on a :

$$\prod_{f \in P_6} f = \frac{(X^{64} - X)(X^2 - X)}{(X^8 - X)(X^4 - X)} \in \mathbb{F}_2[X].$$

En comparant les degrés, on a  $6|P_6| = 64 + 2 - 8 - 4$ , donc  $|P_6| = 9$ .

**Exercice 5 : Dénombrement de polynômes irréductibles**

On définit la fonction  $\mu : \mathbb{N}^* \rightarrow \{-1, 0, 1\}$  par  $\mu(1) = 1$ ,  $\mu(p_1 \dots p_r) = (-1)^r$  si  $p_1, \dots, p_r$  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  $\omega$  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  $Z_p^+ = \{x \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \exists y \in (\mathbb{Z}/p\mathbb{Z})^\times, x = y^2\}$  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  $\omega$ .

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  $X^{17} - 1$ .

**Indications :** Voir le corrigé du partiel 2013.

**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  $\phi_5$ .

**Indications :** Si  $\zeta$  est une racine de  $\phi_5$ , alors les autres racines de  $\phi_5$  sont  $\zeta^2, \zeta^3$  et  $\zeta^4$ .

2. Montrer que  $[L : \mathbb{F}_p]$  est égal à 1 si  $p \equiv 1 \pmod{5}$ , 2 si  $p \equiv -1 \pmod{5}$ , 4 si  $p \equiv \pm 2 \pmod{5}$ .

**Indications :** Si  $p \equiv 1 \pmod{5}$ , alors  $(\mathbb{F}_p)^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$  possède un élément d'ordre 5, qui est une racine de  $\phi_5$ . Donc  $[L : \mathbb{F}_p] = 1$  grâce à la question 1.  
 Supposons  $p \equiv -1 \pmod{5}$ . Dans ce cas,  $(\mathbb{F}_p)^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$  ne possède pas d'élément d'ordre 5, donc  $[L : \mathbb{F}_p] \neq 1$ . Par contre,  $\mathbb{F}_{p^2}^\times \cong \mathbb{Z}/(p^2-1)\mathbb{Z}$  possède un élément d'ordre 5. Donc  $\phi_5$  a une racine dans  $\mathbb{F}_{p^2}$ , et  $[L : \mathbb{F}_p] = 2$ .  
 Supposons  $p \equiv \pm 2 \pmod{5}$ . On remarque que  $\mathbb{F}_{p^2}^\times \cong \mathbb{Z}/(p^2-1)\mathbb{Z}$  ne possède pas d'élément d'ordre 5. Donc  $[L : \mathbb{F}_p] > 2$ . Par contre,  $\phi_5$  possède des racines dans  $\mathbb{F}_{p^4}$ . Donc  $[L : \mathbb{F}_p] = 4$ .

3. Soient  $\zeta \in L$  une racine de  $\phi_5$  et  $\beta = \zeta + \zeta^{-1}$ . Montrer que  $(2\beta + 1)^2 = 5$ .

**Indications :** On calcule

$$(2\beta + 1)^2 = 4\beta^2 + 4\beta + 1 = 4\zeta^2 + 4\zeta^{-2} + 8 + 4\zeta + 4\zeta^{-1} + 1 = 4\phi_5(\zeta) + 5 = 5.$$

4. Dédurre des questions précédentes que 5 est un carré dans  $\mathbb{F}_p$  si, et seulement si,  $p \equiv \pm 1 \pmod{5}$ .

**Indications :** Soit  $\varphi_p : L \rightarrow L, x \mapsto x^p$ . On sait que 5 est un carré dans  $L$ . Une de ses deux racines carrées est  $2\beta + 1$ . On remarque que :

$$\varphi_p(\beta) = \zeta^p + \zeta^{-p}.$$

Cette quantité vaut  $\zeta + \zeta^{-1}$  si  $p \equiv \pm 1 \pmod{5}$ ,  $\zeta^2 + \zeta^{-2}$  sinon. On a donc  $\varphi_p(\beta) = \beta$  si, et seulement si,  $p \equiv \pm 1 \pmod{5}$ . Donc  $2\beta + 1 \in \mathbb{F}_p$  si, et seulement si,  $p \equiv \pm 1 \pmod{5}$ , ce qui achève la preuve.

**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  $x, x + 1, \dots, x + p - 1$ .
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  $P \in \mathbb{F}_q[X_1, \dots, X_n]$  homogène de degré  $d$  avec  $0 < d < n$ . Soit  $V = \{(x_1, \dots, x_n) \in \mathbb{F}_q^n | P(x_1, \dots, x_n) = 0\}$ .

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  $\mathbb{F}_q$ .

**Indications :** Pour  $x \in \mathbb{F}_q^n$ , on remarque que  $Q(x) = 0$  si  $P(x) \neq 0$  et  $Q(x) = 1$  si  $P(x) = 0$ .

2. Montrer que  $S = 0$ .

**Indications :** Soit  $\zeta$  un générateur de  $\mathbb{F}_q^\times$ . On considère un monôme  $x_1^{r_1} \dots x_n^{r_n}$  avec  $r_1 + \dots + r_n = d(q-1)$  :

$$\begin{aligned} \sum_{x \in \mathbb{F}_q^n} x_1^{r_1} \dots x_n^{r_n} &= \prod_{i=1}^n \sum_{x \in \mathbb{F}_q} x^{r_i} \\ &= \prod_{i=1, r_i \neq 0}^n \sum_{j=1}^{q-1} \zeta^{jr_i} \times q^{|\{i|r_i=0\}|} \end{aligned}$$

avec la convention  $q^0 = 1$ . Cette quantité vaut 0 s'il existe  $i$  tel que  $q-1$  ne divise pas  $r_i$  ou tel que  $r_i = 0$ . Ces conditions sont forcément satisfaites pour  $r_1 + \dots + r_n = d(q-1)$  puisque  $d < n$ . Donc :

$$\sum_{x \in \mathbb{F}_q^n} x_1^{r_1} \dots x_n^{r_n} = 0.$$

Par linéarité,  $\sum_{x \in \mathbb{F}_q^n} Q(x) = 0$ , et  $S = 0$ .

3. Dédurre de ce qui précède que  $P$  admet un zéro non trivial dans  $\mathbb{F}_q^n$ .

**Indications :** On a  $|V| > 0$  puisque  $P(0, \dots, 0) = 0$ . De plus, avec les deux questions précédentes, si  $p = \text{car}(\mathbb{F}_q)$ , on a  $p||V|$ . Donc  $|V| > 1$ .

4. Par contre, il existe un polynôme  $P \in \mathbb{F}_q[X_1, \dots, X_n]$  homogène de degré  $n$  dont l'unique zéro dans  $\mathbb{F}_q^n$  est  $(0, \dots, 0)$ . Pouvez-vous exhiber un tel polynôme ? Vous pourrez vous aider de la fonction norme  $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ .

**Indications :** Soit  $\omega_1, \dots, \omega_n$  une  $\mathbb{F}_q$ -base de  $\mathbb{F}_{q^n}$ . On remarque immédiatement que :

$$f : \mathbb{F}_q^n \rightarrow \mathbb{F}_q, (x_1, \dots, x_n) \mapsto N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x_1\omega_1 + \dots + x_n\omega_n)$$

est en fait une fonction induite par un polynôme  $P \in \mathbb{F}_q[X_1, \dots, X_n]$  homogène de degré  $n$ . Ce polynôme convient, puisque le seul élément de  $\mathbb{F}_{q^n}$  de norme nulle est 0.

**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  $\mathbb{Q}$  :

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

**Indications :**

- Le corps de décomposition de  $X^2 - 3$  est  $\mathbb{Q}(\sqrt{3})$ . Comme  $\sqrt{3} \notin \mathbb{Q}$ ,  $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ .
- Le corps de décomposition de  $X^3 - 2$  est  $\mathbb{Q}(\sqrt[3]{2}, \rho)$ . Comme  $X^3 - 2$  est irréductible sur  $\mathbb{Q}$ , on a  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ . De plus,  $\rho^2 + \rho + 1 = 0$ , donc  $[\mathbb{Q}(\sqrt[3]{2}, \rho) : \mathbb{Q}(\sqrt[3]{2})] \leq 2$ . Mais  $\rho \notin \mathbb{Q}(\sqrt[3]{2})$ . Donc  $[\mathbb{Q}(\sqrt[3]{2}, \rho) : \mathbb{Q}(\sqrt[3]{2})] = 2$  et  $[\mathbb{Q}(\sqrt[3]{2}, \rho) : \mathbb{Q}] = 6$ .
- Le corps de décomposition de  $(X^3 - 2)(X^2 - 2)$  est  $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}, \rho) = \mathbb{Q}(\sqrt[6]{2}, \rho)$ . En procédant comme dans le point précédent, on a  $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$  et  $[\mathbb{Q}(\sqrt[6]{2}, \rho) : \mathbb{Q}(\sqrt[6]{2})] = 2$ . Donc  $[\mathbb{Q}(\sqrt[6]{2}, \rho) : \mathbb{Q}] = 12$ .
- Le corps de décomposition de  $X^5 - 7$  est  $\mathbb{Q}(\sqrt[5]{7}, \zeta_5)$  où  $\zeta_5$  est une racine primitive 5-ième de l'unité. Le polynôme  $X^5 - 7$  est irréductible par le critère d'Eisenstein. Donc  $[\mathbb{Q}(\sqrt[5]{7}) : \mathbb{Q}] = 5$ . Le polynôme  $\phi_5 = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ , qui annule  $\zeta_5$ , est aussi irréductible (appliquer le critère d'Eisenstein à  $\phi_5(X + 1)$ ). Donc  $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ . On en déduit que  $20 \mid [\mathbb{Q}(\sqrt[5]{7}, \zeta_5) : \mathbb{Q}]$ . Mais  $[\mathbb{Q}(\sqrt[5]{7}, \zeta_5) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{7}, \zeta_5) : \mathbb{Q}(\sqrt[5]{7})][\mathbb{Q}(\sqrt[5]{7}) : \mathbb{Q}] \leq 20$ . Donc  $[\mathbb{Q}(\sqrt[5]{7}, \zeta_5) : \mathbb{Q}] = 20$ .
- Le corps de décomposition de  $X^4 + 4$  est  $\mathbb{Q}(\sqrt{2}\zeta_8, i) = \mathbb{Q}(i)$  où  $\zeta_8 = e^{\frac{i\pi}{4}} = \sqrt{2}(1 + i)$ . On a  $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ .
- Le corps de décomposition de  $X^6 + 3$  est  $\mathbb{Q}(i\sqrt[6]{3}, \zeta_6) = \mathbb{Q}(i\sqrt[6]{3})$  avec  $\zeta_6 = e^{\frac{i\pi}{3}} = \frac{1+i\sqrt{3}}{2}$ . Comme le polynôme  $X^6 - 3$  est irréductible d'après le critère d'Eisenstein,  $[\mathbb{Q}(i\sqrt[6]{3}) : \mathbb{Q}] = 6$ .
- Le corps de décomposition de  $X^8 + 16$  est  $\mathbb{Q}(\zeta_{16}\sqrt{2}, \zeta_8) = \mathbb{Q}(\zeta_{16})$  où  $\zeta_8 = e^{\frac{i\pi}{4}} = \sqrt{2}(1 + i)$  et  $\zeta_{16} = e^{\frac{i\pi}{8}}$ . Le polynôme  $\phi_8 = X^8 + 1$  annule  $\zeta_{16}$  et est irréductible (appliquer le critère d'Eisenstein à  $\phi_8(X + 1)$ ). Donc  $[\mathbb{Q}(\zeta_{16}) : \mathbb{Q}] = 8$ .

**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  $[L : K] \in \{1, 2, 3, 6\}$ .

**Indications :** Soient  $x, y$  et  $z$  les racines de  $P$  dans  $L$ . On suppose sans perte de généralité que  $[K(x) : K] \leq [K(y) : K] \leq [K(z) : K]$ . On a  $L = K(x, y, z) = K(x, y)$ . Si  $P$  est irréductible, on a  $[K(x) : K] = 3$  et  $[K(x, y) : K(x)] \leq 2$ , donc  $[L : K] \in \{3, 6\}$ . Sinon,  $x \in K$ , et donc  $L = K(y)$  est de degré au plus 2 sur  $K$ .

2. Montrer que  $P$  est irréductible si, et seulement si,  $[L : K] \in \{3, 6\}$ .

**Indications :** Voir question 1.

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  $L$ .

**Indications :** Si  $P = X^3 + aX^2 + bX + c$ , il suffit de prendre  $Q(X) = P(X - a/3)$ .

- (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  $\delta^2$  est le discriminant de  $P$ .

**Indications :** Calcul !

- (c) Montrer que  $[L : K] = 3$  si, et seulement si,  $\delta \in K$ .

**Indications :** Notons  $x, y, z$  les racines de  $Q$ . Supposons que  $\Delta \notin (K^\times)^2$ . Alors  $L$  contient  $K(\sqrt{\Delta})$  et  $[K(\sqrt{\Delta}) : K] = 2$ . Donc  $2 \mid [L : K]$ . En utilisant la question 2., on en déduit que  $[L : K] = 6$ .

Réciproquement, supposons maintenant que  $\Delta \in (K^\times)^2$ . Si  $x = y = z$ , le résultat est évident. Supposons alors, sans perte de généralité, que  $x \neq y$  et  $x \neq z$ . On a alors  $(x - y)(x - z)(y - z) \in K$ . Notons  $a = yz$  et  $b = y + z$ . Ce sont des éléments de  $K(x)$ , et on a :

$$(x - y)(x - z) = x^2 - bx + a \in K(x)^\times.$$

Donc  $y - z \in K(x)$ . On en déduit que  $y$  et  $z$  sont dans  $K(x)$ , et donc que  $[L : K] = [K(x) : K] = 3$ .

4. Calculer  $[L : K]$  dans les cas suivants :

- (a)  $K = \mathbb{Q}$ ,  $P = X^3 - 3X^2 - 6X - 20$ ;

**Indications :** On remarque que  $P(5) = 0$ . On factorise  $P = (X - 5)(X^2 + 2X + 4)$ . Le polynôme  $X^2 + 2X + 4$  est irréductible. Donc  $[L : K] = 2$ .

- (b)  $K = \mathbb{Q}$ ,  $P = X^3 + 3X^2 - 3X - 4$ ;

**Indications :** On remarque que  $P(X + 1)$  est un polynôme d'Eisenstein donc  $P$  est irréductible. Soit  $Q = P(X - 1) = X^3 - 6X + 1$ . Le discriminant de  $Q$  vaut  $-4(-6)^3 - 27 = 837$ . Ce n'est pas un carré dans  $\mathbb{Q}$ . Donc  $[L : K] = 6$ .

- (c)  $K = \mathbb{Q}(i)$ ,  $P = X^3 - 6iX^2 - 9X + 3i$ ;

**Indications :** On sait que 3 est irréductible dans  $\mathbb{Z}[i]$ . Le critère d'Eisenstein montre donc que  $P$  est irréductible. Soit  $Q = P(X + 2i) = X^3 + 3X + i$ . Le discriminant de  $Q$  vaut  $-4 \cdot 3^3 - 27 \cdot i^2 = -81$ . C'est un carré dans  $\mathbb{Q}(i)$ . Donc  $[L : K] = 3$ .

- (d)  $K = \mathbb{R}(T)$ ,  $P = X^3 + (T^2 - 1)X + T^3 - 1$ .

**Indications :** Le critère d'Eisenstein montre que  $P$  est irréductible. Son discriminant vaut  $-4(T^2 - 1)^3 - 27(T^3 - 1)^2 = -(T - 1)^2(31T^4 + 62T^3 + 81T^2 + 46T + 23)$ . Comme  $-23$  n'est pas un carré dans  $\mathbb{R}$ , on en déduit que  $[L : K] = 6$ .

### 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.

**Indications :** Voir le corrigé du partiel 2011.

**Exercice 17 : Automorphismes de corps**

Déterminer les groupes d'automorphismes suivants :

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

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

**Exercice 18 : Non functorialité 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  $f \in \text{Aut}_K(L)$  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  $\bar{\phantom{x}}$  vérifiant :
  - (i) à tout corps  $k$  est associé un corps  $\bar{k}$ , algébriquement clos et extension algébrique de  $k$ , et un morphisme de corps  $k \rightarrow \bar{k}$ ;
  - (ii) à tout morphisme de corps  $f : k \rightarrow k'$  est associé un morphisme  $\bar{f} : \bar{k} \rightarrow \bar{k}'$  tel que le diagramme

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

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

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

**Exercice 19 : Théorème de Lüroth**

Soit  $K$  un corps.

1. Soit  $F \in K(X) \setminus K$ . 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 ?

**Indications :** Voir le lemme 6.7 du polycopié d'Algèbre 2 d'Olivier Debarre (<http://www.math.ens.fr/~debarre/>).

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

**Indications :** Voir le théorème 6.8 du polycopié d'Algèbre 2 d'Olivier Debarre (<http://www.math.ens.fr/~debarre/>).

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

**Indications :** Les questions 3, 4, 5 sont le théorème 6.9 du polycopié d'Algèbre 2 d'Olivier Debarre (<http://www.math.ens.fr/~debarre/>).

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

**Indications :** Soit  $F \in K(X)$  telles que  $F \circ F \circ \dots \circ F = X$ . On a alors  $K(F) = K(X)$ . Par conséquent,  $F = \frac{aX+b}{cX+d}$  pour certains  $a, b, c, d \in K$ . La relation  $F^n = F \circ F \circ \dots \circ F = X$  signifie alors que :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^n = Id$$

dans  $PGL_2(K)$ .

**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 :

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

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

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

Si  $\mathbb{F}$  est un corps fini, on note  $V(\mathbb{F})$  l'ensemble des solutions dans  $\mathbb{F}^n$  du système  $f_1 = \dots = f_m = 0$ . 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  $\mathbb{Z}[X_1, \dots, X_n]$ .

**Indications :** Pour les questions 1-5, voir le paragraphe 7.12 de la partie III du polycopié d'algèbre 2 de Jan Nekovář : <https://webusers.imj-prg.fr/~jan.nekovar/co/ens/>.

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 :

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

**Indications :** Voir l'exercice (plus détaillé) 7.13 de la partie III du polycopié d'algèbre 2 de Jan Nekovář : <https://webusers.imj-prg.fr/~jan.nekovar/co/ens/>.