# Feuille de TD 3
# Extension de corps

**Exercice 1**
Soit $a \in \mathbb{C}$ algébrique sur $\mathbb{Q}$ et $P$ le polynôme minimal de $a$ sur $\mathbb{Q}$. On suppose que $a$ est racine d'un polynôme unitaire de $\mathbb{Z}[X]$ (autrement dit, $a$ est un *entier algébrique*). Montrer que $P \in \mathbb{Z}[X]$.

**Exercice 2**
Soient $k$ un corps et $f, g \in k[X,Y]$ deux polynômes premiers entre eux. On note $C_f = \{(x,y) \in k^2 : f(x,y) = 0\}$ et $C_g = \{(x,y) \in k^2 : g(x,y) = 0\}$, de sorte que $C_f$ et $C_g$ sont deux courbes de $k^2$. On va montrer que l'intersection de ces deux courbes est un ensemble de cardinalité finie.

1. Soit $P \in k[X,Y] \simeq k[X][Y] \subseteq k(X)[Y]$. Expliquer comment on peut déduire de la décomposition en produits d'irréductibles de $P$ dans $k[X][Y]$ celle dans $k(X)[Y]$.
2. Montrer que $f$ et $g$ vus comme éléments de $k(X)[Y]$ sont premiers entre eux.
3. Montrer que l'ensemble $A$ des abscisses des points de $C_f \cap C_g$ est de cardinalité finie.
4. En déduire que $C_f \cap C_g$ est un ensemble fini.

**Exercice 3**
Soient $P = X^3 + 2X + 2$ et $a$ une racine de $P$ dans $\mathbb{C}$.

1. Montrer que $P$ est irréductible sur $\mathbb{Q}[X]$. Que vaut $[\mathbb{Q}(a) : \mathbb{Q}]$ ?
2. Exprimer $u = a^{-1}$, $v = a^6 + a^4 + 3a^3 - a^2 + 3$ et $w = (a^2 + a + 1)^{-1}$ en fonction de 1, $a$ et $a^2$.
3. Quel est le polynôme minimal de $v$ sur $\mathbb{Q}$ ?

**Exercice 4**

1. Montrer que $i$ et $j = (-1 + i\sqrt{3})/2$ sont algébriques sur $\mathbb{Q}$ et déterminer $[\mathbb{Q}(i) : \mathbb{Q}]$ et $[\mathbb{Q}(j) : \mathbb{Q}]$.
2. Calculer $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}]$, $[\mathbb{Q}(\sqrt{3}, j) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt{3}, i, j) : \mathbb{Q}]$.
3. Comparer $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt{3} + i) : \mathbb{Q}]$.
4. Déterminer le polynôme minimal de $\sqrt{3} + i$ sur $\mathbb{Q}$.

**Exercice 5**

1. Déterminer $[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}]$ et donner une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt{3}, \sqrt{7})$.
2. Comparer $[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt{3} + \sqrt{7}) : \mathbb{Q}]$.
3. Déterminer le polynôme minimal de $\sqrt{3} + \sqrt{7}$ sur $\mathbb{Q}$.
4. Quelles sont les racines de $\mathrm{Irr}(\sqrt{3} + \sqrt{7}, \mathbb{Q})$ dans $\mathbb{C}$ ?
5. (i) Montrer qu'il existe un automorphisme de corps de $\mathbb{Q}(\sqrt{3})$ qui envoie $\sqrt{3}$ sur $-\sqrt{3}$.
   (ii) Existe-t-il d'autres automorphismes du corps $\mathbb{Q}(\sqrt{3})$ distincts de l'identité ?
6. On note $L = \mathbb{Q}(\sqrt{3}, \sqrt{7})$.
   (i) Montrer qu'il existe des automorphismes $\Phi_3$ et $\Phi_7$ du corps $L$ qui vérifient $\Phi_3(\sqrt{3}) = -\sqrt{3}$ et $\Phi_3(\sqrt{7}) = \sqrt{7}$ d'une part et $\Phi_7(\sqrt{3}) = \sqrt{3}$ et $\Phi_7(\sqrt{7}) = -\sqrt{7}$ d'autre part.
   (ii) Montrer qu'il existe un automorphisme de corps $\Phi_{3,7}$ du corps $L$ qui vérifie $\Phi_{3,7}(\sqrt{3}) = -\sqrt{3}$ et $\Phi_{3,7}(\sqrt{7}) = -\sqrt{7}$.
   (iii) Les automorphismes $\Phi_3$, $\Phi_7$ et $\Phi_{3,7}$ sont-ils les seuls automorphismes du corps $L$ distincts de l'identité ?

**Exercice 6**

1. Les éléments de $\mathbb{Q}(\sqrt{2})$ ont-ils tous le même polynôme minimal sur $\mathbb{Q}$?
2. On considère deux extensions de corps de même degré. Sont-elles nécessairement isomorphes?
3. Soient $a$ et $b$ deux entiers non nuls. Donner une condition nécessaire et suffisante pour que $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ (où par convention $\sqrt{n} = i\sqrt{-n}$ si $n < 0$).

**Exercice 7**

1. Déterminer $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{5}) : \mathbb{Q}]$ et donner une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt[3]{3}, \sqrt{5})$.
2. Comparer $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{5}) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt[3]{3} + \sqrt{5}) : \mathbb{Q}]$.
3. Déterminer le polynôme minimal de $\sqrt[3]{3} + \sqrt{5}$ sur $\mathbb{Q}$.
4. Quelles sont les racines de $\mathrm{Irr}(\sqrt[3]{3} + \sqrt{5}, \mathbb{Q})$ dans $\mathbb{C}$ ?

**Exercice 8**
Soient $L \supseteq K \supseteq k$ une tour d'extension de corps et $a \in L$. Montrer que si $K$ est une extension algébrique de $k$ et $a$ est algébrique sur $K$, alors $a$ est algébrique sur $k$.

**Exercice 9**
Soit $\alpha$ un élément algébrique sur un corps $K$.

1. Quels sont les degrés possibles de l'extension $K(\alpha) \supseteq K(\alpha^2)$ ?
2. Montrer que si $[K(\alpha) : K]$ est impair, alors $K(\alpha^2) = K(\alpha)$. La réciproque est-elle vraie ?

**Exercice 10**
Soient $k$ un corps et $F \in k(X) \setminus k$. On pose $F = A/B$ avec $A, B \in k[X]$ premiers entre eux. On s'intéresse à $k(F)$, le sous-corps de $k(X)$ engendré par $F$.

1. Soit $P(X,T) = B(T)F(X) - A(T) \in k(X)[T]$. Montrer que $P$ définit un élément non nul de $k(F)[T]$, dont une racine est $X$.
2. En déduire que $X$ est algébrique sur $k(F)$, et donc que $F$ est transcendant sur $k$.
3. Montrer que $B(T)U - A(T)$ est un polynôme irréductible de $k[T,U]$, puis que c'est un polynôme irréductible de $k(U)[T]$.
4. En déduire que $P$ est le polynôme minimal de $X$ sur $k(F)$. Quel est le degré de l'extension $k(X) \supseteq k(F)$?

**Exercice 11**
Soient $K$ et $M$ deux corps et $\varphi : K \to M$ un morphisme de corps.

1. Rappeler pourquoi $\varphi$ est injective.
2. Montrer qu'il existe un sur-corps $L \supseteq K$ et un morphisme de corps $\psi : L \to M$ tels que :
   (i) $\psi$ est bijective,
   (ii) $\psi|_K = \varphi$.

**Exercice 12**
Soit $K$ un corps et $L = K(\alpha)$ une extension de $K$ de degré fini engendrée par un élément $\alpha$. Le but de cet exercice est de montrer que $L$ ne contient qu'un nombre fini de sous-corps $F$ tels que $K \subseteq F$.

1. Soit $F$ un sous-corps de $L$ qui contient $K$ et $A$ l'ensemble des coefficients du polynôme minimal $\mathrm{Irr}(\alpha, F)$ de $\alpha$ sur $F$. Montrer que $\mathrm{Irr}(\alpha, K(A)) = \mathrm{Irr}(\alpha, F)$ et en déduire que $K(A) = F$.
2. Montrer que $\mathrm{Irr}(\alpha, F) | \mathrm{Irr}(\alpha, K)$ dans $F[X]$.
3. En déduire une application injective de l'ensemble des sous-corps de $L$ qui contiennent $K$ dans l'ensemble des polynômes unitaires de $L[X]$ qui divisent $\mathrm{Irr}(\alpha, K)$ dans $L[X]$.

4. Montrer que $\mathrm{Irr}(\alpha, K)$ n'admet qu'un nombre fini de diviseurs unitaires dans $L[X]$. Conclure.

5. On considère l'application suivante. On prend $K = \mathbb{Q}$ et $L = \mathbb{Q}(i, \sqrt{2})$.

   (i) Montrer que $L = \mathbb{Q}(i + \sqrt{2})$. Calculer $[L : \mathbb{Q}]$.

   (ii) Quelles sont les racines de $\mathrm{Irr}(i + \sqrt{2}, \mathbb{Q})$ dans $L$?

   (iii) Établir la liste des sous-corps de $L$.

**Exercice 13 (**Dénombrabilité de $\overline{\mathbb{Q}}$**)** 1. On rappelle que $\overline{\mathbb{Q}}$ désigne l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$. Démontrer que $\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.

2. Pour tout $n \in \mathbb{N}$, on note $\mathbb{Q}_n[X]$ l'espace vectoriel des polynômes de $\mathbb{Q}[X]$ de degré inférieur ou égal à $n$. Montrer que $\mathbb{Q}_n[X]$ est dénombrable.

3. Montrer que $\mathbb{Q}[X]$ est dénombrable. En déduire que $\overline{\mathbb{Q}}$ est dénombrable.

4. Montrer que $\mathbb{C}$ contient une infinité non dénombrable d'éléments transcendants sur $\mathbb{Q}$.

**Exercice 14 (**Théorème de l'élément primitif**)**
Soit $K$ un corps de caractéristique 0 et $L$ une extension finie de $K$, engendrée par deux éléments $\alpha$ et $\beta$. On veut prouver qu'il existe un élément $\theta \in L$ tel que $L = K(\theta)$ (on dit que $\theta$ est un *élément primitif* de l'extension).

1. Soient $P_\alpha = \mathrm{Irr}(\alpha, K)$ et $P_\beta = \mathrm{Irr}(\beta, K)$. On considère une extension $M$ de $L$ dans laquelle $P_\alpha$ et $P_\beta$ sont scindés, par exemple une clôture algébrique de $L$. On note $\alpha_1 = \alpha$, $\alpha_2$, …, $\alpha_m$ les racines de $P_\alpha$ dans $M$, et $\beta_1 = \beta$, $\beta_2$, …, $\beta_n$ celles de $P_\beta$.

   (i) Justifier que $K$ est de cardinalité infinie. En déduire qu'il existe $\lambda \in K$ tel que $\lambda \neq (\alpha - \alpha_i)/(\beta - \beta_j)$ pour tout $(i, j)$ avec $1 \leq i \leq m$ et $1 < j \leq n$.

   (ii) On pose $\theta = \alpha - \lambda\beta \in L$ et $Q = \mathrm{Irr}(\beta, K(\theta))$. Montrer que $P_\alpha(\theta + \lambda X)$ est un polynôme non nul de $K(\theta)[X]$ dont $\beta$ est une racine. En déduire que $Q | P_\alpha(\theta + \lambda X)$ et $Q | P_\beta$ dans $K(\theta)[X]$.

   (iii) Montrer que $P_\alpha(\theta + \lambda X)$ et $P_\beta$ sont scindés à racines simples dans $M[X]$, et que $\beta$ est leur seule racine commune.

   (iv) En déduire que $Q = X - \beta$, puis que $L = K(\theta)$.

2. On considère la généralisation suivante. Soit $L$ une extension finie d'un corps $K$ de caractéristique 0. Montrer qu'il existe $\theta \in L$ tel que $L = K(\theta)$.

3. Déterminer un élément primitif des extensions suivantes de $\mathbb{Q}$ :

   (i) $\mathbb{Q}(j, \sqrt[3]{2})$,

   (ii) $\mathbb{Q}(e^{2i\pi/n}, e^{2i\pi/m})$ avec $(m, n) \in (\mathbb{N}^*)^2$,

   (iii) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \sqrt[5]{5})$.

**Exercice 15**

1. Montrer que l'identité est le seul automorphisme de corps de $\mathbb{Q}$. Même question avec $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ où $p$ est un nombre premier.

2. (i) Soit $L$ un corps de caractéristique 0. Montrer que $L$ contient un sous-corps $k$ isomorphe à $\mathbb{Q}$ et que tout automorphisme de corps de $L$ induit l'identité sur $k$.

   (ii) Soit $L$ un corps de caractéristique $p$ où $p$ est un nombre premier. Montrer que $L$ contient un sous-corps $k$ isomorphe à $\mathbb{F}_p$, et que tout automorphisme de corps de $L$ induit l'identité sur $k$.

3. Automorphismes de $\mathbb{R}$.

   (i) Soit $\varphi$ un automorphisme de corps de $\mathbb{R}$. Montrer que $\varphi(\mathbb{R}^+) \subseteq \mathbb{R}^+$ (on pourra réfléchir à une caractérisation algébrique des réels positifs).

   (ii) En déduire que $\varphi$ est croissant (en tant qu'application $\mathbb{R} \to \mathbb{R}$), puis que $\varphi$ est l'identité.

4. Automorphismes continus de $\mathbb{C}$.

   (i) Soit $\varphi$ un automorphisme de corps continu de $\mathbb{C}$. Montrer que $\varphi(x) = x$ pour tout $x \in \mathbb{R}$.

   (ii) En déduire que $\varphi$ est soit l'identité, soit la conjugaison complexe.

5. K-automorphismes de K(X).

   (i) Montrer que tout $K$-automorphisme de $K(X)$ est de la forme

   $$f \mapsto f\left(\frac{aX+b}{cX+d}\right).$$

   *Indication :* utiliser l'exercice 10.

   (ii) En déduire que le groupe des $K$-automorphismes de $K(X)$ est isomorphe à $\mathrm{PGL}(2,K)$.

**Exercice 16**

1. Montrer que le polynôme $P = X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$. Justifier que $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $P$, mais pas un corps de décomposition.
2. Soit $L = \mathbb{Q}(\sqrt[3]{2}, j)$. Montrer que $L$ est le corps des racines de $P$.
3. Déterminer $[L : \mathbb{Q}]$.
4. (i) Quels sont les automorphismes du corps de $\mathbb{Q}(j)$ ?

   (ii) Quels sont les automorphismes du corps de $\mathbb{Q}(\sqrt[3]{2})$?
5. (i) Montrer que pour tout $(m,n) \in \{1,2\} \times \{0,1,2\}$, il existe un automorphisme $\varphi_{m,n}$ de $L$ tel que $\varphi_{m,n}(\sqrt[3]{2}) = j^n \sqrt[3]{2}$ et $\varphi_{m,n}(j) = j^m$.

   (ii) Les automorphismes $\varphi_{m,n}$ sont-ils les seuls automorphismes de corps de $L$?
6. (i) Pour $(m,n) \in \{1,2\} \times \{0,1,2\}$, montrer que $\varphi_{m,n}(\sqrt[3]{2} + j)$ est une racine de $\mathrm{Irr}(\sqrt[3]{2} + j, \mathbb{Q})$.

   (ii) Déterminer le degré de $\mathrm{Irr}(\sqrt[3]{2} + j, \mathbb{Q})$.

**Exercice 17**

Soient $p$ un entier premier et $P = X^p - X - 1$ un polynôme de $\mathbb{Z}[X]$.

1. Soient $\overline{P}$ la classe d'équivalence de $P$ dans $\mathbb{F}_p[X]$ et $L$ un corps de rupture de $\overline{P}$ avec $a$ une racine de $\overline{P}$ dans $L$. Montrer que l'ensemble des racines de $\overline{P}$ dans $L$ est $\{a + i \,(\mathrm{mod}\, p) : 0 \leq i \leq p-1\}$.
2. En déduire que $\overline{P}$ est irréductible sur $\mathbb{F}_p[X]$ et donc sur $\mathbb{Z}[X]$ et sur $\mathbb{Q}[X]$.