TD6 : Extensions de corps ; corps finis

Diego Izquierdo

Nous avons traité les exercices 3, 7, 9, 11, 13, 25 et 15 pendant la séance. J'ai mis un corrigé partiel de l'exercice 24 du TD5, puisque nous ne l'avons finalement pas traité pendant le séance...

Exercice 24 du TD5 : Quelques calculs explicites

1. Déterminer le polynôme minimal de $\sqrt{2}+\sqrt{3}$ sur $\mathbb{Q}$.
2. Déterminer le polynôme minimal de $1+\sqrt[3]{2}+3\sqrt[3]{4}$ sur $\mathbb{Q}$.

> **Indications :** Le polynôme $X^3-2 \in \mathbb{Q}[X]$ est irréductible d'après le critère d'Eisenstein. Donc l'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ est de degré 3. Une base est donnée par $(1, \sqrt[3]{2}, \sqrt[3]{4})$. Dans cette base, la matrice de la multiplication par $1+\sqrt[3]{2}+3\sqrt[3]{4}$ est :
> $$\begin{pmatrix} 1 & 6 & 2 \\ 1 & 1 & 1 \\ 3 & 1 & 1 \end{pmatrix}.$$
> Son polynôme caractéristique est $-X^3+3x^2+10X+8$. Comme $1+\sqrt[3]{2}+3\sqrt[3]{4}$ n'est pas dans $\mathbb{Q}$, son polynôme minimal est de degré 3 : c'est $X^3-3X^2-10X-8$.

3. Calculer $[\mathbb{Q}(\alpha):\mathbb{Q}]$ où $\alpha = 10^{1/5}+7^{1/3}$.

> **Indications :** Par le critère d'Eisentein, les polynômes X^5-10 et X^3-7 de $\mathbb{Q}[X]$ sont irréductibles donc $[\mathbb{Q}(10^{1/5}):\mathbb{Q}]=5$ et $[\mathbb{Q}(7^{1/3}):\mathbb{Q}]=3$. Comme 3 et 5 sont premiers entre eux, cela montre que $[\mathbb{Q}(10^{1/5},7^{1/3}):\mathbb{Q}]=15$. On en déduit que $[\mathbb{Q}(\alpha):\mathbb{Q}]|15$.
> Soit maintenant $P \in \mathbb{Q}[X]$ le polynôme minimal de α sur $\mathbb{Q}$. Soit $Q=(X-7^{1/3})^5-10 \in \mathbb{Q}(7^{1/3})[X]$. On remarque que $Q(\alpha)=0$. Comme $\mathbb{Q}(\alpha,7^{1/3})=\mathbb{Q}(10^{1/5},7^{1/3})$, le polynôme minimal de α sur $\mathbb{Q}(7^{1/3})$ est de degré 5. C'est donc le polynôme Q. On en déduit que Q divise P. Comme $Q \notin \mathbb{Q}[X]$, le degré de P est au moins 6. Par conséquent, $[\mathbb{Q}(\alpha):\mathbb{Q}] \geq 6$. Comme $[\mathbb{Q}(\alpha):\mathbb{Q}]|15$, on a $[\mathbb{Q}(\alpha):\mathbb{Q}]=15$.

Exercice 1 : Partiel 2012

Soit K un corps. Soit L une extension algébrique de K contenue dans $K(X)$. Montrer que $L=K$.

> **Indications :** Voir le corrigé du partiel 2012.

Exercice 2 : Fractions rationnelles telles que $F(x)=F\left(\frac{1}{x}\right)$

Soit K un corps. Soit $L=\{F \in K(x) \mid F(x)=F\left(\frac{1}{x}\right)\}$. Montrer que $K(y) \to L, F(y) \mapsto F(x+\frac{1}{x})$ est un K-isomorphisme de corps. C'est ce résultat qui explique par exemple pourquoi, pour résoudre les équations de la forme $\sum_{k=0}^{6} a_k x^k = 0$ avec $a_k = a_{6-k}$ pour chaque k, il suffit de savoir résoudre les équations de degré 3.

Indications : On voit immédiatement que $K(x+\frac{1}{x}) \subseteq L$. De plus, comme x est racine du polynôme $t^2 - (x+\frac{1}{x})t + 1 \in K(x+\frac{1}{x})[t]$, l'extension $K(x)/K(x+\frac{1}{x})$ est de degré au plus 2. Comme $L \neq K(x)$, on en déduit que $L = K(x+\frac{1}{x})$. Reste à voir que $x+\frac{1}{x}$ est transcendant sur K, ce qui découle immédiatement de l'exercice 1.

Exercice 3 : Polynômes minimaux

Soient K un corps et L une extension finie de K. Soient x, y deux éléments de L, et P_x, P_y leurs polynômes minimaux respectifs sur K. Montrer que P_x est irréductible sur $K(y)$ si et seulement si P_y est irréductible sur $K(x)$.

Indications : Supposons que P_x est irréductible sur $K(y)$. On a alors $[K(x,y) : K(y)] = \deg(P_x)$. Donc $[K(x,y) : K] = [K(x,y) : K(y)][K(y) : K] = \deg(P_x)\deg(P_y)$. Comme $[K(x,y) : K] = [K(x,y) : K(x)][K(x) : K] = [K(x,y) : K(x)]\deg(P_x)$, on en déduit que $\deg(P_y) = [K(x,y) : K(x)]$. Cela montre que P_y est irréductible sur $K(x)$. En renversant les rôles de x et y, on obtient l'implication réciproque.

Exercice 4 : Partiel 2012

Soit L/K une extension de corps algébrique de corps. Soit $P \in L[X]$. Montrer qu'il existe $Q \in K[X]$ divisible par P dans $L[X]$.

Indications : Voir le corrigé du partiel 2012.

Exercice 5 : Irréductibilité de polynômes et extension de scalaires

Soient K un corps et P un polynôme irréductible de degré n sur K. Soit L une extension finie de K de degré premier à n. Montrer que P est irréductible sur L.

Indications : Soit M un corps de décomposition de P sur L. Soit x une racine de P dans M. On a $\deg(P) = [K(x) : K]$. De plus, $[K(x) : K]$ et $[L : K]$ divisent $[L(x) : K]$. Comme $[L(x) : K]$ et $[L : K]$ sont premiers entre eux, on en déduit que $[K(x) : K][L : K]$ divise $[L(x) : K]$. Or $[L(x) : K] = [L(x) : L][L : K] \leq [K(x) : K][L : K]$. Donc $[L(x) : K] = [K(x) : K][L : K]$, et $[L(x) : L] = [K(x) : K] = \deg(P)$. On en déduit que P est irréductible.

Exercice 6 : Un contre-exemple

Soient $K = \mathbb{Q}(T)$ et ses deux sous-corps $K_1 = \mathbb{Q}(T^2)$ et $K_2 = \mathbb{Q}(T^2 - T)$. Montrer que K est algébrique sur K_1 et K_2, mais pas sur $K_1 \cap K_2$.

Indications : Comme T est racine des polynômes $X^2 - T^2 \in K_1(X)$ et $X^2 - X - T^2 + T \in K_2(X)$, le corps K est algébrique sur K_1 et K_2. Montrons que $K_1 \cap K_2 = \mathbb{Q}$. Soient $F_1 \in \mathbb{Q}(T)$ et $F_2 \in \mathbb{Q}(T)$ telles que $F_1(T^2 - T) = F_2(T^2)$. Soit $F = F_2(T^2)$. Comme $F_1(T - T^2)$ est invariante par $T \mapsto 1 - T$ et $F_2(T^2)$ est invariante par $T \mapsto -T$, F est invariante par $T \mapsto T + 1$. Mais alors, les zéros et les pôles de F dans $\overline{\mathbb{Q}}$ sont invariants par $t \mapsto t + 1$. Comme F ne peut avoir qu'un nombre fini de zéros et de pôles, on en déduit que F n'a pas zéros ni de pôles. Par conséquent, $F \in \mathbb{Q}$ et $K_1 \cap K_2 = \mathbb{Q}$.

Exercice 7 : 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 ζ_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 ζ_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 $20 | [\mathbb{Q}(\sqrt[5]{7}, \zeta_5) : \mathbb{Q}]$. 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 ζ_{16} et est irréductible (appliquer le critère d'Eisenstein à $\phi_8(X+1)$). Donc $[\mathbb{Q}(\zeta_{16}) : \mathbb{Q}] = 8$.

Exercice 8 : 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 9 : 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 $x, x+1, ..., x+p-1$.

Indications : Soit $y \in \{0, 1, ..., p-1\}$. On calcule $P(x+y) = (x+y)^p - (x+y) - 2a = x^p + y^p - x - y - 2a = P(x) + P(y) = 0$. Cela montre que $x, x+1, ..., x+p-1$ sont des racines de P. Comme P a au plus p racines, ce sont les seules.

2. Montrer que P est soit scindé soit irréductible.

Indications : Si P possède une racine dans K, alors il est scindé d'après la question précédente. Supposons donc P sans racines. Soit $Q \in K[X]$ un polynôme irréductible divisant P. Soit y une racine de Q dans L. D'après la question 1., si $d = \deg Q$, le coefficient de degré $d-1$ dans Q s'écrit sous la forme $dy + b$ avec $b \in K$. On en déduit que $dy \in K$. Comme $y \notin K$, on en déduit que $d = p$, et donc P est irréductible.

3. Montrer que, si P n'a pas de racines dans K, alors $[L : K] = p$.

> **Indications :** D'après 1., $L = K(x)$. D'après 2., P est irréductible. Cela impose que $[L : K] = \deg P = p$.

Exercice 10 : 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. Supposons P irréductible. Soit Δ son discriminant. Montrer que $[L : K] = 3$ si, et seulement si, Δ est un carré dans K.

> **Indications :** Notons x, y, z les racines de P. Supposons que $\Delta \notin (K^\times)^2$. Alors L contient $K(\sqrt{\Delta})$ et $[K(\sqrt{\Delta}) : K] = 2$. Donc $2|[L : K]$. 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 11 : Extensions de degré 2

Soient K un corps et L/K une extension de degré 2. On suppose la caractéristique de K différente de 2.

1. Montrer qu'il existe $x \in L \setminus K$ tel que l'on ait $L = K(x)$ et $x^2 \in K$.
2. Montrer alors l'égalité $L^{\times 2} \cap K^\times = K^{\times 2} \sqcup x^2 K^{\times 2}$.
3. Soient $y, z \in K^\times$. Montrer que $K(\sqrt{y})$ et $K(\sqrt{z})$ sont isomorphes en tant que K-algèbres si et seulement si zy^{-1} est un carré dans K.

Exercice 12 : Extensions de degré 2 en caractéristique 2

Soient K un corps et L/K une extension de degré 2. On suppose que caractéristique de K est égale à 2.

1. Supposons que L n'est pas de la forme $K(x)$ avec $x^2 \in K$. Montrer qu'il existe $z \in L$ tel que l'on ait $L = K(z)$ et $z^2 - z \in K$.

   Indications : Un élément y de $L \setminus K$ engendre L et vérifie une équation du type $y^2 - ay - b = 0$ avec $a, b \in K$. Parce que L n'est pas de la forme $K(\sqrt{x})$, on a $a \neq 0$ et on peut donc prendre $z = a^{-1}y$.
2. En déduire une classification des extensions de degré 2 de K à isomorphisme de K-algèbres près.

   Indications : Les éléments a de L vérifiant $a^2 - a \in K$ sont $K \cup (z + K)$. De ce fait, deux extensions $K[X]/(X^2-X-x)$ et $K[X]/(X^2-X-y)$ sont isomorphes en tant que K-algèbres si et seulement si $x - y$ est dans l'image de l'automorphisme $\mathbb{F}_2$-linéaire $a \mapsto a^2 - a$ de K. De plus, pour $x \in K^\times$, $K[X]/(X^2 - X - x)$ n'est isomorphe à aucun $K[X]/(X^2 - y)$ puisque les seuls éléments de carré dans K de $K[X]/(X^2 - X - x)$ sont les éléments de K.

Exercice 13 : Extensions engendrées par deux racines carrées

Soient K un corps de caractéristique différente de 2. Soient $x, y \in K^\times$.

1. Montrer que l'extension $K(\sqrt{x}, \sqrt{y})$ de K est de degré 4 si et seulement si on a $x, y, xy \in K^\times \setminus K^{\times 2}$.

   Indications : Si $x \in (K^\times)^2$, alors $K(\sqrt{x}, \sqrt{y}) = K(\sqrt{y})$ est de degré au plus 2 sur K. Il en est de même si $y \in (K^\times)^2$. Si $xy \in (K^\times)^2$, alors $K(\sqrt{x}, \sqrt{y}) = K(\sqrt{x}, \sqrt{xy}) = K(\sqrt{x})$ est de degré au plus 2 sur K.
   Réciproquement, supposons que x, y et xy ne sont pas des carrés dans K. Alors $K(\sqrt{x})/K$ et $K(\sqrt{y})/K$ sont des extension de degré 2. De plus, comme x/y n'est pas un carré dans K, on a $K(\sqrt{x}) \neq K(\sqrt{y})$. On en déduit que $K(\sqrt{x}, \sqrt{y})/K(\sqrt{x})$ est une extension non triviale, a fortiori de degré 2. Donc $[K(\sqrt{x}, \sqrt{y}) : K] = 4$.
2. Dans ce cas, montrer que les seuls corps intermédiaires entre K et $K(\sqrt{x}, \sqrt{y})$ sont K, $K(\sqrt{x})$, $K(\sqrt{y})$ et $K(\sqrt{x}, \sqrt{y})$.

Indications : On dispose de deux extensions intermédiaires évidentes, à savoir K et $K(\sqrt{x},\sqrt{y})$. Les autres extensions intermédiaires sont de degré 2 sur K. Soit L une telle extension intermédiaire. Il existe $z \in L \setminus K$ et $a \in K$ tels que $z^2 = a$. On a $L = K(z)$. On écrit $z = a + b\sqrt{x} + c\sqrt{y} + d\sqrt{xy}$. On a alors les relations $ab+ycd = ac+xbd = ad+bc = 0$. On obtient alors $b(-c^2+xd^2) = acd+xbd^2 = 0$. Comme x n'est pas un carré dans K, cela montre que $b = 0$ ou $c = d = 0$. Si $b = 0$, on obtient aussi $c = 0$ ou $d = 0$, donc $L = K(\sqrt{xy})$ ou $L = K(\sqrt{y})$. Si $c = d = 0$, $L = K(\sqrt{x})$. Les extensions intermédiaires sont donc K, $K(\sqrt{x})$, $K(\sqrt{y})$, $K(\sqrt{xy})$, $K(\sqrt{x},\sqrt{y})$.

Exercice 14 : Partiel 2014

Soit K un corps de caractéristique différente de 2. Soient $a, b \in K^\times$, avec $b \notin K^{\times 2}$. Soient $K_1 = K(\sqrt{b})$ et $L = K(\alpha)$ avec $\alpha^2 = a + \sqrt{b}$. On rappelle (exercice 12) que $K^\times \cap K_1^{\times 2} = K^{\times 2} \sqcup bK^{\times 2}$.

1. Montrer que $L = K_1$ si, et seulement si, il existe $d \in K^\times$ tel que $a^2 - b = d^2$ et $2(a + d) \in K^{\times 2}$.
2. Montrer qu'il existe $\beta \in L^\times$ tel que $\beta^2 = a - \sqrt{b}$ si, et seulement si, $a^2 - b \in K^{\times 2} \sqcup bK^{\times 2}$.
3. Calculer $K^\times \cap L^{\times 2}$.
4. Montrer qu'il existe $c \in K^\times$ tel que $L = K(\sqrt{b},\sqrt{c})$ si, et seulement si, $a^2 - b \in K^{\times 2}$.

Exercice 15 : Sommes de carrés

Soit $\alpha \in \mathbb{C}$ tel que $\alpha^2 = 1 + \rho\sqrt[3]{2}$.

1. Montrer que le corps $\mathbb{Q}(\alpha)$ est une extension de degré 6 de $\mathbb{Q}$.

   Indications : On remarque que α est racine de $P = X^6 - 3X^4 + 3X^2 - 3$. Ce polynôme est irréductible par le critère d'Eisenstein. Donc $\mathbb{Q}(\alpha)$ est une extension de degré 6 de $\mathbb{Q}$.

2. Dans $\mathbb{Q}(\alpha)$, le nombre -1 est-il une somme de carrés ?

   Indications : Le polynôme P a aussi $\beta = \sqrt{1 + \sqrt[3]{2}}$ pour racine. On a donc des $\mathbb{Q}$-isomorphismes de corps :

   $$\mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/(P) \cong \mathbb{Q}(\beta).$$

   Comme $\mathbb{Q}(\beta) \subseteq \mathbb{R}$, on ne peut pas écrire -1 comme somme de carrés dans $\mathbb{Q}(\beta)$. Il en est donc de même dans $\mathbb{Q}(\alpha)$.

Exercice 16 : Penser à utiliser la trace !

Le nombre $\sqrt[7]{2}$ est-il dans $\mathbb{Q}(\sqrt[7]{3})$?

Indications : Soient $L = \mathbb{Q}(\sqrt[7]{2})$ et $M = \mathbb{Q}(\sqrt[7]{3})$. Ce sont des extensions de degré 7 de $\mathbb{Q}$. Supposons que $\sqrt[7]{2}$ soit dans $\mathbb{Q}(\sqrt[7]{3})$. Alors $L = M$ et, pour chaque entier naturel j, la famille $B_j = (\sqrt[7]{2^k 3^{kj}})_{0\leq k\leq 6}$ est une $\mathbb{Q}$-base de $L = M$. Il en est de même de la famille $B = (\sqrt[7]{3^k})_{0\leq k\leq 6}$. Écrivons $\sqrt[7]{2} = \sum_{k=0}^{6} a_k \sqrt[7]{3^k}$ avec les $a_i \in \mathbb{Q}$. Pour chaque entier j, en calculant dans la base B_j, on remarque que $\mathrm{Tr}_{L/\mathbb{Q}}(\sqrt[7]{2\cdot 3^j}) = 0$. De même, en calculant dans la base B, on voit que $\mathrm{Tr}_{L/\mathbb{Q}}(\sqrt[7]{3}) = 0$. En écrivant pour chaque $j \in \{0, ...6\}$ la relation : $\sqrt[7]{2\cdot 3^j} = \sum_{k=0}^{6} a_k \sqrt[7]{3^{k+j}}$ et en prenant les traces de ces relations, on obtient que $a_0 = a_1 = ... = a_6 = 0$: absurde !

Exercice 17 : Est-il un carré ?

Le nombre $1 + \sqrt[3]{2}$ est-il un carré dans $\mathbb{Q}(\sqrt[3]{2})$?

Indications : La famille $(1, \sqrt[3]{2}, \sqrt[3]{4})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt[3]{2})$. Dans cette base, on calcule $N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(1 + \sqrt[3]{2}) = 3$. Comme 3 n'est pas un carré dans $\mathbb{Q}$, on en déduit que $1 + \sqrt[3]{2}$ n'est pas un carré dans $\mathbb{Q}(\sqrt[3]{2})$.

Exercice 18 : 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 19 : 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 $\varphi_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, x \mapsto x^p$ le Frobenius. Soit G le sous-groupe de $\mathrm{Aut}(\mathbb{F}_{p^n})$ engendré par φ_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 φ_p^s et φ_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 20 : 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 sue $\mathbb{F}_3$: ils sont donc isomorphes à $\mathbb{F}_9$. On définit un isomorphisme par :

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

Exercice 21 : Rattrapage 2014

Pour tout entier $n > 0$, on note P_n l'ensemble des polynômes irréductibles de degré n à coefficients dans $\mathbb{F}_2$.

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

2. Expliciter tous les éléments de P_4.

> **Indications :** D'après la question précédente, $|P_4| = 3$. Soit $Q \in P_4$ et écrivons $Q = X^4 + q_3X^3 + q_2X^2 + q_1X + q_0$. 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 $X^4 + X + 1$.

3. 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 22 : 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 23 : 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 $X^{17} - 1$.

Indications : Voir le corrigé du partiel 2013.

Exercice 24 : 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.

Indications : Si ζ est une racine de ϕ_5, alors les autres racines de ϕ_5 sont ζ^2, ζ^3 et ζ^4.

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 $p \equiv \pm 2 \mod 5$.

Indications : Si $p \equiv 1 \mod 5$, alors $(\mathbb{F}_p)^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ possède un élément d'ordre 5, qui est une racine de ϕ_5. Donc $[L : \mathbb{F}_p] = 1$ grâce à la question 1.
Supposons $p \equiv -1 \mod 5$. 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 dordre 5. Donc ϕ_5 a une racine dans $\mathbb{F}_{p^2}$, et $[L : \mathbb{F}_p] = 2$.
Supposons $p \equiv \pm 2 \mod 5$. 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, ϕ_5 possède des racines dans $\mathbb{F}_{p^4}$. Donc $[L : \mathbb{F}_p] = 4$.

3. Soient $\zeta \in L$ une racine de ϕ_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. Déduire des questions précédentes que 5 est un carré dans $\mathbb{F}_p$ si, et seulement si, $p \equiv \pm 1 \mod 5$.

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

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

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

Exercice 25 : 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 10).

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 26 : 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 $\mathbb{F}_q$.

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

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

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 $r_1 + ... + r_n = d(q-1)$ puisque $d < n$. Donc :

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

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

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

Indications : On a $|V| > 0$ puisque $P(0,...,0) = 0$. 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 $P \in \mathbb{F}_q[X_1,...,X_n]$ 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 $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$.

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

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

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

Exercice 27 : 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 $\mathbb{F}_p$.