Leçon 125 : Extensions de corps : Exemples et applications

Mathieu Alix

–

1 Rapport du Jury

« Les extensions de degré fini, le théorème de la base téléscopique et ses applications à l'irréductibilité de certains polynômes, ainsi que les corps finis, sont incontournables. Il est souhaitable d'introduire la notion d'élément algébrique et d'extension algébrique en en donnant des exemples. Il faut savoir calculer le polynôme minimal d'un élément algébrique dans des cas simples, notamment pour quelques racines de l'unité. La leçon peut être illustrée par des exemples d'extensions quadratiques et leurs applications en arithmétique, ainsi que par des extensions cyclotomiques.

Pour aller plus loin, les candidates et candidats peuvent montrer que l'ensemble des nombres algébriques forme un corps algébriquement clos, par exemple en expliquant comment l'utilisation du résultant permet de calculer des polynômes annulateurs de sommes et de produits de nombres algébriques. Il est possible de s'intéresser aux nombres constructibles à la règle et au compas, et éventuellement s'aventurer en théorie de Galois. »

Remarque importante : Ce document se limitera aux extensions de corps, en ne parlant qu'une seule fois de corps finis pour le dernier exercice tiré de jury d'agreg. Le concepteur de cette feuille faisant le choix de réorienter le lecteur vers la fiche correspondante à la leçon 123 sur les corps finis.

2 Questions classiques

1. Le polynôme $P(X) = X^3 - 127X^2 + 3608X + 19$ est -il irréductible dans $\mathbb{Z}[X]$?

   Solution: Oui en appliquant le critère d'irréductibilité mod un idéal premier (p. 12 [GOZ]). Le polynôme est primitif (car unitaire) et irréductible dans $\mathbb{Q}[X]$ car son réduit modulo 2, $X^3 - X + 1$ est irréductible (sans racines dans $\mathbb{F}_2$).

2. Calculer $[\mathbb{R} : \mathbb{Q}]$.

   Solution: $[\mathbb{R} : \mathbb{Q}] = +\infty$. En effet, si c'était fini de degré N, alors $\mathbb{R} = \mathbb{Q}^N$ et donc $\mathbb{R}$ serait dénombrable, contradiction.

3. Montrer que $e^{2i\pi/5} \notin \mathbb{Q}(e^{2i\pi/7})$.

Solution: Si c'était le cas, alors $\mathbb{Q} \subseteq \mathbb{Q}(e^{2i\pi/5}) \subseteq \mathbb{Q}(e^{2i\pi/7})$. et donc par la base téléscopique

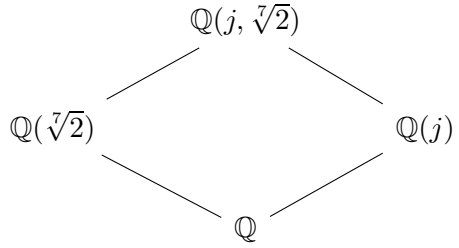
$$\varphi(7) = [\mathbb{Q}(e^{2i\pi/7}) : \mathbb{Q}] = [\mathbb{Q}(e^{2i\pi/7}) : \mathbb{Q}(e^{2i\pi/5})][\mathbb{Q}(e^{2i\pi/5}) : \mathbb{Q}] = \varphi(5)[\mathbb{Q}(e^{2i\pi/7}) : \mathbb{Q}(e^{2i\pi/5})]$$

Contradiction car 4 ne divise pas 6

4. (Jury d'agreg) :
   (a) $X^7 - 2$ est il réductible sur $\mathbb{Q}$?
   (b) $X^7 - 2$ sur $\mathbb{Q}(j)$?

Solution:

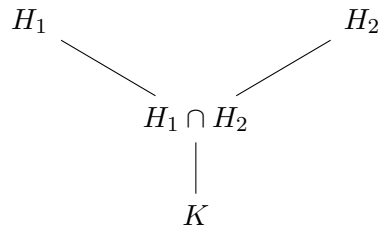
1. Irréductible par le critère d'Eisenstein en prenant $p = 2$.
2. En considérant $\sqrt[7]{2}$, et en écrivant les tours d'extensions suivantes :



On a $[Q(j, \sqrt[7]{2}) : \mathbb{Q}(\sqrt[7]{2})] = 2$ car j est annulé par un polynôme de degré 2 dans $\mathbb{Q}(\sqrt[7]{2})$ ($X^2 + X + 1$ et j n'est pas dans l'extension) alors $[\mathbb{Q}(j, \sqrt[7]{2}) : \mathbb{Q}] = 14$ par le côté gauche de la tour, et donc du côté droit, on tire $[\mathbb{Q}(j, \sqrt[7]{2}) : \mathbb{Q}(j)] = 7$ donc $X^7 - 2$ est le polynôme minimal de $\sqrt[7]{2}$ dans $\mathbb{Q}(j)$ donc est irréductible.

5. Soient K un corps et L une extension de K de degré fini. Soient H_1 et H_2 des corps tels que $K \subseteq H_i \subseteq L$ (pour $i = 1, 2$). Montrer que si $[H_1 : K]$ et $[H_2 : K]$ sont premiers entres eux, $H_1 \cap H_2 = K$.

Solution: Comme L extension de degré fini de K et $K \subseteq H_i \subseteq L$, alors H_i sont des extensions de degrés fini de K. On a la tour d'extension :



Ainsi par la base telescopique, $[H_1 : K] = [H_1 : H_1 \cap H_2][H_1 \cap H_2 : K]$ et $[H_2 : K] = [H_2 : H_1 \cap H_2][H_1 \cap H_2 : K]$. Ainsi $[H_1 \cap H_2 : K]$ est un diviseur commun de $[H_2 : K]$ et $[H_1 : K]$ qui sont premiers entre eux, d'où $[H_1 \cap H_2 : K] = 1$, et donc $H_1 \cap H_2 = K$.

6. Les extensions $\mathbb{Q}(i)/\mathbb{Q}$ et $\mathbb{Q}(j)/\mathbb{Q}$ sont-elles isomorphes ?

Solution: Non car X^2+1 n'a pas de racine dans $\mathbb{Q}(j)$. En effet, l'équation $(a+bj)^2=-1$ pour $(a,b)\in\mathbb{Q}^2$ conduit à $3b^2=1$ ce qui est impossible dans $\mathbb{Q}$.

7. Les extensions $\mathbb{R}(i)/\mathbb{R}$ et $\mathbb{R}(j)/\mathbb{R}$ sont-elles isomorphes ?

Solution: Cette fois oui, car on a les égalités $j=\frac{-1+i\sqrt{3}}{2}$ et $i=\frac{2j+1}{\sqrt{3}}$ ce qui implique que $\mathbb{R}(i)=\mathbb{R}(j)$. On tire donc un isomorphisme entre $\mathbb{R}[X]/(X^2+1)$ et $\mathbb{R}[X]/(X^2+X+1)$.

8. Soient K un corps et L une extension de degré premier. Montrer que tout élément appartenant à L mais non à K engendre avec K, tout L

Solution: Notons $[L:K]=p$ et $\alpha\in L\backslash K$. En regardant la tour $K\subseteq K(\alpha)\subseteq L$, par la base télescopique, $p=[L:K]=[L:K(\alpha)][K(\alpha):K]$. Mais comme p est premier, l'un des deux termes vaux 1. C'est le premier car sinon $[K(\alpha):K]=1$ et donc $K(\alpha)=K$ impossible car $\alpha\in K(\alpha)\backslash K$. Ainsi $[L:K(\alpha)]=1$ d'où $L=K(\alpha)$.

9. Pour quels nombres premiers p,q a-t-on $\mathbb{Q}(\sqrt{p})\subseteq\mathbb{Q}(\sqrt[3]{q})$?

Solution: Vérifier que $\mathbb{Q}(\sqrt{p})=\{a+b\sqrt{p},(a,b)\in\mathbb{Q}\}$ et $\mathbb{Q}(\sqrt[3]{q})=\{a+b\sqrt[3]{q}+c\sqrt[3]{q}^2,(a,b,c)\in\mathbb{Q}^3\}$. $[\mathbb{Q}(\sqrt{p}):\mathbb{Q}]=2$ et $[\mathbb{Q}(\sqrt[3]{q}):\mathbb{Q}]=3$. Si $\mathbb{Q}(\sqrt{p})\subseteq\mathbb{Q}(\sqrt[3]{q})$, alors par base téléscopique

$$3=[\mathbb{Q}(\sqrt[3]{q}):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{q}):\mathbb{Q}(\sqrt{p})][\mathbb{Q}(\sqrt{p}):\mathbb{Q}]=2[\mathbb{Q}(\sqrt[3]{q}):\mathbb{Q}(\sqrt{p})]$$

contradiction.

10. Soit α un élément algébrique de degré impair sur le corps K. Montrer que $K(\alpha)=K(\alpha^2)$.

Solution: Notons $[K(\alpha):K]=2p+1$ et $\pi_\alpha(X)=\sum_{i=0}^{2p+1}a_iX^i\in K[X]$ le polynôme minimal (irréductible) de α sur K (on a donc $a_{2p+1}=1$).

- On a évidemment que $\alpha^2\in K(\alpha)$ et donc $K(\alpha^2)\subseteq K(\alpha)$.
- Réciproquement comme $0=\pi_\alpha(\alpha)=\sum_{j=0}^{p}a_{2j}\alpha^{2j}+\alpha\sum_{j=0}^{p}a_{2j+1}\alpha^{2j}$. Alors en notant $A(X)=\sum_{j=0}^{p}a_{2j}X^j$ et $B(X)=\sum_{j=0}^{p}a_{2j+1}X^j$, ceux-sont des polynômes de $K[X]$ et $\deg(B)=p$ car $a_{2p+1}=1$. Ainsi $\deg(B(X^2))=2p<\deg(\pi_\alpha(X))$ et donc $\pi_\alpha(X)$ ne divise pas $B(X^2)$ et $B(\alpha^2)\neq 0$. Ainsi de $0=\pi_\alpha(\alpha)=A(\alpha^2)+\alpha B(\alpha^2)$, on peut donc réécrire, $\alpha=-\frac{A(\alpha^2)}{B(\alpha^2)}$ et par conséquent $\alpha\in K(\alpha^2)$ d'où l'autre inclusion et donc l'égalité.

11. Montrer que si a et b sont deux éléments non nuls d'un corps K de caractéristique différente de 2, $K(\sqrt{a})=K(\sqrt{b})$ si et seulement si $\frac{b}{a}$ est un carré dans K.

Solution: Il est immédiat que si $\frac{b}{a} = x^2$, avec $x \in K$; alors $\sqrt{b} = \pm x\sqrt{a}$ et donc $K(\sqrt{a}) = K(\sqrt{b})$. Réciproquement, supposons que $K(\sqrt{a}) = K(\sqrt{b})$, Alors il existe $x, y \in K$ tels que $\sqrt{b} = x + y\sqrt{a}$. On a donc $\sqrt{b} - x = y\sqrt{a}$, donc en élevant au carré, on a $b - 2x\sqrt{b} + x^2 = ay^2$. Donc $2x\sqrt{b} = b + x^2 - ay^2$. On a donc deux cas possibles : soit $\sqrt{b} \in K$, auquel cas $\sqrt{a} \in K$ et le résultat est évident. Soit $\sqrt{b} \notin K$, alors $2x\sqrt{b} = 0$, donc $x = 0$ (caractéristique différente de 2), donc $\sqrt{a} = y\sqrt{b}$, $y \in K$, ce qui conclut.

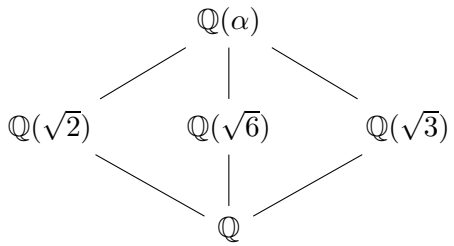
12. Donner les polynômes cyclotomiques rationnels ϕ_n pour n allant de 1 à 8.

Solution: On utilise évidemment la formule $X^n - 1 = \prod_{d|n} \phi_d$ et le fait que $\phi_p = \sum_{k=0}^{p-1} X^k$ pour p premier (le faire remontrer ?). On obtient :

- $\phi_1 = X - 1$
- $\phi_2 = X + 1$
- $\phi_3 = X^2 + X + 1$
- $\phi_4 = X^2 + 1$
- $\phi_5 = X^4 + X^3 + X^2 + X + 1$
- $\phi_6 = X^2 - X + 1$
- $\phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$
- $\phi_8 = X^4 + 1$

13. Faire l'étude de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sur $\mathbb{Q}$. (trouver un élément primitif, extensions intermédiaires, etc..)

Solution: degré 4, élément primitif $\alpha = \sqrt{2} + \sqrt{3}$, et tour d'extension :



— Montrons que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$: L'inclusion réciproque est immédiate (car $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est le sous corps de $\mathbb{R}$ engendré par $\mathbb{Q}, \sqrt{2}, \sqrt{3}$. Dans l'autre sens, $(\sqrt{2} + \sqrt{3})^3 = 5 + 2\sqrt{6}$, donc $\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Mais on a aussi, $\sqrt{6}(\sqrt{2} + \sqrt{3}) = 2\sqrt{3} + 3\sqrt{2}$ ce qui nous assure que $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, d'où l'égalité.

— Vérifier facilement que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Déduire donc le degré $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$, et donc celui de $\mathbb{Q}(\alpha)/\mathbb{Q}$ par base téléscopique.

— Déduire que $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. (toujours par base téléscopique)

— Polynôme minimal de α : $\pi_\alpha = X^4 - 10X^2 + 1 = \prod((X \pm \sqrt{2}) \pm \sqrt{3})$ car annule bien α, de degré 4 et unitaire.

3 Questions plus exotiques

1. (Jury d'agreg) Soient x et y deux éléments algébriques sur un corps K, de polynômes minimaux respectifs $\mu_x \in K[X]$ et $\mu_y \in K[X]$. On suppose que μ_x est irréductible sur $K[y]$. Montrer que μ_y est irréductible sur $K[x]$.

Solution: Puisque x est algébrique sur K, son polynôme minimal μ_x est unitaire et irréductible sur K. On suppose que μ_x reste irréductible sur $K[y]$. Cela signifie que x est algébrique sur $K(y)$, de degré $\deg \mu_x =: d_x$. Ainsi :

$$[K(x,y) : K(y)] = d_x.$$

De même, y est algébrique sur K, de degré $\deg \mu_y =: d_y$, donc :

$$[K(y) : K] = d_y.$$

En utilisant la base téléscopique à la tour d'extension : $K \subseteq K(y) \subseteq K(x,y)$

$$[K(x,y) : K] = [K(x,y) : K(y)] \cdot [K(y) : K] = d_x d_y.$$

Par symétrie : sur $K \subseteq K(x) \subseteq K(x,y)$

$$[K(x,y) : K(x)] = \frac{[K(x,y) : K]}{[K(x) : K]} = \frac{d_x d_y}{d_x} = d_y.$$

On a donc :

$$[K(x,y) : K(x)] = d_y = \deg \mu_y.$$

Cela implique que le polynôme minimal μ_y de y sur K reste irréductible sur $K[x]$.

2. Soit L/K une extension de corps, et α un élément de L algébrique sur K. Notons π_α le polynôme minimal de α sur K. Considérons $\mu : \overline{Q} \in K(\alpha) = K[X]/(\pi_\alpha) \mapsto \alpha \cdot \overline{Q} \in K(\alpha)$. Comparer π_α et le polynôme minimal de μ.

Solution: Posons $\pi_\alpha(X) = \sum_{k=0}^{n} a_k X^k$ avec $a_n = 1$. L'endomorphisme $\pi_\alpha(\mu)$ est la multiplication par $\sum_{k=0}^{n} a_k \alpha^k$ qui est nul dans $K(\alpha)$, ainsi on a donc que $\pi_\alpha(\mu) = 0$. Ainsi le polynôme minimal de μ divise $\pi_\alpha(X)$. Or les endomorphismes $Id, \mu, \ldots, \mu^{n-1}$ sont linéairement indépendants sur K, puisque les images de $1 \in K(\alpha)$ par ces endomorphismes, c'est à dire $1, \alpha, \ldots, \alpha^{n-1}$ sont linéairement indépendants sur K. Il suit que le polynôme minimal de μ est de degré $\geq n$, mais il divise $\pi_\alpha(X)$ qui est unitaire de degré n, il y est donc égal.

3. (Jury d'agreg - en une seule question la dernière, ici détaillée en 3) :
   (a) Soit p un nombre premier impair. Démontrer que $p^2 - 1$ est divisible par 8.
   (b) En déduire que $\mathbb{F}_{p^2}^\times$ admet un élément α d'ordre 8, que α^3, α^5 et α^7 sont aussi d'ordre 8 et que $X^4 + 1$ est scindé sur $\mathbb{F}_{p^2}$.

(c) En déduire que X^4+1 est réductible sur $\mathbb{F}_p$.

Solution:

1. $p = 2k+1$ et donc $p^2 - 1 = 4k(k+1) \equiv 0 \mod [8]$.
2. Le groupe $G = \mathbb{F}_{p^2}^\times$ est cyclique d'ordre p^2-1. Considérons γ un générateur de G, alors $\alpha = \gamma^{(p^2-1)/8}$ est d'ordre 8, de même pour les puissances demandées. Or $\alpha^8 = 1$, donc $\alpha^4 = \pm 1$, mais comme l'ordre de α est 8, alors $\alpha^4 = -1$, ainsi α est racine de X^4+1 ; de même pour les autres puissances. En conclusions, X^4+1 est scindé sur $\mathbb{F}_{p^2}$.
3. Si $\alpha \in \mathbb{F}_p$, alors $X^4+1 \in \mathbb{F}_p$, avec pour racines $\alpha, \alpha^3, \alpha^5$ et α^7. Sinon, $\mathbb{F}_p(\alpha)$ est une extension de degré 2 de $\mathbb{F}_p$, c'est donc $\mathbb{F}_{p^2}$. Le polynôme minimal de α est alors de degré 2, il divise X^4+1 qui est donc le produit de deux polynômes de degré 2 dans $\mathbb{F}_p[X]$. Dans les deux cas, X^4+1 est réductible sur $\mathbb{F}_p$.