Algèbre approfondie.

Exercice 1 — Questions de cours.

a) Supposons P irréductible. Soit $x \in k[\mathrm{X}]/(\mathrm{P}) \smallsetminus \{0\}$. Ainsi $x = \pi(\mathrm{Q})$ où Q est un polynôme non divisible par P ($\pi : k[\mathrm{X}] \to k[\mathrm{X}]/(\mathrm{P})$ désigne la surjection canonique). Comme P est irréductible et $\mathrm{P} \nmid \mathrm{Q}$, on a $\mathrm{pgcd}(\mathrm{P}, \mathrm{Q}) = 1$. On peut ainsi écrire une relation de Bézout, $\mathrm{PU} + \mathrm{VQ} = 1$. En appliquant π, on obtient $\pi(\mathrm{V})x = 1$ et x est inversible.

Supposons que $k[\mathrm{X}]/(\mathrm{P})$ est un corps. Soit Q un diviseur de P, on écrit $\mathrm{P} = \mathrm{QR}$. En appliquant π, on obtient $\pi(\mathrm{Q})\pi(\mathrm{R}) = 0$. Comme $k[\mathrm{X}]/(\mathrm{P})$ est un corps, on obtient $\pi(\mathrm{Q}) = 0$ ou $\pi(\mathrm{R}) = 0$. Dans le premier cas, on a $\mathrm{P} \mid \mathrm{Q}$ et donc P et Q sont associées. Dans le deuxième cas, on obtient $\mathrm{P} \mid \mathrm{R}$. Comme $\mathrm{R} \mid \mathrm{P}$, on obtient que P et R sont associés. Ainsi Q est inversible. Finalement, les seuls diviseurs de P sont 1 et les éléments associés à P donc P est irréductible.

b) Soit K une extension finie de k et $x \in \mathrm{K}$ de degré n. La famille $(1, x, \ldots, x^n)$ est liée (elle a un cardinal plus grand que la dimension). Il existe donc une famille $(\lambda_i)_{i=0,\ldots,n} \in k^{n+1}$ non nulle telle que $\lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n = 0$. Ainsi x est racine de $\lambda_0 + \lambda_1 \mathrm{X} + \cdots + \lambda_n \mathrm{X}^n \in k[\mathrm{X}]$.

c) On écrit $\mathrm{Q} = c(\mathrm{Q})\widetilde{\mathrm{Q}}$ et $\mathrm{R} = c(\mathrm{R})\widetilde{\mathrm{R}}$ avec $c(\mathrm{Q}), c(\mathrm{R}) \in \mathbb{Q}$ qui sont les contenus de Q et R et $\widetilde{\mathrm{Q}}, \widetilde{\mathrm{R}} \in \mathbb{Z}[\mathrm{X}]$ primitif. On a alors $\mathrm{P} = \mathrm{QR} = c(\mathrm{Q})c(\mathrm{R})\widetilde{\mathrm{Q}}\widetilde{\mathrm{R}}$. Comme Q et R sont unitaires, P l'est et donc P est primitif. On en déduit que $c(\mathrm{P}) = c(\mathrm{Q})c(\mathrm{R}) = 1$. Ainsi $\mathrm{P} = \widetilde{\mathrm{Q}}\widetilde{\mathrm{R}}$. Comme P est unitaire, le produit des coefficients de plus haut degré de $\widetilde{\mathrm{Q}}$ et $\widetilde{\mathrm{R}}$ est 1. On obtient qu'ils sont égaux à 1 (ou tous les deux égaux à -1 auxquels cas, on multiplie $\widetilde{\mathrm{Q}}$ et $\widetilde{\mathrm{R}}$ par -1). Comme Q et R sont unitaires, on obtient ainsi $\mathrm{Q} = \widetilde{\mathrm{Q}} \in \mathbb{Z}[\mathrm{X}]$ et $\mathrm{R} = \widetilde{\mathrm{R}} \in \mathbb{Z}[\mathrm{X}]$.

d) Le polynôme $\mathrm{X}^n - 2 \in \mathbb{Q}[\mathrm{X}]$ annule $\sqrt[n]{2}$. Il est irréductible sur $\mathbb{Q}$ par Eisenstein. C'est donc le polynôme minimal de $\sqrt[n]{2}$ sur $\mathbb{Q}$. Ainsi $\sqrt[n]{2}$ est de degré n sur $\mathbb{Q}$. Or on vu que pour qu'un nombre soit constructible, il fallait que son degré soit un puissance de 2. Ainsi si $\sqrt[n]{2}$ est constructible alors il existe k tel que $n = 2^k$. Inversement on suppose que $n = 2^k$, comme $\sqrt[2^k]{2}^2 = \sqrt[2^{k-1}]{2}$ a la suite d'extensions quadratiques

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt[4]{2}] \subset \cdots \subset \mathbb{Q}[\sqrt[2^k]{2}]\,;$$

ce qui assure que $\sqrt[n]{2}$ est constructible.

Exercice 2

a) Le polynôme $\mathrm{X}^6 - 11$ est irréductible sur $\mathbb{Q}$ d'après le critère d'Eisenstein appliqué avec $p = 11$.

b) Les racines de $\mathrm{X}^6 - 11$ sur $\mathbb{Q}$ dans $\mathbb{C}$ sont $x = \sqrt[6]{11}$, $\exp(i\pi/3)x$, $\exp(2i\pi/3)x$, $-x$, $\exp(4i\pi/3)x$, $\exp(5i\pi/3)x$. Ainsi $\mathrm{K} = \mathbb{Q}(x, \exp(i\pi/3)x, \exp(2i\pi/3)x, -x, \exp(4i\pi/3)x, \exp(5i\pi/3)x)$. Comme $\exp(i\pi/3)x/x = \exp(i\pi/3)$, on a $\exp(i\pi/3) \in \mathrm{K}$ et donc $\mathbb{Q}(x, \exp(i\pi/3)) \subset \mathrm{K}$. Inversement, on a évidemment $\exp(ki\pi/3)x \in \mathbb{Q}(x, \exp(i\pi/3))$. Donc $\mathrm{K} = \mathbb{Q}(x, \exp(i\pi/3))$. En posant, $j = \exp(2i\pi/3) \in \mathrm{K}$ et en remarquant que $\exp(i\pi/3) = 1 + j$, on obtient aussi que $\mathrm{K} = \mathbb{Q}(j, x)$.

c) On a $[\mathrm{K} : \mathbb{Q}] = [\mathrm{K} : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}]$. On a vu que $[\mathbb{Q}(x) : \mathbb{Q}] = 6$. Par ailleurs, $\exp(i\pi/3) \notin \mathbb{Q}(x) \subset \mathbb{R}$. Donc $[\mathrm{K} : \mathbb{Q}(x)] \geqslant 2$. De plus $\exp(i\pi/3)$ est racine de $\mathrm{X}^2 - \mathrm{X} + 1 \in \mathbb{Q}[\mathrm{X}] \subset \mathbb{Q}(x)[\mathrm{X}]$. Ainsi $[\mathrm{K} : \mathbb{Q}(x)] \leqslant 2$. On en déduit que $[\mathrm{K} : \mathbb{Q}(x)] = 2$ et que $\mathrm{X}^2 - \mathrm{X} + 1$ est irréductible sur $\mathbb{Q}(x)$ (la même argumentation marche avec j et le polynôme $\mathrm{X}^2 + \mathrm{X} + 1$ à la place de $\exp(i\pi/3)$ et $\mathrm{X}^2 - \mathrm{X} + 1$).

Ainsi $[\mathrm{K} : \mathbb{Q}] = 12$ et une base est donnée par

$$(1, x, x^2, x^3, x^4, x^5, \exp(i\pi/3), \exp(i\pi/3)x, \exp(i\pi/3)x^2, \exp(i\pi/3)x^3, \exp(i\pi/3)x^4, \exp(i\pi/3)x^5).$$

On peut aussi bien sûr considérer la base $(1, x, x^2, x^3, x^4, x^5, j, jx, jx^2, jx^3, jx^4, jx^5)$.

d) Un sous-corps isomorphe à un corps de rupture va être de la forme $\mathbb{Q}(y)$ où y est une racine de $\mathrm{X}^6 - 11$. A priori, il y a donc 6 candidats : $\mathrm{L}_0 = \mathbb{Q}(x)$, $\mathrm{L}_1 = \mathbb{Q}(\exp(i\pi/3)x)$, $\mathrm{L}_2 = \mathbb{Q}(\exp(2i\pi/3)x)$, $\mathrm{L}_3 = \mathbb{Q}(-x) = \mathrm{L}_0$, $\mathrm{L}_4 = \mathbb{Q}(\exp(4i\pi/3)x) = \mathbb{Q}(-\exp(i\pi/3)x) = \mathrm{L}_1$, $\mathrm{L}_5 = \mathrm{L}2$. On en trouve déjà plus que 3. Peut-on avoir $\mathrm{L}_0 = \mathrm{L}_1$? Si c'est le cas, on a $\exp(i\pi/3)x \in \mathrm{L}_0$ et donc $\exp(i\pi/3) = \exp(i\pi/3)x/x \in \mathrm{L}_0 \subset \mathbb{R}$. NON. De même, si $\mathrm{L}_0 = \mathrm{L}_2$, on aurait $j \in \mathbb{R}$. NON. Enfin si $\mathrm{L}_1 = \mathrm{L}_2$, on a $\exp(i\pi/3) = \exp(2i\pi/3)x/(\exp(i\pi/3)x) \in \mathrm{L}_1$ et donc $x \in \mathrm{L}_1$ et $\mathrm{L}_1 = \mathrm{K}$. Or $[\mathrm{L}_1 : \mathbb{Q}] = 6$ puisque c'est un corps de rupture de P alors que $[\mathrm{K} : \mathbb{Q}] = 12$. NON. Ainsi, il y a trois sous-corps de K qui sont des corps de rupture.

e) Le polynôme $\mathrm{P} \in \mathbb{Q}[\mathrm{X}] \subset \mathbb{Q}(j)[\mathrm{X}]$ est scindé dans K et K est engendré sur $\mathbb{Q}$ donc sur $\mathbb{Q}(j)$ par les racines de P. C'est donc un corps de décomposition de P sur $\mathbb{Q}(j)$.

f) Soit Q le polynôme minimal de x sur $\mathbb{Q}(j)$. Il divise donc $\mathrm{X}^6 - 11$. Par ailleurs, on a $[\mathbb{Q}(j, x) : \mathbb{Q}(j)] = \deg \mathrm{Q}$. Mais $[\mathrm{Q}\mathbb{Q}(j) : \mathbb{Q}] = 2$ et donc par multiplicativité des degrés, on a $[\mathbb{Q}(j, x) : \mathbb{Q}(j)] = 6$. Ainsi $\deg \mathrm{Q} = 6$ et $\mathrm{X}^6 - 11$ est le polynôme minimal de x sur $\mathbb{Q}(j)$ qui est donc irréductible sur $\mathbb{Q}(j)$. Ainsi $\mathbb{Q}(j, x)$ est engendré sur $\mathbb{Q}(j)$ par un élément donc le polynôme minimal est P c'est donc un corps de rupture de P sur $\mathbb{Q}(j)$.

g) La propriété universelle des corps de rupture l'existence d'une bijection entre les $\mathbb{Q}(j)$-morphismes de K dans lui-même et les racines de P contenue dans K. Il y a donc 6 tels morphismes. Ce sont des morphismes de $\mathbb{Q}(j)$-extensions, ils envoient donc j sur j et x sur l'une des racines de P c'est-à-dire sur $\exp(ik\pi/3)x$ avec $k = 0, \ldots, 5$.