École Polytechnique 2009-2010

Théorie de Galois

Corrigé de la Feuille d'exercices 6

Exercice 1.

(i) Comme $(x^2-1)^2 = 2$, $[\mathbf{Q}[x] : \mathbf{Q}]$ divise 4. Ce n'est pas 1 car $\sqrt{2} \in \mathbf{Q}[x]$ n'est pas dans $\mathbf{Q}$. Si c'est 2, alors $\mathbf{Q}[x] = \mathbf{Q}(\sqrt{2})$ et

$$x = \alpha\sqrt{2} + \beta \text{ avec } \alpha, \beta \in \mathbf{Q}.$$

Donc

$$x^2 = 2\alpha^2 + \beta^2 + 2\alpha\beta\sqrt{2} = 1 + \sqrt{2}$$

et

$$\beta^2 + \frac{1}{2\beta^2} = 1,$$

contradiction car $\beta \in \mathbf{Q}$.

(ii) On a $\pi_x(\sqrt{1-\sqrt{2}}) = 0$ avec

$$\pi_x(X) = (X^2-1)^2 - 2,$$

le polynôme minimal de x sur $\mathbf{Q}$. donc $\sqrt{1-\sqrt{2}}$ est un conjugué de x sur $\mathbf{Q}$. Il s'agit d'un imaginaire pure, il n'est donc pas dans $\mathbf{Q}[x] \subset \mathbf{R}$. L'extension $\mathbf{Q}[x]/\mathbf{Q}$ n'est donc pas galoisienne.

Par contre, le polynôme minimal de x sur $\mathbf{Q}[\sqrt{2}]$ est $X^2 - 1 - \sqrt{2}$, donc les conjugués de x sont x et $-x$. On a donc une extension galoisienne. De même, les conjugués de $\sqrt{2}$ sur $\mathbf{Q}$ sont $\sqrt{2}$ et $-\sqrt{2}$.

Les conjugués de i sur $\mathbf{Q}$ sont i et $-i$. Les conjugués de x sur $\mathbf{Q}$ sont

$$x\ ,\ -x\ ,\ \sqrt{1-\sqrt{2}}\ ,\ -\sqrt{1-\sqrt{2}}.$$

Il sont tous dans $\mathbf{Q}[i,x]$ avec $\sqrt{1-\sqrt{2}} = ix^{-1}$. On a

$$[\mathbf{Q}[x,i] : \mathbf{Q}] = [\mathbf{Q}[x,i], \mathbf{Q}[x]][\mathbf{Q}[x], \mathbf{Q}].$$

Or $[\mathbf{Q}[x], \mathbf{Q}] = 4$. De plus $[\mathbf{Q}[x,i], \mathbf{Q}[x]] \neq 1$ car $i \notin \mathbf{R} \supset \mathbf{Q}[x]$. Donc $[\mathbf{Q}[x,i], \mathbf{Q}[x]] = 2$.

(iii) On montre comme dans (i) que le degré est 4. Le polynôme minimal de $\sqrt{2+\sqrt{2}}$ sur $\mathbf{Q}$ est $(X^2-2)^2 - 2$, donc les conjugués sur $\mathbf{Q}$ de $\sqrt{2+\sqrt{2}}$ sont

$$\sqrt{2+\sqrt{2}}\ ,\ -\sqrt{2+\sqrt{2}}\ ,\ \sqrt{2-\sqrt{2}}\ ,\ -\sqrt{2-\sqrt{2}}.$$

On peut conclure car

$$\sqrt{2-\sqrt{2}} = (\sqrt{2+\sqrt{2}})^{-1}\sqrt{2}.$$

Exercice 2.

(i) On a $\pi_x = X^3 - 2$ (qui est irréductible sur $\mathbf{Q}$ d'après le critère d'Eisenstein par exemple) et $\pi_j = X^2 + X + 1$. Les conjugués de x sont

$$x\ ,\ jx\ ,\ j^2x$$

et de j sont j et j^2. Ces conjugués sont tous dans K, on a donc une extension galoisienne. Maintenant,

$$[K : \mathbf{Q}] = [K : \mathbf{Q}[x]][\mathbf{Q}[x] : \mathbf{Q}] = 3[K : \mathbf{Q}[x]].$$

Mais $[K : \mathbf{Q}[x]] \neq 1$ car $j \notin \mathbf{R}$, c'est donc 2. On obtient $[K : \mathbf{Q}] = 6$.

$Gal(K/\mathbf{Q})$ agit sur $\{x, jx, j^2x\}$, donc on a un morphisme de groupe

$$Gal(K/\mathbf{Q}) \to \mathfrak{S}_3.$$

Ce morphisme est injective car l'action de $Gal(K/\mathbf{Q})$ sur $j = (jx)x^{-1}$ et sur x est déterminée par l'image dans $\mathfrak{S}_3$. On peut conclure car les deux groupes ont le même cardinal 6.

(ii) On a 6 sous corps de K :

$$\mathbf{Q} \ , \ \mathbf{Q}[j] \ , \ \mathbf{Q}[x] \ , \ \mathbf{Q}[jx] \ , \ \mathbf{Q}[j^2x] \ , \ K.$$

Ils correspondent respectivement aux 6 sous-groupes de $\mathfrak{S}_3$ suivants : $\mathfrak{S}_3$, $\mathfrak{A}_2$, les 3-sous groupes d'ordre 3, le sous-groupe d'ordre 1.

Exercice 3.

(i) $\mathbf{F}_{q^n}$ peut être construire comme le corps de décomposition de $X^{q^n} - X$. Soit x l'image de X dans $\mathbf{F}_{q^n}$. C'est un élément primitif, c'est à dire $\mathbf{F}_{q^n} = \mathbf{F}_q[x]$. Les q^n racines de $X^{q^n} - X$ sont les éléments de $\mathbf{F}_{q^n}$. Donc les conjugués de x sont dans $\mathbf{F}_{q^n}$ et on a une extension galoisienne.

Un élément du groupe de Galois est déterminé par son image y en x. y doit être d'ordre $q^n - 1$. C'est donc un élément de

$$\{x, x^q, x^{q^2}, \cdots, x^{q^{n-1}}\}.$$

(On rappelle que $\mathbf{F}_{q^n}^*$ est un groupe cyclique). Le groupe de Galois est donc au plus d'ordre n.

Mais on obtient de telles images en utilisant des puissances du Frobenius $x \mapsto x^q$. Les n puissances du Frobenius sont bien des éléments du groupe de Galois. On peut donc conclure.

(ii) On identifie le groupe de Galois avec $\mathbf{Z}/n\mathbf{Z}$. Pour d qui divise n, on a un unique sous-groupe d'ordre n/d (le sous-groupe engendré par d). La sous-extension associée est l'ensemble des racines de $X^{q^d} - X$, qui est un sous-corps isomorphe à $\mathbf{F}_{q^d}$.