École Polytechnique 2022-2023

Algèbre et théorie de Galois

Corrigé de la Feuille d'exercices 8

Exercice 1. C'est une sous-extension de $\mathbf{Q}[e^{2i\pi/7}]/\mathbf{Q}$ qui a pour degré 6. Soit $\zeta = e^{2i\pi/7}$, et $\alpha = \cos(\frac{2\pi}{7}) = \frac{\zeta+\zeta^{-1}}{2}$. On a des inclusions $\mathbf{Q} \subseteq \mathbf{Q}[\alpha] \subseteq \mathbf{Q}[\zeta]$; l'equation $\zeta^2 - 2\alpha\zeta + 1 = 0$ montre que $[\mathbf{Q}[\zeta] : \mathbf{Q}[\alpha]] \leq 2$. Le degré de l'extension $\mathbf{Q}[\zeta]/\mathbf{Q}[\alpha]$ ne peut pas être égal à 1 car $\mathbf{Q}[\alpha]$ inclus dans $\mathbf{R}$ contrairement à $\mathbf{Q}[\zeta]$.
L'extension $\mathbf{Q}[\zeta]/\mathbf{Q}[\alpha]$ est donc de degré 2, et $\mathbf{Q}[\alpha]/\mathbf{Q}$ est de degré 3.
On peut également prouver que $\mathbf{Q}[\alpha]$ est le sous-corps de $\mathbf{Q}[\zeta]$ fixé par la conjugaison complexe, et retrouver le résultat par la correspondance de Galois.

Exercice 2.

(i) Cours (sous ces hypothèses le polynôme est premier avec sa dérivée).

(ii) On le montre par récurrence sur N en utilisant la formule de factorisation

$$\overline{X^N - 1} = \prod_{d|N} \overline{\Phi}_d(X)$$

qui passe à la réduction modulo p. En effet, c'est clair pour $N = 1$. En géneral, dire qu'une racine N-ième n'est pas primitive signifie qu'elle est d'ordre $d < N$ divisant N, et donc racine de $\overline{\Phi}_d(X)$. On obtient donc le résultat.

(iii) On factorise en produit de polynômes irréducibles dans $\mathbf{F}_p[X]$:

$$\overline{\Phi}_N = P_1 \dots P_g.$$

Comme $\overline{\phi}_N$ est séparable (car $X^N - 1$ l'est), les P_i sont distincts. Pour x une racine de P_i, les autres racines de P_i sont ses conjugués sur $\mathbf{F}_p$. Le groupe de Galois du corps de décomposition de $\overline{\Phi}_N$ étant engendré par le morphisme de Frobenius, les racines de P_i sont les $x^{(p^k)}$ avec $k \geq 0$. Comme x est primitive, c'est un élément d'ordre N dans $(\mathbf{F}_p)^*$. On a donc $x^{(p^k)} = x$ si et seulement si $p^k \equiv 1 \bmod N$. Or le plus petit $k > 0$ tel que $p^k \equiv 1 \bmod N$ est l'ordre M de p dans le groupe des inversibles de $\mathbf{Z}/N\mathbf{Z}$. Donc P_i a M racines. Comme il est séparable, il est de degré M.

(iv) Φ_N est irréductible dans $\mathbf{F}_p[X]$ si et seulement si $g = 1$ ce qui équivaut à $M = \deg(\Phi_N) = \phi(N)$. Comme $(\mathbf{Z}/N\mathbf{Z})^*$ est d'ordre $\phi(N)$, la condition équivaut à p engendre $(\mathbf{Z}/N\mathbf{Z})^*$.

(v) On a

$$X^4 + 1 = \Phi_8(X)$$

irréductible dans $\mathbf{Q}[X]$. Mais le groupe

$$(\mathbf{Z}/8\mathbf{Z})^* = \{1, 3, 5, 7\}$$

n'est pas cyclique (les éléments qui le composent sont d'ordre 1 ou 2). Donc pour tout nombre $p > 2$ premier, son image dans $(\mathbf{Z}/8\mathbf{Z})^*$ ne peut engendrer le groupe. D'après (iv), la réduction modulo p de $X^4 + 1$ est donc réductible. Pour $p = 2$, on a une factorisation $X^4 + 1 = (X + 1)^4$.

Exercice 3.

(i) Le groupe de Galois de l'extension cyclotomique étant commutatif, tous ses sous-groupes sont distingués.

(ii) L'extension $\mathbf{Q}[\sqrt[3]{2}]$ n'est pas galoisienne sur $\mathbf{Q}$ car le conjugué $j\sqrt[3]{2}$ de $\sqrt[3]{2}$ n'appartient pas à cette extension. D'après (i), ce n'est donc pas une sous-extensions d'une extension cyclotomique.

Exercice 4.

Il s'agit de la Proposition 6.4.1 du cours.

Exercice 5.

(i) On a

$$\Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = 1 + X^{p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}.$$

On note que

$$\Phi_6(X) = (X^6-1)(X^2-1)^{-1}(X^2+X+1)^{-1} = X^2 - X + 1$$

a un coefficient négatif.

(ii) Le degré de l'extension cyclotomique est $\Phi(12) = 4$. Les corps de décomposition K_3, K_4 respectivement de $\Phi_3(X)$ et de $\Phi_4(X)$ forment des sous-extensions de degré 2. On regarde les projections sur les quotients par $\mathrm{Gal}(K/K_3)$ et $\mathrm{Gal}(K/K_4)$, ce qui donne un morphisme Φ du groupe de Galois vers $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$. Le sous corps engendré par K_3 et K_4 est K. Donc un élément dans le noyau du morphisme Φ est l'identité et Φ est injectif. Par cardinalité on obtient un isomorphisme.

Exercice 6.

(i) Puisque S_n est engendré par les transpositions, il suffit de montrer que toute transposition (j,k) avec $k > j$ peut être écrite comme composition de transpositions de la forme $(i, i+1)$. Pour cela, on observe que $\sigma = (k-1,k)(k-2,k-1)\cdots(j,j+1) = (k,k-1,\ldots,j+1,j)$. De manière analogue on a $\sigma' = (j,j+1)(j+1,j+2)\cdots(k-2,k-1) = (j,j+1,\ldots,k-2,k-1)$, et donc $\sigma'\sigma = (j,k)$.

(ii) D'après la partie précédente il suffit de prouver que, étant donné $1 \leq i \leq n-1$, la transposition $(i,i+1)$ peut s'exprimer à l'aide de $(1,\ldots,n)$ et $(1,2)$. Or, on a $(i,i+1) = (1,\ldots,n)^{i-1}(1,2)(1,\ldots,n)^{-(i-1)}$.

(iii) En réordonnant les entiers $\{1,\ldots,n\}$ on peut supposer que $c = (1,\ldots,n)$ et que le support $\mathrm{Supp}(b)$ de b est $\{2,\ldots,n\}$. En choisissant un entier convenable k et raisonnant comme dans la partie précédente on obtient une transposition $a' = c^{-k}ac^k$ dont le support $\mathrm{Supp}(a')$ n'est pas contenu dans $\{2,\ldots,n\}$, c'est-à-dire que $a'(1) \neq 1$. De manière similaire, pour un entier l convenable on a que $b^{-l}a'b^l = (1,2)$, et la partie (ii) permet donc de conclure.

(iv) On rappelle que le groupe A_n est le noyau du morphisme signature $S_n \to \{\pm 1\}$. Il consiste donc de ces permutations qui peuvent s'écrire comme composition d'un nombre pair de transpositions. Tout 3-cycle étant composition de deux transpositions, les 3-cycles sont bien des éléments de A_n. Il reste à démontrer que toute composition non triviale de deux transpositions est engendrée par des 3-cycles. Cela est immédiat, car si les deux transpositions ont supports non disjoints on a $(i,k)(i,j) = (i,j,k)$; si elles ont supports disjoints on a $(i,j)(k,l) = (i,j,k)(j,k,l)$.