École Polytechnique
Algèbre et théorie de Galois MAT 451

Contrôle classant du 24 mai 2023 - 3 heures

Avertissement

Les calculatrices et documents autres que le polycopié de cours sont interdits. La rédaction doit être concise et précise. Les exercices sont indépendants. Il n'est pas nécessaire de terminer le sujet pour avoir une excellente note.

Exercice 1

1. Cela découle du fait que $N(x) = x\overline{x}$.

2. Le polynôme est de degré 3 donc il est irréductible si et seulement s'il n'a pas de racine. Soit $a \in \mathbf{Q}$ qui n'est pas un cube (par exemple $a = 2$). S'il existe $x \in K$ avec $x^3 = a$, alors $N(x)^3 = a^2$, donc a^2 est un cube, ce qui n'est pas possible.

3. Les conjugués de θ sur K sont $\theta, j\theta, j^2\theta$. Donc $L = K[\theta, j]$, ce qui prouve que L/K est de degré 6 (il contient deux sous-extensions de degrés 2 et 3). On a $i\sqrt{3} \in L$, donc $\sqrt{5} \in L$.

4. Soit σ l'élément du groupe de Galois défini par $\sigma(\sqrt{5}) = \sqrt{5}$, et $\sigma(\theta) = j\theta$. Soit τ l'élément défini par τ l'élément défini par $\tau(\sqrt{5}) = -\sqrt{5}$, $\tau(\theta) = \theta$. On a $\tau\sigma\tau^{-1} = \sigma^2$. Le groupe de Galois est non commutatif d'ordre 6, donc isomorphe à S_3.

5. Il y a une extension de degré 2 sur K, $K[\sqrt{5}]$. Il y a trois extensions de degré 3 sur K : $K[\theta], K[j\theta], K[j^2\theta]$.

6. Si $a \in \mathbf{Q}$, alors $N(a) = a^2 = b^3$. Alors les exposants des facteurs premiers de a sont multiples de 3 et a est un cube, ce qui contredit l'irréductibilité de $X^3 - a$.

7. On a $a\overline{a} = b^3$ L'élément θ est annulé par $(X^3 - a)(X^3 - \overline{a}) = (X^3 - a)(X^3 - \frac{b^3}{a})$, qui est un polynôme à coefficients rationnels (les coefficients sont dans K et invariants par la conjugaison complexe). Si $P \in \mathbf{Q}[X]$ est un polynôme irréductible le divisant, alors il le divise dans $K[X]$. Or les polynômes $X^3 - a$ et $X^3 - \frac{b^3}{a}$ sont irréductibles dans $K[X]$, et ne sont pas à coefficients rationnels. Donc $P = (X^3 - a)(X^3 - \frac{b^3}{a})$, ce qui prouve l'irréductibilité du polynôme. Les conjugués de θ sur $\mathbf{Q}$ sont donc $j^k\theta$, et $j^k\frac{b}{\theta}$, pour $k = 0, 1, 2$.

8. On a $L = K[\sqrt{5}, j, \theta]$, et les conjugués sur $\mathbf{Q}$ de chacun de ces éléments sont dans L. Donc $L/\mathbf{Q}$ est galoisienne.

9. On fixe l'automorphisme sur $K_0 := \mathbf{Q}[\sqrt{5}, i\sqrt{15}]$, et on cherche les possibilités de l'étendre à L. Il y a $[L : K_0] = 3$ possibilités, déterminés par l'image de θ. Le polynôme minimal de θ sur K_0 est $X^3 - a$, et ϕ envoie ce polynôme sur $X^3 - \overline{a} = X^3 - \frac{b^3}{a}$. On a donc nécessairement $\phi(\theta) = j^k\frac{b}{\theta}$, $k = 0, 1, 2$.

10. La restriction de ϕ à K_0 est d'ordre 2, donc l'ordre de ϕ est pair. De plus, $\phi^2(\theta) = j^{2k}\frac{b}{j^k\theta} = j^k\frac{b}{\theta}$. Pour $k = 0$, ϕ est d'ordre 2, sinon il est d'ordre 6.

11. Soit ϕ_0 le morphisme précédent obtenu pour $k = 0$. On vérifie que ϕ_0 commute avec σ et τ, donc avec $\mathrm{Gal}(L/K)$. D'où

$$\mathrm{Gal}(L/K) \simeq < \phi_0 > \times \mathrm{Gal}(L/K) \simeq (\mathbf{Z}/2\mathbf{Z}) \times S_3$$

12. Par la correspondance de Galois, on cherche un sous-groupe H d'ordre 6, et cyclique. Il doit être engendré par un élément d'ordre 6. La description précédente montre qu'il y a un unique tel sous-groupe, engendré par ϕ_0 et σ. Il est égal à $\mathbf{Q}[\sqrt{5}]$ car $\sqrt{5}$ est fixé par cex deux morphismes.

13. Il faut déterminer le nombre d'éléments d'ordre 2 dans le groupe de Galois : il y en a 7, et un seul engendre un sous-groupe distingué. Il y a donc 7 extensions de degré 6, dont une seule est galoisienne (celle fixée par ϕ_0).

14. On cherche un sous-groupe d'ordre 4 du groupe de Galois. Le sous-groupe H engendré par ϕ_0 et τ convient. Soit L_0 l'extension correspondante. Elle est de degré 3 et contient $x = \theta + \frac{b}{\theta}$. On a $\mathbf{Q} \subseteq \mathbf{Q}[x] \subseteq L_0$. Le degré de x sur $\mathbf{Q}$ vaut donc 1 ou 3. S'il valait 1, on aurait $x \in \mathbf{Q}$,

et θ serait de degré 2 sur $\mathbf{Q}$. C'est impossible car θ est de degré 3 sur K. Donc x est de degré 3 sur $\mathbf{Q}$, et convient.

Exercice 2

1. Puisque n est premier à p, le polynôme $X^n - 1$ est séparable, et a donc n racines distinctes dans $\overline{\mathbf{F}_p}$.

2. Si $\mu_n \subseteq \mathbf{F}_p$, c'est un sous-groupe de $\mathbf{F}_p^\times$, donc n divise $p-1$. Réciproquement, si n divise $p-1$, tout élément $x \in \mathbf{F}_p$ vérifie $x^{p-1} = 1$, donc $x^p = x$ et $x \in \mathbf{F}_p$.

3. D'après ce qui précède, on a $\mu_n \subseteq \mathbf{F}_{p^d}$ si et seulement si $p^d = 1$ modulo n. Le plus petit entier d qui convient est égal à l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^\times$.

4. Il s'agit d'une extension de corps finis, donc l'extension est galoisienne et le groupe de Galois est isomorphe à $\mathbf{Z}/r\mathbf{Z}$, avec $r = [k_n : \mathbf{F}_q]$. Explicitement, on a $k_n = \mathbf{F}_{p^{l_n}}$, avec $l_n = ppcm(d, d_n)$, où d_n est l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^\times$. Donc $r = \frac{l_n}{d} = \frac{ppcm(d,d_n)}{d}$.

5. On a $k_n \cap k_m = \mathbf{F}_{p^{pgcd(l_n,l_m)}}$ et $k_n k_m = \mathbf{F}_{p^{ppcm(l_n,l_m)}}$.

Exercice 3

1. Montrons que $\mathbf{Q}[x]$ est de degré 4 sur $\mathbf{Q}$. On a $\mathbf{Q}[\sqrt{7}] \subseteq \mathbf{Q}[x]$, donc le degré est un multiple de 2. De plus, x est racine de $(X^2-2)^2 - 7 = X^4 - 2X^2 - 3$, donc le degré est inférieur ou égal à 4. Il vaut donc 2 ou 4. S'il était égal à 2, on aurait $x \in \mathbf{Q}[\sqrt{7}]$. Soit σ l'automorphisme non trivial de $\mathbf{Q}[\sqrt{7}]$; on aurait alors $\sigma(x)^2 = 2 - \sqrt{7} < 0$ ce qui est impossible puisque $\sigma(x)$ est réel.
   Le degré vaut donc 4, et le polynôme minimal vaut $X^4 - 2X^2 - 3$.

2. Les conjugués de x sur $\mathbf{Q}$ sont $\pm\sqrt{2+\sqrt{7}}, \pm i\sqrt{\sqrt{7}-2}$. Puisque $\mathbf{Q}[x]$ est inclus dans $\mathbf{R}$, il ne contient pas tous les conjugués de x, et l'extension n'est pas galoisienne.

3. Le corps L doit nécessairement contenir $i\sqrt{\sqrt{7}-2}$ d'après ce qui précède. L'extension $\mathbf{Q}[x, i\sqrt{\sqrt{7}-2}]$ est galoisienne, et est donc égale à L. Puisque $i\sqrt{\sqrt{7}-2}$ est de degré 2 sur $\mathbf{Q}[\sqrt{7}]$, L est de degré 1 ou 2 sur $\mathbf{Q}[x]$. Or $\mathbf{Q}[x]$ n'est pas galoisienne sur $\mathbf{Q}$, donc L est de degré 8 sur $\mathbf{Q}$.

4. $\mathrm{Gal}(L/\mathbf{Q}[\sqrt{7}])$ est un groupe d'ordre 4, il est donc égal à $\mathbf{Z}/4\mathbf{Z}$ ou $(\mathbf{Z}/2\mathbf{Z})^2$. En considérant les extensions $\mathbf{Q}[x], \mathbf{Q}[i\sqrt{\sqrt{7}-2}]$, on voit que ce groupe a au moins deux éléments d'ordre 2. Il est donc égal à $(\mathbf{Z}/2\mathbf{Z})^2$.

5. Si le groupe était abélien, toutes les sous-extensions seraient galoisiennes, ce qui n'est pas le cas.

6. Le groupe est non abélien d'ordre 8, donc isomorphe à D_4 ou H_8. Puisqu'il contient au moins 3 éléments d'ordre 2 d'après la question précédente, il est isomorphe à D_4.
   On peut aussi identifier le groupe de Galois à un sous-groupe de S_4. Il est d'ordre 8, donc contient le sous-groupe des doubles transposition. A isomorphisme près, il est égal au sous-groupe formé de
   $$\mathrm{id}, \tau_{1,2}, \tau_{3,4}, \tau_{1,2}\tau_{3,4}, \tau_{1,3}\tau_{2,4}, \tau_{1,4}\tau_{2,3}, (1324), (1423)$$

7. Il suffit de déterminer les sous-groupes d'ordre 4 contenus dans le groupe de Galois. Il y en a 3, ce qui correspond à trois extensions quadratiques Le calcul $x(i\sqrt{\sqrt{7}-2}) = i\sqrt{5}$ montre que ces extensions sont
   $$\mathbf{Q}[\sqrt{7}] \qquad \mathbf{Q}[i\sqrt{5}] \qquad \mathbf{Q}[i\sqrt{35}]$$