École Polytechnique
Algèbre et théorie de Galois MAT 451

Contrôle classant du 27 mai 2022 - 3 heures

Avertissement

Les calculatrices et documents autres que le polycopié de cours et notes personnelles 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) D'après le cours, ζ_5 est de degré $\phi(5) = 4$, et son polynôme minimal est $\Phi_5 = X^4 + X^3 + X^2 + X + 1$.

2) On a $0 = \zeta_5^2 + \zeta_5 + 1 + \zeta_5^{-1} + \zeta_5^{-1} = (\zeta_5 + \zeta_5^{-1})^2 + \zeta_5 + \zeta_5^{-1} - 1$. Puisque $\zeta_5 + \zeta_5^{-1} = 2a$, on obtient

$$4a^2 + 2a - 1 = 0$$

d'où $a = \frac{-1+\sqrt{5}}{4}$ (puisque $a \geq 0$).

3) On a $a^2 + b^2 = 1$, donc $b^2 = (5 + \sqrt{5})/8$. D'où $\mathbf{Q}[\sqrt{5}] \subseteq \mathbf{Q}[b]$, et $\mathbf{Q}[b]$ est de degré 1 ou 2 sur $\mathbf{Q}[\sqrt{5}]$. Montrons qu'il est de degré 2, ce qui permettra de conclure. Si ce n'est pas le cas, $10 + 2\sqrt{5}$ est un carré dans $\mathbf{Q}[\sqrt{5}]$, et il existe des rationnels x, y avec $(x + y\sqrt{5})^2 = 10 + 2\sqrt{5}$, soit $x^2 + 5y^2 = 10$, $xy = 1$. On vérifie que ces équations n'admettent pas de solution rationnelle.
On a $(8b^2 - 5)^2 = 5$, donc le polynôme minimal de b est $X^4 - \frac{5}{4}X^2 + \frac{5}{16} = 0$.

4) Les conjugués de ζ_5 sont les ζ_5^k avec $1 \leq k \leq 4$, les conjugués de i sont $i, -i$. Puisque ces éléments sont dans K, cette extension est galoisienne.

5) On a $K = \mathbf{Q}[\zeta_5, \zeta_4] = \mathbf{Q}[\zeta_{20}]$, qui est donc de degré $\phi(20) = 8$ sur $\mathbf{Q}$. Le groupe de Galois est isomorphe à

$$(\mathbf{Z}/20\mathbf{Z})^\times \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$$

6) A part les extensions triviales $\mathbf{Q}$ et K, le degré divise 8 donc vaut 2 ou 4. Pour le degré 4, il faut compter le nombre de sous-groupes de G de cardinal 2, il y en a 3. Pour le degré 2, il faut compter le nombre de sous-groupes de G de cardinal 4, il y en a 3.

7) Les extensions de degré 2 sont $\mathbf{Q}[i]$, $\mathbf{Q}[\sqrt{5}]$ et $\mathbf{Q}[i\sqrt{5}]$. Les extensions de degré 4 sont $\mathbf{Q}[i,\sqrt{5}]$, $\mathbf{Q}[\zeta_5]$ et $\mathbf{Q}[b]$.

8) Traitons tout d'abord le cas où k est premier avec n. Alors $\cos(k\theta_n) = \frac{\zeta_n^k+\zeta_n^{-k}}{2}$. Puisque ζ_n^k est une racine primitive n-ème, $\mathbf{Q}[\zeta_n^k]$ est de degré $\phi(n)$. On a $\mathbf{Q}[\cos(k\theta_n)] \subseteq \mathbf{Q}[\zeta_n^k]$, et le degré de cette extension est 1 ou 2. Il ne peut être égal à 1 car un des corps est réel. On obtient donc que le degré de $\cos(k\theta_n)$ est $\phi(n)/2$.
Dans le cas général, soit d le PGCD de k et n, $k = dk'$ et $n = dn'$. Alors $\cos(k\theta_n) = \cos(k'\theta_{n'})$, et est donc de degré $\phi(n')/2$.

9) Par l'absurde, si $i \in \mathbf{Q}[\zeta_n]$, alors

$$\mathbf{Q}[\zeta_n] = \mathbf{Q}[\zeta_n, i] = \mathbf{Q}[\zeta_n, \zeta_4] = \mathbf{Q}[\zeta_{4n}]$$

ce qui n'est pas possible car le degré de $\mathbf{Q}[\zeta_{4n}]$ est $\phi(4n) = 2\phi(n)$.

10) En utilisant la formule $\sin(x) = \cos(\frac{\pi}{2} - x)$, on obtient $\sin(\theta_n) = \cos(\frac{\pi(n-4)}{2n}) = \cos((n-4)\theta_{4n})$. Puisque $n-4$ est premier avec $4n$, la question 8 donne que $\sin(\theta_n)$ est de degré $\phi(4n)/2 = \phi(n)$.

11) Si $t = \tan(\theta_n)$, on utilise la formule $\cos(2\theta_n) = \frac{1-t^2}{1+t^2}$.

12) D'après ce qui précède, $\mathbf{Q}[\cos(2\theta_n)] \subseteq \mathbf{Q}[\tan(\theta_n)] \subseteq \mathbf{Q}[\cos(\theta_n), \sin(\theta_n)]$. Le premier corps est de degré $\phi(n)/2$, et le dernier $\phi(n)$ sur $\mathbf{Q}$. Si $\tan(\theta_n)$ était de degré $\phi(n)/2$, alors $\sin(\theta_n)$ serait de degré au plus $\phi(n)/2$ ce qui n'est pas. Donc $\tan(\theta_n)$ est de degré $\phi(n)$.

13) Si $n = 2k$ avec k impair, on trouve que $\sin(\theta_n)$ est de degré $\phi(n)$, et $\tan(\theta_n)$ est de degré $\phi(n)$.
Si $n = 4k$ avec k impair, on trouve que $\sin(\theta_n)$ est de degré $\phi(n)/4$, et $\tan(\theta_n)$ est de degré $\phi(n)/2$.
Si n est divisible par 8, on trouve que $\sin(\theta_n)$ est de degré $\phi(n)/2$, et $\tan(\theta_n)$ est de degré $\phi(n)/4$.

Exercice 2

1) On vérifie que e est dans $Com_{G,x}$, et si $y, z \in Com_{G,x}$, alors $yz^{-1} \in Com_{G,x}$.

2) Soit $G_y = \{g \in G, y = gxg^{-1}\}$, et on écrit $y = g_1 x g_1^{-1}$. Alors $g \in G_0$ si et seulement si $gxg^{-1} = g_1 x g_1^{-1}$, ce qui est équivalent à $g_1^{-1} gx = x g_1^{-1} g$, c'est-à-die $g_1^{-1} g \in Com_{G,x}$. D'où $G_0 = g_1 Com_{G,x}$, et son cardinal est égal à celui de $Com_{G,x}$.

3) G est l'union disjoint des G_y, avec y dans $C_{G,x}$, donc

$$|G| = \sum_{yinC_{G,x}} |G_y| = \sum_{y \in C_{G,x}} |Com_{G,x}| = |Com_{G,x}||C_{G,x}|$$

4) On considère le morphisme quotient $G \to G/H$, que l'on restreint à $Com_{G,x}$. Le noyau de la restriction est $Com_{G,x} \cap H = Com_{H,x}$. Soit K l'image de $Com_{G,x}$ par le morphisme quotient; si r est le cardinal de K, il divise n puisque G/H est un groupe de cardinal n.
Puisque K est isomorphe à $Com_{G,x}/Com_{H,x}$, on obtient que $|Com_{G,x}| = r|Com_{H,x}|$. On a alors

$$|C_{G,x}| = \frac{|G|}{|Com_{G,x}|} = \frac{n|H|}{r|Com_{H,x}|} = d|C_{H,x}|$$

avec $d = n/r$, qui est bien un entier divisant n.

5) $C_{S_4,t}$ est la classe de conjugaison de t dans S_4, et consiste des doubles transpositions. Il est de cardinal 3.
Puisque A_4 est d'indice 2 dans S_4, il existe d divisant 2 avec $|C_{S_4,t}| = d|C_{A_4,t}|$. Nécessairement $C_{A_4,t}$ est de cardinal 3.

6) $C_{S_4,s}$ est l'ensemble des 3-cycles, donc de cardinal 8. On en déduit que $C_{A_4,s}$ est de cardinal 4 ou 8. Puisque ce cardinal divise le cardinal de A_4 qui vaut 12, il est égal à 4. En faisant agir les doubles transpositions par conjugaison, on obtient que cet ensemble consiste de

$$(123) \quad (142) \quad (134) \quad (243)$$

7) On sait que A_5 est une union de classes de conjugaisons de S_5 : l'identité, les 3-cycles, les 5-cycles, et les doubles traspositions. Il suffit de voir pour

chacune de ces classes de conjugaisons dans S_5 la décomposition en classes de conjugaisons dans A_5.
Soit x un 3-cycle. Alors $C_{S_5,x}$ est de cardinal 20, et $Com_{S_5,6}$ est de cardinal 6. Si $x = (123)$, alors $Com_{S_5,x}$ est engendré par x et $\tau_{4,5}$. Donc $Com_{A_5,x}$ est de cardinal 3 (engendré par x), et $C_{A_5,x}$ est de cardinal 20.
Soit y une double transposition. Alors $C_{S_5,y}$ est de cardinal 15, et par le même argument que la question précédente est égal à $C_{A_5,y}$.
Soit z un 5-cycle. Alors $C_{S_5,z}$ est de cardinal 24, et $Com_{S_5,z}$ est de cardinal 5, et est donc engendré par z. Donc $Com_{A_5,x}$ est de cardinal 5, et $C_{A_5,z}$ est donc de cardinal 12.
On obtient que A_5 a 5 classes de conjugaisons : l'identité (cardinal 1), les 3-cycles (cardinal 20), les doubles transpositions (cardinal 15), et deux classes de conjugaisons de cardinal 12, chacune étant composée de 5-cycles.

Exercice 3

1) Il y a p^2 polynômes unitaires de degré 2 à coefficients dans $\mathbf{F}_p$. Les polynômes réductibles sont soit de la forme $(X-a)^2$ (au nombre de p), soit de la forme $(X-a)(X-b)$ avec a, b distincts (au nombre de $p(p-1)/2$). On obtient donc qu'il y a $p(p-1)/2$ polynômes irréductibles de degré 2.

2) Les polynômes réductibles de degré 3 sont soit de la forme $(X-a)^3$ (au nombre de p), soit de la forme $(X-a)^2(X-b)$ avec a, b distincts (au nombre de $p(p-1)$), soit de la forme $(X-a)(X-b)(X-c)$ avec a, b, c distincts (au nombre de $p(p-1)(p-2)/6$), soit de la forme $(X-a)Q(X)$ avec Q irréductible de degré 2 (au nombre de $p^2(p-1)/2$). On obtient donc que le nombre de polynômes irréductibles de degré 3 est égal à

$$p^3 - p - p(p-1) - p(p-1)(p-2)/6 - p^2(p-1)/2 = p(p^2-1)/3$$

3) Soit $P \in \mathbf{F}_p[X]$ un polynôme irréductible de degré d, et $K = \mathbf{F}_p[X]/P$. Alors K est un corps fini de cardinal p^d. Si x est égal à la classe de x dans K, alors $x^{p^d-1} = 1$ puisque $K^\times$ est un groupe de cardinal $p^d - 1$. Donc $x^{p^d} - x = 0$, et puisque le polynôme minimal de x est P, on en déduit que P divise $X^{p^d} - X$.

4) Soit r le degré de P et $L = \mathbf{F}_p[X]/P$. Alors L est un corps fini de cardinal p^r, et si x désigne la classe de X, on a $x^{p^d} = x$. On obtient donc que L est inclus dans $\mathbf{F}_{p^d}$. Comme L est isomorphe à $\mathbf{F}_{p^r}$, r divise d.

5) Considérons la factorisation de $X^{p^q} - X$: ses facteurs irréductibles ont un degré divisant q, donc égal à 1 ou q. De plus, chaque polynôme irréductible de degré 1 ou q le divise. Puisque $X^q - X$ est séparable, on en déduit qu'il est égal au produit de tous les polynômes irréductibles de degré 1 ou q.
Le produit de tous les polynômes irréductibles de degré 1 est égal à $X^p - X$.
Si $P_1, \ldots, P_N$ sont les polynômes irréductibles de degré q, on a donc

$$X^{p^q} - X = (X^p - X)P_1 \ldots P_N$$

L'égalité des degrés donne

$$N = \frac{p^q - p}{q}$$

6) De même que précédemment, les polynômes irréductibles divisant $X^{p^{q^d}} - X$ ont un degré divisant q^d, donc égal à q^i, avec $0 \leq i \leq d$. On a également que $X^{p^{q^d}} - X$ est égal au produit de tous les polynômes irréductibles de degré q^i avec $0 \leq i \leq d$.
Si $P_1, \ldots, P_M$ sont les polynômes irréductibles de degré q^d, on a donc

$$X^{p^{q^d}} - X = (X^{p^{q^{d-1}}} - X)P_1 \ldots P_M$$

L'égalité des degrés donne

$$M = \frac{p^{q^d} - p^{q^{d-1}}}{q^d}$$