

G04. Théorie de Galois

Épreuve du 14 décembre 2005. Texte et corrigé.

Durée : 4 heures. Sans documents.

Les trois exercices sont indépendants. Voici un barème probable : 5 ; 5 ; 7 ; 5 .

1. - Question de cours. Démontrer l'un, au choix, des résultats suivants :

- 1) Une extension de décomposition d'un polynôme séparable est une extension galoisienne.
- 2) Existence d'une base normale lorsque le corps de base est infini.

2. - Soit K un corps de caractéristique $\neq 2$. Soit a un élément de K tel que le polynôme $P(X) = X^4 + aX^2 + 1$ soit irréductible dans $K[X]$.

2.1 Montrer que P est séparable.

Comme la caractéristique de K est $\neq 2$, une racine u du polynôme dérivé $P' = 2X(2X^2 + a)$ est soit nulle (mais $P(0) \neq 0$), soit elle vérifie la relation $u^2 = -a/2$; si c'était une racine de P , on aurait $a^2/4 - a.a/2 + 1 = 0$, d'où $a^2 = 4$, c'est-à-dire $a = \pm 2$; mais alors on aurait $P(X) = (X^2 \pm 1)^2$, et ce polynôme est réductible.

2.2 On désigne par x la classe de X dans $L = K[X]/(P)$. Montrer que l'extension $K \subset L$ est galoisienne et déterminer son groupe de Galois (On exprimera les racines de P en fonction de x , en remarquant que ce polynôme est « réciproque »).

Les racines de P dans L sont $x, -x, 1/x, -1/x$; par suite, L est une extension de décomposition du polynôme séparable P ; c'est donc une extension galoisienne de K . Deux automorphismes σ et τ sont apparents, définis par : $\sigma(x) = -x$, et $\tau(x) = 1/x$. Ils sont d'ordre 2 et commutent. Le groupe de Galois est donc le produit direct de deux groupes d'ordre 2.

2.3 Décrire toutes les extensions intermédiaires entre K et L , en donnant pour chacune d'elles un générateur et son polynôme minimal.

Le groupe de Galois possède trois sous-groupes non triviaux engendrés respectivement par, σ, τ et $\sigma\tau$. Il est clair que $L^\sigma = K(x^2)$, et que le polynôme minimal de x^2 est $Y^2 + aY + 1$.

L'élément $x + 1/x$ est invariant par τ ; on a $(x + 1/x)^2 = 2 - a$; si $2 - a$ était un carré dans K , soit $2 - a = b^2$, on aurait $x^2 \pm bx + 1 = 0$, ce qui est impossible puisque x est de degré 4; donc $x + 1/x$ est de degré 2 sur K , et, par suite, $L^\tau = K(x + 1/x)$, et le polynôme minimal de $x + 1/x$ est $Y^2 + a - 2$.

Par le même raisonnement, on voit que $L^{\sigma\tau} = K(x - 1/x)$, et que le polynôme minimal de $x - 1/x$ est $Y^2 + a + 2$.

3. - Pour tout entier $n \geq 1$, on note R_n l'extension cyclotomique de niveau n , c'est-à-dire le sous-corps $\mathbb{Q}(\mu_n) \subset \mathbb{C}$ engendré par les racines n -ièmes de l'unité (dans cet exercice, on abrège $\mu_n(\mathbb{C})$ en μ_n). L'exercice conduit au résultat suivant : pour deux entiers a et b tels que $1 \leq a \leq b$, on a $R_a = R_b$ si et seulement si $a = b$, ou bien a est impair et $b = 2a$.

L'indicateur d'Euler $\varphi(n)$ sera utile; c'est, rappelons-le, le cardinal du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, et par suite, c'est aussi le cardinal de l'ensemble μ'_n des racines primitives n -ièmes de l'unité

dans C. Si la décomposition de n en facteurs premiers s'écrit

$$n = \prod_{p|n} p^{v_p(n)}, \quad \text{alors} \quad \varphi(n) = \prod_{p|n} p^{v_p(n)-1} (p-1).$$

3.1 Soit $a \geq 1$ un entier impair. Montrer que $R_a = R_{2a}$.

Si on se souvient que $\Phi_{2a}(X) = \Phi_a(-X)$ puisque a est impair, il est clair que l'application $\zeta \mapsto -\zeta$ établit une bijection de μ'_a sur μ'_{2a} ; cela implique l'égalité demandée $R_a = R_{2a}$. Voici comment on peut établir directement cette bijection. L'unique racine primitive d'ordre 2 est -1 ; si ζ est primitive d'ordre impair a , $(-1).\zeta$ est donc primitive d'ordre $2a$. Réciproquement, soit $\eta \in \mu'_{2a}$; écrivons $a = 2b + 1$, de sorte que $\eta = \eta^a \eta^{-2b}$; l'ordre de η^a est égal à 2, donc $\eta^a = -1$; de plus, $\text{ord}(\eta^2) = a$, donc $\text{ord}(\eta^{-2}) = a$ et aussi $\text{ord}(\eta^{-2b}) = a$ puisque a et b sont premiers entre eux.

Les questions 3.2 et 3.3 ne sont pas utilisées dans la suite, si ce n'est pour mettre en garde contre des tentatives de démonstrations trop simplistes de 3.5.

3.2 Calculer $\varphi(77)$ et $\varphi(61)$. Les groupes $(\mathbf{Z}/77\mathbf{Z})^\times$ et $(\mathbf{Z}/61\mathbf{Z})^\times$ sont-ils isomorphes ?

On a $\varphi(77) = \varphi(7)\varphi(11) = 6.10$; comme 61 est premier $\varphi(61) = 60$. Les deux groupes ne sont cependant pas isomorphes car, d'après le théorème chinois, le premier est isomorphe au produit des deux groupes cycliques $(\mathbf{Z}/7\mathbf{Z})^\times \times (\mathbf{Z}/11\mathbf{Z})^\times$, d'ordres respectifs 6 et 10; comme ces ordres ne sont pas premiers entre eux, le produit n'est pas un groupe cyclique, alors que $(\mathbf{Z}/61\mathbf{Z})^\times$ est un groupe cyclique.

3.3 Montrer que les groupes $(\mathbf{Z}/15\mathbf{Z})^\times$ et $(\mathbf{Z}/16\mathbf{Z})^\times$ sont isomorphes.

Le premier, isomorphe au produit $(\mathbf{Z}/3\mathbf{Z})^\times \times (\mathbf{Z}/5\mathbf{Z})^\times$, est le produit d'un groupe d'ordre 2 par un groupe cyclique d'ordre 4; le second est (supposé) connu pour être le produit du groupe $\{\pm 1\}$ par le groupe cyclique engendré par la classe de 5, laquelle est d'ordre 4 puisque $5^2 \equiv 9 \pmod{16}$, d'où $5^4 \equiv 81 = 5.16 + 1 \equiv 1 \pmod{16}$. On peut aussi vérifier directement que dans le groupe multiplicatif $(\mathbf{Z}/16\mathbf{Z})^\times$ les classes de 3 et de 7 engendrent respectivement des groupes d'ordre 4 et 2, et dont l'intersection est 1; cela donne la décomposition en produit cherchée.

3.4 Soient a et a_0 deux entiers ≥ 1 tels que $\varphi(aa_0) = \varphi(a)$. Montrer que $a_0 = 1$, ou bien $a_0 = 2$ et a est impair (On peut écrire $a_0 = a_1 a_2$, où chaque diviseur premier de a_1 divise a , et où a_2 est étranger à a ; vérifier que $\varphi(aa_0) = \varphi(a)a_1\varphi(a_2)$).

La décomposition est claire. L'égalité $a_1\varphi(a_2) = 1$ implique d'abord que $a_1 = 1$, c'est-à-dire que a et a_0 sont premiers entre eux, et ensuite que $\varphi(a_2) = 1$ ce qui n'a lieu que si $a_2 = 1$, ou si $a_2 = 2$, mais alors a doit être impair.

3.5 Soient deux entiers a et b tels que $1 \leq a \leq b$, et $R_a = R_b$. On désigne par c le ppcm de a et b ; montrer que $\mu_a \mu_b = \mu_c$; en déduire que $R_a = R_b = R_c$. Conclure.

L'ensemble P des diviseurs premiers de c (c'est-à-dire de a et de b) peut être décomposé en la réunion de deux parties disjointes $P = P' \cup P''$, en prenant pour P' l'ensemble des p tels que $v_p(a) \geq v_p(b)$, et pour P'' les autres. En posant

$$a' = \prod_{p \in P'} p^{v_p(a)}, \quad \text{et} \quad b' = \prod_{p \in P''} p^{v_p(b)},$$

on voit que $c = a'b'$, $a'|a$, $b'|b$ et que a' et b' sont premiers entre eux. Soit ζ et η des racines primitives d'ordre respectivement a et b ; $\zeta^{a/a'}$ et $\eta^{b/b'}$ sont d'ordre a' et b' , lesquels sont premiers entre eux, donc le produit est d'ordre $a'b' = c$. Cela montre l'égalité $\mu_a \mu_b = \mu_c$; elle implique $R_a = R_b = R_c$.

L'irréductibilité sur $\mathbf{Q}$ des polynômes cyclotomiques entraîne, via l'égalité des degrés, que l'on a $\varphi(a) = \varphi(b) = \varphi(c)$. Comme $a|c$ et $b|c$, on peut utiliser 3.4, et en déduire que $a = c$, ou bien a est impair et $c = 2a$; dans le premier cas, comme b divise $c = a$, et que $a \leq b$, on a $a = b$; dans le second cas, on a soit $b = c = 2a$, soit $c = 2b$ mais alors $a = b$.

4. - Détermination d'un élément primitif.

4.1 (Préliminaire) On considère deux extensions finies $K \subset L \subset M$, et un élément $x \in M$. On notera $P_K(X) \in K[X]$ (resp. $P_L(X) \in L[X]$) le polynôme minimal de x relativement à K (resp. à L), et on pose $\deg_K(x) = \deg(P_K)$ et $\deg_L(x) = \deg(P_L)$. Montrer l'équivalence : $\deg_L(x) < \deg_K(x) \iff P_L(X) \notin K[X]$.

Dans $L[X]$, il est toujours vrai que P_L divise P_K puisque $P_K(x) = 0$ et que P_L est le polynôme minimal; considérons les contraposées des propriétés envisagées : la relation $\deg_L(x) \geq \deg_K(x)$ équivaut donc à $P_L = P_K$, et elle entraîne que $P_L \in K[X]$; réciproquement, comme P_K est irréductible dans $K[X]$ et que $P_L|P_K$, si P_L est à coefficients dans K , alors $P_L = P_K$.

Soit $K \subset K(\alpha, \beta) = M$ une extension finie engendrée par deux éléments. On fait les hypothèses suivantes :

- i) L'extension $K \subset K(\alpha) = L$ est galoisienne de degré premier p ;
- ii) $\alpha \notin K(\beta)$;
- iii) L'entier $q = \deg_K(\beta)$ est inversible dans K .

Il s'agit de montrer que $\alpha + \beta$ est un élément primitif pour l'extension $K \subset M$.

4.2 Montrer que l'extension $K(\beta) \subset M$ est de degré p . En déduire que $\deg_L(\alpha + \beta) = q$ (on peut utiliser l'égalité $K(\alpha, \beta) = K(\alpha, \alpha + \beta)$).

L'extension M est composée de $L = K(\alpha)$ et de $K(\beta)$, ce qui conduit au carré commutatif suivant.

$$\begin{array}{ccc} L & \longrightarrow & M \\ \uparrow & & \uparrow \\ K & \longrightarrow & K(\beta) \end{array}$$

Comme $K \rightarrow L$ est galoisienne de degré p , le degré de M sur $K(\beta)$ divise celui, p , de L sur K , et ne peut pas être égal à 1 puisque $\alpha \notin K(\beta)$; il est donc égal à p ; par suite, en calculant des deux façons le degré de M sur K , on trouve $(M : L) = (K(\beta) : K) = q$; mais $M = K(\alpha, \beta) = K(\alpha)(\alpha + \beta)$, donc $\deg_L(\alpha + \beta) = q$.

4.3 Soit $P(X) \in K[X]$ le polynôme minimal de β relativement à K ; montrer que le polynôme $Q(X) = P(X - \alpha) \in L[X]$ est le polynôme minimal de $\alpha + \beta$ relativement à L . En considérant le coefficient de X^{q-1} dans Q vérifier que $Q \notin K[X]$.

On a $Q(\alpha + \beta) = P(\beta) = 0$ et $\deg(Q) = \deg(P) = q = \deg_L(\alpha + \beta)$; donc, Q est le polynôme minimal de $\alpha + \beta$ relativement à L . Si $P(X) = X^q + a_{q-1}X^{q-1} + \dots$, on a $Q(X) = P(X - \alpha) = X^q + (a_{q-1} - q\alpha)X^{q-1} + \dots$. Mais a_{q-1} est dans K , tandis que $\alpha \notin K$; q étant supposé inversible dans K , on voit que $a_{q-1} - q\alpha$ n'est pas dans K .

4.4 Utiliser 4.1 pour montrer que $\deg_K(\alpha + \beta) > q$, et en déduire que $\deg_K(\alpha + \beta) = p.q$.

D'après 4.1, on a $\deg_K(\alpha + \beta) > \deg_L(\alpha + \beta) = q$; or, comme $K(\alpha + \beta)$ est un sous-corps de M , son degré sur K divise $(M : K) = pq$. On en déduit, p étant premier, que $\deg_K(\alpha + \beta) = pq$, donc que $K(\alpha + \beta) = M$.