Partiel Algèbre 2

Responsable : Mr O. DEBARRE

Exercice 1. Montrer que le degré du corps de décomposition d'un polynôme de degré d divise $d!$.

Exercice 2. Soit K un corps de caractéristique $p > 0$ et soit $a \in K$. On pose $P(X) = X^p - X - a$ et on note $K \subset L$ un corps de décomposition de P.

a) Si x est une racine de P dans L, montrer que les racines de P sont $x, x+1, \ldots, x+p-1$.

b) Montrer que P est soit scindé, soit irréductible dans $K[X]$.

c) Si P n'a pas de racine dans K, montrer $\mathrm{Gal}(L/K) \simeq \mathbf{Z}/p\mathbf{Z}$.

Exercice 3. Soit L un corps de décomposition d'un polynôme $P \in K[X]$ *irréductible* séparable. L'extension $K \subset L$ est donc galoisienne ; on suppose que son groupe de Galois est *abélien.* Soit x une racine de P dans L. Montrer $L = K(x)$.

Exercice 4. Considérons le polynôme $P(X) = X^4 - X - 1 \in \mathbf{Q}[X]$.

a) Montrer que P a exactement deux racines réelles distinctes x_1 et x_2.

b) On écrit $(X - x_1)(X - x_2) = X^2 + aX + b$ avec a, $b \in \mathbf{R}$. Montrer $[\mathbf{Q}(a^2) : \mathbf{Q}] = 3$.

c) En déduire qu'aucune des racines de P n'est constructible à la règle et au compas.

Exercice 5. Soient $p_1, \ldots, p_m$ des nombres premiers distincts.

a) Montrer que l'extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m})$ est galoisienne. On note G son groupe de Galois.

b) Montrer que tout élément de G est d'ordre 2. En déduire que G est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^r$ pour un certain entier $r \leq m$.

c) Exprimer en fonction de r le nombre de sous-extensions de $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m})$ de degré 2 sur $\mathbf{Q}$.

d) Montrer que G est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^m$.

e) Le réel $\sqrt{15}$ est-il dans le corps $\mathbf{Q}(\sqrt{10}, \sqrt{42})$?

Exercice 6. Soient K et K' des sous-corps d'un corps L tels que les extensions $K \subset L$ et $K' \subset L$ soient normales. Montrer que l'extension $K \cap K' \subset L$ est aussi normale.

Corrigé du partiel Algèbre 2

Responsable : Mr O. DEBARRE

Exercice 1. *Montrer que le degré du corps de décomposition d'un polynôme de degré d divise $d!$.*

Si le polynôme $P \in K[X]$ est séparable, son corps de décomposition est une extension galoisienne de groupe G et de degré $\mathrm{Card}(G)$. Comme G opère fidèlement sur l'ensemble des d racines de P, il s'identifie à un sous-groupe de $\mathfrak{S}_d$, donc son cardinal divise $d!$.

Si P n'est pas séparable, il faut raisonner autrement, en procédant par exemple par récurrence sur d. Considérons le corps de rupture $K \subset L$ d'un facteur irréductible Q de $P = QR$. Il est de degré $q := \deg(Q)$ et on a $P(X) = (X-a)Q_1(X)R(X)$ dans $L[X]$. Par hypothèse de récurrence, le corps de décomposition L_1 de Q_1 sur L est de degré un diviseur de $(q-1)!$, tandis que le corps de décomposition M de R sur L_1 (qui est un corps de décomposition de P sur K) est de degré sur L un diviseur de $(d-q)!$. On en déduit que le degré de L_1 sur K divise $q!$, puis que le degré de M sur K divise $q!(d-q)!$, donc aussi $d! = q!(d-q)!\binom{d}{q}$.

Exercice 2. *Soit K un corps de caractéristique $p > 0$ et soit $a \in K$. On pose $P(X) = X^p - X - a$ et on note $K \subset L$ un corps de décomposition de P.*

a) Si x est une racine de P dans L, montrer que les racines de P sont $x, x+1, \dots, x+p-1$.

Pour tout $j \in \mathbf{Z}/p\mathbf{Z} \subset K$, on a $j^p = j$ donc $(x+j)^p - (x+j) = x^p + j^p - x - j = a$.

b) Montrer que P est soit scindé, soit irréductible dans $K[X]$.

Si P a une racine dans K, il y est scindé par a). Sinon, on considère une décomposition $P = QR$ en produit de polynômes unitaires dans $K[X]$. Si Q est de degré $d > 0$ et si x est une racine de Q dans $L - K$, son second coefficient est, par a), dx plus un élément de K. Comme $x \notin K$, on a $d = p$. Donc P est irréductible.

c) Si P n'a pas de racine dans K, montrer $\mathrm{Gal}(L/K) \simeq \mathbf{Z}/p\mathbf{Z}$.

Si P n'a pas de racine dans K, il est irréductible dans $K[X]$ par b). Il est aussi séparable (puisque $P'(X) = -1 \neq 0$), donc L est une extension galoisienne de degré p de K. Son groupe de Galois est alors un groupe d'ordre p, donc isomorphe à $\mathbf{Z}/p\mathbf{Z}$ (plus concrètement, un générateur g est défini par $g(x) = x+1$).

Exercice 3. *Soit L un corps de décomposition d'un polynôme $P \in K[X]$* irréductible séparable. *L'extension $K \subset L$ est donc galoisienne ; on suppose que son groupe de Galois est abélien. Soit x une racine de P dans L. Montrer $L = K(x)$.*

Comme le groupe $\mathrm{Gal}(L/K)$ est abélien, son sous-groupe $\mathrm{Gal}(L/K(x))$ est distingué et l'extension $K \subset K(x)$ est galoisienne, donc normale. Comme elle contient une racine du polynôme irréductible P, elle les contient toutes, et $K(x) = L$.

Exercice 4. *Considérons le polynôme $P(X) = X^4 - X - 1 \in \mathbf{Q}[X]$.*

a) Montrer que P a exactement deux racines réelles distinctes x_1 et x_2.

Cela se fait par une étude de fonction.

b) On écrit $(X - x_1)(X - x_2) = X^2 + aX + b$ avec $a, b \in \mathbf{R}$. Montrer $[\mathbf{Q}(a^2) : \mathbf{Q}] = 3$.

Si on écrit $P(X) = (X^2+aX+b)(X^2-aX+c)$ et que l'on identifie les coefficients, on obtient $b = \frac{1}{2}(a^2+1/a)$ et $c = \frac{1}{2}(a^2 - 1/a)$, puis $a^6 + 4a^2 - 1 = 0$. Comme le polynôme $X^3 + 4X - 1$ n'a pas de racine dans $\mathbf{Q}$, il est irréductible dans $\mathbf{Q}[X]$, donc c'est le polynôme minimal de a^2.

c) En déduire qu'aucune des racines de P n'est constructible à la règle et au compas.

Comme $a \notin \mathbf{Q}$, le polynôme P est irréductible sur $\mathbf{Q}$. C'est donc le polynôme minimal de chacune de ses racines. Si l'une d'elles est constructible, le cours nous apprend qu'elles le sont toutes, donc aussi $a^2 = (x_1+x_2)^2$. Mais cela contredit un résultat du cours, puisque par b), a^2 n'est pas de degré une puissance de 2 sur $\mathbf{Q}$.

Exercice 5. *Soient $p_1, \dots, p_m$ des nombres premiers distincts.*

a) Montrer que l'extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m})$ *est galoisienne.*

Cette extension est le corps de décomposition du polynôme séparable $P(X) := (X^2 - p_1) \cdots (X^2 - p_m)$. Elle est donc galoisienne.

b) Montrer que tout élément de G *est d'ordre 2. En déduire que* G *est isomorphe à* $(\mathbf{Z}/2\mathbf{Z})^r$ *pour un certain entier* $r \leq m$.

Soit g un élément de G. Pour chaque $i \in \{1, \ldots, m\}$, on a $g(\sqrt{p_i})^2 = g(p_i) = p_i$ donc $g(\sqrt{p_i}) = \pm\sqrt{p_i}$. On a donc $g^2 = \mathrm{Id}$. Cela entraîne que G est abélien : pour tout g et tout g' dans G, on a $\mathrm{Id} = (gg')^2 = gg'gg'$, donc $gg' = g(gg'gg')g' = g'g$. D'après le théorème de structure des groupes abéliens finis, G est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^r$ pour un certain r.

Comme $g(\sqrt{p_i}) = \pm\sqrt{p_i}$ pour tout $i \in \{1, \ldots, m\}$, on a d'autre part $\mathrm{Card}(G) \leq 2^m$, donc $r \leq m$.

c) Exprimer en fonction de r *le nombre de sous-extensions de* $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m})$ *de degré 2 sur* $\mathbf{Q}$.

Les sous-extensions de $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m})$ de degré 2 sur $\mathbf{Q}$ correspondent aux sous-groupes d'indices 2 de G, c'est-à-dire aux noyaux des morphismes de groupes surjectifs $G \to \mathbf{Z}/2\mathbf{Z}$. On peut voir ces morphismes comme des formes linéaires non nulles du $\mathbf{F}_2$-espace vectoriel $\mathbf{F}_2^r$. Il y en a donc $\mathrm{Card}((\mathbf{F}_2^r)^*) - 1 = 2^r - 1$.

d) Montrer que G *est isomorphe à* $(\mathbf{Z}/2\mathbf{Z})^m$.

Pour toute partie I *non vide* de $\{1, \ldots, m\}$, notons $p_I = \prod_{i \in I} p_i$. Comme p_i n'est pas un carré, le corps $\mathbf{Q}(\sqrt{p_I})$ est une extension de degré 2 de $\mathbf{Q}$ contenue dans $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m})$. Montrons que ces $2^m - 1$ extensions sont toutes distinctes : si $\sqrt{p_I} = x + y\sqrt{p_J}$, avec $x = a/c$ et $y = b/c$ dans $\mathbf{Q}$ ($c \neq 0$), on a $p_I c^2 = a^2 + 2ab\sqrt{p_J} + b^2 p_J$, donc $2ab = 0$. Comme $b = 0$ est impossible, on a $a = 0$ et $p_I c^2 = b^2 p_J$, ce qui, par unicité de la décomposition en facteurs irréductibles, entraîne $I = J$.

En combinant cela avec le résultat de c), on obtient $2^m - 1 \leq 2^r - 1$, soit $m \leq r$. Comme $r \leq m$, on a égalité. Cela entraîne que pour chaque $\varepsilon_1, \ldots, \varepsilon_m \in \{-1, 1\}$, il existe $g \in G$ tel que $g(\sqrt{p_i}) = \varepsilon_i\sqrt{p_i}$ pour chaque $i \in \{1, \ldots, m\}$.

e) Le réel $\sqrt{15}$ *est-il dans le corps* $\mathbf{Q}(\sqrt{10}, \sqrt{42})$ *?*

D'après ce qu'on a vu en d), la sous-extension $\mathbf{Q}(\sqrt{10}, \sqrt{42})$ de $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$ est de degré 4 sur $\mathbf{Q}$, de groupe de Galois formé des $\mathbf{Q}$-automorphismes $\sqrt{10} \mapsto \pm\sqrt{10}$, $\sqrt{42} \mapsto \pm\sqrt{42}$. Elle a donc 3 sous-extensions propres : $\mathbf{Q}(\sqrt{10})$, $\mathbf{Q}(\sqrt{42})$ et $\mathbf{Q}(\sqrt{420}) = \mathbf{Q}(\sqrt{105})$. Celles-ci sont toutes distinctes de $\mathbf{Q}(\sqrt{15})$ par d), donc $\sqrt{15} \notin \mathbf{Q}(\sqrt{10}, \sqrt{42})$.

Exercice 6. *Soient* K *et* K' *des sous-corps d'un corps* L *tels que les extensions* $K \subset L$ *et* $K' \subset L$ *soient normales. Montrer que l'extension* $K \cap K' \subset L$ *est aussi normale.*

Soit $P \in (K \cap K')[X]$ un polynôme irréductible qui a une racine dans L. On l'écrit $P(X) = Q(X) \prod_{i=1}^{n} (X - a_i)$, où $a_1 \in K \cap K'$ et $a_i \in L$, et où $Q \in L[X]$ n'a aucune racine dans L. Cette décomposition est unique et il s'agit de montrer que Q est constant. Considérons la factorisation irréductible de P dans $K[X]$. Si un facteur irréductible a une racine dans L, il est scindé dans $L[X]$ (par normalité de l'extension $K \subset L$) ; on écrit ainsi P comme produit d'un polynôme de $K[X]$ scindé dans $L[X]$ et d'un polynôme sans racine dans L. Par unicité de la décomposition ci-dessus, on obtient $Q \in K[X]$ et de la même façon, $Q \in K'[X]$, c'est-à-dire que Q est dans $(K \cap K')[X]$. Comme P est irréductible dans $(K \cap K')[X]$, le polynôme Q est constant.

Si on ajoute l'hypothèse que l'extension $K \cap K' \subset L$ est finie et séparable (de sorte que les extensions $K \subset L$ et $K' \subset L$ ont les mêmes propriétés), on peut donner une démonstration utilisant la théorie de Galois. Posons $G := \mathrm{Gal}(L/K)$ et $G' := \mathrm{Gal}(L/K')$. Alors $K \cap K'$ est le corps fixe du groupe d'automorphismes H de L engendré par G et G'. Par le lemme d'Artin, il suffit de montrer que ce groupe H est fini. Or l'extension $K \cap K' \subset L$ étant finie et séparable est engendrée par un élément a (« théorème de l'élément primitif »), de polynôme minimal $P \in (K \cap K')[X]$. Tout h dans H est uniquement déterminé par $h(a)$, qui est une racine de P, donc H est fini (on peut aussi utiliser l'exercice II.6.29 du poly).