Université Paris 7-Denis Diderot — Algèbre – Année 2006-07
M1 mathématiques

Feuille d'exercices 8

Corps

Exercice 1

Soit $\sqrt{2}+\sqrt{3} \in \mathbf{R}$.

1. Montrer que c'est un élément algébrique sur $\mathbf{Q}(\sqrt{6})$.
2. En déduire que c'est un élément algébrique sur $\mathbf{Q}$.
3. Quel est le degré de $\sqrt{2}+\sqrt{3}$ sur $\mathbf{Q}$?

Exercice 2

Soit K un corps. Soit L une extension finie de K de degré impair. Soit $\alpha \in L$ tel que $L = K(\alpha)$.

1. Notons P le polynôme minimal de α. Montrer que P est de degré impair.
2. Montrer qu'il existe Q, $R \in K[X]$ tels que $P = XQ(X^2) + R(X^2)$. En déduire qu'il existe $F \in K(X)$ tel que $\alpha = F(\alpha^2)$.
3. Montrer que $K(\alpha) = K(\alpha^2)$.

Exercice 3

Posons $P = X^6 + X^3 + 1 \in \mathbf{Q}[X]$. Soit α une racine de P dans $\mathbf{C}$. Soit ϕ un plongement $\mathbf{Q}(\alpha)$ dans $\mathbf{C}$.

1. Montrer que P divise $X^9 - 1$. En déduire que $\phi(\alpha)^9 = 1$ et que $\phi(\alpha)^3 \neq 1$.
2. Donner toutes les possibilités pour $\phi(\alpha)$.
3. Soient ϕ_1 et ϕ_2 deux plongements de $\mathbf{Q}(\alpha)$ dans $\mathbf{C}$. Montrer que si $\phi_1(\alpha) = \phi_2(\alpha)$ on a $\phi_1 = \phi_2$.
4. Combien y a-t-il de plongements de $\mathbf{Q}(\alpha)$ dans $\mathbf{C}$.
5. Quel est le degré d'un corps de rupture de P sur $\mathbf{Q}$?
6. Déterminer un corps de décomposition de P. Quel est son degré sur $\mathbf{Q}$?

Exercice 4

Soit K un corps. On identifie K à un sous-corps de $K(X)$.

1. Montrer que $X \in K(X)$ est transcendant sur K.
2. Soient P, $Q \in K[X]$ de degré $d > 0$ et $e > 0$ respectivement. Quel est le degré de $P \circ Q$? $P \circ Q$ peut-il être nul ?
3. Montrer que les seuls éléments algébriques de $K[X]$ sont les éléments de K.
4. Soit L une extension de K. Soit $t \in L$ un élément transcendant sur K. Démontrer que L contient un sous-corps isomorphe à $K(X)$.

Exercice 5

Notons $\mathbf{Q}(i)$ le sous-corps de $\mathbf{C}$ engendré par i. Notons $\bar{\mathbf{Q}}$ la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$. Notons $\bar{\mathbf{Q}}^r = \bar{\mathbf{Q}} \cap \mathbf{R}$.

1. Démontrer que tout élément de $\mathbf{C}$ est algébrique sur $\mathbf{R}$.
2. Démontrer que tout élément de $\mathbf{C}$ algébrique sur $\mathbf{Q}(i)$ est algébrique sur $\mathbf{Q}$.
3. Soit α une racine cubique de 2 dans $\mathbf{C}$ qui n'est pas réelle. Quel est le degré de l'extension $\bar{\mathbf{Q}}^r(\alpha)|\bar{\mathbf{Q}}^r$?
4. L'extension $\bar{\mathbf{Q}}|\bar{\mathbf{Q}}^r$ est-elle quadratique ? Est-elle finie ?

Exercice 6

Soit K un corps. On note $K[[T]]$ l'ensemble des suites à valeurs dans K. La suite $(u_n)_{n\geq 0}$ est notée $\sum_{n=0}^{\infty} u_n T^n$.

1. Montrer que l'addition et la multiplication des polynômes de $K[T]$ s'étend à $K[[T]]$, faisant ainsi de $K[[T]]$ un anneau intègre.
2. Notons $K((T))$ le corps des fractions de $K[[T]]$. Montrer que c'est une extension de $K(T)$.
3. Montrer qu'on a $\sum_{n=0}^{\infty} T^n = 1/(1-T)$ dans $K((T))$. En déduire que $K(T) \cap K[[T]] \neq K[T]$.
4. Soit I un idéal de $K[[T]]$. En considérant un élément $F \in I$ dont le plus petit terme non nul est de degré minimal parmi les éléments de I, montrer que I est principal et engendré par F. Montrer que tout idéal de $K[[T]]$ est de la forme (T^k) avec k entier ≥ 0.
5. Montrer que (T) est l'unique idéal maximal de $K[[T]]$ et que $K[[T]]^* = K[[T]] - (T)$.
6. Montrer que le polynôme $X^k - (T+1)$ est irréductible sur $K(T)$. Quel est le degré de l'extension $K(T)[X]/(X^k - (T+1))|K(T)$?
7. Supposons dsormais K de caractéristique 0. Considérons $U_k = \sum_{n=0}^{\infty} u_n T^n/n! \in K[[T]]$ tel que $u_0 = 1$, $u_1 = 1/k$, $u_2 = 1/k(1/k-1)$... $u_n = 1/k(1/k-1)...(1/k-n+1)$.... Montrer que U_k est une racine de $X^k - (T+1)$. Quel est le degré de l'extensioin $K(T)(U_k)|K(T)$?
8. En déduire que l'extension $K((T))|K(T)$ n'est pas finie.

Exercice 7

Notons $\bar{\mathbf{Q}}$ le sous-corps de $\mathbf{C}$ formé par les éléments algébriques sur $\mathbf{Q}$.

1. Montrer qu'il existe une application $\bar{\mathbf{Q}} \to \mathbf{Z}[X]$ telle que l'image réciproque de tout élément soit finie.
2. On dit qu'un ensemble E est *dénombrable* s'il existe une application injective $E \to \mathbf{N}$. On pourra essayer de montrer qu'il existe des nombres transcendants dans $\mathbf{R}$ en utilisant les faits suivants : *(i)* $\mathbf{Z}[X]$ est dénombrable, *(ii)* $\mathbf{R}$ n'est pas dénombrable et *(iii)* si E est un ensemble dénombrable et s'il existe une application $F \to E$ telle que l'image réciproque de tout élément de E est finie, l'ensemble F est dénombrable.

Exercice 8

Considérons le polynômes $X^4 - 3 \in \mathbf{Q}[X]$.

1. Ce polynôme est-il irréductible sur $\mathbf{Q}$?
2. En déterminer un corps de rupture dans $\mathbf{R}$. Quel est son degré ?
3. Ce polynôme admet-il un corps de décomposition dans $\mathbf{R}$?

Exercice 9

Soit $\mathbf{F}_q$ un corps fini à q éléments, où q est impair.

1.Montrer que l'application $\mathbf{F}_q^* \to \mathbf{F}_q^*$ qui à x assoxie x^2 est un homomorphisme de groupes dont le noyau a 2 éléments. En déduire qu'il y a $(q-1)/2$ carrés parfaits dans $\mathbf{F}_q^*$.
2. Soit $a \in \mathbf{F}_q$. Montrer que les ensembles $\{x^2/x \in \mathbf{F}_q\}$ et $\{a - y^2/y \in \mathbf{F}_q\}$ ont chacun $(q+1)/2$ éléments.
3. En déduire que tout élément de $\mathbf{F}_q$ est somme de deux carrés.

Exercice 10

Soit $\mathbf{F}_q$ un corps fini à q éléments. Soit $P \in \mathbf{F}_q[X]$ un polynôme irréductible de degré d distinct de X.

1. Montrer que P est sans racine multiple dans une clôture algébrique $\bar{\mathbf{F}}_q$ de $\mathbf{F}_q$.
2. Montrer que les racines de P dans $\bar{\mathbf{F}}_q$ sont des racines de l'unité. Plus précisément que P divise $X^{q^d-1} - 1$ dans $\mathbf{F}_q[X]$.
3. Montrer que tout corps de rupture de P est un corps de décomposition.
4. Montrer que tout polynôme irréductible de $\mathbf{F}_q[X]$ et de degré divisant d divise $X^{q^d} - X$.
5. Montrer que le polynôme $X^{q^d} - X$ est sans racine multiple. En déduire la formule

$$\prod_Q Q = X^{q^d} - X,$$

où Q parcourt les polynômes unitaires, irréductibles de $\mathbf{F}_q[X]$ et de degré divisant d.
6. Notons i_n le nombre de polynômes irréductibles de degré n de $\mathbf{F}_q[X]$. Établir la formule

$$\sum_{d|n} di_d = q^n.$$

Exercice 11

Soit n un entier ≥ 1. Posons $P_n = X^{2^n} + X + 1 \in \mathbf{F}_2[X]$. Fixons $\bar{\mathbf{F}}_2$ une clôture algébrique de $\bar{\mathbf{F}}_2$. Pour t entier ≥ 1, on note $\mathbf{F}_{2^t}$ le sous-corps à 2^t éléments de $\bar{\mathbf{F}}_2$. Soit k_n un sous-corps de $\bar{\mathbf{F}}_2$ qui est un corps de décomposition de P_n sur $\mathbf{F}_2$. Notons E_n l'ensemble des racines de P_n dans k_n.

1. Démontrer que P_n n'a pas de racine multiple. Quel est le cardinal de E_n ?
2. Soient α_n, $\alpha'_n \in E_n$. Démontrer que $x = \alpha_n - \alpha'_n$ vérifie $x^{2^n} + x = 0$. En déduire que $x \in \mathbf{F}_{2^n}$.
3. Démontrer que $\alpha_n^{2^n} + \alpha_n \neq 0$. En déduire que α_n n'appartient pas à $\mathbf{F}_{2^n}$.
4. Démontrer que $\alpha_n^{2^{2n}} + \alpha_n = 0$. En déduire que α_n appartient à $\mathbf{F}_{2^{2n}}$.
5. En déduire que $E_n = \{\alpha_n + x / x \in \mathbf{F}_{2^n}\}$, puis que $k_n = \mathbf{F}_{2^{2n}}$.
6. Démontrer que le polynôme P_n divise le polynôme $X^{2^{2n}} + X$ dans $\mathbf{F}_2[X]$.
7. Quels sont les degrés des extensions $\mathbf{F}_{2^{2n}}|\mathbf{F}_{2^n}$ et $\mathbf{F}_{2^{2n}}|\mathbf{F}_2$?
8. Démontrer que tout polynôme irréductible divisant P_n est de degré divisant $2n$ mais ne divisant pas n.
9. Supposons que $n = 2^k$ avec k entier ≥ 0. Montrer que tous les facteurs irréductibles de P_n sont de degré 2^{k+1}. Combien y en a-t-il ?
10. Démontrer que le polynôme P_{2^k} admet $\mathbf{F}_{2^{2^{k+1}}}$ comme corps de rupture et de décomposition (autrement dit $\mathbf{F}_{2^{2^{k+1}}}$ est engendré par l'une quelconque des racines de P_{2^k}).

Exercice 12

Soit K un corps de caractéristique $\neq 2$. Soit $\bar{K}$ une clôture algébrique de K. Posons $K_0 = K$, K_1 le sous-corps de $\bar{K}$ engendré par les éléments de degré 2 sur K_0, ..., K_n le sous-corps de $\bar{K}$ engendré par les éléments de degré 2 sur K_{n-1}..... Posons $\bar{K}^{(2)} = \cup_{n\geq 0} K_n$.

1. Soit $L|K$ une extension de corps de degré 2 (on parle d'extension quadratique). Démontrer qu'il existe $a \in L$ tel que $A = a^2 \in K$ et $K(a) = L$. On écrit alors $L = K(\sqrt{A})$.
2. Démontrer que si K est un corps fini, on a $K(\sqrt{A}) = K(\sqrt{B})$ (A, $B \in K$).
3. Démontrer que l'extension $K_n|K$ est algébrique.
4. Démontrer que $\bar{K}^{(2)}$ est un corps. On l'appelle la *clôture quadratique* de K dans $\bar{K}$.
5. Démontrer qu'il n'existe pas d'extension de degré 2 de $\bar{K}^{(2)}$.
6. Lorsque K est le corps fini $\mathbf{F}_p$, montrer que les éléments non nuls de $\bar{K}^{(2)}$ sont les racines $p^{2^n} - 1$-èmes de l'unité lorsque n varie parmi les entiers ≥ 0.
7. La clôture quadratique de $\mathbf{Q}$ coïncide-t-elle avec sa clôture algébrique ?

Exercice 13

Soit $\bar{\mathbf{Q}}$ l'ensemble des nombres algébriques dans $\mathbf{C}$. Soit $\alpha \in \bar{\mathbf{Q}}$. On dit que α est *totalement réel* (resp. *totalement imaginaire*) si pour tout plongement ϕ de $\mathbf{Q}(\alpha)$ dans $\mathbf{C}$, on a $\phi(\alpha) \in \mathbf{R}$ (resp. $\phi(\alpha) \notin \mathbf{R}$). On dit que α est *totalement positif* si de plus $\phi(\alpha) \geq 0$ pour tout ϕ.

1. Montrer que l'ensemble des nombres algébriques totalement réels est un sous-corps $\bar{\mathbf{Q}}^{\mathbf{R}}$ de $\bar{\mathbf{Q}}$.
2. Démontrer que les nombres rationnels sont totalement réels. Lesquels des nombres suivants sont totalement réels : $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt{2+\sqrt{2}}$, $1+\sqrt{2}$, $2+\sqrt{2}$. Lesquels sont totalement positifs ?
3. Soit $L = \bar{\mathbf{Q}}^{\mathbf{R}}(\sqrt{A})$ un sous-corps de $\mathbf{C}$ qui est une extension quadratique de $\bar{\mathbf{Q}}^{\mathbf{R}}$, avec $A \in \mathbf{R}$. Montrer que si A est totalement positif L est totalement réel. En déduire que A n'est pas totalement positif.
4. Un sous-corps de $\bar{\mathbf{Q}}$ est dit *totalement réel* si tous ses éléments sont totalement réels. Indiquer des corps quadratique et cubique (i.e. des extensions de $\mathbf{Q}$ de degré 2 et 3 respectivement) qui sont totalement réels, puis de tels corps qui ne sont pas totalement réels.
5. Un sous-corps L de $\bar{\mathbf{Q}}$ est dit CM si $L = K(\alpha)$ avec K totalement réel, $L|K$ quadratique et α totalement imaginaire. Lesquels des corps suivants sont CM : $\mathbf{Q}(i)$, $\mathbf{Q}(i, \sqrt{2})$, $\mathbf{Q}(\sqrt{1+\sqrt{2}})$?