Travaux Dirigés – Exercices. Série VI

Semaine VII-VIII-IX. 26/11/07 – 08/12/07

A – Polynômes minimaux

1. Déterminer le polynôme minimal sur $\mathbf{Q}$ des nombres complexes suivants : $1+i$, $\sqrt{2}$, $(\sqrt{2}+i\sqrt{2})/2$, $\sqrt{1+\sqrt{2}}$, $e^{2i\pi/9}$, $(1+i\sqrt{3})/2$, $\cos(2\pi/5)$, $(2+\sqrt{2})^{1/3}+(2-\sqrt{2})^{1/3}$.
2. Déterminer le polynôme minimal sur $\mathbf{Q}(i)$ du nombre complexe $e^{i\pi/4}$.
3. Déterminer le polynôme minimal de $\int_{-\infty}^{\infty} e^{-x^2}\,dx$ sur $\mathbf{Q}(\zeta(2))$ où $\zeta(2)=\sum_{n=1}^{\infty} 1/n^2$.

B – Extension biquadratique

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 $\mathbf{Q}$. Quel est son polynôme minimal sur $\mathbf{Q}$?
3. Quel est le degré de $\sqrt{2}+\sqrt{3}$ sur $\mathbf{Q}$?
4. Montrer que $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ est une base du corps $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ sur $\mathbf{Q}$.
5. Soient ϵ_2, $\epsilon_3 \in \{-1, 1\}$. Montrer que l'application $a_1+a_2\sqrt{2}+a_3\sqrt{3}+a_6\sqrt{6} \mapsto a_1+\epsilon_2 a_2\sqrt{2}+\epsilon_3 a_3\sqrt{3}+\epsilon_2\epsilon_3 a_6\sqrt{6}$ $(a_1, a_2, a_3, a_6 \in \mathbf{Q})$ est un automorphisme du corps $\mathbf{Q}(\sqrt{2}, \sqrt{3})$.
6. Combien y a-t-il de plongements de $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ dans $\mathbf{C}$?

C – Extensions de degré impair

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 $K(\alpha) = K(\alpha^2)$.

D – Racines neuvièmes de l'unité dans $\mathbf{C}$

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. Déterminer un corps de décomposition de P. Quel est son degré sur $\mathbf{Q}$?

E – Éléments algébriques et transcendants sur K dans $K(X)$

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 sur K 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 $K(X)$.
5. Soit $F \in K(X)$, $F \notin K$. Montrer que $K(X)$ est une extension finie de $K(F)$. En déduire que l'extension $K(F)|K$ n'est pas finie.
6. Posons $F = X^3/(1+X)$. Montrer que $K(X)$ est une extension cubique de $K(F)$.

F – Nombres algébriques réels

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 ?

G – Corps de rupture, corps de décomposition

Considérons les polynômes $X^3 - 3X + 1$ et $X^4 - 3 \in \mathbf{Q}[X]$.

1. Ces polynômes sont-il irréductibles sur $\mathbf{Q}$?
2. En déterminer un corps de rupture de $X^4 - 3$ dans $\mathbf{R}$. Quel est son degré ?
3. Ce polynôme admet-il un corps de décomposition dans $\mathbf{R}$?
4. Quel est le degré d'un corps de décomposition de $X^4 - 3$ sur $\mathbf{Q}$?
5. Soit a une racine de $X^3 - 3X + 1$ dans $\mathbf{C}$.
6. Quel est le degré d'un corps de décomposition de $X^3 - 3X + 1$ sur $\mathbf{Q}$?

H – Existence de nombres réels transcendants

Notons $\bar{\mathbf{Q}}$ le sous-corps de $\mathbf{C}$ formé par les éléments algébriques sur $\mathbf{Q}$. On dit qu'un ensemble E est *dénombrable* s'il existe une application injective $E \to \mathbf{N}$.

1. Montrer que $\mathbf{N} \times \mathbf{N}$ est dénombrable.
2. Montrer que si E est un ensemble dénombrable et si $\phi : F \to E$ est une application dont les fibres sont dénombrables, alors F est dénombrable. (Les fibres de ϕ sont les sous-ensembles de F de la forme $\phi^{-1}(\{e\})$ avec $e \in E$.)
3. En déduire que les ensembles suivants sont dénombrables : $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{Q}^n$ (n entier ≥ 0), $\mathbf{Q}[X]$, $\bar{\mathbf{Q}}$.

4. Montrer que $\mathbf{R}$ n'est pas dénombrable. On pourra procéder par l'absurde comme suit (c'est la *diagonale de Cantor*). Soit ϕ une application injective $\mathbf{R} \to \mathbf{N}$. Soit $(a_n)_{n\in\mathbf{N}}$ une suite d'éléments de $\{0,1\}$ telle que a_n est distinct du n-ème chiffre dans l'écriture décimale de $\phi^{-1}(n)$. Considérer alors le nombre réel $A = 0, a_1a_2...$ (écriture décimale).
5. En déduire qu'il existe des nombres réels transcendants.
6. Si $\mathbf{F}$ est un corps fini, montrer que toute clôture algébrique de $\mathbf{F}$ est dénombrable.

I –Sous-corps algébrique du corps des nombres réels

Soit E l'ensemble des sous-corps de $\mathbf{R}$ ne contenant pas $\sqrt{2}$.

1. Montrer que $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{6}) \in E$. Existe-t-il un élément de E contenant ces deux corps ? La réunion des éléments de E forme-t-elle un corps ?
2. Montrer que E est inductif pour la relation d'inclusion.
3. En appliquant le lemme de Zorn, montrer qu'il existe un sous-corps K de $\mathbf{R}$ maximal parmi les éléments de E ne contenant pas $\sqrt{2}$. Le corps K est-il unique ?
4. Soit $x \in \mathbf{R} - K$. Montrer que $\sqrt{2} \in K(x)$. En déduire que x est algébrique sur K. L'extension $\mathbf{R}|K$ est-elle algébrique ?
5. Quel est le polynôme minimal de $\sqrt{2}$ sur K ? Montrer que le polynôme $X^4 - 2$ est irréductible sur K. En déduire qu'on a les inclusions strictes $K \subset K(\sqrt{2}) \subset \mathbf{R}$.
6. Montrer que le polynôme $X^4 - \sqrt{2}$ est irréductible sur $K(\sqrt{2})$. En déduire que qu'on a les inclusions strictes $K \subset K(\sqrt{2}) \subset K(2^{1/4}) \subset \mathbf{R}$. En itérant cette construction montrer que l'extension $\mathbf{R}|K$ n'est pas finie. Est-elle de type fini ?

J – Le corps $K((T))$

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 désormais K de caractéristique 0. Considérons $U_k = \sum_{n=0}^{\infty} u_n T^n/n! \in K[[T]]$ tel que $u_0 = 1$, $u_1 = 1/k$, $u_2 = 1/k(1/k-1), \cdots, u_n = 1/k(1/k-1)...(1/k-n+1)....$ Montrer que U_k est une racine de $X^k - (T+1)$. Quel est le degré de l'extension $K(T)(U_k)|K(T)$?
8. En déduire que l'extension $K((T))|K(T)$ n'est pas finie.

K – Une extension du corps à deux éléments

Soit L un corps contenant $\mathbf{F}_2$. Soient x et y des éléments de L vérifiant $x^2+x+1=0$ et $y^3+y+1=0$.

1. Combien les corps $\mathbf{F}_2(x)$, $\mathbf{F}_2(y)$ et $\mathbf{F}_2(x,y)$ ont-ils d'éléments ?
2. Déterminer le polynôme minimal sur $\mathbf{F}_2$ de $x+y$.
3. Quels sont les ordres de xy et $x+y$ dans $\mathbf{F}_2(x,y)^*$?

L – Somme de deux carrés dans un corps fini

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.

M – Dénombrement des polynômes irréductibles sur les corps finis

Soit $\mathbf{F}_q$ un corps fini à q éléments. Soit $P \in \mathbf{F}_q[X]$ un polynôme irréductible de degré n 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 $X^{q^n-1}-1$ 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 n divise $X^{q^n}-X$.
5. Montrer que le polynôme $X^{q^n}-X$ est sans racine multiple. En déduire la formule
$$\prod_Q Q = X^{q^n} - X,$$
où Q parcourt les polynômes unitaires, irréductibles de $\mathbf{F}_q[X]$ et de degré divisant n.
6. Notons i_d le nombre de polynômes irréductibles unitaires de degré n de $\mathbf{F}_q[X]$. Établir la formule
$$\sum_{d|n} d i_d = q^n.$$
7. Calculer i_3 lorsque $q=5$.
8. Établir la formule, dans $\mathbf{Z}[[X]]$,
$$\prod_P (1 - X^{d^0(P)}) = 1 - qX,$$
où le produit porte sur les polynômes irréductibles unitaires de $\mathbf{F}_q[X]$.

N – Algorithme de Berlekamp

Soit $\mathbf{F}_q$ un corps fini à q éléments. Soit $P \in \mathbf{F}_q[X]$ de degré d. On va mettre au point une méthode pour factoriser P. Posons $A = \mathbf{F}_q[X]/(P)$.

1. Donner un moyen de déterminer les facteurs multiples de P.
2. On suppose maintenant P sans facteur multiple. Posons $P = P_1 P_2 \cdots P_n$, avec $P_1, \cdots, P_n \in \mathbf{F}_q[X]$ irréductibles. Soient A, $B \in \mathbf{F}_q[X]$, montrer qu'on a $A \equiv B \pmod{P}$ si, et seulement si, $A \equiv B \pmod{P_i}$ $(i \in \{1, 2, \cdots, n\})$.
3. Montrer que l'image dans A de $\{Q \in \mathbf{F}_q[X]/Q^q \equiv Q \pmod{P}\}$ est un sous-anneau B de A. C'est l'*algèbre de Berlekamp*. Montrer que les classes modulo P des polynômes constants forment un sous-anneau de B isomorphe à $\mathbf{F}_q$.
4. Soient $i \in \{1, 2, \cdots, n\}$ et $Q \in \mathbf{F}_q[X]$. Montrer qu'on a $Q^q \equiv Q \pmod{P_i}$ si et seulement si il existe $s_i \in \mathbf{F}_q$ tel que P_i divise $Q - s_i$.
5. Soit $Q \in \mathbf{F}_q[X]$ tel que $Q^q \equiv Q \pmod{P}$ et tel que l'image de Q dans B est non constante. Montrer que le pgcd $(P, Q - s)$ de P et $Q - s$ est non trivial pour au moins une valeur de $s \in \mathbf{F}_q$. En déduire la formule
$$P = \prod_{s \in \mathbf{F}_q} (P, Q - s).$$
6. Montrer que P est irréductible si, et seulement si, B ne contient que des éléments constants.
7. Montrer que A est un espace vectoriel sur $\mathbf{F}_q$ de dimension d et que l'élévation à la puissance q dans A est $\mathbf{F}_q$-linéaire. Exprimer B comme le noyau d'une application linéaire sur A dont on écrira la matrice.

O – Corps finis de caractéristique 2

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. Démontrer que $\alpha_n^{2^{2n}} + \alpha_n = 0$. En déduire que α_n appartient à $\mathbf{F}_{2^{2n}}$.
6. En déduire que $E_n = \{\alpha_n + x / x \in \mathbf{F}_{2^n}\}$, puis que $k_n = \mathbf{F}_{2^{2n}}$.
7. Démontrer que le polynôme P_n divise le polynôme $X^{2^{2n}} + X$ dans $\mathbf{F}_2[X]$.
8. Quels sont les degrés des extensions $\mathbf{F}_{2^{2n}} | \mathbf{F}_{2^n}$ et $\mathbf{F}_{2^{2n}} | \mathbf{F}_2$?
9. Démontrer que tout polynôme irréductible divisant P_n est de degré divisant $2n$ mais ne divisant pas n.

10. 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 ?

11. 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}).

P – Clôture quadratique

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 ?

Q – Nombres algébriques totalement réels

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* : $\mathbf{Q}(i)$, $\mathbf{Q}(i, \sqrt{2})$, $\mathbf{Q}(\sqrt{1+\sqrt{2}})$?