Université P. et M. Curie (Paris VI), Michel Waldschmidt
Deuxième semestre 2007/2008

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales MO11 : Théorie des nombres (12 ECTS)

`Seul document autorisé : le polycopié`

Examen du Jeudi 15 Mai 2008
Durée : 3 heures

Exercice 1. Soit $P(X) \in \mathbb{Q}[X]$ un polynôme irréductible unitaire de degré n ; on note K son corps de rupture, L son corps de décomposition, G le groupe de Galois de l'extension $L/\mathbb{Q}$.

(1) Donnez un exemple où $K \neq L$.

(2) En faisant opérer G sur l'ensemble des racines de P, construire un morphisme de G dans le groupe symétrique $\mathfrak{S}_n$ de $\{1, \cdots, n\}$. Pour $n = 6$, l'image de ce morphisme peut-elle être le sous-groupe de $\mathfrak{S}_6$ engendré par la permutation dont la décomposition en cycles à supports disjoints est $(12) \circ (345)$?

(3) Montrez que si $G \simeq \mathbb{Z}/n\mathbb{Z}$, alors $L = K$. La réciproque est-elle toujours vraie ?

(4) Donnez une condition nécessaire et suffisante sur le discriminant D de P, pour que l'image de G par l'isomorphisme précédent soit un sous-groupe du groupe alterné $\mathcal{A}_n$.

(5) On suppose $L \neq K$; le groupe G peut-il être abélien ?

(6) On note $\mathcal{O}_L$ l'anneau des entiers de L. Pour $p \in \mathbb{Z}$ premier, on considère la décomposition $p\mathcal{O}_L = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$ de l'idéal engendré par p en idéaux premiers de $\mathcal{O}_L$.

(i) Montrez que pour tout $g \in G$ il existe un élément σ_g dans le groupe symétrique $\mathfrak{S}_r$ tel que, pour tout $1 \leq i \leq r$, on ait $g(\mathcal{P}_i) = \mathcal{P}_{\sigma_g(i)}$. Montrez que l'application $g \mapsto \sigma_g$ est un morphisme du groupe G dans $\mathfrak{S}_r$.

(ii) Montrez qu'il existe $x \in \mathcal{O}_L$ tel que $x \equiv 0 \mod \mathcal{P}_1$ (c'est-à-dire $x \in \mathcal{P}_1$) et $x \equiv 1 \mod \mathcal{P}_i$ pour tout $i = 2, \ldots, r$.

(iii) Soit $x \in \mathcal{P}_1$. Montrez que $N_{L/K}(x) \in \mathcal{P}_i$ pour tout $i = 2, \ldots, r$.
Soit $i \in \{2, \ldots, r\}$. En utilisant (ii), montrez qu'il existe $g \in G$ tel que $g(\mathcal{P}_i) = \mathcal{P}_1$.
En déduire que l'action de G sur $\{\mathcal{P}_1, \cdots, \mathcal{P}_r\}$ définie en (i) est transitive.

(7) Soit $\mathcal{P}$ un idéal premier de $\mathcal{O}_L$.

(i) Montrez que l'ensemble $D_{\mathcal{P}}$ formé des éléments $g \in G$ tels que $g(\mathcal{P}) = \mathcal{P}$ est un sous-groupe de G.

(ii) Montrez que l'ensemble $I_{\mathcal{P}}$ formé des éléments $g \in D_{\mathcal{P}}$ tels que $g(x) - x \in \mathcal{P}$ pour tout $x \in \mathcal{O}_L$ est un sous-groupe de $D_{\mathcal{P}}$.

(iii) Soit $g \in D_{\mathcal{P}}$. Montrez que l'application $g : \mathcal{O}_L \to \mathcal{O}_L$ induit par passage au quotient un élément du groupe de Galois de $\mathcal{O}_L/\mathcal{P}$ sur $\mathbb{Z}/p\mathbb{Z}$. Montrez que cela définit un morphisme de $D_{\mathcal{P}}$ dans groupe de Galois du corps $\mathcal{O}_L/\mathcal{P}$ sur $\mathbb{Z}/p\mathbb{Z}$. Quel est le noyau de ce morphisme ?

Exercice 2. Soit $\omega = i\sqrt{17}$ et $K = \mathbb{Q}(\omega)$.

(1) Quel est l'anneau des entiers $\mathcal{O}_K$ de K ?
Quels sont les éléments de $\mathcal{O}_K$ dont la norme (sur $\mathbb{Q}$) est positive et < 17 ?
(2) Calculez la constante de Minkowski M_K de $K/\mathbb{Q}$ ainsi que son discriminant.
(3) Montrez que $2\mathcal{O}_K = \mathcal{P}_2^2$ avec $\mathcal{P}_2 = \langle 2, 1+\omega \rangle$.
(4) Montrez que $3\mathcal{O}_K = \mathcal{P}_{3,+}\mathcal{P}_{3,-}$ avec $\mathcal{P}_{3,+} = \langle 3, \omega+1 \rangle$ et $\mathcal{P}_{3,-} = \langle 3, \omega-1 \rangle$.
(5) Déduisez de ce qui précède que le nombre de classe h_K de K est ≤ 4, > 1 et divisible par 2.
(6) Montrez que le groupe de classes de $\mathcal{O}_K$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ et donnez-en un générateur.
(7) Donnez la liste de tous les idéaux de $\mathcal{O}_K$ de norme 18.
(8) Donnez toutes les factorisations en irréductibles dans $\mathcal{O}_K$ de 18.

Exercice 3. On rappelle les définitions des fonctions arithmétiques ω (nombre de diviseurs premiers), μ (Möbius), τ (nombre de diviseurs) et φ (indicatrice d'Euler),

$$\omega(n) = \sum_{p|n} 1, \qquad \mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{si } n \text{ est sans facteur carré,} \\ 0 & \text{sinon,} \end{cases}$$

$$\tau(n) = \sum_{d|n} 1, \qquad \varphi(n) = \sum_{\substack{1 \leq k \leq n \\ \operatorname{pgcd}(k,n)=1}} 1.$$

Quelles sont les fonctions arithmétiques $\tau \star \mu$, et $\varphi \star \tau$?

Université P. et M. Curie (Paris VI), Michel Waldschmidt
Deuxième semestre 2007/2008

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales MO11 : Théorie des nombres (12 ECTS)

Examen du Jeudi 15 Mai 2008
Corrigé

Solution exercice 1.

(1) Il y a beaucoup de réponses valables. On peut prendre un polynôme avec une racine réelle et d'autres complexes, par exemple X^3-2 qui est irréductible car d'Eisenstein pour $p=2$.

(2) Le groupe de Galois permute les racines du polynôme. De plus cette action est transitive (le polynôme étant irréductible, les racines sont conjuguées sur $\mathbb{Q}$). Le sous-groupe de $\mathfrak{S}_6$ d'ordre 6 engendré par la permutation dont la décomposition en cycles à supports disjoints est $(12)\circ(345)$ n'est pas transitif (l'image de 1 n'est jamais 3), donc il ne peut pas être l'image par ce morphisme d'un groupe de Galois.

(3) Comme K est le corps de rupture d'un polynôme irréductible de degré n, son degré sur $\mathbb{Q}$ est n. L'ordre du groupe de Galois est $[L:\mathbb{Q}]$, donc il est égal à n si et seulement si $K=L$. Un exemple avec $L=K$ et $G\neq\mathbb{Z}/n\mathbb{Z}$ est donné par n'importe quelle extension galoisienne non cyclique. On peut prendre le corps de décomposition de X^3-2 sur $\mathbb{Q}$ (on prend pour P le polynôme irréductible d'un élément primitif, par exemple celui de $j+\sqrt[3]{2}$), ou bien une extension cyclotomique $\mathbb{Q}(\zeta_m)$ avec m tel que $(\mathbb{Z}/m\mathbb{Z})^\times$ ne soit pas cyclique, par exemple $m=15$, ou encore $m=8$.

(4) Une condition nécessaire et suffisante est que D soit un carré de $\mathbb{Q}$, puisque l'action de G sur D est donnée par la signature.

(5) Si $L\neq K$, alors L possède une sous-extension non galoisienne sur $\mathbb{Q}$, à savoir K, donc G possède un sous-groupe non distingué. Par conséquent G n'est pas abélien.

(6-i) Pour tout $g\in G$ et $1\leq i\leq r$, $g(\mathcal{P}_i)$ est un idéal de $\mathcal{O}_L$ qui contient $p\mathcal{O}_L$; il est en outre maximal, donc égal à un $\mathcal{P}_j$. Par ailleurs comme g est bijectif, g induit une permutation des $\mathcal{P}_i$, d'où l'existence de σ_g. Le fait que σ soit un homomorphisme de groupe est immédiat.

(6-ii) L'existence d'un tel x est assurée par le lemme chinois : comme les $\mathcal{P}_i$ sont maximaux, on a $\mathcal{P}_i+\mathcal{P}_j=\mathcal{O}_L$ pour tout $i\neq j$. Précisément, pour tout $i\in\{2,\dots,r\}$, on a

$$\mathcal{O}_L=\mathcal{P}_i+\mathcal{P}_1\prod_{j\geq 2,\ j\neq i}\mathcal{P}_j,$$

ce qui fait que le morphisme canonique

$$\mathcal{O}_L \to \mathcal{O}_L/\mathcal{P}_i \times \mathcal{O}_L/\mathcal{P}_1 \prod_{j\geq 2,\, j\neq i} \mathcal{P}_j$$

est surjectif de noyau $\mathcal{P}_1 \prod_{i\geq 2} \mathcal{P}_i$; on conclut par récurrence.

(6-iii) La norme $N_{L/K}(x) = \prod_{g\in G} g(x)$ de x appartient à $\mathcal{O}_L$ et à $\mathcal{P}_1$, donc à $p\mathcal{O}_L$ et par conséquent à $\mathcal{P}_i$ pour tout i. Soit $i \geq 2$. Comme $\mathcal{P}_i$ est premier, il existe $g \in G$ tel que $g(x) \in \mathcal{P}_i$; donc $x \in g^{-1}(\mathcal{P}_i)$. Mais $g^{-1}(\mathcal{P}_i)$ est l'un des idéaux $\mathcal{P}_1, \ldots, \mathcal{P}_r$. Si on a choisi $x \notin \mathcal{P}_j$ pour $2 \leq j \leq r$, comme nous l'y autorise la question (ii), on en déduit , $g^{-1}(\mathcal{P}_i) = \mathcal{P}_1$, i.e. l'un des conjugués de $\mathcal{P}_i$ est égal à $\mathcal{P}_1$.

(7-i) Pour g_1 et g_2 dans $D_{\mathcal{P}}$ on a $g_1 \circ g_2(\mathcal{P}) = g_1(\mathcal{P}) = \mathcal{P}$.

(7-ii) Pour $x \in \mathcal{O}_L$ et g_1, g_2 dans $I_{\mathcal{P}}$ on a

$$g_1 \circ g_2(x) - x = g_1\big(g_2(x) - x\big) + g_1(x) - x \in \mathcal{P}.$$

(7-iii) Un élément de $D_{\mathcal{P}}$ stabilise $\mathcal{O}_L$ et $\mathcal{P}$; par passage au quotient il définit un morphisme du quotient $\mathcal{O}_L/\mathcal{P}$ dans lui-même qui stabilise $\mathbb{Z}/\mathcal{P} \cap \mathbb{Z} = \mathbb{Z}/p\mathbb{Z}$. Le noyau de ce morphisme est $I_{\mathcal{P}}$.

Solution exercice 2.

(1) D'après le cours $\mathcal{O}_K = \mathbb{Z}[\omega]$ car $-17 \equiv 3 \pmod 4$.

Un élément $x + y\omega$ de $\mathcal{O}_K$ de norme N vérifie $x^2 + 17y^2 = N$. De plus x et y sont des entiers. Si N est positif et < 17 alors $y = 0$. Les solutions sont donc $x = \pm 1, \pm 2, \pm 3$ et ± 4.

(2) On a $D_K = -4 \cdot 17 = -68$ et $M_K = 2/\pi$.

(3) On a $\mathcal{O}_K/2\mathcal{O}_K \simeq \mathbb{F}_2[X]/(X^2+1) \simeq \Big(\mathbb{F}_2[X]/(X+1)\Big)^2$. Donc $2\mathcal{O}_K = \mathcal{P}_2^2$ où $\mathcal{P}_2$ est engendré par 2 et $\omega + 1$.

(4) Pour $p = 3$, on a de la même façon, $\mathcal{O}_K/3\mathcal{O}_K \simeq \mathbb{F}_3[X]/(X+1) \times \mathbb{F}_3[X]/(X-1)$, d'où le résultat.

(5) Pour $p = 5$, $X^2 + 17$ est irréductible, de sorte que $5\mathcal{O}_K$ est premier. D'après le théorème de Minkowski, toute classe d'idéaux a un représentant entier de norme < 6 ; or on a trouvé que 4 tels idéaux. Comme $\mathcal{O}_K$ ne possède aucun élément de norme 2 ou 3, on en déduit que $\mathcal{P}_2$ et $\mathcal{P}_{3,\pm}$ ne sont pas principaux. Par conséquent $h_K > 1$. Par ailleurs comme $\mathcal{P}_2$ est d'ordre 2, on en déduit $2|h_K$.

(6) Comme $\mathcal{P}_2$ est son propre inverse dans $Cl(K)$, si $\mathcal{P}_{3,+}$ était dans sa classe, l'idéal $\mathcal{P}_2\mathcal{P}_{3,+}$ serait principal, ce qui ne se peut pas car $\mathcal{O}_K$ ne contient aucun élément de norme 6. On en déduit donc $h_K > 2$. Il en résulte $h_K = 4$. Par ailleurs comme ± 3 sont les seuls éléments de norme 9, on en déduit que $\mathcal{P}_{3,+}^2$ n'est pas principal car sinon $\mathcal{P}_{3,+}$ serait égal à $\mathcal{P}_{3,-}$ ce qui n'est pas. Donc les deux idéaux $\mathcal{P}_{3,\pm}$ sont d'ordre 4.

(7) Les trois idéaux idéaux de norme 18 sont $\mathcal{P}_2\mathcal{P}_{3,\pm}^2$ et $\mathcal{P}_2\mathcal{P}_{3,+}\mathcal{P}_{3,-}$.

(8) On écrit $18\mathcal{O}_K = \mathcal{P}_2^2\mathcal{P}_{3,+}^2\mathcal{P}_{3,-}^2$; il s'agit alors de regrouper ces idéaux de sorte que chaque regroupement donne un idéal principal. D'après ce qui précède les seules possibilités sont : $(\mathcal{P}_2^2)(\mathcal{P}_{3,+}\mathcal{P}_{3,-})^2$, $(\mathcal{P}_2\mathcal{P}_{3,+}^2)(\mathcal{P}_2\mathcal{P}_{3,-}^2)$ ce qui donne $18 = 2.3^2 = (1+\omega)(1-\omega)$.

Solution exercice 3.

Rappelons les définitions des fonctions arithmétiques $\mathbf{1}$, j et δ : pour tout $n \geq 1$ on a $\mathbf{1}(n) = 1$, $j(n) = n$ et

$$\delta(n) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n \geq 2. \end{cases}$$

Ainsi δ est l'élément neutre pour la convolution $\star$.

On a vu dans le cours (§ 5.3.2)

$$\mathbf{1} \star \mu = \delta \quad \text{et} \quad \mathbf{1} \star \mathbf{1} = \tau.$$

La convolution étant associative, on en déduit

$$\tau \star \mu = \mathbf{1} \star \mathbf{1} \star \mu = \mathbf{1} \star \delta = \mathbf{1}.$$

On a aussi, d'après le cours, $\mathbf{1} \star j = \sigma$ avec

$$\sigma(n) = \sum_{d|n} d$$

et $\varphi = j \star \mu$, donc

$$\varphi \star \tau = j \star \mu \star \tau = j \star \mathbf{1} = \sigma.$$

On peut aussi utiliser les séries de Dirichlet pour vérifier ces relations :

$$D(\delta; s) = 1,\ D(\mathbf{1}; s) = \zeta(s),\ D(\mu; s) = 1/\zeta(s),\ D(\tau; s) = \zeta(s)^2,$$

$$D(\varphi; s) = \zeta(s-1)/\zeta(s),\ D(j; s) = \zeta(s-1),\ D(\sigma; s) = \zeta(s-1)\zeta(s),$$

donc

$$D(\tau \star \mu; s) = D(\tau; s)D(\mu; s) = D(\mathbf{1}; s) \quad \text{et} \quad D(\varphi \star \tau; s) = D(\varphi; s)D(\tau; s) = D(\sigma; s)$$

ce qui redonne $\tau \star \mu = \mathbf{1}$ et $\varphi \star \tau = \sigma$.