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 Lundi 9 Juin 2008
Durée : 3 heures

Exercice 1. Soient K et L deux extensions finies d'un corps k, de degrés m et n. Soit E le compositum de K et L.
(1) Quel est le plus grand degré possible pour E sur k ?
(2) Quel est le plus petit degré possible pour E sur k ?
(3) On suppose m et n premiers entre eux. En utilisant les réponses aux questions (1) et (2) en déduire le degré de E sur k.

Exercice 2. Donner un exemple d'une extension finie monogène $k(\alpha)$ d'un corps k qui n'est pas séparable.

Soit L/k une extension finie non séparable et N une extension normale de k qui contient L. Que peut-on dire du nombre de k-homomorphismes de L dans N ?

Exercice 3. Quel est le polynôme cyclotomique Φ_9 ?

Exercice 4. Soit P un polynôme à coefficients rationnels de degré n et soit ζ une racine primitive de degré d de l'unité.
(1) Montrer que le polynôme

$$R(X) = \prod_{j=0}^{d-1} P(\zeta^j X)$$

a ses coefficients rationnels.
(2) Montrer qu'il existe un polynôme Q à coefficients rationnels tel que $R(X) = Q(X^d)$.
(3) Quelles sont les racines de Q ?

Exercice 5. Soit P un polynôme unitaire et α une racine de P. On suppose que la dérivée P' de P s'annule au point α. Que pouvez-vous dire du discriminant de P ? La réciproque est-elle vraie ?

Exercice 6. Soient $\mathbb{F}_3$ le corps fini à 3 éléments et F une extension finie de $\mathbb{F}_3$.
(1) Quels sont les degrés des facteurs irréductibles de $X^{10} - 1$ sur $\mathbb{F}_3$? On ne demande pas d'expliciter ces facteurs mais seulement de déterminer leur degré.
(2) Quel est le corps de décomposition sur $\mathbb{F}_3$ du polynôme $X^{10} - 1$?
(3) Quels sont, suivant le nombre d'éléments de F, les degrés des facteurs irréductibles de $X^{10} - 1$ sur F ?
(4) Mêmes questions avec le polynôme $X^{30} - 1$ au lieu de $X^{10} - 1$.

Exercice 7. Le nombre 91 est-il un carré modulo 19 ?

Exercice 8. Soient p un nombre premier et $f \in \mathbb{Z}[X]$ un polynôme. Montrer que les deux conditions suivantes sont équivalentes.

(i) Pour tout $a \in \mathbb{Z}$, $f(a) \equiv 0 \pmod{p}$.

(ii) Il existe deux polynômes g et h dans $\mathbb{Z}[X]$ tels que

$$f(X) = (X^p - X)g(X) + ph(X).$$

Exercice 9. Soient $\omega = i\sqrt{26}$ et $K = \mathbb{Q}(\omega)$.

(1) Quel est l'anneau des entiers $\mathcal{O}_K$ de K ?
(2) Calculez la constante de Minkowski et le discriminant de $K/\mathbb{Q}$.
(3) Pour $p = 2, 3, 5$, donnez la décomposition en idéaux premiers de $p\mathcal{O}_K$ et déduisez-en que le nombre de classes h_K de K est > 1, pair et ≤ 8.
(4) Décrivez tous les idéaux de norme 9 puis de norme 27 ; déduisez-en que $h_K = 6$.
(5) Résolvez dans $\mathbb{Z}$ l'équation diophantienne $y^5 = x^2 + 26$.

Exercice 10. On rappelle la définition de la fonction de Möbius :

$$\mu(n) = \begin{cases} (-1)^r & \text{si } n = p_1 \cdots p_r \text{ est produit de } r \text{ nombres premiers distincts,} \\ 0 & \text{si } n \text{ a un facteur carré.} \end{cases}$$

La fonction $|\mu|$ est donc la fonction caractéristique de l'ensemble des entiers ≥ 1 sans facteurs carrés.

(1) Montrez que la fonction μ est l'unique application $\mathbb{N} \setminus \{0\} \to \{0,\ 1\}$ qui satisfasse $\mu(1) = 1$ et

$$\sum_{d|n} \mu(d) = 0 \quad \text{pour } n \geq 2.$$

(2) Quel est le produit d'Euler de la série de Dirichlet

$$D(|\mu|; s) := \sum_{n \geq 1} \frac{|\mu(n)|}{n^s}$$

associé à la fonction $|\mu|$?

(3) On définit $c : \mathbb{N} \setminus \{0\} \to \{0,\ 1\}$ comme la fonction caractéristique de l'ensemble des carrés : pour $n \geq 1$,

$$c(n) = \begin{cases} 1 & \text{si } n = m^2 \text{ avec } m \in \mathbb{Z}, \\ 0 & \text{si } n \text{ n'est pas un carré.} \end{cases}$$

Quelle est la série de Dirichlet $D(c; s)$ associée à c ? Quel est son produit d'Euler ?

(4) Calculez, pour $n \geq 1$,

$$\sum_{d|n} c(d)|\mu(n/d)|.$$

Quel est le produit $D(|\mu|; s)D(c; s)$?

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 Lundi 9 Juin 2008
Corrigé

Solution exercice 1.

Le degré de E sur k est majoré par le produit des degrés mn. Il est multiple de m et n, donc est minoré par le ppcm de m et n.

Si m et n sont premiers entre eux, le seul nombre vérifiant ces propriétés est mn.

Solution exercice 2. Un exemple d'extension monogène non séparable est $K(\sqrt{T})$ quand $K = \mathbb{F}_2(T)$. Son degré est 2 et $\sqrt{T}$ n'a qu'un conjugué dans une extension normale de K. De façon générale quand N est une extension finie normale de K et L un sous-corps de N qui est une extension non séparable de K, alors le nombre de K-isomorphismes de L dans N est ≥ 1 (puisqu'il y a l'identité, injection de L dans N) et il est strictement inférieur au degré de L sur K.

Solution exercice 3. Comme les diviseurs de P sont 1, 3 et 9, on peut écrire

$$X^9 - 1 = \Phi_1(X)\Phi_3(X)\Phi_9(X),$$

avec $\Phi_1(X) = X - 1$,

$$\Phi_3(X) = \frac{X^3 - 1}{X - 1} = X^2 + X + 1$$

et

$$\Phi_9(X) = \frac{X^9 - 1}{X^3 - 1} = X^6 + X^3 + 1.$$

Le polynôme $\Phi_9(X)$ est $\Phi_3(X^3)$, car $9 = 3^2$. En général pour p premier et $s \geq 1$ on a $\Phi_{p^s} = \Phi_p(X^{p^{s-1}})$.

Solution exercice 4. Chacun des facteurs $P(\zeta^j X)$ est un polynôme à coefficients dans le corps cyclotomique $\mathbb{Q}(\zeta)$, donc il en est de même du produit. Mais le polynôme R est invariant sous l'action du groupe de Galois de $\mathbb{Q}(\zeta)$ sur $\mathbb{Q}$ (qui permute les racines d–ièmes de l'unité), donc R a ses coefficients rationnels.

On décompose P dans une extension normale :

$$P(X) = a_0(X - \alpha_1)\cdots(X - \alpha_d).$$

Les racines de R sont les $\zeta^j \alpha_h$:

$$R(X) = \prod_{j=0}^{d-1} \prod_{h=1}^{n} (X - \zeta^j \alpha_h).$$

Mais

$$\prod_{j=0}^{d-1} (X - \zeta^j \alpha_h) = X^d - \alpha_h^d.$$

Donc $R(X) = Q(X^d)$ avec

$$Q(T) = \prod_{h=1}^{n} (T - \alpha_h^d).$$

Le coefficient directeur de Q est a_0^d, le terme constant de Q est a_n^d quand a_n est le terme constant de P. Les autres coefficients sont donnés par les fonctions symétriques élémentaires des α_h^d, $1 \leq h \leq n$.

Solution exercice 5. Le discriminant d'un polynôme s'annule si et seulement si le polynôme a au moins une racine multiple, donc si et seulement s'il existe une racine α de P telle que $P'(\alpha) = 0$.

Solution exercice 6.

Les diviseurs de 10 sont 1, 2, 5 et 10, donc le polynôme $X^{10} - 1$ est le produit des polynômes cyclotomiques $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$ et

$$\Phi_{10}(X) = \frac{X^5 + 1}{X + 1} = \Phi_5(-X) = X^4 - X^3 + X^2 - X + 1.$$

Noter que la relation $\Phi_{10}(X) = \Phi_5(-X)$ montre que les degrés des facteurs irréductibles de $\Phi_{10}(X)$ et $\Phi_5(X)$ sont les mêmes !

De façon générale (théorème 3.8), quand n est premier avec q, le polynôme cyclotomique Φ_n se décompose sur $\mathbb{F}_q$ en produit de polynômes irréductibles tous de même degré d, où d est l'ordre de q modulo n (c'est-à-dire l'ordre de la classe de q dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$).

Comme 3 est d'ordre 4 dans le groupe multiplicatif $(\mathbb{Z}/5\mathbb{Z})^\times$ aussi bien que dans $(\mathbb{Z}/10\mathbb{Z})^\times$, les deux polynômes Φ_5 et Φ_{10} sont irréductibles sur $\mathbb{F}_3$, ce qui fait que $X^{10} - 1$ est produit de deux polynômes de degré 1 et de deux polynômes irréductibles de degrés 4 sur $\mathbb{F}_3$.

Comme 9 est congru à -1 modulo 5 et modulo 10, il est d'ordre 2 dans le groupe multiplicatif $(\mathbb{Z}/5\mathbb{Z})^\times$ aussi bien que dans $(\mathbb{Z}/10\mathbb{Z})^\times$, donc Φ_5 et Φ_{10} sont tous deux produits de deux polynômes de degré 2 sur $\mathbb{F}_9$. Ainsi $X^{10} - 1$ est produit de deux polynômes de degré 1 et de quatre polynômes irréductibles de degrés 2 sur $\mathbb{F}_9$.

Le corps de rupture d'un polynôme quadratique irréductible sur un corps est une extension quadratique de ce corps, ce qui fait que Φ_5 et Φ_{10} sont totalement décomposés dans $\mathbb{F}_{81}$. On le vérifie aussi en disant que 81 est congru à 1 modulo 5 et modulo 10, donc d'ordre 1 dans les groupes multiplicatifs correspondants. Le corps de décomposition de $X^{10} - 1$ est par conséquent $\mathbb{F}_{81}$.

Finalement si le corps fini F de caractéristique 3 contient $\mathbb{F}_{81}$ (ce qui veut dire que son degré sur $\mathbb{F}_3$ est multiple de 4, ou encore que son nombre d'éléments est 3^s avec s multiple de 4), alors

le polynôme $X^{10}-1$ est complètement décomposé dans F. Si le corps F contient $\mathbb{F}_9$ mais pas $\mathbb{F}_{81}$ (ce qui veut dire que son degré sur $\mathbb{F}_3$ est multiple de 2 mais pas de 4, ou encore que son nombre d'éléments est 3^s avec s congru à 2 modulo 4), alors $X^{10}-1$ est produit de deux polynômes de degré 1 et de quatre polynômes irréductibles de degré 2 à coefficients dans F. Enfin si F ne contient pas $\mathbb{F}_9$ (ce qui veut dire que son degré sur $\mathbb{F}_3$ est impair, ou encore que son nombre d'éléments est 3^s avec s impair), alors $X^{10}-1$ est produit de deux polynômes de degré 1 et de deux polynômes irréductibles de degré 4 sur F.

Quand n est multiple de la caractéristique p on écrit $n = p^t m$ avec $t \geq 1$ et m premier avec p ; alors

$$X^n - 1 = (X^m - 1)^{p^t}.$$

Ainsi $X^{30}-1 = (X^{10}-1)^3$ sur un corps de caractéristique 3.

Solution exercice 7.

On remarque déjà que $91 = 7 \cdot 13$, donc le symbole de Legendre vaut

$$\left(\frac{91}{19}\right) = \left(\frac{7}{19}\right)\left(\frac{13}{19}\right).$$

On utilise la loi de réciprocité quadratique : comme 7 et 19 sont congrus à 3 modulo 4 et que 13 est congru à 1 modulo 4, on a

$$\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right) \quad \text{et} \quad \left(\frac{13}{19}\right) = \left(\frac{19}{13}\right).$$

Ensuite $19 \equiv 5 \pmod 7$,

$$\left(\frac{19}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

ce qui fait que 7 est un carré modulo 19 (en effet 7 est congru à 8^2 modulo 19).

De même

$$\left(\frac{19}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right)$$

et

$$\left(\frac{2}{13}\right) = -1 \quad \text{car} \quad 13 \equiv -3 \pmod 8,$$

$$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1,$$

ce qui fait que 13 n'est pas résidu quadratique modulo 19, et donc 91 non plus.

Solution exercice 8.

Si $f(X) = (X^p - X)g(X) + ph(X)$, alors pour tout $a \in \mathbb{Z}$ en utilisant la congruence $a^p \equiv a \pmod p$ on en déduit que le nombre p divise $f(a)$.

Inversement supposons que pour tout $a \in \mathbb{Z}$ le nombre p divise $f(a)$. On divise le polynôme f par $X^p - X$ dans $\mathbb{Z}[X]$:

$$f(X) = (X^p - X)g(X) + r(X)$$

avec g et r dans $\mathbb{Z}[X]$, et r est soit nul, soit de degré $< p$. Alors $r(a) \equiv 0 \pmod p$ pour tout $a \in \mathbb{Z}$, donc l'image de r dans $\mathbb{F}_p[X]$ est nulle. Cela signifie qu'il existe $h \in \mathbb{Z}[X]$ tel que $r = ph$.

Solution exercice 9.

(1) D'après le cours, comme $-26 \equiv 2 \pmod 4$, on a $\mathcal{O}_K = \mathbb{Z}[\omega]$.

(2) On a $M_K = 2/\pi$ et $D_K = -4 \cdot 26 = -104$.

(3) Il s'agit de factoriser X^2+26 : on obtient $2\mathcal{O}_K = \mathcal{P}_2^2$ avec $\mathcal{P}_2 = (2, \omega)$, $3\mathcal{O}_K = \mathcal{P}_{3,+}\mathcal{P}_{3,-}$ avec $\mathcal{P}_{3,\pm} = \langle 3, \omega \pm 1\rangle$ et $5\mathcal{O}_K = \mathcal{P}_{5,+}\mathcal{P}_{5,-}$ avec $\mathcal{P}_{5,\pm} = \langle 5, \omega \pm 2\rangle$. D'après le théorème de Minkowski toute classe d'idéaux rencontre un idéal entier de norme ≤ 6, ce qui donne ici $\mathcal{O}_K, \mathcal{P}_2, \mathcal{P}_{3,\pm}, \mathcal{P}_{5,\pm}, \mathcal{P}_2\mathcal{P}_{3,\pm}$, soit au plus 8 tels idéaux. Par ailleurs comme $\mathcal{O}_K$ ne contient pas d'éléments de norme $2, 3, 5, 6$ aucun de ces idéaux n'est principal. Comme $\mathcal{P}_2$ est d'ordre 2, on en déduit $2|h_K$.

(4) Les idéaux de norme 9 sont $3\mathcal{O}_K, \mathcal{P}_{3,+}^2, \mathcal{P}_{3,-}^2$; comme les deux derniers sont conjugués, ils sont soit tous deux principaux soit tous deux non principaux. Or ± 3 sont les seuls éléments de norme 9 ; donc les deux idéaux $\mathcal{P}_{3,\pm}$ ne sont pas principaux.

De même les idéaux de norme 27 sont $3\mathcal{P}_{3,\pm}$ et $\mathcal{P}_{3,\pm}^3$: les deux derniers étant conjugués, s'il l'un deux est principal ils le sont tous les deux. Par ailleurs d'après ce qui précède les deux idéaux $3\mathcal{P}_{3,\pm}$ ne sont pas principaux. Or $1 \pm \omega$ sont deux élément de norme 27 ce qui impose que $\mathcal{P}_{3,\pm}^3$ sont tous deux principaux. Donc $3|h_K$, ce qui impose $6|h_K$.

(5) Dans K, on a $y^5 = (x+\omega)(x-\omega)$; comme $\mathcal{O}_K$ n'est pas principal, on passe au niveau des idéaux. Regardons le pgcd des idéaux $(x+\omega)$ et $(x-\omega)$: il doit contenir $(2\omega) = \mathcal{P}_2^2\mathcal{P}_{13}^2$ où $\mathcal{P}_{13} = \langle 13, \omega\rangle$ est premier. On a ainsi

$$(x \pm \omega)\mathcal{O}_K = \mathcal{P}_2^a \mathcal{P}_{13}^b \prod_i \mathcal{Q}_i^{e_\pm(i)}$$

où $e_+(i)e_-(i) = 0$ pour tout i. Comme $(x+\omega)(x-\omega) = y^5$ on en déduit, grâce à l'unicité de la décomposition en facteurs d'idéaux premiers, que $a \equiv b \equiv e_\pm(i) \equiv 0 \mod 5$ soit $(x \pm \omega) = \left(\mathcal{P}_2^{2a'}\mathcal{P}_{13}^{2b'}\prod_i \mathcal{Q}_i^{f_\pm(i)}\right)^5$; comme 5 est premier avec h_K, on en déduit que l'idéal $\mathcal{P}_2^{2a'}\mathcal{P}_{13}^{2b'}\prod_i \mathcal{Q}_i^{f_\pm(i)}$ est principal, i.e. il existe $a, b \in \mathbb{Z}$ tels que $x + \omega = (a + b\omega)^5$. On en déduit alors que $1 = 5a^4b - 260a^2b^3 + 26^2b^5$ ce qui impose $b = \pm 1$ et $5a^4 - 260a^2 + 26^2 = \mp 1$, équation qui n'a pas de solutions entières (regarder modulo 2).

Solution exercice 10.

a) C'est une question de cours (fascicule 8, § 5.3.2) : la relation demandée s'écrit $\mathbf{1} \star \mu = \delta$, où $\mathbf{1}$ est la fonction constante égale à 1, tandis que δ est l'élément neutre pour la convolution :

$$\delta(1) = 1, \quad \delta(n) = 0 \quad \text{pour} \quad n \geq 2.$$

b) La relation

$$D(|\mu|; s) := \sum_{n \geq 1} \frac{|\mu(n)|}{n^s} = \prod_p (1 + p^{-s})$$

résulte de la Proposition 5.32 appliquée à la fonction $f = |\mu|$, car cette fonction est multiplicative et vérifie, pour p premier,

$$|\mu(p^m)| = \begin{cases} 1 & \text{si } m = 1, \\ 0 & \text{si } m \geq 2. \end{cases}$$

On peut aussi refaire la démonstration en se restreignant d'abord aux nombres entiers produits de nombres premiers $\leq N$, puis en faisant tendre N vers l'infini, comme dans le cours.

c) On a

$$D(c;s) := \sum_{n\geq 1} \frac{c(n)}{n^s} = \sum_{m\geq 1} \frac{1}{m^{2s}} = \zeta(2s) = \prod_p (1-p^{-2s})^{-1}.$$

d) Dans le membre de droite de

$$(c \star |\mu|)(n) = \sum_{d|n} c(d)|\mu(n/d)|$$

un terme et un seul est non nul, il est obtenu pour d le plus grand diviseur carré de n, et pour cette valeur de d on a $c(d) = |\mu(n/d)| = 1$. Donc

$$(c \star |\mu|)(n) = \mathbf{1}(n) = 1 \quad \text{pour tout } n \geq 1.$$

Une autre démonstration de la relation $c \star |\mu| = \mathbf{1}$ consiste à vérifier que pour p premier et $m \geq 1$, on a $(c \star |\mu|)(p^m) = 1$, ce qui donne le même résultat : les fonctions c et $|\mu|$ sont multiplicatives, donc $c \star |\mu|$ aussi.

La série de Dirichlet associée à la fonction $\mathbf{1}$ est celle de la fonction zêta de Riemann, ce qui donne la relation

$$D(c;s)D(|\mu|;s) = D(c \star |\mu|;s) = \zeta(s).$$

On vérifie d'ailleurs directement

$$D(|\mu|;s) = \prod_p (1+p^{-s}), \quad D(c;s) = \prod_p (1-p^{-2s})^{-1}, \quad 1-p^{-2s} = (1-p^{-s})(1+p^{-s}),$$

donc

$$D(|\mu|;s) = \frac{D(c \star |\mu|;s)}{D(c;s)} = \frac{\zeta(s)}{\zeta(2s)}.$$