UE Théorie des nombres. Examen du 7 mai 2019, 9h-12h

Tous documents interdits.

Qing Liu

Exercice 1 Soit $L = \mathbb{Q}[\sqrt{-3}]$.

(1) Montrer que $\mathcal{O}_L = \mathbb{Z}[\zeta]$ où $\zeta = (-1 + \sqrt{-3})/2$.

(2) Quel est le discriminant de L ?

(3) Montrer que $\mathcal{O}_L$ est principal.

(4) Trouver les unités de $\mathcal{O}_L$.

Exercice 2 Soit $L = \mathbb{Q}[\sqrt{7}]$.

(1) Quels sont $\mathcal{O}_L$ et le discriminant de L ?

(2) Montrer que l'extension $L/\mathbb{Q}$ est ramifiée au-dessus de 2 et que $2\mathcal{O}_L = \mathfrak{q}^2$ avec $\mathfrak{q}$ maximal.

(3) Calculer $N(\mathfrak{q})$ et trouver un générateur de $\mathfrak{q}$ (de la forme $\sqrt{7} + k$).

(4) Montrer que $\mathcal{O}_L$ est principal.

(5) Déterminer les unités de $\mathcal{O}_L$.

Exercice 3 Soit A un anneau principal, de corps de fractions K. Soit L une extension finie séparable de K. On suppose que $L = K[\theta]$ avec θ entier sur A. Considérons

$$C = A[\theta] := \{f(\theta) \ \mid \ f(T) \in A[T]\} \subseteq L.$$

On sait que C est fini (donc entier) sur A.

(1) Soit $w \in L$ entier sur A. Considérons

$$I_w = \{a \in A \mid aw \in C\}.$$

Montrer que I_w est un idéal de A. On sait par le cours que $I_w \neq \{0\}$.

(2) On suppose que pour tout élément irréductible π de A, l'anneau $C/\pi C$ est réduit (les éléments nilpotents sont nuls). On veut montrer que C est alors la clôture intégrale de A dans L. Soit $w \in L$ entier sur A. Soit t un génerateur de I_w.

   (a) Si t est inversible dans A, montrer que $1 \in I_w$ et que $w \in C$.

   (b) Supposons que t n'est pas inversible dans A. Montrer que $\alpha := tw \in C$ satisfait une relation

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

   avec $a_i \in tA$ (utiliser une équation entière satisfaite par w).

   (c) Soit π un facteur premier de t. Montrer que $\alpha^n \in \pi C$. En déduire que $\alpha \in \pi C$ et que $t/\pi \in I$. Conclure.

Le but des trois exercices suivant est de traiter au maximum le deuxième cas de Fermat pour les premiers réguliers et de résoudre complètement le problème quand $p = 3$. L'exercice 6 est extrait de l'écrit de MG du concours d'agrégation de 2019.

Exercice 4 Soit $p \geq 3$ un nombre premier. Soit $L = \mathbb{Q}[\zeta_p]$ l'extension cyclotomique engendrée par une racine primitive p-ième de l'unité $\zeta \in \mathbb{C}$. On sait que $\mathcal{O}_L = \mathbb{Z}[\zeta]$. On note $\Phi_p(X) \in \mathbb{Z}[X]$ le p-ième polynôme cyclotomique.

(1) Soit ℓ un nombre premier distinct de p.
   (a) Montrer que l'image de $X^p - 1$ dans $\mathbb{F}_\ell[X]$ est séparable. En déduire le même résultat pour $\Phi_p(X)$.
   (b) Montrer que l'extension $\mathbb{Z} \subset \mathcal{O}_L$ est non-ramifiée au-dessus de ℓ.
   (c) Supposons $\ell \equiv 1\ [p]$. Montrer qu'il existe un élément dans $\mathbb{F}_\ell^*$ d'ordre exactement p. En déduire que ℓ est totalement décomposé dans $\mathcal{O}_L$: l'idéal $\ell\mathcal{O}_L$ est le produit de $p-1$ idéaux maximaux 2 à 2 distincts.

(2) Posons $\lambda = \zeta - 1 \in \mathcal{O}_L$.
   (a) Montrer que l'image de $\Phi_p(X)$ dans $\mathbb{F}_p[X]$ est égale à $(X-1)^{p-1}$.
   (b) Soit $\mathfrak{q} = (\lambda, p)$ l'idéal de $\mathcal{O}_L$ engendré par λ et p. Montrer que $\mathfrak{q}$ est maximal, que $p\mathcal{O}_L = \mathfrak{q}^{p-1}$ et que $\mathbb{Z}/p\mathbb{Z} = \mathcal{O}_L/\mathfrak{q}$.
   (c) En développant la relation $1 = (1+\lambda)^p$, montrer que
   $$\frac{\lambda^{p-1}}{p} = -1 + \lambda a, \quad \text{pour un } a \in \mathcal{O}_L.$$
   (d) Montrer que $p \in \lambda\mathcal{O}_L$, que $\mathfrak{q} = \lambda\mathcal{O}_L$ et que $p\mathcal{O}_L = \lambda^{p-1}\mathcal{O}_L$.

(3) Rappelons que pour tous $i, j \in \mathbb{Z}$ premiers à p, $(\zeta^i - 1)/(\zeta^j - 1) \in U(\mathcal{O}_L)$. Montrer que $(\zeta^i - 1)\mathcal{O}_L = \lambda\mathcal{O}_L$ pour tout i premier à p.

(4) (Indépendante de (1)-(3)). Pour tous $\alpha, \beta \in \mathcal{O}_L$, montrer que
$$\sum_{0 \leq i \leq p-1} \zeta^i(\alpha + \zeta^i\beta) = 0.$$

Exercice 5 Nous conservons les hypothèses et notations de l'exercice précédent. On fixe $\alpha, \beta, \gamma \in \mathcal{O}_L$ non nuls tels que $\alpha, \beta \notin \lambda\mathcal{O}_L$, $\gamma \in \lambda\mathcal{O}_L$ et que
$$\alpha^p + \beta^p + u\gamma^p = 0$$
pour un certain $u \in U(\mathcal{O}_L)$. Nous avons donc une relation
$$-u\gamma^p = \prod_{0 \leq i \leq p-1} (\alpha + \zeta^i\beta). \tag{1}$$
Nous allons trouver des propriétés sur les facteurs du terme de droite.

(1) (Étude des puissances p-ièmes dans $\mathcal{O}_L$). On a vu dans le cours que $\alpha^p \in \mathbb{Z}+p\mathcal{O}_L$. Nous allons améliorer ce résultat en utilisant l'hypothèse $\alpha \notin \lambda\mathcal{O}_L$.
   (a) Montrer que $\mathcal{O}_L \subseteq \mathbb{Z} + \lambda\mathcal{O}_L$ (utiliser 2(a)). En déduire qu'il existe $k, r \in \mathbb{Z}$ et $\alpha' \in \mathcal{O}_L$ tels que
   $$\alpha = k + \lambda r + \lambda^2\alpha'.$$
   De plus on peut choisir k compris entre $-(p-1)/2$ et $(p-1)/2$.
   (b) Montrer que
   $$\alpha^p \in k^p + \lambda p(k^{p-1}r + (\lambda^{p-1}/p)r^p) + p\lambda^2\mathcal{O}_L$$
   et
   $$\alpha^p \in k^p + \lambda p(k^{p-1}r - r^p) + p\lambda^2\mathcal{O}_L$$
   (c) Montrer que pour tout $s \in \mathbb{Z}$, on a $s^p \equiv s\ [p]$, et que $s^{p-1} \equiv 1\ [p]$ si $s \notin p\mathbb{Z}$.
   (d) Montrer que $k \notin p\mathbb{Z}$ et que $\alpha^p - k^p \in p\lambda^2\mathcal{O}_L = \lambda^{p+1}\mathcal{O}_L$.

(2) On veut montrer que $\gamma \in \lambda^2\mathcal{O}_L$.
   (a) Similairement à α, choisissons un entier m compris entre $-(p-1)/2$ et $(p-1)/2$ tel que $\beta^p - m^p \in \lambda^{p+1}\mathcal{O}_L$. Montrer que $k+m \equiv k^p + m^p \equiv 0\ [p]$.
   (b) En déduire que $k + m = 0$ et que $\gamma \in \lambda^2\mathcal{O}_L$.

(3) Calcul de "pgcd". Supposons dans la suite que α, β sont premiers entre eux (dans le sens que $\alpha\mathcal{O}_L + \beta\mathcal{O}_L = \mathcal{O}_L$).
   (a) Montrer que la différence entre deux facteurs quelconques de droite dans la relation (1) est toujours divisible par λ mais jamais par λ^2 (utiliser l'exercie 4.3).
   (b) Montrer que λ divise un des facteurs de droite, et que par suite il divise tous les facteurs de droite.
   (c) En déduire que λ^2 divise un et un seul facteur $\alpha + \zeta^{i_0}\beta$. Quitte à remplacer β par $\zeta^{p-i_0}\beta$, on peut supposer que λ^2 divise $\alpha + \beta$.
   (d) Soient $i \neq j$ compris entre 0 et $p-1$. Supposons qu'il existe un idéal maximal $\mathfrak{m}$ de $\mathcal{O}_L$ tel que $\alpha+\zeta^i\beta, \alpha+\zeta^j\beta \in \lambda\mathfrak{m}$. Montrer que $\alpha, \beta \in \mathfrak{m}$.
   (e) Montrer que les éléments $(\alpha + \zeta^i\beta)/\lambda \in \mathcal{O}_L$ sont 2 à 2 premiers entre eux.

(4) Enfin, supposons de plus que p soit un premier régulier. Montrer qu'il existe $u_i \in U(\mathcal{O}_L)$, et des $\delta_i \in \mathcal{O}_L$ 2 à 2 premiers entre eux tels que $\alpha+\zeta^i\beta = \lambda u_i\delta_i^p$ et que $\delta_0 \in \lambda\mathcal{O}_L$. Plus précisément, si λ^n est la plus grande puissance de λ divisant γ (i.e. $v_\lambda(\gamma) = n$), alors $v_\lambda(\delta_0) = n-2$.

Exercice 6 (Fermat pour $p = 3$) On veut montrer que si $x, y, z \in \mathbb{Z}$ vérifient $x^3 + y^3 + z^3 = 0$, alors $xyz = 0$.

Supposons qu'il existe une solution avec $xyz \neq 0$. On peut supposer que x, y, z sont premiers entre eux. Soit $L = \mathbb{Q}[\zeta]$ engendrée par une racine primitive 3-ième de l'unité ζ. On utilisera librement les résultats des exercices 1, 4 et 5. Soit $\lambda = \zeta - 1$.

(1) Montrer que x, y, z sont deux à deux premiers entre eux et que $3 \mid xyz$.

(2) Soient $a, b \in \mathbb{Z}$ et $c = \text{pgcd}(a, b) \in \mathbb{Z}$. Montrer que c est aussi un pgcd de a, b dans $\mathcal{O}_L$.

(3) Nous allons montrer un résultat dans $\mathcal{O}_L$ plus fort que Fermat. Supposons qu'il existe $\alpha, \beta \in \mathcal{O}_L \setminus \lambda\mathcal{O}_L$ premiers entre eux, $u \in U(\mathcal{O}_L)$ et $\gamma \in \lambda\mathcal{O}_L$ non nul tels que

$$\alpha^3 + \beta^3 + u\gamma^3 = 0.$$

Nous allons conclure à une contradiction.

(a) Montrer qu'il existe $\delta_1, \delta_2 \in \mathcal{O}_L \setminus \lambda\mathcal{O}_L$ premiers entre eux, $\delta_0 \in \lambda\mathcal{O}_L$ et $u_0, u_1, u_2 \in U(\mathcal{O}_L)$ tels que $\alpha + \beta = u_0\delta_0^3$, $\alpha + \zeta\beta = u_1\delta_1^3$ et $\alpha + \zeta^2\beta = u_2\delta_2^3$.

(b) Montrer qu'il existe $w_0, w_2 \in U(\mathcal{O}_L)$ tels que

$$\delta_1^3 + w_2\delta_2^3 + w_0\delta_0^3 = 0$$

(utiliser l'exercice 4.4).

(c) Montrer que $w_2 \equiv \pm 1\ [\lambda^3]$. En déduire que $w_2 \notin \{\pm\zeta, \pm\zeta^2\}$.

(d) Montrer que $w_2 = \pm 1$ (utiliser la description explicite de $U(\mathcal{O}_L)$) et que λ^2 divise δ_0.

(e) Nous avons donc obtenu un quadruplet $(\delta_1, w_2\delta_2, u_0, \delta_0)$ satisfaisant les mêmes propriétés que $(\alpha, \beta, u, \gamma)$ et tel que $v_\lambda(\delta_0) = v_\lambda(\gamma) - 1$. Conclure.

(4) Montrer Fermat pour $p = 3$.

◇◇ Fin ◇◇