Corrigé examen TDN
7/5/2019

Exercice 1

(1) On a $-3 \equiv 1 \ [4]$. D'après le cours

$$\mathcal{O}_L = \mathbb{Z}\left[\frac{\sqrt{-3}-1}{2}\right]$$

(2) $D_L = -3$ toujours d'après le cours.

(3) La borne de Minkowski dit que tout idéal fractionnaire est équivalent à un idéal J de norme

$$N(J) \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{2!}{2^2}\sqrt{3} \quad , \ r_2 = 1$$

$$= \frac{4}{\pi}\cdot\frac{\sqrt{3}}{2} = \frac{2\sqrt{3}}{\pi} < 1{,}2$$

donc $N(J) = 1$ et $J = \mathcal{O}_L$. D'où $\mathcal{O}_L$ principal.

(4) Les unités de $\mathcal{O}_L$ sont les $a+b\xi$ avec $a, b \in \mathbb{Z}$ et $N_{L/\mathbb{Q}}(a+b\xi) = 1$ ou -1.

C'est-à-dire $\left(a+b\cdot\frac{\sqrt{-3}-1}{2}\right)\left(a+b\frac{\sqrt{-3}+1}{2}\right) = \pm 1$

$\Leftrightarrow (a+b\zeta)(a+b\bar{\zeta}) = \pm 1$

$\Leftrightarrow a^2 - ab + b^2 = \pm 1$

$\Leftrightarrow \left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4} = \pm 1$

$\Leftrightarrow \left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4} = 1$

$\Leftrightarrow (2a-b)^2 + 3b^2 = 4$

- si $b=0 \Rightarrow a = \pm 1$
- si $b \neq 0 \Rightarrow b^2 \leq 2 \Rightarrow b = \pm 1$.
  - si $b=1 \Rightarrow (2a-1)^2 + 3 = 4$
    $\Rightarrow (2a-1)^2 = 1 \Rightarrow a = 0$ ou
  - si $b=-1 \Rightarrow (2a+1)^2 = 1 \Rightarrow a = 0$ ou

Donc les unités sont $\{\pm 1, \pm\zeta, \pm(1+\zeta)\}$

On a $1 + \zeta + \zeta^2 = 0 \Rightarrow 1 + \zeta = -\zeta^2$

$\Rightarrow U(\mathcal{O}_L) = \{\pm 1, \pm\zeta, \pm\zeta^2\}$

Comme $\zeta = \zeta_3$ est une racine primitive 3-ième de l'unité, on peut aussi utiliser le cas qui dit que $U(\mathcal{O}_{\mathbb{Q}[\zeta_p]}) = \{\pm\zeta_p^k \mid k \in \mathbb{Z}\}$. $U(\mathcal{O}_{\mathbb{Q}(\zeta}$

Exercice 2.

(1) $7 \not\equiv 1 \ [4] \Rightarrow d_L = 4 \times 7 = 28$, $\mathcal{O}_L = \mathbb{Z}[\sqrt{7}]$

(2) On a $\mathcal{O}_L = \mathbb{Z}[\sqrt{7}]$ car $7 \not\equiv 1 \ [4]$

Le polynôme minimal de $\sqrt{7}$ est $X^2 - 7$.

On $X^2 - 7 \equiv (X-1)^2 \ [2]$

$\Rightarrow 2\mathcal{O}_L = \mathfrak{p}^2$, $\mathfrak{p} = (2, \sqrt{7}-1)$.

(3) $N(\mathfrak{p})^2 = N(\mathfrak{p}^2) = N(2\mathcal{O}_L) = |N_{L/\mathbb{Q}}(2)| = 4$

Donc $N(\mathfrak{p}) = 2$. Si $\sqrt{7}+k$ est un générateur de $\mathfrak{p}$, on doit avoir

$$|N_{L/\mathbb{Q}}(\sqrt{7}+k)| = N(\mathfrak{p}) = 2,$$

donc $|7 - k^2| = 2$. La seule possibilité est $k = 3$. On a

$$\sqrt{7} - 3 = \sqrt{7} - 1 + 4 = \sqrt{7} - 1 + 2 \times 2 \in \mathfrak{p}$$

Comme $|N_{L/\mathbb{Q}}(\sqrt{7}-3)| = N(\mathfrak{p})$, on a

bien $\mathfrak{p} = (\sqrt{7}-3)\mathcal{O}_L$

(4) La borne de Minkowski $\Rightarrow$ tout idéal fractionnaire est équivalent à un idéal J de norme

$$N(J) \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{2!}{2^2} \sqrt{4 \times 7} = \sqrt{7} < 3$$

$$\Rightarrow \quad N(J) \leq 2$$

Donc J est une puissance d'un idéal maximal $\mathfrak{p}$ tq $\mathfrak{p} \cap \mathbb{Z} = 2\mathbb{Z}$.

D'après (3), on a $\mathfrak{p}$ principal. Donc J est principal et $\mathcal{O}_L$ est principal.

(5) On sait d'après le cours qu'on peut trouver une unité fondamentale

$$\alpha = a + b\sqrt{7} \qquad a \in \mathbb{Z},\ b \in \mathbb{N}$$

et b est le plus petit entier > 0 tq

$$7b^2 = \text{carré} \pm 1.$$

On teste $b = 1, 2, 3, \ldots$ et on trouve

$$b = 3 : \quad 7 \times 3^2 = 16^2 - 1$$

$\Rightarrow \quad N_{L/\mathbb{Q}}(16+3\sqrt{7}) = 1$

et toujours d'après le cours

$$U(\mathcal{O}_L) = \{ \pm \alpha^k \mid k \in \mathbb{Z} \}$$

avec $\alpha = 16+3\sqrt{7}$.

Exercice 3

(1). Vérification directe.

(2) (a) si $t \in A^* \Rightarrow I_w = tA = A \Rightarrow 1 \in I_w$.

$\Rightarrow 1 \cdot w \in C \to w \in C$.

(b) Supp $t \notin A^*$. On a $\alpha = tw \in C$.

Soit

$$w^n + a'_{n-1} w^{n-1} + \dots + a'_1 w + a'_0 = 0$$

une relation entière avec $a'_i \in A$

(puisque w est entier sur A).

On multiplie la relation par α^n,

alors

$$\alpha^n + (t a'_{n-1}) \alpha^{n-1} + \dots + (t^{n-1} a'_1)\alpha + t^n a'_0 = 0$$

On a $a_i = t^{n-i} a'_i \in tA \quad \forall \ i = 0, \dots, n-1$.

(c) On a

$$\alpha^n = t\left(-\frac{a_{n-1}}{t}\alpha^{n-1} - \cdots - \frac{a_0}{t}\right) \in tC \subseteq \pi C$$

On a donc $\bar{\alpha}^n = 0$ pour $\bar{\alpha}$ = classe de α dans $C/\pi C$. Comme ce dernier est réduit par hypothèse, on a $\bar{\alpha} = 0$, c'est-à-dire

$\alpha \in \pi C$. Soit $\alpha = \pi c_0$, $c_0 \in C$.

Alors $tw = \pi c_0 \Rightarrow \frac{t}{\pi} w = c_0 \in C$

$\Rightarrow \frac{t}{\pi} \in I_w = tA \Rightarrow \frac{t}{\pi} = ta \Rightarrow 1 = \pi a$

impossible. Donc $t \in A^*$ et $w \in C$.

Exercice 4

(1)

(a). La dérivée $(X^p-1)' = pX^{p-1}$ n'a pas de racine commune avec X^p-1 dans $\overline{\mathbb{F}_\ell}$

Donc $X^p-1 \in \mathbb{F}_\ell[X]$ est séparable.

Comme $\Phi_p(X)$ divise X^p-1, il n'a pas de racine multiple dans $\overline{\mathbb{F}_\ell}$ non plus.

(b) $\Phi_p(X) \in \mathbb{F}_\ell[X]$ séparable.

$\mathcal{O}_L = \mathbb{Z}[\zeta]$

D'après le cours, les indices de ramification au-dessus de p sont égaux à 1.

(c) Card $\mathbb{F}_\ell^* = \ell-1$ divisible par p,

donc il existe $\alpha \in \mathbb{F}_\ell^*$ d'ordre exactement p car $\mathbb{F}_\ell^*$ est un groupe cyclique. Il suit que

$\alpha, \alpha^2, \dots, \alpha^{p-1}$ sont 2 à 2 distincts et d'ordre exactement p.

Dans $\mathbb{F}_\ell[X]$ on a

$$X^p - 1 = (X-1)\,\Phi_p(X)$$

car c'est déjà vrai dans $\mathbb{Z}$. Il suit que $\Phi_p(X)$ admet $p-1$ racines distinctes dans $\mathbb{F}_\ell$. Comme $\deg \Phi_p(X) = p-1$, on a

$$\Phi_p(X) = (X-\alpha)(X-\alpha^2)\cdots(X-\alpha^{p-1}) \in \mathbb{F}_\ell[X]$$

$$\Rightarrow \quad \mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_{p-1}$$

avec $\mathfrak{P}_i = (\mathfrak{p}, \zeta - a^i)$.

où $a \in \mathbb{Z}$ est un antécédent de $\alpha \in \mathbb{Z}/\ell\mathbb{Z}$.

(2) (a) Dans $\mathbb{Z}[X]$ on a $X^p - 1 = (X-1)\Phi_p(X)$.

Donc dans $\mathbb{F}_p[X]$, on a

$$(X-1)^p = X^p - 1 \equiv (X-1)\Phi_p(X) \quad (p)$$

$$\Rightarrow \quad \Phi_p(X) \equiv (X-1)^{p-1} \quad [p].$$

(b) Comme $\mathcal{O} = \mathbb{Z}[\zeta]$ et que $\Phi_p(X)$ est le polynôme minimal de ζ sur $\mathbb{Q}$, l'énoncé résulte du cours et de (a).

(c) On a

$$1 = 1 + p\lambda + \binom{p}{2}\lambda^2 + \cdots + \binom{p}{p-1}\lambda^{p-1} + \lambda^p$$

$$\Rightarrow \lambda^{p-1} = p\left(-1 + \frac{\binom{p}{2}}{p}\cdot\lambda - \cdots - \frac{\binom{p}{p-1}}{p}\lambda^{p-2}\right)$$

(on sait que $p \mid \binom{p}{k}$ $k = 1, 2, \ldots, p-1$).

$$\Rightarrow \frac{\lambda^{p-1}}{p} = -1 + \lambda\underbrace{\left(-\frac{\binom{p}{2}}{p} + \frac{\binom{p}{3}}{p}\lambda - \cdots - \lambda^{p-3}\right)}_{a \in \mathcal{O}_L}$$

(d) D'après (c)

$$-p + p\lambda a = \lambda^{p-1} \Rightarrow p = -\lambda^{p-1} + p\lambda a$$
$$= \lambda(-\lambda^{p-2} + pa) \in \lambda\mathcal{O}_L$$

$$\Rightarrow \mathfrak{p} = (p, \lambda) = \lambda\mathcal{O}_L$$
$$p\mathcal{O}_L = \mathfrak{p}^{p-1} = \lambda^{p-1}\mathcal{O}_L$$

(3) $\zeta^i - 1 = (\zeta - 1)\cdot u$, $u \in \mathcal{O}_L^*$

$$\Rightarrow (\zeta^i - 1)\mathcal{O}_L = (\zeta - 1)\mathcal{O}_L = \lambda\mathcal{O}_L$$

(4). On a

$$\sum_{0\le i\le p-1} \zeta^i = -(\text{Coefficient en } X^{p-1} \text{ de } X^p - 1)$$

$$= 0.$$

Car $X^p - 1 = \prod_{0\le i\le p-1} (X - \zeta^i)$.

Comme $p \neq 2$, ζ^2 est une racine primitive p-ième de l'unité, donc

$$\sum_{0\le i\le p-1} (\zeta^2)^i = 0.$$

Il suit que $\sum_{0\le i\le p-1} \zeta^i(\alpha + \zeta^i\beta) = 0.$

Exercice 5.

(1) D'après l'exercice 4.2.b,

$$\mathcal{O}_L = \mathbb{Z} + \mathfrak{p}$$

et $\mathfrak{p} = \lambda \mathcal{O}_L$ d'après 4.2.d.

D'où $\mathcal{O}_L = \mathbb{Z} + \lambda\mathcal{O}_L$

$$= \mathbb{Z} + \lambda(\mathbb{Z} + \lambda\mathcal{O}_L)$$

$$= \mathbb{Z} + \lambda\mathbb{Z} + \lambda^2\mathcal{O}_L$$

Donc $\alpha = k + \lambda r + \lambda^2 \alpha'$

avec $k, r \in \mathbb{Z}$ et $\alpha' \in \mathcal{O}_L$

Il existe $k_0 \in \mathbb{Z} \cap \left[-\frac{p-1}{2}, \frac{p+1}{2}\right]$ t.q.

$$k = k_0 + p k_1, \qquad k_1 \in \mathbb{Z}.$$

$$\Rightarrow \quad \alpha = k_0 + \lambda r + \lambda^2 \left(\alpha' + \frac{p}{\lambda^2} k_1\right)$$

avec $\frac{p}{\lambda^2} k_1 \in \mathcal{O}_L$ d'après l'ex. 4.2(d).

(b) On développe

$$\alpha^k = \left(k + \lambda r + \lambda^2 \alpha'\right)^p = (k + \lambda r)^p + p(\lambda^2 \alpha')(\quad) \underbrace{\in \mathcal{O}_L}.$$

$$+ \lambda^{2p} \alpha'^p$$

$$\left((x+y)^p = x^p + p y (x^{p-1} + \dots) + y^p \right)$$

$$p \mid \binom{p}{k} \quad 1 \le k \le p-1$$

$$\lambda^{2p} = \lambda^{p-1} \cdot \lambda^2 \cdot \lambda^{p-1} \in p \lambda^2 \mathcal{O}_L$$

$$(k + \lambda r)^p = k^p + p k^{p-1} \lambda r + p (\lambda r)^2 * + \lambda^p r^p$$

$$= k^p + p k^{p-1} \lambda r + \lambda^p r^p + p \lambda^2 *$$

(ici, $*$ veut dire un élément de $\mathcal{O}_L$)

Enfin $\frac{\lambda^{p-1}}{p} = -1 + \lambda a$ d'après 4.2(c).

(c) $\forall x \in \mathbb{F}_p$ on a $x^p = x$,

donc $\forall s \in \mathbb{Z}$ $\quad s^p \equiv s \ [p]$.

si $s \notin p\mathbb{Z}$, $\quad \overline{s} \in \mathbb{F}_p^* \Rightarrow \overline{s}^{p-1} = \overline{1} \in \mathbb{F}_p$

(d) Comme $\alpha \notin \lambda \mathcal{O}_L$ et que $p \in \lambda \mathcal{O}_L$,

on a $k \notin p\mathbb{Z}$, donc $k^{p-1} \equiv 1 \ [p]$

$\Rightarrow \quad k^{p-1} r - r^p \equiv r - r^p \equiv 0 \ [p]$

$\Rightarrow \quad k^{p-1} r - r^p \in p\mathbb{Z} \subset \lambda \mathcal{O}_L$.

et $\quad \alpha^p - k^p \in p\lambda^2 \mathcal{O}_L = \lambda^{p+1} \mathcal{O}_L$

$(\ p\mathcal{O}_L = \lambda^{p-1}\mathcal{O}_L\ )$

(2).

(a) On a $\quad \alpha^p + \beta^p = -u\gamma^p \in \lambda^p \mathcal{O}_L$

$\Rightarrow \quad k^p + m^p \in -\alpha^p - \beta^p + \lambda^{p+1}\mathcal{O}_L \in \lambda^p \mathcal{O}_L \subseteq \lambda \mathcal{O}_L$

$\begin{cases} k^p + m^p \in \mathbb{Z} \end{cases}$

$\Rightarrow \quad k^p + m^p \in \lambda \mathcal{O}_L \cap \mathbb{Z} = \mathbb{Q} \cap \mathbb{Z} = p\mathbb{Z}$

$\Rightarrow \quad k + m \equiv k^p + m^p \equiv 0 \ [p]$

(b) Comme $\left(\frac{p-1}{2}\right) \leq k, m \leq \frac{p+1}{2} \Rightarrow -(p+1) \leq k + m \leq p-1$

$p \mid k+m \Rightarrow \quad k+m = 0 \Rightarrow k^p + m^p = 0$

$\Rightarrow \quad u\gamma^p = -\alpha^p - \beta^p \in k^p + m^p + \lambda^{p+1}\mathcal{O}_L = \lambda^{p+1}\mathcal{O}_L$

$\Rightarrow \quad u\gamma^p \in \lambda^{p+1}\mathcal{O}_L$ Comme $u \in \mathcal{O}^*$, on a

$\gamma^p \in \lambda^{p+1}\mathcal{O}_L$. donc $\gamma \in \lambda^2 \mathcal{O}_L$.

(3). $\quad 0 \leq i \neq j \leq p-1$

(a) $\quad (\alpha + \zeta^i \beta) - (\alpha + \zeta^j \beta)$

$= (\zeta^i - \zeta^j)\beta = \zeta^j(\zeta^{i-j} - 1)\beta$

$= \left(\zeta^j \cdot \frac{\zeta^{i-j}-1}{\zeta - 1}\right)(\zeta - 1)\beta$

comme $p \nmid j$, $p \nmid i-j$, on a

$\zeta^j, \frac{\zeta^{i-j}-1}{\zeta-1} \in \mathcal{O}_L^*$

$\zeta - 1 = \lambda$

$\beta \notin \lambda \mathcal{O}_L$.

Donc $(\alpha + \zeta^i \beta) - (\alpha + \zeta^j \beta) \in \lambda \mathcal{O}_L$

$\notin \lambda^2 \mathcal{O}_L$.

(b) On a

$$\prod_{0\le i\le p-1}(\alpha+\zeta^i\beta) \in \lambda\mathcal{O}_L$$

et $\lambda\mathcal{O}_L = \mathfrak{P}$ est premier, donc un des facteurs $\alpha+\zeta^i\beta \in \lambda\mathcal{O}_L$. Il suit de (a) que $\alpha+\zeta^i\beta \in \lambda\mathcal{O}_L \ \forall\ 0\le i\le p-1$.

(c) On a $\prod_{i=0}^{p-1}\left(\frac{\alpha+\zeta^i\beta}{\lambda}\right) = u\left(\frac{\gamma}{\lambda}\right)^p \in \lambda^p\mathcal{O}_L \subseteq \lambda\mathcal{O}_L$

(question (2)).

Donc λ divise un $\frac{\alpha+\zeta^{i_0}\beta}{\lambda}$.

Il ne divise pas les autres d'après (a).

(d) Si $\alpha+\zeta^i\beta,\ \alpha+\zeta^j\beta \in \lambda\mathfrak{m}$, alors

$$\zeta^i\beta-\zeta^j\beta \in \lambda\mathfrak{m}$$

On a vu dans (a) que le terme de gauche est égal à $u'\lambda\beta$, $u'\in\mathcal{O}_L^*$.

Donc $\beta\in\mathfrak{m} \Rightarrow \alpha=(\alpha+\zeta^i\beta)-\zeta^i\beta\in\mathfrak{m}$.

(e) Sinon, il existe

$$0 < i - j \leq p-1$$

et m maximal de $\mathcal{O}_L$ tels que

$$\frac{\alpha + \zeta^i \beta}{\lambda} \quad \frac{\alpha + \zeta^j \beta}{\lambda} \in m.$$

Il suit de (d) que $\alpha, \beta \in m$

Contradiction.

Exercice 6.

(1) Cours.

(2) On sait que $\mathcal{O}_L$ est principal (exercice 1)

Par Bézout,

$$a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$$

Donc $a\mathcal{O}_L + b\mathcal{O}_L = c\mathcal{O}_L$

Donc $c = pgcd(a, b)$ dans $\mathcal{O}_L$.

~~(3) (a) D'après~~

(3) (a) On a

$$-u\gamma^3 = (\alpha+\beta)(\alpha+\zeta\beta)(\alpha+\zeta^2\beta)$$

$$-u\left(\frac{\gamma}{\lambda}\right)^3 = \underbrace{\left(\frac{\alpha+\beta}{\lambda}\right)\left(\frac{\alpha+\zeta\beta}{\lambda}\right)\left(\frac{\alpha+\zeta^2\beta}{\lambda}\right)}$$

2 à 2 permis entre eux

d'après l'ex. 5.3(e)

Comme Q est principal, chaque facteur de droite est un cube modulo une unité.

(b) D'après l'ex. 4.4, on a

$$(\alpha+\beta) + \zeta(\alpha+\zeta^2\beta) + \zeta^2(\alpha+\zeta\beta) = 0$$

Donc $$u_0\delta_0^3 + (\zeta u_1)\delta_1^3 + \zeta^2 u_2 \delta_2^3 = 0$$

$$\Rightarrow \quad \delta_1^3 + \underbrace{(\zeta u_2 u_1^{-1})}_{w_2}\delta_2^3 + \underbrace{(\zeta u_1 u_0^{-1})}_{w_0}\delta_0^3 = 0$$

avec $w_0, w_2 \in Q^*$ car $u_0, u_1, u_2, \zeta \in Q^*$

(c) Comme $\delta_0 \in \lambda\mathcal{O}_L$, on a

$$w_0 \delta_0^3 \equiv 0 \quad [\lambda^3]$$

Donc $\quad \delta_1^3 + w_2 \delta_2^3 \equiv 0 \quad [\lambda^3]$.

D'après l'ex. 5.1 (d), $\quad \delta_1^3 \equiv \pm 1 \quad [\lambda^4]$

$$\delta_2^3 \equiv \pm 1 \quad [\lambda^4]$$

(les seuls entiers k premiers à 3 et compris entre $-\frac{3-1}{2}$ et $\frac{3-1}{2}$ sont 1 et -1).

Donc $\quad \pm 1 \pm w_2 \equiv 0 \quad [\lambda^3]$

$$\Rightarrow \quad w_2 \equiv \pm 1 \quad [\lambda^3].$$

(d) $\mathcal{O}_L^* = \{\pm 1, \pm\zeta, \pm\zeta^2\}$ d'après l'ex. 1.4. Comme

$$\zeta - 1, \ \zeta^2 - 1, \ \zeta^2 - \zeta \in \lambda\mathcal{O}_L^*$$

$$1 + \zeta = -\zeta^2, \ 1 + \zeta^2 = -\zeta, \ \zeta + \zeta^2 = -1 \in \mathcal{O}_L^*$$

On voit que $w_2 = \pm 1$.

$\Rightarrow \delta_1^3 + (w_2\delta_2)^3 + w_0\delta_0^3 = 0.$

Il suit de l'ex. 5.1.2 que $d^2 \mid \delta_0$.

(e). Comme $v_d(\delta_0) \in \mathbb{N}$, on ne peut pas continuer le processus en définissant.

(4). On utilise (1), (2) et (3).