

## Feuille 5 : Corps de classe

Soit  $K$  un corps de nombres. On appelle *cycle arithmétique* ou *module* un produit formel de places

$$\mathcal{M} = \prod_{v \in S_K} \mathcal{P}_v^{e_v}$$

où  $e_v \geq 0$  est de support fini, et  $e_v \in \{0, 1\}$  si  $v$  est réelle et  $e_v = 0$  si  $v$  est complexe (ici  $\mathcal{P}_v$  est l'idéal maximal de  $\mathcal{O}_K$  associé à  $v$  si  $v$  est non archimédienne et il est juste un symbole si  $v$  est archimédienne). On le voit également comme la donnée d'un idéal entier  $\mathcal{M}_f$  de  $\mathcal{O}_K$  et d'un sous-ensemble  $\mathcal{M}_\infty$  de places réelles. Soit  $\mathcal{M} = \prod_{v \in S_K} \mathcal{P}_v^{e_v}$  un module. Pour  $(x_v)_{v \in S_K}$  on écrit  $x \equiv 1 \pmod{\mathcal{M}}$  si  $x_v \equiv 1 \pmod{\mathcal{P}_v^{e_v}}$  pour tout  $v \in S_K$ , avec la convention que  $x_v \equiv 1 \pmod{\mathcal{P}_v^{e_v}}$  signifie :

- la congruence habituelle si  $v$  est non archimédienne et  $e_v > 0$  ;
- $x \in \mathcal{O}_{K_v}^*$  si  $v$  est non archimédienne et  $e_v = 0$  ;
- $x_v > 0$  si  $v$  est réelle et  $e_v = 1$  ;
- aucune condition sinon.

On note  $\mathcal{I}(K)^\mathcal{M}$  le sous-groupe du groupe  $\mathcal{I}(K)$  des idéaux fractionnaires de  $K$  engendrés par les idéaux de  $\mathcal{O}_K$  premiers à  $\mathcal{M}$ . On écrit  $\mathcal{P}(K)^\mathcal{M}$  pour le sous-groupe de  $\mathcal{I}(K)^\mathcal{M}$  engendré par les idéaux principaux de  $K$  de la forme  $a\mathcal{O}_K$ , avec  $a \neq 0$  et  $a - 1 \in \mathcal{P}_v^{e_v}$  pour tous  $v$  place fini et  $a_v > 0$  si  $v$  est une place infinie avec  $e_v = 1$ . On pose

$$\mathbb{A}_K^*(\mathcal{M}) = \{(x_v)_{v \in S_K} \text{ tel que } x_v \equiv 1 \pmod{\mathcal{P}_v^{e_v}} \forall v \in S_K\}$$

On note  $C_K^\mathcal{M} = \mathbb{A}_K^*(\mathcal{M}) \cdot K^*/K^*$  et  $\text{Cl}(K)^\mathcal{M} = \mathcal{I}(K)^\mathcal{M}/\mathcal{P}(K)^\mathcal{M} \cong C_K/C_K^\mathcal{M}$  le groupe de classes de rayon  $\mathcal{M}$  (où  $C_K = \mathbb{A}_K^*/K^*$ ). On écrit  $H^\mathcal{M}$  pour le corps de classes de rayon  $\mathcal{M}$ .

**Exercice 1.** Soit  $p$  un nombre premier impair. Combien existe-t-il d'extensions de  $\mathbb{Q}_p$  ayant pour groupe de Galois  $\mathbb{Z}/p\mathbb{Z}$ ? Combien sont-elles non ramifiées?

**Indications 1.** Il faut trouver les sous-groupes de  $\mathbb{Q}_p^*$  d'indice  $p$ . On a

$$\mathbb{Q}_p^* \cong \mathbb{Z}_p^* \times p^\mathbb{Z} \cong (1 + p\mathbb{Z}_p) \times \mu_{p-1} \times p^\mathbb{Z} \cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}$$

Un sous-groupe  $\mathbb{Q}_p^*$  d'indice  $p$  contient  $x^p$  pour tout  $x \in \mathbb{Q}_p^*$ . On a

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{\times p} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Il y a  $p+1$  sous-groupes non triviaux de  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  (les droites) et chacun correspond à un sous-groupe de  $\mathbb{Q}_p^*$  d'indice  $p$ . Il y a donc  $p+1$  extensions  $L/\mathbb{Q}_p$  telles que  $\text{Gal}(L/\mathbb{Q}_p) \cong \mathbb{Z}/p\mathbb{Z}$ . Une seule est non ramifiée.

**Exercice 2.** Soit  $L/K$  une extension finie abélienne de corps locaux  $p$ -adiques. Montrer qu'elle est non ramifiée si et seulement si  $\mathcal{O}_K^* \subseteq \text{Norm}_{L/K}(L^*)$  (dans ce cas  $L$  est la seule extension non ramifiée de degré  $[L : K]$  de  $K$ ).

**Indications 2.** Si  $L/K$  est non ramifiée, alors  $\text{Norm}_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*$  et donc  $\mathcal{O}_K^* \subseteq \text{Norm}_{L/K}(L^*)$ . Pour le réciproque, soit  $n = [L : K]$ , On a

$$K^* \cong \pi_K^{\mathbb{Z}} \times \mathcal{O}_K^*$$

où  $\pi_K$  est une uniformisante de  $K$ . Or,  $\text{Norm}_{L/K}(L^*)$  contient  $\mathcal{O}_K^*$  par hypothèse et donc

$$\text{Norm}_{L/K}(L^*) = \pi_K^{d\mathbb{Z}} \times \mathcal{O}_K^*$$

pour un certain  $d$  et forcément  $d = n$  car  $\text{Gal}(L/K) \cong K^*/\text{Norm}_{L/K}(L^*) \cong \mathbb{Z}/d\mathbb{Z}$  doit avoir  $n$  éléments. Si  $\pi_L$  est une uniformisante de  $L$  on a

$$1 = v_L(\pi_L) = \frac{1}{f} v_K(\text{Norm}_{L/K}(\pi_L))$$

où  $f$  est le degré d'inertie de l'extension  $L/K$ . En particulier,  $\text{Norm}_{L/K}(\pi_L) = u\pi_K^f$  ou  $u \in \mathcal{O}_K^*$ . Vu qu'on a supposé  $\mathcal{O}_K^* \subseteq \text{Norm}_{L/K}(L^*)$  on obtient  $\pi_K^f \in \text{Norm}_{L/K}(L^*) = \pi_K^{n\mathbb{Z}} \times \mathcal{O}_K^*$  ce qui implique  $n \leq f$ , donc  $n = f$  et l'extension est non ramifiée.

**Exercice 3.** Soit  $L/K$  une extension finie abélienne de corps locaux  $p$ -adiques. Montrer qu'elle est totalement ramifiée si et seulement si  $\text{Norm}_{L/K}(L^*)$  contient une uniformisante de  $\mathcal{O}_K$ .

**Indications 3.** Si  $L/K$  est totalement ramifiée et  $\pi$  est une uniformisante de  $\mathcal{O}_L$ , alors  $L = K(\pi)$  et le polynôme minimal  $P$  de  $\pi$  est Eisenstein. La norme de  $\pi$  est donc le terme constant de  $P$ , qui est une uniformisante de  $\mathcal{O}_K$ . Pour le réciproque, soit  $\pi$  une uniformisante de  $\mathcal{O}_K$  tel que  $\pi \in \text{Norm}_{L/K}(L^*)$  et soit  $M \subseteq L$  la plus grande sous-extension non ramifiée de  $K$  : en raisonnant comme dans l'exercice précédent on a que

$$\text{Norm}_{M/K}(M^*) = \pi^{f\mathbb{Z}} \times \mathcal{O}_K^*$$

où  $f = [M : K]$ . D'autre part, par transitivité de la norme,  $\text{Norm}_{L/K}(L^*) \subseteq \text{Norm}_{M/K}(M^*)$ , donc  $\pi \in \text{Norm}_{M/K}(M^*)$  et  $f = 1$ .

**Exercice 4.** On considère le corps  $K = \mathbb{Q}$ .

1. Quels sont les diviseurs arithmétiques ?
2. Supposons  $\mathcal{M} = 1$ .
  - (a) Expliciter  $\mathcal{I}(\mathbb{Q})^{\mathcal{M}}$  et  $\mathcal{P}(\mathbb{Q})^{\mathcal{M}}$  puis déterminer  $\text{Cl}(\mathbb{Q})^{\mathcal{M}}$ .
  - (b) Expliciter  $\mathbb{A}_{\mathbb{Q}}^*(\mathcal{M})$  et  $C_{\mathbb{Q}}^{\mathcal{M}}$ . Vérifier que

$$C_{\mathbb{Q}}/C_{\mathbb{Q}}^{\mathcal{M}} \cong \text{Cl}(\mathbb{Q})^{\mathcal{M}}$$

En déduire que

$$C_{\mathbb{Q}} \cong \left( \mathbb{R}^* \times \prod_p \mathbb{Z}_p^* \right) / \{\pm 1\}$$

(c) Déterminer  $H^{\mathcal{M}}$ .

3. Mêmes questions pour  $\mathcal{M} = (\infty)$ , en déduisant que

$$C_{\mathbb{Q}} \cong \mathbb{R}_{>0}^* \times \prod_p \mathbb{Z}_p^*$$

(Attention : cette dernière décomposition n'est pas utile dans la pratique, car elle ne respecte pas l'inclusion diagonale.)

4. Mêmes questions pour  $\mathcal{M} = (5)$ .

5. Mêmes questions pour  $\mathcal{M} = ((5)\infty)$  (pour la dernière question, considérer le corps  $\mathbb{Q}(\zeta_5)$ ).

**Indications 4.** 1. Ils sont de la forme  $(n)$  ou  $((n)\infty)$  pour  $n \in \mathbb{N}_{>0}$ .

2. (a) On a  $\mathcal{I}(\mathbb{Q})^1 = \mathcal{P}(\mathbb{Q})^1 = \mathcal{I}(\mathbb{Q})$  donc  $\text{Cl}(\mathbb{Q})^1 = 1 = \text{Cl}(\mathbb{Q})$ .

(b) Par définition

$$\mathbb{A}_{\mathbb{Q}}^*(1) = \mathbb{R}^* \times \prod_p \mathbb{Z}_p^*.$$

On a  $\mathbb{A}_{\mathbb{Q}}^*(1) \cdot \mathbb{Q}^* = \mathbb{A}_{\mathbb{Q}}^*$ . En particulier,  $C_{\mathbb{Q}}^1 = \mathbb{A}_{\mathbb{Q}}^*(1)\mathbb{Q}^*/\mathbb{Q}^* = \mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q}^* = C_{\mathbb{Q}}$ , donc  $C_{\mathbb{Q}}/C_{\mathbb{Q}}^1 = 1$ . En particulier,

$$C_{\mathbb{Q}} = \left( \mathbb{R}^* \times \prod_p \mathbb{Z}_p^* \right) \cdot \mathbb{Q}^*/\mathbb{Q}^*$$

Vu que

$$\left( \mathbb{R}^* \times \prod_p \mathbb{Z}_p^* \right) \cap \mathbb{Q}^* = \{\pm 1\}$$

on trouve

$$C_{\mathbb{Q}} \cong \left( \mathbb{R}^* \times \prod_p \mathbb{Z}_p^* \right) / \{\pm 1\}$$

(c) On a évidemment  $H^1 = \mathbb{Q}$ .

3. (a) On a  $\mathcal{I}(\mathbb{Q})^{(\infty)} = \mathcal{I}(\mathbb{Q})$  et  $\mathcal{P}(\mathbb{Q})^{(\infty)} = \{(a) \text{ tels que } a \in \mathbb{Q}_{>0}^{\times}\}$  et  $\text{Cl}(\mathbb{Q})^{(\infty)} = 1 = \text{Cl}(\mathbb{Q})$ .

(b) Par définition

$$\mathbb{A}_{\mathbb{Q}}^*((\infty)) = \mathbb{R}_{>0}^* \times \prod_p \mathbb{Z}_p^*.$$

On a  $\mathbb{A}_{\mathbb{Q}}^*((\infty)) \cdot \mathbb{Q}^* = \mathbb{A}_{\mathbb{Q}}^*$  : si  $x = (x_{\infty}, x_p) \in \mathbb{A}_{\mathbb{Q}}^*$ , quitte à multiplier pour un nombre naturel on peut supposer  $x_p \in \mathbb{Z}_p^*$  pour tout  $p$ , et quitte à multiplier par  $-1$  on peut supposer  $x_{\infty} > 0$  et donc  $x \in \mathbb{A}_{\mathbb{Q}}^*((\infty)) \cdot \mathbb{Q}^*$ . En particulier,  $C_{\mathbb{Q}}^{(\infty)} = \mathbb{A}_{\mathbb{Q}}^*((\infty))\mathbb{Q}^*/\mathbb{Q}^* = \mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q}^* =$

$C_{\mathbb{Q}}$ , donc  $C_{\mathbb{Q}}/C_{\mathbb{Q}}^{(\infty)} = 1$  (bien évidemment cela suit immédiatement du fait que  $\text{Cl}(\mathbb{Q})^{(\infty)} \cong C_{\mathbb{Q}}/C_{\mathbb{Q}}^{(\infty)}$ ), c'est-à-dire,

$$C_{\mathbb{Q}} = \left( \mathbb{R}_{>0}^* \times \prod_p \mathbb{Z}_p^* \right) \cdot \mathbb{Q}^*/\mathbb{Q}^*$$

On a cette fois

$$\left( \mathbb{R}_{>0}^* \times \prod_p \mathbb{Z}_p^* \right) \cap \mathbb{Q}^* = \{1\}$$

et donc

$$C_{\mathbb{Q}} \cong \mathbb{R}_{>0}^* \times \prod_p \mathbb{Z}_p^*$$

(c) On a évidemment  $H^{(\infty)} = \mathbb{Q}$ .

On a montré que  $C_{\mathbb{Q}} = C_{\mathbb{Q}}^{(\infty)}$  et on a

$$C_{\mathbb{Q}}^{(\infty)} = \mathbb{A}_{\mathbb{Q}}^*((\infty))\mathbb{Q}^*/\mathbb{Q}^* \cong \mathbb{A}_{\mathbb{Q}}^*((\infty))/(\mathbb{Q}^* \cap \mathbb{A}_{\mathbb{Q}}^*((\infty))) = \mathbb{A}_{\mathbb{Q}}^*((\infty))$$

car  $\mathbb{Q}^* \cap \mathbb{A}_{\mathbb{Q}}^*((\infty)) = \{1\}$ .

4. (a) On a

$$\mathcal{I}(\mathbb{Q})^{(5)} = \{(1), (1/2), (2), (1/3), \dots, (a/b) \text{ tels que } a, b \not\equiv 0 \pmod{5}\}$$

et

$$\mathcal{P}(\mathbb{Q})^{(5)} = \{(1), (2/3), (3/2), (1/4), (4), (6), (1/6), (2/7), (7/2), \dots, (a/b) \text{ tels que } a \equiv \pm b \pmod{5} \text{ et } \text{pgcd}(a, b) = 1\}$$

On en déduit que

$$\text{Cl}(\mathbb{Q})^{(5)} = \{[(1)], [(2)]\}$$

est un groupe avec 2 éléments ( $[1]$  correspond à  $a \equiv \pm b$  et  $[2]$  à  $a \equiv \pm b + 1$  et il n'y a pas d'autres possibilités).

(b) On a

$$\mathbb{A}_{\mathbb{Q}}^*((5)) = \mathbb{R}^* \times \prod_{p \neq 5} \mathbb{Z}_p^* \times (1 + 5\mathbb{Z}_5)$$

et donc

$$C_{\mathbb{Q}}^{(5)} = \mathbb{A}_{\mathbb{Q}}^*((5)) \cdot \mathbb{Q}^*/\mathbb{Q}^* = \left( \mathbb{R}^* \times \prod_{p \neq 5} \mathbb{Z}_p^* \times (1 + 5\mathbb{Z}_5) \right) \cdot \mathbb{Q}^*/\mathbb{Q}^*$$

On a

$$\begin{aligned} C_{\mathbb{Q}}/C_{\mathbb{Q}}^{(5)} &= C_{\mathbb{Q}}^1/C_{\mathbb{Q}}^{(5)} \cong \\ &\left( \left( \mathbb{R}^* \times \prod_p \mathbb{Z}_p^* \right) \cdot \mathbb{Q}^* \right) / \left( \mathbb{R}^* \times \prod_{p \neq 5} \mathbb{Z}_p^* \times (1 + 5\mathbb{Z}_5) \right) \cdot \mathbb{Q}^* \cong \\ &\left( \mathbb{R}^* \times \prod_p \mathbb{Z}_p^* \right) / \left( \mathbb{R}^* \times \prod_{p \neq 5} \mathbb{Z}_p^* \times (1 + 5\mathbb{Z}_5) \right) \cdot \{\pm 1\} \end{aligned}$$

où pour le dernier isomorphisme on utilise que  $(\mathbb{R}^* \times \prod_p \mathbb{Z}_p^*) \cap \mathbb{Q}^* = \{\pm 1\}$  (on peut facilement écrire l'isomorphisme à la main, le seul point pas trivial est que un élément de  $(\mathbb{R}^* \times \prod_p \mathbb{Z}_p^*) \cdot \mathbb{Q}^*$  s'écrit de manière *presque* unique comme un produit, la seule ambiguïté est le signe de la partie rationnelle). On en déduit

$$\begin{aligned} C_{\mathbb{Q}}/C_{\mathbb{Q}}^{(5)} &\cong \mathbb{Z}_5^*/((1 + 5\mathbb{Z}_5) \cdot \{\pm 1\}) \cong \\ &(\mathbb{Z}_5^*/(1 + 5\mathbb{Z}_5))/\{\pm 1\} \cong (\mathbb{Z}/5\mathbb{Z})^*/\{\pm 1\} \end{aligned}$$

- (c) On a que  $\text{Gal}(H^{(5)}/\mathbb{Q}) \cong \text{Cl}(\mathbb{Q})^{(5)}$  est un groupe à 2 éléments, donc  $H^{(5)} = \mathbb{Q}(\sqrt{d})$  pour un certain  $d$ . La compatibilité locale-globale et l'exercice précédent impliquent que  $H^{(5)}$  est non ramifié en dehors de (5), donc  $d = 5$  et  $H^{(5)} = \mathbb{Q}(\sqrt{5})$ . Le fait que  $d$  ne peut pas être  $-5$  est une conséquence du fait que  $H^{(5)}$  est non ramifiée en (2) ou qu'elle est non ramifié en  $\infty$  (attention à la place  $\infty$  : non ramifiée en  $\infty$  signifie réelle).

5. (a) On a

$$\mathcal{I}(\mathbb{Q})^{(5)\infty} = \{(1), (1/2), (2), (1/3), \dots, (a/b) \text{ tels que } a, b \not\equiv 0 \pmod{5}\}$$

et

$$\begin{aligned} \mathcal{P}(\mathbb{Q})^{(5)\infty} &= \{(1), (6), (1/6), (2/7), (7/2), \dots, \\ &(a/b) \text{ tels que } a \equiv b \pmod{5} \text{ et } \text{pgcd}(a, b) = 1\} \end{aligned}$$

On en déduit que

$$\text{Cl}(\mathbb{Q})^{(5)\infty} = \{[(1)], [(2)], [(3)], [(4)]\}$$

est un groupe cyclique avec 4 éléments.

(b) On a

$$\mathbb{A}_{\mathbb{Q}}^*((5)\infty) = \mathbb{R}_{>0}^* \times \prod_{p \neq 5} \mathbb{Z}_p^* \times (1 + 5\mathbb{Z}_5)$$

En raisonnant comme ci-dessus on trouve

$$\begin{aligned} \mathbb{C}_{\mathbb{Q}}/C_{\mathbb{Q}}^{(5)\infty} &\cong (\mathbb{R}^*/\mathbb{R}_{>0}^* \times \mathbb{Z}_5^*/(1 + 5\mathbb{Z}_5))/\{\pm 1\} \cong \\ &(\mathbb{R}^*/\mathbb{R}_{>0}^* \times (\mathbb{Z}/5\mathbb{Z})^*)/\{\pm 1\} \cong (\mathbb{Z}/5\mathbb{Z})^* \end{aligned}$$

où le dernier isomorphisme est donné par  $x \in (\mathbb{Z}/5\mathbb{Z})^* \mapsto (1, x)$ .

(c) Soit  $L = \mathbb{Q}(\zeta_5)$ , on montre que  $H^{(5)\infty} = L$ . Il suffit de prouver que le sous-groupe de  $C_{\mathbb{Q}}$  associé à  $L$  est  $C_{\mathbb{Q}}^{(5)\infty}$ . On calcul le noyau de l'homomorphisme d'Artin global  $\theta: \mathbb{A}_{\mathbb{Q}}^* \rightarrow \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = (\mathbb{Z}/5\mathbb{Z})^*$ , c'est-à-dire l'image de la norme  $\text{Norm}_{L/\mathbb{Q}}: C_L \rightarrow C_{\mathbb{Q}}$ . Cela revient à calculer l'image de la norme entre les différents complétés. Il y a trois cas :

- L'extension est complexe donc ramifié en  $\infty$  et l'image en  $\infty$  est  $\mathbb{R}_{>}$ .
- si  $p \neq 5$ , alors  $p$  est un premier non ramifié dans  $\mathbb{Q}(\zeta_5)$ . Si  $v$  est une place de  $L$  au-dessus de  $p$ , l'image de  $\text{Norm}_{L_v/\mathbb{Q}_p}$  contient donc  $\mathbb{Z}_p^*$ .
- pour  $p = 5$ , on regard l'image de la norme dans  $\mathbb{Q}_5^*$ . On sait que  $\mathbb{Q}(\zeta_5)/\mathbb{Q}$  est totalement ramifiée en 5 et donc l'image  $N = \text{Norm}_{\mathbb{Q}_5(\zeta_5)/\mathbb{Q}_5}(\mathbb{Q}_5(\zeta_5)^*)$  contient une uniformisante. En effet on peut être plus précis : la norme de  $\zeta_5 - 1$  vaut  $5 \in N$ . On a la décomposition

$$\mathbb{Q}_5^* = 5^{\mathbb{Z}} \times \mu_4 \times (1 + 5\mathbb{Z}_5)$$

De plus,

$$\mathbb{Q}_5^*/N \cong \text{Gal}(\mathbb{Q}_5(\zeta_5)/\mathbb{Q}_5) = \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = (\mathbb{Z}/5\mathbb{Z})^*,$$

donc  $N$  est d'indice 4 dans  $\mathbb{Q}_5^*$  et donc  $1 + 5\mathbb{Z}_5 \subseteq N$ . On en déduit que  $N = 5^{\mathbb{Z}} \times \{1\} \times (1 + 5\mathbb{Z}_5)$ .

En utilisant l'isomorphisme

$$C_{\mathbb{Q}} \cong \left( \mathbb{R}^* \times \prod_p \mathbb{Z}_p^* \right) / \{\pm 1\}$$

on a que que l'image de la norme  $\text{Norm}_{L/\mathbb{Q}}: C_L \rightarrow C_{\mathbb{Q}}$  est exactement  $C((5)\infty)$  comme on voulait.

On peut aussi calculer l'image d'une idèle  $x = (x_v)$  dans  $\mathbb{A}_{\mathbb{Q}}^*((5)\infty)$  par l'homomorphisme d'Artin global  $\theta: \mathbb{A}_{\mathbb{Q}}^* \rightarrow \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ , qui est donné par les homomorphismes d'Artin locaux

$$\theta_v: \mathbb{Q}(\zeta_5)^* \rightarrow \text{Gal}(\mathbb{Q}(\zeta_5)_v/\mathbb{Q}_p) \subseteq \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$$

En raisonnant comme ci-dessus, on a que

- $\theta_{\infty}(x_{\infty}) = v$  et donc  $\theta_{\infty}(x_{\infty}) = 1$  si  $x \in \mathbb{A}_{\mathbb{Q}}^*((5)\infty)$ .
- si  $p \neq 5$ ,  $\theta_v(up^v) = p \in (\mathbb{Z}/5\mathbb{Z})^*$  : en effet l'image d'une uniformisante  $\pi_v$  est la substitution de Frobenius de  $\mathbb{Q}(\zeta_5)$  en  $p$ , qui envoie  $\zeta_5$  sur  $\zeta_5^p$ . En particulier  $\theta_p(x_p) = 1$  si  $x \in \mathbb{A}_{\mathbb{Q}}^*((5)\infty)$ .
- $\theta_5(x_5) = 1$  car  $x_5 \in 1 + 5\mathbb{Z}_5$ .

Finalement,  $\theta(x) = 1$  si  $x \in \mathbb{A}_{\mathbb{Q}}^*((5)\infty)$ . On a donc  $\mathbb{A}_{\mathbb{Q}}^*((5)\infty) \subseteq \ker(\theta)$ , et  $C_{\mathbb{Q}}((5)\infty) \subseteq \ker(\tilde{\theta})$  où  $\tilde{\theta}: C_{\mathbb{Q}} \rightarrow \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ . On obtient

$$C_{\mathbb{Q}}((5)\infty) = \ker(\tilde{\theta})$$

car les deux ont indice 4.

**Exercice 5.** Soient  $a$  et  $b$  des entiers premiers entre eux.

1. Montrer que

$$\mathbb{Q}(\zeta_a)\mathbb{Q}(\zeta_b) = \mathbb{Q}(\zeta_{ab})$$

et en déduire que si  $a \geq 3$  alors un premier  $p$  est ramifié dans  $\mathbb{Q}(\zeta_a)$  si et seulement si  $p \mid a$ .

2. Montrer que

$$\mathbb{Q}(\zeta_a) \cap \mathbb{Q}(\zeta_b) = \mathbb{Q}$$

3. En déduire que  $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ .

**Indications 5.** 1.  $\zeta_a \zeta_b$  est une racine primitive  $ab$ -ème de l'unité, donc  $\mathbb{Q}(\zeta_{ab}) \subseteq \mathbb{Q}(\zeta_a)\mathbb{Q}(\zeta_b)$ . L'autre inclusion est évidente.

On écrit  $a = \prod_p p^{e_p}$ , on a alors

$$\mathbb{Q}(\zeta_a) = \prod_p \mathbb{Q}(\zeta_{p^{e_p}})$$

et  $\mathbb{Q}(\zeta_a)/\mathbb{Q}$  est non ramifiée en  $p$  si et seulement si chaque  $\mathbb{Q}(\zeta_{p^{e_p}})/\mathbb{Q}$  est non ramifiée en  $p$ .

2. Soit  $K$  l'intersection. Si  $K \neq \mathbb{Q}$ , il existe  $p$  qui est ramifié dans  $K$  et il est donc ramifié dans  $\mathbb{Q}(\zeta_a)$  et  $\mathbb{Q}(\zeta_b)$ , donc  $p \mid a$  et  $p \mid b$ , absurde.
3. Si  $K$  et  $L$  sont linéairement disjoints avec discriminants premiers entre eux, on a  $\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L$ .

**Exercice 6.** On considère encore le corps  $K = \mathbb{Q}$  et soit  $n \in \mathbb{N}$ .

1. Montrer que le groupe de classes d'idèles de rayon  $\mathcal{M}$  de  $\mathbb{Q}$  est isomorphe à  $(\mathbb{Z}/n\mathbb{Z})^*/\{\pm 1\}$  si  $\mathcal{M} = (n)$  et à  $(\mathbb{Z}/n\mathbb{Z})^*$  si  $\mathcal{M} = (n)\infty$ .
2. Soit  $p$  un premier non divisant  $n$  et soit  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  correspondant à  $p \in (\mathbb{Z}/n\mathbb{Z})^*$ . Montrer que  $\sigma$  est la substitution de Frobenius en  $p$ .
3. Montrer que le corps de classe de  $\mathbb{Q}$  de rayon  $(n)\infty$  est  $\mathbb{Q}(\zeta_n)$ .

**Indications 6.** 1. On raison comme dans l'exercice 4 en utilisant que

$$(\mathbb{Z}/n\mathbb{Z})^* \cong \prod_{p \mid n} \mathbb{Z}_p^*/(1 + p^{e_p}\mathbb{Z}_p)$$

si  $n = \prod_p p^{e_p}$  est la décomposition en produit de nombres premiers de  $n$ .

2. Utiliser que  $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ .
3. Raisonner comme dans l'exercice 4.

**Exercice 7.** 1. Montrer le *théorème de Kronecker-Weber* : toute extension abélienne finie de  $\mathbb{Q}$  est incluse dans une extension cyclotomique.

2. En déduire que tout groupe abélien est groupe de Galois d'une extension de  $\mathbb{Q}$ .

**Indications 7.** 1. Si  $K/\mathbb{Q}$  est une extension abélienne, elle correspond à  $G$  sous groupe d'indice fini de  $C_{\mathbb{Q}}$ . Or,  $G$  contient un sous-groupe de congruence  $\mathbb{A}_{\mathbb{Q}}(\mathcal{M}) \cdot \mathbb{Q}^*/\mathbb{Q}^*$ . En particulier,  $G$  contient  $\mathbb{A}_{\mathbb{Q}}(\mathcal{M}) \cdot \mathbb{Q}^*/\mathbb{Q}^*$  pour  $\mathcal{M}$  de la forme  $n\infty$  (il y a juste deux types de diviseurs, ceux de la forme  $n\infty$  et ceux de la forme  $n$ , et le sous groupe de congruence pour  $n\infty$  est plus petit). Donc  $K$  est dans l'extension associée à  $n\infty$ , qui est la  $n$ -ème extension cyclotomique.

2. Soit  $G$  un groupe abélien isomorphe à

$$\prod_{i=1}^r \mathbb{Z}/c_i \mathbb{Z}$$

On choisit des premiers  $p_i$  congrus à 1 modulo  $c_i$  et on pose  $n = \prod p_i$ . Soit  $K = \mathbb{Q}(\zeta_n)$  la  $n$ -ème extension cyclotomique. Le groupe de Galois  $\text{Gal}(K/\mathbb{Q})$  est isomorphe à

$$\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^* = \prod_{i=1}^r (\mathbb{Z}/p_i\mathbb{Z})^* \cong \prod_{i=1}^r \mathbb{Z}/(p_i - 1)\mathbb{Z}$$

et il a donc un quotient isomorphe à  $G$ .

**Exercice 8.** Pour  $L$  une extension abélienne finie de  $K$ , on note  $N(L) = \text{Norm}_{L/K}(L^*)$  le sous-groupe des normes. Soit  $L_1$  et  $L_2$  deux extensions abéliennes finies d'un corps local  $K$  contenues dans  $K^{\text{ab}}$ .

1. Montrer que si  $L_1 \subseteq L_2$  alors  $N(L_2) \subseteq N(L_1)$ .
2. Montrer que  $N(L_1 L_2) = N(L_1) \cap N(L_2)$ .
3. En déduire que  $L_1 \subseteq L_2 \iff N(L_2) \subseteq N(L_1)$ .
4. Montrer que  $N(L_1 \cap L_2) = N(L_1) N(L_2)$ .

**Indications 8.** 1. Si  $L_1 \subseteq L_2$  on a

$$\text{Norm}_{L_2/K} = \text{Norm}_{L_1/K} \circ \text{Norm}_{L_2/L_1}$$

et donc  $N(L_2) \subseteq N(L_1)$ .

2. On a  $L_1 \subseteq L_1 L_2$  et  $L_2 \subseteq L_1 L_2$ , donc  $N(L_1 L_2) \subseteq N(L_1) \cap N(L_2)$ . Pour l'autre inclusion considérons le diagramme commutatif

$$\begin{array}{ccc} K^* & \xrightarrow{\quad} & \text{Gal}(L_1 L_2/K) \\ & \searrow & \downarrow \\ & & \text{Gal}(L_1/K) \times \text{Gal}(L_2/K) \end{array}$$

où  $\theta$  est le morphisme donné la théorie du corps de classe locale. Tout  $x \in N(L_1) \cap N(L_2)$  est dans le noyau de  $K^* \rightarrow \text{Gal}(L_1/K)$  et de  $K^* \rightarrow \text{Gal}(L_2/K)$  et donc dans le noyau de  $K^* \rightarrow \text{Gal}(L_1 L_2/K)$  à cause de la commutativité. Donc tout  $x \in N(L_1) \cap N(L_2)$  appartient à  $(L_1 L_2)^*$ .

3. Il suffit de montrer que  $L \mapsto N(L)$  est une bijection. Elle est surjective par définition. Si  $N(L_1) = N(L_2)$  alors

$$N(L_1 L_2) = N(L_1) \cap N(L_2) = N(L_1) = N(L_2)$$

donc  $\text{Gal}(L_1 L_2/K) \cong \text{Gal}(L_1/K) \cong \text{Gal}(L_2/K$  et donc  $L_1 = L_2$ .

4. Clair parce qu'on a montré que  $L \mapsto N(L)$  est une bijection qui renverse les inclusions.

**Exercice 9.** Soit  $K$  un corps de nombres. On appelle *corps de classe de Hilbert de  $K$* , noté  $K_H$ , la plus grande extension abélienne non ramifiée de  $K$ .

1. Montrer que le corps de classes de Hilbert  $K_H$  existe, et que

$$\text{Gal}(K_H/K) \cong \text{Cl}(K).$$

2. Déterminer le corps de classes de Hilbert de  $K = \mathbb{Q}(\sqrt{-5})$ .  
 3. Soit encore  $K = \mathbb{Q}(\sqrt{-5})$ . Montrer qu'un nombre premier  $p \neq 5$  s'écrit  $p = x^2 + 5y^2$  si et seulement si  $p$  est totalement décomposé dans  $K_H$ , si et seulement si  $p \equiv 1, 9 \pmod{20}$ .  
 4. On suppose que  $K$  est de nombre de classe 1, et  $L/K$  une extension galoisienne non ramifiée (avec  $L \neq K$ ). Montrer que  $[L : K] \geq 60$ .  
 5. Montrer que 3 divise le nombre de classes de  $\mathbb{Q}(\sqrt{-23})$  (indication :  $\text{disc}(x^3 - x - 1) = -23$ ).

**Indications 9.** 1. La théorie du corps de classe énonce que toute extension abélienne  $L/K$  est incluse dans un corps de classes de rayon  $\mathcal{M}$  pour un module  $\mathcal{M}$  divisible par les seuls premiers ramifiés dans  $L$ . On considère le module  $\mathcal{M} = 1$ , alors aucun premier n'est ramifié dans  $K_H = K_1$ , et réciproquement toute extension abélienne non ramifiée est dans  $K_1$ , c'est donc l'extension maximale non ramifiée. Le groupe de Galois est  $\text{Cl}(K)^1 \cong \text{Cl}(K)$ .

2. Le groupe de classes est d'ordre 2, donc  $K_H$  est une extension quadratique de  $K$ . On va montrer que  $L = K(i) = K(\sqrt{5})$  est le corps de classes de Hilbert de  $K$ . Considérons  $M = \mathbb{Q}(i)$  et  $N = \mathbb{Q}(\sqrt{5})$ . L'extension  $M/\mathbb{Q}$  est ramifiée seulement en 2 et  $N/\mathbb{Q}$  seulement en 5. De plus  $K/\mathbb{Q}$  est ramifiée seulement en 2 et 5. Or,  $L$  est le compositum de  $M$  et  $N$ , donc  $L/\mathbb{Q}$  est ramifiée seulement en 2 et 5 et en particulier  $L/K$  est non ramifié en  $\mathfrak{p}$  sauf si  $\mathfrak{p}$  est un idéal de  $\mathcal{O}_L$  qui divise 2 ou 5 (on peut aussi calculer le discriminant de  $L/\mathbb{Q}$  qui vaut  $2^4 \cdot 5^2$ ).

— On regarde l'indice de ramification  $e$  et le degré d'inertie  $f$  de (2) dans l'extension  $L/\mathbb{Q}$ . On a que (2) est ramifié dans  $M/\mathbb{Q}$  et donc aussi dans  $L/\mathbb{Q}$ , en particulier  $e \geq 2$ . D'autre part, (2) a degré d'inertie 2 dans  $N/\mathbb{Q}$  (car  $\mathcal{O}_N = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ ), donc  $f \geq 2$ . On a donc  $e = f = 2$ . On sait aussi que (2) est ramifié dans  $\mathcal{O}_K$ , donc (2) =  $\mathfrak{q}^2$  pour un certain idéal  $\mathfrak{q}$  de  $\mathcal{O}_K$ . On en déduit que  $\mathfrak{q}$  reste premier dans  $\mathcal{O}_L$  (avec degré d'inertie 2) et donc  $L/K$  est non ramifié en  $\mathfrak{q}$ .

— On fait le même raisonnement avec (5), en échangeant les rôles de  $N$  et  $M$ . La seule différence est que (5) est le produit des deux premiers dans  $\mathcal{O}_M = \mathbb{Z}[i]$ , donc il y a deux idéaux de  $\mathcal{O}_L$  au-dessus de l'idéal  $\mathfrak{q}$  de  $\mathcal{O}_K$  tel que  $\mathfrak{q}^2 = (5)$ . En tout cas  $\mathfrak{q}$  est non ramifié dans  $L/K$ .

On a donc que  $L/K$  est abélienne, partout non ramifiée et de degré égal à  $[K_H : K]$ , donc  $K_H = L$ .

3. On peut supposons  $p \neq 2, 5$ , c'est-à-dire  $p$  non ramifié dans  $K$ . Alors  $p$  s'écrit  $p = x^2 + 5y^2$  si et seulement si  $p$  se décompose en le produit de deux idéaux principaux de  $\mathcal{O}_K$ . On a l'application surjective (induite par l'homomorphisme d'Artin)

$$\mathbb{A}_K^* \twoheadrightarrow \text{Gal}(K_H/K)$$

dont le noyau contient  $K^*$  et donc on obtient

$$C_K = \mathbb{A}_K^*/K^* \twoheadrightarrow \text{Gal}(K_H/K)$$

dont le noyau est par construction le sous-groupe de congruence  $C_K^1$  associé au cycle arithmétique 1. Or, on a  $\text{Gal}(K_H/K) \cong \text{Cl}(K)^1 = \text{Cl}(K)$ , donc un idéal de  $\mathcal{O}_K$  est principal si et seulement si il correspond à l'identité par l'application d'Artin, ce qui équivaut à être totalement décomposé dans  $K_H$  (on a donc montré qu'un idéal est principal si et seulement si il est totalement décomposé dans le corps de classe de Hilbert). On obtient finalement que  $p$  s'écrit  $p = x^2 + 5y^2$  si et seulement si  $p$  est totalement décomposé dans  $K_H/\mathbb{Q}$ . Or,  $K_H$  est le compositum de  $M$  et  $N$  (voir ci-dessus), donc  $p$  est totalement décomposé dans  $K_H$  si et seulement si il l'est dans  $M$  et  $N$  (exercice!). On a

- $p$  est totalement décomposé dans  $M = \mathbb{Q}(i)$  si et seulement si  $-1$  est un carré mod  $p$ , si et seulement si  $p \equiv 1 \pmod{4}$ .
- $p$  est totalement décomposé dans  $N = \mathbb{Q}(\sqrt{5})$  si et seulement si 5 est un carré modulo  $p$ , si et seulement si  $p$  est un carré modulo 5 (loi de réciprocité quadratique), si et seulement si  $p \equiv \pm 1 \pmod{5}$ .

En conclusion, par le lemme chinois,  $p$  s'écrit  $p = x^2 + 5y^2$  si et seulement si  $p \equiv 1, 9 \pmod{20}$ .

Une autre manière de traiter l'exercice, plus compliquée mais qui explique mieux d'où vient le 20, consiste en l'observer que  $K_H$  est une extension abélienne de  $\mathbb{Q}$ , et donc elle est dans un corps cyclotomique  $\mathbb{Q}(\zeta_n)$ . Le plus petit  $n$  qui marche est  $n = 20$  (c'est le conducteur de  $K_H$ ) : en effet  $i \in \mathbb{Q}(\zeta_{20})$  et  $\sqrt{5} \in \mathbb{Q}(\zeta_5) \subseteq \mathbb{Q}(\zeta_{20})$ . Ainsi, la décomposition d'un premier  $p$  dans  $K_H$  dépend de sa décomposition dans  $\mathbb{Q}(\zeta_{20})$ , qui ne dépend que de la congruence de  $p \pmod{20}$  dans  $\text{Gal}(\mathbb{Q}(\zeta_{20})/\mathbb{Q}) = (\mathbb{Z}/20\mathbb{Z})^*$ . On peut éliminer les classes  $p \equiv 11, 13, 17, 19 \pmod{20}$  pour lesquelles  $p$  est inerte dans  $K$  (loi de réciprocité quadratique comme ci-dessus), ainsi que les classes  $p \equiv 3, 7 \pmod{20}$  où le degré d'inertie dans  $\mathbb{Q}(\zeta_{20})$  vaut 4 car le Frobenius est d'ordre 4 (sinon on peut encore regarder dans  $M$ ), ce qui interdit que  $p$  soit décomposé dans  $K_H$ . Il reste  $p \equiv 1, 9 \pmod{20}$  qui sont nécessairement valides.

- C'est évident pour  $p \equiv 1 \pmod{20}$ , qui est totalement décomposé dans  $\mathbb{Q}(\zeta_{20})$ .
- Pour  $p \equiv 9 \pmod{20}$  on observe qu'il est totalement décomposé si et seulement si le symbole d'Artin, relatif à  $K_H$ , est l'identité. Pour calculer ce symbole d'Artin on peut le calculer relativement à  $\mathbb{Q}(\zeta_{20})$  et après faire la restriction à  $K_H$ . Or, il y a  $[\mathbb{Q}(\zeta_{20}) : K_H] = 2$  éléments qui fixent  $K_H$  dans  $(\mathbb{Z}/20\mathbb{Z})^*$  et par Chebotarev il y a une infinité de premiers pour lesquels le Frobenius correspond à l'élément non trivial de  $(\mathbb{Z}/20\mathbb{Z})^*$  qui fixe  $K_H$ . Ces premiers sont forcément congruents à  $9 \pmod{20}$  : ils se décomposent en produit de 4 premiers dans  $K_H$ , chacun inerte dans  $\mathbb{Q}(\zeta_{20})$ .
- 4. L'extension est nécessairement non abélienne, et ne doit pas non plus contenir de sous-extension non triviale abélienne sur  $K$ . En particulier son groupe de Galois n'a pas de quotients abélien non trivial, donc il est parfait. Puisque  $A_5$  est le plus petit groupe parfait, on a l'inégalité.
- 5. On veut montrer que  $K_H$ , le corps de classes de Hilbert de  $K = \mathbb{Q}(\sqrt{-23})$ , contient un corps de degré 3, précisément  $K(\alpha)$  avec  $\alpha$  racine de  $x^3 - x - 1$ . Il faut donc montrer que l'extension  $K(\alpha)/K$  est abélienne et non ramifiée.
  - On note  $L = \mathbb{Q}(\alpha)$ , une extension de degré 3 qui est ramifiée qu'en 23 (il s'agit d'une extension non galoisienne car  $x^3 - x - 1$  a une seule racine réelle). Sa clôture galoisienne est encore ramifiée qu'en 23 (les premiers ramifiés ne changent pas en considérant la clôture galoisienne) et elle est forcément de degré 6, donc elle est  $\mathbb{Q}(\alpha, \sqrt{-23}) = K(\alpha)$ , puisque l'unique sous-corps quadratique ne peut pas être ramifié qu'en 23. En résumant, on a donc bien une extension abélienne  $K(\alpha)/K$  de groupe de Galois  $A_3$ . (En général une extension cubique est galoisienne si et seulement si le discriminant du polynôme est un carré, ce qui équivaut à avoir trois racines réelles, avec groupe de Galois  $A_3$ , et sinon on trouve la clôture galoisienne en rajoutant la racine du discriminant.)
  - On examine la ramification. On a que  $K(\alpha)$  n'est pas ramifiée en dehors de 23 car c'est un compositum de deux extensions non ramifiées en dehors de 23. Maintenant, l'indice de ramification de 23 en  $\mathbb{Q}(\sqrt{-23})/\mathbb{Q}$  est 2, donc  $(23) = \mathfrak{p}^2$  pour un certain  $\mathfrak{p}$ . Si  $\mathfrak{p}$  était ramifié dans  $K(\alpha)$ , son indice de ramification doit être 3, donc  $(23) = \mathfrak{q}^6$  serait totalement ramifié dans  $K(\alpha)/\mathbb{Q}$  et donc aussi dans  $\mathbb{Q}(\alpha)/\mathbb{Q}$ , ce qui n'est pas le cas (en pratique  $\mathbb{Q}(\sqrt{-23})$  "absorbe" toute la ramification).

**Exercice 10.** 1. Soit  $L/K$  une extension de corps de nombres telle que  $L \cap K_H = K$ . Montrer que l'application norme  $\text{Cl}(L) \rightarrow \text{Cl}(K)$  est surjective.  
 2. Soit  $L/K$  une extension telle qu'un premier  $\mathfrak{p}$  de  $\mathcal{O}_K$  est totalement ramifié dans  $L$ . Montrer que les nombres de classes vérifient  $h_K \mid h_L$ .

**Indications 10.** 1. Les extensions  $L/K$  et  $K_H/K$  sont disjointes et de plus  $\text{Gal}(K_H L/L) \cong \text{Cl}(K)$  est abélien. Cet isomorphisme respecte les groupes

de décomposition et d'inertie, donc  $K_H L/L$  est non-ramifiée et c'est une sous-extension du corps de classes de Hilbert de  $L$ . En particulier  $\text{Cl}(K)$  est bien un quotient de  $\text{Cl}(L)$  par la norme.

2. Dans  $L \cap K_H$  on a que  $\mathfrak{p}$  est à la fois totalement ramifié et non ramifié, donc  $L \cap K_H = K$ . On applique la question précédente qui implique la divisibilité.

**Exercice 11.** On considère  $K = \mathbb{Q}(\zeta_3)$ , le module  $\mathcal{M} = (5 + 3\zeta_3)$  et  $L$  le corps de classe de rayon  $\mathcal{M}$ .

1. Montrer que  $\text{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$ . En déduire que  $L$  est de la forme

$$L = K \left( \sqrt[3]{\zeta_3^k (5 + 3\zeta_3)} \right).$$

2. Identifier  $L$  (considérer le Frobenius en  $4 + 3\zeta_3$ ).

**Indications 11.** 1. Notons  $\pi = 5 + 3\zeta_3$ . On a que  $\mathcal{M}$  est un idéal de norme  $\pi\bar{\pi} = (5 + 3\zeta_3)(5 + 3\bar{\zeta}_3) = 25 - 10 + 9 = 19$  et donc c'est un premier décomposé dans  $K$ . Par ailleurs, puisque  $\mathcal{O}_K$  est principal, on a

$$\mathbb{A}_K^* = K^*/\mathcal{O}_K^* \times \mathbb{C}^* \times \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*$$

En regardant le quotient, on obtient la structure du groupe de classes de rayon qui vaut

$$C_{\mathcal{M}} = \mathbb{F}_{19}/\mu_6 \cong \mathbb{Z}/3\mathbb{Z}$$

et donc  $\text{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$ . Puisque  $K$  contient  $\zeta_3$ , c'est une extension de Kummer de la forme  $L = K(\theta)$  avec  $\theta^3 = a \in K^*/K^2$ . Puisqu'elle est non ramifiée en dehors de  $\mathcal{M}$ , on a  $a = \zeta_3^k \pi$  pour un certain  $k \in \mathbb{Z}/3\mathbb{Z}$ .

2. Considérons l'élément  $\beta = \pi - 1 = 4 + 3\zeta_3$ . Il est de norme 13, donc c'est un premier décomposé de  $\mathcal{O}_K$ . Dans le groupe  $C_{\mathcal{M}}$ , on a que  $(\beta)$  est trivial car c'est un idéal principal engendré par  $1 - \pi \equiv 1 \pmod{\mathcal{M}}$ . Donc le Frobenius  $F_{\beta}$  est trivial. On a donc  $\theta = F_{\beta}(\theta) = \theta^{13} \pmod{1 - \pi}$ . Or,  $\theta^{13} = \theta(\theta^3)^4$ , donc on a  $(\zeta_3^k \pi)^4 \equiv 1 \pmod{1 - \pi}$ , soit  $\zeta_3^{4k} \equiv 1 \pmod{\beta}$ , ce qui impose  $k = 0$ . Ainsi,  $L = K(\sqrt[3]{\pi})$ .