ENS de Lyon
M1 Introduction à la théorie des nombres

Examen du 23 avril 2019

*Ce sujet comporte un exercice et deux problèmes*

## Exercice

Soit $f \in \mathbf{Z}[T]$ un polynôme unitaire non constant et soit $g$ un facteur irréductible de $f$. Le polynôme $g$ est également unitaire (lemme de Gauss) et tout zéro de $g$ est un zéro de $f$, donc il suffit de démontrer qu'il existe une infinité de nombres premiers $p$ tels que $g$ admette un zéro modulo $p$.

Posons $K = \mathbf{Q}[T]/(g) = \mathbf{Q}(\alpha)$, en désignant par $\alpha$ l'image de $T$ dans $K$. Pour tout nombre premier $p$ ne divisant pas $D_K$, la factorisation de $p$ en produit d'idéaux premiers de $\mathcal{O}_K$ reflète la factorisation de $g$ en produit d'irréductibles modulo $p$ ; dès lors, l'existence d'un zéro de $g$ modulo $p$ équivaut à celle d'un diviseur premier de $p$ dans $K$ de degré 1.

La conclusion découle donc de l'existence d'une infinité d'idéaux premiers de degré 1 dans $\mathcal{O}_K$, laquelle a été démontrée en cours en établissant la divergence de la série

$$\sum_{\deg(\mathfrak{p})=1} \frac{1}{\mathrm{N}(\mathfrak{p})}$$

(Corollaire 4.8).

## Problème 1

### *Première partie*

1.(i) Si $(x, y) \in \mathbf{Z}^2$ et $\mathrm{pgcd}(x, y) = 1$, alors il existe $(u, v) \in \mathbf{Z}^2$ tel que $xu - yv = 1$ (Bézout), donc

$$\begin{pmatrix} x & v \\ y & u \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \quad \text{et} \quad \begin{pmatrix} x & v \\ y & u \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}.$$

1.(ii) Supposons qu'il existe $(x, y) \in \mathbf{Z}^2$ tel que $\mathrm{pgcd}(x, y) = 1$ et $q(x, y) = n$. En considérant une matrice $M \in \mathrm{SL}_2(\mathbf{Z})$ telle que $(1, 0)\ {}^tM = (x, y)$, la forme binaire $q' = q \cdot M$ vérifie $q'(1, 0) = n$ et donc s'écrit $q' = (n, b', c')$ avec $b', c' \in \mathbf{Z}$. Réciproquement, si $q \overset{+}{\sim} q'$ avec $q' = (n, b', c')$, alors $q$ et $q'$ représentent primitivement les mêmes entiers, donc en particulier $n$ puisque $n = q'(1, 0)$.

2. Si $q = (a, b, c)$ est une forme binaire de discriminant $D$ représentant primitivement $n$, alors $q \overset{+}{\sim} (n, b', c')$ en vertu de la question précédente et $D = \mathrm{disc}(n, b', c') = {b'}^2 - 4nc'$ est un carré modulo $4n$.

Réciproquement, si $D = b^2 + 4nc$ avec $b, c \in \mathbf{Z}$, alors la forme binaire $q = (n, b, -c)$ représente primitivement $n$ puisque $q(1, 0) = n$ et son discriminant est égal à $D$.

3. Supposons qu'une forme binaire $q$ de discriminant $D$ représente $n$ et que $p$ soit un nombre premier tel que $\left(\frac{D}{p}\right) = -1$. Écrivons $n = q(x, y) = m^2 q(x', y')$ avec $(x, y) \in \mathbf{Z}^2$, $m = \mathrm{pgcd}(x, y)$ et $x = mx', y = my'$. Il découle de la question précédente que $p$ ne peut diviser l'entier $q(x', y')$ puisque sinon $D$, qui est un carré modulo $4q(x', y')$, le serait également modulo $p$. Par suite,

$$v_p(n) = v_p(m^2) = 2v_p(m)$$

est un nombre pair.

*Seconde partie*

4. Posons $K = \mathbf{Q}(\sqrt{-5})$. Pour tout $(x, y) \in \mathbf{Z}^2$,

$$\begin{aligned} q_2(x,y) &= 2x^2 + 2xy + 3y^2 \\ &= 2\left(x + \frac{y}{2}\right)^2 + \frac{5}{2}y^2 \\ &= 2\left(x + \frac{1+\sqrt{-5}}{2}y\right)\left(x + \frac{1-\sqrt{-5}}{2}y\right) \\ &= \frac{1}{2}\mathrm{N}_{K/\mathbf{Q}}\left(2x + y - \sqrt{-5}y\right). \end{aligned}$$

On en déduit l'identité

$$\begin{aligned} q_2(x,y)q_2(u,v) &= \frac{1}{4}\mathrm{N}_{K/\mathbf{Q}}\left((2x + y + y\sqrt{-5})(2u + v + v\sqrt{-5})\right) \\ &= \frac{1}{4}\mathrm{N}_{K/\mathbf{Q}}\left(2(2xu + xv + yu - 2yv) + 2(xv + yv + uy)\sqrt{-5}\right) \\ &= \mathrm{N}_{K/\mathbf{Q}}\left((2xu + xv + yu - 2yv) + (xv + yv + yu)\sqrt{-5}\right) \\ &= q_1(2xu + xv + yu - 2yv, xv + yv + yu) \end{aligned}$$

pour tous $(x, y), (u, v) \in \mathbf{Z}^2$, donc le produit de deux entiers représentés par $q_2$ est représenté par $q_1$.

5. Observons que toute représentation d'un nombre premier $p$ par une forme binaire est nécessairement primitive. En vertu de la question 2, un nombre premier est représenté par une forme binaire de discriminant $-20$ si et seulement si $-20$ est un carré modulo $4p$, donc si et seulement si $-5$ est un carré modulo $p$. Par ailleurs, une telle forme binaire est nécessairement définie positive puisque $p > 0$. Toute forme binaire définie positive de discriminant $-20$ étant proprement équivalente à l'une des deux formes réduites $q_1, q_2$, nous en déduisons que $p$ est représenté par l'une des formes $q_1, q_2$ si et seulement si

$$\left(\frac{-5}{p}\right) = 1.$$

Pour $p \neq 2, 5$, la loi de réciprocité quadratique permet d'écrire

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right)$$

et donc

$$\begin{aligned} \left(\frac{-5}{p}\right) = 1 \iff \left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) &\iff \begin{cases} p \equiv 1 \pmod 4 \text{ et } p \equiv \pm 1 \pmod 5 \\ p \equiv -1 \pmod 4 \text{ et } p \equiv \pm 2 \pmod 5 \end{cases} \\ &\iff p \equiv 1, 3, 7, 9 \pmod{20} \end{aligned}$$

Soit $p \equiv 1, 3, 7, 9 \pmod{20}$ un nombre premier. Pour tous entiers $x, y$ premiers entre eux,

$$q_1(x,y) \equiv x^2 + y^2 \equiv 1, 2 \pmod 4 \quad \text{et} \quad q_2(x,y) \equiv -1, 0, 2 \pmod 4$$

donc un nombre premier impair ne peut être simultanément représenté par $q_1$ et $q_2$. Un nombre premier $p \neq 2, 5$ est représenté par $q_1$ (resp. par $q_2$) si et seulement s'il est congru à 1 (resp. $-1$) modulo 4, donc si et seulement si $p \equiv 1, 9$ (resp. $p \equiv 3, 7$) modulo 20.

Il est par ailleurs immédiat que $q_1$ (resp. $q_2$) représente 5 (resp. 2), et que $q_1$ (resp. $q_2$) ne représente pas 2 (resp. 5).

*Remarque : on peut également démontrer qu'un nombre premier $p \equiv 1, 3, 7, 9 \pmod{20}$ est représenté par $q_1$ (resp. par $q_2$) si et seulement si les diviseurs premiers de $p$ dans $\mathcal{O}_K$ sont principaux (resp. non principaux).*

6. Soit $n$ un nombre entier de la forme $x^2+5y^2$ avec $x,y\in\mathbf{Z}$. En vertu des questions 3 et 5, la valuation $p$-adique de $n$ est paire pour tout nombre premier $p\equiv 11,13,17,19 \pmod{20}$. D'après la question précédente, tous les facteurs premiers $p$ de $n$ tels que $p\equiv 1,5,9$ modulo 20 sont de la forme $u^2+5v^2$, tous ceux tels que $p\equiv 2,3,7$ sont de la forme $q_2(u,v)$. Nous allons prouve que la somme des valuations $p$-adiques de $n$ pour $p\equiv 2,3,7 \pmod{20}$ est *paire* en raisonnant par l'absurde. Si elle est impaire, on déduit des observations précédentes et de la question 4 que l'on peut écrire

$$n=x^2+5y^2=(u^2+5v^2)p$$

avec $(u,v)\in\mathbf{Z}^2$ et $p$ premier congru à $2,3,7$ modulo 20. En écrivant

$$\frac{x^2+5y^2}{u^2+5v^2}=\mathrm{N}_{K/\mathbf{Q}}\left(\frac{x+y\sqrt{-5}}{u+v\sqrt{-5}}\right)=\mathrm{N}_{K/\mathbf{Q}}\left(\frac{(xu-5yv)+(uy-xv)\sqrt{-5}}{u^2+5v^2}\right)=\frac{1}{d^2}(a^2+5b^2)$$

avec $a=xu-5yv, b=uy-xv$ et $d=u^2+5v^2$, on en déduit l'identité

$$a^2+5b^2=pd^2.$$

Quitte à simplifier par $\mathrm{pgcd}(a,b)$, on peut supposer $a$ et $b$ premiers entre eux ; modulo 4, le membre de gauche est alors congru à 1 ou 2 tandis que le membre de droite est congru à $-1$ ou 0, donc nous aboutissons à une contradiction.

Réciproquement, si un nombre entier $n$ satisfait aux conditions (a) et (b) de l'énoncé, alors chacun des trois termes

$$\prod_{p\equiv 11,13,17,19 \pmod{20}} p^{v_p(n)},\qquad \prod_{p\equiv 1,5,9 \pmod{20}} p^{v_p(n)},\qquad \prod_{p\equiv 2,3,7 \pmod{4}} p^{v_p(n)}$$

est représenté par $q_1$ en vertu des questions 4 et 5, donc $n$ est représenté par $q_1$.

## Problème 2

### *1. Questions préliminaires*

1. Si le corps $K$ n'admet pas de plongement réel, alors $\mathrm{N}_{K/\mathbf{Q}}(x)>0$ et $x\gg 0$ pour tout $x\in K^\times$. Sinon, soit $\tau_1,\tau_2$ les deux plongements réels de $K$. Pour tout $x\in K^\times$,

$$\mathrm{N}_{K/\mathbf{Q}}(x)=\tau_1(x)\tau_2(x)$$

est strictement positif si et seulement si $\tau_1(x),\tau_2(x)>0$, c'est-à-dire $x\gg 0$, ou $\tau_1(x),\tau_2(x)<0$, c'est-à-dire $-x\gg 0$.

2. Les deux membres de l'égalité souhaitée sont multiplicatifs, donc il suffit de l'établir lorsque $\mathfrak{a}=\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$. Distinguons trois cas de figure :

— $\mathfrak{p}$ est non ramifié et de degré résiduel 1, auquel cas $p=\mathrm{N}(\mathfrak{p})$ est un nombre premier et $\mathfrak{p}$, $\sigma(\mathfrak{p})$ sont les deux diviseurs premiers de $p$ dans $\mathcal{O}_K$ en vertu de la proposition 2.16 du cours ; on a donc

$$(p)=\mathfrak{p}\cdot\sigma(\mathfrak{p}).$$

— $\mathfrak{p}$ est non ramifié et de degré résiduel 2, auquel cas $\mathfrak{p}=(p)$ pour un certain nombre premier $p$ et donc $\sigma(\mathfrak{p})=\mathfrak{p}$ ; on a $\mathrm{N}(\mathfrak{p})=p^2$ et

$$\mathfrak{p}\cdot\sigma(\mathfrak{p})=\mathfrak{p}^2=(p)^2=(p^2).$$

— $\mathfrak{p}$ est ramifié, auquel cas son degré résiduel est 1 et $p=\mathrm{N}(\mathfrak{p})$ est un nombre premier. On a $\sigma(\mathfrak{p})=\mathfrak{p}$ et $(p)=\mathfrak{p}^2$, donc

$$\mathfrak{p}\cdot\sigma(\mathfrak{p})=\mathfrak{p}^2=(p).$$

3. (i) Désignons par $\lambda$ l'application $K \to K,\ y \mapsto y - x\sigma(y)$. Puisque $x\sigma(x) = 1$,

$$\sigma(\lambda(y)) = \sigma(y) - \sigma(x)\sigma^2(y) = \sigma(y) - x^{-1}y = -x^{-1}(y - x\sigma(y)) = -x^{-1}\lambda(y)$$

pour tout $y \in K^\times$ et donc l'image de $\lambda$ est contenue dans le sous-$\mathbf{Q}$-espace vectoriel $\ker(\sigma + x\mathrm{id}_K)$. Ce dernier est distinct de $K$ en vertu du lemme d'indépendance des caractères de Dedekind, donc $\mathrm{im}(\lambda) \neq K$.

3. (ii) L'application $\lambda$ est $\mathbf{Q}$-linéaire et non surjective, donc il existe $y \in K^\times$ tel que $\lambda(y) = 0$, c'est-à-dire tel que $x = y/\sigma(y)$.

*2. Unités totalement positives*

4. Distiguons deux cas de figure, selon que $K$ est quadratique réel ou quadratique imaginaire.

Si $K$ est quadratique imaginaire, alors $\mathcal{O}_K^\times$ est un groupe fini, formé des racines de l'unité contenues dans $K$. Ce groupe est cyclique et $E(K) = \mathcal{O}_K^\times$.

Si $K$ est quadratique réel, alors $\mathcal{O}_K^\times = \{\pm 1\} \times \varepsilon^{\mathbf{Z}}$, où $\varepsilon$ est une unité fondamentale.

— Si $\mathrm{N}_{K/\mathbf{Q}}(\varepsilon) = 1$, alors l'une des deux unités fondamentales $\varepsilon$, $-\varepsilon$ est totalement positive et $E(K) = \varepsilon^{\mathbf{Z}}$ ou $E(K) = (-\varepsilon)^{\mathbf{Z}}$ selon le cas.

— Si $\mathrm{N}_{K/\mathbf{Q}}(\varepsilon) = -1$, alors $\mathrm{N}_{K/\mathbf{Q}}(\pm\varepsilon^m) = 1$ si et seulement si $m$ est pair. L'une des deux unités $\varepsilon^2$, $-\varepsilon^2$ est totalement positive et $E(K) = \varepsilon^{2\mathbf{Z}}$ ou $E(K) = (-\varepsilon^2)^{\mathbf{Z}}$ selon le cas.

5. Si $K$ est quadratique imaginaire et $E(K) = \langle\zeta\rangle$, alors $\sigma$ s'identifie à la conjugaison complexe et donc $\sigma(\zeta) = \zeta^{-1}$ ; on en déduit $\psi(\zeta) = \zeta/\zeta^{-1} = \zeta^2$, donc $(E(K) : \psi(E(K)) = 2$.

Si $K$ est quadratique réel et $E(K) = \varepsilon^{\mathbf{Z}}$, où $\varepsilon$ est une unité fondamentale de norme 1, alors $\sigma(\varepsilon) = \varepsilon^{-1}$ ; on en déduit $\psi(\varepsilon) = \varepsilon^2$, donc $(E(K) : \psi(E(K)) = 2$.

Si $K$ est quadratique réel et $E(K) = \varepsilon^{2\mathbf{Z}}$, où $\varepsilon$ est une unité fondamentale de norme $-1$, alors $\sigma(\varepsilon^2) = \varepsilon^{-2}$ ; on en déduit $\psi(\varepsilon^2) = \varepsilon^4$, donc $(E(K) : \psi(E(K))) = 2$.

6. Supposons $D_K > 0$ et $D_K$ divisible par un nombre premier $p \equiv 3 \pmod 4$. Il s'agit de voir que toutes les unités de $K$ sont de norme 1.

Si $D_K \equiv 0 \pmod 4$, alors $\mathcal{O}_K = \mathbf{Z}[\sqrt{D_K}/2]$. Les unités s'écrivent $u = x + y\sqrt{D}_K/2$ avec $x, y \in \mathbf{Z}$ et $\mathrm{N}_{K/\mathbf{Q}}(u) = x^2 - y^2 D_K/4 = \pm 1$, ce qui implique $x^2 \equiv \pm 1 \pmod p$. Comme $-1$ n'est pas un carré modulo $p$ puisque $p \equiv 3 \pmod 4$, le signe $-$ ne peut pas apparaître et donc $\mathrm{N}_{K/\mathbf{Q}}(u) = 1$.

Si $D_K \equiv 1 \pmod 4$, alors $\mathcal{O}_K = \mathbf{Z}[(1 + \sqrt{D_K})/2]$. Les unités s'écrivent $u = x + y(1 + \sqrt{D_K})/2$ avec $x, y \in \mathbf{Z}$ et $\mathrm{N}_{K/\mathbf{Q}}(u) = x^2 + xy + y^2(1 - D_K)/4 = \pm 1$, ce qui implique

$$\pm 4 \equiv 4x^2 + 4xy + y^2 \equiv (2x + y)^2 \pmod p.$$

Le signe $-$ ne peut apparaître puisque $-1$ n'est pas un carré modulo $p$, donc $\mathrm{N}_{K/\mathbf{Q}}(u) = 1$.

*3. Classes ambiguës*

7. Considérons une classe ambiguë $c = [\mathfrak{a}]_+$. L'égalité $\sigma(c) = c$ se traduit par l'existence d'un élément $x \in K^\times$ tel que $\mathrm{N}_{K/\mathbf{Q}}(x) > 0$ et $\sigma(\mathfrak{a}) = (x)\mathfrak{a}$. En prenant les normes, il vient

$$\mathrm{N}(\sigma(\mathfrak{a})) = \big|\mathrm{N}_{K/\mathbf{Q}}(x)\big|\mathrm{N}(\mathfrak{a}),$$

donc $\big|\mathrm{N}_{K/\mathbf{Q}}(x)\big| = 1$ puisque $\mathrm{N}(\sigma(\mathfrak{a})) = \mathrm{N}(\mathfrak{a})$ et, finalement, $\mathrm{N}_{K/\mathbf{Q}}(x) = 1$ d'après l'hypothèse de positivité.

En vertu de la question 3.(ii), il existe $y \in K^\times$ tel que $x = y/\sigma(y)$. On en déduit

$$\sigma((y)\mathfrak{a}) = (\sigma(y))\sigma(\mathfrak{a}) = (\sigma(y))(x)\mathfrak{a} = (y)\mathfrak{a},$$

donc $(y)\mathfrak{a}$ est un idéal ambigu.

Il reste à voir que l'on peut choisir $y$ ci-dessus avec $\mathrm{N}_{K/\mathbf{Q}}(y) > 0$. D'après la question 1, on peut supposer $x \gg 0$. L'identité $y = x\sigma(y)$ implique $\tau(y) = \tau(x)\tau(\sigma(y))$ pour tout plongement réel $\tau$ de $K$, donc $\tau(y)$ et $\tau(\sigma(y))$ sont de même signe ; on en déduit

$$\mathrm{N}_{K/\mathbf{Q}}(y) = \tau\left(\mathrm{N}_{K/\mathbf{Q}}(y)\right) = \tau(y\sigma(y)) = \tau(y)\tau(\sigma(y)) > 0.$$

En conclusion,

$$c = [\mathfrak{a}]_+ = [(y)\mathfrak{a}]_+ = \lambda^+((y)\mathfrak{a}).$$

8. On a $\sigma(\mathfrak{p}_i) = \mathfrak{p}_i$ pour tout $i \in \{1, \ldots, t\}$, donc tous les idéaux fractionnaires de la forme $(r) \cdot \mathfrak{p}_1^{\varepsilon_1} \cdots \mathfrak{p}_t^{\varepsilon_t}$ sont ambigus.

Réciproquement, considérons un idéal fractionnaire ambigu $\mathfrak{a}$ et sa factorisation

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

en produit d'idéaux premiers. Si $\mathfrak{p}$ est de degré 2, alors $\mathfrak{p} = (p)$ pour un certain nombre premier $p$ et donc

$$\mathfrak{a} = (r_1) \cdot \prod_{\deg(\mathfrak{p})=1} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

avec $r_1 \in \mathbf{Q}^\times$. Pour tout idéal premier $\mathfrak{p}$ non ramifié et de degré 1,

$$v_{\sigma(\mathfrak{p})}(\mathfrak{a}) = v_{\mathfrak{p}}(\sigma(\mathfrak{a})) = v_{\mathfrak{p}}(\mathfrak{a})$$

et $\mathfrak{p} \cdot \sigma(\mathfrak{p}) = (p)$, donc

$$\mathfrak{a} = (r_1) \cdot \prod_{\substack{\mathfrak{p} \text{ non ramifié} \\ \deg(\mathfrak{p}) = 1}} (\mathfrak{p} \cdot \sigma(\mathfrak{p}))^{v_{\mathfrak{p}}(\mathfrak{a})} \cdot \prod_{\mathfrak{p} \text{ ramifié}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} = (r_2) \cdot \prod_{\mathfrak{p} \text{ ramifié}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

avec $r_2 \in \mathbf{Q}^\times$. Enfin, pour $\mathfrak{p}$ ramifié, $\mathfrak{p}^2 = (p)$ et donc

$$\mathfrak{a} = (r) \cdot \prod_{\mathfrak{p} \text{ ramifié}} \mathfrak{p}^{\varepsilon_{\mathfrak{p}}}$$

avec $r \in \mathbf{Q}^\times$ et $\varepsilon_{\mathfrak{p}} \in \{0, 1\}$.

On conclut en observant que les idéaux premiers ramifiés sont précisément ceux divisant $D_K$, c'est-à-dire $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$.

9. Le noyau de l'application $\lambda^+$ est consituté des idéaux principaux $(\alpha)$ avec $\mathrm{N}_{K/\mathbf{Q}}(\alpha) > 0$ et tels que $(\sigma(\alpha)) = (\alpha)$. Cette dernière condition équivaut à $\alpha/\sigma(\alpha) \in \mathcal{O}_K^\times$. Quitte à remplacer $\alpha$ par $-\alpha$, on peut supposer $\alpha \gg 0$ et alors $\mu(\alpha) = \alpha/\sigma(\alpha)$est une unité totalement positive (même argument qu'à la fin de la question 7). L'application $\mu : \ker(\lambda^+) \to E(K)$ ainsi définie est un morphisme de groupes.

Si $\mu(\alpha) = \psi(u)$ avec $u \in E(K)$, alors $\alpha/\sigma(\alpha) = u/\sigma(u)$, donc $\sigma(u^{-1}\alpha) = u^{-1}\alpha$ et $u^{-1}\alpha \in \mathbf{Q}$. Réciproquement, si $\alpha \in \mathbf{Q}$, alors $\mu(\alpha) = 1 \in \psi(E(K))$. L'application $\mu$ induit donc un isomorphisme entre les groupes $\ker(\lambda^+)/I$ et $E(K)/\psi(E(K))$.

10. Considérons la suite exacte courte

$$1 \longrightarrow \ker(\lambda^+)/I \longrightarrow A(K)/I \longrightarrow \mathrm{Am}^+(K) \longrightarrow 1.$$

D'après les questions 8, 9 et 5, les groupes $A(K)/I$ et $\ker(\lambda^+)/I$ sont respectivement isomorphes à $(\mathbf{Z}/2\mathbf{Z})^t$ et $\mathbf{Z}/2\mathbf{Z}$. On en déduit que la suite exacte précédente est une suite exacte de $\mathbf{Z}/2\mathbf{Z}$-espaces vectoriels et donc

$$\mathrm{Am}^+ \simeq (\mathbf{Z}/2\mathbf{Z})^{t-1} \simeq \{\pm 1\}^{t-1}.$$

11. L'identité $\mathfrak{a} \cdot \sigma(\mathfrak{a}) = (\mathrm{N}(\mathfrak{a})$ implique $[\mathfrak{a}]_+[\sigma(\mathfrak{a})]_+ = 1$, c'est-à-dire

$$\sigma([\mathfrak{a}]_+) = [\mathfrak{a}]_+^{-1}.$$

On en déduit

$$\mathrm{Am}^+(K) = \{c \in \mathrm{Cl}^+(K) \mid c = c^{-1}\} = \{c \in \mathrm{Cl}^+(K) \mid c^2 = 1\}.$$

Le groupe abélien fini $\mathrm{Cl}^+(K)$ est d'ordre impair si et seulement si l'application $c \mapsto c^2$ est un isomorphisme, donc si et seulement si $\mathrm{Am}^+(K) = \{1\}$. En vertu de la question précédente, cette condition est équivalente à $t = 1$.

*4. Application : une démonstration de la loi de réciprocité quadratique*

12. Soit $p$ un nombre premier congru à 1 modulo 4.

(i) On a $D_K = p$ et $D_L = p^*$, donc $h_K^+$ et $h_L^+$ sont impairs en vertu de la question 11. Puisque $h_F | h_F^+$ pour tout corps de nombres $F$ en vertu de la suite exacte courte

$$1 \longrightarrow \mathrm{P}(F)/\mathrm{P}^+(F) \longrightarrow \mathrm{Cl}^+(F) \longrightarrow \mathrm{Cl}(F) \longrightarrow 1$$

il en découle que les entier $h_K$ et $h_L$ sont impairs.

(ii) Si $\left(\frac{p}{q}\right) = 1$, alors $q$ est décomposé dans $K$, i.e. $(q) = \mathfrak{q}\sigma(\mathfrak{q})$. L'idéal $\mathfrak{q}^{h_K}$ est principal, donc $q^{h_K} = \pm \mathrm{N}_{K/\mathbf{Q}}(\alpha)$ avec $\alpha \in \mathcal{O}_K$. En observant que $\mathcal{O}_K = \mathbf{Z}[(1+\sqrt{p})/2]$ puisque $p \equiv 1 \pmod 4$, on obtient

$$q^{h_K} = \pm(a^2 + ab + b^2(1-p)/4 = \pm\frac{1}{4}\left((2a+b)^2 - pb^2\right)$$

avec $a, b \in \mathbf{Z}$.

On en déduit

$$\left(\frac{q}{p}\right) = \left(\frac{4q^{h_K}}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{(2a+b)^2}{p}\right) = \left(\frac{\pm 1}{p}\right) = (\pm 1)^{(p-1)/2} = 1.$$

Par symétrie, nous avons démontré l'identité

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

pour tous nombres premiers $p, q$ congrus à 1 modulo 4.

(iii) Comme précédemment, on déduit de la condition $\left(\frac{q}{p}\right) = 1$ l'existence de deux entiers $x, y \in \mathbf{Z}$ tels que $4p^{h_L} = \pm(x^2 - q^* y^2) = \pm(x^2 + qy^2)$, donc tels que $4p^{h_L} = x^2 + qy^2$. Il en découle

$$\left(\frac{p}{q}\right) = \left(\frac{4p^{h_L}}{q}\right) = \left(\frac{x^2}{q}\right) = 1.$$

Comme $p \equiv 1 \pmod 4$,

$$\left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right).$$

13. Soit $p, q$ deux nombres premiers congrus à 3 modulo 4. Posons $K = \mathbf{Q}(\sqrt{pq})$.

(i) On déduit de la suite exacte courte de la question 12.(i) et du lemme du serpent la suite exacte courte

$$1 \longrightarrow \mathrm{P}(K)/\mathrm{P}^+(K) \longrightarrow \mathrm{Cl}^+(K)[2] \longrightarrow \mathrm{Cl}(K)[2] \longrightarrow 1$$

où [2] désigne la 2-torsion. Comme toutes les unités de $K$ sont de norme 1 en vertu de la question 6, le groupe $\mathrm{P}(K)/\mathrm{P}^+(K)$ est d'ordre 2. Le groupe $\mathrm{Cl}^+(K)[2] = \mathrm{Am}^+(K)$ est également d'ordre 2 en vertu de la question 10, donc $\mathrm{Cl}(K)[2] = \{1\}$ et $h_K$ est impair.

(ii) L'idéal $\mathfrak{p}^{h_K}$ est principal. Par ailleurs, $\mathfrak{p}^2 = (p^2, p\sqrt{pq}, pq) = (p)$, donc $\mathfrak{p}^2$ est également principal. Comme $h_K$ est impair, on en déduit que l'idéal $\mathfrak{p}$ est principal.

(iii) Si $\mathfrak{p} = (\alpha)$ avec $\alpha \in \mathcal{O}_K = \mathbf{Z}[(1+\sqrt{pq})/2]$, alors

$$p = \mathrm{N}(\mathfrak{p}) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)| = \pm(a^2 + ab + b^2(1-pq)/4$$

avec $a, b \in \mathbf{Z}$. On en déduit $4p = \pm(c^2 - pqd^2)$ avec $c = 2a + b$ et $d = b$, puis, en observant que $c$ est divisible par $p$,

$$4 = \pm(px^2 - qy^2)$$

avec $x = c/p$ et $y = d$.

(iv) Si $4 = px^2 - qy^2$, alors $\left(\frac{p}{q}\right) = \left(\frac{4}{q}\right) = 1$ et $\left(\frac{q}{p}\right) = \left(\frac{-4}{p}\right) = (-1)^{(p-1)/2} = -1$.

Si $4 = -(px^2 - qy^2)$, alors $\left(\frac{p}{q}\right) = \left(\frac{-4}{q}\right) = -1$ puisque $q \equiv 3 \pmod 4$ et $\left(\frac{q}{p}\right) = \left(\frac{4}{p}\right) = 1$.

Dans chaque cas de figure, nous avons obtenu

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) = \left(\frac{q^*}{p}\right).$$