Introduction à la théorie du genre

Sylvain Rairat

Avril 2004

1 Préliminaires

Soit m un entier non nul, et sans facteurs carré. $\mathbb{K} = \mathbb{Q}[\sqrt{m}]$, un corps quadratique, $\mathcal{O}_{\mathbb{K}}$: l'anneau des entiers. d est son discriminant et σ le morphisme de conjugaison.

Définition 1.1. *$\lambda \in \mathbb{K}$ est dit totalement positif si :*
- *$\lambda \neq 0$ dans le cas d'un corps imaginaire*
- *$\lambda > 0$ et $\sigma(\lambda) > 0$ dans le cas d'un corps réel.*

On le note $\lambda \gg 0$

Proposition 1.1. *$N(\alpha) > 0 \Leftrightarrow \alpha \gg 0$ ou $-\alpha \gg 0$*
Démonstration
2 cas : le corps est imaginaire, ou reel... □

Remarque 1.1. *si $\alpha \gg 0$ et $\beta \gg 0$ alors $\alpha\beta \gg 0$.*

Théorème 1.2 (90 de Hilbert). *Soient $\mathbb{K}$ un corps inclu dans $\mathbb{C}$, et $\mathbb{L} \in \mathbb{C}$ une extension cyclique de degré n de $\mathbb{K}$, G le groupe de Galois de $\mathbb{L}/\mathbb{K}$, engendré par un élément σ.*
Alors $\forall x \in \mathbb{L}\ N(x) = 1 \Leftrightarrow \exists y \neq 0\ x = \frac{y}{\sigma(y)}$.
Démonstration
$\Rightarrow$: clair
$\Leftarrow$: Si $N(x) = 1$, soit $\tau = id + x\sigma + ... + x\sigma(x)...\sigma^{n-2}(x)\sigma^{n-1} \neq 0$.
Par le Théorème de Dedekind, $\exists z \in L\ \tau(z) \neq 0$
Soit $y = \tau(z)$.
On a bien $x = \frac{y}{\sigma(y)}$. □

Notation : $\frac{y}{\sigma(y)} = y^{1-\sigma}$

Proposition 1.3. *Dans le cas où $\mathbb{K}$ est quadratique :*
Soit $\mathfrak{a}$, un idéal fractionaire de $\mathcal{O}_{\mathbb{K}}$
Si $N(\mathfrak{a}) = 1$, alors $\exists \mathfrak{b} \in I(\mathcal{O}_{\mathbb{K}})$ tel que $\mathfrak{a} = \frac{\mathfrak{b}}{\sigma(\mathfrak{b})} = \mathfrak{b}^{1-\sigma}$
Démonstration
Soit $\mathfrak{c} = \mathcal{O}_{\mathbb{K}} + \mathfrak{a}$
$\exists \lambda \in \mathbb{Z}$ tel que $\lambda \neq 0$ et $\mathfrak{b} = \lambda\mathfrak{c} \in I(\mathcal{O}_{\mathbb{K}})$
$\mathfrak{a}\sigma(\mathfrak{b}) = \lambda\mathfrak{a}(\mathcal{O}_{\mathbb{K}} + \sigma(\mathfrak{a})) = \lambda(\mathfrak{a} + \mathfrak{a}\sigma(\mathfrak{a})) = \lambda(\mathfrak{a} + \mathcal{O}_{\mathbb{K}}) = \lambda\mathfrak{c} = \mathfrak{b}$
Donc $\mathfrak{a} = \frac{\mathfrak{b}}{\sigma(\mathfrak{b})}$ □

2 Définitions

Définition 2.1. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux fractionnaires de $\mathcal{O}_{\mathbb{K}}$ alors :*
- *$\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \exists \lambda \in \mathbb{K}\ \mathfrak{a} = \lambda\mathfrak{b}$*
- *$\mathfrak{a} \overset{+}{\sim} \mathfrak{b} \Leftrightarrow \exists \lambda \in \mathbb{K}\ \lambda \gg 0$ et $\mathfrak{a} = \lambda\mathfrak{b}$*
- *$\mathfrak{a} \approx \mathfrak{b} \Leftrightarrow \exists \lambda \in \mathbb{K}\ N(\mathfrak{a}) = N(\lambda)N(\mathfrak{b})$*
  On dit alors $\mathfrak{a}$ et $\mathfrak{b}$ similaires.
- *$\mathfrak{a} \overset{+}{\approx} \mathfrak{b} \Leftrightarrow \exists \lambda \in \mathbb{K}\ \lambda \gg 0$ et $N(\mathfrak{a}) = N(\lambda)N(\mathfrak{b})$*
  On dit alors $\mathfrak{a}$ et $\mathfrak{b}$ de genre similaire. Si $\mathfrak{a} \overset{+}{\approx} (1)$ alors $\mathfrak{a}$ est de genre principal.

Proposition 2.1. *Les quatres relations définies sont des relations d'équivalence compatibles avec la mutliplication des idéaux.*
Démonstration *La premiere a déja été vue, les autres découlent du fait que la norme est multiplicative et de la remarque 1.1.* $\square$

Théorème 2.2. *Soit $\mathcal{J}(\mathbb{K})$, l'ensemble des idéaux fractionnaires de $\mathcal{O}_{\mathbb{K}}$. Soient :*
- $Cl(\mathbb{K}) = \mathcal{J}(\mathbb{K})/\sim$
- $Cl^+(\mathbb{K}) = \mathcal{J}(\mathbb{K})/\overset{+}{\sim}$
- $Cl_{gen}(\mathbb{K}) = \mathcal{J}(\mathbb{K})/\approx$
- $Cl^+_{gen}(\mathbb{K}) = \mathcal{J}(\mathbb{K})/\overset{+}{\approx}$

Ces quatres ensembles, muni de la mutiplication des idéaux sont des groupes finis et commutatifs.

Notation : *On notera $[\mathfrak{a}]_+$ et $[\mathfrak{a}]$ les classes de $\mathfrak{a}$ dans $Cl^+(\mathbb{K})$ et $Cl(\mathbb{K})$ respectivement.*
$h(\mathbb{K})$ et $h^+(\mathbb{K})$ désigneront les cardinaux de $Cl(\mathbb{K})$ et $Cl^+(\mathbb{K})$.
On a de plus $\frac{h^+(\mathbb{K})}{h(\mathbb{K})} \leq 2$ et vaut exactement 1 si $d < 0$.

Démonstration *Le cas de $Cl(\mathbb{K})$ a déjà été vu.*
Le fait que les autres sont des groupes commutatifs est clair.
Montrons la finitude :
On a la suite exacte suivante :
$$1 \longrightarrow <\sqrt{m}> \xrightarrow{i} Cl^+(\mathbb{K}) \xrightarrow{\pi} Cl(\mathbb{K}) \longrightarrow 1$$
Où $<\sqrt{m}> = \{1, [\sqrt{m}]_+\}$, et $\pi : [\mathfrak{a}]_+ \longmapsto [\mathfrak{a}]$
i est clairement injectif et π clairement surjective.
On a aussi $Imi \subset Ker\pi$
Soit $[\mathfrak{a}]_+ \in Ker\pi$
$\exists \alpha \in \mathbb{K}\ \mathfrak{a} = \alpha\mathcal{O}_{\mathbb{K}}$
Si $N(\mathfrak{a}) > 0$, alors on peut prendre $\alpha \gg 0$ et alors, $[\mathfrak{a}]_+ = 1$.
Sinon, on peut prendre $\alpha > 0$ et $\sigma(\alpha) < 0$, alors $\frac{\alpha}{\sqrt{m}} \gg 0$ et alors $[\mathfrak{a}]_+ = [\sqrt{m}]_+$.
Donc $Cl(\mathbb{K}) \simeq Cl^+(\mathbb{K})/<\sqrt{m}>$
Donc $Cl^+(\mathbb{K})$ est fini, et on a $h^+ \leq 2h$
Si $d < 0$, on a $\sqrt{m} \overset{+}{\sim} 1$ donc $h^+ = h$
Les deux autres groupes sont clairement finis. $\square$

3 premières proprietés

Proposition 3.1. *On a les équivalences :*
- $\mathfrak{a} \overset{+}{\approx} \mathfrak{b} \Leftrightarrow \exists \mathfrak{c}\ \mathfrak{a} \overset{+}{\sim} \mathfrak{b}\mathfrak{c}^2$
- $\mathfrak{a} \approx \mathfrak{b} \Leftrightarrow \exists \mathfrak{c}\ \mathfrak{a} \sim \mathfrak{b}\mathfrak{c}^2$

Démonstration *Il suffit de montrer que $\mathfrak{a} \overset{+}{\approx} 1 \Leftrightarrow \exists \mathfrak{c}\ \mathfrak{a} \overset{+}{\sim} \mathfrak{c}^2$*
Si $\mathfrak{a} \overset{+}{\sim} \mathfrak{c}^2$ alors $\exists \lambda \gg 0\ \mathfrak{a} = \lambda\mathfrak{c}^2$.
D'où $N(\mathfrak{a}) = N(\lambda)N(\mathfrak{c})^2 = N(c\lambda)$ où $c = N(\mathfrak{c})$.
Comme $c\lambda \gg 0$, alors $\mathfrak{a} \overset{+}{\approx} 1$.
Si $\mathfrak{a} \overset{+}{\approx} 1$ alors $\exists \lambda \gg 0\ N(\mathfrak{a}) = N(\lambda)$
D'où $N(\lambda^{-1}\mathfrak{a}) = 1$ donc $\exists \mathfrak{c}\ \lambda^{-1}\mathfrak{a} = \mathfrak{c}^{1-\sigma}$, par le théorème 90.
Or, $\mathfrak{c}^{1-\sigma} \overset{+}{\sim} \mathfrak{c}^2$ car $\sigma(\mathfrak{c}) \overset{+}{\sim} \mathfrak{c}^{-1}$, car $N(\mathfrak{c}) \gg 0$.
D'où le résultat. $\square$

Corollaire 3.2. $Cl^+_{gen}(\mathbb{K}) \simeq Cl^+(\mathbb{K})/Cl^+(\mathbb{K})^2 = C_+/{C_+}^2$
$Cl_{gen}(\mathbb{K}) \simeq Cl(\mathbb{K})/Cl(\mathbb{K})^2$
Démonstration *On a la suite exacte suivante :*
$$1 \longrightarrow {C_+}^2 \xrightarrow{i} C_+ \xrightarrow{\pi} Cl^+_{gen} \longrightarrow 1$$
Ceci, grâce à la proposition, d'où le résultat. $\square$

4 calcul du cardinal de C_+/C_+^2

Soit t le nombre de nombres premiers ramifiés dans $\mathbb{K}/\mathbb{Q}$
On va montrer que le cardinal cherché est 2^{t-1}.

Définition 4.1. *Un idéal $\mathfrak{a}$ est dit ambiguë si $\sigma(\mathfrak{a}) = \mathfrak{a}$.*
De même, $c \in C_+$ est dit ambigüe si $c^\sigma = c$.
(on a clairement $\mathfrak{a} \overset{+}{\sim} \mathfrak{b} \Rightarrow \sigma(\mathfrak{a}) \overset{+}{\sim} \sigma(\mathfrak{b})$).

Définition 4.2. $Am^+ = \{c \in C_+ \ c$ *ambiguë* $\}$.
Am^+ est un sous-groupe de C_+.

Proposition 4.1. *On a la suite exacte :*
$1 \longrightarrow Am^+ \longrightarrow C_+ \overset{1-\sigma}{\longrightarrow} C_+^{1-\sigma} \longrightarrow 1$
Démonstration

$$\begin{aligned} c = [\mathfrak{a}]_+ \in Ker(1-\sigma) &\iff c^{1-\sigma} = 1 \\ &\iff c = c^\sigma \\ &\iff c \in Am^+ \end{aligned}$$

□

Corollaire 4.2. $Am^+ \simeq C_+/C_+^2$

On voit donc qu'un idéal ambiguë engendre une classe ambiguë. On a aussi la réciproque :

Proposition 4.3. *Les classes ambiguës de C_+ sont exactement celles engendrées par les idéaux ambiguës.*
Démonstration *Si $c = [\mathfrak{a}]_+$ est ambiguë, $\exists \lambda \gg \mathfrak{a}^\sigma = \lambda\mathfrak{a}$*
Donc $N(\lambda) = 1$ et λ est une unité. Comme $\lambda \gg 0$, on a donc $N(\lambda) = +1$.
Par le théorème 90, on a $\lambda = \alpha^{1-\sigma}$ pour un α dans $\mathbb{K}$.
$N(\alpha) = \alpha\sigma(\alpha) = \lambda\sigma(\alpha)^2 \gg 0$
Donc $N(\alpha) > 0$, et donc soit $\alpha \gg 0$, soit $-\alpha \gg 0$.
Quitte à remplacer α en $-\alpha$, on peut supposer $\alpha \gg 0$.
$\mathfrak{a}^\sigma = \frac{\alpha}{\sigma(\alpha)}\mathfrak{a}$ *donc $(\alpha\mathfrak{a})^\sigma = \alpha\mathfrak{a}$, donc $\alpha\mathfrak{a}$ est ambigu et $\mathfrak{a} \overset{+}{\sim} \alpha\mathfrak{a}$.*
On en déduis donc que $c = [\alpha\mathfrak{a}]_+$ est engendré par un idéal ambigu. □

Remarque 4.1. *Ceci est faux dans $Cl(\mathbb{K})$.*

Proposition 4.4. *Si A est l'ensemble des idéaux ambigus alors on a :*
$A \simeq (\mathbb{Z}/2\mathbb{Z})^t \oplus I$ où I désigne le groupe des idéaux engendrés par un rationel.
Démonstration *Laissée en exercice...* □

Lemme 4.5 (du serpent). *Si on a le diagramme exact et commutatif de groupes abéliens suivant :*

$$\begin{tikzcd} & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 1 \\ 1 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' & \end{tikzcd}$$

Alors on a la suite exacte :

$$1 \longrightarrow ker\ f \longrightarrow ker\ \alpha \longrightarrow ker\ \beta \longrightarrow ker\ \gamma \overset{\delta}{\longrightarrow} coker\ \alpha \longrightarrow coker\ \beta \longrightarrow coker\ \gamma \longrightarrow coker\ g' \longrightarrow 1$$

Démonstration *Laissée en exercice...* □

Proposition 4.6. *Si E désigne le groupe des unités totalement positives dans $\mathcal{O}_\mathbb{K}$, alors : le cardinal de Am^+ est* $\frac{2^t}{[E:E^{1-\sigma}]}$.

Démonstration *On a :*

$$\begin{array}{ccc} A & \xrightarrow{\pi} & Am^+ \\ \mathfrak{a} & \longmapsto & [\mathfrak{a}]_+ \end{array}$$

est surjective, d'apres la proposition.
ker $\pi = \{\mathfrak{a}/\mathfrak{a}^\sigma = \mathfrak{a}$ *et* $\mathfrak{a} \overset{+}{\sim} 1\}$
ker $\pi = \{\mathfrak{a}/\mathfrak{a}^\sigma = \mathfrak{a}$ *et* $\mathfrak{a} = (\alpha)$ *pour un* $\alpha \gg 0\} = H$
On a donc $I \subset H$
On a le diagramme exact et commutatif suivant :

$$\begin{tikzcd} 1 \arrow[r] & I \arrow[r, "Id"] \arrow[d, "i"] & I \arrow[r] \arrow[d, "i"] & 1 \arrow[d] & \\ 1 \arrow[r] & H \arrow[r, "j"] & A \arrow[r, "\pi"] & Am^+ \arrow[r] & 1 \end{tikzcd}$$

On applique donc le lemme du serpent à notre diagramme et on obtient la suite exacte :

$$1 \longrightarrow H/I \longrightarrow A/I \longrightarrow Am^+ \longrightarrow 1$$

Caluculons le cardinal de H/I.
Soit $(\alpha) \in H$ *tq* $\alpha \gg 0$
(α) *ambigu* $\Rightarrow \epsilon = \alpha^{1-\sigma}$ *est une unité totalement positive.*

- *Soit :*

$$\begin{array}{rccc} \rho \ : & H & \longrightarrow & E/E^{1-\sigma} \\ & (\alpha) & \longmapsto & \alpha^{1-\sigma} \end{array}$$

  est bien défini car si $(\alpha) = (\alpha')$, *alors* $(\alpha/\alpha') = 1$
  donc $\alpha/\alpha' = \eta \in E \Rightarrow \alpha^{1-\sigma} = \eta^{1-\sigma} \times \alpha'^{1-\sigma}$, *et* $\eta^{1-\sigma} \in E^{1-\sigma}$

- *ker* $\rho = I$ *En effet :*
  $\alpha^{1-\sigma} = 1 \Leftrightarrow \alpha = \sigma(\alpha) \Leftrightarrow \alpha \in \mathbb{Q}$
- ρ *est surjective :*
  Soit $\epsilon \in E$, *on a donc* $N(\epsilon) = +1 \Rightarrow \exists \alpha \in \mathbb{K}\ \epsilon = \alpha^{1-\sigma}$
  $N(\alpha) = \alpha\sigma(\alpha) = \epsilon(\sigma(\alpha))^2 \gg 0 \Rightarrow N(\alpha) > 0$
  On peut choisir $\alpha \gg 0$, *ainsi* $(\alpha) \in H$ *car* $\sigma(\alpha) = \alpha\epsilon^{-1} \Rightarrow \sigma((\alpha)) = (\alpha)$
  $\rho((\alpha)) = \epsilon E^{1-\sigma}$

On en déduit donc que $H/I \simeq E/E^{1-\sigma}$ *(fini grâce à la suite exacte).*
Comme on a aussi $A/I \simeq (\mathbb{Z}/2\mathbb{Z})^t$, *on a alors :*

$$|Am^+| = \frac{2^t}{[E : E^{1-\sigma}]}$$

□

Théorème 4.7. $Am^+ \simeq C_+/{C_+}^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$
Démonstration *On avait déjà :*
- $Am^+ \simeq \frac{(\mathbb{Z}/2\mathbb{Z})^t}{E/E^{1-\sigma}}$
- $Am^+ \simeq C_+/{C_+}^{1-\sigma}$

Or $\mathfrak{a}^{-1} \overset{+}{\sim} \sigma(\mathfrak{a})$, *d'où* $\mathfrak{a}^{1-\sigma} \overset{+}{\sim} \mathfrak{a}^2$ *et donc* ${C_+}^{1-\sigma} = {C_+}^2$.
Il ne reste plus qu'à montrer que $[E : E^{1-\sigma}] = 2$, *car* Am_+ *sera alors un groupe d'ordre* 2^{t-1} *dont tous les élément* $\neq 0$ *seront d'ordre 2.*

- *Si* $d < 0$ *:*
  E *est l'ensemble des unités de* $\mathcal{O}_{\mathbb{K}}$ *car toutes les unités sont totalement positives.*
  E *est donc un groupe cyclique (car* $E = \{\frac{x+y\sqrt{m}}{2} \in \mathcal{O}_{\mathbb{K}} \ / \ x^2 - my^2 = \pm 4\}$ *)*
  soit $E = \langle \xi \rangle$*, on a* $\xi^{1-\sigma} = \xi^2$
  $2 | \# E$ *car* $\{-1, 1\}$ *est un sous-groupe de* E*.*
  Donc $\langle \xi^2 \rangle \neq E \Rightarrow [E : E^{1-\sigma}] = 2$*.*
- *Si* $d > 0$ *:*
  L'equation de Pells a un nombre infini de solution, et $E_{\mathbb{K}}$*, l'ensemble des unités de* $\mathbb{K}$ *est monogene, engendré par un élément* ϵ*.*
  - *Si* $N(\epsilon) = +1$*, alors* $E = \langle \epsilon \rangle$ *et* $E^{1-\sigma} = \langle \epsilon^2 \rangle$*, d'où le résultat.*
  - *Si* $N(\epsilon) = -1$*, alors* $E = \langle \epsilon^2 \rangle$ *et* $E^{1-\sigma} = \langle \epsilon^4 \rangle$*, d'où le résultat.*

□

Proposition 4.8. *Si* $\mathbb{K}$ *est réel, alors sont équivalents :*
1. ${Cl_{gen}}^+(\mathbb{K}) \simeq Cl_{gen}(\mathbb{K})$
2. $(\sqrt{m}) \stackrel{+}{\approx} (1)$
3. m *est la somme de deux carrés*

De plus : $Cl_{gen}(\mathbb{K}) \simeq (\mathbb{Z}/2\mathbb{Z})^s$*, où* $s = t - 1$ *si* m *est la somme de deux carrés, et* $t - 2$ *sinon.*
Démonstration *Soit :*

$$\begin{array}{rcl} \pi : {Cl_{gen}}^+(\mathbb{K}) & \longrightarrow & Cl_{gen}(\mathbb{K}) \\ {[\mathfrak{a}]_+}^g & \longmapsto & [\mathfrak{a}]^g \end{array}$$

- *Supposons (1).*
  $(\sqrt{m}) \approx (1)$ *donc* $(\sqrt{m}) \stackrel{+}{\approx} (1)$*.*
- *réciproquement, supposons (2).*
  si ${[\mathfrak{a}]_+}^g \in ker\ \pi$*, alors* $\mathfrak{a} \approx (1)$*, et donc* $\exists \mathfrak{c}\ \mathfrak{a} \sim \mathfrak{c}^2$*, d'où* $\exists \lambda\ \mathfrak{a} = \lambda \mathfrak{c}^2$*.*
  - *si* $N(\lambda) > 0$*, alors on peut prendre* $\lambda > 0$ *et* $\mathfrak{a} \stackrel{+}{\sim} \mathfrak{c}^2 \Rightarrow \mathfrak{a} \stackrel{+}{\approx} (1) \Rightarrow {[\mathfrak{a}]_+}^g = {[1]_+}^g$*.*
  - *Si* $N(\lambda) < 0$*, alors* $N(\lambda\sqrt{m}) > 0$*, et* $\mathfrak{a}\sqrt{m} = \lambda\sqrt{m}\mathfrak{c}^2$ *donc* $\mathfrak{a}\sqrt{m} \stackrel{+}{\approx} (1)$*, et comme* $\sqrt{m} \stackrel{+}{\approx} (1)$*, on a* $\mathfrak{a} \stackrel{+}{\approx} (1)$

  Donc π *est injectif, et (1)⇔(2).*
- *Supposons (2)*
  $\exists \lambda \gg 0\ \exists \mathfrak{c}\ (\sqrt{m}) = \lambda \mathfrak{c}^2$
  On peut prendre $\lambda = \frac{1}{2}(a + b\sqrt{m})$
  En passant aux normes ($c = N(\mathfrak{c})$*), on a donc :*

$$4m = (a^2 - mb^2)c^2$$

  Donc $m | a$*, d'où* $a = mA$
  Et on en déduit :

$$mA^2c^2 = 4 + b^2c^2$$

  De là, on peut en tirer (3).
- *réciproquement, si* $m = r^2 + s^2$*, avec* s *impair ;* $s \geqslant 0$ *et* $r \geqslant 0$*.*
  Soit $\mathfrak{c} = (s, r + \sqrt{m})$*, on a donc* $\mathfrak{c}^2 = (r + \sqrt{m})$*, d'où* $\sqrt{m}\mathfrak{c}^2 = (r\sqrt{m} + m) = (\lambda)$
  $\lambda > 0$*, et* $\sigma(\lambda) = m - r\sqrt{m} > 0$ *donc* $\lambda \gg 0$*, et* $\sqrt{m} \stackrel{+}{\sim} \mathfrak{c}^2$ *Donc* $(\sqrt{m}) \stackrel{+}{\approx} (1)$*.*

Finalement, si m *est somme de deux carrés, alors* ${Cl_{gen}}^+(\mathbb{K}) \simeq Cl_{gen}(\mathbb{K}) \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$*.*
Sinon, π *n'est pas injective, et son noyau est de cardinal* 2*. Donc* $Cl_{gen}(\mathbb{K}) \simeq (\mathbb{Z}/2\mathbb{Z})^{t-2}$ □

5 Références

Lemmermeyer Franz, Reciprocity laws from Euler to Eisenstein, Springer monographs in mathematics.

Kenneth Ireland & Michael Rosen, A Classical Introduction to Modern Number Theory, Graduate texts in mathematics 84.