Représentation des nombres premiers par les formes quadratiques de discriminant -39

Il existe quatre formes quadratiques primitives réduites de discriminant -39 :

$$q_0 = x^2 + xy + 10y^2, \qquad q_2 = 3x^2 + 3xy + 4y^2, \qquad q_1, q_3 = 2x^2 \pm xy + 5y^2.$$

Le groupe des classes de formes quadratiques de discriminant -39 est engendré par q_1 et l'on a $q_i = q_1^i$, pour $0 \leqslant i \leqslant 3$. On veut essayer de trouver quels nombres premiers sont représentés par ces formes respectives.

1. Genre

On appelle *discriminant* un entier non nul congru à 0 ou 1 modulo 4.

Entiers représentés par une forme quadratique

1.1. — Lemme. *Soient q une forme quadratique et m un entier. Alors q représente proprement m si et seulement si elle est équivalente à une forme dont le coefficient en x^2 est m.*

Démonstration — Supposons que q soit équivalente à $mx^2+bxy+cy^2$. Alors, il existe des entiers $\alpha, \beta, \gamma, \delta$ tels que

$$q(\alpha x + \beta y, \gamma x + \delta y) = mx^2 + bxy + cy^2 \qquad \text{et } \alpha\delta - \beta\gamma = 1.$$

Pour $x = 1$ et $y = 0$, on obtient $q(\alpha, \gamma) = m$. De plus, α et γ sont premiers entre eux puisqu'ils vérifient l'identité de Bezout.

Inversement, supposons qu'il existe des entiers α, γ premiers entre eux tels que $q(\alpha, \gamma) = m$. D'après bezout, il existe β, γ tels que $\alpha\delta - \beta\gamma = 1$. Le coefficient en x^2 de la forme $q(\alpha x + \beta y, \gamma x + \delta y)$ est m. □

1.2. — Lemme. *Soit D un discriminant, et soit m un entier étranger à $2D$. Alors m est proprement représenté par (au moins) une forme primitive de discriminant D si et seulement si D est un carré modulo m.*

Démonstration — Si m est proprement représenté par une telle forme q alors, d'après 1.1, la forme q est équivalente à une forme du type $mx^2+bxy+cy^2$. Mais alors son discriminant b^2-4mc est D, ce qui montre que D est un carré modulo m.

Supposons que D est un carré modulo m. Notons que D est aussi un carré modulo 4, puisque congru à 0 ou 1 modulo 4. Puisque m est impair, on en déduit que D est un carré modulo $4m$. Ainsi, $D = b^2 - 4mc$ avec $b, c \in \mathbb{Z}$. La forme $mx^2 + bxy + cy^2$ est de discriminant D et représente proprement m. De plus, elle est primitive puisque m est étranger à D. □

1.3. — Corollaire. *Soient D un discriminant et p un nombre premier ne divisant pas $2D$. Alors p est représenté par (au moins) une forme de discriminant D si et seulement si $(D/p) = 1$.*

Remarque. Si $D \equiv 1$ modulo 4, la démonstration du lemme 1.2 s'adapte facilement au cas $m = 2$. On s'aperçoit alors que 2 est proprement représenté par une forme quadratique de discriminant D si et seulement si D est un carré modulo 8, c'est-à-dire $D \equiv 1$ modulo 8. Cela permet d'étendre le corollaire ci-dessus à tout premier p ne divisant pas D en posant $(D/2) = (2/D)$ pour $D \equiv 1$ modulo 4.

1.4. — Proposition. *Soient q_1 et q_2 deux formes de même discriminant représentant le même nombre premier p. Alors q_1 et q_2 sont équivalentes ou improprement équivalentes.*

Démonstration — D'après le lemme 1.1, on peut supposer que

$$q_1 = px^2 + b_1xy + c_1y^2 \quad \text{et} \quad q_2 = px^2 + b_2xy + c_2y^2 \qquad \text{avec } b_1, b_2, c_1, c_2 \in \mathbb{Z}.$$

On a $b_1^2 - 4pc_1 = b_2^2 - 4pc_2$. Il en résulte que b_1 et b_2 ont même parité et que $b_1^2 \equiv b_2^2 \pmod{p}$, soit $b_1 \equiv \pm b_2 \pmod{p}$. Si p est impair, on en déduit $b_1 \equiv \pm b_2 \bmod 2p$. Si $p = 2$, on fait la même déduction $b_1 \equiv \pm b_2 \bmod 4$ en remarquant que $b_1^2 \equiv b_2^2 \pmod{8}$. Il est alors facile de voir que q_1 et q_2 sont équivalentes dans le cas du signe $+$, et improprement équivalentes dans le cas du signe $-$. □

1.5. — **Lemme.** *Soit D un discriminant négatif.* • *L'ensemble des valeurs représentées par la forme principale de discriminant D :*

$$q_0(x,y) = \begin{cases} x^2 - \dfrac{D}{4}y^2 & \text{si } D \equiv 0 \pmod 4 \\ x^2 + xy + \dfrac{1-D}{4}y^2 & \text{si } D \equiv 1 \pmod 4 \end{cases}$$

est une partie multiplicative de $\mathbb{Z}$, contenant les carrés.

• *Soit q une forme quadratique de discriminant D. Notons Q et Q_0 les ensembles d'entiers représentés respectivement par q et q_0. On a*

$$QQ_0 \subseteq Q \qquad \text{et} \qquad QQ \subseteq Q_0.$$

Démonstration — • Soit $\tau = \sqrt{D}$ si $D \equiv 0$ modulo 4 et $\tau = (-1+\sqrt{D})/2$ si $D \equiv 1$ modulo 4. Alors, $q_0(x,y)$ est la norme $N(x - y\tau)$. Comme l'ensemble $\mathbb{Z} + \mathbb{Z}\tau$ est stable par produit (parce que τ est un entier quadratique), et parce que la norme est multiplicative, l'ensemble Q_0 est stable par produit. Il est évident qu'il contient les carrés.

• Notons $q = ax^2 + bxy + cy^2$. Si $D \equiv 0$ modulo 4 (donc b pair), on pose $b' = b/2$; si $D \equiv 1$ modulo 4 (donc b impair), on pose $b' = (b-1)/2$. Alors, les identités

$$x^2 + bxy + acy^2 = \begin{cases} (x+b'y)^2 - \dfrac{D}{4}y^2 & \text{si } D \equiv 0 \pmod 4 \\ (x+b'y)^2 + (x+b'y)y + \dfrac{1-D}{4}y^2 & \text{si } D \equiv 1 \pmod 4 \end{cases}$$

montrent que la forme q_0 est équivalente à $x^2 + bxy + acy^2$. L'ensemble des entiers représentés par cette dernière est donc Q_0. Mais on a l'identité

$$(ax^2+bxy+cy^2)(x'^2+bx'y'+cy'^2) = a(xx'-cyy')^2 + b(xx'-cyy')(axy'+yx'+byy') + c(axy'+yx'+byy')^2$$

qui prouve alors la première inclusion $QQ_0 \subseteq Q$.

Enfin, l'identité

$$(ax^2+bxy+cy^2)(ax'^2+bx'y'+cy'^2) = (axx'+bxy'+cyy')^2 + b(axx'+bxy'+cyy')(yx'-xy') + ac(yx'-xy')^2$$

montre que $QQ \subseteq Q_0$. □

Classes de $(\mathbb{Z}/D\mathbb{Z})^*$ représentées par une forme de discriminant D

1.6. — **Lemme.** *Soit D un discriminant et m, n deux entiers positifs relativement premiers à $2D$ tels que $m \equiv n$ modulo D. Alors, on a l'identité*

$$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right)$$

entre symboles de Jacobi.

Démonstration — C'est un énoncé caché de la loi de réciprocité quadratique. Exercice. Attention aux cas $D < 0$ ou D pair. □

Considérons l'application définie sur les entiers positifs étrangers à $2D$ et envoyant ces entiers n sur le symbole de Jacobi (D/n). Le lemme 1.6 montre que cette application induit un homomorphisme de groupes χ :

$$\chi \begin{cases} (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\} \\ [n] \longmapsto \left(\dfrac{D}{n}\right). \end{cases}$$

On montre alors que

$$\chi([-1]) = \begin{cases} 1 & \text{si } D > 0 \\ -1 & \text{si } D < 0 \end{cases} \qquad \text{et, pour } D \equiv 1 \pmod 4, \quad \chi([2]) = \left(\frac{2}{D}\right).$$

Cela permet un retour de définir le *symbole de Kronecker*, pour D discriminant et n étranger à D (éventuellement négatif ou pair) par $(D/n) = \chi([n])$. Le corollaire 1.3 et la remarque sur $p = 2$ qui le suit indiquent que les premiers ne divisant pas D représentés par une forme quadratique de discriminant D sont ceux dont la classe modulo D appartient au noyau de χ. Ce noyau est un sous-groupe d'indice 2 de $(\mathbb{Z}/D\mathbb{Z})^*$.

1.7. — Lemme. *Soit q une forme primitive et m un entier non nul. Alors q représente proprement un entier étranger à m.*

DÉMONSTRATION — Notons d'abord que, puisque q est primitive, que les trois entiers

$$q(1,0) = a, \qquad q(0,1) = c, \qquad q(1,1) = a+b+c$$

sont globalement premiers entre eux. Donc, pour chaque p premier diviseur de m, on peut trouver $(x_p, y_p) \in \{(1,0),(0,1),(1,1)\}$ tels que $q(x_p, y_p)$ ne soit pas divisible par p. Enfin, le théorème chinois assure l'existence d'entiers x, y tels que $x \equiv x_p$ et $y \equiv y_p$ modulo p pour chaque p premier divisant m. Alors $q(x,y)$ est étranger à m. De plus, si d désigne $\operatorname{pgcd}(x,y)$, l'entier $q(x/d, y/d)$ est aussi étranger à m et est proprement représenté. □

1.8. — Proposition. *Soit D un discriminant négatif.* • *Les valeurs de $(\mathbb{Z}/D\mathbb{Z})^*$ représentées par la forme réduite principale de discriminant D forment un sous-groupe H de $\ker\chi$. De plus, ce sous-groupe H est donné par*

$$H = \begin{cases} \{[u^2], [u^2 - D/4] \in (\mathbb{Z}/D\mathbb{Z})^* \mid u \in \mathbb{Z}\} & \text{lorsque } D \equiv 0 \text{ modulo } 4 \\ \{[u^2] \in (\mathbb{Z}/D\mathbb{Z})^* \mid u \in \mathbb{Z}\} & \text{lorsque } D \equiv 1 \text{ modulo } 4. \end{cases}$$

• *Les valeurs de $(\mathbb{Z}/D\mathbb{Z})^*$ représentées par une forme primitive q forment une classe modulo H dans $\ker\chi$.*

DÉMONSTRATION — • Le lemme 1.5 indique que la partie H est multiplicative et, d'après 1.3, qu'elle est contenue dans $\ker\chi$. De plus, elle contient la classe [1] (car 1 est un carré). Or, pour $[x] \in H$, l'application $H \ni [y] \mapsto [xy] \in H$ est injective puisque $[y]$ est inversible dans $\ker\chi$. Comme H est fini, cette application est surjective donc $[x]$ est inversible dans H. On a montré que H est un sous-groupe de $(\mathbb{Z}/D\mathbb{Z})^*$. Il reste à expliciter H.

D'abord le cas où $D \equiv 1$ modulo 4. Toute classe de type $[u^2]$ est représentée par la forme principale (prendre $x = u$ et $y = 0$). Inversement, l'identité

$$4(x^2 + xy + \frac{1-D}{4}y^2) \equiv (2x+y)^2 \quad \text{modulo } D$$

montre que toute classe représentée est de type $[u^2]$.

Ensuite, le cas où $D \equiv 0$ modulo 4. Il est clair que les classes de type $[u^2]$ sont les classes représentées par $x^2 - (D/4)y^2$ pour y pair et que les classes de $[u^2 - D/4]$ sont celles représentées pour y impair.

• Soit C l'ensemble des classes de $(\mathbb{Z}/D\mathbb{Z})^*$ représentées par q et soient Q et Q_0 les ensembles d'entiers représentés respectivement par q et q_0. D'après le lemme 1.7, l'ensemble Q contient un entier a étranger à D. En conséquence, C est non vide. Nous allons montrer que $C = aH$. L'inclusion $aQ \subseteq QQ \subseteq Q_0$ démontrée dans le lemme 1.5 implique que $aC \subseteq H$. Mais $[a]$ est inversible dans $(\mathbb{Z}/D\mathbb{Z})^*$ et, puisque $a^2 \in H$, son inverse est $[a]$. On obtient donc $C \subseteq [a]^{-1}H = aH$. Enfin, l'inclusion $aQ_0 \subseteq QQ_0 \subseteq Q$ implique $aH \subseteq C$. □

Pour être précis, en utilisant le fait que a est un carré modulo 2^e ($e \in \mathbb{N}^*$) si et seulement si $a \equiv 1$ modulo 8, on peut montrer (je crois) que le sous-groupe H est strictement plus grand que le sous-groupe des carrés si et seulement si $D \equiv 0$ modulo 4 mais $D \not\equiv 0$ modulo 32 et $D \not\equiv 12$ modulo 16.

1.9. — Définition. On dit que deux formes quadratiques primitives de discriminant D appartiennent au même *genre* lorsqu'elles représentent les mêmes classes inversibles modulo D.

Le cas $D = -39$

Par le théorème chinois, on a

$$(\mathbb{Z}/39\mathbb{Z})^* \simeq (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/13\mathbb{Z})^*.$$

Puisque les sous-groupes des carrés dans $(\mathbb{Z}/3\mathbb{Z})^*$ et $(\mathbb{Z}/13\mathbb{Z})^*$ sont respectivement $\{1\}$ et $\{1,3,4,9,10,12\}$, on en déduit que le sous-groupe H des carrés de $(\mathbb{Z}/39\mathbb{Z})^*$ est

$$H = \{1,4,10,16,22,25\} \simeq \{1\} \times \{1,3,4,9,10,12\}.$$

L'unique autre classe H' de $\ker\chi$ modulo H est

$$H' = \{2,5,8,11,20,32\} \simeq \{2\} \times \{2,5,6,7,8,11\}$$

et $\ker\chi = H \cup H' = \{1,2,4,5,8,10,11,16,20,22,25,32\}$.

Les formes q_0 et q_2 représentent respectivement 1 et 4 dont les classes appartiennent à H. Ces deux formes appartiennent au *genre principal*. Les formes q_1 et q_3 représentent 2 dont la classe est dans H'. Elles appartiennent à l'autre genre.

1.10. — Proposition. *Pour qu'un nombre premier impair p ne divisant pas 39 soit représenté par q_1 (resp. q_3), il faut et il suffit que p soit congru à 2, 5, 8, 11, 20 ou 32 modulo 39.*

DÉMONSTRATION — Les formes q_1 et q_3 sont improprement équivalentes ; elles représentent donc les mêmes entiers. Elles constituent l'unique genre non principal donc représentent p si et seulement si $[p] \in H'$. □

1.11. — Problème. Les formes q_0 et q_2 appartiennent au même genre (le genre principal) mais ne sont pas improprement équivalentes. A elles deux, elles représentent les nombres premiers dont la classe est dans H. Parmi ceux-ci, il reste à déterminer lesquels sont représentés par q_0 et lesquels sont représentés par q_2.

2. Corps de classes

2.1. — Proposition. *Soit L une extension galoisienne d'un corps de nombres K. Soient a un entier algébrique primitif de l'extension L/K et f le polynôme minimal de a sur K. On désigne par $\mathfrak{p}$ un premier de K et on suppose que f est séparable modulo $\mathfrak{p}$ (en conséquence $\mathfrak{p}$ est non-ramifié dans L). Soit*

$$f \equiv f_1 f_2 \cdots f_g \pmod{\mathfrak{p}}$$

la décomposition de f dans $K[X]/\mathfrak{p}$. Alors, la décomposition de l'idéal $\mathfrak{p}\mathcal{O}_L$ en idéaux premiers est

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g \qquad \text{où } \mathfrak{P}_i \text{ est l'idéal de } L \text{ engendré par } \mathfrak{p} \text{ et } f_i(a).$$

De plus, les f_i ont tous le même degré, qui est le degré résiduel des $\mathfrak{P}_i$.

DÉMONSTRATION — Voir [1] page 102. □

2.2. — Rappels (symbole d'Artin). *Soit L/K une extension galoisienne de corps de nombres de groupe de Galois G. Soient $\mathfrak{p}$ un premier de K et $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. Notons D le groupe de décomposition de $\mathfrak{P}$, c'est-à-dire les éléments $\sigma \in G$ tels que $\sigma(\mathfrak{P}) = \mathfrak{P}$. Tout élément σ de D définit par passage au quotient un élément $\hat{\sigma}$ de $\hat{G} = \mathrm{Gal}(L/\mathfrak{P}, K/\mathfrak{p})$. Alors, l'application $\sigma \mapsto \hat{\sigma}$ est surjective et, si $\mathfrak{p}$ est non ramifié, elle est injective. Dans ce cas, on appelle symbole d'Artin de $\mathfrak{P}$ et on note $(L/K/\mathfrak{P})$ l'élément de G dont l'image est l'automorphisme de Frobenius de $\hat{G}$. Il résulte de la définition que l'ordre de ce symbole d'Artin est $|\hat{G}|$, c'est-à-dire le degré résiduel de $\mathfrak{P}$. Par multiplicativité, on définit le symbole d'Artin de n'importe quel idéal non nul et non ramifié de L. Lorsque l'extension L/K est abélienne, le symbole d'Artin $(L/K/\mathfrak{P})$ ne dépend pas de l'idéal $\mathfrak{P}$ de L mais seulement de l'idéal $\mathfrak{p}$ de K. Cela permet alors de définir le symbole d'Artin sur les idéaux de K.*

Soit K un corps de nombres. L'ensemble des extensions abéliennes non ramifiées de K contient un élément maximal, appelé le *Corps des classes de Hilbert de K*. De plus, on a le résultat fondamental suivant :

2.3. — Théorème (Réciprocité d'Artin). *Soit K un corps de nombres et L son corps des classes de Hilbert. Alors l'application d'Artin :*

$$\begin{cases} \{\text{idéaux de } K\} \longrightarrow \mathrm{Gal}(L/K) \\ I \longmapsto \left(\dfrac{L/K}{I}\right) \end{cases}$$

est surjective et définit par passage au quotient un isomorphisme de l'ensemble des classes d'idéaux de K sur $\mathrm{Gal}(L/K)$.

DÉMONSTRATION — Jamais vue. □

2.4. — Théorème. *Soit L le corps des classes de Hilbert d'un corps de nombres K et soit $\mathfrak{p}$ un premier de K. Alors*

$$\textit{l'idéal } \mathfrak{p} \textit{ est totalement décomposé dans } L \iff \textit{l'idéal } \mathfrak{p} \textit{ est principal.}$$

DÉMONSTRATION — D'après la réciprocité d'Artin 2.3, l'ideal $\mathfrak{p}$ est principal si et seulement si le symbole d'Artin $(L/K/\mathfrak{p})$ est l'identité. Or, on a vu plus haut que l'ordre de ce symbole d'Artin est le degré résiduel des idéaux au dessus de $\mathfrak{p}$. Cet ordre vaut donc 1 si et seulement si $\mathfrak{p}$ est totalement décomposé. □

On appelle discriminant *fondamental* un discriminant d'un corps de nombres. Autrement dit, c'est un entier D tel que

$$\begin{cases} D \equiv 1 \text{ modulo } 4 \\ D \text{ sans facteur carré} \end{cases} \quad \text{ou} \quad \begin{cases} D \equiv 0 \text{ modulo } 4 \\ D/4 \equiv 2 \text{ ou } 3 \text{ modulo } 4 \text{ et sans facteur carré} \end{cases}$$

2.5. — Proposition. *Soit D un discriminant fondamental négatif et soit L le corps de classes de Hilbert de $K = \mathbb{Q}(\sqrt{D})$. Soit p est un premier ne divisant pas D.*

• *L'entier p est représenté par la forme principale si et seulement si l'idéal $p\mathbb{Z}$ se décompose en deux idéaux principaux de K.*

• *L'idéal $p\mathbb{Z}$ de décompose en deux idéaux principaux dans K si et seulement s'il est totalement décomposé dans L.*

DÉMONSTRATION — • Puisque D est fondamental, l'anneau des entiers de K est $\mathbb{Z}+\tau\mathbb{Z}$ où $\tau = \sqrt{D}$ si $D \equiv 0$ modulo 4 ou $\tau = (-1+\sqrt{D})/2$ si $D \equiv 1$ modulo 4. La forme quadratique principale q_0 de discriminant D est la norme

$$q_0(x,y) = N(x - y\tau) = \begin{cases} x^2 - \dfrac{D}{4}y^2 & \text{si } D \equiv 0 \text{ modulo } 4 \\ x^2 + xy + \dfrac{1-D}{4}y^2 & \text{si } D \equiv 1 \text{ modulo } 4 \end{cases}$$

On voit alors que p est représenté par q_0 si et seulement si $p\mathbb{Z}$ se décompose en deux idéaux principaux dans K, à savoir les idéaux engendrés par $x - y\tau$ et $x - y\bar{\tau}$.

• Supposons que $p\mathbb{Z}$ se décompose dans K en produit $pK = (\pi)(\overline{\pi})$ de deux idéaux principaux. D'après 2.4, les idéaux (π) et $(\overline{\pi})$ sont totalement décomposés dans L, donc $p\mathbb{Z}$ est totalement décomposé dans L.

Inversement, si $p\mathbb{Z}$ est totalement décomposé dans L, alors il est (totalement) décomposé $pK = \mathfrak{p}_1\mathfrak{p}_2$ dans K et les idéaux $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont totalements décomposés dans L. D'après 2.4, les idéaux $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont principaux. □

Il doit exister un énoncé voisin dans le cas où le discriminant D n'est plus supposé fondamental. Voir [1] exercice 9.3.

2.6. — Proposition. *Soit K un corps quadratique et L son corps des classes de Hilbert.*

• *Le corps L est une extension galoisienne de $\mathbb{Q}$.*

• *L'extension $L : K$ admet un générateur réel.*

• *Soit a un générateur réel de L sur K et soit f le polynôme minimal de a sur $\mathbb{Q}$. Alors, pour p premier ne divisant pas le discriminant de f, on a l'équivalence*

$$p \textit{ est totalement décomposé dans } L \iff \begin{cases} p \textit{ est décomposé dans } K \\ f \textit{ admet une racine modulo } p. \end{cases}$$

DÉMONSTRATION — • Le corps L est une extension abélienne non ramifiée de K. Désignons par τ la conjugaison complexe. Il est clair que $\tau(L)$ est une extension abélienne non ramifiée de $\tau(K) = K$. Par maximalité de L, on obtient $\tau(L) = L$.

Il reste à montrer que $\sigma(L) = L$ pour tout automorphisme σ de $\mathbb{C}$. Si σ laisse K fixe alors $\sigma(L) = L$ puisque L est une extension galoisienne de K. Sinon, c'est $\tau\sigma$ qui laisse fixe K. Mais alors $\sigma(L) = \tau(\tau\sigma(L)) = \tau(L) = L$. Cela montre le premier point.

• Le sous-corps de L fixé par τ est $L\cap\mathbb{R}$. Donc L est une extension de degré 2 de $L\cap\mathbb{R}$. Notons $h=[L:K]$ de telle sorte que $[L:\mathbb{Q}]=2h$. On a aussi $[L\cap\mathbb{R}:\mathbb{Q}]=h$.

Soit a tel que $L\cap\mathbb{R}=\mathbb{Q}(a)$. Le corps $K(a)$ est une extension stricte de $\mathbb{Q}(a)$ (l'un est réel, l'autre pas). Donc le degré de $K(a)$ sur $\mathbb{Q}$ est un multiple strict de h. Puisque $K(a)\subseteq L$, on a forcément $K(a)=L$. Ceci démontre le deuxième point.

• Le degré de a sur K est h, donc son degré sur $\mathbb{Q}$ est $\geqslant h$. Mais $\mathbb{Q}(a)\subseteq L\cap\mathbb{R}$, donc $\mathbb{Q}(a)=L\cap\mathbb{R}$. En conséquence, f est aussi le polynôme minimal de a sur K.

Supposons que p soit totalement décomposé dans L. Alors il est décomposé $p=\mathfrak{p}\bar{\mathfrak{p}}$ dans K et $\mathfrak{p}$ est totalement décomposé dans L. Il résulte de 2.1 que f est complètement scindé dans $\mathcal{O}_K/\mathfrak{p}$. Mais puisque l'idéal $\mathfrak{p}$ est de degré résiduel 1, on a $\mathcal{O}_K/\mathfrak{p}\simeq\mathbb{Z}/p\mathbb{Z}$. Ainsi le polynôme f admet des racines modulo p (en fait, il en admet h).

Inversement, supposons que $p=\mathfrak{p}\bar{\mathfrak{p}}$ soit décomposé dans K et que f admette une racine modulo p. Alors f admet une racine dans $\mathcal{O}_K/\mathfrak{p}\simeq\mathbb{Z}/p\mathbb{Z}$, donc $\mathfrak{p}L$ admet un facteur de degré 1. Puisque l'extension $L:K$ est galoisienne, on en déduit que $\mathfrak{p}L$ est totalement décomposé dans L. Il en est de même de $\bar{\mathfrak{p}}L$ et donc de pL. L'équivalence du troisième point est montrée. □

Le cas $D=-39$

2.7. — Proposition. *Soit $K=\mathbb{Q}(\sqrt{-39})$. Le corps L des classes de Hilbert de K est $K(\sqrt{7+2\sqrt{13}})$.*

Démonstration — Soit $a=\sqrt{7+2\sqrt{13}}$. Montrons d'abord que a^2 n'est pas un carré dans $K(\sqrt{13})=\mathbb{Q}(\sqrt{13},\sqrt{-3})$. En effet, on aurait alors

$$7+2\sqrt{13}=(\alpha+\sqrt{-3}\beta)^2\qquad\alpha,\beta\in\mathbb{Q}(\sqrt{13})$$

et donc $\alpha^2-3\beta^2=7+2\sqrt{13}$ et $\alpha\beta=0$. Mais alors

$$7+2\sqrt{13}=(\gamma+\sqrt{13}\delta)^2\qquad\text{ou}\qquad 7+2\sqrt{13}=-3(\gamma+\sqrt{13}\delta)^2\qquad\text{avec }\gamma,\delta\in\mathbb{Q}.$$

Mais ces équations n'ont pas de solution. Donc, a est un entier algébrique de degré 4 sur K et son polynôme minimal est $f=X^4-14X^2-3$. Posons $a'=\sqrt{7-2\sqrt{13}}$. On a $aa'=\sqrt{-3}\in K(a)$ car $\sqrt{13}=(a^2-7)/2\in K(a)$. On voit donc que les quatres conjugués $\pm a,\pm a'$ de a sont dans L, et donc que l'extension $L:K$ est galoisienne. Puisque cette extension est de degré 4 (donc abélienne) il ne reste plus qu'à montrer qu'elle est non ramifiée.

Pour cela, considérons le corps intermédiaire $K_1=K(\sqrt{-3})=K(\sqrt{13})$. Les premiers de K ne divisant pas $\mathrm{disc}(X^2-13)=56$ ne sont pas ramifiés dans K_1. De même, puisque K_1 est engendré sur K par $(-1+\sqrt{-3})/2$, dont le polynôme minimal X^2+X+1 est de discriminant -3, les premiers de K ne divisant pas 3 ne sont pas ramifiés dans K_1. Puisque 3 et 56, sont premiers entre eux, on a montré que l'extension $K_1:K$ est non ramifiée.

Il reste à montrer que l'extension $L:K_1$ est non ramifiée. Les polynômes minimaux de a et a' sur K_1 ont pour idéaux discriminants $4(7\pm2\sqrt{13})$. Si $\mathfrak{p}$ est un premier de K_1 ramifié dans L alors il divise ces deux discriminants, donc leur somme et leur différence. Ainsi $\mathfrak{p}\mid 8\cdot 7$ et $\mathfrak{p}\mid 16\sqrt{13}\mid 16\cdot 13$. Puisque 7 et 13 sont premiers entre eux, on a $\mathfrak{p}\mid 2$. Enfin, on peut vérifier que $(a+1)/2$ est un entier de L et que son polynôme minimal sur K_1 est $X^2-X-(a^2-1)/4$, d'idéal discriminant (a^2) étranger à 2. □

2.8. — Proposition. *Soit p un premier distinct de 2, 3, 13. Alors*

$$p=x^2+xy+10y^2\quad\Longleftrightarrow\quad\begin{cases}p\ mod\ 39\in\{1,4,10,16,22,25\}\\ X^4-14X^2-3=0\quad a\ une\ solution\ modulo\ p.\end{cases}$$

$$p=3x^2+3xy+4y^2\quad\Longleftrightarrow\quad\begin{cases}p\ mod\ 39\in\{1,4,10,16,22,25\}\\ X^4-14X^2-3=0\quad n'a\ pas\ de\ solution\ modulo\ p.\end{cases}$$

DÉMONSTRATION — Nous avons vu (problème 1.11) que les formes q_0 et q_2 constituent le genre principal des formes quadratiques de discriminant -39 et qu'un nombre premier p est représenté par l'une de ces deux formes si et seulement si il vérifie les congruences indiquées. Nous avons vu aussi que ces conditions impliquent $(-39/p) = 1$ et donc que p est décomposé dans $K = \mathbb{Q}(\sqrt{-39})$. Enfin, le réel $\sqrt{7+2\sqrt{13}}$ engendre le corps de classes L sur K et il admet f pour polynôme minimal. Le résultat est alors conséquence de 2.5 et de 2.6 puisque les nombres premiers distincts de 2, 3 et 13 ne divisent ni le discriminant $-2^{12}\cdot 3\cdot 13^2$ de f ni D. □

Exemples

En conclusion, voici quelques exemples de représentations de nombres premiers p (tels que $(-39/p) = 1$) et la factorisation de f modulo p correspondante.

p décomposé	factorisation de f modulo p
$5 = q_1(0,1)$	$X^4 - 14X^2 - 3$
$11 = q_1(-2,5)$	$X^4 - 14X^2 - 3$
$41 = q_1(4,1)$	$X^4 - 14X^2 - 3$
$43 = q_0(1,2)$	$(X-2)(X-15)(X-28)(X-41)$
$47 = q_1(-2,3)$	$X^4 - 14X^2 - 3$
$59 = q_1(2,3)$	$X^4 - 14X^2 - 3$
$61 = q_2(3,2)$	$(X^2-35)(X^2-40)$
$71 = q_1(6,-1)$	$X^4 - 14X^2 - 3$
$79 = q_2(5,-4)$	$(X^2-69)(X^2-24)$
$83 = q_1(6,1)$	$X^4 - 14X^2 - 3$
$89 = q_1(4,3)$	$X^4 - 14X^2 - 3$
$103 = q_0(9,-2)$	$(X-20)(X-51)(X-52)(X-83)$
$127 = q_2(7,-4)$	$(X^2-75)(X^2-66)$
$137 = q_1(-4,5)$	$X^4 - 14X^2 - 3$
$139 = q_0(9,2)$	$(X-8)(X-28)(X-111)(X-131)$
$149 = q_1(8,-3)$	$X^4 - 14X^2 - 3$

Au moins deux questions se posent encore si l'on veut être capable de traiter explicitement le cas de chaque discriminant :

• Existe-t-il une méthode générale permettant de calculer le corps des classes de Hilbert de n'importe quel corps quadratique (et plus généralement le corps de classes de rayon de n'importe quel anneau quadratique) ?

• Existe-t-il des critères généraux pour "séparer" deux formes quadratiques de même genre ? Nous avons seulement montré jusqu'ici comment faire lorsque l'une d'elle est proprement équivalente à la forme principale.

Ces deux questions admettent une réponse positive. La première fait l'objet de la dernière partie de [1] et fait appel à la théorie des formes modulaires. La deuxième est plus abordable et contenue dans [2].

3. Bibliographie

[1] D.A. COX : *Primes of the Form $x^2 + ny^2$.* Wiley-Interscience, John Wiley & Sons, 1989.

[2] S. GURAK : *On the representation theory for full decomposable forms.* Journal of Number Theory, vol. 13, 1981, pp. 421–442.