Contents

Quadratic fields

24 aout 2023

Le but est de pouvoir lire grosso modo ça pour ça. Je suis le traitement de Cox.

1 Bases

Une extension quadratique de $\mathbb{Q}$ est tjr de la forme :

- $\mathbb{Q}(\sqrt{n})$, n sans facteurs carrés. (Facile)
- Ensuite le discriminant usuel $D_{K/\mathbb{Q}} = \mathrm{Det}(\mathrm{Tr}(x_i x_j))$: Si $n \equiv 1 \ mod\ 4$ alors $D = D_{K/\mathbb{Q}} = n$ si $n \equiv 2, 3 \ mod\ 4$ alors $D = -4n$. (Penser à $X^2 - X + (1-n)/4$)
- Aussi $\frac{1+\sqrt{n}}{2}$ engendre $\mathcal{O}_K$ dans le premier cas $\sqrt{n}$ dans le second.
- La ramification est simple aussi, avec le lemme chinois on prédit :
  $\left(\frac{d_K}{p}\right) = -1,\ 0,\ 1$ donne p inerte, p ramifié, p split.

2 Formes quadratiques binaires

2.1 Binary quadratic forms

Bon là c'est plus pour moi, je note des défs pour avoir des trucs à écrire et travailler dessus. On regarde des formes quadratiques entières en deux variables, $f(x,y) = ax^2 + bxy + cy^2$, a b et c $\in \mathbb{Z}$.

Definitions :

- f est primitive si les coeffs sont premiers entre eux.

- f représente un entier m si $\exists\ x, y \in \mathbb{Z}$ tq $f(x, y) = m$
- f représente proprement m si x, y sont premiers entre eux.
- f et g sont équivalentes si il existe un $M = \begin{pmatrix} p & r \\ q & s \end{pmatrix} \in GL_2(\mathbb{Z})$ tq $f = g \circ M$.
- L'equivalence est propre si $\mathrm{Det}(M) = 1$ impropre sinon.
- à noter : si $ps - qr = 1$, alors $f(px + qy,\ rx + sy) = f(p, r)x^2 + (2apq + bps + brq + 2crs) + f(q, s)y^2$.
- ducoup f représente proprement m ssi f est proprement eq à $mx^2 + Bxy + Cy^2$.

La plupart des notions sont invariantes par équivalences. En particulier, le fait d'être primitive, positive et définie. (fait le c'est simple)

2.1.1 Discriminant

On note $D = b^2 - 4ac$ le discriminant de f. En particulier, $x^2 + ny^2$ a discriminant $-4n$.

Représentants et discriminants :

- $D_f = \mathrm{Det}(M)^2 D_{f \circ M}$. D'où deux formes **équivalentes** ont même **discriminant**.
- $D_f \equiv 0, 1\ mod\ 4$ car $D_f \equiv b^2\ mod\ 4$.
- $4af(x, y) = (2ax + by)^2 - D_f y^2$ d'où f est **définie** si $D_f < 0$ **indéfinie** sinon.
- Si m est impair premier à $D \equiv 0, 1\ mod\ 4$ alors il existe f **primitive** qui représente **proprement** m ssi $\left(\frac{D}{m}\right) = 1$. ($m$ impair comme ça on peut supp $D \equiv b^2\ mod\ 4$)
- En particulier $\left(\frac{-n}{p}\right) = 1$ ssi p est représentée par une **forme primitive** de $D = -4n$. ($\left(\frac{-n}{p}\right) = \left(\frac{-4n}{p}\right)$)

Pour résumer, si par exemple on cherche à représenter p via $x^2 + ny^2$ alors on doit avoir $\left(\frac{-n}{p}\right) = 1$. Par contre $\left(\frac{-n}{p}\right) = 1$ a une solution ne précise pas la forme de discriminant $-4n$ qui représente p. Il faut donc déterminer des représentants des classes d'équivalences.

2.1.2 Reduced form

On se ramène au cas des formes **définies positives**($-D_f,\ a \geq 0$). (cas de x^2+ny^2) Une forme f est réduite si $|b| \leq a \leq c$ et $b \geq 0$ si $|b| = a$ ou $a = c$.

Premiere réduction :

- Toute forme **primitive**, **définie**, **positive** est **proprement équivalente** à une forme **réduite**.

A noter de la preuve [p.25, Cox],

Step 1 On prend b minimale dans la classe d'équivalence propre, alors $\mid b \mid \leq a, c$.

Step 2 Une telle forme est proprement équivalente à une forme réduite.

Step 3 L'étape de l'unicité est intéressante : Cas général, $\mid b \mid < a < c$ alors

$$f(x,y) \geq (a- \mid b \mid +c)\min(x^2,y^2)$$

d'ou en regardant les valeurs de x, y on remarque que a est la valeur minimale non nulle de f, c la suivante et $(a- \mid b \mid +c)$ la suivante ! L'**unicité** en découle.

En particulier avoir les formes réduites c'est avoir les 3 valeurs minimales de toutes les formes de la classe. Enfin : Si f est réduite alors : $-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$ d'où

$$a \leq \sqrt{-D/3}$$

D'où un nombre fini de a possible pour une forme réduite de discriminant D.

Nombre de classes Comme $\mid b \mid \leq a$ et $D = b^2 - 4ac$ on a un nombre fini de formes réduites possible de discriminant D. Et on note $h(D)$ le nombre de classe d'équivalences propre de discriminant D.

On a donc :

Première réduction $\left(\frac{-n}{p}\right) = 1$ ssi p est representé par une des $h(-4n)$ formes réduites.

Dû au fait que $\left(\frac{-n}{p}\right) = \left(\frac{-4n}{p}\right)$ et la dernière remarque de la dernière section.

Généralisation Si χ est le caractère quadratique de $(\mathbb{Z}/D\mathbb{Z})^\times$ alors pour $p \neq D$, $[p] \in ker(\chi)$ ssi p est representé par une des $h(D)$ formes réduites de discriminant D.

Le point est que cette fois, on regarde que la classe de p mod D. Les théorèmes sont surpuissants là, par exemple on peut résoudre le problème pour $n = 2, 3, 7$ facile. Parce qu'en fait :

- $x^2 + y^2$ est la seule forme réduite de discriminant -4. ($\sqrt{4/3} < 2$)
- $x^2 + 2y^2$ est la seule forme réduite de discriminant -8. ($\sqrt{8/3} < 2$)
- x^2+3y^2 est la seule forme réduite de discriminant -12. ($\sqrt{4} = 2 > a$) ($\mid b \mid < a$)
- $x^2 + 7y^2$ est la seule forme réduite de discriminant -28. ($\sqrt{28/3} \approx 3 > a$) (On vérifie directement que $a = 2$ n'est pas poss.)

D'où via le théorème :

Via ker$(\chi_4) \cap \{\overline{p} \mid p \neq 4, \ \left(\frac{4}{p}\right) = 1\} = \{1\}$ **:** On a, $p = x^2 + y^2 \leftrightarrow p \equiv 1 \ mod \ 4$.

Via ker$(\chi_8) \cap \{\overline{p} \mid p \neq 8, \ \left(\frac{8}{p}\right) = 1\} = \{1, 3\}$ **:** On a, $p = x^2+y^2 \leftrightarrow p \equiv 1, 3 \ mod \ 8$.

Via ker$(\chi_{12}) \cap \{\overline{p} \mid p \neq 12, \ \left(\frac{12}{p}\right) = 1\} = \{1, 7\}$ **:** Dans cette étape comme 2 est un facteur d'exposant pair, on peut réduire à $1 \ mod \ 3$ ou $p = 3$. On a,

$$p = x^2 + 3y^2 \leftrightarrow p \equiv 1 \ mod \ 3$$

Via ker$(\chi_{28}) \cap \{\overline{p} \mid p \neq 28, \ \left(\frac{24}{p}\right) = 1\} = \{1, 9, 11, 15, 23, 25\}$ **:**

$$p = x^2 + 7y^2 \leftrightarrow p \equiv 1, 9, 11, 15, 23, 25 \ mod \ 28$$

.

L'idée marche quand y'a qu'une seule forme réduite mais c'est que rarement le cas. En fait :

- (Landau) $h(-4n) = 1$ ssi $1, 2, 3, 4, 7$.

2.2 elementary genus theory

Seconde réduction : Ducoup pour l'instant ker(χ) est l'ensemble des premiers représentés par UNE des classes de disc D. Maintenant on réduit à des un sous groupe, i.e. on a des formes qui représentent des coset d'un sous groupe.

Forme principale, $D \equiv 0 \ mod \ 4$ Def comme $x^2 - \frac{D}{4}y^2$.

Forme principale, $D \equiv 1 \ mod \ 4$ Def comme $x^2 + xy + \frac{1-D}{4}y^2$.

Maintenant la réduction.

Déjà, Les valeurs dans $\mathbb{Z}/D\mathbb{Z}$ représentées par la forme principale forment un sous groupe $H \leq$ker(χ)!

En plus, Toute forme de discriminant D représentent un élément de ker(χ)$/H$.

La preuve de la premiere partie est assez simple :

Premiere assertion : $(x^2 + ny^2)(z^2 + nw^2) = (xz \pm nyw)^2 + n(xw \pm yz)^2$ montre la stabilité dans le premier cas ($D = -4n$), et de $4(x^2 + xy + \frac{1-D}{4}y^2) \equiv (2x + y)^2 \ mod \ D$ On déduit le second.

Seconde assertion : Pour montrer que les valeurs représentées sont dans un coset c'est malin : y suffit de l'existence d'une valeur representée proprement première à D. Disons a. Alors déjà on peut supposer que $f(x, y) = ax^2 + bxy + cy^2$ on est passé d'une valeur au cas général ! mtn faut se ramener à la forme principale : On a dans le cas $D = -4n$: $af(x, y) = (ax + b/2y)^2 + ny^2$ (b est pair). D'où les valeurs sont dans $a^{-1}H$. Le fait que toute les valeurs soient représentées c'est : Si $ac \in H$ alors $ac = z^2 + nw^2 \ mod \ D$ et via l'équation précédente on résout $f(x, y) \equiv c \ mod \ D$.

Le corollaire intéressant pour la forme principale c'est que :

- ($D = -4n$) Si p est représenté par une forme du genre principal alors la forme principale représente un entier congru à p mod D. D'où p est représenté par une forme de genre principal ssi il existe β t.q

$$p \equiv \beta^2, \beta^2 + n \ mod \ 4n$$

En particulier, si le genre principal est formé d'une seule classe on peut résoudre directement $p = x^2 + ny^2$. C'est le cas pour : $n = 5, 6, 10, 13, 15, 21, 22, 30$ par exemple. (Exo : résoudre le problème.)

Deux continuation : on peut déterminer des infos sur le groupe, on peut chercher à représenter des produits de premier. C'est vraiment joli, c'est la suite.

2.3 Genus theory

L'idée va être de généraliser et simplifier ce genre d'équivalence : (il existe une "composition")

- $(2x^2 + 2xy + 3y^2)(2z^2 + 2zw + 3w^2) = (2xz + xw + yz + 3yw)^2 + 5(xw - yz)^2$
- Si et seulement si il existe p tel que $(2x^2 + 2xy + 3y^2)$ représente p. Il existe q tel que $(2z^2 + 2zw + 3w^2)$ représente q et $x^2 + 5y^2$ représente pq.

Pour $D < 0$ un discriminant. On appelle $C(D)$ l'ensemble des classes de formes de discriminant D modulo équivalence **propre**. On écrit aussi $f(x, y) = ax^2 + bxy + cy^2$ et $g(x, y) = a'x^2 + b'xy + c'y^2$.

2.3.1 Dirichlet composition, class group

Construction de la composition : grosso modo ce sera une opération qui donnera une structure de groupes a $C(D)$. On cherche donc une manière de "composer" systématiquement deux formes primitives de discriminant D pour en obtenir une nouvelle. De la forme $f(x, y)g(z, w) = F(B_1(x, y, z, w), B_2(x, y, z, w))$ où B_1, B_2 sont des formes bilinéaires.
Bon déjà un petit rappel sur l'équivalence **propre** : (qui permet aussi d'expiquer l'algo de réduction)

Diviser b par $2a/2c$: $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \leftrightarrow \ (x + ky,\ y)$ et donne $a,\ b + 2ak,\ f(1, k)$. D'où on peut réduire b par la division euclidienne de b par $2a$. $\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}$ Pour diviser par c.

Echanger a et c : $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ a pour déterminant -1 donc l'équivalence est pas propre. A la place on utilise $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ qui donne $c,\ -b,\ a$. En particulier, $cx^2 + bxy + ay^2$ est proprement équivalente à $ax^2 - bxy + cy^2$.

Combinaison des deux $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & k \end{pmatrix}$ et cette matrice donne c, $-(b+2kc)$, $f(-1, k)$. Au lieu de k on met $sgn(c)k$ on écrit $-b = 2|c|k + r$ avec $|c| \leq r < |c|$. Ce qui donne l'algorithme de réduction. ($|-b - 2k|c|| \leq c$, si le nouveau c est plus grand que le nouveau a on a fini, sinon on recommence.)

Maintenant il convient de chercher

- $B \equiv b \ mod \ 2a$ et $B \equiv b' \ mod \ 2a'$

de sorte qu'on peut prendre $f(x,y) = ax^2 + Bxy + aCy^2$ et $g(x,y) = a'x^2 + Bxy + a'Cy^2$. (Ecrire $B^2 - 4aC = D$ et $B^2 - 4a'C' = D$, de sorte que $a'C' = aC$ et on peut écrire la forme donnée.) En écrivant $f(x,y)g(x,y)$ on trouve une forme $F(x,y) = aa'x^2 + Bxy + Cy^2$ le problème c'est que le C là est pas forcément entier. D'où y faut rajouter

- $B^2 \equiv D \ mod \ 4aa'$.

. Résoudre la dernière necessite des hypothèses sur f, g. On doit ajouter

- $pgcd(a, a', \frac{b+b'}{2}) = 1$, car la dernière congruence, avec les deux premières équivaut à :
$$\frac{b+b'}{2}B \equiv \frac{bb'+D}{2} \ mod \ 2aa'$$

Les trois congruences sont résolues p.43-44 du Cox.

Composition de Dirichlet : La forme obtenue est **primitive**, **définie**, **positive** de discriminant D.

L'interêt est que dans chaque deux classes il existe toujours deux formes vérifiant les hypothèses pour obtenir une composition. On obtient

C(D) est un groupe abélien avec la composition de Dirichlet.
On a :

- L'inverse de $ax^2 + bxy + cy^2$ est $ax^2 - bxy + cy^2$. (C'est là qu'on utilise $ax^2 - bxy + cy^2 \leftrightarrow cx^2 + bxy + ay^2$ qui permet de composer les deux.)
- La classe principale est l'élément neutre. (Ca revient à H est un sous-groupe de $(\mathbb{Z}/D\mathbb{Z})^\times$. Mais la preuve est simple et directe avec Dirichlet.)

2.3.2 Elements of order 2 of the class group

On va chercher la structure du groupe de classe. On commence par les élements d'ordre ≤ 2 qui sont en fait cruciaux.

Une condition n et s pour être d'ordre 2 **:** $b = 0$, $a = b$ ou $a = c$. (C'est clair $f = -f$ veut dire qu'elles sont proprement équiv, prendre f réduite.)

Une conséquence : en notant,

- r le nb de divisieurs premiers de D.
- Si $D \equiv 1 \ mod \ 4$, $\mu = r$.
- Si $D \equiv 0 \ mod \ 4$,

$$\begin{aligned} n \equiv 3 \ mod \ 4,\ \mu = r \\ n \equiv 1, 2 \ mod \ 4,\ \mu = r + 1 \\ n \equiv 4 \ mod \ 8,\ \mu = r + 1 \\ n \equiv 0 \ mod \ 4,\ \mu = r + 2 \end{aligned}$$

On a :

Nombre d'élements d'ordre 2 **:** $C(D)$ a exactement $2^{\mu-1}$ éléments d'ordre ≤ 2 !

L'idée est d'utiliser la caractérisation des éléments d'ordre ≤ 2 et de compter le nombre de formes réduites de ce type. (p.47 du Cox)

Par exemple pour $D \equiv 0 \ mod \ 4$, $n \equiv 1 \ mod \ 4$, $b = 0$. On a $n = ac$ et $2 \neq n$ et $pgcd(a, c) = 1$ avec $a < c$ pour être réduite. Alors on a 2^{r-1} choix pour a. (le produit des puissances max de $p_i \mid n$)

On regarde maintenant le lien entre les élements d'ordre 2 et le groupe de classes.

2.3.3 The form class group

On considère

$$\begin{aligned}\Phi\ :\ C(D) &\to \ker(\chi)/H\\ \overline{f} &\mapsto \text{Une valeur représentée}\end{aligned}$$

Chaque fibre $\Phi^{-1}(aH)$ est l'ensemble des classes d'un genre (genus) donné, ici a. Pour l'instant on est pas sûrs de la surjectivité, mais l'image de Φ est identifiée à l'ensemble des genres (genera) possibles.

- Φ est un morphisme de groupe ! (Par construction)

Un corollaire :

Fibres : Chaque genre consiste en le même nombre de classes ! (morphisme de groupe)

Nombre de genres : Le nombre de genre de formes de discriminant D est une puissance de 2.

Le second point vient du fait que H contient les carrés ! D'où $(\ker(\chi)/H)^2 = \{H\}$ et $|\ker(\chi)/H| = 2^k$. En fait on a un résultat bien plus précis, on redéfini :

- r le nb de divisieurs premiers de D.
- Si $D \equiv 1\ mod\ 4$, $\mu = r$.
- Si $D \equiv 0\ mod\ 4$,

$$\begin{aligned}n \equiv 3\ mod\ 4,\ \mu &= r\\ n \equiv 1, 2\ mod\ 4,\ \mu &= r + 1\\ n \equiv 4\ mod\ 8,\ \mu &= r + 1\\ n \equiv 0\ mod\ 4,\ \mu &= r + 2\end{aligned}$$

Et on a alors :

Cardinal de $ker(\chi)/H$: On a $|ker(\chi)/H| = 2^{\mu-1}$.

Pour le prouver, on construit un morphisme de $(\mathbb{Z}/D\mathbb{Z})^{\times}$ dans $\{\pm 1\}^k$ surjectif et de kernel H. (le k sera μ)

$ker(\chi)$ étant d'indice 2 on aura fini. Le morphisme s'écrit en décomposant $(\mathbb{Z}/D\mathbb{Z})^{\times}$ via le lemme chinois. On écrit :

$$\Psi \ : \ (\mathbb{Z}/D\mathbb{Z})^{\times} \simeq \prod_i \mathbb{Z}/p_i^{k_i}\mathbb{Z} \times \mathbb{Z}/2^{k+2}\mathbb{Z} \longrightarrow \{\pm 1\}^{\mu} \qquad (*)$$

ou chaque $\mathbb{Z}/p_i^{k_i}\mathbb{Z}$ est envoyé via $\left(\frac{\cdot}{p_i}\right)$. ($p_i$ impair)
La difficulté vient du 2. Si $D \equiv 1 \ mod\ 4$ c'est facile de montrer la surjectivité pour $k = \mu = r$, la forme principale a pour image l'ensemble des carrés mod D. Sinon y'a pleins de cas à séparer pour $n \equiv i \ mod\ 8$. Et on envoie $a \ mod\ D$ via $\left(\frac{2}{\cdot}\right)$ et $\left(\frac{-1}{\cdot}\right)$ ou leur produit. L'idée est que les éléments de H s'écrivent $\beta^2, \beta^2 + n \ mod\ D$ et il faut utiliser judicieusement les deux morphismes plus haut pour gérer les différents cas.

Théorème 2.3.4. *On considère le morphisme*

$$\begin{aligned} \Phi \ : \ C(D) &\longrightarrow ker(\chi)/H \\ f(x,y) &\mapsto \textit{coset representé} \end{aligned}$$

Alors :

(i) Φ *est surjectif.*

(ii) $ker(\Phi) = C(D)^2$, *autrement dit* $C(D)/C(D)^2 \cong ker(\chi)/H \cong \{\pm 1\}^{\mu-1}$, *d'ou en particulier il y'a* $2^{\mu-1}$ *genres et les formes de genres principales sont toutes des carrés.*

Preuve : On prouve (i) simplement avec Dirichlet. On prouve (ii) à l'aide de la suite exacte :

$$0 \to C(D)_2 \to C(D) \to C(D)^2 \to 0$$

ou $C(D)_2$ désigne les éléments d'ordre 2, que $C(D)/C(D)^2 \simeq C(D)_2$ qui a pour cardinal $2^{\mu-1}$. Comme Φ est surjective et $C(D)/C(D)^2 \approx ker(\chi)/H$ comme on vient de le voir on obtient :

$$C(D)/C(D)^2 \simeq ker(\chi)/H$$

. □

A noter, on a écrit un morphisme $\Phi : (\mathbb{Z}/D\mathbb{Z})^{\times} \to \{\pm 1\}^{\mu}$ de ker H. D'où chaque classe d'un même genre est envoyée sur un meme élément de $\{\pm 1\}^{\mu}$ ce qui permet de déterminer rapidement le genre d'une classe.

Ce qui conclut l'étude basique du groupe de classe !

2.3.5 Convenient numbers

Quelques résultats interessants de Euler/Gauss sur les discriminants ou chaque genre est constitué d'une unique classe :

Nombre convénient : n est dit convénient si pour tout m impair premier à n, $m = x^2 + ny^2$ (proprement) n'a qu'une solution avec $x, y \geq 0$ alors m est premier.

Equivalence due à Gauss : n est convénient si et seulement $h(-4n) = 2^{\mu-1}$ ou autrement dit, chaque genre de $C(-4n)$ consiste qu'en une classe.

La preuve de l'équivalence se base sur le nombre de représentations d'un nombre p.55 du Cox.

Schema à faire sur les morphismes/interdépendances

3 Ordres

On définit les ordres de plusieurs manières : Un ordre $\mathcal{O} \subset K$ d'un corps quadratique est :

(i) Un sous anneau de K

(ii) Un sous $\mathbb{Z}$-module de type fini contenant une $\mathbb{Q}$-base de K.

Comme $\mathcal{O}$ est sans torsion, (ii) revient à être un $\mathbb{Z}$-module libre de rang 2.

- $\mathcal{O}_K$ est un ordre maximal. Et on a $\mathcal{O}_K = [1, w_K]$ avec $w_K = \frac{d_K + \sqrt{d_K}}{2}$.
- $[\mathcal{O}_K : \mathcal{O}] = f$ est fini et $\mathcal{O} = [1, f w_K]$. (même index et inclus trivialement l'un dans l'autre)
- On note f le conducteur de $\mathcal{O}$.

Avec la formule usuelle du discriminant on obtient :

- $D_{\mathcal{O}} = f^2 d_K$.

On obtient que chaque discriminant correspond de manière unique à un ordre.

3.1 Idéaux et Groupe de classe d'un ordre

Si $\mathfrak{a} \leq \mathcal{O}$ est un idéal alors :(On peut prendre $\mathfrak{b}$ fractionnaire aussi.)

- $N(\mathfrak{a}) := |\mathcal{O}/\mathfrak{a}|$ est fini.
- $\mathcal{O}$ est noethérien et de dimension 1 mais clairement pas intégralement clos dès que $f > 1$. D'ou en particulier on a pas de décomposition unique en idéaux premiers.

En fait la décomposition existe pour un sous-ensemble d'idéaux un peu plus petit que les suivants.

Idéaux propres : $\mathfrak{a}$ est propre ssi $\{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}$. (En général on peut avoir $= \mathcal{O}_K$)

En fait, on pourra former un groupe de classe grâce à au fait que

- Les idéaux propres sont exactement les idéaux inversibles.
- $\Longrightarrow$ se montre en remarquant que sachant $dim_{\mathbb{Z}}\mathfrak{a} = 2$, $\mathfrak{a} = [\alpha, \beta] = \alpha[1, \tau]$ ($\mu_\tau = ax^2+bx+c$), alors $\mathcal{O} = [1, a\tau]$. ($[1, \tau]$ est propre pour $[1, a\tau]$) En notant τ' le conjugué de τ et $\mathfrak{a}' = \alpha'[1, \tau']$. On a enfin $a\mathfrak{a}\mathfrak{a}' = a\alpha\alpha'[1, \tau][1, \tau'] = N(\alpha)\mathcal{O}$.

Groupe de classe : On note $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ le groupe de classe formé par les idéaux propres.

3.2 Liens avec les formes quadratiques binaires

En fait y'a une correspondance, même un isomorphismes entre les groupes de classes. On parlera tjr de l'ordre $\mathcal{O}$ de discriminant D.

La relation : Une forme primitive définie positive de discriminant D fait naître un idéal propre de $\mathcal{O}$, $[a, (-b+\sqrt{D})/2]$.

L'isomorphisme :

$$\begin{aligned}\theta \ : \ C(D) &\to C(\mathcal{O}) \\ f(x,y) &\mapsto [a, (-b+\sqrt{D})/2]\end{aligned}$$

Représentation/norme : Un entier positif m est représenté par une forme f ssi m est une norme de la classe de l'idéal correspondant dans $C(\mathcal{O})$.

En particulier, $h(D) = h(\mathcal{O})$.

3.2.1 Preuves

On note $\mathcal{O}$ l'ordre de discriminant D.

- **La relation**, on a

$$\begin{aligned}[a, (-b+\sqrt{D})/2][a, (-b-\sqrt{D})/2] =& [a^2, a(-b+\sqrt{D})/2, -ab, ac] \\ =& a[a, a(-b+f\sqrt{d_K})/2a, -b, c] \\ =& a[1, fw_K]\end{aligned}$$

En remarquant que $-b$ et fd_K ont la même parité. D'ou $\theta(f(x,y) = ax^2+bxy+cy^)$ est propre car inversible.

- **L'isomorphisme**, qu'on prouve en deux parties. D'abord la bijection puis l'isomorphisme.

- Pour **l'injectivité** de θ, avec τ, τ' tq $f(\tau, 1) = g(\tau') = 0$. On a

$$\begin{aligned}f \sim g \leftrightarrow \tau' = \frac{p\tau+q}{r\tau+s}, &\quad \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z}) \\ \leftrightarrow [1,\tau] = \lambda[1,\tau'], &\quad \lambda \in K\end{aligned}$$

En particulier $\theta(f) = \theta(g) \implies f = g$. La surjectivité se montre facilement.
On a pour l'instant

$$C(D) \approx C(\mathcal{O})$$