Primes - Handout 2

Quadratic forms and quadratic number fields (NON-EXAMINABLE)

For simplicity, we will restrict to *fundamental discriminants*, those which occur as the discriminant Δ_K of some quadratic number field $K = \mathbb{Q}(\sqrt{d})$. But this correspondence can be generalised to orders $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_K$ inside the field $K = \mathbb{Q}(\sqrt{d})$.

For the case of $\mathcal{O}_K$, see Section VII.2 in [FT93]. For the more general case, see Section 5.2 in [Coh13].

1.1. Narrow idea class group of a quadratic number field

A quadratic number field K is

$$\mathbb{Q}(\sqrt{d}) := \left\{ a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Q} \right\}.$$

The ring of integers $\mathcal{O}_K \subset K$ consists of all elements of K which satisfy a *monic* polynomial over $\mathbb{Q}$. We can assume d is square-free, then we have

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{ x + y\frac{1+\sqrt{d}}{2} \;\middle|\; x, y \in \mathbb{Z} \right\} & \text{if } d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}] = \left\{ x + y\sqrt{d} \;\middle|\; x, y \in \mathbb{Z} \right\} & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

The *norm* of $a+b\sqrt{d} \in K$ is defined by $N(a+b\sqrt{d}) := (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2$, so

$$N(x + y\tfrac{1+\sqrt{d}}{2}) = x^2 + xy - dy^2$$
$$N(x + y\sqrt{d}) = x^2 - dy^2.$$

Consider the set $\mathcal{I}(K)$ of all non-zero *fractional ideals* $\lambda\mathfrak{a}$ of $\mathcal{O}_K$, where $\lambda \in K^*$ and $\mathfrak{a} \subset \mathcal{O}_K$ is an ideal.

An element λ of K is *totally positive*, if $\sigma(\lambda) > 0$ for every real embedding $\sigma\colon K \to \mathbb{R}$. For $d < 0$, there are no real embeddings, so every element of K is totally positive. For $d > 0$, we require $a + b\sqrt{d}, a - b\sqrt{d} > 0$ for $\lambda = a + b\sqrt{d}$ to be totally positive.

Write $\mathcal{P}^+(K)$ for the set of all *totally positive* principal fractional ideals (λ) where λ is totally positive.

Definition 1 (Narrow ideal class group)**.** The *narrow ideal class group* of K is

$$\mathcal{C}^+(K) = \mathcal{I}(K)/\mathcal{P}^+(K),$$

and the (usual) *ideal class group* of K is

$$\mathcal{C}(K) = \mathcal{I}(K)/\mathcal{P}(K)\,.$$

Theorem 2. *If $d < 0$, so K is imaginary-quadratic, then $\mathcal{C}^+(K) = \mathcal{C}(K)$. If $d > 0$, so K is real-quadratic, then $\mathcal{C}^+(K) \supset \mathcal{C}(K)$. Equality holds if and only if there is a unit $u = x + y\sqrt{d}$, or if appropraite $u = x + y\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ with norm -1. Otherwise $\mathcal{C}^+(K)/\mathcal{C}(K) = \mathbb{Z}/2\mathbb{Z}$.*

Proof. If there is a unit with negative norm then $N(u) = \sigma_1(u)\sigma_2(u) = -1$, so without loss of generality $\sigma_1(u) < 0$ and $\sigma_2(u) > 0$, for the two embeddings $\sigma_i\colon K \to \mathbb{R}$. We can then take any principal ideal $(\lambda) = (u\lambda)$, and see one of λ and $u\lambda$ is totally positive. This shows $\mathcal{P}^+(K) = \mathcal{P}(K)$.

The converse follows by considering, say $(\sqrt{d})$, and finding a generator $u\sqrt{d}$ which is totally positive, whence $N(u) = -1$.

If no unit has negative norm, then $\mathcal{P}(K) = \mathcal{P}^+(K) \cup \sqrt{d}\mathcal{P}^+(K)$, which shows $\mathcal{C}^+(K)/\mathcal{C}(K) = \mathbb{Z}/2\mathbb{Z}$. $\square$

1.2. Correspondence between narrow ideal classes and quadratic forms

Now we construct a map from narrow ideal classes in $\mathcal{C}(K)$, to proper equivalence classes of binary quadratic forms of discriminant Δ_K.

Every non-zero (fractional) ideal $\mathfrak{a}$ has a $\mathbb{Z}$-basis of the form $\{\, \alpha_1, \alpha_2 \,\}$. Using this the *norm* of the ideal can be calculated as

$$N(\mathfrak{a}) \coloneqq \#(\mathcal{O}_K/\mathfrak{a}) = \left| \frac{1}{\Delta_K} \det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \widetilde{\alpha_1} & \widetilde{\alpha_2} \end{pmatrix} \right|^{1/2}$$

where $\widetilde{\cdot}\colon K \to K$ is the non-trivial Galois automorphism $a + b\sqrt{d} \mapsto a - b\sqrt{d}$.

So call the basis $\{\, \alpha_1, \alpha_2 \,\}$ normalised if

$$\det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \widetilde{\alpha_1} & \widetilde{\alpha_2} \end{pmatrix} = N(\mathfrak{a})\sqrt{\Delta_K}\,,$$

where $\sqrt{\cdot}$ is the principal branch: $\sqrt{\Delta_K} > 0$ when $\Delta_K > 0$ and $\Im\sqrt{\Delta_K} > 0$ when $\Delta_K < 0$. Exactly one of $\{\, \alpha_1, \alpha_2 \,\}$ and $\{\, \alpha_2, \alpha_1 \,\}$ is a normalised basis.

Definition 3. Given a normalised basis $\{\, \alpha_1, \alpha_2 \,\}$ of an ideal $\mathfrak{a}$, define the quadratic form

$$Q_{\alpha_1,\alpha_2}(x, y) \coloneqq \frac{1}{N(\mathfrak{a})} N(\alpha_1 x + \alpha_2 y)\,.$$

Proposition 4. *The quadratic form $Q_{\alpha_1,\alpha_2}(x, y)$ is a primitive integral binary quadratic form, with discriminant Δ_K. If $\Delta_K < 0$, it is positive definite.*

Proof. This is certainly a binary quadratic form $ax^2 + bxy + cy^2$, for some a, b, c. We check the coefficients are integers. We can assume $\mathfrak{a}$ is an integral ideal, with

$\alpha_1, \alpha_2 \in \mathcal{O}_K$. Then any $z = x\alpha_1 + y\alpha_2$ is in $\mathfrak{a}$, so $\mathfrak{a} \mid (z)$ and $N(\mathfrak{a})|N(z)$. Applying this to $a = Q_{\alpha_1,\alpha_2}(1,0)$, $c = Q_{\alpha_1,\alpha_2}(0,1)$ and $a+b+c = Q_{\alpha_1,\alpha_2}(1,1)$ shows that the coefficients are integers.

Expanding out gives $a = \frac{1}{N(\mathfrak{a})}\alpha_1\widetilde{\alpha_1}$, $b = \frac{1}{N(\mathfrak{a})}(\alpha_1\widetilde{\alpha_2} + \widetilde{\alpha_1}\alpha_2)$, $c = \frac{1}{N(\mathfrak{a})}\alpha_2\widetilde{\alpha_2}$. A direct computation shows the discriminant of Q is

$$D_Q = \frac{1}{N(\mathfrak{a})} \det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \widetilde{\alpha_1} & \widetilde{\alpha_2} \end{pmatrix}^2 = \Delta_K$$

Since $a = \frac{1}{N(\mathfrak{a})}N(\alpha_1) > 0$, the form is positive-definite if $\Delta_K < 0$.

Finally, for a fundamental discriminant Δ_K, any binary quadratic form is primitive. Notice that $\gcd(a,b,c)^2$ must divide the discriminant $D = b^2 - 4ac$. If $d \equiv 1 \pmod 4$ then $\Delta_K = d$ is square free. If $d \equiv 2, 3 \pmod 4$ then $\Delta_K = 4d$, so $\gcd(a,b,c) \leq 2$. And $\gcd(a,b,c) = 2$ cannot occur, otherwise $d = \frac{1}{4}\Delta_K = (\frac{b}{2})^2 - 4\frac{a}{2}\frac{c}{2} \equiv \square \equiv 0, 1 \pmod 4$. $\square$

Example 5. Consider $K = \mathbb{Q}(\sqrt{-5})$ of discriminant $\Delta_K = -20$, and the ideals $\mathcal{O}_K = (1) = [1, -\sqrt{-5}]$ of norm 1 and $\mathfrak{p}_3 = [3, 1+\sqrt{-5}]$ of norm 2. These bases are normalised.

The corresponding quadratic forms are

$$\begin{aligned} Q_{1,-\sqrt{-5}}(x,y) &= \frac{1}{N(\mathcal{O}_K)} N(1 \cdot x - \sqrt{-5} \cdot y) \\ &= x^2 + 5y^2 \\ Q_{3,1+\sqrt{-5}}(x,y) &= \frac{1}{N(\mathfrak{p}_3)} N(3x + (1+\sqrt{-5})y) \\ &= \frac{1}{3} N((3x+y) + \sqrt{-5}y) \\ &= \frac{1}{3}((3x+y)^2 + 5y^2) \\ &= 3x^2 + 2xy + 2y^2 \end{aligned}$$

Claim: $\mathcal{C}(K) = \{\, [\mathcal{O}_K], [\mathfrak{p}_3] \,\} \cong \mathbb{Z}/2\mathbb{Z}$, and the above are representatives of all equivalence classes of primitive positive-definite BQF's of discriminant -20.

Now consider $K = \mathbb{Q}(\sqrt{65})$, of discriminant $\Delta_K = 65$ and the ideals $\mathcal{O}_K = (1) = [1, \frac{1-\sqrt{65}}{2}]$ of norm 1 and $\mathfrak{p}_2 = [2, \frac{1-\sqrt{65}}{2}]$ of norm 2. These bases are normalised.

The corresponding quadratic forms are

$$\begin{aligned} Q_{1,\frac{1-\sqrt{65}}{2}}(x,y) &= \frac{1}{N(\mathcal{O}_K)} N(1 \cdot x + \tfrac{1-\sqrt{65}}{2} \cdot y) \\ &= N((x + \tfrac{y}{2}) - \tfrac{\sqrt{65}}{2}y) \\ &= (x + \tfrac{y}{2})^2 - \tfrac{65}{4}y^2 \\ &= x^2 + xy - 16y^2 \\ Q_{2,\frac{1-\sqrt{65}}{2}}(x,y) &= \frac{1}{N(\mathfrak{p}_2)} N(2x + \tfrac{1-\sqrt{65}}{2}y) \end{aligned}$$

$$= 2x^2 + xy - 8y^2$$

Claim $\mathcal{C}^+(K) = \{ [\mathcal{O}_K], [\mathfrak{p}_2] \} \cong \mathbb{Z}/2$, and the above are representatives of all equivalence classes of primitive BQF's of discriminant 65. Moreover, since $N(7+2\frac{1+\sqrt{65}}{2}) = -1$, we also have $\mathcal{C}(K) = \mathcal{C}^+(K)$.

Remark 6. The forms $x^2 + 5y^2$ and $x^2 + xy - 16y^2$ arise from the class of *principal* ideals the quadratic field. This explains why we call $x^2 + ny^2$, and $x^2 + xy + ny^2$ the principal forms for discriminant $D = -4d$ and $D = 1 - 4n$, respectively. See Sheet 5, Q2.

Need to check some things to ensure this map is well-defined.

Proposition 7. *Changing the normalised basis of the ideal $\mathfrak{a} = [\alpha_1, \alpha_2]$ gives a properly equivalent binary quadratic forms.*

Proof. A change of basis $\underline{\beta} = B\underline{\alpha}$ between bases $\mathfrak{a} = [\alpha_1, \alpha_2] = [\beta_1, \beta_2]$ gives a matrix B in $\mathrm{GL}_2(\mathbb{Z})$. Since both are normalised $\det(B) = 1$, so $B \in \mathrm{SL}_2(\mathbb{Z})$.

A direct computation shows

$$Q_{\beta_1,\beta_2}(\underline{\mathbf{x}}) = Q_{\alpha_1,\alpha_2}(B\underline{\mathbf{x}})$$

meaning the two binary quadratic forms are properly equivalent. □

Proposition 8. *If $\mathfrak{a} = [\alpha_1, \alpha_2]$ and $\mathfrak{b} = [\beta_1, \beta_2]$ are two ideals in the same narrow ideal class, then the quadratic forms $Q_{\alpha_1,\alpha_2}(x, y)$ and $Q_{\beta_1,\beta_2}(x, y)$ are properly equivalent.*

Proof. Since $\mathfrak{a}$ and $\mathfrak{b}$ are in the same narrow idea class, we have $\mathfrak{b} = (\lambda)\mathfrak{a}$, for some totally positive λ. If $[\alpha_1, \alpha_2]$ is a normalised basis for $\mathfrak{a}$, then $[\lambda\alpha_1, \lambda\alpha_2]$ is a normalised basis for $\mathfrak{b}$, since $N(\lambda) > 0$.

Then a direct calculation gives

$$Q_{\lambda\alpha_1,\lambda\alpha_2}(x, y) = Q_{\alpha_1,\alpha_2}(x, y)$$

showing the two forms are properly equivalent, and indeed for equal for choice of basis. □

So the map

$$\mathcal{C}^+(K) \to \{ \text{BQF's of discriminant } \Delta_K \}$$

is well defined. Moreover, it is bijective.

Proof. Check surjectivity and injectivity separately.

Surjectivity: Let $ax^2 + bxy + cy^2$ be a (primitive) integral BQF of discriminant Δ_K (positive-definite if $\Delta_K < 0$). Then

$$\mathfrak{a} = [a, \tfrac{b-\sqrt{\Delta_K}}{2}]$$

is a fractional ideal of K with indicated $\mathbb{Z}$-basis. If $\Delta_K < 0$, set $\lambda = 1$ otherwise, take $\lambda = \sqrt{\Delta_K}$. Then

$$\lambda\mathfrak{a} = [\lambda a, \lambda\tfrac{b-\sqrt{\Delta_K}}{2}]$$

is an ideal of norm $aN(\lambda)$, with normalied basis.

A direct calculation gives

$$Q_{\lambda a, \lambda \frac{b-\sqrt{\Delta_K}}{2}}(x,y) = ax^2 + bxy + cy^2 \,.$$

Injctivity: Suppose $\mathfrak{a} = [\alpha_1, \alpha_2]$ and $\mathfrak{b} = [\beta_1, \beta_2]$ map to the same class of quadratic forms. We can assume these bases are normalised, and by changing bases, that we have $Q_{\alpha_1,\alpha_2}(x,y) = Q_{\beta_1,\beta_2}(x,y)$.

The roots of the quadratic polynomial $Q_{\alpha_1,\alpha_2}(1,y)$ are $y = -\frac{\alpha_1}{\alpha_2}$ and $-\frac{\widetilde{\alpha_1}}{\widetilde{\alpha_2}}$. So we mus have either $\alpha_1/\alpha_2 = \beta_1/\beta_2$, or $\alpha_1/\alpha_2 = \widetilde{\beta_1}/\widetilde{\beta_2}$.

The second case cannot occur: for it does, set $\lambda = \alpha_1/\widetilde{\beta_1} = \alpha_2/\widetilde{\beta_2}$. Normalised bases means $N(\lambda) < 0$, whereas equality of quadratic forms leads to $N(\lambda) > 0$.

Therefore the first case occurs. Set $\lambda = \alpha_1/\beta_1 = \alpha_2/\beta_2$. Normalised bases means $N(\lambda) > 0$. Then we have $\mathfrak{a} = \mu\mathfrak{b}$, for some totally positive $\mu = \pm\lambda$. This shows $\mathfrak{a}$ and $\mathfrak{b}$ are in the same narrow idea class. □

1.3. Properties of the correspondence

Corollary 9. *For a real quadratic field $K = \mathbb{Q}(\sqrt{d})$ of discriminant $\Delta_K > 0$, the narrow class number $h^+(K)$ is equal to the class number $h^+(\Delta_K)$ of primitive integral binary quadratic forms of discriminant Δ_K.*

For an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ of discriminant $\Delta_K < 0$, the class number $h(K)$ is equal to the class number $h(\Delta_K)$ of primitive positive-definite integral binary quadratic forms of dicriminant Δ_K.

Corollary 10. *Since the (narrow) ideal class group $\mathcal{C}^+(K)$ is a group, there is a natural group structure on the set of binary quadratic forms of discriminant Δ_K. Note: this turns out to be Gauss's composition of binary quadratic forms.*

Moreover, we can connect representations of positive integers m, to existence of ideals of norm m, under this correspondence.

Proposition 11. *A positive integer m is represented by the quadratic form $f(x,y) \leftrightarrow \mathfrak{a}$, if and only if there is an integral ideal of norm m in the smae narrow class as $\mathfrak{a}$.*

Proof. Write $f(x,y) = Q_{\alpha_1,\alpha_2}(x,y)$ for some normalised basis $\mathfrak{a} = [\alpha_1, \alpha_2]$. Notice that $\mathfrak{c}^{-1}$ and $\widetilde{\mathfrak{c}}$ are in the same narrow ideal class since $\mathfrak{c}^{-1} = \frac{1}{N(\mathfrak{c})}\widetilde{\mathfrak{c}}$.

'$\Leftarrow$': If $\mathfrak{b}$ is an integral ideal with norm m in the same narrow class as $\mathfrak{a}$, rite $\widetilde{\mathfrak{b}} = \lambda\mathfrak{a}^{-1}$, for some totally positive λ. Write $\lambda = x_0\alpha_1 + y_0\alpha_2$. Then

$$Q_{\alpha_1,\alpha_2}(x_0,y_0) = \frac{1}{N\mathfrak{a})} N(\lambda) = N(\widetilde{\mathfrak{b}}) = N(\mathfrak{b}) = m \,.$$

'⇒': If $m = Q_{\alpha_1,\alpha_2}(x_0, y_0)$, then $m = \frac{1}{N(\mathfrak{a})}N(\lambda)$, for $\lambda = x_0\alpha_1 + y_0\alpha 2$. Since $N(\lambda) > 0$, one of $\pm\lambda$ is totally positive. Then $\mathfrak{b} = \widetilde{\lambda\alpha^{-1}}$ is an integral ideal of norm m in the same narrow ideal class as $\mathfrak{a}$. □

As a corollary, we can obtain our prime representability condition in a different way.

Corollary 12. *An odd prime $p \mid \Delta_K$ is represented by some BQF of discriminant Δ_K if and only if $\left(\frac{\Delta_K}{p}\right) = 1$.*

Proof. The positive integer p is represented by some BQF of discriminant Δ_K if and only if there is some ideal of norm p in K.

An ideal I divides its norm $N(I)$. So there is an ideal of norm p if and only if (p) splits or ramifies in K. Assuming $p \mid \Delta_K$ means (p) does not ramify.

It is well-known that splitting of (p) is described by when $\left(\frac{D_K}{p}\right) = 1$. □

Corollary 13. *The primes represented by two different quadratic forms $f(x, y)$ and $g(x, y)$ of discriminant Δ_K are either disjoint, or identical. Moreover, if they are identical then $f(x, y)$ and $g(x, y)$ either properly equivalent, or are inverses (under Gauss composition) meaning they are improperly equivalent.*

Proof. If $f(x, y)$ and $g(x, y)$ represent a prime p, then (p) decomposes as $\mathfrak{p}\widetilde{\mathfrak{p}}$ in K, where both $\mathfrak{p}$ and $\widetilde{\mathfrak{p}}$ have norm p.

Then either $f(x, y)$ and $g(x, y)$ correspond to the same idea class, or they correspond to inverse ideal classes as $[\mathfrak{p}]^{-1} = [\widetilde{\mathfrak{p}}]$. If they correspond to the same ideal class, they are equivalent and so represent the same values. Otherwise a prime q represented by $f(x, y)$ corresponds to an ideal $\mathfrak{q}$ of norm q, then $\widetilde{\mathfrak{q}}$ is an ideal of norm q in the class corresponding to $g(x, y)$. This shows $g(x, y)$ also represents q.

Finally the inverse under Gauss composition of $ax^2 + bxy + cy^2$ can be shown to be $ax^2 - bxy + cy^2$, which is equivalent (possibly improperly) to the original. □

References

[Coh13] Henri Cohen. *A course in computational algebraic number theory*. Vol. 138. Springer Science & Business Media, 2013.

[FT93] A Fröhlich and MJ Taylor. *Algebraic number theory, volume 27 of Cambridge Studies in Advanced Mathematics*. 1993.