Quadratic fields

A quadratic field is a field $K \supset \mathbb{Q}$ such that $[K:\mathbb{Q}] = 2$.

Given K, $\exists!\ d \in \mathbb{Z} \setminus \{0,1\}$ square-free such that $K = \mathbb{Q}(\sqrt{d})$.

K is a $\left\{\begin{matrix}\text{real}\\ \text{imaginary}\end{matrix}\right\}$ quadratic field if $\left\{\begin{matrix}d>0\\ d<0\end{matrix}\right\} \iff \left\{\begin{matrix}r_1=2, r_2=0\\ r_1=0, r_2=1\end{matrix}\right\}$.

We know: (a) $\mathcal{O}_K = \left\{\begin{matrix}\mathbb{Z}[\sqrt{d}] & , \ d \equiv 2,3 \pmod 4\\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & , \ d \equiv 1 \pmod 4\end{matrix}\right\}$, $\underbrace{D_K = D}_{\text{fundamental discriminant}} = \left\{\begin{matrix}4d & , \ d \equiv 2,3 \pmod 4\\ d & , \ d \equiv 1 \pmod 4\end{matrix}\right.$

(b) $\mathcal{O}_K = \mathcal{O}_D = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$, $(\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]) = \left\{\begin{matrix}1\\ 2\end{matrix}\right.$

(c) $\mathcal{O}_K^* = \left\{\begin{matrix}\mu_4 & d=-1\\ \mu_6 & d=-3\\ \{\pm 1\} & d \neq -1,-3,\ d<0\end{matrix}\right.$, $\mathcal{O}_K^* = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$, $\varepsilon > 1$ fundamental unit

---

Factorisation of primes: (1) If $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$: $\mathbb{Z}[i] = UFD$,

$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$, $2 = (-i)(1+i)^2$, $p \equiv 3 \pmod 4$ prime $\Rightarrow p$ irreducible in $\mathbb{Z}[i]$,

$p \equiv 1 \pmod 4 \Rightarrow \exists\, u, v \in \mathbb{Z}$ $u^2+v^2 = p$, $p = \pi\overline{\pi}$, $\pi = u+vi$, $\overline{\pi} = u-vi \notin \pi\,\mathbb{Z}[i]^*$

$\mathbb{Z}[X]/(X^2+1) \xrightarrow{\sim} \mathbb{Z}[i]$, $\mathbb{Z}[i]/p\,\mathbb{Z}[i] \xleftarrow{\simeq} \mathbb{Z}[X]/(p, X^2+1) = \mathbb{F}_p[X]/(X^2+1)$

$\overline{a+bX} \longmapsto a+bi$

$p=2$: $\mathbb{Z}[i]/2\mathbb{Z}[i] \twoheadrightarrow \mathbb{F}_2[X]/((X+1)^2) \xrightarrow{\sim} \mathbb{F}_2[Y]/(Y^2)$ $\quad Y = X+1$

$\overline{a+bi} \longmapsto a+b(\overline{Y}-1)$

$p \equiv 3 \pmod 4$: $\mathbb{Z}[i]/p\,\mathbb{Z}[i] \xrightarrow{\sim} \mathbb{F}_p[X]/\underbrace{(X^2+1)}_{\text{irreducible in } \mathbb{F}_p[X]} \xrightarrow{\simeq} \mathbb{F}_{p^2}$

$p \equiv 1 \pmod 4$: $\mathbb{Z}[i]/p\,\mathbb{Z}[i] \xrightarrow{\sim} \mathbb{F}_p[X]/(X^2+1) = \mathbb{F}_p[X]/((X-t)(X+t))$

$\exists\, t \in \mathbb{Z}$ $t^2 \equiv -1 \pmod p$

$\overline{a+bi} \longmapsto \overline{a+bX}$

$\mathbb{F}_p[X]/(X-t) \times \mathbb{F}_p[X]/(X+t)$

$(a+bt,\ a-bt) \in \mathbb{F}_p \times \mathbb{F}_p$

---

(2) General K, $p \neq 2$ prime: $p \nmid (\mathcal{O}_K : \mathbb{Z}[\sqrt{d}])$

$f(X) = X^2 - d$ minimal polynomial of $\sqrt{d}$ over $\mathbb{Q}$

Kummer–Dedekind: $\mathcal{O}_K/p\,\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]/p\,\mathbb{Z}[\sqrt{d}] \simeq \underbrace{\mathbb{Z}[X]/(p, X^2-d)}_{\mathbb{F}_p[X]/(X^2-d)}$

$p \mid d \Rightarrow f \equiv X^2 \pmod p$, $(p) = p\,\mathcal{O}_K = \mathfrak{P}^2$, $\mathfrak{P} = (p, \sqrt{d})$, $N(\mathfrak{P}) = p$, $e_{\mathfrak{P}} = 2$

$\left(\frac{d}{p}\right) = -1 \Rightarrow f \equiv \underbrace{X^2-d}_{\text{irreducible in } \mathbb{F}_p[X]} \pmod p$, $(p) = \mathfrak{P}$, $N(\mathfrak{P}) = p^2$, $e_{\mathfrak{P}} = 1$

$\left(\frac{d}{p}\right) = 1 \Rightarrow f \equiv (X-t)(X+t) \pmod p$, $(p) = \mathfrak{P}_+\mathfrak{P}_-$, $\mathfrak{P}_\pm = (p, \sqrt{d} \pm t)$, $N(\mathfrak{P}_\pm) = p$,

$(t^2 \equiv d \pmod p)$ $\quad e_{\mathfrak{P}_\pm} = 1$

(3) General K, $p=2$: (a) if $d \equiv 2,3 \pmod 4$ $(D=4d)$: $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$,

$f = x^2 - d \equiv \begin{cases} x^2 \pmod 2 \\ (x-1)^2 \pmod 2 \end{cases}$ if $\begin{matrix} d \equiv 2 \pmod 4 \\ d \equiv 3 \pmod 4 \end{matrix}$ $\Rightarrow (2) = \mathfrak{P}^2$, $\mathfrak{P} = \begin{cases} (2, \sqrt{d}) \\ (2, \sqrt{d}-1) \end{cases}$

$N(\mathfrak{P}) = 2$, $e_{\mathfrak{P}} = 2$

(b) if $d \equiv 1 \pmod 4$ $(D=d)$: $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, $\alpha = \frac{1+\sqrt{d}}{2}$ has minimal polynomial $f = x^2 - x + \frac{1-d}{4}$ over $\mathbb{Q}$.

if $d \equiv 1 \pmod 8$ $\Rightarrow f \equiv x(x-1) \pmod 2$, $(2) = \mathfrak{P}_+ \mathfrak{P}_-$, $\mathfrak{P}_\pm = (2, \frac{\sqrt{d} \pm 1}{2})$

$N(\mathfrak{P}_\pm) = 2$, $e_{\mathfrak{P}_\pm} = 1$

if $d \equiv 5 \pmod 8$ $\Rightarrow f \equiv \underbrace{x^2 - x + 1}_{\text{irreducible in } \mathbb{F}_2[X]} \pmod 2$, $(2) = \mathfrak{P}$, $N(\mathfrak{P}) = 2^2$, $e_{\mathfrak{P}} = 1$

Summary:

- $(p) = \mathfrak{P}^2$ is ramified in $K/\mathbb{Q} \iff p \mid D$
- p splits completely in $K/\mathbb{Q}$, $(p) = \mathfrak{P}_+ \mathfrak{P}_- \iff \begin{cases} p \neq 2, \left(\frac{d}{p}\right) = 1 \\ p = 2, \quad D = d \equiv 1 \pmod 8 \end{cases}$
- p is inert in $K/\mathbb{Q}$, $(p) = \mathfrak{P} \iff \begin{cases} p \neq 2, \left(\frac{d}{p}\right) = -1 \\ p = 2, \quad D = d \equiv 5 \pmod 8 \end{cases}$

Minkowski's bounds

We know: every non-zero ideal $I \subset \mathcal{O}_K$ contains an element $0 \neq \alpha \in I$ such that $|N_{K/\mathbb{Q}}(\alpha)| \leq M_K N(I)$, $M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D_K|^{1/2}$ (Minkowski's constant)

$\Rightarrow$ the ideal class $[I]^{-1} \in Cl_K$ contains the ideal $J = (\alpha) I^{-1} \subset \mathcal{O}_K$ of norm $N(J) = \frac{|N_{K/\mathbb{Q}}(\alpha)|}{N(I)} \leq M_K$

Our case: $n=2$, $M_K = \begin{cases} \frac{1}{2} D^{1/2} & d>0 \\ \frac{2}{\pi} |D|^{1/2} & d<0 \end{cases}$

The correspondence $Cl_K^+ = Cl^+(\mathcal{O}_K) \xleftrightarrow{\sim} Cl^+(D)$ and reduction theory for binary quadratic forms gives bounds

$\exists\, J \in$ given class $N(J) \leq \begin{cases} \frac{1}{2} D^{1/2} & d>0 \\ \frac{1}{\sqrt{3}} |D|^{1/2} & d<0 \end{cases}$ $\left(\frac{1}{\sqrt{3}} < \frac{2}{\pi}\ !!\right)$

($\iff \exists\, [a,b,c] \in$ given class $\min(|a|, |c|) \leq$ — " —).

Above, $Cl_K^+ = I(\mathcal{O}_K) / \{(\alpha) \mid \alpha \in K^*,\ N_{K/\mathbb{Q}}(\alpha) > 0\}$,

$h_K^+ = |Cl_K^+| = \underbrace{|Cl_K|}_{h_K} \cdot \begin{cases} 2 & d>0,\ N_{K/\mathbb{Q}}(\varepsilon) = 1 \\ 1 & \text{otherwise.} \end{cases}$

Ex: $d=-5$, $K=\mathbb{Q}(i\sqrt{5})$, $\mathcal{O}_K=\mathbb{Z}[i\sqrt{5}]$, $D=-20$: $M_K=\frac{2}{\pi}\sqrt{20}<\frac{9}{\pi}<3$

ideals of norm $=1$: (1)

— " — $=2$: factorise $(2)=(2,i\sqrt{5}+1)^2$, $P=(2,1+i\sqrt{5})$ is the unique ideal with $N(P)=2$

$P\neq(\alpha)$: if $\alpha=u+vi\sqrt{5}\in\mathcal{O}_K$ ($u,v\in\mathbb{Z}$) $\Rightarrow N(\alpha)=u^2+5v^2\neq 2$.

Therefore $h_K=|Cl_K|=2$, $Cl_K\simeq\mathbb{Z}/2\mathbb{Z}$, the non-trivial class is represented by P. This is in line with the fact that there are exactly two reduced forms of discriminant $\Delta=-20$, namely, $x^2+5y^2=[1,0,5]$ and $2x^2+2xy+3y^2=[2,2,3]$.

Application to diophantine equations:

Prop. Let $[L:\mathbb{Q}]<\infty$. If $0\neq I\subset\mathcal{O}_L$ is an ideal such that $I^n=(\alpha)$ is principal for some integer $n\geq 1$ satisfying $\gcd(n,h_L)=1$, then $I=(\beta)$ is principal.

Pf: $\exists\, u,v\in\mathbb{Z}$ $un+vh_L=1$; Lagrange's Thm for $Cl_L\Rightarrow I^{h_L}=(\beta)$ is principal $\Rightarrow$ $I=(I^n)^u(I^{h_L})^v=(\alpha^u\beta^v)$ is principal.

$$y^2+5=x^3 \qquad (x,y\in\mathbb{Z})$$

Factorisation in $\mathbb{Z}[i\sqrt{5}]$: $(y+i\sqrt{5})(y-i\sqrt{5})=x^3$ $\qquad K=\mathbb{Q}(i\sqrt{5})$

We have $\gcd(x,y)=\gcd(x,5)=\gcd(y,5)=1$ in $\mathbb{Z}$.

Let $J=\gcd((y+i\sqrt{5}),(y-i\sqrt{5}))$, ideal in $\mathbb{Z}[i\sqrt{5}]$.

If $J\neq(1)\Rightarrow\exists$ non-zero prime ideal $P\mid J$

$\Rightarrow P\mid(y\pm i\sqrt{5})\Rightarrow P\mid(2y)$, $P\mid(2i\sqrt{5})$, $P\mid(x^3)$, $P\mid p$ (prime number)

$\Rightarrow p\mid \underbrace{N_{K/\mathbb{Q}}(2y)}_{4y^2}$, $\underbrace{N_{K/\mathbb{Q}}(2i\sqrt{5})}_{20}$, $\underbrace{N_{K/\mathbb{Q}}(x^3)}_{x^6}$, but

$\gcd(4y^2,20,x^6)=\gcd(4,x^6)$ in $\mathbb{Z}$. Can $2\mid x$? If $2\mid x\Rightarrow$ $2\nmid y$, $y^2\equiv 1\pmod 8\Rightarrow x^3\equiv 6\pmod 8$ — impossible.

Therefore $p\mid\gcd(4,x^6)=1$ — impossible $\Rightarrow J=(1)$.

Unique factorisation for ideals $\Rightarrow$ $(y+i\sqrt{5})=I^3$, $(y-i\sqrt{5})=\bar{I}^3$

As $h_K=2\overset{\text{Prop.}}{\Rightarrow}$ $I=(\alpha)$ is principal $\Rightarrow$ $(y+i\sqrt{5})=(\alpha^3)$,

$y+i\sqrt{5}=u\alpha^3$, $u\in\mathcal{O}_K^*=\mathbb{Z}[i\sqrt{5}]^*=\{\pm 1\}\Rightarrow u=u^3$,

$y+i\sqrt{5}=(u\alpha)^3=(a+bi\sqrt{5})^3$ for some $a,b\in\mathbb{Z}$.

The equations $y \pm i\sqrt{5} = (a \pm bi\sqrt{5})^3$ give $(a, b \in \mathbb{Z})$

$x^3 = (a^2+5b^2)^3 \Rightarrow x = a^2+5b^2$,

$y = a(a^2-15b^2)$, $1 = b(3a^2-5b^2)$

$\Rightarrow b = \pm 1$, $3a^2-5b^2 = \pm 1$, $3a^2 = 5 \pm 1 = \begin{cases} 6 \\ 4 \end{cases}$ — impossible.

Conclusion: $y^2+5 = x^3$ has no solution $x, y \in \mathbb{Z}$.

General equation $y^2+k = x^3$ $(x, y \in \mathbb{Z})$ $(k \in \mathbb{Z}, \sqrt{k} \notin \mathbb{Z})$

can be reduced to a finite set of cubic Thue equations

$F(a, b) = m$, $(a, b \in \mathbb{Z})$, where $F(X, Y) \in \mathbb{Z}[X, Y]$ (*)

is homogeneous of degree 3, $m \in \mathbb{Z} \setminus \{0\}$.

Above, $F(X, Y) = Y(3X^2-5Y^2)$ is reducible over $\mathbb{Q}$

$\Rightarrow$ there are only finitely many solutions of (*).

Thue's Thm: $F \in \mathbb{Z}[X, Y]$ homogeneous of degree $n \geq 3$, irreducible over $\mathbb{Q}$, $m \in \mathbb{Z} \setminus \{0\} \Rightarrow F(a, b) = m$ has only finitely many solutions $a, b \in \mathbb{Z}$.

Thue deduced this from his strengthening of Liouville's Thm (which had exponent $|q|^n$ in the denominator):

Thm (Thue): If $K = \mathbb{Q}(\alpha)$, $[K : \mathbb{Q}] = n \geq 3$, then

$$\forall \varepsilon > 0 \quad \exists\, c = c(\varepsilon) > 0 \quad \forall \frac{p}{q} \in \mathbb{Q} \qquad \left|\alpha - \frac{p}{q}\right| \geq \frac{c(\varepsilon)}{|q|^{n/2+1+\varepsilon}}.$$

Further improvements were due to Siegel and others.

An optimal exponent $|q|^{2+\varepsilon}$ was obtained by K. Roth (Fields medal).

One can invert the above arguments to construct quadratic fields K with $Cl_K \supset \mathbb{Z}/n\mathbb{Z}$ (even $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if $d < 0$).

Exercise (Nagell). Assume: $p \neq 2$ prime number, $d < 0$, $|d|$ square-free, $d \neq -3$ if $p = 3$, $x, y, z \in \mathbb{Z}$, $x^2 - dy^2 = 4z^p$, $\gcd(x, z) = 1$, $p \mid x$, $p^2 \nmid x \Rightarrow \left(\frac{x + y i\sqrt{|d|}}{2}\right) = I^p$ for some ideal $I \subset \mathcal{O}_K \subset K = \mathbb{Q}(i\sqrt{|d|})$, $I \neq (\alpha)$. Therefore $p \mid h_K$.

From Jacobi's to Kronecker's symbol

$d \in \mathbb{Z} \setminus \{0,1\}$ square-free, $K = \mathbb{Q}(\sqrt{d})$, $D = D_K = \begin{cases} 4d & d \equiv 2,3 \pmod 4 \\ d & d \equiv 1 \pmod 4 \end{cases}$.

Goal: write $\left(\frac{d}{a}\right)$ (defined only for $a>0$, $\gcd(a,2d)=1$) as a product and extend its domain of definition.

Ex: $\left(\frac{-5}{a}\right) = \left(\frac{-1}{a}\right)\left(\frac{5}{a}\right) = (-1)^{\frac{a-1}{2}}\left(\frac{a}{5}\right)$, $\left(\frac{-14}{a}\right) = \left(\frac{2}{a}\right)\left(\frac{-7}{a}\right) = \left(\frac{2}{a}\right)\left(\frac{a}{7}\right) = (-1)^{\frac{a^2-1}{8}}\left(\frac{a}{7}\right)$

Notation: $\mathrm{Ram} = \mathrm{Ram}(K/\mathbb{Q}) = \{$prime numbers q ramified in $K/\mathbb{Q}\} = \{$ —— " —— , $q \mid D\}$

Step 1. Write $\boxed{D = \prod_{q \mid D} D_q}$, D_q discriminant, $|D_q|$ = power of the prime q

For $q \neq 2$, $D_q = q^* = (-1)^{\frac{q-1}{2}} q$ $(\equiv 1 \pmod 4)$

(a) $d \equiv 1 \pmod 4$: $D = d = \prod_{q \mid D} q^*$

(b) $d \equiv 3 \pmod 4$: $-d = \prod_{2 \neq q \mid D} q^*$, $D = 4d = \underbrace{(-4)}_{D_2} \prod_{2 \neq q \mid D} q^*$

(c) $d \equiv 2 \pmod 4$: $\prod_{2 \neq q \mid D} q^* = (-1)^{d/2-1} d/2$, $D = 4d = \underbrace{\left((-1)^{d/2-1} 8\right)}_{D_2} \prod_{2 \neq q \mid D} q^*$

Step 2. Use QRL to extend the domain of definition of each $\left(\frac{D_q}{a}\right)$:

If $a>0$, $q \mid D$ prime, $(a, 2q)=1$:

(a) $q \neq 2$: $\left(\frac{D_q}{a}\right) = \left(\frac{q^*}{a}\right) \overset{QRL}{=} \left(\frac{a}{q}\right)$ **Def:** $\chi_{D_q} : \underbrace{(\mathbb{Z}/|D_q|\mathbb{Z})^*}_{(\mathbb{Z}/q\mathbb{Z})^*} \longrightarrow \{\pm 1\}$, $b \longmapsto \left(\frac{b}{q}\right)$

(b) $q = 2$: $\left(\frac{-4}{a}\right) = (-1)^{\frac{a-1}{2}} = \begin{cases} 1 & a \equiv 1 \pmod 4 \\ -1 & a \equiv -1 \pmod 4 \end{cases}$, $\left(\frac{8}{a}\right) = \begin{cases} 1 & a \equiv \pm 1 \pmod 8 \\ -1 & a \equiv \pm 3 \pmod 8 \end{cases}$,

$\left(\frac{8}{a}\right) = (-1)^{\frac{a^2-1}{8}}$, $\left(\frac{-8}{a}\right) = \left(\frac{-4}{a}\right)\left(\frac{8}{a}\right)$.

Def: $\chi_{-4} : (\mathbb{Z}/4\mathbb{Z})^* \longrightarrow \{\pm 1\}$, $\chi_8 : (\mathbb{Z}/8\mathbb{Z})^* \longrightarrow \{\pm 1\}$, $\chi_{-8} : (\mathbb{Z}/8\mathbb{Z})^* \longrightarrow \{\pm 1\}$

$\overline{1} \longmapsto 1$, $\overline{-1} \longmapsto -1$; $\overline{\pm 1} \longmapsto 1$, $\overline{\pm 3} \longmapsto -1$; $\chi_{-8} = \chi_{-4}\chi_8$

Summary: $\chi_{D_q} : (\mathbb{Z}/|D_q|\mathbb{Z})^* \longrightarrow \{\pm 1\}$, $\chi_{D_q}(a \bmod |D_q|) = \left(\frac{D_q}{a}\right)$ if $a>0$, $(a, 2q)=1$.

Step 3. **Def** (Kronecker's symbol)

$$\chi_D = \prod_{q \mid D} \chi_{D_q} : (\mathbb{Z}/|D|\mathbb{Z})^* \simeq \prod_{q \mid D} (\mathbb{Z}/|D_q|\mathbb{Z})^* \longrightarrow \{\pm 1\}$$

If $a>0$, $(a, 2D)=1$ $\Longrightarrow$ $\chi_D(a) = \left(\frac{D}{a}\right) = \left(\frac{d}{a}\right)$.

Thm (Properties of Kronecker's symbol)

(1) $0<a\in\mathbb{Z}$, $(a,2D)=1 \Rightarrow \underbrace{\chi_D(a \pmod{|D|})}_{\text{Kronecker}} = \underbrace{\left(\frac{D}{a}\right)}_{\text{Jacobi}} = \left(\frac{d}{a}\right)$

(2) $\forall\, 2\mid D \quad \chi_{D_2}(-1)=\operatorname{sgn}(D_2) \Rightarrow \chi_D(-1)=\operatorname{sgn}(D)$.

(3) If $2\nmid D \Rightarrow D=d\equiv 1 \pmod 4$, $\chi_D(2)=\prod_{2\mid D}\chi_8(2^{*}\pmod 8)=\chi_8(|d| \pmod 8)$
$=\begin{cases}1 & d\equiv 1 \pmod 8\\ -1 & d\equiv 5\pmod 8\end{cases}$

(4) A prime $p\nmid D$ $\begin{cases}\text{splits}\\ \text{is inert}\end{cases}$ in $K/\mathbb{Q} \Leftrightarrow \chi_D(p)=\begin{cases}1\\-1\end{cases}$.

(5) $\forall\, 2\mid D \quad \forall\, u\in\mathbb{Z}_2^{*} \quad \underbrace{(D,u)_2}_{\text{Hilbert}} = (D_2,u)_2 = \underbrace{\chi_{D_2}(u \pmod{|D_2|})}_{\text{Kronecker}}$

$$\begin{array}{ccccc}\mathbb{Z}_2^{*} & \longrightarrow & (\mathbb{Z}/|D_2|\mathbb{Z})^{*} & \xrightarrow{\chi_{D_2}} & \{\pm 1\}\\ \cap & & & \nearrow & \\ \mathbb{Q}_2^{*} & & \xrightarrow{(D,\cdot)_2=(D_2,\cdot)_2} & & \end{array}$$

Pf: (1) OK

(2) $2\neq 2 \Rightarrow \chi_{D_2}(-1)=\left(\frac{-1}{2}\right)=2^{*}/2=\operatorname{sgn}(2^{*})$; $\chi_{-4}(-1)=\chi_{-8}(-1)=-1=-\chi_8(-1)$.

(3) $d=D=\prod_{2\mid D}2^{*}$, $\chi_{D_2}(2)=\left(\frac{2}{2}\right)=\chi_8(2 \pmod 8)$, $\chi_D(2)=\chi_8\Big(\underbrace{\prod_{2\mid D}2 \pmod 8}_{|d|}\Big)=\chi_8(d \pmod 8)$

$\chi_8(-1)=1$

(4) Follows from (1) (resp. (3)) if $p\neq 2$ (resp. $p=2$).

(5) $2\neq 2 \Rightarrow (D,u)_2=\underbrace{(D/D_2,u)_2}_{1}(D_2,u)_2=\left(\frac{u}{2}\right)^{v_2(D_2)}=\left(\frac{u}{2}\right)=\chi_{D_2}(u \pmod 2)$.

$2=2 \Rightarrow \forall\, 2\neq 2'\mid D \quad D_{2'}\equiv 1 \pmod 4 \Rightarrow (D_{2'},u)_2=1 \Rightarrow (D,u)_2=(D_2,u)_2$ ✗

but $(-4,u)_2=(-1,u)_2=\chi_{-4}(u \pmod 4)$, $(8,u)_2=(2,u)_2=\chi_8(u \pmod 8)$.

Prop. $\forall$ prime $p\nmid D$ $\forall a\in\mathbb{Q}_p^{*}$ $\boxed{(D,a)_p=\chi_D(p)^{v_p(a)}}$.

Pf. $p\neq 2 \Rightarrow (D,a)_p=(D,p^{v_p(a)})_p=\left(\frac{D}{p}\right)^{v_p(a)}$

$p=2 \Rightarrow D=d\equiv \begin{cases}1 \pmod 8 & \Rightarrow D\in\mathbb{Z}_2^{*2},\ (D,a)_2=1=1^{v_2(a)}\\ 5\pmod 8 & \Rightarrow (D,a)_2=(D,2^{v_2(a)})_2=\left(\frac{2}{5}\right)^{v_2(a)}=(-1)^{v_2(a)}\end{cases}$.

Cor. $\underbrace{\{N(I)\mid I\in I(\mathcal{O}_K)\}}_{N(I(\mathcal{O}_K))}=\left\{\prod_p N(\mathfrak{p})^{m_p}\;\middle|\; m_p\in\mathbb{Z}\right\}$

$N(\mathfrak{p})=\begin{cases}p^2 & \chi_D(p)=1\\ p & \chi_D(p)=-1\end{cases}$

$=\left\{a=\prod_p p^{n_p}\;\middle|\; \underbrace{n_p\in\mathbb{Z}}_{2\mid n_p \text{ if } \chi_D(p)=-1}\right\}$

$=\{a\in\mathbb{Q}_{>0}^{*}\mid \forall\, p\nmid D \quad (D,a)_p=1\}$

$\{N(\mathfrak{J})\mid \mathfrak{J}\subset\mathcal{O}_K\}=$ idem with $m_p,n_p\in\mathbb{Z}_{\geq 0}$

$=\{a\in\mathbb{Z}_{>0}\mid \forall\, p\nmid D \quad (D,a)_p=1\}$

Gauss's genus theory (for fundamental discriminants only)

[See J.W.C. Cassels, Rational Quadratic Forms, ch. 14, for the general case]

$K = \mathbb{Q}(\sqrt{d})$, $d \neq 0, 1$ square-free, $D = D_K = \begin{cases} d & d \equiv 1 \pmod 4 \\ 4d & d \equiv 2, 3 \pmod 4 \end{cases}$

Recall: (1) $\mathcal{Cl}^+(D) = \mathrm{Quad}(D)/SL_2(\mathbb{Z}) \xleftrightarrow{\sim} \mathcal{Cl}^+(\mathcal{O}_K) = I(\mathcal{O}_K)/P^+(\mathcal{O}_K)$

$f = f_{I,(\alpha_1,\alpha_2)}(x,y) = \frac{N(\alpha_1 x + \alpha_2 y)}{N(I)}$ $\quad [f] \longleftrightarrow [I]$ $\quad I = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$ (positive basis)

(2) **Group law**: multiplication of ideals

Neutral element $= [\mathcal{O}_K] = [\text{principal form} = \{x^2 + xy + \frac{1-d}{4}y^2,\ x^2 - dy^2\}]$

Inverse: $II' = (N(I)) \Rightarrow [I]^{-1} = [I']$, $N(I') = N(I)$.

$[f]^{-1} = [f_{I,(\alpha_1,\alpha_2)}]^{-1} = [f_{I',(\alpha_2',\alpha_1')}] = [f\left|\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)\right.]$

(3) **If $d > 0$**: $\mathcal{Cl}^+(\mathcal{O}_K) \longrightarrow \mathcal{Cl}(\mathcal{O}_K)$ maps $[f]$ and $[-f\left|\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)\right.]$ to the same class in $\mathcal{Cl}(\mathcal{O}_K)$.

(4) Given $0 \neq \alpha \in I$ with $N_{K/\mathbb{Q}}(\alpha) > 0$, then $(\alpha) \subset I$ and there are bijections

$$\begin{array}{ccc} I_{N>0}/\mathcal{O}^*_{K,N=1} & \xleftrightarrow{\sim} & \{J \subset \mathcal{O}_K \text{ ideal},\ [J] = [I]^{-1}\} \\ \cap & & \cap \\ K^*_{N>0}/\mathcal{O}^*_{K,N=1} & \xleftrightarrow{\sim} & \{J \in I(\mathcal{O}_K),\ [J] = [I]^{-1}\} \\ \downarrow & & \downarrow \\ \alpha \cdot \mathcal{O}^*_{K,N=1} & \longleftrightarrow & J = (\alpha)I^{-1} \end{array}$$

If $\alpha = \alpha_1 u + \alpha_2 v$, then $f_{I,(\alpha_1,\alpha_2)}(u,v) = \frac{N_{K/\mathbb{Q}}(\alpha)}{N(I)} = N(J)$

$\alpha \in I \Longleftrightarrow (u,v) \in \mathbb{Z}^2$

$\alpha \in K \Longleftrightarrow (u,v) \in \mathbb{Q}^2$

Def. For $f \in \mathrm{Quad}(D)$, $S(f) = f(\mathbb{Z}^2) \cap (\mathbb{Z} - \{0\}) \subset S_{\mathbb{Q}}(f) = f(\mathbb{Q}^2) \cap \mathbb{Q}^*$ (#)

$S^+(f) = f(\mathbb{Z}^2) \cap (\mathbb{Z}_{>0}) \subset S^+_{\mathbb{Q}}(f) = f(\mathbb{Q}^*) \cap \mathbb{Q}_{>0}$

these sets depend only on the class $C = [f] \in \mathcal{Cl}^+(D) = \mathcal{Cl}^+(\mathcal{O}_K) \Rightarrow$ we denote them by $S(C)$, $S^+(C)$, $S_{\mathbb{Q}}(C)$, $S^+_{\mathbb{Q}}(C)$, respectively.

Note: The inclusion $S^+(C) \subset (S^+_{\mathbb{Q}}(C) \cap \mathbb{Z})$ is not an equality, in general: we know that $S^+(34x^2 - y^2) \not\ni 1 \in S^+_{\mathbb{Q}}(34x^2 - y^2) \cap \mathbb{Z}$.

Reformulation using (4) above (and $N(J) = N(J')$, $[J'] = [J]^{-1}$):

$S^+(C) = \{N(J) \mid J \subset \mathcal{O}_K \text{ ideal},\ [J] = C\}$

$S^+_{\mathbb{Q}}(C) = \{-\text{''}- \mid \underbrace{J \in I(\mathcal{O}_K),\ -\text{''}-}_{J = J_0(\beta),\ (\beta) \in P^+(\mathcal{O}_K)}\} = N(J_0)\, N(K^*_{N>0})$, for any $J_0 \in I(\mathcal{O}_K)$ such that $[J_0] = C$

Prop. let $f_1, f_2 \in \mathrm{Quad}(D)$, $C_i = [f_i] \in \mathcal{C}\ell^+ = \mathcal{C}\ell^+(D) = \mathcal{C}\ell^+(\mathcal{O}_K)$. Then:

(1) $f_1 \sim f_2$ over $\mathbb{Q} \Longleftrightarrow$ (2) $S_{\mathbb{Q}}(C_1) \cap S_{\mathbb{Q}}(C_2) \neq \emptyset \Longleftarrow$ (3) $S^+_{\mathbb{Q}}(C_1) \cap S^+_{\mathbb{Q}}(C_2) \neq \emptyset$

$\Updownarrow$

(4) $S_{\mathbb{Q}}(C_1) = S_{\mathbb{Q}}(C_2)$

Pf: (1) $\Rightarrow$ (4) $\Rightarrow$ (2) $\Leftrightarrow$ (3) are automatic (note that $\exists\ \alpha \in K^*$ $N_{K/\mathbb{Q}}(\alpha) < 0$ $\Leftrightarrow$ if $d > 0$)

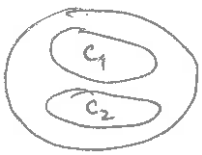
(2) $\Rightarrow$ (1): if $a \in S_{\mathbb{Q}}(C_1) \cap S_{\mathbb{Q}}(C_2) \Rightarrow$ $f_i \sim \langle a, \frac{d(f_i)}{a} \rangle = \langle a, \frac{-D}{a} \rangle$ over $\mathbb{Q}$.

Note: $\forall\ a \in S_{\mathbb{Q}}(f)$ $\forall\ v \in P \cup \{\infty\}$ $c_v(f) = \left(a, \frac{-D}{a}\right)_v = (D, a)_v$.

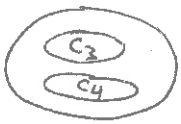
Def. Two classes $C_1 = [f_1]$, $C_2 = [f_2] \in \mathcal{C}\ell^+$ belong to the same genus (notation: $G(C_1) = G(C_2)$) if $\boxed{f_1 \sim f_2 \text{ over } \mathbb{Q}}$

$\overset{\text{Prop.}}{\Longleftrightarrow}$ $S^+_{\mathbb{Q}}(C_1) = S^+_{\mathbb{Q}}(C_2)$. Let Gen = the set of all genera.

By definition, $\mathcal{C}\ell^+ \longrightarrow \mathrm{Gen}$, $C \longmapsto G(C)$ is surjective.



$G(C_1) = G(C_2)$



$G(C_3) = G(C_4)$

Notation: $S^+_{\mathbb{Q}}(G) = S^+_{\mathbb{Q}}(C)$ for any $C \in \mathcal{C}\ell^+$ such that $G(C) = G$ $(G \in \mathrm{Gen})$

Rmk. This definition of Gen is correct only for discriminants that are fundamental (or not too far from being fundamental). For general $\Delta \equiv 0, 1 \pmod 4$ $(\sqrt{\Delta} \notin \mathbb{Z})$, $[f_1], [f_2] \in \mathcal{C}\ell^+(\Delta)$ are in the same genus $\Longleftrightarrow$ $f_1 \sim f_2$ over $\mathbb{R}$ (automatic) and over all $\mathbb{Z}_p$ (it does not matter if we consider proper or improper equivalence over $\mathbb{Z}_p$, since $\exists\ U \in GL_2(\mathbb{Z}_p)$ with $\det(U) = -1$ and $f_1 | U = f_1$).

Note: (1) $\bigcup_{C \in \mathcal{C}\ell^+} S^+_{\mathbb{Q}}(C)$ $\left(= \bigcup_{G \in \mathrm{Gen}} S^+_{\mathbb{Q}}(G)\right.$ disjoint union$\left.\right)$ is equal to

$$N(I(\mathcal{O}_\Delta)) = \{N(J) \mid J \in I(\mathcal{O}_K)\} = \{a \in \mathbb{Q}^*_{>0} \mid \forall\ p \nmid D\ \ (D, a)_p = 1\}$$

$\Updownarrow$

$2 \mid v_p(a)$ $\forall\ p$ such that $\chi_D(p) = -1$

(2) $\bigcup_C S^+(C) = \{N(J) \mid J \subset \mathcal{O}_K,\ J \neq (0)\} = \{a \in \mathbb{Z}_{>0} \mid$ — " — $\} = \mathbb{Z}_{>0} \cap \bigcup_C S^+_{\mathbb{Q}}(C)$

(3) $\forall\ G \in \mathrm{Gen}$

$$\boxed{\bigcup_{C \in G} S^+(C) = \mathbb{Z}_{>0} \cap S^+_{\mathbb{Q}}(G)}$$

(since $S^+_{\mathbb{Q}}(G_1) \cap S^+_{\mathbb{Q}}(G_2) = \emptyset$ if $G_1 \neq G_2$)

(1) $S_{\mathbb{Q}}^+(G) = N(J_0)\, N(K^*_{N>0})$, for any $J_0 \in I(\mathcal{O}_K)$ such that $G([J_0]) = G$

Conclusion : (1) the surjective group morphism induced by the norm of ideals

$$\begin{aligned} Cl^+ = I(\mathcal{O}_K)/P^+(\mathcal{O}_K) &\xrightarrow{\overline{N}} N(I(\mathcal{O}_K))/N(K^*_{N>0}) \\ [J] &\longmapsto N(J)\cdot N(K^*_{N>0}) \\ C &\longmapsto S_{\mathbb{Q}}^+(C)/N(K^*_{N>0}) \end{aligned}$$

identifies Gen with the quotient group $N(I(\mathcal{O}_K))/N(K^*_{N>0}) = Cl^+/\mathrm{Ker}(\overline{N})$.

(2) $G(C_1) = G(C_2) \iff C_1 C_2^{-1} \in \mathrm{Ker}(\overline{N}) = \underbrace{G(\text{principal class } [\mathcal{O}_K])}_{\text{the principal genus}}$

$\Rightarrow$ each genus is a coset of $\mathrm{Ker}(\overline{N})$ $\Rightarrow$ it contains $|\mathrm{Ker}(\overline{N})|$ classes.

Def : $\mathrm{Ram} = \{\text{primes } \mathfrak{p} \text{ that ramify in } K/\mathbb{Q}\} = \{\mathfrak{p} \mid D\}$, $t = |\mathrm{Ram}| \geq 1$.

Genus characters : the Hilbert symbols

$$(D,\cdot)_v : \mathbb{Q}^*/N_{K/\mathbb{Q}}(K^*) \longrightarrow \{\pm 1\}, \quad a \longmapsto (D,a)_v \qquad (v \in Pu\{\infty\})$$

give rise to the following diagram

$$\begin{array}{ccccccc} Cl^+ = I/P^+ & \xrightarrow{\overline{N}} & \overbrace{N(I)/N(K^*_{N>0})}^{\text{Gen}} & \subset & \mathbb{Q}^*_{>0}/N(K^*_{N>0}) & \ni & a \\ [\mathfrak{f}] & & e \downarrow ((\mathfrak{p}D,\cdot)_{\mathfrak{p}}) & & e' \downarrow ((D,\cdot)_v) & & \downarrow \\ & \searrow^{e\circ\overline{N}} & \left(\bigoplus_{\mathfrak{p}\mid D}\{\pm 1\}\right)\times\{1\} & \subset & \bigoplus_{v\in Pu\{\infty\}} \underbrace{\text{“}\mathbb{Q}_v^*/N(K_v^*)\text{”}}_{\{\pm 1\}} & \ni & (e'_v(a) = (D,a)_v)_v \\ & & & & & & \| \\ & & & & & & c_{\mathfrak{f}}(f) = (D,b)_v \\ & & & & & & b \in S_{\mathbb{Q}}(f) \end{array}$$

We know : (1) $N(I(\mathcal{O}_K)) = \mathrm{Ker}\left(\mathbb{Q}^*_{>0} \xrightarrow{((D,\cdot)_p)} \bigoplus_{p\mid D}\{\pm 1\}\right)$

(2) Legendre's thm $\iff$ $\forall d$ $\mathrm{Ker}(e') = 0 \overset{(1)}{\iff} \forall d$ $\mathrm{Ker}(e) = 0$.

(3) Product formula for the Hilbert symbol $\Rightarrow$ $\forall a \in \mathbb{Q}^*$ $\prod_v (D,a)_v = 1$

$\Rightarrow$ $\forall G \in \mathrm{Gen}$ $\prod_{\mathfrak{p}\mid D} \underbrace{e_{\mathfrak{p}}(G)}_{(D,a)_{\mathfrak{p}} \text{ for any } a \in S_{\mathbb{Q}}^+(G)} = 1$ $\qquad ((D,a)_\infty = 1 \text{ if } a>0)$

$\Rightarrow$ e induces an injective morphism

$$\overline{e} : \mathrm{Gen} \hookrightarrow \mathrm{Ker}\left(\bigoplus_{\mathfrak{p}\mid D}\{\pm 1\} \xrightarrow{\text{product}} \{\pm 1\}\right) \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$$

Main Thm of genus theory (Gauss)

(1) $\mathrm{Ker}(\overline{N}) = (Cl^+)^2$, hence $\overline{N}$ induces an isomorphism $Cl^+/(Cl^+)^2 \xrightarrow{\sim} Gen$.

(2) $\overline{e}: Gen \xrightarrow{\sim} \mathrm{Ker}\left(\bigoplus_{2|D} \{\pm 1\} \xrightarrow{\text{prod}} \{\pm 1\}\right)$ is an isomorphism.

Cor 1. There are 2^{t-1} genera; each of them contains $|(Cl^+)^2|$ classes.

Cor 2. Each genus contains only one class $\iff Cl^+ \simeq (\mathbb{Z}/2\mathbb{Z})^k$ $(k = t-1)$.

Cor 3 $\forall\, G \in Gen$ $\quad S^+_{\mathbb{Q}}(G) = \{a \in \mathbb{Q}^*_{>0} \mid \forall\, p \in \mathcal{P}\ \ (D, a)_p = e_p(G)\ \ (=1 \text{ if } p \nmid D)\}$

$\bigcup_{C \in G} S^+(C) = \mathbb{Z}_{>0} \cap S^+_{\mathbb{Q}}(G) = \{a \in \mathbb{Z}_{>0} \mid \forall\, p \text{ such that } \chi_D(p) = -1 \quad 2 \mid v_p(a)$

$\forall\, q \mid D \quad \underbrace{(D, a)_q}_{\chi_{D_q}(a) \text{ if } \gcd(a, D) = 1} = e_q(G)\}$

Cor 4. $\forall\, G \in Gen$ If $p \nmid 2D$ is a prime, then:

$$p \in \bigcup_{C \in G} S^+(C) \iff \begin{cases} \left(\frac{d}{p}\right) = 1 \\ \forall\, q \mid D \quad \left(\frac{D_q}{p}\right) = e_q(G) \end{cases}$$

Cor 5. $2 \nmid |Cl^+| \iff t = 1 \iff D = \pm$ power of a prime q

$$\iff \begin{cases} d = -1, -2, -q & q \equiv 3 \pmod 4 \text{ prime} \\ d = 2, q & q \equiv 1 \pmod 4 \text{ prime} \end{cases}$$

($\Rightarrow$ if $q \equiv 1 \pmod 4$ prime, then $N(\varepsilon) = -1$, ε = fund. unit of $\mathbb{Z}\left[\frac{1+\sqrt{q}}{2}\right]$)

Rmk: $(Cl^+)^2 \subset \mathrm{Ker}(\overline{N})$, for trivial reasons: $\forall\, I \in I(\mathcal{O}_K)$

$N(I^2) = N(I)^2 = N_{K/\mathbb{Q}}(N(I)) \in N(K^*_{N>0})$.

Gauss's proof: (A) "Fundamental formula": $\quad |Cl^+[2]| = 2^{t-1}$

($\Rightarrow |(Cl^+)/(Cl^+)^2| = 2^{t-1} \Rightarrow |\underbrace{\mathrm{Im}(e \circ \overline{N})}_{\text{quotient of } Cl^+/(Cl^+)^2}| \leq 2^{t-1} \Rightarrow$ $\exists$ non-trivial relation between the e_q's $\Downarrow$ QRL (see below))

(B) $\mathrm{Ker}(e \circ \overline{N}) = (Cl^+)^2$ ("Duplication theorem")

($\iff \mathrm{Ker}(\overline{N}) = (Cl^+)^2$ and $\underbrace{\mathrm{Ker}(e) = 0}_{\text{Legendre's thm}}$)

Gauss's proof of the duplication thm relied on a very ingenious use of indefinite quadratic forms of dim = 3 and their reduction theory. See [Cassels, ch. 14] for a proof involving only binary quadratic forms.

Rk: An abstract version of (A) is one of the basic building blocks of class field theory.

Ex: $K = \mathbb{Q}(\sqrt{-26})$, $d = -26$, $D = -104 = (-8)\cdot 13$

Minkowski's bound: every $C \in Cl_K = Cl(\mathcal{O}_K) = Cl^+(\mathcal{O}_K)$ contains an ideal $I \subset \mathcal{O}_K = \mathbb{Z}[i\sqrt{26}]$ with $N(I) \le \frac{2}{\pi}\sqrt{104} < 7$.

Factorisation of small primes: $(2) = P^2$, $P = (2, i\sqrt{26})$, $(3) = Q\overline{Q}$, $(5) = R\overline{R}$

$Q = (3, 1+i\sqrt{26})$, $\overline{Q} = (3, 1-i\sqrt{26})$, $R = (5, 2+i\sqrt{26})$, $\overline{R} = (5, 2-i\sqrt{26})$

$N(P) = 2$, $N(Q) = 3$, $N(R) = 5$ $\qquad [P]^2 = 1$, $[\overline{Q}] = [Q]^{-1}$, $[\overline{R}] = [R]^{-1}$

$\Rightarrow Cl_K$ is generated by $[P]$, $[Q]$, $[R]$.

$2\cdot 3\cdot 5 = 30 = 2^2 + 26\cdot 1^2 = N((2+i\sqrt{26}))$ $\qquad [R] = [P]^{-1}[Q] = [PQ]$ (⇑)

$2+i\sqrt{26} \in P, \overline{Q}, R \Rightarrow \underbrace{P\overline{Q}R}_{N(\ )} \mid (2+i\sqrt{26}) \Rightarrow P\overline{Q}R = (2+i\sqrt{26})$, $\quad N(\ ) = N(\ ) = 30$

$Q^2 = (9, 6+6i\sqrt{26}, -25+2i\sqrt{26}) = (9, 2+2i\sqrt{26})$ $\qquad [Q]^3 = 1$ (⇑)

$Q^3 = (27, 6+6i\sqrt{26}, 9+9i\sqrt{26}, -50+4i\sqrt{26}) = (3+3i\sqrt{26}, 4+4i\sqrt{26}) = (1+i\sqrt{26})$

$N_{K/\mathbb{Q}}(u+vi\sqrt{26}) = u^2+26v^2 \neq 2, 3 \Rightarrow [P] \neq 1 \neq [Q]$ $\qquad u+vi\sqrt{26} \in \mathbb{Z}[i\sqrt{26}]$

Conclusion: $Cl_K \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$

($\mathbb{Z}/2\mathbb{Z}$ gen. by $[P]$; $\mathbb{Z}/3\mathbb{Z}$ gen. by $[Q]$; $\mathbb{Z}/6\mathbb{Z}$ gen. by $[PQ] = [R]$)

Equivalent description of $Cl_K \simeq Cl^+(-104) = Cl(-104)$:

reduced forms of $\Delta = -104$: $[a, b, c]$, $|b| \le a \le c$, $104 = 4ac - b^2$,

$2 \mid b$, $1 \le a \le \sqrt{\frac{104}{3}} < 6 \Rightarrow |b/2| = 0, 1, 2$

$b=0$: $[1, 0, 26]$, $[2, 0, 13]$ $\qquad |b|=2$: $[3, \pm 2, 9]$ $\qquad |b| = 4$: $[5, \pm 4, 6]$

Genus characters:

$e_2 = (-26, \cdot)_2$	1	$(-26, 2)_2 = -1$	$(-26, 9)_2 = 1$	$(-26, 5)_2 = -1$
$e_{13} = (-26, \cdot)_{13}$	1	$(-26, 2)_{13} = \left(\frac{2}{13}\right) = -1$	$(-26, 9)_{13} = 1$	$(-26, 5)_{13} = \left(\frac{5}{13}\right) = -1$

$\Rightarrow$ **2** genera, each containing **3** classes:

$\{[1, 0, 26], [3, \pm 2, 9]\}$ — principal genus

represents primes $p \neq 2, 13$ such that

$\left(\frac{-8}{p}\right) = 1$ ($p \equiv 1, 3 \pmod 8$), $\quad \left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) = 1$ ($p \equiv \pm 1, \pm 3, \pm 4 \pmod{13}$)

$\{[2, 0, 13], [5, \pm 4, 6]\}$ — the other genus

represents primes $p \neq 2, 13$ such that

$\left(\frac{-8}{p}\right) = -1$ ($p \equiv 5, 7 \pmod 8$), $\quad \left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) = -1$ ($p \equiv \pm 2, \pm 5, \pm 6 \pmod{13}$)

Ex: $K=\mathbb{Q}(\sqrt{-21})$, $d=-21$, $D=-84=(-4)(-3)(-7)$, $t=3$, $|Gen|=2^{t-1}=4$

reduced forms of $\Delta=-84$: $[1,0,21]$, $[3,0,7]$, $[2,2,11]$, $[5,4,5]$ $\Rightarrow |Cl|=4$

$\Rightarrow$ $Cl \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, every genus contains one class $(=|Cl^+|)$

genus characters:

	$[1,0,21]$	$[3,0,7]$	$[2,2,11]$	$[5,4,5]$
$(-84,\cdot)_2=(3,\cdot)_2$	1	$(3,3)_2=-1$	$(3,2)_2=-1$	$(3,5)_2=1$
$(-84,\cdot)_3=(-3,\cdot)_3$	1	$(-3,3)_3=1$	$(-3,2)_3=-1$	$(-3,5)_3=-1$
$(-84,\cdot)_7=(7,\cdot)_7$	1	$(7,3)_7=\left(\frac{3}{7}\right)=-1$	$(7,2)_7=1$	$(7,5)_7=-1$

A prime $p\neq 2,3,7$ is represented by:

$[1,0,21] \Leftrightarrow \left(\frac{-1}{p}\right)=\underbrace{\left(\frac{-3}{p}\right)}_{\left(\frac{p}{3}\right)}=\underbrace{\left(\frac{-7}{p}\right)}_{\left(\frac{p}{7}\right)}=1 \Leftrightarrow \begin{matrix} p\equiv 1 \pmod{12} \\ p\equiv 1,2,4 \pmod 7 \end{matrix} \Leftrightarrow p\equiv 1,25,37 \pmod{84}$

$[3,0,7] \Leftrightarrow \left(\frac{-1}{p}\right)=\left(\frac{p}{7}\right)=-1,\ \left(\frac{p}{3}\right)=1 \Leftrightarrow \begin{matrix} p\equiv 7 \pmod{12} \\ p\equiv 3,5,6 \pmod 7 \end{matrix} \Leftrightarrow p\equiv 19,31,55 \pmod{84}$

$[2,2,11] \Leftrightarrow \left(\frac{-1}{p}\right)=\left(\frac{p}{3}\right)=-1,\ \left(\frac{p}{7}\right)=1 \Leftrightarrow \begin{matrix} p\equiv -1 \pmod{12} \\ p\equiv 1,2,4 \pmod 7 \end{matrix} \Leftrightarrow p\equiv 11,23,71 \pmod{84}$

$[5,4,5] \Leftrightarrow \left(\frac{-1}{p}\right)=1,\ \left(\frac{p}{3}\right)=\left(\frac{p}{7}\right)=-1 \Leftrightarrow \begin{matrix} p\equiv 5 \pmod{12} \\ p\equiv 3,5,6 \pmod 7 \end{matrix} \Leftrightarrow p\equiv 5,17,41 \pmod{84}$

Ex: $K=\mathbb{Q}(\sqrt{15})$, $d=15$, $D=60=(-4)(-3)5$, $t=3$, $|Gen|=2^{t-1}=4$

We know: $|Cl^+|=4$, $N(\varepsilon)=1$, $|Cl|=2$, $Cl^+=Gen$

Four classes of reduced cycles: $[1,6,-6] \hookleftarrow [-6,6,1]$ $(\sim[1,0,-15])$

$[2,6,-3] \hookrightarrow [-3,6,2]$ $(\sim[-3,0,5])$ $\quad [-1,6,6] \hookleftarrow [6,6,-1]$ $(\sim[-1,0,15])$

$[-2,6,3] \hookrightarrow [3,6,-2]$ $(\sim[3,0,-5])$

same class in Cl (for $[1,0,-15]$, $[-1,0,15]$); same class in Cl (for $[3,0,-5]$, $[-3,0,5]$)

Genus characters:

	$[1,0,-15]$	$[-1,0,15]$	$[3,0,-5]$	$[-3,0,5]$
$(60,\cdot)_2=(-1,\cdot)_2$	1	$(-1,-1)_2=-1$	-1	$(-1,-3)_2=1$
$(60,\cdot)_3=(-3,\cdot)_3$	1	$(-3,-1)_3=-1$	1	$(-3,-3)_3=-1$
$(60,\cdot)_5=(15,\cdot)_5$	1	$(15,-1)_5=1$	-1	$(15,-3)_5=-1$

$p\neq 2,3,5$ prime: $p=x^2-15y^2 \Leftrightarrow \left(\frac{-1}{p}\right)=\underbrace{\left(\frac{-3}{p}\right)}_{\left(\frac{p}{3}\right)}=\left(\frac{5}{p}\right)=1 \Leftrightarrow p\equiv 1,49 \pmod{60}$ $(p\equiv 1,-11 \pmod{60})$

$p=-x^2+15y^2 \Leftrightarrow \left(\frac{-1}{p}\right)=\left(\frac{p}{3}\right)=-1,\ \left(\frac{p}{5}\right)=1 \Leftrightarrow p\equiv -1,11 \pmod{60}$

$p=3x^2-5y^2 \Leftrightarrow \left(\frac{-1}{p}\right)=\left(\frac{p}{5}\right)=-1,\ \left(\frac{p}{3}\right)=1 \Leftrightarrow p\equiv 7,-17 \pmod{60}$

$p=-3x^2+5y^2 \Leftrightarrow \left(\frac{p}{3}\right)=\left(\frac{p}{5}\right)=-1,\ \left(\frac{-1}{p}\right)=1 \Leftrightarrow p\equiv -7,17 \pmod{60}$

Exercise: (1) $d=34$, $D=4\cdot 34=8\cdot 17 \Rightarrow$ $Cl^+\simeq \mathbb{Z}/4\mathbb{Z}$, $Cl\simeq \mathbb{Z}/2\mathbb{Z}$, $Gen\simeq \mathbb{Z}/2\mathbb{Z}$

same image in Cl: $[1,0,-34]$, $[-1,0,34]$ — principal genus — represents primes $p\neq 2,17$ such that $\left(\frac{2}{p}\right)=1$, $\left(\frac{17}{p}\right)=\left(\frac{p}{17}\right)=1$

$[3,2,-11]$, $[-3,2,11]$ — same image in Cl — the other genus — $\left(\frac{2}{p}\right)=-1$, $\left(\frac{p}{17}\right)=-1$

---

(2) $d=79$, $D=4\cdot 79 \Rightarrow$ $Cl^+\simeq \mathbb{Z}/6\mathbb{Z}$, $Cl\simeq \mathbb{Z}/3\mathbb{Z}$, $Gen\simeq \mathbb{Z}/2\mathbb{Z}$

$D=(-4)(-79)$

$[1,0,-79]$ ← same image in Cl → $[-1,0,79]$

$[-3,2,26]$ — " —

$[-3,-2,26]$ — " —

principal genus

represents primes $p\neq 2,79$ such that $\left(\frac{-1}{p}\right)=1$, $\left(\frac{-79}{p}\right)=\left(\frac{p}{79}\right)=1$

$[3,2,-26]$

$[3,-2,-26]$

the other genus

— " —

$\left(\frac{-1}{p}\right)=-1$, $\left(\frac{p}{79}\right)=-1$

---

(3) $d=82$, $D=4\cdot 82=8\cdot 41 \Rightarrow$ $Cl^+=Cl\simeq \mathbb{Z}/4\mathbb{Z}$, $Gen\simeq \mathbb{Z}/2\mathbb{Z}$

$[1,0,-82]$

$[2,0,-41]$

principal genus

represents primes $p\neq 2,41$ such that $\left(\frac{2}{p}\right)=1$, $\left(\frac{41}{p}\right)=\left(\frac{p}{41}\right)=1$

$[3,2,-27]$

$[3,-2,-27]$

the other genus

— " —

$\left(\frac{2}{p}\right)=-1$, $\left(\frac{p}{41}\right)=-1$

---

4) Which primes can be written as $p=x^2-11y^2$?

Which ones as $p=-x^2+11y^2$?

Proof of $\ker(\overline{N}) = (Cl^+)^2$: $(\supseteq)$ known already

$(\subseteq)$ If $J \in I(\mathcal{O}_\Delta)$ and $N(J) = N_{K/\mathbb{Q}}(\alpha)$ for some $\alpha \in K^* \Rightarrow I = J(\alpha)^{-1} \in I(\mathcal{O}_\Delta)$ satisfies $[I] = [J]$ and $N(I) = 1$. Factorise I as a product of powers of prime ideals: $I = \prod_{\mathfrak{P}} \mathfrak{P}^{n_\mathfrak{P}}$ $(n_\mathfrak{P} \in \mathbb{Z}) \Rightarrow 1 = N(I) = \prod_{\mathfrak{P}} N(\mathfrak{P})^{n_\mathfrak{P}}$, $\mathfrak{P} \mid p$.

If $\mathfrak{P}$ is ramified or inert $\Rightarrow N(\mathfrak{P}) = p$ or p^2 and $p \nmid N(\mathfrak{Q})$ for $\mathfrak{Q} \neq \mathfrak{P}$
$\Rightarrow n_\mathfrak{P} = 0$.

If $\mathfrak{P}$ is split in $K/\mathbb{Q} \Rightarrow (p) = \mathfrak{P}\mathfrak{P}'$ and $p \nmid N(\mathfrak{Q})$ for $\mathfrak{Q} \neq \mathfrak{P}, \mathfrak{P}'$
$N(\mathfrak{P}) = N(\mathfrak{P}') = p \Rightarrow n_\mathfrak{P} + n_{\mathfrak{P}'} = 0$.

Therefore $I = \prod_{\mathfrak{P} \neq \mathfrak{P}'} (\mathfrak{P}\mathfrak{P}'^{-1})^{n_\mathfrak{P}} = \prod_{\mathfrak{P} \neq \mathfrak{P}'} (\mathfrak{P}^2/\mathfrak{P}\mathfrak{P}')^{n_\mathfrak{P}} = \left(\prod_{\mathfrak{P} \neq \mathfrak{P}'} \mathfrak{P}^{n_\mathfrak{P}}\right)^2 \prod_{\mathfrak{P} \neq \mathfrak{P}'} (p)^{-n_\mathfrak{P}}$
$\Rightarrow [I] \in (Cl^+)^2$.

Proof of the fact that $\overline{e}: Gen \longrightarrow \ker\left(\bigoplus_{\ell \mid D} \{\pm 1\} \xrightarrow{\text{prod}} \{\pm 1\}\right)$ is surjective:

given $e_\ell \in \{\pm 1\}$ for all $\ell \mid D$ such that $\prod_{\ell \mid D} e_\ell = 1$, there exist $a_\ell \in \mathbb{Z}_{>0}$ prime to 2ℓ such that $e_\ell = \left(\frac{D_\ell}{a_\ell}\right) = (D, a_\ell)_\ell \overset{CRT}{\Rightarrow} \exists a \in \mathbb{Z}_{>0}$

$a \equiv a_\ell \pmod{|D_\ell|}$ $\forall \ell \mid D$ $(\gcd(a, 2|D|) = 1)$.

Dirichlet's thm on primes $\Rightarrow \exists$ prime $\ell \equiv a \pmod{2|D|}$. $(\ell \neq 2)$

Hilbert's symbol
$$(D, \ell)_\nu = \begin{cases} 1 & \nu = \infty \quad (\ell > 0) \\ e_\ell & \nu = \ell \mid D \quad (\ell^{-1} a_\ell \in \mathbb{Z}_\ell^{*2}) \\ 1 & \nu = p \nmid 2D\ell \quad (v_p(D) = v_p(\ell) = 0) \\ 1 & \nu = 2 \nmid D \quad (D \equiv 1 \pmod 4) \end{cases}$$

QRL $\Rightarrow (D, \ell)_\ell^{-1} = \prod_{\nu \neq \ell} (D, \ell)_\nu = \prod_{\ell \mid D} e_\ell = 1 \Rightarrow (D, \ell)_\ell = 1$.

As $\forall p \nmid D$ $(D, \ell)_p = 1$, $\ell = N(J)$ for some $J \in I(\mathcal{O}_K)$

$\Rightarrow e(N(J)) = \{(e_\ell)\}_{\ell \mid D}$.

As $\ker(\overline{e}) = 0$ by Legendre's thm $\Rightarrow \overline{e}$ is an isomorphism.

Rmk: the above proof is not very satisfactory. After all, Gauss did not have Dirichlet's thm at his disposal. What is more serious is the fact that some proofs of Dirichlet's thm (notably, Selberg's "elementary" proof) rely on genus theory! For this reason we give another proof, based on Gauss's Fundamental formula and Legendre's thm (but not on QRL, which is deduced from the formula).

Proof of Gauss's formula $|Cl^+/(Cl^+)^2| = |Cl^+[2]| = 2^{t-1}$

Lemma 1. $G \xrightarrow{f} H$ morphism of finite abelian groups
$\Rightarrow$ $|\ker(f)| \cdot |G|^{-1} \cdot |H| \cdot |\mathrm{Coker}(f)|^{-1} = 1$ ($\mathrm{Coker}(f) = H/\mathrm{Im}(f)$)

(the sequence $0 \to \ker(f) \to G \xrightarrow{f} H \to \mathrm{Coker}(f) \to 0$ — the cokernel of f is exact)

Pf: $G/\ker(f) \xrightarrow{\sim} \mathrm{Im}(f) \Rightarrow |G|/|\ker(f)| = |\mathrm{Im}(f)| = |H|/|\mathrm{Coker}(f)|$.

Cor. $|G[2]| = |G/G^2|$ (take $G \xrightarrow{f} G$, $f(g) = g^2$)

Lemma 2. Each class in $Cl^+[2]$ contains an ideal $I \in I(\mathcal{O}_K)$ such that $I = I'$ (conversely, if $I = I'$, then $[I] = [I'] = [I]^{-1}$) $\Rightarrow [I]^2 = 1$.

Pf. If $J \in I(\mathcal{O}_K)$, $J^2 = (\beta)$, $N_{K/\mathbb{Q}}(\beta) > 0$, then $JJ' = (N(J))$ implies that $J' = J^{-1}(N(J)) = J(\alpha)$, $\alpha = N(J)/\beta$, $N_{K/\mathbb{Q}}(\alpha) > 0$
$\Rightarrow$ $J = J'(\alpha')$, $JJ' = JJ'(\alpha\alpha')$, $\alpha\alpha' \in \mathcal{O}_K^* \cap \mathbb{Q}_{>0} = \{1\}$.
If $d > 0$, after replacing α by $\pm\alpha$ can assume $\sigma_1(\alpha) > 0$.
Hilbert's Thm 90 $\Rightarrow$ $\exists\, \gamma \in K^*$ $\alpha = \gamma/\gamma' \Rightarrow N_{K/\mathbb{Q}}(\gamma) = \gamma\gamma' = \alpha\gamma'^2 \in \mathbb{Q}^*$.
If $d > 0$ $\Rightarrow$ $N_{K/\mathbb{Q}}(\gamma) = \sigma_1(N_{K/\mathbb{Q}}(\gamma)) = \sigma_1(\alpha)\sigma_1(\gamma')^2 > 0$. Therefore $I = J(\gamma)$ satisfies $[I] = [J]$ and $I' = J'(\gamma') = J(\gamma) = I$.

Lemma 3. Each class in $Cl^+[2]$ contains an ideal of the form $\prod_{q \mid D} Q^{c_q}$, $c_q \in \{0,1\}$, $(q) = Q^2$.

Pf: If $I = I'$ is as in Lemma, unique factorisation into ideals implies that
$$I = \prod_{\substack{p \text{ splits} \\ (p) = P\mathfrak{P}'}} \underbrace{(P\mathfrak{P}')}_{(p)}{}^{a_p} \prod_{\substack{p \text{ inert} \\ (p) = P}} \underbrace{P}_{(p)}{}^{b_p} \prod_{\substack{q \text{ ramified} \\ (q) = Q^2}} Q^{c_q + 2d_q} \qquad c_q \in \{0,1\}$$
$$= (\alpha) \prod_{q \mid D} Q^{c_q}, \quad \alpha \in \mathbb{Q}^* \quad (\Rightarrow N_{K/\mathbb{Q}}(\alpha) = \alpha^2 > 0)$$

Cor. The group morphism
$$\bigoplus_{q \mid D} \mathbb{Z}/2\mathbb{Z} \xrightarrow{f} Cl^+[2], \qquad (a_q \pmod 2) \longmapsto \Big[\prod_{q \mid D} Q^{a_q}\Big]$$
is surjective.
$\Rightarrow$ $|Cl^+[2]| = 2^t/|\ker(f)|$.

It remains to investigate $\ker(f)$, i.e., relations of the form $Q_1 \cdots Q_k = (\alpha)$, $N_{K/\mathbb{Q}}(\alpha) > 0$ $Q_i^2 = (q_i)$ (*)
$\emptyset \neq \{q_1, \dots, q_k\} \subset \mathrm{Ram} = \{q \mid D\}$.

Lemma 4. $|\mathrm{Ker}(f)| \le 2$

Pf. We must show that $\{\mathfrak{q}_1, \dots, \mathfrak{q}_k\} \subset \mathrm{Ram}$ in (*) are unique (if they exist). As $(\alpha') = \mathfrak{Q}_1' \cdots \mathfrak{Q}_k' = (\alpha)$ and $(\alpha^2) = (\mathfrak{q}_1 \cdots \mathfrak{q}_k)$, we have

$\alpha' = \alpha\eta$, $\eta \in \mathcal{O}_K^*$ $\Rightarrow$ $\alpha = \alpha'\eta'$, $\eta\eta' = 1$, $\alpha^2 = N_{K/\mathbb{Q}}(\alpha)\eta = \mathfrak{q}_1 \cdots \mathfrak{q}_k \eta$

If $d < 0$: can assume $d \neq -1, -3$ ($\alpha = 0$ for $d = -1, -3$) $\Rightarrow$ $\eta = \pm 1$.

If $\eta = 1 \Rightarrow \alpha \in \mathbb{Q}^*$, $\mathfrak{q}_1 \cdots \mathfrak{q}_k \in \mathbb{Q}^{*2} \Rightarrow k = 0$ false
If $\eta = -1 \Rightarrow \alpha \in \mathbb{Q}^*\sqrt{d} \Rightarrow \mathfrak{q}_1 \cdots \mathfrak{q}_k = |d|$
} uniqueness

If $d > 0$: $\mathcal{O}_K^* = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$. Replacing α by $\alpha\varepsilon^i$ changes η to $\eta\varepsilon^{-2i}$.

For each $\sigma_j : K \hookrightarrow \mathbb{R}$ $\quad \sigma_j(\mathfrak{q}_1 \cdots \mathfrak{q}_k \eta) = \sigma_j(\alpha)^2 > 0 \quad (\sigma_j(\varepsilon) > 0)$

If $N(\varepsilon) = -1$: can replace $\alpha \longmapsto \alpha\varepsilon^{2\mathbb{Z}}$, $\eta \longmapsto \eta\varepsilon^{4\mathbb{Z}}$; modulo this transformation, the only possibilities with $\sigma_j(\eta) > 0$ are $\eta = 1, \varepsilon^2$ $\Rightarrow$ result,
~~since~~ since $\eta = 1$ impossible (as above), $\eta = \varepsilon^2$ $\Rightarrow$

$\mathfrak{q}_1 \cdots \mathfrak{q}_k = (\alpha/\varepsilon)^2 \in (\mathbb{Q}^{*2} \cap K^{*2}) \setminus \mathbb{Q}^{*2} = d\mathbb{Q}^{*2} \Rightarrow \mathfrak{q}_1 \cdots \mathfrak{q}_k = d$.

If $N(\varepsilon) = 1$: can replace $\alpha \longmapsto \alpha\varepsilon^{\mathbb{Z}}$, $\eta \longmapsto \eta\varepsilon^{2\mathbb{Z}}$, are left with $\eta = 1$ (impossible), $\eta = \varepsilon$ $\Rightarrow$ determines α up to $\mathbb{Q}^*$ $\Rightarrow$ $\mathfrak{q}_1 \cdots \mathfrak{q}_k$ up to $\mathbb{Q}^{*2}$ $\Rightarrow$ uniqueness.

Lemma 5. $\mathrm{Ker}(f) \neq 0$.

Pf. We must show that a relation (*) exists. Note that

$\prod_{\mathfrak{q} \mid d} \mathfrak{q} = d$, $(\sqrt{d}) = \prod_{\mathfrak{q} \mid d} \mathfrak{Q}$, but $N_{K/\mathbb{Q}}(\sqrt{d}) = -d > 0$ only if $d < 0$ ($\Rightarrow$ result if $d < 0$).

If $d > 0$, $N(\varepsilon) = -1$: $\prod_{\mathfrak{q} \mid d} \mathfrak{Q} = (\varepsilon\sqrt{d})$, $N_{K/\mathbb{Q}}(\varepsilon\sqrt{d}) = d > 0$ $\Rightarrow$ result.

If $d > 0$, $N(\varepsilon) = 1$: this is the most interesting case, when (*) comes from a "descent" applied to ε. The fundamental unit of $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_K$ also has $N(-) = 1$.

[**Ex:** $d = 6$, $N(2+\sqrt{6}) = -2$
$(2+\sqrt{6})^2 = (2\varepsilon) = (2)$, $\varepsilon = 5+4\sqrt{6}$]

The calculation on the following page produces a positive square-free divisor of D of the form $2d_i$ (resp. $d_i \neq 1$) such that $(2d_i)$ (resp. $(d_i) \neq (1)$) is of the form $(\beta)^2$;

$N_{K/\mathbb{Q}}(\beta) > 0$ $\Rightarrow$ $\mathfrak{q}_1 \cdots \mathfrak{q}_k = 2d_i$ (resp. d_i) satisfies

$$\mathfrak{Q}_1 \cdots \mathfrak{Q}_k = (\beta).$$

---

this completes the proof of $|Cl^+/(Cl^+)^2| = 2^{t-1}$.

Fundamental units and elements of norm dividing Δ

$d > 1$, square-free ($\Rightarrow \sqrt{d} \notin \mathbb{Z}$)

ε = fundamental unit of $\mathbb{Z}[\sqrt{d}]$, $\varepsilon = x + y\sqrt{d}$ $\quad (x, y > 1)$

Assume: $N(\varepsilon) = x^2 - dy^2 = +1$

the factorisation $(x+1)(x-1) = x^2 - 1 = dy^2$ has the following consequences.

Case 1: $2 \mid x$ ($\Rightarrow 2 \nmid y$, $y^2 \equiv 1 \pmod 8$, $d \equiv 3 \pmod 4$) $\qquad \mathbb{Z}[\sqrt{d}] = \mathcal{O}_\Delta$, $\Delta = 4d$

$\gcd(x+1, x-1) = 1 \Rightarrow$ $\quad x+1 = d_1 u^2$, $\quad x-1 = d_2 v^2$ $\quad d_1 d_2 = d$, $\ uv = y$

$\Rightarrow \underline{d_1 u^2 - d_2 v^2 = 2}$, $\quad \underbrace{(d_1 u)^2 - d v^2}_{N(d_1 u + v\sqrt{d})} = 2d_1$, $\quad \underbrace{(d_2 v)^2 - d u^2}_{N(d_2 v + u\sqrt{d})} = -2d_2$

Case 2: $2 \nmid x$ $\Rightarrow dy^2 \equiv 0 \pmod 8 \Rightarrow 2 \mid y$, $\gcd\left(\frac{x+1}{2}, \frac{x-1}{2}\right) = 1$

$$\Rightarrow \left\{ \begin{array}{ll} \frac{x+1}{2} = d_1 u^2, & d_1 d_2 = d \\ \frac{x-1}{2} = d_2 u^2, & uv = y/2 \end{array} \right\} \Rightarrow \underline{d_1 u^2 - d_2 v^2 = 1}, \quad \underline{d_1, d_2 \neq 1} \text{ (since } \varepsilon \text{ is the smallest unit } \varepsilon > 1)$$

$$\underbrace{(d_1 u)^2 - d v^2}_{N(d_1 u + v\sqrt{d})} = d_1, \quad \underbrace{(d_2 v)^2 - d u^2}_{N(d_2 v + u\sqrt{d})} = -d_2$$

Equivalently: $\underline{\beta_1 = d_1 u + v\sqrt{d}}$, $\underline{\beta_2 = d_2 v + u\sqrt{d}}$ satisfy

$$\beta_1^2 = d_1(d_1 u^2 + d_2 v^2 + 2uv\sqrt{d}) = \begin{cases} 2d_1\varepsilon & \text{Case 1} \\ d_1\varepsilon & \text{Case 2} \end{cases}$$

$$\beta_2^2 = d_2(\text{---}''\text{---}) = \begin{cases} 2d_2\varepsilon & \text{Case 1} \\ d_2\varepsilon & \text{Case 2} \end{cases}$$

Exercise: If $\beta \in \mathbb{Z}[\sqrt{d}]$ satisfies $\beta^2 = n\varepsilon$, $n \in \mathbb{Z}_{>0}$,

then (without assuming in advance that $N(\varepsilon) = +1$):

$n > 0$, $N(\varepsilon) = 1$ and $\exists!\, i \in \{1, 2\}$ $\sqrt{n/d_i} \in \mathbb{Z}$.

[Hint: $\mathbb{Q}(\sqrt{d})^{*2} \cap \mathbb{Q}^* = \mathbb{Q}^{*2} \cup d\mathbb{Q}^{*2}$]

Another approach to relations $\mathfrak{Q}_1^{a_1} \cdots \mathfrak{Q}_t^{a_t} = (\beta)$, $N_{K/\mathbb{Q}}(\beta) > 0$

$K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z} \setminus \{0,1\}$ square-free, $D = D_K$, $\mathrm{Ram} = \{q_1, \dots, q_t \mid D\}$, $(q_i) = \mathfrak{Q}_i^2$. If $d > 0$, let $\mathcal{O}_K^\times = \{\pm \varepsilon^{\mathbb{Z}}\}$ with $\sigma_1(\varepsilon) > 0$.

Note: (1) $\prod_{q \mid d} \mathfrak{Q} = (\sqrt{d}) = \begin{cases} \prod_{q \mid D} \mathfrak{Q} & \text{if } d \equiv 1, 2 \pmod 4 \\ \prod_{2 \neq q \mid D} \mathfrak{Q}, & \text{if } d \equiv 3 \pmod 4 \end{cases}$

(2) If $d > 0$ and if $\exists\, q_j \mid d$ $q_j \equiv 3 \pmod 4 \Rightarrow N(\varepsilon) = 1$

(3) If $\prod_{q \mid D} \mathfrak{Q}^{a_q} = (\beta)$, $a_q \in \{0,1\}$, $\underbrace{N(\beta)}_{\beta\beta'} > 0 \Rightarrow (\beta') = (\beta)$, $\beta' = \beta\eta$, $\eta \in \mathcal{O}_K^\times$, $N(\eta) = 1$

(4) If $D < -4$: $\eta \in \mathcal{O}_K^\times = \{\pm 1\}$, $\beta' = (-1)^m \beta$, $\beta = (\sqrt{d})^m b$, $b \in \mathbb{Q}^\times$

$\prod_{q \mid D} q^{a_q} = \pm \beta^2 = \pm d^m b^2 \Rightarrow$ the only (non-trivial) relation is (1) $(N(\sqrt{d}) = -d > 0)$

(5) If $d > 0$ and $N(\varepsilon) = -1$: after possibly replacing η by $-\eta$, $\eta = \varepsilon^{2m}$.

As $N(\varepsilon\sqrt{d}) > 0$ and $\varepsilon\sqrt{d} / (\varepsilon\sqrt{d})' = -\varepsilon/\varepsilon' = \varepsilon^2$, $\beta = (\varepsilon\sqrt{d})^m b$, $b \in \mathbb{Q}^\times \Rightarrow$

$\prod_{q \mid D} q^{a_q} = d^m b^2 \Rightarrow$ again, the only non-trivial relation is (1):

$$\prod_{q \mid d} \mathfrak{Q} = (\varepsilon\sqrt{d}), \qquad N(\varepsilon\sqrt{d}) > 0.$$

(6) If $d > 0$ and $N(\varepsilon) = 1$: $\varepsilon = \frac{1+\varepsilon}{1+\varepsilon'}$ and $\eta = \varepsilon^m = \left(\frac{1+\varepsilon}{1+\varepsilon'}\right)^m \Rightarrow$

$\beta = (1+\varepsilon)^m b$, $b \in \mathbb{Q}^\times$. We have $(1+\varepsilon) = (1+\varepsilon')$, $\sigma_1(N(1+\varepsilon)) = \sigma_1(\varepsilon(1+\varepsilon')^2) > 0$.

Claim: $(1+\varepsilon) \neq (b_1)$, $b_1 \in \mathbb{Q}^\times$ (if $(1+\varepsilon) = (b_1) \Rightarrow 1+\varepsilon = \pm b_1 \varepsilon^k$,

$\varepsilon = (1+\varepsilon)/(1+\varepsilon') = (\varepsilon/\varepsilon')^k = \varepsilon^{2k}$ – impossible). Therefore

$\prod_{q \mid D} q^{a_q} = N(1+\varepsilon)^m b^2$ with $N(1+\varepsilon) \notin \mathbb{Q}^{\times 2} \Rightarrow$ the only possible non-triv. relation is $\prod_{q \mid D} \mathfrak{Q}^{a_q} = (1+\varepsilon) b$, $b \in \mathbb{Q}^\times$. Conversely,

Claim above $\Rightarrow$ $(1+\varepsilon) = (1+\varepsilon)' = (b_1) \prod_{q \mid D} \mathfrak{Q}^{a_q}$, $b_1 \in \mathbb{Q}^\times$, $a_q \in \{0,1\}$, not all 0

(7) If $d > 0$, $N(\varepsilon) = 1$ and $d \not\equiv 3 \pmod 4$, then $(1+\varepsilon) = (b_1) \prod_{q \mid D} \mathfrak{Q}^{a_q}$ as in (6) ($a_q \in \{0,1\}$, not all 0), $\exists\, q \mid D$ $a_q \neq 1$.

Indeed, if $\forall\, q \mid D$ $a_q = 1$, then (1) $\Rightarrow$ $(1+\varepsilon) = (b_1)(\sqrt{d}) \Rightarrow$

$\alpha = \frac{1+\varepsilon}{b_1}$ satisfies $N(\alpha) > 0$ and $(\alpha) = (\sqrt{d}) \Rightarrow \eta = \alpha/\sqrt{d} \in \mathcal{O}_K^\times$,

$N(\eta) = -1$ contradiction

Cor 1. $2 \nmid h_K^+ \iff t=1 \iff D = \pm q^k \iff d = \begin{cases} -1, \pm 2 \\ q \equiv 1 \pmod 4 \\ -q, \ q \equiv 3 \pmod 4 \end{cases}$.

Cor 2. If $q_1, q_2 \equiv 3 \pmod 4$ are primes, $q_1 \neq q_2$, then in $K = \mathbb{Q}(\sqrt{q_1 q_2})$ either $\mathfrak{Q}_1 = (\alpha)$, $N(\alpha) > 0$, or $\mathfrak{Q}_2 = (\beta)$, $N(\beta) > 0$, but not both, $(q_j) = \mathfrak{Q}_j^2$.

Cor 1, Cor 2 $\Longrightarrow$ QRL

① $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$: $K = \mathbb{Q}(\sqrt{-1})$, $h^+ = 1$. If $\left(\frac{-1}{p}\right) = 1 \Rightarrow (p) = PP'$ $(P \neq P')$ in $\mathcal{O}_K$

$h^+ = 1 \Rightarrow P = (u+vi)$, $p = NP = u^2 + v^2 \Rightarrow p \equiv 1 \pmod 4$.

If $p \equiv 1 \pmod 4$ $\overset{\text{Cor 1}}{\Longrightarrow}$ $K = \mathbb{Q}(\sqrt{p})$ satisfies $2 \nmid h^+ \Rightarrow N(\varepsilon) = -1$,

$\varepsilon = (x + y\sqrt{p})/2$, $x^2 - py^2 = -4 \Rightarrow \left(\frac{-1}{p}\right) = \left(\frac{-4}{p}\right) = \left(\frac{x}{p}\right)^2 = 1$.

---

② $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$: (a) $p \equiv q \equiv 1 \pmod 4$: if $\left(\frac{q}{p}\right) = 1 \Rightarrow (q) = PP'$ $(P \neq P')$ in $\mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{q})$. As $2 \nmid h_K^+$ (Cor. 1) $\Rightarrow$ $P^{h^+} = \left(\frac{x+y\sqrt{q}}{2}\right)$ satisfies $x^2 - qy^2 = 4p^{h^+} \Rightarrow 1 = \left(\frac{x}{q}\right)^2 = \left(\frac{p}{q}\right)^{h^+} \Rightarrow \left(\frac{p}{q}\right) = 1$. It follows that $\left[\left(\frac{p}{q}\right) = -1 \Rightarrow \left(\frac{q}{p}\right) = -1\right]$. We conclude by symmetry.

(b) $q \equiv -p \equiv 1 \pmod 4$: as in (a), $\left(\frac{q}{p}\right) = 1 \Rightarrow \left(\frac{p}{q}\right) = 1 \left(\overset{(1)}{\Longleftrightarrow} \left(\frac{-p}{q}\right) = 1\right)$.

If $\left(\frac{p}{q}\right)\left(= \left(\frac{-p}{q}\right)\right) = 1 \Rightarrow q = \mathfrak{Q}\mathfrak{Q}'$ $(\mathfrak{Q} \neq \mathfrak{Q}')$ in $\mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{-p})$, $\mathfrak{Q}^{h} = \left(\frac{x+y\sqrt{-p}}{2}\right)$,

$x^2 + py^2 = 4q^h$. Again, Cor 1 $\Rightarrow 2 \nmid h$, hence $\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)^h = \left(\frac{x}{p}\right)^2 = 1$.

(c) $p \equiv q \equiv 3 \pmod 4$: as in (b), $\left[\left(\frac{-p}{q}\right)\left(= -\left(\frac{p}{q}\right)\right) = 1 \Rightarrow \left(\frac{q}{p}\right) = 1\right]$.

Consider now $K = \mathbb{Q}(\sqrt{pq})$; $(p) = \mathfrak{P}^2$, $(q) = \mathfrak{Q}^2$ in $\mathcal{O}_K$. By Cor. 2,

either $\mathfrak{P} = \left(\frac{x+y\sqrt{pq}}{2}\right)$ or $\mathfrak{Q} = \left(\frac{x+y\sqrt{pq}}{2}\right)$, with $x^2 - pqy^2 > 0 \Rightarrow$

$x^2 - pqy^2 = 4p$ or $4q$. If $x^2 - pqy^2 = 4p \Rightarrow x = pu$, $4 = pu^2 - qy^2 \Rightarrow \left(\frac{p}{q}\right) = 1$, $\underbrace{\left(\frac{-q}{p}\right)}_{-\left(\frac{q}{p}\right)} = 1$

If $x^2 - pqy^2 = 4q \Rightarrow x = qv$, $4 = qv^2 - py^2 \Rightarrow \left(\frac{q}{p}\right) = 1$, $-\left(\frac{p}{q}\right) = \left(\frac{-p}{q}\right) = 1$.

---

③ $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$: if $\left(\frac{2}{p}\right) = 1 \Rightarrow (p) = PP'$ $(P \neq P')$ in $\underbrace{\mathcal{O}_K}_{\mathbb{Z}[\sqrt{2}]}$, $K = \mathbb{Q}(\sqrt{2})$.

As $h_K = 1$, $P = (x + y\sqrt{2}) \Rightarrow p = N(P) = |x^2 - 2y^2| \equiv \pm 1 \pmod 8$

$\left(\begin{matrix} x^2 \equiv 1 \pmod 8 \\ 2y^2 \equiv 0 \pmod 8 \end{matrix}\right)$

If $p \equiv \pm 1 \pmod 8$, then $K = \mathbb{Q}(\sqrt{\pm p})$ has $2 \nmid h^+$ (by Cor. 1),

$\Downarrow$ Kummer – Dedekind

$(2) = \mathfrak{Q}\mathfrak{Q}'$ $(\mathfrak{Q} = \mathfrak{Q}')$ in $\mathcal{O}_K$, $\mathfrak{Q}^{h^+} = \left(\frac{x+y\sqrt{\pm p}}{2}\right)$, $x^2 \mp py^2 = 4q^{h^+}$

$\Rightarrow \left(\frac{2}{p}\right) = \left(\frac{2}{p}\right)^{h^+} = \left(\frac{x}{p}\right)^2 = 1$.

Gauss's formula $|\mathcal{C}\ell^+/(\mathcal{C}\ell^+)^2| = 2^{t-1} \Longrightarrow$ QRL

Deducing Quadratic Reciprocity Law from Gauss's formula is very simple: as $(\mathcal{C}\ell^+)^2 \subset \mathrm{Ker}(\overline{N})$, the image of the vertical map e has order $\leq 2^{t-1}$, which means that there is a non-trivial relation

$$\mathcal{C}\ell^+/(\mathcal{C}\ell^+)^2 \xrightarrow[\text{surjective}]{\overline{N}} I(\mathcal{O}_K)/N(K^*_{N>0}) \xrightarrow{e} \bigoplus_{q|D} \{\pm 1\} = \{\pm 1\}^t$$

$$\forall I \quad \prod_{q|D} (D, N(I))_q^{c_q} = 1 \quad , \quad \text{for suitable } c_q \in \{0,1\} \text{ (not all } \neq 0)$$

Choosing appropriately D and I, one obtains the QRL and the two complementary laws for $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ $\Longrightarrow$ if $\forall q$ $c_q = 1$, then holds

Ex: (1) If $t=1$ ($D = \pm$ power of q), then $(D, N(I))_q = 1$ $\forall$ ideal I

(a) $D=-4$: if $\left(\frac{-1}{p}\right)=1 \Rightarrow \exists\, I$ $N(I)=p \Rightarrow (-4,p)_2 = 1 \Rightarrow p \equiv 1 \pmod 4$

(b) $D=8$: if $\left(\frac{2}{p}\right)=1 \Rightarrow$ — " — $(8,p)_2 = 1 \Rightarrow p \equiv \pm 1 \pmod 8$

(c) $D=-8$: if $\left(\frac{-2}{p}\right)=1 \Rightarrow$ — " — $(-8,p)_2 = 1 \Rightarrow p \equiv 1, 3 \pmod 8$

this yields the values of $\left(\frac{-1}{p}\right), \left(\frac{\pm 2}{p}\right)$ for all $p \equiv 3,5,7 \pmod 8$.

(d) $D=q^*$: if $\left(\frac{q^*}{p}\right)=1 \Rightarrow$ — " — $(q^*,p)_p = 1 \Rightarrow \left(\frac{p}{q}\right) = 1$.

(2) If $q \equiv 3 \pmod 4$, $D = 4q = (-4)(-q)$ $(t=2)$: $\exists\, I, J$ $N(I)=q$, $N(J)=2$

$$1 = \underbrace{(D,q)_2^{c_2}}_{-1} \underbrace{(D,q)_q^{c_q}}_{\left(\frac{-1}{q}\right)=-1} \Rightarrow c_2 = c_q = 1$$

if $\left(\frac{q}{p}\right)=1 \Rightarrow \exists\, P$ $N(P)=p \Rightarrow 1 = \underbrace{(4q,p)_2}_{(-1)^{\frac{p-1}{2}}} \underbrace{(4q,p)_q}_{\left(\frac{p}{q}\right)} \Rightarrow \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}}$.

A little bit of fiddling around shows that $\left(\frac{-1}{p}\right)=1$ for $p \equiv 1 \pmod 4$ and that $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

(e) If $p \equiv 1 \pmod 8$: $D=p$: $\exists\, I$ $N(I)=2 \overset{t=1}{\Longrightarrow} \underbrace{(p,2)_p}_{\left(\frac{2}{p}\right)} = 1$.

Rmk: (1) As we know, QRL $\Longrightarrow$ product formula $\prod_v (D,a)_v = 1$ $\overset{\sim}{\Longrightarrow}$ $\mathrm{Im}(e) \subset \mathrm{Ker}\left(\bigoplus_{q|D} \{\pm 1\} \xrightarrow{\text{prod}} \{\pm 1\}\right)$. the statement of the Main Theorem of Genus Theory is then equivalent to: $\overline{e}$ is injective $\Longleftrightarrow$ $\overline{e}$ is surjective

injective: Legendre's Thm; surjective: the first proof we gave using Dirichlet's Thm.

$\Longleftrightarrow$ $\mathrm{Ker}(e \circ \overline{N}) = (\mathcal{C}\ell^+)^2$ (Gauss's duplication thm).

Structure of $Cl^+/(Cl^+)^4$ (after Reidei)

If $Ram = \{2/D\} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$, Gauss's Thm tells us that $Cl^+/(Cl^+)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$. Is there anything else going on?

Ex(1): consider $\mathbb{Q}(\sqrt{-p})$ for primes $p \neq 2$. We know that $h_{-p} = |Cl_{\mathbb{Q}(\sqrt{-p})}|$ is odd if $p \equiv 3 \pmod 4$. What if $p \equiv 1 \pmod 4$?

$p \equiv 1 \pmod 8$	17	41	73	89	97	113
h_{-p}	4	8	4	12	4	8

$p \equiv 5 \pmod 8$	5	13	29	37	53	61	101	109
h_{-p}	2	2	6	2	6	6	14	6

$D = -4p$, $t = 2$

$\Downarrow$ Gauss

$Cl/Cl^2 \simeq \mathbb{Z}/2\mathbb{Z}$

$\Downarrow$

$Cl \simeq (\mathbb{Z}/2^m\mathbb{Z}) \times H$, $m \geq 1$, $2 \nmid |H|$

The two tables seem to suggest that the 2-primary component of Cl (which is cyclic in this case) $Cl[2^\infty] = \bigcup_{i \geq 1} Cl[2^i] \simeq \mathbb{Z}/2^m\mathbb{Z}$ satisfies

$m \geq 2 \overset{?}{\iff} p \equiv 1 \pmod 8$

$m = 1 \overset{?}{\iff} p \equiv 5 \pmod 8$

Ex(2): consider $h_{-2p} = |Cl_{\mathbb{Q}(\sqrt{-2p})}|$ for primes $p \neq 2$

$p \equiv 1 \pmod 8$	17	41	73	89	97
h_{-2p}	4	4	16	8	20

$p \equiv -1 \pmod 8$	7	23	31	47	71	79	103
h_{-2p}	4	4	8	8	4	8	20

$p \equiv 5 \pmod 8$	5	13	29	37	53	61	101
h_{-2p}	2	6	2	10	6	10	6

$p \equiv 3 \pmod 8$	3	11	19	43	59	67	83
h_{-2p}	2	2	6	10	6	14	10

$D = -8p$, $t = 2$, $Cl[2^\infty] \simeq \mathbb{Z}/2^m\mathbb{Z}$, $m \geq 1$.

It seems that

$m \geq 2 \overset{?}{\iff} p \equiv \pm 1 \pmod 8$

$m = 1 \overset{?}{\iff} p \equiv \pm 3 \pmod 8$

What is going on?

$Cl^+ \simeq Cl^+[2^\infty] \times H$, $2 \nmid |H|$

$Cl^+[2^\infty] \simeq \bigoplus_{i=1}^{t-1} \mathbb{Z}/2^{m_i}\mathbb{Z}$, $m_i \geq 1$

Consider the canonical map

$\alpha_i = 0$ if $m_i \geq 2$

α_i = isomorphism if $m_i = 1$

$$Cl^+[2] \hookrightarrow Cl^+ \xrightarrow{\alpha} Cl^+/(Cl^+)^2$$

$$\bigoplus_{i=1}^{t-1} \frac{2^{m_i-1}\mathbb{Z}}{2^{m_i}\mathbb{Z}} \xrightarrow{(\alpha_i)} \bigoplus_{i=1}^{t-1} \mathbb{Z}/2\mathbb{Z}$$

$$a \mapsto a \pmod 2$$

Conclusion: $\mathrm{Im}(\alpha) \simeq (\mathbb{Z}/2\mathbb{Z})^k$, $k = |\{i=1,\dots,t-1 \mid m_i = 1\}|$

$$\Rightarrow \boxed{Cl^+/(Cl^+)^4 \simeq (\mathbb{Z}/2\mathbb{Z})^k \times (\mathbb{Z}/4\mathbb{Z})^{t-1-k}}$$

Explicit matrix representing α (or a closely related map):

$$\begin{array}{ccc}
\left[\prod Q^{a_Q}\right] \in Cl^+[2] & \xrightarrow{\alpha} & Cl^+/(Cl^+)^2 \\
\uparrow & & \downarrow e \text{ (injective)} \\
\uparrow \text{surjective} & & \\
(a_Q) \in \bigoplus_{2\mid D} \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \bigoplus_{2\mid D} \{\pm 1\} \simeq \bigoplus_{2\mid D} \mathbb{Z}/2\mathbb{Z}
\end{array}$$

$(q) = Q^2$

matrix A

$$\boxed{A = (a_{ij}) \in M_t(\mathbb{Z}/2\mathbb{Z}) \qquad (-1)^{a_{ij}} = (D, \underbrace{q_i}_{N(Q_i)})_{q_j}}$$

$$\dim_{\mathbb{F}_2}\left(\mathrm{Im}(\alpha)\right) = k = \mathrm{rk}(A)$$

Ex (1): [redacted], $D = -4p$: $t = 2$ $\qquad p \equiv 1 \pmod 4$ prime

$$\left((-1)^{a_{ij}}\right)_{1\le i,j\le 2} = \begin{pmatrix} (-4p,2)_2 & (-4p,p)_2 \\ (-4p,2)_p & (-4p,p)_p \end{pmatrix} = \begin{pmatrix} \left(\frac{2}{p}\right) & 1 \\ \left(\frac{2}{p}\right) & 1 \end{pmatrix}$$

$p \equiv 1 \pmod 8 \Rightarrow \left(\frac{2}{p}\right) = 1 \Rightarrow A = (a_{ij}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $k = \mathrm{rk}(A) = 0$

$Cl/Cl^4 \simeq \mathbb{Z}/4\mathbb{Z}$

$p \equiv 5 \pmod 8 \Rightarrow \left(\frac{2}{p}\right) = -1 \Rightarrow A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{F}_2)$, $k = \mathrm{rk}(A) = 1$

$Cl[2^\infty] = \mathbb{Z}/2\mathbb{Z}$

---

(2) $D = -8p$: $p \neq 2$ prime, $t = 2$

$$\left((-1)^{a_{ij}}\right)_{1\le i,j\le 2} = \begin{pmatrix} (-8p,2)_2 & (-8p,p)_2 \\ (-8p,2)_p & (-8p,p)_p \end{pmatrix} = \begin{pmatrix} \left(\frac{2}{p}\right) & \left(\frac{2}{p}\right) \\ \left(\frac{2}{p}\right) & \left(\frac{2}{p}\right) \end{pmatrix}$$

$p \equiv \pm 1 \pmod 8 \Rightarrow \left(\frac{2}{p}\right) = 1 \Rightarrow A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $k = \mathrm{rk}(A) = 0 \Rightarrow Cl/Cl^4 \simeq \mathbb{Z}/4\mathbb{Z}$

$p \equiv \pm 3 \pmod 8 \Rightarrow \left(\frac{2}{p}\right) = -1 \Rightarrow A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $k = \mathrm{rk}(A) = 1 \Rightarrow Cl[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z}$

Exercise: (1) When is $2 \nmid |Cl_{\mathbb{Q}(\sqrt{d})}|$ (for $d > 0$)?

(2) For which d is $Cl^+_{\mathbb{Q}(\sqrt{d})}[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z}$?

$Cl_{\mathbb{Q}(\sqrt{d})}[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z}$?

Binary quadratic forms and primality testing

$K=\mathbb{Q}(\sqrt{d})$, $d\in\mathbb{Z}\setminus\{0,1\}$ square-free, $\Delta=D_K=\begin{cases} d & d\equiv 1 \pmod 4 \\ 4d & d\equiv 2,3 \pmod 4 \end{cases}$

Let $f\in \mathrm{Quad}(\Delta)$ with class $C=[f]\in Cl(\Delta)=Cl_K^+$. Fix an ideal I (fractional) of $\mathcal{O}_K$ and a positive basis $I=\mathbb{Z}\alpha_1+\mathbb{Z}\alpha_2$ such that $f(x,y)=(\alpha_1 x+\alpha_2 y)(\alpha_1' x+\alpha_2' y)/N(I)$ $\quad([I]=C)$.

Def: for $m\in\mathbb{Z}_{>0}$, let $r_f(m)=r_C(m)=\left|\{\beta\in I \mid N(\beta)/N(I)=m\}/(\mathcal{O}_K^\times)^{N=1}\right|$

($r_C(m)=r_{C^{-1}}(m)$, since $\beta'\in I'$, $[I']=C^{-1}$, $N(\beta')/N(I')=N(\beta)/N(I)$)

For $G\in \mathrm{Gen}(\Delta)$, let $r_G(m)=\sum_{C\in G} r_C(m)$.

Ex: (1) $K=\mathbb{Q}(\sqrt{-1})$: $\mathcal{O}_K=\mathbb{Z}[i]$, $|Cl(\Delta)|=1$, $f=x^2+y^2=(x+iy)(x-iy)$,

$\mathcal{O}_K^\times=\{\pm 1,\pm i\}$, $I=\mathbb{Z}[i]$, $\beta=a+bi$ $(a,b\in\mathbb{Z})$

$r(m)=r_{x^2+y^2}(m)=\frac{1}{4}\left|\{(a,b)\in\mathbb{Z}^2 \mid a^2+b^2=m\}\right|=\frac{1}{4}\left|\{\beta\in\mathbb{Z}[i] \mid \beta\overline{\beta}=m\}\right|$

Factorisation in $\mathbb{Z}[i]$: $m=2^{v_2(m)}\prod_{q\equiv 3[4]} q^{v_q(m)}\prod_{p\equiv 1[4]} p^{v_p(m)}$ $\quad(p,q \text{ prime})$

$p=\pi_p\overline{\pi_p}$

$\beta=i^k(1+i)^a\prod_{q\equiv 3[4]} q^{b_q}\prod_{p\equiv 1[4]}\left(\pi_p^{a_p}\overline{\pi_p}^{a_p'}\right)$ $\xrightarrow{N(\beta)=m}$ $a=v_2(m)$, $2b_q=v_q(m)$, $a_p+a_p'=v_p(m)$

$(k\in\mathbb{Z}/4\mathbb{Z})$

$$r(m)=\frac{|\mathbb{Z}/4\mathbb{Z}|}{4}\cdot 1\cdot\prod_{\substack{q\equiv 3[4]\\ q\mid m}}\begin{cases}1 & \text{if } 2\mid v_2(m)\\ 0 & \text{if } 2\nmid v_2(m)\end{cases}\cdot\prod_{\substack{p\equiv 1[4]\\ p\mid m}}(v_p(m)+1)$$

Let $r_{prim}(m)=\frac{1}{4}\left|\{(a,b)\in\mathbb{Z}^2 \mid a^2+b^2=m,\ \gcd(a,b)=1\}\right|$.

If $2\nmid m$ ($a=0$): $\gcd(a,b)=1 \iff \beta=a+bi$ satisfies $\gcd(\beta,\overline{\beta})=1$ in $\mathbb{Z}[i]$

$$\iff \beta=i^k\prod_{\substack{p\equiv 1[4]\\ p\mid m}}\begin{cases}\pi_p^{a_p}, & a_p=v_p(m)\\ \overline{\pi_p}^{a_p'}, & a_p'=v_p(m)\end{cases}$$

Therefore: $2\nmid m \Rightarrow r_{prim}(m)=\prod_{\substack{p\equiv 1[4]\\ p\mid m}} 2\prod_{\substack{q\equiv 3[4]\\ q\mid m}} 0$

Conclusion: $m\equiv 1 \pmod 4$ is a prime $\iff r_{x^2+y^2,prim}(m)=2$.

---

(2) $K=\mathbb{Q}(\sqrt{-3})$: $\mathcal{O}_K=\mathbb{Z}[\zeta_3]$, $\mathcal{O}_K^\times=\mu_6$, $|Cl(\Delta)|=1$, $f=x^2+xy+y^2$

$r_{x^2+xy+y^2}(m)=\frac{1}{6}\left|\{\beta\in\mathbb{Z}[\zeta_3] \mid \beta\overline{\beta}=m\}\right|$; $\beta=\zeta_6^k(1-\zeta_3)^a\prod_{q\equiv -1[3]} q^{b_q}\prod_{p\equiv 1[3]}\pi_p^{a_p}\overline{\pi_p}^{a_p'}$

$(\pi_p\overline{\pi_p}=p)$, $m=3^{v_3(m)}\prod_{q\equiv -1[3]} q^{v_q(m)}\prod_{p\equiv 1[3]} p^{v_p(m)}$ $\quad(p,q \text{ prime})$

$N(\beta)=m \Rightarrow a=v_3(m)$, $2b_q=v_q(m)$, $a_p+a_p'=v_p(m)$

$\cdot\ \beta=a-b\zeta_3$

If $3\nmid m$, $(a,b)=1 \iff (\beta,\overline{\beta})=1$

$$r_{x^2+xy+y^2}(m)=\prod_{\substack{q\equiv -1[3]\\ q\mid m}}\begin{cases}1 & \text{if } 2\mid v_2(m)\\ 0 & \text{if } 2\nmid v_2(m)\end{cases}\prod_{\substack{p\equiv 1[3]\\ p\mid m}}(v_p(m)+1)$$

Again: $3\nmid m \Rightarrow r_{x^2+xy+y^2,prim}(m)=\prod_{\substack{p\equiv 1[3]\\ p\mid m}} 2\prod_{\substack{q\equiv -1[3]\\ q\mid m}} 0$

So: $m\equiv 1[3]$ is a prime $\iff r_{x^2+xy+y^2,prim}(m)=2$.

(3) General case: primitive representations $m = f(a,b)$, $\gcd(a,b)=1$ correspond to $\beta \in I$ with $N(\beta) = m\,N(I)$ such that $\forall n \in \mathbb{Z}_{\geq 2}$ $\beta \notin nI$.

$\Updownarrow$ $\qquad\qquad$ $\Updownarrow$

$J = (\beta) I^{-1} \subset \mathcal{O}_K$ ideal, $N(J) = m$ $\qquad$ $(n) \nmid J$

$[J] = [I]^{-1} = C^{-1}$

So: $r_C(m) = r_{C^{-1}}(m) = \left| \{ J \subset \mathcal{O}_K \text{ ideal} \mid [J] = C,\ N(J) = m \} \right|$

$r_G(m) = \quad\quad \left| \{ \text{---} \parallel \text{---} \mid [J] \in G,\ \text{---} \parallel \text{---} \} \right|$

For $r_{G,\text{prim}}(m)$, add the condition $\forall n \in \mathbb{Z}_{\geq 2}$ $(n) \nmid J$.

Factorisation in $\mathbb{Z}$: $m = \prod_{r \mid D_K} r^{\nu_r(m)} \prod_{\chi_K(p)=1} p^{\nu_p(m)} \prod_{\chi_K(q)=-1} q^{\nu_2(m)}$ $\qquad$ (p, q, r prime)

---"--- into ideals of $\mathcal{O}_K$: $J = \prod \mathfrak{R}^{c_R} \prod \mathfrak{P}^{a_P} (\mathfrak{P}')^{a_{P'}} \prod \mathfrak{Q}^{b_Q}$

$(r) = \mathfrak{R}^2$, $(p) = \mathfrak{P}\mathfrak{P}'$ $(\mathfrak{P} \neq \mathfrak{P}')$, $(q) = \mathfrak{Q}$ $\quad$ $N(J) = m \iff c_R = \nu_r(m)$, $a_P + a_{P'} = \nu_p(m)$, $2b_Q = \nu_2(m)$

$[J] \in G \iff \forall r \ (D_K, \overbrace{N(J)}^{m})_r = e_r(G)$ $\quad$ (automatic if $v = \infty$ or $v = p$, $\chi_K(p) = 1$)

$\iff \begin{cases} \forall q \text{ such that } \chi_K(q) = -1 & 2 \mid \nu_2(m) \\ \forall r \mid D_K & (D_K, m)_r = e_r(G) \end{cases}$

Special case: $(m, D_K) = 1$: then $(D_K, m)_r = \chi_{D_r}(m \pmod{|D_r|})$ $\quad$ $\left(= \left(\frac{D_r}{m}\right)$ if $2 \nmid m\right)$

$D_K = \prod_{r \mid D_K} D_r$, $|D_r| =$ power of r, $D_r \equiv 0, 1 \pmod 4$

As in (1), (2): if $\gcd(m, D_K) = 1$, then:

$$r_G(m) = \prod_{r \mid D_K} \underbrace{\begin{cases} 1 & \text{if } (D_K, m)_r = e_r(G) \\ 0 & \text{if not} \end{cases}}_{= 1 \iff m \in S^+(G)} \prod_{\substack{q \mid m \\ \chi_K(q) = -1}} \begin{cases} 1 & \text{if } 2 \mid \nu_2(m) \\ 0 & \text{if not} \end{cases} \prod_{\substack{p \mid m \\ \chi_K(p) = 1}} (\nu_p(m) + 1)$$

Primitive representations $\iff$ $J = \prod_P \begin{cases} \mathfrak{P}^{a_P} \\ \text{or } (\mathfrak{P}')^{a_{P'}} \end{cases}$, hence, if $\gcd(m, D_K) = 1$,

$$r_{G,\text{prim}}(m) = \prod_{r \mid D_K} \begin{cases} 1 & \text{if } (D_K, m)_r = e_r(G) \\ 0 & \text{if not} \end{cases} \prod_{\substack{p \mid m \\ \chi_K(p) = 1}} 2 \prod_{\substack{q \mid m \\ \chi_K(q) = -1}} 0$$

Conclusion: if $\gcd(m, D_K) = 1$, $\left[r_{G,\text{prim}}(m) = 2 \iff m = \text{prime and } m \in S^+(G) \right]$

this criterion was used by Euler if $D_K < 0$ and $G = \{C\}$ contains one class only ($\Leftarrow$ $D_K =$ one of 65 specific values).

Chebyshev extended this to the case $D_K > 0$. In particular, he was able to check that 8520191 is a prime (a question left open in Legendre's Théorie des Nombres).

What more can one say about ideal class groups of quadratic fields ?

(1) Gauss observed that $|Cl(\Delta)|$ seemed to be growing as $\Delta \to -\infty$. He found 13 negative discriminants for which $|Cl(\Delta)| = 1$:

- 9 fundamental ones, corresponding to 9 imaginary quadratic fields $K = \mathbb{Q}(\sqrt{d})$, $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$, for which $\mathcal{O}_K$ is a PID;
- 4 non-fundamental ones: $-12, -16, -27, -28$.

(2) In 1934, Heilbronn and Linfoot showed that there is at most one additional $K = \mathbb{Q}(\sqrt{d})$ $(d < -163)$ with $|Cl_K| = 1$.

(3) Heegner (1952) showed that no such K exists ($\Rightarrow$ Gauss's list is complete), but his proof seemed to rely on unjustified properties of special values of certain modular functions. In mid/late 1960's alternative proofs were given by Baker and by Stark. Birch and Stark showed that Heegner's proof was, in fact, correct.

(4) Siegel (1935) showed that, for d square-free,

$$\lim_{d \to -\infty} \frac{\log |Cl_{\mathbb{Q}(\sqrt{d})}|}{\log (|d|^{1/2})} = \frac{1}{2}$$

$$\lim_{d \to +\infty} \frac{\log \left(|Cl_{\mathbb{Q}(\sqrt{d})}| \log (\text{fundamental unit of } \mathcal{O}_{\mathbb{Q}(\sqrt{d})}) \right)}{\log (d^{1/2})} = \frac{1}{2}$$

(5) There are explicit lower bounds of the form

$$|Cl(\mathcal{O}_K)| > C \prod_{p | D_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right) \log |D_K| \qquad K = \mathbb{Q}(\sqrt{d}),\ d < 0$$

(Goldfeld + Gross–Zagier, with improvements by Oesterlé)

(6) Extensive computer calculations (Watkins) have given complete lists of all imaginary quadratic fields with $|Cl_K| \leq 100$.

(7) There are 65 known imaginary quadratic fields K for which $Cl_K \simeq (\mathbb{Z}/2\mathbb{Z})^k$ ($\Leftrightarrow$ each genus of binary quadratic forms of discriminant D_K contains only one class). Weinberger (1972) showed that there is at most one more such a field, but its existence would contradict the generalised Riemann hypothesis.

(8) According to conjectures of Cohen and Lenstra, the odd part of Cl_K (= the quotient of Cl_K by its 2-primary part $Cl_K[2^\infty]$) for $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, should be, on average, a "random" finite abelian group of odd order.
A very special case of this conjecture is confirmed by a result of Davenport and Heilbronn about the average values of $|Cl_K[3]|$.

(9) A very special case of Leopoldt's "mirror principle" (proved earlier by Reichardt and by Scholz) states that

$$|Cl_{\mathbb{Q}(\sqrt{d_+})}[3]| \leq |Cl_{\mathbb{Q}(\sqrt{d_-})}[3]| \leq 3 \cdot |Cl_{\mathbb{Q}(\sqrt{d_+})}[3]|,$$

if $d_+ > 1$ is square-free and $d_- = \begin{cases} -3d_+ & 3 \nmid d_+ \\ -d_+/3 & 3 \mid d_+ \end{cases}$

Exercise. Euler discovered that the polynomial $f(x) = x^2+x+41$ takes prime values for $x = 0, 1, \cdots, 39$ (not for $x=40$, since $f(40) = 41^2$). This is related to the fact that $\mathrm{disc}(f) = -163$ and $|Cl_{\mathbb{Q}(\sqrt{-163})}| = 1$.

Assume that $k \in \mathbb{Z}_{\geq 2}$, $4k-1$ square-free; let $f_k(x) = x^2+x+k$, $f_k(\alpha) = 0$, $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{1-4k})$, $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(1) For a prime p, it is equivalent:
$\exists\, m \in \mathbb{Z}$ $\quad p \mid f_k(m) \iff p\mathcal{O}_K = P\overline{P}$, $N(P) = p$ $\quad (P = \overline{P}$ is allowed)

(2) If $m \in \mathbb{Z}$ and $p = f_k(m)$ is a prime, then $p\mathcal{O}_K = P\overline{P}$, $P = (m-\alpha)$. principal

(3) If p is a prime, $p\mathcal{O}_K = P\overline{P}$, $p < k \Rightarrow P \neq (\beta)$ is not principal.

(4) $|Cl_K| = 1 \Rightarrow \forall m = 0, 1, \cdots, k-2$ $\quad f_k(m) =$ prime

[Hint: if $ab = f_k(m) < k^2$, $(a,b) > 1) \Rightarrow \exists$ prime $p < k$, $p \mid f_k(m)$]

(5) If $p =$ prime such that $\exists\, m' \in \mathbb{Z}$ $p \mid f_k(m') \Rightarrow \exists\, m \in \mathbb{Z}$, $0 \leq m \leq \frac{p-1}{2}$, $p \mid f_k(m)$

(6) If $\forall\, m = 0, 1, \cdots, M$ $f_k(m) =$ prime $\Rightarrow \{p$ prime $\mid p \leq 2M+2$, $p\mathcal{O}_K = P\overline{P}\} =$
$= \{p$ prime $\mid p \leq 2M+2\} \cap \{f_k(0), f_k(1), \cdots, f_k(M)\}$.

(7) If $\forall\, m = 0, 1, \cdots, \left[\frac{\sqrt{4k-1}}{\pi}\right] - 1$ $\quad f_k(m) =$ prime $\Rightarrow |Cl_K| = 1$ $\quad (k \geq 3)$

[Hint: use (6) and Minkowski's bound]

Summary: $|Cl_K| = 1 \iff \forall m = 0, 1, \cdots, \left[\frac{4k-1}{\pi}\right] - 1$ $\quad f_k(m) =$ prime
$\iff \forall\, m = 0, 1, \cdots, k-2$ $\quad$ —— " ——

Ex: values of $f_k(m)$

k \ m	0	1	2	3	$4k-1$	$\left[\frac{4k-1}{\pi}\right] - 1$
41	41	43	47	53	163	3
17	17	19			67	1
11	11	13			43	1
5	5				19	0
3	3				11	0
2	2				7	