Gauss's Genus Theory

Gauss's genus theory describes the 2-torsion elements of the narrow class group of quadratic fields.

We will use $Cl(K)$ to denote the <u>class group</u> of a number field K;

$Cl(K) = I/P$

- I is the set of all fractional ideals of $\mathcal{O}_K$
- P is all principal fractional ideals

The <u>narrow class group</u> of K is

$Cl^+(K) = I/P^+$

- P^+ is the group of totally positive principal fractional ideals of $\mathcal{O}_K$; that is ideals $\alpha\mathcal{O}_K$, $\alpha \in K$, such that $\sigma(\alpha)$ positive for every embedding $\sigma: K \hookrightarrow \mathbb{R}$.

The Narrow Class Group of Quadratic Fields

a will always be a positive, squarefree rational integer

$\mathbb{Q}(\sqrt{-a})$, imaginary quadratic field:
There are no embeddings $\sigma: \mathbb{Q}(\sqrt{-a}) \hookrightarrow \mathbb{R}$, so the narrow class group is equal to the class group:

$$\boxed{Cl(\mathbb{Q}(\sqrt{-a}) = Cl^+(\mathbb{Q}(\sqrt{-a}))}$$

This doesn't necessarily happen for real quadratic fields $\mathbb{Q}(\sqrt{a})$ $a \neq 1$.
However, since

$$Cl(K) = I/P \cong {}^{(I/P^+)}/_{(P/P^+)} = Cl^+(K)/_{(P/P^+)}$$

it is clear that if the narrow class number $= 1$ then class number is also $= 1$.

Let ${}_2Cl^+(K)$ denote the 2-torsion elements of $Cl^+(K)$; that is, $J \in {}_2Cl^+(K) \iff J^2 = (\alpha)$ for some totally positive $\alpha \in K$.

Note that the definition of ${}_2Cl^+(K)$ implies that
$N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(I^2) = \left(N_{K/\mathbb{Q}}(I)\right)^2 = r^2$ for some $r \in \mathbb{Q}$.

From this we can deduce (the following argument comes from a short note on genus theory by Xuejun Guo, Columbia University):

- Hilbert's Theorem 90 $\Rightarrow$ $\alpha = r \cdot \frac{\beta}{\sigma(\beta)}$ for some $\beta \in K$
- we can assume β has no rational factor
- we can also assume β totally positive because $\beta/\sigma(\beta)$ must be.

$\Rightarrow$ $\alpha = r\, N(\beta) \cdot \frac{1}{(\sigma(\beta))^2}$.

$\Rightarrow \exists\, q \in \mathbb{Q},\ q = r\,N(\beta)$ such that $\left(\sigma(\beta)\, J\right)^2 = (q)$

i.e. there is an ideal equivalent to J in ${}_2Cl^+(K)$ which squares to a rational number

- By multiplying some positive rational number to $\sigma(\beta) J$ we can assume that q is a rational integer
  $\Rightarrow$ q ramifies in K

Therefore, we would expect there to be a connection between the primes ramified in K and the elements of ${}_2Cl^+(K)$!

In fact, Gauss's genus theory states that if there are t primes which ramify in K,

$$\#\left({}_2Cl^+(K)\right) = 2^{t-1}$$

The field $\mathbb{Q}(\sqrt{6})$ is known to have class number 1, but there are two primes, 2 and 3, which ramify in this field, so genus theory states that the narrow class number is divisible by $2^{2-1} = 2$.

What causes this disagreement between the narrow class number and class number?

I think it's because the extension $\rightarrow$ is unramified at all finite places but ramified at an infinite place.

$$\begin{array}{c} \mathbb{Q}(\sqrt{-2}, \sqrt{-3}) \\ | \\ \mathbb{Q}(\sqrt{6}) \end{array}$$

This requires a discussion of Hilbert class fields.

The <u>Hilbert class field</u> L of a number field K is the maximal unramified Galois extension of K (unramified applies to infinite places as well).

These fields have the amazing property that

$$\mathrm{Gal}(L/K) \cong Cl(K).$$

Any unramified abelian Galois extension K' of K is contained in the Hilbert class field L, so $[K' : K] \mid h_K$, where h_K is the class number of K.

This explains why 2 doesn't divide the class number of $\mathbb{Q}(\sqrt{6})$. If we try out a few degree 2 extensions, we see that these are not unramified:

$$\begin{array}{c} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ (= \mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{3}, \sqrt{6})) \\ | \\ \mathbb{Q}(\sqrt{6}) \end{array}
\qquad
\begin{array}{c} \text{any imaginary} \\ \text{degree 2 extension} \\ | \\ \mathbb{Q}(\sqrt{6}) \end{array}
\qquad
\begin{array}{c} \mathbb{Q}(\sqrt{6}, \sqrt{m}) \\ m \text{ s.f. and div by} \\ \text{a prime } p \neq 2, 3 \\ | \\ \mathbb{Q}(\sqrt{6}) \end{array}$$

$\boxed{\text{here 2 ramifies}}$ $\quad$ $\boxed{\text{an infinite place ramifies}}$ $\quad$ $\boxed{p \mid m \text{ ramifies}}$

So I think that ${}_2\mathcal{Cl}(K)$ can be completely described via unramified degree 2 extensions of real quadratic fields. Genus theory takes care of the imaginary quadratic case.

I also conjecture that

$$\#_2\mathcal{Cl}(K) \geq \begin{cases} \#_2\mathcal{Cl}^+(K) & \text{If every degree 2 extension which is ramified at an infinite place is also ramified at a finite place.} \\ \frac{1}{2} \times \#_2\mathcal{Cl}(K) & \text{If } \exists \text{ a degree 2 extension which is ramified at an infinite place but not a finite place} \end{cases}$$

To look at this further it is important to know the following fact about biquadratic fields:

The <u>only</u> rational prime which can ramify to a fourth power is 2, and that only happens when we can write the field as $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2})$, with $a_1 \equiv 2 \pmod 4$ and $a_2 \equiv 3 \pmod 4$ (or the other way around).

Let $K = \mathbb{Q}(\sqrt{a})$, $a = 2^{\varepsilon} p_1 \cdots p_n$ ($\varepsilon = 0$ or 1) be a real quadratic field.

If $\varepsilon = 1$:

(1) If $a/2 \equiv 3 \pmod 4$ then there is no biquadratic field containing K which is unramified (but genus theory gives 2-torsion since $\mathbb{Q}(\sqrt{a}, \sqrt{a/2})$ is unramified at finite places.

(2) If $a/2 \equiv 1 \pmod 4$ then $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $b > 0$ and $b =$ the product of primes dividing a s.t. $b \equiv 1 \pmod 4$ is unramified

→ We can do a counting argument to describe ${}_2\mathcal{Cl}^+(K)$ in terms of # of distinct unramified degree 2 extensions of K!

$\varepsilon = 0$ is easier.