Gauss's Genus Theory

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

We will use C(K) to denote the class group of a number field K; C(K) = 1/P

- · I is the set of all fractional ideals of BOK
- · P is all principal fractional ideals

The narrow class group of K is

C(+(K) = I/p+

· P+ is the group of totally positive principal fractional ideals of Ok; that is ideals aok, ack, such that o(a) positive for every embedding o: KC-R.

The Narrow Class Group of Quadratic Fields

a will always be a positive, squarefree rational integer 🕶

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

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

This doesn't necessarily happen for real quadratic fields Q(va) a = 1. However, since

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

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

Let $_2(l^+(K))$ denote the 2-torsion elements of $(l^+(K))$; that is, $J \in _2(l^+(K)) \iff J^2 = (\alpha)$ for some totally positive $\alpha \in K$.

Note that the definition of $_2(l^+(K))$ implies that $N_{K/a}(\alpha) = N_{K/a}(I^3) = (N_{K/a}(I))^2 = r^2$ 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 & has no rational factor

· we can also assume B totally positive because Block must be.

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

 \Rightarrow 3 g \in Q, g = r N(B) such that $(\sigma(B)J)^2 = (g)$ i.e. there is an ideal equivalent to J in $(l^+(K))$ which squares to a rational number

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

Therefore, we would expect there to be a connection between the primes ramified in K and the elements of ,Cl+(K)!

In fact, Gauss's genus theory states that if there are t primes which ramify in K, $\#(2(l^+(K)) = 2^{t-1})$

The field Q(16) 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 $2^{2-1} = 2$.

Q (V6)

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

I think it's because the extension - Q(J-2, J-3) is unramified at all finite places but ramified at an infinite place.

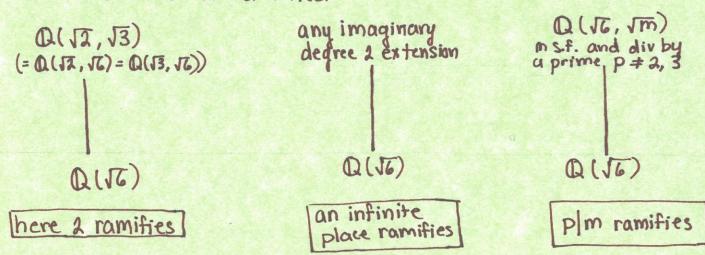
This requires a discussion of Hilbert class fields.

The Hilbert class field 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 Gal (L/K) = (L(K).

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

This explains why 2 doesn't divide the class number of Q(16). If we try out a few degree 2 extensions, we see that these are not unramified:



So I think that a C(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

$$2U^+(K)$$
 If every degree a extension which is ramified at an infinite place is also ramified at a finite place.

1 # $2U(K) \ge \frac{1}{2} = \frac{1}{2}U(K)$ If I a degree a extension which is romified at an infinite place but not a finite place

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

The only rational prime which can ramify to a fourth power is 2, and that only happens when we can write the field as $Q(\overline{1a}, \overline{1a})$, with $a_1 \equiv 2 \pmod{4}$ and $a_2 \equiv 3 \pmod{4}$ (or the other way around).

Let $K = Q(\sqrt{a})$, $\alpha = 2^{\epsilon}p_1 \cdots p_n$ ($\epsilon = 0 \text{ or 1}$) be a real quadratic field. If $\epsilon = 1$:

- (1) If $a_{1/2} \equiv 3 \pmod{4}$ then there is no biquadratic field containing K which is unramified (but genus theory gives 2-torsion since $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_1/2})$ is unramified at finite places.
- (2) If $a/a \equiv 1 \pmod{4}$ then $Q(\sqrt{a}, \sqrt{b})$ with b>0 and b= the product of primes dividing a s.t. b= 1 (mod 4) is unramified → We can do a counting argument to describe $a(l^+(K))$ in terms of # of distinct unramified degree 2 extensions of K!