ideal class group

J_L = abelian group of all fractional ideals.

$$= \left\{ \prod p_i^{e_i} \;\middle|\; \begin{array}{l} e_i \in \mathbb{Z} \\ \text{almost all } 0 \end{array} \right\}$$

P_L = subgp of principal frac. ideals

$$= \{ (a) \mid a \in L^\times \}$$

$Cl(L) = J_L / P_L$ ideal class group

abelian group

Fact: finite gp (prove later)

$h_L = |Cl(L)|$ class number.

$\mathcal{O}_L$ is PID $\iff h_L = 1$.

e.g. $Cl(\mathbb{Z}[\sqrt{5}]) \cong \mathbb{Z}/2\mathbb{Z}$

e.g. $Cl(\mathbb{Z}[\sqrt{-23}]) \cong \mathbb{Z}/3\mathbb{Z}$.

e.g. Thm: Let D be squarefree. Then as $D \to \infty$, we have $|Cl(\mathcal{O}_{-D})| \to \infty$.

$\mathcal{O}_{-D}$ = ring of ints in $\mathbb{Q}(\sqrt{-D})$

$\#\{ D \mid |Cl(\mathcal{O}_{-D})| < K \}$ is finite for all constants K.

e.g. class # 1 imaginary quadratic fields

$D = 1, 2, 3, 7, 11, 19, 43, 67, 163.$

e.g. real quadratic fields

Gauss's conjecture:

$|Cl(\mathcal{O}_D)| = 1$ infinitely often for $D > 0$.

Far from proving this.

In fact don't even know if $|Cl(L)| = 1$ infinitely often as L ranges over all number fields.

$$L^\times \to J_L \to Cl(L) \to 1.$$

$$a \xrightarrow{i} (a)$$

ker of i is $\mathcal{O}_L^\times$ (2)

$$1 \to \mathcal{O}_L^\times \to L^\times \to J_L \to Cl(L) \to 1$$

fundamental exact sequence.

Factorization in extensions

$$\begin{array}{ccc} L & \supset & B \\ | & & | \\ K & \supset & A \end{array}$$

A: Dedekind domain.

K: fraction field

L/K finite, separable extension.

B = integral closure of A in L.

can show: B is also a Dedekind domain.

$p \subset A$ prime ideal.
has a factorization in B.

$$pB = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}$$

$\mathcal{P}_i$ prime ideals in B, distinct.

we say that each $\mathcal{P}_i$ divides p, and we write $\mathcal{P}_i | p$.

Def We say p is unramified in B if all $e_i = 1$. otherwise we say p is ramified.

$e_i = e(\mathcal{P}_i | p)$ is called the ramification index of $\mathcal{P}_i$

Def Suppose $\mathcal{P} | p$. Then $B/\mathcal{P}$, A/p are finite fields.

we get an extension

$$\begin{array}{ccc} B/\mathcal{P} & & \mathbb{F}_{q^f} \\ | & \text{finite extension of finite fields.} & | \\ A/p & & \mathbb{F}_q \end{array}$$

Let $f = f(\mathcal{P}/p)$ be the degree of this extension we call it the residue class degree. The finite fields involved are called the residue fields.

We say that p is split in B if all residue class degrees are 1.

Example $K = \mathbb{Q}$, $A = \mathbb{Z}$

$L = \mathbb{Q}(\sqrt{-2})$, $B = \mathbb{Z}[\sqrt{-2}]$.

choose different primes $p \in \mathbb{Z}$, look at factorization of

$(p)\,\mathbb{Z}[\sqrt{-2}]$

— only ramified prime is $p = 2$.

$(2) = (\sqrt{-2})^2 = \mathfrak{p}^2$

— can show that p is split in L iff $x^2 + 2y^2 = p$ has an integral solution.

$N_{L/\mathbb{Q}}(a + b\sqrt{-2}) = a^2 + 2b^2$

e.g. $17 = 3^2 + 2 \cdot 2^2$

$\Rightarrow (17) = (17, 3 + 2\sqrt{-2})(17, 3 - 2\sqrt{-2})$

$\mathfrak{p}_1 \qquad \mathfrak{p}_2$

$(17) = \mathfrak{p}_1 \mathfrak{p}_2$

$e_1 = e_2 = 1$

$f_1 = f_2 = 1$.

e.g. $7 \neq x^2 + 2y^2$

$\rightarrow$ $(7)\,\mathbb{Z}[\sqrt{-2}] = \mathfrak{p}$

11 same ideal.

i.e. this ideal remains prime.

$|B/(7)| = 49$

$B/(7) \cong \mathbb{F}_{49}$.

$A/(7) \cong \mathbb{F}_7$

residue field extension looks like

$\mathbb{F}_{49}$
| 2.
$\mathbb{F}_7$

$\Rightarrow f = 2.$

Summary.

consider $(p)\mathbb{Z}[\sqrt{-2}]$.

- only ramified prime is $p = 2$.
  $(2) = (\sqrt{-2})^2$
- p splits iff $x^2 + 2y^2 = p$ has an integral solution
  $e_1 = e_2 = 1$, $f_1 = f_2 = 1$
- p remains prime otherwise
  (p is inert).

Cubic examples

(I) $x^3 + x^2 - 2x - 1$ $(3,0)$ totally real cubic field, disc $= 49$.

(II) $x^3 + x^2 - 1$ $(1,1)$ non real cubic, disc $= -23$

deg n, signature (r,s)
$n = r + 2s$.

(I) using computer, we find

(1) 7 is ramified.
nothing else appears to be.

(2) p splits $\Longleftrightarrow p \equiv \pm 1 \bmod 7$
$g = 3$,
all f's $= 1$
all e's $= 1$.

(3) otherwise, (p) is prime.
$g = 1$, $e = 1$, $f = 3$

using computer

(1) 23 is ramified. nothing else appears to be.

(2) some primes appear to split.
e.g. $p = 59, 101, 167, \ldots$
appears to be more rare.

(3) some primes are inert.
$p = 2, 3, 13, 29, \ldots$

(4) others have mixed structure

$(p) = \mathfrak{p}_1\mathfrak{p}_2$ $\quad f(\mathfrak{p}_1/p) = 1$
$\quad\quad f(\mathfrak{p}_2/p) = 2$

$e = 1$. $\quad p = 5, 7, 11, \ldots$