Last time:

L/K Galois of #-fields, $G = \mathrm{Gal}(L/K)$

$\mathfrak{q} \subseteq \mathcal{O}_L$ max'l, $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_K$

$\Rightarrow$ s.e.s.

$$1 \to I(\mathfrak{q}|\mathfrak{p}) \to D(\mathfrak{q}|\mathfrak{p}) \xrightarrow{\varphi_{\mathfrak{q}}} \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \to 1$$

$I(\mathfrak{q}|\mathfrak{p})$: inertia subgroup (at $\mathfrak{q}$)

$D(\mathfrak{q}|\mathfrak{p})$: decomp. group (at $\mathfrak{q}$)

$\mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \cong \mathbb{Z}/f \cdot \mathrm{Frob}_{\mathfrak{q}}$

$q = \#k(\mathfrak{p})$

$f = f(\mathfrak{q}|\mathfrak{p})$

$\#D(\mathfrak{q}|\mathfrak{p}) = f \cdot e$, $e := e(\mathfrak{q}|\mathfrak{p})$

$\#I(\mathfrak{q}|\mathfrak{p}) = e$ ($\rightsquigarrow$ {1} f.a.a. $\mathfrak{q}$)

If $\mathfrak{p}$ unramified ξ

$\Rightarrow$ $\sigma_{\mathfrak{q}} := \varphi_{\mathfrak{q}}^{-1}(\mathrm{Frob}_q) \in G$ (depends on $\mathfrak{q}$)

$c_\mathfrak{p} := \{\sigma_{\mathfrak{q}} \mid \mathfrak{q} \mid \mathfrak{p}\} \subseteq G$ conj. class

(depends only on $\mathfrak{p}$)

If G abelian $\Rightarrow c_\mathfrak{p} = \{\overset{\sigma_\mathfrak{p}}{\overset{\shortparallel}{\sigma_{\mathfrak{q}}}}\}$ $\forall \mathfrak{q} \mid \mathfrak{p}$

Note: 1) $\sigma_{\mathfrak{q}}$ has order $f(\mathfrak{q}|\mathfrak{p})$

In part, $\sigma_{\mathfrak{q}} = 1 \iff c_\mathfrak{p} = \{1\}$

iff $\mathfrak{p}$ is split in $\mathcal{O}_L$

2) $\sigma_{\mathfrak{q}}$ is the unique elt. in G,

s.t. $\sigma_{\mathfrak{q}}(x) \equiv x^q \bmod \mathfrak{q}$ $\forall x \in \mathcal{O}_L$

($\mathrm{Frob}_\mathfrak{q}: k(\mathfrak{q}) \to k(\mathfrak{q})$, $y \mapsto y^q$)

(here $q = \#k(\mathfrak{p})$)

«3)
$$\begin{array}{ccc} L & & \supseteq \mathcal{O}_L \\ \text{Galois} \uparrow & & \\ M & & \supseteq \mathcal{O}_M := \mathcal{O}_L \cap \mathcal{O}_M \\ \downarrow & & \\ K & & G \twoheadrightarrow \mathrm{Gal}(M/K) \end{array}$$

and $\mathfrak{o}_{\mathcal{O}_L, L/K} \longmapsto \mathfrak{o}_{\mathcal{O}_M, M/K}$ (by 2)

$$\begin{array}{ccc} \uparrow & & \uparrow \\ G & & \mathrm{Gal}(M/K) \end{array}$$

(note: $\mathcal{O}_M$ unramified over $\mathfrak{p}$)

3.5. Prime decom. in cyclotomic fields

$N \geq 3$, $K := \mathbb{Q}(\zeta_N)$

Thm: 1) $p \in \mathbb{Z}$ prime is ramified in K iff $p \mid N$ $K/\mathbb{Q}$

2) If $p \nmid N$, $* \sigma_p \in \mathrm{Gal}(K/\mathbb{Q})$

corresponds to $p \in (\mathbb{Z}/N)^\times \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q})$

Proof: 1) ✓ $\{$prime divisors of $\Delta_K\}$

$= \{$prime div. of $N\}$

2) Fix prime p, $p \nmid N$

Let $\sigma \in Gal(K/\mathbb{Q})$, s.t.

$\sigma(\zeta_N) = \zeta_N^p$ ($\sigma \hookrightarrow p$ under $Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/N)^\times$)

$\Rightarrow \sigma(x) \equiv x^p \bmod p \cdot \mathcal{O}_K = p \cdot \mathbb{Z}[\zeta_N]$

$\forall x \in \mathcal{O}_K = \mathbb{Z}[\zeta_N]$

$\Rightarrow \forall \mathfrak{a} \mid p$ in $\mathcal{O}_K$, $\sigma \in D(\mathfrak{a}|p)$

$\&\ \sigma(x) \equiv x^p \bmod \mathfrak{a}$ $\forall x \in \mathcal{O}_K$

$\Rightarrow \sigma = \sigma_{\mathfrak{a}}$ $\forall \mathfrak{a} \mid p$

∎

Cor: $p \nmid N$ p is split in in $\mathbb{Q}(\zeta_N)$

iff $p \equiv 1 \ (N)$ $\quad (\mathbb{Z}/2)^\times = \{1\}$

E.g.: $N = 4$ $\quad ((\mathbb{Z}/3)^\times \simeq (\mathbb{Z}/6)^\times)$

$\Rightarrow$ p split in $\mathbb{Z}[i]$

$(\Leftrightarrow p = x^2 + y^2, \ x, y \in \mathbb{Z})$

$\mathbb{Z}[i]$ PID

$\Leftrightarrow p \equiv 1 \ (4)$

Lemma: p odd prime

$\Rightarrow$ $\mathbb{Q}(\zeta_p)$ contains a unique quadratic field

$$K = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } p \equiv 1 \ (4) \\ \mathbb{Q}(\sqrt{-p}) & \text{if } p \equiv 3 \ (4) \end{cases}$$

Pf: $\#(\mathbb{Z}/p)^\times = p-1$, λ $\#(\mathbb{Z}/p)^\times$ cyclic

$\Rightarrow$ ex. + uniqueness clear

Note only p can ramify in K
(as p # is the only prime ramified in $\mathbb{Q}(\zeta_p)$)

$\Rightarrow \Delta_K \mid p \Rightarrow$

Def: p prime, $n \in \mathbb{Z}$, $p \nmid n$

$$\Rightarrow \left(\frac{n}{p}\right) := \begin{cases} 1, & \text{if } x^2 - n \equiv 0 \text{ has sol. mod } p \\ -1, & \text{otherwise} \end{cases}$$

Ex: i) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 (4) \\ -1, & p \equiv 3 (4) \end{cases}$

ii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv 1, 7 (8) \\ -1, & p \equiv 3, 5 (8) \end{cases}$

Thm (Quadratic reciprocity law)
p, q odd primes, $p \neq q$

$$\Rightarrow \left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{2}}$$

$$= \begin{cases} 1, & \text{if } p \text{ or } q \equiv 1 (4) \\ -1, & \text{otherwise} \end{cases}$$

Proof: Set $p^* := (-1)^{\frac{p-1}{2}} p$

$(\leadsto p^* \equiv 1 \pmod 4$, $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p))$

STP w.r.t. $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$

$\left(\frac{p^*}{q}\right) = 1 \iff x^2 - p^* \equiv 0 \bmod q$ has a solution

$\iff$ q splits compl. in $\mathbb{Q}(\sqrt{p^*})$

Kummer

$\iff$ $\sigma_{q, \mathbb{Q}(\sqrt{p^*})} \in \mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$ is trivial

$\iff$ $\sigma_{q, \mathbb{Q}(\zeta_p)} \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ lies in kernel

$(\mathbb{F}_p^\times)^2 = \ker(\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}))$

$\mathbb{F}_p^\times \simeq \mathbb{Z}_{p-1} \twoheadrightarrow \mathbb{Z}_2$

~~Progr. prop~~

~~$\iff$~~

$\Leftrightarrow \left(\frac{q}{p}\right) = 1$

prev. prop. ∎

Note: 1) $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \{\pm 1\}$

identifies with surj.

$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$

In part,

$$\left(\frac{n \cdot m}{p}\right) = \left(\frac{n}{p}\right) \cdot \left(\frac{m}{p}\right) \quad \forall n, m \\ p \nmid n, m$$

2) $D \in \mathbb{Z}$ squarefree

$K = \mathbb{Q}(\sqrt{D})$

* p ramifies in $K \Leftrightarrow p \mid \Delta_K$
* If $p = 2$, p unramified ($\rightsquigarrow D \equiv 1 (4)$)

$\omega_D := \frac{1 + \sqrt{D}}{2}$

has min. poly

$$X^2 - X + \frac{1-D}{4} \equiv X^2 + X + 1 \pmod 2$$

$$\equiv X^2 + X \pmod 2$$

$\Rightarrow$ p inert in K, $D \equiv 5 \pmod 8$

split : $D \equiv 1 \pmod 8$

* p odd unramified in K $(p \nmid D)$

p splits $\iff$ $x^2 - D \equiv 0$ has sol. mod p

Kummer

$$\iff \left(\frac{D}{p}\right) = 1$$

E.g: $D = 32\frac{3}{4} = 17 \cdot 19$, $p = 7$

$$\Rightarrow \left(\frac{D}{p}\right) = \left(\frac{17}{7}\right)\left(\frac{19}{7}\right)$$

$$= \left(\frac{3}{7}\right)\cdot\left(\frac{5}{7}\right) = \left(\frac{7^*}{3}\right)\cdot\left(\frac{7}{5}\right)$$

$$= \left(\frac{2}{3}\right)\cdot\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1$$

$\Rightarrow$ 7 splits in K

More gen, $p \neq 17, 19$

$$\left(\frac{D}{p}\right) = \left(\frac{17}{p}\right)\cdot\left(\frac{19}{p}\right) = \left(\frac{p}{17}\right)\cdot\left(\frac{p}{19}\right)$$

depends only on the residue class of $p \bmod D = 323$

p is split in $K \Leftrightarrow p \equiv \ldots\ldots \pmod{323}$

/ Similar to $K = \mathbb{Q}(i)$ /

Thm (Kronecker-Weber)

$K/\mathbb{Q}$ abelian $\Leftrightarrow K \subseteq \mathbb{Q}(\zeta_N)$ for some $N \geq 1$

(N can be chosen to have same prime divisors as Δ_K)

$\Rightarrow$ understand how primes split in abelian ext. of $\mathbb{Q}$ theoret.

answer in terms of congruences modulo N

Langlands programme

$\Rightarrow$ For $K/\mathbb{Q}$ Galois

the answer should be (roughly) in terms of coeff. of modular forms

Say $K/\mathbb{Q}$ has Galois group S_3

K — Assume K' imaginary

$\downarrow$

K' $\Rightarrow$ LP $\exists$ modular form $f = \sum_{n=1}^{\infty} a_n q^n$

$|$ $\ast \mathbb{Z}/2$

$\mathbb{Q}$

s.t. p split in K iff $a_p = 2$

(for almost all p)

4.1. Finiteness thm

Aim: Minkowski bound
$\Rightarrow$ finiteness of class number

Thm: $K/\mathbb{Q}$ finite, $n = [K:\mathbb{Q}]$, $r_2 = \#$ pairs of cplx. emb.

Then every ideal class in Cl_K contains an ideal $\alpha \subseteq \mathcal{O}_K$ with

$$N(\alpha) \leq \underbrace{\left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \sqrt{|\Delta_K|}}_{\text{Mink. bdd.}}$$

In part, $\#Cl_K < \infty$

$\Rightarrow$ Can compute Cl_K in some cases

1) Ex $K = \mathbb{Q}(\sqrt{-5})$

Recall: $\mathfrak{p}_1 = (3, \sqrt{-5} - 1) \subseteq \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$
not princ.

$\mathfrak{p}_1^2 = (2, \sqrt{-5})$ principal $\quad \mathfrak{p}_2 = \overline{\mathfrak{p}_1}$, $\mathfrak{p}_1 \cdot \mathfrak{p}_2 = (3)$ (13)

$\Delta_K = -20$, $n = 2$, $r_2 = 1$

$\Rightarrow$ Cl_K gen. by $\mathfrak{a} \subseteq \mathcal{O}_K$ with

Minkowski bound $N(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right) \cdot \frac{2}{4} \cdot 2\sqrt{5} < 4$

$\Rightarrow$ Cl_K has at most 4 elements

namely $[\mathcal{O}_K]$, $[\mathfrak{q}]$, $[\mathfrak{p}_1] = [\mathfrak{p}_2]$

($\mathfrak{q}$: unique prime above (2))

$\Rightarrow$ $Cl_K = \mathbb{Z}/2 \cdot [\mathfrak{p}_1] = \mathbb{Z}/2[\mathfrak{q}]$

2) $K = \mathbb{Q}(\sqrt[3]{2})$ $\Rightarrow$ $n = 3$, $r_2 = 1$, $\Delta_K = -2^2 \cdot 3^3$

$\Rightarrow$ Minkowski $d = \left(\frac{4}{\pi}\right) \frac{3!}{3^3} \sqrt{3^3 \cdot 2^2} < 3$

$N(\mathfrak{a}) = 2 \Rightarrow \mathfrak{a} = (\sqrt[3]{2})$

$\mathfrak{a} \subseteq \mathcal{O}_K$

$\Rightarrow Cl_K = 1$ $\quad (K = \mathbb{Q}(\sqrt[3]{2}))$