Last time, proved Kronecker-Weber Thm using main thm. of local CFT.

Guaranteed any abelian extn $L/\mathbb{Q}$ is contained in cyclotomic extn $\mathbb{Q}(\zeta_n)$

(even understood that n in terms of ramified parts of local extns)

Do example showing how K-W thm can be used to determine splitting:

$L = \mathbb{Q}(\sqrt{p})$. $p \equiv 1\ (4)$ $\mathrm{Disc}(L) = p$. (not $4p$).

What is n s.t. $L \subseteq \mathbb{Q}(\zeta_n)$? Could study ramification, or compute

$$\mathrm{disc}(\mathbb{Q}(\zeta_p)) = (-1)^{p-1/2}\, p^{p-2}$$

which is square of elt. in $\mathcal{O}_L$.

so $\mathbb{Q}(\sqrt{\underbrace{(-1)^{p-1/2} p^{p-2}}}) \subseteq \mathbb{Q}(\zeta_p)$

$\sqrt{\pm p}$ if $p \equiv 1, 3\ (4)$

Or use "Gauss sum"

$$\sum_{a \,(\mathrm{mod}\, p)} \left(\frac{a}{p}\right) \underbrace{e^{2\pi i a/p}}_{\zeta_p^a} = \sqrt{p}$$

(up to 4^{th} root of unity)

exactly if $p \equiv 1\ (4)$.

So $L \subseteq \mathbb{Q}(\zeta_p)$, can't have any smaller n since p. prime.

so have natural map: $\left(\frac{L}{\cdot}\right) : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow \mathrm{Gal}(L/\mathbb{Q})$

$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

$\left(\frac{L}{a}\right) : a \longmapsto (\zeta \mapsto \zeta^a)$ restricted to L

If $L = \mathbb{Q}(\sqrt{p})$, $\mathrm{Gal}(L/\mathbb{Q}) \cong \{\pm 1\}$

then have surjective hom:

$(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow\!\!\!\!\rightarrow \{\pm 1\}$ with kernel the unique index 2 s.bgp in our cyclic gp. the square classes

so $a \longmapsto \left(\frac{a}{p}\right)$

Call it I_L.

When does a prime q split completely? If $e, f = 1$ in factorization above q.

If $q \nmid \mathrm{disc}(L)$, then $e_q = 1$. and f_q = order of $q \cdot I_L$ in $(\mathbb{Z}/n\mathbb{Z})^\times / I_L$.

For us $(\mathbb{Z}/p\mathbb{Z})^\times / I_L \simeq \{\pm 1\}$ under hom.

and sends $q \longmapsto \left(\frac{q}{p}\right)$.

i.e. q splits completely $\Longleftrightarrow$ $q \neq p$ and q among quad. res. mod p.

so only depends on modulus p, the order of ζ_p.

Neukirch proves Q.R. earlier in book using similar connection to cyclotomic fields.

Nice theorem on how set of primes that split characterize Galois extn:

Thm: K_f, K_g be normal extns corresp. to min polys f, g.

$Spl(f)$, $Spl(g)$ set of primes that split completely.

Then $K_f \supseteq K_g \Longleftrightarrow Spl(f) \subseteq^* Spl(g)$ where $\subseteq^*$ means containment is up to finitely many exceptions.

pf: $(\Rightarrow)$ mult. of e, f in towers.

$(\Leftarrow)$ Tchebotarev density thm. — result of analytic techniques you'll learn next semester.

In our example: $Spl(L = \mathbb{Q}(\sqrt{p}))$: $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = 1$

$Spl(\mathbb{Q}(\zeta_p))$: $q \equiv 1 \ (p)$ $\rightsquigarrow$ so residue field mod q has p^{th} roots of unity.

To connect to Global CFT: Bundle together local fields:

K: Global field. K_v: completions w.r.t. valuation v.

$$\mathbb{A}_K := \prod_{v:\text{val}}' K_v$$ where $'$ means that elts in $\mathbb{A}_K$ must be in compact gp. $\mathcal{O}_v$: val. ring, for almost all v.

(permits harmonic analysis with measure s.t. $\mu(\mathcal{O}_v)=1$)

$\mathbb{A}_K^\times$: units of $\mathbb{A}_K$ – "idèles" I_K

$$:= \prod_{v:\text{val}}' K_v$$ so $'$ means elts are units in $\mathcal{O}_v^\times$ at almost all v.

$K^\times$ embeds diagonally $a \mapsto (a, a, \dots) \in I_K$ "principal idèles"

and $I_K / K^\times$: idèle class gp. ($=$ ideal class gp. with extra info at infinite places)

this is module A_K in our abstract class field theory framework.

$$\alpha = (\alpha_v)_{v:\text{val}} \mapsto \prod_{\mathfrak{p}:\text{fin}} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})}$$

d, v maps come from products of local d, v maps.

(well-defined since elts live in restricted tensor prods.)

Given ideal $\mathfrak{m} = \prod_i \mathfrak{p}_i^{e_i} \rightsquigarrow I_K^\mathfrak{m} = \prod_\mathfrak{p} U_\mathfrak{p}^{(e_\mathfrak{p})}$ with $U_\mathfrak{p}^{(0)} = U_\mathfrak{p}$.

then $A_K^\mathfrak{m} = I_K^\mathfrak{m} \cdot K^\times / K^\times$ are closed subgps of finite index in A_K: idèle class gp.

If $K = \mathbb{Q}$, $A_\mathbb{Q} / A_\mathbb{Q}^{\mathfrak{m}=(m)} \cong (\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.

In general, there will be a class field $K^{m} \longleftrightarrow A_K^{m} \subseteq A_K$

"ray class field"

in 1-1 correspondence of Global CFT sending abelian extns of K to ~~closed~~ open subgps of finite index in A_K.

so ray class fields of $\mathbb{Q}$ $\leftrightarrow$ gen'd by cyclotomic fields

(closed subgps of finite index in A_K)

Difficult open problem to find generating set of elts for ray class fields over # field K. If K : imag. quadratic, adjoin to K special values of the elliptic functions on the lattice of integers $\mathcal{O}_K \subseteq \mathbb{C}$.