Algebra II:

Cyclotomic Extns:

μ_n = group of n-th r.o.u.

We've seen: ζ_n primitive n-th r.o.u. $\rightsquigarrow \mu_n = \langle \zeta_n \rangle$.

$\Phi(\zeta_n) = spl_{\mathbb{Q}}(x^n - 1)$, order of $\zeta_n^a = \frac{n}{(n,a)}$.

and $\left(x^n - 1, \frac{d}{dx}(x^n - 1)\right) = (x^n - 1, n x^{n-1}) = 1$

$\Rightarrow x^n - 1$ separable $\rightsquigarrow \mathbb{Q}(\zeta_n)/\mathbb{Q}$ Galois.

We saw also: min poly $_{\mathbb{Q}}(\zeta_n) = \Phi_n(x) := \prod_{\substack{\text{primitive} \\ n\text{-th r.o.u. } \zeta}} (x - \zeta)$

$= \prod_{\substack{(a,n)=1 \\ 1 \le a \le n}} (x - \zeta_n^a) \in \mathbb{Z}[x] \Rightarrow [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

More generally, if K is a field, as long as

$\mathrm{char}(K) = 0$ or $(\mathrm{char}(K), n) = 1$,

then $x^n - 1 / K$ is separable ($n x^{n-1} \neq 0$ in K).

$\Rightarrow K(\mu_n) = spl_K(x^n - 1)$ is Galois $/K$.

Moreover, $\mu_n \subseteq K(\mu_n)^\times$ is a finite subgroup of units in a field

$\Rightarrow \mu_n$ is cyclic, $\mu_n = \langle \zeta_n \rangle$ some generator ζ_n.

$\Rightarrow K(\mu_n) = K(\zeta_n)$.

Lemma: ~~the map $Gal(K(\zeta_n)/K) \longrightarrow \mathbb{Z}_n^\times$~~

$\sigma \longmapsto$

Note: If $\sigma \in Gal(K(\zeta_n)/K)$, then $\sigma(\zeta)$ must be a primitive n-th root of unity (generator of μ_n)!

As $\zeta_n^n = 1$, $\zeta_n^j \neq$ $\forall\ 1 \leq j \leq n$ (σ injective)

$\Rightarrow \sigma(\zeta_n)^n = 1$, $\sigma(\zeta_n)^j \neq 1$ $\forall\ 1 \leq j \leq n$.

$\Rightarrow \sigma(\zeta_n)$ primitive $\Rightarrow |\sigma(\zeta_n)| = n$, say $\sigma(\zeta_n) = \zeta_n^a$

$\Rightarrow \frac{n}{(n,a)} = n \Rightarrow \boxed{(n,a) = 1}$

Now all $\zeta \in \mu_n$ are ζ_n^k, some k

$\Rightarrow \sigma(\zeta) = \sigma(\zeta_n^k) = \sigma(\zeta_n)^k = (\zeta_n^a)^k$

$= (\zeta_n^k)^a = \zeta^a$ $\forall$ ~~ζ~~ $\zeta \in \mu_n$

i.e., σ acts on μ_n as $\zeta \mapsto \zeta^a$.

Associate this # a to σ, call it σ_a.

Lemma: The map $\sigma \mapsto \sigma_a$ is an injective

$$\mathrm{Gal}(K(\mu_n)/K) \hookrightarrow \mathbb{Z}_n^\times.$$

Pf: If $\sigma, \tau \in \mathrm{Gal}(K(\mu_n)/K)$, on a generator:

$(\sigma\tau)(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{a_\tau}) = \sigma(\zeta_n)^{a_\tau}$

$= \zeta_n^{a_\sigma a_\tau}$.

Also, $(\sigma\tau)(\zeta_n) = \zeta_n^{a_{\sigma\tau}} \Rightarrow \zeta_n^{a_{\sigma\tau}} = \zeta_n^{a_\sigma a_\tau}$

As $|\mu_n| = n$, $a_{\sigma\tau} \equiv a_\sigma a_\tau \pmod n$ $\Rightarrow$ the map is a hom.

To check injective, check trivial kernel:

If $a_\sigma \equiv 1 \pmod n$, then $\sigma(\zeta_n) = \zeta_n$

$\Rightarrow \sigma$ fixes $\mu_n \Rightarrow \sigma$ fixes $K(\mu_n) \Rightarrow \sigma = \mathrm{id} \in \mathrm{Gal}(K(\mu_n)/K)$

Special Case: $k = \mathbb{Q}$.

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

Pf: We just need that the map above is surjective. But we know

$$|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n) = |\mathbb{Z}_n^\times| \Rightarrow \square$$

This is false for more general fields.

But can say $K(\zeta_n)/K$ is abelian (ab. Gal. gp.) in general. (as $\mathrm{Gal} \cong$ a subgp of $\mathbb{Z}_n^\times$).

Abelian gps are a bit hard to find in general.

Amazing Thm (Kronecker–Weber)

All finite abelian ext'ns of $\mathbb{Q}$ are contained in a cyclotomic field.

Ex: $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, $d \neq \square$ is always Galois (normal is clear as $= \sqrt{d}$ comes "free"), deg. $= 2 \Rightarrow$ always abelian.

So $\mathbb{Q}(\sqrt{d})$ must lie in some $\mathbb{Q}(\zeta_n)$.

Special case: $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$.

Explicitly, the quadratic Gauss sum

$$\text{(*)} \quad \sum_{k=0}^{p-1} \zeta_p^{k^2} = \begin{cases} \sqrt{p}, & p \equiv 1 \ (4) \\ \sqrt{-p}, & p \equiv 3 \ (4) \end{cases}$$

"finds" square roots, and can use these to find all $\sqrt{\ }$'s in cyclotomic fields.

(+ the facts that $i = \zeta_4$, $\sqrt{2} = \zeta_8 + \zeta_8^7$).

Hilbert's 12th problem: Given a # field K.

Find a transcendental fn "generating" all abelian ext^{ns}.

Kronecker-Weber $\Rightarrow$ $K \subset \mathbb{Q}$ use $e^{2\pi i x}$.

Kronecker's Jugendtraum: $\mathbb{Z}$

$K = \mathbb{Q}(\sqrt{-d})$, imaginary quadratics.

use a modular form, $j(\tau)$.

(related to "my favorite #" $e^{\pi\sqrt{163}} = 262537\,412640\,768\,743.$
$999999\,999999\,25\ldots$

Brand new (2023) work: Dasgupta, Kakde, Sillima, totally real fields (like real quadratics), using Hilbert modular forms

Ex: $\mathrm{Gal}(\mathbb{F}_2(\zeta_7)/\mathbb{F}_2)$. This is a finite field, so it's generated by the Frobenius elt.

Thus, we see what powers of Frob_2 do to ζ_7:

$\zeta_7 \mapsto \zeta_7$ (id)

$\zeta_7 \mapsto \zeta_7^2$ (Frob_2)

IV

$\zeta_7 \mapsto \zeta_7^4$ (Frob_2^2)

$\zeta_7 \mapsto \zeta_7^8 = \zeta_7$ (Frob_2^3)

$\Rightarrow \mathrm{Frob}_2^3 = id \Rightarrow \exists$ 3 automorphisms of $\mathbb{F}_2(\zeta_7)$

$\Rightarrow [\mathbb{F}_2(\zeta_7) : \mathbb{F}_2] = 3$, and the Galois group is a proper subgp. of $\mathbb{Z}_7^\times$.

In particular, ζ_7, ζ_7^3 are both primitive 7th roots in $\mathbb{F}_2$, but are not conjugate.

What we're saying over $\mathbb{Q}$ is that all primitive nth roots of unity are conjugate. (We're constructed a minimal poly of $\zeta_n/\mathbb{Q}$ to be the one w/ these as roots, so it really comes from there, which is the non-trivial heart of the surjectivity onto $\mathbb{Z}_n^\times$).

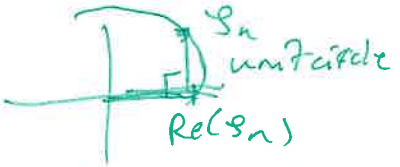
Constructibility of regular n-gons:

Recall: We showed $\alpha \in \mathbb{R}$ is constructible $\iff$ α is contained in a 2-tower ext^n

$$\mathbb{Q}(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_r})$$
$$\vdots \ 2$$
$$\mathbb{Q}(\sqrt{\alpha_1})$$
$$2$$
$$\mathbb{Q}$$

Constructing the regular n-gon in the plane is the same as constructing the n-th roots of unity (as then we just draw lines b/w them).

To do this is equivalent to constructing the real pt. of ζ_n (x-coordinate).



Now $\mathrm{Re}(\zeta_n) = \frac{1}{2}(\zeta_n + \overline{\zeta_n}) = \frac{1}{2}(\zeta_n + \zeta_n^{-1})$.

So we study

$$\mathbb{Q}\left(\tfrac{1}{2}(\zeta_n + \zeta_n^{-1})\right) \subseteq \mathbb{Q}(\cos(2\pi/p))$$

↑ maximal totally real in $\mathbb{Q}(\zeta_n)$!

We showed before that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\tfrac{\zeta_n + \zeta_n^{-1}}{2})] = 2$.

As before, we see that the degree of $\cos(2\pi/p)/\mathbb{Q}$ must be a power of 2.

$\Rightarrow \varphi(p^n)$ is a power of 2

$\Rightarrow n = 2^k \cdot p_1 \cdots p_r$, $k \geq 0$,

p_j Fermat primes of form $2^m + 1$.

Conversely, if $\varphi(n)$ is a power of 2, say, $\varphi(n) = 2^m$, then $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian, order 2^m, so $\mathrm{Gal}(\mathbb{Q}(\zeta_n + \zeta_n^{-1})/\mathbb{Q})$ is abelian, and a 2-gp.

G. //

By the fund. Th^{m} of finite abelian gps,

$\exists$ chain of subgps.

$$G = G_m > G_{m-1} > \cdots > G_0 = 1$$

where $[G_{i+1} : G_i] = 2$, $i = 0, \ldots, m-1$.

Galois Theory $\Rightarrow$ a corresponding tower of field exts:

$$\mathbb{Q} = k_0 \overset{2}{\subseteq} k_1 \overset{2}{\subseteq} \cdots \overset{2}{\subseteq} k_m = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$$

where each degree is $2 \Rightarrow$ each is adjoining a square root $\square$