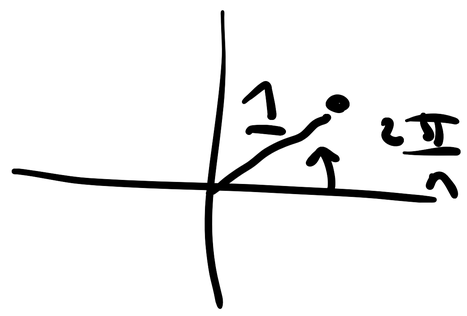
Lec 23 3/5/2021

Cyclotomic extensions.

Work inside $\mathbb{C}$

$$\mu_n = \left\{ e^{2\pi mi/n} \;\middle|\; 0 \le m \le n-1 \right\}$$

$= \{$ set of powers of $e^{2\pi i/n}$



$=$ nth roots of 1 in $\mathbb{C}$

$=$ all roots of $x^n - 1$ in $\mathbb{C}$.

a subgroup of $\mathbb{C}^\times$ (under mult.) $\cong \mathbb{Z}_n$.

$\zeta \in \mu_n$ is a <u>primitive</u> nth root if $\langle \zeta \rangle = \mu_n$ as groups.

Recall generators of $(\mathbb{Z}_n, +)$ are $\{ \overline{j} \mid \gcd(j,n) = 1 \}$.

So primitive nth roots of 1 are

$$\left\{ e^{2\pi i m/n} \;\middle|\; \gcd(m,n) = 1 \right\}$$

there are $\varphi(n)$ of them.

Def. Let $P_n = \{ e^{2\pi m i/n} \mid \gcd(m,n) = 1 \}$

= set of prim. nth roots.

$$\Phi_n(x) = \prod_{\alpha \in P_n} (x - \alpha) \in \mathbb{C}[x]$$

so $\deg \Phi_n(x) = \varphi(n)$.

Lemma. Let $n \geq 1$. Then

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

Pf. if ζ is an nth root of 1, $|\zeta| = d$

for some $d \mid n$, and then $\zeta \in P_d$.

Ex. $\Phi_1(x) = (x - 1)$

$$\Phi_2(x) = (x + 1)$$

$$\Phi_3(x) = \frac{x^3 - 1}{\Phi_1(x)} = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

$$\Phi_4(x) = \frac{x^4-1}{\Phi_2(x)\Phi_1(x)} = \frac{x^4-1}{(x-1)(x+1)}$$

$$= \frac{x^4-1}{x^2-1} = x^2+1.$$

$$\Phi_6(x) = x^2-x+1$$

---

if p is prime, then

$$\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1}+\cdots+x+1$$

$= \text{minpoly}_{\mathbb{Q}}(\zeta)$ $\zeta = e^{2\pi i/p}$.

So $\Phi_p(x)$ is irr. / $\mathbb{Q}$.

Thm. For all $n \geq 1$, $\Phi_n(x) \in \mathbb{Z}[x]$ and it is monic and irreducible over $\mathbb{Q}$.

(pf in note)

Thm. $n \geq 1$. Consider the nth cyclotomic field $K = \mathbb{Q}(\zeta)$ where ζ is a primitive nth root of 1.

then $[K:\mathbb{Q}] = \varphi(n)$, $K/\mathbb{Q}$ is Galois, and $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_n^*$ = mult. group of units mod n.

Pf: K is the splitting field of $x^n - 1$ over $\mathbb{Q}$; because its roots are $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$. So $K/\mathbb{Q}$ is Galois.

Since $\overline{\Phi}_n(x)$ is irreducible over $\mathbb{Q}$ it = minpoly$_{\mathbb{Q}}(\zeta)$

so $[\mathbb{Q}(\zeta):\mathbb{Q}] = \deg \overline{\Phi}_n = \varphi(n)$.

if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then σ is determined by it action on ζ, and $\sigma(\zeta)$ is another root of $\overline{\Phi}_n(x)$, ζ^m where $\gcd(m,n) = 1$.

There are $\varphi(n)$ choices, and $|\mathrm{Gal}(K/\mathbb{Q})| = \varphi(n)$, so all occur.

For each $0 \le m \le n$ with $\gcd(m,n) = 1$

Here is $\sigma_m \in \mathrm{Gal}(K(\Phi))$ s.t.

$$\sigma_m(\varphi) = \varphi^m.$$

So $\mathrm{Gal}(K(\Phi)) = \{\sigma_m \mid 0 \le m \le n,\ \gcd(m,n)=1\}$

Now notice

$$\sigma_m \sigma_j(\varphi) = \sigma_m(\varphi^j)$$

$$= \sigma_m(\varphi)^j = (\varphi^m)^j = \varphi^{mj}$$

$$= \varphi^s \quad \text{where } 0 \le s \le n \quad s \equiv mj \pmod n.$$

$$\sigma_m \sigma_j = \sigma_s$$

Then $\phi : \mathbb{Z}_n^* \longrightarrow \mathrm{Gal}(K(\Phi))$

$$\overline{m} \longmapsto \sigma_m$$

is an isomorphism of groups.

Recall $\mathbb{Z}_n^* \cong \prod \mathbb{Z}_{p_i^{e_i}}^*$ if

$n = p_1^{e_1} \cdots p_m^{e_m}$ p_i distinct primes.

$\mathbb{Z}_{p_i^{e_i}}^*$ is cyclic of order $p_i^{e_i} - p_i^{e_{i-1}}$

if p_i is odd

$$\mathbb{Z}_{2^n}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}.$$

Ex. $n = 9$. $K = \mathbb{Q}(\zeta)$

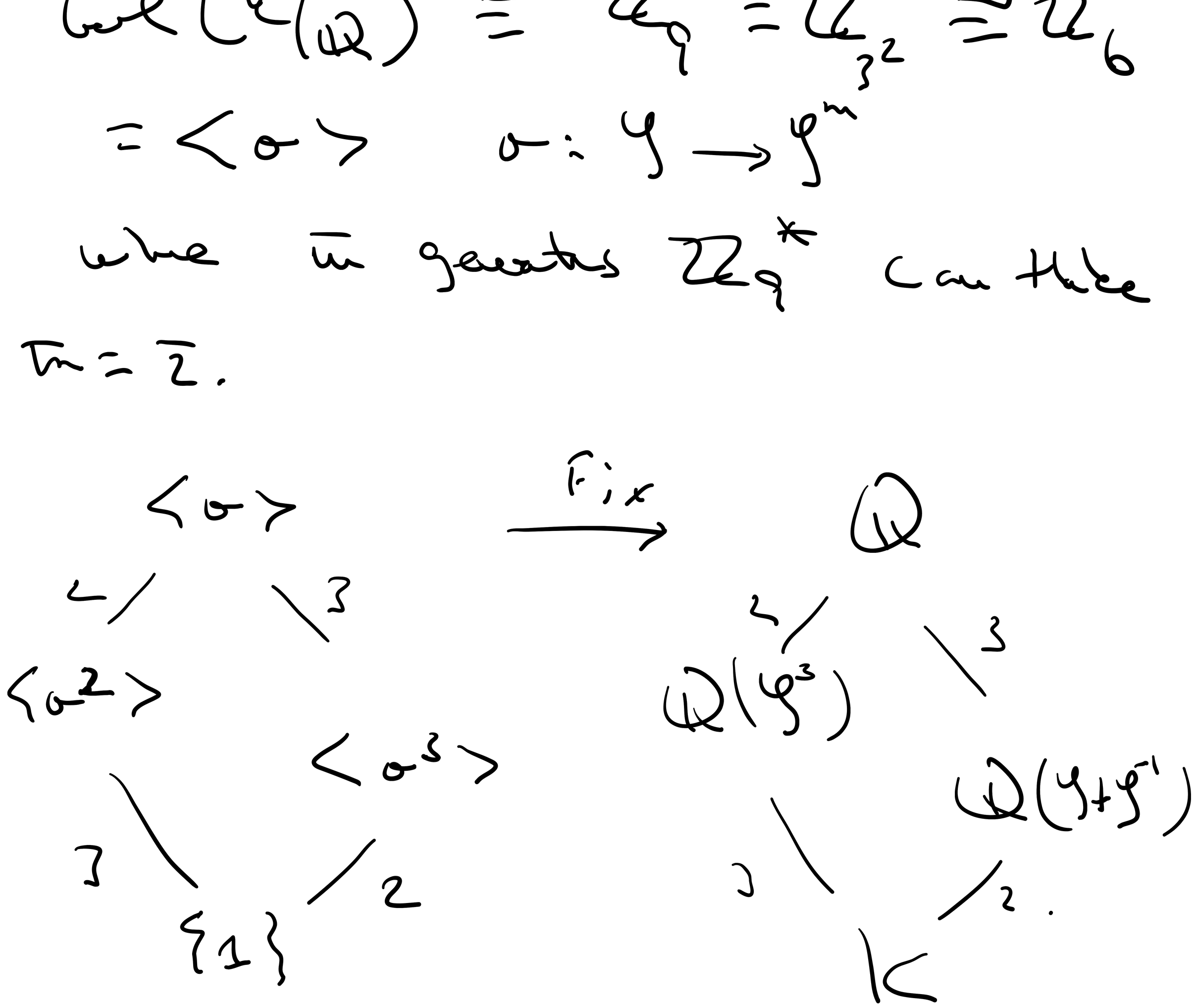
ζ prim 9th root.

$$\mathrm{Gal}(K(\mathbb{Q})) \cong \mathbb{Z}_9^* = \mathbb{Z}_{3^2}^* \cong \mathbb{Z}_6$$

$$= \langle \sigma \rangle \qquad \sigma : \zeta \to \zeta^m$$

where m generates $\mathbb{Z}_9^*$ can take

$m = 2$.



note ζ^3 is a prim. 3rd root of 1.

So $\mathbb{Q}(\zeta^3) \subseteq \mathbb{Q}(\zeta)$

$$[\mathbb{Q}(\zeta^7) : \mathbb{Q}] = 2.$$

Note that $\zeta + \zeta^{-1} = \zeta + \zeta^8$

is fixed by σ^3 w.l.

$$\sigma^3(\zeta + \zeta^8) = \sigma^3(\zeta + \sigma^3(\zeta))$$
$$= \sigma^3(\zeta) + \zeta = \zeta^8 + \zeta.$$

So $\zeta + \zeta^{-1} \in \mathrm{Fix}(\langle \sigma^3 \rangle)$

just need $\zeta + \zeta^{-1} \notin \mathbb{Q}$ since

if it were, $\zeta + \zeta^{-1} = q \in \mathbb{Q}$

$$\zeta^2 + 1 = q\zeta$$

So ζ satisfies a poly of deg 2

over $\mathbb{Q}$. $\min\text{poly}_{\mathbb{Q}}(\zeta) = \deg 6$ X

Recall, the field with p^n elements

p a prime is the splitting field of

$x^{p^n} - x$ over $\mathbb{F}_p$.

Write this field as $\mathbb{F}_{p^n}$.

Thm. $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$ and $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_n$ with $\sigma : \mathbb{F}_p^{\times} \to \mathbb{F}_p^{\times}$ as a generator.

$$a \longmapsto a^p$$

Pf. We've seen σ is an aut. of any finite field of characteristic p. If $a \in \mathbb{F}_p$, $\sigma(a) = a$ since $a^p = a$ by Fermat's little thm. $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

We've seen $\mathbb{F}_{p^n} = \mathbb{F}_p(\gamma)$ for some γ, we can choose γ as a generator of $\mathbb{F}_{p^n}^{\times}$ under mult.

Then $\gamma^{p^n-1} = 1$ $|\gamma| = p^n - 1$.

So $\gamma^i \neq \gamma$ for $i < p^n$.

Now $\sigma i(\gamma) = \gamma^{p^i} \neq \gamma$

for $0 < i < n$.

So $|\sigma| = n$. $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n =$

$|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|$.

So $\langle \sigma \rangle = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Cor. $\mathbb{F}_{p^n}$ has a unique subfield of order p^d for each $d \mid n$, and these are the only subfields.

Pf. $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_n$ has one subgroup of order d

for each divisor d of n.

Then we get one subfield E with $[E : \mathbb{F}_p] = d$ for each divisor d of n. Then $|E| = p^d$.

In fact E = splitting field of $X^{p^d} - X$ inside $\overline{\mathbb{F}}_{p^n}$

i.e. $E = \{ a \in \overline{\mathbb{F}}_{p^n} \mid a^{p^d} = a \}$.

Prop. $X^{p^n} - X \in \mathbb{F}_p(X)$ is the product of all monic irreducible polys over $\mathbb{F}_p$ of degree d dividing n.

Ex. $x^8 - x \in \mathbb{F}_2[x]$.

= product of all deg 1, deg 3

irreducibles over $\mathbb{F}_2$ $\quad 8 = 2^3$

$$= (x-1)x(x^3+x+1)(x^3+x^2+1)$$