lect 19 Midterm 2 next Monday.

$F \subset E$ $\quad E$ vs$/F$

$\mathbb{F}_p \to \overline{\mathbb{F}_p}$

$\bigcup_{n\geq 0} \mathbb{F}_{p^n}$ $\quad \mathbb{F}_{p^k} \subset \mathbb{F}_{p^{km}}$

$k \mid km$

$|E| = |F|^n$

$\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^6}$

$\subset \mathbb{F}_{p^3}$

$\subset \mathbb{F}_{p^5} - \mathbb{F}_{p^{30}}$

$\mathbb{F}_q$ $\quad \mathbb{F}_{p^n}$

$$\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^6} \subset \mathbb{F}_{p^{24}} \subset \mathbb{F}_{p^{120}} \subset \cdots \subset \mathbb{F}_{p^{n!}}$$

$2=2!$ $\quad 6=3!$ $\quad 24=4!$ $\quad 5!$

$\forall m$ $\quad m \mid n!$ $\quad m \mid m!$ $\quad \mathbb{F}_m$

single chain of inclusions

$\mathbb{F}_p$ $\quad \mathbb{F}_{p^m}$ splitting field of $x^{p^m} - x$

$\parallel$

sp. field $\forall$ irr. $f(x) \in \mathbb{F}_p[x]$ deg m

$\mathbb{F}_{p^{n!}} \subset \mathbb{F}_{p^{(n+1)!}}$ (same $\approx$ isomorphic field)

$x^{p^{n!}} - x$ $\quad x^{p^{(n+1)!}} - x$

$x^{p^m} - x \mid x^{p^{mk}} - x$

$$\overline{\mathbb{F}_p} = \bigcup_{n\geq 0} \mathbb{F}_{p^{n!}}$$

$\bigcup_{m\geq 0} \mathbb{F}_{p^m}$

Thm 1) $\overline{\mathbb{F}_p}$ is an infinite field, char $\overline{\mathbb{F}_p} = p$

2) $\overline{\mathbb{F}_p} \supset \mathbb{F}_{p^m}$ $\forall m$ $\qquad \mathbb{F}_{p^m} \subset \mathbb{F}_{p^{m!}} \subset \overline{\mathbb{F}_p}$

3) $\overline{\mathbb{F}_p}$ is algebraically closed

$f(x) \in \overline{\mathbb{F}_p}[x]$ $\quad f(x)$ has a root in $\overline{\mathbb{F}_p}$

factors in $\overline{\mathbb{F}_p}$.

$\left[f(x) = x^k + a_{k-1}x^{k-1} + \ldots + a_0 \right]$ irr

Proof of 3)? a_i - coeff of $f(x)$

$a_i \in \mathbb{F}_{p^{m!}}$ various m $\longrightarrow$ take largest m.

$a_i \in \mathbb{F}_{p^{m!}}$ $\forall i = 0, 1, 2, \ldots k-1$

$$\mathbb{F}_{p^{r!}} \supset \mathbb{F}_{p^{m!}}[x] \big/ (f(x)) \subset \mathbb{F}_{p^{(mk)!}}$$

some r $\qquad r = mk$ $\qquad$ $f(x)$ fully factors.

$\square$

$\mathbb{C}$ - alg. closed. $\mathbb{C} \supset \mathbb{Q}$

uncount.

$\overline{\mathbb{F}_p}$ - countable. $\qquad \overline{\mathbb{F}_p} \supset \mathbb{F}_q \quad q = p^m$

$\sigma: a \mapsto a^p$ Frob aut $\overline{\mathbb{F}_p} = \overline{\mathbb{F}_p}$

extends to $\overline{\mathbb{F}_p}$, aut. ∞ order

finite $\qquad$ infinite

$\mathbb{F}_p \subset \mathbb{F}_q \subset \overline{\mathbb{F}_p}$ alg. closure, each el't is algebraic $/\mathbb{F}_p$

$q = p^m$

$\mathbb{F}_p(t)$ ← rational functions in t $\qquad \frac{f(t)}{g(t)}$

$\uparrow$
x $\quad$ no polyn rel. on t

t is transcendental / $\mathbb{F}_p$

$\mathbb{F}_p(t) \neq \overline{\mathbb{F}_p}$

$\cup \qquad \cup$

$\mathbb{F}_p$

Cyclic extensions $\rightsquigarrow \sqrt[n]{a}$.

F, $f(x) = x^n - 1$ $\quad$ $\underline{n \text{ distinct roots}}$ in splitting field.

$f'(x) = n x^{n-1}$ $\quad$ $\gcd(f(x), f'(x)) =$

$= (x^n - 1, n x^{n-1}) = (x^n - 1, x^{n-1}) = 1$

$\uparrow \qquad \uparrow$

if n invertible in F $\qquad$ char F

always true if char $F = 0$, $\qquad$ $p \mid n$

$\Rightarrow$ mult. root.

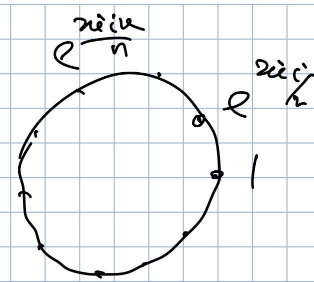
Rotman: cycl. extensions

Assume char $F = 0$, $\mathbb{Q} \subset F$

E/F splitting field of f.

Def An element ω of a field K is called an n-th root of unity if $\omega^n = 1$.
If ω has order n in K^*, call ω a primitive n-th root of unity. If $F \subset K$, field extension $F(\omega)/F$ is called a cyclotomic extension of F.

$\omega^n = 1$, $\omega^k \neq 1$ $1 \le k \le n-1$



$K = \mathbb{C}$ $\qquad e^{\frac{2\pi i}{n}}$ $\qquad \underline{e^{\frac{2\pi i k}{n}}}$ ← n-th root of unity.

<u>n roots of 1</u> in $\mathbb{C}$, ↗ primitive iff $\underline{(k,n)=1}$.

$\varphi(n)$ - Euler phi function

$$\varphi(n) = \left| \{ k \mid 1 \le k \le n-1, \underline{\gcd(k,n)=1} \} \right|$$

<u>Properties</u>

1) $\varphi(p) = p-1$

2) $\underline{\varphi(p^k) = p^k - p^{k-1}}$

3) $\varphi(nm) = \varphi(n)\varphi(m)$ if $(n,m)=1$.

$K \longrightarrow \mu_n(K)$ = el's of K^* that are n-th roots of unity

$\mu_n(K) \subset K^*$ subgroup $\qquad \underline{x^n - 1}$

$|\mu_n(K)|$ is at most n $\qquad \mathbb{C}$

$\underline{|\mu_n(K)| = n}$ if K <u>contains split. field of x^n-1</u>

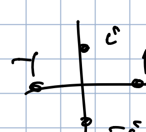
char $\underline{K=0}$ $(*)$

$\forall$ fin. subgroup of K^* is cyclic $\Rightarrow$

$\mu_n(K)$ - cyclic, for K as in $(*)$

$\mu_n(K) \simeq C_n$ cyclic group if K as in $(*)$.

$\mu_3(\mathbb{R}) = \{1\}$ $\qquad \mu_4(\mathbb{R}) = \{\pm 1\}$



$a \in \mu_n(E) \simeq C_n$ $\qquad a \in C_n$ $\qquad C_d \subset C_n$

$\langle a \rangle \subset C_n$ subgroup $\qquad \langle a \rangle \simeq C_d$

a is a prim d-th root of unit. $\qquad$ d order of $\underline{a}$

$a^{10} = 1$ → primitive 10-th
→ prim 5-th roots $\quad a^5 = 1,\ a \neq 1$
→ prim 2nd roots $\quad a^2 = 1 \Rightarrow a = -1$
→ -1

$1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^7, c\ \omega^9$

prim $\quad$ 5 $\quad$ prim $\quad$ 5 $\quad$ 2 $\qquad \varphi(10) = 4.$

Prop C_n has $\varphi(n)$ generators.

Prop For E, F as before, ($x^n - 1$, char 0) $\mu_n(E) \simeq C_n$

$\varphi(n)$ primitive n-th roots of unity.

$\underline{E = F(\omega)}$ $\quad \omega$ is a primitive n-th root.

$x^n - 1 = (x - \omega)(x - \underline{\omega^2}) \ldots \quad (x - \underline{\omega^{n-1}})(x - 1)$

other roots are powers of ω.

ω generates the splitting field E.

$G = Gal(F(\omega)/F)$

$\sigma \in G.$ $\qquad \sigma(\omega)$ – also a prim n-th root of unity.

$\sigma(\omega) = \omega^m$ some m $\qquad (m, n) = 1.$

This determines σ..

on other roots $\sigma(\omega^k) = \sigma(\omega)^k = (\omega^m)^k = \omega^{mk}$

$\omega \xmapsto{\sigma} \omega^m$ $\quad (m, n) = 1$.

m determines σ.

<u>Corollary</u> $\underline{G} = \underline{\mathrm{Gal}(F(\underset{\overset{\cap}{F}}{\omega})/F)} \subset (\mathbb{Z}/n)^*$.

subgroup of invertible elements in $\mathbb{Z}/n$

$$\begin{array}{ccccccc} & \overset{\omega^1}{\shortparallel} & & & & & \overset{\omega^0}{\shortparallel} \\ 1, & \underline{\omega}, & \omega^2, & \omega^3, & \ldots & \underline{\omega^{n-1}} & \omega^n = 1 \\ \downarrow & \downarrow & \downarrow & & & \downarrow & \\ \{0, & 1, & 2, & 3, & \ldots & n-1\} & \end{array}$$

additive labelling

$\mathbb{Z}/n \quad n = 0$

residues mod n

$\underline{\omega} \mapsto \underline{\underline{\omega^m}}$ on exponents

$\underline{\omega^k} \mapsto \underline{\omega^{km}}$

$1 \longmapsto m$ $\quad$ our map on exponents

$\underline{\underline{k}} \longmapsto \underline{\underline{km}}$

$(k, n) = 1$.

$$\begin{array}{ccc} & \not{p}\, i & \\ -1 & \downarrow & 1 \\ & p - i & \end{array}$$

$\mathbb{Q} \subset \mathbb{Q}(i)$

scaling or multiplication action on $(\mathbb{Z}/n)$ by its invertible elements.

$G \subset (\mathbb{Z}/n)^*$ $\qquad \underset{\wr\shortparallel}{C_{p-1}}$

<u>Example</u> $n = p$ prime $\qquad \underline{\underline{(\mathbb{Z}/p)^*}}$ - $\underline{\underline{p-1}}$ elements

$\overset{\curvearrowright}{1, \omega, \omega^2, \ldots}, \omega^{p-1}$ $\qquad \omega \mapsto \omega^k \quad 1 \le k \le p-1$.

$(\mathbb{Z}/p)^* \simeq C_{p-1}$ $\qquad (\mathbb{Z}/n)^*$ is a group of order $\varphi(n)$; not always cyclic

$G = Gal(E/F) \subset (\mathbb{Z}/n)^*$.

$x^n - 1$ n roots ~~distinct~~, μ_n - all roots of degree n in E

ω group, cyclic E^*

fin. subgroup of E^* is cyclic.

$E \setminus \{0\}$

$1, \omega$

$\mu_n = C_n$ primitive root

if choose a generator ω of μ_n

$1, \omega, \omega^2, \dots, \omega^{n-1}$.

$\sigma(\omega) = \omega^k$

$n = 4$ 4 roots

$\sigma(i) = i^2$ $\{1, i, \underbrace{i^2}_{-1}, \underbrace{i^3}_{-i}\}$ i, -1, 1, $-i$

$1, i, -1, i$

$1, -1, 1, -1, 1$

$\sigma(i^2) = \sigma(i)^2$

σ a homomorphism $\sigma(ab) = \sigma(a)\sigma(b)$

$\sigma(a^m) = \sigma(a)^m$.

not an automorphism

σ^{-1} $1, \omega, \omega^2, \dots \omega^{n-1}$

$1, \omega \; . \xrightarrow{\sigma} \omega^k$

$\sigma^{-1}(\omega^k) = \omega$

$\sigma^{-1}(\omega) = \omega^l$

$\sigma: \omega \to \omega^k$ $\qquad \sigma\sigma^{-1} \qquad \sigma(a^m) = \sigma(a)^m$

$\sigma^{-1}: \omega \to \omega^\ell$

$$\omega \xrightarrow{\sigma^{-1}} \omega^\ell \xrightarrow{\sigma} \omega^{k\ell} = \omega = \omega^1$$

$k\ell \equiv 1 \pmod n \qquad (k,n)=1$

$n=10 \qquad 1, \omega, \omega^2, \dots \qquad \omega^9 \qquad \omega^{10}=1$

$\downarrow \mathrm{id}$

$1, \omega \qquad \omega^3 \qquad \omega^7, \omega^9$

$\sigma(\omega)=\omega^7 \qquad (7,10)=1$

gives an automorphism (necessary condition).

$F \subset F(\omega) = E$

σ is identity on F $\qquad$ if $F=\mathbb{Q}$

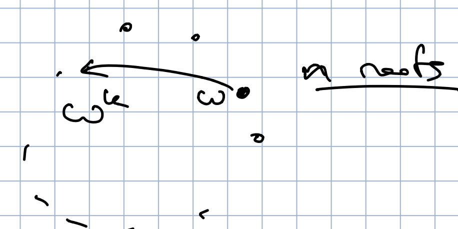
In general, $G \subset (\mathbb{Z}/n)^*$ $\qquad \omega \xrightarrow{\sigma} \omega^k \quad (k,n)=1$

$\sigma \mapsto$ el't k of $(\mathbb{Z}/n)^*$

For ex, if $F=\mathbb{Q}$, all such symmetries are realized $\quad K=\mathbb{Q}(\omega) \quad \omega$ - prim root of n

$\mathbb{Q}(\omega) \subset \mathbb{C}$

$\varphi(n)$ - prim.



$|G| = \varphi(n)$

G is abelian, for cyclotomic extensions.

$n = p$ prime $\qquad F = \mathbb{Q}$.

$$x^p - 1 = (x-1)(\underline{x^{p-1} + x^{p-2} + \dots + 1})$$

$\Psi_p(x)$ – p-th cyclotomic polynomial $\deg = p-1$

Proved that $\underline{\Psi_p(x)}$ is $\underline{\text{irreducible}}$ $/\mathbb{Q}$

$\underline{\Psi_p(x+1)}$ – $\underline{\text{Eisenstein polyn}}$.

let $\underline{\omega}$ be a root of $\Psi_p(x)$

$$\mathbb{C} \qquad \omega = e^{2\pi i/p}$$

$$e^{2\pi i k/p}$$

$$1 \le k \le p-1$$

$\mathbb{Q}(\omega)/\mathbb{Q}$

$$[\underline{\mathbb{Q}(\omega) : \mathbb{Q}}] = \deg \Psi_p(x) = \underline{p-1}$$

basis of $\mathbb{Q}(\omega)/\mathbb{Q}$ $\qquad$ $\underline{\text{splitting field}}$ E

$$1, \underbrace{\omega, \underline{\omega^2}, \dots \underline{\omega^{p-1}}}_{\text{primitive } p\text{-th roots}}.$$

$$\underline{x^p - 1} = (x-1)(x-\omega)(x-\omega^2)\dots(x-\omega^{p-1}).$$

$$\# \text{ of sym} = |\underset{\substack{\shortparallel \\ G}}{\mathrm{Gal}}(\mathbb{Q}(\omega)/\mathbb{Q})| = [\mathbb{Q}(\omega) : \mathbb{Q}] = \underline{p-1}$$

$\sigma \in G$

$$\omega \longrightarrow \sigma(\omega) = \underline{\omega^k}$$

$1 \le k \le p-1$ $\qquad$ σ def. by k

$$\Rightarrow \quad G = \{\sigma \mid \sigma(\omega) = \omega^k, \ \underline{1 \le k \le p-1}\}.$$

$$G \simeq (\mathbb{Z}/p)^{*} \leftarrow \text{mult.}$$

$\underline{\omega^m} \xrightarrow{\ \sigma\ } \underline{\omega^{km}}$ act on res. mod p.

$m \mapsto km$.

$\omega^a \cdot \omega^b = \omega^{\underline{a+b}}$

additive group: exponents of roots a

group ~~of~~ roots μ_p $\omega^a \cdot \omega^b = \omega^{a+b}$.

Galois group $\underline{\omega} \xrightarrow{\ \sigma\ } \underline{\omega^k}$ $\sigma(\omega^m) = \omega^{km}$

multiplicative group

$\mathbb{Z}/n$ $\mathbb{Z}/p$.

$(\mathbb{Z}/n, +)$

$m \Leftrightarrow \omega^m$

additive roots

multiplicative symmetries $\omega \mapsto \omega^k$

$(\mathbb{Z}/n, \cdot)$ ← only keep invertible els.

$((\mathbb{Z}/n)^*, \cdot) \longleftrightarrow$ Galois group G

a subgroup

$\underline{\text{If}}$ $F = \mathbb{Q}$ $G = (\mathbb{Z}/n)^*$.

$n = p$ $G = (\mathbb{Z}/p)^*$.

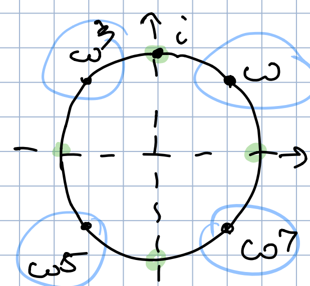
$\underline{\text{Thm}}$ $F = \mathbb{Q}$, $f = x^n - 1$, splitting field E is gen by a prim nth root of 1, $E = \mathbb{Q}(\omega)$.

$G = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \underline{(\mathbb{Z}/n)^*}$.

Proved for $n = p$, proved inclusion

$\underline{G \hookrightarrow (\mathbb{Z}/n)^*}$ for any F

$\underline{n=8}$ $\mathbb{Q}$. $x^8-1=(x^4-1)(x^4+1)=(x-1)(x+1)(x^2+1)(x^4+1)$



primitive

$\omega, \omega^3, \omega^5, \omega^7$

x^4+1 - irr$/\mathbb{Q}$. $x \to x+1$

$\Phi_8(x)$

$\omega = e^{\frac{2\pi i}{8}} = \frac{1+i}{\sqrt{2}}$

$[\mathbb{Q}(\omega):\mathbb{Q}] = 4$

$|G| = 4$.

$1: \omega \xrightarrow{id} \omega$

$\sigma: \omega \to \omega^3$

$\tau: \omega \to \omega^5$

$\sigma\tau: \omega \to \omega^7$

$\sigma: \omega \to \omega^3 \quad \omega^m \to \omega^{3m}$.

$\sigma^2: \omega \to \omega^3 \to \omega^9 = \omega$

$\omega^8 = 1$

$\sigma^2 = id$

$\tau^2 = id$

$(\sigma\tau)^2 = id$

$G \cong C_2 \times C_2$

$\sigma \quad \tau$.

abelian Galois group

fixed fields

$\omega \mapsto \omega^7 = \omega^{-1}$

$\omega \mapsto \omega^{-1} \quad |\omega| = 1$

$\omega \mapsto \omega^{-1}$

$\omega^{-1} \mapsto \omega$. comes from complex conj

$\omega + \omega^{-1}$ - invariant under $\sigma\tau$

$\omega = \frac{1+i}{\sqrt{2}}$ $\quad$ $\underset{\longrightarrow}{\overset{\curvearrowleft\, 6\tau}{\omega + \omega^{-1}}} = \frac{1+i}{\sqrt{2}} + \frac{1-i}{\sqrt{2}} = \sqrt{2}$

$$\mathbb{Q}(\omega)^{\langle 6\tau \rangle} = \mathbb{Q}(\sqrt{2})$$ fixed field

$$\cup_2$$
$$\mathbb{Q}$$

D.

<u>Ref</u> Rotman Cyclot. extension.

<u>Morandi</u> (proof of Φ_m).