Cyclotomic Fields

F $\quad x^n - 1 \in F[x]$ has at most n roots in F.

When x^n-1 is separable, we get n distinct roots in a s.f. of F, the n^{th} roots of unity.

Note: (x^n-1 is sep. if char $F = 0$
or char $F = p$ $\quad p \nmid n$)

The n^{th} roots of unity in F
$\mu_n(F)$ forms a group, and it's cyclic b/c any finite subgp of $F^\times$ is cyclic.

ζ_n = a choice of generator of
$\mu_n(F)$ $\qquad \mu_n$

A cyclotomic extension is of the form $F(\zeta_n)|F$

$F(\mu_n)/F$

$F(\zeta_n)|F$ is the s.f. of x^n-1 over F. When x^n-1 is sep. this ext^n is Galois, what is the Galois gp?

Thm:

$$\mathrm{Gal}(F(\zeta_n)|F) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

Proof:

Any aut. $\sigma \in \mathrm{Gal}(F(\zeta_n)|F)$ is determined completely by what it does to ζ_n.

As $\sigma|_{\mu_n}$ is a gp. auto. $\Rightarrow$

$\sigma(\zeta_n)$ is another prim. n^{th} root

$$\Rightarrow \quad \sigma(\zeta_n) = \zeta_n^{\,i_\sigma}$$

Define $\varphi: \mathrm{Gal}(F(\zeta_n)/F) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$

$\sigma \longrightarrow i_\sigma \bmod n$

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

$$\| $$

$$\zeta_n^{i_{\sigma\tau}} \implies i_{\sigma\tau} \equiv i_\sigma i_\tau \bmod n$$

$$\implies \varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau).$$

if $\sigma \in \ker\varphi$ $i_\sigma \equiv 1 \bmod n$

$$\sigma(\zeta_n) = \zeta_n \implies \sigma = 1.$$

<u>Special Cases:</u>

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

- $F = \mathbb{F}_p$ $\quad \mathrm{Gal}(\mathbb{F}_p(\zeta_n)/\mathbb{F}_p) \cong \langle p \bmod n \rangle$

<u>Proof:</u>

1.) By 29(a), $\Phi_n(x)$ is irred.

b/c $\Phi_n(x)$ min poly of ζ_n $\Rightarrow$

$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ has size $\varphi(n)$.

$\Rightarrow$ Surj.

2.) By 42, $Gal(\mathbb{F}_p(\zeta_n)/\mathbb{F}_p)$

is cyclic generated by $Frob_p$.

We identify $Frob_p$ with the map

$\sigma_p : \zeta_n \rightarrow \zeta_n^p$ and under

φ, $\sigma_p \longmapsto p \bmod n$.

$\Rightarrow$ image is $\langle p \bmod n \rangle$.

Def: K/F Galois, then K/F is called *abelian* if $\mathrm{Gal}(K/F)$ is abelian.

In particular, any cyclotomic field is abelian.

Cyclotomic fields are the heart of number theory:

Thm: (Kronecker-Weber) Any $F/\mathbb{Q}$ abelian is contained in $\mathbb{Q}(\zeta_n)$ for some n.

Main result of Class Field Theory:

goal is to classify abelian extensions.

For finite abelian groups, this is #30, and need Dirichlet's Thm.

From last week, composite of abelian extensions is abelian.

$$\begin{tikzcd}[arrows=dash] \overline{K} \arrow[d] \\ K \arrow[d] \\ \mathbb{Q} \end{tikzcd}$$

$K^{ab} :=$ Composite of all abelian ext^n of K

$=$ maximal abelian extension of K

Kronecker–Weber: $\mathbb{Q}^{ab} =$ composite of all $\mathbb{Q}(\zeta_n)$,

Algebraic number theory is the theory of algebraic numbers (<u>NOT</u> using algebra to study numbers)

$$\begin{array}{c} \overline{\mathbb{Q}} \\ | \\ \mathbb{Q}^{ab} \\ | \\ \mathbb{Q} \end{array}$$

There is an "infinite Galois theory" w/ corresponding correspondence thm

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) := G_{\mathbb{Q}}$

absolute Galois group of $\mathbb{Q}$

$[G_{\mathbb{Q}}, G_{\mathbb{Q}}] \leq G_{\mathbb{Q}}$ commutator subgp

what is fixed field?

$$\begin{array}{c} \overline{\mathbb{Q}} \\ | \\ L = \overline{\mathbb{Q}}^{[G_{\mathbb{Q}}, G_{\mathbb{Q}}]} \\ | \\ \mathbb{Q} \end{array}$$

$G_{\mathbb{Q}} / [G_{\mathbb{Q}}, G_{\mathbb{Q}}] = G_{\mathbb{Q}}^{ab}$

"

$\mathrm{Gal}(L/\mathbb{Q})$ is abelian $\Rightarrow$

$L \subseteq \mathbb{Q}^{ab} \Rightarrow \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}^{ab})$

$\leq [G_{\mathbb{Q}}, G_{\mathbb{Q}}]$.

OTOH, $[G_{\mathbb{Q}}, G_{\mathbb{Q}}]$ fixes

$\mathbb{Q}^{ab}$ b/c $\mathbb{Q}^{ab}$ is abelian

$$[G_{\mathbb{Q}}, G_{\mathbb{Q}}] \leq \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}^{ab})$$

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}^{ab}) = [G_{\mathbb{Q}}, G_{\mathbb{Q}}]$$

$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = G_{\mathbb{Q}}/[G_{\mathbb{Q}}, G_{\mathbb{Q}}]$$

$$\uparrow \quad = \quad G_{\mathbb{Q}}^{ab}$$

we understand this!

$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \prod_p \underbrace{\mathbb{Z}_p^\times}_{\text{p-adic integers}}$$

by class field theory

Conjectured: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

"Grothendieck – Teichmüller Group"

Inverse Galois problem: Given G, can we find $K/\mathbb{Q}$ w/

$$\mathrm{Gal}(K/\mathbb{Q}) = G?$$

Rephrase as what are the quotients of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$?

Representation Theory: Study how $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on certain vector spaces

"Galois representation"

An interesting example w/ cyclotomic polynomials

$\Phi_n(x)$ = min. poly of ζ_n over $\mathbb{Q}$.

$\Phi_1(x) = x-1$

$\Phi_2(x) = x+1$

$\Phi_3(x) = x^2+x+1$

$\Phi_4(x) = x^2+1$

$\vdots$

$\Phi_8(x) = x^4+1$

$\Phi_{10}(x) = x^4-x^3+x^2-x+1$

$\vdots$

$\Phi_{30}(x) =$

$x^8+x^7-x^5-x^4-x^3+x+1$

$\vdots$

If you write these down,

will probably convince yourself all coeff are in $\{0,-1,1\}$.

This is actually false!

$$\Phi_{105}(x) = 1+x^2-x^5-x^6-2x^7+\cdots$$

what happened here??

Some facts about cyclotomic poly.

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

- p, q are prime then

$$\Phi_q(x^p) = \Phi_{pq}(x)\,\Phi_q(x)$$

by using first fact.

- $(x^{pq}-1)\,\Phi_{pq}(x) = \Phi_q(x^p)\,\Phi_p(x^q)\,(x-1)$

$\deg \Phi_{pq} = \varphi(pq) = (p-1)(q-1) < pq$

Coeff. of LHS are (up to sign) Coeff. of $\Phi_{pq}(x)$.

$x\,\Phi_q(x^p)\,\Phi_p(x^q)$ has coeff. in $\{0,1\}$

$\Phi_q(x^p)\,\Phi_p(x^q)$ — " — $\{0,1\}$

$\Rightarrow$ $(x-1)\,\Phi_q(x^p)\,\Phi_p(x^q)$ Coeff. in $\{-1,0,1\}$.

$\Rightarrow$ $\Phi_{pq}(x)$ coeff. in $\{-1,0,1\}$.

$$\Phi_{p^m q^n}(x) = \Phi_{pq}\left(x^{p^{m-1} q^{n-1}}\right)$$

check: have same degree and roots of LHS are roots of RHS $\Rightarrow$ equal.

$$\Phi_{2^l r}(x) = \Phi_{2r}\left(x^{2^{l-1}}\right) = \Phi_r\left(-x^{2^{l-1}}\right)$$

r odd

$r = p^m q^n$

$\Phi_{2^l p^m q^n}$ has coeff. in $\{-1,0,1\}$.

So smallest Φ_n that could not have coeff. in $\{-1,0,1\}$

must be $3 \cdot 5 \cdot 7 = 105$.

Some examples

1.) $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1 \in \mathbb{F}_7[x]$

ζ_{10} is a root and s.f. is

$\mathbb{F}_7(\zeta_{10})$ $\quad$ $\mathrm{ord}_{10}(7) = 4$

$| \; 4$ $\quad$ b/c

$\mathbb{F}_7$ $\quad$ $7^4 \equiv 1 \mod 10$

$7^2 \equiv -1 \mod 10$

$\Rightarrow \; x^4 - x^3 + x^2 - x + 1$ is irred

in $\mathbb{F}_7[x]$.

Had very similar computations

in #18.

2.) $\mathbb{F}_2(\zeta_{15})$ has order 4 b/c

$\quad | \; 4 \qquad \mathrm{ord}_{15}(2) = 4.$

$\mathbb{F}_2$

$\mathrm{Gal}(\mathbb{F}_2(\zeta_{15})/\mathbb{F}_2)$ is then generated by $\zeta_{15} \longrightarrow \zeta_{15}^2$ so the roots of min. poly of ζ_{15} are $\zeta_{15}, \zeta_{15}^2, \zeta_{15}^4, \zeta_{15}^8$.

3.) $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n+\zeta_n^{-1})$ has degree 2 b/c $\alpha = \zeta_n + \zeta_n^{-1}$

ζ_n is a root of $x^2 - \alpha x + 1$
$\in \mathbb{Q}(\alpha)[x]$

and $\alpha = 2\cos(2\pi/n) \in \mathbb{R}$

$\Rightarrow \mathbb{Q}(\alpha) \subset \mathbb{R}$
$\zeta_n \in \mathbb{C} \setminus \mathbb{R} \Rightarrow$ irred.

$$\begin{array}{l} \mathbb{Q}(\zeta_n) \\ \Big| \; 2 \\ \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \leftarrow \text{"maximal real subfield"} \\ \Big| \; \frac{\varphi(n)}{2} \\ \mathbb{Q} \end{array}$$

$\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is fixed field of complex conjugation

4.) For prime p,

$\mathbb{Q}(\zeta_p)/\mathbb{Q}$ has $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$

$\cong \mathbb{Z}/(p-1)\mathbb{Z}$

a cyclic group. For each $d \mid p-1$

there is a unique cyclic subgp H d

order $d \implies$ unique extension

of degree $\frac{p-1}{d}$ w/ Galois gp

$\mathbb{Z}/\frac{p-1}{d}\mathbb{Z}$.

5.) Suppose we wanted a degree

25 cyclic ext^n of $\mathbb{Q}$. How

to get it?

$p = 101$ prime $\qquad 4 \mid 100 = p-1$.

$H := \mathbb{Z}/4\mathbb{Z} \leq \mathbb{Z}/100\mathbb{Z}$

$$\begin{array}{c} \mathbb{Q}(\zeta_{101}) \\ \big|\, 4 \\ \mathbb{Q}(\zeta_{101})^H \\ \big|\, 25 \\ \mathbb{Q} \end{array}$$

How to write down $\mathbb{Q}(\zeta_{101})^H$ explicitly?

$2 \bmod 101$ generates $(\mathbb{Z}/101\mathbb{Z})^\times$

$\Rightarrow \sigma : \zeta \longrightarrow \zeta^2$ generates

$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$

$H = \{1, \sigma^{25}, \sigma^{50}, \sigma^{75}\}$ unique

subgp of order 4.

Note that

$\alpha := \zeta + \sigma^{25}(\zeta) + \sigma^{50}(\zeta) + \sigma^{75}(\zeta)$

is fixed by H, $\Rightarrow$ $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\zeta)^H$

if $\tau \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ is <u>not</u> in H

note $\{\zeta, \zeta^2, \dots, \zeta^{100}\}$ is a basis of

$\mathbb{Q}(\zeta)/\mathbb{Q}$. If $\tau(\alpha) = \alpha$,

$\tau(\alpha) = \tau(\zeta) + \tau\sigma^{25}(\zeta) + \tau\sigma^{50}(\zeta)$
$+ \tau\sigma^{75}(\zeta) = \zeta + \sigma^{25}(\zeta)$
$+ \sigma^{50}(\zeta) + \sigma^{75}(\zeta)$

Since σ, τ just permute basis elements $\Rightarrow$

$\tau(\zeta) = \sigma^i(\zeta)$ for some i

$\Rightarrow \quad \tau = \sigma^i \quad \Rightarrow \tau \in H$

$\Rightarrow \Leftarrow$

So $\mathbb{Q}(\zeta)^H = \mathbb{Q}(\alpha)$.

Note: $\alpha = \zeta + \zeta^{10} + \zeta^{100} + \zeta^{91}$

$$\begin{array}{c} \mathbb{Q}(\zeta) \\ | \; 4 \\ \mathbb{Q}(\zeta + \zeta^{10} + \zeta^{100} + \zeta^{91}) \\ | \; 25 \end{array}$$