Abstract Algebra III

This lecture will be recorded. If you do not want your face in the recording, please turn off your camera. If you do not want your voice in the recording, please participate using the chat.

Cyclotomic extensions and polys

DF Sections 13.6 and 14.5 / Q

Section 13.6 : Let F be a field

Definition: Let $\mu_n(F)$ be the set of nth roots of unity in an algebraic closure of F

These are the roots of the polynomial

$$x^n - 1 \quad \text{in} \quad \bar{F}$$

Book writes $\mu_n = \mu_n(\mathbb{Q})$

We will see that if $\text{char}(F)=0$ or $\gcd(\text{char}(F), n)=1$

then

$$\mu_n(F) \cong C_n \cong (\mathbb{Z}/n\mathbb{Z}, +)$$

Definition: We say $\zeta \in \mu_n(F)$ is a primitive nth root of unity if $\zeta^n = 1$ but $\zeta^d \neq 1$ $0 < d < n$

in $\mathbb{C}$, the primitive n^{th} roots of unity are

$$e^{2\pi i a/n} \qquad \gcd(a, n) = 1$$

If $\mathrm{char}(F)=0$ or $\mathrm{char}(F) \nmid n$, then

there are $\varphi(n)$ = Euler totient function

primitive n^{th} roots of unity in $\mu_n(F)$.

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$$

elements of $\mathbb{Z}/n\mathbb{Z}$ that are units

$$= \#\{a : 0<a<n,\ \gcd(a,n)=1\}$$

$\varphi(n)$ when n is small

Important note:

If $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ $\quad p_i$ prime, $p_i \neq p_j$, $e_i > 0$

then $\varphi(n) = \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2}) \cdots \varphi(p_r^{e_r})$

and $\varphi(p^e) = p^e - p^{e-1}$

p prime, $e > 0$

Example $\quad 72 = 8 \cdot 9$

$\varphi(72) = \varphi(8) \cdot \varphi(9)$

$= (8-4)(9-3)$

$= 4 \cdot 6 = 24$

Assume that $\text{char}(F)=0$ or $\text{char}(F) \nmid n$

$$\mu_n(F) \cong C_n \cong (\mathbb{Z}/n\mathbb{Z}, +)$$
$$J^a \leftrightarrow g^a \leftrightarrow a$$

$\exists$ primitive n^{th} root of unity

$C_n = \langle g \rangle$

$$\mu_n(F) = \bigcup_{d \mid n} \{\text{primitive } d^{th} \text{ roots of unity}\}$$

$n=4$ $\quad x^4-1=0$

$\mathbb{Q}$ $\quad (x-1)(x+1)(x^2+1)$

$d \mid 4$: $d=1$ $\quad d=2$ $\quad d=4$

$x=1$ $\quad x=-1$ $\quad x=i,-i$

$\mu_4(\mathbb{Q}) = \{1, -1, \boxed{i, -i}\}$ PRIM

$\mu_2(\mathbb{Q}) = \{1, \boxed{-1}\}$ PRIM

$\mu_1(\mathbb{Q}) = \boxed{1}$ PRIM

Definition: $\mathrm{char}(F) \nmid n$

Φ_n n^{th} cyclotomic polynomial / F

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive} \\ \mu_n(F)}} (x-\zeta) = \prod_{\substack{a \text{ primitive} \\ \gcd(a,n)=1}} (x-\zeta^a)$$

$F = \mathbb{Q}$

$\Phi_1(x) = x - 1$

$\Phi_2(x) = x + 1$

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

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

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

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

p prime

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

← roots are all μ_p

← remove nonprim

$$= x^{p-1} + x^{p-2} + x^{p-3} + \ldots + x + 1$$

Notice that

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

all n^{th} roots of unity

$$x^4 - 1 = (x-1)(x+1)(x^2+1)$$

$$\Phi_1 \quad \Phi_2 \quad \Phi_4$$

Compute Φ_8

$$x^8 - 1 = \Phi_1(x)\,\Phi_2(x)\,\Phi_4(x)\,\Phi_8(x)$$
$$= (x-1)(x+1)(x^2+1)\,\Phi_8(x)$$

$$\Phi_8(x) = \frac{x^8-1}{(x-1)(x+1)(x^2+1)} = x^4+1$$

$\varphi(8) = 8-4 = 4$ ← 4 primitive 8th roots

Theorem: $\mathrm{char}(F) = 0$

$\Phi_n \in \mathbb{Z}[x]$, Φ_n is monic, Φ_n is irreducible

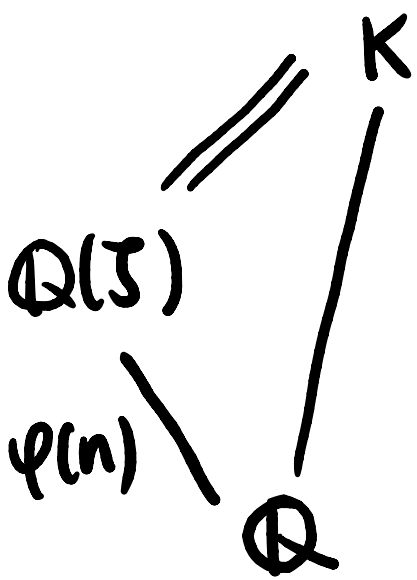
$\deg \Phi_n = \varphi(n)$

$\Rightarrow$ $\exists$ primitive n^{th} root of unity

$$m_{\exists, \mathbb{Q}}(x) = \Phi_n(x)$$

Section 14.5

Consider $\mathbb{Q}(\zeta)$ ζ primitive n^{th} root of unity



K splitting field of Φ_n

equality $K=\mathbb{Q}(\zeta)$ iff every root of Φ_n is in $\mathbb{Q}(\zeta)$

but the roots of Φ_n are of the form ζ^a $\gcd(a,n)=1$ $\zeta^a \in \mathbb{Q}(\zeta)$

Consequence: $\mathbb{Q}(\zeta)$ ζ primitive n^{th} root of unity is a Galois extension of $\mathbb{Q}$ of degree $\varphi(n)$

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

σ determined by $\sigma(\zeta)$

also $\sigma(\zeta) = \zeta^a$ $\gcd(a,n)=1$ because those are the other roots of $m_{\zeta,\mathbb{Q}} = \Phi_n$

This gives us

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

gp isomorphism

$$\sigma_a \leftrightarrow a$$

$$\sigma_a(\zeta) = \zeta^a$$

set $\{a : 0 < a < n, \gcd(a,n) = 1\}$

operation is $\times$

$$\sigma_b(\sigma_a(\zeta)) = \sigma_b(\zeta^a) = (\sigma_b(\zeta))^a = (\zeta^b)^a = \zeta^{ab}$$

$$= \sigma_{ab}(\zeta)$$

$$\Rightarrow \sigma_b \circ \sigma_a = \sigma_{ab}$$

To compute $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is to compute $(\mathbb{Z}/n\mathbb{Z})^\times$ unit gp of $\mathbb{Z}/n\mathbb{Z}$

- abelian gp
- of size $\varphi(n)$

continued on Wednesday

then HW10 #6

That’s all for today!