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

Today: work over $\mathbb{Q}$

Let ζ be a primitive n^{th} root of unity

$$\zeta^n = 1 \quad \text{but} \quad \zeta^k \neq 1 \quad 0 < k < n$$

Then $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension with

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

First facts about $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$

- set $(\mathbb{Z}/n\mathbb{Z})^\times = \{ a : 0 < a < n, \ \gcd(a,n) = 1 \}$

operation is $\times$ (multiplication)

Subtlety if $ab \equiv c \mod n$

$\gcd(a,n) = g(b,n) = 1$

then $\gcd(c,n) = 1$

* if $n=p$ prime

$$((\mathbb{Z}/p\mathbb{Z})^{\times}, \times) \cong C_{p-1} \quad \text{cyclic}$$

$$\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$$

$$\mathbb{F}_p^{\times} = \mathbb{F}_p - \{0\}$$

False in general, $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is not always cyclic.

(most of the time)

$(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic iff
$$\begin{cases} n = 2,4 & \\ \text{or } n = p^k & p \text{ odd prime, } k>0 \\ \text{or } n = 2p^k & p \text{ odd prime, } k>0 \end{cases}$$

Note

$(\mathbb{Z}/2\mathbb{Z})^\times = 1$

$(\mathbb{Z}/4\mathbb{Z})^\times \cong C_2$

$n = 8$ $\quad (\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$

$$\boxed{\begin{array}{c}\varphi(p^e) = p^e - p^{e-1} \\ 8 = 2^3\end{array}}$$

$\varphi(8) = 8 - 4 = 4$

So $(\mathbb{Z}/8\mathbb{Z})^\times \cong \cancel{C_4}$ or $C_2 \times C_2$

not cyclic

$3^2 = 9 \equiv 1 \mod 8$ so 3 has order 2

$5^2 = 25 \equiv 1 \mod 8$ so 5 has order 2

$7^2 = 49 \equiv 1 \mod 8$ so 7 has order 2

Definition: An extension K/F is abelian if it is Galois with abelian Galois group

Easy-ish Theorem

Let G be finite abelian. Then there exists n and $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_n)$ primitive n^{th} root of unity

with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

Kronecker-Weber Theorem

Let $K/\mathbb{Q}$ be finite abelian. Then $\exists\, n$ s.t.

$\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_n)$.

this is the only place you will find such an extension.

Easy-ish Theorem

Let G be finite abelian. Then there exists n

and $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_n)$ primitive n^{th} root of unity

with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

If looking for $\mathrm{Gal}(K/\mathbb{Q}) \cong G$
G finite abelian, can find it in
cyclotomic extension.

If $d|n$ $\quad \mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\zeta_n)$

So n is never unique BUT there is a unique least n.

Not every subextension of $\mathbb{Q}(\zeta_n)$ is cyclotomic

$\mathbb{Q}(\sqrt{d})$ is always finite abelian $/\mathbb{Q}$

so $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_n)$

but not cyclotomic if $d \neq -3$ or -1.

d squarefree

The study of abelian extensions of a field F is called the class field theory of F.

Solvable extensions

G is solvable if $1 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq G_s = G$

G_{i+1}/G_i cyclic

Definition

cyclic

K/F is a solvable extension if it is Galois with solvable Galois gp.

cyclic

Can always associate to K/F the gp $\mathrm{Aut}(K/F)$.

But if $[K:F] \neq \#\mathrm{Aut}(K/F)$

$\mathrm{Aut}(K/F)$ might not be nice / might not give you any info about K/F

Definition

Let α be algebraic over F. We say α can be expressed by radicals if α is an element of a field K/F which can be obtained by successive simple radical extensions

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_s = K \quad \alpha \in$$

$$K_{i+1} = \underbrace{K_i\left(\sqrt[n_i]{\alpha_i}\right)}_{\text{specific and rare}} \qquad \alpha_i \in K_i$$

Example $\mathbb{Q}(\sqrt{2+\sqrt{3}})$

$$\underset{K_0}{\underset{\parallel}{\mathbb{Q}}} \subseteq \underset{K_1}{\underset{\parallel}{\mathbb{Q}(\sqrt{3})}} \subseteq \underset{K_2}{\underset{\parallel}{\mathbb{Q}(\sqrt{2+\sqrt{3}})}}$$

$K_1 = K_0(\sqrt{3})$ $\qquad$ $K_2 = K_1(\sqrt{2+\sqrt{3}})$

$2+\sqrt{3} \in K_1$

Question from chat

$\mathbb{Q}(\sqrt{2}+\sqrt{3})$ vs $\mathbb{Q}(\sqrt{\sqrt{2}+\sqrt{3}})$

?

$$\left[\mathbb{Q}\left(\sqrt{\sqrt{2}+\sqrt{3}}\right) : \underbrace{\mathbb{Q}(\sqrt{2}+\sqrt{3})}_{=\mathbb{Q}(\sqrt{2},\sqrt{3})}\right] = 2$$

Need to show that $\alpha^2 = \sqrt{2}+\sqrt{3}$ has no solution in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

use that $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$

$= a + b(\sqrt{2}+\sqrt{3}) + c(\sqrt{2}+\sqrt{3})^2 + d(\sqrt{2}+\sqrt{3})^3$

Definition

$f(x) \in F[x]$ can be solved by radicals if all of its roots can be expressed by radicals.

If α is a root of f

$$\alpha = \sqrt[3]{\sqrt{a} + 5\sqrt[5]{b + \sqrt[3]{c}}}$$

Theorem 39

Let f be a separable poly in $F[x]$, with splitting field K/F. Then f can be solved by radicals if and only if $Gal(K/F)$ is solvable.

First non solvable gps: A_5, S_5

A_n, S_n not solvable if $n \geq 5$

now

That's all for ~~today~~!