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.

2 Chapters in D&F on field theory

linear algebra / vector spaces   Chap 11   11.1, 11.2

Chapter 13: Basic stuff / Background / Foundational ideas

Chapter 14: Galois theory

This is the study of certain special, very nice field extensions.

"Galois extension"

13.1 Basic theory of fld extensions

What if we have a fld F and a polynomial $p(x) \in F[x]$ and we want to make a bigger field K in which p has a root

Let α be a root of $p(x)$

$$\underset{\text{adjoin } \alpha \text{ to } F}{F(\alpha)} \cong \underbrace{F[x]/(p(x))}$$

this only works if p is irreducible!

If p is not irreducible then $F[x]/(p(x))$ is not a field.

Analogy: $\mathbb{Z}/p\mathbb{Z}$ is a field if p is prime
$\mathbb{Z}/n\mathbb{Z}$ is not a field if n is composite

So if p not irred, factor it $p(x) = \prod_{i=1}^{n} p_i(x)$
p_i irred then do

$$F(\alpha) = F[x]/(p_i(x))$$

13.2 Algebraic extensions

Definition: Let K/F be a fld extension

Then $\alpha \in K$ is <u>algebraic over F</u> if α is a root of a polynomial $p(x) \in F[x]$

Examples: $\sqrt[3]{2}$ is alg / $\mathbb{Q}$ $\quad x^3-2 \in \mathbb{Q}[x]$

π is not alg / $\mathbb{Q}$

not algebraic, transcendental

Definition: K/F is an algebraic extension if

$\forall \alpha \in K$, α is alg $/F$

over

leading coefficient is 1

Prop 9: If $\alpha \in K$ is alg $/F$, then $\exists$ a unique monic irreducible polynomial $m_{\alpha,F} \in F[x]$ with $m_{\alpha,F}(\alpha) = 0$

$m_{\alpha,F}$ is called the minimal polynomial of α over F

If $f(x) \in F[x]$ and $f(\alpha)=0$ then

$$m_{\alpha,F} \mid f \quad \text{in } F[x]$$

$\deg f \geq \deg m_{\alpha,F}$

$\alpha = i$

all polys with $p(\alpha)=0$

$p(x) \in F[x]$

divides every other polynomial in this set

$\boxed{x^2+1} = m_{i,\mathbb{Q}}$

$2x^2+2$

$\frac{x^2}{5}+\frac{1}{5}$

irreducible poly

exciting that it's irreducible

In math/algebra a minimal polynomial is not always irreducible (but it's always of least degree)

In field theory, the min poly of an algebraic element is always irreducible

Quick Corollary (Proposition 11)

$$F(\alpha) \cong F[x] / (m_{\alpha,F}(x))$$

$$[F(\alpha):F] = \deg m_{\alpha,F}$$

Prop 12 α is alg $|F$ iff $[F(\alpha):F] < \infty$

$\Rightarrow [\mathbb{Q}(\pi):\mathbb{Q}] = \infty$

Theorem 14

$F \subseteq K \subseteq L$

$$\begin{array}{c} L \\ | \\ K \\ | \\ F \end{array}$$

$$[L:F] = [L:K][K:F]$$

13.3 Straightedge + compass constructions

historical + fun

13.4 Splitting fields + alg closures

F a field

$f(x) \in F[x]$ be irreducible

Definition Let $p(x) \in F[x]$ be a polynomial, not necessarily irreducible. K/F is the <u>splitting field</u> of p if

1. p factors completely in $K[x]$ into linear factors
2. p does not factor completely in any $F \subseteq E \subsetneq K$

K is the smallest field containing F in which p "splits completely"

↳ factors into linear factors

Example: $x^3 - 1 \in \mathbb{Q}[x]$ is not irreducible but does not split completely

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

← not linear

F field

$f(x) \in F[x]$ irreducible

$\deg f = n$

2 important extensions associated to f

$$\begin{tikzcd}
 & & K \arrow[dll, dash] \arrow[d, dash] \\
F[x]/(f(x)) = F(\alpha) \arrow[rr, dash] & & F
\end{tikzcd}$$

Splitting field of f

this has all roots of f

this has degree dividing $n!$

in general must compute degree

this has one root of f (at least)

this has degree n

Example $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ irreducible, monic

$= m_{\sqrt[3]{2}, \mathbb{Q}}$

In $\mathbb{Q}(\sqrt[3]{2})[x]$

$$x^3 - 2 = (x - \sqrt[3]{2}) \cdot (x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$$

$$\begin{tikzcd}
 & K \arrow[dd, dash, "6"] \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[ur, dash, "2"] & \\
 & \mathbb{Q} \arrow[ul, dash, "3"]
\end{tikzcd}$$

splitting field

$K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

Theorem 25 + Corollary 28

For any $f \in F[X]$, the splitting field K of f over F exists and is unique up to isomorphism.

Definition: let F be a field, then we denote by $\bar{F}$ the extension of F such that $\bar{F}$ is algebraic over F and every polynomial $f(x) \in F[x]$ splits completely in $\bar{F}[x]$

(Prop 31 $\bar{F}$ exists and is unique up to isom)

$\bar{F} = F +$ all algebraic elements over F

Definition: We say that K is algebraically closed if every $p(x) \in K[x]$ splits completely in K already $\quad (\Leftrightarrow K = \overline{K})$

Proposition $\overline{F}$ is alg closed.

$\mathbb{C}$ algebraically closed

$\overline{\mathbb{R}} = \mathbb{C}$ $\quad [\overline{\mathbb{R}} : \mathbb{R}] = 2$ $\quad \mathbb{C} = \mathbb{R}(i)$

$\overline{\mathbb{Q}} \neq \mathbb{C}$ $\quad [\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$

π, e

$i \in \overline{\mathbb{Q}} \not\subseteq \mathbb{R}$

just $\mathbb{Q}$ + algebraic elements over $\mathbb{Q}$

no transcendental elements

That’s all for today!