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.

Recap: All fields have a "characteristic"

- $\mathrm{char}(F) = 0$ then $\mathbb{Q} \subseteq F$ — no finite sum $1+1+\ldots+1=0$

- $\mathrm{char}(F) = p$, prime then $\mathbb{F}_p \subseteq F$ — $\underbrace{1+1+\ldots+1}_{p \text{ summands}} = 0$

Call $\mathbb{Q}$, $\mathbb{F}_p$ p prime, the prime fields

$\varphi : F \to F'$ field homomorphism, $\varphi = 0$ or φ injective

When $F \subseteq F'$ we say F' is an extension of F.
F base field, denoted F'/F

Definition: Let F' be a field extension of F, then F' is a vector space over F

$$[F':F] = \dim_F F'$$

"the degree of F' over F"

Definition: If $[F':F] < \infty$ (degree is finite) we say F' is a <u>finite</u> extension of F

this might not be finite as a set

My first field extension

Example $\mathbb{Q}$ does not contain a root of the irreducible polynomial x^2-2 or $\sqrt{2} \notin \mathbb{Q}$

Using Theorem 3 of Section 13.1, we can create/construct an extension F of $\mathbb{Q}$ where x^2-2 does have a root.

Not using Thm 3: $\mathbb{R} \supseteq \mathbb{Q}$ $\sqrt{2} \in \mathbb{R}$ could use extension $\mathbb{R}/\mathbb{Q}$] Big!

Theorem 3

Let F be a field, $p(x) \in F[x]$ be an irred polynomial ($\Rightarrow$ p has <u>no</u> root in F)

Then $\exists$ a field K which contains an isomorphic copy of F and a root of p. If we identify F with its isomorphic copy in K, then K is an extension of F containing a root of p

Note:

A polynomial can have no root without being irreducible!

e.g.

$(x^2+1)(x^2-2) \in \mathbb{Q}[x]$

proof $K = \underbrace{F[x]}_{\text{polynomials with coefficients in } F} / \underbrace{(p(x))}_{\text{ideal generated by } p}$

- $F[x]$ is (principal ideal) <u>domain</u>
- $(p(x))$ is a maximal ideal since p is irreducible
- a quotient of a domain by a maximal ideal is a field

K contains F (constant polynomials)

contains a root of p, the element x

$\square$

Example $F = \mathbb{Q}$ want to construct an extension containing $\sqrt{2}$, a root of $x^2 - 2$ an irreducible polynomial in $\mathbb{Q}[x]$

One such extension is

$$K = \underbrace{\mathbb{Q}[x]/(x^2-2)}$$

the elements of K are remainders of polynomials after dividing by x^2-2

$$\begin{array}{l} \qquad\qquad\quad x \\ x^3+x+1 \;\big)\; x^2-2 \\ -\;x^3-2x \\ \hline \boxed{3x+1} \end{array}$$

remainder

think of $\mathbb{Z}/n\mathbb{Z}$

can think of elements in here as the remainders of integers when dividing by n

$\mathbb{Z}/3\mathbb{Z} \leftarrow 5 \equiv 2 \bmod 3$

“$\{0,1,2\}$

$$K = \mathbb{Q}[x]/(x^2-2) = \{ax+b : a,b \in \mathbb{Q}\}$$

every polynomial when divided by x^2-2 has remainder of deg 1 or 0

$$= \{a\alpha + b : a,b \in \mathbb{Q}$$

α image of $x\}$

$$\mathbb{Q} = \{b : b \in \mathbb{Q}\}$$

$a=0$

$$\begin{array}{ccc} x & \mapsto & \alpha \\ \mathbb{Q}[x] & \to & \mathbb{Q}[x]/(x^2-2) \\ p(x) & \mapsto & p(x) \bmod x^2-2 \end{array}$$

$$K = \mathbb{Q}[x]/(x^2-2) = \{ a\alpha + b : a, b \in \mathbb{Q}$$
$$\alpha \text{ is } x \bmod x^2-2 \}$$

K

$\cup$

$\mathbb{Q}$

Ring hom so respects $+, \cdot$ of polynomials

$$\mathbb{Q}[x] \to \mathbb{Q}[x]/(x^2-2)$$
$$x \mapsto \alpha$$

α satisfies $\alpha^2 - 2 = 0$

$$x^2 - 2 \mapsto \alpha^2 - 2 = 0$$

$$K = \mathbb{Q}[x]/(x^2-2) = \{ a\alpha + b : a, b \in \mathbb{Q},\ \alpha \equiv x \bmod x^2-2 \}$$

$$= \{ a\sqrt{2} + b : a, b \in \mathbb{Q} \}$$

$[K:\mathbb{Q}]$ = dimension of K as a $\mathbb{Q}$-v.s.

= "how many elements of $\mathbb{Q}$ you must specify to specify one element of K"

$= 2$

$\mathbb{R}^2 \ni (x, y)$

$\dim_{\mathbb{R}} \mathbb{R}^2 = 2$

Theorem 4

Let $p \in F[x]$ be irreducible of degree n

Then if $\theta \equiv x \bmod p(x)$ in $K = F[x]/(p(x))$

(θ is a root of p in K) then

$$1, \theta, \theta^2, \dots, \theta^{n-1}$$

form a basis of K over F. So in particular

$$[K:F] = n$$

Example $K = \mathbb{Q}[x]/(x^3-2)$ $p(x) = x^3-2$ irred in $\mathbb{Q}[x]$

$n=3$

Theorem says that

$1, \sqrt[3]{2}, (\sqrt[3]{2})^2 = \sqrt[3]{4}$

$1, \theta, \theta^2$

θ is a root of p

$\theta = \sqrt[3]{2}$

is a basis for $K/\mathbb{Q}$ so $[K:\mathbb{Q}]=3$ and

$$K = \{ a + b\sqrt[3]{2} + c\sqrt[3]{4} : a,b,c \in \mathbb{Q} \}$$

Definition: Let K/F be a field extension with $\alpha \in K$ but $\alpha \notin F$. Then we define $F(\alpha)$ to be the smallest field in K that contains F and α.

$$\begin{array}{c} K \ni \alpha \\ | \\ F(\alpha) \\ | \\ F \end{array}$$

(Can also do this for multiple elements, if $\alpha, \beta, \gamma \ldots \in K$ then $F(\alpha, \beta, \gamma \ldots)$ smallest field in K containing $\alpha, \beta, \gamma \ldots$ and F)

Theorem 6 of Section 13.1

F fld, p irred in $F[x]$, K/F contains a root α of p

$$\begin{array}{c} K \ni \alpha \\ | \\ F \end{array}$$

Then $F(\alpha) \cong \boxed{F[x]/(p(x))}$

When we constructed an extension that contains a root of p, we actually constructed the smallest one!

$K = \mathbb{Q}[x]/(x^2-2) = \mathbb{Q}(\sqrt{2})$ $\mathbb{Q}$ adjoin the square root of 2

$K = \mathbb{Q}[x]/(x^3-2) = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q} \cup \{\sqrt[3]{2}\}$ not a field

$\quad = \mathbb{Q} + \mathbb{Q}\sqrt[3]{2} + \mathbb{Q}\sqrt[3]{4}$

Uniqueness: There is unique smallest extension containing F and a root α of an irred poly

But in total infinitely many extensions of F contain α

Talk about $F[x]$ vs $F(x)$

$F[x]$ $\downarrow$ adjoin x and make smallest ring

$F(x)$ $\downarrow$ adjoin x and make smallest field

e.g. $\mathbb{Q}[x]$ = polynomials $a_0 + a_1 x + \dots + a_n x^n$

$\mathbb{Q}(x)$ = rational functions $\dfrac{a_0 + a_1 x + \dots + a_n x^n}{b_0 + b_1 x + \dots + b_m x^m}$

$F[x] = F(x)$ if x satisfies a polynomial of finite degree

but not equal otherwise

Examples

$$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$$

$$\mathbb{Q}[\pi] \neq \mathbb{Q}(\pi)$$

$$\begin{array}{ccc} \mathbb{Q}[\pi] & \neq & \mathbb{Q}(\pi) \\ \cong & & \cong \\ \mathbb{Q}[x] & & \mathbb{Q}(x) \end{array}$$

That’s all for today!