Groups & Rings: Lecture #21

Field extensions (§21.1)

- Field extensions
- Examples
- Fundamental theorem of field theory
- Algebraic and transcendental extensions

Overview: (ring part of course)

① **General about rings** (#15–17)

definitions, properties, homomorphisms, isomorphism theorems
ideals, pol. rings

② **Domains** (#18–20)

fraction field, PID, ED, UFD, quadratic rings

③ **Fields** (#21–24)

field extensions, minimal pols, basis, splitting fields, finite fields

TODAY

Field extensions

How do we construct fields?

- **Quotients** R/I I max. ideal.
- **Fraction fields** $\mathrm{Frac}(D)$ D domain ← = integral domain
- **Subfield** $F \subset E$ (a subring of a field is always a domain and sometimes a field)

Observation: Every $\varphi: F \to E$ ring homo b/w fields is injective:

if $\alpha \in F \setminus \{0\}$, $\exists \alpha^{-1} \in F$, $\varphi(\alpha)\varphi(\alpha^{-1}) = \varphi(\alpha\alpha^{-1}) = \varphi(1) = 1$

$\Rightarrow \varphi(\alpha)$ is invertible $\Rightarrow \varphi(\alpha) \neq 0$.

Def: A **field extension** (of F) is an inclusion of fields $F \subseteq E$.

Often denoted E/F (not a quotient!)

Rmk: E becomes an F-vector space.

Ex: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ (or $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$)

Ex: $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$

Def: The **degree** of F/E, denoted $\deg F/E$ or $[E:F]$, is the dimension of E as an F-vector space. ($\dim_F E$)

Examples (degree)

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ $\quad \mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$, basis $\{1, \sqrt{2}\}$, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

$\mathbb{C}/\mathbb{R}$ $\quad \mathbb{C} = \{a+bi : a,b \in \mathbb{R}\}$, basis $\{1, i\}$, $[\mathbb{C} : \mathbb{R}] = 2$

$\mathbb{R}/\mathbb{Q}$ $\quad \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots, \sqrt{p}, \ldots \in \mathbb{R}$ linearly independent over $\mathbb{Q}$ and π, e not even algebraic over $\mathbb{Q}$.

$\mathbb{R}$ has an uncountable basis as a $\mathbb{Q}$-vsp $\quad [\mathbb{R} : \mathbb{Q}] = \infty$

Def: F is a **finite field** if $|F|$ is finite. (Ex: $\mathbb{Z}/p\mathbb{Z}$)

Rmk: $|F| = q$, E/F field ext of deg d, $|E| = |F|^{[E:F]} = q^d$

Def: Let $F \subset E$ field extension. Let $\alpha_1, \ldots, \alpha_n \in E$.

$F(\alpha_1, \ldots, \alpha_n)$ smallest subfield of E containing F and the α_i's.

Warning: $F(x_1, x_2, \ldots, x_n) = \mathrm{Frac}(F[x_1, \ldots, x_n]) \neq F(\alpha_1, \ldots, \alpha_n)$

Ex:

$$\begin{array}{ccccccc} \mathbb{Q} & \subset & \mathbb{Q}[x] & \xrightarrow{ev_{\sqrt{2}}} & \mathbb{Q}(\sqrt{2}) & \subset & \mathbb{R} \\ \| & & \cap & \not\nearrow & \| & & \uparrow \alpha \\ \mathbb{Q} & \subset & \mathbb{Q}(x) & \dashrightarrow & \mathbb{Q}(\alpha) & & \end{array}$$

$\frac{1}{x^2-2} \mapsto ?$ $\qquad ev_{\sqrt{2}}(x^2-2) = 0$

Def: $F \subset E$ is

- **finitely generated** if $E = F(\alpha_1, \ldots, \alpha_n)$, for some $\alpha_i \in E$.
- **simple** if $E = F(\alpha)$, for some $\alpha \in E$

Examples: char 0

- Prime field $\mathbb{Q}$ (smallest field of char 0)
- number fields: Extensions $\mathbb{Q} \subset E$ of finite degree
  $(\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{10}), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt{2}, \sqrt{3}), \dots)$

Ex: $E = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ basis/$\mathbb{Q}$: $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$

but also $E \xrightarrow{\varphi_a} \mathbb{C}$ where $\zeta = e^{\frac{2\pi i}{3}}$ prim. 3rd root of unity

$\sqrt[3]{2} \longmapsto \zeta^a \sqrt[3]{2}$ and $a = 0, 1, 2$ $(\zeta^3 = 1, \zeta \neq 1)$

Why? $\sqrt[3]{2}$ satisfies $x^3 = 2$ and so does $\zeta\sqrt[3]{2}$.

$$E \cong \mathbb{Q}[x]/(x^3 - 2)$$

irr. pol $\Rightarrow$ E field

$\ker \varphi_a = (x^3 - 2) \Rightarrow \mathrm{im}(\varphi_a) \cong E$ for $a = 0, 1, 2$

So images are isomorphic but still different

$\mathbb{Q}[x] \xrightarrow{\varphi_0} \mathbb{R}$ $\varphi_0 = \mathrm{ev}_{\sqrt[3]{2}}$ $\mathrm{im}(\varphi_0) =: \underset{\parallel}{E} E_0 \subset \mathbb{R}$

$\mathbb{Q}[x] \xrightarrow{\varphi_1} \mathbb{C}$ $\varphi_1 = \mathrm{ev}_{\zeta\sqrt[3]{2}}$ $\mathrm{im}(\varphi_1) =: E_1 \subset \mathbb{C}$ (not in $\mathbb{R}$)

$\mathbb{Q}[x] \xrightarrow{\varphi_2} \mathbb{C}$ $\varphi_2 = \mathrm{ev}_{\zeta^2\sqrt[3]{2}}$ $\mathrm{im}(\varphi_2) =: E_2 \subset \mathbb{C}$ (not in $\mathbb{R}$)

$E_a \cong E_b$ but $E_a \cap E_b = \mathbb{Q}$ $\forall a \neq b$, $a, b = 0, 1, 2$

Basis for E_1: $\{1, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{4}\}$

Basis for E_2: $\{1, \zeta^2\sqrt[3]{2}, \zeta\sqrt[3]{4}\}$

Galois theory $\approx$ study of different embeddings of fields

Examples: char p

- prime field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$

Ex (21.2) $\mathbb{F}_2 \subset E = \mathbb{F}_2[x]/(x^2+x+1)$

irreducible b/c no roots $0^2+0+1 \neq 0$, $1^2+1+1 \neq 0$

E has basis $\{1, \alpha\}$ $\alpha = \bar{x} = x + (x^2+x+1)$

b/c $f(x) + (x^2+x+1) = r(x) + (x^2+x+1)$ (div. algo.)

where $f(x) = q(x)(x^2+x+1) + r(x)$ $r(x) = a + bx$

so $\overline{f(x)} = a + b\alpha$

$[E : \mathbb{F}_2] = 2$ so E has $2^2 = 4$ elements.

Rmk: Every field E of char p contains $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$

$\Rightarrow \mathbb{F}_p \subset E \Rightarrow |E| = |\mathbb{F}_p|^{[E:\mathbb{F}_p]}$ a p-power (or ∞)

Fundamental theorem of field theory

Thm (21.5) Let $p(x) \in F[x]$. Then there exists a field extension $F \subset E$ such that $p(x)$, as a polynomial in $E[x]$, has a root $\alpha \in E$.

proof:
- Factor $p(x)$ into irreducibles. Enough to prove thm for one irr factor. WLOG $p(x)$ irreducible.
- $F \longrightarrow F[x] \longrightarrow F[x]/(p(x)) =: E$ (auto. injective)
  irr. $\Rightarrow (p(x))$ maximal $\Rightarrow$ E field
- Let $\alpha = \bar{x} = x + (p(x))$. Then $p(\alpha) = p(x) + (p(x)) = 0 + (p(x))$. $\square$

"$E = F[x]/(p(x))$ is a field where we force $p(x)$ to have a root $(\alpha = \bar{x})$."
We are "formally adjoining a root of $p(x)$ to F".

Algebraic and transcendental extensions

Def: Let $F \subset E$ field extension. An element $\alpha \in E$ is

- **algebraic** (over F) if $\exists p(x) \in F[x]$, $p(x) \neq 0$, $p(\alpha) = 0$.
- **transcendental** (over F) o/w.

Ex: $\sqrt{2} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$: take $p(x) = x^2 - 2$.

$e \in \mathbb{R}$ is transcendental over $\mathbb{Q}$ (Hermite 1873)

$\pi \in \mathbb{R}$ ——————"—————— (Lindemann 1882)

$e + \pi$, $e\pi$ almost surely transcendental but <u>not known</u>!

Fact: $\overline{\mathbb{Q}} := \{x \in \mathbb{C} : x \text{ algebraic over } \mathbb{Q}\}$ algebraic numbers is a <u>field</u>. (proof next lecture?)

Def: F is <u>algebraically closed</u> if $\forall F \subset E$, $\forall \alpha \in E$ algebraic over F $\Rightarrow \alpha \in F$.

Fact: $\overline{\mathbb{Q}}$ algebraically closed. (It is the algebraic closure of $\mathbb{Q}$)

$\mathbb{C}$ ——"——

Ex: $\alpha = \sqrt{2 + \sqrt{3}} \in \mathbb{R}$ algebraic? (will see later any such expr. alg.)

$$\alpha^2 = 2 + \sqrt{3} \Rightarrow (\alpha^2 - 2)^2 = 3 \Rightarrow p(x) = (x^2 - 2)^2 - 3$$

has root α

Ex: $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{R}$ alg? (<u>Yes</u>.)

$\alpha^2 = 2 + 2\sqrt{6} + 3$, ... ?

Thm (21.9) Let $F \subset E$ be a field extension and $\alpha \in E$. TFAE (the following are equivalent)

(i) α is transcendental

(ii) $F(\alpha) \cong F(x) := \mathrm{Frac}(F[x])$ field of rat'l functions

(iii) $[F(\alpha) : F] = \infty$

pf: Consider $F[x] \xrightarrow{ev_\alpha} E$ evaluation at α.

By definition α algebraic $\iff \exists p(x) \in \ker(ev_\alpha) \setminus \{0\}$

$\Rightarrow$ α transcendental $\iff \ker(ev_\alpha) = 0$

(i) $\Rightarrow$ (ii) $F[x] \xhookrightarrow{ev_\alpha} E$ injective

$\Rightarrow F[x] \hookrightarrow F(x) \hookrightarrow E$ $\quad F(x)$ smallest field containing α that is: $F(x) \cong F(\alpha)$

$x \longmapsto x \longmapsto \alpha$

(univ prop of fraction fields)

(ii) $\Rightarrow$ (iii) $F[x]$ is an F-vector space w/ basis $1, x, x^2, \ldots$

$[F(x) : F] > [F[x] : F] = \infty$

(iii) $\Rightarrow$ (i) Suppose α algebraic. Then $\exists p(x)$ s.t. $p(\alpha) = 0$. $\deg p = d$

$\Rightarrow F \longrightarrow F[x] \xrightarrow[\text{surj}]{} F[x]/(p(x)) \xrightarrow[\text{surj}]{} F(\alpha)$

basis $1, x, x^2, \ldots, x^{d-1}$ (see prev. ex. for $p(x) = x^2 + x + 1$)

$\Rightarrow [F(\alpha) : F] \leq d$.

Ex: $\mathbb{Q}(\pi) \cong \mathbb{Q}(x) \cong \mathbb{Q}(e)$

Quadratic integers (cont.)

$\mathbb{Z}[\sqrt{D}] \subset \mathcal{O}_{\mathbb{Q}(\sqrt{D})} \subset \mathbb{Q}(\sqrt{D})$

$\mathbb{Q}(\sqrt{D})$ fraction field of the two domains.

$\mathbb{Z}[\sqrt{D}] \subset \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$: quadratic integers (domains)

$\mathbb{Q}(\sqrt{D})$: quadratic numbers (field)

$\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ can be

- ED with Euclidean function the norm N
  "norm-Euclidean" — Ex: $\mathbb{Z}[\sqrt{-1}]$
- ED but not with the norm. — Ex: $\mathbb{Z}[\sqrt{14}]$
- PID but not ED — Ex: $\mathcal{O}_{\mathbb{Q}(\sqrt{-19})}$

$$\text{norm-ED} \Rightarrow \text{ED} \Rightarrow \text{PID} \overset{\text{for quadratic integers}}{\Leftarrow} \text{UFD}$$

Complete lists of PID, ED, norm-ED, see wikipedia.

about 30 such. most not UFDs.