Groups & Rings: Lecture #22

Algebraic extensions (§21.1)

- Minimal polynomials and simple extensions
- Finite extensions
- Algebraic closure

Recall:

Let E/F field extension $(F \subset E)$.

Def: An element $\alpha \in E$ is **algebraic** (over F) if

$$\exists p(x) \in F[x],\ p(x) \neq 0,\ p(\alpha) = 0.$$

Def: $\overline{\mathbb{Q}} = \{x \in \mathbb{C} : x \text{ algebraic over } \mathbb{Q}\}$ = algebraic numbers

Def: Let $\alpha \in E$. $F(\alpha) \subseteq E$ smallest subfield containing F and α.

Def: E/F is **simple** if $F(\alpha) = E$ for some $\alpha \in E$.

Def: Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$. $F(\alpha_1, \ldots, \alpha_n) \subseteq E$ smallest subfield cont. F and α_i.

Def: E/F is **finitely generated** if $F(\alpha_1, \ldots, \alpha_n) = E$ for some n and $\alpha_1, \ldots, \alpha_n \in E$.

Minimal polynomials and simple extensions

- **Thm 21.10:** E/F field extension, $\alpha \in E$ algebraic. Then
  $\exists!$ monic polynomial $p(x) \in F[x]$ s.th
  (i) $p(\alpha) = 0$
  (ii) if $f(x) \in F[x]$ s.th. $f(\alpha) = 0$, then $p \mid f$.
  Moreover, $p(x)$ is irreducible.

Def: $p(x)$ is the minimal polynomial of α. The degree of α is $\deg(p)$.

Rmk: (ii) $\Rightarrow$ $\deg p$ is minimal for polynomials vanishing at α.

- **Prop 21.12:** $F(\alpha) \cong F[x]/(p(x))$

- **Thm 21.13:** $F(\alpha)/F$ has basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ where $n = \deg(p)$
  In particular, $[F(\alpha) : F] = \deg(p)$.

Ex: (1) $\sqrt{2} \in \mathbb{C}$, $p(x) = x^2 - 2$ monic & irr $\overset{21.10}{\Rightarrow}$ this is the min. pol. $/\mathbb{Q}$

(2) $\alpha = \sqrt{2+\sqrt{5}} \in \mathbb{C}$, $[\alpha^2 = 2+\sqrt{5},\ (\alpha^2-2)^2 = 5] \rightsquigarrow$
$p(x) = x^4 - 4x^2 - 1$ monic, $p(\alpha) = 0$, irr $\Rightarrow$ min. pol. $/\mathbb{Q}$
(exc: $p(x)$ has neither linear nor quadratic factors)

(2') min. pol. $/\mathbb{Q}(\sqrt{5})$: $q(x) = x^2 - 2 - \sqrt{5}$

(3) $i \in \mathbb{C}$, $p(x) = x^2 + 1$ monic & irr $\Rightarrow$ min pol $/\mathbb{Q}$, min pol $/\mathbb{R}$
$\mathbb{C} = \mathbb{R}(i) \cong \mathbb{R}[x]/(x^2+1)$ basis $1, x$ $/\mathbb{R}$
(21.12 over $\cong$; 21.13 over basis)

(4) $\zeta \in \mathbb{C}$ p^{th} root of unity: $\zeta^p = 1$, $\zeta \neq 1$, $f(x) = x^p - 1$ is not irreducible

Claim: The cyclotomic polynomial $p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible.

proven on Lecture #18 (use $t = x + 1$ & Eisenstein's criterion)

Thus, $\mathbb{Q}(\zeta)/\mathbb{Q}$ has degree $p-1$ and basis $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$.

proof of Thm 21.10 ($\exists!$ of min. pol.)

- Have evaluation homomorphism $F[x] \xrightarrow{ev_\alpha} E$ with kernel $\ker(ev_\alpha) = \{f(x) : f(\alpha) = 0\}$. $f(x) \longmapsto f(\alpha)$
- $F[x]$ PID $\Rightarrow$ $\ker(ev_\alpha) = (p(x))$ principal ideal.
- α algebraic $\Leftrightarrow$ $\ker(ev_\alpha) \neq 0 \Leftrightarrow p(x) \neq 0$.
- Can choose $p(x)$ monic. This makes $p(x)$ unique. (o/w only unique up to mult. with a unit)
  This settles (i) and (ii) for $p(x)$.
- If $q(x)$ another pol satisfying (i) and (ii) then $p \mid q$ and $q \mid p \overset{\text{monic}}{\Rightarrow} p = q$.
- Remains to see that $p(x)$ is irreducible.
  We know $F[x]/(p(x)) \xrightarrow{\varphi} E$ is injective
  $\Rightarrow$ $F[x]/(p(x))$ is an integral domain $\Leftrightarrow$ $(p(x))$ prime
  But $p \neq 0$ so p irreducible. □

proof of Prop 21.12: ($F(\alpha) \cong F[x]/(p(x))$) $F[x]/(p(x)) \cong \mathrm{im}(\varphi)$ ← b/c φ injective

$F[x]/(p(x)) \xrightarrow{\varphi} E$ is injective $\Rightarrow$ $\mathrm{im}(\varphi) \subseteq E$ subfield containing α.

field b/c $p(x)$ irreducible $\Leftrightarrow$ $(p(x))$ maximal (or $F[x] \xrightarrow{ev_\alpha} E \Rightarrow \mathrm{im}(ev_\alpha) \cong F[x]/(p(x))$ ↑ 1st iso ev_α)

$\mathrm{im}(\varphi)$ smallest subfield containing α because

$\mathrm{im}(\varphi) = \{f(\alpha) : f(x) \in F[x]\}$ is the smallest ring containing α. □

proof of Thm 21.13: (on basis of $F(\alpha)$)

Follows from the following more general result:

Theorem: Let F be a field, let $R = F[x]/(p(x))$ with $p(x)$ monic of degree n. Then R has basis (as F-space) $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ where $\alpha := \bar{x} = x + (p(x)) \in R$.

proof: **Spans** First note that $\{1, \alpha, \alpha^2, \ldots\}$ spans R because $\{1, x, x^2, \ldots\}$ is a basis for $F[x]$.

If $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then

$$x^n = -(a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) + p(x) \quad \text{in } F[x]$$

$$\Rightarrow \alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \quad \text{in } R$$

$$\alpha^n \in \operatorname{span}\{1, \alpha, \ldots, \alpha^{n-1}\}$$

Then also for any $r > n$: $\alpha^r = \alpha^n \alpha^{r-n} = (\cdots)\alpha^{r-n} \in \operatorname{Span}\{\alpha^{r-n}, \ldots, \alpha^{r-1}\}$

By induction on r it follows that $\alpha^r \in \operatorname{Span}\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Linear independency Suppose $\exists a_i \in F$ s.th

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0 \quad \text{in } R$$

Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. Then $f(\alpha) = 0$ in R ($= ev_\alpha(f)$)

$\Leftrightarrow f(x) \in (p(x))$

$\Leftrightarrow f(x) = p(x)q(x)$ ($ev_\alpha : F[x] \to R$, $\ker(ev_\alpha) = (p(x))$)

$\Rightarrow \deg f \geq \deg p = n$ or $f = 0$ ($\deg f \leq n-1$)

$\Rightarrow f = 0 \Rightarrow a_0 = a_1 = \cdots = a_{n-1} = 0$.

□

Finite extensions

Recall: E/F finite if $[E:F]$ finite.

Thm 21.13 (above) gives us ($\alpha \in E$ alg. $\Rightarrow F(\alpha)/F$ finite)

Def: E/F algebraic if every $\alpha \in E$ is algebraic over F

Thm 21.15: E/F finite $\Rightarrow E/F$ algebraic

pf: Let $n = [E:F]$. Let $\alpha \in E$. Then $1, \alpha, \alpha^2, \dots, \alpha^n$ are linearly dep.

$\Rightarrow \exists\, a_i \in F$ not all zero s.th.

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0 \quad \text{in } E$$

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$. This is a non-zero polynomial s.th. $f(\alpha) = 0$, i.e., α is algebraic. □

Ex: Let $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt[4]{2})$, $\alpha, \beta \in E$

(1) $\alpha = \sqrt[4]{2}$, min pol $p(x) = x^4 - 2$ of deg 4

$\{1, \alpha, \alpha^2, \alpha^3\}$ basis for $F(\alpha) = E$

(2) $\beta = (\sqrt[4]{2})^2 = \sqrt{2}$, min pol $p(x) = x^2 - 2$ of deg 2

$\{1, \beta\}$ basis for $F(\beta) \subseteq E$

$$F = \mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha) = E$$

deg 2 deg 2

deg 4

Thm 21.17: K/E and E/F field extensions $(F \subseteq E \subseteq K)$

Then $[K:F] = [K:E] \cdot [E:F]$.

pf: If one extension is infinite then LHS = RHS = ∞.

Otherwise: pick bases

E: $\alpha_1 = 1, \alpha_2, \alpha_3, \dots, \alpha_n$ basis as an F-vector space

K: $\beta_1 = 1, \beta_2, \beta_3, \dots, \beta_m$ —"— E —"—

Claim: $\{\alpha_i \beta_j\}_{\substack{i=1,\dots,n \\ j=1,\dots,m}}$ basis for K as an F-vectorspace.

Let $z \in K$. Then $\exists! \; z = b_1\beta_1 + b_2\beta_2 + \dots + b_m\beta_m$, $b_j \in E$

Then $\exists! \; b_j = a_{j1}\alpha_1 + a_{j2}\alpha_2 + \dots + a_{jn}\alpha_n$, $a_{ji} \in F$

$\rightsquigarrow z \in \operatorname{span}\{\alpha_i\beta_j\}$. Not difficult to see lin. indep. □

Rmk: Claim often more useful than Thm.

Ex: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, i)$ split up into $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, i)$

$\Rightarrow$ basis $1, \sqrt{2}, i, i\sqrt{2}$.

deg $2 \cdot 2 = 4$.

basis $1, \sqrt{2}$, deg 2 — basis $1, i$, deg 2

Cor 21.19: (i) $F \subset E \subset K \Rightarrow [E:F] \mid [K:F]$ (analogue of Lagrange's theorem)

(ii) $F \subset F(\alpha) \subset F(\beta) \subset K \Rightarrow \deg p_\alpha \mid \deg p_\beta$

Warning: Can happen that $p_\alpha \neq p_\beta$.

Ex: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ $\quad \alpha = \sqrt{2}$, $\quad \beta = \sqrt{2} + 1$

$\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2})$ $\quad p_\alpha = x^2 - 2$, $\quad p_\beta = (x-1)^2 - 2$

Thm 21.22: Let E/F field extension. TFAE:

(i) E/F finite.

(ii) E/F finitely generated and algebraic

(iii) $E = F(\alpha_1, \dots, \alpha_n)$ and $\alpha_1, \alpha_2, \dots, \alpha_n$ are algebraic.

pf: (i) $\Rightarrow$ (ii) Thm 21.15 says finite $\Rightarrow$ algebraic

If $\alpha_1, \dots, \alpha_n$ basis $\Rightarrow E = F(\alpha_1, \dots, \alpha_n)$.

(ii) $\Rightarrow$ (iii) obvious from definition of alg.

(iii) $\Rightarrow$ (i) We have:

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \cdots \subseteq F(\alpha_1, \dots, \alpha_n) = E$$

finite (Thm 21.13) finite finite finite

(note that $F(\alpha_1, \dots, \alpha_i) = F(\alpha_1, \dots, \alpha_{i-1})(\alpha_i)$)

$\Rightarrow E/F$ finite by Thm 21.17. $\square$

Rmk: Not so obvious result!

Ex: $F = \mathbb{Q} \subset E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then Thm 21.22 says that $\alpha = \sqrt{2} + \sqrt{3}$ is algebraic. Takes a bit of work to find the minimal polynomial. (can use a basis of E/F to deduce this)

Algebraic closure

Def: A field F is **algebraically closed** if every $f(x) \in F[x]$ has a root in F.

Factor theorem gives:

Thm 21.25: F is alg. closed $\iff$ every $f(x) \in F[x]$ factors in linear factors.

Cor 21.26: F is alg. closed $\iff$ if $F \subseteq E$ alg extension, then $F = E$

(definition given on lecture #21)

Thm 21.28/23.33 (Fundamental theorem of algebra) $\mathbb{C}$ is alg. closed.

(perhaps proof at end of course)

Def: Let E/F field extension. The **algebraic closure of F in E** is:

$$\{\alpha \in E : \alpha \text{ algebraic over } F\}$$ (sometimes denoted $\overline{F}$)

Thm 21.23: The algebraic closure of F in E is a field.

proof: Let $\alpha, \beta \in E$ be algebraic over F, then $F(\alpha, \beta)$ is finite (Thm 21.22 above)

$\Rightarrow \alpha \pm \beta$, $\alpha\beta$, α/β ($\beta \neq 0$) $\in F(\alpha, \beta)$ are algebraic (Thm 21.22 again) $\square$

Lemma: If $F \subset E$ and E alg closed, then alg. closure of F in E is alg. closed.

pf: Let $\overline{F}$ be alg. closure of F in E. If $f(x) \in \overline{F}[x]$, then $f(x)$ has a root $\alpha \in E$. Thus α is algebraic over $\overline{F}$. More precisely, if

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \qquad a_i \in \overline{F}$$

then α algebraic over $F(a_0, a_1, \ldots, a_n)$. Thus: (Thm 21.22)

$$F \subset F(a_0, \ldots, a_n) \subset F(a_0, \ldots, a_n, \alpha)$$

($F \subset F(a_0, \ldots, a_n)$: finite; $F(a_0, \ldots, a_n) \subset F(a_0, \ldots, a_n, \alpha)$: finite)

$\Rightarrow \alpha$ algebraic over F, that is, $\alpha \in \overline{F}$ so $f(x)$ has root in $\overline{F}$. $\square$

Recall that $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.
Lemma says that $\overline{\mathbb{Q}}$ is algebraically closed.

Can we also embed fields such as $\mathbb{F}_p$ in an alg. closed field?

Fact (Thm 21.27) If F is a field, then $\exists$ algebraic extension $\overline{F}/F$ with $\overline{F}$ algebraically closed. The field $\overline{F}$ is unique (up to non-unique isomorphism).

The field $\overline{F}$ is called the algebraic closure of F. The idea is to take

$$\overline{F} = \text{"union of all finite field extensions } E/F\text{"}$$

If F sits inside an algebraically closed field K then this makes sense:

$$\overline{F} = \bigcup_{F \subset E \subset K \text{ finite}} E \qquad \text{e.g.} \quad \overline{\mathbb{Q}} = \bigcup_{\mathbb{Q} \subset E \subset \mathbb{C} \text{ finite}} E$$

but in general one has to make sense of the "union" without such a K.