Algebraic Extensions § 31

Recall E is a field extension of F if $F \subseteq E$

If $F \subseteq E$ are fields $\alpha \in E$ is algebraic over F if α is a zero of some $f(x) \in F[x]$

Ex
- any $\alpha \in F$ is algebraic over F — α is a zero of $f(x) = x - \alpha \in F[x]$
- $\mathbb{Q} \subseteq \mathbb{C}$ then $\sqrt{2}$, i, $\sqrt[k]{r}$ $(r \in \mathbb{Q})$ algebraic $/ \mathbb{Q}$
- If $\alpha \in E$ is algebraic then $F \subseteq F(\alpha) \subseteq E$ and every $\beta \in F(\alpha)$ is algebraic over F. (By Thm 30.23)

$$F(\alpha) \cong \frac{F[x]}{\langle irr(\alpha, F) \rangle}$$

Def 31.1 31.2 An extension E of F is an algebraic extension if $\forall \alpha \in E$ is algebraic / F.

If an extension E of F is an n-dimensional vector space over F, say E is a finite ext'n of degree n over F. Write $[E:F] = n$.

$[E:F] = n \iff \exists$ a basis $\{\alpha_1, \dots, \alpha_n\}$ of E over F
$E = \{a_1\alpha_1 + \dots + a_n\alpha_n \mid a_i \in F\}$.

Ex if $\alpha \in E$ alg over F
$F(\alpha)$ is algebraic extension over F of degree
$[F(\alpha) : F] = \deg(\operatorname{irr}(\alpha, F)) = n$.
Recall basis of $F(\alpha)/F$ is $\{1, \alpha, \dots, \alpha^{n-1}\}$

Last time The field extension $F(\alpha)$ is a vector space over F:

Thm 30.23 Let $E \supseteq F$ and suppose $\alpha \in E$ is alg. $/F$

1) If $\deg(\alpha, F) = n$ then $F(\alpha)$ is an n-dim'l vector space over F with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$

2) Also every elt β of $F(\alpha)$ is algebraic $/F$ and $\deg(\beta, F) \leq \deg(\alpha, F)$.

Proof sketch 1) $\alpha = x + \langle irr(\alpha, F) \rangle$ let $\underset{\overset{\shortparallel}{irr(\alpha,F)}}{f(x)} = a_0 + a_1 x + \ldots + x^n$ $\quad a_i \in F$

$\Rightarrow \alpha^n = -(a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1})$.

and any α^m $m \geq n$ can be written uniquely in terms of linear combinations $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$

$$F(\alpha) = \{b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} \mid b_i \in F\}$$

$$\downarrow \qquad\qquad \downarrow$$

$$F^n = \{(b_0, \ldots, b_{n-1}) \mid b_i \in F\}.$$

2) $\beta \in F(\alpha)$ $\quad 1, \beta, \beta^2, \ldots\ldots, \beta^n$] $n+1$ elts in a vector space of dim n.

$\in F(\alpha)$

$\Rightarrow$ dependent !

$\exists \; c_0, \ldots, c_n \in F$ not all zero s.t.

$$c_0 + c_1\beta + \cdots + c_n\beta^n = 0 \quad \text{in} \quad F(\alpha)$$

$\Rightarrow$ β is a zero of $g(x) = c_n x^n + \cdots + c_1 x + c_0$
$\in F[x]$.

So β is algebraic over F

and $\quad \mathrm{irr}(\beta, F) \leq \deg(g(x)) \leq \deg(f(x)) = \mathrm{irr}(\alpha, F)$

Thm 31.3 If $[E:F] = n < \infty$ then E is alg. over F
$E \supseteq F$

Proof Let $\alpha \in E$, then $1, \alpha, \alpha^2, \ldots, \alpha^n \in E$ $n+1$ elts
in a vector space of n dimensions $\xRightarrow{\text{Thm } 30.19}$
$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ for $a_i \in F$ not all zero.
$\Rightarrow \alpha$ is a zero of $f(x) = a_n x^n + \cdots + a_0 \Rightarrow$
α is alg over F $\square$.

What about the converse? If E is alg over F it need not have finite dim over F.
$\mathbb{Q} = F$ $E = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})(\sqrt{5})(\sqrt{6}) \ldots (\sqrt{n}) \ldots$ $\forall n \in \mathbb{Z}_+$
is an infinite dimensional vector space over $\mathbb{Q}$.

Example $\mathbb{Q}(\sqrt{2})$ is a simple extension of $\mathbb{Q}$

$\operatorname{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \quad \deg(\sqrt{2}, \mathbb{Q}) = 2 \quad \{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

$$\mathbb{Q}(\sqrt{2}) = \{ a_0 + a_1\sqrt{2} \mid a_0, a_1 \in \mathbb{Q} \}. \quad (*)$$

Notice $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ and $\operatorname{irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = \operatorname{irr}(\sqrt{3}, \mathbb{Q})$
$= x^2 - 3$.

so $\{1, \sqrt{3}\}$ is a basis of $\underbrace{(\underbrace{\mathbb{Q}(\sqrt{2})}_{F'})(\sqrt{3})}_{F'(\sqrt{3})}$ over $\underbrace{\mathbb{Q}(\sqrt{2})}_{F'}$.

$$(\mathbb{Q}(\sqrt{2}))(\sqrt{3}) = \{ b_0 + b_1\sqrt{3} \mid b_0, b_1 \in \mathbb{Q}(\sqrt{2}) \}$$ using $(*)$ for $b_0, b_1 \in \mathbb{Q}(\sqrt{2})$

$$= \{ (a_0 + a_1\sqrt{2}) + (a_0' + a_1'\sqrt{2})\sqrt{3} \mid a_0, a_1, a_0', a_1' \in \mathbb{Q} \}.$$

$$= \{ a_0 + a_1\sqrt{2} + a_0'\sqrt{3} + a_1'\sqrt{6} \mid a_0, a_1, a_0', a_1' \in \mathbb{Q} \}.$$

Turns out $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis of $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ over $\mathbb{Q}$.

$$[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}] = 4$$

$$\begin{tikzcd}
\mathbb{Q}(\beta) \arrow[d, phantom, "//"] & & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[d, phantom, "||"] \\
\mathbb{Q}(\sqrt{2})(\sqrt{3}) \arrow[r, phantom, "="] \arrow[d, dash, "\text{deg 2 ext}"'] \arrow[dr, dash, bend left, "\text{deg 4 extn}"] & & \mathbb{Q}(\sqrt{3})(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "\text{deg 2 ext}"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Aside $\beta = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2})(\sqrt{3})$.

$$\beta^2 = (\sqrt{2}+\sqrt{3})^2 = 2 + 2\sqrt{6} + 3$$

$$(\beta^2 - 5)^2 = (2\sqrt{6})^2$$

$$\Rightarrow \beta^4 - 10\beta^2 + 25 = 24.$$

$$\Rightarrow \beta^4 - 10\beta^2 + 1 = 0$$

β is a zero of $f(x) = x^4 - 10x^2 + 1$.

$f(x)$ factors $/\mathbb{Q}$ $\Longleftrightarrow$ $\underline{x^2 - 10x + 1}$ factors $/\mathbb{Q}$.

$x^2 - 10x + 1$ is irr. over $\mathbb{Q}$.

$\Rightarrow \operatorname{Irr}(\beta, \mathbb{Q}) = x^4 - 10x^2 + 1$

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2})(\sqrt{3}) \arrow[d, dash] \arrow[dd, bend left=60, dash, "\deg 4"] \\
\mathbb{Q}(\beta) \arrow[d, dash, "\deg 4"'] \\
\mathbb{Q}
\end{tikzcd}$$

Both $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ and $\mathbb{Q}(\beta)$ are ~~a~~ 4 dim'l vector spaces over $\mathbb{Q}$ and

$$\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{3})$$

$$\Longrightarrow \quad \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2})(\sqrt{3}).$$

Thm 31.4 Let $K \supseteq E \supseteq F$ be fields then with $[K:E]$ and $[E:F]$ finite then

$$\underset{m}{\overset{\shortparallel}{[K:F]}} = [K:E][E:F]$$

with $[K:E] = m$ and $[E:F] = n$. In particular, K is finite dim'l over F.

Proof Sketch Suppose $\{\alpha_1, \dots, \alpha_n\}$ is a basis for E over F and $\{\beta_1, \dots, \beta_m\}$ is a basis for K over E.

$$K = \{ b_1\beta_1 + \dots + b_m\beta_m \mid b_j \in E \}$$
$$= \{ (a_{11}\alpha_1 + \dots + a_{n1}\alpha_n)\beta_1 + \dots + (a_{1m}\alpha_1 + \dots + a_{nm}\alpha_n)\beta_m \mid a_i \in F \}.$$

$$= \left\{ \sum_{\substack{1 \le i \le n \\ 1 \le j \le m}} a_{ij}(\alpha_i \beta_j) \mid a_{ij} \in F \right\}.$$

Claim (see text) $\{\alpha_i \beta_j\}$ is a basis for K over F

$$|\{\alpha_i \beta_j\}| = nm = [K:F] \qquad \square.$$

$\boxed{\text{In our previous example } \{1, \sqrt{2}\},\ \{1, \sqrt{3}\} \rightsquigarrow \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}}$

Corollaries

31.6 If $F_1 \subseteq F_2 \subseteq \dots \subseteq F_r$ are finite field extensions

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_2 : F_1].$$

31.7 If $E \supseteq F$ and $\alpha \in E$ is alg. over F then $\forall\ \beta \in F(\alpha)$ $\deg(\beta, F)$ divides $\deg(\alpha, F)$.

Proof 31.7 $F(\alpha) \ni \beta$ and $F \subseteq F(\beta) \subseteq F(\alpha)$.

$$\Rightarrow \underbrace{[F(\alpha):F]}_{\deg(\alpha,F)} = [F(\alpha):F(\beta)]\underbrace{[F(\beta):F]}_{\deg(\beta,F)}$$

Ex 81.10 Consider $2^{1/3}, 2^{1/2} \in \mathbb{R}$

$irr(2^{1/3}, \mathbb{Q}) = x^3 - 2$

$irr(2^{1/2}, \mathbb{Q}) = x^2 - 2$.

Algebraic Closure

Let $E \supseteq F$. The algebraic closure of F in E is $\overline{F}_E = \{\alpha \in E \mid \alpha \text{ is alg. over } F\}$.

(This is a subfield of E by Thm 31.12).

Ex 1) E is algebraic over F $\Longleftrightarrow$ $\overline{F}_E = E$

2) Recall $\alpha \in \mathbb{C}$ is an algebraic number if it is algebraic over $\mathbb{Q}$ ($\sqrt{2}$, $\sqrt[3]{n}$, ... $\in \mathbb{C}$ algebraic #'s but e, π not algebraic)

$\overline{\mathbb{Q}}_{\mathbb{C}}$ is the field of algebraic.

$\sqrt{5} \in \mathbb{C}$ is alg.

$\sqrt{5} \in \overline{\mathbb{Q}}_{\mathbb{C}}$ $\Longrightarrow$ $\overline{\mathbb{Q}}_{\mathbb{C}}$ field

$1, \frac{1}{2}$

$\frac{1+\sqrt{5}}{2} \in \overline{\mathbb{Q}}_{\mathbb{C}}$

3) $E = \mathbb{Q}(x)$ then $\overline{\mathbb{Q}}_E = \mathbb{Q}$.

simple transcendental extension of $\mathbb{Q}$.

Def A field F is algebraically closed if every non-constant polynomial $f(x) \in F[x]$ has a zero in F.

Ex $\mathbb{C}$ is alg. closed (Thm 31.18) Fundamental Thm of Alg.

Thm 31.15 A field F is alg closed if and only if every non-constant polynomial factors into linear factors over F $f(x) = c\prod_{i=1}^{\deg f}(x-a_i)$ c, $a_i \in F$, $x-a_i \in F[x]$

Proof $\Leftarrow$ is clear

$\Rightarrow$ Suppose $f(x)$ has a zero $a_1 \in F[x]$ $f(x) = (x-a_1)g(x)$ by division alg. $g(x) \in F[x]$ now find a zero a_2 of $g(x)$ and continue until $f(x) = c\prod(x-a_i)$ $\square$

An algebraically closed field has <u>no</u> algebraic extensions (Cor 31.16) ($\Rightarrow$ all extensions of alg closed fields are ∞ degree).

<u>Thm 31.17</u> Every field F has an algebraic closure $\overline{F}$. (Proof is difficult + omitted!)

(i.e. a field $\overline{F}$ which is alg. closed and with $F \subseteq \overline{F}$)

<u>Ex</u> 1) $\mathbb{R} = F$ $\quad \overline{\mathbb{R}} = \underset{\mathbb{R}(i)}{\overset{\|}{\mathbb{C}}}$ $\quad [\mathbb{C} : \mathbb{R}] = 2$ finite

$\quad\ \ \cup\!\!|$

2) $\mathbb{Q} = F$ $\quad \overline{\mathbb{Q}}$ is the set of algebraic #'s.

$E = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \ldots (\sqrt{n}) \ldots \ldots$ $\forall\ n \in \mathbb{Z}_+$ $\quad$ E is an infinite ext'n $\mathbb{Q}$ and $E \subsetneq \overline{\mathbb{Q}}$ $\Rightarrow$ $\overline{\mathbb{Q}}$ is ∞ over $\mathbb{Q}$.

3) $\mathbb{Z}_p$ p prime what is $\overline{\mathbb{Z}_p}$.

finite Extensions of $\mathbb{Z}_p$ came from $E = \dfrac{\mathbb{Z}_p[x]}{\langle f(x) \rangle}$ $f(x) \in \mathbb{Z}_p[x]$ irreducible.

$\mathbb{Z}_2 = \{0,1\}$. $f(x) = x^2 + x + 1 = g(x)h(x)$ / $\mathbb{Z}_2$.

$f(0) = 1 \neq 0$
$f(1) = 1 \neq 0$
no root so no factorisation so $f(x)$ is irreducible.

$E = \dfrac{\mathbb{Z}_2[x]}{\langle f(x) \rangle} \ni \alpha = x + \langle f(x) \rangle$

$f(\alpha) = (x + \langle f(x) \rangle)^2 + (x + \langle f(x) \rangle) + 1$
$= x^2 + x + 1 + \langle f(x) \rangle = \langle f(x) \rangle = 0$ in E

$$\mathbb{Z}_p[x] \big/ \langle f(x) \rangle = E$$

field

next time

construct finite fields $\mathbb{F}_q$ with $q = p^k$ elts $\forall$ p prime + any k.

"The Weil conjectures" Karen Olsson