Lecture 29: Field extensions

§ 1 of [R3]
§ 13.1 of [DF]

F a field.

Characteristic: smallest $n \geq 1$ such that $\underbrace{1+1+\cdots+1}_{n} = 0$, or 0 if no such n exists.

Ex: $ch(\mathbb{Q}) = 0$, $ch(\mathbb{F}_p) = p$, $char(Frac(\mathbb{F}_p[x])) = p$.

Note: If $ch(F) \neq 0$, it is prime. If $ch(F) = a \cdot b$ then $0 = \sum^{ab} 1 = (\sum^{a} 1)(\sum^{b} 1) \Rightarrow$ one of $\sum^{a} 1$ and $\sum^{b} 1$ is zero.

Prime subfield: Subfield generated by 1.

Is $\mathbb{Q}$ when $ch = 0$ and $\mathbb{F}_p$ when $ch = p$.

Field Extension: [Key concept!] If F is a subfield of K, we call K an extension of F and write K/F or

$$\begin{matrix} K \\ | \\ F \end{matrix}$$

Ex: $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}(i)/\mathbb{Q}$. The field of ration functions $\mathbb{C}(x) := Frac(\mathbb{C}[x])$ is an extension of $\mathbb{C}$. [Any field is an ext. of its prime subfield.]

Given K/F, as $F \subseteq K$ is a subring, can view K as an F-vector space: $f \cdot k = fk$.

Ex: ① $\mathbb{C}/\mathbb{R}$ $\mathbb{C}$ has $\{1, i\}$ for an $\mathbb{R}$-basis.

② $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}/\mathbb{Q}$ has basis $\{1, \sqrt{2}\}$

Degree: $[K : F] = \dim_F K$

Ex: $[\mathbb{C} : \mathbb{R}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{R} : \mathbb{Q}] = \infty$

Tower Law: Suppose $F \subseteq K \subseteq L$ are fields. Then

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

[Infinite degrees allowed here]

Idea: Suppose $\alpha_1, \ldots, \alpha_m$ is an F basis for K and $\beta_1, \ldots, \beta_n$ is a K basis for L. Then $\{\alpha_i \beta_j\}$ is an F basis for L.

Span: Suppose $\gamma \in L$. Then $\gamma = \sum \delta_j \beta_j$ for some $\delta_j \in K$. Each $\delta_j = \sum (\text{in } F) \alpha_i$, now expand. See text for F-lin. indep.

Building fields by adding roots: Start with a field F and $p(x) \in F[x]$ irreducible. Then

$K = F[x]/(p(x))$ is a field (Why? $F[x]$ is a PID)

Elts of K are $g(x) + I$ where $g \in F[x]$ and $I = (p)$.

Can assume $\deg g < \deg p$ as $g = qp + r$ with $\deg r < \deg p$, and $g + I = r + I$. Moreover, if $\deg g < \deg p$, then $g + I = 0 \iff g = 0$ as 0 is the only elt of $I = (p)$ of deg $<$ deg p.

So:

$$K \xleftrightarrow{\text{bijection}} \left\{ \begin{array}{l} \text{polys of } F[x] \\ \text{of deg} < \deg p \end{array} \right\}$$

Ex: $F = \mathbb{R}$, $p = x^2 + 1$ which is irred as no roots in $\mathbb{R}$.

$$K = \mathbb{R}[x]/(x^2+1) = \{ ax + b + I \mid a, b \in \mathbb{R} \}$$

Q: What is an $\mathbb{R}$-basis for K? A: $\{1 + I, x + I\}$

In general, $\left[K = F[x]/_{(p(x))} : F\right] = \deg p := d$

since, setting $\theta := x + (p)$, we see $1, \theta, \theta^2, \ldots, \theta^{d-1}$ is an F-basis for K.

Note: θ is a root of $p(x)$ since $p(\theta) = p(x) + (p(x)) = 0$ in K. We think of K as adding a root of $p(x)$ to F!

Ex: $F = \mathbb{R}$, $p = x^2 + 1$ $\quad K = \mathbb{R}[x]/_{(x^2+1)} \cong \mathbb{C}$

$1 \longleftrightarrow 1$

$\theta \longleftrightarrow i$ (or $-i$)

Notation: $\alpha_1, \ldots, \alpha_n \in K$ with $F \subseteq K$. Then

$K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ = field generated by F and the α_i

[i.e. smallest subfield containing $F \cup \{\alpha_i\}$.]

Ex: $K = \mathbb{C}$, $F = \mathbb{Q}$: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$

$\mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{11})$

Simple extension: $K = F(\alpha)$ for some $\alpha \in K$
(α: primitive element.)

Ex: $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$ is simple as $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{2}+\sqrt{5})$ since $\sqrt{2} = \frac{1}{6}(\alpha^3 - 11\alpha)$.

Ex: $K = F[x]/(p(x))$ is simple over F with $\alpha = x + (p(x))$.

Thm: $p(x) \in F[x]$ irreducible. Suppose K/F is simple with prim. elt α. If $p(\alpha) = 0$ then $F[x]/(p(x))$ is isomorphic to K.

$L :=$

Pf: Consider $F[x] \xrightarrow{\tilde{\psi}} K$, a ring homom.
$f(x) \longmapsto f(\alpha)$

As $p \in \ker \tilde{\psi}$, get an induced ring homom

$\psi : L \to K$. Now $\psi(L) \subseteq K$ is a subfield containg F and α, so $\psi(L) \supseteq F(\alpha) = K$. Now $\ker(\psi) = \{0\}$ or L and its not the latter as $1_L \longmapsto 1_K$. So ψ is a bijection, as claimed. ▨