Lecture 19

Let F be a field, and let $\operatorname{char} F$ be its characteristic, the order of 1_F in the additive group F. (Review field theory basics if needed!)

defn The prime subfield of F is the subfield of F generated by 1, and is isom to either

- $\mathbb{Q}$ (if $\operatorname{char} F = 0$) or
- $\mathbb{F}_p$ (if $\operatorname{char} F = p$).

defn If F is a subfield of a field K, then K is an (field) extension of F; we call F the base field of the extension "K over F"
↳ denoted K/F (not quotient)

Diagram:
K
|
F

ie. a field extension is the data "$F \subseteq K$."; cf.

defn The degree (or index) of the extension K/F, denoted $[K:F]$
(just as we denote indices of subgroups)
is $\dim_F K$ (dim of K as a VF over F).

- K/F is a finite extension of $[K:F] < \infty$
- K/F is infinite otherwise.

eg. ① any field is an extension of its prime subfield.
② $\mathbb{C} = \mathbb{R} + \mathbb{R}i$ or, $\mathbb{C} \cong \mathbb{R}[x]/(x^2-1)$.

Algebraic field extensions: add roots of irred. polynomials to the ground field.

rmk. Let $\varphi: F \to F'$ be a field hom.

Then φ is either 0 or injective.

because $\ker\varphi$ is an ideal of F. $\Rightarrow \ker\varphi \in \{0, F\}$.

thm. Let $p(x) \in F[x]$ be an irred polynomial. (recall? important!)

Then there is an extension field K of F where $p(x)$ has a root.

(more precisely, K contains an isom copy of F)

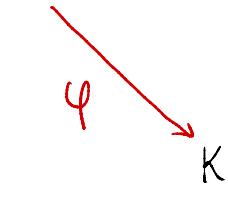
Pf Let $K = F[x]/(p(x))$.

- Since $p(x)$ is irreducible in the PID $F[x]$,

  $(p(x))$ is a maximal ideal. Therefore K is a field.

  Recall $m \subset R$ is maximal iff R/m is a field.

- Furthermore,



$\varphi(1) = 1$ so $\varphi \neq 0$.

$\Rightarrow \varphi$ is injective.

$\Rightarrow \varphi(F) \cong F$.

So now we view F as its image $\varphi(F) \subseteq K$.

Finally, $\bar{x} := \pi(x)$ is a root of $p(x)$ in K:

$p(\bar{x}) = \underbrace{\overline{p(x)}}_{p(x) \pmod{p(x)}} = 0 \in K$.

as the polyn. fn p and π commute, since π is a ring hom.

∎

defn. An extension of F containing all the roots of $p(x)$ is a splitting field of $p(x)$, because we can factor $p(x)$ into linear factors.

eg. $p(x) = x^2+1 \in \mathbb{R}[x]$ is irreducible.

But over $\mathbb{C}$, the polynomial $p(x)$ factors as $p(x) = (x-i)^2$.

thm. Let $p(x) \in F[x]$ be irreducible, degree n.

Let $K = F[x]/(p(x))$.

Let $\theta = x \bmod (p(x)) = x + (p(x)) \in K$.

Then $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ are a basis for K as a VS over F.

Rmk. ① $\Rightarrow [K:F] = n$

② In other words,

$$K = \left\{ \sum_{i=0}^{n-1} a_i \theta^i \mid a_i \in F \ \forall i \right\}.$$

= polys of degree $< n$ with coeffs in F.

pf.

$$\pi : F[x] \longrightarrow K = F[x]/(p(x))$$
$$a(x) \longmapsto a(x) \bmod p(x)$$

Notation: "$a(x) \equiv a(x)\ p(x)$" etc.

① Every $a(x) \equiv$ a polyn of degree $< n$:

$F[x]$ is a ED $\Rightarrow$ we can write (using div. algorithm)

$a(x) = q(x) \cdot p(x) + r(x)$ where $q(x), r(x) \in F[x]$,

$\deg r(x) < n$.

$\Rightarrow a(x) \equiv r(x)$

② $\{1, \theta, \ldots, \theta^{n-1}\}$ are linearly independent

Suppose BWOC $\sum_{i=0}^{n-1} b_i \theta^i = 0$ $\quad b_i \in F \ \forall i$, with not all $b_i = 0$.

Then $\sum_{i=0}^{n-1} b_i x^i \equiv 0 \mod (p(x))$

$\Rightarrow p(x)$ divides $\sum_{i=0}^{n-1} b_i x^i$

But $\deg p(x) = n > \deg \sum_{i=0}^{n-1} b_i x^i$. ↯. ∎

Rmk.

① So we describe elements of $K = F[x]/(p(x))$ as polynomials in θ where $p(\theta) = 0$.

We'll actually write $a(x)$, but take only the remainder.

② addition & multiplication of assets as usual:

For $a(x), b(x)$ of degree $< n$,

- addition: $a(x) + b(x)$
- mult: remainder of $a(x)b(x) \mod (p(x))$.

③ Also, note that if $c \in F$, $F[x]/(p(x)) \cong F[x]/(c \cdot p(x))$.

So it suffices to only consider monic polynomials.

If $p(x)$ is monic, then

$$p(\theta) = \theta^n + p_{n-1}\theta^{n-1} + \ldots + p_1\theta^1 + p_0 = 0$$

$$\Rightarrow \theta^n = -(p_{n-1}\theta^{n-1} + \ldots + p_1\theta^1 + p_0)$$