Announcement: H/w #1 posted on course website
due Tues. 1/17 noon via Gradescope

Last time: whole course in 30 minutes

Today: back to the beginning (§13.1)

Recall: A fied F is a commutative ring with identity in which every nonzero elt. has an inverse

$$F^\times = F \setminus \{0\} \text{ is an abelian group under multiplication}$$

Def: <u>Characteristic</u> of F: $ch(F)$ = smallest pos. int. n such that

$$n \cdot 1_F := \underbrace{1_F + 1_F + \cdots + 1_F}_{n \text{ terms}} = 0_F$$

(usually write "$n = 0$")

If no such n exists, then $ch(F) = 0$.

$Ch(F)$ must be prime (or 0):

If $ch(F) = ab$, then

$$0 = ab \cdot 1_F \underset{\uparrow}{=} (a \cdot 1_F)(b \cdot 1_F)$$

distributive law

one of these must be 0 since F: integral domain

Ex:

1) $ch(\mathbb{Q}) = ch(\mathbb{R}) = ch(\mathbb{C}) = ch(\mathbb{Z}) = 0$

2) $ch(\mathbb{F}_p) = p$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ p: prime

3) The polynomial ring $\mathbb{F}_p[x]$ has char. p,

as does its field of fractions $\mathbb{F}_p(x)$

Natural ring homomorphism

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow F \\ n &\longmapsto n \cdot 1_F \end{aligned} \qquad \left(\begin{array}{l} 0 \cdot 1_F := 0_F \\ (-n) \cdot 1_F := -(n \cdot 1_F) \end{array} \right)$$

F : char $0 \Rightarrow \varphi$ injective

Extend φ to $\mathbb{Q}$: $\varphi(\frac{a}{b}) = \frac{\varphi(a)}{\varphi(b)}$ is still injective

F : char $p \Rightarrow \ker \varphi = p\mathbb{Z} \Rightarrow \mathbb{Z}/p\mathbb{Z} \to F$ is injective

So we have an inj. homom φ' from $\underset{(\text{char } 0)}{\mathbb{Q}}$ or $\underset{(\text{char } p)}{\mathbb{Z}/p\mathbb{Z}}$ into F

Def: The <u>prime subfield</u> of F is $\operatorname{im}(\varphi')$. It is generated by 1_F (i.e. smallest subfield of F containing 1_F) and is isom. to $\begin{cases} \mathbb{Q} & \text{if } \operatorname{char}(F) = 0 \\ \mathbb{F}_p & \text{if } \operatorname{char}(F) = p \end{cases}$

Ex: 1) The prime subfield of $\mathbb{Q}$, $\mathbb{R}$, or <u>any</u> field containing $\mathbb{Q}$ is $\mathbb{Q}$.

2) The " " of $\mathbb{F}_p(x)$ is $\mathbb{F}_p$.

Def: If K, F are fields w/ $F \subseteq K$, then the pair of fields K/F is called a field extension $\quad F$: base field

K: extn field

(<u>not</u> a quotient!

Also write: $\begin{array}{c} K \\ | \\ F \end{array}$ for K/F

E.g.: Every field is an extension of its prime subfield

Fix a field F and an irreducible poly. $p \in F[x]$:

$$p(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_1 x + p_0$$

Is there always a field ext'n containing a root of p?

Ans: Yes! DBF

Thm 3: $K := F[x]/(p(x))$ is a field containing a root of p and a subfield isom. to F.

Pf: Since $F[x]$ is a PID,

$$\underset{\text{irred.}}{p(x)} \Rightarrow \underset{\text{max'l ideal}}{(p(x))} \Rightarrow K: \text{field}$$

Let $\pi: F[x] \twoheadrightarrow K$ canonical projection

π inj. on F, so $\pi(F) \cong F$ (field has no nontriv. ideals)

$p(\pi(x)) = \pi(p(x)) = 0$, so $\pi(x) \in K$ is a root of p

---

$\square$

Def: The degree of a field ext'n K/F is

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

Thm 4: Let $\theta = \pi(x) \in K$. Then,

$$1, \theta, \theta^2, \ldots, \theta^{n-1} \quad \text{is a basis for } K \text{ as an } F\text{-v.s.}$$

i.e. $K = \{a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1} \mid a_i \in F\}$ polys of deg $< n$ in θ

In particular, $[K:F] = n$.

Pf Sketch: $F[x]$: Euclidean domain, so divide w/ remainder:

$$a(x) = q(x)\,p(x) + \underbrace{r(x)}_{\deg < n} \mapsto r(\theta)$$