Apr 12: Field extensions

Quiz 1
- download "Quiz 1" when you want to start your 30 min
- upload "Upload quiz 1"

Today
- field extensions $F \to K$
- degree $[K:F] = \dim_F K$
- vector spaces & basis
- irreducible polynomial & Eisenstein
- simple field extension

Following 11.1 in Hungerford

§1. Vector spaces

Let V be a vector space over a field F.

[Have addition in V
scalar mult of F acting on V]

- A basis of V is a set $\{v_1, v_2, \ldots\}$ such that every $x \in V$ can be uniquely written as

$$x = a_1 v_1 + a_2 v_2 + \cdots$$

- $\dim_F V$ = # elements of basis

Ex: $\dim_F F[x] = \infty$

$\{1, x, x^2, \ldots\}$ is basis

$\dim_F F[x]/x^n = n$ b/c

$\{1, x, x^2, \ldots x^{n-1}\}$

Defn A field extension is a homomorphism $F \to K$ of fields.

Rmk: $F \to K$ is injective.

If $F \xrightarrow{\phi} K$ is a field extension, then we can view K as a vector space over F.

add in K is addition

Given $\alpha \in F$ and $x \in K$, then $\alpha x \in K$ product when I view $\alpha \in K$

$$\left(\alpha x = \underbrace{\phi(\alpha)}_{\text{in } K} \cdot \underbrace{x}_{\text{in } K} \right)$$

Ex: $\mathbb{R} \overset{\phi}{\hookrightarrow} \mathbb{C}$

Ex: $\mathbb{R} \to \mathbb{R}[x]$ not field ext

$\mathbb{R} \to \mathbb{R}(x)$ field ext

Defn A *field extension* is a homomorphism $F \to K$ of fields

Rmk: $F \to K$ is injective.

If $F \to K$ is a field extension, then we can view K as a vector space over F.

$\mathbb{R}$, $\mathbb{C}$ both fields

$\mathbb{R} \subset \mathbb{C}$

$\mathbb{R} \xrightarrow{\phi} \mathbb{C}$, $\phi(\mathbb{R}) \subset \mathbb{C}$

$x \longmapsto x + 0 \cdot i$

$i = \sqrt{-1}$

Defn The degree of a field extension $F \to K$ is

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

dim of K as a vector space over F

Ex: $[\mathbb{C}:\mathbb{R}] = 2$

$[\mathbb{Q}(i):\mathbb{Q}] = 2$

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

(reason: $1, \sqrt[3]{2}, \sqrt[3]{4}$ basis)

HW 3.2(b)

Defn Let $F \to K$ field ext.

- Let $\alpha \in K$. $F(\alpha)$ is the smallest subfield of K containing α and F.
- Let $\alpha_1, \dots, \alpha_n \in K$. $F(\alpha_1, \dots, \alpha_n)$ is the smallest subfield of K containing α_i and F.
- We say $F \to K$ is *simple* if $K = F(\alpha)$ for some $\alpha \in K$.

§2. Irred polynomial

F field

FACT If $f \in F[x]$ irred., then $F[x]/(f)$ is a field and $F \to F[x]/(f)$ field ext.

Related to Problem 3.3

$\rightsquigarrow$ Fact: $\{1, x, x^2, \ldots, x^{d-1}\}$ is a basis of $F[x]/(f)$ over F.

Here: $d = \deg f$

$$\Rightarrow \dim_F F[x]/(f) = d$$

$$[F[x]/(f) : F] = d$$

Ex 1 $x^2+1 \in \mathbb{R}[x]$ irred

$$\mathbb{R} \to \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$$

Ex 2

$$\mathbb{Q}[\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3-2)$$

Recall a couple techniques to show that $f \in \mathbb{Z}[x]$ irred

① If $\deg f = 2$ or 3, can just check it has no roots

② If $\exists$ prime $p \in \mathbb{Z}$ such that the image of f under $\mathbb{Z}[x] \to \mathbb{Z}/p[x]$ is irreducible, then f is irreducible

③ Eisenstein's criterion $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$

$\exists$ prime $p \in \mathbb{Z}$ such that

① $p \nmid a_n$

② $p \mid a_{n-1}, \ldots, a_0$

③ $p^2 \nmid a_0$

Question: Is $\mathbb{Q} \to \mathbb{Q}(\sqrt{2},\sqrt{3})$ a simple field extension?

Recall this means $\exists\, \alpha \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ s.t. $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2},\sqrt{3})$

$$\sqrt{6} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$$

$$\mathbb{Q} \longrightarrow \mathbb{Q}(\sqrt{6}) \longrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})$$

Can view

$$\mathbb{Q} \xrightarrow[\text{simple}]{} \mathbb{Q}(\sqrt{2}) \xrightarrow[\text{simple}]{} \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$$

Answer: $\mathbb{Q} \longrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})$ is simple.

candidates $\sqrt[4]{6}$

$\sqrt{2}\cdot\sqrt{3} = \sqrt{6}$

$\boxed{\sqrt{2}+\sqrt{3}}$ ✓

$$|\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}| = 4$$

$$|\mathbb{Q}(\sqrt{6}) : \mathbb{Q}| = 2$$