Field extensions

Recall: A field is a comm. ring w/ 1 in which every nonzero elt. has an inverse

Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_{p^n}$ (p: prime)

$\mathbb{Q}(x) = \left\{ \begin{matrix} \text{rational} \\ \text{functions} \end{matrix} \ \frac{p(x)}{q(x)},\ p,q \in \mathbb{Q}[x] \right\} =$ field of fractions of $\mathbb{Q}[x]$

$\mathbb{Q}((t)) = \left\{ \begin{matrix} \text{formal Laurent} \\ \text{power series} \end{matrix} \ a_n t^n + a_{n+1} t^{n+1} + \dots ,\ n \in \mathbb{Z} \right\}$

$\mathbb{Q}(i)$ "Gaussian rationals"

$\mathbb{Q}(\zeta_n)$ nth root of 1

$\mathbb{Q}(\sqrt{D})$ $D \in \mathbb{Q}$

Characteristic: Smallest $n > 0$ s.t.

$$n \cdot 1 = \underbrace{1 + \cdots + 1}_{n} = 0 \text{ in } F$$

OR char $F = 0$ if no such n exists

E.g.: $\text{char } \mathbb{C} = \text{char } \mathbb{Q} = \text{char } \mathbb{Q}(\zeta_n) = 0$

$\text{char } \mathbb{F}_p = \text{char } \mathbb{F}_p(x) = \text{char } \mathbb{F}_p((x)) = p$

Prop: $n := \text{char } F$

a) n is either 0 or prime.

b) If $\alpha \in F$, $n \cdot \alpha = \underbrace{\alpha + \cdots + \alpha}_{n} = 0$

Pf: a) If $n = ab \neq 0$, then

$(a \cdot 1) \cdot (b \cdot 1) = (ab \cdot 1) = 0$, so

$a \cdot 1$ or $b \cdot 1$ is 0, contradicting the minimality of n.

b) $\overbrace{\alpha + \cdots + \alpha}^{n} = \alpha(1 + \cdots + 1) = \alpha(0) = 0$ $\square$

Prime subfield: subfield of F generated by 1_F

(smallest subfield of F containg 1)

it is (isom. to) $\begin{cases} \mathbb{Q}, & \text{if char } F = 0 \\ \mathbb{F}_p, & \text{if char } F = p \end{cases}$

Def: If K, F are fields w/ $F \subseteq K$, the pair $\underbrace{K/F}_{\text{not a quotient!}}$ is called a <u>field extension</u>

F: base field

K: extension field

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

E.g.: $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, $\mathbb{F}_p((t))/\mathbb{F}_p$

$F/$prime subfield of F

Def: A set V is an F-vector space if given $f \in F$, $v \in V$, $f \cdot v \in V$ and

$$f \cdot (v_1 + v_2) = f v_1 + f v_2$$

$$f_1 (f_2 \cdot v) = (f_1 f_2) \cdot v$$

$$(f_1 + f_2) \cdot v = f_1 \cdot v + f_2 \cdot v$$

$$1_F \cdot v = v$$

A <u>basis</u> of V (over F) is a set $S \subseteq V$ s.t.

- S <u>spans</u> V: every $v \in V$ can be written

$$v = f_1 v_1 + \cdots + f_n v_n, \quad f_i \in F,\ v_i \in S$$

- S is <u>linearly independent</u>:

If $f_1 v_1 + \cdots + f_n v_n = 0$, then $f_1 = \cdots = f_n = 0$

$f_i \in F,\ v_i \in S$

Equivalent definition of a basis:

Every $v \in V$ can be written <u>uniquely</u> as

$$v = f_1 v_1 + \cdots + f_n v_n, \quad f_i \in F,\ v_i \in S$$

The dimension of V over F is $\dim_F V := |S|$ for any basis S (Prop: This is independent of the basis chosen)

If $T \subseteq V$ and

- $|T| < \dim V$, then $\operatorname{span} T \subsetneq V$
- $|T| > \dim V$, then T is linearly dependent

E.g. a) $\mathbb{R}^3 = \{(a,b,c) \mid a,b,c \in \mathbb{R}\}$ is an $\mathbb{R}$-v.s. of dim 3

$\{(1,0,0), (0,1,0), (0,0,1)$ is a basis$\}$

So is $\{(1,1,1), (1,-1,0), (0,1,-1)\}$

b) $\mathbb{Q}[x] = \{a_0 + \cdots + a_n x^n \mid a_i \in \mathbb{Q}\}$ is an ∞-dim'l $\mathbb{Q}$-v.s.

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

c) $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ is a 2-dim'l $\mathbb{Q}$-v.s.
w/ basis $\{1, \sqrt{2}\}$.

(See D&F §11.1 for more)

Prop: An extension field K of F is a vector space over F

Pf: check axioms

The <u>degree</u> $[K:F] := \dim_F K$

Examples:

a) $\mathbb{C}/\mathbb{R}$: $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, so

$S = \{1, i\}$, $[\mathbb{C}:\mathbb{R}] = 2$

b) $\mathbb{Q}/_{\mathbb{Q}(\sqrt{2})}$: $\mathbb{Q} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, so

$S = \{1, \sqrt{2}\}$ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

c) $\mathbb{F}_p(x)/\mathbb{F}_p$: $1, x, x^2, \ldots$ are linearly indep.,

so $[\mathbb{F}_p(x) : \mathbb{F}_p] = \infty$

Goal: form field extensions by adding roots of polys.

F: field, $p(x) \in F[x]$ irred., nonconstant

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

Prop: K is a field

Pf: $p(x)$ irred. $\Rightarrow$ $p(x)$ prime (since $F[x]$ is a PID)

$\Rightarrow (p(x))$ prime

$\Rightarrow (p(x))$ maximal (since $F[x]$ is a PID)

$\Rightarrow K$ is a field. $\square$

Thm: K is an extension field of F containing a root θ of p. If $\deg p = n$, then $\{1, \theta, \dots, \theta^{n-1}\}$ is a basis for K over F, so $[K:F] = n$.

Pf: $F \xhookrightarrow[\text{inclusion}]{} F[x] \xrightarrow[\text{projection}]{} \!\!\!\rightarrow F[x]/(p) = K$,

and the composition of these maps is inj.,

so $F \subseteq K$.

Let $\theta = x + (p(x)) \in F[x]/(p(x)) = K$

Then,

$$p(\theta) = p\big(x + (p(x))\big) \overset{\text{proj. is hom.}}{=} p(x) + (p(x)) = 0 + (p(x)),$$

which is 0 in K.

Let $a(x) \in F[x]$. Since $F[x]$: Euc. dom.,

$$a(x) = q(x)\,p(x) + r(x), \quad \deg r < n.$$

so $\bar{a} = r + (p) \in K$, so K is spanned by $1, \theta, \dots, \theta^{n-1}$. On the other hand, if $1, \dots, \theta^{n-1}$ are linearly dep., then $\exists b_0, \dots, b_{n-1} \in F$ not all 0 s.t. $b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1} = 0 \in K$.

Thus,

$$b_0 + b_1 x + \dots + b_{n-1}x^{n-1} + (p(x)) = 0 + (p(x)) \text{ in } K,$$

so $b_0 + b_1 x + \dots + b_{n-1}x^{n-1}$ is a multiple of $p(x)$ in $F[x]$. But this is impossible since $\deg p = n > n-1$. $\square$

Remark: need p to be <u>irred.</u>, otherwise K is not a field