

Announcements

Midterm 1: Wednesday 2/19 7:00-8:30pm Sidney Lu 1043

- Covers roughly everything through Friday
(will be more precise)
- Will send policy email & practice problems (from DLF)
later this week

HW4 will be due Wed. 2/26 (will post later this week)

Field extensions (cont.)

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.

□

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 $[K:F] = n$.

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

and the composition of these maps is inj., so $F \subseteq K$.

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

Then, proj. is hom.

$$p(\theta) = p(x + (p(x))) \stackrel{\downarrow}{=} p(x) + (p(x)) = 0 + (p(x)),$$

which is 0 in K .

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

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

So $\bar{a}(x) = r(x) + (p) \in K$, 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 $\deg p = n > n-1$. □

Remark: need p to be irred., otherwise K is not a field

Trick to reduce polys. mod p :

$$p(x) = x^n + p_{n-1}x^{n-1} + \dots + p_1x + p_0$$

$$p(\theta) = 0, \text{ so}$$

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

$$\begin{aligned}\theta^{n+1} &= \theta \theta^n = -(p_{n-1}\theta^n + \dots + p_1\theta^2 + p_0\theta) \\ &= -p_{n-1}(-p_{n-1}\theta^{n-1} + \dots + p_1\theta + p_0) \\ &\quad + \dots + p_1\theta^2 + p_0\theta \quad \text{etc.}\end{aligned}$$

Example: $F = \mathbb{R}$, $p(x) = x^2 + 1$

$$K = \mathbb{R}[x] / (x^2 + 1) = \{a + b\theta \mid a, b \in \mathbb{R}\} \quad \begin{array}{l} \theta^2 = -1 \\ \text{since } \theta^2 + 1 = 0 \end{array}$$

$$(a + b\theta)(c + d\theta) = (ac - bd) + (ad + bc)\theta$$

$$\text{So } K \cong \mathbb{C}!$$

Two isoms.: $\theta \mapsto \pm i$


Many more examples in D&F (p. 515-516)

Let's relate our new construction w/ a more "intuitive" way of thinking about field ext's

Def : Let $F \subseteq K$, $\alpha, \beta, \dots \in K$.

$F(\alpha, \beta, \dots)$ is the smallest subfield of K containing F and α, β, \dots

Equivalently, $\Gamma(\alpha, \beta, \dots) =$ intersection of all subfields of K w/ this property

Simple ext'n: $E = F(a)$
 primitive elt.

Examples: nontriv.

a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \stackrel{\downarrow}{=} \mathbb{Q}(\sqrt{2} + \sqrt{3})$ is simple

b) $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \dots)$ is not simple

Thm: $p(x) \in F[x] : \text{irred.}$

Let K : extn field of F containing a root α of p .

Then, $F[x]/(p(x)) \cong F(\alpha) \subseteq K$

Pf: Consider the map given by $x + (p) \mapsto \alpha$ i.e.

$g(x) + (p(x)) \mapsto g(\alpha)$.

- Well defined: $g(\alpha) = 0$ if $g \in (p)$
- Ring homom.: check the axioms
- Injective: $\ker \varphi$ is an ideal, which for a field is either (0) or $F[x]/(p)$. Not the latter since $1 \mapsto 1$
- Surjective: image is a field containing F and α

□

Cor: Let $E = F(\alpha) \subseteq K$ w/ $[K:F] = n < \infty$. Then,

a) \exists irred. $p(x) \in F[x]$ s.t. $p(\alpha) = 0$.

b) $\deg p = n$

c) $E \cong F[x]/(p)$

d) E is indep. of the choice of root of p
i.e. if $p(\beta) = 0$, $F(\alpha) \cong F(\beta)$.

Pf: a) Since $[K:F] = n$, $1, \alpha, \dots, \alpha^n$ are linearly dep. i.e.

$$a_n \alpha^n + \dots + a_1 \alpha + a_0 = 0$$

Let $p(x)$ be an irred. factor of $a_n x^n + \dots + a_1 x + a_0$, chosen such that $p(\alpha) = 0$.

b) This follows from our first theorem today

c) Follows from previous theorem

d) Follows from c)

□

Extension Theorem: Let $\varphi: F \xrightarrow{\sim} F'$ be an isom. of fields. Let $p(x) \in F[x]$ be irred., and let $p'(x) \in F'[x]$ be the irred. poly obtained by applying φ to the coeffs. of p .

Let α be a root of p (in some extn of F)

Let β be a root of p' (in some extn of F')

Then \exists isom.

$$\sigma: F(\alpha) \xrightarrow{\sim} F'(\beta)$$

$$f \mapsto \varphi(f) \quad (\sigma|_F = \varphi)$$

$$\alpha \mapsto \beta$$

(Seems unintuitive now, but useful later)

$$\sigma: F(\alpha) \xrightarrow{\sim} F'(\beta)$$

$$\begin{array}{c} | \qquad \qquad | \end{array}$$

$$\varphi: F \xrightarrow{\sim} F'$$

Pf (skip in class): Let $\tilde{\varphi}$ be the isom.

$$\tilde{\varphi} : F[x] \xrightarrow{\sim} F'[x]$$

$$f \mapsto \varphi(f)$$

$$x \mapsto x$$

Then $\tilde{\varphi}$ maps $(p(x))$ to $(p'(x))$, so it induces an isom

$$F[x] / (p(x)) \xrightarrow{\sim} F'[x] / (p'(x))$$

$$f \mapsto \varphi(f) + (p')$$

$$x + (p) \mapsto x + (p')$$

Combining this w/ our previous isoms., σ is the map

$$F(\alpha) \xrightarrow{\sim} F[x] / (p(x)) \xrightarrow{\sim} F'[x] / (p'(x)) \xrightarrow{\sim} F'(\beta)$$

$$f \mapsto f + (p) \mapsto \varphi(f) + (p') \mapsto \varphi(f)$$

$$\alpha \mapsto x + (p) \mapsto x + (p') \mapsto \beta$$

□