Lecture 2: finite field extensions

Monday, January 23, 2017 4:34 PM

Some sources/references

- Jacobsen: Basic Alg I (II)
- Isaacs: Algebra, a graduate course

Def A Division ring is a ring (associative, unital) s.t. the nonzero elts form a group.

Def If F is a field, an F-algebra is a F-vectospace A w/ a ring structure s.t. $i: F \to A$, $i(x) = x \cdot 1_A$ is a ring hom

s.t. $i(F) \subset Z(A) = \{a \in A \mid ab = ba \ \forall b \in A\}$

Def If R is a commutative ring, an R-algebra is an R-module A w/ a ring structure s.t. $i: F \to A$, $i(x) = x \cdot 1_A$ is a ring hom

s.t. $i(F) \subset Z(A)$

Lemma: If A is a finite dimensional algebra over a field F and if $a \in A$ is a non-zerodivisor ($ab = 0 \Rightarrow b = 0$ and $ba = 0 \Rightarrow b = 0$ all b)

then a is invertible.

Pf: to find $x \in A$ s.t. $ax = 1$:

consider $A \longrightarrow A$
$x \longmapsto ax$ injective since a non zero div.

$\Rightarrow$ surjective $\Rightarrow$ $ax = 1$ some x .... □

Cor: a commutative, finite dimensional domain over a field is a field.

Def If A is a commutative F-algebra, and $a_1, \dots, a_m \in A$, then we define $F[a_1, \dots, a_m]$ to be the ring generated by $a_1, \dots, a_m$

$\cap$ subring containing or equals to all poly expressions

$$F[x_1, \dots, x_m] \xrightarrow{\varphi_{\vec{a}}} A \qquad F[a_1, \dots, a_m] = \operatorname{im}(\varphi_{\vec{a}})$$
$$x_i \longmapsto a_i$$

Def if E/F is a field extension, and $a_1, \dots, a_m \in E$ we define $F(a_1, \dots, a_m)$ to be the subfield gen. by $a_1, \dots, a_m$

If E/F is a field extension, $\alpha \in E$, can consider evaluation homomorphism

$$\varphi_\alpha : F[x] \longrightarrow E \text{ via}$$
$$x \longmapsto \alpha$$

If φ_α is injective, we say α is transcendental, otherwise α is called algebraic, and the unique monic generator

of ker φ_α is called the min. poly of α

$m_\alpha(x)$

Lemma TFAE for $\alpha \in E$ E/F field ext

1. α algebraic over F
2. $F[\alpha]$ is f.dim'l ov F (w/ dim = deg $(m_\alpha(x))$)
3. $F[\alpha] = F(\alpha)$

Pf: α alg $\Rightarrow$ im $\varphi_\alpha \simeq \frac{F[x]}{(m_\alpha(x))}$ = v.space of dim deg $(m_\alpha(x)) = d$ w/ basis $1, x, \dots, x^{d-1}$

$1 \Rightarrow 2$

$2 \Rightarrow 3$ Fdim'l domain is field.

$3 \Rightarrow 1$ (not $1 \Rightarrow$ not 3)

α not alg $\Rightarrow$ φ_α injective $\Rightarrow$ im $\varphi_\alpha \simeq F[x]$ not a field.

$\|$

$F[\alpha]$

Ref E/F is algebraic if $\alpha \in E$ algebraic for all $\alpha \in E$.

Cor finite field extensions are algebraic

Prop If F is a field, $H \subset F^*$ a finite subgroup, then H is cyclic

Lem If F is a field, $\alpha \in F$, $f \in F[x]$, then $f(\alpha) = 0 \iff (x-\alpha) | f$

Pf: $F[x] \xrightarrow{\varphi_\alpha} F$, $x \mapsto \alpha$ $\qquad f(\alpha)=0 \iff \varphi_\alpha(f) = f(\alpha) = 0$

$x-\alpha \in \ker \varphi_\alpha \Rightarrow \ldots$ □.

Pf of prop:

follows from prevs stuff you know that H cyclic

$\iff$ H has at most 1 cyclic subgp of order p each p.

($H = H_1 \times H_2 \times \cdots \times H_r \qquad |H_i| = n_i \qquad n_{i+1} \mid n_i$

$n_2 \mid n_1 \qquad n_2$)

elmts of order p are roots of $x^p - 1$ — distract!

if we have $\alpha_1, \ldots, \alpha_\ell$ of them, then

$x-\alpha_i$ divides x^p-1 all $i \Rightarrow \prod (x-\alpha_i) \mid x^p-1$

by degs $\Rightarrow \ell \le p$

if we have a elmts $\alpha \in E$ w/ $\alpha^p = 1$ then have at least p of them $\alpha \neq 1$

$\ldots$ □

Prop A finite field extension E/F is simple $\iff$ there are only finitely many intermediate subfields $F \subset K \subset E$.

Pf: Suppose $E = F(\alpha)$ some $\alpha \in E$, we'll show $\exists$ injection

$K \longrightarrow$ divisors of $m_{\alpha,F}$ in $E[x]$

given K, consider $m_{\alpha,K}$ in $K[x]$, note $m_{\alpha,K} \mid m_{\alpha,F}$

(by def $m_{\alpha,K}$ divides every poly f in $K[x]$ s.t. $f(\alpha)=0$)

thinking of $F[x] \subset K[x] \subset E[x]$

claim, can recover K from $m_{\alpha,K}$ (thought of as a factor of $m_{\alpha,F}$ in $E[x]$)

write $m_{\alpha,K} = \sum_{i=0}^{n} a_i x^i$ Let $L = F(a_0, \ldots)$

Claim: $L = K$ (note $L \subset K$)

Pf of claim: know $E = F(\alpha) = L(\alpha) = K(\alpha)$

further $[E:L] = [L(\alpha):L] = \deg m_{\alpha,L}$

$[E:K] = \deg m_{\alpha,K}$

know that every poly w/ coeffs in L s.t. $f(\alpha)=0$ is a mult. of $m_{\alpha,L} \Rightarrow m_{\alpha,L} \mid m_{\alpha,K}$

$\deg m_{\alpha,L} \leq \deg m_{\alpha,K}$

$[E:L] \leq [E:K]$

$[E:K] \mid [E:L] \Rightarrow [E:K] = [E:L]$

But $[E:L] = [E:K][K:L]$

$\Rightarrow [K:L] = 1 \Rightarrow K = L$.

E
$|$
K
$|$
L

Conversely: Suppose that there are only finitely many intermediate subfields

Case 1: F finite $\Rightarrow$ E finite $\Rightarrow$ $E\setminus\{0\} = E^*$ is cyclic

$\Rightarrow$ can choose $\alpha \in E$ generator of $E^* \Rightarrow F(\alpha) = E$

Case 2: F infinite, induction on $[E:F]$.

Choose $\alpha \in E \setminus F$, consider $E/F(\alpha)$ (if $E = F(\alpha)$ done)

by induction, since $[E:F(\alpha)] < [E:F]$ (tower law)

$\Rightarrow E = F(\alpha)(\beta) = F(\alpha,\beta)$

Consider for $t \in F$, $F(\alpha + t\beta)$. this is an infinite list of intermediate fields of E/F

$\Rightarrow \exists s \neq t$ in F w/ $F(\alpha + t\beta) = F(\alpha + s\beta) = L$

in this case, we have $\alpha + t\beta, \alpha + s\beta \in L \Rightarrow (t-s)\beta \in L$

$t \neq s$, $(t-s) \in F^* \Rightarrow \beta \in L \Rightarrow s\beta \in L$

$\alpha + s\beta \in L \Rightarrow \alpha \in L$

$\Rightarrow \alpha, \beta \in L \Rightarrow F(\alpha,\beta) \in L$ ⊥.

$\| E$