Lecture 4: Stuff about finite field extensions

Friday, February 3, 2017 2:28 PM

Alternate proof of the existence of algebraic closures

Axiom: all sets may be well-ordered

recall: a well ordering is a total order on a set s.t.

every subset has a minimal elmt. all elemts comparable, anti-sym., ...

$F_0 = F$ field, let $\mathcal{I}_F = \{$all irred poly's in $F[x]\}$, choose a well ordering.

I claim: can choose a collection of fields F_λ, $\lambda \in \mathcal{I}_F$

s.t. $F_{\lambda+1} = F_\lambda[x]/p_{\lambda+1}$ where $p_{\lambda+1}$ is some irred factor of $\lambda+1$ in $F_\lambda[x]$

or if $\lambda = \lim_{\mu<\lambda} \mu$ then $F_\lambda = \bigcup_{\mu<\lambda} F_\mu$

Set $F_1 = \bigcup_\lambda F_\lambda$

Inductively define $F_2 = (F_1)_1$, ... $\quad F_0 \subset F_1 \subset F_2 \subset \cdots$

$F_\infty = \bigcup F_i$

Asside on well ordered sets:

if Ω well ordered, $\lambda \in \Omega$, can consider $\{\mu \mid \mu < \lambda\}$

an either has a max'l element ν $(\lambda = \nu + 1)$

or not $(\lambda = \lim_{\mu<\lambda} \mu)$

Note. F_A is algebraic over F & alg. closed $\Rightarrow F_A$ is an algebraic closure.

Lem Algebraic closures are unique up to isom.

Pf: built from simple exts & $\frac{F[x]}{\min_{\alpha,F}} \simeq F(\alpha)$ $\square$

Gal Theory:

Def if E/F is any field ext. $G(E/F) = \mathrm{Gal}(E/F)$
$= \mathrm{Aut}(E)$ which fix F.

let $\mathcal{F}(E/F) = \{K \mid F \le K \subseteq E\}$

and $\mathcal{G}(E/F) = \{H \mid H < G = \mathrm{Gal}(E/F)\}$

$$\begin{tikzcd}
K \arrow[r, mapsto] & \{h \in G \mid h(x) = x \text{ all } x \in K\} = \mathrm{Gal}(E/K) \\
\mathcal{F} \arrow[r, bend left, "\mathrm{Gal}"] & \mathcal{G} \arrow[l, bend left, "\mathrm{Inv}"] \\
\{x \in E \mid h(x) = x \text{ all } h \in H\} = E^H & H \arrow[l, mapsto, bend left]
\end{tikzcd}$$

Satisfy following thms: $H \subseteq \mathrm{Gal}(E/E^H)$

$K \subseteq E^{\mathrm{Gal}(E/K)}$

$H_1 \subseteq H_2 \qquad E^{H_1} \supseteq E^{H_2}$

$K_1 \subseteq K_2 \qquad Gal(E/K_2) \subseteq Gal(E/K_1)$

$$\Longrightarrow \qquad H \subseteq Gal(E/E^H)$$

$$H \rightsquigarrow Gal(E/E^H) \longrightarrow Gal\left(E/E^{Gal(E/E^H)}\right)$$

$$ \overset{\shortparallel}{Gal(E/E^H)}$$

Follows that:

the compositons

$$H \longrightarrow Gal(E/E^H) \qquad \mathcal{G} \circlearrowleft$$

is idempotent (doing twice = doing once)

$$K \rightsquigarrow E^{Gal(E/K)} \qquad \mathcal{F} \circlearrowleft$$

<u>Define</u>: a subgp $H \in \mathcal{G}$ is "closed" if H is in image of this compositon.

a subfield $K \in \mathcal{F}$ closed if in image of comp.

It follows from (nothing) that there is a bijection between closed objects on either side

<u>Moreover</u>: all subgps are closed!

One formulation of Gal thy:

All subfields are closed $\Leftrightarrow$ F is closed.

$$F = E^{Gal(E/F)}$$

<u>Def</u>: E/F Galois if $F = E^{Gal(E/F)}$

Follows that if G is any group of Auts of E, then

E/E^G is Galois.

<u>Def</u> A field ext E/F is normal $\Leftrightarrow$ every irred poly w/ a root in E splits in E.

<u>Thm</u>: E/F finite ext is normal $\Leftrightarrow$
E/F is a splitting field for a polynomial $\Leftrightarrow$
whenever $F \subset E \subset K$ w/ $\sigma \in Gal(K/F)$, then
$\sigma(E) = E$.

<u>Pf</u>: E normal, choose $\alpha_1, \ldots, \alpha_n$ basis for E/F
$\prod \min_{\alpha_i}$

<u>Separability</u>

- we say $f \in F[x]$ has distinct roots if it has dist. roots in every field ext.

• we say that $f \in F[x]$ is separable if each irred factor of f has distinct roots.

ex: $F = \mathbb{F}_p(t)$ then $x^p - t$ is not separable

$$\frac{F[x]}{x^p - t} = F[\sqrt[p]{t}] = F(\sqrt[p]{t})$$ then poly factors as

$$x^p - (\sqrt[p]{t})^p = (x - \sqrt[p]{t})^p$$

Def E/F is separable if the min poly of every $\alpha \in E$ is separable.

Lem $E = F(\alpha)$ then E sep $\Leftrightarrow$ $\min_\alpha$ separable.

Remark: if $E = \frac{F[x]}{f} \simeq F(\alpha)$ w/ dist. roots.

$$\frac{E[x]}{f} = \frac{E[x]}{(x-\alpha)g}$$ if f separable $\Rightarrow x - \alpha \nmid g$

$$\simeq \frac{E[x]}{x-\alpha} \times \frac{E[x]}{g} \simeq E \times \frac{E[x]}{g}$$

E separable if $\frac{E[x]}{f}$ has "a factor of E" $(1,0) = e$

$$\frac{E[x]}{f} e \simeq E$$

Alternate formulation of sep:

$F[\alpha] = E/F$ separable if $\exists\, e \in E[x]/f = R$

$\frac{E[x]}{f} e \simeq E$

$\frac{F[x]}{f} = E/F$ separable if $\exists e \in E[x]/f$

s.t. $e^2 = e$ $\quad eR \simeq E$ via

$E \hookrightarrow \frac{E[x]}{f} \to eR$

$$\frac{E[x]}{f(x)} = E \otimes \frac{F[x]}{f(x)}$$

Tensor Interlude

Formally: given ring R, R-modules M, N

$M \otimes_R N$ = free ab gp gen by symbols $m \otimes n$ w/ $(m,n) \in M \times N$

rel's: $rm \otimes n = m \otimes rn$, $(m+m') \otimes n = m \otimes n + m' \otimes n$

$m \otimes (n+n') = m \otimes n + m \otimes n'$

has the structure of an R-mod via $r(m \otimes n) = rm \otimes n$

& extend by linearity

if $M = S$ a ring extension of R

$S \otimes N$ "N w/ coefficients extended to S"

$s \otimes n \quad s(1 \otimes n) = s \otimes n$

in particular: if V/F is a v.space, E/F field ext.

$E \otimes V$ has same basis (just w/ new coeffs)

$F[x]/f$ = vr space /F w/ basis $1, x, x^2, \dots, x^{d-1}$ $\quad d = \deg f.$

$$E \otimes F[x] = E[x] \qquad E \otimes \frac{F[x]}{f} = \frac{E[x]}{f}$$

$\alpha \otimes 1 \qquad 1 \otimes \alpha$

$E \otimes E$

$$\frac{E[x]}{f} \xrightarrow{\sim} \overset{E}{\frac{E[x]}{x-\alpha}} \times \frac{E[x]}{g} \longrightarrow \frac{E[x]}{x-\alpha} = E$$

$$E \otimes E \xrightarrow{\text{mult.}} E$$

$$\alpha \otimes 1 \longrightarrow \alpha$$

$$\underset{\text{"}x\text{"}}{1 \otimes \alpha} \longrightarrow \alpha$$

$$a \otimes b = (a \otimes 1)(1 \otimes b) \longrightarrow a \cdot b$$

<u>Alternate formulation</u>

E/F is separable $\iff \exists$ map $E \xrightarrow{\sigma} E \otimes E$

s.t. $E \otimes E \xrightarrow{\text{mult.}} E$, $\quad \mathrm{id}$, $\quad \sigma$

$$\sigma(ab) = (a \otimes 1)\sigma(b) = (1 \otimes a)\sigma(b)$$

"Pf" $\quad \underset{\frac{E[x]}{f}}{E \otimes E} \cong E \times \frac{E[x]}{g} \qquad \sigma : E \to E \otimes E$

inclusion of

f

$(a\otimes 1)\sigma(b)$ (in the world of $\frac{E[x]}{f} \simeq E \times \frac{E[x]}{g}$)

$a\otimes 1 \rightsquigarrow (a, a)$ $\qquad \sigma(b) = (b, 0)$

$1\otimes a \longrightarrow (a, ?)$

$(a\otimes 1)\sigma(b) = (1\otimes a)\sigma(b) = (ab, 0)$
$= \sigma(ab)$

element $e = (1,0)$ in $E\otimes E$ is called the "separability idempotent"

$\square$

Should also recall: $f \in F[x]$ has distinct roots $\Leftrightarrow$
$(x-\alpha)^2 \nmid f$ any field ext, any α,
$\Leftrightarrow$
f, f' have no common factors.

in particular if f is irred, and doesn't have dist roots
$\Rightarrow$ F is infinite w/ finite characteristic.

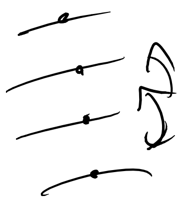
f irred, f', f have common factr. $\Rightarrow f' = 0$

$\Rightarrow$ all monomials in f look like $ax^{p^n m}$
& char $= p$

if F finite $\Rightarrow ax^{p^n m} = (ax^{p^{n-1} m})^p = f = g^p$
$\Rightarrow$ not irred.

Def F is imperfect if $\exists$ insep. extensions. E/F
finite

<u>Def</u> F is <u>imperfect</u> if ∃ insep. finite extensions. E/F



sep ext.

Gal(E/F)

insep ext.

Der(E/F)

<u>Thm</u> TFAE for E/F finite extension

i - E/F is Galois $\left(F = E^{Gal(E/F)} \right)$

ii - E/F is normal & separable

iii - E = spfield of a separable polynomial

consequence of ii: E/F Gal, $F \subset K \subset E \Rightarrow E/K$ Gal

$\Rightarrow K = E^{Gal(E/K)} \Rightarrow$ all subfields are "closed"

$\Rightarrow$ <u>Galois Correspondence</u>!

<u>Also</u>: follows that if E/F is finite Galois $\Rightarrow \exists$ finite # subfields.

moreover if K/F sep. finite, then going to normal closure $\Rightarrow$ Gal ext. $\Rightarrow$ finitely many subfields of finite sep. $\Rightarrow$ simple!

find E/K s.t. E/F normal

<u>Note</u>: if K/F finite ext, can find E/K s.t. E/F normal

via: $b_1, \ldots, b_n$ basis for K/F, then let m_i = min poly α_i

$f = \prod m_i$ E sp. field for E

$\bigcap$ normal = normal $\Rightarrow \exists$ sm. normal = normal closure.

<u>Consequently</u>: $|G| = [E:F] \Longleftarrow E/F$ Galois

since $E = F(\alpha) = \frac{F[x]}{f}$ f splits, roots of f permuted by G

they are permuted <u>transitively</u>

since all generate simple ext w/ same presentation

but action is determined by any one of roots

$\Rightarrow |G| = \deg f = [E:F]$.

How to construct field extensions w/ gp G for a given G?
(over some field F?)

If we don't fix F, easy: given $\overset{\text{finite}}{\vee}$ G, choose a $\overset{\text{finite}}{\vee}$ set X,

and a faithful action $G \circlearrowright X$ ($G \to Sym(X)$ is injective)

consider $F(x_1, \ldots, x_n)$ where $\{x_1, \ldots, x_n\} = X$

$G \curvearrowright$ Aut's of $F(x_1, \ldots, x_n)$

$F(x_1, \ldots, x_n) / F(x_1, \ldots, x_n)^G$ is G-Galois

Suppose we have a poly in $F(t)[x] \ni f_t(x)$

and $\dfrac{F(t)[x]}{f_t(x)}$ is a G-Galois extension of $F(t)$

we would like to get a G-Gal. ext of F by setting $t = a \in F$

more concretely, $f_t(x) = \displaystyle\sum_{i=0}^{d} \frac{a_i(t)}{b_i(t)} x^i$, want to find

$a \in F$ s.t.

$b_i(a) \neq 0$ and $f_a(x) = \sum \frac{a_i(a)}{b_i(a)} x^i$ is irred

and $\dfrac{F[x]}{f_a(x)}$ G-Galois.

<u>Def</u>: F is called <u>Hilbertian</u> if we can always find a as above for every $f_t(x)$ as above.

<u>Facts</u>: • Number fields (finite exts of $\mathbb{Q}$) are Hilbertian

• $F(s)$ is Hilbertian for any F

<u>Hilbertian</u>: $\forall f_t(x)$ irred $/F(t)$ w/ $\dfrac{F(t)[x]}{f_t(x)}$ G-Gal. $/F(t)$

Hilbertian: $\forall f_t(x)$ irred $/F(t)$ w/ $\frac{\quad}{f_t(x)}$

$\exists a \in F$ s.t. $\frac{F[x]}{f_a(x)}$ is G-Galois $/F$

$f_a(x)$ irred,

Example application: if F Hilbertian, C_2 is a Gal gp.

$\tilde{F} = F(t_1, t_2)$ $\quad \sigma : t_1 \leftrightarrows t_2$ $\quad \tilde{F}^{\sigma} = \tilde{F}^{\{1,\sigma\}}$

know: $\tilde{F}/\tilde{F}^{\sigma}$ is C_2-Galois $\Rightarrow [\tilde{F} : \tilde{F}^{\sigma}] = 2$

what's in $\tilde{F}^{\sigma}$? $\quad t_1 + t_2,\ t_1 t_2$

let $K = F(t_1 + t_2, t_1 t_2)$

$$\tilde{F} \overset{2}{\supset} \tilde{F}^{\sigma} \overset{1}{\supset} K, \qquad [\tilde{F}:K] = 2$$

$K(t_1) = \tilde{F}$ and t_1 satisfies the poly

$$x^2 - (t_1 + t_2)x + t_1 t_2$$

$$t_1^2 - (t_1 + t_2)t_1 + t_1 t_2$$
$$= t_1^2 - t_1^2 - t_1 t_2 + t_1 t_2 = 0.$$

Set $s_1 = t_1 + t_2$ $\quad s_2 = t_1 t_2$

Claim: $K = F(s_1, s_2)$ is isom to rat'l fcns in 2-variables.

follows from notion of tr. degree:

$F(s_1)$ is either finite sep or transc $/F$

$F(s_1, s_2)$: $\quad$ — $/F(s_1$

$\quad$ trdeg $F(s_1, s_2) =$ trdeg $F(t_1, t_2) = 2 \Rightarrow$ both but trag ... transcendental

$\Rightarrow$ $\tilde{F}/K = F(s_1,s_2)$ $\tilde{F} = \frac{K[x]}{f_{s_1,s_2}}$ C_2 - Galois

$= F(s_1)(s_2)$

specialize to get C_2 Gal/F.

$$f_{s_1,s_2}(x) = x^2 - s_1 x + s_2$$

Similarly: S_n

$\tilde{F} = F(x_1, \ldots, x_n) \circlearrowleft S_n$ $\tilde{F}^{S_n}$

$K = F^{(S)}$ $s_1 = \sum x_i$ $s_2 = \sum_{i<j} x_i x_j$ $s_3 = \sum_{i<j<k} x_i x_j x_k \ldots$

$\sum (-1)^{n-i} s_i x^i$ then x_1 root, $\tilde{F} = K(x_1)$
