Lecture 28: Galois and normal closure

Wednesday, March 7, 2018 10:50 AM

The following is a corollary of Fundamental theorem of Galois theory.

<u>Corollary</u>. Suppose E/F is a finite separable extension. Then there are only finitely many intermediate fields $F \subseteq K \subseteq E$.

<u>Pf.</u> Suppose $E = \sum_{i=1}^{n} F\alpha_i$. And let E' be a splitting field of $\prod m_{\alpha_i,F}(x)$ over F. Then E'/F is a finite Galois extension. (Since E/F is separable, $\prod m_{\alpha_i,F}(x)$ is a separable polynomial.) Hence by the fundamental theorem of Galois theory there are only finitely many intermediate fields $F \subseteq L \subseteq E'$. Since $E \subseteq E'$, claim follows. ∎

• <u>Remark</u>. Let $F \subseteq E \subset \overline{F}$; let $E' \subseteq \overline{F}$ be a splitting field of $\{m_{\alpha,F}\}_{\alpha\in E}$. Then $E' \supseteq E$, E'/F is normal, and E' is the smallest subfield of $\overline{F}$ with these properties. That is why E' is called <u>the normal closure of E</u>.

• In the above argument we showed, if E/F is a finite separable extension, then E'/F is Galois where E' is a normal closure of E over F. this is true for infinite separable closures as well.

Lecture 28: Simple extensions

Sunday, March 4, 2018 11:29 PM

Theorem. Suppose E/F is a finite field extension. Then there are only finitely many intermediate fields $F \subseteq K \subseteq E$ if and only if $\exists\, \theta \in E$ s.t. $E = F[\theta]$

(in this case θ is called a primitive element, and E/F is called a simple extension.)

Corollary. If E/F is a finite separable extension, then $E = F[\theta]$ for some $\theta \in E$.

Pf. It is an immediate consequence of the previous theorem and corollary. ■

Pf of theorem. ($\Leftarrow$) If $|F| < \infty$, then $|E| < \infty$; and so $E^{\times} = \langle \theta \rangle$, which implies $E = F[\theta]$. Now suppose $|F| = \infty$. Since $E = F[\alpha_1, \ldots, \alpha_m]$, it is enough to show: for any $\alpha, \beta \in E$, $F[\alpha, \beta]/F$ is a simple extension. Since there are only finitely many intermediate subfields and $|F| = \infty$, $\exists\, c \neq c' \in F$ s.t. $F[\alpha + c\beta] = F[\alpha + c'\beta]$. Hence $F[\alpha + c\beta] \ni (\alpha + c\beta) - (\alpha + c'\beta) = (c - c')\beta$; and so $\beta, \alpha \in F[\alpha + c\beta]$.

Lecture 28: Simple extensions

Sunday, March 4, 2018 11:45 PM

And so $F[\alpha,\beta]\subseteq F[\alpha+c\beta]$. As $c\in F$, we get $F[\alpha,\beta]=F[\alpha+c\beta]$.

($\Leftarrow$) Suppose $E=F[\theta]$ and $F\subseteq K\subseteq E$. Then $m_{\theta,K}(x)\mid m_{\theta,F}(x)$.

So there are only finitely many possiblity for the polynomial

$g(x):=m_{\theta,K}(x)\in E[x]$.

Let K' be the field generated by F and coeff. of $g(x)$. Hence

$F\subseteq K'\subseteq K$, $g(x)\in K'[x]$ is irreducible, and $g(\theta)=0$. Therefore

$m_{K',\theta}(x)=g(x)$; this implies $[E:K']=[K'[\theta]:K']=\deg g$

$$=[K[\theta]:K]=[E:K].$$

and so $K=K'$. Therefore, there are only finitely many possiblities for K. ■

So now we have extra motivation to study separability condition. Since any algebraic extension E/F can be realized as a subfield of an algebraic closure $\overline{F}$ of F, when $\overline{F}/F$ is separable, all algebraic extensions are going to be separable. So next we will find exactly when $\overline{F}/F$ is a separable (and so Galois) extension.

Lecture 28: Separability condition

Monday, March 5, 2018 12:04 AM

Recall that we have seen that the minimal polynomial of $t^{1/p}$ over $\mathbb{F}_p(t)$ is $x^p - t$, and it is NOT separable. So $\overline{\mathbb{F}_p(t)}/\mathbb{F}_p(t)$ is NOT separable.

$\overline{F}/F$ is not separable $\Leftrightarrow$ $\exists\, \alpha \in \overline{F}$ s.t. $m_{\alpha,F}(x)$ has multiple roots in $\overline{F}$.

So we need to study the possibility of an irreducible polynomial $p(x) \in F[x]$ having multiple roots.

<u>Lemma</u>. (1) zeros of $f(x)$ in $\overline{F}$ are distinct $\Leftrightarrow$ $\gcd(f, f') = 1$.

(2) Suppose $f(x) \in F[x]$ is irreducible. Then $f(x) = g(x^{p^n})$ such that $g(x) \in F[x]$ is an <u>irreducible</u> <u>separable</u> polynomial.

<u>Pf.</u> We have already mentioned that because of the uniqueness of quotient and remainder we have:
$$\left.\begin{array}{l} E/F \text{ field extension} \\ p_1(x), p_2(x) \in F[x] \end{array}\right\} \Rightarrow \underset{\text{in } E[x]}{p_1(x) \mid p_2(x)} \Leftrightarrow \underset{\text{in } F[x]}{p_1(x) \mid p_2(x)}$$
and so
$$\left.\begin{array}{l} E/F \text{ field extension} \\ h_1(x), h_2(x) \in F[x] \end{array}\right\} \Rightarrow \underset{\text{in } E[x]}{\gcd(h_1(x), h_2(x))} = \underset{\text{in } F[x]}{\gcd(h_1(x), h_2(x))}.$$

In $\overline{F}[x]$, $f(x) = \prod_{i=1}^{m} (x - \alpha_i)^{n_i}$ where $\alpha_i \neq \alpha_j$. Then

Lecture 28: Separability condition

Thursday, March 8, 2018 10:43 PM

$$f'(x) = \prod_{i=1}^{m} (x-\alpha_i)^{n_i-1} \underbrace{\left(\sum_{i=1}^{m} n_i \prod_{\substack{j=1 \\ j\neq i}}^{m} (x-\alpha_j) \right)}_{p(x)}$$

Notice $p(\alpha_i) = n_i \prod_{\substack{j=1 \\ j\neq i}}^{m} (\alpha_i-\alpha_j) \neq 0$. Hence $(x-\alpha_i) \nmid p(x)$.

Therefore $\gcd(f(x), p(x)) = 1$; this implies

$$\gcd(f(x), f'(x)) = \prod_{i=1}^{m} (x-\alpha_i)^{n_i-1}.$$

Hence $\gcd(f(x), f'(x)) = 1 \iff f$ has no multiple zeros.

(2) If $f(x)$ is separable, there is nothing to prove. If not, $\gcd(f(x), f'(x)) \neq 1$. As $f(x)$ is irreducible and $\deg f' < \deg f$, we deduce that $f' = 0$. Suppose $f(x) = \sum_{i=0}^{n} a_i x^i$. So

$f'(x) = \sum_{i=0}^{n} i\, a_i x^{i-1} = 0$ implies $i a_i = 0$ for $0 \le i \le n$. $\circledast$

- If $\mathrm{char}(F) = 0$, then $a_1 = \cdots = a_n = 0$; this implies $f(x)$ is a unit, which is a contradiction. For $\mathrm{char}(F) = p > 0$, we proceed by induction on $\deg f$. By $\circledast$, either $p \mid i$ or $a_i = 0$. Hence

$f(x) = \sum a_{pi} x^{pi} = g_1(x^p)$, for some $g_1(x) \in F[x]$.

<u>Claim</u>. $g_1(x)$ is irreducible in $F[x]$.

Lecture 28: When is algebraic closure Galois?

Thursday, March 8, 2018 10:58 PM

Pf of claim. If not, $g_1(x)=p(x)h(x)$, and $\deg p, \deg h \geq 1$.

$\Rightarrow f(x)=g_1(x^p)=p(x^p)h(x^p)$ which contradicts irreducib. of f.

Therefore by the induction hypothesis, $g_1(x)=g(x^{p^k})$ for some irreducible separable polynomial $g(x)\in F[x]$. Therefore $f(x)=g_1(x^p)=g(x^{p^{k+1}})$; and claim follows. ∎

Theorem. The following are equivalent.

(a) Either $\mathrm{char}(F)=0$, or $\mathrm{char}(F)=p>0$ and $F^p=F$.

(b) $\overline{F}/F$ is Galois.

(c) Any algebraic extension E/F is separable.

Pf. (a) $\Rightarrow$ (b) Since $\overline{F}/F$ is normal, it is enough to show $\overline{F}/F$ is separable. Let $\alpha\in\overline{F}$. Then $\exists g_\alpha(x)\in F[x]$: separable and irreducible such that $m_{\alpha,F}(x)=g_\alpha(x^{p^k})$ (If char $F=0$, then any poly. is separable.)

Suppose $g_\alpha(x)=\sum_{i=0}^m a_i x^i$. Since $F^p=F$, by induction $F^{p^k}=F$.

Hence $a_i=b_i^{p^k}$ for some $b_i\in F$. Thus $g_\alpha(x^{p^k})=\left(\sum_{i=0}^m b_i x^i\right)^{p^k}=m_{\alpha,F}(x)$.

Lecture 28: Perfect fields

Thursday, March 8, 2018 11:14 PM

Since $m_{\alpha,F}(x)$ is irred. in $F[x]$, we deduce that $p^k=1$. And so $m_{\alpha,F}(x)=g(x)$ is separable.

(b) $\Rightarrow$ (c) $\exists\, \sigma: E \hookrightarrow \overline{F}$ s.t. $\sigma|_F = \mathrm{id}_F$. Since $\overline{F}/F$ is separable, E/F is separable.

(c) $\Rightarrow$ (a) For $c\in F$, let E be the splitting field of x^p-c and $\alpha\in E$ be a zero of x^p-c. Then $c=\alpha^p$; and so $x^p-c=(x-\alpha)^p$. Hence $m_{\alpha,F}(x) \mid (x-\alpha)^p$. As E/F is separable, $m_{\alpha,F}(x)$ does not have multiple zeros. Hence $m_{\alpha,F}(x)=x-\alpha$; this implies $\alpha\in F \Rightarrow c\in F^p$. (If char $F=0$, then there is nothing to prove.) ∎

<u>Def</u> We say F is a perfect field if $\overline{F}/F$ is Galois.

<u>Corollary</u>. Suppose F is a perfect field, and E/F is a finite extension. Then $\exists\, \theta\in E$, $E=F[\theta]$.