Lecture 22: Algebraic elements

Tuesday, February 27, 2018 8:38 AM

<u>Def.</u> Let E/F be a field extension. $\alpha \in E$ is called algebraic over F if α is a zero of a polynomial $f(x) \in F[x] \setminus \{0\}$. Otherwise α is called transcendental over F.

<u>Theorem.</u> Suppose E/F is a field extension, and $\alpha \in E$ is algebraic over F. Then

(1) $\exists$ a monic polynomial $m_\alpha(x) \in F[x]$ such that for $f(x) \in F[x]$,

$$f(\alpha) = 0 \iff m_\alpha(x) \mid f(x).$$

(2) $m_\alpha(x)$ is irreducible in $F[x]$.

(3) $F[x]/\langle m_\alpha(x) \rangle \simeq F[\alpha] := \{\sum_{i=0}^{m} a_i \alpha^i \mid a_i \in F\}$; and $F[\alpha]$ is a field.

(4) $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is an F-basis of $F[\alpha]$ where $d = \deg m_\alpha$; and so

$$\dim_F F[\alpha] = \deg m_\alpha.$$

Before we get to proof of the above theorem, let's point out that if E/F is a field extension, then E can be viewed as an F-vector space. The dimension $\dim_F E$ of E as an F-vector space is denoted by $[E:F]$, and sometimes called the degree of the field extension E/F.

Lecture 22: Algebraic elements; minimal polynomials

Monday, February 26, 2018 12:09 AM

Pf. Let $\phi_\alpha : F[x] \to E$ be the evaluation at α. We have seen that ϕ_α is a ring homomorphism. And so $F[x]/\ker\phi_\alpha \simeq \operatorname{Im}\phi_\alpha$.

Since $F[x]$ is a PID and $\ker\phi_\alpha \neq 0$ (α is algebraic), $\exists!$ monic polynomial such that $\ker\phi_\alpha = \langle m_\alpha(x)\rangle$.

And so $p(\alpha) = 0 \Leftrightarrow p(x) \in \ker\phi_\alpha \Leftrightarrow m_\alpha(x) \mid p(x)$.

. $\operatorname{Im}\phi_\alpha = F[\alpha] \hookrightarrow E$; and so it is an integral domain. Hence $\langle m_\alpha(x)\rangle \in \operatorname{Spec}(F[x]) \setminus \{0\}$. Since $F[x]$ is a PID, we deduce that $\langle m_\alpha(x)\rangle$ is a maximal ideal. Therefore $m_\alpha(x)$ is irreducible in $F[x]$ and $F[x]/\langle m_\alpha(x)\rangle \simeq F[\alpha]$ is a field.

For any $p(x) \in F[x]$, let $q(x)$ and $r(x)$ be the quotient and remainder of $p(x)$ divided by $m_\alpha(x)$. So we have

$p(\alpha) = q(\alpha)\, m_\alpha(\alpha) + r(\alpha) = r(\alpha)$ and $\deg r < \deg m_\alpha$. This implies

$F[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{d_0-1}\alpha^{d_0-1} \mid a_i \in F\}$; and so $F[\alpha]$ is the F-span of $1, \alpha, \ldots, \alpha^{d_0-1}$ and $\dim_F F[\alpha] \leq \deg m_\alpha$.

Claim. $1, \alpha, \ldots, \alpha^{d_0-1}$ are linearly indep. over F.

Lecture 22: Minimal polynomial

Monday, February 26, 2018 8:10 AM

<u>Pf of claim.</u> If not, $c_0 + c_1\alpha + \cdots + c_{d_0-1}\alpha^{d_0-1} = 0$ for some $(c_0, \ldots, c_{d_0-1}) \in F^{d_0} \setminus \{\vec{0}\}$. Hence $p(\alpha) = 0$ where $p(x) = \sum_{i=0}^{d_0-1} c_i x^i$; this implies $m_\alpha(x) \mid p(x)$. From this we deduce either $p = 0$ or $\deg m_\alpha \le \deg p$, which is a contradiction. ■

<u>Def.</u> $m_\alpha(x) \in F[x]$ in the previous theorem is called the minimal polynomial of α over F.

<u>Observation.</u> Suppose E/F is a field extension, and $\alpha \in E$ is algebraic over F. If $p(x) \in F[x]$ is irreducible and $p(\alpha) = 0$, then $p(x) = c\, m_\alpha(x)$ for some $c \in F^\times$.

<u>Pf.</u> $m_\alpha(x) \mid p(x)$ and $p(x)$ is irreducible $\Rightarrow p(x) = c\, m_\alpha(x)$ for some $c \in F^\times$. ■

<u>Proposition.</u> Let F be a field and suppose $p(x) \in F[x]$ is irreducible. Then $\exists$ a field extension E of F and $\alpha \in E$ such that

(1) $m_\alpha(x) = c\, p(x)$, (2) $E = F[\alpha]$.

<u>Pf.</u> Since $p(x)$ is irreducible, $\langle p(x) \rangle$ is a maximal ideal of $F[x]$. Hence $E := F[x]/\langle p(x) \rangle$ is a field. Since $F \cap \langle p(x) \rangle = 0$, $F \hookrightarrow E$. Let $\alpha := x + \langle p(x) \rangle \in E$. Then $p(\alpha) = 0$ and

Lecture 22: Towards splitting field

Monday, February 26, 2018 8:26 AM

$f(\alpha)=0 \iff f(x)\in\langle p(x)\rangle$. Therefore if the leading coeff. of p is c, then $m_\alpha(x)=c\,p(x)$. And clearly we have $E=F[\alpha]$. ∎

We can continue this process and get a field $E=F[\alpha_1,\dots,\alpha_d]$ such that $p(x)=(x-\alpha_1)\cdots(x-\alpha_d)$. Next we will show that this field is essentially unique.

<u>Lemma.</u> Suppose $\phi: F\to F'$ is an isomorphism. Then

(1) ϕ can be extended to an isomorphism $\phi: F[x]\to F'[x]$,

$$\phi\Big(\sum_{i=0}^{n} a_i\cdot x^i\Big)=\sum_{i=0}^{n}\phi(a_i)\,x^i.$$

(2) Let $p(x)$ be an irred. polynomial in $F[x]$. Then $\phi(p(x))$ is irreducible in $F'[x]$.

(3) Suppose E/F and E'/F' are field extensions, $\alpha\in E$ is a zero of $p(x)$, and $\alpha'\in E'$ is a zero of $\phi(p(x))$. Then

$\exists!\ \widetilde{\phi}: F[\alpha]\xrightarrow{\sim}F'[\alpha']$ s.t. (1) $\widetilde{\phi}|_F=\phi$

$$\begin{tikzcd} F[\alpha] \arrow[r, "\sim"] & F'[\alpha'] \\ F \arrow[u, hook] \arrow[r, "\sim", "\phi"'] \arrow[ur, phantom, "\circlearrowright"] & F' \arrow[u, hook] \end{tikzcd}$$

(2) $\widetilde{\phi}(\alpha)=\alpha'$

Lecture 22: Towards splitting field

Monday, February 26, 2018 8:37 AM

Pf. Parts (1) and (2) are clear. Based on the first two parts

we get that $F[x]/\langle p(x)\rangle$ and $F'[x]/\langle \phi(p(x))\rangle$

are isomorphic fields. Using evaluation maps we get that

$$\begin{tikzcd}
x+\langle p(x)\rangle \arrow[rr, mapsto] & & x+\langle \phi(p(x))\rangle \\
F[x]/\langle p(x)\rangle \arrow[r, "\sim", "\phi"'] \arrow[d, "\wr"] & F'[x]/\langle \phi(p(x))\rangle \arrow[d, "\wr"] & \\
F[\alpha] \arrow[r, "\sim"] & F'[\alpha'] & \\
\alpha \arrow[rr, mapsto] & & \alpha'
\end{tikzcd}$$

clearly onto;

A field does not have non-trivial ideal. And so any non-zero homomorphism is an injection.

And clearly the restriction to F is ϕ. ■

Def. Let $f(x) \in F[x]$. A field extension E/F is called the splitting field of f if ① f can be written as a product of degree 1 polynomials in $E[x]$, ② If $F \subseteq E' \subsetneq E$, then f cannot be written as a product of degree 1 polynomials in $E'[x]$.

This is equivalent to say $\exists\, \alpha_1, \ldots, \alpha_n \in E$ s.t.

(1) $f(x) = c\,(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ (2) $E = \underbrace{F(\alpha_1, \ldots, \alpha_n)}$

subfield generated by F and $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Lecture 22: Existence of Splitting fields

Tuesday, February 27, 2018 9:54 AM

<u>Lemma</u>. Let $f(x) \in F[x] \setminus F$. Then there is a splitting field of $f(x)$ over F.

<u>Pf</u>. We proceed by induction on $\deg f$.

Let $p(x)$ be an irreducible factor of $f(x)$. Then by a propo. $\exists$ a field extension $E_1 = F[\alpha_1]$ such that $p(\alpha_1) = 0$; and so $f(x) = (x-\alpha_1) f_1(x)$ for some $f_1(x) \in E_1[x]$ and $\deg f_1 = \deg f - 1$.

By the induction hypothesis f_1 has a splitting field E over E_1.

And so $\exists\, \alpha_2, \ldots, \alpha_n \in E$ s.t. (1) $f_1(x) = c(x-\alpha_2)(x-\alpha_3) \cdots (x-\alpha_n)$

(2) $E = E_1(\alpha_2, \ldots, \alpha_n)$.

And so $f(x) = c(x-\alpha_1)(x-\alpha_2) \cdots (x-\alpha_n)$ and

$$E = F(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

So E is the splitting field of $f(x)$ over F. ∎

<u>Theorem.</u> Suppose $\phi: F \xrightarrow{\sim} F'$ is an isomorphism of fields F and F'. We extend ϕ to an isomorphism $\phi: F[x] \xrightarrow{\sim} F'[x]$.

Let $f(x) \in F[x] \setminus F$. Suppose E is a splitting field of $f(x)$ over

Lecture 22: Uniqueness of splitting field

Tuesday, February 27, 2018 10:17 AM

F and E' is a splitting field of $\phi(f(x))$ over F'. Then there is an isomorphism $\tilde{\Phi}: E \xrightarrow{\sim} E'$ such that $\tilde{\Phi}|_F = \phi$.

$$\begin{tikzcd} E \arrow[r, "\tilde{\Phi}", "\sim"'] & E' \\ F \arrow[u, hook] \arrow[r, "\phi", "\sim"'] \arrow[ur, phantom, "?"] & F' \arrow[u, hook] \end{tikzcd}$$

<u>Pf.</u> We proceed by induction on degree of f. If all the irreducible factors of f are of degree 1, then $f(x) = c\prod(x-\alpha_i)$ for $c, \alpha_i \in F$. And so $\phi(f(x)) = \phi(c)\prod(x-\phi(\alpha_i))$. Hence $E=F$ and $E' = F'$. And $\tilde{\Phi} = \phi$ works.

Suppose $p(x)$ is an irreducible factor of $f(x)$ and $\deg p \geq 2$. Then $\phi(p(x))$ is an irreducible factor of $\phi(f(x))$. Since E is an splitting field of $f(x)$ over F and $p(x) \mid f(x)$, $\exists \alpha_1 \in E$ s.t. $p(\alpha_1) = 0$. Similarly $\exists \alpha_1' \in E'$ s.t. $\phi(p)(\alpha_1') = 0$. So by a lemma proved earlier, $\exists \phi_1 : F[\alpha_1] \xrightarrow{\sim} F'[\alpha_1']$, $\phi_1|_F = \phi$, $\phi_1(\alpha_1) = \alpha_1'$.

And so $f(x) = (x-\alpha_1)f_1(x)$ and

$$\begin{tikzcd} F[\alpha_1] \arrow[r, "\sim", "\phi_1"'] & F'[\alpha_1'] \\ F \arrow[u, hook] \arrow[r, "\sim"] & F' \arrow[u, hook] \end{tikzcd}$$

$$\begin{aligned} \phi(f(x)) &= \phi_1(f(x)) = \phi_1(x-\alpha_1)\,\phi_1(f_1)(x) \\ &= (x-\alpha_1')\,\phi_1(f_1)(x) \end{aligned}$$

Lecture 22: Uniqueness of splitting field

Tuesday, February 27, 2018 10:39 AM

Claim. E is the splitting field of $f_1(x)$ over $F[\alpha_1]$.

Pf. $\exists\, \alpha_2, \dots, \alpha_n \in E$, $f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$

and $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

And so $f_1(x) = c(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n)$ and

$E = F(\alpha_1)(\alpha_2, \dots, \alpha_n) = \big(F[\alpha_1]\big)(\alpha_2, \dots, \alpha_n)$. ✓

Claim. E' is the splitting field of $\phi(f_1)(x)$ over $F[\alpha_1']$.

Pf. is similar to the previous claim $+\ \phi(f) = (x-\alpha_1')\,\phi(f_1)$.

So by the induction hypothesis, $\exists\, \widetilde{\Phi}: E \xrightarrow{\sim} E'$ s.t.

$$\begin{tikzcd}
E \arrow[r, "\sim", "\widetilde{\Phi}"'] & E' \\
F[\alpha_1] \arrow[u, hook] \arrow[r, "\sim", "\phi_1"'] \arrow[ur, phantom, "\circlearrowleft"] & F'[\alpha_1'] \arrow[u, hook] \\
F \arrow[u, hook] \arrow[uu, bend left, hook] \arrow[r, "\sim", "\phi"'] \arrow[ur, phantom, "\circlearrowleft"] & F' \arrow[u, hook] \arrow[uu, bend right, hook]
\end{tikzcd}$$

And the claim follows. ∎

Corollary. If E and E' are two splitting fields of $f(x)$ over F,

then $\exists\, \Phi: E \xrightarrow{\sim} E'$ s.t.

$\Phi|_F = id_F$.

$$\begin{tikzcd}
E \arrow[rr, "\sim"] & & E' \\
& F \arrow[ul, hook] \arrow[ur, hook] \arrow[u, phantom, "\circlearrowleft"] &
\end{tikzcd}$$