date: thursday, march 28, 2024

Algebraic Closure and Splitting Fields

I. Algebraic Closure

Given a polynomial $p(x) \in F[x]$, can find an extension E of F such that E has a root of $p(x)$. Is there a field extension E' of F that contains all the roots of $p(x)$?

Theorem: Let E be an extension of F. Consider the set

$$E' = \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$$

Then E' is an extension of F (ie. E' is a subfield of E)

Proof

Given $\alpha, \beta \in E'$, need to show $\alpha \pm \beta$, $\alpha\beta$, α/β $(\beta \neq 0)$ all belong to E'. Both α, β are algebraic over F, so $F(\alpha, \beta)$ is a finite extension of F. But $\alpha \pm \beta$, $\alpha\beta$, $\alpha/\beta \in F(\alpha,\beta)$. So all these elements are algebraic over F. So they belong to E'.

$\square$

Def^n: Let E be an extension of F. Then the algebraic closure of F in E is the field E'.

Def^n: A field F is algebraically closed if every nonconstant polynomial $p(x) \in F[x]$ has a root.

eg. (nonexample) $\mathbb{R}$ is not algebraically closed since x^2+1 has no root.

Theorem: F is algebraically closed iff every nonconstant polynomial $p(x) \in F[x]$ factors into linear polynomials.

Proof

"=>" Let $p(x)$ be a nonconstant polynomial. Because F is algebraically closed, $p(x)$ has a root α. So $p(x)=(x-\alpha)q(x)$ with $\deg q(x) < \deg p(x)$. Repeat with $q(x)$. This has a root α_2 so $q(x)=(x-\alpha_2)q'(x)$. Repeat to end with $p(x)=(x-\alpha_1)(x-\alpha_2)\ldots$

"<=" Let $p(x)\in F[x]$. We know $p(x)=c(x-\alpha_1)\cdots(x-\alpha_n)$ with $c,\alpha_1,\ldots,\alpha_n\in F$. But then $\alpha_i\in F$ is a root of $p(x)$.

□

Corollary: If F is algebraically closed, there is no proper algebraic extension.

Proof

Suppose E is an algebraic extension of F (so $F\subseteq E$). Let $\alpha\in E$ and let $p(x)\in F[x]$ be its minimal polynomial. But F algebraically closed imples $p(x)$ factors into linear factors in $F[x]$. Also $p(x)$ is irreducible. This forces $p(x)=c(x-\alpha)$. So $\alpha\in F$. Thus, $E\subset F\subset E$.

□

Theorem: Every field has a unique (up to isomorphism) algebraic closure.

Proof

Needs axiom of choice (if you believe in it lol)

Theorem: (Fundamental Theorem of Algebra)
The field $\mathbb{C}$ is algebraically closed iff polynomial $p(x)\in\mathbb{C}[x]$ can be factored into linear factors.

Splitting Fields

Given a specific $p(x)\in F[x]$, we want a field that contains all the roots of $p(x)$ (in fact, smallest).

eg. Want a field with all the roots of $x^4-2x^2-3\in\mathbb{Q}[x]$.
$$x^4-2x^2-3=(x^2-3)(x^2+1)=(x+\sqrt{3})(x-\sqrt{3})(x-i)(x+i)$$

The field $\mathbb{Q}(\sqrt{3}, i)$ will work.

Def$^{\underline{n}}$: An extension E is a splitting field of $p(x)$ if exists $\alpha_1, \dots, \alpha_n \in E$ such that $E = F(\alpha_1, \dots, \alpha_n)$ and $p(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$. A polynomial $p(x) \in F[x]$ splits in E if it is a product of linear factors in $E[x]$.

eg. $p(x) = x^3 - 5 \in \mathbb{Q}[x]$

This has a root $\sqrt[3]{5}$ in $\mathbb{Q}(\sqrt[3]{5})$ but this is not a splitting field since it has two other complex roots.

$$(x^3-5) = (x - \sqrt[3]{5})\underbrace{(x^2 + \sqrt[3]{5}x + (\sqrt[3]{5})^2)}_{\substack{\text{has complex roots since} \\ b^2-4ac = (\sqrt[3]{5})^2 - 4(\sqrt[3]{5})^2 < 0}}$$

Theorem: Let $p(x) \in F[x]$ be a nonconstant polynomial. Then a splitting field of $p(x)$ exists.

Proof

Do induction on $\deg p(x)$. If $\deg p(x) = 1$, then $p(x) = c(x-\alpha)$ with $\alpha \in F$ so F is the splitting field. Assume true for all $q(x)$ with $\deg q(x) < n$. Let $\deg p(x) = n$. If $p(x)$ is not irreducible, $p(x) = p_1(x) \cdots p_r(x)$ each irreducible and $\deg p_i(x) < n$. By induction, there is a field $E_i = F(\alpha_{i_1}, \dots, \alpha_{i s_i})$ that is a splitting field for $p_i(x)$. But then $E = F(\alpha_{11}, \dots, \alpha_{1s_1}, \alpha_{21}, \dots, \alpha_{2s_2}, \dots)$ is the splitting field of $p(x)$.

If $p(x)$ is irreducible, there is a field K such that $p(x)$ has a root $\alpha \in K$. So $p(x) = (x-\alpha)q(x)$ with $q(x) \in K[x]$ and degree $q(x) < n$.

In fact, $K = F(\alpha)$. By induction, there is a splitting field $K(\alpha_2, \dots, \alpha_n)$ for $q(x)$. But $K(\alpha_2, \dots, \alpha_n) = F(\alpha)(\alpha_2, \dots, \alpha_n) = F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

$\square$

Theorem: Splitting field of $p(x) \in F[x]$ is unique up to isomorphism.

eg. $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}(-\sqrt{2})$

Theorem: Suppose E is the splitting for $p(x) \in F[x]$. If $\deg p(x) = n$, then

$$[E:F] \leq n.$$