date: monday, march 25, 2024

Algebraic Extensions

Assumption: E is an extension of the field F, ie. $E \supseteq F$, E a field

Def^n: $\alpha \in E$ is algebraic over F if there exists $p(x) \in F[x]$ such that $p(\alpha) = 0$.

eg. $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since $\sqrt{2}$ is a root of $x^2 - 2 = 0$.

eg. $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ since i is a root of $x^2 + 1 = 0$

Def^n: An element $\alpha \in E$ is transcendental over F if α satisfies no polynomial in $F[x]$

eg. $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$ (hard to prove!)

Note: It is hard to prove an element is transcendental. But most real numbers are transcendental (need set theory to show only countable number of polynomials over $\mathbb{Q}$, so only countable number of algebraic number. But $\mathbb{R}$ is uncountable)

eg. Show $\sqrt{3+\sqrt{5}}$ is algebraic over $\mathbb{Q}$.
Let $\alpha = \sqrt{3+\sqrt{5}}$. Then

$$\alpha^2 = 3 + \sqrt{5}$$
$$\alpha^2 - 3 = \sqrt{5}$$
$$(\alpha^2 - 3)^2 = 5$$
$$\alpha^4 - 6\alpha^2 + 9 - 5 = 0$$
$$\alpha^4 - 6\alpha^2 + 4 = 0$$

So α is a root of

$$x^4 - 6x^2 + 4 = 0.$$

Def^n: An extension E of F is algebraic if every element of E is algebraic over F.

eg. $\mathbb{C}$ is an algebraic-extension of $\mathbb{R}$.

Def^n: Suppose $\alpha_1, \dots, \alpha_n \in E$. Let $F(\alpha_1, \dots, \alpha_n)$ be the smallest field containing both F and $\alpha_1, \dots, \alpha_n$. If $E = F(\alpha)$ for some $\alpha \in E$, then E is called a simple extension of F.

eg. $\mathbb{C} = \mathbb{R}[i]$ <- simple extension
$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

Recall: $F[x]$ is a domain (F is a field). Can form its field of fractions.

$$F[x] = \left\{\frac{p(x)}{q(x)} \mid p(x), q(x) \in F[x],\ q(x) \neq 0\right\}$$
$$= F_{F[x]} \quad \text{<- book notation}$$

Theorem: $\alpha \in F$ is transcendental over F if and only if $F(\alpha) \simeq F(x)$.

Says that α "behaves" like a variable.
Proof in the text.

eg. $\mathbb{Q}(\pi) \simeq \mathbb{Q}(x)$
So, can think of elements of $\mathbb{Q}(\pi)$ as $\frac{p(\pi)}{q(\pi)}$ where $p(x), q(x) \in \mathbb{Q}[x]$.

eg. $\frac{3\pi^2 + 2\pi + 17}{\frac{1}{3}\pi^3 + 5} \in \mathbb{Q}(\pi)$

Theorem: Suppose $\alpha \in E$ is algebraic over F. Then there exists a unique monic irreducible polynomial $p(x) \in F[x]$ of smallest degree such that $p(\alpha) = 0$. Also, if $f(\alpha) = 0$, then $p(x) \mid f(x)$.

Proof
Consider evaluation homomorphism
$$\varphi: F[x] \to E$$
$$q(x) \mapsto q(\alpha).$$

Then $\ker\varphi = \{f(x) \mid f(\alpha)=0\} \subseteq F[x]$. Since $F[x]$ is a PID, $\ker\varphi = \langle p'(x)\rangle$.
We can find a unit u such that $p(x) = up'(x)$ is monic. Since $p(x)$ and $p'(x)$ associates, $\langle p(x)\rangle = \langle p'(x)\rangle$.
Claim: $p(x)$ is the desired polynomial.
This has smallest degree by our choice of generator of $\ker\varphi$. Suppose $p(x) = r(x)s(x)$ with $\deg r(x), \deg s(x) \geq 1$. Then,
$0 = p(\alpha) = r(\alpha)s(\alpha)$.
But E is a field, so $r(\alpha)$ or $s(\alpha) = 0$. So $r(x)$ or $s(x) \in \ker\varphi$.
But this contradicts choice $p(x)$.
Finally, if $f(\alpha) = 0$, $f(x) \in \ker\varphi = \langle p(x)\rangle$. So $p(x) \mid f(x)$.

$\square$

Def^{n}: The polynomial $p(x)$ in previous result is the minimal polynomial of α over F. $\deg p(x)$ is called the degree of α over F.

eg. $\sqrt{3+\sqrt{5}}$ has degree 4 over $\mathbb{Q}$

Theorem: Suppose $\alpha \in E$ is algebraic over F. Then, the subfield $F(\alpha)$ satisfies

$$F(\alpha) \simeq F[x]/\langle p(x)\rangle$$

where $p(x)$ is the minimal polynomial of α.

<u>Proof</u>

There is a homomorphism

$$\varphi : F[x] \to F(\alpha) \in E$$
$$q(x) \mapsto q(\alpha).$$

As before, $\ker\varphi = \langle p(x)\rangle$, so by First Isomorphism Theorem,

$$F[x]/\langle p(x)\rangle \simeq \operatorname{Im}\varphi \subseteq F(\alpha).$$

Note $F[x]/\langle p(x)\rangle$ is a field (since $p(x)$ is irreducible) and it contains a copy of F. So $\operatorname{Im}\varphi$ contains a copy of F. At the same time, $\alpha \in \operatorname{Im}\varphi$, since $x \mapsto \alpha$. So $\operatorname{Im}\varphi$ contains F and α, and is a field. But $F(\alpha)$ is smallest field that contains F and α. So $F(\alpha) \subseteq \operatorname{Im}\varphi \subseteq F(\alpha)$.

$\square$

Note: x^2-2 has two roots, $\sqrt{2}$ and $-\sqrt{2}$. So $\sqrt{2}, -\sqrt{2}$ algebraic over $\mathbb{Q}$. So $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[x]/\langle x^2-2 \rangle \simeq \mathbb{Q}(-\sqrt{2})$.

More generally, if α, β are roots of the irreducible polynomial $p(x)$, then

$$F(\alpha) \simeq F(\beta) \simeq F[x]/\langle p(x) \rangle .$$

Different roots are not algebraically distinguishable.