

Lecture 22 (Simple Field Extensions)

Definition 22.1 (Ring Extensions) Let $\alpha \in S$, a commutative ring with an identity element, and R be a subring. Set

$$R[\alpha] = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \mid n \in \mathbb{N}, a_0, a_1, \dots, a_n \in R\}$$

This is called the extension of R by $\alpha \in S$.

Note

- $R[\alpha]$ is the smallest subring of S which contains R and $\alpha \in S$.
- It is the image of the evaluation map $f(x) \mapsto f(\alpha)$, from $R[x]$ to S .
- By First Isomorphism Theorem, if I is the kernel of evaluation at α , $R[x]/I \cong R[\alpha]$.
- In the case the kernel of the evaluation map is $\{0\}$, the evaluation map is injective. Then by the First Isomorphism Theorem, $R[x] \cong R[\alpha]$.

Simple Field Extensions

Definition 22.2 (Simple Field Extensions) Suppose F a field, K an extension field and $\alpha \in K$. Set

$$F(\alpha) = \{f(\alpha)/g(\alpha) \mid f(x), g(x) \in F[x], g(\alpha) \neq 0\} \supseteq F[\alpha].$$

Note that $F(\alpha)$ is the minimal subfield of K containing F and α . If $K = F(\alpha)$ we call K a *simple* field extension.

Definition 22.3 (Transcendental and Algebraic)

(1) Suppose α is not a root of any non-zero $f(x) \in F[x]$.

Then α is said to be *transcendental* over F .

(2) Suppose α is a root of some (non-zero) $f(x) \in F[x]$.

Then α is said to be *algebraic* over F .

Let $\varphi = \text{eval}_\alpha : F[x] \rightarrow K$. The two cases above correspond to $\ker \varphi = \{0\}$ and $\ker \varphi \neq \{0\}$. So α transcendental over $F \Leftrightarrow \ker \varphi = \{0\}$. In this case $F[\alpha] \cong F[x]$. Otherwise α is algebraic over F , $\ker \varphi = p(x)F[x]$ where $p(x) \in F[x]$ is a non-zero polynomial of minimal degree in $\ker \varphi$. We can replace $p(x)$ by any non-zero multiple, and so ensure its leading term is 1.

Aside In \mathbb{Z} every non-zero integer has exactly one positive associate. So there is a 1–1 correspondence between non-zero ideals and positive integers, $n\mathbb{Z} \leftrightarrow n$. Analogously in a polynomial domain $F[x]$ over a field F each non-zero polynomial has exactly one monic associate and there is thus a 1–1 correspondence between non-zero ideals of $F[x]$ and monic polynomials, $\langle p(x) \rangle \leftrightarrow p(x)$. Just as for \mathbb{Z} we have unique factorisation of positive integers into prime numbers, in a polynomial domain with coefficients in a field we have unique factorisation of monic polynomials into irreducible monic polynomials.

Definition 22.4 (Minimal Polynomial) Suppose F a field, K an extension field and $\alpha \in K$ is algebraic. Then the (unique) monic polynomial $p(x) = p_{\alpha, F}(x)$ of minimal degree with $p(\alpha) = 0$ is called the *minimal polynomial* of α over F . Note that a minimal polynomial has at least one root. So minimal polynomials have degree at least 1.

Lemma 22.5 Let F be a subfield of a field K and $\alpha \in K$ be algebraic over F . Then the minimal polynomial $p(x)$ of α with respect to F is irreducible in $F[x]$.

Proof The minimal polynomial is a polynomial of minimal degree in $F[x]$ such that $p(\alpha) = 0$. Suppose $p(x) = r(x)s(x)$, $\deg(r(x)), \deg(s(x)) < \deg p(x)$, is a non-trivial factorisation of $p(x)$ in $F[x]$. Then $r(\alpha)s(\alpha) = p(\alpha) = 0$ in the field K . Consequently $r(\alpha) = 0$ or $s(\alpha) = 0$, contradiction the minimality of $p(x)$. \square

Theorem 22.6) Let F be a subfield of a field K and $\alpha \in K$.

(1) Suppose α is transcendental over F .

Then $F[\alpha] \cong F[x]$ and $F(\alpha) \cong F(x)$.

(2) Suppose α is algebraic over F with minimal polynomial $p(x)$.

Then $F(\alpha) = F[\alpha] \cong F[x]/\langle p(x) \rangle$.

Proof

(1) The fact $F[\alpha] \cong F[x]$ in the case α transcendental was noted above. Recall $F(x) = \{f(x)/g(x) \mid f(x), g(x) \in F[x], g(x) \neq 0\}$. If α is transcendental given $g(x) \in F[x]$, $g(\alpha) = 0$ if and only if $g(x) = 0$. Hence $f(x)/g(x) \mapsto f(\alpha)/g(\alpha)$ is a well defined bijective homomorphism. The fact that $F[\alpha] \cong F[x]$ in this case was noted above.

- (2) In this case $F[\alpha] \cong F[x]/\langle p(x) \rangle$. By the previous Lemma, $p(x)$ is irreducible. Hence $F[x]/\langle p(x) \rangle$ is a field. By the discussion above $F[\alpha] \cong F[x]/\langle p(x) \rangle$. So $F[\alpha]$ is a subfield of K . But $F[\alpha] \subseteq F(\alpha)$, the minimal subfield of K containing F and α . Hence $F[\alpha] = F(\alpha)$. \square

Corollary Given a field F , an element α in an extension field is algebraic over F if and only if $F[\alpha]$ is a field. \square

Examples

- $\sqrt{2} \in \mathbb{R}$ and $i \in \mathbb{C}$ are algebraic over \mathbb{Q} .
- Every element of \mathbb{C} is algebraic over \mathbb{R} .
- If F is a field the elements of F are algebraic over F .
- There are only countably many elements of \mathbb{R} which are algebraic over \mathbb{Q} , but \mathbb{R} is uncountable. So uncountably infinitely many real number are transcendental over \mathbb{Q} .
- Louville 1851 showed how to construct some number which are transcendental numbers over \mathbb{Q} . For example $\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$.
- Showing a naturally occurring number is transcendental over \mathbb{Q} is harder.
Hermite (1873): e is transcendental over \mathbb{Q} .
Lindemann (1882): π is transcendental over \mathbb{Q} .
It is unknown if, for example, Euler's constant

$$\gamma = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n \right)$$

is rational, let alone transcendental over \mathbb{Q} .

- Gelfond and independently Schneider (1934): if a and b are algebraic and over \mathbb{Q} and b is irrational, a^b is transcendental over \mathbb{Q} .