

§ 29 Introduction to ~~a~~ extension of fields

F : field $\rightsquigarrow$ extension field of F : a field E that contains F as a subfield

Ex. $F = \mathbb{Q} \rightsquigarrow E = \mathbb{R}, \mathbb{C}, \mathbb{Q}(i) = \{a+bi \mid a, b \in \mathbb{Q}\}$ etc.

We can create extensions by taking $f(X) \in F[X]$

irreducible over F , and

$\hookrightarrow$ write $F(\alpha)$

$E = F[X] / \underbrace{f(X)F[X]}_{\text{maximal ideal}} =$ field obtained by adding " α s.t. $f(\alpha) = 0$ " to F

But there are also extensions "bigger" than this:

Some complex numbers (ex. π, e) are not roots of any polynomial with rational coefficients

Def. E : ext. field of F

$\alpha \in E$ is algebraic over F if $f(\alpha) = 0$ for some polynomial $f(X) \in F[X]$

α is transcendental otherwise over F

Ex. $\sqrt{2}, i, \sqrt{1+\sqrt{3}}$, etc. are algebraic over $\mathbb{Q}$

π, e , etc. are transcend. over $\mathbb{Q}$

we call them algebraic / transcend. numbers

Rem (cf. Thm 29.12) If $\alpha \in E$ is transc. over F

then $F(X) \xrightarrow{\phi_\alpha} E$, $\frac{f(X)}{g(X)} \mapsto \frac{f(\alpha)}{g(\alpha)}$ field hom.
 $\left\{ \frac{f(X)}{g(X)} \mid f(X), g(X) \in F[X], g(X) \neq 0 \right\}$

Suppose $\alpha \in E$ is algebraic over F

So there is a polynomial $f(X) \in F[X]$ s.t. $f(\alpha) = 0$

What is the most "economical" way to describe α in this way?

Rem If $f(\alpha) = 0$, then $g(X) = f(X)h(X)$
would also satisfy $g(\alpha) = 0$

$\leadsto$ Take $0 \neq p(X) \in F[X]$ s.t.

- $p(\alpha) = 0$, - highest deg term has coeff. 1
- $\deg p(X)$ is smallest among $\deg f(X)$
s.t. $f(\alpha) = 0, f(X) \neq 0$

call this the minimal polynomial of α (over F)
(or irreducible polynomial of α over F)

Thm 29.13 $p(X)$ min. polynomial of α (alg. over F)

1. $p(X)$ is irred. over F

2. if $f(X) \in F[X]$ satisfies $f(\alpha) = 0$ then

$$f(X) = p(X)q(X) \text{ for some } q(X) \in F[X]$$

3. if $f(X)$ is irred., $f(\alpha) = 0$ then $f(X) = c \cdot p(X)$
for some $c \in F$

Proof for point 1: want $p(X) = r(X)s(X)$
 $\Rightarrow r(X)$ or $s(X)$ const.

$$\text{Writing } p(X) = r(X)s(X), \quad 0 = p(\alpha) = r(\alpha)s(\alpha)$$

$$\text{implies } \underline{r(\alpha) = 0} \text{ or } s(\alpha) = 0$$

We assume this

$$\begin{cases} \text{minimality of } \deg p(X) \leadsto \deg p(X) \leq \deg r(X) \\ p(X) = r(X)s(X) \leadsto \deg r(X) \leq \deg p(X) \end{cases}$$

$$\leadsto \deg p(X) = \deg r(X), \quad s(X) = \text{const}$$

Proof for point 2: set $N = \{f(X) \mid f(\alpha) = 0\}$

Step 1 N is an ideal of $F[X]$

$$\begin{cases} f(X) \in N, g(X) \in F[X] \Rightarrow f(X)g(X) \in N \\ f_1(X), f_2(X) \in N \Rightarrow f_1(X) + f_2(X), -f_1(X) \in N \\ 0 \in N \end{cases}$$

Step 2 claim of point 2 : $N = p(X) F[X]$

from Thm 27.24 (March 28, from Euclid division)

Proof for point 3

$$f(X) = p(X) q(X) \quad \text{from } f(\alpha) = 0$$

$$f(X) \text{ irred.} \Rightarrow \underbrace{p(X)}_{\text{nonconst}} \text{ or } q(X) \text{ const.} \Rightarrow q(X) \text{ const.}$$

~~from $p(X) \neq 0$~~

Def. ext. field $E \supset F$ is a simple extension if
 $E = F(\alpha)$ for some $\alpha \in E$

Ex. finite extensions of $\mathbb{Q}$, $\mathbb{Z}_n$ for prime n

Non-ex. $\mathbb{Z}_n(X^{1/n}, Y^{1/n}) \supset \mathbb{Z}_n(X, Y)$ for prime n

$$(f(X^{1/n}, Y^{1/n})^n = f(X, Y))$$

n : deg. of
min. poly.
of α

Thm 29.18 $E = F(\alpha)$ simple ext. of F

any elem. of E is of the form

$$\beta = b_0 + b_1 \alpha + \dots + b_{n-1} \alpha^{n-1}$$

for unique coeffs $b_0, \dots, b_{n-1} \in F$

Existence of such expr.

Step 1 E is a quot. ring of $F[X]$ by $p(X) F[X]$

$\leadsto$ any β can be written as polynom. of α

Step 2 deg. of polynom. is at most $n-1$

$$\alpha^n = -(a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1})$$

$$\text{from } \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_0 = 0$$

$$\alpha^{n+1} = -(a_0 \alpha + \dots + a_{n-1} \underbrace{\alpha^n}_{\text{deg } n-1 \text{ poly of } \alpha}) = \text{deg } n-1 \text{ poly. of } \alpha$$

$\dots$ by induction $\alpha^k = \text{deg } n-1 \text{ poly of } \alpha$ if $k \geq n$

Uniqueness : minimality of $p(X)$

Handwritten text at the top of the page, possibly a title or introductory paragraph.

Second paragraph of handwritten text.

Third paragraph of handwritten text.

Fourth paragraph of handwritten text.

Fifth paragraph of handwritten text.

Sixth paragraph of handwritten text.

Seventh paragraph of handwritten text.

Eighth paragraph of handwritten text.

Ninth paragraph of handwritten text at the bottom of the page.