Theorem / Let F be a field and let $p(x) \in F[x]$, $p(x)$ non-constant. Then there exists an extension field E of F and $\alpha \in E$ s.t. $p(\alpha) = 0$.

Proof: we may assume $p(x)$ is irreducible.

- want to find extension field E of F s.t $p(\alpha) = 0$ for some $\alpha \in E$

Consider $$E = F[x]/\langle p(x) \rangle$$

$p(x)$ irreducible $\Rightarrow$ $\langle p(x) \rangle$ is maximal $\therefore$ E is field.

- First show E is an extension field

$\deg(p(x)) \geq 1$ $\therefore$ we would expect $F \cong \{ a + \langle p(x) \rangle \mid a \in F \}$

Define a hom $\psi : F \longrightarrow F[x]/\langle p(x) \rangle$

$a \longmapsto a + \langle p(x) \rangle$

$$\psi(a) + \psi(b) = (a + \langle p(x) \rangle) + (b + \langle p(x) \rangle)$$
$$= (a+b) + \langle p(x) \rangle = \psi(a+b)$$

$$\psi(a)\,\psi(b) = (a + \langle p(x)\rangle)(b + \langle p(x)\rangle)$$

$$= ab + \langle p(x)\rangle = \psi(ab)$$

Show ψ is 1-1

If $a + \langle p(x)\rangle = \psi(a) = \psi(b) = b + \langle p(x)\rangle$

$$a - b + \langle p(x)\rangle = \langle p(x)\rangle$$

$$a - b \in \langle p(x)\rangle \qquad \text{but } \deg(p(x)) \geq 1$$

$$\therefore \quad a - b = 0 \quad \Rightarrow \quad a = b \quad \therefore \psi \text{ is 1-1}$$

$\ker \psi = 0$

$\therefore$ By 1st iso. thm

$$F \simeq \psi(F) = \{a + \langle p(x)\rangle \mid a \in F\}$$

$\uparrow$ subfield of E

$\therefore$ E is an extension field of F

Now show $\exists\ \alpha \in E$ s.t. $p(\alpha) = 0$

Take $\alpha = x + \langle p(x)\rangle \in E$

$p(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$

E valuate at α

$$p(\alpha) = a_0 + \langle p(x)\rangle + a_1(x + \langle p(x)\rangle) + \cdots + a_n(x + \langle p(x)\rangle)^n$$

$$= a_0 + \langle p(x)\rangle + a_1(x + \langle p(x)\rangle) + \cdots + a_n(x^n + \langle p(x)\rangle)$$

$$= (a_0 + a_1 x + \cdots + a_n x^n) + \langle p(x)\rangle$$

$$= p(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle$$

$$= 0 \in F[x]/\langle p(x)\rangle$$

$\therefore p(\alpha) = 0$ in E.

$\therefore \alpha$ is a zero of $p(x)$ in E

!!

∎

Mult. in $F[x]/\langle p(x)\rangle$

$(g(x) + \langle p(x)\rangle)(f(x) + \langle p(x)\rangle)$

$= g(x)f(x) + \langle p(x)\rangle$

Ex] Let $p(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$

$$= \underbrace{(x^2 + x + 1)}_{f(x)}(x^3 + x + 1)$$

to find an extension field E s.t. $p(x)$ has a root in E

take

$E = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$

or

$E = \mathbb{Z}_2[x]/\langle x^3 + x + 1$

$\alpha = x + \langle x^2 + x + 1\rangle$

$$f(\alpha) = x^2 + \langle f(x)\rangle + x + \langle f(x)\rangle + 1 + \langle f(x)\rangle$$

$$= (x^2 + x + 1) + \langle f(x)\rangle = f(x) + \langle f(x)\rangle$$

$$= 0 + \langle f(x)\rangle$$

$\therefore \alpha$ is a root in E.

Algebraic Elements

E an extension field over F.

- An element $\alpha \in E$ is said to be algebraic if $\exists$ a polynomial $f(x) \in F[x]$ s.t. $f(\alpha) = 0$, $f(x) \neq 0 \in F[x]$
- E is <u>algebraic</u> over F if <u>for all</u> $\alpha \in E$ there exists some $f(x) \in F[x]$ such that $f(\alpha) = 0$, $f(x) \neq 0$

In this case E is an <u>algebraic extension</u> of F

- If E is a field extension of F, $\alpha_1, \dots, \alpha_n \in E$

$F(\alpha_1, \dots, \alpha_n)$ = smallest field containing $\alpha_1, \dots, \alpha_n$

L = concretely, this is the field of fractions of $F[x_1, \dots, x_n]$ evaluated at $x_i = \alpha_i$.

- $E = F(\alpha)$ for some $\alpha \in E$

E is a <u>simple extension</u> of F.

- If an element $\alpha \in E$ is not algebraic it is <u>transcendental</u>.

Ex] $\sqrt{2}$ is a zero of $x^2 - 2$

i is a zero of $x^2 + 1$

$\therefore$ $\sqrt{2}$, i are algebraic elements over $\mathbb{Q}$

$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ is an algebraic extension

π, e are algebraic over $\mathbb{R}$ (or $\mathbb{C}$) but are transcendental over $\mathbb{Q}$

Almost all real numbers are transcendental over $\mathbb{Q}$.

Def: A complex number α that is algebraic over $\mathbb{Q}$ is an algebraic number, otherwise α is a transcendental number.

Ex) $\alpha = \sqrt{2+\sqrt{3}}$ is algebraic over $\mathbb{Q}$

$$\alpha^2 = 2+\sqrt{3} \Rightarrow (\alpha^2-2)^2 = 3$$

$$= \alpha^4 - 4\alpha^2 + 1 = 0$$

$\therefore$ α is a root of $f(x) = x^4 - 4x^2 + 1 \in \mathbb{Q}[x]$.

Thm Let E be a extension field of F, $\alpha \in E$ is transcendental over F if and only if

$$F(\alpha) \cong F(x)$$

↑ Field of rational functions, i.e. field of fractions of $F[x]$.

Proof:

$$\phi_\alpha : F[x] \longrightarrow E$$

$$f(x) \longmapsto f(\alpha)$$

By def. α is transcendental over F if f

$$\phi_\alpha(p(x)) = p(\alpha) \neq 0 \quad \forall\ p(x) \neq 0 \in F[x]$$

This is true if and only if

$\ker \phi_\alpha = \{0\}$, i.e. iff ϕ_α is 1-1

If ϕ_α is 1-1 $\Rightarrow$ $F[x] \cong \phi_\alpha(F[x]) = F[\alpha] \subseteq E$

So α is transcendental iff E contains a subring isomorphic to $F[x]$

The smallest field containing $F[x]$ is $F(x)$ ← field of fractions

$\therefore$ by Thm 18.4, $F(x) \subseteq E$

$\therefore$ $F(\alpha) \cong F(x)$

↑ By def. the smallest field containing α, i.e. containing all polynomial expressions of α with coefficients in F.

[goal: explicit description of $F(\alpha)$ as a quotient ring]

Thm Let E be an extension field of F, $\alpha \in E$ algebraic over F. Then there exists a unique irreducible monic polynomial $f(x) \in F[x]$ of smallest degree s.t. $f(\alpha) = 0$, and if $g(x) \in F[x]$, $g(\alpha) = 0$ $\Rightarrow$ $f(x) \mid g(x)$.

Proof: $\alpha \in E$ alg. over F

Let $\phi_\alpha : F[x] \longrightarrow E$

$f(x) \longmapsto f(\alpha)$

$\ker \phi_\alpha = \langle f(x) \rangle$ with $\deg(f(x)) \geq 1$ for some $f(x) \in F[x]$.

↑ since $F[x]$ is a PID and α is algebraic

$\therefore$ $\ker(\phi_\alpha) \neq 0$

So let $f(x)$ have least degree s.t. $f(\alpha)=0$

- $\langle f(x)\rangle$ consists exactly of all $g(x)\in F[x]$ s.t. $g(\alpha)=0$

  since $=\ker \phi_\alpha$

$\therefore$ if $g(\alpha)=0$, $g\neq 0$, $\Rightarrow g(x)\in\langle f(x)\rangle$ $\therefore f(x)\,|\,g(x)$

Note $f(x)$ is irreducible since if $f(x)=r(x)s(x)$

for r is lower degree $\Rightarrow f(\alpha)=r(\alpha)s(\alpha)=0$

$\Rightarrow r(\alpha)=0$ or $s(\alpha)=0$

which is a contradiction since

$f(x)$ has minimal degree s.t. α is a root.

Show $f(x)$ monic, unique $\qquad f=a_nx^n+\cdots+a_1x+a_0$

So if $f(x)$ is not monic, take $\hat{f}(x)=\dfrac{f(x)}{LC(f)}=\dfrac{f}{a_n}$

$\langle f(x)\rangle=\langle \hat{f}(x)\rangle$

$\therefore$ Assume $f(x)$ is monic.

Uniqueness: Suppose $\langle f(x)\rangle=\langle g(x)\rangle$ (Both monic, minimal degree)

$\Rightarrow f(x)=\beta g(x)$ But both f,g monic

$\therefore \beta=1$ and $f(x)=g(x)$. ∎

Def: Let E be an extension field of F, $\alpha\in E$ alg. over F. The unique monic polynomial $f(x)$ in thm. above is called the **minimal polynomial** for α over F,

the degree of α over F = $\deg(f(x))$

Ex| • $x^2 - 2$ is the minimal poly. of $\sqrt{2}$ over $\mathbb{Q}$

• $x^2 + 1$ is min. poly. of i over $\mathbb{Q}$ (or over $\mathbb{R}$)

$\sqrt{2}$, i have degree 2 over $\mathbb{Q}$.

Prop| Let E be a field extension of F, $\alpha \in E$ alg. over F. Then $F(\alpha) \cong F[x]/\langle p(x) \rangle$ where $p(x)$ is the minimal polynomial of α over F.

Proof: $\phi_\alpha : F[x] \longrightarrow E$

$f(x) \longmapsto f(\alpha)$

$\ker(\phi_\alpha) = \langle p(x) \rangle$

↑ where p is min poly. of α. (from last proof)

By 1st isc theorem

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

$\alpha = \phi_\alpha(x)$

Since $\alpha \in \phi_\alpha(F[x])$

and $\phi_\alpha(F[x])$ is a field

Since it's isc morphic to a field

check that $\exists$ no smaller field inside $\phi_\alpha(F[x])$.

Suppose E is a field containg α, s.t. $E \subsetneq \phi_\alpha(F[x])$

Suppose $\beta \in \phi_\alpha(F[x])$, $\beta \notin E$, $\beta = f(\alpha)$ for f a poly; i.e. they are F. lin. combinations of powers of α, but every power of α, and every F linear combo of α must be in E since E is a field containg F and α.

if β is not in $E \Rightarrow E$ is not a field, which is a contradiction $\therefore E = F(\alpha) = \phi_\alpha(F[x])$. ∎

Thm1 $E \simeq F(\alpha)$ ← simple extension, $\alpha \in E$ algebraic over F.

Suppose degree of α over F is n. Then every element $\beta \in E$ can be expressed uniquely in the form

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

for $b_i \in F$. That is, $F(\alpha)$ is a F-vector space of dim. n, with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Proof:

$\phi_\alpha(F[x]) \simeq F(\alpha)$ $\therefore$ every $\beta \in F(\alpha)$ is $\beta = \phi_\alpha(f(x)) = f(\alpha)$ ← Poly. in α, with coefficents in F

Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be the minimal poly of α

$p(\alpha) = 0$ $\therefore$ $0 = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0$

$\Rightarrow \alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$

Now note

$$\alpha^{n+1} = \alpha\,\alpha^n = -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha$$

$$= a_{n-1}(a_{n-1}\alpha^{n-1} + \cdots + a_0) - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha$$

By induction α^m, $m \geq n$ can be written as a F linear combination of $1, \alpha, \ldots, \alpha^{n-1}$

$\therefore$ $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ for all $\beta \in F(\alpha)$

Now show rep ↑ of $\beta \in F(\alpha)$ is unique

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

$$g(x) = (b_0 - c_0) + (b_1 - c_1)x + \cdots + (b_{n-1} - c_{n-1})x^{n-1} \in F[x]$$

$$g(\alpha) = \beta - \beta = 0 \qquad \text{but } \deg(g(x)) < \deg(p(x))$$

$$\Rightarrow \quad g(x) = 0 \quad \text{since } p(x) \text{ is minimal poly of } \alpha.$$

$\therefore$ $b_i = c_i$ ∎

Ex) $E = \mathbb{R}[x]/\langle x^2+1\rangle$ ← field extension of $\mathbb{R}$
$= \mathbb{R}(i)$

contains a root $\alpha = x + \langle x^2+1\rangle$ of x^2+1

$$\alpha^2 = x^2 + \langle x^2+1\rangle = -1 + \langle x^2+1\rangle$$

$\therefore$ $\alpha^2 = -1$ in E

$\phi : \mathbb{R}(\alpha) \longrightarrow \mathbb{C}$

$a + b\alpha \longrightarrow a + bi$ is an iso morphism.

$\therefore$ $\mathbb{C}$ is a degree two field extension of $\mathbb{R}$.

Def1 If E is an extension field of F which is a finite dimensional V. space over F of, $\dim = n$ we say E is a finite extension of degree n over F write $[E:F] = n$.

Thm1 If E is a finite extension of F, then E is an algebraic extension.

Proof:

Let $\alpha \in E$, $[E:F] = n$

then $1, \alpha_1 \dots, \alpha^n$ can not be linearly independent.

$\therefore$ $\exists\ a_i \in F$, not all zero, s.t

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0 = 0$$

$\therefore$ $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ is a non-zero polynomial and $p(\alpha) = 0$ $\therefore$ E is an algebraic extension

$\blacksquare$