Rmk The thm is also true in the following form

Let f be a non-constant poly in $F[x]$. Then $\exists$ a field K containing an isom copy of F and an element $\alpha \in K$ s.t $f(\alpha) = 0$.

If f is not irreducible, then it can be factored into irreducibles, $f = p_1 \cdots p_r$. Then can take $K = F[x]/(p_i)$ for any of the irreducible factors.

Note if one of the factors is linear then f already has a root in F.

To understand the field $K = F[x]/(p(x))$ better we have the following simple representation of its elements

Thm 2.4 Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over F.

Let $K = F[x]/(p(x))$, and $\alpha = x + (p(x)) \in K$

Then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ form a basis of K as a vector space over F, hence $[K:F] = n$

Moreover $K = \{ a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in F \}$

$= \underbrace{F_{n-1}[\alpha]}_{\text{polys of degree} \leq n-1} = F(\alpha)$.

Proof let $f(x) \in F[x]$ be any poly w/ coefs in F. Using division alg.

$$f(x) = p(x)\,q(x) + r(x) \quad \text{w/} \quad q, r \in F[x]$$
$$\deg r < \deg p =$$

Since $p(x)q(x) \in (p(x))$

$$f(x) \equiv r(x) \mod (p(x))$$

Hence every poly $f(x) \in F[x]$ is residue class in $F[x]/(p(x))$ is represented by a poly $r(x)$ of degree $< n$.

ie. Images of $1, x, x^2, \ldots, x^{n-1}$ in the quotient $K = F[x]/(p(x))$, ie $1, \alpha, \alpha^2 \ldots \alpha^{n-1}$ span the quotient K as a vector space over F.

If the elements $1, \alpha, \ldots, \alpha^{n-1}$ were lin. dependent in K, then there would be $b_0, \ldots b_{n-1} \in F$ not all zero s.t

$$0_K = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} = g(x) + (p(x))$$

Hence

$$g(x) = b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} \in (p(x))$$

ie $$p(x) \mid b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} \text{ in } F[x]$$

But this is impossible since $\deg p = n > \deg g = n-1$

Hence $1, \alpha, \ldots \alpha^{n-1}$ is a basis of K over F and $K = \{ a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in F \}$

$$= F_{n-1}[\alpha]$$

$K = F_{n-1}[\alpha]$ contains F and α. But $F(\alpha)$ is by definition the smallest field which contains F and α. Since it also contains $F_{n-1}[\alpha]$ we have $K = F(\alpha)$.

$F_{n-1}[\alpha] = F[\alpha]$

∎.

Rmk. How does the arithmetic in $F[x]/(p(x))$ work in practice?

eg ① $F = \mathbb{R}$, $p(x) = x^2+1$, $\alpha = x + (x^2+1)$

$$K = \mathbb{R}[x]/(x^2+1) = \{ a + b\alpha \mid a, b \in \mathbb{R} \}.$$

$$(a+b\alpha) + (c+d\alpha) = (a+c) + (b+d)\alpha$$

$$\begin{aligned}(a+b\alpha)\cdot(c+d\alpha) &= ac + (ad+bc)\alpha + bd(\alpha^2) \\ &= ac + (ad+bc)\alpha + bd(-1) \\ &= ac - bd + (ad+bc)\alpha\end{aligned}$$

These look like the addition and multiplication formulas in $\mathbb{C}$ up to $\alpha \leftrightarrow i$

$\varphi : \mathbb{R}[x]/(x^2+1) \longrightarrow \mathbb{C}$, $a + b\alpha \longmapsto a + bi$

φ is a hom, it is bijective hence

an isomorphism $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$

(2) $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ irred. by Eisenstein $p = 2$.

$K = \mathbb{Q}[x]/(x^3-2) \cong \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$

with $\alpha^3 - 2 = 0$ in K.

How do we find inverses of elts in K, say $(1-\alpha)^{-1}$

Since $x^3 - 2$ is irreducible, it is relatively prime to every polynomial of smaller degree. In particular to $1-x$

Hence $\exists$ $a(x), b(x) \in \mathbb{Q}[x]$ s.t

$$a(x)(1-x) + b(x)(x^3-2) = 1$$

Hence $a(x)(1-x) \equiv 1 \mod (x^3-2)$

and $(1-x)^{-1} = a(x)$. To find $a(x)$ note

$$(x^3-2) = (1-x)(-x^2-x-1) - 1$$

Hence can take $a(x) = -x^2 - x - 1$, $b(x) = -1$

so that

$$(1-\alpha)^{-1} = -\alpha^2 - \alpha - 1$$

Similarly to find $(\alpha^2+1)^{-1}$ we use

eucl. alg to write

$$(x^3-2) = (x^2+1)x + (-x-2)$$

$$(x^2+1) = (-x-2)(-x+2) + 5$$

Going backwards

$$5 = (x^2+1) - (-x-2)(-x+2)$$

$$5 = (x^2+1) - (2-x)[(x^3-2) - (x^2+1)x]$$

$$5 = (x^2+1)(1+2x-x^2) + (x-2)(x^3-2)$$

Hence $$1 = (x^2+1)\left(\frac{1}{5} + \frac{2}{5}x - \frac{x^2}{5}\right) + \left(\frac{x}{5} - \frac{2}{5}\right)(x^3-2)$$

and $$(\alpha^2+1)^{-1} = \frac{1}{5} + \frac{2}{5}\alpha - \frac{\alpha^2}{5}$$

Recall If K/F an extention of fields, $\alpha_1, \ldots \alpha_n \in K$ a collection of elements of K. Then the smallest s/field of K containing both F and $\alpha_1, \ldots \alpha_n$ is denoted by $F(\alpha_1 \ldots \alpha_n)$ and is called the Field generated by $\alpha_1, \ldots, \alpha_n$ over F.

If K is generated by a single element α over F, ie $K = F(\alpha)$ then K is called a simple extention.

The connection between simple extention $F(\alpha)$ generated by α over F where α is a root of some irred poly $p(x) \in F[x]$ and the field constructed in Thm 2.3 (Kronecker's thm) is

---

Thm 2.5 Let F be a field $p(x) \in F[x]$ irred. poly. Suppose L is an extention field of F containing a root α of $p(x)$, and let $F(\alpha)$ denote the subfield of L generated over F by α. Then

$$F(\alpha) \cong F[x]/(p(x))$$

Proof. Exercise: $\varphi: F[x] \to F(\alpha) \subset L$ $p(\alpha) \in \ker \varphi$
$f(x) \mapsto f(\alpha)$

hence $\exists$ hom $\bar{\varphi}: F[x]/(p(x)) \to F(\alpha)$.

Rmk. Thm 2.5 assumes the existence of a root α of $p(x)$ in some field L where as the main point of Thm 2.3 is to show that such an extension exists.

Thm 2.5 says any field L over F in which $p(x)$ contains a root contains a subfield isomorphic to the extension of F constructed in Thm 2.3, (Thm 2.4) and that this field is (up to isom.) the smallest extension of F containing such a root.

Hence the roots of an irred polynomial $p(x)$ are algebraically indistinguishable in the sense that the fields obtained by adjoining any root of an irred poly. are isomorphic.

Ex Consider $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ irred. by Eisenstein

It has one real root $\sqrt[3]{2} =: \alpha$ and 2 complex roots $\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right) =: \beta$

$\sqrt[3]{2}\left(\frac{-1-i\sqrt{3}}{2}\right) =: \gamma$

$\alpha, \underbrace{\alpha e^{2\pi i/3}}_{\beta}, \underbrace{\alpha e^{4\pi i/3}}_{\gamma}$

$\alpha \in \mathbb{R}$ $\quad \beta \notin \mathbb{R}$ $\quad \gamma \notin \mathbb{R}$

Hence $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta) \cong \mathbb{Q}(\gamma) \cong \mathbb{Q}[x]/(x^3-2)$

We have in general

Thm 2.6 Let $\varphi : F \to \tilde{F}$ be an isom of fields. Let $p(x) \in F[x]$ be an irred poly, and let $\tilde{p}(x) = \tilde{F}'(x)$ be the irred poly obtained by applying the map φ to the coefs of p

ie if $p(x) = \sum a_i x^i$ then $\tilde{p}(x) = \sum \varphi(a_i) x^i$

Let α be a root of $p(x)$ (in some ext. of F) and let β be a root of $\tilde{p}(x)$ (in an ext. of $\tilde{F}$). Then $\exists$ unique isom

$$\sigma : F(\alpha) \to \tilde{F}(\beta) \quad \text{s.t}$$

$$\sigma(\alpha) = \beta \quad \text{and} \quad \sigma|_F = \varphi.$$

Rmk. Note Thm 2.6 with $F = \tilde{F}$ says $F(\alpha) \cong F(\beta)$ for any 2 zeroes of an irred. poly $p(x) \in F[x]$.

Proof $\varphi : F \to \tilde{F}$, induces an isom of poly. ring

$$\varphi : F[x] \to \tilde{F}[x]$$
$$\sum a_i x^i \mapsto \sum \varphi(a_i) x^i \quad , \quad \varphi(p(x)) = \tilde{p}(x)$$

hence $\tilde{p}(x)$ is irreducible and φ induces the isom. of fields $F[x]/(p(x)) \cong \tilde{F}(x)/(\tilde{p}(x))$

Thm 2.5 gives $F(\alpha) \cong F[x]/(p(x))$

and $\tilde{F}(\beta) = \tilde{F}[x]/(\tilde{p}(x))$

and we have $\sigma : F(\alpha) \cong \tilde{F}(\beta)$

$\varphi : F \cong \tilde{F}$

(Note $\sigma : F(\alpha) \to \tilde{F}(\beta)$, $\sum a_i \alpha^i \mapsto \sum \varphi(a_i)\beta^i$) ∎

Before we move to algebraic extensions we note 2 useful results.

Lemma 2.7 Let f, g be polynomials over a field F. Then f and g are relatively prime if and only if f and g have no common root in any extension of F.

Proof : Exercise (Sets 2)

Cor. 2.8 If f and g are distinct polynomials which are monic, then f and g have no common roots in any extension of F.

Proof Exercise (Sets 2)

§ 2.2 Algebraic extensions

Defn (1) Let $F \subset K$ be fields. An element $\alpha \in K$ is said to be algebraic over F if α is a root of a non-zero polynomial with coefs in F. $F(\alpha)$ is called alg ext. generated by α. If there is no such poly, then α is called transcendental over F.

(2) An Extention K/F is called an algebraic extention if every element of K is algebraic over F.

Rmk If $\alpha \in K$ is alg. over F, then clearly it is algebraic over any extention L of F.

Prop 2.9 Let α be algebraic over F. Then $\exists$ a unique monic irred. polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. If $f(x) \in F[x]$ also has α as a root then $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.

Proof Since α is algebraic over F there is a poly over F which has a root. Let $m(x) \in F[x]$ be a poly of minimal degree having α as a

root. By multiplying it by a constant if necessary, we can assume that $m(x)$ is monic.

First we note that $m(x)$ is irreducible since if it were not then we could write $m(x) = a(x)\,b(x)$ for some $a(x), b(x) \in F[x]$ with $\deg a < \deg m$, $\deg b < \deg m$.

Since $m(\alpha) = 0$ we have either $a(\alpha) = 0$ or $b(\alpha) = 0$. Hence either $a(x)$ or $b(x)$ has α as a root which contradicts the minimality of degree $m(x)$.

Hence $m(x)$ is irreducible.

Now let $f(x) \in F[x]$ be such that $f(\alpha) = 0$. Using Euclidean alg. in $F[x]$, we can find $q(x)$, $r(x)$ s.t

$$f(x) = m(x)\,q(x) + r(x), \quad \deg r < \deg m \text{ or } r = 0$$

Since $0 = f(\alpha) = m(\alpha)\,q(\alpha) + r(\alpha)$
$= r(\alpha)$

we get a contradiction to minimality of m unless $r = 0$. But in that case $m \mid f$.

In particular $m(x)$ will divide any irred monic polynomial in $F[x]$ which has α as a root. But that shows $m = \tilde{m}$ and m is unique

For $\alpha \in K$, algebraic over F

Defn The polynomial $m_{\alpha,F}(x) \in F[x]$, the unique monic irreducible polynomial which has α as a root, is called the minimal polynomial of α over F

The degree of $m_{\alpha,F}(x)$ is called the degree of α over F.

Cor 2.10 If $L : F$ is an extention and α is algebraic over F and L. Then

$$m_{\alpha,L}(x) \mid m_{\alpha,F}(x) \text{ in } L[x]$$

Proof We apply Prop 2.9 to $m_{\alpha,L}(x) \in L[x]$ since $m_{\alpha,F}[x]$ is also in $L[x]$, and $m_{\alpha,F}(\alpha) = 0$

$m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$ in $L[x]$.

Rmk The minimal poly and degree of α depend on the base field.

eg Let $\alpha = \sqrt{2}$. it is of degree 2 / $\mathbb{Q}$ since $m_{\alpha,\mathbb{Q}}(x) = x^2 - 2$ is irred in $\mathbb{Q}[x]$ and has $\sqrt{2}$ has a root.

But α is of degree 1 over $\mathbb{R}$ with $m_{\alpha,\mathbb{R}} = x - \sqrt{2}$

Note that $\underbrace{x - \sqrt{2}}_{m_{\alpha,\mathbb{R}}} \mid \underbrace{x^2 - 2}_{m_{\alpha,\mathbb{Q}}}$ in $\mathbb{R}[x]$.