# Theorem 20.1 (Kronecker FT FT)

Let $F$ be a field and $f(x) \in F[x]$ non constant. Then there is an extension field $E$ of $F$ in which $F(x)$ has a zero.

**Proof**

$F[x]$ a UFD $\overset{\text{(Cor./Thm 18.3)}}{\Longrightarrow}$ $f(x)$ has an irreducible factor $p(x)$.
We proceed to find a zero of $p(x)$ in $E = F[x]/\langle p(x)\rangle$, which is a field by Cor 1 of Thm. 17.5.
$F$ "is a subfield" of $F[x]/\langle p(x)\rangle$, by verifying that

$$\varphi : F \to F[x]/\langle p(x)\rangle$$
$$\varphi(a) = a + \langle p(x)\rangle$$

is a 1-1 ring homomorphism.
Write
$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0.$$

**Claim** The element $x + \langle p(x)\rangle$ in $F[x]/\langle p(x)\rangle$ is a zero of $p(x)$.

**Proof of Claim**

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

$$= a_n(x^n + \langle p(x)\rangle) + \cdots + a_1(x \langle p(x)\rangle) + a_0$$
$$= \sum_{i=0}^n a_i(x^i + \langle p(x)\rangle)$$
(definition of coset multiplication in $F[x]/\langle p(x)\rangle$)

$$= \sum_{i=0}^n (a_i x^i + a_i\langle p(x)\rangle)$$
(distributivity in $F[x]/\langle p(x)\rangle$)

$$= \sum_{i=0}^n (a_i x^i + \langle p(x)\rangle)$$
(ideals absorb elements in $F[x]$)

$$= \left(\sum_{i=0}^n a_i x^i\right) + \langle p(x)\rangle$$
(definition of coset addition in $F[x]/\langle p(x)\rangle$)

$$= p(x) + \langle p(x)\rangle$$
$$= 0 + \langle p(x)\rangle$$, the zero of $F[x]/\langle p(x)\rangle$. $\square$

Theorem 20.3 Let $p(x) \in F[x]$ be irreducible over $F$.
Let $a$ be a zero of $p(x)$ in extension $E$ of $F$.
Then

$$F(a) \approx F[x]/\langle p(x)\rangle;$$

and if $\deg p(x) = n$, then all $\alpha \in F(a)$ can be uniquely expressed in the form

$$\alpha = c_{n-1}a^{n-1} + \cdots + c_1 a^1 + c_0,$$

where $c_{n-1}, \ldots, c_1 \in F$.

Proof

Thm 20.1 $\Rightarrow$ $\exists$ an extension $E$ of $F$ containing a zero $a$ of $p(x)$.
Define $F(a)$ = smallest extension of $F$ containing $a$.
Define

$$\varphi: F[x] \to F(a)$$
$$\varphi(f(x)) = f(a).$$

$\operatorname{Ker}\varphi = \langle p(x)\rangle$

($\supseteq$) $p(a) = 0 \Rightarrow p(x) \in \operatorname{Ker}\varphi$, and so $\langle p(x)\rangle \subseteq \operatorname{Ker}\varphi$.
($\subseteq$) Thm 17.5: $p(x)$ irreducible $\Rightarrow \langle p(x)\rangle$ is a maximal ideal in $F[X]$.
Thm 15.2: $\operatorname{Ker}\varphi$ is an ideal in $F[x]$.
$1 \notin \operatorname{Ker}\varphi$ since $\varphi(1) = 1 \neq 0$.

$$\left.\begin{array}{l}\langle p(x)\rangle \subseteq \operatorname{Ker}\varphi \subseteq F[x] \text{ and} \\ \operatorname{Ker}\varphi \neq F[x],\ \langle p(x)\rangle \text{ maximal}\end{array}\right\} \Rightarrow$$

$\langle p(x)\rangle = \operatorname{Ker}\varphi$.

First Isom. Thm. Rings $\Rightarrow$

$$F[x]/\langle p(x)\rangle \approx \varphi(F[x])$$

Cor 1 to Thm. 17.5 $\Rightarrow$

$F[x]/\langle p(x)\rangle$, $\varphi(F[x])$ are isomorphic fields

$$\begin{cases} F = \varphi(\{f\cdot x^0 \mid f \in F\}) \subseteq \varphi(F[x]) \\ a = \varphi(x) \in \varphi(F[x]) \\ F(a) \text{ is the smallest field containing } F \text{ and } a \end{cases}$$

$$\Rightarrow \quad \varphi(F[x]) = F(a) \approx F[x]/\langle p(x)\rangle.$$

Ex. 21, Chapter 16:

Every $f(x) \in F[x]/\langle p(x)\rangle$ has a unique description

$$f(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 + \langle p(x)\rangle$$

Therefore every $\alpha \in F(a)$ has the unique description

$$\alpha = c_{n-1}a^{n-1} + \cdots + c_1 a + c_0. \quad \square$$

<u>Corollary</u> $p(x)$ irreducible in $F[x]$.

$p(a) = 0$ for $a \in E$, extension of $F$

$p(b) = 0$ for $b \in E'$, extension of $F$.

Then
$$F(a) \underset{\substack{\uparrow \\ \text{Thm 20.3}}}{\approx} F[x]/\langle p(x)\rangle \underset{\substack{\uparrow \\ \text{Thm 20.3}}}{\approx} F(b).$$

Lemma
- $p(x) \in F[x]$ irreducible
- $p(a) = 0$, some $a$ in an extension of $F$
- $\varphi : F \to F'$ a field isomorphism
- $b$ a zero of $\varphi(p(x))$ in an extension of $F'$

Then $\exists\, \theta : F(a) \to F'(b)$ with
- $\theta$ a field isomorphism
- $\theta = \varphi$ on $F$
- $\theta(a) = b$.

Proof sketch

$p(x)$ irred. over $F$ $\Leftrightarrow$ $\varphi(p(x))$ irred. over $F'$.

So $\varphi : F \to F'$ extends to

$$\varphi : F[x]/\langle p(x)\rangle \to F'[x]/\langle \varphi(p(x))\rangle$$

by setting $\varphi(f(x) + \langle p(x)\rangle) = \varphi(f(x)) + \langle \varphi(p(x))\rangle$

and is a field isomorphism.

$$F(a) \xrightarrow[\alpha]{\text{Thm 20.3}} F[x]/\langle p(x)\rangle \xrightarrow[\varphi]{\text{above}} F'[x]/\langle \varphi(p(x))\rangle \xrightarrow[\beta]{\text{Thm 20.3}} F'(b)$$

are all isomorphisms. Furthermore

$$\begin{aligned} \beta\varphi\alpha(a) &= \beta\varphi(x + \langle p(x)\rangle) \\ &= \beta(x + \langle \varphi(p(x))\rangle) \\ &= b \end{aligned}$$

$\square$

Theorem 20.4 • $\varphi : F \to F'$ a field isomorphism

- $f(x) \in F[x]$ has splitting field $E$
- $\varphi(f(x)) \in F'[x]$ has splitting field $E'$

Then there is an extension of $\varphi$

with $\varphi : E \to E'$ a field isomorphism.

Proof Sketch

Induction on $\deg(f(x))$.

$\deg(f(x)) = 1 \Rightarrow E = F, \ E' = F'$, done.

$\deg(f(x)) > 1$ Let $p(x)$ be an irred factor of $f(x)$, with zero $a \in E$, and let $\varphi(p(x))$ have zero $b \in E'$.

Lemma $\Rightarrow$ $\varphi : F(a) \to F'(b)$

- agrees with $\varphi$ on $F$
- $\varphi(a) = b$.

$f(x) = p(x)\, g(x)$ with $\deg(g(x)) < \deg(f(x))$.

Set $F \leftarrow F(a)$

$F' \leftarrow F'(b)$

and apply induction, since

$E$ is a splitting field for $f(x)$ over $F(a)$

$E'$ is a splitting field for $\varphi(f(x))$ over $F'(b)$

$\square$