Recall: $p \in F[x]$ $\quad F$: field $\quad p$: irred

$K = F[x]/(p)$ is an ext'n field of F

$\theta = x + (p)$ is a root of p in K

Multiplication in K:

Write $a(x)b(x) = q(x)p(x) + r(x)$ $\quad \deg r < n$

Then, $a(\theta)b(\theta) = r(\theta)$

Trick to reduce polys. mod p:

$$p(\theta) = 0, \text{ so } \theta^n = -(p_{n-1}\theta^{n-1} + \dots + p_1\theta + p_0)$$

$$\begin{aligned}\theta^{n+1} &= -(p_{n-1}\theta^n + \dots + p_1\theta^2 + p_0\theta) \\ &= -\big(p_{n-1}\big(-(p_{n-1}\theta^{n-1} + \dots + p_1\theta + p_0)\big) \\ &\quad + p_{n-2}\theta^{n-1} + \dots + p_0\theta\big)\end{aligned}$$

etc.

Examples:

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

$$K = \mathbb{R}[x]/(x^2+1) = \{a + b\theta \mid a+b \in \mathbb{R}\} \quad \theta^2 = -1$$

$$(a+b\theta)(c+d\theta) = (ac-bd) + (ad-bc)\theta$$

So $K \cong \mathbb{C}$!

(when $F = \mathbb{Q}$, $K \cong \mathbb{Q}(i)$)

b) $F = \mathbb{Q}$, $p(x) = x^3 - 2$.

p is irred by Eisensteins criterion

$\left(\begin{array}{l} a_n x^n + \cdots + a_0 \text{ is irred if } \exists \text{ prime } p \\ - \ p \mid a_{n-1}, \ldots, p \mid a_0 \\ - \ p \nmid a_n \\ - \ p^2 \mid a_0 \end{array} \right)$

Def: Let $F \subseteq K$, and let $\alpha, \beta, \ldots \in K$.
Then $F(\alpha, \beta, \ldots)$ is the smallest subfield of K containing F and $\alpha, \beta, \ldots$

Depends on K (for now)

Equivalently, $F(\alpha, \beta, \ldots)$ is the intersection of all fields w/ this property

Def: If $K = F(\alpha)$, K is called a <u>simple</u> ext'n of F, α is called a <u>primitive</u> element for the ext'n.

Thm 6: $p(x) \in F[x]$: irred.,
Suppose K: ext'n field of F containing a root α of $p(x)$

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

via the map $\begin{cases} f \mapsto f, & f \in F \\ x \mapsto \alpha \end{cases}$

Takeaways:

- $F(\alpha)$ is indep. of K
- If β is another root of p, then $F(\alpha) \cong F(\beta)$

Ex: Let $\omega := \dfrac{-1 + i\sqrt{3}}{2}$. Then $\omega^3 = 1$ and $x^3 - 2$ has roots $\underset{\in \mathbb{R}}{\sqrt[3]{2}}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$

Then,

$$F(\sqrt[3]{2}) \cong F(\omega\sqrt[3]{2}) \cong F(\omega^2\sqrt[3]{2}) \cong F[x]/(x^3 - 2)$$

---

§13.2 Algebraic Ext'ns

Def: Let K/F be any field ext'n

$\alpha \in K$ is <u>algebraic</u> over F if $\exists$ nonzero poly. $f(x) \in F[x]$ s.t. $f(\alpha) = 0$.

Otherwise, α is <u>transcendental</u>

K/F is algebraic if α is alg. $\forall \alpha \in K$

Def: If α is algebraic / F, the minimal polynomial $m_\alpha(x) := m_{\alpha,F}(x)$ is the monic poly. in $F[x]$ of minimal degree having α as a root. Let $\deg \alpha := \deg m_{\alpha,F}$

Properties:

- $m_{\alpha,F}(x)$ is unique
- $m_{\alpha,F}(x)$ is irreducible
- $\underset{\in F[x]}{f}(\alpha) = 0 \Leftrightarrow m_{\alpha,F}(x) \mid f(x)$

To prove: assume not, and find a smaller minimal poly.

- If $F \subseteq L$, α is alg. $/L$ and $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$

Prop 11:

$$[F(\alpha) : F] = \deg m_\alpha(x) = \deg \alpha$$

by def'n

Pf: By Thm. 6, $F(\alpha) \cong F[x]/(m_\alpha(x))$

By Thm. 4, $\left[F[x]/(m_\alpha(x)) : F\right] = \deg m_\alpha(x)$

Example: pos. real nth root of p

$\alpha = \sqrt[n]{p}$ $\quad$ p: prime

$m_{\alpha,\mathbb{Q}}(x) = x^n - p$ (irred. by Eisenstein)

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$

However, $m_{\alpha,\mathbb{R}}(x) = x - \sqrt[n]{p}$ $\quad$ $[\underbrace{\mathbb{R}(\alpha)}_{\mathbb{R}} : \mathbb{R}] = 1$

If n is even, then

$$m_{\alpha,\mathbb{Q}(\sqrt{p})} = x^{n/2} - \sqrt{p}, \quad [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{p})] = \frac{n}{2}$$

Next: Tower law and composites of field ext'ns