Thm Let $K \subseteq L$ be a field extension and $\alpha \in L$ algebraic with minimal poly. $f \in K[x]$. The homomorphism $ev_\alpha : K[x] \to L$, $f(x) \mapsto f(\alpha)$ induces an isomorphism

$$K[x]/(f) \xrightarrow{\sim} K[\alpha] \subseteq L.$$

Thus $K[\alpha] = K(\alpha)$ and $[K(\alpha):K] = \deg f$.

Pf By the first isomorphism theorem,

$$ev_\alpha : K[x] / {\ker ev_\alpha} \simeq \operatorname{im} ev_\alpha = K[\alpha].$$

I have previously shown that $f(\alpha) = 0 \Leftrightarrow x - \alpha \mid f$. Thus $\ker ev_\alpha = (f)$. This proves the first part.

Since f is irreducible $\Rightarrow (f)$ maximal

$\Rightarrow K[x]/(f)$ a field.

Thus $K(\alpha) \subseteq K[\alpha] \subseteq K(\alpha) \Rightarrow K[\alpha] = K(\alpha)$.

Finally $[K(\alpha):K] = [K[x]/(f) : K] = \deg f$ ∎

Cor $K \subseteq L$ extension and $\alpha \in L$ algebraic with min poly $f \in K[x]$. If β is another root of f, then $K(\alpha) \cong K(\beta)$. (NOT EQUAL)

Ex
- $\mathbb{Q}(i) = \mathbb{Q}(-i)$ as subfields of $\mathbb{C}$.
- $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\omega\sqrt[3]{2})$ but $\underset{\substack{\cap \\ \mathbb{R}}}{\mathbb{Q}(\sqrt[3]{2})} \neq \underset{\substack{\not\subset \\ \mathbb{R}}}{\mathbb{Q}(\omega\sqrt[3]{2})}$

Defn A field extension $K \subseteq L$ is said to be simple if $L = K(\alpha)$ for some $\alpha \in L$. The element α is called the primitive element.

NOTE For the rest of the course we restrict to subfields of $\mathbb{C}$.

Thm (Primitive element thm) Let $K, L \subseteq \mathbb{C}$ and $K \to L$ a finite extension (thus algebraic) then $L = K(\alpha)$ for some $\alpha \in L$.

Ex
- Consider $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$. Since $x^2 - 2$ is irreducible over $\mathbb{Q}$, monic and kills $\sqrt{2}$, it's the minimal polynomial

- Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$. Again $x^3 - 2$ is irreducible (Eisenstein) over $\mathbb{Q}$, monic and kills $\sqrt[3]{2}$. Thus it's the minimal polynomial. Thus $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

- Consider $\mathbb{Q} \subseteq \mathbb{Q}(i\sqrt[3]{2})$. This one is trickier. Let's first find SOME polynomial that annihilates $i\sqrt[3]{2}$. The idea is to mimic the proof of the thm that every finite extension is algebraic.

$(i\sqrt[3]{2})^0 = 1$

$(i\sqrt[3]{2})^1 = i\sqrt[3]{2}$

$(i\sqrt[3]{2})^2 = -\sqrt[3]{4}$

$(i\sqrt[3]{2})^3 = -2i$

$(i\sqrt[3]{2})^4 = 2\sqrt[3]{2}$

$(i\sqrt[3]{2})^5 = 2i\sqrt[3]{4}$

$(i\sqrt[3]{2})^6 = -4$

So we see $(i\sqrt[3]{2})^6 \in \mathbb{Q}$. Thus $x^6 + 4$ is a polynomial that kills $i\sqrt[3]{2}$. How do we know it's the minimal one (is it irreducible)?

Prop (Multiplicativity of degrees) Let $K \subseteq L$ and $L \subseteq M$ be field extensions. If $K \subseteq M$ is finite, then

① $K \subseteq L$ and $L \subseteq M$ are finite

② $[M:K] = [M:L]\cdot[L:K]$.

Pf Hwk 7 ■

Going back to our example, assume that f of degree $n \leq 6$ was the minimal polynomial of $i\sqrt[3]{2}$. Since $i = \frac{-i}{2} = -\frac{(i\sqrt[3]{2})^3}{2} \in \mathbb{Q}(i\sqrt[3]{2})$

$$\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(i\sqrt[3]{2})$$

Thus $2 = [\mathbb{Q}(i):\mathbb{Q}]$ divides $[\mathbb{Q}(i\sqrt[3]{2}):\mathbb{Q}] = n$

Similarly $\sqrt[3]{2} = \frac{2\sqrt[3]{2}}{2} = \frac{(i\sqrt[3]{2})^4}{2} \in \mathbb{Q}(i\sqrt[3]{2})$ implies

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(i\sqrt[3]{2}).$$

Thus $3 = [\mathbb{Q}(i\sqrt[3]{2}):\mathbb{Q}]$ divides n

Thus $6 \mid n \Rightarrow n = 6 \Rightarrow x^6 + 4$ is the min. poly ■

- Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Let $\alpha = \sqrt{2}+\sqrt{3}$, we want to find the min poly. of α.

Note $\alpha^2 = (\sqrt{2}+\sqrt{3})^2 = 2+3+\sqrt{6} = 5+\sqrt{6}$

and thus $\alpha^2 - 5 = \sqrt{6}$

$$\Rightarrow (\alpha^2-5)^2 = 6 .$$

So $f(x) = (x^2-5)^2-6$ is a monic, degree 4 polynomial that kills α. Is this the minimal one?

Yes because $1, \sqrt{2}+\sqrt{3}, 5+\sqrt{6}, \alpha^3 = 4\sqrt{3}+6\sqrt{2}$ is linearly independent (Exercise: Use the following theorem to prove this!)

Thm The set $\{\sqrt{n} : n \in \mathbb{Z}-\{0\} \text{ square-free}\}$ is linearly independent over $\mathbb{Q}$.

- $n \in \mathbb{Z}$ is square-free if the only square dividing n is 1
- linear independence means if $a_1\sqrt{n_1} + \dots + a_k\sqrt{n_k} = 0$ then $a_1 = \dots = a_k = 0$.

Ex $\text{span}_{\mathbb{Q}}\{\sqrt{-2}, \sqrt{2}, \sqrt{14}\} \subseteq \mathbb{C}$ is 3-dimensional over $\mathbb{Q}$.

Finally lets end by proving that every polynomial factors completely in some field extension: