Thm: If K/F, $K=F(\alpha_1,\dots,\alpha_m)$, then any element $\sigma\in \mathrm{Aut}(K/F)$ is uniquely determined by $\sigma(\alpha_1),\dots,\sigma(\alpha_m)$.

Pf: Every element $\alpha\in K$ can be written as

$$\alpha=\frac{f(\alpha_1,\dots,\alpha_m)}{g(\alpha_1,\dots,\alpha_m)},\quad \text{for some } f,g\in F[x_1,\dots,x_m].$$

Write $f(x_1,\dots,x_m)=\sum_{i=1}^{m} a_i\, x_1^{k_{i1}} x_2^{k_{i2}}\cdots x_m^{k_{im}}$, $a_i\in F$

Then

$$\sigma(f(\alpha_1,\dots,\alpha_m)) = \sum_{i=1}^{m}\sigma(a_i)\,\sigma(\alpha_1)^{k_{i1}}\cdots\sigma(\alpha_m)^{k_{im}}$$

σ is an aut.

$$= \sum_{i=1}^{m} a_i\,\sigma(\alpha_1)^{k_{i1}}\cdots\sigma(\alpha_m)^{k_{im}}.$$

σ fixes F

Similarly for g, and then the result follows. ▣

Thm: Suppose K/F and $\alpha\in K$ is algebraic over F. If $f(x)=\min_F(\alpha)$ and if $\sigma\in\mathrm{Aut}(K/F)$ then $f(\sigma(\alpha))=0$.

Pf: Write $f(x)=\sum_{i=0}^{n} a_i x^i$, $a_i\in F$. Then

$$f(\sigma(\alpha)) = \sum_{i=1}^{n} a_i\cdot\sigma(\alpha)^i = \sum_{i=0}^{n}\sigma(a_i\alpha^i) = \sigma(f(\alpha)) = \sigma(0)=0. \ ▣$$

$a_i=\sigma(a_i)$, since σ fixes F

Exs: 1) $K=\mathbb{Q}(\sqrt{2})$, $F=\mathbb{Q}$. $(\mathrm{Aut}(K/\mathbb{Q})=\mathrm{Aut}(K))$

Every element $\sigma\in\mathrm{Aut}(K/F)$ is determined by $\sigma(\sqrt{2})$

Since $\min_{\mathbb{Q}}(\sqrt{2})=x^2-2$, there are two possibilities:

$(\sigma:\sqrt{2}\mapsto\sqrt{2})$ $\qquad$ $(\sigma:\sqrt{2}\mapsto-\sqrt{2})$

(identity map) $\qquad$ ... can show that this to an autom. of K.

$(a+b\sqrt{2}\to a-b\sqrt{2})$

So $\mathrm{Aut}(K/F)\cong C_2$.

2) $K=\mathbb{Q}(\sqrt[3]{2})\subseteq\mathbb{R}\subseteq\mathbb{C}$, $F=\mathbb{Q}$.

$\sigma\in\mathrm{Aut}(K/\mathbb{Q})$ is uniquely determined by $\sigma(\sqrt[3]{2})$

" $\mathrm{Aut}(K)$

Since $\min_{\mathbb{Q}}(\sqrt[3]{2})=x^3-2=(x-2^{1/3})(x-\zeta_3 2^{1/3})(x-\zeta_3^2 2^{1/3})$,

there are 3 possibilities:

$\sigma:\sqrt[3]{2}\mapsto\sqrt[3]{2}$ $\qquad$ $\sigma:\sqrt[3]{2}\mapsto\zeta_3 2^{1/3}$ $\qquad$ $\sigma:\sqrt[3]{2}\mapsto\zeta_3^2 2^{1/3}$

(identity) ✓

$\notin\mathbb{R}\implies$ these don't extend to autms. of K.

$\mathrm{Aut}(K/F)\cong C_1$.

Thm: If K/F is a finite separable ext. then

$$|\mathrm{Aut}(K/F)| \le [K:F].$$

Pf: By the Prim. Elem. Thm., $\exists \alpha \in K$ s.t. $K = F(\alpha)$.

Let $f = \min_F(\alpha)$. Then $\deg f = [K:F]$ (Kron. ++).

Any element $\sigma \in \mathrm{Aut}(K/F)$ is determined by $\sigma(\alpha)$, and $f(\sigma(\alpha)) = 0 \Rightarrow$ there are at most $\deg f = [K:F]$ possibilities. $\boxtimes$

Comment: It is actually true that for any finite extension K/F (even without the assumption of separability),

$$|\mathrm{Aut}(K/F)| \le [K:F].$$

Def: If K/F is a finite (degree) extension of fields and if $|\mathrm{Aut}(K/F)| = [K:F]$ then K/F is called a Galois extension, and $\mathrm{Aut}(K/F) = \mathrm{Gal}(K/F)$ is called the Galois group of the extension.