

Mid term topics: Ch. 13 & §14.1

Survey: do more proofs

Last time: $\text{Aut}(K/F)$ gp. of automs. of K fixing F

Today: Galois extn, Galois gp.

Eg. a) $K = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$. Let $\tau \in \text{Aut}(K/F)$.

Then

$$\tau(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\tau(\sqrt[3]{2}) + c(\tau(\sqrt[3]{2}))^2$$

depends only on $\tau(\sqrt[3]{2})$.

By Prop 2, $\tau(\sqrt[3]{2})$ is a root of $x^3 - 2$.

But $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, and $\sqrt[3]{2}$ is the only real root of $x^3 - 2$,

so $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, and $\tau = 1$.

Hence, $|\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$.

b) If $K = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$, then $\tau \in \text{Aut}(K/F)$ is det'd
by $\tau(\sqrt{2})$, which can be $\pm\sqrt{2}$. So $|\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2$.

Def: If $H \leq \text{Aut}(K)$ (or $H \subseteq \text{Aut}(K)$), the fixed field of H is

$$\text{Fix}(H) := \text{Fix}_K(H) = \{a \in K \mid \sigma a = a \forall \sigma \in H\}$$

Prop 3: This is a field

Pf: Let $h \in H$, $a, b \in \text{Fix}(H)$, so $h(a) = a$, $h(b) = b$.

Use fact that h is a homomorphism.

$$h(a \pm b) = h(a) \pm h(b) = a \pm b, \quad h(ab) = h(a)h(b) = ab, \quad h(a^{-1}) = h(a)^{-1} = a^{-1}.$$

Prop 4: (Inclusion reversal)

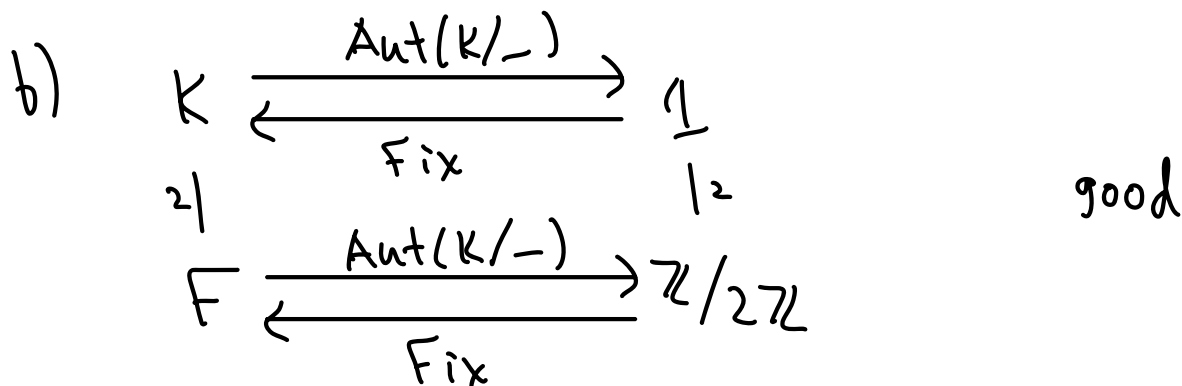
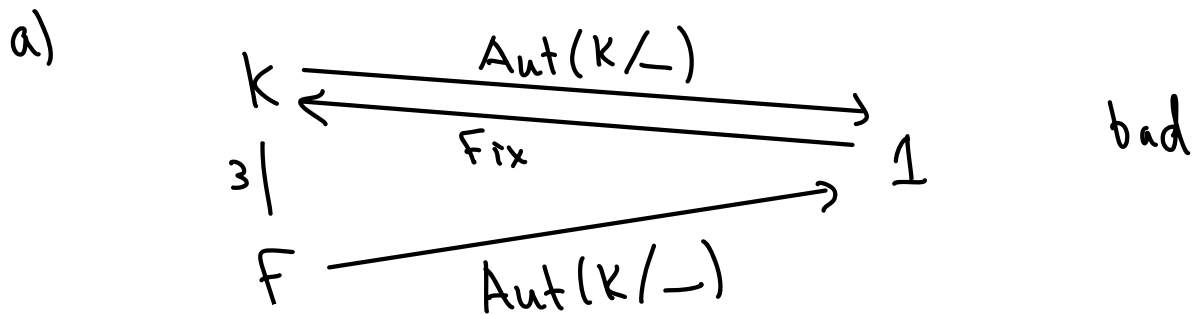
(a) If $F \subseteq E \subseteq K$, then $\text{Aut}(K/E) \leq \text{Aut}(K/F)$

(b) If $G \subseteq H \subseteq \text{Aut}(K)$, then $\text{Fix}_K(H) \subseteq \text{Fix}_K(G)$

Pf: a) Every autom. that fixes E fixes F since $F \subseteq E$

b) Every elt fixed by H is fixed by G since $G \subseteq H$.

E.g. (cont from above):



Prop 5: If K is the splitting field of $f(x) \in F[x]$, then

$$|\text{Aut}(K/F)| \leq [K:F]$$

Remark: holds for any finite field ext'n (Cor. 10)

Pf: Recall Thm 13.27:

Any isom. $F \xrightarrow{\varphi} F'$ extends to an isom. $K \xrightarrow{\sigma} K'$

where K is a splitting field of $f := \varphi(f)$ over F .

Claim: The number of such extensions is $\leq [K:F]$.

Result follows from claim since if $F = F'$,

$K = K'$, $\varphi = \varphi'$, $f = f'$, these ext'n's are precisely automs. of K fixing F .

Pf of claim: Induction on $[K:F]$. If $[K:F] = 1$, then $K = F$, so $K' = F'$, $\sigma = \varphi \cdot 1$ extension.

If $[K:F] > 1$, let $p(x)$ be an irred. factor of $f(x)$, $p' = \varphi(p)$. Let α be a root of $p(x)$, and let $\sigma: K \rightarrow K'$ be an isom. By Prop 2, $\beta := \varphi(\alpha)$ is a root of $p'(x)$. Thus, we have an isom.

$$F(\alpha) \xrightarrow{\tau} F(\beta).$$

$$\begin{array}{ccc}
 \sigma: E & \xrightarrow{\sim} & E' \\
 | & & | \\
 \tau: F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\
 | & & | \\
 \psi: F & \xrightarrow{\sim} & F'
 \end{array}$$

By Thms 13.8, 13.27, \exists such a Diag. for any root β of $p'(x)$. $|\{\text{roots of } p'\}| \leq \deg p' = [F(\alpha):F]$

Using the induction hypothesis and the field isom.

$F(\alpha) \xrightarrow{\sim} F(\beta)$, there are at most $[K:F(\alpha)]$ ext'ns of a given τ to σ , so there are at most

$$[K:F(\alpha)][F(\alpha):F] = [K:F]$$

ext'ns of ψ to σ . □

Cor: $|\text{Aut}(K/F)| \leq [K:F]$ precisely when f is separable.

Def: K is Galois over F if $|\text{Aut}(K/F)| = [K:F]$. When this holds, we define the Galois gp. $\text{Gal}(K/F) := \text{Aut}(K/F)$

Cor 6: If K is the splitting field $/F$ of a separable poly, then K/F is Galois

Def: If $f \in F[x]$ is separable, w/ splitting field K , then the Galois gp. of $f(x)$ is $\text{Gal}(K/F)$.

E.g.:

a) From above, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois, but $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not.

b) Let $F = \mathbb{Q}$ and let K be the splitting field of $x^3 - 2$

$$K = \mathbb{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \rho), \quad \rho = \rho_3 = e^{2\pi i/3}$$

Cor 6: K/F is Galois and $|\text{Gal}(K/F)| = [K:F] = 6$

$\sigma \in \text{Gal}(K/F)$ permutes the roots of $x^3 - 2$

equivalently, it sends $\sqrt[3]{2}$ to a root of $x^3 - 2$

and sends ρ to a prim. cube root of 1 i.e. to ρ or ρ^2

$$\text{Let } \sigma: \begin{cases} \sqrt[3]{2} \mapsto \rho\sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \quad \tau: \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \rho \mapsto \rho^2 = -1 - \rho \end{cases}$$

Write explicitly on basis:

$$\sigma: a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 + d\rho + e\rho\sqrt[3]{2} + f\rho(\sqrt[3]{2})^2$$

$$\mapsto a + b\rho\sqrt[3]{2} + c(-1-\rho)(\sqrt[3]{2})^2 + d\rho + e(-1-\rho)\sqrt[3]{2} + f(\sqrt[3]{2})^2$$

$$\sigma^3 = \tau^2 = 1$$

$$\sigma\tau: \begin{cases} \sqrt[3]{2} \xrightarrow{\tau} \sqrt[3]{2} \xrightarrow{\sigma} \rho \sqrt[3]{2} \\ \rho \xrightarrow{\tau} \rho^2 \xrightarrow{\sigma} \rho^2 \end{cases}$$

~~X~~

$$\tau\sigma: \begin{cases} \sqrt[3]{2} \xrightarrow{\sigma} \rho \sqrt[3]{2} \xrightarrow{\tau} \rho^2 \sqrt[3]{2} \\ \rho \xrightarrow{\sigma} \rho \xrightarrow{\tau} \rho^2 \end{cases}$$

$$\text{So } \text{Gal}(K/F) \cong S_3$$