

Midterm Wed 2/8 7-9 pm in 200-205 (here!)

H/w 4 posted

Fill out midterm feedback form

Thm 41: $\Phi_n(x)$ is an irred, monic poly in $\mathbb{Z}[x]$ of deg. $\varphi(n)$

Irreducible: Suppose not, and let

$$\Phi_n(x) = f(x)g(x), \quad f, g \text{ monic in } \mathbb{Z}[x], f \text{ irred.}$$

Claim: If p is any prime w/ $p \nmid n$, then ζ_n^p is a root of f .

This implies that every prim. n th root of ζ is a root of f , so $\Phi_n = f$ is irred.

PF of claim: Suppose $g(\zeta^p) = 0$. ($\zeta := \zeta_n$)

Then $f(x) \mid g(x^p)$, say:

$$g(x^p) = f(x)h(x), \quad h(x) \in \mathbb{Z}[x]$$

Reduce mod p :

$$(\bar{g}(x))^p = \bar{g}(x^p) = \bar{f}(x)\bar{h}(x) \quad \text{in } \mathbb{F}_p[x]$$

↑
Frobenius

Since $\mathbb{F}_p[x]$ is a UFD, $\bar{f}(x)$ & $\bar{g}(x)$ have common factor, so $x^n - 1$ has a multiple root over \mathbb{F}_p .

But, $\gcd(x^n - 1, D(x^n - 1)) = \gcd(x^n - 1, nx^{n-1}) = 1$
 $\neq 0 \text{ in } \mathbb{F}_p$
 Contradiction! \square

Remark: many proofs of irreducibility of Φ_n (see link on course website)

Cor. 42: $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

E.g.: $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \varphi(8) = 4$.

$$\zeta_8 = \frac{1}{\sqrt{2}}(1+i), \text{ so } \zeta_8^2 = i \text{ and } \zeta_8 + \zeta_8^7 = \sqrt{2}$$

Therefore, $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$

but $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$, so

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8)$$

Chapter 14: Galois Theory

§14.1: Basic Definitions

K/F : field ext'n

Let $\text{Aut}(K)$ be the set of automorphisms of K
(isoms. $K \xrightarrow{\sim} K$)

Def: $\sigma \in \text{Aut}(K)$ fixes $\alpha \in K$ if $\sigma\alpha = \alpha$.

σ fixes F if σ fixes every elt. of F ($\sigma a = a, a \in F$)

Let $\text{Aut}(K/F)$ be the subset of $\text{Aut}(K)$ fixing F .

E.g. Suppose F is the prime subfield of K . If $\sigma \in \text{Aut}(K)$,
 σ fixes $\mathbb{1}$, so σ fixes F . Thus, $\text{Aut}(K) = \text{Aut}(K/F)$

Prop 1: $\text{Aut}(K)$ is a gp. under composition, and $\text{Aut}(K/F)$ is
a subgp.

Prop 2: Let $\alpha \in K$ be alg. / F w/ min'l poly $f(x)$.

If $\sigma \in \text{Aut}(K/F)$, $\sigma\alpha$ is also a root of $f(x)$.

Pf: Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$. Then

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0, \text{ so}$$

$$\begin{aligned}
0 = \sigma(0) &= \sigma(f(\alpha)) = \sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha)^{n-1} + \dots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\
&= \sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \dots + a_1\sigma(\alpha) + a_0 \quad \text{since } \sigma \text{ fixes } F \\
&= f(\sigma(\alpha))
\end{aligned}$$

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 $H \leq \text{Aut}(k)$), the fixed field of H is

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

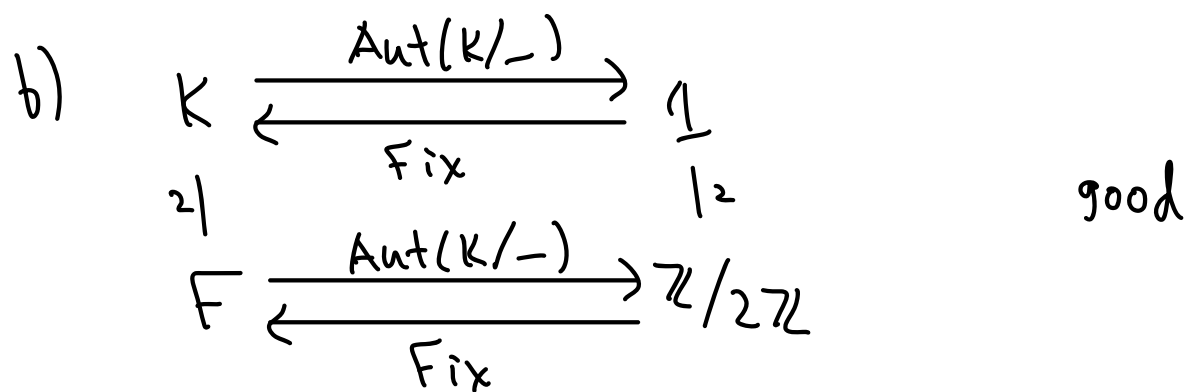
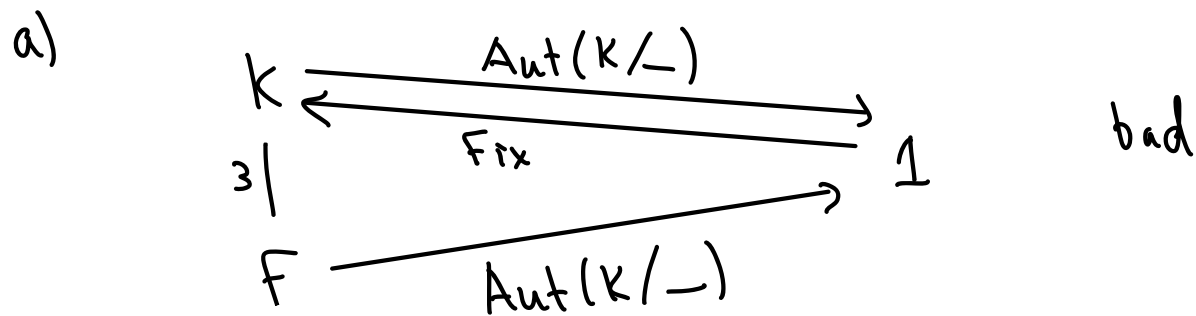
Prop 3: This is a field

Prop 4: (Inclusion reversal)

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

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

E.g. (cont from above):



Cor 10 (from next section): Let K/F be a finite ext'n.

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

Next time: prove case where K is a splitting field (Prop 5)

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