Midterm Wed 2/8 7-9pm 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

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

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

This implies that <u>every</u> prim. $n$th root of $1$ is a root of $f$, so $\Phi_n = f$ is irred.

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

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

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

Reduce mod $p$:

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

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, $\gcd(x^n-1, D(x^n-1)) = \gcd(x^n-1, \overset{\neq 0 \text{ in } \mathbb{F}_p}{n} x^{n-1}) = 1$

Contradiction! $\square$

Remark: many proofs of irreducibility of $\Phi_n$ (see link on course website)

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

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

$\zeta_8 = \frac{1}{\sqrt{2}}(1+i)$, so $\zeta_8^2 = i$ 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 $\mathrm{Aut}(K)$ be the set of automorphisms of $K$
(isoms. $K \xrightarrow{\sim} K$)

Def: $\sigma \in \mathrm{Aut}(K)$ <u>fixes</u> $\alpha \in K$ if $\sigma\alpha = \alpha$.
$\sigma$ fixes $F$ if $\sigma$ fixes every elt. of $F$ ($\sigma a = a$, $a \in F$)

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

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

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

Prop 2: Let $\alpha \in K$ be alg. $/F$ w/ min'l poly $f(x)$.
If $\sigma \in \mathrm{Aut}(K/F)$, $\sigma\alpha$ is also a root of $f(x)$.

Pf: Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then
$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, so

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

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

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

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

---

Def: If $H \leq \mathrm{Aut}(K)$ (or $H \subseteq \mathrm{Aut}(K)$), the <u>fixed</u> field of $H$ is

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

Prop 3: This is a field

Prop 4: (Inclusion reversal)

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

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

E.g. (cont from above):

a)

$$\begin{tikzcd} K \arrow[rr, shift left, "\mathrm{Aut}(K/\_)"] \arrow[d, dash, "3"'] & & 1 \arrow[ll, shift left, "\mathrm{Fix}"] \\ F \arrow[urr, "\mathrm{Aut}(K/\_)"'] & & \end{tikzcd}$$

bad

---

b)

$$\begin{tikzcd} K \arrow[r, shift left, "\mathrm{Aut}(K/\_)"] \arrow[d, dash, "2"'] & 1 \arrow[l, shift left, "\mathrm{Fix}"] \arrow[d, dash, "2"] \\ F \arrow[r, shift left, "\mathrm{Aut}(K/\_)"] & \mathbb{Z}/2\mathbb{Z} \arrow[l, shift left, "\mathrm{Fix}"] \end{tikzcd}$$

good

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

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

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

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