H/W 7 posted (due Tues. 3/14)

Final exam: Thurs. 3/23 8:30-11:30 Room 200-205 (see email)

§14.7: Insolvability of the Quintic

Recall: A finite group G is solvable if $\exists$

$$1 = G_s \triangleleft G_{s-1} \triangleleft \cdots \triangleleft G_0 = G$$

s.t. G_i / G_{i+1} is cyclic

Def: $f(x) \in F[x]$ can be solved by radicals if $\exists$

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = K$$

simple rad. ext'n

radical ext'n

s.t. $K_{i+1} = K(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$

Thm 39: Let $f(x) \in F[x]$ w/ char $F = 0$. Then $f(x)$ can be solved by radicals $\Leftrightarrow$ Gal(f) is solvable.

Cor 40: The general poly. of deg $n \geq 5$ is not solvable by radicals

Pf: S_n, $n \geq 5$ is not solvable since A_n is simple and not cyclic.

Def: K/F is cyclic if it is Galois and $\mathrm{Gal}(K/F)$ is cyclic

Prop 36/37: Suppose $\mu_n \subseteq F$, char $F \nmid n$.
Let K/F be an ext'n of degree dividing n.
Then,

$$K/F \text{ is cyclic} \iff K = F(\sqrt[n]{a}),\ a \in F$$

Pf: $\Leftarrow$: Since $\mu_n \subseteq F \subseteq K$ and $\sqrt[n]{a} \in K$, the poly. $x^n - a$ splits over K, so K/F is Galois.

$\sigma \in G := \mathrm{Gal}(K/F)$ is det'd by $\sigma(\sqrt[n]{a})$, which must equal $\zeta_\sigma \sqrt[n]{a}$ for some prim. nth root of unity ζ_σ.

Since $\mu_n \subseteq F$, all nth roots of 1 are fixed by G.
Hence, if $\sigma, \tau \in G$,

$$\sigma\tau(\sqrt[n]{a}) = \sigma(\zeta_\tau \sqrt[n]{a}) = \sigma(\zeta_\tau)\sigma(\sqrt[n]{a}) = \zeta_\sigma \zeta_\tau \sqrt[n]{a}.$$

This means that $\sigma \longmapsto \zeta_\sigma$

is an inj. hom. $G \longrightarrow \mu_n$.

μ_n is a cyclic gp. under multiplication, so G is cyclic.

$\Rightarrow$: Let $[K:F]=d \mid n$

Note: some n's have been changed to d's.

Def: $\alpha \in K$, $\zeta \in \mu_d$. Define the Lagrange resolvent:

$$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{d-1}\sigma^{d-1}(\alpha) \in K$$

Let $\langle \sigma \rangle = G := \mathrm{Gal}(K/F)$. Then,

$$\sigma(\alpha,\zeta) = \sigma\alpha + \zeta\sigma^2(\alpha) + \cdots + \zeta^{d-1}\alpha = \zeta^{-1}(\alpha,\zeta),$$

so $\sigma(\alpha,\zeta)^d = \zeta^{-d}(\alpha,\zeta)^d = (\alpha,\zeta)^d \leftarrow \in \mathrm{Fix}\, G = F$.

Now suppose ζ is a primitive dth root of 1.

By linear indep. of chars,

$\exists \alpha \in K$ s.t. $(\alpha,\zeta) \neq 0$. Then, $\sigma^i((\alpha,\zeta)) = \zeta^{-i}(\alpha,\zeta) \neq (\alpha,\zeta)$,

So no $\mathrm{Gal}(K/F((\alpha,\zeta))) = 1$, and so

$K = F((\alpha,\zeta)) = F(\sqrt[d]{a}) = F(\sqrt[n]{a^{n/d}})$ where $a := (\alpha,\zeta)^d \in F$. $\square$

Suppose char $F = 0$.

Lemma 38: Let K/F be a radical ext'n, $\alpha \in K$. Then α is contained in a radical Galois ext'n of F s.t. each intermediate ext'n is cyclic.

Pf: Can assume $\mu_{n_1}, \mu_{n_2}, \dots, \mu_{n_s} \subseteq F$ for any finite $n_1, \dots, n_s$ since $F(\mu_{n_1}, \dots, \mu_{n_s})$ is abelian; hence radical.

Claim: the composite of radical ext'ns is radical

Pf of claim:

$$F \subseteq K_1 \subseteq \dots \subseteq K_{s-1} \subseteq K$$

$$F \subseteq K_1' \subseteq \dots \subseteq K_{t-1}' \subseteq K'$$

$$F \subseteq K_1 \subseteq \dots \subseteq K \subseteq KK_1' \subseteq KK_2' \subseteq \dots \subseteq KK'$$

Let L = Galois closure of K/F. If $\sigma \in \mathrm{Gal}(L/F)$, apply σ to

$$F = K_0 \subseteq \dots \subseteq K_s = K, \quad K_{i+1} = K_i(\sqrt[n_i]{a_i})$$

$$F = \sigma K_0 \subseteq \sigma K_1 \subseteq \dots \subseteq \sigma K_s = \sigma K$$

$\sigma K_{i+1}/\sigma K_i$ is still simple radical since

$$\sigma K_{i+1} = \sigma K_i(\underbrace{\sigma(\sqrt[n_i]{a_i})}_{\substack{\text{root of} \\ x^n - \sigma(a_i) \in \sigma K_i}})$$

By claim, the composite of all σK, $\sigma \in Gal(L/F)$ is a rad. ext'n., and is Galois and contains α. $\square$

Pf of Thm 39: Let K be the splitting field of f.

$\Rightarrow$: By Lemma 38, every root of f is contained in a radical Galois ext'n s.t. every radical extn is cyclic, so the composite L is also such a field. Let

$$F \subseteq K_0 \subseteq \cdots \subseteq K_s = L, \quad K_{i+1} = K_i(\sqrt[n_i]{a_i})$$

$\Updownarrow$ Gal. corresp. $\quad K_{i+1}/K_i$ cyclic

$$Gal(L/F) = G_s \supseteq \cdots \supseteq G_0 = 1$$

Since $\mathrm{Gal}(K_{i+1}/K_i) = G_{i+1}/G_i$ cyclic, $\mathrm{Gal}(L/F)$ is solvable. Since K/F is Galois, $\mathrm{Gal}(K/F)$ is a quotient of $\mathrm{Gal}(L/F)$; hence solvable.

$\Leftarrow$: Let K be the splitting field for F.

$$\mathrm{Gal}(K/F) = G_s \supseteq \cdots \supseteq G_0 = 1 \qquad G_i/G_{i+1} \cong \mathbb{Z}/n_i\mathbb{Z}$$

$\Updownarrow$ Gal. corresp.

$$F = K_0 \subseteq \cdots \subseteq K_s = K \qquad K_{i+1}/K_i \text{ cyclic of deg } n_i$$

Let $F' = F(\zeta_{n_1}, \zeta_{n_2}, \dots, \zeta_{n_s})$

Then,

$$\underbrace{F \subseteq F'}_{\text{abelian}} = F'K_0 \subseteq F'K_1 \subseteq \underbrace{\cdots}_{\text{cyclic of deg dividing } n_i} \subseteq F'K_s = F'K$$

Since $\mu_{n_i} \subseteq F'K_i$, all these ext'ns are simple radical, so $F'K$ is radical. $\square$