Final exam: Thurs., 3/23 8:30-11:30AM Rm 200-205

Substitute proctor (Hunter Spink)

Covers entire course (§9.4, §13.1-6, §14.1-9)

Handwritten reference sheet allowed

(See Canvas announcement from 3/7)

Where do I go from here?

Math 122: Representation theory (Spr. '23, Spink)

Idea: "represent" arbitrary group as a group of matrices

Reduce problems in gp. theory to problems in linear alg.

Math 154: Algebraic number theory (Spr. '23, Conrad)

Study alg. ext'ns of $\mathbb{Q}$ in more ways besides Galois theory

Use to study Diophantine eqns.

Math 210 ABC: Graduate algebra (2023-24)

Like 120, but more material, more sophisticated

Partial list of topics

Basic tools: irreducibility, field ext'ns, degrees, splitting fields, min'l polys., linear alg. of field ext'ns, tower law

Constructability: 4 classical problems; type of ext'ns allowed

Separability: derivative criterion, sep./insep. degree

Galois theory:

- Compute automorphisms
- Characterizations of Galois ext'n (autom. gp. size, poly. splitting)
- Galois corresp. (including properties e.g. normal subgps.)
- Composites, intersections, subext'ns
- trace and norm (lie in base field)

Important cases:

- finite fields
- cyclotomic ext'ns
- abelian ext'ns
- infinite/transcendental ext'ns

Compute Galois gps:

- General poly. (symm. fns.)
- Discriminant: def, alt. gp. criterion
- compute Gal. gp. for deg 2, 3, 4
- reduction mod p (cycle type)

Solvability by radicals:

- Solvable Galois gp. criterion (Abel-Ruffini)
- Cardano's formula (don't need to memorize)

Example problems:

1) Let $F = \mathbb{F}_3(u)$, and let E/F be an ext'n of deg 7 such that E is a splitting field/F. Prove that E/F is separable.

Pf: By Tower Law, since 7 is prime E/F is simple, say $E = F(\alpha)$.

Then α is a root of an irred monic deg. 7 poly $f(x) \in F[x]$.

$f(x) = x^7 + \cdots$

$Df(x) = 7x^6 + \cdots = x^6 + \cdots \neq 0$

Since f is irred., $\gcd(f, Df) = f$ or 1, and since $\deg Df = 6 < 7$, $\gcd(f, Df) = 1$, so f is sep.

Therefore, E is the splitting field of a sep. poly.

Thus, E/F is Galois, so by D&F Thm 14.13, E/F is separable. $\square$

[Recall: splitting field of any (sep.) poly $\Leftrightarrow$ splitting field of every irred. (sep.) poly. over the base field w/ a root in the ext'n field]

2) D&F Ex 14.3.6: Let $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ w/ $D_1, D_2 \in \mathbb{Z}$, where $\theta = a + b\sqrt{D_1} + c\sqrt{D_2} + d\sqrt{D_1 D_2}$, $\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_1 D_2} \notin \mathbb{Z}$. Prove that $f(x) = m_{\theta, \mathbb{Q}}$ is irred of deg 4. over $\mathbb{Q}$, but is reducible modulo every prime p.

Pf: $[K:\mathbb{Q}]=4$ since $\sqrt{D_2} \notin \mathbb{Q}(\sqrt{D_1}) = \{a+b\sqrt{D_1} \mid a,b \in \mathbb{Q}\}$.

Thus, $f(x)$ must be irred. since θ is a prim. elt. by assumption

On the other hand, by the Theorem in D&F §14.8, the Galois gp. $G := Gal(\mathbb{F}_p(\sqrt{D_1},\sqrt{D_2})/\mathbb{F}_p)$ is a subgp. of $Gal(K/\mathbb{Q}) \cong V_4$ as long as p doesn't divide the discriminant D of f. Since $\mathbb{F}_p$ is a finite field, G is cyclic, and so it must have order ≤ 2 since it's a subgp. of V_4. This means there can't be a degree ≥ 3 poly. in $\mathbb{F}[x]$ w/ a root in $\mathbb{F}_p(\sqrt{D_1},\sqrt{D_2})$, so $f(x)$ must be reducible.

If $p \mid D$, then the discriminant $\overline{D}$ of $\overline{f}$ is 0, so $\overline{f}$ is not separable. Since $\mathbb{F}_p$ is perfect, every irred poly $\in \mathbb{F}_p[x]$ is separable, so $\overline{f}(x)$ is reducible. $\square$

3) a) Let K/F be a nontriv. Galois ext'n of odd order, and let $\alpha \in E \setminus F$.

Prove that $|\{\sigma \in Gal(K/F) \mid \sigma(\alpha) \neq \alpha\}| > |\{\sigma \in Gal(K/F) \mid \sigma(\alpha) = \alpha\}|$

Pf: Since K/F is Galois, $Gal(K/F(\alpha))$ is a proper subgp. of $Gal(K/F)$. Since $[K:F]$ is odd, so is $|Gal(K/F)|$, so every proper subgp has index ≥ 3. Therefore, the subset of $Gal(K/F)$ of automs. that fix α is at most $1/3$ of the total.

b) Give a nontriv. ext'n of odd order s.t.

$$|\{\sigma \in \mathrm{Aut}(K/F) \mid \sigma(\alpha) \neq \alpha\}| \leq |\{\sigma \in \mathrm{Aut}(K/F) \mid \sigma(\alpha) = \alpha\}|.$$

Ans: $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$

$\mathrm{Aut}(K/F) = 1$, so every autom. of K fixes $\alpha = \sqrt[3]{2}$.