# Introduction to Algebraic Information Theory for Quantitative Finance
# Homework 5

August 30, 2025

Timothy Tarter
James Madison University
Department of Mathematics

## Proving the Fundamental Theorem of Galois Theory

**Theorem:** Let L be a Galois extension of a field K, with finite degree $n$. (1) For all subfields E of L containing K, and for all subgroups H of $Gal(L : K)$,

$$\Phi(\Gamma(E)) = E \qquad \& \qquad \Gamma(\Phi(H)) = H. \tag{1}$$

(2) Also,

$$|\Gamma(E)| = [L : E] \qquad \& \qquad |Gal(L : K)|/|\Gamma(E)| = [E : K]. \tag{2}$$

(3) Finally, A subfield E is a normal extension of K iff $\Gamma(E) \triangleleft Gal(L : K)$. (4) If E is a normal extension, then $Gal(E : K) \simeq Gal(L : K)/\Gamma(E)$.

Prove the following in order - it proves the whole theorem:

1. Show that $|\Gamma(E)| = [L : E]$ (2.1). How does this prove (1)?
2. Use Theorem 3.3 and Corollary 7.29 in Howie to show (2.2), $|Gal(L : K)|/|\Gamma(E)| = [E : K]$.
3. Prove that $\Gamma(E) \triangleleft Gal(L : K)$.
4. Use FHT to show (4), that $Gal(E : K) \simeq Gal(L : K)/\Gamma(E)$ if E is a normal extension.

## Solvability of Groups

1. Show that $S_4$ is solvable.
2. Show that the alternating group, $A_5$, is simple. Why does that make $S_5$ not solvable? (Link to a reference for $A_5$: https://groupprops.subwiki.org/wiki/Alternating_group:A5).

3. Show that the Galois group of any monic irreducible polynomial of degree 5 is isomorphic to $S_5$. (Hint: pick arbitrary coefficients that make the polynomial irreducible. Don't torture yourself with abstraction - if it holds for one polynomial of degree 5, it holds for the general case.)

# What's It All About?

1. In class, we said that the core idea of Galois Theory to someone with a math background was that $\Phi$ and $\Gamma$ are mutually inverse if $L$ is a Galois Extension of $K$. What happens if it isn't?

2. Are there any theorems about quotient groups that make (2), (3), and (4) easier to understand from finite group theory?

3. Why do we care about the set equality in (1)? I.e., how does that tie the idea of $Gal(f)$ back to $Gal(L : K)$, as well as solvability of $f$?

4. When we say that Galois theory proves the insolvability of the general quintic equation by $S_5$ being a non-solvable group, we really mean that since $S_5$ isn't solvable, the Galois group of a degree 5 monic irreducible polynomial isn't solvable. How do we generalize this idea of polynomial solvability from $Gal(f)$ to $Gal(L : K) \simeq S_n$?

5. If someone were to ask you, "why should I learn abstract algebra?", what would your answer be? What have you learned in this course so far? What did you / didn't you expect? **Please be detailed here, it will help me teach better in the future.**

6. Do you have any course feedback? Also, are you okay with me posting your answer to this question as a reference for the course?