Math 250: Higher Algebra

Handout #1 (22 September 2004): Galois theory overview, part 1

As noted in Monday's handout, we shall base our development of Galois theory on the fourth chapter of Jacobson's *Basic Algebra*. But we shall not cover every part of this chapter at the same level of detail. Jacobson organizes his exposition as follows:

Introductory comments
4.1 Preliminaries on field extensions
4.2 Euclidean construction
4.3 Splitting fields
4.4 Multiple roots
4.5 The Galois group and fundamental Galois correspondence
4.6 Some results on finite groups
4.7 Galois' criterion for solvability by radicals
4.8 The Galois group as a group of permutation of the roots
4.9 The general n-th degree equation; symmetric functions
4.10 Polynomials over $\mathbf{Q}$ with Galois group S_n
4.11 Constructible regular n-gons; cyclotomic fields
[4.12 Transcendence of e and π, and the Lindemann-Weierstrass Theorem]
4.13 Finite fields
4.14 Special bases for finite-dimensional field extensions
4.15 Trace and norm, and the structure of cyclic extensions

The **boldfaced** sections are those that we will cover in detail, sometimes slightly updating Jacobson's terminology or approach. The other sections contain some results that we shall either mention briefly without proof, or skip entirely; generally these are the results that detail the application of Galois theory to the classical problems of geometry and algebra that were its initial impetus. In particular, we shall omit 4.12 entirely. Jacobson must have included this section so as to prove in one chapter the impossibility of all the classically unsolved construction problems; but the Lindemann-Weierstrass theorem, though a mathematical landmark, belongs in a different and more specialized branch of mathematics than the one we are pursuing here. This section does contain the important notions of integrality and integral closure, but we will have already introduced these ideas in their natural context of the preliminary Section 4.1.

Galois theory concerns the structure of solutions of polynomial equations. The development of the theory was motivated by some classical problems in Euclidean geometry (angle trisection, duplication of the cube, etc.) and algebra (solvability in radicals of general or specific polynomial equations). As often happens in mathematics, the original problems are now quite well understood, but meanwhile the theory they spawned has found many further applications both within and outside mathematics, and given rise to many new results and questions.

We quickly move from polynomial equations to field extensions E/F, and then via splitting fields to "normal" (equivalently "Galois") field extensions K/F (provided that E/F was "separable"[1]).

Let K/F be any field extension with $[K : F] < \infty$. The *Galois group* $\mathrm{Gal}(K/F)$ is defined to be the group of automorphisms of K that are the identity on F. We shall see that there are at most $[K : F]$ such automorphisms, and that equality holds if and only if every element of K fixed by $\mathrm{Gal}(K/F)$ is in F (that is, if $F = K^G$ where G is the Galois group). In this case we shall say that K/F *normal* or *Galois.* The fundamental result of Galois theory is the following correspondence between subgroups of the Galois group and subfields of K/F.

Fundamental theorem of Galois theory. *Let K/F be a normal field extension with Galois group G. Every subfield E of K that contains F is of the form K^H for some subgroup $H \subset G$, namely the subgroup of isomorphisms that fix every element of E. Moreover, E/F is normal if and only if H is a normal subgroup of G, in which case Gal(E/F) is canonically isomorphic with G/H.*

It follows that if E, E' are subfields associated with subgroups H, H' then $E \subseteq E'$ if and only if $H \supseteq H'$; that is, the lattice of subfields is isomorphic with the lattice of subgroups, with inclusions reversed.

In sections 4.1 through 4.5 we get from polynomials to field extensions to splitting fields to normal fields, and prove the fundamental theorem. In the remaining sections of this chapter we interpret G as a permutation group, obtain some results on finite groups that are relevant to Galois theory, and then apply these results and the fundamental theorem to study more general field extensions.

[1] We shall say more about this condition; for now we note that separability is automatic if F is either a field of characteristic zero or a finite field such as $\mathbf{Z}/p\mathbf{Z}$.