Galois Theory
TCU Graduate Student Seminar
George Gilbert
October 2015

The coefficients of a polynomial are symmetric functions of the roots $\{\alpha_i\}$:

$$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n,$$

where $s_1 = \sum \alpha_i$, $s_2 = \sum \alpha_i \alpha_j$, $\ldots$, $s_n = \alpha_1 \cdots \alpha_n$. Every symmetric polynomial in $\{\alpha_i\}$ is a polynomial in $\{s_i\}$.

An element that is algebraic over K is *separable* over K if its minimal polynomial has distinct roots. Since a root of f is a multiple root if and only if it is also a root of f'. For f irreducible, this implies $f' = 0$. Separability holds, in particular, for all elements algebraic over a field of characteristic 0 and over a finite field. An extension is *separable* if every element is separable, which holds if the elements of a generating set are separable. A finite extension L of K is separable if and only if there are $[L : K]$ isomorphisms of L into the algebraic closure $\bar{K}$ that fix K.

Theorem of the Primitive Element. If a finite extension L of K is separable, it is simple, i.e. $L = K(\alpha)$.

An algebraic extension L of K is *normal* if the minimal polynomial over K of every element of L splits over L. An extension is normal if and only if it is the splitting field of some set of polynomials.

An algebraic extension L of K is *Galois* if it is a separable, normal extension of K. Its group of automorphisms is the *Galois group* of L over K. A finite Galois group acts transitively on a generator of the extension. Thus, the Galois group may be realized naturally as a transitive subgroup of $S_{[L:K]}$.

Fundamental Theorem of Galois Theory (for finite extensions). Let L be a finite, Galois extension of K with Galois group G. Then there is a one-one correspondence between subgroups of G and subfields of L containing K. The subgroup H corresponds to the field L^H of elements of L fixed by H. The intermediate subfield M corresponds to the Galois group of L over M.

H is a normal subgroup if and only if L^H is a normal extension of K and the quotient group is then the Galois group.

My notes from the Graduate Student Seminar from a couple years back (http://faculty.tcu.edu/richardson/Prelims/GeorgeFields.pdf) list the transitive subgroups of S_4, go into more detail on polynomials and field extensions than I do here, and have some additional examples.

The Galois group may be expressed in abstractly in terms of known groups or by giving generators and relations or concretely as a subgroup of a permutation group. To compute a Galois group of a polynomial, first compute the degree of its splitting field. Then determine how the Galois group acts on the roots of this polynomial.

Example 1: Finite Fields. Write finite fields as $\mathbb{F}_{p^k}$ (not $\mathbb{Z}_p, \ldots$). Note that $\mathbb{F}_{p^k}$ is the set of roots of $x^{p^k} - x$. By counting, we see that the vector space dimension of $\mathbb{F}_{p^{nk}}$ over $\mathbb{F}_{p^k}$ is n. The Galois group is cyclic and generated by the Frobenius automorphism $x \mapsto x^{p^k}$ (just think about the solutions to $x^{p^{dk}} - x = 0$).

Example 2: What is the Galois group over $\mathbb{Q}$ of the splitting field of

$$\left(x^2 - 2\right)\left(x^2 - 3\right)?$$

The splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Exercise: For nonzero integers m and n, $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$ if and only if mn is a perfect square.

Thus, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. The Galois group G must be cyclic of order 4 or the Klein 4-group $C_2 \times C_2$. The former has only one subgroup of order 2, but the splitting field contains $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{6})$, so G must be the Klein 4-group.

The four elements of G are the automorphisms taking $\sqrt{2} \mapsto \pm\sqrt{2}$ and $\sqrt{3} \mapsto \pm\sqrt{3}$ (independently). This shows $\sqrt{2} + \sqrt{3}$ has four distinct conjugates, hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Example 3: What is the Galois group over $\mathbb{Q}$ of the splitting field of

$$\left(x^2 - 2\right)\left(x^2 - 3\right)\left(x^2 - 5\right)?$$

Is $\mathbb{Q}(\sqrt{5})$ contained in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$? If so, it would have to be one of $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, which it isn't. Thus, the splitting field has degree 8 over $\mathbb{Q}$. An automorphism is determined by the images of $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{5}$. All 8 possibilities must correspond to automorphisms and it follows that the Galois group is $C_2 \times C_2 \times C_2$.

Example 4: Cyclotomic Extensions of $\mathbb{Q}$. The nth cyclotomic polynomial Φ_n is the monic polynomial of degree $\phi(n)$ whose roots are the primitive nth roots of unity. It may be computed by dividing $x^n - 1$ by the cyclotomic polynomials for the proper factors of n, so, inductively, is a monic polynomial with integral coefficients.

Over $\mathbb{Q}$, if Φ_n were reducible, there would be a primitive nth root of unity ζ and a prime p not dividing n such that ζ and ζ^p are roots of different irreducible factors of Φ_n, say f and g, respectively. Because ζ is a root is of $g(x^p)$, it is divisible by $f(x)$. However, $g(x^p) \equiv [g(x)]^p \pmod{p}$, so that $f(x)$ and $g(x)$ would have a common root over $\mathbb{F}_p$. However, the derivative of $x^n - 1$ shows that, over $\mathbb{F}_p$, the nth roots of unity are distinct.

We see that primitive nth roots of unity are conjugate. For a primitive nth root of unity ζ and a an integer relatively prime to n, there is an automorphism taking ζ to ζ^a, which in turn determines the automorphism. It follows that the Galois group is isomorphic to $(\mathbb{Z}/(n\mathbb{Z}))^*$.

Remark. The Kronecker-Weber theorem shows that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

Example 5: Find the Galois group of the splitting field of $x^5 - 6$ over $\mathbb{Q}$.

The polynomial is irreducible by Eisenstein's criterion.

The roots are $\sqrt[5]{6}\,\zeta^k$, $k = 0, 1, 2, 3, 4$, where $\zeta = e^{2\pi i/5}$. The splitting field is $\mathbb{Q}(\sqrt[5]{6}, \zeta)$. Because $[\mathbb{Q}(\sqrt[5]{6}) : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$, we have $[\mathbb{Q}(\sqrt[5]{6}, \zeta) : \mathbb{Q}] = 20$. The Galois group has a normal subgroup of order 5, the Galois group of $\mathbb{Q}(\sqrt[5]{6}, \zeta)$ over $\mathbb{Q}(\zeta)$ with generator σ taking $\zeta \mapsto \zeta$, $\sqrt[5]{6} \mapsto \sqrt[5]{6}\,\zeta$. It also has a cyclic subgroup of order 4, the Galois group of $\mathbb{Q}(\sqrt[5]{6}, \zeta)$ over $\mathbb{Q}(\sqrt[5]{6})$ with generator τ taking $\sqrt[5]{6} \mapsto \sqrt[5]{6}$ and $\zeta \mapsto \zeta^2$. We know $\tau^{-1}\sigma\tau = \sigma^k$ for some $k = 1, 2, 3, 4$ and hence that it fixes ζ. It maps $\sqrt[5]{6}$ to $\sqrt[5]{6}\,\zeta^3$, so equals σ^3.

We can represent the Galois group as a subgroup of S_5 as

$$\langle (1, 2, 3, 4, 5), (1, 2, 4, 3) \rangle.$$

Example 6: Find the Galois group of the splitting field of $x^4 - \sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$.

If we knew that $Z[\sqrt{2}]$ were a principal ideal domain, we could conclude $x^4 - \sqrt{2}$ is irreducible by a straightforward generalization of Eisenstein's

criterion. Not assuming this, observe that

$$x^8 - 2 = \left(x^4 - \sqrt{2}\right)\left(x^4 + \sqrt{2}\right)$$

is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Thus,

$$8 = [\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2\,[\mathbb{Q}(\sqrt[8]{2} : \mathbb{Q}(\sqrt{2})].$$

Therefore, $[\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}(\sqrt{2})] = 4$, $x^4 - \sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt{2})$, and the Galois group is a transitive subgroup of S_4. We obtain the splitting field by adjoining the 4th roots of unity, i.e. by adjoining i, which clearly has degree 2 over the real field $\mathbb{Q}(\sqrt[8]{2})$. Thus, the spitting field has degree 8 over $\mathbb{Q}(\sqrt{2})$. There are three conjugate Sylow subgroups of S_4. They are isomorphic to the dihedral group D_8.

Explicitly, the Galois group is generated by the automorphism σ of order 4 that fixes i and takes $\sqrt[8]{2}$ to $\sqrt[8]{2}i$ and by complex conjugation, denoted say by τ. The orders are easily checked, as is the relation $\tau^{-1}\sigma\tau = \sigma^3$.

Example 7: Find the Galois group of the splitting field of $x^8 - \sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$.

As in Example 6, the polynomial is irreducible over $\mathbb{Q}(\sqrt{2})$, and hence $[\mathbb{Q}(\sqrt[16]{2}) : \mathbb{Q}(\sqrt{2})] = 8$. We obtain the splitting field by adjoining the 8th roots of unity.

None of the primitive 8th roots of unity lie in $\mathbb{Q}(\sqrt[16]{2})$, so the 8th cyclotomic polynomial ($\Phi_4(x) = x^4 + 1$) is either irreducible or factors into irreducible quadratics over $\mathbb{Q}(\sqrt[16]{2})$.Thus, the Galois group has order 16 or 32. More generally, if the Galois extension L of K is the compositum of M_1 and M_2, with M_2 Galois over K, then there is an injection of $\mathrm{Gal}(L, M_1) \hookrightarrow \mathrm{Gal}(M_2, K)$ so that $|\mathrm{Gal}(L, M_1)|$ divides $|\mathrm{Gal}(M_2, K)|$.

Two ways to see the degree is 2:

$$x^4 + 1 = (x^2 + 1)^2 - 2x^2 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1),$$

$$e^{2\pi i/8} = \cos(2\pi i/8) + i\sin(2\pi i/8) = \frac{1}{\sqrt{2}} + i\,\frac{1}{\sqrt{2}}.$$

Therefore, the Galois group is isomorphic to the dihedral group D_{16}, with details very similar to Example 6.

Example 8: The discriminant of a polynomial with roots $\alpha_1, \ldots, \alpha_n$ is defined to be

$$\prod_{i<j} (\alpha_i - \alpha_j)^2 .$$

Note that it is a test, even without the square, for whether the α_i are distinct. With the square, it is a symmetric polynomial in the α_i, so is a polynomial in the coefficients of the monic polynomial with roots $\alpha_1, \ldots, \alpha_n$.

Theorem. Suppose that $\alpha_1, \ldots, \alpha_n$ are the roots an a separable, irreducible polynomial over K. The discriminant is the square of an element of K if and only if the Galois group of $K(\alpha_1, \ldots, \alpha_n)$ over K is contained in the alternating group A_n.

Proof. It is easy to see that a transposition changes the sign of

$$\prod_{i<j} (\alpha_i - \alpha_j) .$$

This implies that A_n fixes this product, whereas any odd permutation changes its sign.

Example 9: Let $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ have Galois group $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Then G acts on α and its conjugates as a permutation group. Determine all possible subgroups of the symmetric group S_9 that could correspond to this action.

An element of order 3 in S_n is a product of 3-cycles. Because the Galois group has order 9 and is transitive on the 9 conjugates of α, it follows that every nontrivial element of G is the product of three 3-cycles. We may label the conjugates so that one such element is $\sigma = (1,2,3)(4,5,6)(7,8,9)$. The element τ of G that takes root 1 to root 4, must take root 4 to one of root 7, 8, or 9, or else $\sigma^k\tau$ would fix one of roots 1 to 6 for some $k = 1$ or 2. Relabeling roots 7, 8, 9 if necessary, we may assume $\tau = (1,4,7)(2,\ldots)(3,\ldots)$. From $\tau\sigma = \sigma\tau$, look at the images of roots 1, then 2, then 4, and finally 5, we conclude $\tau = (1,4,7)(2,5,8)(3,6,9)$. The only choices we made were in labelling the roots. Thus, any representation of the Galois group would simply be relabeling the roots, hence is a conjugate of $\langle \sigma, \tau \rangle$ by an element of S_n.