VIGRE Algebra QR Review, September 30, 2002

We will continue to meet in 3096 East Hall. Below is a summary of some field theory including some of the main theorems of Galois theory, followed by some new problems. Some are group theory while others involve Galois theory but should be attackable using the brief summary below.

A very brief summary of Galois theory

Consider a field K and a larger field L. Then the dimension of L as a K-vector space is called the *degree* of L over K, and is denoted $[L : K]$. It is the largest number of elements of L linearly independent over K, and it is the smallest number of elements of L needed to span L as K-vector space. It is finite if and only if L is finitely generated over K by elements algebraic over K, i.e., by elements that are roots of polynomial equations in one variable over K. If $[L : K]$ is finite then every element of L is algebraic over K, and L is called a *finite algebraic extension* of K. In that case, any intermediate field M is finite algebraic over K, and $[L : K] = [L : M][M : K]$.

Given an element θ of L algebraic over K, the polynomials $f(X)$ in $K[X]$ such that $f(\theta) = 0$ form an ideal: a generator for this ideal is called a *minimal polynomial* for the θ: it is an irreducible polynomial. If the minimal polynomial of θ over K has degree d, then $1, \theta, \ldots, \theta^i, \ldots, \theta^{d-1}$ is a K-vector space basis for $K[\theta] = L$ over d, and $[K[\theta] : K] = d$. It follows that the degree of the minimal polynomial of any element of a finite algebraic field extension L of K divides $[L : K]$. Note that if L is obtained from K by a finite sequence of field extensions of degree 2, then $[L : K]$ is a power of 2, and an irreducible cubic equation over K cannot have a root in L. This leads to a proof that a $60°$ angle cannot be trisected with ruler and compass.

Given a family of polynomials over K, one may construct a field containing and generated by all the roots of these polynomials. It is called the *splitting field* of the family of polynomials, and is unique up to non-unique isomorphism. A field that arises in this way is called a *normal extension* of K. If $K \subseteq L \subseteq M$ are fields and L is a normal algebraic extension of K, then L is mapped onto itself by every automorphism of M that fixes all the elements of K.

The splitting field associated with the set of all polynomials over K is called the *algebraic closure* of K. It has no strictly larger algebraic extension.

An element θ in an algebraic extension field L of K is called *separable* if its minimal polynomial has all distinct roots in the algebraic closure of K. The separable elements form a subfield of L, and L is called a *separable* algebraic extension of K if all of its elements are separable over K (it suffices if the elements in a set of field generators are separable over K). In characteristic 0, all algebraic extensions are separable, because the roots of an irreducible polynomial g are always distinct. (The formal derivative g' will be nonzero and satisfied by any multiple root, and then the GCD(g', g) gives a proper divisor of g other than 1, contradiciting its irreducibility.) In positive characteristic p, an irreducible polynomial has all distinct roots in an algebraic closure of K if and only some exponent h that occurs in a nonzero term of the polynomial is not divisible by p.

If a finite algebraic extension L of K is of the form $K[\theta]$ for one element θ of L, then θ is called a *primitive element* for L over K. The very important *theorem on the primitive element* asserts that every separable finite algebraic extension has a primitive element.

In characteristic $p > 0$, if a has no pth root in K, then $x^p - a$ is irreducible over K but all of its roots are equal. The splitting field is therefore not separable over K. An extension of K is called *purely inseparable* if every element has some p^eth power in K.

A field K of characteristic $p > 0$ is called *perfect* if it contains pth roots for all of its elements. Finite fields are perfect, as are algebraically closed fields. If a field is perfect, every algebraic extension is separable.

A finite separable normal algebraic extension L of K is called a *finite Galois* extension of K, and the group $G = \mathrm{Gal}\,(L/K)$, the *Galois group of* L *over* K, is defined as the group of all field automorphisms of L that fix every element of K (K-automorphisms). L may always be viewed as the splitting field of a finite set of polynomials, which may be taken to be irreducible, or as the splitting field of a single polynomial (their product). The elements of G automatically permute the finitely many roots of the finite set of polynomials, and the automorphism given by $g \in G$ is determined by this permutation of the roots, because the roots generate L over K. Thus, $G = \mathrm{Gal}\,(L/K)$ embeds in the permutation group of the roots. In this situation, the fundamental theorem of Galois theory, the *Galois correspondence* says the following:

(a) $|G| = [L : K]$.

(b) There is an order-reversing bijection between the fields F with $K \subseteq F \subseteq L$ and the subgroups H of G, under which F corresponds to $\mathrm{Gal}\,(L/F)$, and $H \subseteq G$ to $L^H = \{a \in L : h(a) = a \text{ for all } h \in H\}$. Note that $|\mathrm{Gal}\,(L/F)| = [L : F] = [L : K]/[F : K] = |G|/[F : K]$, so that the degree of the field corresponding to $H \subseteq G$ is the index of H in G.

(c) H is normal in G iff the corresponding field F is normal over K.

The Galois group of the splitting field of a polynomial f over K is also referred to as the *Galois group* of f over K. What is more:

Suppose that K has characteristic 0 for the rest of this discussion. Then the elements of L can be expressed in terms of those of K using only expressions formed using addition, subtraction, multiplication, division, and extraction of roots — these operations may be iterated — if and only if $G = \mathrm{Gal}\,(L/K)$ is a solvable group. Briefly said, solvability of an equation by radicals corresponds to solvability of its Galois group. Two facts that are important in the proof are first, that the splitting field of $x^n - 1 = 0$ has an abelian Galois group, and, second, that if $x^p - 1$ splits over K and $[L : K] = p$, a prime, then $L = K[a^{1/p}]$ for some element $a \in K$.

Galois theory implies that if a polynomial over a field of characteristic 0 has degree at most 4, then it can be "solved" by radicals, i.e., its roots can be expressed as described in the second sentence of the preceding paragraph, because all subgroups of S_n are solvable if $n \leq 4$.

Explicit examples show that there are equations of degree 5 over the rationals with Galois group A_5 or S_5, which are not solvable groups. Therefore, in general, fifth degree equations over the rationals cannot be solved by radicals.

Problems new this week

1. (Not a QR problem) Show that the only $\mathbb{Q}$-automorphism of $\mathbb{Q}[r]$, where r is the real cube root of 2, is the identity. (Failure of Galois theory for extensions that are not normal.)

2. (Not a QR problem) Let K be field of characteristic $p > 0$ and let L be a purely inseparable extension of K. Show that the only K-automorphism of L is the identity. (Failure of Galois theory without separability.)

3. Prove that A_6 (the alternating grouup in S_6) has no subgroup of order $72 = 6 \cdot 4 \cdot 3$. You may assume that A_6 is simple.

4. Find the splitting field K of the polynomial $x^4 - 7x^2 + 10$ over the field $\mathbb{Q}$ of rational numbers. Describe the Galois group G of K over $\mathbb{Q}$. Illustrate the fundamental correspondence of Galois theory in this example by finding all subgroups of G, all intermediate fields between $\mathbb{Q}$ and K, and describing their relationship. Which intermediate fields are normal extensions of $\mathbb{Q}$?

5. Consider the extension of fields $L = \mathbb{C}(X) \supseteq \mathbb{C}(X^2 + \dfrac{1}{X^2}) = K$, where X is a variable, and $\mathbb{C}(X)$ denotes the field of rational functions in X.

(a) Show that this is a Galois extension of degree 4, with Galois group $G = \mathrm{Gal}\,(L/K)$ generated by the two automorphisms σ and τ such that $\sigma(X) = -X$ and $\tau(X) = 1/X$.

(b) Find the minimal polynomial of X over K.

(c) Find explicitly all intermediate fields lying between L and K, and find the subgroup to which each corresponds under the Galoois correspondence.

6. (Not a QR problem) Show that for any prime integer $p > 0$, the symmetric group on p elements is generated by any pair of elements consisting of a 2-cycle and a p-cycle. Conclude that a free group on two or more elements cannot be solvable.

7. Find the Galois group of the splitting field of $f(x) = x^5 - 6x + 3$ over the field of rational numbers.

8. Let k be a perfect field of characteristic $p > 0$, and suppose that k is infinite (which is true, for example, if k is algebraically closed). Let x and y be algebraically independent variables over k, and let $K = k(x^p,\, y^p) \subseteq k(x, y) = L$. Show that L is purely inseparable finite algebraic over K of degree p^2. Show that as c varies in k, the intermediate fields $H_c = K(x + cy)$ are all distinct, so that there are infinitely many intermediate fields. (This illustrates another way in which Galois theory fails for purely inseparable extensions.)