Math 154: Course Summary

Rich Schwartz

September 26, 2009

General Information: M154 is a course in abstract algebra. It is the second half of the undergraduate algebra series 153-4. The core of M154 is Galois Theory, a subject that combines fields, polynomials and groups in a very beautiful way. Some people teach additional topics in M154, such as group representation theory, or elliptic curves. In this summary (which presumes you know about groups, polynomials, rings, and field) I will only discuss Galois Theory.

The Fundamental Theorem of Algebra: The Fundamental Theorem of Algebra says that every polynomial

$$P(z) = a_0 + a_1 z + ... + a_n z^n; \qquad a_0, .., a_n \in \boldsymbol{C}.$$

has a root in $\boldsymbol{C}$. The easiest proofs of this result use elementary facts from complex analysis and/or differential topology, rather than abstract algebra. While you may not see a proof of the Fundamental Theorem of Algebra in M154, it is nice to keep the result in mind for perspective.

Extension Fields: Let F be a field. An *extension field* of F is simply a field E such that $F \subset E$. Here are some examples.

- Let $F = \boldsymbol{R}$ the reals and $E = \boldsymbol{C}$, the complex numbers.
- Let $F = \boldsymbol{Q}$, the rationals, and let $E = \boldsymbol{Q}[\sqrt{2}]$, the field consisting of all expressions of the form $a + b\sqrt{2}$, where $a, b \in \boldsymbol{Q}$. Then E is an extension of F. In this example, it is actually a bit surprising that E is a field. The basic point is that

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

- More generally, $F = \boldsymbol{Q}$ and let $S \subset \boldsymbol{C}$. Let E consist of all elements of the form

$$\frac{\sum a_j s_j}{\sum b_j t_j}; \qquad a_j, b_t \in \boldsymbol{Q}; \qquad s_j, t_j \in S.$$

  These are supposed to be finite sums.

If E is an extension field of F, then E is naturally a vector space over F. In our first example $\{1, i\}$ serves as a basis for this vector space, because every element of $\boldsymbol{C}$ can be written as $x + iy$ for $x, y \in \boldsymbol{R}$. In the second example $\{1, \sqrt{2}\}$ serves as a basis. In the third example, the structure of the vector space depends on the set S.

Creating Roots: Let F be a field and let $P(x)$ be an irreducible polynomial with coefficients in F. This means that $P(x)$ does not factor into lower degree polynomals in the ring $F[x]$. Here $F[x]$ is the polynomial ring in a variable x. One of the first nontrivial constructions in M154 is the construction of an extension field E of F such that E contains a root of P.

Some remarks are in order. In case $F = \boldsymbol{Q}$, we can always take $E = \boldsymbol{C}$, by the Fundamental Theorem of Algebra. However, this approach has several shortcomings. First of all $\boldsymbol{C}$ is a giant field that contains all roots of all such polynomials. Second of all, F might be some other kind of field, like $\boldsymbol{Z}/p$, and then the Fundamental Theorem doesn't apply. In M154 you learn a uniform way of constructing a "minimal" extension field that contains a root of P that works for all fields.

Here is the construction. Let $I \subset F[x]$ denote the ideal consisting of all polynomals of the form $P(x)Q(x)$, where $P(x)$ is our initial polynomial and $Q(x)$ is allowed to vary. It turns out that I is a maximal ideal and that, therefore, the quotient $E = P(x)/I$ is a field.

Strictly speaking, E is not an extension field of F because F is not quite a subfield of E. However, there is an isomorphic copy of F contained in E. Namely, the map $a \to [a]$, the class of a, gives an embedding of F into E. We idenfify F with the copy of F sitting inside E. Let $\alpha = [x]$, the equivalence class of x. Since P has coefficients in F and now we have $F \subset E$, we can think of P as a polynomial with coefficients in E. We have $P(\alpha) = [P(x)]$. But $P(x) \in I$, so $[P(x)] = [0]$. In short α is a root of P. So, E is an extension field of F that contains a root of P.

Let $[E : F]$ denote the dimension of E, considered as a vector space over F. It turns out that

$$[E : F] = \text{degree}(P).$$

Letting α be a root of P, a basis for E over F is given by $\{1, \alpha, ..., \alpha^{d-1}\}$, where d is the degree of P.

Associating a Group: Let E be an extension field of F. We let $G(E, F)$ denote the set of all field automorphisms $\tau : E \to E$ such that that $\tau(a) = a$ for all $a \in F$. We can compose two such isomorphisms and get another one. This makes $G(E, F)$ into a group. Here are a few examples.

- If $F = \boldsymbol{Q}$ and $E = \boldsymbol{Q}[\sqrt{2}]$ then $G(E, F) = \{\iota, \tau\}$. Here ι is the identity map and $\tau(a + b\sqrt{2}) = a - b\sqrt{2}$. This $G(E, F)$ is isomorphic to $\boldsymbol{Z}/2$.

- Let $F = \boldsymbol{Q}$ and ω be a primitive nth root of unity. Then the map $\tau(\omega) = \omega^d$ extends to an automorphism of E provided that d is relatively prime to n. In this case $G(E, F)$ is isomorphic to $(\boldsymbol{Z}/n)_*$, the multiplicative group associated to $\boldsymbol{Z}/n$.

- Let $\overline{\boldsymbol{Q}}$ denote the field consisting of all algebraic numbers. An *algebraic number* is the root of some polynomial in $\boldsymbol{Q}[x]$. The infinite group $G(\boldsymbol{Q}, \overline{\boldsymbol{Q}})$, known as the *absolute Galois group*, is one of the deepest groups in all of mathematics.

Splitting Fields: Let F be a field and let P be a polynomial with coefficients in F. One can construct a field E that contains all the roots of P, in the sense that P splits into linear factors when considered as an element of $E[x]$. The idea is simply to iterate the construction we gave above. We let $E_0 = F$. In general, we factor P into irreducible polynomials in $E_k[x]$ and then let E_{k+1} be an extension of E_k that contains a root of one of the irreducible pieces we have just found. This procedure stops in a finite number of steps.

E is called a *splitting field* for P if P factors into linear factors in $E[x]$, but no proper subfield E' of E has this property. To construct a splitting field, we first find some field extension in which P factors into linear factors, and then we take a minimal subfield that has this property.

One of the beautiful results in M154 is that any two splitting fields for the same pair (F, P) are isomorphic as fields. Thus, the splitting field is unique. If turns out that $[E : F] \leq n!$, where n is the degree of P and E is the splitting field.

The Galois Group: Let F be a field, and let P be a polynomial in $F[x]$. Let E be the splitting field for (F, P). The group $G(E, F)$ is known as the *Galois group* of P. This group acts on E in such a way as to fix F and permute the roots of E.

An *intermediate field* (relative to E and F) is a field K such that

$$F \subset K \subset E.$$

We can convert back and forth between subgroups of the Galois group and intermediate fields.

- To the field K we associate the subgroup $G(E, K)$ of field automorphisms of E that fix all element of K.
- To the subgroup $H \subset G(E, F)$ we associate the field K such that every element of H fixes every element of K. This field K is called the *fixed field* of H.

Beautifully, this sets up a bijective correspondence between subgroups of the Galois group and intermediate field extensions. This correspondence is known as the *Galois correspondence*.

Normal Extensions and Normal Subgroups: A field extension K of F is called *normal* if F is precisely the fixed field of $G(F, K)$. It turns out that K is a normal extension of F if and only if K is the splitting field for some polynomial in F.

Referring to the Galois correspondence, it turns out that $G(K, E)$ is normal in $G(F, E)$ if and only K is a normal extension of F. In this case, the quotient group $G(F, E)/G(K, E)$ is isomorphic to $G(F, K)$. Thus, the Galois correspondence pairs up normal subgroups of the Galois group with intermediate fields that are normal extensions of F.

Solvability by Radicals: A group G is called *solvable* if there is a sequence of subgroups $G_n \subset G_{n-1} \subset ... \subset G_0 = G$ such that G_k is normal in G_{k-1} for all k and G_{k-1}/G_k is abelian for all k. Let S_n denote the permutation group on n letters. It turns out that S_n is a solvable group if and only if $n \leq 4$.

At the same time, a polynomal $P(x) \in \boldsymbol{Q}[x]$ is said to be *solvable by radicals* if one can produce all roots of P just by considering iterated kth roots. Such a root might look like

$$\sqrt{\frac{1+(7)^{1/3}}{19^{1/5}}+1}.$$

If $P(x)$ has degree 2, then the quadratic formula gives us the roots of P in these terms. There are similar formulas in the case when P has degree 3 and 4, but they are much more complicated. In any case, P is solvable by radicals provided that $\deg(P) \leq 4$.

One of the great results proved in M154 is that P is solvable by radicals if and only if its Galois group is a solvable group. It is easy to produce quintic polynomials (meaning degree 5) having S_5 as Galois group. Such polynomials are not solvable by radicals, by the theorem we just mentioned. This famous "unsolvability result" dashed the longstanding hope that there were formulas like the quadratic formula that worked in any degree.

Ruler and Compass Constructions: One of the ancient problems in geometry is the question of which figures can be constructed with a ruler and a compass. A ruler allows you to draw straight lines, and also to copy line segments that have already been drawn. A compass allows you to draw circles.

Suppose you start with the points $(x_1, y_1), ..., (x_n, y_n)$ marked in the plane. Let F be the field $\boldsymbol{Q}(x_1, y_1, ..., x_n, y_n)$, the smallest field containing both $\boldsymbol{Q}$ and all these coordinates. It turns out that you can construct the point (x, y) if and only if both x and y lie in a field extension E of F such that $[E : F]$ is a power of 2. The basic idea here is that one step of a ruler and compass construction allows you to take square roots and rational combinations of coordinates of points you already have.

Using this basic result, you can show that various constructions are impossible. For instance, it is impossible to trisect an angle, because this construction involves a degree 3 field extension of the relevant fields. You can also use the basic result to show that various constructions are possible. For instance, you can establish Gauss's famous theorem that it is possible to construct a regular 17-gon.

Finite Fields: Another application of Galois Theory is the complete classification of finite fields. It turns out that a finite field has order p^n for some

prime p and some $n \geq 1$. Moreover, there is a unique field of this order, up to isomorphism. To construct the field $F(p, n)$ of this order, we consider the splitting field of the polynomial

$$P(x) = x^{p^n} - x$$

over $F = \boldsymbol{Z}/p$. It turns out that this splitting field has order p^n. Conversely, we recognize and such field of order p^n as the splitting field for this particular polynomial over $\boldsymbol{Z}/p$. This gives the existence and uniqueness.

There is more to say about the structure of finite fields. For instance, the group of nonzero elements is cyclic. That is, there is a single element a such that every nonzero element is a power of a.