Math 153: Course Summary

Rich Schwartz

October 13, 2009

General Information: Math 153, *Abstract Algebra*, is a course on algebraic structures. In some ways, Math 153 is an easy course and in some ways it is a hard course. It is easy in that it does not require much background information. The course generally starts from scratch, assuming very little previous mathematics. The course is hard in that the material is rather different from what most people have seen in other classes. The course is also difficult in that the students are required to do a lot of proofs. A typical book for this course would be I.N. Herstein's *Topics in Algebra*.

Algebraic Structures: The basic idea of an algebraic structure is that you have a set, together with some relations between the elements in the set. One place where you have probably seen an algebraic structure before is in linear algebra, where you encountered *vector spaces*. In Math 153, the three basic structures considered are *groups*, *rings*, and *fields*. The course introduces each of these basic objects, and then proves various theorems about them.

Groups A *group* is a set G, together with a single operation. This operation is often denoted by $*$. So, if $a, b \in G$, then $a * b \in G$ as well. The operation obeys several axioms, namely:

- $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
- There is a unique element $e \in G$ such that $e * a = a * e = a$.
- For any $a \in G$ there is a unique $b \in G$ such that $a * b = b * a = e$.

These axioms at first might seem arbitrary, but some examples show that they are quite ubiquitous in mathematics. Here are some examples.

- $G = \boldsymbol{Z}$, the integers, and $* = +$, addition. In this case $e = 0$.

- $G = S^1$ the unit complex numbers, $*$ is multiplication, and $e = 1$. (A unit complex number is a complex number $x+iy$ such that $x^2+y^2 = 1$.) In this case, given $a = x + iy \in S^1$, the element $b = \overline{a} = x - iy$ (the conjugate of a) is such that $ab = ba = 1$.

- G is the group of symmetries of a cube – all the different ways of picking up a cube and putting it back down so that it occupies the same space. In this case, $(*)$ is the composition of symmetries. If you have a symmetry a and a symmetry b, the symmetry $a * b$ means "first do a and then do b". The element e is just the symmetry that does nothing.

- The group of moves one can make on Rubik's cube.

- $G = \boldsymbol{Z}/p$, the group of hours on a clock with p hours. Here $*$ is addition. For instance, $5 + 9 = 3$ in $\boldsymbol{Z}/11$, because 5 hours after 9-oclock is 3-oclock on a clock with 11 hours.

- When p is prime, the nonzero hours of $\boldsymbol{Z}/p$ form a group, with $*$ being multiplication. This group is called $(\boldsymbol{Z}/p)_*$. For instance $3 * 5 = 4$ in $(\boldsymbol{Z}/11)_*$ because $3 * 5 = 15$, and then $15 = 4$ in $\boldsymbol{Z}/11$. In this case $e = 1$.

Once a group is defined, one studies its structure. I'll explain the (usually) first nontrivial structure theorem that arises in M 153. Given a group G and an element $a \in G$, define $a^2 = a * a$ and $a^3 = a * a^2$, etc.

Theorem 0.1 *Let G be a finite group – that is, a group with finitely many elements – having N elements. For any $a \in G$ there is some n such that $a^n = e$ and n divides N. In particular, $a^N = e$.*

This structure theorem has some interesting consequences when done in particular cases. The group $G = (\boldsymbol{Z}/p)_*$ has $p - 1$ elements, That means that n^{p-1} is 1 in G. Put another way, this means that $n^{p-1} - 1$ is divisible by p. Let's try it out. If $p = 5$ and $n = 2$ then $2^4 - 1 = 15$. It works in this case. This simple corollary of the structure theorem is the beginning of a famous application in applied math: public key cryptography.

Here is a deeper example of a structure theorem.

Theorem 0.2 *Let G be a finite group with N elements. Let p be a prime number that divides N. Then $a^p = e$ for some $a \in G$.*

Not all the structure theorems have to do with taking powers of a single element. These are just the ones that I can explain without a big buildup of terminology.

Rings: A group G is called *abelian* if $a * b = b * a$ for all $a, b \in G$. In this case, $*$ is customarily denoted by $+$. A ring is a group R together with a second operation $\times$, that satisfies certain axioms.

- $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$.
- $a \times (b + c) = a \times b + a \times c$ for all $a, b, c \in R$.
- $(b + c) \times a = b \times a + c \times a$ for all $a, b, c \in R$.

Of course, $+$ has to satisfy the axioms for an abelian group. It's customary to use the letter R for rings, even though R counts as a group if we just forget the second operation. As with groups, the subject comes alive through its examples.

- The integers $\boldsymbol{Z}$ form a ring, with the operations being the usual addition and multiplication.
- $R = M_{n,n}(\boldsymbol{R})$, the ring of $n \times n$ matrices with real entries. Here $(+)$ is componentwise addition and $(\times)$ is the matrix multiplication that you learned in linear algebra or calc 3.
- $R = \boldsymbol{Z}[x]$, the ring of polynomnials in a variable x. A typical element of R has the form $a_0 + ... + a_n x^n$, where $a_0, ..., a_n$ are integers. These polynomials are added and multiplied as you learned in high-school algebra.
- R is the set of all complex numbers $a + bi$ where a, b are integers. Elements of R are added and multiplied as complex numbers.
- $R = \boldsymbol{R}[[x]]$, the ring of power series with real coefficients. When you learn Taylor series in calculus, the objects you construct are naturally elements of R.

Once rings are introduced, a number of structure theorems are proved about them. These theorems are not so easy to state concisely, but I'll give a couple number-theoretic consequences of the results about rings that get proved in Math 153:

- An odd positive prime p is the sum of two integer squares ($n = a^2 + b^2$) if and only if $p - 1$ is divisible by 4. For instance, the prime 607 is not the sum of 2 squares because 606 is not divisible by 4. On the other hand the prime 613 is the sum of two squares because 612 is divisible by 4. For instance $613 = 17^2 + 18^2$.

- Any positive integer is the sum of four integer squares.

Fields: An informal way to describe a field is that it is a ring in which multiplication commutes ($a \times b = b \times a$) and in which you can do division. Fields might be familiar from linear algebra. Here is a more formal definition of a field. Let R be a ring. Since R is an abelian group, there is an element e such that $e + a = a + e = a$ for all $a \in R$. This element is typically denoted by 0. Let R_* denote the set of all nonzero elements of R. Then R is called a field if R_* makes an abelian group relative to the operation $\times$.

An example may clarify this definition. Let R denote the set of real numbers, with the usual operations of addition and multiplication. Then R_* is the set of nonzero real numbers. Relative to $\times$, the number 1 plays the role of e, because $1 \times r = r \times 1 = r$ for all $r \in R_*$. Also, given any $a \in R_*$, we have $b = 1/a \in R_*$ as well, and $a \times b = b \times a = 1$. So, the set of real numbers forms a field. Here are some other examples of fields.

- $\boldsymbol{Q}$ the field of rational numbers.

- $\boldsymbol{C}$, the field of complex numbers.

- $\boldsymbol{Q}(\sqrt{2})$ the field of numbers of the form $a + b\sqrt{2}$, where $a, b \in \boldsymbol{Q}$.

- $\boldsymbol{R}(x)$, the field of real-valued rational functions. A typical element of $\boldsymbol{R}(x)$ has the form $P(x)/Q(x)$, where P and Q are polynomials with real coefficients.

Again, once fields are introduced, a number of structure theorems are proved. One of the most famous examples of a structure theorem for fields is as follows.

Theorem 0.3 *Suppose F is a finite field with N elements. Then $N = p^n$ where p is some prime. Moreover, for any number of the form p^n, there is a unique field F having exactly p^n elements.*

These finite fields have an amazing structure, and one of the goals of Math 153 is to explore it.

Overall, Math 153 tends to do somewhat less with fields than with groups and rings. Math 154 studies fields in much more detail. It turns out that there is a three-fold correspondence between fields, groups, and roots of polynomials that is known as Galois theory. Math 153 touches on Galois theory, and sets up some of the basic terminology, but Math 154 is the place where it comes up in detail.