13 ALGEBRAIC STRUCTURES

Groups, rings, and fields are familiar objects to us, we just haven't used those terms. Roughly, these are all sets of elements with additional structure (that is, various ways of combining elements to produce an element of the set). Studying this finer structure is the key to many deep facts in number theory.

Informal Definitions A GROUP is a set in which you can perform one operation (usually addition or multiplication mod n for us) with some nice properties. A RING is a set equipped with two operations, called addition and multiplication. A RING is a GROUP under addition and satisfies some of the properties of a group for multiplication. A FIELD is a GROUP under both addition and multiplication.

Definition 1. *A* **GROUP** *is a set G which is CLOSED under an operation $*$ (that is, for any $x, y \in G$, $x * y \in G$) and satisfies the following properties:*

(1) *Identity – There is an element e in G, such that for every $x \in G$, $e * x = x * e = x$.*
(2) *Inverse – For every x in G there is an element $y \in G$ such that $x * y = y * x = e$, where again e is the identity.*
(3) *Associativity – The following identity holds for every $x, y, z \in G$:*

$$x * (y * z) = (x * y) * z$$

Examples:

(1) $\mathbb{Z}/n\mathbb{Z}$, fancy notation for the integers mod n under addition. Let's see how this satisfies the axioms:
   (a) CLOSURE: Given any two integers mod n, their sum (via addition modulo n) is an integer mod n by definition. (Again, to be clear, the operation $*$ described above is addition modulo n.)
   (b) IDENTITY: 0 mod n is the identity element, since $a * 0$ means $a + 0$ mod n, which is clearly a mod n.
   (c) INVERSE: Given any a (mod n), we must find an inverse b so that $a * b = e$ in the group, i.e. $a + b \equiv 0 \pmod{n}$. The inverse to any a in this case is $n - a$.
   (d) ASSOCIATIVITY: The integers are associative, by basic rules of addition, so the integers mod n are also associative. That is, since

$$a + (b + c) = (a + b) + c, \quad \text{then it follows that} \quad a + (b + c) \equiv (a + b) + c \ (n)$$

(2) $(\mathbb{Z}/n\mathbb{Z})^\times$, more fancy notation for the integers mod n under multiplication. IMPORTANT: the elements of this set are NOT all integers mod n, but rather all integers RELATIVELY PRIME to n. See if you can show how these relatively prime elements form a group mod n and why including all integers mod n would not be a group (i.e. fails one or more of the axioms).

(3) $\mathbb{Z}$, the integers under addition. Groups don't have to be finite. Also note that you can't make the integers into a group under multiplication, since elements like 2 don't have a multiplicative inverse (i.e. an element y such that $2y = 1$, since $1/2$ isn't in the integers). But in Math 152, we mainly only care about examples of the type above.

A group is said to be "abelian" if $x * y = y * x$ for every $x, y \in G$. All of the examples above are abelian groups. The set of symmetries of an equilateral triangle forms a group of size 6 under composition of symmetries. It is the smallest group which is NOT abelian.

Definition 2. *A* **RING** *is a set R which is CLOSED under two operations $+$ and $\times$ and satisfying the following properties:*

(1) *R is an abelian group under $+$.*
(2) *Associativity of $\times$ – For every $a, b, c \in R$,*

$$a \times (b \times c) = (a \times b) \times c$$

(3) *Distributive Properties – For every $a, b, c \in R$ the following identities hold:*

$$a \times (b + c) = (a \times b) + (a \times c)$$

and

$$(b + c) \times a = b \times a + c \times a.$$

Examples:

(1) Both the examples $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}$ from before are also RINGS. Note that we don't require multiplicative inverses.
(2) $\mathbb{Z}[x]$, fancy notation for all polynomials with integer coefficients. Multiplication and addition is the usual multiplication and addition of polynomials.

Definition 3. *A* **FIELD** *is a set F which is closed under two operations $+$ and $\times$ such that*

(1) *F is an abelian group under $+$ and*
(2) *$F - \{0\}$ (the set F without the additive identity 0) is an abelian group under $\times$.*

Examples: $\mathbb{Z}/p\mathbb{Z}$ is a field, since $\mathbb{Z}/p\mathbb{Z}$ is an additive group and $(\mathbb{Z}/p\mathbb{Z}) - \{0\} = (\mathbb{Z}/p\mathbb{Z})^\times$ is a group under multiplication. Sometimes when we (or Cox) want to emphasize that $\mathbb{Z}/p\mathbb{Z}$ is a field, we use the notation $\mathbb{F}_p$. Other examples: $\mathbb{R}$, the set of real numbers, and $\mathbb{C}$, the set of complex numbers are both infinite fields. So is $\mathbb{Q}$, the set of rational numbers, but not $\mathbb{Z}$, the integers. (What fails?)

Another NON-Example: If n is not a prime, then $\mathbb{Z}/n\mathbb{Z}$ is not a field, since $(\mathbb{Z}/n\mathbb{Z}) - \{0\} \neq (\mathbb{Z}/n\mathbb{Z})^\times$. There are, in general, lots of other elements than 0 which are not relatively prime to n and hence have no inverse under multiplication.

The theory of these abstract structures is sometimes simpler than dealing with specific examples because we've pared down and listed all the essential properties that should be used in proofs. Here's a simple result from group theory (though we don't bother with the proof since there's already enough notation so far in this document):

Theorem 1 (Corollary to Lagrange's Theorem). *If $x \in G$, a group of size N, then $x^N = e$.*

In particular when $G = (\mathbb{Z}/p\mathbb{Z})^\times$, the group of integers which are non-zero mod p under multiplication, this implies Fermat's Little Theorem. Indeed, there are $p - 1$ elements in this group, so the above theorem implies that

$$x^{p-1} = e \quad \text{for all elements } x \text{ in } G$$

What does this equality mean in the group? The identity element is given by 1 mod p, and equality in this group means two numbers are congruent mod p. So this statement translates to:

$$x^{p-1} \equiv 1 \ (p) \text{for all elements } x \text{ which are non-zero mod } p$$

More generally, when $G = (\mathbb{Z}/n\mathbb{Z})^\times$, the group of integers mod n which are relatively prime to n (NOTICE: this generalizes the definition we made when $n = p$), we get a special case of the above theorem known as Euler's theorem. We denote the size of G by the number $\phi(n)$ and the statement

$$x^N = e$$

in the corollary to Lagrange's theorem similarly translates to (since e, the identity under multiplication, is 1 in this case)

$$x^{\phi(n)} \equiv 1 \ (\text{mod } n).$$

You might try investigating the properties of $\phi(n)$, the number of relatively prime integers to n mod n, by doing a few examples. Since divisibility is so important to us, this turns out to be a very important function.

Again, WHY do we ever need to consider groups?

Believe it or not, this added abstraction often makes problems easier. By reducing to a generic object defined by axioms, you can often see a clearer picture of what's going on (that is, what depends on what) and why. For example, working on arithmetic problems mod 11 all the time, you might be able to prove many things, and even guess a general picture, so working out these specific examples as we did for our proof of Fermat's Little Theorem is a good idea. However, you'll never see how far your theory extends unless you think about what makes the proof work and what axioms are essential to demonstrating its truth.