CLASS 19, GIVEN ON 11/03/2010, FOR MATH 25

1. Groups: definition

Even though we have been learning number theory without using any other parts of mathematics, in secret we have been doing a lot of abstract algebra. We make a brief digression to give some definitions from algebra which will be useful in describing what we will be doing next.

Consider a set G with a binary operation $\cdot : G \times G \to G$ satisfying the following properties:

- The operation $\cdot$ is *associative*: given any $g_1, g_2, g_3 \in G$, $(g_1 g_2)g_3 = g_1(g_2 g_3)$.
- The operation $\cdot$ has an identity: there exists a (unique) element $e \in G$ such that $g \cdot e = e \cdot g = g$ for all $g \in G$.
- Every element in G has an *inverse*: for all $g \in G$, there exists $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$.

Any set G with a binary operation $\cdot$ which satisfies the above three properties is called a *group*, and denoted $(G, \cdot)$, although frequently we will just write G, with the understanding that $\cdot$ is the binary operation defined on G.

There is a familiar property which is only satisfied by some groups: we say that G is *abelian* if $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$.

Examples.

- Familiar groups include $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$.
- Familiar sets with operations which are not groups are $(\mathbb{N}, +)$ and $(\mathbb{Z}, \cdot)$. Indeed, notice that $\mathbb{N}$ has no additive identity, while $\mathbb{Z}$ has a multiplicative identity (namely, 1), but most of its elements have no multiplicative inverses; for instance, 2 has no multiplicative inverse in $\mathbb{Z}$, since $2x = 1$ has no solutions in integers.
- Notice that $(\mathbb{Q}, \cdot)$ is not a group, because the element 0 has no multiplicative inverse. However, removing this element does give a group, and we write $\mathbb{Q}^*$ for the group of nonzero rationals under multiplication. Similarly, $\mathbb{R}^*, \mathbb{C}^*$ are groups.
- Recall that $\mathbb{Z}/n\mathbb{Z}$ is the set of congruences classes mod n. Under addition (of congruence classes), this also forms a group.
- Every example we have listed above is an abelian group. There are many groups of interest which are non-abelian (symmetry groups, permutation groups, matrix groups, for instance) which are important in mathematics and physics, but in this class we will not have to worry about these. The fact that we will only be interested in abelian groups reduces a lot of potential complications.
- $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ (multiplication of congruence classes mod n) is not a group, because certain elements (such as $0 \mod n$) have no multiplicative inverse. We saw that $(\mathbb{Q}, \cdot)$ was not a group, but removing the number 0 made it a group. Which elements do we have to remove from $\mathbb{Z}/n\mathbb{Z}$ to obtain a group under multiplication?

  In other words, we want to determine which $a \mod n$ have multiplicative inverses. Recall that we have already answered this question: precisely when a satisfies $\gcd(a, n) = 1$. We write $(\mathbb{Z}/n\mathbb{Z})^*$, or what the textbook writes as U_n, for the set of $a \mod n$ with $\gcd(a, n) = 1$ under multiplication of congruence classes. One can check that this actually is a group; in particular, you can check that this set is closed under multiplication. This is sometimes called the *unit group* mod n.

- When $n = p$ is prime, the unit group U_p consists of $1 \mod p, \ldots, (p-1) \mod p$, and has size $p - 1$.

2. Subgroups

Suppose we have a group G (not necessarily abelian, though you can assume this if you want). A subset of H is called a *subgroup* of G if $(H, \cdot)$ is itself a group, where $\cdot$ is the operation H inherits from G. In practice, if you want to check that H is a subgroup, there are three things to check: first, you need to check that $h_1 h_2 \in H$ is true for all $h_1, h_2 \in H$. This property is sometimes known as *closure*; notice that this does not appear in the definition of a group because it is built into the fact that the binary operation $\cdot$ maps $G \times G$ to G. You also need to check that $e \in H$, and that every element in H has an inverse. Notice that you already know $\cdot$ is associative on H because it is so on G.

Example. Consider the group $(\mathbb{Z}, +)$. We claim the set of even numbers is actually a subgroup of $\mathbb{Z}$. Indeed, notice that the sum of any two even numbers is still even, so closure is satisfied. The additive identity 0 is itself an even number, and finally, the additive inverse of an even number x is $-x$, which is still even.

Contrast this to the set of odd numbers. This is not a subgroup of $\mathbb{Z}$, because it is not closed and has no additive identity (although it is closed under additive inverses).

More generally, one can show that every subgroup of $(\mathbb{Z}, +)$ has the form $n\mathbb{Z}$ for some integer n, where $n\mathbb{Z}$ denotes the set of all integer multiples of n. A proof of this basically boils down to using Euclidean division!

Let G be an arbitrary group (not necessarily abelian), and let $g \in G$ be some element of G. Then the set of all powers, both positive, negative, as well as zero, of G is a subgroup of G, and is denoted $\langle g \rangle$. Indeed, notice that $g^0 = e$, so the identity is contained in $\langle g \rangle$. This set is also closed, since $g^{n_1} g^{n_2} = g^{n_1 + n_2}$. Finally, given any $g^n \in \langle g \rangle$, we also have $g^{-n} \in \langle g \rangle$, and $g^{-n} \cdot g^n = e$, so $\langle g \rangle$ is closed under inverses as well. We call $\langle g \rangle$ the cyclic (sub)group generated by g. Any group G which has the form $\langle g \rangle$ for some G is called a *cyclic group.*

Examples.

- Notice that cyclic groups can be either finite or infinite. Indeed, $(\mathbb{Z}, +)$ is a cyclic group, being generated by the element 1 (or the element -1). On the other hand, $\mathbb{Z}/n\mathbb{Z}$ is also cyclic, being generated by $1 \mod n$, but is of finite size.
- In contrast to $(\mathbb{Z}, +)$, groups like $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are not cyclic. For instance, given any $x \in \mathbb{Q}$, there is no way $\langle x \rangle = \mathbb{Q}$, because $\langle x \rangle$ consists of integer multiples of x, and so $x/2 \notin \langle x \rangle$, unless $x = 0$, but then $\langle x \rangle = \langle 0 \rangle$ consists of only one element.
- U_n may or may not be cyclic, depending on the value of n. Indeed, the main objective of the next week is to determine when U_n is cyclic. For now, consider the two examples U_5, U_8. Notice that U_5 is cyclic, because $2 \mod 5$ generates U_5: its powers are $2 \mod 5, 4 \mod 5, 8 \equiv 3 \mod 5, 16 \equiv 1 \mod 5$. On the other hand, U_8 is not cyclic: it consists of $1 \mod 8, 3 \mod 8, 5 \mod 8, 7 \mod 8$, but the squares of these elements are all $\equiv 1 \mod 8$, and so multiplying $a \mod 8$ (a odd) repeatedly by itself only gives the two elements $a \mod 8, 1 \mod 8$.

The *order* of an element $g \in G$ is defined as the smallest positive integer d such that $g^d = e$. If no such integer exists, then we say that g has infinite order. If you remember the definition of the order of a class $a \mod p$ given a few homework assignments ago, this new definition is compatible with the old homework definition.

Examples.

- In $(\mathbb{Z}, +)$, 0 has order 1, while every other element has infinite order.
- In $\mathbb{Z}/n\mathbb{Z}$, $1 \mod n$ has order n. More generally, $a \mod n$ has order equal to $n/(\gcd(a, n))$. You will show this on next week's homework assignment.
- In U_n, $1 \mod n$ has order 1. Be sure that the binary operation associated to a group is clear when you start talking about orders or other properties of the group.
- If an element $g \in G$ has order $d < \infty$, then $\langle g \rangle$ has size d. Indeed, if g has order d, then the d elements $e, g^1, \ldots, g^{d-1}$ are all not equal to e except for e itself. We claim that these are all distinct. If $g^i = g^j$, then $g^{i-j} = g^{j-i} = e$. But at least one of $i - j, j - i \geq 0$, and these are both $< d$, so this is only possible if $i = j$. Finally, any g^n is equal to one of the g^i in our list. Indeed, divide n with remainder by d to get $n = qd + r$, for some q, $0 \leq r < d$. Then $g^n = g^{qd+r} = g^{qd}g^r = e^q g^r = g^r$.
- Let's list the orders of the various elements in U_5. First, U_5 has 4 elements: $1 \mod 5, 2 \mod 5, 3 \mod 5, 4 \mod 5$. Clearly $1 \mod 5$ has order 1, being the multiplicative identity. $2 \mod 5$ and $3 \mod 5$ both have order 4, since their powers are $4 \mod 5, 8 \mod 5, 16 \equiv 1 \mod 5$ and $3 \mod 5, 9 \mod 5, 27 \mod 5$, and $81 \equiv 1 \mod 5$ respectively. Finally, $4 \mod 5$ has order 2, since $4^2 = 16 \equiv 1 \mod 5$.

The following theorem is of fundamental importance in elementary group theory. Recall that $|G|$ refers to the number of elements in G; when G is a group $|G|$ equals the number of elements in the set underlying that group.

Theorem 1 (Lagrange's Theorem)**.** *Let G be a finite group, and let H be a subgroup of G. Then $|H| \mid |G|$.*

We will not prove the theorem, although it is not hard, because its proof more properly lies in algebra than number theory. However, this theorem makes the proofs of various facts and theorems we have seen in this class trivial:

Examples.

- Recall the homework assignment which asked you to prove that the order of $a \mod p$ divides $p - 1$. The cyclic group generated by $a \mod p$ has size d (see the previous examples), and is a subgroup of U_p. As U_p has size $p-1$, this implies that $d|(p - 1)$. As a matter of fact, notice that this proves Fermat's Little Theorem as well, because if $a^d \equiv 1 \mod p$ and $d|(p - 1)$, then $a^{p-1} \equiv 1 \mod p$.
- Actually, Lagrange's Theorem instantly proves the Fermat-Euler theorem. We know that U_n has $\phi(n)$ elements. Given any $a \mod n$ with $\gcd(a, n) = 1$, the cyclic group generated by $a \mod n$ has order d, for some d. In particular, $a^d \equiv 1 \mod n$. On the other hand, Lagrange's Theorem says that $d \mid \phi(n)$, so $a^{\phi(n)} \equiv 1 \mod n$ as well.

3. Isomorphisms

Consider the group U_3. This consists of the two elements $1 \mod 3, 2 \mod 3$, and $2^2 \equiv 1 \mod 3$. On the other hand, consider the group $\mathbb{Z}/2\mathbb{Z}$. This consists of two elements, $0 \mod 2, 1 \mod 2$, and $1 + 1 \equiv 0 \mod 2$. In both cases, we have groups consisting of two elements, one of which is the identity, and the other which when added/multiplied by itself gave the identity. From the standpoint of their group structure, these groups seem identical. The names and operations look slightly different, but from the perspective of the relationship of the elements in each group to each other under their respective group operations, the groups are indistinguishable. We want to give this property a name.

Two groups G and G' are called *isomorphic* if there exists a bijective function $f : G \to G'$ such that $f(g_1g_2) = f(g_1)f(g_2)$ for all $g_1, g_2 \in G$. We call any such f an *isomorphism* of G with G'. Notice that the multiplication on the left hand side takes place in G, while the multiplication on the right hand side takes place in G'. (Recall that a bijection $f : G \to G'$ is a function for which given any $g' \in G$, there is exactly element $g \in G$ such that $f(g) = g'$.)

From the standpoint of group theory, isomorphic groups are indistinguishable. While we might think of $U_3, \mathbb{Z}/2\mathbb{Z}$ as being different, they are only so by virtue of the fact that we label their elements differently and use different group operations on them. But the actual relationships of the elements to each other under their respective group operations are identical.

Examples.

- We claim U_5 is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Indeed, consider the map which sends $2^n \mod 5$ to $n \mod 4$. First, this map is well-defined: if $2^n \equiv 2^m \mod 5$, then $2^{n-m} \equiv 1 \mod 5$, and because $2 \mod 5$ has order 4, this implies that $4 \mid (n-m)$, or equivalently that $n \equiv m \mod 4$.

  Next, this map is a bijection. This is clear because the four elements $2 \mod 5, 4 \mod 5, 8 \equiv 3 \mod 5, 16 \equiv 1 \mod 5$ are mapped to $1 \mod 4, 2 \mod 4, 3 \mod 4, 0 \mod 4$. Finally, $2^n 2^m \equiv 2^{n+m} \mod 5$ is mapped to $(n+m) \mod 4 = (n \mod 4) + (m \mod 4)$, so this map is an isomorphism.
- More generally, we claim that any cyclic group $\langle g \rangle$ is isomorphic to either $\mathbb{Z}/d\mathbb{Z}$, if $\langle g \rangle$ has order d, or $(\mathbb{Z}, +)$.

  Indeed, if $\langle g \rangle$ has order d, then one checks that the map $g^n \mapsto n \mod d$ is an isomorphism, while if $\langle g \rangle$ has infinite order, one checks that the map $g^n \mapsto n$ is an isomorphism.
- If G, G' are two groups, let $G \times G'$ be the group whose underlying set is the set of all ordered pairs (g, g') with $g \in G, g' \in G'$, and multiplication given by $(g_1, g_1')(g_2, g_2') = (g_1 g_1', g_2 g_2')$. One can check that this is indeed a group.

  We claim that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. One could write down an explicit isomorphism, but we will instead use the Chinese Remainder Theorem. Given any $(a \mod 2, b \mod 3) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, we know there exists a unique $c \mod 6$ such that $c \equiv a \mod 2, c \equiv b \mod 3$, by the CRT. We claim that the map $(a \mod 2, b \mod 3) \mapsto c \mod 6$ given by the CRT is an isomorphism. First, the CRT tells us that this map not only exists but is a bijection. To check that it is an isomorphism, we need only check that it preserves group operation.

  Suppose $(a \mod 2, b \mod 3)$ maps to $c \mod 6$, while $(a' \mod 2, b' \mod 3)$ maps to $c' \mod 6$. Then $(c + c') \equiv (a + a') \mod 2$, and $(c + c') \equiv (b + b') \mod 3$, so $(a + a' \mod 2, b + b' \mod 3)$ maps to $c + c' \mod 6$.

  As you probably have noticed, there was nothing in this example which used anything special about the numbers $2, 3$ other than the fact that we were able to apply the Chinese Remainder Theorem to $\mod 2$, $\mod 3$. So this example really shows that if m, n are relatively prime numbers, then $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is isomorphic to $\mathbb{Z}/nm\mathbb{Z}$.
- If $f : G \to G'$ is an isomorphism, then $g, f(g)$ have the same order. Indeed, $g^d = e$ if and only if $f(g^d) = f(g)^d = f(e) = e'$ (one checks that $f(e) = e'$). Therefore the smallest d which makes $g^d = e$ true is also the smallest d which makes $f(g)^d = e'$ true. A consequence of this fact is that isomorphic groups have the same number of elements of any given order. (The converse, however, is not true: it is possible for groups to have the same number of elements of each order and not be isomorphic.)

  In particular, this provides a method for determining when two groups are not isomorphic. For example, we can show that $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$, for any prime p. Indeed, notice the latter group has an element (actually, many elements) of order p^2, but the former has none: one easily sees that $p(a$

$\bmod p, b \bmod p) = (ap \bmod p, bp \bmod p) = (0 \bmod p, 0 \bmod p)$, so that every element of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ has order at most p, and therefore not p^2. As a consequence, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is not cyclic, because this group has order p^2 but is not isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$.

That was a lot of group theory in a short amount of time! Actually, it probably is not necessary to remember everything we talked about today, but we will use the language of groups a little for the remainder of the class, so knowing what a subgroup is, what a cyclic group is, and what the order of an element is.

The primary question we want to answer in the next week or two is determining when U_n is cyclic, and if so, how to find generators for this group, and how knowing generators helps us solve congruences. Based on today's brief tour of algebra, it is probably clear that algebra and number theory are quite close to each other.