Recitation 2: Group theory

6.5610, Spring 2023

February 17, 2023

1 Modular arithmetic

A modulus operator find the remainder after division. For example $19 \pmod 4 = 3$, because $19/4$ is 4 with remainder 3.

Suppose we want to do $5 * 5 \pmod 4$. We could do this as $5 * 5 = 25 = 24 + 1 = 1 \pmod 4$. However, we could also do this as $(4 + 1)(4 + 1) = 4 * 4 + 4 * 1 + 4 * 1 + 1 * 1$. Note that every term except the last is a multiple of 4. Therefore the remainder when we divide by 4 only comes from the last term, $1 * 1 = 1$.

So we can take the modulus operator first and still get the same answer – this is very useful. We can group the integers by their remainder from the modulus operator. Two numbers a and b are in the same group (called a residue class) if there difference is a multiple of the modulus.

Formally, $a \equiv b \pmod n$ if $n|(a - b)$, where the symbol $|$ indicates divisibility. So $1 \equiv 5 \pmod 4$ because 4 divides $5 - 1 = 4$.

2 Groups

A group is a set S equipped with an operation, commonly notated as addition with $+$, that satisfies the following properties:

1. The operation maps elements of the set into the set. Formally, for all $s_1, s_2 \in S$, $s_1 + s_2 \in S$.
2. There is an identity element, commonly notated 0. Formally, for all $s_1 \in S$, $s_1 + 0 = s_1$ and $0 + s_1 = s_1$.
3. Each element has an inverse. This means that there is another element that takes the result to the identity. Formally, for all $s_1 \in S$, there exists s_2 such that $s_1 + s_2 = 0$ and $s_2 + s_1 = 0$.
4. The order of operations does not matter (associativity). Formally, for all $s_1, s_2, s_3 \in S$, $(s_1 + s_2) + s_3 = s_1 + (s_2 + s_3)$.

2.1 Examples of groups

A common example of a group is the integers modulo n, for some number n. For example, let's consider the integers mod 4 with the operation of addition. There are 4 elements in the set S: $\{0, 1, 2, 3\}$. The operation of addition maps the elements in the following way:

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

This looks a lot like a multiplication table, and is referred to as a Cayley table for a group.

Is there another group with 4 elements?

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

This group is formed by the exclusive or operator on 2 bits.

We can notice some patterns about groups

- The element 0 appears in every row and column, because every element has an inverse.
- No value repeats in any row or column. Consider if it did then we would have $x + y_1 = x + y_2$, but this means $y_1 = y_2$.
- Every value appears in every row and column. As there are no repeats and only 4 values, they all must appear.

What other groups of 4 elements are there?

We can consider a group where we rotate a square. The group operation is to apply the rotations consecutively

	0	90	180	270
0	0	90	180	270
90	90	180	270	0
180	180	270	0	90
270	270	0	90	180

If this looks like a familiar pattern, you're right. This group is actually the same as Z_4, but all of the elements have different "names." This is called an isomporphism.

We can also consider the group made by reflections of a non-square rectangle. We can flip over the vertical, horizontal axis. To close the group, we also need to consider flipping over both axis.

	nothing	horizontal	vertical	both
nothing	nothing	horizontal	vertical	both
horizontal	horizontal	nothing	both	vertical
vertical	vertical	both	nothing	horizontal
both	both	vertical	horizontal	nothing

This group is isomorphic to the xor group we saw above. In fact, there are only 2 commutative groups with 4 elements. A commutative group is one where the operator also satisfies $a + b = b + a$. This can be proven precisely (the fundamental theorem of finite Abelian groups), but it has to do with the fact that 4 can only be factored as $4 * 1$ and $2 * 2$.

2.2 Generators, order

The behvaior of a group can be analyzed at looking at the order of the group elements. The order of an element is the number of times an element has to be added to itself to get the identity.

For example, in Z_4

- $0 = 0$, trivial
- $1 + 1 + 1 + 1 = 0$, order 4
- $2 + 2 = 0$, order 2
- $3 + 3 + 3 + 3 = 0$, order 4

In the xor group, which I will call K_4. Because of isomorphism, you can also call it D_2 or Z_2^2 and many other names.

- $00 = 00$, trivial
- $01 \oplus 01 = 00$, order 2
- $10 \oplus 10 = 00$, order 2
- $11 \oplus 11 = 11$, order 2

How do we know that an element eventually reaches the identity? Pigeonhole principle - if must eventually reach a duplicate element after $|S|$ additions. Let this duplicate element appear for the first time after k_1 and k_2 additions, where $k_1 < k_2$ without loss of generality. Then, we can subtract x k_1 times from both sides. We get $0 = x(k_2 - k_1)$. This means that adding x to itself $k_2 - k_1$ times results in the identity, and therefore every element eventually reaches the identity, and in no more that $|S|$ times (we need $|S|$ elements for pigeonhole.

If there is an element of order $|S|$, it is called a generator. Notice that Z_4 has 2 generators (1 and 3) but K_4 has no generators, so not all groups have generators. The number of generators in Z_n can be found by the **totient function** $\phi(n)$, which counts the number of relatively prime numbers from 1 to $n-1$. The reason 2 is not a generator is because 2 and 4 share a common factor, 2, and so we only iterate through even numbers (multiples of 2) and not all of the numbers in the group. We can calculate the value of the totient function as follows: for each prime factor p of n, $1/p$ of the numbers will share this factor. For example, with $n = 10$

0	1	2	3	4	5	6	7	8	9
0	1	0	1	0	1	0	1	0	1
0	1	2	3	4	0	1	2	3	4

Exactly half of the numbers from 0 to 10 are even - because they are either 0 or 1 mod 2. Exactly one fifth of the numbers from 0 to 10 are multiples of 5 - because they cycle through $0, 1, 2, 3, 4$ repeatedly. Therefore the number of relatively prime integers to 10 is $10 * (1/2) * (4/5) = 4$ and there are 4 generators - 1, 3, 7, 9 which we can see are the only numbers that do not share a factor with 10.

3 Rings, Fields

A ring is a group equipped with an additional operation, commonly referred to as multiplication.

1. All the properties of a group must be satisfied.
2. There exists a multiplicative identity, denoted 1 such that for all $s \in S$, $s * 1 = s = 1 * s$.
3. Multiplication is associative so for all $s_1, s_2, s_3 \in S$, $(s_1 * s_2) * s_3 = s_1 * (s_2 * s_3)$.
4. Addition and multiplication follow the distributive law. For all $s_1, s_2, s_3 \in S$, $s_1 * (s_2 + s_3) = s_1 * s_2 + s_1 * s_3$ and $(s_1 + s_2) * s_3 = s_1 * s_3 + s_2 * s_3$.

A field is a ring with one additional property - that a multiplicative inverse for every element (except 0) exists.

1. All the properties of a ring must be satisfied.
2. Each element (except for the additive identity) has a multiplicative inverse. For all $s_1 \in S \neq 0$, there exists s_2 such that $s_1 * s_2 = 1 = s_2 * s_1$.

3.1 Examples of rings

Let us conside the integers modulo 4. We can build a multiplication table:

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

This is a ring not a field, because there is no element x such that $2 * x = 1 \pmod 4$.

3.2 Examples of fields

3.2.1 Integers modulo a prime

The integers mod a prime number are a field. Since every element has a multiplicative inverse, we can define another group, the multiplicative group, over these elements. For the integers mod p, this is a group where the operation is multiplication! Let's consider the integers mod 5, rather than mod 4.

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Note that although 0 does not have a multiplicative inverse, it does not matter. Each of the other elements now has an inverse - an element where it multiplies to 1. It is common to consider the multiplicative group of a field - the elements other than 0. Several notations can be used for this, we will denote this as $Z_5^\times$.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

But $Z_5^\times$ has 4 elements, and we already listed out all the groups with 4 elements. This means $Z_5^\times$ must be the same group with the number renamed somehow. Specifically, $Z_5^\times$ isomorphic to Z_4. To see why, consider writing each number in terms of the generator 2.

	2^0	2^1	2^3	2^2
2^0	2^0	2^1	2^3	2^2
2^1	2^1	2^2	2^0	2^3
2^3	2^3	2^0	2^2	2^1
2^2	2^2	2^3	2^1	2^0

The second and third columns have been swapped, but this is the same as the Cayley table for Z_4. In fact, any of the generators of $Z_5^\times$ work. We could even do multiplication with addition if you had a function called log that performed this isomorphism such that $\log(a) + \log(b) = \log(ab)$.

3.2.2 The Galois field of size 4

This field extends the xor group K_4 we saw earlier. However multiplication in this group is not repeated addition! This group interprets the elements of K_4 as polynomials with coefficients in Z_2 - so the coefficients are either 0 or 1 and $1 + 1 = 0$. So for example $(x + 1) + x = 2x + 1 = 0x + 1 = 1$, and this corresponds to xor-ing 11 with 10 to get 01. Specifically, multiplication is defined by

1. Interpret each bit as the coefficient of a polynomial. So 10 is $1x + 0$, 11 is $1x + 1$, 01 is $0x + 1$ and 0 is $0x + 0$.
2. Multiply the polynomials modulo $x^2 + x + 1$ and take each coefficient mod 2.

The multiplication table for this group looks like this:

	0	1	x	1+x
0	0	0	0	0
1	0	1	x	1+x
x	0	x	1+x	1
1+x	0	1+x	1	x

This can be generalized to all finite fields in fact. The field of order p^k can be constructed by considering a k degree polynomial with coefficients in Z_p (so the trivial p^1 case is just the field Z_p!). The multiplication is taken modulo an irreducible polynomial - a k degree polynomial that doesn't factor over the field Z_p. It's a bit outside of group theory, but the choice of $x^2 + x + 1$ is in fact forced for a field of 4 elements. $x^2 + 1$ factors as $(x + 1)(x + 1) = x^2 + 2x + 1 = x^2 + 1 \pmod 2$, and $x^2 + x$ and x^2 clearly factor.