Announcements and Ideas

- Office Hours (via Zoom): MW, 8pm-9:30pm
- Don't read math line by line. Try not to spend time understanding the technical details and instead extract the key idea.

We now talk about different ways of describing groups, and a few common groups. To think about this, consider how awful it would be to describe a group with 100 elements via a 100×100 table to describe the operation $\cdot : S \times S \to S$.

Definition .0.1

The **order of a group** G is its size as a set.

Definition .0.2

The **cyclic group generated by an element** g (in a group S) is the smallest (ordered by inclusion) subgroup of S which contains g. We often denote this group by $\langle g \rangle$.

Equivalently, this is $\{g^n \mid n \in \mathbb{Z}\}$, where $g^n = \underbrace{ggg\cdots g}_{n \text{ copies}}$ (taking inverses for negative n). Note that all powers of g commute, that is $g^n g^m = g^m g^n$.

Proposition .0.1

If this group is finite, then it's $\{g, g^2, \ldots, g^k\}$ where k is the smallest positive integer such that $g^k = e$.

Proof. Finiteness gives $g^i = g^j$ for some $0 < i < j$, so $(g^{-1})^i g^i = (g^{-1})^i g^j = g^{j-i}$. There is then a positive integer with $g^k = e$. Pick the smallest such k.

Then if $0 < a < b \leq n$ and $g^a = g^b$ then we would have $e = g^{b-a}$, which is impossible. Now just note that $\{g, g^2, \ldots, g^n\}$ is closed under multiplication, contains the identity, and contains inverses. Namely for $0 < i < n$ we have $g^i g^{n-i} = g^n = e$, and $g^n g^n = e$.

Definition .0.3

We define the **order of an element** g (in a group S) to be the size of $\langle g \rangle$. That is:

$$|g| = \begin{cases} n & \text{if } \langle g \rangle \text{ has } n \in \mathbb{N} \text{ elements} \\ \infty & \text{if } \langle g \rangle \text{ is infinite} \end{cases}$$

Definition .0.4

We say a group G is **abelian** provided that any two elements of G commute. That is for all $g, h \in G$, $gh = hg$.

There is also a cancellation law for groups. If G is a group and $gh = gr$ for $g, h, r \in G$ then $h = r$ by mulitplying on the left by g^{-1}. Likewise if $hg = rg$ then $h = r$.

Recall that last time we proved the subgroups of $\mathbb{Z}$ are cyclic groups $n\mathbb{Z}$, with n being a non-negative integer. The key to the proof was that if a subgroup contains two positive integers a, b, then it also contains $a - bz$ for all $z \in \mathbb{Z}$. We then combine this iwth the division algorithm, which says that there is some $z, r \in \mathbb{Z}$ such that $a = bz + r$ and $0 \leq r < |b|$. We then can run through this multiple times to find that the subgroup is $n\mathbb{Z}$ for the smallest positive n in the group.

We can actually get more out of this!!!

Proposition .0.2

Consider the subgroup $G = \langle a, b \rangle$ generated by two nonzero integers a, b. Then $G = \gcd(a, b)\mathbb{Z}$. Furthermore this does some number theory for us!

- There is a greatest common divisor of two nonzero integers.
- Every common divisor of a, b divides the greatest common divisor.
- The greatest common divisor is expressible as $\gcd(a, b) = ax + by$ for $x, y \in \mathbb{Z}$. This is called Bezout's Lemma.

Proof. Note that $G = a\mathbb{Z} + b\mathbb{Z}$, that is integer multiples of a plus integer multiples of b. G must clearly contain this set, and this set contains G by using commutativity of addition.

We know $G = n\mathbb{Z}$ for some $n > 0$. Note then that $a, b \in n\mathbb{Z}$, so n divides both a, b. But also $n \in a\mathbb{Z} + b\mathbb{Z}$, so $n = ax + by$ for some $x, y \in \mathbb{Z}$. Now if $d \in \mathbb{Z}$ divides both a and b then $d \mid n$. Why? Well, $dA = a$, $dB = b$ so $n = ax + by = d(Ax + By)$. Therefore n is the greatest common divisor of a, b.

Corollary .0.3

If a prime $p \in \mathbb{Z}$ divides $p \mid ab$ with $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.

Proof. If $p \mid a$ then $\gcd(p, a) = 1$ since p is prime. Therefore $1 = ax + py$ for $x, y \in \mathbb{Z}$. Then $b = abx + pby$. Since $p \mid ab$, we know then that $p \mid b$.

Theorem .0.4

Every positive integer can be written as a product of positive primes in exactly one way, up to permuting the prime factors. Where the empty product is one by convention.

Proof. Induct on n to show existence of a prime factorization (clear if $n = 1$ or n is prime, otherwise $n = ab$ for $a, b < n$, apply induction).

Now we must show uniqueness by induction as well. If $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ with p_i, q_j prime. Then we use that $p_1 \mid q_1 q_2 \cdots q_\ell$, so $p_1 \mid q_i$ for some i. Because they are primes, $p_1 = q_i$, and by rearrangement we may assume $i = 1$.

By cancellation, $p_2 \cdots p_k = q_2 \cdots q_\ell < n$ because $p_1 = q_1 > 1$. By induction we're done.

We now list some order-theoretic properties of these subgroups, noting that the intersection of two subgroups of a group G is always a subgroup of G. Let $a, b \in \mathbb{Z} \setminus \{0\}$.

- $a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$ with $n = \operatorname{lcm}(a, b)$. The proof is easy and is left as an exercise.
- $\langle a, b \rangle = a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ where $d = \gcd(a, b)$.

There is also an alternative proof of unique factorizations. Lets sketch it! Suppose n is the least positive integer with at least two prime factorizations $n = p_1 \cdots p_k = q_1 \cdots q_\ell$, and we might as well assume $p_1 \leq \cdots \leq p_k$ and $q_1 \leq \cdots \leq q_\ell$. Then one may consider $n - p_1 q_1$, and go from there, noting that if $p_1 = q_1$ then we're already done by the above ide ideaa.