SEPTEMBER 19 NOTES

Last time, we introduced several examples of subgroups. We'll use them again today, so we briefly recap.

1. 2.2: Centralizers, normalizers, stabilizers, and kernels

In what follows, G will denote a group and A will denote a nonempty set.

Definition 1.1. If A is a subset of G, the **centralizer** $C_G(A)$ is the set

$$C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}.$$

Equivalently,

$$C_G(A) = \{g \in G \mid ga = ag \text{ for all } a \in A\}.$$

For any A, the center is a subgroup of G.

Definition 1.2. The **center** of a group G is the set $Z(G)$ of elements

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

The center is the set of elements that commute with all elements of G.

By definition, $Z(G) = C_G(G)$ so it is a subgroup of G. In general, for any A subset of G, $Z(G) \leq C_A(G)$.

Definition 1.3. If $g \in G$ is an element of a group and A is a nonempty subset of G, then $gAg{-}1 = \{gag^{-1} \mid a \in A\}$. The **normalizer** of A in G is the set

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

For any A, the normalizer is a subgroup of G.

Note that if $g \in C_G(A)$, then $gag^{-1} = a$ for all $a \in A$, so $gAg^{-1} = A$, which implies that $C_G(A) \subset N_G(A)$. In particular:

Proposition 1.4. *$C_G(A) \leq N_G(A)$ and $N_G(A) \leq G$.*

So, in general, we have the chain of inclusions of subgroups

$$Z(G) \leq C_G(A) \leq N_G(A) \leq G.$$

The following example will illustrate this.

Example 1.5. Let $G = D_8$. Then, $Z(G) = \{1, r^2\}$. We show this by demonstrating that these elements commute with all elements of D_8, and by exhibiting an example to show that no other elements commute with everything.

Write $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Recall that $r^k s = sr^{4-k}$.

First, $1 \in Z(G)$ by definition. Also, $r^2 \in Z(G)$ because $r^2 r^j = r^{2+j} = r^j r^2$ for any $j \in \mathbb{Z}$, and $r^2 sr^j = sr^{4-2}r^j = sr^2 r^j = sr^j r^2$ for any $j \in \mathbb{Z}$.

Now, $r, r^3 \neq Z(G)$ because $sr \neq rs = sr^3$, and $sr^3 \neq r^3 s = sr$. Also, $s \neq Z(G)$ again because $sr \neq rs$. Similarly, $sr^j \neq Z(G)$ because $sr^j r = sr^{j+1} \neq rsr^j = sr^{3+j}$. Therefore, no other elements of D_8 can be in the center so $Z(D_8) = \{1, r^2\}$.

Now, let $A = \{1, r, r^2, r^3\}$. We can show (using the same ideas as above) that

$$C_G(A) = \{1, r, r^2, r^3\}.$$

The key points are that: (1) by our computation above of the center, powers of r commute with other powers of r, and (2) s doesn't commute with all powers of r.

Finally, we can compute $N_G(A)$. In this case, we will find that $N_G(A) = G$! We know that $C_G(A) \subset N_G(A)$, so definitely all powers of r are in the normalizer, but it turns out that the sr's are also in the normalizer. Let's check this for just s. To be in the normalizer, we must have $sAs^{-1} = A$. Because $s^{-1} = s$, we must show $sAs = A$. We just compute:

$$sAs = \{s1s, srs, sr^2s, sr^3s\} = \{1, r^3, r^2, r\} = A.$$

Note that we are *not* asking for $sas = a$ for any $a \in A$, simply that $sas \in A$ for $a \in A$. Even though conjugating by s changes the order of the elements of A, it still gives us the same set, so $s \in N_G(A)$. You can perform a similar computation for any other element in G.

In summary, for $A = \{1, r, r^2, r^3\}$, we have:

$$Z(G) = \{1, r^2\} \leq C_G(A) = \{1, r, r^2, r^3\} \leq N_G(A) = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}.$$

2. 2.3: Cyclic groups and cyclic subgroups

We will spend the next section focusing on a specific type of subgroup.

Recall from last time:

Definition 2.1. If G is a group and $x \in G$ is any element, the **subgroup generated by** x is the set

$$\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\} = \{\dots, x^{-1}, 1, x, x^2, \dots\}.$$

Definition 2.2. A group G is **cyclic** if there exists an element $x \in G$ such that $G = \langle x \rangle$. In this case, we say G is **generated** by x.

Lemma 2.3. *Cyclic groups are abelian.*

Proof. If G is cyclic, then $G = \langle x \rangle$ for some $x \in G$. Therefore, for any $a, b \in G$, $a = x^n$ and $b = x^m$ for some $n, m \in \mathbb{Z}$, so

$$ab = x^n x^m = x^{n+m} = x^{m+n} = x^m x^n = ba.$$

Because a, b commute for arbitrary $a, b \in G$, G is abelian. □

Example 2.4. Any non-abelian group cannot be cyclic. So, D_{2n} and S_n, $n \geq 3$, are not cyclic.

In this section, we will encounter many additive groups (groups with binary operation addition) so we will sometimes switch to additive notation and write

$$\langle x \rangle = \{nx \mid n \in \mathbb{Z}\}.$$

Example 2.5. $\mathbb{Z}$ is cyclic because $\mathbb{Z} = \langle 1 \rangle$. Similarly, $\mathbb{Z}_n$ is cyclic because $\mathbb{Z}_n = \langle 1 \rangle$.

Proposition 2.6. *If $G = \langle x \rangle$ is a cyclic group, then:*

(1) *If $\operatorname{ord}(x) = n < \infty$, then $G = \{1, x, \dots, x^{n-1}\}$ and $x^n = 1$.*
(2) *If $\operatorname{ord}(x) = \infty$, then for all $n \neq 0$, $x^n \neq 1$. For all integers $a \neq b$, $x^a \neq x^b$.*

In particular, $|G| = \operatorname{ord}(x)$.

Proof. Suppose $G = \langle x \rangle$ and suppose $\operatorname{ord}(x) = n$. Then, $\{1, x, \dots, x^{n-1}\}$ are distinct elements of G: if $x^a = x^b$ for $0 \leq a < b < n$, then $x^{b-a} = x^0 = 1$, so $\operatorname{ord}(x) \leq b - a < n$, a contradiction. Therefore, G has at least $\operatorname{ord}(x)$ elements. Now, we show that every element of G is one of the ones listed above. If $y \in G$ is any element, then $y = x^a$ for some $a \in \mathbb{Z}$. By the division algorithm, we can write $a = qn + r$ where $0 \leq r < n$, so $x^a = x^{qn+r} = (x^n)^q x^r = 1x^r = x^r$. Therefore, $y = x^r \in \{1, x, \dots, x^{n-1}\}$ so $G = \{1, x, \dots, x^{n-1}\}$.

Now suppose $\operatorname{ord}(x) = \infty$. If $x^a = x^b$ for integers $a \neq b$, $a < b$, then $x^{b-a} = 1$, so $\operatorname{ord}(x) \leq b - a$, a contradiction. Therefore, every power of x is distinct so $|G| = \infty$. □

We can use this proposition to classify *all* cyclic groups.

Theorem 2.7. *Any two cyclic groups of the same order are isomorphic. In fact,*

1. *If $\langle x \rangle$ is a cyclic group of order n, then the map $\phi : \mathbb{Z}_n \to \langle x \rangle$ given by $k \mapsto x^k$ is an isomorphism. In other words, every finite cyclic group is isomorphic to $\mathbb{Z}_n$.*
2. *If $\langle x \rangle$ is an infinite cyclic group, then the map $\phi : \mathbb{Z} \to \langle x \rangle$ given by $k \mapsto y^k$ is an isomorphism. In other words, every infinite cyclic group is isomorphic to $\mathbb{Z}$.*

Proof. We start with (1). Let us prove this is a bijective homomorphism. We first check the homomorphism condition. If $a, b \in \mathbb{Z}_n$ such that $a + b < n$, then $a + b \pmod n = a + b$, so

$$\phi(a + b) = x^{a+b} = x^a x^b = \phi(a)\phi(b).$$

If $a + b \geq n$, then $a + b \pmod n = a + b - n$, so

$$\phi(a + b \pmod n) = \phi(a + b - n) = x^{a+b-n} = x^a x^b x^{-n} = x^a x^b 1 = \phi(a)\phi(b).$$

Therefore, the homomorphism condition holds.

Also, the map is injective by definition, since the previous proposition says the elements $\{1, x, \ldots, x^{n-1}\}$ are distinct. An injection between finite sets of the same order must be a bijection, so we have proved that ϕ is an isomorphism.

Now, we prove (2). Assume $\langle x \rangle$ is an infinite cyclic group. The map satisfies the homomorphism condition by laws of exponents:

$$\phi(a + b) = x^{a+b} = x^a x^b = \phi(a)\phi(b).$$

It is also injective by the previous proposition. Finally, by definition of a cyclic group, it is surjective. Therefore, it is an isomorphism. □

This says that, up to isomorphism, cyclic groups are either $\mathbb{Z}_n$ or $\mathbb{Z}$.

Next, we will begin to classify all subgroups of cyclic groups. We start with a few propositions.

Proposition 2.8. *Let G be a group and $x \in G$. If $x^n = 1$ and $x^m = 1$ for integers m, n, then $x^d = 1$ where $d = (m, n)$. In particular, if $x^m = 1$, then $\mathrm{ord}(x)$ divides m.*

Proof. Suppose $x^n = x^m = 1$. By the Euclidean algorithm, there exist integers r, s such that $d = (m, n) = rm + sn$, so

$$x^d = x^{rm+sn} = (x^m)^r (x^n)^s = 1^r 1^s = 1.$$

Now suppose $x^m = 1$ and let $n = \mathrm{ord}(x)$, so $x^n = 1$. If $m = 0$, then $n \mid m$, so the proposition holds. If $m \neq 0$, let $d = (m, n)$. By definition, $d \mid m$, and by the first statement, $x^d = 1$. Because the order is the smallest positive power such that $x^n = 1$, we must have $d = n$, so $n \mid m$. □

We will continue next time.