SEPTEMBER 21 NOTES

1. 2.3: Cyclic groups and cyclic subgroups

First, reminders and propositions from last time:

Definition 1.1. 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.

Proposition 1.2. *If $G = \langle x \rangle$ is a cyclic group, then:*

(1) If $|G| = \operatorname{ord}(x) = n < \infty$, then the distinct elements of G are $\{1, x, \ldots, x^{n-1}\}$ with $x^n = 1$.
(2) If $|G| = \operatorname{ord}(x) = \infty$, then for all $n \neq 0$, $x^n \neq 1$. For all integers $a \neq b$, $x^a \neq x^b$.

Proposition 1.3. *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 $\operatorname{ord}(x)$ divides m.*

Our goal is to use these, together with the next propositions, to classify all subgroups of cyclic groups.

Proposition 1.4. *Let G be a group and $x \in G$ and a a nonzero integer.*

(1) If $\operatorname{ord}(x) = \infty$, then $\operatorname{ord}(x^a) = \infty$.
(2) If $\operatorname{ord}(x) = n$, then $\operatorname{ord}(x^a) = \frac{n}{(n,a)}$. In particular, if a divides n, then $\operatorname{ord}(x^a) = \frac{n}{a}$.

Proof. For (1), assume for contradiction that $\operatorname{ord}(x) = \infty$ but $\operatorname{ord}(x^a) = n$. Then, $(x^a)^n = 1$, so $x^{an} = 1$ and hence $x^{-an} = 1$. As one of an and $-an$ is positive, we have $\operatorname{ord}(x) \leq |an|$, a contradiction.

Now, for (2), let $y = x^a$ and denote $d = (n, a)$. By definition, $n = db$ and $a = dc$ for some integers b, c such that $(b, c) = 1$. To prove (2), we must show that $\operatorname{ord}(y) = b$. First, note that $y^b = (x^a)^b = x^{ab} = x^{nc} = (x^n)^c = 1^c = 1$, so $\operatorname{ord}(y) \leq b$. By a previous proposition, we also know that $\operatorname{ord}(y) \mid b$, so write $k = \operatorname{ord}(y)$. Therefore, $y^k = x^{ak} = 1$. Because $n = \operatorname{ord}(x)$, $n \mid ak$, so $db \mid dck$ and hence $b \mid ck$. But, $(b, c) = 1$, so this implies $b \mid k$. Because $b \mid k$ and $k \mid b$, we must have $k = b$, i.e. $\operatorname{ord}(y) = b$, as desired. ☐

Proposition 1.5. *Let $G = \langle x \rangle$ be a cyclic group.*

(1) If $\operatorname{ord}(x) = \infty$, then x^a is a generator of G if and only if $a = \pm 1$.
(2) If $\operatorname{ord}(x) = n$, then x^a is a generator of G if and only if $(a, n) = 1$.

Before the proof, note that this says the *number* of generators of a finite cyclic group is equal to the number of integers in $\{1, \ldots, n-1\}$ that are relatively prime to n. This is called *Euler's totient function* or *Euler's ϕ function*, denoted $\phi(n)$.

Proof. (1) is an exercise. For (2), note that the previous propositions say that $\operatorname{ord}(x^a) = \frac{n}{(n,a)}$ and the size of the group $\langle x^a \rangle$ is exactly $\operatorname{ord}(x^a)$. This contains all elements of G if and only if it is the same size as G, if and only if $\operatorname{ord}(x^a) = n$, if and only if $(n, a) = 1$. ☐

Example 1.6. Which elements of $\mathbb{Z}_{12}$ generate $\mathbb{Z}_{12}$? Because $\mathbb{Z}_{12} = \langle 1 \rangle$ and $\operatorname{ord}(1) = 12$, the only elements $a1$[1] that can generate $\mathbb{Z}_{12}$ are those that are relatively prime to 12, i.e. $1, 5, 7, 11$.

Example 1.7. If p is prime, every nonzero element of $\mathbb{Z}_p$ generates $\mathbb{Z}_p$.

Finally, we classify all subgroups of cyclic groups.

[1] here, $x = 1$, and instead of writing x^a, we write ax because we are in an additive group

Theorem 1.8. *Let $G = \langle x \rangle$ be a cyclic group. Then:*

1. *Every subgroup H of G is cyclic and can be written as either $H = \{1\}$ or $H = \langle x^d \rangle$ where d is the smallest positive power of x appearing in H.*
2. *If $|G| = \infty$, then for any distinct nonnegative integers a, b, $\langle x^a \rangle \neq \langle x^b \rangle$.*
3. *If $|G| = \infty$, for any integer a, then $\langle x^a \rangle = \langle x^{|a|} \rangle$.*
4. *If $|G| = n$, then for each positive integer a dividing n, there is a unique subgroup H of order a given by $H = \langle x^{n/a} \rangle$.*
5. *If $|G| = n$, for any integer b, $\langle x^b \rangle = \langle x^{(b,n)} \rangle$.*

Proof. We prove (1) and (4) leaving the others as exercises.

For (1), let $H \leq G$ be any subgroup. If $H = \{1\}$, then the statement holds. So, assume there is an element $x^a \in H$, $a \neq 0$. Because $x^a \in H$ implies $x^{-a} \in H$, we may assume that $a > 0$. In particular, we know that H contains positive powers of x. Let d be the smallest positive power of x that appears in H. Because H is a subgroup and $x^d \in H$, we have $\langle x^d \rangle \leq H$. We aim to show these are equal. Let $x^b \in H$ be any element. By the division algorithm, we may write $b = qd + r$ where $0 \leq r < d$, so $x^b = x^{qd+r} = (x^d)^q x^r$. Because $x^d \in H$, $(x^d)^{-q} \in H$, and therefore $x^b (x^d)^{-q} = x^r \in H$. Because d was chosen to be the smallest positive power appearing in H, we must have $r = 0$. Therefore, every element of H is $(x^d)^q$ for some integer q, so $H \leq \langle x^d \rangle$ and we conclude $H = \langle x^d \rangle$.

For (4), suppose $|G| = n$ and let a be a positive integer dividing n. If $d = n/a$, then by the previous propositions, $\langle x^d \rangle$ has order a so is a subgroup of order a. To prove uniqueness, let H be any subgroup of G of order a. By (1), $H = \langle x^b \rangle$ where b is the smallest positive integer such that $x^b \in H$, and by the previous propositions, $a = |H| = \mathrm{ord}(x^b) = \frac{n}{(b,n)}$. Because $d = n/a$, we have $d = (b, n)$ and hence $d \mid b$. Therefore, $x^b \in \langle x^d \rangle$, so $H \leq \langle x^d \rangle$. However, both of these sets have a elements, so they must be equal, and we conclude $H = \langle x^d \rangle$. □

Example 1.9. The subgroups of $\mathbb{Z}_6$ are:

- (order 6) $\langle 1 \rangle = \langle 5 \rangle$
- (order 3) $\langle 2 \rangle = \langle 4 \rangle$
- (order 2) $\langle 3 \rangle$
- (order 1) $\langle 0 \rangle$

2. 2.4: Subgroups generated by subsets of a group

We want to generalize the idea of subgroup generated by *one* element to subgroup generated by *several* elements.

Note: in class, we only gave the second definition below. It is more useful and practical than the first. But, feel free to read both if you want to follow Dummit and Foote.

Proposition 2.1. *If $\mathcal{A}$ is a nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is a subgroup of G.*

Proof. Exercise, or see the book. □

Definition 2.2. If A is any nonempty subset of a group G, then the **subgroup generated by** A is the subgroup

$$\langle A \rangle = \bigcap_{A \subset H, H \leq G} H$$

In words, it is the intersection of all subgroups of G containing A.

While this definition is short, there is an alternative that can sometimes be more useful.

Definition 2.3. Let A be a nonempty subset of a group G and define the **subgroup generated by** A to be

$$\overline{A} = \{\Pi_{i\in\{1,\ldots,n\}} a_i^{e_i} \mid n \in \mathbb{Z}^{\geq 0}, a_i \in A, e_i = \pm 1.\}$$

This is the collection of all finite products of elements of A and their inverses. Note that any element $a \in A$ can appear as several different a_i's: we do not require that the a_i's are distinct.

We show that the two definitions are the same:

Proposition 2.4. *For any nonempty subset A of a group G, $\langle A\rangle = \mathcal{A}$.*

Proof. First, one shows that $\overline{A}$ is indeed a subgroup of G. This is left as an exercise.

If $a \in A$ is any element, then $a = a^1 \in \overline{A}$, so $A \subset \overline{A}$, so $\langle A\rangle \subset \overline{A}$. But, $A \subset \langle A\rangle$, so any product of elements of A and their inverses is contained in $\langle A\rangle$, so $\langle A\rangle = \overline{A}$. □

Remark 2.5. If G is not abelian, the subgroup generated by an arbitrary subset can be very complicated and in general we can essentially nothing about the size/order of elements/etc of $\langle A\rangle$.