FEBRUARY 27 NOTES

1. Section 4: Powers of an element, cyclic groups

Definition 1.1. Let G be a group and $x \in G$. If there exists a positive integer n such that $x^n = e$, then x is said to have **finite order** and the order of x is $o(x)$, the minimal positive integer n such that $x^n = e$.

If no such n exists, x is said to have **infinite order** and we write $o(x) = \infty$.

Example 1.2. For any group G, $e^1 = e$, so $o(e) = 1$.

Definition 1.3. Let G be a group and $x \in G$. The **set generated by** x is the set

$$\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\} = \{\dots, x^{-2}, x^{-1}, e, x, x^2, x^3, \dots\}.$$

Definition 1.4. A group G is called a **cyclic group** if there exists an element $x \in G$ such that $G = \langle x \rangle$. In this case, we say that x **generates** G.

Example 1.5. $\mathbb{Z}_3 = \langle 1 \rangle = \{0, 1, 2\}$ so $\mathbb{Z}_3$ is cyclic generated by 1.

It is also generated by 2: $\langle 2 \rangle = \{0, 2, 1\} = \mathbb{Z}_3$.

In order for a group to be cyclic, there *must* be an element whose order is equal to the total number of elements in G.

Theorem 1.6. *Let G be a group and $x \in G$ such that $o(x) = n$. Then,*

$$\langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}.$$

In particular, $\langle x \rangle$ has n elements. If $o(x) = \infty$, then $\langle x \rangle = \{\dots x^{-2}, x^{-1}, e, x, x^2, \dots\}$ and for any $i \neq j$, $x^i \neq x^j$, so in particular, $\langle x \rangle$ has infinitely many elements.

Proof. Let $S = \{e, x, x^2, \dots, x^{n-1}\}$. We have $S \subset \langle x \rangle$ by definition, so we must show that $\langle x \rangle \subset S$.

Let x^m be any element of $\langle x \rangle$. By the division algorithm, we can find $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that

$$m = nq + r$$

which means

$$\begin{aligned} x^m &= x^{nq+r} \\ &= (x^n)^q x^r \\ &= e^q x^r \quad \text{because the order of } x \text{ was } n \\ &= e x^r \\ &= x^r. \end{aligned}$$

So, any power of x has $x^m = x^r$ for some $r \in \{0, 1, 2, \dots, n-1\}$, which implies $x^m \in S$.

Next, suppose that $o(x)$ is infinite. Suppose for contradiction that x^i, x^j are two powers of x with $i \neq j$ such that $x^i = x^j$. Either $i > j$ or $j > i$; suppose without loss of generality that $i > j$. Multiplying both sides by x^{-j}, we find $x^i x^{-j} = x^j x^{-j}$, or $x^{i-j} = e$. Because $i > j$, $i - j > 0$, so this says there is some positive power of x that equals the identity. This contradicts the fact that the order of x is infinite.

Therefore, we must have $x^i \neq x^j$ and therefore $\langle x \rangle$ has infinitely many elements. □

Corollary 1.7. Suppose G is a group with n elements. Then, G is cyclic if and only if there is an element $x \in G$ with $o(x) = n$.

Proof. By definition, if G is cyclic, then $G = \langle x \rangle$ for some $x \in G$. By the previous proposition, $\langle x \rangle$ has $o(x)$ elements, so this implies that $o(x) = n$.

Conversely, suppose there is an element $x \in G$ such that $o(x) = n$. Then, $\langle x \rangle \subset G$, but each set has n elements, so in fact $\langle x \rangle = G$ and G is cyclic. □

First, some reminders from previous classes:

Definition 1.8. Suppose $n, m \in \mathbb{Z}$ are two integers, not both 0. The **greatest common divisor** of n and m, $\gcd(n, m)$ is the largest positive integer d such that $d \mid n$ and $d \mid m$.

Theorem 1.9. *If $d = \gcd(n, m)$, then there exist integers a and b such that*

$$an + bm = d.$$

Example 1.10. For instance, $\gcd(3, 5) = 1$, and we can write $1 = 2(3) - 1(5)$.

Or, $\gcd(6, 16) = 2$, and we can write $2 = 3(6) - 16$.

Theorem 1.11. *Suppose $n, m, k \in \mathbb{Z}$. If $\gcd(n, m) = 1$ and m divides nk, then m divides k.*

Proof. Because $\gcd(n, m) = 1$, we know we can find integers $a, b \in \mathbb{Z}$ such that $an + bm = 1$, and multiplying everything by k, this says $ank + bmk = k$. Because m divides nk, it divides ank, and m divides bmk, so therefore m divides $ank + bmk$. Therefore, m divides k. □

We'll use these arithmetic properties to prove facts about orders of elements.

Theorem 1.12. *Suppose G is a group and $x \in G$. Then:*

(1) $o(x) = o(x^{-1})$,
(2) if $o(x) = n$ and $x^m = e$, then n divides m, and
(3) if $o(x) = n$, then $o(x^m) = \frac{n}{\gcd(n,m)}$.

Before we prove this, let's do an example: rephrasing this for an additive group, this says: if $o(x) = n =$ minimal positive integer such that $nx = 0$, then $o(mx) = \frac{n}{\gcd(n,m)}$.

Example 1.13. In $\mathbb{Z}_6$, $o(1) = 6$. We can use this to determine $o(m)$ for all other $m \in \mathbb{Z}_6$: for any m, $m = m \cdot 1$, so

$$o(m) = \frac{6}{\gcd(6, m)}$$

which gives us:

$$o(2) = \frac{6}{\gcd(6, 2)} = \frac{6}{2} = 3, \quad o(3) = \frac{6}{\gcd(6, 3)} = \frac{6}{3} = 2,$$

$$o(4) = \frac{6}{\gcd(6, 4)} = \frac{6}{2} = 3, \quad o(5) = \frac{6}{\gcd(6, 5)} = \frac{6}{1} = 6.$$

and these numbers give us the size of the set generated by each element:

$$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\}$$

$$\langle 2 \rangle = \{0, 2, 4\}$$

$$\langle 3 \rangle = \{0, 3\}$$

$$\langle 4 \rangle = \{0, 4, 2\}$$

$$\langle 5 \rangle = \{0, 5, 4, 3, 2, 1\}.$$

Now, let's prove the theorem:

Proof. Part (1) is on your homework!

For part (2), suppose $o(x) = n$ and $x^m = e$. Using the division algorithm, we can write $m = nq+r$ for some $0 \leq r < n$, so

$$\begin{aligned} e = x^m &= x^{nq+r} \\ &= (x^n)^q x^r \\ &= e^q x^r \quad \text{because the order of } x \text{ was } n \\ &= ex^r \\ &= x^r. \end{aligned}$$

Therefore, $x^r = e$, but $r < n$ and n was defined to be the smallest *positive* integer such that $x^n = e$. Therefore, we must have $r = 0$, which says $m = nq$ and therefore n divides m.

For part (3), let assume $x^n = e$ and let $d = \gcd(n, m)$. Because $n/d \in \mathbb{Z}$, we know

$$(x^m)^{n/d} = x^{mn/d} = (x^n)^{m/d} = e^{m/d} = e.$$

This says x^m has order at most n/d because n/d is a positive integer such that $(x^m)^{n/d} = e$, i.e. $o(x) \leq n/d$. Suppose now that $o(x) = k$. We know already $k \leq n/d$. Then, because $x^{mk} = e$, the previous part says n divides mk, which means n/d divides $(m/d)k$. Because $\gcd(n/d, m/d) = 1$, by the previous properties of gcd's, this says that n/d must divide k. Therefore, $n/d \leq k$. Because $k \leq n/d$ and $n/d \leq k$, we can conclude that $k = n/d$ so $o(x) = n/\gcd(n, m)$ as desired. □

2. Section 5: Subgroups

Finally, we define the notion of subgroup.

Definition 2.1. Let H be a subset of a group $(G, \star)$. We say H is **closed under** $\star$ if, for any $a, b \in H$, $a \star b \in H$.

We say H is **closed under inverses** if, for any $a \in H$, a^{-1} (which exists in G because G is a group!) also satisfies $a^{-1} \in H$.

Example 2.2. The set $GL_2(\mathbb{R}) \subset (M_2(\mathbb{R}), +)$ is **not** closed under $+$ because the sum of two invertible matrices does not have to be invertible: $I, -I \in GL_2(\mathbb{R})$, but $I + -I = 0$ and $0 \notin GL_2(\mathbb{R})$.

The set $\mathbb{Z}^+ \subset (\mathbb{Q}^+, \times)$ is **not** closed under inverses. We know $2 \in \mathbb{Z}^+$, but $2^{-1} = 1/2$ and $1/2 \notin \mathbb{Z}^+$.

This leads us to the definition of subgroup:

Definition 2.3. A **subgroup** H of a group G is a subset $H \subset G$ such that:

(1) H is nonempty, which we usually check as: $e \in H$ (where $e \in G$ is the identity of G),
(2) H is closed under the binary operation $\star$ in G, and
(3) H is closed under inverses.

Note the first property says $e \in H$ so H has an identity, and the second says H has an associative binary operation (because $\star$ on G is associative by definition), and the third says every element of H has an inverse. So, we see that subgroups are *groups* and an alternative way of phrasing the definition is: a subgroup H is a subset of G that is also a group (with the same binary operation).

Example 2.4. $\mathbb{Z}$ is a subgroup of $(\mathbb{Q}, +)$.

Proof: (1) 0 is the identity of $\mathbb{Q}$, and $0 \in \mathbb{Z}$, so $\mathbb{Z}$ contains the identity.

(2) $\mathbb{Z}$ is closed under $\star$ because the sum of any two integers is still an integer.

(3) $\mathbb{Z}$ is closed under inverses because the inverse of an integer n is $-n$, which is still an integer.

Example 2.5. For any $x \in G$ and any group G, $\langle x \rangle$ is a subgroup of G.

Proof: let $H = \langle x \rangle$. We know $e = x^0 \in H$ so (1) is true. We know H is closed under $\star$ because the elements of H are of the form x^a, x^b, and $x^a \star x^b = x^{a+b} \in H$, so (2) is true. Finally, any element of H is of the form x^n, and $(x^n)^{-1} = x^{-n} \in H$, so (3) is true.

Definition 2.6. For any group G, the **center** of G is the set

$$Z(G) = \{x \in G \mid xy = yx \text{ for all } y \in G\}.$$

In words, the center of G is the set of elements that commute with *every* other element of G.

Example 2.7. $Z(G)$ is a subgroup of G. Homework!