FEBRUARY 20 NOTES

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

Notational reminder from last time: it gets cumbersome to write $\star$ all the time; e.g. $x \star y$ can be tedious to write over and over again. So, when dealing with *abstract* groups, we will denote the operation by $x \star y = xy$. We will also write powers of a given element by x^n, where:

$$\begin{aligned} x^1 &= x \\ x^2 &= x \star x \\ x^3 &= x \star (x \star x) \\ &\dots \end{aligned}$$

and so on.

So, whenever you see the notation xy in this class, it always means $x \star y$, where $\star$ is whatever the binary operation is. When we know the operation, we may choose to change notation. For example, if the operation is $+$, we will write $x + y$ instead of xy. For powers, instead of writing x^2, which means $x \star x$, we would write $2x$ because $x + x = 2x$.

Definition 1.1. Let G be a group and $x \in G$. The **powers** of x are defined as:

(1) $x^0 = e$
(2) positive powers: $x^n = x \star x \star \cdots \star x$ (n x's)
(3) negative powers: $x^{-n} = x^{-1} \star x^{-1} \star \cdots \star x^{-1}$ (n x^{-1}'s)

As above, we may use different notation in additive groups. For example, in $G = \mathbb{Z}$ with $\star = +$, the 'power' of x is **not** the power in the usual sense; the nth power is

$$x \star x \star \cdots \star x$$

(n x's) which is more commonly written as

$$nx = x + x + \cdots + x.$$

Powers behave as we expect:

Definition 1.2. Suppose G is a group, $x \in G$, and $n, m \in \mathbb{Z}$. Then:

(1) $x^n x^m = x^{n+m}$
(2) $(x^n)^{-1} = x^{-n}$
(3) $(x^n)^m = x^{nm}$.

Proof. We prove only the first one and leave (2) and (3) as exercises. To prove (1), we use cases. Suppose $n = 0$. By definition of the identity, because $x^0 = e$, we know

$$x^n x^0 = x^n e = x^n$$

and because $n = n + 0$, we have

$$x^n x^0 = x^{n+0}.$$

A similar argument holds if $m = 0$.

Next, suppose $n, m > 0$. Then, by definition,

$$x^n x^m = (x \star \cdots \star x) \star (x \star \cdots \star x)$$

where the first set of parentheses holds n xs and the second has m. Using associativity, as the right side has a total of $n+m$ xs, this is

$$x^n x^m = x \star \cdots \star x \star x \star \cdots \star x = x^{n+m}.$$

Replacing x with x^{-1}, a similar argument holds if $n, m < 0$.

Next, suppose $n > 0$ and $m < 0$. If $|n| \geq |m|$, write $n = k + |m|$ where $k \geq 0$ and $k = n + m$. Then, we know (from what we've already proven) $x^n = x^k x^{|m|}$, so

$$\begin{aligned} x^n x^m &= x^k x^{|m|} x^m \\ &= x^k \star (x \star \cdots \star x) \star (x^{-1} \star \cdots \star x^{-1}) \text{ where there are } m \quad x\text{s and } m \quad x^{-1}\text{s} \\ &= x^k \star e \text{ because each } x \text{ will cancel with each } x^{-1} \\ &= x^k = x^{n+m}. \end{aligned}$$

If $|n| \leq |m|$, write $m = -n - k$ where $k \geq 0$ and $-k = n + m$. Then, $x^m = x^{-n} x^{-k}$, and as above, we can write:

$$\begin{aligned} x^n x^m &= x^n x^{-n-k} = x^n x^{-n} x^{-k} \\ &= (x \star \cdots \star x) \star (x^{-1} \star \cdots \star x^{-1}) \star x^{-k} \text{ where there are } n \quad x\text{s and } n \quad x^{-1}\text{s} \\ &= e \star x^{-k} \text{ because each } x \text{ will cancel with each } x^{-1} \\ &= x^{-k} = x^{n+m}. \end{aligned}$$

A similar argument holds if $n < 0$ and $m > 0$. □

Definition 1.3. 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 1.4. For any group G, $e^1 = e$, so $o(e) = 1$.

Example 1.5. If $G = (\mathbb{Z}, +)$, the order of an element x is the minimal positive integer n such that $nx = 0$. This says $o(0) = 1$ because $1 \cdot 0 = 0$, but $o(x) = \infty$ for every $x \neq 0$ because $nx \neq 0$ for any $n > 0$.

Example 1.6. If $G = (\mathbb{Z}_n, +_n)$, recalling that $+_n$ means addition mod n, then for *every* element $x \in \mathbb{Z}_n$, $nx = 0$, so every element has order $\leq n$.

For instance, in $n = 4$, then $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. We can compute the orders and get: $o(0) = 1$, $o(1) = 4$, $o(2) = 2$, and $o(3) = 4$.

Definition 1.7. Let G be a group and $x \in G$. The **set generated by** x is the set

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

Example 1.8. If $G = \mathbb{Z}_4$, what is $\langle x \rangle$ for any $x \in G$?

$$\begin{aligned} \langle 0 \rangle &= \{0\} \\ \langle 1 \rangle &= \{0, 1, 2, 3\} \\ \langle 2 \rangle &= \{0, 2\} \\ \langle 3 \rangle &= \{0, 3, 2, 1\} \end{aligned}$$

Definition 1.9. 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 1.10. $\mathbb{Z} = \langle 1 \rangle = \{\dots, -2, -1, 0, 1, 2, \dots\}$ so $\mathbb{Z}$ is cyclic generated by 1.

This doesn't mean that every element $x \in \mathbb{Z}$ generates $\mathbb{Z}$; for instance, $\langle 2 \rangle = \{\dots, -4, -2, 0, 2, 4, \dots\} \neq \mathbb{Z}$.

Example 1.11. $\mathbb{Z}_3 = \langle 1 \rangle = \{0, 1, 2\}$ so $\mathbb{Z}_3$ is cyclic generated by 1.

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

We observed a few things at the end of class; namely: 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. This is stated precisely in the following theorem, which we will prove next time.

Theorem 1.12. *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.

Example 1.13. Let G be the group D_3 from last week's worksheet. Is G cyclic?

The answer is **no**, for two reasons: first, you could compute the order of any element of G. The order of the identity is 1, the order of any rotation is 3 (because, if you rotate 3 times clockwise or counterclockwise, you get back to the original configuration), and the order of any flip is 2 (because flipping over twice gets you back to the original configuration). Therefore, G has no elements of order 6, so can't be cyclic.

Secondly, you could give an easier reason: cyclic groups **must be abelian**. Why? If G is cyclic, then every element of G is of the form x^n for some integer n, and $x^n x^m = x^{n+m} = x^{m+n} = x^m x^n$. Because D_3 is not abelian, it cannot be cyclic.