Previously.

- Subgroups
- The Subgroup Test
- The center of a group, $Z(G)$

This Section.

- Subgroups generated by one or more elements of a group
- Cyclic groups
- The order of an element
- Subgroup lattices

Subgroups Generated by Elements

Theorem 2.4.1. Let g be an element of a group G, and write

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}.$$

Then $\langle g \rangle$ is a subgroup of G, and $\langle g \rangle \subseteq H$ for every subgroup H of G with $g \in H$.

Exercise 1. Compute $\langle \overline{2} \rangle \leq (\mathbb{Z}_5, +)$

Exercise 2. Compute $\langle i \rangle \leq (\mathbb{C} \setminus \{0\}, \cdot)$

Cyclic Groups

Definition. A group G is `cyclic` if there is some $g \in G$ for which $G = \langle g \rangle$.

Question 3. Is the additive group $\mathbb{Z}_5$ cyclic?

Exercise 4. Is $\mathbb{Z}_5^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ cyclic?

Exercise 5. Is $\mathbb{Z}_{12}^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ cyclic?

Definition. The generic group C_n is the `cyclic group of order` n. If no generator is specified, we will assume it is a and write $C_n = \langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\}$.

Orders of Groups and Elements

Definition. If G is a finite group, the `order of a group` G is denoted $|G|$ and is the cardinality of the set G.
The `order of an element` $g \in G$ is denoted $|g|$ or $o(g)$ and equals the smallest positive integer n such that $g^n = e$.

Exercise 6. Compute the orders.

(a) $|\mathbb{Z}_{10}| =$

(b) Using $\overline{2} \in \mathbb{Z}_{10}$, $o(\overline{2}) =$

(c) $|\mathbb{Z}_8^\times| =$

(d) Using $\overline{3} \in \mathbb{Z}_8^\times$, $o(\overline{3}) =$

Theorem 2.4.2. Let $g \in G$ with $o(g) = n$. Then

1. $g^k = e$ if and only if $n|k$.

2. $g^k = g^m$ if and only if $k \equiv m \pmod{n}$

3. $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$ where $e, g, g^2, \dots, g^{n-1}$ are all distinct.

* The proof is in the textbook, and uses laws of exponents.

Exercise 7. Suppose G is a group and $g \in G$ has order 15.

1. What is g^{30}?

2. What is $\langle g \rangle$?

3. Write g^{2452} as g^k for some $0 \le k < 15$.

Theorem 2.4.3. Let G be a group and let $g \in G$ satisfy $o(g) = \infty$. Then

1. $g^k = e$ if and only if $k = 0$.

2. $g^k = g^m$ if and only if $k = m$.

3. $\langle g \rangle = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$ where the g^i are distinct.

Exercise 8. Let $G = \mathbb{R}$. Consider $g = \pi \in \mathbb{R}$.

1. What is $o(\pi)$?

2. What is $\langle \pi \rangle$?

Corollary. For all g in a group G, $o(g) = |\langle g \rangle|$.

Note. Some cool properties.

- The identity is the only element of order 1 in a group.
- $o(g) = o(g^{-1})$ for all $g \in G$

Order in $\mathbb{Z}_n$

Theorem. Given $\overline{a} \in \mathbb{Z}_n$, with $1 \leq a \leq n-1$,

$$|\overline{a}| = \frac{n}{\gcd(a,n)}.$$

Exercise 9. What is the order of $\overline{14}$ in $\mathbb{Z}_{30}$?

Order in $\mathbb{Z}_n^\times$

Note. There is no formula....... In section 2.6 we'll see that $|g|$ divides $|G|$ if $|G|$ is finite.

Exercise 10. Consider $\mathbb{Z}_{12}^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. What is the order of each of these elements?

Order of an element in S_n

Theorem. If $\gamma = (k_1\ k_2\ \dots\ k_r)$ is an r-cycle in S_n, then $o(\gamma) = r$.

Question 11. You proved $(1\ 2\ 3\ \dots\ n)$ has order n for homework, how might you extend this proof to work for any cycle?

Theorem 2.4.4. If $\gamma = \sigma_1\sigma_2\dots\sigma_r$ where σ_i are disjoint cycles, then

$$o(\gamma) = \operatorname{lcm}(o(\sigma_1), o(\sigma_2), \dots, o(\sigma_r)).$$

Exercise 12. Let $\sigma = (1\ 2\ 3)(4\ 5)$ and $\tau = (1\ 3)(4\ 5)$.
Then

(a) $o(\sigma) =$

(b) $o(\tau) =$

(c) $o(\sigma\tau) =$

Properties of Cyclic Groups

Theorem 2.4.6. Every cyclic group is abelian, but the converse does not hold.

Theorem 2.4.7. Every subgroup of a cyclic group is cyclic.

Theorem 2.4.8. Let $G = \langle g \rangle$ be a cyclic group, where $o(g) = n$. Then $G = \langle g^k \rangle$ if and only if $\gcd(k, n) = 1$.

Finite Cyclic Groups and Their Subgroups

The Fundamental Theorem of Finite Cyclic Groups (Theorem 2.4.9). Let $G = \langle g\rangle$ be a cyclic group of order n.

1. If H is a subgroup of G, then $H = \langle g^d\rangle$ for some $d|n$. Hence $|H|$ divides n.
2. Conversely if $k|n$, then $\langle g^{n/k}\rangle$ is the unique subgroup of G of order k.

Example. The subgroup lattice of the cyclic subgroup $C_{12} = \langle a\rangle = \{1, a, a^2, \ldots, a^{11}\}$:
We see that $|C_{12}| = 12$ and the divisors of 12 are $1, 2, 3, 4, 6, 12$. There is exactly one subgroup for each of those divisors.
Pictorally, the chart here shows all of the subgroups and if a subgroup is above another with a line connecting them, this means that the higher one contains the lower one. (Verify this!)

$$\begin{tikzcd}
 & & \langle a\rangle & \\
 & \langle a^2\rangle \arrow[ur, no head] & & \langle a^3\rangle \arrow[ul, no head] \\
\langle a^4\rangle \arrow[ur, no head] & & \langle a^6\rangle \arrow[ul, no head] \arrow[ur, no head] & \\
 & \langle 1\rangle \arrow[ul, no head] \arrow[ur, no head] & &
\end{tikzcd}$$

Example. The subgroup lattice of $\mathbb{Z}_{15} = \langle\overline{1}\rangle$:

Groups Generated by Several Elements

Example. The Klein-4 Group K_4:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(1,0),(0,1),(1,1)\} = \langle(\overline{0},\overline{1}),(\overline{1},\overline{0})\rangle$$

Example. The symmetric group S_3: Let $\sigma = (1\ 2\ 3)$ and $\tau = (1\ 2)$. Then every element of S_3 can be written as $\sigma^i\tau^j$ for some i, j.

- $\varepsilon = \sigma^0\tau^0$
- $(1\ 2) = \sigma^0\tau^1$
- $(1\ 3) = \sigma^1\tau^1$
- $(2\ 3) = \sigma^2\tau^1$
- $(1\ 2\ 3) = \sigma^1\tau^0$
- $(1\ 3\ 2) = \sigma^2\tau^0$

Thus $S_3 = \langle\sigma, \tau\rangle$.

Definition. In general, if X is a nonempty subset of a group G, then the `subgroup of` G `generated by` X is defined as

$$\begin{aligned}\langle X\rangle &= \{\text{products of powers (not nec. distinct) of elements of X}\}\\ &= \{x_1^{k_1}x_2^{k_2}\cdots x_m^{k_m} \mid x_i \in X,\ k_i \in \mathbb{Z},\ m \geq 1\}\end{aligned}$$

We will always have $\langle X\rangle \leq G$.

Exercise 13. Find two elements of $\mathbb{Z}_{12}^\times$ that generate the set.