Section I.6. Cyclic Groups

Note. We'll see that cyclic groups are fundamental examples of groups. In some sense, all finite abelian groups are "made up of" cyclic groups. Recall that the *order* of a finite group is the number of elements in the group.

Definition. Let G be a group and $a \in G$. If G is cyclic and $G = \langle a \rangle$, then (1) if G is finite of order n, then *element a is of order n*, and (2) if G is infinite then *element a is of infinite order*.

Theorem 6.1. Every cyclic group is abelian.

Note. We now state a result from number theory. The text offers "an intuitive digrammatic explanation." A truly rigorous proof would require a clear definition of $\mathbb{N}$ in terms of sets.

Theorem 6.3. The Division Algorithm for $\mathbb{Z}$
If m is a positive integer (i.e., $m \in \mathbb{N}$) and n is any integer (i.e., $n \in \mathbb{Z}$), then there exist unique integers q and r such that $n = mq + r$ and $0 \leq r < m$. q is called the *quotient* and r the *remainder* when n is divided by m.

Example. For $n = 25$ and $m = 3$, we have $25 = 3(8) + (1)$, so $q = 8$ and $r = 1$. For $n = -15$ and $m = 6$ we have $-15 = 6(-3) + (3)$, so $q = -3$ and $r = 3$ (notice that $r \geq 0$). In terms of the least integer function $\lfloor x \rfloor$, we have for general m and n that $q = \left\lfloor \frac{n}{m} \right\rfloor$ and $r = n - m \left\lfloor \frac{n}{m} \right\rfloor = n - mq$.

Note. The division algorithm is necessary when studying subgroups of cyclic groups.

Theorem 6.6. A subgroup of a cyclic group is cyclic.

Recall. From the previous section we know that for all $n \in \mathbb{Z}$, $\langle n \rangle = \langle -n \rangle = n\mathbb{Z}$. Since $\mathbb{Z}$ itself is cyclic ($\mathbb{Z} = \langle 1 \rangle$), then by Theorem 6.6 every subgroup of $\mathbb{Z}$ must be cyclic. We therefore have the following.

Corollary 6.7. The subgroup of $\langle \mathbb{Z}, + \rangle$ are precisely the groups $n\mathbb{Z} = \langle n \rangle$ (under $+$) for $n \in \mathbb{Z}$.

Exercise 6.20. Find the number of elements in the cyclic subgroup of the group $\mathbb{C}^*$ (of nonzero complex numbers under multiplication) generated by $(1 + i)/\sqrt{2}$.

Exercise 6.45. Let $r, s \in \mathbb{N}$. Then $A = \{nr + ms \mid n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

Note. By Corollary 6.7, the subgroup A of $\mathbb{Z}$ in Exercise 6.45 must be isomorphic to $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Therefore A is a cyclic group and has some (positive) generator (namely, n). This generator is the greatest common divisor of r and s.

Definition 6.8. Let $r, s \in \mathbb{N}$. The positive generator d of the cyclic group $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$ under addition is the *greatest common divisor* of r and s, denoted $\gcd(r, s)$.

Note. You are probably familiar with finding greatest common divisors using factoring into powers of primes and the Fundamental Theorem of Arithmetic. Recall that if $\gcd(r, s) = 1$, then r and s are relatively prime.

Note. The next result is a **BIG DEAL**!!! It gives a classification (up to isomorphism) of all cyclic groups. (It should be called "The Fundamental Theorem of Cyclic Groups.")

Theorem 6.10. Let G be a cyclic group with generator a. If G is of infinite order then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

Note. We have seen (page 30) that $\langle U_n, \cdot \rangle$ and $\langle \mathbb{Z}_n, + \rangle$ are isomorphic groups. This is consistent with the idea that addition modulo n is called "clock arithmetic." Under multiplication, the elements of U_n cycle around the unit circle in the complex plane (see page 63 for a picture). This further inspires the term "cyclic" group.

Note. Recall Corollary 6.7: "The subgroup of $\mathbb{Z}$ under addition are precisely the groups $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$." So by Theorem 6.10, we can completely classify the subgroup of infinite cyclic groups: "If G is an infinite cyclic group with generator a, then the subgroup of G (under multiplication) are precisely the groups $\langle a^n \rangle$ where $n \in \mathbb{Z}$." We now turn to subgroups of finite cyclic groups.

Theorem 6.14. Let G be a cyclic group with n elements and with generator a. Let $b \in G$ where $b = a^s$. Then b generates a cyclic subgroup H of G containing n/d elements where $d = \gcd(n, s)$. Also, $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$.

Exercise 6.28. Find all orders of subgroups of $\mathbb{Z}_{20}$.

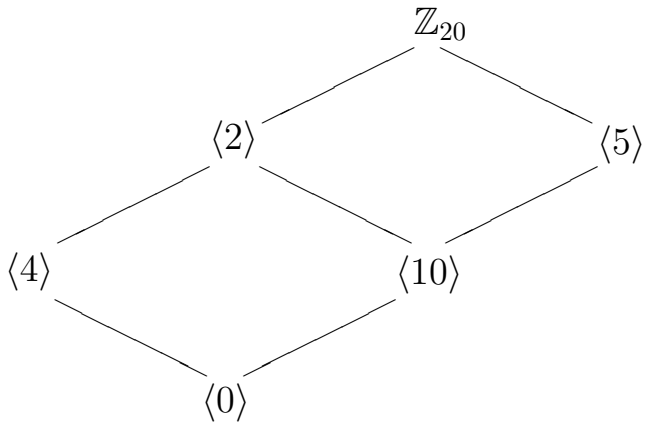
Solution. This is an additive group with generator $a = 1$. With $s = 2$, $b = a^s = 2(1) = 2$ and 2 generates a subgroup of order n/d where $d = \gcd(20, 2) = 2$, so $n/d = 20/2 = 10$. With $s = 4$, $\langle 4 \rangle$ has order $n/d = 20/4 = 5$ elements. With $s = 5$, $\langle 5 \rangle$ has order $n/d = 20/5 = 4$. With $s = 10$, $\langle 10 \rangle$ has order $n/d = 20/10 = 2$. Next, for $s \in \{3, 7, 9, 11, 13, 17, 19\}$, $d = \gcd(n, s) = 1$ and $n/d = 20$; each of these generate $\mathbb{Z}_{20}$. In totality, we get the subgroups:

ORDER	GENERATORS
1	0
2	10
4	5, 15
5	4, 8, 12, 16
10	2, 6, 14, 18
20	1, 3, 7, 9, 11, 13, 17, 19

This result based on Theorem 6.14, inspires the following.

Corollary 6.16. If a is a generator of a finite cyclic group G of order n, then the other generators of G are the elements of the form a^r, where r is relatively prime to n.

Example. A subgroup diagram of $\mathbb{Z}_{20}$ is:



Example (like Exercise 6.37). Give an example of a group which is finite, cyclic, and has six generators.

Solution. By Theorem 6.10, we need only consider $\mathbb{Z}_n$. By Corollary 6.16 we want n such that there are six elements of $\mathbb{Z}_n$ which are relatively prime to n. We find $n = 9$ yields generators 1, 2, 4, 5, 7, and 8.

Revised: 7/7/2023