Chapter 4

Cyclic Groups

4.1 Definitions, Review and Examples

In this chapter we will study cyclic groups. More precisely, we will answer the following questions:

1. What are their properties?
2. What do cyclic groups look like?
3. What kind of elements do they have?
4. What is the order of their elements?
5. What kind of subgroups can they have and what is the order of each subgroup?

You will recall from the previous chapter that a group G is cyclic if $G = \langle a \rangle$ for some $a \in G$ and $\langle a \rangle = \left\{a^k \mid k \in \mathbb{Z}\right\}$. Such an element is called a generator of G.

Since in this chapter we will deal with groups which elements are powers of a fixed element, we begin by reviewing the properties of exponents. We will state all properties using the notation of multiplication. Remember these properties must be adapted to whatever operation a given group uses.

Proposition 192 *Get G be a group and $a \in G$. Let m and n be integers. The following is true:*

1. $a^m a^n = a^{m+n}$
2. $(a^m)^n = a^{mn}$
3. $(a^n)^{-1} = a^{-n} = \left(a^{-1}\right)^n$
4. $a^0 = e$

We have already seen some examples of cyclic groups.

Example 193 *$\mathbb{Z}$ is cyclic since $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$*

Example 194 *$\mathbb{Z}_n$ with addition $\bmod n$ is a cyclic group, 1 and $-1 = n-1$ are generators.*

Example 195 *$U(10)$ is cyclic since, as we have seen, $U(10) = \langle 3 \rangle$ and also $U(10) = \langle 7 \rangle$.*

Example 196 *$U(8)$ is not cyclic. $U(8) = \{1, 3, 5, 7\}$. $\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{1, 3\}$, $\langle 5 \rangle = \{1, 5\}$, $\langle 7 \rangle = \{1, 7\}$. So we see that there does not exist an element a of $U(8)$ such that $U(8) = \langle a \rangle$.*

4.2 Properties of Cyclic Groups

4.2.1 Elements of a Cyclic Groups

Since the elements of a cyclic group are the powers of an element, properties of cyclic groups are closely related to the properties of the powers of an element. We begin with properties we have already encountered in the homework problems.

Theorem 197 *Every cyclic group is Abelian*
Proof. *The elements of cyclic groups are of the form a^i. Commutativity amounts to proving that $a^i a^j = a^j a^i$.*

$$\begin{aligned} a^i a^j &= a^{i+j} \\ &= a^{j+i} \text{ addition of integers is commutative} \\ &= a^j a^i \end{aligned}$$

■

The next theorem tells us what the elements of a cyclic group are. It also gives us a criterion for $a^i = a^j$. This is an important theorem, which has several corollaries.

Theorem 198 *Let G be a group and $a \in G$.*

1. *If a has infinite order, then $a^i = a^j \iff i = j$. Hence, $\langle a \rangle = \left\{e, a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, ...\right\}$*
2. *If $|a| = n < \infty$, then $a^i = a^j \iff n \mid (i - j)$ and $\langle a \rangle = \left\{e, a, a^2, a^3, ..., a^{n-1}\right\}$.*

Proof. *The various results of this theorem have already been proven in the homework problems. We repeat the proof here to have all its important elements together.*

1. *We need to prove both directions.*

$\Longrightarrow$ *Suppose that* $a^i = a^j \Longrightarrow a^{i-j} = 0$. *This is obviously true if* $i = j$. *Could it be true also if* $i \neq j$? *The answer is no, otherwise* a *would have finite order.*

$\Longleftarrow$ *This direction is trivial.*

2. *There are two things to prove here. First, we prove that* $\langle a \rangle = \left\{e, a, a^2, a^3, ..., a^{n-1}\right\}$. *Clearly,* $\left\{e, a, a^2, a^3, ..., a^{n-1}\right\} \subseteq \langle a \rangle$ *by closure since* $\langle a \rangle$ *is a subgroup of* G. *We now show these are the only elements* $\langle a \rangle$ *contains . If* a^k *is an arbitrary element of* $\langle a \rangle$ *then by the division algorithm,there exits integers* q *and* r *with* $0 \leq r < n$ *such that* $k = nq + r$. *Therefore,* $a^k = a^{nq+r} = (a^n)^q a^r = a^r$ *so,* $a^r \in \left\{e, a, a^2, a^3, ..., a^{n-1}\right\}$. *Finally, we prove* $a^i = a^j \Longleftrightarrow n \mid (i - j)$. *There are two directions to prove.*

   $\Longrightarrow$ *Suppose* $a^i = a^j \Longrightarrow a^{i-j} = e$. *Either* $i - j = 0$ *in which case* $n \mid (i - j)$ *or* $i \neq j$. *By the division algorithm, there exists integers* q *and* r *such that* $i - j = qn + r$ *with* $0 \leq r < n$. *Hence, as we saw above,* $a^{i-j} = a^r = e$. *If we did not have* $r = 0$ *this would contradict the fact that* $|a| = n$. *Thus,* $n \mid (i - j)$.

   $\Longleftarrow$ *Suppose that* $n \mid (i - j)$ *then there exists an integer* k *such that* $i - j = kn$. *Hence* $a^{i-j} = a^{kn} = (a^n)^k = e$. *So we have* $a^{i-j} = e \Longrightarrow a^i a^{-j} = e \Longrightarrow a^i = a^j$.

■

Remark 199 *Let us make a few remarks before we continue.*

1. *The second part of the theorem says that if* $|a| = n$ *and* $a^m = e$ *then* $n \mid m$.
2. *The second part of the theorem also says If* $|a| = n < \infty$, *then* $a^i = a^j \Longleftrightarrow i \bmod n = j \bmod n$. *Note that this way of saying it resembles more the first part of the theorem.*
3. *If* $|a| = n$ *then* $a^i a^j = a^r$ *where* $(i + j) \bmod n = r$. *Indeed, by the division algorithm* $i + j = nq + r$ *where* $0 \leq r < n$ *so that*

$$\begin{aligned} a^i a^j &= a^{i+j} \\ &= a^{nq+r} \\ &= (a^n)^q a^r \\ &= ea^r \\ &= a^r \end{aligned}$$

Corollary 200 $|a| = |\langle a \rangle|$.
Proof. *If* $|a|$ *is infinite, then* $\langle a \rangle = \left\{e, a, a^2, a^3, ...\right\}$ *so* $|\langle a \rangle|$ *is also infinite . If* $|a| = n < \infty$, $\langle a \rangle = \left\{e, a, a^2, a^3, ..., a^{n-1}\right\}$ *so that* $|\langle a \rangle| = n$. *In both cases, the two are equal.* ■

Corollary 201 *If $|a| < \infty$ then $a^k = e \implies |a| \mid k$.*
Proof. *$a^k = e \implies a^k = a^0$ hence, from the theorem, $|a| \mid (k-0)$.* ■

The above theorems and corollaries basically say that no matter what cyclic group we are working with, if it has order n, then the operation in the group amounts to addition $\bmod n$ and hence that group can be associated with $\mathbb{Z}_n$. Indeed, if $|\langle a \rangle| = n$ then $a^i a^j = a^r$ where $(i+j) \bmod n = r$. If the cyclic group has infinite order, then it can be associated with $\mathbb{Z}$ for the same reasons.

We illustrate the theorem and its corollaries with a few examples.

Example 202 *Suppose G is a finite group and $a \in G$. If $|a| = 6$, then $\langle a \rangle = \left\{e, a, a^2, a^3, a^4, a^5\right\}$. Moreover,*

$$\begin{aligned} ... &= a^{-6} = a^0 = a^6 = a^{12} = ... \\ ... &= a^{-5} = a = a^7 = ... \\ ... &= a^{-4} = a^2 = a^8 = ... \end{aligned}$$

Example 203 *Suppose G is a finite group and $a \in G$. If $|a| = 10$, then the powers of a equal to a^4 are $..., a^{-6}, a^4, a^{14}, a^{24}, ...$*

Example 204 *Suppose G is a finite group and $a \in G$. What are the possibilities for $|a|$ if $a^6 = e$?*
Since $|a| \mid 6$, $|a| = 1, 2, 3, 6$.

Example 205 *Same question as above if $a^7 = e$.*
Since $|a| \mid 7$, $|a| = 1, 7$.

4.2.2 Order of a Cyclic Group and of its Elements, Generators of a Cyclic Group

The next theorem and corollaries are related to the order of a^k and the groups generated by it. They will help us find generators of a cyclic group.

Theorem 206 ($\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle$) *Let G be a group and $a \in G$ such that $|a| = n$. Suppose further that $k \in \mathbb{Z}^+$. Then:*

1. $\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle$
2. $\left|a^k\right| = \dfrac{n}{\gcd(n,k)}$.

Proof. *There two things to prove.*

1. $\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle$. *We prove inclusion both ways.*
   - $\left\langle a^k \right\rangle \subseteq \left\langle a^{\gcd(n,k)} \right\rangle$. *Let $d = \gcd(n,k)$. So, in particular, d is a divisor of k so there exists an integer r such that $k = dr$. So, $a^k = \left(a^d\right)^r$. This means that $a^k \in \left\langle a^d \right\rangle$ hence $\left\langle a^k \right\rangle \subseteq \left\langle a^{\gcd(n,k)} \right\rangle$ by closure.*

- $\left\langle a^{\gcd(n,k)}\right\rangle \subseteq \left\langle a^k\right\rangle$. *With d as above, we know there exist integers s and t such that $d = ns + kt$. So,*

$$\begin{aligned} a^d &= a^{ns+kt} \\ &= (a^n)^s \left(a^k\right)^t \\ &= e\left(a^k\right)^t \\ &= \left(a^k\right)^t \end{aligned}$$

Therefore, $a^d \in \left\langle a^k\right\rangle$ and so $\left\langle a^d\right\rangle \subseteq \left\langle a^k\right\rangle$ by closure.

2. $\left|a^k\right| = \dfrac{n}{\gcd(n,k)}$. *Here, we actually prove a stronger result. We prove that if d is a positive divisor of n, then $\left|a^d\right| = \dfrac{n}{d}$. Clearly, $\left(a^d\right)\dfrac{n}{d} = a^n = e$, so that $\left|a^d\right| \leq \dfrac{n}{d}$. We cannot have $\left|a^d\right| < \dfrac{n}{d}$. If we did, that is it there existed $i < \dfrac{n}{d}$ such that $\left|a^d\right| = i$, then $a^{di} = e$ and $di < n$ which would contradict $|a| = n$. Thus, $\left|a^d\right| = \dfrac{n}{d}$. This is true for every positive divisor of n. $\gcd(n,k)$ is such a divisor. So, we have: $\left|a^k\right| = \left|\left\langle a^k\right\rangle\right| = \left|\left\langle a^{\gcd(n,k)}\right\rangle\right| = \left|a^{\gcd(n,k)}\right| = \dfrac{n}{\gcd(n,k)}$.*

■

In proving part 2 of the theorem, we actually proved a stronger result we now state as a theorem.

Theorem 207 *Let G be a group, $a \in G$ such that $|a| = n$ and d a positive divisor of n. Then, $\left|a^d\right| = \dfrac{n}{d}$.*

Proof. *This result was proven in the proof of the previous theorem.* ■

Example 208 *If $\langle a\rangle$ is a cyclic group of order 10, then $\left|a^4\right| = \dfrac{10}{\gcd(10,4)} = 5$.*

Example 209 *In $\mathbb{Z}_{12}$, $|3| = \left|1^3\right| = \dfrac{12}{3} = 4$.*

Example 210 *In $\mathbb{Z}_6$, recall that $\langle 2\rangle = \{0,2,4\}$ and $\langle 4\rangle = \{0,4,2\}$. We see that $|2| = |4| = 3$. This is what our formula would also give us. since $2 = 1^2$ so $|2| = \left|1^2\right| = \dfrac{6}{\gcd(2,6)} = 3$ and $4 = 1^4$ so $|4| = \left|1^4\right| = \dfrac{6}{\gcd(4,6)} = 3$. We also see that $\langle 2\rangle = \langle 4\rangle$, which is what the theorem told us.*

Several important corollaries follow from this theorem. Remembering that the elements of a cyclic group $\langle a\rangle$ are of the form a^k, we try to determine when two elements a^i and a^j generate the same subgroup and when they generate the entire cyclic group.

Corollary 211 (Order of Elements in a Finite Cyclic Group) *In a finite cyclic group, the order of an element divides the order of the group.*
Proof. *The elements of a finite cyclic group generated by a are of the form* a^k. *If* $|a| = n$, *then* $|\langle a\rangle| = n$. *By the theorem,* $\left|a^k\right| = \dfrac{n}{\gcd(n,k)}$ *which is a divisor of* n. ■

Corollary 212 *Let* $|a| = n$. *Then:*

1. $\left\langle a^i\right\rangle = \left\langle a^j\right\rangle \iff \gcd(n,i) = \gcd(n,j)$.
2. $\left|a^i\right| = \left|a^j\right| \iff \gcd(n,i) = \gcd(n,j)$.

Proof. *We have two parts to prove.*

1. *We know that* $\left\langle a^i\right\rangle = \left\langle a^{\gcd(n,i)}\right\rangle$, *so we need to prove that* $\left\langle a^{\gcd(n,i)}\right\rangle = \left\langle a^{\gcd(n,j)}\right\rangle \iff \gcd(n,i) = \gcd(n,j)$. *Clearly, if* $\gcd(n,i) = \gcd(n,j)$ *then* $\left\langle a^{\gcd(n,i)}\right\rangle = \left\langle a^{\gcd(n,j)}\right\rangle$. *Now, assume that* $\left\langle a^{\gcd(n,i)}\right\rangle = \left\langle a^{\gcd(n,j)}\right\rangle$. *Then,* $\left|a^{\gcd(n,i)}\right| = \left|a^{\gcd(n,j)}\right| \implies \dfrac{n}{\gcd(n,i)} = \dfrac{n}{\gcd(n,j)} \implies \gcd(n,i) = \gcd(n,j)$.
2. *If* $\left|a^i\right| = \left|a^j\right|$ *then* $\dfrac{n}{\gcd(n,i)} = \dfrac{n}{\gcd(n,j)} \implies \gcd(n,i) = \gcd(n,j)$. *Conversely, if* $\gcd(n,i) = \gcd(n,j) \implies \left\langle a^i\right\rangle = \left\langle a^j\right\rangle \implies \left|a^i\right| = \left|a^j\right|$ *since* $|a| = |\langle a\rangle|$.

■

Corollary 213 (Generators of a Finite Cyclic Group) *Let* $|a| = n$. *Then:*

1. $\langle a\rangle = \left\langle a^j\right\rangle \iff \gcd(n,j) = 1$.
2. $|a| = \left|a^j\right| \iff \gcd(n,j) = 1$.

Proof. *This is just the theorem with* $i = 1$, *and noting that* $\gcd(n,1) = 1$. ■

Corollary 214 (Generators of $\mathbb{Z}_n$) *Let* $k \in \mathbb{Z}_n$. k *is a generator of* $\mathbb{Z}_n \iff \gcd(n,k) = 1$.
Proof. *Again, we apply the theorem knowing that* $\mathbb{Z}_n = \langle 1\rangle$ *and remembering that the operation in* $\mathbb{Z}_n$ *is addition* $\bmod n$ *so that* $1^k = k$. ■

The theorem and corollaries tell us that once we know one generator of a cyclic group, we can find all the other generators easily.

Example 215 *In* $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$, *the generators of* $\mathbb{Z}_6$ *are the integers* k *between* 0 *and* 5 *such that* $\gcd(6,k) = 1$ *that is* $1, 5$. *We can verify that,* $\langle 1\rangle = \{0,1,2,3,4,5\}$ *and* $\langle 5\rangle = \{0,5,4,3,2,1\} = \{0,1,2,3,4,5\}$ *but* $\langle 0\rangle = \{0\}$, $\langle 2\rangle = \{0,2,4\}$, $\langle 3\rangle = \{0,3\}$, $\langle 4\rangle = \{0,4,2\} = \{0,2,4\}$.

Example 216 *Suppose that* $\langle a\rangle$ *is a cyclic group of order* 10, *then the generators of* $\langle a\rangle$ *are the elements* a^k *for which* $\gcd(10,k) = 1$ *that is when* $k = 1, 3, 7, 9$.

4.3 Classification of Cyclic Groups

We now focus an the subgroups of a cyclic group. We will learn to determine how many subgroups a given cyclic group has, how to find them and what their order is.

We give the next theorem without proof.

Theorem 217 (Fundamental Theorem of Cyclic Groups) *Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of every subgroup of $\langle a\rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k, namely $\left\langle a^{\frac{n}{k}} \right\rangle$.*

Example 218 *Let us see what this theorem means. Suppose that $G = \langle a\rangle$ and $|a| = |G| = 30$. The divisors of 30 are $1, 2, 3, 5, 6, 10, 15$ and 30. G has one and only one subgroup of order each of these divisors. They are $\left\langle a^{\frac{30}{k}} \right\rangle$ for each $k = 1, 2, 3, 5, 6, 10, 15$ and 30. The table below gives us for each order what the subgroup is and what its generator is.*

Order	Generator	Group
1	$\langle a^{30}\rangle$	$\{e\}$
2	$\langle a^{15}\rangle$	$\{e, a^{15}\}$
3	$\langle a^{10}\rangle$	$\{e, a^{10}, a^{20}\}$
5	$\langle a^{6}\rangle$	$\{e, a^{6}, a^{12}, a^{18}, a^{24}\}$
6	$\langle a^{5}\rangle$	$\{e, a^{5}, a^{10}, a^{15}, a^{20}, a^{25}\}$
10	$\langle a^{3}\rangle$	$\{e, a^{3}, a^{6}, a^{9}, a^{12}, a^{15}, a^{18}, a^{21}, a^{24}, a^{27}\}$
15	$\langle a^{2}\rangle$	$\{e, a^{2}, a^{4}, ..., a^{28}\}$
30	$\langle a\rangle$	$\{e, a, a^{2}, a^{3}, ..., a^{29}\}$

Corollary 219 (Subgroups of $\mathbb{Z}_n$) *For each positive divisor k of n, the set $\left\langle \frac{n}{k} \right\rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k; moreover these are the only subgroups of $\mathbb{Z}_n$.*

Proof. *This follows from the theorem if we remember that $\mathbb{Z}_n = \langle 1\rangle$ and since the operation in this group is addition $\bmod n$, $1^{\frac{n}{k}}$ means $\frac{n}{k}$.* ■

Example 220 *Similar to the above examples, we let $G = \mathbb{Z}_{30}$. The table below lists the subgroups of $\mathbb{Z}_{30}$ and their generator.*

Order	Generator	Group
1	$\langle 30 \rangle$	$\{0\}$
2	$\langle 15 \rangle$	$\{0, 15\}$
3	$\langle 10 \rangle$	$\{0, 10, 20\}$
5	$\langle 6 \rangle$	$\{0, 6, 12, 18, 24\}$
6	$\langle 5 \rangle$	$\{0, 5, 10, ..., 25\}$
10	$\langle 3 \rangle$	$\{0, 3, 6, ..., 27\}$
15	$\langle 2 \rangle$	$\{0, 2, 4, ..., 28\}$
30	$\langle 1 \rangle$	$\{0, 1, 2, 3, ..., 29\}$

We finish by stating two theorems which give the number of elements of a specific order in a finite group.

Definition 221 (Euler Phi Function) *Let $n \in \mathbb{Z}^+$. The **Euler phi function** of n, denoted $\phi(n)$ is the number of positive integers less than n and relatively prime to n and we set $\phi(1) = 1$.*

Example 222 *$\phi(10) = 4$.*

Example 223 *The table below gives $\phi(n)$ for $n = 1, 2, ..., 15$.*

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\boldsymbol{\phi}(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Example 224 *By definition $|U(n)| = \phi(n)$.*

Theorem 225 *If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.*
Proof. *There is exactly one group of such order, call it $\langle a \rangle$. Then, every element of order d also generates $\langle a \rangle$ (since there is only one group of such order, and the order of the group generated by an element of order d is also d). So, counting the elements of order d is the same as counting the elements which can generate $\langle a \rangle$. We know that an element a^k generates $\langle a \rangle$ if and only if $\gcd(k, d) = 1$. This number is precisely $\phi(d)$.* ■

Example 226 *In $\mathbb{Z}_8$, there are $\phi(8) = 4$ elements of order 8.*

Example 227 *In $\mathbb{Z}_{64}$, there are $\phi(8) = 4$ elements of order 8.*

Example 228 *In $\mathbb{Z}_{800}$, there are $\phi(8) = 4$ elements of order 8.*

Corollary 229 *In a finite group, the number of elements of order d is divisible by $\phi(d)$.*

4.4 Problems

- Do # 1, 2, 3, 4, 5, 9, 10, 11, 13, 15, 17, 19, 21,23, 24, 29, 31 on pages 81 and following.
- Do # 1, 2 on page 91.