PMATH 336: INTRODUCTION TO GROUP THEORY WITH APPLICATIONS
NOTES FOR WEEK 3

INSTRUCTOR: ARUNDHATHI KRISHNAN

4. Cyclic Groups

4.1. **Properties of Cyclic Groups.** We recap the definition of a cyclic group.

Definition 4.1.1. A group G is said to be cyclic if there exists an element $a \in G$ such that $G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$.

Example 4.1.2.

(i) The group $(\mathbb{Z}, +)$ is cyclic with generators 1 and -1. Recall here that for $n \in \mathbb{N}$, "a^n" translates to $a + a + \ldots + a$ n times and $a^{-1} = -a$ for $a \in \mathbb{Z}$. Clearly any positive integer n can be written as $1 + \ldots + 1$ n times and negative integer $-n$ as $-1 - \ldots - 1$ n times. By definition, a^0 here is the identity 0.

(ii) The group $\mathbb{Z}_n$ with addition mod n for $n \in \mathbb{N}$ is cyclic with generators 1 and $(n-1) \equiv (-1) \mod n$. In some cases, $\mathbb{Z}_n$ may have other generators. For example, $\mathbb{Z}_7 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle$! $\mathbb{Z}_8$ has generators $1, 3, 5, 7$. We will formalize exactly what generators $\mathbb{Z}_n$ has in Corollary 4.1.11.

(iii) We already saw that $U(10) = \langle 3 \rangle = \langle 7 \rangle$.

(iv) On the other hand, $U(8)$ is not cyclic. Indeed, $U(8) = \{1, 3, 5, 7\}$ and $\langle 1 \rangle = \{1\}, \langle 3 \rangle = \{3, 1\}, \langle 5 \rangle = \{5, 1\}$ and $\langle 7 \rangle = \{7, 1\}$.

(v) Is the quaternion group cyclic? Evaluate $\langle a \rangle$ for each $a \in Q = \{1, -1, i, -i, j, -j, k, -k\}$ to check!

We now examine various properties of cyclic groups and subgroups.

Theorem 4.1.3. *Let G be a group and $a \in G$. If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order, say $n \in \mathbb{N}$, then $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$, and $a^i = a^j$ if and only if n divides $j - i$.*

Proof. Suppose a has infinite order and $a^i = a^j$. Then $a^{j-i} = e$. But as a has infinite order, $j - i = 0$, so $j = i$. If $i = j$, of course $a^i = a^j$.

Next, suppose a has finite order equal to n, then $a^n = e$. It is clear that $\{e, a, \ldots, a^{n-1}\} \subset \langle a \rangle$. We are left to show the other inclusion. Suppose $a^k \in \langle a \rangle$. By the division algorithm, there exist unique $q, r \in \mathbb{Z}$ such that $k = qn + r$ with $0 \leq r < n$. Hence $a^k = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r$, so $a^k \in \{e, a, \ldots, a^{n-1}\}$.

Finally, we are left to show that if $|\, a \,| = n$, then $a^i = a^j$ if and only n divides $j - i$. Suppose $a^i = a^j$, then $a^{j-i} = e$. By the division algorithm, there exist $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $j - i = qn + r$. Hence $e = a^{j-i} = (a^n)^q a^r = e^q a^r = a^r$. But by the definition of order of an element, n is the *least* positive integer such that $a^n = e$. So we must have $r = 0$ and hence $j - i = qn$, so that n divides $j - i$.

Conversely, suppose n divides $j - i$, then there exists $q \in \mathbb{Z}$ such that $j - i = nq$. Hence $a^{j-i} = (a^n)^q = e$, so that $a^j = a^i$.

□

Theorem 4.1.3 tells us immediately that the order of a cyclic subgroup generated by an element is equal to the order of the element itself as there are precisely $|\,a\,|$ elements in $\langle a\rangle$, both when $|\,a\,|$ is finite and infinite. This also explains why we use the same terminology for the order of both a group and an element of a group.

Corollary 4.1.4. *Let G be a group and $a \in G$. Then $|\,a\,| = |\,\langle a\rangle\,|$.*

Proof. In Theorem 4.1.3 we showed that if a has finite order $n \in \mathbb{N}$, then $\langle a\rangle = \{e, a, \ldots, a^{n-1}\}$, which clearly has n elements. On the other hand, if a is of infinite order, then Theorem 4.1.3 gives that $a^j \neq a^i$ for distinct i and j in $\mathbb{Z}$. Hence the group $\langle a\rangle = \{e, a, a^2, \ldots,\}$ is of infinite order. □

Corollary 4.1.5. *Let G be a group and $a \in G$ be such that $a^k = e$. Then $|\,a\,|$ divides k.*

Proof. Let $|\,a\,| = n$. As $a^k = e = a^0$, by Theorem 4.1.3, n divides $k - 0$, that is $n|k$.

□

Theorem 4.1.3 actually tells us the following. In a cyclic group of order n, multiplication of powers of a corresponds to the addition of the powers mod n. Indeed, if $a^n = e$, then $a^{n+1} = a, a^{n+2} = a^2, \ldots$, and $a^i a^j = a^{(i+j) \mod n}$ for $i, j \in \mathbb{Z}$. Hence a cyclic group of order n behaves exactly like $\mathbb{Z}_n$ with addition modulo n. Similarly, a cyclic group of order ∞ behaves just like $\mathbb{Z}$ with addition, as products of powers of the generator a correspond to adding the powers of a in $\mathbb{Z}$. We formalize what we mean by "behaves like" when we talk about group homomorphisms.

In the next theorem, we show that if we know the order of an element $a \in G$, then we can compute the order of a^k for any $k \in \mathbb{N}$.

Theorem 4.1.6. *Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k\rangle = \langle a^{\gcd(n,k)}\rangle$ and $\left|\, a^k \,\right| = \frac{n}{\gcd(n,k)}$.*

Proof. Let $d = \gcd(n, k)$. Then $k = dq$ for some $q \in \mathbb{Z}$ and $a^k = (a^d)^q$, so that $\langle a^k\rangle \subset \langle a^d\rangle$. To show the other inclusion, recall from the property of the gcd that there exists $s, t \in \mathbb{Z}$ such that $d = ns + kt$. Hence $a^d = a^{ns+kt} = (a^n)^s(a^k)^t = e(a^k)^t = (a^k)^t \in \langle a^k\rangle$, so that $\langle a^d\rangle \subset \langle a^k\rangle$. Thus, in fact, $\langle a^d\rangle = \langle a^k\rangle$.

Next, let b be any positive divisor of n. Then $(a^b)^{\frac{n}{b}} = a^n = e$, so that $\left|\, a^b \,\right| \leq \frac{n}{b}$. But if $i < \frac{n}{b}$, then $(a^b)^i \neq e$ as $bi < n$. Hence $\left|\, a^b \,\right| = \frac{n}{b}$ for any divisor b of n. In particular, for $d = \gcd(n, k)$, $\left|\, a^d \,\right| = \frac{n}{d}$. Altogether, along with Corollary 4.1.4 we get

$$\left|\, a^k \,\right| = \left|\, \langle a^k\rangle \,\right| = \left|\, \langle a^d\rangle \,\right| = \left|\, a^d \,\right| = \frac{n}{d} = \frac{n}{\gcd(n,k)}.$$

□

The advantage of Theorem 4.1.6 is that we can consider a more convenient generator of a given cyclic subgroup.

Example 4.1.7. Consider the group $\mathbb{Z}_{24}$. Then $\langle 21\rangle = \langle \gcd(21, 24)\rangle = \langle 3\rangle$ which is the group given by $\{3, 6, 9, 12, 15, 18, 21, 0\}$. Similarly, in $\mathbb{Z}_{27}$, $\langle 25\rangle = \langle \gcd(25, 27)\rangle = \langle 1\rangle = \mathbb{Z}_{27}$.

As a consequence of Theorem 4.1.6 we get the following corollary which gives that the order of *any* element of a cyclic group divides the order of the group.

Corollary 4.1.8. *In a finite cyclic group, the order of an element divides the order of the group.*

Proof. Let $G = \langle a \rangle$ and $a^k \in G$ for some $k \in \mathbb{Z}$, and let $|\, G \,| = |\, a \,| = n$. By Theorem 4.1.6, $\left|\, a^k \,\right| = \frac{n}{\gcd(n,k)}$, so the order of a^k divides the order of G.

□

Corollary 4.1.9. *Let G be a group and $a \in G$ with $|\, a \,| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$, and $\left|\, a^i \,\right| = \left|\, a^j \,\right|$ if and only if $\gcd(n, i) = \gcd(n, j)$, for $i, j \in \mathbb{Z}$.*

Proof. Suppose $\gcd(n, i) = \gcd(n, j)$. Then by Theorem 4.1.6 $\langle a^i \rangle = \langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle = \langle a^j \rangle$. Conversely, suppose $\langle a^i \rangle = \langle a^j \rangle$, then $\left|\, a^i \,\right| = \left|\, a^j \,\right|$, which implies by the second part of Theorem 4.1.6 that $\frac{n}{\gcd(n,i)} = \frac{n}{\gcd(n,j)}$ so that $\gcd(n, i) = \gcd(n, j)$.

The second part of the corollary follows by using $\left|\, a^i \,\right| = \frac{n}{\gcd(n,i)}$. □

Corollary 4.1.10. *Let $|\, a \,| = n$. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $\gcd(n, j) = 1$ and $|\, a \,| = \left|\, a^j \,\right|$ if and only if $\gcd(n, j) = 1$.*

Proof. Simply substitute $i = 1$ in Corollary 4.1.9. □

The above corollary allows us to identify *all* the generators of a cyclic subgroup once we have found one. We observed in the examples that $\mathbb{Z}_n$ always has 1 as a generator, but has other generators too. The following corollary lists out these generators explicitly.

Corollary 4.1.11. *An integer j in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $\gcd(n, j) = 1$.*

Proof. 1 is a generator of $\mathbb{Z}_n$, so $\mathbb{Z}_n = \langle 1 \rangle$. By Corollary 4.1.10, $\langle j \rangle = \langle 1 \rangle = \mathbb{Z}_n$ if and only if $\gcd(n, j) = 1$.

□

Example 4.1.12. We return to our favourite example $U(10) = \{1, 3, 7, 9\}$ with order 4. We know that $\langle 3 \rangle = U(10)$. By Corollary 4.1.10, $\langle 3^j \mod 10 \rangle = \langle 3 \rangle$ if and only if $\gcd(4, j) = 1$, so j is either 1 or 3, giving us that $3 = 3^1 \mod 10$ and $7 = 3^3 \mod 10$ are the generators of $U(10)$.

4.2. **Classification of subgroups of cyclic groups.**

Theorem 4.2.1. *Every subgroup of a cyclic group is cyclic. Moreover, if $|\, \langle a \rangle \,| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n. For each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k, namely $\langle a^{\frac{n}{k}} \rangle$.*

Proof. Let $G = \langle a \rangle$ and $H \leq G$. If $H = \{e\}$, it is of course cyclic with generator e. Suppose H is a proper non-trivial subgroup. We first show that there exists $t \in \mathbb{N}$ such that $a^t \in H$. Indeed, we must have $a^t \in H$ for some $t \in \mathbb{Z} \setminus \{0\}$, so a^{-t} is also in H as H is a subgroup, and one of t and $-t$ is in $\mathbb{N}$. Now let m be the smallest positive integer such that $a^m \in H$. We will prove that a^m generates H, that is, $H = \langle a^m \rangle$.

Suppose $a^k \in H$ for some $k \in \mathbb{Z}$. We will show that k must be a multiple of m. By the division algorithm, there exists $q, r \in \mathbb{Z}$ with $0 \leq r < m$ such that $k = qm + r$. Hence $a^k = a^{qm} a^r$, so that $a^r = a^k (a^m)^{-q} \in H$ as both a^k and a^m are in H. But due to the way we have chosen m, this means that $r = 0$, so that indeed k is a multiple of m and consequently $a^k \in \langle a^m \rangle$ and $H = \langle a^m \rangle$, a cyclic subgroup.

Suppose now that G has finite order and $|\, G \,| = |\, a \,| = n$. The order of H is given by $|\, \langle a^m \rangle \,| = |\, a^m \,| = \frac{n}{\gcd(n,m)}$, so the order of H divides n. We also note that $a^n = e \in H = \langle a^m \rangle$, and so m divides n.

Finally, let k be any positive divisor of n. Then $\langle a^{\frac{n}{k}} \rangle$ has order given by $\frac{n}{\gcd(n, \frac{n}{k})} = \frac{n}{\frac{n}{k}} = k$. On the other hand, we will show that any subgroup of order k of $\langle a \rangle$ must be equal to $\langle a^{\frac{n}{k}} \rangle$.By the first part of the theorem, the subgroup must be of the form $\langle a^m \rangle$ for some $m \in \mathbb{N}$ where $m|n$. As $m = \gcd(m, n)$, $k = |\langle a^m \rangle| = \frac{n}{\gcd(m,n)} = \frac{n}{m}$. Hence $m = \frac{n}{k}$ and $H = \langle a^{\frac{n}{k}} \rangle$. □

We get the following corollary for the cyclic group $\mathbb{Z}_n$.

Corollary 4.2.2. *For each $n \in \mathbb{N}$ and positive divisor k of n, the cyclic subgroup $\langle \frac{n}{k} \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k. Moreover, these are the only subgroups of $\mathbb{Z}_n$.*

Example 4.2.3. The group $\mathbb{Z}_{10}$ has subgroups of order $1, 2, 5$ and 10. These are $\langle 0 \rangle = \{0\}$, $\langle 5 \rangle = \{0, 5\}$, $\langle 2 \rangle = \{0, 2, 4, 6, 8\}$ and $\langle 1 \rangle = \mathbb{Z}_{10}$ respectively.

We now see how to enumerate the number of elements of a given order in a finite cyclic group, and in *any* finite group. For this we first define the Euler φ function.

Definition 4.2.4 (Euler φ function)**.** Define a function $\varphi : \mathbb{N} \to \mathbb{N}$ as follows:

$\varphi(1) = 1$; $\varphi(n) =$ number of positive integers less than n and relatively prime to n for $n \geq 2$.

φ is called the Euler φ function or the totient function.

We note straightaway from the definition of φ that the cardinality of $U(n)$ is equal to $\varphi(n)$ for each integer $n \geq 2$. We show now that $\varphi(d)$ gives the number of elements of order d in a cyclic group whose order is a multiple of d.

Theorem 4.2.5. *If d is a positive divisor of n, then the number of elements of order d in a cyclic group of order n is $\varphi(d)$.*

Proof. Let $G = \langle b \rangle$ with $|G| = |b| = n$, and H be the unique subgroup of order d given by $\langle b^{\frac{n}{d}} \rangle$. For the sake of simplicity, let us write $b^{\frac{n}{d}}$ as a and note that $|a| = d$. By Corollary 4.1.9, any element of order d also generates $\langle a \rangle$. Then by Corollary 4.1.10, an element a^k generates the subgroup $\langle a \rangle$ of order d if and only if $\gcd(k, d) = 1$. Hence the number of elements of order d in G is equal to $\varphi(d)$.

□

Note in the above theorem that the number of elements of order d in a cyclic group whose order is *any* multiple n of d depends only on d, and not on n.

Corollary 4.2.6. *In a finite group, the number of elements of order d is a multiple of $\varphi(d)$.*

Proof. If G has no elements of order d, the statement is true as $\varphi(d)$ divides 0. Suppose there exists $a \in G$ with $|a| = d$. Then $\langle a \rangle$ has $\varphi(d)$ elements of order d by Theorem 4.2.5. Suppose there exists $b \in G$ of order d such that $b \notin \langle a \rangle$. Then $\langle b \rangle$ has $\varphi(d)$ elements of order d. If there exists some c of order d such that $c \in \langle a \rangle \cap \langle b \rangle$, then $\langle a \rangle = \langle c \rangle = \langle b \rangle$, contradicting the fact that $b \notin \langle a \rangle$. We continue enumerating in this way for each element of order d in G which is not contained in the previously enumerated cyclic subgroups. As G is finite, this process comes to an end to give us that there exists a multiple of $\varphi(d)$ elements of order d. □

The Euler φ function is easily computed for powers of prime numbers, and for products of relatively prime integers.

Theorem 4.2.7.

(i) For a prime p and $n \in \mathbb{N}$, $\varphi(p^n) = p^n - p^{n-1}$.
(ii) Suppose $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$. Then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof.

(i) We want to enumerate the number of positive integers less than or equal to p^n that are relatively prime to p^n. There are p^n positive integers less than or equal to p^n. Let m be a positive integer less than or equal to p^n. To have $\gcd(p, m) > 1$, p must be a divisor of m, so m can be one of $p, 2p, \ldots, p^{n-1}p$. There are p^{n-1} such possibilities. Hence $\gcd(p^n, m) = 1$ for $p^n - p^{n-1}$ positive integers m less than p^n, hence $\varphi(p^n) = p^n - p^{n-1}$.

(ii) We want to enumerate the number of positive integers less than mn that are relatively prime to mn. We list the integers between 1 and mn out as follows:

$$\begin{array}{cccccc} 1 & m+1 & 2m+1 & \ldots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \ldots & (n-1)m+2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m & m+m & 2m+m & \ldots & (n-1)m+m = mn. \end{array}$$

For each $r \in \{1, \ldots, m\}$, the r-th row contains the elements $km + r$, for $k \in \{0, \ldots, n-1\}$. Now, clearly $gcd(km + r, m) = \gcd(r, m)$, so that all entries of the r-th row are relatively prime to m if and only if $\gcd(r, m) = 1$. If an integer r is not relatively prime to m, it is not relatively prime to mn, hence to compute $\varphi(mn)$ we can ignore all rows numbered by r where $\gcd(r, m) > 1$. Hence we only consider $\varphi(m)$ rows.

Now, within each of these $\varphi(m)$ rows, we only need those elements that are relatively prime to mn. As $\gcd(m, n) = 1$, the set $\{[0(m)+r], [1(m)+r], \ldots, [(n-1)m+r]\}$ consists of all the possible congruence classes under congruence mod n, for each r that is relatively prime to m. Out of these, we only need to consider those integers that are relatively prime to n, so there are $\varphi(n)$ such integers. By being in this row, they are also relatively prime to m, hence they are relatively prime to mn.

Thus in total, there are $\varphi(m)$ rows with $\varphi(n)$ elements each that are relatively prime to mn. Hence $\varphi(mn) = \varphi(m)\varphi(n)$.

□

References

[1] Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.