Section 6: Cyclic Groups

Theorem 0.1. *Any subgroup of a cyclic group is cyclic.*

Proof. Let H be a subgroup of a cyclic group $G = \langle a \rangle$. If $H = \langle e \rangle$, then H is cyclic, so assume there exists $a^m \in H$ such that $m > 0$. Let m be the smallest positive integer such that $a^m \in H$.

We claim that $H = \langle a^m \rangle$. We must show that every element of H is a power of a^m. Suppose $b = a^n$ is in H. By the division algorithm, we can find q and r, $0 \leq r < m$ such that $n = mq + r$. Therefore, $b = a^n = a^{mq+r} = (a^m)^q a^r$. Because H is a subgroup of G and $a^m \in H$, $(a^m)^k \in H$ for any $k \in \mathbb{Z}$. In particular, $(a^m)^{-q} \in H$, so $a^r = (a^m)^{-q} a^n \in H$. But, $0 \leq r < m$ and m was chosen to be the minimal positive integer such that $a^m \in H$. Therefore, we must have $r = 0$, so $b = a^n = (a^m)^q$ is a power of a^m. This holds for any element $b \in H$, so H is cyclic. □

Corollary 0.2. All subgroups of $\mathbb{Z}$ are of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$.

Proof. The previous theorem tells us that, if H is a subgroup of $\mathbb{Z}$, then either $H = \langle 0 \rangle$ or $H = \langle m \rangle$ where m is the smallest positive integer in H. Because $\langle m \rangle = m\mathbb{Z}$, $H = m\mathbb{Z}$. □

Theorem 0.3. *Let $G = \langle a \rangle$ be a cyclic group. If the order of G is infinite, then G is isomorphic to $\mathbb{Z}$. If the order of G is n, then G is isomorphic to $\mathbb{Z}_n$.*

This tells us that, even though we've been talking about cyclic groups in great generality, they really are just groups that we've seen before (and there are not too many choices!).

Proof. **Case 1: order is infinite.** We define a map $\phi : G \to \mathbb{Z}$ by $\phi(a^i) = i$. We first must ask ourselves if this map makes sense: if $h \neq k$, can $a^h = a^k$? Let's say $a^h = a^k$, which implies $a^{h-k} = e$. But, because G has infinite order, this implies that $h - k = 0$, or $h = k$. Therefore, if $h \neq k$, $a^h \neq a^k$. So, for any element $g \in G$, $g = a^m$ for a *unique* integer m. This implies the map is well-defined, one-to-one, and onto. Now we need to check that it satisfies the homomorphism condition:

$$\phi(a^i a^j) = \phi(a^{i+j}) = i + j$$

and

$$\phi(a^i) + \phi(a^j) = i + j$$

so

$$\phi(a^i a^j) = \phi(a^i) + \phi(a^j).$$

Case 2: order is finite, i.e. $a^m = e$ for some integers m. Let n be the smallest positive integer such that $a^n = e$. For any integer $s \in \mathbb{Z}$, $a^s = a^{nq+r}$ by the division algorithm, so $a^s = (a^n)^q a^r = ea^r = a^r$, where $0 \leq r < n$, so the elements $e = a^0, a^1, \ldots, a^{n-1}$ comprise all elements of G. Exactly as in Case 1, these elements are unique. Therefore, we can define a one-to-one and onto function $\phi : G \to \mathbb{Z}_n$ by $\phi(a^i) = i$. Because $a^n = e$, $a^i a^j = a^k$ where $k = i +_n j$. Therefore, we can check the homomorphism condition

$$\phi(a^i a^j) = i +_n j = \phi(a^i) +_n \phi(a^j).$$

□

See? For all the build-up, we have already encountered all possible cyclic groups!

Example 0.4. We define a subgroup $U_n = \{z \in \mathbb{C} \mid z^n = 1\} \subset (\mathbb{C}^\times, \times)$ called the n^{th} **roots of unity.** We can describe these complex numbers by the angle they make with the real axis: $U_n = \{\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \mid n \in \mathbb{Z}.\}$ This gives us a collection of n points on the unit circle, and we multiply these two complex numbers by adding their angles. From the previous theorem, we know that this is isomorphic to $\mathbb{Z}_n$, so occasionally will use this description to 'picture' finite cyclic groups.

Now, we will use everything we've done so far to classify all subgroups of finite cyclic groups. We already know they are cyclic, but we can say more about them. *Note: we did not have time for the proof in class today, but I left it here in case you would like to read it. You need to know this theorem for the exam, but you will not need to know the proof for the exam.*

Theorem 0.5. *Let G be a cyclic group with n elements, so $G = \langle a\rangle$ and $a^n = e$. Let $b \in G$ be $b = a^s$. Then, b generates a cyclic subgroup of G with n/d elements, where $d = \gcd(n, s)$. Furthermore, this uniquely determines the subgroup: $\langle a^s\rangle = \langle a^t\rangle$ if and only if $\gcd(n, s) = \gcd(n, t)$.*

Before getting to the proof, we give an alternate definition of the greatest common divisor.

Definition 0.6. The **greatest common divisor** of two integers r and s is the largest positive integer that divides both r and s and is equal to positive generator d of the cyclic group $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$. We write $d = \gcd(r, s)$.

Look in your book for more information on this! It is equivalent to the definition you already know. Let's use this to prove the theorem!

Proof. We know b generates a cyclic subgroup, so we just need to show that $H = \langle b\rangle = \langle a^s\rangle$ has exactly n/d elements. We know that H has m elements, where m is the minimal integer such that $b^m = (a^s)^m = e$. In other words, m is the minimal integer such that n divides sm.

Let $d = \gcd(n, s)$. By our new definition of gcd, there exist integers u, v such that $d = un+vs$. Because d divides n and s, we can divide by d to get $1 = u\frac{n}{d}+v\frac{s}{d}$. Because $\frac{n}{d}$ and $\frac{s}{d}$ are relatively prime, and $\frac{ms}{n} = \frac{m\frac{s}{d}}{\frac{n}{d}}$, we must have $\frac{n}{d}$ divides m. But, m was chosen to be the minimal integer such that n divides sm, and n definitely divides $s\frac{n}{d} = \frac{s}{d}n$, so we must have $\frac{n}{d} = m$. Therefore, H contains exactly n/d elements.

To see the last statement, we know G is isomorphic to $\mathbb{Z}_n$, so we just need to prove it for $G = \mathbb{Z}_n$. We know in this case that for any divisor d of n, $\langle d\rangle$ has exactly n/d elements and contains every element such that $\gcd(m, n) = d$, so there is only *one* subgroup of $\mathbb{Z}_n$ of order n/d, and the argument in the preceding paragraph shows that the generators of that subgroup are elements $m \in G$ such that $\gcd(n, m) = d$. □

Phrasing the last statement slightly differently, we have the following corollary:

Corollary 0.7. If a is a generator of a finite cyclic group G of order n, then the other elements of G are a^r where r is relatively prime to n.

Let's apply this in some examples.

Example 0.8. Find all subgroups (and all generators of each subgroup) of $\mathbb{Z}_{12}$.

We have a subgroup coming from each divisor of 12: 1, 2, 3, 4, 6, 12. The subgroups are $\langle 1\rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ generated by $1, 5, 7$, or 11 $\langle 2\rangle = \{0, 2, 4, 6, 8, 10\}$ generated by 2 or 10, $\langle 3\rangle = \{0, 3, 6, 9\}$ generated by 3 or 9, $\langle 4\rangle = \{0, 4, 8\}$ generated by 4 or 8, $\langle 6\rangle = \{0, 6\}$ generated by 6, or $\langle 0\rangle$ generated by 0.

Example 0.9. Find all subgroups (and generators of each subgroup) of $\mathbb{Z}_p$, where p is prime.
Ans: the only subgroups are $\langle 0 \rangle$ and $\mathbb{Z}_p$, and $\mathbb{Z}_p$ is generated by any nonzero element.