# NOTES ON GROUPS, MATH 369.101

## Cyclic groups

Cyclic groups are simple compared to most groups. Remember that saying $G$ is **cyclic** means that there is an $a \in G$ so that every $x \in G$ is $x = a^k$ for some $k \in \mathbb{Z}$.

**Proposition 1.** *If $G$ is a cyclic group and $|G|$ is infinite, then $G \cong \mathbb{Z}$. If $|G|$ is finite (say $n$ is a positive number so that $|G| = n$), then $G \cong \mathbb{Z}_n$.*

*Proof.* We know from before (Proposition 4 in the last set of notes) that there is an onto homomorphism $\varphi : \mathbb{Z} \to G$. Recall that $a = \varphi(1)$ is a generator of $G$.

**Case 1:** $|G|$ is infinite. Since $n$ is 1 added to itself $n$ times, $n = n \cdot 1 =$" $1^n$ " (see the note below). That means, since $a = \varphi(1)$ and $\varphi$ is a homomorphism that $\varphi(n) = a^n$. We know that $\varphi$ is onto.

To see that $\varphi$ is one-to-one, consider if $\varphi(n) = \varphi(m)$. In other words, $a^n = a^m$. If $m \neq n$, then assume $m < n$ (which we may do without loss of generality). Then $a^{n-m} = e$, and $n - m > 0$, which implies that $a$ has finite order. But then $|G| = |\langle a \rangle| = o(a)$ is finite, a contradiction. So $a^n = a^m$ implies $m = n$ and so $\varphi$ is one-to-one and is an isomorphism from $\mathbb{Z}$ to $G$.

**Note:** The reason for the quotes here is that we are not referring to repeated multiplication, as is usually done with powers of numbers. We wrote " $1^n$ " to make reference to how we've been writing group operations: $a^n$ is $a * a * \ldots * a$ ($n$ times). Since the group operation in $\mathbb{Z}$ is addition, this agrees in that setting with $a + a + \ldots + a$ ($n$ times).

**Case 2:** $|G|$ is finite. We again use our onto homomorphism $\varphi : \mathbb{Z} \to G$. Since $|G| = n$ is finite and $G = \langle a \rangle$, we know that $o(a) = n$. So $\varphi(n) = a^n = e$, implying $n \in \ker \varphi$. Moreover any multiple of $n$ is in $\ker \varphi$. Since $n = o(a)$, no smaller (in absolute value) power of $a$ equals the identity, and so $\ker \varphi = n\mathbb{Z}$.

Before the end of the semester, we will prove the Fundamental Theorem of Homomorphisms (for groups), which in this case says $\varphi(\mathbb{Z}) \cong \mathbb{Z}/\ker \varphi$. Since $\varphi$ is onto and $\ker \varphi = n\mathbb{Z}$ this implies

$$\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z} \cong G.$$

□

**Corollary 1.** *A subgroup of a cyclic group is also cyclic.*

---

*Date*: Nov. 16, Nov. 21.

*Proof.* Let $H$ be a subgroup of a cyclic group $G = \langle a \rangle$ and let $\varphi$ be the isomorphism from the Proposition (so $\varphi : \mathbb{Z} \to G$ or $\varphi : \mathbb{Z}_n \to G$, depending on whether $G$ is infinite or finite).

Then $\varphi^{-1}(H)$ is a subgroup of $\mathbb{Z}$ (or $\mathbb{Z}_n$), and the only subgroups of these groups are of the form $k\mathbb{Z}$ (or $k\mathbb{Z}_n$). That means that (in the case that $G$ is an infinite group)

$$H = \varphi(\varphi^{-1}(H)) = \varphi(k\mathbb{Z}) = \{a^{km} \mid m \in \mathbb{Z}\}$$

which is a cyclic group generated by $a^k$. □

**Corollary 2.** *Let $G = \langle a \rangle$ be a finite cyclic group with $|G| = n$. Then*

1. *for any $m \in \mathbb{Z}$, set $d = \gcd(m, n)$. Then $\langle a^m \rangle = \langle a^d \rangle$ as subgroups of $G$.*
2. *$a^k$ generates $G$ if and only if $\gcd(k, n) = 1$.*
3. *for any divisors $m$ and $k$ of $n$ (where $m, k$ might be equal to 1), $\langle a^m \rangle \subset \langle a^k \rangle$ if and only if $k$ divides $m$.*

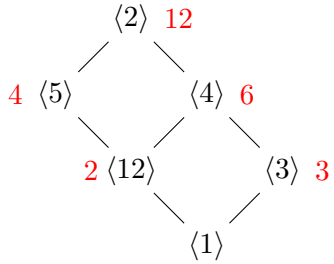
*Proof.* We know all these properties to hold true when translated to $\mathbb{Z}_n$. □

**Examples:**

The group $\mathbb{Z}_{13}^\times$ is cyclic, generated by (the congruence class of) 2. So $\langle 2 \rangle = \mathbb{Z}_{13}^\times$. In this group $o(12) = 2$, $o(3) = 3 = o(9)$, $o(5) = 4 = o(8)$, and $o(4) = 6 = o(10)$ and all other non-identity elements have order 12.

The group has proper subgroups: $\langle 3 \rangle \subset \langle 4 \rangle \subset \langle 2 \rangle$, and $\langle 12 \rangle \subset \langle 4 \rangle \subset \langle 2 \rangle$ $\langle 12 \rangle \subset \langle 5 \rangle \subset \langle 2 \rangle$.

We could draw the inclusions in a diagram as below. (The sizes of the subgroups are in red.)




**Exercise:** Create a similar diagram for $(\mathbb{Z}_{18})^\times$ or for $(\mathbb{Z}_{16})^\times$ (one of these groups is cyclic, and the other is not. If the group is not cyclic, there won't be a $\langle a \rangle$ subgroup at the top, just the group $(\mathbb{Z}_n)^\times$ with some number of subgroups directly below it).

## Normal subgroups

We want to construct "factor groups" like we did factor rings (that is, think of using a subgroup $H \subset G$ to make congruence classes, and have a group structure on those congruence classes).

The thing that would be like factor rings would be to define: for $a, b \in G$, set $a \sim b$ if $ab^{-1} \in H$. This is equivalent to saying $Hb = Ha$ as sets, where

$Ha$ is the set of all group elements that are of the form $xa$ for some $x \in H$, a **coset** of $H$.

Let us prove it.

**Proposition 2.** *Let $H$ be a subgroup of $G$ and consider two elements $a, b \in G$. Then the following are equivalent.*

(1) $ab^{-1} \in H$
(2) $a \in Hb$
(3) $Ha = Hb$

*Proof.* Suppose that $ab^{-1} \in H$, that is there is some $h \in H$ so that $ab^{-1} = h$. Then $a = hb \in Hb$, so $a \in Hb$.

Suppose that $a \in Hb$, then there is an $h \in H$ so that $a = hb$. Any element of $Ha$ has the form $xa$ for some $x \in H$, and we see that $xa = x(hb) = (xh)b \in Hb$, so $Ha \subset Hb$. Any element in $Hb$ is $xb$ for some $x \in H$. Since $a = hb$, $xb = x(h^{-1}a) = (xh^{-1})a \in Ha$, so $Hb \subset Ha$, and so $Ha = Hb$.

Suppose that $Ha = Hb$. Since $e \in H$, $a$ is an element of $Ha$ and so $a \in Hb$, and so there is an $h \in H$ with $a = hb$, which implies $ab^{-1} = h \in H$.

We have shown (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1). This implies that any one of the three conditions is true if and only if one of the others is true. □

Recall from the lemma right before Lagrange's theorem, that this is always an equivalence relation, so the sets $Ha$ partition $G$ and for a fixed $a$ the number of elements in $Ha$ (in the case that $H$ is finite) equals $|H|$, the number of elements in $H$, regardless of which $a$ was chosen.

We have yet to point it out explicitly, but if $|G| = n$ is finite, then since $|H|$ is a factor of $|G|$,

**Proposition 3.** *If $|G|$ is finite, the number of cosets of $H$ in $G$ is $|G|/|H|$. This number is called the* **index** *of $H$ in $G$ (sometimes written $[G : H]$).*

If $|G|$ is infinite then sometimes there are infinitely many cosets of $H$, sometimes a finite number. In the first case we say $H$ has infinite index, in the second case its index is the number of cosets.

Like in factor rings, we would like to define an operation through the operation of the group. Something like $Ha * Hc = H(a \cdot c)$, where $\cdot$ is the operation of $G$.

But there is a **problem**. We could have $b \neq a$ but $b \in Ha$, in which case $Hb = Ha$ by the above Proposition. This is not the problem, but it means that $Hc * Ha$ should equal $Hc * Hb$ – our answer should not depend on how we choose to represent the coset. But there are cases where $H(c \cdot a) \neq H(c \cdot b)$.

**Example:** Let $H = \{e, (1, 2)\}$ be the subgroup of $S_3$ generated by the transposition $(1, 2)$. Let's write out all the cosets.

Take $\tau_1 = (2,3)$ and $\tau_2 = (1,3)$. Then

$$H = \{e, (1,2)\}$$
$$H\tau_1 = \{(2,3), (1,2,3)\}$$
$$H\tau_2 = \{(1,3), (1,3,2)\}$$

Now, referring to the discussion of the **problem** above: consider this case, with $a = (2,3)$, $b = (1,2,3)$ and $c = (1,3)$.

Since $\tau_1 = (2,3)$ and $(1,2,3)$ are in the same coset (that is, $(2,3) \sim (1,2,3)$) then we have $H(2,3) = H(1,2,3)$.

So it ought to be that $H(1,3) * H(2,3) = H(1,3) * H(1,2,3)$ (that is, $Hc * Ha = Hc * Hb$). But is $H(c \cdot a) = H(c \cdot b)$?

Since $c \cdot a = (1,3)(2,3) = (1,3,2)$ and $c \cdot b = (1,3)(1,2,3) = (1,2)$, this would require $H(1,3,2)$ to equal $H(1,2) = H$, but these cosets are not the same!

But not all is lost. The answer is to focus on subgroups where this definition will work, and this is the reason for the following definition.

**Definition 1.** A subgroup $H \subset G$ is **normal** if for any $x \in G$ and any $h \in H$, $xhx^{-1} \in H$.

Technically our cosets here are "right cosets" and for a left coset you multiply by $a$ on the left. In general, a left coset of $H$ is not necessarily a right coset of $H$, but there is a one-to-one correspondence between left cosets and right cosets. We will stick with right cosets.

Notice that the subgroup $H = \{e, (1,2)\} \subset S_3$ from our example above is not normal: $(2,3)$ is the inverse of $(2,3)$, and we can calculate that $(2,3)(1,2)(2,3) = (2,3)(1,2,3) = (1,3) \notin H$.

However, the subgroup $\{e, (1,2,3), (1,3,2)\} \subset S_3$ is normal (use problem 2.3.13 from the homework):

for any $\sigma \in S_3$, $\sigma \cdot (1,2,3) \cdot \sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3))$ which is another 3-cycle, so it either equals $(1,2,3)$ or $(1,3,2)$.

**Observation:** If $G$ is an abelian group, then every subgroup of $G$ is normal (since $xhx^{-1} = h$ if $G$ is abelian). So, any subgroup of a cyclic group is normal, since cyclic groups are abelian. Also, for any $n$, any subgroup of $(\mathbb{Z}_n)^\times$ will be normal as $(\mathbb{Z}_n)^\times$ is abelian (since multiplication modulo $n$ is a commutative operation).

**Exercise 1:** Let $H = 4\mathbb{Z}_{24}$ be the cyclic subgroup of $\mathbb{Z}_{24}$ generated by the congruence class of 4. Write out all the cosets of $H$. How many elements are there in $\mathbb{Z}_{24}/H$? Does our proposed operation on cosets make $\mathbb{Z}_{24}/H$ cyclic?

**Exercise 2:** Consider the set of matrices

$$\mathfrak{M} = \left\{ \begin{pmatrix} \varepsilon & a \\ 0 & \delta \end{pmatrix} \;\middle|\; \text{where } \varepsilon, \delta \in \{1, -1\} \text{ and } a \in \mathbb{Z} \right\}.$$

Check that $\mathfrak{M}$, with matrix multiplication, is a group.

Find $M_1, M_2 \in \mathfrak{M}$ so that $M_1 M_2 \neq M_2 M_1$. Such matrices show that $\mathfrak{M}$ is not abelian.

Fix an integer $n$. Let $\mathfrak{N}(n) = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \;\middle|\; \text{where } a \in n\mathbb{Z} \right\}$. Show that $\mathfrak{N}(n)$ is a normal subgroup of $\mathfrak{M}$ for any choice of $n$.

Show also that $\mathfrak{M}(2) = \left\{ \begin{pmatrix} \varepsilon & a \\ 0 & \delta \end{pmatrix} \;\middle|\; \text{where } \varepsilon, \delta \in \{1, -1\} \text{ and } a \in 2\mathbb{Z} \right\}$ is a normal subgroup.

In the next class we will show that if $H$ is a normal subgroup, then we can define a group operation on cosets like we want to, and this gives us a new group, called a factor group.