2 Subgroups and Cyclic Groups

2.1 Review

Last time, we discussed the concept of a group, as well as examples of groups. In particular, a group is a set G with an associative composition law $G \times G \longrightarrow G$ that has an identity as well inverses for each element with respect to the composition law $\times$.

Our guiding example was that of the group of invertible $n \times n$ matrices, known as the **general linear group** ($GL_n(\mathbb{R})$ or $GL_n(\mathbb{C})$, for matrices over $\mathbb{R}$ and $\mathbb{C}$, respectively.)

Example 2.1
Let $GL_n(\mathbb{R})$ be the group of $n \times n$ invertible real matrices.

- **Associativity.** Matrix multiplication is associative; that is, $(AB)C = A(BC)$, and so when writing a product consisting of more than two matrices, it is not necessary to put in parentheses.
- **Identity.** The $n \times n$ identity matrix is $I_n = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$, which is the matrix with 1s along the diagonal and 0s everywhere else. It satisfies the property that $AI = IA = A$ for all $n \times n$ matrices A.
- **Inverse.** By the invertibility condition of GL_n, every matrix $A \in GL_n(\mathbb{R})$ has an inverse matrix A^{-1} such that $AA^{-1} = A^{-1}A = I_n$.

Furthermore, each of these matrices can be seen as a transformation from $\mathbb{R}^n \longrightarrow \mathbb{R}^n$, taking each vector $\vec{v}$ to $A\vec{v}$. That is, there is a bijective correspondence between matrices A and invertible transformations $T_A : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ taking $T_A(\vec{v}) = A\vec{v}$.

Another example that showed up was the integers under addition.

Example 2.2
The integers $\mathbb{Z}$ with the composition law $+$ form a group. Addition is associative. Also, $0 \in \mathbb{Z}$ is the additive identity, and $-a \in \mathbb{Z}$ is the inverse of any integer a.

On the other hand, the natural numbers $\mathbb{N}$ under addition would *not* form a group, because the invertibility condition would be violated.

Lastly, we looked at the symmetric group S_n.

Example 2.3
The **symmetric group** S_n is the permutation group of $\{1, \cdots, n\}$.

2.2 Subgroups

In fact, understanding S_n is important for group theory as a whole because *any* finite group "sits inside" S_n in a certain way[9], which we will begin to discuss today.

Guiding Question
What does it mean for a group to "sit inside" another group?

If a subset of a group satisfies certain properties, it is known as a *subgroup*.

[9] This is known as *Cayley's Theorem* and is discussed further in section 7.1 of Artin.

Definition 2.4
Given a group $(G, \cdot)$, a subset $H \subset G$ is called a **subgroup** if it satisfies:

- **Closure.** If $h_1, h_2 \in H$, then $h_1 \cdot h_2 \in H$.
- **Identity.** The identity element e in G is contained in H.
- **Inverse.** If $h \in H$, its inverse h^{-1} is also an element of H.

As notation, we write $H \leq G$ to denote that H is a subgroup of G.

Essentially, these properties consists solely of the necessary properties for H to also be a group under the same operation $\cdot$, so that it can be considered a subgroup and not just some arbitrary subset. In particular, any subgroup H will also be a group with the same operation, independent of the larger group G.

Example 2.5
The integers form a subgroup of the rationals under addition: $(\mathbb{Z}, +) \subset (\mathbb{Q}, +)$.

The rationals are more complicated than the integers, and studying simpler subgroups of a certain group can help with understanding the group structure as a whole.

Example 2.6
The symmetric group S_3 has a three-element subgroup $\{e, (123), (132)\} = \{e, x, x^2\}$.

However, the natural numbers $\mathbb{N} = \{0, 1, 2, \cdots\} \subset (\mathbb{Z}, +)$ are **not** a subgroup of the integers, since not every element has an inverse.

Example 2.7
The matrices with determinant 1, called the **special linear group**, form a subgroup of invertible matrices: $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$.

The special linear group is closed under matrix multiplication because $\det(AB) = \det(A)\det(B)$.

2.3 Subgroups of the Integers

The integers $(\mathbb{Z}, +)$ have particularly nice subgroups.

Theorem 2.8
The subgroups of $(\mathbb{Z}, +)$ are $\{0\}, \mathbb{Z}, 2\mathbb{Z}, \cdots$.[a]

[a] Where $n \in \mathbb{Z}$, $n\mathbb{Z}$ consists of the multiples of n, $\{nx : x \in \mathbb{Z}\}$.

This theorem demonstrates that the condition that a subset H of a group be a subgroup is quite strong, and requires quite a bit of structure from H.

Proof. First, $n\mathbb{Z}$ is in fact a subgroup.

- **Closure.** For $na, nb \in n\mathbb{Z}$, $na + nb = n(a + b)$.
- **Identity.** The additive identity is in $n\mathbb{Z}$ because $0 = n \cdot 0$.
- **Inverse.** For $na \in n\mathbb{Z}$, its inverse $-na = n(-a)$ is also in $n\mathbb{Z}$.

Now, suppose $S \subset \mathbb{Z}$ is a subgroup. Then clearly the identity 0 is an element of S. If there are no more elements in S, then $S = \{0\}$ and the proof is complete. Otherwise, pick some nonzero $h \in S$. Without loss of generality, we assume that $h > 0$ (otherwise, since $-h \in S$ as well by the invertibility condition, take $-h$ instead of h.) Thus, S contains at least one positive integer; let a be the smallest positive integer in S.

Then we claim that $S = a\mathbb{Z}$. If $a \in S$, then $a + a = 2a \in S$ by closure, which implies that $2a + a = 3a \in S$, and so on. Similarly, $-a \in S$ by inverses, and $-a + (-a) = -2a \in S$, and so on, which implies that $a\mathbb{Z} \subset S$.

Now, take any $n \in S$. By the Euclidean algorithm, $n = aq + r$ for some $0 \leq r < a$. From the subgroup properties, $n - aq = r \in S$ as well. Since a is the smallest positive integer in S, if $r > 0$, there would be a contradiction, so $r = 0$. Thus, $n = aq$, which is an element of $a\mathbb{Z}$. Therefore, $S \subset a\mathbb{Z}$.

From these two inclusions, $S = a\mathbb{Z}$ and the proof is complete. □

Corollary 2.9
Given $a, b \in \mathbb{Z}$, consider $S = \{ai + bj : i, j \in \mathbb{Z}\}$. The subset S satisfies all the subgroup conditions, so by Theorem 2.8, there is some d such that $S = d\mathbb{Z}$. In fact, $d = \gcd(a, b)$.

Proof. Let $e = \gcd(a, b)$. Since $a \in S$, $a = dk$ and $b = d\ell$ for some k, ℓ. Since the d from before divides a and b, it must also divide e, by definition of the greatest common divisor. Also, since $d \in S$, by the definition of S, $d = ar + bs$ for some r and b. Since e divides a and b, e divides both ar and bs and therefore d.

Thus, d divides e, and e divides d, implying that $e = d$. So $S = \gcd(a, b)\mathbb{Z}$. □

In particular, we have showed that $\gcd(a, b)$ can always be written in the form $ar + bs$ for some r, s.

2.4 Cyclic Groups

Now, let's discuss a very important type of subgroup that connects back to the work we did with $(\mathbb{Z}, +)$.

Definition 2.10
Let G be a group, and take $g \in G$. Let the **cyclic subgroup generated by** g be

$$\langle g \rangle \coloneqq {}^{a}\{\cdots g^{-2}, g^{-1}, g^{0} = e, g^{1}, g^{2}, \cdots\} \leq G.$$

[a] The $\coloneqq$ symbol is usually used by mathematicians to mean "is defined to be." Other people may use $\equiv$ for the same purpose.

Since $g^a \cdot g^b = g^{a+b}$, the exponents of the elements of a cyclic subgroup will have a related group structure to $(\mathbb{Z}, +)$.

Example 2.11
The identity element generates the trivial subgroup $\{e\} = \langle e \rangle$ of any group G.

There are also nontrivial cyclic subgroups.

Example 2.12
In S_3, $\langle (123) \rangle = \{e, (123), (132)\}$.

Evidently, a cyclic subgroup of any finite group must also be finite.

Example 2.13
Let $\mathbb{C}^\times$ be the group of nonzero complex numbers under multiplication. Then $2 \in \mathbb{C}$ will generate

$$\langle 2 \rangle = \{\cdots, 1/4, 1/2, 1, 2, 4, \cdots.\}$$

On the other hand, $i \in \mathbb{C}$ will generate

$$\langle i \rangle = \{1, i, -1, -i\}.$$

This example shows that a cyclic subgroup of an infinite group can be either infinite or finite.[10]

[10] Can you work out the cases for which $g \in \mathbb{C}$ the cyclic subgroup of $\mathbb{C}^\times$ is finite or infinite?

Guiding Question
What does a cyclic subgroup look like? Can they be classified?

Theorem 2.14
Let $S = \{n \in \mathbb{Z} : g^n = e\}$. Then S is a subgroup of $\mathbb{Z}$, so $S = d\mathbb{Z}$ or $S = \{0\}$, leading to two cases:

- If $S = \{0\}$, then $\langle g \rangle$ is infinite and all the g^k are distinct.
- If $S = d\mathbb{Z}$, then $\langle g \rangle = \{e, g, g^2, \cdots, g^{d-1}\} \subset G$, which is finite.

Proof. First, S must be shown to actually be a subgroup of $\mathbb{Z}$.

- **Identity.** The identity $0 \in S$ because $g^0 = e$.
- **Closure.** If $a, b \in S$, then $g^a = g^b = e$, so $g^{a+b} = g^a g^b = e \cdot e = e$, so $a + b \in S$.
- **Inverse.** If $a \in S$, then $g^{-a} = (g^a)^{-1} = e^{-1} = e$, so $a \in S$.

Now, consider the first case. If $g^a = g^b$ for any a, b, then multiplying on right by g^{-b} gives $g^a \cdot g^{-b} = g^{a-b} = e$. Thus, $a - b \in S$, and if $S = \{0\}$, then $a = b$. So any two powers of g can only be equal if they have the same exponent, and thus all the g^i are distinct and the cyclic group is infinite.

Consider the second case where $S = d\mathbb{Z}$. Given any $n \in \mathbb{Z}$, $n = dq + r$ for $0 \leq r < d$ by the Euclidean algorithm. Then $g^n = g^{dq} \cdot g^r = g^r$, which is in $\{e, g, g^2, \cdots, g^{d-1}\}$. □

Definition 2.15
So if $d = 0$, then $\langle g \rangle$ is infinite; we say that g has **infinite order.** Otherwise, if $d \neq 0$, then $|\langle g \rangle| = d$ and g has **order** d.

It is also possible to consider more than one element g.

Definition 2.16
Given a subset $T \subset G$, the subgroup generated by T is

$$\langle T \rangle := \{t_1^{e_1} \cdots t_n^{e_n} \mid t_i \in T, e_i \in \mathbb{Z}\}.$$

Essentially, $\langle T \rangle$ consists of all the possible products of elements in T. For example, if $T = \{t, n\}$, then

$$\langle T \rangle = \{\cdots, t^2 n^{-3} t^4, n^5 t^{-1}, \cdots\}.$$

Definition 2.17
If $\langle T \rangle = G$, then T **generates** G.[a]

[a] Given a group G, what is the smallest set that generates it? Try thinking about this with some of the examples we've seen in class!

Example 2.18
The set $\{(123), (12)\}$ generates S_3.

Example 2.19
The invertible matrices $GL_n(\mathbb{R})$ are generated by elementary matrices[a].

[a] The matrices giving row-reduction operations.