PMATH 336: INTRODUCTION TO GROUP THEORY WITH APPLICATIONS
NOTES FOR WEEK 2

INSTRUCTOR: ARUNDHATHI KRISHNAN

3. Subgroups

3.1. Definition and basic properties.

Definition 3.1.1. A subset H of a group G which is itself a group under the operation of G is called a subgroup of G. This is denoted by $H \leq G$.

Suppose $H \leq G$ and $H \neq G$, then H is called a *proper* subgroup of G. G is, of course, a subgroup of itself. The subgroup $\{e\}$ is called the *trivial* subgroup of G; any subgroup H of G which is not the trivial subgroup is called a non-trivial subgroup of G.

We have already seen some examples of subgroups of groups. For instance, consider $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$ for $n \in \mathbb{N}$ where the operation is matrix multiplication; $\mathbb{Q} \leq \mathbb{R}$, where the operation is addition; $\mathbb{Q}^+ \leq \mathbb{R}^*$, where the operation is multiplication; and $\{1, -1, i, -i\} \leq \mathbb{C}^*$, where the operation is multiplication.

The following theorem shows that we do not need to check all the group axioms to determine whether a subset of a group is a subgroup or not.

Theorem 3.1.2. *Let G be a group and H be a non-empty subset of G. If $ab^{-1} \in H$ for all $a, b \in H$, then H is a subgroup of G.*

Proof. For H to be a subgroup, we need the following:

(i) The associativity of the operation is inherited from G.

(ii) As $H \neq \emptyset$, there exists some $a \in H$, so $e = aa^{-1} \in H$.

(iii) Let $a \in H$. Then $a^{-1} = ea^{-1} \in H$ by the hypothesis.

(iv) We need to show that the operation of G defines a binary operation on H, that is, H is closed under the operation. Let $x, y \in H$. Then $xy = x(y^{-1})^{-1} \in H$ by the hypothesis.

Hence H is a group in its own right, and thus a subgroup of G.

□

This criterion for a subset of G to be a subgroup is sometimes called the one-step subgroup test. It can be seen easily to be equivalent to the so-called two-step subgroup test given as follows:

Theorem 3.1.3. *Let G be a group and H be a non-empty subset of G. If $ab \in H$ for all $a, b \in H$, and $a^{-1} \in H$ for all $a \in H$, then H is a subgroup of G.*

Example 3.1.4. Let G be an Abelian group.

(i) $\{x \in G \mid x^2 = e\}$ is a subgroup.

(ii) $\{x^2 \mid x \in G\}$ is a subgroup.

(iii) Let H and K be two subgroups of G. Then $HK := \{hk \mid h \in H, k \in K\}$ is a subgroup of G.

Example 3.1.5. Let $G = \mathbb{R}^*$ with multiplication and H be the set of irrational numbers. Then H is not a subgroup. (Show that there exist $a, b \in H$ such that $ab \notin H$.)

The criterion for a finite subset of a group to be a subgroup is even simpler.

Theorem 3.1.6. *Let H be a non-empty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.*

Proof. As $ab \in H$ for all $a, b \in H$, it suffices to show that for each $a \in H$, its inverse in G, a^{-1} also belongs to H. The finiteness of the set H plays a key role here.

Let $a \neq e$. As H is closed under the operation of G, $a, a^2, \ldots \in H$. As H is finite, we must have $a^i = a^j$ for some $i < j$. Hence, we may assume that $a^{j-i} = e$ for $j - i > 1$ (if $j - i = 1$, then $a = e$ and $a^{-1} = e$). Rewriting, we get $a(a^{j-i-1}) = e = (a^{j-i-1})a$ which implies that a^{j-i-1} (which is an element of H by the hypothesis) is the inverse of a. □

What can we say about the intersection and union of subgroups? Are they subgroups?

Proposition 3.1.7. *Let H and K be subgroups of a group G. Then*

(i) $H \cap K$ is a subgroup of G.
(ii) $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$.

Proof. (i) This is left as an easy exercise.

(ii) Suppose $H \subseteq K$ or $K \subseteq H$. Then $H \cup K = K$ or $H \cup K = H$, and in either case it is of course a subgroup.

Conversely, suppose $H \cup K$ is a subgroup and suppose, if possible, that $H \not\subseteq K$ and $K \not\subseteq H$. Then there exists $h \in H \setminus K$ and $k \in K \setminus H$. Then as h and k are in $H \cup K$, so is their product hk. Hence $hk \in H$ or $hk \in K$. But this means that either $k = h^{-1}(hk) \in H$ or $h = (hk)k^{-1} \in K$, both of which are impossible. Hence it must be true that one subgroup is included in the other.

□

The argument used in (i) and the first part of part (ii) of Proposition 3.1.7 easily extends to show that an arbitrary intersection and arbitrary union of *nested* subgroups is a subgroup.

3.2. **Cyclic Groups.**

Theorem 3.2.1. *Let G be any group and $a \in G$. Let $\langle a \rangle := \{a^m \mid m \in \mathbb{Z}\}$. Then $\langle a \rangle$ is a subgroup of G.*

Proof. Let $a^m, a^n \in \langle a \rangle$. By Theorem 3.1.2, it suffices to show that $a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$, which follows from the definition of $\langle a \rangle$. Hence $\langle a \rangle$ is a subgroup of G. □

$\langle a \rangle$ is called the *cyclic* subgroup of G generated by a. If $G = \langle a \rangle$, then G is called a cyclic group, and a is a called a *generator* of G.

Exercise 3.2.2. Prove that a cyclic group is Abelian.

Example 3.2.3.

(i) Recall the group $U(10) = \{1, 3, 7, 9\}$ with multiplication mod 10. Consider the cyclic (sub)groups generated by the element $3, 7$ and 9.

$\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$ as $3^2 \mod 10 = 9, 3^3 \mod 10 = 7$ and $3^4 \mod 10 = 1$. Similarly, $\langle 7 \rangle = \{7, 9, 3, 1\} = U(10)$, whereas $\langle 9 \rangle = \{9, 1\}$, a proper subgroup of

$U(10)$. Hence $U(10)$ is a cyclic group with generators 3 and 7. 9 is not a generator of the cyclic group $U(10)$.

(ii) Let $G = \mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$ with addition mod 12. Then $\langle 3\rangle = \{3, 6, 9, 0\}$. Compute the cyclic groups generated by the other elements of G. Recall here that the operation is addition, so the symbol a^n here means the sum $a + a + \ldots + a$ taken n times.

Intrinsic to the discussion above is the *order* of an element which will be defined shortly. A cyclic group by definition is a subgroup generated by a single element of the group G. We can generalize this notion to a subgroup generated by any subset S of the group G.

Definition 3.2.4. Let S be a non-empty subset of a group G. The subgroup generated by S is the smallest subgroup of G containing S.

Consider for a moment why this subgroup should exist, and what it looks like explicitly. Let $\mathcal{C}_S$ be the collection of all subgroups of G that contain S. As G is a subgroup of itself containing S, $\mathcal{C}_S$ is non-empty. Now consider the intersection of all subgroups of G containing S, that is, $\cap_{H\in\mathcal{C}_s} H$. This intersection is a subgroup and by virtue of being the intersection of all such subgroups, it is contained in any other subgroup of G containing S. Hence it is *the* subgroup generated by S and we denote it by $\langle S\rangle$. More concretely, $\langle S\rangle$ is the subgroup of G containing all finite products of elements of S and their inverses.

Exercise 3.2.5. If $S \subseteq G$ is a subgroup, then $\langle S\rangle = S$.

Note that different subsets can generate the same subgroup.

Example 3.2.6. Let $G = \mathbb{Z}_{12}$ with addition modulo 12. Then $\langle\{2, 8\}\rangle = \{0, 2, 4, 6, 8, 10\} = \langle 2\rangle$.

3.3. **Center of a group and centralizer of an element.**

Definition 3.3.1. The center $Z(G)$ is a group G is the subset of elements of G that commute with every element of G, that is,

$$Z(G) = \{a \in G \mid ax = xa \ \forall x \in G\}.$$

Theorem 3.3.2. *The center of a group $Z(G)$ is a subgroup of G.*

Proof. The identity e of the group G commutes with every element of G, so $e \in Z(G)$ and $Z(G)$ is non-empty. Let $a, b \in Z(G)$. We will show that $ab \in G$ and $a^{-1} \in Z(G)$. Then, applying Theorem 3.1.3, $Z(G)$ is a subgroup. First note that $a \in Z(G) \implies a^{-1} \in Z(G)$ as $ax = xa \implies a^{-1}axa^{-1} = a^{-1}xaa^{-1} \implies xa^{-1} = a^{-1}x$.

Let $x \in G$. Then

$$\begin{aligned}(ab)x &= a(bx) = a(xb)\\ &= (ax)b = (xa)b\\ &= x(ab),\end{aligned}$$

so $ab \in Z(G)$. □

Clearly, $Z(G)$ is an Abelian group.

Definition 3.3.3. Let $a \in G$. The centralizer $C(a)$ of a in G is the set of all elements of G that commute with a, that is,

$$C(a) = \{g \in G \mid ag = ga\}.$$

Theorem 3.3.4. *For each $a \in G$, $C(a)$ is a subgroup of G.*

Proof. Clearly, $Z(G) \subseteq C(a)$ for each $a \in G$, so $C(a)$ is non-empty. Use Theorem 3.1.3 just as in the proof of Theorem 3.3.2 to prove the rest of the theorem. □

Exercise 3.3.5.

(i) Show that $Z(G) = \cap_{a \in G} C(a)$.

(ii) Show that G is Abelian if and only if $C(a) = G$ for every $a \in G$.

Example 3.3.6 (Quaternion Group)**.** The *quaternion group* Q is given by the set $\{1, -1, i, -i, j, -j, k, -k\}$ with multiplication table given as follows:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Then it is easy to see from the multiplication table that $Z(Q) = \{1, -1\}$. $C(i)$ is easily seen to be $\{1, -1, i, -i\}$. Compute $C(g)$ for all elements of Q.

Example 3.3.7 (Heisenberg Group)**.** Let

$$H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbb{R} \right\}.$$

Show that H is a group.

We will show that $Z(H) = \left\{ \begin{bmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \mid y \in \mathbb{R} \right\}$.

For an element A in H to be in the center of H, we must have $A = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}$ and

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \qquad (a, b, c \in \mathbb{R}).$$

We compute to check that this implies that y can be arbitrary and $az = xc$ for all $a, c \in \mathbb{R}$. Hence $x = z = 0$ and A has the claimed form.

3.4. **Order of a group and of an element.**

Definition 3.4.1. The number of elements of a group G (finite or infinite) is called the order of G and denoted by $|\, G \,|$.

Definition 3.4.2. The order of an element $g \in G$ is the smallest positive integer n such that $g^n = e$. If no such n exists, the element g is said to have infinite order. The order of $g \in G$ is denoted by $|\, g \,|$.

Example 3.4.3.

(i) Let $G = U(10) = \{1, 3, 7, 9\}$ with multiplication mod 10. Then $|\,U(10)\,| = 4$. Verify that $|\,1\,| = 1, |\,3\,| = 4, |\,7\,| = 4, |\,9\,| = 2$.

(ii) Let $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with addition mod 6. Then $|\,\mathbb{Z}_6\,| = 6$ and $|\,0\,| = 1, |\,1\,| = 6, |\,2\,| = 3, |\,3\,| = 2, |\,4\,| = 3, |\,5\,| = 6$.

(iii) Let $G = \mathbb{Z}$ with addition. Then $\mathbb{Z}$ has infinite order and so does each of its non-zero elements.

Suppose G is a group and $a \in G$. We will show that the order of the element a is equal to the order of the cyclic group $\langle a \rangle$ generated by a.

References

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