MATH 417 WRITING ASSIGNMENT

GABRIEL KOSMACHER

Humans are often compelled to understand the underlying algebraic objects that govern our interactions with the world. Starting at a young age, we harness notions of arithmetic and symmetry to describe what we observe in nature, allowing us to quantify how we operate with objects and interpret patterns in physical phenomena. A mathematician seeks to understand these algebraic objects on an *abstract* level, hoping to organize mathematical knowledge so that efficient arguments can be made to describe a myriad of diverse objects that share core relations.

1. Groups and Subgroups

A quintessential object of mathematical intrigue is that of a *group*: a set of objects G with a rule for composing two elements of G such that *(1)* the composition is *associative*; *(2)* the set G has an *identity element* that, when composed with any element of a of G, yields the element a; and *(3)* for any element a of G, there exists an *inverse element* a^{-1} such that the composition of a and its inverse yields the identity element.

Examples of mathematical groups include: The set of integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ together with the $+$ addition operation, the set of symmetries of a geometric figure together with composition of symmetries, and the set of permutations of a finite set together with compositions of permutations.

Definition 1.1. A *group* is a set G equipped with a *group operation* $* : G \times G \to G$ such that

- For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$. We call this the associative property $*$.
- There exists an element $\mathbf{e} \in G$ such that for all $g \in G$, $g * \mathbf{e} = \mathbf{e} * g = g$. We say $\mathbf{e}$ is the identity element of G.
- Given an identity element $\mathbf{e} \in G$, for all $g \in G$ there is an element $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = \mathbf{e}$. We say that g^{-1} is the inverse element of g.

We denote the group of G equipped with the operation $*$ as $(G, *)$.

It is common shorthand to denote a group $(G, *)$ as G and to denote the product of a group operation $a * b$ as ab for some $a, b \in G$. We adopt this shorthand throughout the remainder of this paper.

The following proposition gives us *uniqueness* of the identity element and inverse elements for a group and is proved in [Goo14] Propositions 2.1.1 and 2.1.2.

Proposition 1.2. *For any group G, we have*

(1) The identity element $\mathbf{e} \in G$ is unique. That is, for any two elements $\mathbf{e}$ and $\mathbf{e}'$ in G, for all $g \in G$, if $g\mathbf{e} = \mathbf{e}g = g = \mathbf{e}'g = g\mathbf{e}'$ then $\mathbf{e} = \mathbf{e}'$; and

Date: Fall 2022.

(2) any element $g \in G$ has a unique inverse element $g^{-1} \in G$. That is, for any $g, g^{-1}, h \in G$, if $hg = gh = \mathbf{e} = g^{-1}g = gg^{-1}$ then $h = g^{-1}$.

A common property that many groups share is that of commutativity; that the result of applying the group operation on any two elements is independent of the order in which the elements are written. A classic group with the commutative property is the integers equipped with addition $(\mathbb{Z}, +)$, as for any integers a and b we have $a + b = b + a$. Another important group with the commutative property is the the additive group of integers modulo n, $(\mathbb{Z}_n, +)$. $(Z_n, +)$, also called the *cyclic group* of n elements, is comprised of *congruence classes*, denoted $[k]_n$, where $0 \leq k \leq n - 1$, and where each congruence class $[k]_n$ contains all the integers a such that n divides the difference of a and k. It is common to think of congruence classes as containing any number that *wraps around* n to get back to k. To get a concrete visualization, picture the group $(Z_{12}, +)$ as a wall clock, and let the congruence class $[3]_{12}$ contain not only `3:00`, but also `15:00`. Addition in this group is given by the structure $[a]_n + [b]_n = [a + b]_n$. Again, using the wall clock analogy, we know that `4` hours after `9`, our clock will point to `3`, just as $[4]_n + [9]_n = [4 + 9]_n = [3]_n$. Similarly, we now that `9` hours after `4`, our clock will again point to `3`, as $[9]_n + [4]_n = [9 + 4]_n = [3]_n$. We can extrapolate this example to see that addition of congruence classes is, in fact, commutative. We call groups with the commutative property *abelian groups.*

Yet not all groups are commutative. Take, for instance, the group of permutations S_n of size $n \geq 3$. We have that (12) and (23) are in S_n, but $(12)(23) \neq (23)(12)$.

Definition 1.3. We say a group G is *abelian*, or *commutative*, if for all $g, h \in G$, we have $gh = hg$. It is common to denote the group operation as $+$ for abelian groups.

Once a group is found, one may find it interesting to study certain instances of the group that maintain the group property. If one has the general linear group $\mathrm{GL}(n, \mathbb{R})$ of real $n \times n$ invertible matrices, they might take interest in studying only those particular matrices with determinant ± 1, $\mathrm{O}(n, \mathbb{R})$, called the real orthogonal matrices of size n. For instance, they may ask if $\mathrm{O}(n, \mathbb{R})$ is itself a group with the same operation of the General Linear group.

Definition 1.4. Given a group G, we say that the subset H of G forms a subgroup of G if H, equipped with the operation $*$, is itself a group. We denote a subgroup H of G by $H \leq G$.

It can be tedious to check if a given set forms a subgroup via definition alone. However, the following propositions decreases the labor needed to showing that two special conditions are satisfied.

Proposition 1.5. *For any nonempty subset H of G, then H is a subgroup of G if, and only if,*

(1) for all $a, b \in H$, $ab \in H$; and,

(2) for all $h \in H$, $h^{-1} \in G$ is an element of H such that $hh^{-1} = \mathbf{e}$.

Proof. Let H be a subgroup of G. Then *(1)* and *(2)* hold by definition.

Now consider that for all $a, b \in H$, $ab \in H$ and for all $h \in H$, there is an inverse element $h^{-1} \in H$ such that $hh^{-1} = \mathbf{e}$. But by *(1)* we have that H has an operation, and we know that operation is associative as G is a group. Since H is nonempty, there contain an element h. But then by *(2)* we have $h^{-1} \in H$ and by *(1)* we have $hh^{-1} = \mathbf{e} \in H$. Thus, H is a subgroup of G. □

It is common to refer to condition *(1)* of Proposition 1.5 as *closure under group product* and to refer to condition *(2)* of Proposition 1.5 as *closure under group inverse.*

2. Center of a Group

An important concept in the theory of groups is the *center of a group*; the set of elements of a group G that commute with every element of G.

Definition 2.1. For any group G, the *center* $Z(G)$ is the set of elements that commute with every element of G,

$$Z(G) = \{z \in G \mid gz = zg \text{ for all } g \in G\}$$

Proposition 2.2. *For any group G, the center $Z(G)$ is an abelian subgroup of G.*

Proof. We first need to show that $Z(G)$ is a subgroup of G. By Proposition 1.5, it is sufficient to show that $Z(G)$ is closed under group multiplication and group inverse. We have that the identity element e is in $Z(G)$ as $ex = x = xe$ for any $x \in G$, so $Z(G)$ is non empty.

Pick some $x, y \in Z(G)$. Then for any $g \in G$, by associativity of the group operation, and recalling that yg and gx are elements of G by definition of the group operation,

$$(xy)g = x(yg) = (yg)x = y(gx) = (gx)y = g(xy)$$

and thus $xy \in G$ and $Z(G)$ is closed under group multiplication.

Now consider any $x \in Z(G)$ with inverse $x^{-1} \in G$. Then for any $g \in G$, recalling that $x^{-1}gx^{-1} \in G$ by definition of the group operation, we have

$$x(x^{-1}gx^{-1}) = (x^{-1}gx^{-1})x \iff (xx^{-1})gx^{-1} = x^{-1}g(xx^{-1}) \iff gx^{-1} = x^{-1}g$$

and thus $Z(G)$ is closed under group inverse.

It is easy to see that $Z(G)$ is abelian, as for any $x \in Z(G)$, by construction we have that for all $y \in G$, $xy = yx$. In other words, for any $x, y \in Z(G)$, $xy = yx$, so $Z(G)$ is abelian. □

The group of symmetries of a regular n sided polygon, called the Dihedral group and denoted D_n, is among the most studied finite groups. It is composed of n rations of $2\pi/n$ about the origin and 2 flips about. The group multiplication is given by the properties that n rotations r or 2 flips j both equal the identity, and a rotation r followed by a flip j is equal to the flip j followed by the inverse rotation r^{-1}. Furthermore, we have that any number of rotations followed by a flip is its own inverse, as given in the following lemma.

Lemma 2.3. *For any Dihedral group D_n, for all integers n, we have $(r^n j)^2 = e$, where $r^n, j \in D_n$.*

Proof. We prove by mathematical induction. Let $n = 0$. Then $(r^0 j)^2 = j^2 = \mathbf{e}$. Now assume that for all k less than an arbitrary integer n and greater than 0 that $(r^k j)^2 = \mathbf{e}$ and consider

$$\begin{aligned}(r^n j)^2 &= rr^{n-1}jr^{n-1}rj \\ &= rr^{n-1}jr^{n-1}jj^{-1}rj \\ &= r(r^{n-1}jr^{n-1}j)j^{-1}rj \\ &= rj^{-1}rj \\ &= rj^{-1}jr^{-1} \\ &= rr^{-1} \\ &= \mathbf{e}\end{aligned}$$

□

Investigating the group D_4, the symmetries of the square, we can deduce that the center $Z(D_4)$ is the subgroup $\{\mathbf{e}, r^2\}$.

Proof. It is easy to see that $\mathbf{e}$ is in the center, as $\mathbf{e}g = g\mathbf{e} = g$ for any $g \in D_4$. Now consider a rotation of the form r^n where $1 \leq n \leq 3$. We have that rotation multiplication commutes, so we only need to consider multiplying r^n by elements of the form $r^m j$, where $0 \leq m \leq 3$. We simplify this to checking whether elements of the form $r^m j$ are self inverses, as if they are $r^n r^m j = (r^m j)^{-1} r^n = r^m j r^n$. But we also have that every element of the form $r^m j$ is a self inverse by Lemma 2.3, so we only need to check when r^n is a self inverse, which happens when $n = 2$, and thus r^2 is in the center. Finally, we have that no element of the form $r^m j$ is in the center, where $0 \leq m \leq 3$, as $rr^m j = r^{m+1} j = jr^{-m} r^{-1} = r^m j r^{-1} \neq r^m j r$. Thus, we have that $Z(D_4) = \{\mathbf{e}, r^2\}$. □

Another important concept is the *centralizer of an element* x in group G; a set of elements of G that commute with the element x.

Definition 2.4. For any nonempty group G and any element $x \in G$, we define the *centralizer* $C(x)$ of x to be

$$C(x) = \{g \in G \mid gx = xg\}$$

Proposition 2.5. *For any nonempty group G, the centralizer $C(x)$ for any element $x \in G$ is a subgroup of G.*

Proof. The element x of G is an element of $C(x)$, so $C(x)$ is nonempty.

Pick some g, h in $C(x)$. Then, using the substitutions $hx = xh$ and $gx = xg$, we have

$$(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh)$$

and thus $gh \in C(x)$, so $C(x)$ is closed under group multiplication.

First, notice that $x^{-1} \in C(x)$ as $x^{-1} \in G$ and $x^{-1}x = e = xx{-}1$. Now consider any $g \in C(x)$ with inverse $g^{-1} \in G$. Then, using the substitution $gx = xg$, we have

$$x^{-1}g = x^{-1}g(xx^{-1}) = x^{-1}(gx)x^{-1} = x^{-1}(xg)x^{-1} = (x^{-1}x)gx^{-1} = gx^{-1}$$

and thus $x^{-1} \in C(x)$, so $C(x)$ is closed under group inverse. □

We can compute the centralizers of every element of D_4 to be

$$\begin{aligned} C(\mathbf{e}) &= C(r^2) = D_4 \\ C(r) &= C(r^3) = \{\mathbf{e}, r, r^2, r^3\} \\ C(j) &= C(r^2j) = \{\mathbf{e}, r^2, j, r^2j\}, \\ C(rj) &= C(r^3j) = \{\mathbf{e}, r^2, rj, r^3j\} \end{aligned}$$

where $0 \leq n \leq 3$.

Proof. We have that $\mathbf{e}$ and r^2 are in the center of D_4, and it is clear to see that the centralizer of any element in the center is the whole group D_4. As disused when computing the center of D_4, each rotation commutes, but r and r^3 do not commute with elements in the form $r^m j$, where $0 \leq m \leq 3$, so the centralizers of r and r^3 are $\{\mathbf{e}, r, r^2, r^3\}$. Finlay, the centralizer of any element in the form $C(r^n j)$, where $0 \leq n \leq 3$, must contain $\mathbf{e}$ and r^2 as they are in the center of D_4, but the centralizer does not contain any other rotations; a direct result of our proof of the center of D_4. Furthermore, we have that each element commutes with itself, and it can be checked that j commutes with r^2j but not with rj or r^3j, and that rj commutes with r^3j but not with j or r^j. Thus, the centralizers $C(j)$ and $C(r^2j)$ must be $\{\mathbf{e}, r^2, j, r^2j\}$, while the centralizers $C(rj)$ and $C(r^3j)$ must be $\{\mathbf{e}, r^2, rj, r^3j\}$. □

Theorem 2.6. *Let G be a group. Then the center $Z(G)$ is equal to the intersection of all centralizers $C(x)$ of G. In other words,*

$$Z(G) = \bigcap_{x \in G} C(x)$$

Proof. We first show that $Z(G)$ is contained in $\cap_{x \in G} C(x)$. Suppose that $z \in Z(G)$. Then it follows that for all $x \in G$, $xz = za$. But by the definition of the centralizer, this is equivalent to saying that for all $x \in G$, $z \in C(x)$. Thus, $Z(G) \subseteq \cap_{x \in G} C(x)$.

We now show that $\cap_{x \in G} C(x)$ is contained in $Z(G)$. Let $c \in \cap_{x \in G} C(x)$. Then by the definition of the intersection, for all $x \in G$ we have $c \in C(x)$. That is, by the definition of the centralizer, for all $x \in G$ we have $cx = xc$. But by the definition of the center, $c \in Z(G)$. Thus, $\cap_{x \in G} C(x) \subseteq Z(G)$ □

References

[Goo14] F. Goodman. *Algebra: Abstract and Concrete, edition 2.6.* SemiSimple Press (Frederick Goodman), 2014.