

## PSET 1 — September 27, 2022

Prof. Voight

Student: Amittai Siavava

## Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

- (a) *Abstract Algebra* by David S. Dummit & Richard M. Foote.
- (b) *Algebra* by Jacob K. Goldhaber & Gertrude Ehrlich

## Problems

1. Let  $f: A \rightarrow B$  and  $g: B \rightarrow C$  be maps. Suppose that  $g \circ f: A \rightarrow C$  is injective.

- (a) Show that  $f$  is injective.

By definition of composition,  $(g \circ f)(x) = g(f(x))$ .

By definition of injectivity,  $g \circ f$  is injective if and only if  $(g \circ f)(a) = (g \circ f)(a')$  implies  $a = a'$ .

Suppose  $f$  is not injective.

Then there exists  $a, a' \in A, b \in B$  such that  $f(a) = f(a') = b \wedge a \neq a'$ .

Then:

$$(g \circ f)(a) = g(f(a)) = g(b) = g(f(a')) = (g \circ f)(a')$$

Thus,  $(g \circ f)(a) = (g \circ f)(a')$  for some  $a, a' \in A$  such that  $a \neq a'$ , implying that  $g \circ f$  is not injective. This contradicts the fact that  $g \circ f$  is injective.

Therefore, it must hold that  $f(a) = f(a') \implies a = a'$  and  $f$  is injective.

- (b) Is  $g$  necessarily injective? Give a proof or a counterexample.

$g$  is necessarily injective when restricted to the codomain of  $f$ .

For instance, consider  $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$  and  $g: \mathbb{R}^+ \rightarrow \mathbb{R}^+$  such that  $f(x) = x + 1$  and  $g(x) = x^2$ .

We can note that:

- (a)  $f$  is injective, since  $f(x) = x + 1 = y + 1 = f(y) \implies x = y$ .

- (b)  $g$  is injective *as defined* because its domain is limited to  $\mathbb{R}^+$ , the codomain of  $f$ . However, if the domain of  $g$  is extended to include all of  $\mathbb{R}$ , then  $g$  would no longer be injective since  $b^2 = (-b)^2$  for all  $b \in \mathbb{R}$ .

2. (sorta DF 1.1.1, 1.1.8) Determine which of the following are groups. Justify your answer.

- (a) The set  $G = \mathbb{R} \setminus \{0\}$  under the binary operation  $*$  defined by  $a * b = a/b$  for  $a, b \in G$ .

$G$  is not a group.

- (a)  $G$  is not closed under the operation  $*$ , since  $a * b = a/b$  gives elements in  $\mathbb{Q}$  for any  $a, b \in \mathbb{R}$  such that  $b \nmid a$ .  
 (b)  $G$  is not associative, since  $a * (b * c) = a/(b/c) = ac/b \neq a/bc = (a/b)/c = (a * b) * c$   
 (c)  $G$  does not have an identity element, since:

$$e * a = e/a = a \implies e = a^2$$

$$a * e = a/e = a \implies e = 1$$

$$e/a = a/e = a \implies e = a^2 \wedge e = 1 \implies a = \pm 1.$$

There is no unique identity unique identity that leaves **all** elements in  $G$  invariant.

- (d) However, **if we invented the identity to be 1**, then each element in  $G$  would be it's own inverse since:

$$\forall a \in G: \quad a/a^{-1} = a^{-1}/a = 1 \implies a = a^{-1}$$

- (b) The set  $G = \mathbb{R}$  under the binary operation  $*$  defined by  $a * b = a + b + ab$  for  $a, b \in G$ .

$G$  is not a group.

- (a)  $G$  has a unique identity  $e = 0$ .  
 (b)  $G$  is closed under  $*$ .  
 (c)  $*$  is not an associative operation on  $G$ .

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) = a * b + a * c + a * bc \\ &= a + b + ab + a + c + ac + a + bc + abc \\ &= 3a + b + c + ab + ac + bc + abc \end{aligned}$$

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c = a * c + b * c + ab * c \\ &= a + c + ac + b + c + bc + ab + c + abc \\ &= a + b + 3c + ab + ac + bc + abc \end{aligned}$$

As we can see,  $a * (b * c) \neq (a * b) * c$ .

- (c) The set  $G = \{z \in \mathbb{C} : z^n = 1 \text{ for some } n \in \mathbb{Z}_{>0}\}$  under multiplication. [Hint: be sure to check multiplication is a binary operation on  $G$  in the first place!]

$G$  is a group.

- (a)  $G$  has a unique identity  $e = 1 + 0i = 1$ , since 1 leaves all elements in the group invariant after multiplication.  
 (b)  $G$  is closed under multiplication.  
 $\forall z_1, z_2 \in G, \exists n_1, n_2 \in \mathbb{Z}_{>0}$ :

$$z_1 * z_2 = z_1 z_2$$

We need to find an exponent  $n$  such that  $(z_1 z_2)^n = 1$ .

Taking  $n = n_1 n_2$  gives:

$$\begin{aligned} (z_1 z_2)^{n_1 n_2} &= z_1^{n_1 n_2} z_2^{n_1 n_2} \\ &= (z_1^{n_1})^{n_2} (z_2^{n_2})^{n_1} \\ &= 1^{n_2} 1^{n_1} \\ &= 1 \end{aligned}$$

Therefore, it holds that multiplication of 2 elements in  $G$  gives an element in  $G$ .

- (c)  $*$  is associative following from associativity of  $\mathbb{C}$ .  
 (d)  $G$  has inverses. By definition, if  $z \in G$  then  $z^n = 1$  for some  $n \in \mathbb{Z}_{>0}$ .  
 The multiplicative inverse of  $z$  is  $1/z$ , and  $z^n = 1$  implies  $(1/z)^n = 1$ .

3. (DF 1.1.20) Let  $G$  be a group and let  $x \in G$ . Show that  $x$  and  $x^{-1}$  have the same order.

Let  $n$  be the order of  $x$  such that  $x^n = e$ .

Furthermore, let  $x^{-1}$  be the inverse of  $x$ , such that  $x * x^{-1} = e$ .

Using algebraic substitution, we can show that:

$$x^n = e$$

$$x^n = x * x^{-1} \quad (\text{an element multiplied by its inverse})$$

$$x^n = (x * x^{-1})^n \quad (\text{multiplying } e \text{ by itself } n \text{ times.})$$

$$x^n = x^n * x^{-n}$$

$$e = e * x^{-n} \quad (\text{since we already know that } x^n = e)$$

$$e = x^{-n} = (x^{-1})^n$$

We see that  $(x^{-1})^n = e$ . By definition of order,  $x^{-1}$  has order  $n$ .

4. (sorta DF 1.2.2–1.2.5) Let  $D_{2n} = \{1, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$  be the dihedral group of order  $2n$  with presentation  $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \text{ rangle}$ .

(a) Write out the multiplication (Cayley) table for  $D_6$ .

	1	$r$	$r^2$	$s$	$sr$	$sr^2$
1	1	$r$	$r^2$	$s$	$sr$	$sr^2$
$r$	$r$	$r^2$	1	$sr$	$sr^2$	$s$
$r^2$	$r^2$	1	$r$	$sr^2$	$s$	$sr$
$s$	$s$	$sr^2$	$sr$	1	$r^2$	$r$
$sr$	$sr$	$s$	$sr^2$	$r$	1	$r^2$
$sr^2$	$sr^2$	$sr$	$s$	$r^2$	$r$	1

(b) Show that if  $x \in D_{2n}$  is a power of  $r$  (including  $x = r^0 = 1$ !), then  $rx = xr$  and  $x$  has order at most  $n$ .

Suppose  $x = r^k$  for some  $k \in \mathbb{Z}$ . Then  $rx = rr^k = r^{k+1} = r^k r = xr$ .

Furthermore, we know that  $r^n = 1$  in  $D_{2n}$ .

Therefore:

$$x = r^k$$

$$x^n = (r^k)^n$$

$$x^n = r^{kn} \quad (\text{multiplication of exponents for nested exponentiation})$$

$$x^n = (r^n)^k \quad (\text{rearranging the powers})$$

$$\therefore r^n = 1$$

$$\therefore x^n = 1^k = 1$$

Therefore, for any element  $x \in D_{2n}$  such that  $x = r^k$  for some  $k \in \mathbb{Z}$ , we see that  $x^n = 1$  and  $x$  has order at most  $n$ .

**The order can be lower, if  $k > 1$  and  $k \mid n$**

(c) Otherwise, if  $x \in \{s, sr, \dots, sr^{n-1}\}$  (not a power of  $r$ ), then show that  $rx = xr^{-1}$  and  $x$  has order 2. [Hint: first prove by induction that  $r^m s = sr^{-m}$  for all  $m \geq 1$ .]

We aim to prove that  $r^m s = sr^{-m}$  for all  $m \geq 1$ .

**Base case:** We aim to show that  $r^m s = sr^{-m}$  for  $m = 1$ .

$$rs = sr$$

The proof is trivial. Since  $s$  is a flip, it translates a rotation done in any direction (counter-clockwise, in this case) *before the flip* into equivalent rotations done in the opposite direction (clockwise) *after the flip*.

**Induction hypothesis:** incrementally, we aim to show that  $r^m s = sr^{-m}$  if  $r^{m-1} s = sr^{-(m-1)}$ .

Let  $m = i + 1$ , assuming it has been proven that  $r^i s = sr^{-i}$ .

$$r^i s = sr^{-i}$$

$$r(r^i s) = r(sr^{-i})$$

$$r^{(i+1)} s = r s r^{-i} \quad (\text{Simplifying the left side of the equation})$$

$$r^{(i+1)} s = (rs) r^{-i} \quad (\text{Grouping the right side of the equation})$$

$$r^{(i+1)} s = (sr^{-1}) r^{-i}$$

$$r^{(i+1)} s = sr^{-i-1} \quad (\text{Simplifying the left side of the equation})$$

$$r^{(i+1)} s = sr^{-(i+1)}$$

We now aim to show that if  $x = r^m s$  for some  $m \in \mathbb{Z}$  then  $x$  has order 2, i.e.  $x^2 = 1$ .

$$x^2 = (r^m s)^2$$

$$x^2 = (r^m s)(sr^{-m}) \quad (\text{Substituting the equality})$$

$$x^2 = r^m s^2 r^{-m} \quad (\text{Expanding the right side of the equation})$$

$$x^2 = r^m r^{-m} \quad (\text{Simplifying } s^2 = 1)$$

$$x^2 = r^{m-m} = r^0 = 1$$

- (d) For a group  $G$  under  $*$ , we say that  $a$  is *central* if  $a * x = x * a$  for all  $x \in G$ . Show that if  $n = 2k$  is even that  $z = r^k$  is an element of order 2 which is central.

- (a)  $z = r^k$  is an element of order 2

Given  $z = r^k$ , then  $z^2 = (r^k)^2 = r^{2k}$ .

Furthermore, we know that  $n = 2k$ , which means the Dihedral group is  $D_{4k}$ . It then follows from the Group axioms that  $r^{2k} = 1$  in  $D_{4k}$ .

Thus,  $(z^k)^2 = 1$  and  $z$  has order 2.

- (b)  $z$  is central

We aim to show that  $z * x = x * z$  for all  $x \in D_{4k}$ .

Given  $z = r^k = r^{n/2}$ :

$$\begin{aligned} z * x &= r^{(n/2)} * x \\ (zx)^2 &= (r^{n/2}x)^2 && \text{(Squaring both sides)} \\ z^2x^2 &= r^n x^2 \\ z^2x^2 &= x^2 \\ zx &= x \end{aligned}$$

$$\begin{aligned} x * z &= xr^{(n/2)} \\ (xz)^2 &= (xr^{n/2})^2 && \text{(Squaring both sides)} \\ xz^2 &= x^2r^n \\ xz^2 &= x^2 \\ xz &= x \end{aligned}$$

Thus, we see that  $zx = xz = x$  for all  $x \in D_{4k}$ .

5. (DF 1.2.10) Let  $G$  be the group of rigid motions in  $\mathbb{R}^3$  of a cube. Show that  $G$  is a nonabelian group of order 24. [Hint: Find the number of positions to which an adjacent pair of vertices can be sent; alternatively, find the number of places to which a given face may be sent and, once a face is fixed, the number of positions to which a vertex on that face may be sent.]

(a)  $|G| = 24$

There are 6 faces on a cube, and each face has 4 edges.

If we visualize a person placing the cube on a table, there are 6 possible faces that can face the person, and, for each face, there are 4 orientations (or 4 possible edges that could be touching the table). This makes for  $6 \cdot 4 = 24$  possible positions for the cube.

(b)  $G$  is nonabelian  $G$  has order 24. For  $G$  to be prime, then  $|G|$  must either be prime, a square of a prime, or a product of two primes  $p, q \in \mathbb{Z}, p < q$  such that  $p \nmid (q - 1)$ .

However,  $|G| = 24 = 2^3 \cdot 3$  and does not satisfy any of those properties.