

PMAT 315 ASSIGNMENT 1 SOLUTIONS

1. (a) Page 26 # 49.

(b) Suppose instead that S is a *subset* of \mathbb{Z} . Again for $a, b \in S$ define aRb if $ab \geq 0$. Find all subsets $S \subseteq \mathbb{Z}$ so that R is an equivalence relation on S . Also, for each $S \subseteq \mathbb{Z}$ so that R is an equivalence relation on S , describe all the equivalence classes of R .

1. (a) No, R is **not** an equivalence relation on the set S of all integers. The reason is that R is not transitive. A counterexample is that $1R0$ because $1 \cdot 0 = 0 \geq 0$, and $0R(-1)$ because $0 \cdot (-1) = 0 \geq 0$, but $1 \not R (-1)$ because $1 \cdot (-1) = -1 \not\geq 0$.

(b) As in part (a) we can see that if S contains 0 and any elements a, b where $a > 0$ and $b < 0$, then R will not be an equivalence relation because R will not be transitive. But any other subset $S \subset \mathbb{Z}$ will work. In particular:

- if $S \subseteq \{0, 1, 2, \dots\}$, then $\forall a, b \in S, ab \geq 0$, so aRb . Thus every pair of elements of S are related by R , so R is an equivalence relation on S with just the one equivalence class S itself.
- if $S \subseteq \{0, -1, -2, \dots\}$, then again $\forall a, b \in S, ab \geq 0$, so aRb . Once again R is an equivalence relation on S with just the one equivalence class S itself.
- if $S \subseteq \mathbb{Z} - \{0\}$ is any set of *nonzero* integers, then note that if $a, b \in S$ are both positive or both negative, then $ab > 0$ so aRb , while if $a > 0$ and $b < 0$ then $ab < 0$, so $a \not R b$. This means that R is clearly reflexive and symmetric. Also, R is transitive because if we assume that $a, b, c \in S$ satisfy aRb and bRc , then either a, b, c are all positive or they are all negative, and either way $ac \geq 0$ so aRc . In this case there are *two* equivalence classes, the set of all positive integers in S and the set of all negative integers in S (if both are nonempty).

2. (a) For any $a, b \in \mathbb{R} - \{0\}$, let $a \circ b = -2ab$. Prove that $(\mathbb{R} - \{0\}, \circ)$ is a group.

(b) Prove that we do not get a group if $\mathbb{R} - \{0\}$ in part (a) is replaced by \mathbb{R} or by $(0, \infty)$ (the set of all positive real numbers).

(c) Find a nontrivial proper subgroup of the group $(\mathbb{R} - \{0\}, \circ)$.

2. (a)

- $\mathbb{R} - \{0\}$ is closed under the operation, since $a \circ b = -2ab \in \mathbb{R} - \{0\}$ for all $a, b \in \mathbb{R} - \{0\}$.
- \circ is associative: for all $a, b, c \in \mathbb{R} - \{0\}$,

$$(a \circ b) \circ c = (-2ab) \circ c = -2(-2ab)c = -2a(-2bc) = a \circ (-2bc) = a \circ (b \circ c).$$

- $-1/2$ is an identity element, because for all $a \in \mathbb{R} - \{0\}$, $(-1/2) \circ a = a \circ (-1/2) = -2(-1/2)a = a$.
- For any $a \in \mathbb{R} - \{0\}$, the nonzero number $1/(4a)$ is the inverse of a , because $a \circ (1/(4a)) = (1/(4a)) \circ a = -2a(1/(4a)) = -1/2$, the identity.

Therefore $(\mathbb{R} - \{0\}, \circ)$ is a group.

(b) (\mathbb{R}, \circ) is not a group, because although $-1/2$ is an identity element (proved in part (a)), the element 0 does not have an inverse. For if 0 had an inverse b , b would have to satisfy $-1/2 = 0 \circ b = -2 \cdot 0 \cdot b = 0$, which is a contradiction.

$((0, \infty), \circ)$ is not a group, because it is not closed under the operation. For example, $1 \in (0, \infty)$, but $1 \circ 1 = -2 \cdot 1 \cdot 1 = -2 \notin (0, \infty)$.

(c) The set $(-\infty, 0)$ of all negative real numbers is a subgroup of $(\mathbb{R} - \{0\}, \circ)$, because:

- Let $a, b < 0$ be arbitrary negative real numbers. Then $a \circ b = -2ab$ is also negative. Thus $(-\infty, 0)$ is closed under the operation \circ .
- From part (a), the identity is $-1/2$, which is negative.
- If a is an arbitrary negative real number, then from part (a) a^{-1} will be $1/(4a)$ which is negative, so $(-\infty, 0)$ is closed under inverses.

3. A *mattress* is a solid rectangular box whose length, width and height are all different. Find all symmetries of a mattress (using appropriate labels). Then give the Cayley table of the group of symmetries of a mattress, and give the orders of all the elements of this group.

3. There are only **four** symmetries of a mattress: two (the identity E and a 180° rotation R) where the top of the mattress stays on top; and two (L a flip along the long axis, and S a flip along the short axis) where the mattress is turned over. The Cayley table is

	E	R	L	S
E	E	R	L	S
R	R	E	S	L
L	L	S	E	R
S	S	L	R	E

The orders are: $|E| = 1$, $|R| = |L| = |S| = 2$.

4. Recall that for any element a of a group G , and for any positive integer n , a^{-n} is defined to be $(a^{-1})^n$. Prove **by induction on n** that $a^{-n} = (a^n)^{-1}$ for all positive integers n .

4. *Basis step.* When $n = 1$, we want to prove that $a^{-1} = (a^1)^{-1}$, but this is obvious since $a^1 = a$.

Induction step. Assume that $a^{-k} = (a^k)^{-1}$ for some positive integer k . We want to prove that $a^{-(k+1)} = (a^{k+1})^{-1}$. To do this we need to show that $a^{-(k+1)}a^{k+1} = e$ and $a^{k+1}a^{-(k+1)} = e$. Well,

$$\begin{aligned}
 a^{-(k+1)}a^{k+1} &= (a^{-1})^{k+1}a^{k+1} \text{ by definition} \\
 &= (a^{-1})[(a^{-1})^k a^k]a \text{ by associativity} \\
 &= (a^{-1})[a^{-k}a^k]a \text{ by definition} \\
 &= a^{-1}ea \text{ by the assumption that } a^{-k} = (a^k)^{-1} \\
 &= a^{-1}a = e,
 \end{aligned}$$

and similarly $a^{k+1}a^{-(k+1)} = e$. This proves the induction step.

Therefore $a^{-n} = (a^n)^{-1}$ for all positive integers n .

5. (a) Page 91 #8.

(b) Prove that for any elements a, b of a group G , if $ab = c^2$ for some $c \in G$, then $ba = d^2$ for some $d \in G$.

(c) Find an example of a group G and elements $a, b \in G$ so that $ab \neq c^2$ for any $c \in G$.

5. (a) (\implies) Assume that $\exists x \in G$ such that $xax = b$. Then $ab = a(xax) = (ax)(ax) = (ax)^2$, so we can put $c = ax$ and get $ab = c^2$.

(\impliedby) Assume that $\exists c \in G$ so that $ab = c^2$. Put $x = bc^{-1}$. Then $xax = bc^{-1}abc^{-1} = bc^{-1}c^2c^{-1} = bc^{-1+2-1} = be = b$.

Note. How do you guess that $x = bc^{-1}$ works? One way is this. From $ab = c^2$ we get $a = abb^{-1} = c^2b^{-1}$. We want $xax = b$, so we want $xc^2b^{-1}x = b$. This means that $x^{-1}xc^2b^{-1}xx^{-1}b = x^{-1}bx^{-1}b$, or $ec^2b^{-1}eb = (x^{-1}b)^2$, or $c^2 = (x^{-1}b)^2$, so try $c = x^{-1}b$ which would mean we want $xc = b$ or $x = bc^{-1}$.

Note. From $ab = c^2$ we can get $b = a^{-1}ab = a^{-1}c^2$ and so $bc^{-1} = a^{-1}c^2c^{-1} = a^{-1}c$, so $x = a^{-1}c$ will also work in (\impliedby).

(b) Suppose that $a, b, c \in G$ are such that $ab = c^2$. From part (a), $\exists x \in G$ so that $xax = b$. This means that $x^{-1}xaxx^{-1} = x^{-1}bx^{-1}$ which says $a = eae = x^{-1}bx^{-1}$. From part (a), this implies that $\exists d \in G$ so that $ba = d^2$.

(c) We let $G = \mathbb{Z}$ under addition. Then, rewriting what we want in additive notation, we want elements $a, b \in \mathbb{Z}$ so that $a + b \neq 2c$ for any $c \in \mathbb{Z}$. We can choose $a = 1$ and $b = 0$, so that $a + b = 1$, and then there is no integer c so that $2c = 1$.