

Math 580–EXAM 1–Review Problems–Answer Key

I. Here are some problems about equivalence relations.

1. Let \mathbb{R}^\times be the set of **non-zero** real numbers and define a relation aRb if $ab^{-1} \in \mathbb{Q}^\times$ where \mathbb{Q}^\times are the **non-zero** rational numbers (equivalently $R = \{(a, b) \in \mathbb{R}^\times \times \mathbb{R}^\times \mid ab^{-1} \in \mathbb{Q}^\times\}$).

(a) Show that R defines an equivalence relation.

For any $a \in \mathbb{R}^\times$, $aa^{-1} = 1$ and $1 \in \mathbb{Q}^\times$ so aRa . So R is reflexive.

Let $a, b \in \mathbb{R}^\times$, if aRb then $ab^{-1} \in \mathbb{Q}^\times$. Then $(ab^{-1})^{-1}$ is the reciprocal of ab^{-1} so $(ab^{-1})^{-1} \in \mathbb{Q}^\times$. Notice that $(ab^{-1})^{-1} = a^{-1}b = ba^{-1}$, so bRa . So R is symmetric.

Let $a, b, c \in \mathbb{R}^\times$, if aRb and bRc then $ab^{-1}, bc^{-1} \in \mathbb{Q}^\times$. Since the product of non-zero rational numbers is a non-zero rational number, we see that $(ab^{-1})(bc^{-1}) \in \mathbb{Q}^\times$. Notice that $(ab^{-1})(bc^{-1}) = ac^{-1}$ so aRc . So R is transitive.

Thus we have verified the criteria for an equivalence relation.

- (b) Let $\mathbb{R}^\times/\mathbb{Q}^\times$ be the set of equivalence classes for R . Suppose that we want to define an operation on $\mathbb{R}^\times/\mathbb{Q}^\times$ by $[a] \cdot [b] = [ab]$. Show such an operation is well-defined.

Suppose that $[a_1] = [a_2]$ and $[b_1] = [b_2]$. Then $a_1a_2^{-1}, b_1b_2^{-1} \in \mathbb{Q}^\times$. Since the product of two non-zero rational numbers is a rational number, we see that $(a_1a_2^{-1})(b_1b_2^{-1}) \in \mathbb{Q}^\times$. Notice that $(a_1a_2^{-1})(b_1b_2^{-1}) = (a_1b_2)(a_2b_1)^{-1}$ so $[a_1b_1] = [a_2b_2]$.

- (c) Show that the set $\mathbb{R}^\times/\mathbb{Q}^\times$ with the operation as is in (b) defines a group. For any $a, b, c \in \mathbb{R}^\times$,

$$[a] \cdot ([b] \cdot [c]) = [a] \cdot [bc] = [a(bc)] = [(ab)c] = [ab] \cdot [c] = ([a] \cdot [b]) \cdot [c].$$

For any $a \in \mathbb{R}^\times$, $[a] \cdot [1] = [a] = [1] \cdot [a]$. Thus $[1]$ is our identity element.

For any $a \in \mathbb{R}^\times$, $a^{-1} \in \mathbb{R}^\times$ so $[a] \cdot [a^{-1}] = [1] = [a^{-1}] \cdot [a]$.

So $\mathbb{R}^\times/\mathbb{Q}^\times$ satisfies the axioms of a group.

2. Let $\text{Isom}(\mathbb{R}^2)$ be the set of all isometries of the plane \mathbb{R}^2 (with the Euclidean metric) and define a relation f_1Rf_2 if there exists an invertible element $g \in \text{Isom}(\mathbb{R}^2)$ so that $f_1 = g \circ f_2 \circ g^{-1}$. Show that R defines an equivalence relation. First, we notice that the identity function $I : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ (given by $I((x, y)) = (x, y)$) is an invertible element of $\text{Isom}(\mathbb{R}^2)$ with $I^{-1} = I$. For any $f \in \text{Isom}(\mathbb{R}^2)$,

$$I \circ f \circ I^{-1} = I \circ f \circ I = f$$

so fRf for any $f \in \text{Isom}(\mathbb{R}^2)$. So R is reflexive.

Now suppose that f_1Rf_2 , then there exists an invertible isometry $g \in \text{Isom}(\mathbb{R}^2)$ so that $f_1 = g \circ f_2 \circ g^{-1}$. Thus

$$g^{-1} \circ f_1 \circ g = g^{-1} \circ g \circ f_2 \circ g^{-1} \circ g = I \circ f_2 \circ I = f_2$$

so f_2Rf_1 . So R is symmetric.

Finally suppose that f_1Rf_2 and f_2Rf_3 , then there exists invertible isometries g_1, g_2 so that $f_1 = g_1 \circ f_2 \circ g_1^{-1}$ and $f_2 = g_2 \circ f_3 \circ g_2^{-1}$. Thus

$$f_1 = g_1 \circ g_2 \circ f_3 \circ g_2^{-1} \circ g_1^{-1}.$$

Notice that since g_1 and g_2 are invertible, then $g_1 \circ g_2$ is invertible and $(g_1 \circ g_2)^{-1} = g_2^{-1} \circ g_1^{-1}$ so

$$f_1 = (g_1 \circ g_2) \circ f_3 \circ (g_1 \circ g_2)^{-1}$$

and $f_1 R f_3$. So R is transitive.

Thus we have verified the criteria for an equivalence relation.

3. Let S be the set of all people (living or deceased) and define a relation xRy if x has the same biological father as y .

- (a) Show that R defines an equivalence relation.

A person always has the same biological father as himself. So R is reflexive.

If person x has the same biological father as person y , then person y has the same biological father as person x . So R is symmetric.

If person x has the same biological father as person y and person y has the same biological father as person z , then all three persons have the same biological father. Thus person x has the same biological father as person z . So R is transitive.

Thus we have verified the criteria for an equivalence relation.

- (b) In a sentence or two, describe an equivalence class for this equivalence relation.

For a given person x , the equivalence class $[x]$ contains all of siblings of x and half-siblings of x sharing the same biological father as x .

- (c) Let S/R be the set of equivalence classes of our equivalence relation. Suppose we wish to define a function $f : S/R \rightarrow S$ by

$$f([x]) = \text{the biological mother of } x.$$

Is such a function well-defined? Explain your answer in a sentence or two.

No it is not. An equivalence class can contain two people x and x' having the same biological father but different biological mother. In such a case $[x] = [x']$ but $f([x]) \neq f([x'])$.

II. Here are some problems about isometries.

1. Let \mathbb{R} be the set of real numbers and let $d(x, y) = |x - y|$.

- (a) Determine if $f : \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = x^2$ is an isometry.

The function f is not an isometry. Notice that $d(0, 2) = |2 - 0| = 2$ but $d(f(0), f(2)) = d(0, 4) = |4 - 0| = 4$ so $d(0, 2) \neq d(f(0), f(2))$.

- (b) Determine if $f : \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = 7 - x$ is an isometry.

The function f is an isometry. Notice that

$$d(f(x), f(y)) = d(7 - x, 7 - y) = |(7 - x) - (7 - y)| = |y - x| = |x - y| = d(x, y).$$

- (c) For $a \in \mathbb{R}$, let $T_a(x) = x + a$. Show that the set $\{T_a \mid a \in \mathbb{Z}\}$ is a subgroup of $\text{Isom}(\mathbb{R})$.

Let $a, b \in \mathbb{Z}$ and consider $(T_a \circ T_b)(x)$.

$$T_a(T_b(x)) = T_a(x + b) = x + b + a = x + (a + b)$$

so $T_a \circ T_b = T_{a+b}$. Since $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$ and $T_a \circ T_b \in \{T_c \mid c \in \mathbb{Z}\}$.

Consider $T_0 : \mathbb{R} \rightarrow \mathbb{R}$. We have $T_0(x) = x + 0 = x$ for all $x \in \mathbb{R}$. So $T_0 = I$ and $I \in \{T_c \mid c \in \mathbb{Z}\}$.

For any $a \in \mathbb{Z}$, consider $T_a \circ T_{-a} = T_{a-a} = T_0 = I$ and $T_{-a} \circ T_a = T_{-a+a} = T_0 = I$. So $T_a^{-1} = T_{-a}$ and since $-a \in \mathbb{Z}$ we have that $T_a^{-1} \in \{T_c \mid c \in \mathbb{Z}\}$. Our set satisfies all the criteria of a subgroup.

- (d) For $a \in \mathbb{R}$, let $R_a(x) = a - x$. Determine whether the set $\{R_a \mid a \in \mathbb{R}\}$ is a subgroup of $\text{Isom}(\mathbb{R})$.

This set is not a subgroup. For any $a, b \in \mathbb{Z}$ consider $(R_a \circ R_b)(x)$,

$$R_a(R_b(x)) = R_a(b - x) = a - (b - x) = x + (a - b)$$

so $R_a \circ R_b = T_{a-b}$ which is not an element of our set.

2. Let \mathbb{R}^2 be the real plane and let $d((x, y), (z, w)) = |x - z| + |y - w|$ be a metric (don't worry about proving this, you can assume that d is a metric).

- (a) Show that any translation $T_{(a,b)} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ (given by $T_{(a,b)}(x, y) = (x + a, y + b)$) is an isometry (with respect to the metric d).

For any $(x, y), (z, w) \in \mathbb{R}^2$, we see that

$$\begin{aligned} d(T_{(a,b)}(x, y), T_{(a,b)}(z, w)) &= d((x + a, y + b), (z + a, w + b)) \\ &= |(x + a) - (z + a)| + |(y + b) - (w + b)| \\ &= |x - z| + |y - w| \\ &= d((x, y), (z, w)) \end{aligned}$$

so $T_{(a,b)}$ satisfies the property of an isometry.

- (b) Let $r_L : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be reflection across the line $y = mx$. Show that r_L is not an isometry (with respect to the metric d) if $0 < m < 1$.

Consider the point $(0, 0)$, then $r_L(0, 0) = (0, 0)$ so $(0, 0)$ is a fixed point for r_L . Now let us compare $d((0, 0), (1, 0))$ with $d(r_L(0, 0), r_L(1, 0))$. First,

$$d((0, 0), (1, 0)) = |0 - 1| + |0 - 0| = 1.$$

Next we see that $r_L(1, 0) = (\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2})$ so

$$d(r_L(0, 0), r_L(1, 0)) = d((0, 0), (\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2})) = \left|0 - \frac{1-m^2}{1+m^2}\right| + \left|0 - \frac{2m}{1+m^2}\right|.$$

Since $0 < m < 1$, we have $0 < m^2 < 1$ so both $\frac{1-m^2}{1+m^2}$ and $\frac{2m}{1+m^2}$ are positive. Thus

$$d(r_L(0, 0), r_L(1, 0)) = \frac{1-m^2}{1+m^2} + \frac{2m}{1+m^2} = \frac{1+m(2-m)}{1+m^2}.$$

Since $0 < m < 1$, then $2 - m > 1 > m$ so $m(2 - m) > m^2$ and we see

$$d(r_L(0, 0), r_L(1, 0)) > 1$$

and $d(r_L(0, 0), r_L(1, 0)) \neq d((0, 0), (1, 0))$.

III. Here are some problems about abstract groups.

1. Consider the following sets and binary operations. Determine which are groups. If it is a group, prove it. If it is not, show (by example) which group axiom fails.

- (a) Let $S = \mathcal{P}(\{1, 2, 3, 4\})$ (the power set of $\{1, 2, 3, 4\}$) and let $U \cdot V = U \cup V$.

This is not a group. Notice that if it were, then the identity would be the empty set \emptyset since $U \cup \emptyset = \emptyset \cup U = U$. However, for any $V \in \mathcal{P}(\{1, 2, 3, 4\})$, $U \subset U \cup V$. So if U is non-empty then $U \cup V \neq \emptyset$ for any $V \in \mathcal{P}(\{1, 2, 3, 4\})$.

- (b) Let
- $S = \mathbb{Z}$
- and
- $a \cdot b = a - b$
- .

This operation is not associative. Notice for any $a, b, c \in \mathbb{Z}$,

$$a \cdot (b \cdot c) = a \cdot (b - c) = a - (b - c) = a - b + c$$

whereas

$$(a \cdot b) \cdot c = (a - b) \cdot c = (a - b) - c = a - b - c$$

so if $c \neq 0$, then $a \cdot (b \cdot c) \neq (a \cdot b) \cdot c$.

- (c) Let
- $S = \mathbb{R}$
- and let
- $x \cdot y = x^2 - y^2$
- .

This operation is not associative. Notice for any $x, y, z \in \mathbb{R}$, we have

$$x \cdot (y \cdot z) = x \cdot (y^2 - z^2) = x^2 - (y^2 - z^2)^2 = x^2 - y^4 + 2y^2z^2 - z^4$$

whereas

$$(x \cdot y) \cdot z = (x^2 - y^2) \cdot z = (x^2 - y^2)^2 - z^2 = x^4 - 2x^2y^2 + y^4 - z^2.$$

So consider an example like $x = 2$, $y = 1$, and $z = 1$ we get

$$2 \cdot (1 \cdot 1) = 2 \cdot 0 = 4$$

and

$$(2 \cdot 1) \cdot 1 = 3 \cdot 1 = 8$$

which are not equal.

2. Let G be the group of integers (\mathbb{Z}) under the addition operation and let H be the group $\text{Isom}(\mathbb{R})$ under the composition operation.

- (a) Show that the function
- $f : G \rightarrow H$
- given by
- $f(a) = T_a$
- (where
- $T_a : \mathbb{R} \rightarrow \mathbb{R}$
- is given by
- $T_a(x) = x + a$
-) is a homomorphism.

Let $a, b \in \mathbb{Z}$ and consider $T_a \circ T_b$. For $x \in \mathbb{R}$

$$(T_a \circ T_b)(x) = T_a(T_b(x)) = T_a(x + b) = (x + b) + a = x + (a + b) = T_{a+b}(x)$$

so $T_a \circ T_b = T_{a+b}$. So we now consider

$$f(a + b) = T_{a+b} = T_a \circ T_b = f(a) \circ f(b)$$

so f is a homomorphism.

- (b) Determine if the function
- $f : G \rightarrow H$
- given by
- $f(a) = R_a$
- (where
- $R_a : \mathbb{R} \rightarrow \mathbb{R}$
- is given by
- $R_a(x) = a - x$
-) a homomorphism.

The function f is not a homomorphism. Let $a, b \in \mathbb{Z}$ and consider $R_a \circ R_b$. For $x \in \mathbb{R}$

$$(R_a \circ R_b)(x) = R_a(R_b(x)) = R_a(b - x) = a - (b - x) = x - (a - b) = T_{a-b}(x)$$

so $R_a \circ R_b = T_{a-b}$.

Now consider $f(a + b)$ and $f(a) \circ f(b)$. First $f(a + b) = R_{a+b}$ whereas

$$f(a) \circ f(b) = R_a \circ R_b = T_{a-b}.$$

But notice that $R_{a+b}(\frac{a+b}{2}) = (a+b) - \frac{a+b}{2} = \frac{a+b}{2}$ whereas T_{a-b} only fixes a point if $a - b = 0$ (so $T_{a-b} = T_0 = I$). Thus $R_{a+b} \neq T_{a-b}$ and $f(a + b) \neq f(a) \circ f(b)$.

- (c) Show that for any $m \in \mathbb{Z}$, the function $f_m : G \rightarrow G$ given by $f_m(a) = ma$ is a homomorphism. For which m is f_m injective? For which m is f_m surjective?

Let $a, b, m \in \mathbb{Z}$, then $f_m(a + b) = m(a + b) = ma + mb = f_m(a) + f_m(b)$. So f_m is a homomorphism for any $m \in \mathbb{Z}$.

Consider $\ker(f_m) = \{a \in \mathbb{Z} \mid f_m(a) = 0\}$ (since 0 is the identity element of G). However $f_m(a) = ma$. If $ma = 0$, then either $m = 0$ or $a = 0$. If $m = 0$, then $\ker(f_0) = G$ and f_0 is not injective. If $m \neq 0$, then $ma = 0$ if and only if $a = 0$ so $\ker(f_m) = \{0\}$ so f_m is injective. So f_m is injective if and only if $m \in \mathbb{Z} \setminus \{0\}$.

Now let us consider surjectivity. For any $a \in \mathbb{Z}$, $f_m(a) = ma$ so $m \mid f_m(a)$. If $|m| > 1$, then $f_m(a) \neq 1$ for any $a \in \mathbb{Z}$ since $m \nmid 1$, so f_m is not surjective. If $m = 0$, then $f_0(a) = 0$ for all $a \in \mathbb{Z}$ so f_0 is not surjective. If $m = -1$ then $f_{-1}(a) = -a$. So for any $a \in \mathbb{Z}$, we see that $f_{-1}(-a) = (-1)(-a) = a$ so f_{-1} is surjective. If $m = 1$, then $f_1(a) = a$ which is obviously surjective. So f_m is surjective if and only if $m \in \{\pm 1\}$.

3. Let G be a group and let $g \in G$.

- (a) Show that the function $f_g : G \rightarrow G$ given by $f_g(x) = gxg^{-1}$ is an isomorphism.

Let $g \in G$. Let us start by showing that f_g is a homomorphism. For $x_1, x_2 \in G$,

$$f_g(x_1x_2) = gx_1x_2g^{-1} = gx_1(g^{-1}g)x_2g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = f_g(x_1)f_g(x_2).$$

Now let us show that f_g is injective. Let $x \in \ker(f_g)$. Then $f_g(x) = e$ so $gxg^{-1} = e$. Thus $g^{-1}(gxg^{-1})g = g^{-1}e$ which is the same as

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

and $x = e$. So $\ker(f_g) \subset \{e\}$. Further $f_g(e) = geg^{-1} = gg^{-1} = e$ so $\{e\} \subset \ker(f_g)$. Thus $\ker(f_g) = \{e\}$ and f_g is injective.

Now let us show that f_g is surjective. Let $x \in G$, then $g^{-1}xg \in G$ such that

$$f_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = (gg^{-1})x(gg^{-1}) = exe = x$$

so f_g is surjective.

- (b) Assume that $g \neq e$. Determine if the function $L_g : G \rightarrow G$ given by $L_g(x) = gx$ is a homomorphism (**Hint:** If L_g is a homomorphism, what would I know about $\ker(L_g)$.)

The function L_g is not a homomorphism. Suppose it were, then

$$L_g(e) = L_g(ee) = L_g(e)L_g(e)$$

thus $L_g(e)^{-1}L_g(e) = L_g(e)^{-1}L_g(e)L_g(e)$ which shows that $e = L_g(e)$. Thus $e \in \ker(L_g)$.

Now let $x \in \ker(L_g)$, then $L_g(x) = e$, so $gx = e$. Thus $x = g^{-1}$ and $\ker(L_g) \subset \{g^{-1}\}$. This contradicts that $e \in \ker(L_g)$ so L_g is not a homomorphism.