

HOMEWORK 3

Throughout the assignment R denotes a commutative ring (with identity). Recall there is an abstract definition of this, but for our purposes you can think of R as being \mathbb{Z} , \mathbb{Z}_n (for some integer n), \mathbb{Q} , \mathbb{R} , or \mathbb{C} .

- (1) Let $G := \mathbb{R} - \{-1\}$ and define $a * b := a + b + a \cdot b$ (here $+$ and \cdot have their usual meanings). Show that $(G, *)$ is a group. (Students typically forget a lot of steps on this problem. Make sure you show that if a and b are in G that $a * b \in G$, i.e. that it does **not** equal -1 .)
- (2) (**generalized socks and shoes**)
Let g_1, \dots, g_n be elements of a group. Show that

$$(g_1 \cdots g_n)^{-1} = g_n^{-1} \cdots g_1^{-1}.$$

Solution. For elements x, y in a group, we know that $x * y = e$ if and only if $y = x^{-1}$ (multiply both sides of the equation on the left by x^{-1}). Since we have just this when we take $x = g_1 \cdots g_n$ and $y = g_n^{-1} \cdots g_1^{-1}$ we are done.

- (3) Show that the set of matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

(with $a, b, c \in R$) forms a group under matrix multiplication. Make a table of this group when $R = \mathbb{Z}_2$. Does this group look familiar?

Solution. Let's call this set H . All matrices in H have determinant 1. Hence this set of matrices is a subset of the group, $\text{GL}(n, R)$. So we can apply the two step subgroup test (this set of matrices is not empty since taking $a, b, c = 0$, shows us that the identity matrix lives in H).

- Let

$$g_1 := \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad g_2 := \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

be elements of H . Then

$$g_1 g_2 = \begin{pmatrix} 1 & a+x & y+az+b \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix}$$

which is also a member of H . Thus H is closed under multiplication.

- Let $g = g_1$ (as in the previous part). Then

$$g^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

also lives in H .

Putting these two parts together shows that H is a group.

In the special case that $R = \mathbb{Z}_2$ H has $2^3 = 8$ elements. If one makes the table and plays with it a bit (see problem 6) one can see that it is the same table as the table for the symmetries of the square.

- (4) In this problem we deal with quaternions.
- (a) Show for quaternions q_1 and q_2 that $\overline{q_1 q_2} = \overline{q_2} \overline{q_1}$ (notice the reverse! One could prove this relation by “brute force” but there are slicker ways).
- (b) Recall from homework 1 problem 3 that a quaternion is in \mathbb{S}^3 if and only if $\overline{q} = q^{-1}$. Use this fact, socks and shoes, and the first part of this problem to show that \mathbb{S}^3 is closed under multiplication.

Solution. Suppose that q_1 and q_2 are in \mathbb{S}^3 . Then we need only show that $\overline{q_1 q_2} = (q_1 q_2)^{-1}$ for $q_1 q_2 \in \mathbb{S}^3$ as well.

We have

$$\begin{aligned} \overline{q_1 q_2} &= \overline{q_2} \overline{q_1} && \text{(by 4a)} \\ &= q_2^{-1} q_1^{-1} && \text{(since } q_1, q_2 \in \mathbb{S}^3\text{)} \\ &= (q_1 q_2)^{-1} && \text{(socks and shoes)} \end{aligned}$$

which is what we needed.

- (c) Show that \mathbb{S}^3 is a group. (the only thing that you need to do at this point is show that the inverse of an element in \mathbb{S}^3 is also in \mathbb{S}^3).

Solution. Let $q \in \mathbb{S}^3$. We wish to show that $q^{-1} \in \mathbb{S}^3$. That is we want to show that $\overline{q^{-1}} = (q^{-1})^{-1} = q$. But since $q \in \mathbb{S}^3$ we know that $q^{-1} = \overline{q}$. Hence $\overline{q^{-1}} = \overline{\overline{q}} = q$ as desired.

- (5) Show that the following are equivalent for elements g and h in a group (NONE ARE TRUE BY THEMSELVES!! PROVE THIS BY FIRST ASSUMING A PART IS TRUE AND USE THAT TO SHOW THAT ANOTHER PART IS TRUE!)
- (a) $(g * h)^{-1} = g^{-1} * h^{-1}$
- (b) $g^2 * h^2 = (g * h)^2$
- (c) $g * h * g^{-1} * h^{-1} = e$
- (d) g and h commute.

Solution. We show that (4) \Leftrightarrow (2), (4) \Leftrightarrow (3), and (1) \Leftrightarrow (3).

We have that

$$\begin{aligned} &(g * h)^2 = g^2 * h^2 \\ \Leftrightarrow &g * h * g * h = g * g * h * h && \text{(by def)} \\ \Leftrightarrow &h * g * h = g * h * h && \text{(cancel } g\text{'s on left)} \\ \Leftrightarrow &h * g = g * h && \text{(cancel } h\text{'s on right)}. \end{aligned}$$

Hence (4) \Leftrightarrow (2).

Next we set our sights on proving (4) \Leftrightarrow (3).

$$\begin{aligned}
 & g * h * g^{-1} * h^{-1} = e \\
 \Leftrightarrow & \quad g * h * g^{-1} = h \quad (\text{mult both sides on rt by } h) \\
 \Leftrightarrow & \quad g * h = h * g \quad (\text{mult both sides on rt by } g).
 \end{aligned}$$

Hence (4) \Leftrightarrow (3).

The last thing that we need to show, (1) \Leftrightarrow (3), holds by definition of what it means for two elements of a group to be inverses of each other.

- (6) (a) Prove by hand that for matrices $A \in M_2(R)$ and $B \in M_2(R)$ (i.e. A and B are 2 by 2 matrices with coefficients in R) that

$$\det(AB) = \det(A) \det(B).$$

Solution. Let

$$A := \begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix}$$

and

$$B := \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{2,1} & y_{2,2} \end{pmatrix}.$$

Then we have that

$$AB = \begin{pmatrix} x_{1,1}y_{1,1} + x_{1,2}y_{2,1} & x_{1,1}y_{1,2} + x_{1,2}y_{2,2} \\ x_{2,1}y_{1,1} + x_{2,2}y_{2,1} & x_{2,1}y_{1,2} + x_{2,2}y_{2,2} \end{pmatrix}$$

and hence $\det(AB) =$

$$\begin{aligned}
 & (x_{1,1}y_{1,1} + x_{1,2}y_{2,1})(x_{2,1}y_{1,2} + x_{2,2}y_{2,2}) - (x_{1,1}y_{1,2} + x_{1,2}y_{2,2})(x_{2,1}y_{1,1} + x_{2,2}y_{2,1}) \\
 & = x_{1,1}y_{1,1}x_{2,2}y_{2,2} + x_{1,2}y_{2,1}x_{2,1}y_{1,2} - x_{1,1}y_{1,2}x_{2,2}y_{2,1} - x_{1,2}y_{2,2}x_{2,1}y_{1,1}.
 \end{aligned}$$

Meanwhile $\det(A) \det(B) =$

$$\begin{aligned}
 & (x_{1,1}x_{2,2} - x_{2,1}x_{1,2})(y_{1,1}y_{2,2} - y_{1,2}y_{2,1}) \\
 & = x_{1,1}y_{1,1}x_{2,2}y_{2,2} + x_{1,2}y_{2,1}x_{2,1}y_{1,2} - x_{1,1}y_{1,2}x_{2,2}y_{2,1} - x_{1,2}y_{2,2}x_{2,1}y_{1,1}
 \end{aligned}$$

as desired.

- (b) Use the first part of this problem to show that

$$\{A \in M_2(R) : \det(A) = 1\}$$

forms a group under matrix multiplication. It is called the 2 by 2 *special linear group over R* and is denoted $SL(2, R)$.

Solution. (i) If A and B have determinant 1, then AB has determinant $1 \cdot 1 = 1$. Hence $SL(2, R)$ is closed under multiplication.

(ii) Multiplication of matrices is associative in general.

(iii) The identity matrix,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

has determinant 1. Thus $SL(2, R)$ contains an identity.

(iv) If $A \in \text{SL}(2, R)$ then

$$A^{-1} = \begin{pmatrix} x_{2,2} & -x_{1,2} \\ -x_{2,1} & x_{1,1} \end{pmatrix}$$

which still lives in $\text{SL}(2, R)$ (since the determinant is still 1).

(c) Show that $\text{SL}(2, R)$ is finite if and only if R is finite.

Solution. The set of matrices of the form

$$\left\{ \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} : r \in R \right\}$$

all live in $\text{SL}(2, R)$. Hence if R is infinite, so is $\text{SL}(2, R)$ (since it would contain that infinite set). On the other hand, if R is finite, then $M_2(R)$ has $|R|^4$ elements ($|R|$ per entry). Since $\text{SL}(2, R)$ is a subset of $M_2(R)$, it is also finite.

(d) Make a multiplication table of $\text{SL}(2, \mathbb{Z}_2)$. Does table look like a table we have already seen?

Solution. There are 16 two by two matrices with entries \mathbb{Z}_2 . They are

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Of these 16 matrices only

$$\begin{aligned} x &:= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & y &:= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} & e &:= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ b &:= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & z &:= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} & a &:= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \end{aligned}$$

have determinant equal to 1 (in the case \mathbb{Z}_2 this is the same as requiring that the determinant not equal zero). For starters, note that e is the identity and that $a^2 = y$, $a^3 = e$, (so $y = a^{-1}$) $b^2 = e$, $ab = x$, $a^2b = z$, and $ba = a^2b$. So if we make a multiplication table we have

\bullet		e	a	a^2	b	ab	a^2b
e		e	a	a^2	b	ab	a^2b
a		a	a^2	e	ab	a^2b	b
a^2		a^2	e	a	a^2b	b	ab
b		b	a^2b	ab	e	a^2	a
ab		ab	b	a^2b	a	e	a^2
a^2b		a^2b	ab	b	a^2	a	e

This is exactly the same table as the table for the symmetries of the triangle (which in turn is the table for S_3).

(e) **Research**

- Now for matrices $A \in M_n(R)$ and $B \in M_n(R)$ it turns out that one still has that $\det(A)\det(B)$. Cite a reference which proves this fact.
- Use the previous fact to show that $SL(n, R)$ (the set of n by n matrices with coefficients in R and determinant 1) is closed under matrix multiplication.
- Look up the formula for the *adjoint* of a matrix. Show that the adjoint of a matrix with coefficients in R still has coefficients in R (that is $M_n(R)$ is closed under taking adjoints).
- Reference a source which proves that for a matrix A that

$$A^*A = AA^* = \det(A)I_n.$$

- Use these facts to show that the inverse of an element in $SL(n, R)$ is still in $SL(n, R)$ and conclude that this more general set is also a group.

(7) Let $(G, *)$ and (H, \bullet) be groups.

(a) Prove that $G \times H$ with the binary operation

$$(g, h) \cdot (g', h') := (g * g', h \bullet h')$$

forms a group.

- (b) Show that with the operation defined above, $G \times H$ is abelian if and only if G and H are abelian.
- (c) Show that $\mathbb{Z}_2 \times \mathbb{Z}_2$ has the same multiplication table as the set of symmetries of a rectangle which is *not* a square.

Solution. There are four such symmetries.

- e := Do nothing.
- $f1$:= Flip across the horizontal.
- $f2$:= Flip across the vertical.
- r := Rotation by 180° .

With these assignments, the multiplication table is

•		e	$f1$	$f2$	r
—		—	—	—	—
		e	$f1$	$f2$	r
e		e	e	r	$f2$
$f1$		$f1$	r	e	$f1$
$f2$		$f2$	r	e	$f1$
r		r	$f2$	$f1$	e

On the other hand, the table for $\mathbb{Z}_2 \times \mathbb{Z}_2$ is

•		$(0, 0)$	$(1, 0)$	$(0, 1)$	$(1, 1)$
—		—	—	—	—
		$(0, 0)$	$(1, 0)$	$(0, 1)$	$(1, 1)$
$(0, 0)$		$(0, 0)$	$(0, 0)$	$(1, 1)$	$(0, 1)$
$(1, 0)$		$(1, 0)$	$(1, 1)$	$(0, 0)$	$(1, 0)$
$(0, 1)$		$(0, 1)$	$(1, 1)$	$(0, 0)$	$(1, 0)$
$(1, 1)$		$(1, 1)$	$(0, 1)$	$(1, 0)$	$(0, 0)$

These two tables are the “same” in the sense that if we called $(0, 0) = e$, $(1, 0) = f1$, $(0, 1) = f2$, and $(1, 1) = r$ these two tables would be identical.