

## MATH 113 HOMEWORK 6 SOLUTIONS

### 1. ABELIAN GROUPS

**Problem 1.1** (Linear Algebra of Abelian Groups, Part I). Let  $A$  be an abelian group, and suppose that  $\{a_1, \dots, a_n\} \in A$  is a generating set for  $A$ .

- (1) Show that for  $i \neq j$  and  $k \in \mathbb{Z}$ , the set  $\{a_1, \dots, a_{i-1}, a_i + ka_j, a_{i+1}, \dots, a_n\}$  is also a generating set for  $A$ . Show moreover that this set is a basis for  $A$  if and only if  $\{a_1, \dots, a_n\}$  is.
- (2) Show that for all  $i$ , the set  $\{a_1, \dots, a_{i-1}, (-a_i), a_{i+1}, \dots, a_n\}$  is a generating set for  $A$ . Show moreover that this set is a basis if and only if  $\{a_1, \dots, a_n\}$  is.

**Solution 1.1.1** (Solution to Part (1)). Let  $x \in A$  be any element. Then there exist integers  $m_1, \dots, m_n$  such that

$$x = m_1 a_1 + \dots + m_n a_n$$

since  $a_1, \dots, a_n$  is a generating set for  $A$ . Now, since  $a_i = (a_i + ka_j) - ka_j$ , we have  $m_i a_i = m_i(a_i + ka_j) - m_i ka_j$ , so

$$x = m_1 a_1 + \dots + m_i(a_i + ka_j) + \dots + (m_j - m_i k)a_j + \dots + m_n a_n.$$

Hence  $\{a_1, \dots, a_{i-1}, a_i + ka_j, a_{i+1}, \dots, a_n\}$  is also a generating set for  $A$ .

Suppose now that  $\{a_1, \dots, a_n\}$  is linearly independent. Suppose that

$$m_1 a_1 + \dots + m_i(a_i + ka_j) + \dots + m_n a_n = 0$$

for some  $m_1, \dots, m_n \in \mathbb{Z}$ . We want to show that  $m_\ell = 0$  for all  $\ell$ . Expanding the above expression, we get

$$m_1 a_1 + \dots + m_i a_i + \dots + (m_j + m_i k)a_j + \dots + m_n a_n = 0.$$

Since  $a_1, \dots, a_n$  are linearly independent, we have that  $m_\ell = 0$  for all  $\ell \neq j$ , and  $m_j + m_i k = 0$ . But then in particular  $m_i = 0$ , so  $0 = m_j + m_i k = m_j + 0$ , so  $m_j = 0$  also. Hence all the  $m_\ell$  are 0, so  $\{a_1, \dots, a_{i-1}, a_i + ka_j, a_{i+1}, \dots, a_n\}$  are linearly independent, hence a basis of  $A$ .

**Solution 1.1.2** (Solution to Part (2)). This is easier. Let  $x \in A$  be any element. Then there exist integers  $m_1, \dots, m_n$  such that

$$x = m_1 a_1 + \dots + m_n a_n$$

since  $a_1, \dots, a_n$  is a generating set for  $A$ . Then

$$x = m_1 a_1 + \dots + (-m_i)(-a_i) + \dots + m_n a_n,$$

hence  $\{a_1, \dots, a_{i-1}, (-a_i), a_{i+1}, \dots, a_n\}$  is a generating set for  $A$ .

Suppose now that  $\{a_1, \dots, a_n\}$  is linearly independent. Suppose that

$$m_1 a_1 + \dots + m_i (-a_i) + \dots + m_n a_n = 0$$

for some  $m_1, \dots, m_n \in \mathbb{Z}$ . Then also

$$m_1 a_1 + \dots + (-m_i) a_i + \dots + m_n a_n = 0.$$

Since  $a_1, \dots, a_n$  are linearly independent,  $m_j = 0$  for all  $j \neq i$ , and  $-m_i = 0$ . Hence also  $m_i = 0$ , and so  $\{a_1, \dots, a_{i-1}, (-a_i), a_{i+1}, \dots, a_n\}$  is a linearly independent set, hence a basis for  $A$ .

**Problem 1.2** (Linear Algebra of Abelian Groups, Part II). **You are NOT required to write up this problem to submit. However, you must understand it completely, as you will need it for the next problem, and for the final exam, hint hint.**

Let  $H$  be a subgroup of  $\mathbb{Z}^n$ . We know that  $H$  is finitely generated; suppose  $h_1, \dots, h_k$  generate  $H$ . Let  $e_1, \dots, e_n$  be the standard basis of  $\mathbb{Z}^n$ . We know that we can write each  $h_i$  as

$$h_i = (a_{1i}, a_{2i}, \dots, a_{ni}) = \sum_{j=1}^n a_{ji} e_j.$$

Bundle this information as an  $n \times k$ -matrix  $M = (a_{ij})$ , so the  $i$ th column of  $M$  contains the coordinates of  $h_i$ .

- (1) Show that exchanging the generators  $h_i$  and  $h_j$  corresponds to exchanging the  $i$ th and  $j$ th columns of  $M$ .
- (2) Show that exchanging the basis vectors  $e_i$  and  $e_j$  corresponds to exchanging the  $i$ th and  $j$ th rows of  $M$ .
- (3) Show that multiplying the generator  $h_i$  by  $-1$  corresponds to multiplying the  $i$ th column of  $M$  by  $-1$ .
- (4) Show that multiplying the basis vector  $e_i$  by  $-1$  corresponds to multiplying the  $i$ th row of  $M$  by  $-1$ .
- (5) For  $i \neq j$  and  $k \in \mathbb{Z}$ , show that replacing the generator  $h_i$  by  $h_i + kh_j$  corresponds to adding  $k$  times the  $j$ th column of  $M$  to the  $i$ th column of  $M$ .
- (6) For  $i \neq j$  and  $k \in \mathbb{Z}$ , show that replacing the basis vector  $e_i$  by  $e_i + ke_j$  corresponds to *subtracting*  $k$  times the  $i$ th row of  $M$  from the  $j$ th row of  $M$  (note that the roles of  $i$  and  $j$  have also changed!).

Conclude that when calculating  $\mathbb{Z}^n/H$ , we may apply any of the above “elementary row and column operations” to  $M$  and obtain the same quotient.

**Solution 1.2.1.** The most confusing part is number (6), so let’s explain that one. Let  $e_1, \dots, e_n$  be our current basis of  $\mathbb{Z}^n$ , and take some generator  $x = a_1 e_1 + \dots + a_n e_n$  of  $H$ . As a column vector, we express this element as

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Now, suppose we replace  $e_i$  by  $e_i + ke_j$ . Then, as in part 1 of problem 1, we have  $e_i = (e_i + ke_j) - ke_j$ , hence

$$x = a_1e_1 + \cdots + a_i(e_i + ke_j) + \cdots + (a_j - ka_i)e_j + \cdots + a_ne_n.$$

So the coordinates of  $x$  with respect to the new basis are  $(a_1, \dots, a_i, \dots, a_j - ka_i, \dots, a_n)$ , i.e. we have replaced our original column vector by

$$\begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_j - ka_i \\ \vdots \\ a_n \end{pmatrix}.$$

In other words, we have subtracted  $k$  times the  $i$ th row of our vector from the  $j$ th row of our vector.

**Problem 1.3** (Linear Algebra of Abelian Groups, Part III). Let's use the previous problem to actually do some calculations!

- (1) Let  $H$  be the subgroup of  $\mathbb{Z}^2$  generated by  $(6, 9)$ . Use the previous problem to show that  $\mathbb{Z}^2/H \cong \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ . By keeping track of the row operations you do, explain how to choose the basis of  $\mathbb{Z}^2$  that gives this isomorphism.
- (2) Let  $H$  be the subgroup of  $\mathbb{Z}^3$  generated by  $(1, 2, 3)$  and  $(2, 2, 2)$ . Calculate  $\mathbb{Z}^3/H$  as a product of cyclic groups.
- (3) Let  $H$  be the subgroup of  $\mathbb{Z}^3$  generated by  $\{(1, 2, 3), (3, 4, 5), (5, 6, 7), (7, 8, 9)\}$ . Calculate  $\mathbb{Z}^3/H$  as a product of cyclic groups.

**Solution 1.3.1** (Solution to Part (1)). Using elementary row operations, we have

$$\begin{pmatrix} 6 \\ 9 \end{pmatrix} \sim \begin{pmatrix} 6 \\ 3 \end{pmatrix} \sim \begin{pmatrix} 0 \\ 3 \end{pmatrix}.$$

Now, let  $e_1, e_2$  be the original (standard) basis of  $\mathbb{Z}^2$ . From part (6) of the last problem, subtracting  $k$  times row  $i$  from row  $j$  corresponds to adding  $k$  times  $e_j$  to  $e_i$ . So, our first row operation is to subtract 1 times row 1 of our matrix from row 2 of our matrix; this corresponds to replacing  $e_1$  by  $e_1 + e_2$ , so our new basis after the first row operation is  $\{e_1 + e_2, e_2\}$ . Now, our second row operation is to subtract 2 times row 2 from row 1, of our matrix, so we replace  $e_2$  by  $e_2 + 2(e_1 + e_2) = 2e_1 + 3e_2$ . So the final basis we end up with is  $\{e_1 + e_2, 2e_1 + 3e_2\}$ , i.e.  $\{(1, 1), (2, 3)\}$ .

Now, with respect to this new basis,  $H$  is the subgroup of  $\mathbb{Z}^2$  generated by  $(0, 3)$ , i.e.  $H = \{0\} \times 3\mathbb{Z}$ . Hence

$$\mathbb{Z}^2/H \cong \frac{\mathbb{Z} \times \mathbb{Z}}{\{0\} \times 3\mathbb{Z}} \cong \mathbb{Z}/\{0\} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

**Solution 1.3.2** (Solution to Part (2)). Applying elementary row and column operations to the matrix of generators gives:

$$\begin{pmatrix} 1 & 2 \\ 2 & 2 \\ 3 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 2 & -2 \\ 3 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 2 & 2 \\ 3 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 0 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}.$$

Hence there is a basis of  $\mathbb{Z}^3$  such that with respect to this basis,  $H$  is the subgroup generated by  $(1, 0, 0)$  and  $(0, 2, 0)$ , i.e.  $H = \mathbb{Z} \times 2\mathbb{Z} \times \{0\}$ . Then

$$\mathbb{Z}^3/H \cong \frac{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{\mathbb{Z} \times 2\mathbb{Z} \times \{0\}} \cong \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/\{0\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

**Solution 1.3.3** (Solution to Part (3)). Applying elementary row and column operations to the matrix of generators gives:

$$\begin{pmatrix} 1 & 3 & 5 & 7 \\ 2 & 4 & 6 & 8 \\ 3 & 5 & 7 & 9 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 4 & 6 \\ 2 & 2 & 4 & 6 \\ 3 & 2 & 4 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 3 & 2 & 0 & 0 \end{pmatrix}.$$

By part (2) we already know this matrix can be reduced to

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

using elementary row and column operations. Hence, as in part (2), there is a basis of  $\mathbb{Z}^3$  such that with respect to this basis,  $H$  is the subgroup generated by  $(1, 0, 0)$  and  $(0, 2, 0)$ , and again

$$\mathbb{Z}^3/H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

**Problem 1.4.** Let  $A$  and  $B$  be finitely generated abelian groups. Show that  $\text{rank}(A \times B) = \text{rank}(A) + \text{rank}(B)$ . (Hint: use the structure theorem, plus the proposition proved on the last homework that  $\text{rank}(A) = \text{rank}(A/T(A))$ .)

**Solution 1.4.1.** Let  $A$  and  $B$  be finitely generated abelian groups. By the structure theorem, we can write

$$A \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z} \times \mathbb{Z}^r$$

and

$$B \cong \mathbb{Z}/b_1\mathbb{Z} \times \cdots \times \mathbb{Z}/b_m\mathbb{Z} \times \mathbb{Z}^s$$

for some natural numbers  $a_1, \dots, a_n, b_1, \dots, b_m, r$ , and  $s$ . We then have

$$T(A) = \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z} \times \{0\},$$

so

$$A/T(A) \cong \frac{\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z} \times \mathbb{Z}^r}{\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z} \times \{0\}} \cong \mathbb{Z}^r.$$

Likewise  $B/T(B) \cong \mathbb{Z}^s$ . Thus we have  $\text{rank}(A) = \text{rank}(A/T(A)) = \text{rank}(\mathbb{Z}^r) = r$  and likewise  $\text{rank}(B) = s$ .

Now, we have  $T(A \times B) = T(A) \times T(B)$ , so

$$\frac{A \times B}{T(A \times B)} = \frac{A \times B}{T(A) \times T(B)} \cong A/T(A) \times B/T(B) \cong \mathbb{Z}^r \times \mathbb{Z}^s = \mathbb{Z}^{r+s},$$

hence

$$\text{rank}(A \times B) = \text{rank}(A \times B / T(A \times B)) = \text{rank}(\mathbb{Z}^{r+s}) = r+s = \text{rank}(A) + \text{rank}(B).$$

## 2. GROUP ACTIONS

**Problem 2.1.** Let  $G = (\mathbb{R}, +)$ , and define an action of  $G$  on  $\mathbb{R}^2$  by letting  $\theta \in G$  act by clockwise rotation by  $\theta$ . Show that this is in fact an action of  $G$ . Find the orbits of this action (a geometric description will suffice), and for each  $v \in \mathbb{R}^2$ , compute the stabilizer of  $v$ .

**Solution 2.1.1.** Let  $\theta_1, \theta_2 \in \mathbb{R}$  and  $v \in \mathbb{R}^2$  be arbitrary. Then  $(\theta_1 + \theta_2) \cdot (v)$  is  $v$  rotated by the angle  $\theta_1 + \theta_2$ . This is the same as rotating  $v$  by  $\theta_1$ , then by  $\theta_2$ , i.e.

$$(\theta_1 + \theta_2) \cdot v = \theta_2 \cdot (\theta_1 \cdot v).$$

(Note the order here is unimportant since  $\mathbb{R}$  is abelian). We also have to check that the identity of  $\mathbb{R}$  acts trivially. But  $0 \cdot v$  is  $v$  rotated by 0 radians, which is of course just  $v$ .

Let  $v = (x, y) \in \mathbb{R}^2$  be arbitrary. Let  $r = \sqrt{x^2 + y^2}$  be the length of  $v$ . Then the orbit of  $v$  consists of the circle of radius  $r$ ; two vectors  $v_1, v_2 \in \mathbb{R}^2$  differ by a rotation if and only if they have the same length. In the case  $r = 0$ , the orbit of  $v = (0, 0)$  is just the single point  $v$ .

Now, suppose  $v \in \mathbb{R}^2$  is a nonzero vector. Then  $\theta \cdot v = v$  if and only if rotation by  $\theta$  leaves  $v$  unchanged, which occurs only when  $\theta$  is an integer multiple of  $2\pi$ , i.e. the stabilizer  $G_v$  of  $v$  is  $2\pi\mathbb{Z}$ . On the other hand, if  $v = (0, 0)$ , then  $v$  is fixed by every rotation, so in this case  $G_v = G$ .

**Problem 2.2** (Creative Problem: Properties of Group Actions). Let  $G$  be a group and let  $X$  be a  $G$ -set.

- (1) The action of  $G$  on  $X$  is called *faithful* if the only element of  $G$  which acts trivially is the identity, i.e. if for every  $g \in G$ ,  $g \cdot x = x$  for all  $x \in X$  only if  $g = e$ . Give three examples of faithful group actions and three examples of non-faithful group actions.
- (2) The action of  $G$  on  $X$  is called *transitive* if it has a single orbit, i.e. if for every  $x, y \in X$  there is a  $g \in G$  such that  $g \cdot x = y$ . Give three examples of transitive group actions and three examples of non-transitive group actions.
- (3) Suppose that the action of  $G$  on  $X$  is both faithful and transitive and suppose that  $X$  is non-empty. Show that there is a bijection from  $G$  to  $X$ .

**Solution 2.2.1** (Solution to Part (1)). Some faithful group actions:

- (1) If  $G$  is any group, the left regular representation of  $G$  is a faithful action; if  $g \cdot e = e$  then  $ge = e$ , so  $g = e$ .
- (2)  $S_n$  acts faithfully on the set  $\{1, \dots, n\}$ , since the only permutation which does not move any element is the identity. More generally, if  $X$  is any set,  $S_X$  acts faithfully on  $X$ .
- (3)  $D_n$  acts faithfully on the vertices of the  $n$ -gon.
- (4) The group  $GL_2(\mathbb{R})$  acts faithfully on  $\mathbb{R}^2$  by matrix multiplication. If  $M \in GL_2(\mathbb{R})$  and

$$M \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

and

$$M \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

then  $M$  is the identity matrix.

Some non-faithful group actions:

- (1) Let  $G$  be any nontrivial group. Then the trivial action of  $G$  on the one-element set  $\{1\}$  is not faithful.
- (2) Let  $\mathbb{Z}$  act on  $\mathbb{Z}/n\mathbb{Z}$  by  $a + [b] = [a + b]$ . This action is not faithful since every element in  $n\mathbb{Z}$  fixes every element of  $\mathbb{Z}/n\mathbb{Z}$ .
- (3) As in the previous problem,  $(\mathbb{R}, +)$  acts on the plane by rotations; this action is not faithful since  $2\pi\mathbb{Z} \subseteq \mathbb{R}$  fixes every element of  $\mathbb{R}^2$ .

**Solution 2.2.2** (Solution to Part (2)). Some examples of transitive group actions:

- (1) If  $G$  is any group, the left regular representation of  $G$  is transitive; let  $g, h \in G$  be arbitrary. Then  $(hg^{-1}) \cdot g = h$ .
- (2) The action of  $S_n$  on the set  $\{1, \dots, n\}$  is transitive.
- (3) The action of  $D_n$  on the vertices of the  $n$ -gon is transitive.
- (4) If  $G$  is any group, the trivial action of  $G$  on the one-element set is transitive.
- (5) The action of  $\mathbb{Z}$  on  $\mathbb{Z}/n\mathbb{Z}$  by  $a + [b] = [a + b]$  is transitive, since if  $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$  are arbitrary then  $[a] = (a - b) + [b]$ .
- (6) More generally, if  $G$  is any group and  $H$  is any subgroup of  $G$ , the action of  $G$  on the left cosets of  $H$  is transitive.

Some examples of non-transitive group actions:

- (1) The action of  $GL_2(\mathbb{R})$  on  $\mathbb{R}^2$  is not transitive. There is no matrix  $M \in GL_2(\mathbb{R})$  such that

$$M \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

- (2) The actions of  $(\mathbb{R}, +)$  on the plane by rotations is not transitive. Given  $v_1, v_2 \in \mathbb{R}^2$ , there is a  $\theta \in \mathbb{R}$  such that  $v_1 = \theta \cdot v_2$  if and only if  $v_1$  and  $v_2$  have the same length.

- (3) Let  $S_3$  act on the set  $\{1, 2, 3\} \times \{1, 2, 3\}$  by  $\sigma \cdot (a, b) = (\sigma(a), \sigma(b))$ . This action is not transitive; for example, there is no  $\sigma$  such that  $(1, 2) = \sigma \cdot (1, 1)$  since  $\sigma \cdot (1, 1)$  must have equal first and second coordinates.
- (4) Let  $X$  be any set with 2 or more elements, let  $G$  be any group, and let  $G$  act on  $X$  trivially by  $g \cdot x = x$  for all  $x \in X$ . Then this is not a transitive action.

**Solution 2.2.3** (Solution to Part (3)). Part (3) is false. A counterexample is given by the usual action of  $S_3$  on  $\{1, 2, 3\}$ . This is a faithful, transitive action, but  $\{1, 2, 3\}$  has 3 elements whereas  $S_3$  has 6.

The right condition to ask is that the action of  $G$  on  $X$  be *free*: this means that for all  $x \in X$  and for all  $g, h \in G$ , if  $g \cdot x = h \cdot x$  then  $g = h$ . A bijection from  $G$  to  $X$  is then given by choosing any element  $x \in X$  and defining a function  $f : G \rightarrow X$  by  $f(g) = g \cdot x$ .

**Problem 2.3** (Permutation Representations). Let  $G$  be a group and let  $X$  be a  $G$ -set. For each  $g \in G$ , define the function  $\lambda_g : X \rightarrow X$  by  $\lambda_g(x) = g \cdot x$ . Do the following:

- (1) Show that  $\lambda_g$  is a bijection, i.e.  $\lambda_g \in S_X$ .
- (2) Show that the function  $\lambda : G \rightarrow S_X$  defined by  $\lambda(g) = \lambda_g$  is a homomorphism.
- (3) Show that the function  $\lambda$  defined in part (2) is injective if and only if the action of  $G$  on  $X$  is faithful.
- (4) Deduce Cayley's Theorem from parts (2) and (3) applied to the left regular representation of  $G$ .

**Solution 2.3.1** (Solution to Part (1)). We first show that  $\lambda_g$  is injective. Let  $x, y \in X$  be arbitrary, and suppose that  $\lambda_g(x) = \lambda_g(y)$ . Then  $g \cdot x = g \cdot y$ . Hence

$$x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) = (g^{-1}g) \cdot y = y,$$

thus  $\lambda_g$  is injective.

Now I claim that  $\lambda_g$  is surjective. Let  $x \in X$  be arbitrary. Then  $g^{-1} \cdot x \in X$ , and we have

$$\lambda_g(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = e \cdot x = x.$$

Thus  $\lambda_g$  is surjective, hence bijective.

**Solution 2.3.2** (Solution to Part (2)). Let  $g, h \in G$  be arbitrary. We want to show that  $\lambda(gh) = \lambda(g)\lambda(h)$ , i.e.  $\lambda_{gh} = \lambda_g \circ \lambda_h$ . Let  $x \in X$  be arbitrary. We have

$$\lambda_{gh}(x) = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot \lambda_h(x) = \lambda_g(\lambda_h(x)) = (\lambda_g \circ \lambda_h)(x),$$

as desired.

**Solution 2.3.3** (Solution to Part (3)). Suppose that the action of  $G$  on  $X$  is faithful, i.e. if  $g \cdot x = x$  for all  $x \in X$  then  $g = e$ . Suppose that  $g \in \ker(\lambda)$ . Then by definition,  $\lambda_g = \lambda(g) = \text{id}$ , i.e.  $\lambda_g(x) = x$  for all  $x \in X$ . But this says  $g \cdot x = x$  for all  $x \in X$ . Since the action of  $G$  on  $X$  is faithful, we have  $g = e$ . Hence  $\ker(\lambda) = \{e\}$ . Since  $\lambda$  is a homomorphism, this shows that  $\lambda$  is injective.

Suppose on the other hand that  $\lambda$  is injective, and suppose that  $g \cdot x = x$  for all  $x \in X$ . Then  $\lambda_g(x) = x$  for all  $x \in X$ , hence  $\lambda(g) = \lambda_g = \text{id} = \lambda_e = \lambda(e)$ . Since  $\lambda$  is injective, we conclude  $g = e$ . Thus the action of  $G$  on  $X$  is faithful.

**Solution 2.3.4.** Let  $G$  act on itself by the left regular representation. As discussed in the solution to the previous problem, the action of  $G$  on itself is faithful, hence  $\lambda : G \rightarrow S_G$  is an injective homomorphism. By the first isomorphism theorem,  $G \cong \lambda(G) \leq S_G$ , hence  $G$  is isomorphic to a subgroup of  $S_G$ . (Note: this is the *same* proof we originally gave of Cayley's theorem, but rephrased in a more sophisticated manner. Later on, if you learn a little category theory, you'll see even more general versions of this proof that cover some other algebraic structures as well).

**Problem 2.4.** How many different ways can the vertices of a hexagon be colored with the three colors red, green, and blue, up to *rotation* of the hexagon? What about if we allow all symmetries in  $D_6$ ? Give an example of two colorings of the hexagon which are not equivalent in the first case, but are equivalent in the second case.

**Solution 2.4.1.** Number the vertices of the hexagon counter-clockwise from 1 through 6, and let  $r$  be the usual rotation in  $D_6$ , i.e.  $r = (123456)$  as an element of  $S_6$ . The powers of  $r$  are all of the rotations of the hexagon; these are:

$$\text{id}, (123456), (135)(246), (14)(25)(36), (153)(264), (165432).$$

By Burnside's theorem, plus our theorem about counting the number of fixed points, we have that the number of orbits of the action of the rotations on the set of colorings of the hexagon is

$$\frac{1}{6}(3^6 + 3^1 + 3^2 + 3^3 + 3^2 + 3^1) = 130.$$

Glad we didn't have to count those by hand!

Now, suppose we throw in all of the remaining elements of  $D_6$ . These are the 6 reflections:

$$(12)(36)(45), (14)(23)(56), (16)(25)(34), (26)(35), (13)(46), (15)(24).$$

So our expression for Burnside's theorem becomes:

$$\frac{1}{12}(3^6 + 3^1 + 3^2 + 3^3 + 3^2 + 3^1 + 3^3 + 3^3 + 3^3 + 3^4 + 3^4 + 3^4) = 92.$$

An example of two colorings that aren't equivalent via a rotation but are equivalent via a reflection:

$$(1, 2, 3, 4, 5, 6) = (R, G, B, B, B, B) \text{ vs. } (G, R, B, B, B, B).$$

### 3. RINGS

**Problem 3.1** (The Group of Units). Let  $R$  be a ring with unity. Show that the set of all elements in  $R$  which have a multiplicative inverse forms a group under multiplication, called the group of units of  $R$ . We denote this group by  $R^\times$ . What is  $M_2^\times$ ? What is  $\mathbb{Z}^\times$ ?

**Solution 3.1.1.** The operation in  $R^\times$  is given by multiplication as elements of  $R$ . This is an associative operation since multiplication in  $R$  is assumed to be associative. We first check that  $R^\times$  is closed under this operation. Let  $a, b \in R^\times$  be arbitrary. Then  $a$  and  $b$  have multiplicative inverses  $a^{-1}$  and  $b^{-1}$  in  $R$ . We have:

$$(b^{-1}a^{-1})(ab) = b^{-1}1b = 1 = a1a^{-1} = (ab)(b^{-1}a^{-1}),$$

so  $ab$  has multiplicative inverse  $b^{-1}a^{-1}$ , hence in particular  $ab \in R^\times$ .

Since  $1 \in R$  is its own multiplicative inverse,  $1 \in R^\times$ . Let  $a \in R^\times$  be arbitrary. Then since  $aa^{-1} = a^{-1}a = 1$ , we have that  $a^{-1}$  has multiplicative inverse  $a$ , so  $a^{-1} \in R^\times$  also, and clearly  $a^{-1}$  is the inverse of  $a$  for multiplication. Thus  $R^\times$  is a group.

$M_2(\mathbb{R})^\times$  consists of those  $2 \times 2$ -real matrices which have a multiplicative inverse, i.e. this is  $GL_2(\mathbb{R})$ .

The only elements of  $\mathbb{Z}$  which have a multiplicative inverse are 1 and  $-1$ , so  $\mathbb{Z}^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$ .

**Problem 3.2.** Do Judson, Ch. 14, Exercise 4.

**Solution 3.2.1.** (a) By the lattice isomorphism theorem, the ideals of  $\mathbb{Z}/18\mathbb{Z}$  are in one-to-one correspondence with ideals of  $\mathbb{Z}$  which contain  $18\mathbb{Z}$ . All ideals of  $\mathbb{Z}$  are of the form  $n\mathbb{Z}$  for some  $n \in \mathbb{N}$  (or 0), and  $18\mathbb{Z} \subseteq n\mathbb{Z}$  if and only if  $n \mid 18$ , i.e.  $n = 1, 2, 3, 6, 9, 18$ . The correspondence of the lattice isomorphism theorem takes  $n\mathbb{Z}$  to  $n\mathbb{Z}/18\mathbb{Z}$ , so  $\mathbb{Z}/18\mathbb{Z}$  has ideals:

$$(0) = 18\mathbb{Z}/18\mathbb{Z}, (9) = 9\mathbb{Z}/18\mathbb{Z}, (6) = 6\mathbb{Z}/18\mathbb{Z},$$

$$(3) = 3\mathbb{Z}/18\mathbb{Z}, (2) = 2\mathbb{Z}/18\mathbb{Z}, \text{ and } (1) = \mathbb{Z}/18\mathbb{Z}.$$

By the third isomorphism theorem,

$$\frac{\mathbb{Z}/18\mathbb{Z}}{n\mathbb{Z}/18\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z},$$

so  $n\mathbb{Z}/18\mathbb{Z}$  is prime in  $\mathbb{Z}/18\mathbb{Z}$  if and only if  $\mathbb{Z}/n\mathbb{Z}$  is an integral domain, i.e. if and only if  $n$  is prime. Likewise  $n\mathbb{Z}/18\mathbb{Z}$  is maximal in  $\mathbb{Z}/18\mathbb{Z}$  if and only if  $\mathbb{Z}/n\mathbb{Z}$  is a field, which again occurs if and only if  $n$  is prime. So the prime

ideals and maximal ideals of  $\mathbb{Z}/18\mathbb{Z}$  are the same, and they are (3) and (2).

(b) The same argument as in part (a) shows that the ideals of  $\mathbb{Z}/25\mathbb{Z}$  are

$$(0) = 25\mathbb{Z}/25\mathbb{Z}, (5) = 5\mathbb{Z}/25\mathbb{Z}, \text{ and } (1) = \mathbb{Z}/25\mathbb{Z},$$

and (5) is both prime and maximal, while the others are neither.

(c) Let  $J$  be an ideal of  $M_2(\mathbb{R})$ . Suppose that  $A \in J$  is a nonzero element, say

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

By multiplying  $A$  on the left or right by

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

we can swap the rows or columns of  $A$  and obtain a new element of  $J$ . By doing this, we can assume  $a$  is nonzero. Then  $J$  contains

$$\begin{pmatrix} 1/a & 0 \\ 0 & 1/a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Again, using the “swapping rows and columns” trick, we can also obtain the element

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

and so  $J$  contains

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = I,$$

where  $I$  is the identity matrix. Hence  $J$  contains  $B = BI$  for all  $B \in M_2(\mathbb{R})$ . Hence the only ideals of  $M_2(\mathbb{R})$  are (0) and  $M_2(\mathbb{R})$  itself. The whole ring  $M_2(\mathbb{R})$  is not a prime or maximal ideal by definition. The ideal (0) is maximal, but not prime (this only can happen because  $M_2(\mathbb{R})$  is not a commutative ring!). To see that (0) is not prime, note that

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

(d) Suppose  $J$  is an ideal of  $M_2(\mathbb{Z})$ . Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be an element of  $J$ . Then  $J$  contains

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

and likewise  $J$  contains

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

and similarly

$$\begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix} \in J.$$

I claim now that the set of entries of matrices in  $J$  is a subgroup of  $\mathbb{Z}$ . Clearly 0 is an entry of the zero matrix, which is in  $J$ . And if  $a$  and  $b$  are entries of some matrices in  $J$ , the above shows that

$$\begin{pmatrix} a-b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in J,$$

so  $a - b \in J$ .

So, let  $n\mathbb{Z} \subseteq \mathbb{Z}$  be the subgroup of  $\mathbb{Z}$  consisting of all entries of matrices in  $J$ . Then I claim that  $J$  is the set  $nM_2(\mathbb{Z})$  of all matrices of the form

$$\begin{pmatrix} na & nb \\ nc & nd \end{pmatrix}$$

with  $a, b, c, d \in \mathbb{Z}$ . Certainly  $J$  is a subset of  $nM_2(\mathbb{Z})$  by the definition of  $n$ . On the other hand, if  $na, nb, nc, nd \in n\mathbb{Z}$  are arbitrary, then these elements are entries of some four matrices in  $J$ , hence by the above argument (plus the swapping rows and columns trick),  $J$  contains the elements

$$\begin{pmatrix} na & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & nb \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ nc & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & nd \end{pmatrix}.$$

Thus  $J$  also contains the sum of these elements, and hence contains  $nM_2(\mathbb{Z})$ .

So, all ideals of  $M_2(\mathbb{Z})$  are either 0 or of the form  $nM_2(\mathbb{Z})$  for some  $n \in \mathbb{N}$ . It's easy to see that  $nM_2(\mathbb{Z}) \subseteq mM_2(\mathbb{Z})$  if and only if  $m|n$ , so the maximal ideals of  $M_2(\mathbb{Z})$  are exactly  $pM_2(\mathbb{Z})$  for  $p \in \mathbb{N}$  prime. On the other hand,  $M_2(\mathbb{Z})$  has no prime ideals; the whole ring is by definition not a prime ideal. For any  $n \geq 2$ , we have

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin nM_2(\mathbb{Z}).$$

But the product of these two elements is  $0 \in nM_2(\mathbb{Z})$ . So  $nM_2(\mathbb{Z})$  is not prime. And (0) is not prime for the same reason.

(e) Since  $\mathbb{Q}$  is a field, its only ideals are (0) and  $(1) = \mathbb{Q}$ . The ideal (0) is both prime and maximal since  $\mathbb{Q}/(0) \cong \mathbb{Q}$  is a field.