Homework 9 Solutions

Enrique Treviño

April 15, 2016

1 Chapter 14

Problem 1. (**Exercise 2**)
Compute all X_g and all G_x for each of the following permutation groups.

(a) $X = \{1, 2, 3\}$,
$G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$

(b) $X = \{1, 2, 3, 4, 5, 6\}$,
$G = \{(1), (12), (345), (354), (12)(345), (12)(354)\}$

Solution 1. To turn in.

Problem 2. (**Exercise 3**)
Compute the G-equivalence classes of X for each of the G-sets in the previous Exercise. For each $x \in X$ verify that $|G| = |\mathcal{O}_x| \cdot |G_x|$.

Solution 2. To turn in.

Problem 3. (**Exercise 4**)
Let G be the additive group of real numbers. Let the action of $\theta \in G$ on the real plane $\mathbb{R}^2$ be given by rotating the plane counterclockwise about the origin through θ radians. Let P be a point on the plane other than the origin.

(a) Show that $\mathbb{R}^2$ is a G-set.

(b) Describe geometrically the orbit containing P.

(c) Find the group G_P.

Solution 3. To turn in.

Problem 4. (**Exercise 5**)
Let $G = A_4$ and suppose that G acts on itself by conjugation; that is, $(g, h) \mapsto ghg^{-1}$.

(a) Determine the conjugacy classes (orbits) of each element of G.

(b) Determine all of the isotropy subgroups for each element of G.

Solution 4. To turn in.

Problem 5. (**Exercise 6**)
Find the conjugacy classes and the class equation for each of the following groups.

(a) S_4

(b) D_5

(c) $\mathbb{Z}_9$

(d) Q_8

Solution 5.

(a)

$$S_4 = \{(1), (12), (13), (14), (23), (24), (34), (123), (132), (124), (142), (134), (143), (234), (243),$$
$$(12)(34), (13)(24), (14)(23), (1234), (1243), (1324), (1342), (1423), (1432)\}.$$

$$Z(S_4) = \{(1)\}.$$

We know that if $\sigma \in S_4$, then $\sigma(12)\sigma^{-1} = (\sigma(1), \sigma(2))$, so that makes it easier to calculate the conjugacy class of (12). For example

$$(1342)(12)(1342)^{-1} = ((1342)(1), (1342)(2)) = (31) = (13).$$

The orbit of (12) is

$$O_{(12)} = \{(12), (23), (24), (13), (14), (34)\}.$$

It turned out to be all transpositions. The orbit of (123) is

$$O_{(123)} = \{(123), (132), (124), (142), (134), (143), (234), (243)\}.$$

The orbit of (12)(34) is

$$O_{(12)(34)} = \{(12)(34), (13)(24), (14)(23)\}.$$

There is one more conjugacy class:

$$O_{(1234)} = \{(1234), (1243), (1324), (1342), (1423), (1432)\}.$$

The conjugacy classes break out in cycle types.

$$|S_4| = 24, \quad |Z(G)| = 1, \quad |O_{(12)}| = 6, \quad |O_{(123)}| = 8, \quad |O_{(12)(34)}| = 3, \quad |O_{(1234)} = 6|,$$

so

$$24 = 1 + 6 + 8 + 3 + 6.$$

(b) To turn in.

(c) To turn in.

(d)

$$Q_8 = \{1, i, j, k, -1, -i, -j, -k\},$$

where $i^2 = j^2 = k^2 = ijk = -1$. Let's use the Cayley table to help us find the conjugacy classes:

$\times$	1	i	j	k	$-i$	$-j$	$-k$	-1
1	1	i	j	k	-1	$-j$	$-k$	-1
i	i	-1	k	$-j$	1	$-k$	j	$-i$
j	j	$-k$	-1	i	k	1	$-i$	$-j$
k	k	j	$-i$	-1	$-j$	i	1	$-k$
$-i$	$-i$	1	$-k$	j	-1	k	$-j$	i
$-j$	$-j$	k	1	$-i$	$-k$	-1	i	j
$-k$	$-k$	$-j$	i	1	j	$-i$	-1	k
-1	-1	$-i$	$-j$	$-k$	i	j	k	1

Since the first row equals the first column $1 \in Z(Q_8)$. Since the last row equals the last column, then $-1 \in Z(Q_8)$. Every other row is not equal to its corresponding column, so the center contains just 1 and -1. Therefore

$$Z(Q_8) = \{1, -1\}.$$

Now let's find the conjugacy class containing i. Let's compute an example: $jij^{-1} = -jij = -jk = -i$, so $-i$ is in the conjugacy class of i. If we compute xix^{-1} for all $x \in Q_8$, we get the following set:

$$O_i = \{i, -i\}.$$

Since i, j, k are symmetric, then

$$O_j = \{j, -j\}$$
$$O_k = \{k, -k\}.$$

So the conjugacy classes are $\{i, -i\}, \{j, -j\}, \{k, -k\}$ and the center is $\{1, -1\}$. The class equation looks like

$$8 = 2 + 2 + 2 + 2.$$

Problem 6. (**Exercise 20**)
A group acts **faithfully** on a G-set X if the identity is the only element of G that leaves every element of X fixed. Show that G acts faithfully on X if and only if no two distinct elements of G have the same action on each element of X.

Solution 6. Let

$$G_X = \{g \in G \,|\, g \cdot x = x \; \forall x \in X\}.$$

A group action from G to X is faithful when $G_X = \{1\}$.

Let's begin by proving the ($\Rightarrow$) direction: Suppose G acts faithfully on X. Then $G_X = \{1\}$. Now for the sake of contradiction suppose there are two distinct elements $g_1, g_2 \in G$ such that they have the same action on each element of X. Then $g_1 \cdot x = g_2 \cdot x$ for all $x \in X$. Hence, for all $x \in X$:

$$g_2^{-1} \cdot (g_1 \cdot x) = g_2^{-1} \cdot (g_2 \cdot x)$$
$$(g_2^{-1} g_1) \cdot x = x.$$

Therefore $g_2^{-1} g_1 \in G_X$. But since $G_X = \{1\}$, then $g_2^{-1} g_1 = 1$, so $g_1 = g_2$. But g_1 and g_2 are distinct. We have a contradiction! Therefore there are no two distinct elements of G having the same action on each element of X.

Now let's prove the ($\Leftarrow$) direction: Suppose that there are no two distinct elements of G having the same action on each element of X. Now suppose for the sake of contradiction that G does not act faithfully. Therefore there is an element $g \in G$ such that $g \in G_X$ and $1 \neq g$ (since G does not act faithfully on X). But then 1 and g have the same action on each element of x since $g \cdot x = x = 1 \cdot x$ for all $x \in X$. This is a contradiction! Therefore G acts faithfully on X.

Problem 7. (**Exercise 25**)
If G is a group of order p^n, where p is prime and $n \geq 2$, show that G must have a proper subgroup of order p. If $n \geq 3$, is it true that G will have a proper subgroup of order p^2?

Solution 7. Let $g \neq 1$ be an element of G. Then $|g| \neq 1$ and $|g| \,|\, p^n$. Therefore $|g| = p^k$ for some positive integer k. Now, let $h = g^{p^{k-1}}$. Then the order of h is

$$|h| = |g^{p^{k-1}}| = \frac{|g|}{\gcd(|g|, p^{k-1})} = \frac{p^k}{\gcd(p^k, p^{k-1})} = \frac{p^k}{p^{k-1}} = p.$$

Therefore $\langle h \rangle$ is a subgroup of G with order p (and it is proper since it's not the whole group).

Now if G is a group of order p^n with $n \geq 3$, then if there is any element g of order p^k with $k \geq 2$, there exists an element with order p^2 (by doing a similar construction as above, but this time letting $h = g^{p^{k-2}}$). This subgroup would also be proper since the order of the group is at least p^3. So the only way that G could avoid a subgroup of order p^2 is if every non-identity element of G has order p. Let's consider this scenario where we have every element in G with order p. The center of G has p^t elements with $t \geq 1$ by the class equation. Therefore there exists an nonidentity $h \in Z(G)$. Now let $k \notin \langle h \rangle$. Since h and k have order p and $k \notin \langle h \rangle$, then $\langle h \rangle \cap \langle k \rangle = \{1\}$. Since h commmutes with everything, then if $h^a \in \langle h \rangle$ and $k^b \in \langle k \rangle$, then

$$h^a k^b = h^{a-1}(hk^b) = h^{a-1}k^b h = h^{a-2}k^b h^2 = \ldots = k^b h^a.$$

Therefore all the elements of $\langle h \rangle$ commute with all the elements of $\langle k \rangle$. Therefore $\langle h \rangle \langle k \rangle$ is a subgroup of G and it has order p^2. So if $Z(G) = \langle h \rangle$, then G has a subgroup of order p^2.

Therefore there is a proper subgroup of order p^2 in any group of order p^n with $n \geq 3$.

2 Chapter 16

Problem 8. (**Exercise 1**)
Which of the following sets are rings with respect to the usual operations of addition and multiplication? If the set is a ring, is it also a field?

(a) $7\mathbb{Z}$

(b) $\mathbb{Z}_{18}$

(c) $\mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

(d) $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$

(e) $\mathbb{Z}[\sqrt{3}\,] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$

(f) $R = \{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\}$

(g) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\}$

(h) $\mathbb{Q}(\sqrt[3]{3}\,) = \{a + b\sqrt[3]{3} + c\sqrt[3]{9} : a, b, c \in \mathbb{Q}\}$

Solution 8.

(a) $7\mathbb{Z}$ is a ring but not a field (it does not have inverses).

(b) To turn in.

(c) To turn in.

(d) $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$ is a ring and a field.

(e) To turn in.

(f) To turn in.

(g) To turn in.

(h) $\mathbb{Q}(\sqrt[3]{3}\,) = \{a + b\sqrt[3]{3} + c\sqrt[3]{9} : a, b, c \in \mathbb{Q}\}$ is a field. Once one adds $\sqrt[3]{9}$ to the mix, it works out.

Problem 9. (**Exercise 3**)
List or characterize all of the units in each of the following rings.

(a) $\mathbb{Z}_{10}$

(b) $\mathbb{Z}_{12}$

(c) $\mathbb{Z}_7$

(d) $\mathbb{M}_2(\mathbb{Z})$, the 2×2 matrices with entries in $\mathbb{Z}$

(e) $\mathbb{M}_2(\mathbb{Z}_2)$, the 2×2 matrices with entries in $\mathbb{Z}_2$

Solution 9.

(a) To turn in.

(b) To turn in.

(c) The units are the numbers relatively prime to 7, so 1, 2, 3, 4, 5 and 6.

(d) We want to find 2×2 matrices A with integer entries that have an inverse with integer entries. Let A be the following matrix:

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

where a, b, c, d are integers such that $ad - bc = 0$ (otherwise A does not have an inverse). Then

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

For A^{-1} to be an integer we need $\dfrac{a}{ad - bc}, \dfrac{b}{ad - bc}, \dfrac{c}{ad - bc}$, and $\dfrac{d}{ad - bc}$ to be integers. Therefore $ad - bc$ divides each of the terms. Suppose $ad - bc = n$. Now since $n | a, b, c, d$, we can write $a = a'n, b = b'n, c = c'n, d = d'n$ for some integers a', b', c' and d'. Then $ad - bc = n^2(a'd' - b'c')$. But $ad - bc = n$, so then

$$a'd' - b'c' = \frac{1}{n}.$$

Since $a'd' - b'c' \in \mathbb{Z}$, then $n = 1$ or $n = -1$. If $n = 1$ or $n = -1$, then clearly A^{-1} has integer entries. So the units are the matrices with integer entries that have determinant 1 or determinant -1.

(e) Using the same analysis as above, the units are those with determinant 1 or -1. There are only 16 possible matrices in $M_2(\mathbb{Z})$ because each entry is a 0 or a 1. Among these entries, the determinant is always -1, 0 or 1. Therefore the units are all matrices that have non-zero determinant. Since there are only 16, it is easy to find them all. Let A be

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

with $0 \leq a, b, c, d \leq 1$ all integers. Then $ad = 0$ or $ad = 1$. If $ad = 0$, the determinant is non-zero only when $b = c = 1$. So we have 3 cases:

(Case 1) $a = 1, b = 1, c = 1, d = 0$,

(Case 2) $a = 0, b = 1, c = 1, d = 1$, and

(Case 3) $a = 0, b = 1, c = 1, d = 0$.

If $ad = 1$, then $a = 1$ and $d = 1$. Then there are two ways $bc = 0$ (for the determinant to be non-zero):

(Case 4) $a = 1, b = 0, c = 1, d = 1$,

(Case 5) $a = 1, b = 1, c = 0, d = 1$, and

(Case 6) $a = 1, b = 0, c = 0, d = 1$.

So there are 6 unit matrices in $M_2(\mathbb{Z})$:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Problem 10. (**Exercise 11**)
Prove that the Gaussian integers, $\mathbb{Z}[i]$, are an integral domain.

Solution 10. Let's assume we already know that the Gaussian integers are a ring and let's prove that they are an integral domain. Suppose $x, y \in \mathbb{Z}[i]$ such that $xy = 0$. Let $x = a + bi$ and $y = x + di$. Then

$$0 = xy = (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Therefore

$$ac - bd = 0,$$

and

$$ad + bc = 0.$$

If $c = 0$, then $bd = 0$ and $ad = 0$. If $d = 0$, then $c + di = 0 + 0i = 0$, so $y = 0$ (and hence one of x and y is 0). If $d \neq 0$, then since $bd = 0$, $b = 0$; and because $ad = 0$, $a = 0$. Therefore $a + bi = 0 + 0i = 0$, so $x = 0$. Therefore if $c = 0$, one of x and y is zero.

Now let's take care of the case $c \neq 0$. Then $a = \dfrac{bd}{c}$ and so $\dfrac{bd^2}{c} = -bd$, implying $bd^2 = -bc^2$. If $b \neq 0$, then $d^2 = -c^2$. But $d^2 \geq 0$ and $c^2 \geq 0$. The only way $d^2 = -c^2$ is if $d = c = 0$, in which case $y = 0$. Since $c \neq 0$, then $b = 0$. But then

$$a = \frac{bd}{c} = \frac{0}{c} = 0,$$

so $x = a + bi = 0 + 0i = 0$.

In all cases, we have that either $x = 0$ or $y = 0$ and hence $\mathbb{Z}[i]$ is an integral domain.

Problem 11. (**Exercise 12**)
Prove that $\mathbb{Z}[\sqrt{3}\,i] = \{a + b\sqrt{3}\,i : a, b \in \mathbb{Z}\}$ is an integral domain.

Solution 11. To turn in.

Problem 12. (**Exercise 17**)
Let a be any element in a ring R with identity. Show that $(-1)a = -a$.

Solution 12. By distributivity $(1+(-1))a = a+(-1)a$. But $(1+(-1))a = 0a = 0$. Therefore $a+(-1)a = 0$. Therefore $(-1)a$ is the additive inverse of a and hence $(-1)a = -a$.

Problem 13. (**Exercise 30**)
Let R be a ring with identity 1_R and S a subring of R with identity 1_S. Prove or disprove that $1_R = 1_S$.

Solution 13. The identities need not be the same. For example let $R = \mathbb{Z}_6$ and let $S = \{0, 3\}$. Addition in S is commutative and associative because they are commutative and associative in R. Multiplication is associative for the same reason and the two operations satisfy the distributive properties for the same reason. $\{0\} \in S$. If $r, s \in S$, then $r + s \in S, rs \in S$, and $r - s \in S$ (there are only 4 combinations of r and s since each element is either 0 or 3). So S seems to be a subring of R, all it needs to be a subring is to have a multiplicative identity. But $3 \times 0 = 0$ and $3 \times 3 = 3$ (modulo 6), therefore 3 is the multiplicative identity of S. But 1 is the multiplicative identity of R. So they need not be the same.