Solutions for Homework Assignment 1

Solution for Problem 2:

(a) G is not a group because an identity element does not exist.

(b) G is a group. The easiest way to explain this is to point out that the given multiplication table is precisely the multiplication table for the group

$$U(\mathbb{Z}_8) \;=\; \{\; [1]_8,\;\; [3]_8,\;\; [5]_8,\;\; [7]_8 \;\}$$

discussed in class one day. Recall that $U(\mathbb{Z}_8)$ is the group of units in the ring $\mathbb{Z}_8$. We can take

$$a = [1]_8, \quad b = [3]_8, \quad c = [5]_8, \quad d = [7]_8$$

to make the comparison.

(c) G is a group. The easiest way to explain this is to point out that the given multiplication table is precisely the multiplication table for the group $\{1, -1, i, -i\}$ described in class. This group is the group of units in the ring $\mathbb{Z}[i]$ of Gaussian integers. To compare the multiplication tables, take $a = 1,\ c = -1,\ b = i$, and $d = -i$.

(d) G is not a group. One can see this by noticing that a would be the identity element, but d has no inverse.

Solution for Problem 6:

The elements of $U(\mathbb{Z}_{12})$ are of the form $[a]_{12}$, where $0 \leq a \leq 11$ and $gcd(a, 12) = 1$. Explicitly,

$$U(\mathbb{Z}_{12}) \;=\; \{\; [1]_{12},\;\; [5]_{12},\;\; [7]_{12},\;\; [11]_{12} \;\} \;\; .$$

Thus, $U(\mathbb{Z}_{12})$ is a group with 4 elements. For brevity, we will write

$$e = [1]_{12}, \qquad u = [5]_{12}, \qquad v = [7]_{12}, \qquad w = [11]_{12} \;\; .$$

The multiplication table is the following:

$\cdot$	e	u	v	w
e	e	u	v	w
u	u	e	w	v
v	v	w	e	u
w	w	v	u	e

Solution for Problem 7:

As a guide to doing this problem, it is useful to notice that

$$(1+a)(1+b) \;=\; 1+a+b+ab \;=\; 1+a*b \tag{1}$$

Also, note that if $a \neq -1$, then $1+a \neq 0$.

If $a \neq -1$ and $b \neq -1$, then $1+a \neq 0$ and $1+b \neq 0$. It follows that $(1+a)(1+b) \neq 0$. Hence $1+a*b \neq 0$. Therefore, $a*b \neq -1$. This argument shows that the set $S = \{a \in \mathbb{R} | a \neq -1\}$ is indeed closed under the operation $*$.

The identity element in S for $*$ is 0. To verify this, note that for all $a \in \mathbb{R}$, we have

$$0*a \;=\; 0+a+0\cdot a \;=\; a \qquad \textit{and} \qquad a*0 \;=\; a+0+a\cdot 0 \;=\; a \;\;.$$

As for the associative law, we use the above identity (1) and the fact that the associative law of multiplication is valid for $\mathbb{R}$. For $a, b, c \in \mathbb{R}$, we have

$$\big((1+a)(1+b)\big)(1+c) \;=\; \big(1+a*b\big)(1+c) \;=\; 1+(a*b)*c$$

and

$$(1+a)\big((1+b)(1+c)\big) \;=\; (1+a)\big(1+b*c\big) \;=\; 1+a*(b*c) \;\;.$$

Since we know that $\big((1+a)(1+b)\big)(1+c) = (1+a)\big((1+b)(1+c)\big)$ for all $a, b, c \in \mathbb{R}$, it follows that

$$(a*b)*c \;=\; a*(b*c)$$

for all $a, b, c \in \mathbb{R}$.

Finally, we prove the existence of inverses. Suppose $a \in S$. Note that $1+a \neq 0$. Hence $\dfrac{1}{1+a}$ exists in $\mathbb{R}$ and is nonzero. Let $b = \dfrac{1}{1+a} - 1$. Then $b \in \mathbb{R}$ and $b \neq -1$. That is, $b \in S$. We have

$$(1+a)(1+b) \;=\; (1+a)\left(\frac{1}{1+a}\right) \;=1 \;=\; 1+0 \;\;.$$

Using the identity (1), it follows that $a*b = 0$. Recall that the identity element in S is 0. One similarly sees that $b*a = 0$. Therefore, every element $a \in S$ indeed has an inverse $b \in S$.

We have verified that S is a group under the operation $*$.

Solution for Problem 8:

One can almost just take two randomly chosen 2×2 matrices for A and B. It is extremely likely $AB \neq BA$. Let us take

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \textit{and} \qquad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad .$$

Then one finds that

$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \qquad \textit{and} \qquad BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \quad .$$

Clearly, $AB \neq BA$.

Solution for Problem 10:

Let G be the set of matrices of the form stated in this problem. We assume that the entries x, y, and z are in $\mathbb{R}$, although this is not specified in the problem. Note that the matrices in G have determinant equal to 1. Thus, G is a subset of $GL_3(\mathbb{R})$ (and even a subset of $SL_3(\mathbb{R})$).

We will prove that G is a group by verifying that G is a subgroup of $GL_3(\mathbb{R})$. First of all, note that the identity element of $GL_3(\mathbb{R})$, namely the identity matrix I_3, is clearly in G. (Just take $x = y = z = 0$.)

Secondly, we must show that G is closed under the group operation for $GL_3(\mathbb{R})$, which is just matrix multiplication. This is clear from the formula for the product given in the problem.

Finally, we must verify that if $A \in G$, then its inverse in $GL_3(\mathbb{R})$ is also in G. However, we have the following formula for the inverse:

$$A = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}, \qquad A^{-1} = \begin{pmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix}$$

One can check easily that the second matrix is the inverse of A. It is clear that we indeed have $A^{-1} \in G$.

These observations suffice to show that G is a subgroup of $GL_3(\mathbb{R})$ and therefore is a group.

Solution for Problem 15:

The statement is false. The group S_3 has order 6 and is nonabelian. Using the notation from class, let

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \textit{and} \qquad b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Then

$$ab = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \textit{and} \qquad ba = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

and so $ab \neq ba$. This shows that S_3 is nonabelian.

Solution for Problem 25:

Suppose that $a, b \in G$, where G is a group. Let e denote the identity element of G. We want to consider

$$ab^n a^{-1} \;=\; (aba^{-1})^n \tag{2}$$

For brevity, we will let $c = aba^{-1}$ in this proof. Thus, (2) is equivalent to $ab^n a^{-1} = c^n$.

The statement (2) is true if $n = 0$ because $b^0 = e,\ ab^0 a^{-1} = aea^{-1} = e$ and $c^0 = e$.

Let us write down the inverses of both sides in (2). Recall the general fact that if $x, y, z \in G$, then $(xyz)^{-1} = z^{-1}y^{-1}x^{-1}$. Thus,

$$\left(ab^n a^{-1}\right)^{-1} \;=\; (a^{-1})^{-1}(b^n)^{-1}a^{-1} \;=\; ab^{-n}a^{-1}$$

is the inverse of the left hand side in (2). The inverse of the right hand side is $(c^n)^{-1} = c^{-n}$. If the two sides of (2) are equal, then their inverses will also be equal and so we will have

$$ab^{-n}a^{-1} \;=\; c^{-n} \;=\; (aba^{-1})^{-n}$$

which is precisely (2) with n replaced by $-n$. Thus, it is sufficient to prove (2) for all positive integers n. It will then be true for all negative integers n.

We now assume that $n \geq 1$. We will use a mathematical induction argument to prove (2). If $n = 1$, then $ab^1a^{-1} = aba^{-1} = c$ and $c^1 = c$. Both sides in (2) are indeed equal.

For the induction step, assume that the equation in (2) is true for $n = k$, where k is a positive integer. That is, we assume that

$$ab^k a^{-1} \;=\; c^k \quad .$$

Then

$$c^{k+1} \;=\; c^k c \;=\; (ab^k a^{-1})(aba^{-1}) \;=\; ab^k a^{-1} aba^{-1} \;=\; ab^k eba^{-1} \;=\; ab^k ba^{-1} = ab^{k+1}a^{-1} \quad .$$

Hence we have

$$ab^{k+1}a^{-1} \;=\; c^{k+1}$$

which means that (2) is true when $n = k + 1$.

By Mathematical Induction, we can conclude that (2) is true for all positive integers n. We also have verified (2) for $n = 0$. As we stated before, it then follows for all negative integers n.

Solution for Problem 26:

Consider the element $k = -1 + n\mathbb{Z}$. Since $gcd(-1, n) = 1$, we do have $k \in U(n)$. Furthermore,

$$k^2 \;=\; kk \;=\; (-1 + n\mathbb{Z})(-1 + n\mathbb{Z}) \;=\; 1 + n\mathbb{Z}$$

which is the identity element in $U(n)$.

Finally, note that $-1 + n\mathbb{Z} = 1 + n\mathbb{Z}$ implies that $-1 \equiv 1 \pmod{n}$. However, this congruence is only true if n divides 2. Since it is assumed that $n > 2$, it is clear that $-1 + n\mathbb{Z} \neq 1 + n\mathbb{Z}$.

Thus, k^2 is the identity element in $U(n)$, but k^1 is not the identity element. This means that k has order 2.

Solution for Problem 31:

Suppose that G is a group. Let e be the identity element in G. We will assume that $x^2 = e$ for all $x \in G$. Suppose that $a, b \in G$. We will apply the assumption to the elements $x = a,\ x = b$, and $x = ab$ in G. Thus, we have $a^2 = e,\ b^2 = e$, and $(ab)^2 = e$. That is, we have $aa = e,\quad bb = e$, and $(ab)(ab) = e$. These equations imply that

$$a(ba)b = (ab)(ab) = e \qquad \textit{and} \qquad a(ab)b = (aa)(bb) = ee = e$$

and hence we have

$$a(ba)b = a(ab)b \quad .$$

We can use the left cancellation law to conclude that $(ba)b = (ab)b$. We can then use the right cancellation law to conclude that $ba = ab$.

Thus, we have proved that $ab = ba$ for all $a, b \in G$. This proves that G is indeed an abelian group.

Solution for Problem 40:

The notation $SL_2(\mathbb{R})$ refers to the subgroup of $GL_2(\mathbb{R})$ consisting of matrices which have determinant equal to 1.

We will use the notation $R(\theta) = \begin{pmatrix} cos\ \theta & -sin\ \theta \\ sin\ \theta & cos\ \theta \end{pmatrix}$. With this notation,

$$G \ = \ \{ \ R(\theta) \ \big| \ \theta \in \mathbb{R} \ \} \quad .$$

Notice that the determinant of the matrix $R(\theta)$ is given by

$$(cos\ \theta)^2 - \big(- (sin\ \theta)^2 \big) \ = \ (cos\ \theta)^2 + (sin\ \theta)^2 \ = \ 1$$

and hence $R(\theta) \in SL_2(\mathbb{R})$ for all $\theta \in \mathbb{R}$. That is, G is a subset of $SL_2(\mathbb{R})$.

Note that $R(0) == \begin{pmatrix} cos\ 0 & -sin\ 0 \\ sin\ 0 & cos\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, which is the identity element in $SL_2(\mathbb{R})$.

Suppose $\theta, \ \psi \in \mathbb{R}$. Then we have

$$\begin{aligned} R(\theta)R(\psi) \ &= \ \begin{pmatrix} cos\ \theta & -sin\ \theta \\ sin\ \theta & cos\ \theta \end{pmatrix} \begin{pmatrix} cos\ \psi & -sin\ \psi \\ sin\ \psi & cos\ \psi \end{pmatrix} \\ &= \ \begin{pmatrix} (cos\ \theta)(cos\ \psi) - (sin\ \theta)(sin\ \psi) & -(cos\ \theta)(sin\ \psi) - (sin\ \theta)(cos\ \psi) \\ (sin\ \theta)(cos\ \psi) + (cos\ \theta)(sin\ \psi) & -(sin\ \theta)(sin\ \psi) + (cos\ \theta)(cos\ \psi) \end{pmatrix} \\ &= \ \begin{pmatrix} cos\ (\theta + \psi) & -sin\ (\theta + \psi) \\ sin\ (\theta + \psi) & cos\ (\theta + \psi) \end{pmatrix} \ = \ R(\theta + \psi) \quad . \end{aligned}$$

Thus, we have shown that $R(\theta)R(\psi)$ is in G for all $\theta, \ \psi \in \mathbb{R}$. Therefore, G is closed under the group operation for $SL_2(\mathbb{R})$.

Finally, notice that for all $\theta \in \mathbb{R}$, we have

$$R(\theta)R(-\theta) \;=\; R(\theta + (-\theta)) \;=\; R(0) \;=\; \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

which is the identity element in $SL_2(\mathbb{R})$. Therefore, the inverse of the matrix $R(\theta)$ is $R(-\theta)$ and is therefore an element of G.

We have verified that G is indeed a subgroup of $SL_2(\mathbb{R})$.

Solution for Problem 44:

Using the notation from class, the subgroups of Q_8 are as follows:

$$\{1\}, \qquad \{1,\ -1\}, \qquad \{1,\ -1,\ i,\ -i\},$$

$$\{1,\ -1,\ j,\ -j\}, \qquad \{1,\ -1,\ k,\ -k\}, \qquad Q_8$$

One checks easily that all of the above subsets of Q_8 are indeed subgroups. The above list is complete. We illustrate how to verify that by considering an arbitrary subgroup H of Q_8. Assume that H is not one of the first two subgroups in the above list.

To illustrate, suppose that the subgroup H contains i, then H must also contain $i^2 = -1$ and $i^3 = -i$. Thus, H must contain $\{1,\ -1,\ i,\ -i\}$. If $H = \{1,\ -1,\ i,\ -i\}$, then H is in the above list. Otherwise, H must contain at least one more element. Suppose that H also contains k. Then H must contain $\{k1,\ k(-1),\ ki,\ k(-i)\}$. Thus, H also contains $\{1,\ -1,\ i,\ -i\} \cup \{k, -k, -j, j\} = Q_8$. Therefore, $H = Q_8$, and is therefore in the above list.

Similarly, if we assume that H contains $-k, j$, or $-j$, then we find that $H = Q_8$.

This type of argument shows that if H is any subgroup of Q_8, then H is one of the six subgroups listed above.

Solution for Problem 45:

Let H and K be subgroups of a group G. We will prove that $H \cap K$ is a subgroup of G.

Let e be the identity element of G. Since H and K are subgroups of G, we certainly have $e \in H$ and $e \in K$. Therefore, we have $e \in H \cap K$.

Suppose that $a, b \in H \cap K$. Then $a, b \in H$. Since H is a subgroup of G, it follows that $ab \in H$. We also have $a, b \in K$. Since K is a subgroup of G, it follows that $ab \in K$. Hence $ab \in H$ and $ab \in K$. Therefore, $ab \in H \cap K$. We have shown that $H \cap K$ is closed under the group operation for G.

Finally, suppose that $a \in H \cap K$. Since $a \in H$ and H is a subgroup of G, it follows that $a^{-1} \in H$. Since $a \in K$ and K is a subgroup of G, it follows that $a^{-1} \in K$. Thus, $a^{-1} \in H$ and $a^{-1} \in K$. Therefore, $a^{-1} \in H \cap K$. We have shown that if $a \in H \cap K$, then $a^{-1} \in H \cap K$.

We have shown that $H \cap K$ is a subgroup of G.