Solutions for Assignment 2

Solutions for Problem 46 from section 3.4.

The statement is false. We will give two counterexamples to the statement in this problem.

Suppose that G is the quaternion group Q_8. Let $H = \{1, -1, i, -i\}$ and let $K = \{1, -1, j, -j\}$. Both are subgroups of G. Then

$$H \cup K \;=\; \{1, -1, i, -i, j, -j\}$$

But this set is not closed under the group operation for G. For example, we have

$$i,\; j \in H \cup K, \qquad but \qquad ij = k \notin H \cup K \;\; .$$

As a second counterexample, let $G = \mathbb{Z}$, which is a group under the operation $+$. Let $H = 5\mathbb{Z}$ and $K = 7\mathbb{Z}$. Both H and K are subgroups of G. But $H \cup K$ is not a subgroup of G. It is not closed under the group operation for G. For example, $5 \in H \cup K$ and $7 \in H \cup K$, but $5 + 7 = 12$ and $12 \notin H \cup K$.

Solution for Problem 48 from section 3.4.

Let G be a group. Consider the following subset of G:

$$Z(G) \;=\; \{\; z \in G \;\big|\; zg = gz \; for\ all \; g \in G \;\} \;\; .$$

We will prove that $Z(G)$ is actually a subgroup of G.

Let e be the identity element of G. By definition, we have $eg = g$ and $ge = g$ for all $g \in G$. It follows that $eg = ge$ for all $g \in G$. Hence $e \in Z(G)$.

Suppose that $a, b \in Z(G)$. Let g be any element of G. Then we have

$$ag \;=\; ga \qquad and \qquad bg \;=\; gb \;\; .$$

It follows that

$$(ab)g \;=\; a(bg) \;=\; a(gb) \;=\; (ag)b \;=\; (ga)b \;=\; g(ab)$$

and hence we have $(ab)g = g(ab)$. This is true for all $g \in G$. Therefore, we have proved that if $a, b \in Z(G)$, then $ab \in Z(G)$.

Finally, suppose that $a \in Z(G)$. Let g be any element of G. We have $ag = ga$. Also, implicitly using the associative law repeatedly

$$ag = ga \implies a^{-1}ag = a^{-1}ga \implies eg = a^{-1}ga \implies g = a^{-1}ga$$

$$\implies ga^{-1} = a^{-1}gaa^{-1} \implies ga^{-1} = a^{-1}ge \implies ga^{-1} = a^{-1}g \quad .$$

This is true for all $g \in G$. Therefore, if $a \in Z(G)$, then $a^{-1} \in Z(G)$.

We have shown that $Z(G)$ is indeed a subgroup of G.

Solution for Problem 53 from section 3.4.

The argument is very similar to the argument presented in the solution to problem 48. In fact, we can take H to be any subset of G. Define

$$C(H) \;=\; \{\; x \in G \;\big|\; xh = hx \; for \; all \; h \in H \;\} \quad .$$

Since $eh = h = he$ for all $h \in H$, it follows that $e \in C(H)$.

Suppose $a, b \in C(H)$. Let h be any element of H. Then $ah = ha$ and $bh = hb$. As in the solution to problem 47, it follows that $(ab)h = h(ab)$. This is true for all $h \in H$. Hence $ab \in C(H)$.

Suppose $a \in C(H)$. Let h be any element of H. Then $ah = ha$. As before, it follows that $a^{-1}h = ha^{-1}$. This is true for all $h \in H$. Hence $a^{-1} \in C(H)$.

We have shown that $C(H)$ is indeed a subgroup of G.

Solution for Problem 1b,c,d from section 4.4.

(b) In fact, $U(8)$ is not cyclic. To see this, note that

$$U(8) \;=\; \{\; 1 + 8\mathbb{Z}, \quad 3 + 8\mathbb{Z}, \quad 5 + 8\mathbb{Z}, \quad 7 + 8\mathbb{Z} \;\} \quad .$$

Furthermore, the identity element is $1 + 8\mathbb{Z}$. We have

$$(1 + 8\mathbb{Z})^1 = 1 + 8\mathbb{Z}, \qquad (3 + 8\mathbb{Z})^2 = 9 + 8\mathbb{Z} = 1 + 8\mathbb{Z},$$

$$(5 + 8\mathbb{Z})^2 = 25 + 8\mathbb{Z} = 1 + 8\mathbb{Z}, \qquad (7 + 8\mathbb{Z})^2 = 49 + 8\mathbb{Z} = 1 + 8\mathbb{Z} \quad .$$

The group $U(8)$ has order 4, but the elements in $U(8)$ have order 1 or 2. It follows that $U(8)$ is not a cyclic group.

(c) The group $\mathbb{Q}$ is the group of rational numbers under the operation of addition. We will show that $\mathbb{Q}$ is not a cyclic group.

Suppose that $r \in \mathbb{Q}$. Let $H = \langle r \rangle$. If $r = 0$, then $H = \langle r \rangle = \{0\}$ which is a proper subset of $\mathbb{Q}$. Hence $H \neq \mathbb{Q}$ in that case.

Now suppose that $r \neq 0$. We can write $r = \dfrac{m}{n}$, where $m, n \in \mathbb{Z}$. Both m and n are fixed, nonzero integers. Suppose that $h \in H = \langle r \rangle$. By definition, it follows that $h = kr = \dfrac{km}{n}$, where $k \in \mathbb{Z}$. Consequently, we have $nh = km \in \mathbb{Z}$. Thus, for some fixed nonzero integer n, we have $nh \in \mathbb{Z}$ for all $h \in H$.

Consider $s = \dfrac{1}{2n}$. Then $s \in \mathbb{Q}$. However, notice that $ns = \dfrac{1}{2} \notin \mathbb{Z}$. Using the observation in the previous paragraph, it follows that $s \notin H$. Therefore, $H \neq \mathbb{Q}$.

We have proved that every cyclic subgroup of $\mathbb{Q}$ is a proper subgroup of $\mathbb{Q}$. Therefore, $\mathbb{Q}$ is not a cyclic group.

(d) This statement is false. The quaternion group Q_8 is a counterexample. As found in homework assignment 1, there are six distinct subgroups of Q_8. The five proper subgroups of Q_8 are:

$$\{1\} = \langle 1 \rangle, \qquad \{1, \ -1\} = \langle -1 \rangle, \qquad \{1, \ -1, \ i, \ -i\} = \langle i \rangle,$$

$$\{1, \ -1, \ j, \ -j\} = \langle j \rangle, \qquad \{1, \ -1, \ k, \ -k\} = \langle k \rangle$$

They are all indeed cyclic. But Q_8 is not cyclic because none of the elements in Q_8 has order equal to 8. Those elements all have order 1, 2, or 4.

Solution for Problem 4a from section 4.4.

The identity element in the group $GL_2(\mathbb{R})$ is $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. We find that

$$A^1 = A \neq I_2, \qquad A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2 \neq I_2,$$

$$A^3 = A^2 A = -I_2 A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq I_2, \qquad A^4 = A^2 A^2 = (-I_2)(-I_2) = I_2$$

It follows that A has order 4 and that

$$\langle A \rangle = \left\{ I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Solution to problem 31 from section 4.4.

Let e be the identity element in the group G. An element a in G has finite order if and only if there exists a positive integer k such that $a^k = e$. Let T denote the set of elements of G which have finite order.

Notice that $e^1 = e$ and hence e has finite order. Therefore, $e \in T$.

Suppose that $a \in T$. Then a positive integer k exists such that $a^k = e$. By the law of exponents, we have

$$\left(a^{-1}\right)^k \;=\; a^{-k} \;=\; \left(a^k\right)^{-1} \;=\; e^{-1} \;=\; e$$

and therefore we have $a^{-1} \in T$.

So far, we have not assumed that G is abelian. But for the next step, we will need that assumption.

Suppose that G is abelian and that $a,\ b \in G$. Then we will first show that if k is any positive integer, then

$$(ab)^k \;=\; a^k b^k \quad . \tag{1}$$

We will use Mathematical Induction. Obviously, (1) is true for $k = 1$. Assume it is true for $k = n$, where $n \in \mathbb{N}$. We then have

$$(ab)^{n+1} \;=\; (ab)^n(ab) \;=\; (a^n b^n)(ab) \;=\; a^n(b^n a)b \;=\; a^n(ab^n)b \;=\; (a^n a)(b^n b) \;=\; a^{n+1}b^{n+1}$$

and hence (1) is true for $k = n + 1$. By Mathematical Induction, it follows that (1) is true for all $k \in \mathbb{N}$.

Now suppose that $a, b \in T$. Then there exist positive integers s and t such that $a^s = e$ and $b^t = e$. Let $k = st$. Then k is a positive integer and we have

$$a^k \;=\; a^{st} \;=\; (a^s)^t \;=\; e^t \;=\; e \qquad \textit{and} \qquad b^k \;=\; b^{st} \;=\; (b^t)^s \;=\; e^s \;=\; e \quad .$$

Using (1), it follows that

$$(ab)^k \;=\; a^k b^k \;=\; ee \;=\; e \quad .$$

It follows that $ab \in T$. We have proved that if $a, b \in T$, then $ab \in T$.

The above observations show that if G is abelian, then T is indeed a subgroup of G.

Solution for Problem A.

First of all, note that $i^4 = 1$. Hence the order of i must divide 4. The positive divisors of 4 are $1,\ 2,$ and 4. But $i^2 = -1 \neq 1$. Thus, the order of i cannot divide 2. The only possibility left is that the order of i is equal to 4.

Let $\beta = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$. Note that

$$\beta^2 \ = \ \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) \ = \ \left(\frac{1}{2} - \frac{1}{2}\right) + \left(\frac{1}{2} + \frac{1}{2}\right)i \ = \ i \quad .$$

Therefore,

$$\beta^8 = (\beta^2)^4 = i^4 = 1$$

Therefore, the order of β must divide 8. Thus, the order of β is $1,\ 2,\ 4,$ or 8. But

$$\beta^4 = (\beta^2)^2 = i^2 = -1$$

and so $\beta^4 \neq 1$. Therefore, the order of β cannot divide 4. The only possibility is that the order of β is exactly 8.

Let $\gamma = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. Then

$$\gamma^2 = \left(\frac{1}{4} - \frac{3}{4}\right) + \left(\frac{\sqrt{3}}{4} + \frac{\sqrt{3}}{4}\right)i \ = \ -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

and

$$\gamma^3 = \gamma^2\gamma = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \left(-\frac{1}{4} - \frac{3}{4}\right) + \left(-\frac{\sqrt{3}}{4} + \frac{\sqrt{3}}{4}\right)i = -1 \quad .$$

It follows that

$$\gamma^6 = (\gamma^3)^2 = (-1)^2 = 1$$

and hence the order of γ must divide 6. Thus the order of γ is $1,\ 2,\ 3,$ or 6. However, neither γ^2 nor γ^3 is equal to 1. Thus, the order of γ cannot divide 2 or 3. This leaves just one possibility. The order of γ must be 6.

Finally, we consider $\delta = 1 + i$. Note that $\delta^2 = (1+i)(1+i) = -2i$ and

$$\delta^4 = (\delta^2)^2 = (-2i)^2 = -4 \qquad \textit{and} \qquad \delta^8 = (\delta^4)^2 = (-4)^2 = 16.$$

Thus, $16 \in \langle\delta\rangle$. Thus, $\langle 16\rangle$ is a subgroup of $\langle\delta\rangle$. It is clear that $16^k = 1$ holds if and only if $k = 0$. Thus, 16 has infinite order. Thus, $\langle 16\rangle$ is an infinite group. It is a subgroup of $\langle\delta\rangle$ and hence that group must also be infinite. Therefore, δ has infinite order.

Solution for Problem B.

$|G| = 4$: The solution for problem 1b above gives us an example. Take $G = U(8)$. It has order 4 and is noncyclic as explained above.

$|G| = 6$: Let $G = S_3$. The $|G| = 6$. As discussed in class, there is one element in G of order 1, three elements of order 2, and two elements of order 3. There are no elements of order 6. Hence G is not cyclic.

One can also point out that $G = S_3$ is a nonabelian group. However, every cyclic group is abelian. Hence G cannot be cyclic.

$|G| = 8$. We can take $G = Q_8$. Since Q_8 is nonabelian, it cannot be cyclic.

Before finishing this problem, we make the following helpful observation. Suppose that A and B are groups. Let e be the identity element of A and let f be the identity element of B. Suppose that m and n are positive integers with the following property: $a^m = e$ for all $a \in A$ and $b^n = f$ for all $b \in B$. Let $G = A \times B$, which is the direct product of A and B defined in class one day. Then G is a group and the identity element of G is (e, f). Notice that for any element $(a, b) \in G$, we have

$$(a,b)^{mn} \;=\; (a^{mn}, b^{mn}) \;=\; \big((a^m)^n,\ (b^n)^m\big) \;=\; 9e^n, f^m) = (e, f)$$

and hence every element $g \in G$ satisfies $g^{mn} = (e, f)$

Now we continue the solution to this problem. We will use the notation in the above observation.

$|G| = 12$. Let $G = A \times B$, where A is cyclic of order 3 and $B = U(\mathbb{Z}_8)$. Note that B has order 4, but every element in B has order 1 or 2. Thus, we have $a^3 = e$ for all $a \in A$ and $b^2 = f$ for all $b \in B$. We can take $m = 3$ and $n = 2$ in the notation of the observation. Thus, if $g \in G$, then $g^6 = (e, f)$. Thus, every element of G has order dividing 6. However, $|G| = |A||B| = 12$. Since G has no element of order 12, it cannot be a cyclic group.

$|G| = 49$. Now we take A and B to be cyclic groups of order 7. Let $G = A \times B$. Then every element of A has order 1 or 7. Every element of B has order 1 or 7. Thus, if $a \in A$ and $b \in B$, then $a^7 = e$ and $b^7 = f$. Thus,

$$(a,b)^7 \;=\; (a^7, b^7) \;=\; (e, f)$$

which is the identity element in G. Hence every element in G has order dividing 7. However, $|G| = |A||B| = 7 \cdot 7 = 49$. This group G is not cyclic because G has no element of order 49.

$|G| = 64$. One could take $G = A \times B$ where A and B are cyclic groups of order 8. Then just as in the previous case, every element of G has order dividing 8. But $|G| = 64$. The group G cannot be cyclic because it has no element of order 64.

Another example is $G = Q_8 \times Q_8$. It is a nonabelian group of order $8 \cdot 8 = 64$ and hence cannot be cyclic.

Solution for Problem C.

We are assuming that $a, b \in G$ and that $ab = ba$. Let e be the identity element of G. We are also assuming that

$$a^2 = e, \quad b^3 = e \qquad \textit{and} \qquad a \neq e, \quad b \neq e, \qquad b^2 \neq e \ .$$

To prove that ab has order 6, let $c = ab$ and let m denote the order of c. Since $ab = ba$, we have

$$c^6 \ = \ (ab)(ab)(ab)(ab)(ab)(ab) \ = \ a^6 b^6 \ = \ (a^2)^3 (b^3)^2 \ = \ e^3 e^2 \ = \ e$$

Suppose $k \in \mathbb{Z}$. According to a result proved in class, $c^k = e$ if and only if m divides k. It follows that m divides 6. This means that $m \in \{1, \ 2, \ 3, \ 6\}$. However,

$$c^3 \ = \ a^3 b^3 \ = \ a^3 e \ = \ a^3 \ = \ aa^2 \ = \ ae \ = \ a \ \neq \ e, \qquad c^2 \ = \ a^2 b^2 \ = \ eb^2 \ = \ b^2 \ \neq \ e$$

and therefore m doesn't divide 3 or 2. Thus, $m \notin \{1, \ 2, \ 3\}$. It follows that $m = 6$, as stated in the problem.

Solution for Problem D.

The statement is false. Consider the group $G = S_3$. Let

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

Then a has order 2 and b has order 3. However,

$$ab \ = \ = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \ = \ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

which has order 2. Thus, ab has order 2, and not 6.