Solutions For Homework 3

Ch. 2

2. Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. What is the identity element of this group? Can you see any relationship between this group and $U(8)$?

Answer. We need to follow the definition of a group given on page 43:

Notation. Let us denote the operation given in the question, multiplication modulo 40, with $\cdot$ and the usual multiplication of integers a and b with ab or $(a)(b)$. So, we have

$$a \cdot b \quad = \quad ab \mod 40$$

Step 1. *Check that the operation defined in the question is a binary operation:*

	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

Calculations above show that the operation defined in the question assigns to each ordered pair of elements of $\{5, 15, 25, 35\}$ an element in $\{5, 15, 25, 35\}$. Therefore, it is a binary operation.

Step 2. *Check associativity of the given operation:*

Since we have $a(bc) = a(bc)$ for every a,b,c in Z, we get $a(bc) = (ab)c$ for every a, b, c in $\{5, 15, 25, 35\}$. Clearly, $a(bc) = (ab)c$ implies that

$$a(bc) \mod 40 \quad = \quad (ab)c \mod 40.$$

So, we get

$$\begin{aligned}
a \cdot (b \cdot c) &= a(b \cdot c) \mod 40 && \text{(def. of } \cdot) \\
&= [(a \mod 40)((b \cdot c) \mod 40)] \mod 40 && \text{(pr. of mod)} \\
&= [(a \mod 40)((bc \mod 40) \mod 40)] \mod 40 && \text{(def. of } \cdot) \\
&= [(a \mod 40)(bc \mod 40)] \mod 40 && \text{(pr. of mod)} \\
&= a(bc) \mod 40 && \text{(pr. of mod)} \\
&= (ab)c \mod 40 && \text{(assoc. of Z)} \\
&= [((ab) \mod 40)(c \mod 40)] \mod 40 && \text{(pr. of mod)} \\
&= [((ab) \mod 40) \mod 40)(c \mod 40)] \mod 40 && \text{(pr. of mod)} \\
&= [((a \cdot b) \mod 40)(c \mod 40)] \mod 40 && \text{(def. of } \cdot) \\
&= (a \cdot b)c \mod 40 && \text{(pr. of mod)} \\
&= (a \cdot b) \cdot c && \text{(def. of } \cdot).
\end{aligned}$$

So, the operation given in the question is associative.

Step 3. *Check the existence of identity:*

If we look at the Cayley table above, we see that $25 \cdot a = a \cdot 25 = a$ for all a in $\{5, 15, 25, 35\}$. So 25 is the identity.

Step 4. *Check the existence of inverses:*

The Cayley table also shows that for each element a in $\{5, 15, 25, 35\}$, there is an element b in $\{5, 15, 25, 35\}$ such that $a \cdot b = b \cdot a = e$. More explicitly, we see that

$$\begin{aligned} 5 \cdot 5 &= 5 \cdot 5 &&= 25 \\ 15 \cdot 15 &= 15 \cdot 15 &&= 25 \\ 25 \cdot 25 &= 25 \cdot 25 &&= 25 \\ 35 \cdot 35 &= 35 \cdot 35 &&= 25. \end{aligned}$$

Conclusion. Since the set $\{5, 15, 25, 35\}$ with multiplication modulo 40 satisfies all requirements given in the definition of a group, $\{5, 15, 25, 35\}$ is a group under the multiplication modulo 40.

In Step 4, we see that inverse of every element in $\{5, 15, 25, 35\}$ is itself. Since we have

$$\begin{aligned} (1)(1) \mod 8 &= 1 \\ (3)(3) \mod 8 &= 1 \\ (5)(5) \mod 8 &= 1 \\ (7)(7) \mod 8 &= 1 \end{aligned}$$

inverse of every element in $U(8)$ is also itself. This is one relationship between $\{5, 15, 25, 35\}$ and $U(8)$. In fact, if you consider all of the numbers mod 8 in the Cayley table for $\{5, 15, 25, 35\}$ you get the Cayley table for $U(8)$ (with the rows and columns in different orders). Later we will see that this means the two groups are *isomorphic*.

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

16. In a group, prove that $(ab)^{-1} = b^{-1}a^{-1}$. Find an example that shows that it is possible to have $(ab)^{-2} \neq b^{-2}a^{-2}$. Find distinct nonidentity elements a and b from a non-Abelian group with the property that $(ab)^{-1} = a^{-1}b^{-1}$. Draw an analogy between the statement $(ab)^{-1} = b^{-1}a^{-1}$ and the act of putting on and taking off your sock and shoes.

Answer. Let us start with first part. We show that $(ab)^{-1}$ is $b^{-1}a^{-1}$ by showing

that the second expression satisfies the definition of an inverse.

$$\begin{array}{rcll}(ab)(b^{-1}a^{-1}) & = & a(bb^{-1})a^{-1} & \text{associativity}\\ & = & aea^{-1} & \text{inverses}\\ & = & aa^{-1} & \text{identity}\\ & = & e & \text{inverses}\end{array}$$

For the second part, let us consider D_4. Let us use the notation given in the page 32. Let $a = R_{90}$ and $b = D'$, then $a^{-1} = R_{270}$ and $b^{-1} = D'$. So we get

$$\begin{array}{rcl}(ab)^{-2} & = & (ab)^{-1}(ab^{-1})\\ & = & (b^{-1}a^{-1})(b^{-1}a^{-1})\\ & = & (D'R_{270})(D'R_{270})\\ & = & VV\\ & = & R_0\end{array}$$

But we have

$$\begin{array}{rcl}b^{-2}a^{-2} & = & (b^{-1}b^{-1})(a^{-1}a^{-1})\\ & = & (D'D')(R_{270}R_{270})\\ & = & R_0R_{180}\\ & = & R_{180}.\end{array}$$

So we get $(ab)^{-2} \neq b^{-2}a^{-2}$.

For the third part of the question let us consider $SL(2, R)$. Let

$$a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}, a^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, b^{-1} = \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}.$$

Then we see that

$$\begin{array}{rcl}(ab)^{-1} & = & \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}\right)^{-1}\\ & = & \left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right)^{-1}\\ & = & \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},\end{array}$$

$$\begin{array}{rcl}a^{-1}b^{-1} & = & \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right)^{-1}\left(\begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}\right)^{-1}\\ & = & \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}\\ & = & \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.\end{array}$$

So we have $(ab)^{-1} = a^{-1}b^{-1}$. (Remember though, this only happens in this particular example!)

For the last part of the problem: the order of shoes and socks depends whether you're putting them on or taking them off. (Putting on: socks then

shoes, taking off: shoes then socks.) This is similar for multiplying elements or taking their inverses.

18. Show that $(a^{-1})^{-1} = a$. By definition, $(a^{-1})^{-1}$ is the inverse of a^{-1}. That is, it is an element b such that $a^{-1}b = e = b(a^{-1})$. By Theorem 2.3 there is a unique b that has this property. Notice that $b = a$ also solves these equations by the definition of a^{-1} being the inverse of a. Thus these two solutions agree and $(a^{-1})^{-1} = a$.

Ch. 3

2. Let Q be the group of rational nubmers under addition and let Q^* be the group of nonzero rational numbers under multiplication. In Q, list the elements in $\langle \frac{1}{2} \rangle$. In Q^*, list the elements in $\langle \frac{1}{2} \rangle$.

Answer. In Q, we have

$$\begin{aligned} \langle \frac{1}{2} \rangle &= \{n(\frac{1}{2}) | n \in Z\} \\ &= \{\ldots, -\frac{5}{2}, -2, -\frac{3}{2}, -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, \ldots\}. \end{aligned}$$

In Q^*, we have

$$\begin{aligned} \langle \frac{1}{2} \rangle &= \{(\frac{1}{2})^n | n \in Z\} \\ &= \{\ldots, 32, 16, 8, 4, 2, 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32} \ldots\}. \end{aligned}$$

4. Prove that in any group, an element and its inverse have the same order.

Answer. The definition of order of an element is crucial for this question. So we repeat this definition (page 59):

Definition. The *order* of an element g in G is the **smallest positive integer** n such that $g^n = e$. (In additive notation, this would be $ng = 0$). If no such integer exists, we say that g has *infinite order*. The order of an element g is denoted by $|g|$.

Proof. There are two cases: either $|g| = \infty$ or $|g| < \infty$. If $|g| = \infty$ is the case, by the definition above there is **no** positive integer n such that $g^n = e$. Assume that $|g| \neq |g^{-1}|$. Since $|g| \neq |g^{-1}|$, $|g^{-1}|$ has to be a finite positive integer. Let us say $|g^{-1}| = m$. But note that we have

$$\begin{aligned} g^m &= \left((g^{-1})^{-1}\right)^m \\ &= \left((g^{-1})^m\right)^{-1} \\ &= e^{-1} \\ &= e. \end{aligned}$$

Namely, we get a positive integer m such that $g^m = e$. So, the assumption $|g| \neq |g^{-1}|$ gives a contradiction. Hence, if we have $|g| = \infty$, we have to have $|g| = |g^{-1}|$.

If $|g| < \infty$ is the case, let us say $|g| = n$. Note that we have

$$\begin{aligned} (g^{-1})^n &= (g^n)^{-1} \\ &= e^{-1} \\ &= e. \end{aligned}$$

So $|g^{-1}|$ is finite and less than or equal n. Let us assume that $|g^{-1}| = m < n$. If we consider the following calculation

$$\begin{aligned} g^m &= \left((g^{-1})^{-1}\right)^m \\ &= \left((g^{-1})^m\right)^{-1} \\ &= e^{-1} \\ &= e. \end{aligned}$$

we obtain a smaller integer m than n such that $g^m = e$. This is a contradiction. Hence, we get $m = n$. Namely, we have $|g| = |g^{-1}|$. This finishes the proof.

14. If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof showsthat the intersection of any number of subgroups of G, finite of infinite, is again a subgroup of G?)

Answer. Let us use two-step subgroup test (theorem 3.2, page 62). Since H is a subgroup of G, we have $e \in H$. Since K is a subgroup of G, we have $e \in K$. So we get $e \in H \cap K$. Namely, $H \cap K$ is nonempty. Let a and b be two elements in $H \cap K$. Then a and b are in H and in K. Since we know that $H \leq G$, we get $ab \in H$ and $a^{-1} \in H$. Since we also know that $K \leq G$, we have $ab \in K$ and $a^{-1} \in K$. That means $ab \in H \cap K$ and $a^{-1} \in H \cap K$. Hence, $H \cap K$ is a subgroup of G by two-step subgroup test.

The same proof with necessary generalizations shows that the intersection of any number of subgroups of G is again a subgroup of G.