Here are a few practice problems on groups. **You should first work through these WITHOUT LOOKING at the solutions!** After you write your own solution, you can compare to my solution. Your solution does not need to be identical to mine—there are often many ways to solve a problem—but it does need to be CORRECT.

1. Suppose that $G$ is a set and that $*$ is an operation on $G$ that satisfies the following conditions:

(a) $G$ is closed under $*$.
(b) $*$ is associative.
(c) There exists an element $e \in G$ such that $a * e = a$ for every $a \in G$.
(d) For each $a \in G$ there exists an element $b \in G$ such that $a * b = e$.

Show that $G$ is a group.

NOTE: We do NOT know that $G$ is a group—that is what we are trying to prove! We are given that SOME of the requirements of a group are satisfied, and we have to prove that the remaining requirements are also satisfied. We do NOT know that each element has an inverse—that is part of what we must *prove*.

Solution

Here, and in most instances involving generic group notation, I'll omit writing the symbol "$*$" explicitly.

The hypotheses of this problem tell us that *most* of the properties required for $G$ to be a group are satisfied. We just have to show that the remaining properties are also satisfied. Specifically, we have to show the following two things.

(1) $ea = a$ for every $a \in G$.
(2) For each $a \in G$, the element $b \in G$ which satisfies $ab = e$ ALSO satisfies $ba = e$.

Let us work on statement (2) first. (How did I know to do this one first? I didn't, I worked on statement (1) until I decided that I wasn't getting anywhere and then tried statement (2) instead.)

Let $a$ be any element of $G$. Then we know by assumption (c) that $ae = a$, and assumption (d) tells us that there is an element $b \in G$ that satisfies $ab = e$. Further, by assumption (d) there is an element $c$ such that $bc = e$. However, we do NOT yet know whether $c = a$! We cannot assume this! Instead, using the associativity of the operation, we compute that

$$ba = (ba)e = b(ae) = b(a(bc)) = b((ab)c) = b(ec) = (be)c = bc = e.$$

This establishes statement (2).

Now let us prove that statement (1) is true. Let $a \in G$ be given. We have to show that $ea = a$. This follows from the calculation

$$ea = (ab)a = a(ba) = ae = a. \quad \square$$

2. Suppose that $a$ is an element of order 24 in a group $G$.

(a) Find $|\langle a^6\rangle|$ (the order of $\langle a^6\rangle$).

(b) Show that $\langle a\rangle = \langle a^7\rangle$.

Solution

(a) If $n \in \mathbb{Z}$ is given, then we can write $n = 4k + r$ with $r \in \{0, 1, 2, 3\}$. Hence $(a^6)^n = a^{6n} = a^{24k+6r} = a^{6r} \in \{e, a^6, a^{12}, a^{18}\}$. This tells us that

$$\langle a^6\rangle \;=\; \big\{(a^6)^n : n \in \mathbb{Z}\big\} \;\subseteq\; \{e, a^6, a^{12}, a^{18}\}.$$

Do we have equality? Yes, because each of $e$, $a^6$, $a^{12}$, and $a^{18}$ belongs to $\langle a^6\rangle$ (why?). Therefore

$$\langle a^6\rangle \;=\; \big\{(a^6)^n : n \in \mathbb{Z}\big\} \;=\; \{e, a^6, a^{12}, a^{18}\}.$$

Can we conclude from this that the order of $\langle a^6\rangle$ is 4? IF WE KNEW that $e$, $a^6$, $a^{12}$, and $a^{18}$ were all distinct, THEN it would follow that that $\langle a^6\rangle$ has exactly 4 elements, but how do we know that $e$, $a^6$, $a^{12}$, and $a^{18}$ are all different?

Now, we know that $a$ has order 24, so this tells us that $a^j$ cannot equal $e$ for any positive $j$ less than 24. Hence $a^6$, $a^{12}$, and $a^{18}$ are not equal to $e$. But could $a^6$ equal $a^{12}$ or $a^{18}$? You still need to show that *no two* of $e$, $a^6$, $a^{12}$, or $a^{18}$ are equal. Fill in this argument! Once you have done this, you can conclude that $\langle a^6\rangle$ consists of four distinct elements, and therefore $|\langle a^6\rangle| = 4$.

(b) Now we will try to prove that $\langle a\rangle = \langle a^7\rangle$. We want to prove that these two sets are equal, so need to show that the first set is a subset of the second, and the second is a subset of the first.

Showing that $\langle a^7\rangle$ is a subset of $\langle a\rangle$ is easy, because every power of $a^7$ is a power of $a$, and therefore

$$\langle a^7\rangle \;=\; \big\{(a^7)^n : n \in \mathbb{Z}\big\} \;=\; \big\{a^{7n} : n \in \mathbb{Z}\big\} \;\subseteq\; \big\{a^n : n \in \mathbb{Z}\big\} \;=\; \langle a\rangle.$$

To prove the reverse inclusion, choose any particular power $n \in \mathbb{Z}$. After some clever computation, we realize that $7 \cdot 7 - 24 \cdot 2 = 1$, and therefore

$$a^n \;=\; a^{7\cdot 7n - 24\cdot 2n} \;=\; (a^7)^{7n}(a^{24})^{-2n} \;=\; (a^7)^{7n}(e)^{-2n} \;=\; (a^7)^{7n} \;\in\; \langle a^7\rangle.$$

Therefore every power of $a$ is a power of $a^7$, so $\langle a\rangle \subseteq \langle a^7\rangle$. □

3. Suppose that two elements $a$ and $b$ in a group $G$ commute, and suppose that $a^m = e = b^n$. Show that $(ab)^k = e$, where $k = \mathrm{lcm}(m, n)$, the least common multiple of $m$ and $n$. If $m$ and $n$ are the orders of $a$ and $b$, respectively, must $k$ be the order of $ab$?

Solution

If $k$ is the least common multiple of $m$ and $n$, then it is a multiple of both $m$ and $n$, i.e.,

$k = mr$ and $k = ns$ for some integers $r$ and $s$. Therefore, since $a$ and $b$ commute,

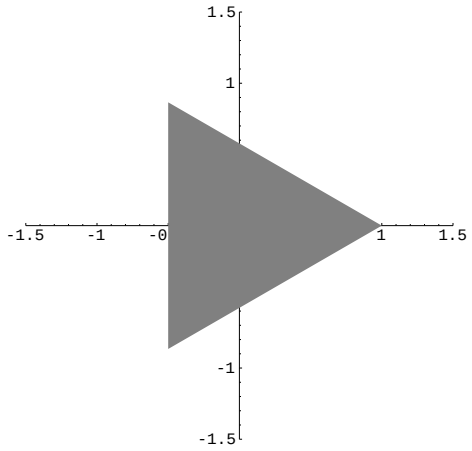
$$\begin{aligned}
(ab)^k &= (ab)(ab)\cdots(ab) \qquad \text{(repeated } k \text{ times)} \\
&= aa\cdots abb\cdots b \qquad \text{(because } a \text{ and } b \text{ commute!)} \\
&= a^k b^k \\
&= a^{mr} b^{ns} \\
&= (a^m)^r (b^n)^s \\
&= e^r e^s \\
&= e.
\end{aligned}$$

However, although we have shown that $(ab)^k = e$, we cannot conclude that $k$ is the ORDER of $ab$! That is because the order of $ab$ is defined to be the SMALLEST positive power of $ab$ which yields the identity. We know here that $(ab)^k = e$, but we don't know whether $k$ is the SMALLEST positive integer with this property. And in fact, $k$ does NOT have to be the order of $ab$. For example, if we happened to have $b = a^{-1}$ then we would have $ab = e$, so in this case the order of $ab$ would be 1, not $k$. □

3. In class we created a group that consists of those rigid motions of the plane that leave the unit square invariant (these are called the *symmetries of the square*). List the analogous symmetries of an equilateral triangle (there are six) and give the "multiplication table" for these symmetries.

Solution

Here is a picture of an equilateral triangle:



The six rigid motions that preserve this triangle are:

$$\begin{aligned} e = r_0 &\quad \text{identity, rotation by 0,} \\ r = r_{2\pi/3} &\quad \text{rotation by } 2\pi/3, \\ r^2 = r_{4\pi/3} &\quad \text{rotation by } 4\pi/3, \\ a = f_0 &\quad \text{flip around } x\text{-axis,} \\ b = f_{2\pi/3} &\quad \text{flip around axis at angle } 2\pi/3, \\ c = f_{4\pi/3} &\quad \text{flip around axis at angle } 4\pi/3. \end{aligned}$$

The multiplication table is:

| $\circ$ | $e$ | $r$ | $r^2$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $r$ | $r^2$ | $a$ | $b$ | $c$ |
| $r$ | $r$ | $r^2$ | $e$ | $c$ | $a$ | $b$ |
| $r^2$ | $r^2$ | $e$ | $r$ | $b$ | $c$ | $a$ |
| $a$ | $a$ | $b$ | $c$ | $e$ | $r$ | $r^2$ |
| $b$ | $b$ | $c$ | $a$ | $r^2$ | $e$ | $r$ |
| $c$ | $c$ | $a$ | $b$ | $r$ | $r^2$ | $e$ |

The table means that, for example, that $ra = c$ and $ar = b$. Hence this group is NOT abelian, because there are elements that do not commute with each other. □

5. Let $H$ be a subgroup of a group $G$. Show that if $g \in G$, then $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is a subgroup of $G$.

Solution

Let $H$ be a subgroup of $G$ and let $g \in G$ be a fixed element. We must show that $gHg^{-1}$ is a subgroup of $G$. To do this we must show that $gHg^{-1}$ is nonempty, closed under compositions, and closed under inverses.

The set $gHg^{-1}$ is nonempty because $e = geg^{-1} \in gHg^{-1}$.

To show that $gHg{-}1$ is closed under compositions, suppose that $x$, $y$ are any two elements of $gHg^{-1}$. By definition, this means that $x = gag^{-1}$ and $y = gbg^{-1}$ for some $a$, $b \in H$. Since $ab \in H$, we therefore have that

$$xy \;=\; gag^{-1}gbg^{-1} \;=\; g(ab)g^{-1} \;\in\; gHg^{-1}.$$

To show that $gHg^{-1}$ is closed under inverses, suppose that $x \in gHg^{-1}$. Then $x = gag^{-1}$ for some element $a \in H$. Since $a^{-1} \in H$, we therefore have that

$$x^{-1} \;=\; (gag^{-1})^{-1} \;=\; (g^{-1})^{-1}a^{-1}g^{-1} \;=\; ga^{-1}g^{-1} \;\in\; gHg^{-1}. \qquad \square$$

6. Define $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$ with an operation $*$ defined by the formula

$$m * n \;=\; mn \bmod 5,$$

where $mn$ is usual product of the integers $m$ and $n$ and the notation $k \bmod 5$ means the integer remainder left when the integer $k$ is divided by 5. Show that $\mathbb{Z}_5^\times$ is a group under this operation, and determine whether or not it is an abelian group.

Solution

a. First we show that $\mathbb{Z}_5^\times$ is closed under the given operation, i.e., $m * n \in \mathbb{Z}_5^\times$ for each $m$, $n \in \mathbb{Z}_5^\times$. This is most easily done by working out the multiplication table, which is:

| $*$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

Hence, $m * n$ is always an element of $\mathbb{Z}_5^\times$ when $m$ and $n$ are elements of $\mathbb{Z}_5^\times$. Furthermore, we have $m * n = n * m$ for every $m$ and $n$, so once we finish showing that $\mathbb{Z}_5^\times$ is a group, we will know that it IS an abelian group. Alternatively, this follows directly from the definition of the operation $*$, because:

$$m * n \;=\; mn \bmod 5 \;=\; nm \bmod 5 \;=\; n * m.$$

b. To show that $\mathbb{Z}_5^\times$ has an identity element, we examine the multiplication table above, and we see that $1 * n = n = n * 1$ for $n = 1, 2, 3, 4$.

c. To show that $\mathbb{Z}_5^\times$ is closed under inverses, we again examine the multiplication table and see that

$$1 * 1 = 1, \qquad 2 * 3 = 1, \quad 3 * 2 = 1, \quad 4 * 4 = 1.$$

Hence for each element $n \in \mathbb{Z}_5^\times$, there exists an element $n^{-1} \in \mathbb{Z}_5^\times$ such that $n * n^{-1} = 1 = n^{-1} * n$. In fact, we have:

$$1^{-1} = 1, \qquad 2^{-1} = 3, \qquad 3^{-1} = 2, \qquad 4^{-1} = 4.$$

d. Finally, we must show that the operation $*$ is associative, i.e., $k * (m * n) = (k * m) * n$ for every $k$, $m$, $n \in \mathbb{Z}_5^\times$. This is the hardest part of the whole problem. First let's prove a useful *lemma*, or "baby theorem." This will make it easier to write the proof of what we really want.

**Lemma 1.** Let $p$ and $q$ be any integers. Let $a = q \bmod 5$. Then:

$$(pq) \bmod 5 \;=\; (pa) \bmod 5.$$

That is,

$$(pq) \bmod 5 \;=\; \big(p(q \bmod 5)\big) \bmod 5. \tag{1}$$

*Proof.* By definition, $a = q \bmod 5$ means that $a$ is the remainder when $q$ is divided by 5. Hence $a$ is one of $0, 1, 2, 3, 4$, and there is an integer $j$ such that $q = 5j + a$. Therefore,

$$(pq) \bmod 5 \;=\; (p(5j + a)) \bmod 5 \;=\; (5pj + pa) \bmod 5.$$

But if we divide 5 into $5pj + pa$, we will get the same remainder as when we divide 5 into $pa$, because of the fact that 5 divides evenly into $5pj$. Therefore,

$$(pq) \bmod 5 \;=\; (5pj + pa) \bmod 5 \;=\; (pa) \bmod 5. \qquad \square$$

$\square$

Now we can return to the problem of showing that the operation $*$ is associative. We have to show that $k * (m * n) = (k * m) * n$. By the lemma and the definition of the operation $*$, we have:

| | | |
|---|---|---|
| $k * (m * n)$ | $= (k(m * n)) \bmod 5$ | by definition of $*$ |
| | $= (k(mn \bmod 5)) \bmod 5$ | by definition of $*$ |
| | $= (k(mn)) \bmod 5$ | use equation (1) with $p = k$ and $q = mn$ |
| | $= ((km)n) \bmod 5$ | since ordinary multiplication is associative |
| | $= ((km \bmod 5)n) \bmod 5$ | use equation (1) with $p = km$ and $q = n$ |
| | $= ((k * m)n) \bmod 5$ | by definition of $*$ |
| | $= (k * m) * n$ | by definition of $*$. |

This shows that the operation $*$ is associative. $\square$

7. Suppose that $G$ is a group that contains exactly 3 elements. Show that $G$ must be abelian.

Solution

Let $G$ be a group that contains exactly three elements. One of these must be the identity element, so let's call that element $e$. Let $a$, $b$ be the other two elements, so that $e$, $a$, and $b$ are the three DISTINCT elements of $G$. Since $G$ is a group, the product $ab$ must be one of the elements in the group. Hence $ab$ must equal either $e$, $a$, or $b$. If we had $ab = a = ae$, then the cancellation law would imply that $b = e$, which is a contradiction. Similarly, $ab = b$ implies $a = e$, another contradiction. Therefore we can only have $ab = e$. Similar reasoning implies $ba = e$, so $b$ is the inverse of $a$, i.e., $b = a^{-1}$. Hence, the three distinct elements of the group are $e$, $a$, and $a^{-1}$. Now, $e$ certainly commutes with both $a$ and $a^{-1}$, since $ae = a = ea$ and $a^{-1}e = a^{-1} = ea^{-1}$. And $a$ and $a^{-1}$ commute since $aa^{-1} = e = a^{-1}a$. Therefore every element of $G$ commutes with every other element of $G$, so $G$ is abelian. $\square$