20.1 The axioms for a group

20.1.1

Let $G = \mathbb{Z}$. Complete the following table, where $+$, $-$, and $\times$ represent the usual operations of arithmetic.

<table>
<thead>
<tr>
<th></th>
<th>Closure</th>
<th>Associativity</th>
<th>Identity</th>
<th>Inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>$+$</td>
<td>$\checkmark$</td>
<td></td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>$-$</td>
<td>$\checkmark$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\times$</td>
<td>$\checkmark$</td>
<td></td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
</tbody>
</table>

Solution

<table>
<thead>
<tr>
<th></th>
<th>Closure</th>
<th>Associativity</th>
<th>Identity</th>
<th>Inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>$+$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>$-$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
</tr>
</tbody>
</table>

So $G$ with the $+$ operation has all four properties, and we have a group. But the other operations do not give rise to groups.
20.1.2

Repeat Ex. 20.1.1 taking $G = \mathbb{N}$, with the same operations.

**Solution**  For $\mathbb{N}$ the situation is as follows.

<table>
<thead>
<tr>
<th></th>
<th>Closure</th>
<th>Associativity</th>
<th>Identity</th>
<th>Inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>$+$</td>
<td>$\sqrt{}$</td>
<td>$\sqrt{}$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>$-$</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>$\times$</td>
<td>$\sqrt{}$</td>
<td>$\sqrt{}$</td>
<td>$\sqrt{}$</td>
<td>$\times$</td>
</tr>
</tbody>
</table>

In this case none of the operations give rise to a group.
20.2 Examples of groups

Write down explicitly the matrices belonging to the group in Example 2 on p. 262. (There are just six of them.) Find the inverse of each one.

**Solution**   The matrices are:

\[
\begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
1 & 1 \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
1 & 2 \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
2 & 0 \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
2 & 1 \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
2 & 2 \\
0 & 1
\end{bmatrix}.
\]

Their inverses are:

\[
\begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
1 & 2 \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
1 & 1 \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
2 & 0 \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
2 & 1 \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
2 & 2 \\
0 & 1
\end{bmatrix}.
\]
20.2.2

There are eight symmetry transformations of a square. List them, and draw up the group table as in Example 1 on p. 261.

Solution  Labelling the corners $A$, $B$, $C$, $D$ in clockwise order, we have the following operations:

- $i$ identity;
- $r$ rotation through $90^\circ$ clockwise;
- $s$ rotation through $180^\circ$;
- $t$ rotation through $270^\circ$ clockwise;
- $m_1$ reflection in the axis joining the midpoints of $AB$ and $CD$;
- $m_2$ reflection in the axis joining the midpoints of $AD$ and $BC$;
- $m_3$ reflection in the axis $BD$;
- $m_4$ reflection in the axis $AC$.

The group table is as follows.

$$
\begin{array}{cccccccc}
i & i & r & s & t & m_1 & m_2 & m_3 & m_4 \\
\hline
i & i & r & s & t & m_1 & m_2 & m_3 & m_4 \\
r & r & s & t & i & m_3 & m_4 & m_2 & m_1 \\
s & s & t & i & r & m_2 & m_1 & m_4 & m_3 \\
t & t & i & r & s & m_4 & m_3 & m_1 & m_2 \\
m_1 & m_1 & m_4 & m_2 & m_3 & i & s & t & r \\
m_2 & m_2 & m_3 & m_1 & m_4 & s & i & r & t \\
m_3 & m_3 & m_1 & m_4 & m_2 & r & t & i & s \\
m_4 & m_4 & m_2 & m_3 & m_1 & t & r & s & i \\
\end{array}
$$
20.3 Basic algebra in groups

20.3.1
Show that the inverse of $ab$ is $b^{-1}a^{-1}$.

Solution  This is an application of the group laws, in particular the associative law.

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1.$$
Solutions to Chapter 20 Exercises
in Discrete Mathematics by Norman L. Biggs;
2nd Edition 2002

20.3.2
Establish the following implications, where \( x \) and \( y \) are any elements of a group:

(i) \( xy = 1 \Rightarrow yx = 1 \);

(ii) \( (xy)^2 = x^2y^2 \Rightarrow xy = yx \).

(In part (ii) \( x^2 \) stands for \( xx \).)

Solution

(i) \( xy = 1 \Rightarrow x = y^{-1} \Rightarrow yx = yy^{-1} = 1 \).

(ii) \( (xy)^2 = x^2y^2 \Rightarrow xyxy = xxyy \Rightarrow yx = xy \) (cancellation).
20.4 The order of a group element

20.4.1

Let \( \alpha \) and \( \beta \) denote the permutations of \( \mathbb{N}_7 \) whose representations in cycle notation are

\[
\alpha = (15)(27436), \quad \beta = (1372)(46)(5).
\]

Calculate the orders of \( \alpha \) and \( \beta \), considered as elements of the symmetric group \( S_7 \). What are the orders of \( \alpha \beta \) and \( \beta \alpha \)?

**Solution**  It is clear that \( \alpha^5 = (15) \), and so \( \alpha^{10} = id \). The order of \( \alpha \) is 10. Similarly, the order of \( \beta \) is 4.

We have

\[
\alpha \beta = (163425)(7), \quad \beta \alpha = (153476)(2),
\]

and it follows that the order of both \( \alpha \beta \) and \( \beta \alpha \) is 6.
20.4.2

Let $x$ and $y$ be elements of a finite group $G$. Show that the orders of $x$ and $y^{-1}xy$ are the same.

Solution

$$x^m = 1 \iff yx^m y^{-1} = 1$$
$$\iff yxy^{-1} \cdot yxy^{-1} \cdots yxy^{-1} = 1$$
$$\iff (yxy^{-1})^m = 1.$$
20.5 Isomorphism of groups

20.5.1
Describe the four symmetries of a rectangle, and construct the group table. By writing down a suitable bijection show that your group is isomorphic to the one whose group table is Table 20.5.2.

Table 20.5.2

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>1</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>1</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>a</td>
<td>1</td>
</tr>
</tbody>
</table>

Solution  Label the corners of the rectangle $A, B, C, D$ in clockwise order. The symmetries are

- $i$ identity;
- $p$ rotation through $180^\circ$;
- $q$ reflection in axis joining mid-points of $AB, CD$;
- $q$ reflection in axis joining mid-points of $BC, AD$.

The group table is

<table>
<thead>
<tr>
<th></th>
<th>i</th>
<th>p</th>
<th>q</th>
<th>r</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>i</td>
<td>p</td>
<td>q</td>
<td>r</td>
</tr>
<tr>
<td>p</td>
<td>p</td>
<td>i</td>
<td>r</td>
<td>q</td>
</tr>
<tr>
<td>q</td>
<td>q</td>
<td>r</td>
<td>i</td>
<td>p</td>
</tr>
<tr>
<td>r</td>
<td>r</td>
<td>q</td>
<td>p</td>
<td>i</td>
</tr>
</tbody>
</table>

By inspection of the tables, an isomorphism is:

\[
\begin{array}{cccc}
i & p & q & r \\
\downarrow & \downarrow & \downarrow & \downarrow \\
1 & a & b & c \\
\end{array}
\]
20.5.2

By analysing the possible group tables show that, if isomorphic groups are regarded as the same, then

(i) there is just one group of order 2;

(ii) there is just one group of order 3;

(iii) there are just two groups of order 4.

Solution

(i) There are two elements, one of which must be the identity. If the other element is \( x \neq 1 \), we must have \( x^2 = 1 \) (why?), and so the group table is as follows.

\[
\begin{array}{ccc}
1 & x & \\
x & 1 & x \\
1 & x & 1 \\
\end{array}
\]

(ii) Suppose the elements are 1, \( x \) and \( y \). The first row and column of the group table are forced by the properties of 1. The remaining four entries can only be as shown below, because of the latin square property.

\[
\begin{array}{ccc}
1 & x & y \\
x & 1 & y \\
y & x & 1 \\
\end{array}
\]

(iii) Suppose the elements are 1, \( x \), \( y \) and \( z \). Either \( x^2 = 1 \) or \( x^2 = y \) (the possibility \( x^2 = z \) is not essentially distinct, it can be obtained by renaming \( y \) and \( z \)). If \( x^2 = 1 \) there are two essentially distinct ways of completing the table, \((G_1)\) and \((G_2)\) below. If \( x^2 = y \), there is only one way, \((G_3)\).

\[
(G_1) \quad \begin{array}{cccc}
1 & x & y & z \\
x & 1 & x & y \\
y & y & z & 1 \\
z & z & y & 1 \\
\end{array}
\]

[continued]
In fact, the groups \((G_2)\) and \((G_3)\) are the same (isomorphic), using the isomorphism:

\[
\begin{array}{c|cccc}
1 & x & y & z \\
\hline
1 & x & y & z \\
x & x & 1 & z & y \\
y & y & z & x & 1 \\
z & z & y & 1 & x \\
\end{array}
\]

\[
\begin{array}{c|cccc}
1 & x & y & z \\
\hline
1 & x & y & z \\
x & x & y & z & 1 \\
y & y & z & 1 & x \\
z & 1 & x & y & \\
\end{array}
\]
20.6 Cyclic groups

20.6.1

Let \( U \) be the subset of \( \mathbb{Z}_7 \) which contains all the elements of \( \mathbb{Z}_7 \) except 0. Show that multiplication in \( \mathbb{Z}_7 \) defines a group operation for \( U \), and that \( U \approx C_6 \).

**Solution**  The fact that \( U = \{1, 2, 3, 4, 5, 6\} \) is a group can be verified by constructing the group table. It is worth noting that, since 7 is a prime, it follows from Theorem 13.3.1 that all members of \( U \) have a multiplicative inverse.

In order to show that \( U \) is a cyclic group we have to find \( x \) such that \( \langle x \rangle = U \). The element 2 is no good, since

\[
2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1.
\]

However

\[
3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1,
\]

so that

\[
U = \langle 3 \rangle = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} \approx C_6.
\]
Solutions to Chapter 20 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

20.7 Subgroups

20.7.1

Which of the following are subgroups of $G_{\triangle}$?

$$K_1 = \{i, x\}, \quad K_2 = \{i, x, y\}, \quad K_3 = \{i, r, s, x, y\}.$$  

Solution

- $K_1$: is a subgroup ($x^2 = 1$).
- $K_2$: is not a subgroup ($xy \notin K_2$).
- $K_3$: is not a subgroup ($ry \notin K_3$).
20.7.2

Use the group $G_{\triangle}$ to provide an example of the fact that if $H$ and $K$ are subgroups then $H \cup K$ need not be a subgroup.

Solution  A counter-example is provided by the subgroups of $G_{\triangle}$

$$H = \{i, x\}, \quad K = \{i, y\}.$$ 

Here $H \cup K = \{i, x, y\}$, which is not a subgroup (see Ex. 20.7.1).
20.8 Cosets and Lagrange’s theorem

20.8.1
Let $H$ be a subgroup of $G$, and define a relation $\sim$ on $G$ by the rule that $x \sim y$ means $x^{-1}y \in H$. Show that $\sim$ is an equivalence relation and its equivalence classes are the left cosets of $H$.

Solution We check the three properties of an equivalence relation.

Reflexive: $x^{-1}x = 1$, and $1 \in H$, therefore $x \sim x$.

Symmetric: Suppose $x \sim y$, that is, $x^{-1}y \in H$. Then $(x^{-1}y)^{-1} \in H$, that is, $y^{-1}x \in H$. Therefore $y \sim x$.

Transitive: Suppose $x \sim y$ and $y \sim z$. Then $x^{-1}y \in H$ and $y^{-1}z \in H$, so $(x^{-1}y)(y^{-1}z) \in H$. That is, $x^{-1}z \in H$, so $x \sim z$.

The class of $x$ is

$$\{y \in G \mid y \sim x\} = \{y \in G \mid x \sim y\}$$
$$= \{y \in G \mid x^{-1}y \in H\}$$
$$= \{y \in G \mid y \in xH\}$$
$$= xH.$$
20.8.2

Describe explicitly the partition of the triangle group by the right cosets of the subgroup $H = \{i, x\}$. Check that the partition is not the same as that given by the left cosets of $H$.

**Solution**  The right cosets are:

- $H = \{i, x\}$,
- $Hr = \{ir, xr\} = \{r, z\}$,
- $Hs = \{is, xs\} = \{s, y\}$.

The left cosets are:

- $H = \{i, x\}$,
- $rH = \{ri, rx\} = \{r, y\}$,
- $sH = \{si, sx\} = \{s, z\}$.
20.8.6

Sketch the lattice of subgroups of the symmetric group $S_4$. [Hint: you will need
a large sheet of paper.]

Solution  Here is a list of the subgroups, in order of size.

1: the identity $\{\text{id}\}$.

2: 6 subgroups containing the identity and a single transposition $(ab)$; and 3
 containing the identity and a double transposition $(ab)(cd)$.

3: 4 cyclic subgroups $\{\text{id}, (abc), (acb)\}$.

4: 3 cyclic subgroups $\{\text{id}, (abcd), (ac)(bd), (adcb)\}$.
  1 non-cyclic subgroup $\{\text{id}, (ab)(cd), (ac)(bd), (ad)(bc)\}$.

6: 4 subgroups isomorphic to $S_3$, obtained by fixing one symbol, for example
 $\{\text{id}, (ab), (ac), (bc), (abc), (acb)\}$.

8: 3 subgroups isomorphic to the symmetry group of a square.

12: 1 subgroup, the alternating group $A_4$ comprising the even permutations.
20.9 Characterization of cyclic groups

20.9.1

Sketch the lattice of subgroups of the cyclic group $C_{24}$. If $z$ is a generator of $C_{24}$, identify the subgroups generated by $z^7$, $z^8$, and $z^9$.

**Solution** As explained in the text, the lattice of subgroups is the same as the lattice of divisors of 24 (there is just one subgroup for each divisor).

Since 7 is coprime with 24, $\langle z^7 \rangle = C_{24}$. The numbers 8, 9 are not coprime with 24, and

$$\langle z^8 \rangle = \{z^8, z^{16}, 1\} = C_3;$$

$$\langle z^9 \rangle = \{z^9, z^{18}, z^3, z^{12}, z^{21}, z^6, z^{15}, 1\} = C_8.$$
20.9.2

How many elements of $C_{60}$ generate the whole group?

**Solution**  According to Theorem 20.9 the number is $\phi(60)$, and by Theorem 11.5.1 $\phi(60)$ is equal to

$$60 \left( 1 - \frac{1}{2} \right) \left( 1 - \frac{1}{3} \right) \left( 1 - \frac{1}{5} \right) = 60 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 16.$$