28. Prove that right- and left-cancellation hold for a group G. That is, prove that when $a, b, c \in G$, then $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.

Proof. Suppose $a, b, c \in G$, and $ba = ca$. Multiply both sides by a^{-1} on the right to get

$$(ba)a^{-1} = (ca)a^{-1}.$$

Using associativity, this becomes

$$\begin{aligned} b(aa^{-1}) &= c(aa^{-1}) \\ be &= ce \\ b &= c. \end{aligned}$$

Thus we have shown $ba = ca$ implies $b = c$.

Now suppose $ab = ac$. Multiply both sides by a^{-1} on the left to get

$$a^{-1}(ab) = a^{-1}(ac).$$

Next use associativity to get

$$\begin{aligned} (a^{-1}a)b &= (a^{-1}a)c \\ eb &= ec \\ b &= c. \end{aligned}$$

Thus we have shown $ab = ac$ implies $b = c$. ■

30. Prove that if G is a group of even order, then there is an element $a \in G$, with $a \neq e$, and $a^2 = e$.

Proof. (Contrapositive) Suppose that there is no element $a \in G$ for which $a \neq e$ and $a^2 = e$. Thus, for each non-identity element $a \in G$, we have $a^2 \neq e$, which is to say $aa \neq e$. This means that $a^{-1} \neq a$. Consequently any $a \in G$ (other than e) has an inverse that is unequal to a.

Thus the non-identity elements of G can be grouped in pairs a and a^{-1}. In fact, imagine listing the non-identity elements of G in a table as follows, so each column contains a particular element $a_i \in G$ and its inverse a_i^{-1}, and every element of G (other than e) appears exactly once in the table.

a_1	a_2	a_3	a_4	$\dots$	a_n
a_1^{-1}	a_2^{-1}	a_3^{-1}	a_4^{-1}	$\dots$	a_n^{-1}

It follows that G has an even number $2n$ of non-identity elements. But, in addition, G has the identity element e. Therefore G has a total of $2n+1$ elements. Consequently G has odd order. ■

31. Let G be a group and suppose $(ab)^2 = a^2b^2$ for each $a, b \in G$. Prove that G is abelian.

Proof. Suppose G is a group and $(ab)^2 = a^2b^2$ for each $a, b \in G$. Take any two elements $a, b \in G$. Then we have $(ab)(ab) = a^2b^2$, that is $abab = aabb$, which is $a(bab) = a(abb)$. Cancellation (Exercise 28 above) gives

$$bab = abb,$$

or $(ba)b = (ab)b$. Cancellation again gives $ba = ab$. We have now shown that $ba = ab$ for any $a, b \in G$. This means G is abelian. ■

32. Find all subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$. Deduce that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not the same as $\mathbb{Z}_9$.

The subgroups are as follows:
$H_1 = \{(0,0)\}$
$H_2 = \{(0,0),(1,0),(2,0)\}$
$H_3 = \{(0,0),(0,1),(0,2)\}$
$H_4 = \{(0,0),(1,1),(2,2)\}$
$H_5 = \{(0,0),(1,2),(2,1)\}$
$H_6 = \{(0,0),(1,0),(2,0),(0,1),(1,1),(2,1),(0,2),(1,2),(2,2)\}$

By contrast, $\mathbb{Z}_9$ has only three subgroups:
$H_1 = \{0\}$
$H_2 = \{0,3,6\}$
$H_3 = \{0,1,2,3,4,5,6,7,8\}$.
Therefore $\mathbb{Z}_3 \times \mathbb{Z}_3$ and $\mathbb{Z}_9$ have different structures and are not the same.

39. Prove that $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q}$ and a and b are not both $0\}$ is a subgroup of $\mathbb{R}^*$ under the group operation of multiplication.

Certainly we have $G \subseteq \mathbb{R}^*$. We will apply Proposition 3.9 to show that G is a subgroup of $\mathbb{R}^*$.

1. The identity 1 of $\mathbb{R}^*$ has form $1 = 1 + 0\sqrt{2} \in G$, so $1 \in G$.
2. Consider two elements $a + b\sqrt{2}$ and $a' + b'\sqrt{2}$ in G, so $a, b \in \mathbb{Q}$ and are not both zero, and likewise for a' and b'. Their product is $(a+b\sqrt{2})(a'+b'\sqrt{2}) = (aa'+2bb') + (ab'+ba')\sqrt{2}$, and this has the required form $x + y\sqrt{2}$, where x and y are rational. (As $x = aa' + 2bb'$ and $y = ab' + ba'$ are products and sums of rational numbers, they are themselves rational.) Moreover, $x = (aa' + 2bb')$ and $y = (ab' + ba')$ are not both zero, for otherwise the product $(a+b\sqrt{2})(a'+b'\sqrt{2}) = x + y\sqrt{2}$ of two nonzero elements of $\mathbb{R}^*$ would be zero, which is impossible. Therefore the product $(a+b\sqrt{2})(a'+b'\sqrt{2})$ is in G.
3. Consider an arbitrary element $a + b\sqrt{2}$ in G. Its inverse in $\mathbb{R}^*$ is

$$(a+b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}}\frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a}{a-2b} + \frac{-b}{a-2b}\sqrt{2} \in G$$

Observations 1–3 above combined with Proposition 3.9 prove that G is a subgroup of $\mathbb{R}^*$. ■

40. Show that $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}$ is a subgroup of the group $G = \mathbb{M}_2(\mathbb{R})$ of 2×2 matrices under matrix addition.

Certainly we have $H \subseteq G$. We will apply Proposition 3.9 to show that H is a subgroup of G.

1. The additive identity matrix $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is in H because $a + d = 0$ for this matrix.
2. Consider two matrices $H_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $H_2 = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ in H, so $a + d = 0$ and $a' + d' = 0$. Observe that $H_1 + H_2 = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$ satisfies $(a+a') + (d+d') = (a+d) + (a'+d') = 0$, so $H_1 + H_2 \in H$.
3. Consider an arbitrary element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in H, so $a + d = 0$. The inverse of this matrix is $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$, and as $(-a) + (-d) = -(a+d) = 0$, this inverse is in H.

Observations 1–3 above combined with Proposition 3.9 prove that H is a subgroup of G. ■