7. Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on $S$ by $a \circ b = a + b + ab$. Prove that $(S, \circ)$ is an abelian group.

*Proof.* First, we check that the operation is indeed an operation. This means that take $a, b \in S$ and we aim to show that $a \circ b \in S$. If per chance, $a \circ b = -1$, then

$$\begin{aligned} -1 &= a + b + ab \\ -1 - a &= b(1 + a) \end{aligned}$$

Dividing both sides by $1 + a$ yields that $b = -1$, which it is not. So $\circ$ is an operation on $S$.

Next, we show that the operation is associative.

$$\begin{aligned} (a \circ b) \circ c &= (a + b + ab) \circ c \\ &= a + b + ab + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \end{aligned}$$

$$\begin{aligned} a \circ (b \circ c) &= a \circ (b + c + bc) \\ &= a + b + c + bc + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \end{aligned}$$

A quick shows that these are equal.

Let's look for the $\circ$-inverse. We use $e$ as the candidate. So

$$a = a \circ e = a + e + ae.$$

Subtracting $a$ from both sides and factoring out an $e$ produces $0 = e(1 + a)$. Since $1 + a \neq 0$, it follows that $e = 0$. So 0 is the identity.

Now we want to look for the inverse so we solve $a \circ x = 0$. Then

$$a + x + ax = 0$$

and which produces $x = \frac{-a}{1+a}$ which never equals $-1$ and so belongs to $S$.

The operation is clearly commutative so $(S, \circ, 0)$ is an abelian group. □

22. Show that addition and multiplication mod $n$ are well defined operations. That is, show that the operations do not depend on the choice of the representative from the equivalence classes mod $n$.

*Proof.* Recall that $a \equiv b \mod n$ means that $n|b - a$. We need to assume that $a \equiv c \mod n$ and $b \equiv d \mod n$ and we want to show that both $(a + b) \equiv (c + d) \mod n$ and $ab \equiv cd \mod n$.

Now, there exists $k, j \in \mathbb{Z}$ such that $nk = c - a$ and $nj = db$. Then

$$\begin{aligned}(c+d)-(a+b) &= (c-a)+(d-b)\\ &= nk+nj\\ &= n(k+j).\end{aligned}$$

Therefore, addition is well-defined. Next,

$$\begin{aligned}(cd)-(ab) &= cd-ad+ad-ab\\ &= (c-a)d+a(d-b)\\ &= nkd+anj\\ &= n(kd+aj).\end{aligned}$$

Therefore, multiplication is well-defined.

□

25. Let $a$ and $b$ be elements in a group $G$. Prove that $ab^n a^{-1} = (aba^{-1})^n$ for all $n \in \mathbb{Z}$.

*Proof.* We prove by induction. Clearly, it's true for $n = 1$. So suppose that it is true for $n$.

$$\begin{aligned}(aba^{-1})^{n+1} &= (aba^{-1})^n(aba^{-1}) &&\\ &= (ab^n a^{-1})aba^{-1} && \text{(by induction)}\\ &= ab^n(a^{-1}a)ba^{-1} && \text{(by associativity)}\\ &= ab^n ba^{-1} && \text{(by inverses)}\\ &= ab^{n+1}a^{-1} &&\end{aligned}$$

□

It follows that it is true for all $n \in \mathbb{N}$. As for the negative integers observe that for any negative integer $n$

$$\begin{aligned}ab^n a^{-1} &= a(b^{-1})^{-n}a^{-1} &&\\ &= (ab^{-1}a^{-1})^{-n} && \text{(by induction)}\\ &= ((a^{-1})^{-1}(b^{-1})^{-1}a^{-1})^{-1})^{-n} && ((gh)^{-1} = h^{-1}g^{-1})\\ &= ((aba^{-1})^{-1})^{-n} && ((g^{-1})^{-1} = g)\\ &= (aba^{-1})^n && \text{(Laws of Exponents)}\end{aligned}$$

27. Prove that $(g_1 g_2 \dots g_n)^{-1} = g_n^{-1} \dots g_2^{-1} g_1^{-1}$.

*Proof.* We prove by induction. Clearly, it's true for any product of $n = 1$ and $n = 2$ elements: $(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$.

Next, suppose it is true for any product of $n$ elements. Then

$$\begin{aligned}(g_1g_2\dots g_ng_{n+1})^{-1} &= ([g_1g_2\dots g_n]g_{n+1})^{-1}\\ &= g_{n+1}^{-1}(g_1g_2\dots g_n)^{-1}\\ &= g_{n+1}^{-1}g_n^{-1}\dots g_2^{-1}g_1^{-1}(\text{by induction})\end{aligned}$$

□

51.If $xy = x^{-1}y^{-1}$ for all $x, y \in G$, prove that $G$ must be abelian.

*Proof.* We aim to show that for all $x, y \in G$, $xy = yx$.. First note that in the hypothesis we can substitute $y = e$ and so $x = xe = x^{-1}e^{-1} = x^{-1}$. This implies that every element is its own inverse. By Problem 31, $G$ is abelian.

Let's prove problem 31. No every element is its own inverse which means that $x = x^{-1}$ and $y = y^{-1}$ and $(xy)^{-1} = xy$. But this last equality we know satisfies

$$y^{-1}x^{-1} = (xy)^{-1} = xy.$$

But since $y^{-1}x^{-1} = yx$ we conclude that $xy = yx$ and therefore $G$ is abelian.

□

32. Show that if $G$ is a finite group of even order, then there is an $a \in G$ such that $a$ is not the identity and $a^2 = e$.

*Proof.* First of all note that $a^2 = e$ if and only if $a = a^{-1}$.

We can partition a group into sets defined by relating an element to its inverse. This means that an equivalence class has the form $\{a, a^{-1}\}$ for each $a \in G$. Clearly, the equivalence class containing the identity is $[e] = \{e\}$ so if there is no other singleton set equivalence class, then $G$ would have to have an odd number of elements. So there must be an odd number of non-identity elements which are their own inverses. □

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

*Proof.* Let $a, b \in G$. We aim to show that $ab = ba$.

$$abab = (ab)^2 = a^2b^2 = aabb$$

so that by left and right cancellation we get

$$ba = ab.$$

□

37. Let $H = \{2^k : k \in \mathbb{Z}\}$. Show that $H \leq \mathbb{Q}^*$.

*Proof.* Recall that $\mathbb{Q}^*$ is the non-zero rationals under multiplication, with 1 as its identity. Since $1 = 2^0$ it follows that $1 \in H$. Now the inverse of a $2^k$ is its reciprocal $2^{-k}$. Since $k \in \mathbb{Z}$ so is $-k$, thus $H$ is closed under inverses. next, let $a, b \in H$ which means that for some $j, k \in \mathbb{Z}$ $a = 2^j$ and $b = 2^k$. Then

$$ab = 2^j 2^k = 2^{j+k} \in H.$$

It follows that $H \leq \mathbb{Q}^*$. □