Examples of Groups and Group Properties

Example 25.1. Show that the set of matrices

\[ S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, \ ad - bc \neq 0 \right\} \]

is a group when the multiplication rule is matrix multiplication.

We need to show three things: (i) that the multiplication rule is associative, (ii) that \( S \) has a multiplicative identity element, and (iii) that every element \( A \in S \) has a multiplicative inverse in \( S \).

(i) The multiplication rule for \( S \) is associative because matrix multiplication is associative.

(ii) The matrix \( I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) is in \( S \) and has the property that \( AI = A = IA \). So \( S \) has \( I \) as its identity element.

(iii) If \( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \), then \( \det A = ad - bc \). From Linear Algebra one know that \( \det A \neq 0 \iff A^{-1} \) exists. Moreover,

\[ \det (A^{-1}) = \frac{1}{\det (A)} = \frac{1}{ad - bc} \neq 0 \]

so \( A^{-1} \in S \). Hence, every element of \( S \) has an inverse in \( S \).

Having verified the three defining properties of a group, we conclude \( S \) is a group.

Example 25.2. Show that the set

\( U_n = \{ u \in \mathbb{Z}_n \mid u \text{ is a unit in } \mathbb{Z}_n \} \)

is a group when group multiplication is the usual multiplication in \( \mathbb{Z}_n \).

(i) Multiplication in \( \mathbb{Z}_n \) is associative and the multiplication rule in \( U_n \) is associative.

(ii) The element \([1]_n \in \mathbb{Z}_n\) is a unit in \( \mathbb{Z}_n \). (Recall a unit in a ring \( R \) with identity \( 1_R \) is an element \( a \in R \) such that there exists \( b, b' \in R \) such that \( ab = 1_R = b'a \).) Clearly, \([1]_n\) is the multiplicative identity in \( U_n \) since \([1]_n [1]_n = [1]_n \).

(iii) If \( a \in U_n \) then \( a \) is a unit in \( \mathbb{Z}_n \) and so there exists \( b \in \mathbb{Z}_n \) such that \( ab = [1]_n \), hence \( a \) has a multiplicative inverse \( b \) and, moreover, this inverse is also a unit in \( \mathbb{Z}_n \) and so belongs to \( U_n \).

Example 25.3. What is the order of \( U_p \) when \( p \) is prime?

The order of a group is the number of elements in the group (as a set). Now we know that \( \mathbb{Z}_p \) has exactly \( p \) elements \([0]_p, [1]_p, \ldots, [p - 1]_p\). Moreover, since \( \mathbb{Z}_p \) is a field when \( p \) is prime, every nonzero element of \( \mathbb{Z}_p \) is a unit. This means \( U_n \) consists of every element of \( \mathbb{Z}_p \) except \([0]_p\). Thus, the order of \( U_p \) is \( p - 1 \).

Example 25.4. Prove that the order of \( a^{-1} \) is equal to the order of \( a^{-1} \).
Suppose first that \( e \) is of finite order. Then there exists a smallest positive integer \( n \) such that \( a^n = e \). Since

\[ e = a^n = a(a^{n-1}) \]

we know \( a^{n-1} = a^{-1} \). But then

\[ (a^{-1})^n = (a^{n-1})^n = a^{n(n-1)} = (a^n)^{n-1} = (e)^{n-1} = e \]

and so \( a^{-1} \) has finite order \( \leq n \).

The problem is now to show that \( n \) is in fact the smallest power of \( a^{-1} \) that produces the identity element \( e \). Suppose the order of \( a^{-1} \) is \( k \leq n \). Then

\[ e = (a^{-1})^k = (a^{n-1})^k = a^{kn-k} \implies a^k = a^ke = a^ka^{kn-k} = a^{kn} \]

Now according to Theorem 7.8, if \( a \) has order \( n \), then \( a^i = a^j \iff i \equiv j \pmod{n} \). So

\[ a^k = a^{kn} \implies k = kn \pmod{n} \implies k = 0 \pmod{n} \implies k = pn \text{ for some positive integer } p \]

But the only positive multiple of \( n \) that’s less than or equal to \( n \) is \( n \) itself. Therefore, \( k = n \), and \( |a^{-1}| = |a| \).

**EXAMPLE 25.5.** Let \( G \) be a group and let \( a \in G \). Prove that the set

\[ N_a = \{ g \in G \mid ga = ag \} \]

is a subgroup of \( G \).

We need to show three things: (i) that \( N_a \) is closed under multiplication, (ii) that the identity element of \( G \) is in \( N_a \) and (iii) that if \( g \in N_a \), then \( g^{-1} \in N_a \).

(i) \( N_a \) is closed under multiplication: Suppose \( g, g' \in N_a \). Then

\[ (gg')a = g(g'a) = g(aga') = (ga)g' = (ag)g' = a(gg') \]

and so \( gg' \in N_a \).

(ii) Clearly, \( ea = a = ae \) and so \( e \in N_a \).

(iii) Suppose \( g \in N_a \). Then

\[ ga = ag \]

Multiplying this equation from the left by \( g^{-1} \) yields

\[ a = g^{-1}ga = g^{-1}ag \]

Multiplying the extreme sides of the above equation from the right by \( g^{-1} \) yields

\[ ag^{-1} = g^{-1}ag^{-1} = g^{-1}ae = g^{-1}a \implies ag^{-1} = g^{-1}a \implies g^{-1} \in N_a \]

And so if \( g \in N_a \), \( g^{-1} \in N_a \).

**EXAMPLE 25.6.** Prove that \( H \) is a subgroup of a group \( G \) if and only if \( ab^{-1} \in H \) for all \( a, b \in H \).

\[ \Leftarrow \]

Suppose \( ab^{-1} \in H \) for all \( a, b \) in \( H \). We need to show the criteria (i), (ii), (iii) of the previous hold.

Choosing \( b = a \in H \), we have \( aa^{-1} \in H \). But \( aa^{-1} = e \) and so \( e \in H \). This proves (ii).

Now choosing \( a = e \) (which we now know belongs to \( H \)) we have \( eb^{-1} = b^{-1} \in H \) for all \( b \in H \). And so we have property (iii).

It remains to prove that \( ab \in H \) whenever \( a, b \in H \). But by (iii) just proven, if \( b \in H \), then \( b^{-1} \in H \) and so

\[ a(b^{-1})^{-1} \in H \implies ab \in H \]
Assume $H$ is a subgroup of $G$. Then if $a, b$ are in $H$, so are $a^{-1}$ and $b^{-1}$ since subgroups are closed under multiplicative inverses. But then

$$ab^{-1} \in H$$

since subgroups are closed under multiplication.