

Groups Part I

We have seen several examples of “number systems” which satisfy the first three of our axioms for integers:

- associativity: $(a + b) + c = a + (b + c)$
- there is an identity (0): $a + 0 = 0 + a = a$
- every element has an inverse: $a + (-a) = (-a) + a = 0$.

The integers modulo n , \mathbb{Z}_n , have an addition with the same three properties.

The invertible elements of \mathbb{Z}_n have a multiplication which satisfies the same three properties. Here the identity is 1 (more properly, $[1]_n$) and $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

The permutations in S_n have a composition which satisfies the same three properties. Here the identity is the identity function.

In the first three examples, the operation is commutative as well. But in the last example, composition of two permutations isn't generally commutative. In the last three examples, there are only finitely many elements. Here we can (and did) make “tables” for the operation.

Since this situation crops up so often, mathematicians came up with a name for it.

Definition: A *group* is a non-empty set with a binary operation (that is, a way to combine two elements to get a third) which is associative, has an identity, and every element has an inverse.

One typically uses the letter G to denote a generic group and generally the binary operation is denoted like multiplication: $a \cdot b$ or more simply ab . The identity element is traditionally denoted e , not 1. In those cases where the binary operation is commutative, it is denoted like addition and the identity element is denoted by 0. Such groups are called *abelian* in honor of the mathematician Abel.

With this notation, a group is a non-empty set G with a binary operation \cdot taking $G \times G$ to G with the following three properties:

1. for all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
2. there is an $e \in G$ such that $e \cdot a = a \cdot e = a$ for all $a \in G$;
3. for all $a \in G$ there is an $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

More Examples: The set of all matrices of a given size, for example 3×5 , form a group under addition. These are abelian groups.

The set of all invertible matrices of a given size form a group under multiplication. These groups aren't abelian (except in the 1×1 case).

The set of all polynomials with real coefficients form an abelian group under addition.

Can you think of more examples?

Recall the first two of our “little results” for the integers:

- The additive identity is unique.
- For any $a \in \mathbb{Z}$, the additive inverse of a is unique.

These two are actually general facts we can prove about groups. Not only that, the way we thought about proving them can be put in general “group-theoretic” terms.

Lemma: Suppose G is a group. The identity element is unique. If $a \in G$, then the inverse of a is unique.

Proof: Suppose e_1 and e_2 are identity elements in G . Then $e_1e_2 = e_1$, since e_2 is an identity element. Also, $e_1e_2 = e_2$ since e_1 is an identity element. Thus, $e_1 = e_2$; the identity element is unique.

Suppose $a \in G$. Suppose b and c are inverses of a . This means that $ab = ba = e$ and also $ac = ca = e$. Then $b(ac) = be = b$. On the other hand, $b(ac) = (ba)c = ec = c$. Thus, $b = c$; the inverse of a is unique.

Three more “little results” we can prove about groups are

Lemma: If G is a group and $a \in G$, then $(a^{-1})^{-1} = a$.

Lemma: If G is a group and $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Lemma: Suppose G is a group and $a, b, c \in G$ satisfy $ab = ac$. Then $b = c$. Similarly, if $ba = ca$ then $b = c$.