Basic Properties of Groups

Proposition 3.2 : The identity element in a group G is unique; that is, there exists only one element $e \in G$ such that $eg = ge = g$ for all $g \in G$.

Proof. Suppose that e and e' are both identities in G. Then $eg = ge=g$ and $e'g=ge'=g$ for all $g \in G$. We need to show that $e=e'$. If we think of e as the identity, then $ee' = e'$; but if e' is the identity, then $ee' = e$. Combining these two equations, we have $e = ee' = e'$.

Proposition 3.3: If g is any element in a group G, then the inverse of g, g^{-1}, is unique.

Proof: Inverses in a group are also unique. If g' and g'' are both inverses of an element g in a group G, then $gg' =g'g=e$ and $gg'' =g''g=e$. We want to show that $g' = g''$, but $g' = g'e = g'(gg'') = (g'g)g'' = eg'' = g''$.

Sandip Chatterjee, Department of Mathematics

Proposition 3.4: Let G be a group. If a, b $\in$ G, then $(ab)^{-1} = b^{-1} a^{-1}$.

Proof. Let a,b $\in$ G. Then $abb^{-1} a^{-1} = aea^{-1} = aa^{-1} = e$. Similarly, $b^{-1}a^{-1} ab = e$. But by the previous proposition, inverses are unique; hence, $(ab)^{-1} = b^{-1} a^{-1}$.

Proposition 3.5: Let G be a group. For any a $\in$ G, $(a^{-1})^{-1} = a$.

Proof. Observe that $a^{-1} (a^{-1})^{-1} = e$. Consequently, multiplying both sides of this equation by a, we have

$$(a^{-1})^{-1} = e(a^{-1})^{-1} = aa^{-1}(a^{-1})^{-1} = ae = a.$$

Proposition 3.6: Let G be a group and a and b be any two elements in G. Then the equations $ax = b$ and $xa = b$ have unique solutions in G.

Proof. Suppose that $ax = b$. We must show that such an x exists. Multiplying both sides of $ax = b$ by a^{-1}, we have $x = ex = a^{-1}ax = a^{-1}b$.

To show uniqueness, suppose that x_1 and x_2 are both solutions of $ax = b$; then $ax_1=b=ax_2$. So $x_1=a^{-1}ax =a^{-1}ax_2 =x_2$. The proof for the existence and uniqueness of the solution of $xa = b$ is similar.

Sandip Chatterjee, Department of Mathematics

Proposition 3.7: If G is a group and $a,b,c \in G$, then $ba = ca$ implies $b = c$ and $ab=ac$ implies $b=c$.

This proposition tells us that the ***right and left cancellation laws*** are true in groups. We leave the proof as an exercise.

We can use exponential notation for groups just as we do in ordinary algebra. If G is a group and $g \in G$, then we define $g^0 = e$. For $n \in N$, we define

$$g^n = g \cdot g \cdots g \text{ (n times) and } g^{-n} = g^{-1} \cdot g^{-1} \cdots g^{-1} \text{ (n times)}$$

Theorem 3.8: In a group, the usual laws of exponents hold; that is, for all $g, h \in G$,

1. $g^m g^n = g^{m+n}$ for all $m,n \in Z$;
2. $(g^m)^n = g^{mn}$ for all $m,n \in Z$;
3. $(gh)^n = (h^{-1} g^{-1})^{-n}$ for all $n \in Z$.

Furthermore, if G is abelian, then $(gh)^n = g^n h^n$.

Proof. We will leave the proof of this theorem as an exercise.

Notice that $(gh)^n \neq g^n h^n$ in general, since the group may not be abelian.

Sandip Chatterjee, Department of Mathematics

Subgroups

Definitions and Examples :

Sometimes we wish to investigate smaller groups sitting inside a larger group. The set of even integers $2Z = \{\ldots,-2,0,2,4,\ldots\}$ is a group under the operation of addition. This smaller group sits naturally inside of the group of integers under addition.

We define a **subgroup** H of a group G to be a subset H of G such that when the group operation of G is restricted to H, H is a group in its own right.

Observe that every group G with at least two elements will always have at least two subgroups, the subgroup consisting of the identity element alone and the entire group itself. The subgroup $H = \{e\}$ of a group G is called the **trivial subgroup**. A subgroup that is a proper subset of G is called a **proper subgroup**. In many of the examples that we have investigated up to this point, there exist other subgroups besides the trivial and improper subgroups.

Sandip Chatterjee, Department of Mathematics

Example 10. Consider the set of nonzero real numbers, R∗, with the group operation of multiplication. The identity of this group is 1 and the inverse of any element a ∈ R∗ is just 1/a. We will show that

$$Q* = \{p/q : p \text{ and } q \text{ are nonzero integers}\}$$

is a subgroup of R∗. The identity of R∗ is 1; however, 1 = 1/1 is the quotient of two nonzero integers. Hence, the identity of R∗ is in Q∗. Given two elements in Q∗, say p/q and r/s, their product pr/qs is also in Q∗. The inverse of any element p/q ∈ Q∗ is again in Q∗ since (p/q)−1 = q/p. Since multiplication in R∗ is associative, multiplication in Q∗ is associative.

Example 11. Recall that C∗ is the multiplicative group of nonzero complex numbers. Let H = {1, −1, i, −i}. Then H is a subgroup of C∗. It is quite easy to verify that H is a group under multiplication and that H ⊂ C∗.

Example 12. Let $SL_2(R)$ be the subset of $GL_2(R)$ consisting of matrices of determinant one; that is, a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in $SL_2(R)$ exactly when $ad - bc = 1$. To show that $SL_2(R)$ is a subgroup of the general linear group, we must show that it is a group under matrix multiplication. The 2×2 identity matrix is in $SL_2(R)$, as is the inverse of the matrix A:

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

It remains to show that multiplication is closed; that is, that the product of two matrices of determinant one also has determinant one. We will leave this task as an exercise. The group $SL_2(R)$ is called the ***special linear group***.

Example 13. It is important to realize that a subset H of a group G can be a group without being a subgroup of G. For H to be a subgroup of G it must inherit G's binary operation. The set of all 2 × 2 matrices, $M_2(R)$, forms a group under the operation of addition. The 2 × 2 general linear group is a subset of $M_2(R)$ and is a group under matrix multiplication, but it is not a subgroup of $M_2(R)$. If we add two invertible matrices, we do not necessarily obtain another invertible matrix. Observe that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

but the zero matrix is not in GL2(R).

Example 14. One way of telling whether or not two groups are the same is by examining their subgroups. Other than the trivial subgroup and the group itself, the group Z_4 has a single subgroup consisting of the elements 0 and 2. From the group Z_2, we can form another group of four elements as follows. As a set this group is $Z_2 \times Z_2$. We perform the group operation coordinate-wise; that is, (a, b) + (c, d) = (a + c, b + d). Since there are three nontrivial proper subgroups of $Z_2 \times Z_2$, $H_1=\{(0,0),(0,1)\}$, $H_2=\{(0,0),(1,0)\}$, and $H_3=\{(0,0),(1,1)\}$, Z_4 and $Z_2 \times Z_2$ must be different groups.

+	(0,0)	(0,1)	(1,0)	(0,1)
(0,0)				
(0,1)				
(1,0)				
(1,1)				

Proposition 3.9: A subset H of G is a subgroup if and only if it satisfies the following conditions.

1. The identity e of G is in H.
2. If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.
3. If $h \in H$, then $h^{-1} \in H$.

Proof. First suppose that H is a subgroup of G. We must show that the three conditions hold. Since H is a group, it must have an identity e_H . We must show that $e_H = e$, where e is the identity of G. We know that $e_H e_H = e_H$ and that $ee_H = e_H e = e_H$; hence, $ee_H = e_H e_H$. By right-hand cancellation, $e = e_H$. The second condition holds since a subgroup H is a group. To prove the third condition, let $h \in H$. Since H is a group, there is an element $h' \in H$ such that $hh' = h'h = e$. By the uniqueness of the inverse in G, $h' = h^{-1}$.

Conversely, if the three conditions hold, we must show that H is a group under the same operation as G; however, these conditions plus the associativity of the binary operation are exactly the axioms stated in the definition of a group.

Sandip Chatterjee, Department of Mathematics

Proposition 3.10: Let H be a subset of a group G. Then H is a subgroup of G if and only if $H \neq \varnothing$, and whenever $g, h \in H$ then gh^{-1} is in H.

Proof. Let H be a nonempty subset of G. Then H contains some element g. So $gg^{-1} = e$ is in H. If $g \in H$, then $eg^{-1} = g^{-1}$ is also in H. Finally, let $g,h \in H$. We must show that their product is also in H. However, $g(h^{-1})^{-1} = gh \in H$. Hence, H is indeed a subgroup of G. Conversely, if g and h are in H, we want to show that $gh^{-1} \in H$. Since h is in H, its inverse h^{-1} must also be in H. Because of the closure of the group operation, $gh^{-1} \in H$.