Basic properties of groups

In this lecture we discuss some basic properties of groups which follow directly from the definition. To begin, a few words on notation. Up to now we have considered a typical group $(G, \circ)$ with operation $a \circ b$. It is convenient to omit "$\circ$" from the notation and write

$$ab = a \circ b$$

Although this is a valid convention for any group, we will not always want to use it. For example, for the group $(\mathbb{Z}, +)$, writing "ab" for $a \circ b = a + b$ has the shortcoming of looking like integer multiplication. But for an arbitrary abstract group it is very convenient.

The associativity property of a group tells us that $(ab)c = a(bc)$. This continues on for more complicated operations. For example, we have

$$((ab)c)d = (a(bc))d = a((bc)d) = a(b(cd)) = (ab)(cd)$$

Each equality uses one use of the associativity axiom. What associativity is really telling us is that we can forget about those pesky parantheses: no matter where we put them, we get the same answer. The above group element can just be written $abcd$.

For what follows we let G be any group, with the conventions above.

▶ **The identity element in G is unique.**

Proof. Let $e, e' \in G$ be two identity elements. Because e is an identity element, $ee' = e$. Because e' is an identity element, $ee' = e'$. Together we get $e = e'$. □

▶ **The inverse of any element in G is unique.**

Proof. Let $a \in G$ be be any element. Let b and c be two inverses of a. (Let us avoid calling either one a^{-1} for now.) Because b is an inverse of a we have $ba = e$. Multiply both sides of this equation on the right by c to get $bac = c$. Because c is an inverse for a, we have $ac = e$. Thus $bac = c$ becomes $be = c$, and finally $b = c$. □

▶ **For every $a \in G$, we have $(a^{-1})^{-1} = a$.**

Proof. The element a satisfies $aa^{-1} = a^{-1}a = e$ and thus is an inverse of a^{-1}. It then makes sense to say $a = (a^{-1})^{-1}$ because inverses are unique. □

▶ **For all $a, b \in G$ we have $(ab)^{-1} = b^{-1}a^{-1}$.**

Proof. We only need check that $b^{-1}a^{-1}$ satisfies the property of being an inverse for ab. To this end: $(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$. Similarly $(b^{-1}a^{-1})(ab) = e$. □

This last property can be used any number of times to show the following relation:

$$(a_1 a_2 \cdots a_{n-1} a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}$$

We introduce some more convenient notation. Suppose n is a positive integer. Then we define the symbol a^n to mean the element $aa\cdots a = a \circ a \circ \cdots \circ a$ formed by applying the group operation to n copies of the element a. If n is negative, define $a^n = a^{-1}\cdots a^{-1}$ for $-n$ copies of a^{-1}. If $n = 0$, define $a^0 = e$, the identity element. The following is straightforward to verify:

▸ **For all $a, b \in G$ and $n, m \in \mathbb{Z}$ we have the following properties:**

$$a^n a^m = a^{n+m}, \qquad (a^n)^m = a^{nm}, \qquad (ab)^n = (b^{-1}a^{-1})^{-n}$$

The above discussion shows that in an arbitrary group G, we have all the properties we are used to with, say, matrix multiplication of invertible matrices. Furthermore:

▸ **If G is abelian, then for all $a, b \in G$ and $n \in \mathbb{Z}$ we have $(ab)^n = a^n b^n$.**

To see this, write $(ab)^n = abab\cdots ab$ and use that $ab = ba$, since G is abelian, to move the terms past one another, yielding $a\cdots ab\cdots b = a^n b^n$. However, for a general group which is not necessarily abelian, just like for matrices, we do not always have $(ab)^n = a^n b^n$. To further illustrate this point:

▸ **If a group G has $(ab)^2 = a^2 b^2$ for all $a, b \in G$ then G is abelian.**

Proof. Suppose $(ab)^2 = a^2b^2$ for all $a, b \in G$, i.e. $abab = aabb$. Multiply both sides of this equation by a^{-1} on the left and b^{-1} on the right to obtain $ba = ab$. Thus G is abelian. □

In the argument just made, we used the following cancellation property, which again follows by multiplying both sides of the equation on the left or right by the appropriate element:

▸ **Let $a, b, c \in G$. If $ab = ac$ then $b = c$. If $ba = ca$ then $b = c$.**

Let us illustrate how to solve equations in an abstract group. Suppose we are given

$$(xax)^2 = abx^2 \qquad x^2 a = (xa)^{-1}$$

where $a, b \in G$ are known and we would like to solve for $x \in G$. We do this as follows:

$$\begin{aligned}
(xax)^2 &= abx^2 \\
xaxxax &= abx^2 \\
xa(x^2a)x &= abx^2 \\
xa(xa)^{-1}x &= abx^2 \\
x &= abx^2 \\
e &= abx \\
x &= (ab)^{-1} = b^{-1}a^{-1}
\end{aligned}$$

Subgroups

A subset $H \subset G$ of a group G is called a *subgroup* if the set H with the group operation restricted from G makes H a group. If we spell this out, we see that a subset $H \subset G$ is a subgroup if and only if the following properties hold:

1. The identity element e is in H.
2. For all $a, b \in H$ we have $ab \in H$.
3. For all $a \in H$ we have $a^{-1} \in H$.

You might like to verify that these properties imply H is a subgroup. The key point is that given these properties, the axioms of a group for H are inherited from those of G. A subgroup $H \subset G$ is *proper* if $H \neq G$. Another good exercise is to check:

▸ **The intersection of two subgroups $H, K \subset G$ is again a subgroup.**

Examples

1. The group $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$, and $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$.

2. The group $(\mathbb{Q}^\times, \times)$ is a subgroup of $(\mathbb{R}^\times, \times)$. Note that $(\mathbb{Q}^\times, \times)$ is *not* a subgroup of $(\mathbb{Q}, +)$, even though $\mathbb{Q}^\times \subset \mathbb{Q}$, because the group operations are not the same.

3. Define $\mathrm{SL}_2(\mathbb{R})$ to be the set of 2×2 matrices with real entries and determinant 1:

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a, b, c, d \in \mathbb{R}, \quad \det(A) = ad - bc = 1 \right\}$$

This is called the *special linear group* of degree 2 over $\mathbb{R}$. This is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

4. A non-trivial group G has at least two subgroups: G itself and $\{e\} \subset G$.

5. Consider $G = \{e, r, b, g, y, o\}$ of order 6 from Lecture 1. Then $\{e, r\}$, $\{e, b\}$, $\{e, g\}$ are subgroups of order 2, while $\{e, y, o\}$ is a subgroup of order 3. Here are their Cayley tables:

	e	r
e	e	r
r	r	e

	e	b
e	e	b
b	b	e

	e	g
e	e	g
g	g	e

	e	y	o
e	e	y	o
y	y	o	e
o	o	e	y