5.2: Examples of Quotient Groups

Now that we've learned a bit about normal subgroups and quotients, we should build more examples.

Integers mod \(\mathbb{Z}/n\), Again

Recall the group \(\mathbb{Z}/n\). This can also be realized as the quotient group!

Let \(n\mathbb{Z}\) denote the set of integers divisible by \(n\): \(n\mathbb{Z}\) = \(
\{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}\). This forms a subgroup: \(0\) is always divisible by \(n\), and if \(a\) and \(b\) are divisible by \(n\), then so is \(a+b\). Since every subgroup of a commutative group is a normal subgroup, we can from the quotient group \(\mathbb{Z}/n\mathbb{Z}\).

To see this concretely, let \(n=3\). Then the cosets of \(3\mathbb{Z}\) are \(3\mathbb{Z}\), \(1+3\mathbb{Z}\), and \(2+3\mathbb{Z}\). We can then add cosets, like so: \((1+3\mathbb{Z}) + (2+3\mathbb{Z}) = 3+3\mathbb{Z} = 3\mathbb{Z}\).

The last equality is true because \(3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}\), so that \((3+3\mathbb{Z}) = \{\ldots, -3, 0, 3, 6, 9, \ldots\}\).

Write out addition tables for \(\mathbb{Z}/5\mathbb{Z}\) as a quotient group, and check that it is isomorphic to \(\mathbb{Z}/5\mathbb{Z}\) as previously defined.

The Alternating Group

Another example is a very special subgroup of the symmetric group called the Alternating group, \(A_n\). There are a couple
different ways to interpret the alternating group, but they mainly come down to the idea of the sign of a permutation, which is always \((\pm 1)\). The set \(\{1, -1\}\) forms a group under multiplication, isomorphic to \((\mathbb{Z}_2)^2\). The sign of a permutation is actually a homomorphism. There are numerous ways to compute the sign of a permutation:

1. **Determinants.** A permutation matrix is the matrix of the linear transformation of \(n\)-dimensional space sending the \(i\)-th coordinate vector \(e_i\) to \(e_{\sigma(i)}\). Such matrices have entries all equal to zero or one, with exactly one 1 in each row and each column. One can easily show that such a matrix has determinant equal to \((\pm 1)\). Since the determinant is a multiplicative function \(\det(MN) = \det(M) \cdot \det(N)\) - we can observe the determinant is a homomorphism from the group of permutation matrices to the group \(\{\pm 1\}\).

2. **Count inversions.** An inversion in a permutation \(\sigma\) is a pair \(i<j\) with \(\sigma(i) > \sigma(j)\). For example, the permutation \([3,1,4,2]\) has \(\sigma(1) > \sigma(2), \sigma(1) > \sigma(3)\) and \(\sigma(3) > \sigma(4)\), and thus has three inversions. If there are \(i\) inversions, then the sign of the permutation is \((-1)^i\).

3. **Count crossings.** Draw a braid notation for the permutation where no more than two lines cross at any point and no line intersects itself. Then count the number of crossings, \(c\). Then \(s(\sigma) = (-1)^c\). The alternating group is the subgroup of \(S_n\) with \(s(\sigma) = 1\). (To prove that this method of counting works, one needs a notion of Reidemeister moves, which originally arise in the fascinating study of mathematical knots.)

Find the inversion number for every permutation in \(S_4\), and then sort the permutations by their inversion number.

Show that each of the three definitions of the sign of a permutation give a homomorphism from \(S_n\) to \(\{1, -1\}\). (For the third definition, a sketch of a proof will suffice. Be sure to argue that different braid notations for the same permutation give the same sign, even if the total number of crossings is different.)

We call a permutation with sign \((+1)\) a positive permutation, and a permutation with sign \((-1)\) a negative permutation.

Show that there are \(\frac{n!}{2}\) positive permutations in \(S_n\).

Now we can define the alternating group.

**Definition 5.1.4: Alternating Groups**

The alternating group \(A_n\) is the kernel of the homomorphism \(s: S_n \rightarrow \mathbb{Z}_2\). Equivalently, \(A_n\) is the subgroup of all positive permutations in \(S_n\).

Write out all elements \(A_4\) as a subgroup of \(S_4\). Find a nice generating set for \(A_4\) and make a Cayley graph.

In fact, the alternating group has exactly two cosets. The quotient group \(S_n/\text{ord } A_n\) is then isomorphic to \((\mathbb{Z}_2)^2\).
Figure 5.1.2: Quotient of \( S_3 \) by \( A_3 \).

Contributors and Attributions

- Tom Denton (Fields Institute/York University in Toronto)