Quotients of commutative groups

Jonas van der Schaaf

I have written everything in additive notation in order to prepare the switch to rings.

Cosets of subgroups

Let $(G, +)$ be a commutative group and $H \subseteq G$ a subgroup. Then we define the left cosets to be sets of the following shape:

$$a + H = \{a + h : h \in H\}.$$

Note that in general $aH \nsubseteq H$. In fact if $a \notin H$ then $aH \cap H = \varnothing$. Similarly, we define right cosets to be

$$H + a = \{h + a : h \in H\}.$$

If the group is commutative then left and right cosets are the same thing ($a + x = x + a$). Notice that $a \in aH$ because $a = a + 1 \in aH$.

The quotient group is a construction to turn these cosets into a new group. We write G/H for the set of cosets. Given some element $a \in G$ we will also write $\overline{a}$ for the coset aH.

Lemma 1. *Any element of the group is in exactly one coset: namely $\overline{a}$.*

Proof. Suppose $a \in \overline{x}$ for some $x \in G$, we show $\overline{x} = \overline{a}$. Because $a \in \overline{x}$ we know that $a = xh'$ for some $h' \in H$. Rewriting the definition of $\overline{a}$ gives

$$\overline{a} = \{a + h : h \in H\} = \left\{x + h' + h : h \in H\right\}.$$

Because $h' + h \in H$ (remember H is a subgroup) we conclude that $\overline{a} \subseteq \overline{x}$. For the converse inclusion notice that $x = a - h$, so we can repeat the same argument to get $\overline{x} \subseteq \overline{a}$: $\overline{x} = \overline{a}$. □

This means that any element $a \in G$ is contained in exactly one coset: the cosets form a partition of G.

Defining the quotient group

Our goal is to define a group operation on the set of cosets G/H. We can do this as follows:

Let $\overline{a}, \overline{b} \in G/H$ be two cosets. We define their product as

$$\overline{a} + \overline{b} = \overline{a + b}.$$

We pick two representatives from the cosets, multiply them and take the coset in which this product lies as the result. It is not a priori clear that this is well-defined: if we had picked $a' \in \overline{a}$ and $b' \in \overline{b}$, do we have $\overline{a + b} = \overline{a' + b'}$? It turns out that it is, first we prove two lemmas.

Lemma 2. *Take two $x, y \in G$. Then $-y + x \in H$ if and only if $\overline{x} = \overline{y}$.*

Proof. By the previous lemma for the left to right implication it suffices to show that $x \in \overline{y}$. This is true because $-y + x = h \in H$ so $x = y - y + x = y + h \in \overline{y}$.

For the converse suppose $\overline{x} = \overline{y}$. Then $x \in \overline{x} = \overline{y}$ so there is some $h \in H$ such that $x = y + h$. Then $-y + x = -y + y + h = h \in H$. □

Lemma 3. *Given $x, y \in G$ the inverse of xy is given by $-y - x$.*

Proof. Simple algebraic manipulation gives

$$\begin{aligned} -y - x + x + y &= -y + 0 + y \\ &= -y + y \\ &= 0. \end{aligned}$$

□

Now we can prove the claim that this operation is well-defined.

Proof. We show $\overline{a+b} = \overline{a'+b'}$ by showing that $-(a'+b') + a + b \in H$. Using the previous lemma we know that $-(a'b') = -b' - a'$. Then $-a' + a = h \in H$ and $-b' + b = h' \in H$ by a previous lemma as well. We then rewrite

$$\begin{aligned} -(a'b') + a + b &= -b' - a' + a + b \\ &= -b' + h + b \\ &= h - b' + b \\ &= h + h' \in H. \end{aligned}$$

This proves that the two cosets are equal. □

In the second to last step of the proof we use commutativity of G. For non-commutative G this construction is more technical and puts stricter demands on the shape of the subgroup. For our purposes we will only consider commutative subgroups.

Now we can prove that this operation turns G/H into a group.

Theorem 1. *The pair $(G/H, +)$ forms a commutative group.*

Proof. We prove the three properties of a group:

1. Associativity of $+$,
2. existence of a neutral element,
3. existence of inverses.

These will follow very naturally from the group structure of G itself.

To show associativity, take any $\overline{a}, \overline{b}, \overline{c} \in G/H$. Then

$$\begin{aligned} (\overline{a} + \overline{b}) + \overline{c} &= \overline{a+b} + \overline{c} \\ &= \overline{(a+b)+c} \\ &= \overline{a+(b+c)} \\ &= \overline{a} + \overline{b+c} \\ &= \overline{a} + (\overline{b} + \overline{c}). \end{aligned}$$

The neutral element of G/H is the coset $\overline{0} = H$. Take any $\overline{a} \in G$. Then

$$\begin{aligned} \overline{a} + \overline{0} &= \overline{a+0} \\ &= \overline{a}. \end{aligned}$$

The same trick works for the other multiplication $\overline{0} + \overline{a}$.

To show existence of inverses we claim that $\overline{-a}$ is the inverse of $\overline{a}$:

$$\begin{aligned}\overline{-a} + \overline{a} &= \overline{-a + a} \\ &= \overline{0}\end{aligned}$$

which is the neutral element of G/H. Therefore, $-\overline{a} = \overline{-a}$.

The group G/H is commutative because

$$\begin{aligned}\overline{a} + \overline{b} &= \overline{a + b} \\ &= \overline{b + a} \\ &= \overline{b} + \overline{a}\end{aligned}$$

by commutativity of G. □

This shows that $(G/H, +)$ is a commutative group.

Quotient map

In case there is still time you can construct the morphism $f : G \to G/H$. It is defined as $f(x) = \overline{x}$. We show that this is a morphism of groups:

Lemma 4. *The map $f : G \to G/H$ defined by $f(x) = \overline{x}$ defines a group morphism.*

Proof. First, we show this map preserves the unit. This is true because $f(0) = \overline{0}$ which is the neutral element of G/H.

To show it preserves the operation take $a, b \in G$. Then

$$f(a + b) = \overline{a + b} = \overline{a} + \overline{b} = f(a) + f(b).$$

To show it preserves inverses take $a \in G$. Then

$$f(-a) = \overline{-a} = -\overline{a} = -f(a).$$

□

Lemma 5. *The map $f : G \to G/H$ is surjective and has kernel H.*

Proof. Given a coset $\overline{a}$ the element $a \in G$ is sent to it by f so f is surjective.

If $a \in G$ has $f(a) = \overline{a} = 0 = H$ then $-0 + a = a \in H$. □