On Quotients Groups and Quotient Rings

R. C. Daileda

By a *quotient* of a group or ring X we mean an object in the same category, whose underlying set is $X/\sim$ for some equivalence $\sim$ on X, with the property that the natural surjection $\pi : X \to X/\sim$ is a homomorphism. Only very specific equivalences can produce quotients. In the case that X is a group, $\sim$ must be congruence modulo a normal subgroup. If X is a ring, we must instead use congruence modulo an ideal. In this brief note we will derive both of these facts.

Let $X = G$ be a group and $\sim$ an equivalence relation on G. Suppose that $\times$ is a binary operation making $G/\sim$ into a group, and that $\pi : G \to G/\sim$ is a homomorphism. This means that for any $a, b \in G$ we have

$$[ab] = \pi(ab) = \pi(a) \times \pi(b) = [a] \times [b], \tag{1}$$

where $[x]$ denotes the equivalence class of $x \in G$. Let $x \in [a]$ and $y \in [b]$. Then $[x] = [a]$, $[y] = [b]$ and (1) implies that $[xy] = [ab]$. In particular, $xy \in [ab]$. Since x and y were arbitrary, this shows that the element-wise set product $[a] \cdot [b]$ is contained in the class $[ab]$, which proves our first lemma.

Lemma 1. *Let G be a group and $G/\sim$ be a quotient of G. Then for any $A, B \in G/\sim$, $A \times B$ is the unique class containing AB.*

Given $A, B, C \in G/\sim$ with $A \times B = C$, we claim that $C = AB$. To see this, let $y \in C$ and set $B' = [a^{-1}y]$. Then $y = a(a^{-1}y) \in AB'$. Because the classes in $G/\sim$ are disjoint, and Lemma 1 implies that AB' is contained in some class, it must be that $AB' \subset C$ and hence $C = A \times B'$. Since we also have $AB \subset A \times B = C$, we find that $A \times B = A \times B'$. Because $(G/\sim, \times)$ is a group, this equality implies that $B = B'$, and therefore $y \in AB' = AB$. It follows that $C = AB$. This proves the next lemma.

Lemma 2. *Let $(G/\sim, \times)$ be a quotient of a group G. Then for any $A, B \in G/\sim$, $A \times B = AB$.*

Lemma 2 shows that in order to understand the quotients of G, we need to investigate the equivalence relations on G for which $G/\sim$ is a group under element-wise multiplication of sets. To that end, let $\sim$ be an equivalence relation on $G/\sim$ so that $(G/\sim, \cdot)$ is a group. For any $x, y \in G$ we have $xy \in [x][y] \in G/\sim$, so that $[xy] = [x][y]$. This proves that the natural surjection $G \to G/\sim$ is a homomorphism, and hence that $(G/\sim, \cdot)$ is a quotient of G. This also implies that $[x^{-1}] = [x]^{-1}$ for all $x \in G$.

Let $H = [e]$. For any $C \in G/\sim$, we then have $C \subset CH \in G/\sim$. Because distinct classes are disjoint, we must then have $C = CH$. Similarly, $C = HC$, so that H is the identity in $G/\sim$. We will now prove that $H < G$. Let $x, y \in H$. According to our work in the preceding paragraph, we have $[xy^{-1}] = [x][y]^{-1} = HH^{-1} = HH = H$, which implies that $xy^{-1} \in H$. Because $H \neq \varnothing$, we conclude that H is a subgroup of G.

What about the other classes in $G/\sim$? Let $C \in G/\sim$. For any $x, y \in C$ we have

$$[x^{-1}y] = [x]^{-1}[y] = C^{-1}C = H \quad \Leftrightarrow \quad x^{-1}y \in H \quad \Leftrightarrow \quad y \in xH.$$

Thus $x \sim y$ if and only if $x \equiv y \pmod{H}$, and $C = xH$. That is, $\sim$ is congruence modulo H, and $G/\sim = G/H$, the corresponding left coset space. Had we started with the class $[yx^{-1}]$ instead, we would have found instead that $C = Hx$. This means that $xH = Hx$ for all $x \in G$, and so $H \lhd G$. Moreover, $xyH = [xy] = [x][y] = (xH)(yH)$ for all $x, y \in G$. Conversely, we know that the coset space of a normal subgroup always yields a quotient in this same manner, and we arrive at the following conclusion.

Theorem 1. *Let G be a group. The quotients of G are precisely the coset spaces G/H with $H \lhd G$ and multiplication given by $(xH)(yH) = xyH$.*

We now turn our attention to quotient rings. Fortunately Let $X = R$ be a ring with quotient $(R/\sim, \oplus, \otimes)$. Because the natural surjection $\pi : R \to R/\sim$ preserves addition, it must be a homomorphism between the additive groups $(R, +)$ and $(R/\sim, \oplus)$. According to Theorem 1, there is an additive subgroup I of R so that $R/\sim = R/I$, and $\oplus$ is just addition of cosets. As far as multiplication goes, for any $a, b \in R$ we have

$$(a + I) \otimes (b + I) = \pi(a) \otimes \pi(b) = \pi(ab) = ab + I.$$

If we omit $\times$ and simply concatenate, this becomes

$$(a + I)(b + I) = ab + I.$$

Because R/I is a ring, and the additive identity is $0 + I = I$, for any $a \in R$ and $b \in I$ we have

$$ab + I = (a + I)(b + I) = (a + I)(0 + I) = a0 + I = 0 + I = I.$$

Therefore $ab \in I$. Reversing the order of a and b we find that we likewise have $ba \in I$. In other words, I is closed under both left and right multiplication by elements of R. This yields our first result on quotient rings.

Theorem 2. *Every quotient of a ring R has the form R/I, where I is an additive subgroup of R satisfying*

$$a \in R, b \in I \quad \Rightarrow \quad ab, ba \in I. \tag{2}$$

Addition and multiplication in R/I are given by

$$\begin{aligned} (a + I) + (b + I) &= (a + b) + I, \\ (a + I)(b + I) &= ab + I. \end{aligned} \tag{3}$$

An additive subgroup I of R satisfying (2) is called an *ideal* of R. One can show that the converse of Theorem 2 also holds. That is, if I is an ideal of R, then R/I is a quotient of R via the binary operations (3). So the quotients of R are precisely the rings R/I, where I is an ideal in R.

Remark. Because it was inherited from the additive group structure of R, addition in R/I is just element-wise addition of cosets. However, the same is not true of multiplication. The element-wise product of $a + I$ and $b + I$ is contained in $ab + I$, but in general will not be equal to it.