# 22. Quotient groups I

22.0. **Digression on the octic group.** In this short section we provide an alternative description of the octic group $D_8$ which is more convenient for computational purposes than the original description.

**Claim 22.1.** *Let $r \in D_8$ be a rotation by 90 degrees (in any direction) and let $s \in D_8$ be any reflection. Then*

(a) $D_8 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$

(b) *The following relations hold in $D_8$: $r^4 = s^2 = e$ and $rs = sr^3$.*

*Proof.* (a) Let $R = \langle r \rangle$, the cyclic subgroup generated by $r$. Then $\langle r \rangle = \{e, r, r^2, r^3\}$ since $o(r) = 4$; it is also clear that $\langle r \rangle$ is the set of all rotations in $D_8$.

Since $\frac{|D_8|}{|R|} = \frac{8}{4}$, there are only two left cosets of $R$ in $D_8$, and one of these cosets is $R$ itself. Since $s$ is not a rotation, $s \notin R$, so $sR \neq R$, and hence $sR$ is the other left coset. Since the union of all left cosets of a subgroup should always be equal to the entire group, we have $D_8 = R \cup sR = \{e, r, r^2, r^3\} \cup \{s, r, sr^2, sr^3\} = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$, as desired.

(b) The relations $r^4 = e$ and $s^2 = e$ are clear. To prove that $rs = sr^3$ we argue as follows. Consider the element $s^{-1}rs$, which is a conjugate of $r$. By Problem 7 in HW#9, conjugate elements must have the same order, so $o(s^{-1}rs) = o(r) = 4$. The only elements of $D_8$ which have order 4 are $r$ and $r^3$ (the rotation by 90 degrees in the opposite direction), so we must have $s^{-1}rs = r$ or $s^{-1}rs = r^3$.

If $s^{-1}rs = r^3$, then multiplying by $s$ on the left, we get $rs = sr^3$, as desired, so we just have to explain why the other alternative ($s^{-1}rs = r$) cannot happen.

So suppose that $rs = sr$, so $s$ and $r$ commute. This means that any two elements of $D_8$ which can be expressed in terms of $s$ and $r$ must commute with each other (since we can freely change the order of $s$ and $r$ in any product containing only $s$ and $r$). Since any element of $D_8$ can be expressed as $r^i s^j$ for some $i, j \in \mathbb{Z}$ by (a) (including $e = r^0 s^0$), it follows that any two elements of $D_8$ commute, that is, $D_8$ is abelian, and we know that the latter is false. □

**Remark:** One can show that the relations in $D_8$ stated in (b) are *defining relations*. Informally this means that any relation between $r$ and $s$ which holds in $D_8$ can be deduced from those relations using just general group-theoretic laws (and not specific properties of $D_8$).

22.1. **Definition of quotient groups.** Let $G$ be a group and $H$ a subgroup of $G$. Denote by $G/H$ the set of distinct (left) cosets with respect to $H$. In other words, we list all the cosets of the form $gH$ (with $g \in G$) without repetitions and consider each coset as a SINGLE element of the newly formed set $G/H$. The set $G/H$ (pronounced as $G$ mod $H$) is called the quotient set.

Next we would like to define a binary operation $*$ on $G/H$ such that $(G/H, *)$ is a group. It is natural to try to define the operation $*$ by the formula

$$gH * kH = gkH \text{ for all } g, k \in G. \tag{Q}$$

Before checking group axioms, we need to find out whether $*$ is at least well defined. Our first result shows that $*$ is well defined whenever $H$ is a normal subgroup.

**Theorem 22.2.** *Let $G$ be a group and $H$ a normal subgroup of $G$. Then the operation $*$ given by (Q) is well defined.*

*Proof.* We need to show that if $g_1, g_2, k_1, k_2 \in G$ are such that $g_1H = g_2H$ and $k_1H = k_2H$, then $g_1k_1H = g_2k_2H$.

Recall that Theorem 19.2 (formulated slightly differently) asserts that given $x, y \in G$ we have $xH = yH \iff x^{-1}y \in H$. Thus, we need to show the following implication

$$\text{if } g_1^{-1}g_2 \in H \text{ and } k_1^{-1}k_2 \in H, \text{ then } (g_1k_1)^{-1}g_2k_2 \in H \tag{!}$$

So, assume that $g_1^{-1}g_2 \in H$ and $k_1^{-1}k_2 \in h$. Then there exist $h, h' \in H$ such that $g_1^{-1}g_2 = h$ and $k_1^{-1}k_2 = h'$, and thus $k_2 = k_1h'$. Hence

$$(g_1k_1)^{-1}g_2k_2 = k_1^{-1}g_1^{-1}g_2k_2 = k_1^{-1}hk_1h' = (k_1^{-1}hk_1)h'.$$

Since $H$ is normal, $k_1^{-1}hk_1 \in H$ by Theorem 20.2, and so $(k_1^{-1}hk_1)h' \in H$. Thus, we proved implication (!) and hence also Theorem 22.2. □

**Remark:** 1. The converse of Theorem 22.2 is also true, that is, if the operation $*$ on $G/H$ is well defined, then $H$ must be normal. This fact is left as an exercise, but we will not use it in the sequel.

2. There is a different approach to defining the group operation in quotient groups (this approach is used, for instance, in Gilbert's book). Eventually, of course, this definition is the same, but initial justification is different. We could define the operation $*$ by setting $gH * kH$ to be the product of $gH$ and $kH$ as subsets of $G$ (this operation was introduced in Lecture 19 and will be referred below as subset product). With this definition, it is clear that

the product is well defined, but it is not clear whether $G/H$ is closed under it, that is, whether the subset product of two cosets is again a coset (and in fact, the latter would be false unless $H$ is normal). So, what one needs to show with this approach is that if $H$ is normal, then for any $g, k \in H$, the subset product of $gH$ and $kH$ is equal to the coset $gkH$. This shows both that $G/H$ is closed under the subset product and also that the subset product coincides with the product given by (Q) (under the assumption $H$ is normal).

Having proved that our operation on $G/H$ is well defined (when $H$ is normal), we check the group axioms, which is quite straightforward.

**Theorem 22.3.** *Let $G$ be a group and $H$ a normal subgroup of $G$. Then the quotient set $G/H$ is a group with respect to the operation $*$ defined by (Q).*

*Proof.* (G0) $G/H$ is closed under $*$ by definition of cosets.

(G1) Associativity of $*$ follows from the associativity of the group operation on $G$: for any $g, k, l \in G$ we have

$$gH*(kH*lH) = gH*klH = (g(kl))H = ((gk)l)H = gkH*lH = (gH*kH)*lH.$$

(G2) The identity element of $G/H$ is the special coset $H = eH$. Indeed, for any $g \in G$ we have $gH * H = gH * eH = (ge)H = gH$ and similarly $H * gH = gH$.

(G3) Finally, the inverse of a coset $gH$ is the coset $g^{-1}H$. This is because $gH * g^{-1}H = (gg^{-1})H = eH = H$, and similarly $g^{-1}H * gH = H$. □

Now we proved that $G/H$ is a group when $H$ is normal, so we will start using the terminology quotient group. From now on we will write products in $G/H$ as $gH \cdot kH$ (or even as $gHkH$), instead of $gH * kH$.

22.2. **Examples of quotient groups.**

**Example 1:** Let $G = D_8$ (the octic group) and $H = \langle r^2 \rangle = \{e, r^2\}$, the cyclic subgroup generated by $r^2$ (recall that $r$ is a 90 degree rotation, so that $r^2$ is a 180 degree rotation). A direct computation shows that $H$ lies in the center $Z(G)$ (in fact, $H = Z(G)$ here, but we will not need the equality). So by Example 2 in Lecture 20, $H$ is normal in $G$, and thus we can form the quotient group $G/H$. We can immediately say that

$$|G/H| = \frac{|G|}{|H|} = \frac{8}{2} = 4.$$

Next we determine the elements of $G/H$, that is, (left) cosets of $H$.

$$H = eH = \{e, r^2\} \quad rH = \{r, r^3\} \quad sH = \{s, sr^2\} \quad srH = \{sr, sr^3\}.$$

Thus,

$$G/H = \{H, rH, sH, srH\}.$$

By describing elements of $G/H$ in this way we are automatically choosing a subset $T$ of $G$ which contains precisely one element from each coset (such subset $T$ is called a transversal; we will study this notion in more detail in Lecture 23). In this example our choice is $T = \{e, r, s, sr\}$.

Note that this choice of $T$ is not unique (e.g. $T' = \{e, r^3, sr^2, sr\}$ would have worked equally fine), but once we made a choice of $T$, we must stick to it in the following sense: when we do computations in $G/H$, every element of $G/H$ must be put in the form $tH$ where $t \in T$ (in order for us to see whether two given elements of $G/H$ are equal or not).

In homework#11 you will be asked to compute the multiplication table for $G/H$. Here we just do a sample computation – let us compute the products $sH \cdot rH$ and $rH \cdot sH$.

By definition of the operation in the quotient group and using the relation $rs = sr^3$ from Claim 22.1 we have

$$sH \cdot rH = srH \text{ and } rH \cdot sH = rsH = sr^3H.$$

In the first case we got the final answer; in the second case we did not since $sr^3$ is not in our transversal $T$. We need to find the (unique) element $t \in T$ such that $tH = sr^3H$. To do this we look at our description of cosets and locate the unique coset containing $sr^3$.

We see that $sr^3 \in srH$. Thus, $srH \cap sr^3H \neq \emptyset$, and since any two cosets either coincide or are disjoint, we conclude that $sr^3H = srH$. Thus, our final answer is

$$sH \cdot rH = srH \text{ and } rH \cdot sH = srH.$$

In particular, we see that $sH$ and $rH$ commute in $G/H$ even though $s$ and $r$ do not commute in $G$. Such phenomenon will happen very often in quotient groups.

**Example 2:** Let $G = \mathbb{Z}$ (with addition) and $H = 4\mathbb{Z}$. Here $G$ is abelian, so normality holds automatically. Since operation in $G$ is $+$, we use additive notation for cosets: $g + H$, with $g \in G$. It will be convenient to denote the operation in the quotient group $G/H$ by $+$ as well.

In this example we cannot use the formula $|G/H| = \frac{|G|}{|H|}$ since $G$ is infinite, but we can see directly that $G/H$ has 4 elements:

$$H = 0 + H = \{\ldots, -4, 0, 4, 8, \ldots\} \qquad 1 + H = \{\ldots, -3, 1, 5, 9, \ldots\}$$

$$2 + H = \{\ldots, -2, 2, 6, 10, \ldots\} \qquad 3 + H = \{\ldots, -1, 3, 7, 11, \ldots\}$$

Thus,

$$G/H = \{H, 1+H, 2+H, 3+H\}.$$

In general, for any $x \in \mathbb{Z}$ we have $x + H = \{y \in \mathbb{Z} : y \equiv x \mod 4\}$.

Arguing as in Example 1, we compute the "multiplication" table (multiplication is in quotes since in this example we use additive notation):

| | $H$ | $1+H$ | $2+H$ | $3+H$ |
|---|---|---|---|---|
| $H$ | $H$ | $1+H$ | $2+H$ | $3+H$ |
| $1+H$ | $1+H$ | $2+H$ | $3+H$ | $H$ |
| $2+H$ | $2+H$ | $3+H$ | $H$ | $1+H$ |
| $3+H$ | $3+H$ | $H$ | $1+H$ | $2+H$ |

This should look very familiar. We see immediately that the "multiplication" table for $G/H$ coincides with the "multiplication" table for $(\mathbb{Z}_4, +)$, up to relabeling $i + H \mapsto [i]_4$. In particular, the quotient group $G/H = \mathbb{Z}/4\mathbb{Z}$ is isomorphic to $\mathbb{Z}_4$.

This makes perfect sense since, as we see from the above computation, the cosets with respect to $H$ are precisely the congruence classes mod 4, and the operation $+$ on $G/H$ was defined by the same formula as addition in $\mathbb{Z}_4$: in $G/H$ we have $(i + H) + (j + H) = (i + j) + H$ (by formula (Q) from the beginning of the lecture), and in $\mathbb{Z}_4$ we have $[i]_4 + [j]_4 = [i + j]_4$, and as we just explained, $x + H$ is just another name for $[x]_4$.

It is clear that the same remains true when 4 is replaced by any integer $n \geq 2$:

**Proposition 22.4.** *Let $n \geq 2$ be an integer. The quotient group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$ via the map $(i + n\mathbb{Z}) \mapsto [i]_n$.*

22.3. **Quotient groups and homomorphisms.** Our next goal is to show that quotient groups are closely related to homomorphisms.

First let us show that each quotient group $G/H$ naturally gives rise to a homomorhism $\pi : G \to G/H$, called the natural projection from $G$ to $G/H$.

**Theorem 22.5.** *Let $G$ be a group and $H$ a normal subgroup of $G$. Define the map $\pi : G \to G/H$ by*

$$\pi(g) = gH \text{ for all } g \in G.$$

*Then $\pi$ is a surjective homomorphism and* $\operatorname{Ker} \pi = H$.

*Proof.* (i) $\pi$ is a homomorphism since $\pi(gk) = gkH = gH \cdot kH = \pi(g)\pi(k)$ (where the middle equality holds by the definition of operation in $G/H$).

(ii) $\pi$ is surjective since by definition every element of $G/H$ is equal to $gH$ for some $g \in G$.

(iii) Finally, $\operatorname{Ker}\pi = \{g \in G : gH = H\}$ (since $H$ is the identity element of $G/H$). By Problem 3(a) in Homework#10 we have $gH = H \iff g \in H$, so $\operatorname{Ker}\pi = H$, as desired. □

Now suppose that we are given two groups $G$ and $H$ and a homomorphism $\varphi : G \to H$. By Theorem 20.3, $\operatorname{Ker}\varphi$ is a normal subgroup of $G$, and thus we can consider the quotient group $G/\operatorname{Ker}\varphi$. The next theorem, called the **fundamental theorem of homomorphisms** (abbreviated as FTH) asserts that $G/\operatorname{Ker}\varphi$ is always isomorphic to the range group $\varphi(G)$.

**Theorem** (FTH)**.** *Let $G$, $Q$ be groups and $\varphi : G \to Q$ a homomorphism. Then*

$$G/\operatorname{Ker}\varphi \cong \varphi(G). \qquad (***)$$

The proof and applications of FTH will be discussed in the next lecture. At this point we just make two simple, but useful observations.

The first one is a special case of FTH dealing with surjective homomorphisms (in which case $\varphi(G) = Q$).

**Corollary 22.6.** *Let $G$, $Q$ be groups and $\varphi : G \to Q$ a surjective homomorphism. Then $G/\operatorname{Ker}\varphi \cong Q$.*

Also note that FTH immediately implies the Range-Kernel Theorem. Indeed, the isomorphism $G/\operatorname{Ker}\varphi \cong \varphi(G)$ implies that $|G/\operatorname{Ker}\varphi| = |\varphi(G)|$. If $G$ is finite, then $|G/\operatorname{Ker}\varphi| = \frac{|G|}{|\operatorname{Ker}\varphi|}$, so $\frac{|G|}{|\operatorname{Ker}\varphi|} = |\varphi(G)|$. Multiplying both sides by $|\operatorname{Ker}\varphi|$, we get the Range-Kernel Theorem.

22.4. **Book references.** The general references for the first lecture are [Pinter, Chapter 15] and [Gilbert, 4.6]. The exposition in Pinter may appear quite different since he defines normal subgroups differently and also uses right cosets instead of left cosets.