5 Homomorphisms, isomorphisms and quotient groups

5.1 Quotient groups

Suppose $H \leq G$. We want to be able to create a group by "dividing" G by H to form the set G/H of cosets of H in G. Can we do this?

No! The set G/H is not always a group. However, when H is normal in G this does work, and is called a quotient group.

Definition 5.1.1. Suppose $N \trianglelefteq G$. The *quotient group* G/N is the set of cosets of N in G with the following operation: for all cosets $aN \in G/N$ and all $bN \in G/N$,

$$aN * bN = (ab)N.$$

[Note that in fact (aN)(bN) = abN even without this definition, since $(aN)(bN) = a(Nb)N = a(bN)N$ (by normality) $= abN$.]

We must prove that this is indeed a group by checking the axioms.
Proof: We must check that the following axioms hold: closure; identity; inverses; associativity. Choose any three cosets $aN, bN, cN \in G/N$.

- *Closure*: Now $aN * bN = (ab)N$, and $(ab)N$ is a coset of N in G so it lies in G/N.
- *Identity*: Define e to be $e_G N = N$. We will show that this definition of e satisfies the properties of the identity for G/N. First note that $e * (aN) = e_G N * aN = (e_G a)N = aN$ and $(aN) * e = (aN)(e_G N) = (ae_G)N = aN$.
- *Inverses*: Now $a^{-1}N$ is a coset of N in G, and so it lies in G/N. Furthermore, $(a^{-1}N) * (aN) = (a^{-1}a)N = N = e$. Also $(aN) * (a^{-1}N) = (aa^{-1})N = N = e$. Therefore $a^{-1}N$ is the inverse of aN.
- *Associativity*: $(aN) * ((bN) * (cN)) = (aN) * ((bc)N) = (a(bc))N = ((ab)c)N = (ab)N * cN = (aN * bN) * cN$.

Example 5.1.2. You probably saw this example in Algebraic Strcutures. Consider the group $(\mathbb{Z}, +)$. It is abelian, so every subgroup is a normal subgroup. We know that $3\mathbb{Z}$ is a subgroup, therefore it is a normal subgroup and hence $(\mathbb{Z}, +)/3\mathbb{Z}$ is a group.
What does $(\mathbb{Z}, +)/3\mathbb{Z}$ look like? Well,

$$(\mathbb{Z}, +)/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$$

(because $3 + 3\mathbb{Z} = 3\mathbb{Z}$, $4 + 3\mathbb{Z} = 1 + 3\mathbb{Z}$, etc)
Hence $(\mathbb{Z}, +)/3\mathbb{Z}$ and $\mathbb{Z}_3$ have the same elements. Moreover, their group operations are the same: both operations are addition mod 3. Hence $(\mathbb{Z}, +)/3\mathbb{Z} = \mathbb{Z}_3$.

Example 5.1.3. Recall that $S_3 = \{e, (123), (132), (12), (13), (23)\}$ and $C_3 = \{e, (123), (132)\}$.
One can show that $C_3 \trianglelefteq S_3$ (this is a question on one of your problem sheets). Therefore S_3/C_3 is a group.
What does S_3/C_3 look like? Well, it has order $[S_3 : C_3] = |S_3|/|C_3| = 6/3 = 2$. There are just two cosets of C_3 in S_3 (and one of these cosets is just C_3 itself). Therefore *any* element not in C_3 will give us the other coset. E.g.

$$S_3 = C_3 \cup (12)C_3.$$

Hence the quotient group is $S_3/C_3 = \{eC_3, (12)C_3\}$. The operation is:

$$\begin{aligned}(eC_3)(eC_3) &= (ee)C_3 = eC_3\\ (eC_3)((12)C_3) &= (e(12))C_3 = (12)C_3\\ ((12)C_3)(eC_3) &= ((12)e)C_3 = (12)C_3\\ ((12)C_3)((12)C_3) &= ((12)(12))C_3 = eC_3\end{aligned}$$

As you can see, the group S_3/C_3 is behaving *exactly* like the group $\{e, (12)\} = C_2$ — the only difference is in the symbols used for the group elements. This is an example of an *isomorphism*, that we will cover in the next section.

5.2 Homomorphisms

Definition 5.2.1. Let G be a group with operation $*$ and let H be a group with operation $\#$. A function $\theta : G \to H$ that satisfies

$$\theta(g_1 * g_2) = \theta(g_1)\#\theta(g_2) \quad \text{for all } g_1, g_2 \in G$$

is called a *homomorphism*.

(Notice that $\theta(g_1)$ and $\theta(g_2)$ are in H which is why the operation becomes $\#$.)

However, because we are now doing grown-up Group Theory, we don't bother writing in the symbols $*$ and $\#$, and instead say that a homomorphism is a map $\theta : G \to H$ that satisfies

$$\theta(g_1 g_2) = \theta(g_1)\theta(g_2).$$

The reader is expected to remember that the group operation between g_1 and g_2 will not necessarily be the same as the group operation between $\theta(g_1)$ and $\theta(g_2)$.

The *kernel* of θ is denoted $\mathrm{Ker}(\theta)$ and is the set of all elements in G that are mapped to e_H. The *image* of θ is denoted $\mathrm{Im}(\theta)$ (or sometimes $\theta(G)$) and is the set of all images of elements in G. More precisely:

$$\mathrm{Ker}(\theta) = \{g \in G : \theta(g) = e_H\} \quad \text{and} \quad \mathrm{Im}(\theta) = \{\theta(g) : g \in G\}.$$

Example 5.2.2. Here is a homomorphism.

- Let $n \in \mathbb{N}$. The map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\varphi(m) = [m]_n$ for all $m \in \mathbb{Z}$ is a homomorphism.
  Proof: Fix $m_1, m_2 \in \mathbb{Z}$. On one hand, $\varphi(m_1 + m_2) = [m_1 + m_2]_n$. On the other hand, $\varphi(m_1) \oplus \varphi(m_2) = [m_1]_n \oplus [m_2]_n$ and by the definition of $\mathbb{Z}_n$ we know $[m_1]_n \oplus [m_2]_n = [m_1 + m_2]_n$. Hence $\varphi(m_1 + m_2) = \varphi(m_1) \oplus \varphi(m_2)$ for all $m_1, m_2 \in \mathbb{Z}$ so φ is a homomorphism.
- $\mathrm{Ker}(\varphi) = \{m \in \mathbb{Z} : [m]_n = [0]_n\} = n\mathbb{Z}$ = the set of multiples of n. Note that φ is not one-to-one because more than one element in $\mathbb{Z}$ is mapped to $[0]_n \in \mathbb{Z}_n$.
- $\mathrm{Im}(\varphi) = \{\varphi(m) : m \in \mathbb{Z}\} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$. Since $\mathrm{Im}(\varphi) = \mathbb{Z}_n$, we see that φ is onto.

Non-Example 5.2.3. Here is an example of a map π from S_3 to C_3 that is not a homomorphism:

- $\pi(e) = e$
- $\pi((1\ 2\ 3)) = (1\ 2\ 3)$ and $\pi((1\ 3\ 2)) = (1\ 3\ 2)$
- $\pi(\sigma) = e$ for all 2-cycles σ

The map π fails to be a homomorphism because $(1\ 3)(1\ 2) = (1\ 2\ 3)$ but

- $\pi((1\ 3))\pi((1\ 2)) = ee = e$
- $\pi((1\ 2\ 3)) = (1\ 2\ 3)$

Hence $\pi((1\ 3))\pi((1\ 2)) \neq \pi((1\ 3)(1\ 2))$, so π cannot be a homomorphism.

Proposition 5.2.4. *Let G and H be groups with $\theta : G \to H$ a homomorphism. Then:*

(i) $\theta(e_G) = e_H$

(ii) $\theta(g^m) = (\theta(g))^m$ *for all $g \in G$ and all $m \in \mathbb{Z}$*

(iii) $\mathrm{Im}(\theta) \leq H$ [Note: in general $\mathrm{Im}(\theta) \not\trianglelefteq H$]

(iv) $\mathrm{Ker}(\theta) \trianglelefteq G$

Proof. You will prove each of these things on a problem sheet. □

An *isomorphism* is a bijective homomorphism between two groups. If there is an isomorphism between groups G and H, they are essentially the same group, and we write $G \cong H$. We will explore isomorphisms in detail in the next subsection.

5.2.1 Handout for Section 5.2

Example 5.2.5. Here is a homomorphism. Recall that:
$S_3 = \{e, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$
$S_2 = \{e, (1\ 2)\}$
Consider the map $\phi : S_3 \to S_2$ given by

- $\phi(e) = e$
- $\phi((1\ 2\ 3)) = e$ and $\phi((1\ 3\ 2)) = e$
- $\phi((1\ 2)) = (1\ 2)$ and $\phi((1\ 3)) = (1\ 2)$ and $\phi((2\ 3)) = (1\ 2)$

We can check this is a homomorphism by checking all the cases.

- If $a, b \in S_3$ and one is equal to e then it is easy to see that $\phi(ab) = \phi(a)\phi(b)$
- If $a, b \in S_3$ and both are 3-cycles then it is easy to see that $\phi(ab) = \phi(a)\phi(b)$
- If $a, b \in S_3$ and one is a 3-cycle and the other is a 2-cycle then (check this!) ab is always a 2-cycle. Since the image (under ϕ) of any 2-cycle is equal to $(1\ 2)$ we have that $\phi(ab) = (1\ 2)$. On the other hand, $\phi(a)\phi(b)$ is equal to $e(1\ 2)$ or $(1\ 2)e$ and so $\phi(a)\phi(b) = (1\ 2)$. Therefore $\phi(ab) = \phi(a)\phi(b)$.
- If $a, b \in S_3$ and both are 2-cycles, then $ab \in \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ and so $\phi(ab) = e$. On the other hand $\phi(a)\phi(b) = (1\ 2)(1\ 2) = e$. Therefore $\phi(ab) = \phi(a)\phi(b)$.

We have checked all the cases, so ϕ is a homomorphism.

- $\mathrm{Ker}(\phi) = \{\mathrm{e}, (1\ 2\ 3), (1\ 3\ 2)\} = \mathrm{C}_3$, so again ϕ is not one-to-one
- $\mathrm{Im}(\phi) = \{\mathrm{e}, (1\ 2)\} = \mathrm{S}_2$.