Contents

Foreword

The course FMA_3F003_EP is a continuation of the Discrete Mathematics and of the second year Algebra courses. There the basic algebraic structures (groups, rings, fields) were introduced. In this course we will go deeper into the understanding of those structures and their relationships, and we will see some geometric and arithmetical situations in which they arise.

All pictures of mathematicians in these course notes are taken from Wikipedia.

Chapter 1

Introduction to Group Theory

1.1 Definitions and Examples

Definition 1.1.1

A **group** is a set G endowed with a binary operation:

$$G \times G \to G$$
$$(g_1, g_2) \mapsto g_1 g_2$$

called the **group law** of G and satisfying the following conditions:

(G1) *Associativity:*

$$\forall (g_1, g_2, g_3) \in G^3, \quad (g_1 g_2) g_3 = g_1 (g_2 g_3). \tag{1.1}$$

(G2) *Identity:* there is an element $e \in G$ such that:

$$\forall g \in G, \quad g = eg = ge. \tag{1.2}$$

The element e is called the **identity element** of G and is often denoted by 1_G or simply by 1.

(G3) *Inverse:* for each $g \in G$, there is an element $h \in G$ such that:

$$e = gh = hg. \tag{1.3}$$

The element h is called an **inverse** of g.

A group G is said to be **abelian** (or **commutative**) if $gh = hg$ for all $g, h \in G$. In that case, the operation on G is generally denoted additively and the identity element by 0_G.

Remark 1.1.2. Let G be a group. As we saw in the previous courses (and/or in Tutorial 1), G has a unique identity, and every $g \in G$ has a unique inverse. We will denote the inverse of $g \in G$ by g^{-1}. If G is an abelian group, the inverse of $g \in G$ is often denoted by $-g$.

Example 1.1.3.

(i) The pair $(\mathbb{Z}, +)$ is an abelian group.

(ii) For each $n > 0$, the pair $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group.

(iii) For each field K (e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), the pairs $(K, +)$ and $(K^\times, \times)$ are abelian groups.

(iv) Let K be a field and n a positive integer.

1. The set of invertible $n \times n$ matrices with coefficients in K endowed with matrix multiplication is a group, called the **general linear group** and denoted $GL_n(K)$ or $GL(n,K)$. This group is not abelian for $n \geq 2$. More generally, if K is a field and V is any K-vector space, the set of K-linear automorphisms $GL(V)$ of V endowed with composition is a group.
2. The $\{A \in GL_n(K) \mid \det(A) = 1\}$ endowed with matrix multiplication is a group called the **special linear group** and denoted either by $SL_n(K)$ or $SL(n,K)$.

(v) Given a set X, the set $\mathrm{Sym}(X) := \{f : X \to X \mid f \text{ is a bilection}\}$ of bijections from X to X endowed with composition is a group. It is called the **symmetric group on** X.

(v') When $X = X_n := \{1,...,n\}$, the group $\mathrm{Sym}(X_n)$ is denoted by $\mathscr{S}_n$ and is called the **symmetric group** of degree n or the symmetric group on n letters. Let us recall few facts about $\mathscr{S}_n$ that we learned in the previous courses.

An element $\sigma \in \mathscr{S}_n$ is called a **permutation** and is often denoted by:

$$\begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}.$$

Given r pairwise distinct integers $a_1,...,a_r$ in $\{1,2,...,n\}$, the permutation that sends a_i to a_{i+1} for $1 \leq i \leq r-1$, that sends a_r to a_1, and that fixes all other elements of $\{1,2,...,n\}$ is also denoted by:

$$(a_1\ a_2\ ...\ a_r)$$

and is called an r**-cycle** or a cycle of length r. Its inverse if again an r-cycle, $(a_r\ ...\ a_2\ a_1)$.

• Any permutation in S_n can be written as a product of disjoint cycles (i.e., cycles with disjoint supports) in a unique way up to the order.

• For $n \geq 3$, the symmetric group $\mathscr{S}_n$ is not abelian. For instance, we have:

$$(1\ 2)(2\ 3) = (1\ 2\ 3) \neq (1\ 3\ 2) = (2\ 3)(1\ 2).$$

Notation 1.1.4. Let G be a group and $g \in G$. We define $g^0 = 1_G$. For $n \in \mathbb{N}$, $n \geq 1$, we define inductively $g^1 = g$ and $g^{n+1} = g^n g$. Also, we define g^{-n} to be the inverse of g^n.

Definition 1.1.5

Let G be a group. If G is finite, $|G|$ is the number of elements of G and is called the **order** of G.
Let $g \in G$. The **order** of g denoted by $|g|$ or $o(g)$ is the least positive integer n such that $g^n = 1_G$, if such n exists. If there is no such n, then g has an infinite order.

Exercise 1.1.6. If $g \in G$, prove that $o(g) = 1$ if and only if $g = 1_G$.

Example 1.1.7. (1) The group $(\mathbb{Z}, +)$ is infinite and if $g \in \mathbb{Z} \setminus \{0\}$, then g has infinite order.

(2) For each $n > 0$, the group $(\mathbb{Z}/n\mathbb{Z}, +)$ is finite of order n.

(3) The group $\mathscr{S}_n$ is finite of order $n!$.

(4) Let $n \geq 3$ be an integer. In the plane $\mathbb{R}^2$, consider a regular n-gon P_n with center $(0,0)$. The set D_{2n} of isometries of P_n (under the operation of compoisition) forms a group called the **dihedral group** of order $2n$. Let us find its elements.

Observe first that the (counterclockwise) rotation r through the angle $\frac{2\pi}{n}$ about $(0,0)$ is in D_{2n}. Hence we get n rotations in D_{2n}:

$$1, r, r^2, ..., r^{n-1}$$

Let A be a fixed vertex of P, the reflection s with respect to the line passing through A and the center of P is in D_{2n}. Then D_{2n} also contains the following n symmetries:

$$s, rs, r^2 s, ..., r^{n-1} s.$$

Let's check that $D_{2n} = \{1, r, r^2, ..., r^{n-1}, s, rs, r^2 s, ..., r^{n-1} s\}$.

To do so, denote by $A_0 = A, A_1 ..., A_{n-1}$ the vertices of P in clockwise order and fix an element $\sigma \in D_{2n}$. Let $i \in \{0, ..., n-1\}$ be such that $\sigma(A_0) = A_i$ and set $\tau := r^i \sigma$. We have $\tau(A_0) = A_0$. Since τ preserves distances,

$$\tau(A_1) \in \{A_1, A_{n-1}\}.$$

If $\tau(A_1) = A_1$, then τ fixes both A_0 and A_1: hence $\tau = 1$ and $\sigma = r^{-i}$.

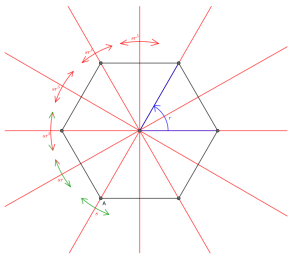
If $\tau(A_1) = A_{n-1}$, then $s\tau$ fixes both A_0 and A_1: hence $s\tau = 1$ and $\sigma = r^{-i} s$.

Since $o(r) = n$, in all cases, $\sigma \in \{1, r, r^2, ..., r^{n-1}, s, rs, r^2s, ..., r^{n-1}s\}$, and hence:

$$D_{2n} = \{1, r, r^2, ..., r^{n-1}, s, rs, r^2s, ..., r^{n-1}s\}.$$

Observe that $r^i r^{n-i} = 1$, $r^i s = sr^{n-i}$ and $(r^i s)^2 = r^i sr^i s = r^i ssr^{n-i} = 1$. One can conclude that D_{2n} is indeed a group of order $2n$. Also remark that $o(r^i s) = 2$ and $r^i s$ is a reflection for all $0 \leq i < n$.

(4a) If $n = 6$, P_n is a regular hexagon.



In this case the group D_{12} contains six rotations and six reflections.

Definition 1.1.8

A group G is called **cyclic** if there exists $g \in G$ such that for every $h \in G$, $h = g^k$ for some $k \in \mathbb{Z}$. In this case g is called a generator of G.

Example 1.1.9.

1. The group $(\mathbb{Z}, +)$ is an infinite cyclic group, $g_1 = 1$ is a generator of $\mathbb{Z}$, $g_2 = -1$ is a generator of $\mathbb{Z}$.
2. For $n \geq 1$, $(\mathbb{Z}/n\mathbb{Z}, +)$ is a cyclic group of order n.

Definition 1.1.10

Let G and H be two groups.
A **group homomorphism** (or a **group morphism**) from G to H is a map $f : G \to H$ such that:

$$\forall (g_1, g_2) \in G^2, f(g_1 g_2) = f(g_1) f(g_2).$$

If f is bijective, then its inverse is also a homomorphism and we say that f is an **isomorphism**. Two groups G and H are called **isomorphic** if there exists an isomorphism between them. In this case we write $G \cong H$.

Finally, if $G = H$ and $f : G \to G$ is an isomorphism, we say that f is an **automorphism** of G.

Exercise 1.1.11. If $f : G \to H$ is a group homomorphism, show that $f(1_G) = 1_H$ and for all $g \in G$, $f(g^{-1}) = f(g)^{-1}$.

The following proposition gives a useful criterion to check whether a homomorphism is injective:

Proposition 1.1.12

Let G and H be two groups, and let $f : G \to H$ be a homomorphism. Define the **kernel** of f by

$$\ker(f) := f^{-1}(\{1_H\}) = \{g \in G \mid f(g) = 1_H\}.$$

Then f is injective if, and only if, $\ker(f) = \{1\}$.

Proof. Assume that $\ker(f) = \{1\}$ and let x and y be elements of G such that $f(x) = f(y)$. Then $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = 1$ and so $xy^{-1} \in \ker(f)$. Then $xy^{-1} = 1$ and $x = y$. This settles the injectivity of f. The converse follows immediately from the definition of injectivity and the fact that $f(1) = 1$. □

Exercise 1.1.13. Prove that any two infinite cyclic groups are isomorphic. Moreover, prove that if G and H are two cyclic groups with $|G| = |H| = n$, $n \geq 1$, then $G \cong H$.

Example 1.1.14.

1. The exponential map:

$$\begin{aligned} \exp : \mathbb{C} &\to \mathbb{C}^\times \\ z &\mapsto e^z \end{aligned}$$

   is a surjective group homomorphism. Its kernel is $2\pi i\mathbb{Z}$.

2. For $n \geq 2$, the signature map $\operatorname{sign} : \mathscr{S}_n \to \{-1, 1\}$ is a surjective group homomorphism. Its kernel is the **alternating group** $\mathscr{A}_n$.

3. Let K be a field and let $n \geq 1$ be an integer. The determinant map

$$\det : GL_n(K) \to K^\times$$

   is a surjective group homomorphism. Its kernel is $SL_n(K)$.

4. The group homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ are the maps $n \mapsto an$ for $a \in \mathbb{Z}$.

5. Let G be a group and let $n \in \mathbb{Z}$ be an integer. The map:

$$\begin{aligned} G &\to G \\ g &\mapsto g^n \end{aligned}$$

is a group homomorphism if G is abelian, but not in general.

6. Let G be a group. Given $g \in G$, the map $\phi_g : G \to G$ such that

$$\phi_g(h) = ghg^{-1}$$

for $h \in G$, is a group automorphism. Such an automorphism is called an **inner** automorphism of G (Tutorial Sheet 1).

1.2 Subgroups

Definition 1.2.1

Let G be a group. A **subgroup** of G is a subset H of G such that the group law $G \times G \to G$ restricts to a group law $H \times H \to H$.
If H is a subgroup of G, we will write $H \leq G$.

Remark 1.2.2. Equivalently, a subset H of G is a subgroup of G if

$$\begin{gathered} 1_G \in H, \\ \forall (h_1, h_2) \in H^2, \quad h_1 h_2 \in H, \\ \forall h \in H, \quad h^{-1} \in H. \end{gathered}$$

Example 1.2.3.

1. The subgroups of $\mathbb{Z}$ are the subsets of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

2. The subgroups of $\mathbb{Z}/n\mathbb{Z}$ are the subsets of form $\{[0], [d], [2d], ..., [n-d]\}$ with d a divisor of n.

3. If K is a field and $n \in \mathbb{N}^*$, $SL_n(\mathbb{F}) \leq GL_n(\mathbb{F})$.

4. Let G and M be two groups and $f : G \to M$ a homomorphism.
Then $\ker(f) \leq G$ and $\mathrm{im}(f) \leq M$.

   For instance, the special linear group $SL_n(K)$ is a subgroup of $GL_n(K)$ since it is the kernel of the determinant map, and the alternating group $\mathscr{A}_n$ is a subgroup of $\mathscr{S}_n$ since it is the kernel of the signature map.

5. Let $f : G \to M$ be a group homomorphism. If $H \leq G$, then $f(H) \leq M$. Also, if $K \leq M$, then $f^{-1}(K) = \{g \in G \mid f(g) \in K\}$ is a subgroup of G.

6. Let $(G_i)_{i \in I}$ be a family of subgroups of a group G. Then the intersection of all the G_i is a subgroup of G. Note however that the union need not be a subgroup of G.

The following lemma gives us a quicker way to check whether a non-empty subset of a group is a subgroup.

Lemma 1.2.4

Let G be a group. If H is a non-empty subset of G, then H is a subgroup of G iff for all $a, b \in H$, $ab \in H$ and $a^{-1} \in H$.

Proposition 1.2.5

Let G be a group and let A be a subset of G. There exists a smallest subgroup H of G containing A. It is called the **subgroup generated by** A and it is usually denoted by $\langle A \rangle$.

Proof. Let H be the intersection of all subgroups of G containing A. It is a subgroup of G containing A and every other subgroup of G containing A contains H. Hence it is the smallest subgroup of G containing A. □

Remark 1.2.6. More explicitly, if $A \neq \emptyset$, the subgroup $\langle A \rangle$ can be described as the set S of elements of G that can be written as $g_1^{\epsilon_1} ... g_r^{\epsilon_r}$ for some $r \in \mathbb{N}$, some $\epsilon_1, ..., \epsilon_r \in \{-1, 1\}$ and some $g_1, ..., g_r \in A$. If $A = \emptyset$, $\langle A \rangle = \{1_G\}$.

Example 1.2.7.

1. If G is a cyclic group and g is a generator of G, then $G = \langle g \rangle$.

2. Let $a_1, ..., a_r$ be r integers. The subgroup of $\mathbb{Z}$ generated by $a_1, ..., a_r$ is:

$$a_1\mathbb{Z} + ... + a_r\mathbb{Z} = \gcd(a_1, ..., a_r)\mathbb{Z}.$$

3. The group $\mathcal{S}_3$ is generated by the elements:

$$\sigma = (1\,2\,3), \quad \tau = (1\,2).$$

Indeed, one can easily check that $\mathcal{S}_3 = \{\mathrm{Id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$. More generally, the following sets generate the symmetric group $\mathcal{S}_n$:

- the set of all transpositions;
- the set $\{(1\,2), (2\,3), ..., ((n-1)\ n)\}$.
- the transposition $(1\,2)$ and the cycle $(1\,2\,...\,n)$.

The alternating group $\mathscr{A}_n$ is generated by the set of 3-cycles. See Tutorial Sheet 2 for more details.

4. The dihedral group D_{2n} is generated by the rotation r and a reflection s. These two generators satisfy the relations $r^n = s^2 = 1$ and $srs^{-1} = r^{-1}$.

5. Consider the following complex matrices:

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Observe that:

$$A^4 = I_2, \quad A^2 = B^2, \quad BA = A^3B.$$

The subgroup of $GL_2(\mathbb{C})$ generated by A and B is:

$$\{I_2, A, A^2, A^3, B, AB, A^2B, A^3B\}.$$

It is called the **quaternion group** and will be denoted by Q_8. It can also be described as the 8-element group $\{\pm 1, \pm i, \pm j, \pm k\}$ subject to the following relations:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad ki = -ik = j, \quad jk = -kj = i.$$

1.2.1 Cosets

Let G be a group and H a subgroup of G. Define a relation $\mathscr{R}$ on G by:

$$x \mathscr{R} y \Leftrightarrow x^{-1}y \in H.$$

We have checked in class that this is an equivalence relation and that given $x \in G$, the equivalence class of x is the set

$$xH = \{xh | h \in H\},$$

which is called a **left coset** of H in G. The set of all left cosets of H in G is usually denoted by G/H. The number of distinct left cosets is denoted by $|G : H|$ and is called the **index** of H in G.

Remark 1.2.8. One can also define an equivalence relation:

$$x\mathscr{R}'y \Leftrightarrow xy^{-1} \in H.$$

In this case, the equivalence class of an element $x \in G$ for $\mathscr{R}'$ is

$$Hx = \{hx | h \in H\}$$

called a **right coset** of H in G. The set of all right cosets of H in G is usually denoted by $H\backslash G$.

One can define a bijection between G/H and $H\backslash G$ by:

$$\begin{aligned} G/H &\to H\backslash G \\ xH &\mapsto Hx^{-1}. \end{aligned}$$

Exercise 1.2.9. Check that this is indeed a bijection.

Theorem 1.2.10 – Lagrange's theorem

Let G be a finite group and let H be any subgroup of G. Then:

$$|G| = |H| \cdot |G : H|.$$

Proof. The left cosets form a partition of G, so that:

$$|G| = \sum_{Y \in G/H} |Y|.$$

But, for each $x \in G$, there is a bijection:

$$\begin{aligned} H &\to xH \\ h &\mapsto xh, \end{aligned}$$

and hence each left coset has $|H|$ elements. We deduce that:

$$|G| = \sum_{Y \in G/H} |H| = |G : H| \cdot |H|.$$

□

Joseph-Louis Lagrange (Turin 1736 - Paris 1813)

Corollary 1.2.11

Let G be a finite group and let $x \in G$. The order of x divides $|G|$.

Proof. Apply Lagrange's theorem to $H = \langle x \rangle$. □

1.3 Normal Subgroups and Quotient Groups

Definition 1.3.1

Let G be a group and let N be a subgroup of G. Then N is called a **normal** subgroup of G if for all $g \in G$,

$$gN = Ng$$

If N is a normal subgroup of G, we will write either $N \triangleleft G$ or $N \trianglelefteq G$.

Example 1.3.2. 1. If G is a group, the subgroups $\{1_G\}$ and G are both normal subgroups of G.

2. If G is an abelian group and N is a subgroup of G, then $N \trianglelefteq G$.

3. Let $G = S_3$. Then $N = \{1, (1,2,3), (3,2,1)\} \trianglelefteq G$, while subgroup $H = \{1, (1,2)\}$ is not normal in G.

In fact, there is a different way to decide whether a given subgroup is normal or not.

Proposition 1.3.3

Let G be a group and N a subgroup of G. Then N is a normal subgroup of G if and only if for all $g \in G$ and $n \in N$, $gng^{-1} \in N$.

Proof. Let N be a normal subgroup of G. Take any $g \in G$ and $n \in N$. Then $gN = Ng$, and so $gn \in gN = Ng$. Thus there exists $n' \in N$ such that $gn = n'g$, and so $gng^{-1} = n' \in N$.

Assume now that $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. Then for any $gn \in gN$, as $gng^{-1} \in N$, there exists $n_1 \in N$ with $gng^{-1} = n_1$. Hence, $gn = n_1 g \in Ng$, and so $gN \subseteq Ng$. Now, $g^{-1}ng \in N$ and so there exists $n_2 \in N$ such that $g^{-1}ng = n_2$. Hence, $ng = gn_2 \in gN$, and so $Ng \subseteq Ng$. Thus $gN \subseteq Ng$ and $Ng \subseteq gN$, and so $gN = Ng$. □

Example 1.3.4. 1. For $n \in \mathbb{N}$, $n \geq 1$, $A_n \trianglelefteq S_n$.

2. Let $n \in \mathbb{N}$, $n \geq 1$. Then $SL(n,\mathbb{R}) \trianglelefteq GL(n,\mathbb{R})$.

These examples can be generalised in the following way.

Lemma 1.3.5

Let $f : G \to M$ be a group homomorphism. Then $\ker(f) \trianglelefteq G$.

Proof. Let $f : G \to M$ be a group homomorphism. We have seen last time that a kernel of a homomorphsim is a subgroup of G. Now take any $g \in G$ and any $k \in \ker(f)$ and consider gkg^{-1}. Since $f(k) = 1$, we have

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)f(k)f(g)^{-1} = f(g)1_H f(g)^{-1} = 1_H,$$

and so $gkg^{-1} \in \ker(f)$. Using Proposition 1.3.3, we obtain that $\ker(f) \trianglelefteq G$. □

Notation 1.3.6. Let G be a group and $A \subseteq G$ and $B \subseteq G$. Then

$$AB := \{ab \mid a \in A, b \in B\}$$

Lemma 1.3.7

Let G be a group and N a normal subgroup of G. Then for $x, y \in G$,

$$(Nx)(Ny) = N(xy)$$

Proof. Take any $x, y \in G$ and $n, n_1, n_2 \in N$. Then $(n_1x)(n_2y) = n_1(xn_2)y$. Now $xn_2 \in xN = Nx$ (as $N \lhd G$), and so there exists $n_2' \in N$ such that $xn_2 = n_2'x$. Therefore $n_1(xn_2)y = n_1(n_2'x)y = (n_1n_2')(xy)$. We conclude that $(Nx)(Ny) \subseteq N(xy)$.

Now $n(xy) = (nx)(1_Gy) \in (Nx)(Ny)$, and so $N(xy) \subseteq (Nx)(Ny)$.

We may now conclude that $(Nx)(Ny) = N(xy)$. □

Remark 1.3.8. Observe that in the proof Lemma 1.3.7, we used the fact that N was a normal subgroup of G. Can you think of an example of a group and a subgroup for which Lemma 1.3.7 does not hold?

Theorem 1.3.9

Let G be a group and let N be a normal subgroup of G. Then the set of cosets of N in G forms a group under the operation of multiplication of cosets. We denote this group by G/N and call it the **quotient group** of G by N.

Proof. As we in Lemma 1.3.7, the set G/N of cosets of N in G is indeed closed under the operation of multiplication of cosets. Now it is easy to check that this operation is associative (check!). Also, as $N = N1_G$, for all $x \in G$, we have

$$(N1_G)(Nx) = N(1_Gx) = Nx = N(x1_G) = (Nx)(N1_G)$$

and

$$(Nx)(Nx^{-1}) = N(xx^{-1}) = N = N(x^{-1}x) = (Nx^{-1})(Nx).$$

Therefore, G/N is a group under multiplication of cosets with

$$1_{G/N} = N \text{ and } (Nx)^{-1} = Nx^{-1}.$$

□

Remark 1.3.10. If G is a finite group and $N \trianglelefteq G$, Lagrange's Theorem implies that that $|G/N| = |G : N| = \frac{|G|}{|N|}$.

Theorem 1.3.11 – First Isomorphism Theorem

Let $f : G \to M$ be a group homomorphism with kernel $\ker(f) := K$. Then $K \trianglelefteq G$ and

$$G/K \cong Im(f)$$

More precisely, there is an isomorphism $\overline{f} : G/K \to Im(f)$ defined by $\overline{f}(Kg) = f(g)$ for all $g \in G$.

Proof. Let us first show that $\overline{f}$ is well-defined. Take any $x, y \in G$ with $Kx = Ky$. Then $\overline{f}(Kx) = f(x)$ and $\overline{f}(Ky) = f(y)$. Since $Kx = Ky$, $x = ky$ for some $k \in K$. Hence, $f(x) = f(ky) = f(k)f(y) = 1_M f(y) = f(y)$ and so, indeed, $\overline{f}(Kx) = \overline{f}(Ky)$. Now

$$\overline{f}((Kx)(Ky)) = \overline{f}(K(xy)) = f(xy) = f(x)f(y) = \overline{f}(Kx)\overline{f}(Ky)$$

for all $Kx, Ky \in G/K$, and so $\overline{f}$ is a homomorphism. Since $Im(\overline{f}) = Im(f)$, $\overline{f}$ is surjective, and as $\ker(\overline{f}) = \{Kx \mid f(x) = 1_M\} = \{Kx \mid x \in K\} = \{1_{G/K}\}$, f is injective. Thus $\overline{f}$ is an isomorphism. □

Lemma 1.3.12

Let G be a group and N a normal subgroup of G. Then the map

$$\pi : G \to G/N$$

defined by $\pi(g) = Ng$ is a surjective homomorphism with kernel N.
This map is called the **natural homomorphism** from G to G/N.

Proof. Take any $x, y \in G$. Then $\pi(xy) = N(xy) = (Nx)(Ny) = \pi(x)\pi(y)$ and so π is a homomorphism. Finally,

$$\ker(\pi) = \{g \in G \mid \pi(g) = 1_{G/N}\} = \{g \in G \mid Ng = N\} = N.$$

□

Theorem 1.3.13 – Second Isomorphism Theorem

Let G be a group, $N \trianglelefteq G$ and $H \leq G$. Then the following conditions hold:

1. $NH \leq G$,
2. $N \cap H \trianglelefteq H$, and

3. $NH/N \cong H/(N \cap H)$.

Proof. As $N \subseteq NH$, $NH \neq \emptyset$. Take any $n_1h_1, n_2h_2 \in NH$. Then

$$(n_1h_h)(n_2h_2) \in Nh_1Nh_2 = N(h_1h_2) \subseteq NH$$

and

$$(n_1h_1)^{-1} = h_1^{-1}n_1^{-1} = (h_1^{-1}n_1^{-1}h_1)h_1^{-1} \in Nh_1^{-1} \subseteq NH$$

proving that $NH \leq G$.

Take the natural map $\pi : G \to G/N$, and consider its restriction to H:

$$\pi_H : H \to G/N.$$

Then π_H is a homomorphism, $Im(\pi_H) = \{Nh \mid h \in H\} = NH/N$. Finally,

$$\ker(\pi_H) = \ker(\pi) \cap H = N \cap H.$$

Therefore, by the First Isomorphism Theorem, $N \cap H \trianglelefteq H$ and $H/(N \cap H) \cong NH/H$. □