Chapter 1

Revision

In this first chapter we mostly will recall definitions and results from earlier lecture courses. There will be only a few new results, and these are clearly marked in these notes. Proofs of results from MT4003 will often be omitted (though these notes will contain them). We will also establish the notation to be used throughout the course. In a number of places the notation will be slightly different from some of the earlier courses, but this is in the interests of agreeing with the majority of group theory textbooks.

1.1 Basic axioms

Definition 1.1 A *group* G is a set with a binary operation (usually written multiplicatively)

$$\begin{aligned} G \times G &\to G \\ (x, y) &\mapsto xy \end{aligned}$$

such that

(i) the binary operation is *associative*:

$$x(yz) = (xy)z \qquad \text{for all } x, y, z \in G;$$

(ii) there is an *identity element* 1 in G:

$$x1 = 1x = x \qquad \text{for all } x \in G;$$

(iii) each element x in G possesses an *inverse* x^{-1}:

$$xx^{-1} = x^{-1}x = 1.$$

Comments:

(i) We have omitted the "closure" axiom. The reason for this is that this condition is actually built into the definition of a binary operation. A binary operation takes two elements of our group and creates a third element *in the group*, and so we have closure automatically.

(ii) Associativity ensures that we can safely omit brackets from a product $x_1x_2\dots x_n$ of n elements $x_1, x_2, \dots, x_n$ of a group. Thus, for example, the following products are all equal:

$$x_1(x_2(x_3x_4)), \qquad (x_1(x_2x_3))x_4, \qquad ((x_1x_2)x_3)x_4, \qquad \text{etc.}$$

(iii) We can define powers x^n where $x \in G$ and $n \in \mathbb{Z}$. Standard power laws hold although we need to remember that in general group elements do not commute (so, for example, we cannot easily expand $(xy)^n$) although we can expand the following inverse:

$$(xy)^{-1} = y^{-1}x^{-1}.$$

[Proof [Omitted in lectures]:

$$(y^{-1}x^{-1})(xy) = y^{-1}x^{-1}xy = y^{-1}1y = y^{-1}y = 1,$$

so multiplying on the right by the inverse of xy yields $y^{-1}x^{-1} = (xy)^{-1}$.]

For completeness, recall the following:

Definition 1.2 A group G is called *abelian* if all its elements *commute*; that is, if

$$xy = yx \qquad \text{for all } x, y \in G.$$

Example 1.3 The integers $\mathbb{Z}$ form an abelian group under addition, as $a + b = b + a$. The permutations $(1, 2)$ and $(1, 3)$ satisfy

$$(1,2)(1,3) = (1,2,3), \quad (1,3)(1,2) = (1,3,2),$$

so any group containing them (such as S_n for $n \geq 3$) is nonabelian.

1.2 Subgroups

Although we might initially be tempted to attack groups by examining their elements, this turns out not to be, for most purposes, a good idea. Even a moderately sized group has an extremely large multiplication table. Instead, one needs to find some sort of "structure" to study, and this is provided by

subgroups and quotient groups. To study quotient groups, we will need to study homomorphisms.

A subgroup of a group is a subset which is itself a group under the multiplication inherited from the larger group. Thus:

Definition 1.4 A subset H of a group G is a *subgroup* of G if

(i) H is non-empty,

(ii) $xy \in H$ for all $x, y \in H$,

(iii) $x^{-1} \in H$ for all $x \in H$.

We write $H \leqslant G$ to indicate that H is a subgroup of G. If G is a group, the set containing the identity element (which we denote by $\mathbf{1}$) and the whole group are always subgroups: $\mathbf{1}$ is the *trivial* subgroup of G, and G is an *improper* subgroup of itself. We shall usually be interested in finding proper nontrivial subgroups.

We mention in passing that the above conditions for a subset to be a subgroup are not the only ones used, but they are sufficient for our needs (and easily memorable).

The identity element of G lies in every subgroup, so it is easy to see that the conditions of Definition 1.4 are inherited by intersections. Therefore:

Lemma 1.5 *If $\{ H_i \mid i \in I \}$ is a collection of subgroups of a group G, then $\bigcap_{i\in I} H_i$ is also a subgroup of G.*

PROOF: [OMITTED IN LECTURES] We have $1 \in H_i$ for all i, so $\bigcap_{i\in I} H_i \neq \varnothing$. Now let $x, y \in \bigcap_{i\in I} H_i$. Then for each i, $x, y \in H_i$, so $xy \in H_i$ and $x^{-1} \in H_i$ since $H_i \leqslant G$. We deduce that $xy \in \bigcap_{i\in I} H_i$ and $x^{-1} \in \bigcap_{i\in I} H_i$. Thus the intersection is a subgroup. □

In general, the union of a family of subgroups of a group is not itself a subgroup. The following construction gives us a way of making a subgroup that contains a given set of elements.

Definition 1.6 Let G be a group and X be a subset of G. The *subgroup of G generated by X* is denoted by $\langle X \rangle$ and is defined to be the intersection of all subgroups of G which contain X.

Lemma 1.5 ensures that $\langle X \rangle$ is a subgroup of G. It is the smallest subgroup of G containing X (in the sense that it is contained in all other such subgroups; that is, if H is any subgroup of G containing X then $\langle X \rangle \leqslant H$).

Lemma 1.7 *Let G be a group and X be a subset of G. Then*

$$\langle X \rangle = \{ x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} \mid n \geqslant 0,\ x_i \in X,\ \varepsilon_i = \pm 1 \text{ for all } i \}.$$

Thus $\langle X \rangle$ consists of all products of elements of X and their inverses.

PROOF: [OMITTED IN LECTURES] Let S denote the set on the right-hand side. Since $\langle X \rangle$ is a subgroup (by Lemma 1.5) and by definition it contains X, we deduce that $\langle X \rangle$ must contain all products of elements of X and their inverses. Thus $S \subseteq \langle X \rangle$.

On the other hand, S is non-empty (for example, it contains the empty product (where $n = 0$) which by convention is taken to be the identity element 1), it contains all elements of X (the case $n = 1$ and $\varepsilon_1 = 1$), is clearly closed under products and

$$(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n})^{-1} = x_n^{-\varepsilon_n} x_{n-1}^{-\varepsilon_{n-1}} \dots x_1^{-\varepsilon_1} \in S.$$

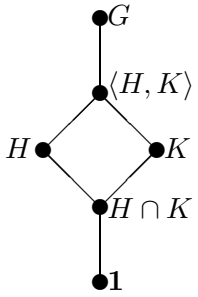
Hence S is a subgroup of G. The fact that $\langle X \rangle$ is the smallest subgroup containing X now gives $\langle X \rangle \leqslant S$ and we deduce the equality claimed in the lemma. □

Example 1.8 Let $G = \mathrm{S}_3$. Then $\{(1,2),(2,3)\}$ is a subset of G. Let's compute $\langle (1,2),(2,3) \rangle$:

$$\begin{gathered}(1,2)(1,2) = \mathbf{1}, \quad (1,2)(2,3) = (1,3), \\ (1,2)(2,3)(1,2) = (1,3)(1,2) = (1,3,2) \\ (2,3)(1,2) = (1,2,3)\end{gathered}$$

We've made all elements of S_3 so $\langle (1,2),(2,3) \rangle = \mathrm{S}_3$.

We will wish to manipulate the subgroups of a group and understand how they relate to each other. Useful in such a situation are diagrams where we represent subgroups by nodes and use an upward line to denote inclusion. For example, the following illustrates the phenomena just discussed:



(For subgroups H and K of G, the intersection $H \cap K$ is the largest subgroup contained in both H and K, and $\langle H, K \rangle$ is the smallest subgroup containing both H and K.)

Before discussing more familiar concepts from previous courses, we prove a **new result** that is extremely useful when manipulating subgroups. To

state it, we need some notation. Let G be a group, and let A and B be subsets of G. Then we write AB for the set:

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

Lemma 1.9 (Dedekind's Modular Law) *Let G be a group and H, K and L be subgroups of G with $K \leqslant L$. Then*

$$HK \cap L = (H \cap L)K.$$

PROOF: $H \cap L \leqslant H$, so $(H \cap L)K \subseteq HK$. Also $H \cap L$ and K are contained in L, so $(H \cap L)K \subseteq L$ (since L is closed under products). Thus

$$(H \cap L)K \subseteq HK \cap L.$$

Now let $x \in HK \cap L$. Then $x = hk$ where $h \in H$ and $k \in K$. Now $h = xk^{-1} \in L$ since $x \in L$ and $k \in K \leqslant L$. Thus $h \in H \cap L$ and so $x = hk \in (H \cap L)K$. □

1.3 Cosets

Subgroups enforce a rigid structure on a group: specifically a group is the disjoint union of the cosets of any fixed subgroup.

Definition 1.10 Let G be a group, H be a subgroup of G and x be an element of G. The (*right*) *coset* of H with *representative* x is the subset

$$Hx = \{\, hx \mid h \in H \,\}$$

of G.

We can equally well define what is meant by a left coset, but we shall work almost exclusively with right cosets. Therefore, we will say 'coset' to mean 'right coset'.

Theorem 1.11 *Let G be a group and H be a subgroup of G.*

(i) *If $x, y \in G$, then $Hx = Hy$ if and only if $xy^{-1} \in H$.*

(ii) *Any two cosets of H are either equal or are disjoint: if $x, y \in G$, then either $Hx = Hy$ or $Hx \cap Hy = \varnothing$.*

(iii) *G is the disjoint union of the cosets of H.*

(iv) *If $x \in G$, the map $h \mapsto hx$ is a bijection from H to the coset Hx.*

PROOF: [OMITTED IN LECTURES] (i) Suppose $Hx = Hy$. Then $x = 1x \in Hx = Hy$, so $x = hy$ for some $h \in H$. Thus $xy^{-1} = h \in H$.

Conversely if $xy^{-1} \in H$, then $hx = h(xy^{-1})y \in Hy$ for all $h \in H$, so $Hx \subseteq Hy$. Also $hy = hyx^{-1}x = h(xy^{-1})^{-1}x \in Hx$ for all $h \in H$, so $Hy \subseteq Hx$. Thus $Hx = Hy$ under this assumption.

(ii) Suppose that $Hx \cap Hy \neq \varnothing$. Then there exists $z \in Hx \cap Hy$, say $z = hx = ky$ for some $h, k \in H$. Then $xy^{-1} = h^{-1}k \in H$ and we deduce $Hx = Hy$ by (i).

(iii) If $x \in G$, then $x = 1x \in Hx$. Hence the union of all the (right) cosets of H is the whole of G. Part (ii) ensures this is a disjoint union.

(iv) By definition of the coset Hx, the map $h \mapsto hx$ is a surjective map from H to Hx. Suppose $hx = kx$ for some $h, k \in H$. Then multiplying on the right by x^{-1} yields $h = k$. Thus this map is also injective, so it is a bijection, as claimed. □

Write $|G : H|$ for the number of cosets of H in G and call this the *index* of H in G. The previous result tells us that our group G is the disjoint union of $|G : H|$ cosets of H and each of these contain $|H|$ elements. Hence:

Theorem 1.12 (Lagrange's Theorem) *Let G be a group and H be a subgroup of G. Then*

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

In particular, if H is a subgroup of a finite group G, then the order of H divides the order of G. □

At this point we insert two **new results** about the index of subgroups. The first is frequently used while the second will be needed (much) later in the course.

Lemma 1.13 *Let H and K be subgroups of a group G with $K \leqslant H \leqslant G$. Then*

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

The proof of this is an exercise on Problem Sheet I.

Lemma 1.14 *Let G be a group and H and K be subgroups of G. Then*

$$|G : H \cap K| \leqslant |G : H| \cdot |G : K|.$$

Furthermore, if $|G : H|$ and $|G : K|$ are coprime, then

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

PROOF: Define a map from the set of cosets of $H \cap K$ to the Cartesian product of the sets of cosets of H and of K by

$$\phi\colon (H \cap K)x \mapsto (Hx, Kx).$$

Now

$$\begin{aligned}(H \cap K)x = (H \cap K)y \quad &\text{if and only if} \quad xy^{-1} \in H \cap K \\ &\text{if and only if} \quad xy^{-1} \in H \text{ and } xy^{-1} \in K \\ &\text{if and only if} \quad Hx = Hy \text{ and } Kx = Ky.\end{aligned}$$

So ϕ is well-defined and injective. Therefore

$$|G : H \cap K| \leqslant |G : H| \cdot |G : K|. \tag{1.1}$$

Now suppose that $|G : H|$ and $|G : K|$ are coprime (and hence finite). First note that Equation (1.1) tells us that tells us that $|G : H \cap K|$ is finite, and hence by Lagrange's Theorem 1.12 is an integer. We need to establish the reverse inequality. Now $H \cap K \leqslant H \leqslant G$, so

$$|G : H \cap K| = |G : H| \cdot |H : H \cap K|$$

by Lemma 1.13. It follows that $|G : H \cap K|$ is divisible by $|G : H|$. It is similarly divisible by $|G : K|$. As these integers are coprime, we deduce

$$|G : H| \cdot |G : K| \text{ divides } |G : H \cap K|.$$

This establishes the required reverse inequality and completes the proof when taken together with Equation (1.1). □

1.4 Orders of elements and Cyclic groups

Definition 1.15 If G is a group and x is an element of G, we define the *order* of x to be the smallest positive integer n such that $x^n = 1$ (if such exists) and otherwise say that x has *infinite order*.

We write $|x|$ for the order of the element x.

If $x^i = x^j$ for $i < j$, then $x^{j-i} = 1$, the element x has finite order, and $|x| \leqslant j - i$. In particular, the powers of x are all pairwise nonequal if x has infinite order.

If x has finite order n and $k \in \mathbb{Z}$, write $k = nq + r$ where $0 \leqslant r < n$. Then

$$x^k = x^{nq+r} = (x^n)^q x^r = x^r \tag{1.2}$$

(since $x^n = 1$). Furthermore $1, x, x^2, \ldots, x^{n-1}$ are distinct (by the first line of the previous paragraph). Hence:

Proposition 1.16 (i) *If $x \in G$ has infinite order, then the powers x^i (for $i \in \mathbb{Z}$) are distinct.*

(ii) *If $x \in G$ has order n, then x has precisely n distinct powers, namely $1, x, x^2, \ldots, x^{n-1}$.* □

Corollary 1.17 *Let G be a group and $x \in G$. Then*

$$|x| = |\langle x \rangle|.$$

If G is a finite group, then $|x|$ divides $|G|$. □

Equation (1.2) yields a further observation, namely:

$$x^k = 1 \qquad \text{if and only if} \qquad |x| \mid k.$$

In the case that a single element generates the whole group, we give a special name:

Definition 1.18 A group G is called *cyclic* (with *generator* x) if $G = \langle x \rangle$.

Using ideas as just described, it is reasonably easy to establish the following (and also a corresponding result for infinite cyclic groups):

Theorem 1.19 *Let G be a finite cyclic group of order n. Then G has precisely one subgroup of order d for every divisor d of n.*

The proof of this theorem can be found on Problem Sheet I.

1.5 Normal subgroups and quotient groups

Definition 1.20 A subgroup N of a group G is called a *normal subgroup* of G if $g^{-1}xg \in N$ for all $x \in N$ and all $g \in G$. We write $N \trianglelefteq G$ to indicate that N is a normal subgroup of G.

The element $g^{-1}xg$ is called the *conjugate* of x by g and is often denoted by x^g. We shall discuss this in greater detail in Section 2.

If $N \trianglelefteq G$, then we write G/N for the set of cosets of N in G:

$$G/N = \{\, Nx \mid x \in G \,\}.$$

Theorem 1.21 *Let G be a group and N be a normal subgroup of G. Define a binary operation on G/N by*

$$Nx \cdot Ny = Nxy$$

for $x, y \in G$. With this multiplication, G/N is a group.

PROOF: [OMITTED IN LECTURES] The part of this proof requiring the most work is to show that this product is actually well-defined. Suppose that $Nx = Nx'$ and $Ny = Ny'$ for some elements $x, x', y, y' \in G$. Then $x = ax'$ and $y = by'$ for some $a, b \in N$. Then

$$xy = (ax')(by') = ax'b(x')^{-1}x'y' = ab^{(x')^{-1}}x'y'.$$

Since $N \trianglelefteq G$, it follows that $b^{(x')^{-1}} \in N$. Hence $(xy)(x'y')^{-1} = ab^{(x')^{-1}} \in N$ and we deduce that $Nxy = Nx'y'$. This shows that the above multiplication of cosets is indeed well-defined.

It remains to show that the set of cosets forms a group under this multiplication. If $x, y, z \in G$, then

$$(Nx \cdot Ny) \cdot Nz = Nxy \cdot Nz = N(xy)z = Nx(yz) = Nx \cdot Nyz = Nx \cdot (Ny \cdot Nz).$$

Thus the multiplication is associative. We calculate

$$Nx \cdot N1 = Nx1 = Nx = N1x = N1 \cdot Nx$$

for all cosets Nx, so $N1$ is the identity element in G/N, while

$$Nx \cdot Nx^{-1} = Nxx^{-1} = N1 = Nx^{-1}x = Nx^{-1} \cdot Nx,$$

so Nx^{-1} is the inverse of Nx in G/N.

Thus G/N is a group. □

Definition 1.22 If G is a group and N is a normal subgroup of G, we call G/N (with the above multiplication) the *quotient group* of G by N.

We shall discuss quotient groups later in this section. They are best discussed, however, in the context of homomorphisms, so we shall move onto these in a moment. First we have a partially **new result**.

Recall that for any subsets A, B of a group G we define $AB = \{\, ab \mid a \in A,\ b \in B \,\}$.

Lemma 1.23 *Let G be a group and let H and K be subgroups of G. Then*

(i) *HK is a subgroup of G if and only if $HK = KH$;*

(ii) *if K is a normal subgroup of G then HK is a subgroup of G (and consequently $HK = KH$);*

(iii) *if H and K are normal subgroups of G, then $H \cap K$ and HK are normal subgroups of G;*

(iv) $|HK| \cdot |H \cap K| = |H| \cdot |K|$.

When H and K are finite, then we can rearrange the last formula to give

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

This holds even when HK is not a subgroup.

PROOF: (i), (ii), (iii) See Problem Sheet I.

(iv) Define a map $\alpha\colon H \times K \to HK$ by

$$(h,k) \mapsto hk.$$

Then α is surjective. Fix a point $x \in HK$, say $x = h_0k_0$ for some fixed $h_0 \in H$ and $k_0 \in K$. Then for $(h,k) \in H \times K$,

$$\begin{aligned}(h,k)\alpha = x \quad &\text{if and only if} \quad hk = h_0k_0\\ &\text{if and only if} \quad h_0^{-1}h = k_0k^{-1} \in H \cap K\\ &\text{if and only if} \quad h = h_0a,\ k = a^{-1}k_0 \quad \text{where } a \in H \cap K.\end{aligned}$$

Thus for each $x \in HK$, we see

$$\{\,(h,k) \in H \times K \mid (h,k)\alpha = x\,\} = \{\,(h_0a, a^{-1}k_0) \mid a \in H \cap K\,\}.$$

Hence we may partition $H \times K$ into $|HK|$ subsets, each corresponding to one point in HK and each of size $|H \cap K|$.

This proves

$$|H \times K| = |HK| \cdot |H \cap K|;$$

that is,

$$|H| \cdot |K| = |HK| \cdot |H \cap K|.$$

□

1.6 Homomorphisms

Definition 1.24 Let G and H be groups. A *homomorphism* from G to H is a map $\phi\colon G \to H$ such that

$$(xy)\phi = (x\phi)(y\phi) \qquad \text{for all } x, y \in G.$$

Thus a homomorphism between two groups is a map which preserves multiplication.

Note that we are writing maps on the right, as is conventional in much of algebra. This has two advantages: the first is that when we compose a number of maps we can read from left to right, rather than from right to left. The second is that it will make certain proofs easier to read.

Related to homomorphisms we have the following definition.

Definition 1.25 Let $\phi\colon G \to H$ be a homomorphism between two groups. Then the *kernel* of ϕ is

$$\ker\phi = \{\,x \in G \mid x\phi = 1\,\},$$

while the *image* of ϕ is

$$\operatorname{im}\phi = G\phi = \{\,x\phi \mid x \in G\,\}.$$

Note that $\ker\phi \subseteq G$ while $\operatorname{im}\phi \subseteq H$ here.

Lemma 1.26 *Let $\phi\colon G \to H$ be a homomorphism between two groups G and H. Then*

(i) $1\phi = 1$;

(ii) $(x^{-1})\phi = (x\phi)^{-1}$ *for all* $x \in G$;

(iii) *the kernel of ϕ is a normal subgroup of G;*

(iv) *the image of ϕ is a subgroup of H.*

PROOF: [OMITTED IN LECTURES] (i) $1\phi = (1 \cdot 1)\phi = (1\phi)(1\phi)$ and multiplying by the inverse of 1ϕ yields $1 = 1\phi$.

(ii) $(x\phi)(x^{-1}\phi) = (xx^{-1})\phi = 1\phi = 1$ and multiplying on the left by the inverse of $x\phi$ yields $(x^{-1})\phi = (x\phi)^{-1}$.

(iii) By (i), $1 \in \ker\phi$. If $x, y \in \ker\phi$, then $(xy)\phi = (x\phi)(y\phi) = 1 \cdot 1 = 1$ and $(x^{-1})\phi = (x\phi)^{-1} = 1^{-1} = 1$, so we deduce $xy \in \ker\phi$ and $x^{-1} \in \ker\phi$. Therefore $\ker\phi$ is a subgroup of G. Now if $x \in \ker\phi$ and $g \in G$, then $(g^{-1}xg)\phi = (g^{-1}\phi)(x\phi)(g\phi) = (g\phi)^{-1}1(g\phi) = 1$, so $g^{-1}xg \in \ker\phi$. Hence $\ker\phi$ is a normal subgroup of G.

(iv) Let $g, h \in \operatorname{im}\phi$. Then $g = x\phi$ and $h = y\phi$ for some $x, y \in G$. Then $gh = (x\phi)(y\phi) = (xy)\phi \in \operatorname{im}\phi$ and $g^{-1} = (x\phi)^{-1} = (x^{-1})\phi \in \operatorname{im}\phi$. Thus $\operatorname{im}\phi$ is a subgroup of G. □

The kernel is also useful for determining when a homomorphism is one-to-one, as the following **new result** shows.

Lemma 1.27 *Let $\phi\colon G \to H$ be a homomorphism between two groups G and H. Then ϕ is one-to-one if and only if* $\ker\phi = \mathbf{1}$.

PROOF: Suppose ϕ is one-to-one. If $x \in \ker\phi$, then $x\phi = 1 = 1\phi$, so $x = 1$. Hence $\ker\phi = \mathbf{1}$.

Conversely suppose that $\ker\phi = \mathbf{1}$. If $x\phi = y\phi$, then $(xy^{-1})\phi = (x\phi)(y\phi)^{-1} = 1$, so $xy^{-1} \in \ker\phi$. Hence $xy^{-1} = 1$ and, upon multiplying on the right by y, we deduce $x = y$. Hence ϕ is one-to-one. □

Example 1.28 Let G be a group and N be a normal subgroup of G. Define a map $\pi\colon G \to G/N$ by

$$\pi\colon x \mapsto Nx.$$

The definition of the multiplication in the quotient group G/N ensures that π is a homomorphism. It is called the *natural map* (or *canonical homomorphism*). We see

$$\ker\pi = \{\, x \in G \mid Nx = N1 \,\};$$

that is,

$$\ker \pi = N,$$

and clearly $\operatorname{im} \pi = G/N$; that is, π is surjective.

Thus, every kernel is a normal subgroup, and conversely every normal subgroup is the kernel of some homomorphism.

1.7 Isomorphism Theorems

We shall finish this chapter by discussing the four important theorems that relate quotient groups and homomorphisms. We shall need the concept of isomorphism, so we recall that first.

Definition 1.29 An *isomorphism* between two groups G and H is a homomorphism $\phi\colon G \to H$ which is a bijection. We write $G \cong H$ to indicate that there is an isomorphism between G and H, and we say that G and H are *isomorphic*.

What this means is that if G and H are isomorphic groups, then the elements of the two groups are in one-one correspondence in such a way that the group multiplications produce precisely corresponding elements. Thus essentially the groups are identical: we may have given the groups different names and labelled the elements differently, but we are looking at identical objects in terms of their structure.

Theorem 1.30 (First Isomorphism Theorem) *Let G and H be groups and $\phi\colon G \to H$ be a homomorphism. Then $\ker \phi$ is a normal subgroup of G, $\operatorname{im} \phi$ is a subgroup of H and*

$$G/\ker \phi \cong \operatorname{im} \phi.$$

Proof (Sketch): We already know that $\ker \phi \trianglelefteq G$, so we can form $G/\ker \phi$. The isomorphism is the map

$$(\ker \phi)x \mapsto x\phi \qquad (\text{for } x \in G).$$

□

Omitted details: Let $K = \ker \phi$ and define $\theta\colon G/K \to \operatorname{im} \phi$ by $Kx \mapsto x\phi$ for $x \in G$. We note

$$\begin{array}{lll} Kx = Ky & \text{if and only if} & xy^{-1} \in K \\ & \text{if and only if} & (xy^{-1})\phi = 1 \\ & \text{if and only if} & (x\phi)(y\phi)^{-1} = 1 \\ & \text{if and only if} & x\phi = y\phi. \end{array}$$

This shows that θ is well-defined and also that it is injective. By definition of the image, θ is surjective. Finally

$$\big((Kx)(Ky)\big)\theta = (Kxy)\theta = (xy)\phi = (x\phi)(y\phi) = (Kx)\theta \cdot (Ky)\theta$$

for all $x, y \in G$, so θ is a homomorphism. Hence θ is the required isomorphism. (All other parts of the theorem are found in Lemma 1.26.) $\square$

Rather than move straight on to the Second and Third Isomorphism Theorems, we consider the Correspondence Theorem next so that we can use it when talking about the other Isomorphism Theorems. The Correspondence Theorem tells us about subgroups of quotient groups.

Theorem 1.31 (Correspondence Theorem) *Let G be a group and let N be a normal subgroup of G.*

(i) *There is a one-one inclusion-preserving correspondence between subgroups of G containing N and subgroups of G/N given by*

$$H \mapsto H/N \qquad \text{whenever } N \leqslant H \leqslant G.$$

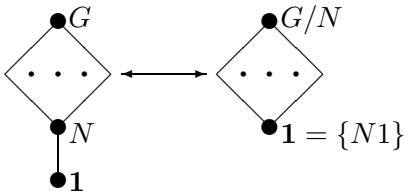
(ii) *Under the above correspondence, normal subgroups of G which contain N correspond to normal subgroups of G/N.*

Note we are saying that every subgroup of G/N has the form H/N where $N \leqslant H \leqslant G$. Specifically, if J is a subgroup of G/N, it corresponds to $H = \{\, x \in G \mid Nx \in J \,\}$ (the set of elements which are mapped into J by the natural map $G \to G/N$) and then $J = H/N$ for this H. Also part (ii) says:

$$H \trianglelefteq G \qquad \text{if and only if} \qquad H/N \trianglelefteq G/N$$

(for $N \leqslant H \leqslant G$).

If we view it that the 'structure' of a group is somehow the shape of the diagram of subgroups (with the normal subgroups indicated), then the Correspondence Theorem 1.31 tells us how the structures of a group and a quotient are related. The diagram of subgroups of the quotient group G/N is simply that part of the diagram of subgroups sandwiched between G and N.



PROOF: [OMITTED IN LECTURES] Let $\mathscr{S}$ denote the set of subgroups of G that contain N (that is, $\mathscr{S} = \{ H \mid N \leqslant H \leqslant G \}$) and let $\mathscr{T}$ denote the set of subgroups of G/N. Let $\pi\colon G \to G/N$ denote the natural map $x \mapsto Nx$.

First note that if $H \in \mathscr{S}$, then N is certainly also a normal subgroup of H and we can form the quotient group H/N. This consists of some of the elements of G/N and forms a group, so is a subgroup of G/N. Thus we do indeed have a map $\Phi\colon \mathscr{S} \to \mathscr{T}$ given by $H \mapsto H/N$. Also note that if $H_1, H_2 \in \mathscr{S}$ with $H_1 \leqslant H_2$, then we immediately obtain $H_1/N \leqslant H_2/N$, so Φ preserves inclusions.

Suppose $H_1, H_2 \in \mathscr{S}$ and that $H_1/N = H_2/N$. Let $x \in H_1$. Then $Nx \in H_1/N = H_2/N$, so $Nx = Ny$ for some $y \in H_2$. Then $xy^{-1} \in N$, say $xy^{-1} = n$ for some $n \in N$. Since $N \leqslant H_2$, we then have $x = ny \in H_2$. This shows $H_1 \leqslant H_2$ and a symmetrical argument shows $H_2 \leqslant H_1$. Hence if $H_1\Phi = H_2\Phi$ then necessarily $H_1 = H_2$, so Φ is injective.

Finally let $J \in \mathscr{T}$. Let H be the inverse image of J under the natural map π; that is,

$$H = \{ x \in G \mid x\pi \in J \} = \{ x \in G \mid Nx \in J \}.$$

If $x \in N$, then $Nx = N1 \in J$, since $N1$ is the identity element in the quotient group. Therefore $N \leqslant H$. If $x, y \in H$, then $Nx, Ny \in J$ and so $Nxy = (Nx)(Ny) \in J$ and $Nx^{-1} = (Nx)^{-1} \in J$. Hence $xy, x^{-1} \in H$, so we deduce that H is a subgroup which contains N. Thus $H \in \mathscr{S}$. We now consider the image of this subgroup H under the map Φ. If $x \in H$, then $Nx \in J$, so $H/N \leqslant J$. On the other hand, an arbitrary element of J has the form Nx for some element x in G and, by definition, this element x belongs to H. Hence every element of J has the form Nx for some $x \in H$ and we deduce $J = H/N = H\Phi$. Thus Φ is surjective.

This completes the proof of Part (i).

(ii) We retain the notation of Part (i). Suppose $H \in \mathscr{S}$ and that $H \trianglelefteqslant G$. Consider a coset Nx in H/N (with $x \in H$) and an arbitrary coset Ng in G/N. Now $g^{-1}xg \in H$ since $H \trianglelefteqslant G$, so $(Ng)^{-1}(Nx)(Ng) = Ng^{-1}xg \in H/N$. Thus $H/N \trianglelefteqslant G/N$.

Conversely suppose $J \trianglelefteqslant G/N$. Let $H = \{ x \in G \mid Nx \in J \}$, so that $J = H/N$ (as in the last paragraph of (i)). Let $x \in H$ and $g \in G$. Then $Nx \in J$, so $Ng^{-1}xg = (Ng)^{-1}(Nx)(Ng) \in J$ by normality of J. Thus $g^{-1}xg \in H$, by definition of H, and we deduce that $H \trianglelefteqslant G$.

Hence normality is preserved by the bijection Φ. □

Theorem 1.32 (Second Isomorphism Theorem) *Let G be a group, let H be a subgroup of G and let N be a normal subgroup of G. Then $H \cap N$ is a normal subgroup of H and*

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

PROOF: Recall that NH is a subgroup of G by Lemma 1.23 (or by the Correspondence Theorem 1.31). The natural map $\pi\colon x \mapsto Nx$ is a homomorphism $G \to G/N$. Let ϕ be the restriction to H; i.e., $\phi\colon H \to G/N$ given by $x \mapsto Nx$ for all $x \in H$. Then ϕ is once again a homomorphism,

$$\ker \phi = H \cap \ker \pi = H \cap N$$

and

$$\operatorname{im} \phi = \{\, Nx \mid x \in H \,\} = \{\, Nnx \mid x \in H,\ n \in N \,\} = NH/N.$$

By the First Isomorphism Theorem 1.30, $H \cap N \trianglelefteq H$, $NH/N \leqslant G/N$ and

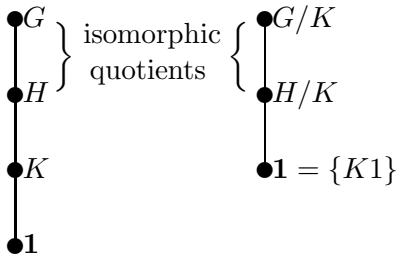
$$H/(H \cap N) \cong NH/N.$$

□

Theorem 1.33 (Third Isomorphism Theorem) *Let G be a group and let H and K be normal subgroups of G such that $K \leqslant H \leqslant G$. Then H/K is a normal subgroup of G/K and*

$$\frac{G/K}{H/K} \cong G/H.$$

This theorem then tells us about the behaviour of normal subgroups of quotient groups and their associated quotients. Specifically, via the Correspondence Theorem we know that a normal subgroup of the quotient group G/K has the form H/K where $K \leqslant H \trianglelefteq G$. Now we would like to know what the quotient group by this normal subgroup is, and the Third Isomorphism Theorem tells us that it is the same as the quotient in the original group. In terms of our diagrams of subgroups we have the following:



PROOF: Define $\theta\colon G/K \to G/H$ by $Kx \mapsto Hx$ for $x \in G$. This is a well-defined map [if $Kx = Ky$, then $xy^{-1} \in K \leqslant H$, so $Hx = Hy$] which is easily seen to be a homomorphism [$\big((Kx)(Ky)\big)\theta = (Kxy)\theta = Hxy = (Hx)(Hy) = (Kx)\theta \cdot (Ky)\theta$ for all $x, y \in G$] and clearly $\operatorname{im} \theta = G/H$. The kernel is

$$\ker \theta = \{\, Kx \mid x \in H \,\} = H/K.$$

Hence, by the First Isomorphism Theorem, $H/K \trianglelefteqslant G/K$ and

$$\frac{G/K}{H/K} \cong G/H.$$

□

This completes our rapid review of previous group theory, at least for now. Certain results will be reviewed later when we need them, while various examples will appear on problem sheets and during the course.