(3) Notice that H^a is a subgroup of G: firstly $1 = a^{-1} \cdot 1 \cdot a = 1^a \in H^a$ and then $x^a y^a = a^{-1}xaa^{-1}ya = a^{-1}(xy)a = (xy)^a$ and $(x^a)^{-1} = (a^{-1}xa)^{-1} = a^{-1}x^{-1}a = (x^{-1})^a$. In fact the group H^a has the same structure as H. (The conjugation by a is a bit like a renaming or an ornament).

Lemma 1.6 *The following are equivalent:*

(a) $H \trianglelefteq G$,
(b) $H^a = H$ *for all* $a \in G$,
(c) $Ha = aH$ *for all* $a \in G$.

Proof (b)⇒(a) is obvious. To prove (a)⇒(b), notice that (a) implies in particular that for any $a \in G$ we have $H^{a^{-1}} \subseteq H$ and therefore

$$H = H^e = H^{a^{-1}a} = (H^{a^{-1}})^a \subseteq H^a.$$

This gives $H^a = H$. It now only remains to show that (b)⇔(c). But this is easy

$$a^{-1}Ha = H \ \Leftrightarrow a \cdot a^{-1}Ha = aH \ \Leftrightarrow Ha = aH.$$

This finishes the proof. □

Definition. Let G be a group with a subgroup H. The number of left cosets of H in G is called the *index* of H in G and is denoted $[G : H]$.

Remark. Suppose that G is finite. Recall from the proof of Lagrange's Theorem that we get a partition of G into a union of pairwise disjoint union of left cosets

$$G = a_1H \cup a_2H \cup \cdots \cup a_nH.$$

As each of the cosets have order $|H|$, it follows that $|G| = r \cdot |H|$. Hence $[G : H] = r = |G|/|H|$. (Likewise we have that G can be written as a pairwise disjoint union of right cosets and the same reasoning shows that their number is also $|G|/|H|$.

Examples. (1) Every subgroup N of an abelian group G is normal (since then obviously $aN = Na$ for all $a \in G$).

(2) The trivial subgroup $\{1\}$ and G itself are always normal subgroups of G.

(3) If H is a subgroup of G such that $[G : H] = 2$ then $H \trianglelefteq G$ (since the left cosets are $H, G \setminus H$ which are also the right cosets. Hence the right cosets are the same as the left cosets).

The quotient group G/N. Let G be a group with a congruence $\simeq$ and a corresponding normal subgroup N. Let

$$G/N = \{\, [a] = aN : \, a \in G\}$$

with a binary operation $[a] \cdot [b] = [ab]$ (that is $aN \cdot bN = abN$). Notice that this is well defined as $\simeq$ is a congruence. To see that G/N is a group with respect to this binary operation we check that the three group axioms hold.

Firstly there is an identity element, namely $[1] = N$ as $[1] \cdot [a] = [1 \cdot a] = [a]$ and

$[a] \cdot [1] = [a \cdot 1] = [a]$.

Secondly every element $[a] \in G/N$ has an inverse, namely $[a^{-1}]$ since $[a] \cdot [a^{-1}] = [a \cdot a^{-1}] = [1]$ and $[a^{-1}] \cdot [a] = [a^{-1} \cdot a] = [1]$.

Finally associativity in G/N follows from associativity in G:

$$[a] \cdot ([b] \cdot [c]) = [a] \cdot [bc] = [a(bc)] = [(ab)c] = [ab] \cdot [c] = ([a] \cdot [b]) \cdot [c].$$

Remark. That the binary operation on G/N is well defined followed from the fact that $\simeq$ is a congruence. There is another way of seeing this using the fact that N is normal in G. First we introduce set products in the natural way. So if $X, Y \subseteq G$ then we let $X \cdot Y = \{xy : x \in X, y \in Y\}$. Then, using this set product as the action on G/N, we get

$$[a] \cdot [b] = aN \cdot bN = abNN = abN = [ab].$$

Hence the binary operation (being the same as the set multiplication) is well defined. Notice that we used the fact that N is normal when applying $Nb = bN$. Also $N \cdot N \subseteq N$ as N is a subgroup and $N = N \cdot \{1\} \subset N \cdot N$ as $1 \in N$. Thus $N \cdot N = N$.

Remark. Notice that the size of the group G/N is $[G : N]$ and when G is finite this is the same as $|G|/|N|$.

Examples. (1) We always have $G \trianglelefteq G$. The congruence with respect to the normal subgroup G is $x \simeq y \Leftrightarrow x^{-1}y \in G$. As the latter holds for any $x, y \in G$ we are identifying all the elements. Hence

$$G/G = \{[1]\} = \{G\}$$

is the trivial group with only one element.

(2) The trivial subgroup $N = \{1\}$ is always normal in G. The congruence in this case is given by $x \simeq y \Leftrightarrow x^{-1}y \in N \Leftrightarrow x^{-1}y = 1 \Leftrightarrow y = x$. Thus

$$G/N = \{\{a\} : a \in G\}.$$

The structure is just like the structure of G: $\{a\} \cdot \{b\} = \{ab\}$. (The curly bracket is there just as a decoration).

(3) Let $G = S_3 = \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ and $N = A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. Here $[G : N] = 2$ and thus G/N has two elements. Notice that these are

$$N = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} = [\mathrm{id}] = [(1\ 2\ 3)] = [(1\ 3\ 2)]$$

and

$$(1\ 2)N = \{(1\ 2), (2\ 3), (1\ 4)\} = [(1\ 2)] = [(1\ 3)] = [(2\ 3)].$$

(So here we have identified all the even permutations and likewise all the odd permutations). $G/N = \{1 = [\mathrm{id}],\ a = [(1\ 2)]\}$. This is the unique group structure with 2 elements: $1 \cdot a = a \cdot 1 = a$, $1 \cdot 1 = 1$ and $a \cdot a = 1$.

IV. Homomorphisms and isomorphisms

Definition. Let G, H be groups. A map $\phi : G \to H$ is a *homomorphism* if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Furthermore ϕ is an *isomorphism* if it is bijective. A group G is said to be *isomorphic to* H if there is an isomorphism $\phi : G \to H$. We then write $G \cong H$.

Remarks. (1) If $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms then their composition $\psi \circ \phi : G \to K$ is also a homomorphism. This is simply because $\psi(\phi(ab)) = \psi(\phi(a) \cdot \phi(b)) = \psi(\phi(a)) \cdot \psi(\phi(b))$. In particular if $G \cong H$ and $H \cong K$ then $G \cong K$.

(2) If $\phi : G \to H$ is an isomorphism then $\phi^{-1} : H \to G$ is also an isomorphism. To see this let $a = \phi(x), b = \phi(y) \in H$. Then

$$\phi^{-1}(a \cdot b) = \phi^{-1}(\phi(x) \cdot \phi(y)) = \phi^{-1}(\phi(xy)) = xy = \phi^{-1}(a) \cdot \phi^{-1}(b).$$

In particular if $G \cong H$ then also $H \cong G$.

(3) If $G \cong H$ then there is no structural difference between G and H. You can think of the isomorphism $\phi : G \to H$ as a renaming function. If $ab = c$ then $\phi(a), \phi(b), \phi(c)$ are the new a, b, c. We want the new c to be the product of the new a and b. This means $\phi(ab) = \phi(a)\phi(b)$.

Lemma 1.7 *Let $\phi : G \to H$ be a homomorphism, then*

(a) $\phi(1_G) = 1_H$,
(b) $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof (a) We have

$$1_H \cdot \phi(1_G) = \phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G) \cdot \phi(1_G)$$

and cancellation gives $1_H = \phi(1_G)$.

(b) Using (a) we have

$$\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(1_G) = 1_H$$

and

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1_G) = 1_H.$$

Hence $\phi(a^{-1})$ is the inverse of $\phi(a)$. □

Examples (1) Let N be a normal subgroup of G. The map $\phi : G \to G/N,\ a \mapsto [a] = aN$ is a homomorphism as $\phi(ab) = [ab] = [a] \cdot [b] = \phi(a) \cdot \phi(b)$.

(2) Let $\mathbb{R}^+$ be the set of all the postive real numbers. There is a (well known) isomorphism $\phi : (\mathbb{R}, +) \to \mathbb{R}^+, \cdot)$ given by $\phi(x) = e^x$. (As $e^{x+y} = e^x e^y$. This is a bijective

homomorphism).

Lemma 1.8 *Let $\phi : G \to H$ be a homomorphism, then*

(a) $A \leq G \;\Rightarrow\; \phi(A) \leq H$.
(b) $B \leq H \;\Rightarrow\; \phi^{-1}(B) \leq G$.
(c) $B \trianglelefteq H \;\Rightarrow\; \phi^{-1}(B) \trianglelefteq G$.

Proof To prove (a) and (b) we apply the usual three subgroup criteria, i.e. the subset in question needs to contain the identity and be closed under multiplication and taking inverses. For (a) this follows from $1_H = \phi(1_G)$, $\phi(x)\phi(y) = \phi(xy)$ and $\phi(x)^{-1} = \phi(x^{-1})$. Notice that, as $A \leq G$, we have $1_G \in A$ and $xy, x^{-1} \in A$ whenever $x, y \in A$. Similarly for proving (b), it is first clear that $1_G \in \phi^{-1}(B)$ as $\phi(1_G) = 1_H \in B$ (since $B \leq H$). Furthermore, if $x, y \in \phi^{-1}(B)$, then $\phi(x), \phi(y) \in B$. As $B \leq H$, it follows that $\phi(xy) = \phi(x)\phi(y) \in B$ and $\phi(x^{-1}) = \phi(x)^{-1} \in B$. This shows that $xy, x^{-1} \in \phi^{-1}(B)$.

For the proof of part (c) suppose furthermore that the subgroup B of H is normal. Let $x \in \phi^{-1}(B)$ and $g \in G$. Then $\phi(g^{-1}xg) = \phi(g)^{-1}\phi(x)\phi(g) \in \phi(g)^{-1}B\phi(g) \subseteq B$. Hence $g^{-1}xg \in \phi^{-1}(B)$. This shows that $\phi^{-1}(B)$ is normal in G. $\square$.

V. The Isomorphism Theorems

Let $N \trianglelefteq G$ and consider the homomorphism $\phi : G \to G/N,\ a \mapsto [a] = aN$. Let

$$\mathcal{S}_N(G) = \{H :\ N \leq H \leq G\}$$

and

$$\mathcal{S}(G/N) = \{R :\ R \leq G/N\}.$$

Consider the map $\Psi : \mathcal{S}_N(G) \to \mathcal{S}(G/N),\ \Psi(H) = \phi(H) = H/N$.

Remark. Thus $\Psi(H)$ is the set $\phi(H) = \{\phi(a) : a \in H\}$.

Theorem 1.9 *(Correspondence Theorem). Ψ is a bijection and furthermore $H \trianglelefteq G$ iff $\Psi(H) \trianglelefteq G/N$.*

Proof. (Ψ is injective). Let $N \leq H, K \leq G$ and suppose that $\Psi(H) = H/N$ is equal to $\Psi(K) = K/N$. Then

$$H = \bigcup_{xN \in H/N} xN = \bigcup_{xN \in K/N} xN = K.$$

(Ψ is surjective). Let R be a subgroup of G/N. Then, by Lemma 1.8, $\phi^{-1}(R)$ is a subgroup of G (that clearly contains N as all the elements in N map to the identity element of G/N that is in R) and as ϕ is surjective, we have

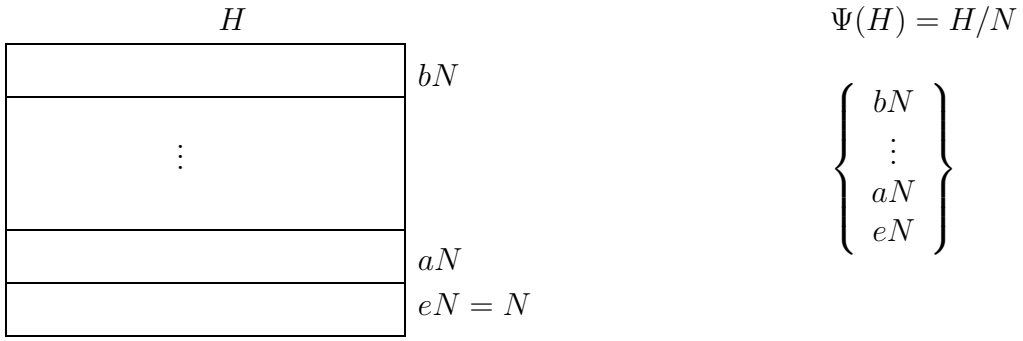
$$\Psi(\phi^{-1}(R)) = \phi(\phi^{-1}(R)) = R.$$

This shows that Ψ is a bijection. Finally we are going to use

$$\Psi(g^{-1}Hg) = \phi(g^{-1}Hg) = \phi(g)^{-1}\phi(H)\phi(g) = \phi(g)^{-1}\Psi(H)\phi(g).$$

(Notice that $N \subseteq H$ implies that $N = g^{-1}Ng \subseteq g^{-1}Hg$ and thus the subgroup $g^{-1}Hg$ is also in $\mathcal{S}_N(G)$). We have that $H \trianglelefteq G$ iff $g^{-1}Hg = H$ for all $g \in G$. As Ψ is a bijection this holds iff $\Psi(g^{-1}Hg) = \Psi(H)$ for all $g \in G$. In view of the identity above this holds iff $\phi(g)^{-1}\Psi(H)\phi(g) = \Psi(H)$ for all $g \in G$. But as ϕ is surjective this is true iff $r^{-1}\Psi(H)r = \Psi(H)$ for all $r \in G/N$ that is iff $\Psi(H) \trianglelefteq G/N$. $\square$

The picture that is good to keep in mind is the following.



$\Psi(H)$ is the collection of all the cosets of N in H and H is the pairwise disjoint union of these cosets. Thus if we know H we get $\Psi(H)$ as the cosets of N in H and if we know $\Psi(H)$ we get H as the union of the cosets in $\Psi(H)$.

Definition. Let $\phi : G \to H$ be a group homomorphism. The *image* of ϕ is

$$\operatorname{im}\phi = \{\phi(g) : \ g \in G\}$$

and the *kernel* of ϕ is

$$\ker\phi = \{g \in G : \phi(g) = 1\}.$$

Notice that as $G \leq G$, it follows from Lemma 1.8 that $\operatorname{im}\phi = \phi(G)$ is a subgroup of H. Also, as $\{1\} \trianglelefteq H$ it follows from Lemma 1.8 that $\ker\phi = \phi^{-1}(\{1\})$ is a normal subgroup of G.

Theorem 1.10 *(1st Isomorphism Theorem). Let $\phi : G \to H$ be a homomorphism. Then $Im\phi \leq H$, $Ker\phi \trianglelefteq G$ and*

$$G/Ker\phi \cong Im\phi.$$