1

Warmup: More Group Theory

> . . . put operations into groups, class them according to their difficulty and not according to their form; that is, according to me, the mission of future geometers . . .
>
> ÉVARISTE GALOIS from *Preface for two memoirs*

1.1 Isomorphism Theorems

The basic notions of Modern Algebra are modeled on the theory of groups. Fundamental concepts include subgroups, normal subgroups, quotient groups, homomorphisms, and isomorphisms. An important result that combines these ideas is the *First Isomorphism Theorem*. The ingredients are a homomorphism $\phi\colon G_1 \to G_2$ between two groups, and the subgroups

$$\ker\phi = \{g \in G_1 \mid \phi(g) = e\} \subset G_1, \text{ the } \textit{kernel} \text{ of } \phi, \text{ and}$$
$$\phi(G_1) = \{h \in G_2 \mid \text{there is } g \in G_1 \text{ with } h = \phi(g)\} \subset G_2, \textit{ image} \text{ of } \phi.$$

The First Isomorphism Theorem *If $\phi\colon G_1 \to G_2$ is a homomorphism of groups, then the kernel of ϕ is a normal subgroup of G_1, and the image of ϕ, $\phi(G_1)$, is isomorphic to the quotient group $G_1/\ker\phi$.*

Recall that a subgroup $N \subset G$ is *normal* if, for all $g \in G$, $gNg^{-1} = N$, or equivalently, $gN = Ng$. This theorem has wide-reaching consequences. There are analogues of the theorem for ring homomorphisms, linear transformations, and many other structures and their mappings. When we speak of *fundamental concepts*, we focus on these key notions.

If there is a *first* such theorem, then what are the subsequent statements? To state the next isomorphism theorem, let us consider a particular situation inside

a group: Let H and N be subgroups of G with N a normal subgroup. Define

$$HN = \{hn \in G \mid h \in H, n \in N\},$$

the set of products of an element in H with an element in N, in that order. Observe that HN is a subgroup of G: if h_1n_1 and h_2n_2 are elements of HN, then, because N is normal in G, we have $h_2^{-1}Nh_2 = N$, and so

$$(h_1n_1)(h_2n_2) = (h_1h_2)\big(h_2^{-1}n_1h_2\big)n_2 = (h_1h_2)(n_3n_2).$$

Thus HN is closed under multiplication. Also,

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}\big(hn^{-1}h^{-1}\big) = h^{-1}n',$$

and HN contains inverses. These arguments show that $HN = NH$. With these constructions, we can prove

The Second Isomorphism Theorem *Suppose H and N are subgroups of G with N a normal subgroup. Then HN is a subgroup of G containing N, and*

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

Proof First notice that N is a normal subgroup of HN because N is normal in G. Consider the mapping $\pi : H \to HN/N$ given by $\pi(h) = hN$. Then $\pi(h_1h_2) = h_1h_2N = (h_1N)(h_2N) = \pi(h_1)\pi(h_2)$, and π is a homomorphism. By the First Isomorphism Theorem, $\pi(H) \cong H/\ker\pi$. Given $hn \in HN$, the coset $hnN = hN$, and so the homomorphism π is surjective. The kernel of π consists of elements of H for which $hN = N$, that is, $h \in H \cap N$. It follows that $\pi(H) = HN/N \cong H/(H \cap N)$. □

Corollary 1.1 *For G a finite group, $\#HN = (\#H)(\#N)/\#(H \cap N)$.*

The subgroups of a group G are partially ordered by inclusion. For small groups, this ordering can be pictured in the *Hasse diagram* of G, which is the graph that depicts this partially ordered set. A vertex is a subgroup, and an edge denotes an inclusion. For example, the Hasse diagrams for Σ_3, the group of permutations of $\{1, 2, 3\}$, and A_4, the group of even permutations of $\{1, 2, 3, 4\}$, take the form as in Fig. 1.1. Here $\langle g\rangle$ denotes the cyclic subgroup generated by g. Subgroups of the same cardinality are arranged horizontally.

Each element of a group G determines a homomorphism by conjugation: If $g \in G$, then the mapping *conjugation by g*, $c_g : G \to G$, is defined by $c_g(h) = ghg^{-1}$.

Proposition 1.2 *Conjugation by g is an isomorphism called an inner automorphism of G.*

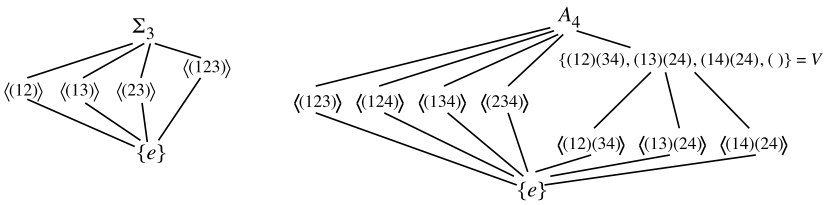

Figure 1.1

Proof We have $c_g(hk) = g(hk)g^{-1} = (ghg^{-1})(gkg^{-1}) = c_g(h)c_g(k)$, and c_g is a homomorphism. If g^{-1} is the inverse of g, then $c_{g^{-1}}$ satisfies $c_{g^{-1}}(c_g(h)) = g^{-1}(ghg^{-1})g = h$, and c_g is an isomorphism. □

Two elements h, k of G are said to be *conjugates* if there is an element $g \in G$ such that $c_g(h) = k$, that is, $k = ghg^{-1}$. This relation is an equivalence relation on G: $exe^{-1} = x$, so x is a conjugate of x; if x is a conjugate of y, that is, $y = c_g(x)$, then $x = c_{g^{-1}}(y)$, and y is a conjugate of x; finally, if x is conjugate to y and y is conjugate to z, then $y = c_g(x)$ and $z = c_h(y)$ for some $g, h \in G$. It follows that $z = c_h(c_g(x)) = h(gxg^{-1})h^{-1} = (hg)x(hg)^{-1} = c_{hg}(x)$ and x is conjugate to z.

Definition 1.3 The equivalence classes under conjugation of elements of G are called *conjugacy classes*. We denote a conjugacy class by $[g] = \{xgx^{-1} \mid x \in G\}$, and the set of equivalence classes is denoted by $\mathrm{Cl}(G)$.

The set $\mathrm{Cl}(G)$ tells us something about the binary operation on G. For example, if G is abelian, then $ghg^{-1} = gg^{-1}h = h$, and so the conjugacy class of h is a singleton set $\{h\}$. When G is nonabelian, the set $Z(G)$ of elements whose conjugacy classes are singletons, that is, $[g] = \{g\}$, determines a subgroup of G called the *center* of G: Suppose $x, y \in Z(G)$. Then $c_g(x) = x$ and $c_g(y) = y$ for all $g \in G$; $c_g(xy) = c_g(x)c_g(y) = xy$ for all $g \in G$, and so $xy \in Z(G)$; if $x \in Z(G)$, then $c_g(x^{-1}) = gx^{-1}g^{-1} = (g^{-1}xg)^{-1} = x^{-1}$ for all $g \in G$.

Let us explore the important example of conjugacy classes in Σ_n, the *symmetric group on n letters*, which is the group of all permutations of the set $[n] = \{1, 2, \ldots, n\}$. Recall that a *permutation* is a one-to-one correspondence of $[n]$ with itself. There are various notations for permutations. For example, if $\sigma \in \Sigma_7$, then we can write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 5 & 7 & 6 \end{pmatrix} = (1, 2, 3, 4)(6, 7).$$

In the first case, we present the function values explicitly; reading downward $\sigma(1) = 2, \sigma(2) = 3$, etc. In the second case, we use *cycle notation*: $(1, 2, 3, 4)$ means $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 1$. Notice that 5 does not appear in the cycle notation because it is fixed by σ, $\sigma(5) = 5$. Every permutation has a unique presentation as a composite of disjoint cycles. Simply apply σ repeatedly to an element until it cycles back to itself. This gives one cycle. Apply σ to any remaining elements, leaving off any that are fixed, and repeat until every element fits into a cycle or is fixed. We denote the identity permutation $\mathrm{Id}(j) = j$ for all j by $(\,)$, the empty cycle. A given cycle has as many presentations as elements in its cycle; for example, $(1, 2, 3) = (2, 3, 1) = (3, 1, 2)$. The pattern of the bijection is fixed by the cyclic order of the elements.

The binary operation on Σ_n is a composition, and so when we compute the product of permutations, we compute the resulting cycle decomposition of the product **reading from right to left**. For example,

$$(3, 4, 5) \circ (1, 3, 5, 2, 4) = (1, 4)(2, 5).$$

We call a 2-cycle (a, b) a *transposition* because only two elements move and they are interchanged. Every permutation can be expressed as a product of transpositions. For example, $(a, b, c) = (a, b)(b, c)$. We say that a permutation is an *odd permutation* (*even permutation*) if it has a presentation as a product of an odd (even) number of transpositions. It is left as an exercise to prove that this is independent of the choice of presentation. Products of even permutations are even, and so they form a subgroup A_n of Σ_n, called the *alternating group* on n letters.

In 1844 [11], AUGUSTIN CAUCHY (1789–1857) first developed some of the key properties of symmetric groups. In particular, he proved the following:

Cauchy's Formula *If $\sigma \in \Sigma_n$ and $(a_1, a_2, \ldots, a_k)$ is a k-cycle in Σ_n, then*

$$\sigma \circ (a_1, a_2, \ldots, a_k) \circ \sigma^{-1} = \big(\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k)\big).$$

Proof If $(a_1, \ldots, a_k)$ fixes $i \in [n]$, then $\sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1}$ fixes $\sigma(i)$:

$$\sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1}\big(\sigma(i)\big) = \sigma \circ (a_1, \ldots, a_k)(i) = \sigma(i).$$

For $1 \leq j \leq k$, we have

$$\sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1}\big(\sigma(a_j)\big) = \sigma \circ (a_1, \ldots, a_k)(a_j) = \sigma(a_{j+1}),$$

where we understand $a_{k+1} = a_1$. Because we have accounted for everything in $[n]$, the permutation $\sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))$. □

Since conjugation is a homomorphism,

$$c_\sigma\big((a_1,\dots,a_k)(b_1,\dots,b_l)\big) = c_\sigma\big((a_1,\dots,a_k)\big)\circ c_\sigma\big((b_1,\dots,b_l)\big)$$
$$= \big(\sigma(a_1),\dots,\sigma(a_k)\big)\big(\sigma(b_1),\dots,\sigma(b_l)\big).$$

Cauchy's Formula extends to arbitrary products of cycles.

When a permutation $\sigma \in \Sigma_n$ is written as a product of disjoint cycles involving m_1 elements fixed by σ, m_2 2-cycles, m_3 3-cycles, and so on, we write the *type* of σ as $(1^{m_1}, 2^{m_2}, 3^{m_3}, \dots, n^{m_n})$. Here $m_1 + 2m_2 + \cdots + nm_n = n$. For example, $\sigma = (1,2,3,4)(6,7) \in \Sigma_7$ has type $(1^1, 2^1, 3^0, 4^1, 5^0, 6^0, 7^0)$.

Corollary 1.4 *Two permutations in Σ_n are conjugate if and only if they share the same type.*

Proof By Cauchy's Formula conjugation preserves the length of a cycle. If σ and τ are conjugate, then they have the same type. Suppose conversely that σ and τ have the same type. We use the functional presentation of a permutation. Suppose the type shared by σ and τ is $(1^{m_1}, 2^{m_2}, \dots, n^{m_n})$. Write the domain $[n]$ as an ordered set $1 < 2 < \cdots < n$ and place parentheses according to the type giving a permutation $\alpha \in \Sigma_n$. For example, in Σ_7, a type $(1^1, 2^1, 3^0, 4^1, 5^0, 6^0, 7^0)$ gives us $\alpha = (1)(2,3)(4,5,6,7)$. Write σ and τ as products of disjoint cycles that follow the type in the manner of α. For example, $\sigma = (1,2,3,4)(6,7)$ can be written as $(5)(6,7)(1,2,3,4)$. This gives us an ordering of [7] by ignoring the parentheses. We obtain a permutation θ by stacking the natural order over the order given by σ:

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 7 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

Cauchy's Formula tells us that $\theta\circ\alpha\circ\theta^{-1} = \theta\circ(1)(2,3)(4,5,6,7)\circ\theta^{-1} = \sigma$. Reversing the conjugation by θ, we get $\alpha = \theta\sigma\theta^{-1}$. For τ of the same type, we get another permutation ζ with $\alpha = \zeta\tau\zeta^{-1}$, and so $\theta\sigma\theta^{-1} = \zeta\tau\zeta^{-1}$; it follows that σ and τ are conjugate. □

The restriction that the type satisfies $m_1 + 2m_2 + \cdots + nm_n = n$ with $m_i \geq 0$ corresponds to a *partition* of the integer n, that is, an expression of n as a sum of positive integers in nondecreasing order. For example, $4 = 1+1+1+1 = 1+1+2 = 1+3 = 2+2$. Each partition of 4 corresponds to a type: $4 \leftrightarrow (1^0, 2^0, 3^0, 4^1)$, $1+1+1+1 \leftrightarrow (1^4, 2^0, 3^0, 4^0)$, $1+1+2 \leftrightarrow (1^2, 2^1, 3^0, 4^0)$, $1+3 \leftrightarrow (1^1, 2^0, 3^1, 4^0)$, and $2+2 \leftrightarrow (1^0, 2^2, 3^0, 4^0)$. The analysis above shows that the number of conjugacy classes filling Σ_n is $p(n)$, the *number of partitions of n*. The function $p(n)$ was introduced by Leibniz and is the subject of some remarkable mathematics (see, for example, [1]).

Get to know conjugation

1. For a group G, an element $g \in G$, and a subgroup H of G, show that gHg^{-1} is a subgroup of G that is isomorphic to H.
2. What are the conjugacy classes of the groups Σ_3 and Σ_4? What is the cardinality of each conjugacy class?
3. Show that a group G is abelian if and only if all of its conjugacy classes are singletons.
4. What is the partition into conjugacy classes for the group $A_4 \subset \Sigma_4$ of even permutations of four objects? What is the partition into conjugacy classes for the dihedral group of eight elements, D_8, the set of symmetries of a square?

   The *dihedral groups* D_{2n} are the groups of symmetries of a regular n-gon in the plane. There is a symmetry by rotating the n-gon through $2\pi/n$ radians. Denote this rotation by r and notice that $r^n = \mathrm{Id}$. If we situate the n-gon in the plane with its center of gravity at the origin and one vertex at the point $(1, 0)$, then there is a symmetry of the plane obtained by (x, y) going to $(x, -y)$ (complex conjugation?). Denote this reflection by f and notice that $f^2 = \mathrm{Id}$. These two elements *generate* the dihedral group, that is, every symmetry of the regular n-gon in the plane is a finite product of the form $f^{a_1}r^{b_1}f^{a_2}r^{b_2}\cdots$. We simplify using $f^2 = \mathrm{Id} = r^n$ whenever they occur. There is also another relation that follows from the geometry: $fr = r^{n-1}f$. (Can you picture this?) We write these data as a *presentation* of the group:

$$D_{2n} = \langle f, r \mid r^n = \mathrm{Id},\ f^2 = \mathrm{Id},\ fr = r^{n-1}f \rangle.$$

   The dihedral group D_{2n} has order $2n$.

   If G is a group and $S \subset G$ is a subset of G, then $\langle S \rangle$ is the smallest subgroup of G that contains S, that is, $\langle S \rangle = \bigcap_{S \subset H, \text{subgroup}} H$.
5. Suppose that N is a normal subgroup of G. Show that N is the union of the conjugacy classes of its elements. If $[g]$ is a conjugacy class of G and $H = \langle [g] \rangle$ is the subgroup of G generated by the elements of $[g]$, then show that H is normal in G.

For a subgroup of a group, the conjugacy classes of elements in the subgroup need not coincide with those of the group. For example, if $H = \langle g \rangle$ is a cyclic subgroup generated by $g \in G$, then the conjugacy classes in H are singletons.

If G is nonabelian, then there are conjugacy classes of cardinality greater than one.

In a finite group, what is the cardinality of a conjugacy class? The *centralizer* of an element g in any group G is the subset $C_G(g) = \{x \in G \mid xgx^{-1} = g\}$. In other words, the centralizer consists of those elements x of G that commute with g.

Proposition 1.5 *For $g \in G$ a group, the centralizer $C_G(g)$ is a subgroup of G. Furthermore, if G is finite, then $\#[g]$, the cardinality of the conjugacy class of g, is given by the index of $C_G(g)$ in G, $[G : C_G(g)] = \#G/\#C_G(g)$.*

Proof If $x, y \in C_G(g)$, then $(xy)g(xy)^{-1} = x(ygy^{-1})x^{-1} = xgx^{-1} = g$. So $C_G(g)$ is closed under the binary operation. Because $g = xgx^{-1}$ implies $x^{-1}gx = g$, $C_G(g)$ is closed under inverses, and $C_G(g)$ is a subgroup of G. Recall that $G/C_G(g)$ denotes the set of left cosets of $C_G(g)$ in G.

Consider the function of sets $f : G/C_G(g) \to [g]$ given by $f : xC_G(g) \mapsto xgx^{-1}$. If $xC_G(g) = yC_G(g)$, then $y^{-1}x \in C_G(g)$ from which it follows that $(y^{-1}x)g(y^{-1}x)^{-1} = g$. This implies that $xgx^{-1} = ygy^{-1}$ and the mapping f is well-defined. It is clearly surjective. To see that f is injective, suppose $f(x) = f(y)$. Then $xgx^{-1} = ygy^{-1}$ and $(y^{-1}x)g(y^{-1}x)^{-1} = g$, that is, $y^{-1}x \in C_G(g)$, and so $xC_G(g) = yC_G(g)$. The bijection implies that $\#[g] = \#(G/C_G(g)) = [G : C_G(g)]$. □

For a subgroup H of G and $h \in H$, we have $C_H(h) = \{k \in H \mid khk^{-1} = h\} = C_G(h) \cap H$.

Let us examine in detail the case of A_n, the subgroup of Σ_n consisting of even permutations. Suppose $\sigma \in A_n$. In Σ_n the conjugates of σ are permutations of the same type as σ. If τ is an odd permutation, then $\tau\sigma\tau^{-1}$ is an even permutation that might not be in the conjugacy class of σ in A_n. It can be that $\tau\sigma\tau^{-1} \neq \alpha\sigma\alpha^{-1}$ for all $\alpha \in A_n$. How can we recognize when this happens? Following Proposition 1.5,

$$\#[\sigma]_{A_n} = \left[A_n : C_{A_n}(\sigma)\right] = \left[A_n : A_n \cap C_{\Sigma_n}(\sigma)\right].$$

Because A_n is normal in Σ_n, the Second Isomorphism Theorem implies $C_{\Sigma_n}(\sigma)A_n/A_n \cong C_{\Sigma_n}(\sigma)/A_n \cap C_{\Sigma_n}(\sigma)$. Cross multiply to obtain $\#A_n/\#(A_n \cap C_{\Sigma_n}(\sigma)) = \#C_{\Sigma_n}(\sigma)A_n/\#A_n$, and

$$\left[A_n : A_n \cap C_{\Sigma_n}(\sigma)\right] = \left[C_{\Sigma_n}(\sigma)A_n : C_{\Sigma_n}(\sigma)\right].$$

Suppose there is an odd permutation that commutes with σ. Then $C_{\Sigma_n}(\sigma)$ contains an odd permutation, and so $C_{\Sigma_n}(\sigma)A_n = \Sigma_n$. From this identity,

$$\#[\sigma]_{A_n} = \big[A_n : A_n \cap C_{\Sigma_n}(\sigma)\big] = \big[C_{\Sigma_n}(\sigma)A_n : C_{\Sigma_n}(\sigma)\big] = \big[\Sigma_n : C_{\Sigma_n}(\sigma)\big] = \#[\sigma]_{\Sigma_n}.$$

When there are no odd permutations that commute with σ, we have $C_{\Sigma_n}(\sigma) = C_{A_n}(\sigma)$, and $\#[\sigma]_{A_n} = [A_n : C_{\Sigma_n}(\sigma)]$, but then

$$\#[\sigma]_{\Sigma_n} = \big[\Sigma_n : C_{\Sigma_n}(\sigma)\big] = [\Sigma_n : A_n]\big[A_n : C_{\Sigma_n}(\sigma)\big] = 2\#[\sigma]_{A_n}.$$

So if σ commutes only with even permutations, then the conjugacy class of σ in Σ_n splits into two equal pieces in A_n.

For example, in Σ_3, $[(1,2,3)]_{\Sigma_3} = \{(1,2,3),(1,3,2)\}$, whereas $[(1,2,3)]_{A_3} = \{(1,2,3)\}$. It would nice to be able to tell directly from σ when $C_{\Sigma_n}(\sigma) = C_{A_n}(\sigma)$.

Proposition 1.6 *Suppose $\sigma \in A_n$ has type $(1^{m_1}, 2^{m_2}, \ldots, n^{m_n})$. Then $C_{\Sigma_n}(\sigma) = C_{A_n}(\sigma)$ and $\#[\sigma]_{\Sigma_n} = 2\#[\sigma]_{A_n}$ if and only if, for all i, $m_{2i} = 0$ and $m_{2i+1} = 0$ or 1.*

For example, in Σ_3, the type of $(1,2,3)$ is $(1^0, 2^0, 3^1)$.

Proof If $m_{2i} > 0$, then $\sigma = \alpha\beta$ with α a $2i$-cycle and β a product of cycles disjoint from α. This implies $\alpha\beta = \beta\alpha$, and multiplying by α on the left gives

$$\alpha\sigma = \alpha\alpha\beta = \alpha\beta\alpha = \sigma\alpha.$$

A $2i$-cycle is an odd permutation and α is in $C_{\Sigma_n}(\sigma)$ but not in A_n.

If $m_{2i} = 0$ but $m_{2i+1} > 1$ for some i, then, after renumbering, we have $\sigma = (1,2,\ldots,2i+1)(1',2',\ldots,(2i+1)')\nu$, where the numbers 1 through $2i+1$ and $1'$ through $(2i+1)'$ are taken from $[n]$ and are disjoint from one another. The permutation ν is also disjoint from these numbers. Let $\zeta = (1,1')(2,2')\cdots(2i+1,(2i+1)')$, an odd permutation. Then $\zeta\sigma\zeta^{-1} = \sigma$ by Cauchy's Formula, and so $\zeta \in C_{\Sigma_n}(\sigma)$. This proves one direction of the proposition.

To prove the other direction, suppose the type of σ has $m_{2i} = 0$ and $m_{2i+1} = 0$ or 1 for all i. Then σ is a product of disjoint k-cycles with k odd. Since the type determines the conjugacy class in Σ_n, we can count the number of elements in $[\sigma]_{\Sigma_n}$ combinatorially. Take any of the $n!$ orderings of $[n]$ and form the permutation θ as in the proof of Proposition 1.5 by removing the first m_1 entries and introducing parentheses according to the type of σ. Wherever $m_{2i+1} = 1$, the corresponding $(2i+1)$-cycle can start from any of its entries and so is counted $2i+1$ times. We divide $n!$ by $2i+1$ for each $m_{2i+1} = 1$ to adjust for the overcounting. Thus $\#[\sigma] = n!/t$ with t an odd number. This implies $\#C_{\Sigma_n}(\sigma) = t$, a subgroup of Σ_n of odd order, and every permutation in $C_{\Sigma_n}(\sigma)$ has odd order. The order of a permutation is the least common

multiple of the lengths of each constituent disjoint k-cycle. Since the order is odd, no $2m$-cycle appears in the disjoint cycle presentation of any element of $C_{\Sigma_n}(\sigma)$. Then $C_{\Sigma_n}(\sigma) \subset A_n$ and $C_{\Sigma_n}(\sigma) = C_{A_n}(\sigma)$. □

For example, in A_5 the permutation $\sigma = (1, 2, 3, 4, 5)$ has type $(1^0, 2^0, 3^0, 4^0, 5^1)$, and so $C_{\Sigma_n}(\sigma) = C_{A_n}(\sigma)$ and $\#[\sigma]_{\Sigma_n} = 2\#[\sigma]_{A_n}$. On the other hand, the permutation $\tau = (1, 2, 3)$ has type $(1^2, 2^0, 3^1, 4^0, 5^0)$, and so the conjugacy class of τ satisfies $[(1, 2, 3)]_{\Sigma_5} = [(1, 2, 3)]_{A_5}$ and contains all 3-cycles.

1.2 The Jordan–Hölder Theorem

When $\phi\colon G_1 \to G_2$ is a homomorphism, we obtain subgroups of G_1 by taking the *inverse image* of subgroups of G_2: let $K \subset G_2$ denote a subgroup of G_2, and let

$$\phi^{-1}(K) = \{g \in G_1 \mid \phi(g) \in K\}.$$

If g and g' are in $\phi^{-1}(K)$, then $\phi(g) = k$ and $\phi(g') = k'$, both in K. Since K is a subgroup, $\phi(gg') = \phi(g)\phi(g') = kk'$ is in K, and so $gg' \in \phi^{-1}(K)$. For a subgroup $H \subset G_1$, the image $\phi(H) = \{\phi(h) \in G_2 \mid h \in H\}$ is a subgroup of G_2. Hence we can go to and fro between the collections of subgroups in this manner. In fact, we get a strong connection between these collections.

The Correspondence Theorem *Let $\phi\colon G_1 \to G_2$ be a surjective group homomorphism. Then there is a bijection*

$$\begin{aligned}\Phi\colon \mathcal{S}_\phi = \{&H, \textit{ a subgroup of } G_1, \textit{ with } \ker\phi \subset H\}\\ &\to \mathcal{T}_{G_2} = \{K, \textit{ a subgroup of } G_2\}\end{aligned}$$

given by $\Phi(H) = \phi(H)$. Furthermore, Φ and its inverse take normal subgroups to normal subgroups.

Proof We prove Φ is a bijection by presenting its inverse. For a subgroup K of G_2, let $\Phi^{-1}(K) = \phi^{-1}(K)$. In general, notice that $\phi^{-1}(\phi(H)) = (\ker\phi)H$ as subgroups of G_1: let $l \in \phi^{-1}(\phi(H))$. Then $\phi(l) \in \phi(H)$, and we can write $\phi(l) = \phi(h)$ for some $h \in H$. Then $\phi(lh^{-1}) = e$ and $lh^{-1} = k \in \ker\phi$, but then $l = kh \in (\ker\phi)H$ and $\phi^{-1}(\phi(H)) \subset (\ker\phi)H$. For $nh \in (\ker\phi)H$, $\phi(nh) = \phi(n)\phi(h) = \phi(h) \in \phi(H)$, and so $(\ker\phi)H \subset \phi^{-1}(\phi(H))$.

For any subgroup $H \in \mathcal{S}_\phi$, we have $\ker\phi \subset H$, and so $H = (\ker\phi)H = \phi^{-1}(\phi(H)) = \Phi^{-1}(\Phi(H))$. In the other direction, $\Phi(\Phi^{-1}(K)) =$

$\phi(\phi^{-1}(K))$. Because ϕ is a surjection, $\phi(\phi^{-1}(K)) = K$, and so $\Phi \circ \Phi^{-1}$ is the identity mapping on $\mathcal{T}_{G_2}$.

If N is a normal subgroup, $N \triangleleft G_1$, and $k \in G_2$, then we can write $k\Phi(N)k^{-1} = \phi(g)\phi(N)\phi(g^{-1})$ because ϕ is surjective. It follows then that $\phi(g)\phi(N)\phi(g^{-1}) = \phi(gNg^{-1}) = \phi(N)$, and so $\Phi(N)$ is normal in G_2. For a normal subgroup M of G_2, and $h \in G_1$, $\phi(h\phi^{-1}(M)h^{-1}) = \phi(h)M\phi(h^{-1}) = M$, and $h\phi^{-1}(M)h^{-1} = \phi^{-1}(M)$, that is, $\Phi^{-1}(M)$ is normal in G_1. □

The Correspondence Theorem implies that a surjective homomorphism gives a correspondence between the Hasse diagram of the codomain and portions of the Hasse diagram of the domain. Correspondences will figure prominently in other parts of the book.

One way to carry out inductive sorts of arguments on finite groups is choosing a normal subgroup N of a finite group G that gives a surjection $\pi : G \to G/N$ to a smaller group G/N. Properties of G/N may lift to G over π as in the Correspondence Theorem. However, some groups are not susceptible to this strategy, lacking nontrivial normal subgroups.

Definition 1.7 A group G is called a *simple group* if whenever N is a normal subgroup of G, then $N = \{e\}$ or $N = G$.

For example, an abelian finite group G is simple if and only if G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for a prime p. (Can you prove this?) Simple groups turn out to play a role similar to atoms in a molecule or to primes in the prime factorization of a positive integer. To make this analogy precise, we introduce the following notion.

Definition 1.8 Suppose G is a finite group. A proper subgroup N is a *maximal normal subgroup* if N is normal in G, and if $N \triangleleft H \triangleleft G$ for some subgroup H, then either $H = N$ or $H = G$.

Proposition 1.9 *For a group G and a normal subgroup N, the quotient group G/N is a simple group if and only if N is a maximal normal subgroup.*

Proof Let $\pi : G \to G/N$ be the quotient homomorphism, $\pi(g) = gN$. Suppose H is a normal subgroup of G/N. Then $\pi^{-1}(H)$ is a normal subgroup of G that contains $N = \ker\pi$. If N is a maximal normal subgroup, then $N \triangleleft \pi^{-1}(H) \triangleleft G$ implies either that $\pi^{-1}(H) = N$, and so $H = \{eN\} \subset G/N$, or that $\pi^{-1}(H) = G$ and $H = G/N$. Hence G/N is a simple group.

In the case that G/N is a simple group, any normal subgroup M of G with $N \triangleleft M \triangleleft G$ is mapped to $\pi(M)$ a normal subgroup of G/N. This implies that $\pi(M) = \{eN\}$ or $\pi(M) = G/N$, which implies that $M = N$ or $M = G$ and N is a maximal normal subgroup of G. □