Group Theory: Basic Concepts

Robert B. Griffiths
Version of 9 Feb. 2009

References:

EDM = Encyclopedic Dictionary of Mathematics, 2d English edition (MIT, 1987)
HNG = T. W. Hungerford: Algebra (Springer-Verlag, 1974)

Contents

1 Definitions

★ Group: (G, γ) where G is a set and γ a binary operation $\gamma : G \times G \to G$. If γ is clear from the context the group is simply denoted by G.

∘ In place of $\gamma(f, g)$ write $f\gamma g$ or simply fg when there is no ambiguity, as in most of what follows.

∘ Example: $G = Z = \{\ldots -2, -1, 0, 1, 2 \ldots\}$, $\gamma = +$, $\gamma(f, g) = f + g$.

• For G to be a group three conditions must be satisfied:
(i) γ is *associative*: $\gamma(f, \gamma(g, h)) = \gamma(\gamma(f, g), h)$, or $f(gh) = (fg)h$.
(ii) There is an *identity* $e \in G$: $eg = ge = e$ for all $g \in G$.
(iii) Every g in G has an inverse $\bar{g}$, usually denoted by g^{-1}, such that $g\bar{g} = \bar{g}g = e$.

★ If (i) is satisfied, (G, γ) is a *semigroup*, and if (i) and (ii) are satisfied, (G, γ) is a *monoid*. Thus every group is a monoid, and every monoid is a semigroup.

• In the definition e is both a left identity, $eg = g$, and a right identity, $ge = g$. Likewise g^{-1} is both a left inverse, $g^{-1}g = e$ and a right inverse $gg^{-1} = e$. HNG shows, p. 25, that a semigroup equipped with both a left identity and a left inverse is necessarily a group. Similarly if it has both a right identity and a right inverse.

• We do *not* require the γ operation, "group multiplication," to be symmetrical or *commutative*, so in general $\gamma(f, g) \neq \gamma(g, f)$, or $fg \neq gf$. Groups with a commutative group multiplication, $fg = gf$ for all f and g in G, are called *commutative* or *abelian* or *Abelian*.

★ A *subgroup* of a group (G, γ) is a subset f of G that forms a group using the same binary operation γ. Since (i) is automatically satisfied, all one needs to check is that F contains e and the inverse f^{-1} of each of its elements.

∘ A *proper* subgroup of G is a subgroup which is not G itself, or simply the identity e, which by itself forms a rather trivial subgroup of G.

★ Properties of a group that everyone should know.
(i) The identity is unique: if $\bar{e}g = g$ for some $g \in G$, then $\bar{e} = e$.
(ii) The inverse g^{-1} is uniquely determined by g.
(iii) Right and left cancellation: $ag = bg \Rightarrow a = b; \quad ga = gb \Rightarrow a = b$.
(iv) The equations $ax = b$ and $ya = b$ have unique solutions $x = a^{-1}b$ and $y = ba^{-1}$.
(v) $(a^{-1})^{-1} = a; \quad (ab)^{-1} = b^{-1}a^{-1}$.

★ The *order* of a group is the number of elements in the set G, its cardinality. Similar definition for a subgroup.

★ Quasigroup: (G, γ) in which γ need not be associative, but the equations $\gamma(a, x) = a\gamma x = b$ and $\gamma(y, a) = y\gamma a = b$ have unique solutions x and y in G for every a and b in G.

2 Examples of Groups

2.1 Integers and Integers Mod D

★ The integers $Z = \{\ldots -2, -1, 0, 1, 2 \ldots\}$ form a group under addition. Since integers have various other algebraic properties the group might best be labeled as $(Z, +)$, but we will use Z since there is unlikely to be confusion.

★ By the additive group Z_D, the integers mod D, with $D \geq 2$, we shall mean the set $\{0, 1, 2, \ldots D - 1\}$, with addition defined in the usual way, except that if the sum falls outside this range subtract D to put it back in the range. Again, Z_D has other interesting properties besides being an additive group, so if precision is needed use $(Z_D, +)$.

• The symbol C_D (or C_n, etc.) is often used in place of Z_D; here C means "cyclic."

2.2 Permutations and the Symmetric Group

★ A permutation can be thought of as a 1 to 1 map of some set onto itself, i.e., a bijection.

∘ Terminology: An *injection* is a 1 to 1 map from some set A to another set B. A *surjection* is a map from A onto all of B. A map which is both an injection and a surjection is called a *bijection*: a 1 to 1 map from A onto B. The corresponding adjectives are injective, surjective, and bijective.

• Let the set of interest be $N = \{1, 2, \ldots n\}$, the collection of the first n positive integers. It is customary to denote a permutation P by a $2 \times n$ matrix

$$P = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix} \tag{1}$$

where the map carries j on the top row to the i_j just beneath it.

• We shall follow the convention in HNG that $R = PQ$ means that the permutation Q is carried out first, and after that P. That is to say, $R(j) = P(Q(j))$. For example

$$P = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}. \quad PQ = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}. \tag{2}$$

Warning! This convention is *not* universal.

★ A simpler notation employs *cycles* in which $(abc\cdots z)$ means a maps to b, b maps to c, etc., and finally z maps to a. Thus

$$(12)=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad (123)=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\tag{3}$$

are cycles of *length* 2 and 3.

• A cycle of length 2, thus (ab), is called a *transposition*.

∘ Any permutation can be written as a product of disjoint cycles, i.e., no symbol appears in more than one cycle. For example $(13)(246)(5)$ for $n=6$. Customarily one omits cycles of length 1, writing this as $(13)(246)$.

★ There are $n!$ distinct permutations possible on $N=\{1,2,\dots n\}$. With multiplication defined as above, these permutations form a group S_n, the *symmetric* group of *degree* n.

★ The *alternating* group A_n of degree $n\geq 2$ is the collection of $n!/2$ *even* permutations on N. A permutation is even if it can be written as the product of an even number of transpositions, and odd if it can be written as the product of an odd number of transpositions. Thus (12) is odd, while $(123)=(23)(12)$ is even.

2.3 Dihedral Groups

★ For the present discussion we shall regard the dihedral group of degree D_n as the symmetry group of a regular polygon of n lying in a plane. However, the crystallographers regard D_n as the symmetry group in which an n-fold axis—think of it as in the z direction—has n 2-fold rotation axes perpendicular to it, each of these in the x,y plane.

★ The group D_2 from the crystallography perspective is just a set of three 2-fold axes perpendicular to each other. Let e be the identity, and a, b, and c the 2-fold rotations. Here is the group multiplication table, where $\gamma(f,g)$ is the element that occurs at the intersection of row f and column g.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

• Comments on the multiplication table:

∘ First row and column duplicate the labels at top and left, so they could be omitted, but it is sometimes useful to have other forms of such tables with explicit labels.

∘ Each row contains each element just once. Same for each column. This is necessary if we have a group, because if one row contained the same element twice it would violate left cancellation, and right cancellation means that no two elements in a column can be the same.

∘ The table is symmetrical about the main diagonal, thus equal to its transpose. This means D_2 is an abelian group.

• As an abstract group D_2 is often called the "four group" and denoted by the symbol V (in German "four" is "vier"). It is isomorphic to $Z_2\times Z_2$.

★ The dihedral group $D_3=\{e,a,b,c,r,s\}$ is of order 6.

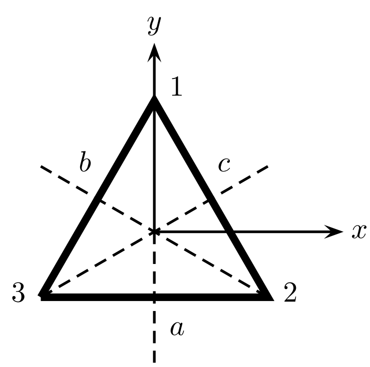
• Multiplication table. Again, $\gamma(f,g)$ is the element that occurs at the intersection of row f and column g.

	e	a	b	c	r	s
e	e	a	b	c	r	s
a	a	e	r	s	b	c
b	b	s	e	r	c	a
c	c	r	s	e	a	b
r	r	c	a	b	s	e
s	s	b	c	a	e	r

◦ The table is not symmetrical across the main diagonal (upon interchanging rows and columns). Thus D_3 is not abelian.

◦ From the table itself it is not immediately obvious that the multiplication is associative. (It is, but checking it takes some work.)

★ In geometrical terms, the group D_3 is the symmetry group of an equilateral triangle, i.e., the collection of transformations that maps the triangle onto itself. For ease of discussion we place the triangle in the x, y plane as shown here, with its vertices labeled $1, 2, 3$. Then a, b, c are reflections about the dashed lines (in three dimensions 180° rotations about these lines), while r and s are 120° clockwise and counterclockwise rotations.



★ The reflection a interchanges vertices 2 and 3 while leaving 1 fixed, whereas r maps 1 to 2 to 3. Thus we can associate them with permutations of the integers $\{1, 2, 3\}$, see Sec. 2.2, writing

$$e = (),\ \ a = (23),\ \ b = (13),\ \ c = (12),\ \ r = (123),\ \ s = (132), \tag{4}$$

where () is the identity permutation.

• In fact these are all the 6 permutations possible on $\{1, 2, 3\}$, so D_3 is essentially the same thing as the symmetric group S_3, see Sec. 2.2.

★ Rotations about the origin and reflections in lines through the origin of the x, y plane can be represented by matrices. Thus a counterclockwise rotation by an angle θ will move a point (x, y) to a new point (x', y'), where

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. \tag{5}$$

• Thinking of the elements of D_3 as mapping the plane in the manner shown in the figure we can associate them with 2×2 matrices as follows, where I corresponds to the identity e, A to a, etc.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad B = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix} \quad C = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}$$
$$R = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix} \quad S = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix} \tag{6}$$

• The group operation then corresponds to, or can be represented by, matrix multiplication. Thus

$$AR = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix} = B \tag{7}$$

in agreement with $ar = b$ from the group multiplication table.

★ Subgroups of D_3. There are four proper subgroups:

$$F_a = \{e, a\} = \langle a\rangle, \;\; F_b = \{e, b\} = \langle b\rangle, \;\; F_c = \{e, c\} = \langle c\rangle, \;\; F_r = \{e, r, s\} = \langle r\rangle, \tag{8}$$

∘ Here $\langle a\rangle$ means the subgroup generated by a. See additional comments in Sec. 5

3 Conjugacy and Classes

★ Two members a and b of a group G are said to be *conjugate*, which we write as $a \sim b$, provided there is some $g \in G$ such that $a = gbg^{-1}$. It is obvious that $a \sim a$, that $a \sim b$ implies $b \sim a$, and easily checked that if $a \sim b$ and $b \sim c$, then $a \sim c$. This means $\sim$ is an *equivalence relation*, and the set G will split up into disjoint *equivalence classes*, referred to as *conjugacy classes* or simply *classes*.

• For D_3, Sec. 2.3, the classes are

$$\mathcal{C}_1 = \{e\}, \quad \mathcal{C}_2 = \{a, b, c\}, \quad \mathcal{C}_3 = \{r, s\} \tag{9}$$

∘ Note that e is always in a class by itself.

• The reflections are all in one class, and the rotations are in another. It is typical that members of a class somehow resemble one another, or at least seem more similar than two group elements belonging to different classes.

★ Two subgroups are said to be *conjugate* if for some *fixed* g the the map $a \to gag^{-1}$ carries one subgroup into the other. Again, the intuition is that the subgroups are in some sense very similar.

□ Exercise. Which subgroups of D_3 are conjugate?

★ If the subgroup is carried into itself by the $a \to gag^{-1}$ map for *every* $g \in G$, the subgroup is said to be *normal* or *self conjugate* or *invariant*. Equivalently, such a subgroup consists of complete conjugacy classes: if it contains one member of a class it contains them all.

□ Exercise. What are the normal subgroups of D_3?

4 Morphisms

★ A *homorphism* is a map $\phi : G \to H$ from a group G to a group H that preserves group multiplication: $\phi(a)\phi(b) = \phi(ab)$ for any a and b in G.

∘ If γ is the binary operation in G and η the one in H, what one requires is $\eta(\phi(a), \phi(b)) = \phi(\gamma(a, b))$.

★ Note that in general ϕ is neither injective nor surjective. HNG, Ch. I, Sec. 2 (p. 30) uses separate terms as follows: the homomorphism is

a *monomorphism* if ϕ is an injection (one-to-one)

an *epimorphism* if ϕ is a surjection (onto)

an *isomorphism* if ϕ is a bijection (one-to-one and onto).

In addition, in the case of a surjective homomorphism from G to H one says that "H is *homomorphic* to G", unless one knows that the homomorphism is actually an isomorphism, in which case say "H is *isomorphic* to G," and write $G \cong H$.

★ To add to the terminological overload. If H is the same as G, a homomorphism is called an *endomorphism* and an isomorphism is an *automorphism*.

★ Two groups which are isomorphic to each other are "the same group" in the sense that they contain the same number of elements obeying identical multiplication rules. However, in a particular context two isomorphic groups may well have a different physical significance. Thus the crystallographers distinguish D_3, meaning three 2-fold axes perpendicular to the 3-fold axis, from C_{3v}, meaning a 3-fold axis and 3 reflection planes that contain that axis. The groups are isomorphic to each other and to S_3, but no crystallographer is going to confuse the symmetry class of quartz (D_3) with that of lithium sodium sulfate (C_{3v}).

★ The *kernel* of a homomorphism $\phi : G \to H$ is the set of elements of G which are mapped into the identity element of H. It is always a normal subgroup.

□ Exercise. Prove it.

5 Generators and Free Groups

★ Let a be some element of a group G, define $a^0 = e$, and for n a positive integer, $a^n = aa \cdots a$ the product of a with itself n times, $a^{-n} = a^{-1}a^{-1} \cdots a^{-1}$ the product of a^{-1} with itself n times. The collection of these a^n, where n can be positive or negative or zero, is then a subgroup of G denoted by $\langle a \rangle$. It is the *cyclic* group *generated* by a, and "cyclic group" means a group of this form.

• If there is a smallest $N \geq 1$ such that $a^N = e$, this N is called the *order* of a. In fact it is the order of the subgroup $\langle a \rangle$. In this case $\langle a \rangle \cong Z_N$.

• If the order of a is infinite, $\langle a \rangle \cong Z$.

★ More generally, if T is any subset of G, $\langle T \rangle$ is defined to be the smallest subgroup containing T as a subset, the subgroup *generated* by T. If $\langle T \rangle = G$, one says that T, or the elements in T, generate G. The $\{\}$ denoting a set can be omitted; $\langle \{a, b\} \rangle$ can be written $\langle a, b \rangle$.

★ When discussing a group it is often useful to focus on a set of *generators* which together with some *relations* determine the whole group and its multiplication table.

• Let us illustrate the idea with an example in which there are two generators a and b. As a first step we consider the *free group* generated by a and b, which is the collection of all "words" of the form $a^{m_1}b^{n_1}a^{m_2}b^{n_2} \cdots a^{m_r}b^{n_r}$, where r is any positive integer, and the m_j and n_j may be any integers, including negative values and 0. If $m_2 = 0$ we can remove this term from the word, leaving $a^{m_1}b^{n_1+n_2} \cdots$, whereas if $m_1 = 0$ we obtain a word beginning with some power of b. The product of two words is defined the way you would expect, for example:

$$(ab)(a^2b) = aba^2b, \quad (b^2a^2b^2)(b^{-1}a^{-1}) = b^2a^2ba^{-1}, \quad (a^2b^{-2})(b^2a^{-3}b^{-2}) = a^{-1}b^{-2}. \tag{10}$$

• Consider what happens to our free group generated by a and b when we employ the three relations

$$a^2 = e, \quad b^2 = e, \quad (ab)^3 = ababab = e. \tag{11}$$

Since the first two tell us that $a^{-1} = a$ and $b^{-1} = b$, we can eliminate all negative exponents from all the words in the free group, and we can also eliminate all positive exponents larger than 2. So we need only consider words of the sort a, b, ab, ba, aba, and so forth. There are still an infinite number of these, but the third relation along with others obtained from it using the first two, such as

$$babab = a, \quad abab = ba, \quad bab = aba \tag{12}$$

allow us to get rid of anything longer than three letters. A bit of checking shows that only six distinct elements remain:

$$e, \ a, \ b, \ ab, \ ba, \ aba \tag{13}$$

Furthermore, the group table can be worked out by taking products of these and again using the relations when needed: e.g., $(b)(ab) = bab = aba$.

□ Exercise. Show that the group constructed in this way is isomorphic to D_3.

6 Cosets and the Quotient Group

★ Multiplication of subsets S and T of a group G. Define ST to be the subset of elements of G of the form st for some $s \in S$ and some $t \in T$.

○ In general $ST \neq TS$, for a nonabelian group.

○ If some element of ST can be obtained in more than one way, thus $st = s't'$, it is still only counted once in the set ST.

• We use gT to denote $\{gt_1, gt_2, \ldots\}$ when $T = \{t_1, t_2, \ldots\}$

★ Let S be a *subgroup* of G. Then gS, where g is any element of G is called a *left coset*. Similarly, Sg is a *right coset*.

• The number of elements in a coset is the same as the number in the original subgroup.

□ Exercise. Prove it.

★ For a given subgroup S, two left cosets are either identical (they contain the same elements of G) or they are disjoint—no elements in common. This follows from the fact that g and h belong to the same left coset if $g^{-1}h$ is an element of S, and the property just mentioned is an equivalence relation.

□ Exercise. Prove it.

★ Since every group element belongs to one and only one coset of S, the group G is the union of these disjoint cosets. The number of distinct cosets is called the *index* of S in G, denoted by $[G : S]$.

• This means among other things that if G is finite, the order $|S|$ of any subgroups S must divide $|G|$.

• Naturally, what has just been said about left cosets applies equally well to right cosets; e.g., we could define the index in terms of the number of right cosets.

∘ Remember, however, that in general left cosets are *not* the same as right cosets. Splitting a group into left cosets or into right cosets are two distinct ways of cutting the cake into pieces of equal size.

★ In the case of a *normal* (invariant, self-conjugate) subgroup, see the definition in Sec. 3, the left cosets and right cosets are identical, so one can speak of "cosets" without an adjective.

• A normal subgroup N can be characterized in various ways. It consists of complete classes (Sec. 3). It commutes with every $g \in G$ in the sense that $gN = Ng$. (Note that this does *not* imply that g commutes with each element of N!) For each $g \in G$ it is the case that $gNg^{-1} = N$.

□ Exercise. Check that these characterizations are equivalent.

□ Exercise. Show that if $[G : S] = 2$, S is necessarily a normal subgroup. Could we replace 2 with 3?

★ Given a group G and N a normal subgroup of G, the *quotient group* or *factor group* G/N is defined to the group whose elements are the different cosets of N, and group multiplication is defined by multiplying the cosets together as sets. Thus

$$(gN)(hN) = gNhN = ghNN = ghN. \tag{14}$$

∘ Note that the same coset may be written gN using various choices for g—any g that lies in the coset provides an equally good "label." Hence the preceding equation deserves a little thought; one should check that it makes sense.

□ Exercise. Go ahead and check it.

• The order of the quotient group times that of the normal subgroup is equal to the order of the original group G: $|N| \cdot |G/N| = |G|$.

• Example. Let $2Z = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$. It is a subgroup of Z, and since Z is abelian, any subgroup is normal. Then $Z/2Z \cong Z_2$.

• Example. The subgroup $S = \{e, r, s\}$ is a normal subgroup of D_3, and $D_3/S \cong Z_2$.

7 Products

• If $Q \cong G/N$ one would expect that in some sense G is the product of Q and N, and this is indeed the case. However, elucidating "in some sense" is a trifle tricky, since there is more than one useful way to define the product of two (or more) groups.

★ The *direct product* $G \times H$ of two groups G and H is defined as follows. First form the Cartesian product $J = G \times H$ of the two sets, which is to say the set of all pairs of the form (g, h) with $g \in G$ and $h \in H$. Next, define group multiplication by

$$(g, h)(g', h') = (gg', hh'). \tag{15}$$

The identity is (e, e), the inverse of (g, h) is (g^{-1}, h^{-1}). It is straightforward to show that J satisfies all the rules and is thus a genuine group.

∘ The order of J is $|G|\,|H|$, the product of the orders of G and H.

• One can think of the factors G and H as subgroups of J in the sense that each $g \in G$ is identified with (g, e), and each $h \in H$ with (e, h). Thought of in this way, both G and H are normal subgroups of J, and the elements of G commute with those of H, since

$$(g, e)(e, h) = (g, h) = (e, h)(g, e). \tag{16}$$

Further, every element of J can be expressed in a *unique* way as a product of an element of G and one of H.

• Extending these ideas to the direct product of any finite collection of groups is straightforwad. For infinite collections, consult HNG, Ch. I, Sec. 8.

★ Suppose that N is a normal subgroup of G, and $Q = G/N$. In general G is *not* isomorphic to the direct product of Q and N, as can be seen in various examples. Thus $D_3/S \cong Z_2$, but S and Z_2 are abelian groups, and therefore so is $S \times Z_2$, unlike D_3. Or let $2Z$ be the even integers; then $Z/2Z \cong Z_2$. But Z is not isomorphic to the direct product of $2Z$ and Z_2.

□ Exercise. Show that Z is not isomorphic to the direct product of $2Z$ and Z_2.

★ A group G is a direct product if and only if one can find *two* nontrivial (neither of them is just the identity) normal subgroups with the property that: (i) they have no elements in common apart from the identity; (ii) together they generate the group.

• For G to be the direct product of r groups one must be able to find r normal subgroups which together generate G, and the "no element in common" condition is that each normal subgroup j should have nothing in common with the subgroup *generated by* the remaining $r-1$ normal subgroups, aside from the identity e. See HNG, p. 61.

★ In cases in which G is *not* a direct product of a normal subgroup N and the quotient $Q = G/N$, is there still some "natural" way to reconstitute G from Q and N? Yes there is, but it is not altogether straightforward. We define an *extension* of a group Q by a group N in the following manner.

• Form the Cartesian product $N \times Q$, where it will be convenient to use lower case Roman for elements of N and lower case Greek for elements of Q, thus pairs of the form (a, λ). We have the same number of pairs as elements of G, which is a good beginning.

• A very natural way of associating each pair of this type with an element of G is as follows. We know that λ refers to a coset of N in G. For each coset, choose one of its members to "represent" it, and let the representative of coset λ, which is an element of G, be denoted by $k(\lambda)$. There is no obvious way to choose it, except for the identity ϵ of Q, which means the coset equal to N itself: in this case let $k(\epsilon) = e$.

• Now make the following association of pairs in $N \times Q$ with elements of G.

$$(a, \lambda) \leftrightarrow ak(\lambda). \tag{17}$$

□ Exercise. Show that this association is a bijection from $N \times Q$ to G.

★ Next we need a multiplication rule for pairs of the form (a, λ). We already know the meaning of ab when a and b are members of N. The product $\lambda\mu$ for Q is also well defined, and one can think of it as the coset that contains $k(\lambda)k(\mu)$, the product (in G) of the two representatives. But of course we cannot simply write $(a, \lambda)(b, \mu) = (ab, \lambda\mu)$, for that takes us back to a direct product, which (in general) won't work.

★ The trick is to use the association (17) to *define* the multiplication of pairs so that it corresponds exactly to the multiplication of elements of G. Here is how it works:

$$(a, \lambda)(b, \mu) \leftrightarrow ak(\lambda)bk(\mu) = as_\lambda(b)k(\lambda)k(\mu) = as_\lambda(b)c_{\lambda,\mu}k(\lambda\mu). \tag{18}$$

where

$$s_\lambda(b) = k(\lambda)bk^{-1}(\lambda), \quad k(\lambda)k(\mu) = c_{\lambda,\mu}k(\lambda\mu). \tag{19}$$

• That is to say, in taking the product of (a, λ) with (b, μ), we follow the same rule as a direct product for the Q part—the result is $\lambda\mu$—but not for the N part. Instead there is a rather complicated product of three different elements of N, $as_\lambda(b)c_{\lambda,\mu}$. The a part is the same as a direct product, but in place of b we carry out a transformation $b \to s_\lambda(b)$, where s_λ is an automorphism of N (since it is an inner automorphism of G), and $c_{\lambda,\mu}$ is a "correction" that depends upon both λ and μ, and arises for the following reason. It is a simple exercise to show that the product $k(\lambda)k(\mu)$ (in G) is an element of the coset labeled $\lambda\mu$, but of course it need not be equal to the $k(\lambda\mu)$ we have, somewhat arbitrarily, chosen to represent this coset. It can, however, only differ from $k(\lambda\mu)$ by something which lies in N, and it is this something that we write as $c_{\lambda,\mu}$. Granted, we might have made other choices for coset representatives, replacing $k(\lambda)$ with $\bar{k}(\lambda)$, and maybe some clever choice would have eliminated the need to introduce the $c_{\lambda,\mu}$, but looking at particular examples shows that this is not possible in general.

• The multiplication rule constructed in this way will be associative, because we obtained it by starting with G, where the multiplication rule was associative to begin with. One can, however, imagine starting out instead with two arbitrary groups N and Q, forming pairs, introducing automorphisms s_λ and $c_{\lambda,\mu}$ corrections, and defining multiplication by the preceding formulas. Will the result be an associative multiplication? Generally not, unless the s_λ and the $c_{\lambda,\mu}$ satisfy some rather complicated rules given in EDM Sec. 190 N.

★ But sometimes life is simpler and one can set $c_{\lambda,\mu} = e$, which is to say ignore it, for all λ and μ. In that case one calls the result a *semidirect* product: for each $\lambda \in Q$ there is some automorphism s_λ of N, and

$$(a, \lambda)(b, \mu) = (as_\lambda(b), \lambda\mu) \tag{20}$$

is the multiplication rule.

□ Exercise. Produce D_3 as the semidirect product of S (playing the role of N in the above discussion) and Z_2 playing the role of Q.

□ Exercise. Reconstitute the group Z from $2Z$ (as N) and Z_2 (as Q). Hint: make s_λ the identity automorphism, which means you can forget it, and employ a suitable $c_{\lambda,\mu}$, which is not hard to find.