

Der Spiegel (The Mirror) Duet

VIOLINI *Allegro* ♩=120

W.A. Mozart

Public Domain. Sequenced by Fred Nachbaur using NoteWorthy
Confused? Try playing this from opposite sides of a table.

Allegro
VIOLINI

(Note: the attribution to Mozart is dubious)

DOPPELGÄNGER

Entering the lonely house with my wife
 I saw him for the first time
 Peering furtively from behind a bush—
 Blackness that moved,
 A shape amid the shadows,
 A momentary glimpse of gleaming eyes
 Revealed in the ragged moon.
 A closer look (he seemed to turn) might have
 Put him to flight forever—
 I dared not
 (For reasons that I failed to understand),
 Though I knew I should act at once.

I puzzled over it, hiding alone,
 Watching the woman as she neared the gate.
 He came, and I saw him crouching
 Night after night.
 Night after night
 He came, and I saw him crouching,
 Watching the woman as she neared the gate.

I puzzled over it, hiding alone—
 Though I knew I should act at once,
 For reasons that I failed to understand
 I dared not
 Put him to flight forever.

A closer look (he seemed to turn) might have
 Revealed in the ragged moon
 A momentary glimpse of gleaming eyes,
 A shape amid the shadows,
 Blackness that moved.

Peering furtively from behind a bush,
 I saw him, for the first time,
 Entering the lonely house with my wife.

—by J. A. Lyndon,
 from *Palindromes and Anagrams*,
 H. W. Bergerson, Dover 1973.

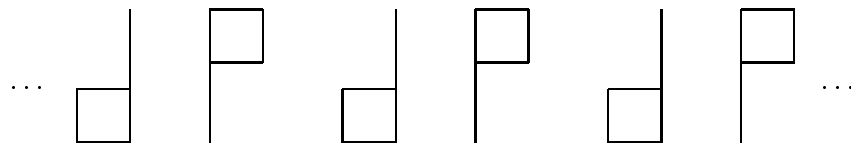


This is the musical equivalent of the *palindrome*. One example of a musical form involving this kind of symmetry is the *retrograde canon* or *crab canon* (Cancrizans). This term denotes a work in the form of a canon and exhibiting temporal reflectional symmetry by means of playing the melody forwards and backwards at the same time. For example, the first canon of J. S. Bach's *Musical Offering* (BWV 1079) is a retrograde canon formed by playing Frederick the Great's royal theme, consisting of the following 18 bars

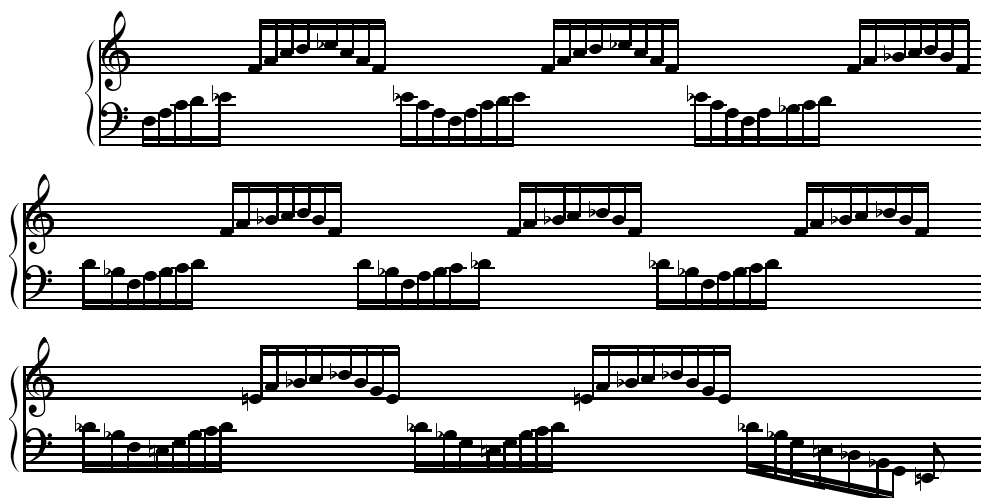


simultaneously forwards and backwards in this way. The first voice starts at the beginning of the first bar and works forward to the end, while the second voice starts at the end of the last bar and works backwards to the beginning. Other examples can be found at the end of this section, under "further listening."

Examples of *rotational* symmetry can also be found. This really means that we have translations and rotations, as in the following diagram. In group theoretic language, the symmetries form an *infinite dihedral group*.



In the following example, from the middle of Mozart's *Capriccio*, KV 395 for piano, the symmetry is approximate. It is easy to observe that each beamed set of notes for the right hand has a gradual rise followed by a steeper descent, while those for the left hand have a steep descent followed by a more gradual rise. Each pair of beams is slightly different from the previous, so we do not get bored. Our expectations are finally thwarted in the last beam, where the descent continues all the way down to a low E♭.



Further listening: (see Appendix R)

William Byrd, *Diliges Dominum* exhibits temporal reflectional symmetry, making it a perfect palindrome.

In Joseph Haydn's *Sonata 41* in A, the movement *Menuetto al rovescio* is also a perfect palindrome.

Guillaume de Machaut, *Messe de Notre Dame*, *Ma fin est mon commencement* (My end is my beginning), a retrograde canon in three voices, with a palindromic tenor line.

8.2. Sets and groups

The mathematical structure which captures the notion of symmetry is the notion of a *group*. In this section, we give the basic axioms of group theory, and we describe how these axioms capture the notion of symmetry.

A *set* is just a collection of objects. The objects in the set are called the *elements* of the set. We write $x \in X$ to mean that an object x is an element of a set X .

Strictly speaking, a set shouldn't be too big. For example, the collection of all sets is too big to be a set, and if we allow it to be a set then we run into Russell's paradox, which goes as follows. If the collection of all sets is regarded as a set, then it is possible for a set to be an element of itself: $X \in X$. Now form the set S consisting of all sets X such that $X \notin X$. If $S \notin S$ then $S \in S$, and if $S \in S$ then $S \notin S$. This contradictory conclusion is Russell's paradox. Fortunately, finite and countably infinite collections are small enough to be sets, and we are mostly interested in such sets.¹ If a set X is finite, we write $|X|$ for the number of elements in X .

¹For a reasonably modern and sophisticated introduction to set theory, I recommend W. Just and M. Weese, *Discovering modern set theory*, two volumes, published by the American Mathematical Society, 1995. None of the sophistication of modern set theory is necessary for music theory.

A *group* is a set G together with an operation which takes any two elements g and h of G and multiplies them to give again an element of G , written gh . For G to be a group, this multiplication must be defined for all pairs of elements g and h in G , and it must satisfy three axioms:

(i) (Associative law) Given any elements g , h and k in G (not necessarily different from each other), if we multiply gh by k we get the same answer as if we multiply g by hk :

$$(gh)k = g(hk).$$

(ii) (Identity) There is an element $e \in G$ called the *identity element*, which has the following property. For every element g in G , we have $eg = g$ and $ge = g$.

(iii) (Inverses) For each element $g \in G$, there is an *inverse* element written g^{-1} , with the property that $gg^{-1} = e$ and $g^{-1}g = e$.

It is worth noticing that a group does *not* necessarily satisfy the commutative law. An *abelian group* is a group satisfying the following axiom in addition to axioms (i)–(iii):

(iv) (Commutative law)² Given any elements g and h in G , we have $gh = hg$.

We can give a group by writing down a *multiplication table*. For example, here is the multiplication table for a group with three elements.

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

To multiply elements g and h of a group using a multiplication table, we look in row g and column h , and the entry is gh . So for example, looking in the above table, we see that $ab = e$. The above example is an abelian group, because the table is symmetric about its diagonal. The following multiplication table describes a nonabelian group G with six elements.

	e	v	w	x	y	z
e	e	v	w	x	y	z
v	v	w	e	y	z	x
w	w	e	v	z	x	y
x	x	y	z	e	v	w
y	y	z	x	w	e	v
z	z	x	y	v	w	e

In this group, we have $xy = v$ but $yx = w$, which shows that the group is not abelian. We write $|G| = 6$ to indicate that the group G has six elements.

²In real life, as in group theory, operations seldom satisfy the commutative law. For example, if we put on our socks and then put on our shoes, we get a very different effect from doing it the other way round. The associative law is much more commonly satisfied.

Groups don't have to be finite of course. For example, the set \mathbb{Z} with operation of *addition* forms an abelian group. Usually, a group operation is only written additively if the group is abelian. The identity element for the operation of addition is 0, and the inverse of an integer n is $-n$.

It should be now be apparent that multiplication tables aren't a very good way of describing a group. Suppose we want to check that the above multiplication table satisfies the axioms (i)–(iii). We would have to make $6 \times 6 \times 6 = 216$ checks just for the associative law. Now try to imagine making the checks for a group with thousands of elements, or even millions.

Fortunately, there is a better way, based on permutation groups. A *permutation* of a set X is a function f from X to X such that each element x of X can be written as $f(y)$ for a unique $y \in X$. See page 248 for more discussion of this definition. This ensures that f has an *inverse function*, f^{-1} which takes x back to y . So we have $f^{-1}(f(y)) = f^{-1}(x) = y$, and $f(f^{-1}(x)) = f(y) = x$.

For example, if $X = \{1, 2, 3, 4, 5\}$, the function f defined by

$$f(1) = 3, \quad f(2) = 5, \quad f(3) = 4, \quad f(4) = 1, \quad f(5) = 2$$

is a permutation of X . There are two common notations for writing permutations on finite sets, both of which are useful. The first notation lists the elements of X and where they go. In this notation, the above permutation f would be written as follows.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

The other notation is called *cycle notation*. For the above example, we notice that 1 goes to 3 goes to 4 goes back to 1 again, and 2 goes to 5 goes back to 2. So we write the permutation as

$$f = (1, 3, 4)(2, 5).$$

This notation is based on the fact that if we apply a permutation repeatedly to an element of a finite set, it will eventually cycle back round to where it started. The entire set can be split up into disjoint cycles in this way, so that each element appears in one and only one cycle. If a permutation is written in cycle notation, to see its effect on an element, we locate the cycle containing the element. If the element is not at the end of the cycle, the permutation takes it to the next one in the cycle. If it is at the end, it takes it back to the beginning. The *length* of a cycle is the number of elements appearing in it. If a cycle has length one, then the element appearing in it is a *fixed point* of the permutation. Fixed points are often omitted when writing a permutation in cycle notation.

To multiply permutations, we compose functions. In the above example, suppose we have another permutation g of the same set X , given by

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$$

or in cycle notation,

$$g = (1, 2, 5, 3)(4).$$

If we omit the fixed point 4 from the notation, this element is written $g = (1, 2, 5, 3)$. Then $f(g(1)) = f(2) = 5$. Continuing this way, fg is the following permutation,

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix} = (1, 5, 4)$$

whereas gf is given by

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

The *identity permutation* takes each element of X to itself. In the above example, the identity permutation is

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1)(2)(3)(4)(5).$$

Omitting fixed points from the identity permutation leaves us with a rather embarrassing empty space, which we fill with the sign e denoting the identity element. The *order* of a permutation is the number of times it has to be applied, to get back to the identity permutation. In the above example, f has order six, g has order four, and both fg and gf have order three. The order of an element g of any group is defined in the same way, as the least positive value of n such that $g^n = 1$. If there is no such n , then g is said to have *infinite order*. For example, the translation which began the chapter is a transformation of infinite order, whereas a reflection is a transformation of order two.

Notice how the commutative law is not at all built into the world of permutations, but the associative law certainly is. The inverse of a permutation is a permutation, and the composite of two permutations is also a permutation. So it is easy to check whether a collection of permutations forms a group. We just have to check that the identity is in the collection, and that the inverses and composites of permutations in the collection are still in the collection.

The set of *all* permutations of a set X forms a group which is called the *symmetric group* on the set X , with the multiplication given by composing permutations as above. We write the symmetric group on X as $\text{Symm}(X)$. If $X = \{1, 2, \dots, n\}$ is the set of integers from 1 to n , then we write S_n for $\text{Symm}(X)$. Notice that the sets X and $\text{Symm}(X)$ are quite different in size. If $X = \{1, 2, \dots, n\}$ then X has n elements, but $\text{Symm}(X)$ has $n!$ elements. To see this, if $f \in \text{Symm}(X)$ then there are n possibilities for $f(1)$. Having chosen the value of $f(1)$, there are $n - 1$ possibilities left for $f(2)$. Continuing this way, the total number of possibilities for f is $n(n - 1)(n - 2) \dots 1 = n!$.

The definition of a *permutation group* is that it is a subgroup of $\text{Symm}(X)$ for some set X . In general, a *subgroup* H of a group G is a subset of G which is a group in its own right, with multiplication inherited from G . This is the same as saying that the identity element belongs to H , inverses

of elements of H are also in H , and products of elements of H are in H . So to check that a set H of permutations of X is a group, we check these three properties so that H is a subgroup of $\text{Symm}(X)$. Notice that the associative law is automatic for permutations, and does not need to be checked.

Exercises

1. If g and h are elements of a group, explain why gh and hg always have the same order.

8.3. Change ringing

The art of change ringing is peculiar to the English, and, like most English peculiarities, unintelligible to the rest of the world. To the musical Belgian, for example, it appears that the proper thing to do with a carefully tuned ring of bells is to play a tune upon it. By the English campanologist, the playing of tunes is considered to be a childish game, only fit for foreigners; the proper use of the bells is to work out mathematical permutations and combinations. When he speaks of the music of his bells, he does not mean musicians' music—still less what the ordinary man calls music. To the ordinary man, in fact, the pealing of bells is a monotonous jangle and a nuisance, tolerable only when mitigated by remote distance and sentimental association. The change-ringer does, indeed, distinguish musical differences between one method of producing his permutations and another; he avers, for instance, that where the hinder bells run 7, 5, 6, or 5, 6, 7, or 5, 7, 6, the music is always prettier, and can detect and approve, where they occur, the consecutive fifths of Tittums and the cascading thirds of the Queen's change. But what he really means is, that by the English method of ringing with rope and wheel, each several bell gives forth her fullest and her noblest note. His passion—and it is a passion—finds its satisfaction in mathematical completeness and mechanical perfection, and as his bell weaves her way rhythmically up from lead to hinder place and down again, he is filled with the solemn intoxication that comes of intricate ritual faultlessly performed.

Dorothy L. Sayers, *The Nine Tailors*, 1934

The symmetric group, described at the end of the last section, is essential to the understanding of *change ringing*, or *campanology*. This art began in England in the tenth century, and continues in thousands of English churches to this day. A set of swinging bells in the church tower is operated by pulling ropes. There are generally somewhere between six and twelve bells. The problem is that the bells are heavy, and so the timing of the peals of the bells is not easy to change. So for example, if there were eight bells, played in sequence as

$$1, 2, 3, 4, 5, 6, 7, 8,$$

then in the next round we might be able to change the positions of some adjacent bells in the sequence to produce

$$1, 3, 2, 4, 5, 7, 6, 8,$$

but we would not be able to move a bell more than one position in the sequence. So the general rules for change ringing state that a change ringing composition consists of a sequence of rows. Each row is a permutation of the set of bells, and the position of a bell in the row can differ by at most one from its previous position. It is also stipulated that a row is not repeated in a composition, except that the last row returns to the beginning. So for example Plain Bob on four bells goes as follows.

1	2	3	4	
2	1	4	3	
2	4	1	3	
4	2	3	1	
4	3	2	1	
3	4	1	2	
3	1	4	2	
1	3	2	4	
1	3	4	2	
3	1	2	4	
3	2	1	4	
2	3	4	1	
2	4	3	1	Plain Bob
4	2	1	3	
4	1	2	3	
1	4	3	2	
1	4	2	3	
4	1	3	2	
4	3	1	2	
3	4	2	1	
3	2	4	1	
2	3	1	4	
2	1	3	4	
1	2	4	3	
1	2	3	4	

This sequence of rows is really a walk around the symmetric group S_4 . So the image of the first row under each of the $4! = 24$ elements of S_4 appears exactly once in the list, except that the first is repeated as the last.

In order to fix the notation, we think of a row as a function from the bells to the time slots. To go from one row to the next, we compose with a permutation of the set of time slots. The permutation is only allowed to fix a time slot, or to swap it with an adjacent time slot. So in the above example, the first few steps involve alternately applying the permutations $(1,2)(3,4)$ and $(1)(2,3)(4)$. Then when we reach the row 1 3 2 4, this prescription would take us back to the beginning. In order to avoid this, the permutation $(1)(2)(3,4)$ is applied, and then we may continue as before. At the line 1 4 3 2 we again have the problem that we would be taken to a previously used row, and we avert this by the same method. When we have exhausted all the permutations in S_4 , we return to the beginning.

Exercises

- The *Plain Hunt* consists of alternately applying the permutations

$$a = (1,2)(3,4)(5,6) \dots$$

$$b = (1)(2,3)(4,5) \dots$$

If the number of bells is n , how many rows are there before the return to the initial order?

[Hint: treat separately the cases n even and n odd.]

Further reading:

Wilfred G. Wilson, *Change Ringing*, October House Inc., New York, 1965.

8.4. Cayley's theorem

Cayley's theorem explains why the axioms of group theory exactly capture the physical notion of symmetry. It says that any abstract group, in other words, any set with a multiplication satisfying the axioms described in Section 8.2, can be realised as a group of permutations of some set.

There is something mildly puzzling about this theorem. Where are we going to produce a set from? We're just given a group, and nothing else. So we do the obvious thing, and use the set of elements of the group itself as the set on which it will act as permutations. So before reading this, make very sure you have separated in your mind the set of elements of a permutation group and the set on which it acts by permutations. Because otherwise what follows will be very confusing.

Let G be a group. Then to each element $g \in G$, we assign the permutation in $\text{Symm}(G)$ which sends an element $h \in G$ to $gh \in G$. We want to say that this displays a copy of the group G as a permutation group inside $\text{Symm}(G)$. The best way to say this is to introduce the notion of a *homomorphism* of groups.

Recall that a *function* f from one set X to another set Y , written $f: X \rightarrow Y$, simply assigns an element $f(x)$ of Y to each element x of X in a well defined manner. Many elements of X are allowed to go to the same place in Y , and not every element of Y needs to be assigned. The *image* of f is the subset of Y consisting of the elements of the form $f(x)$. The function f is *injective* if no two elements of X go to the same place in Y . The function f is *surjective* if every element of Y is in the image of f . A function f which is both injective and surjective is said to be *bijective*. A bijective function is also called a one-one correspondence. A bijective function is the same thing as a function which has an *inverse*, namely a function $f': Y \rightarrow X$ with the property that $f'(f(y)) = y$ for all $y \in Y$, and $f(f'(x)) = x$ for all $x \in X$. Namely, f' takes y to the unique x such that $y = f(x)$. In this language, a permutation of a set X is just a bijective function from X to itself.

If G and H are groups, then a *homomorphism* $f: G \rightarrow H$ is a function from the set G to the set H which "preserves the multiplication" in the sense that it sends the identity element of G to the identity element of H , and for elements g_1 and g_2 in G we have

$$f(g_1g_2) = f(g_1)f(g_2).$$

The image of a homomorphism f has the property that it is a subgroup of H . An injective homomorphism is called a *monomorphism*. A surjective homomorphism is called an *epimorphism*. A bijective homomorphism is called an *isomorphism*. If there is an isomorphism from G to H , we say that G and H are *isomorphic*. This means that they are "really" the same group, except that the elements happen to have different names. If f is a monomorphism, it can be regarded as identifying G with a subgroup of H . In other words, it induces an isomorphism between G and its image, which is a subgroup of H .

EXAMPLE 8.4.1. Consider the group G of rotational symmetries of a cube. In other words, an element of G consists of a way of rotating a cube so that the faces are aligned in the same direction as they started. There are 24 elements of G , because we can put any one of six faces downwards, and four different ways round. Once we have decided which face to put downwards, and which way round to put it, the rotational symmetry is completely described. To multiply elements g and h of G to get gh is to do the rotational symmetry h followed by the rotational symmetry g , so that

$$gh(x) = g(h(x)).$$

The confusing order in which things happen is because we write our functions on the left of their arguments, so that $g(h(x))$ means first do h , then do g .

There is an isomorphism between this group G of symmetries of the cube and the group $\text{Symm}\{a, b, c, d\}$ of permutations on a set of four objects. This may be visualized by labeling the four main diagonals of the cube with the symbols a, b, c, d and seeing the effect of a rotation on this labeling.

In the language of homomorphisms, we can describe Cayley's theorem as follows.

THEOREM 8.4.2 (Cayley). *If G is a group, let f be the function from G to $\text{Symm}(G)$ which is defined by $f(g)(h) = gh$. Then f is a monomorphism, and so G is isomorphic with a subgroup of $\text{Symm}(G)$.*

PROOF. First, we check that f does indeed take an element $g \in G$ to a permutation. In other words, we must check that $f(g)$ is a bijection. This is easy to check, because $f(g^{-1})$ is its inverse. Namely, for $h \in G$ we have

$$f(g^{-1})(f(g)(h)) = f(g^{-1})(gh) = g^{-1}(gh) = (g^{-1}g)h = h$$

and similarly $f(g)(f(g^{-1})(h)) = h$.

Clearly f takes the identity element of G to the identity permutation. The fact that f is a homomorphism is really a statement of the associative law in G . Namely,

$$\begin{aligned} f(g_1g_2)(h) &= (g_1g_2)h = g_1(g_2h) = f(g_1)(g_2h) \\ &= f(g_1)(f(g_2)(h)) = (f(g_1)f(g_2))(h). \end{aligned}$$

Finally, to prove that f is injective, if $f(g_1) = f(g_2)$ then for all $h \in G$, $f(g_1)(h) = f(g_2)(h)$. Taking for h the identity element of G , we see that $g_1 = g_2$. \square

8.5. Clock arithmetic and octave equivalence

Clock arithmetic is where we count up to twelve, and then start back again at one. So for example, to add $6 + 8$ in clock arithmetic, we count six up from 8 to get 9, 10, 11, 12, 1, 2, and so in this system we have $6 + 8 = 2$.

It's probably better to write 0 instead of 12, so that we go from 11 back to 0 instead of 12 to 1. So here is the addition table for this clock arithmetic.

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

In terms of group theory, the above addition table makes the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ into a group. The operation is written as addition; of course, clock arithmetic is abelian. The identity element is 0, and the inverse of i is either $-i$ or $12 - i$, depending which is in the range from 0 to 11. This group is written as $\mathbb{Z}/12$.

There is an obvious homomorphism from the group \mathbb{Z} to $\mathbb{Z}/12$. It takes an integer to the unique integer in the range from 0 to 11 which differs from it by a multiple of 12.

In musical terms, we could think of the numbers from 0 to 11 as representing musical intervals in multiples of semitones, in the twelve tone equal tempered octave. So for example 1 is represented by the permutation which increases each note by one semitone, namely the permutation

$$\begin{pmatrix} C & C\sharp & D & E\flat & E & F & F\sharp & G & G\sharp & A & B\flat & B \\ C\sharp & D & E\flat & E & F & F\sharp & G & G\sharp & A & B\flat & B & C \end{pmatrix}$$

The circulating nature of clock arithmetic then becomes *octave equivalence* in the musical scale, where two notes belong to the same *pitch class* if they differ by a whole number of octaves. Each element of $\mathbb{Z}/12$ is then represented by a different permutation of the twelve pitch classes, with the number i representing an increase of i semitones. So for example the number 7 represents the permutation which makes each note higher by a fifth. Then addition has an obvious interpretation as addition of musical intervals.

This permutation representation looks like Cayley's theorem. But making this precise involves choosing a starting point somewhere in the octave. We choose to start by representing C as 0, so that the correspondence becomes

$$\begin{array}{cccccccccccc} C & C\sharp & D & E\flat & E & F & F\sharp & G & G\sharp & A & B\flat & B \\ \hline 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \end{array}$$

Under this correspondence, each element of $\mathbb{Z}/12$ is being represented by the permutation of the twelve notes of the octave given by Cayley's theorem.

Of course, there is nothing special about the number 12 in clock arithmetic. If n is any positive integer, we may form the group \mathbb{Z}/n whose elements are the integers in the range from 0 to $n - 1$. Addition is described by adding as integers, and then subtracting n if necessary to put the answer back in the right range. So for example, if we are interested in 31 tone equal temperament, which gives such a good approximation to quarter comma meantone (see Section 6.5), then we would use the group $\mathbb{Z}/31$.

8.6. Generators

If G is a group, a subset S of the set of elements of G is said to *generate* G if every element of G can be written as a product of elements of S and their inverses.³ We say that G is *cyclic* if it can be generated by a single element g . In this case, the elements of the group can all be written in the form g^n with $n \in \mathbb{Z}$. The case $n = 0$ corresponds to the identity element, while negative values of n are interpreted to give powers of the inverse of g .

There are two kinds of cyclic groups. If there is no nonzero value of n for which g^n is the identity element, then the elements g^n multiply the same way that the integers n add. In this case, the group is isomorphic to the additive group \mathbb{Z} of integers. If there is a nonzero value of n for which g^n is the identity element, then by inverting if necessary, we can assume that n is positive. Then letting n be the smallest positive number with this property, it is easy to see that G is isomorphic to the group \mathbb{Z}/n described in the last section.

How many generators does \mathbb{Z}/n have? We can find out whether an integer i generates \mathbb{Z}/n with the help of some elementary number theory.

LEMMA 8.6.1. *Let d be the greatest common divisor of n and i . Then there are integers r and s such that $d = nr + is$.*

PROOF. This follows from Euclid's algorithm for finding the greatest common divisor of two integers. \square

If i has no common factor with n , then $d = 1$, and the above equation says that i times s , considered as the s th power of i in the additive group \mathbb{Z}/n , is equal to 1. Since the element 1 is a generator of \mathbb{Z}/n , it follows that i is also a generator.

On the other hand, if n and i have a common factor $d > 1$, then all powers of i in \mathbb{Z}/n (i.e., all multiples of i when thinking additively) give numbers divisible by d , so the number 1 is not a power of i . So we have the following.

THEOREM 8.6.2. *The generators for \mathbb{Z}/n are precisely the numbers i in the range $0 < i < n$ with the property that n and i have no common factor.* \square

³To clarify, an empty product is considered to be the identity element. So if S is empty and G is the group with one element, then S does generate G .

The number of possibilities for i in the above theorem is written $\phi(n)$, and called the *Euler phi function* of n .

For example, if $n = 12$, then the possibilities for i are 1, 5, 7 and 11, and so $\phi(12) = 4$. In terms of musical intervals, the fact that 7 is a generator for $\mathbb{Z}/12$ corresponds to the fact that all notes can be obtained from a given notes by repeatedly going up by a fifth. This is the *circle of fifths*. So it can be seen that apart from the circle of semitones upwards and downwards, the only other ways of generating all the musical intervals is via the circle of fifths, again upwards or downwards. This, together with the consonant nature of the fifth, goes some way toward explaining the importance of the circle of fifths in music.

It is interesting to see that if n happens to be a prime number, for example $n = 31$, then *every* element of \mathbb{Z}/n apart from zero is a generator.

Exercises

1. Write down the generators for $\mathbb{Z}/24$.

Further reading:

Gerald J. Balzano, *The group-theoretic description of 12-fold and microtonal pitch systems*, Computer Music Journal 4 (4) (1980), 66–84.

8.7. Tone rows

In twelve tone music, one begins with a *twelve tone row*, which consists of a sequence of twelve pitch classes in order, so that each of the twelve possible pitch classes appears just once.

More generally, we consider sequences of pitch classes, of any length, and with possible repetitions.

A *transposition* of a sequence \mathbf{x} of pitch classes by n semitones is the sequence $\mathbf{T}^n(\mathbf{x})$ in which each of the pitch classes in \mathbf{x} has been increased by n semitones. So for example if

$$\mathbf{x} = 3 \ 0 \ 8$$

then

$$\mathbf{T}^4(\mathbf{x}) = 7 \ 4 \ 0.$$

Inversion $\mathbf{I}(\mathbf{x})$ of a sequence \mathbf{x} just replaces each pitch class by its negative (in clock arithmetic). So in the above example

$$\mathbf{I}(\mathbf{x}) = 9 \ 0 \ 4.$$

The sequences $\mathbf{T}^n\mathbf{I}(\mathbf{x})$ are also regarded as inversions of \mathbf{x} . So for example

$$\mathbf{T}^6\mathbf{I}(\mathbf{x}) = 3 \ 6 \ 10$$

is an inversion of the above sequence \mathbf{x} .

The *retrograde* $\mathbf{R}(\mathbf{x})$ of \mathbf{x} is just the same sequence in reverse order. So in the above example,

$$\mathbf{R}(\mathbf{x}) = 8 \ 0 \ 3.$$

The relations among the operations \mathbf{T} , \mathbf{I} and \mathbf{R} are

$$\mathbf{T}^{12} = e, \quad \mathbf{T}^n \mathbf{R} = \mathbf{R} \mathbf{T}^n, \quad \mathbf{T}^n \mathbf{I} = \mathbf{I} \mathbf{T}^{-n}, \quad \mathbf{R} \mathbf{I} = \mathbf{I} \mathbf{R}.$$

where e represents the identity operation which does nothing.

There are four forms of a tone row \mathbf{x} . The *prime* form is the original form \mathbf{x} of the row, or any of its transpositions $\mathbf{T}^n(\mathbf{x})$. The *inversion* form is any one of the rows $\mathbf{T}^n \mathbf{I}(\mathbf{x})$. The *retrograde* form is any one of the rows $\mathbf{T}^n \mathbf{R}(\mathbf{x})$. Finally, the *retrograde inversion* form of the row is any one of the rows $\mathbf{T}^n \mathbf{R} \mathbf{I}(\mathbf{x})$.

In group theoretic terms, the operations \mathbf{T}^n ($0 \leq n \leq 11$) form a cyclic group $\mathbb{Z}/12$. The operation \mathbf{R} together with the identity operation form a cyclic group $\mathbb{Z}/2$. The operations \mathbf{T} and \mathbf{R} commute. The group theoretic way of describing a group with two types of operations which commute with each other is a Cartesian product.

8.8. Cartesian products

If G and H are groups, then the *Cartesian product*, or *direct product* $G \times H$ is the group whose elements are the ordered pairs (g, h) with $g \in G$ and $h \in H$. The multiplication is defined by

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2).$$

The identity element is formed from the identity elements of G and H . The inverse of (g, h) is (g^{-1}, h^{-1}) . The axioms of a group are easily verified, so that $G \times H$ with this multiplication does form a group.

Suppose that G and H are subgroups of a bigger group K , with the properties that each element of G commutes with each element of H , the only element which G and H have in common is the identity element (written $G \cap H = \{1\}$), and every element of K can be written as a product of an element of G and an element of H (written $K = GH$). Then there is an isomorphism from $G \times H$ to K given by sending (g, h) to gh . In this case, K is said to be an *internal direct product* of G and H .

For example, the group whose elements are the operations \mathbf{T}^n and $\mathbf{T}^n \mathbf{R}$ of §8.7 is an internal direct product of the subgroup consisting of the operations \mathbf{T}^n and the subgroup consisting of the identity and \mathbf{R} . So this group is isomorphic to $\mathbb{Z}/12 \times \mathbb{Z}/2$.

As another example, the lattice \mathbb{Z}^2 which we used in order to describe just intonation in §6.8 is really a Cartesian product $\mathbb{Z} \times \mathbb{Z}$, where \mathbb{Z} is the group of integers under addition, as usual. Similarly, the lattice \mathbb{Z}^3 of §6.9 is $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

Exercises

1. Find an isomorphism between $\mathbb{Z}/3 \times \mathbb{Z}/4$ and $\mathbb{Z}/12$. Interpret this in terms of transpositions by major and minor thirds.
2. Show that there is no isomorphism between $\mathbb{Z}/12 \times \mathbb{Z}/2$ and $\mathbb{Z}/24$.
[Hint: how many elements of order two are there?]

8.9. Dihedral groups

The operations \mathbf{T} and \mathbf{I} of §8.7 do not commute, but rather satisfy the relations $\mathbf{T}^n\mathbf{I} = \mathbf{I}\mathbf{T}^{-n}$. So we do not obtain a direct product in this case, but rather a more complicated construction, which in this case describes a *dihedral group*.

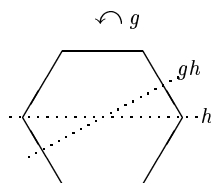
A dihedral group has two elements g and h such that $h^2 = 1$ and $gh = hg^{-1}$. Every element is either of the form g^i or of the form $g^i h$. The powers of g form a cyclic subgroup which is either \mathbb{Z}/n or \mathbb{Z} . In the former case, the group has $2n$ elements and is written⁴ D_{2n} . In the latter case, the group has infinitely many elements, and is written D_∞ and called the *infinite dihedral group*. This is one of the groups which appeared in Section 8.1.

So the operations \mathbf{T}^n and $\mathbf{T}^n\mathbf{I}$ form a group isomorphic to the dihedral group D_{24} . Finally, putting all this together, the group whose operations are

$$\mathbf{T}^n, \quad \mathbf{T}^n\mathbf{R}, \quad \mathbf{T}^n\mathbf{I}, \quad \mathbf{T}^n\mathbf{RI}$$

form a group which is isomorphic to $D_{24} \times \mathbb{Z}/2$.

The dihedral group D_{2n} has an obvious interpretation as the symmetries of a regular polygon with n sides.



The element g corresponds to counterclockwise rotation through $1/n$ of a circle, while h corresponds to reflection about a horizontal axis. Then $g^i h$ corresponds to a reflection about an axis of symmetry which is rotated from the horizontal by i/n of a semicircle. The above diagram is for the case $n = 6$.

Exercises

1. Find an isomorphism between the dihedral group D_6 and the symmetric group S_3 .
2. Find an isomorphism between D_{12} and $S_3 \times \mathbb{Z}/2$.
3. Show that D_{24} is not isomorphic to $S_3 \times \mathbb{Z}/4$.

8.10. Orbits and cosets

If a group G acts on a set X , then we say that two elements x and x' of X are in the same *orbit* if there is an element $g \in G$ such that $g(x) = x'$. This partitions X into disjoint subsets, each consisting of elements related this way. These subsets are the orbits of G on X .

So for example, if G is a cyclic group generated by an element g , then the cycles of g as described in §8.2 are the orbits of G on X .

⁴Some authors write D_n for the dihedral group of order $2n$, just to confuse matters. Presumably these authors think that I'm confusing matters.

As another example, the group $\mathbb{Z}/12$ acts on the set of tone rows of a given length, via the operations \mathbf{T}^n . Two tone rows are in the same orbit exactly when one is a transposition of the other.

If there is only one orbit for the action of G on X , we say that G acts *transitively* on X .

We discussed the related concept of cosets briefly in §6.8. Here we make the discussion more precise, and show how this concept is connected with permutations. If H is a subgroup of a group G , we can partition the elements of G into *left cosets* of H as follows. Two elements g and g' are in the same left coset of H in G if there exists some element $h \in H$ such that $gh = g'$. This partitions the group G into disjoint subsets, each consisting of elements related this way. These subsets are the left cosets of H in G . The notation for the left coset containing g is gH . So gH and $g'H$ are equal precisely when there exists an element $h \in H$ such that $gh = g'$; in other words, when $g^{-1}g'$ is an element of H . The coset gH consists of all the elements gh as h runs through the elements of H . The way of writing this is

$$gH = \{gh \mid h \in H\}.$$

The left cosets of H in G all have the same size as H does. So the number of left cosets, written $|G : H|$, is equal to $|G|/|H|$.

The example in §6.8 goes as follows. The group G is $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$. The subgroup H is the unison sublattice. Each coset consists of a set of vectors related by translation by the unison sublattice. The group theoretic notion corresponding to a periodicity block is a *set of coset representatives*. A set of left coset representatives for a subgroup H in a group G just consists of a choice of one element from each left coset.

If G acts as permutations on a set X , then there is a close connection between orbits and cosets of subgroups, which can be described in terms of *stabilizers*. If x is an element of X , then the stabilizer in G of x , written $\text{Stab}_G(x)$, is the subgroup of G consisting of the elements h satisfying $h(x) = x$.

THEOREM 8.10.1. *Let $H = \text{Stab}_G(x)$. Then the map sending the coset gH to the element $g(x) \in X$ is well defined, and establishes a bijective correspondence between the left cosets of H in G and the elements of X in the orbit containing x .*

PROOF. To say that the map is well defined is to say that if we are given another element g' such that $gH = g'H$, then $g(x) = g'(x)$. The reason why this is true is that there is an element $h \in H$ such that $gh = g'$, and then $g'(x) = gh(x) = g(h(x)) = g(x)$.

To see that the map is injective, if $g(x) = g'(x)$ then $x = g^{-1}g'(x)$ and so $g^{-1}g' \in H$, and $gH = g'H$. It is obviously surjective, by the definition of an orbit. \square

A consequence of this theorem is that the size of an orbit is equal to the index of the stabilizer of one of its elements,

$$|\text{Orbit}(x)| = |G : \text{Stab}_G(x)|. \quad (8.10.1)$$

8.11. Normal subgroups and quotients

In the last section, we discussed left cosets of a subgroup. Of course, right cosets make just as much sense; the reason why left rather than right cosets made their appearance in understanding orbits was that we write functions on the left of their arguments. We write Hg for the right coset containing g , so that

$$Hg = \{hg \mid h \in H\}.$$

It does not always happen that the left and right cosets of H are the same. For example, if G is the symmetric group S_3 , and H is the subgroup consisting of the identity and the permutation (12), then the left cosets are

$$\{e, (12)\}, \quad \{(123), (13)\}, \quad \{(132), (23)\}$$

while the right cosets are

$$\{e, (12)\}, \quad \{(123), (23)\}, \quad \{(132), (13)\}.$$

This is because $(123)(12) = (13)$ while $(12)(123) = (23)$.

A subgroup N of G is said to be *normal* if the left cosets and the right cosets agree. For example, if G is abelian, then every subgroup is normal.

THEOREM 8.11.1. *A subgroup N of G is normal if and only if, for each $g \in G$ we have $gNg^{-1} = N$.*

PROOF. To say that the subgroup N is normal means that for each $g \in G$ we have $gN = Ng$. Multiplying on the right by g^{-1} , and noticing that this can be undone by multiplication on the right by g , we see that this is equivalent to the condition that for each $g \in G$ we have $gNg^{-1} = N$. \square

If N is normal in G , then the cosets can be made into a group as follows. If gN and $g'N$ are cosets then we multiply them to form the coset $gg'N$. If you check that this is well defined, in other words, that the product does not depend on which elements are used to define the cosets, you will discover that it works precisely when N is normal in G . To check the axioms for a group, we need an identity element, which is provided by the coset $eN = N$ containing the identity element e of G . The inverse of the coset gN is the coset $g^{-1}N$. It is an easy exercise to check the axioms with these definitions.

Clock arithmetic is a good example of a quotient group. Inside the additive group \mathbb{Z} of integers, we have a (normal) subgroup $n\mathbb{Z}$ consisting of the integers divisible by n . The quotient group $\mathbb{Z}/n\mathbb{Z}$ is the clock arithmetic group, which we have been writing in the more usual notation \mathbb{Z}/n .

Another example is given by the unison vectors and periodicity blocks of §6.8. The quotient of \mathbb{Z}^2 (or more generally \mathbb{Z}^n) by the unison sublattice is a finite abelian group whose order is equal to the absolute value of the determinant of the matrix formed from the unison vectors.

There is a standard theorem of abstract algebra which says that every finite abelian group can be written in the form

$$\mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_r.$$

The positive integers n_1, \dots, n_r are not uniquely determined; for example $\mathbb{Z}/12$ is isomorphic to $\mathbb{Z}/4 \times \mathbb{Z}/3$. However, they can be chosen in such a way that each one is a divisor of the next one. If they are chosen in this way, then they are uniquely determined, and then they are called the *elementary divisors* of the finite abelian group. There is a standard algorithm for finding the elementary divisors, which can be found in many books on abstract algebra. From the point of view of scales, it seems relevant to try to choose the unison sublattice so that the quotient group is cyclic, which corresponds to the case where there is just one elementary divisor.

There is an intimate relationship between normal subgroups and homomorphisms. If f is a homomorphism from G to H , then the *kernel* of f is defined to be the set of elements $g \in G$ for which $f(g)$ is equal to the identity element of H . Writing N for the kernel of f , it is not hard to check that N is a normal subgroup of G .

THEOREM 8.11.2 (First Isomorphism Theorem). *Let f be a homomorphism from G to H . Then there is an isomorphism between the quotient group G/N and the subgroup of H consisting of the image of the homomorphism f . This isomorphism takes a coset gN to $f(g)$.*

PROOF. There are a number of things to check here. We need to check that the function from G/N to the image of f which takes gN to $f(g)$ is well defined, that it is a group homomorphism, that it is injective, and that its image is the same as the image of f . These checks are all straightforward, and are left for the reader to fill in. \square

There are actually three isomorphism theorems in elementary group theory, but we shall not mention the second or third.

An example of the first isomorphism theorem is again provided by clock arithmetic. The homomorphism from \mathbb{Z} to $\mathbb{Z}/12$ is surjective and has kernel $12\mathbb{Z}$, and so $\mathbb{Z}/12$ is isomorphic to the quotient of \mathbb{Z} by $12\mathbb{Z}$, as we already knew.

8.12. Burnside's lemma

This section and the next are concerned with problems of counting. A typical example of the kind of problem we are interested in is as follows. Recall that a tone row consists of the twelve possible pitch classes in some order. The total number of tone rows is

$$12 \times 11 \times 10 \times 9 \times \cdots \times 3 \times 2 \times 1 = 12!$$

or 479001600.

We might wish to count the number of possible twelve tone rows, where two tone rows are considered to be the same if one can be obtained from the other by applying an operation of the form \mathbf{T}^n . In this case, each tone row has twelve distinct images under these operations. So the total number of tone rows up to this notion of equivalence is $1/12$ of the number of tone rows, or $11! = 39916800$.

If we want to complicate the situation further, we might consider two tone rows to be equivalent if one can be obtained from the other using the operations \mathbf{T}^n , \mathbf{I} and \mathbf{R} . Now the problem is that some of the tone rows are fixed by some of the elements of the group. So the counting problem degenerates into a lot of special cases, unless we find a more clever way of counting. This is the kind of problem that can be solved using Burnside's counting lemma.

The abstract formulation of the problem is that we have a finite group acting as permutations on a finite set, and we want to know the number of orbits.

Burnside's lemma allows us to count the number of orbits of G , provided we know the number of fixed points of each element. It says that the number of orbits is the average number of fixed points.

LEMMA 8.12.1 (Burnside). *Let G be a finite group acting by permutations on a finite set X . For an element $g \in G$, write $n(g)$ for the number of fixed points of g on X . Then the number of orbits of G on X is equal to*

$$\frac{1}{|G|} \sum_{g \in G} n(g).$$

PROOF. We count in two different ways the number of pairs (g, x) consisting of an element $g \in G$ and a point $x \in X$ such that $g(x) = x$. If we count the elements of the group first, then for each element of the group we have to count the number of fixed points, and we get $\sum_{g \in G} n(g)$. On the other hand, if we count the elements of X first, then for each x , equation (8.10.1) shows that the number of elements $g \in G$ stabilizing it is equal to $|G|$ divided by the length of the orbit in which x lies. So each orbit contributes $|G|$ to the count. \square

So let us return to the problem of counting tone rows. Suppose that we wish to count the number of tone rows, and we wish to regard one tone row as equivalent to another if the first can be manipulated to the second using the operations \mathbf{T} , \mathbf{I} and \mathbf{R} . In other words, we wish to count the number of orbits of the group $G = D_{24} \times \mathbb{Z}/2$ generated by \mathbf{T} , \mathbf{I} and \mathbf{R} on the set X of tone rows.

In order to apply Burnside's lemma, we should find the number of tone rows fixed by each operation in the group. The identity operation fixes all tone rows, so that one is easy. The operations \mathbf{T}^n with $1 \leq n \leq 11$ don't fix any tone rows, so that's also easy. The operation \mathbf{R} fixes the tone rows whose last six entries are the reverse of the first six; but then there are repetitions so these aren't allowed as tone rows. For the operation $\mathbf{T}^6\mathbf{R}$, the fixed tone rows are the ones where the last six entries are the reverse of the first six, but transposed by a tritone (half an octave). So the first six have to be chosen in a way that uses just one of each pair related by a tritone. The number of ways of doing this is

$$12 \times 10 \times 8 \times 6 \times 4 \times 2 = 46080.$$

For values of n other than zero or six, $\mathbf{T}^n\mathbf{R}$ does not fix any tone rows, because doing this operation twice gives \mathbf{T}^{2n} , which doesn't fix any tone rows.

Next, we need to consider inversions. The operation \mathbf{I} fixes only those tone rows comprised of the entries 0 and 6; but then there must be repetitions, so these aren't tone rows. The same goes for any operation of the form $\mathbf{T}^n\mathbf{I}$; the entries come from a subset of size at most two, so we can't form a tone row this way.

Finally, for an operation $\mathbf{T}^n\mathbf{IR}$, the entries in a fixed tone row are again determined by the first six entries. So the tone row has the form

$$a_1, a_2, a_3, a_4, a_5, a_6, n - a_6, n - a_5, n - a_4, n - a_3, n - a_2, n - a_1.$$

If n is even, there is some tone fixed by $\mathbf{T}^n\mathbf{I}$, which forces us to repeat a tone, so there are no fixed tone rows. If n is odd, however, there are fixed tone rows, and there are

$$12 \times 10 \times 8 \times 6 \times 4 \times 2 = 46080$$

of them.

We summarize this information in the following table.

operation	how many in G	fixed points
identity	1	479001600
\mathbf{T}^n ($1 \leq n \leq 11$)	11	0
$\mathbf{T}^6\mathbf{R}$	1	46080
$\mathbf{T}^n\mathbf{R}$ ($n \neq 6$)	11	0
$\mathbf{T}^n\mathbf{I}$	12	0
$\mathbf{T}^n\mathbf{IR}$ (n even)	6	0
$\mathbf{T}^n\mathbf{IR}$ (n odd)	6	46080

So the sum over $g \in G$ of the number of fixed points of g on X is

$$479001600 + 7 \times 46080 = 479324160.$$

Dividing by $|G| = 48$, the total number of orbits of G on tone rows is equal to 9985920. This proves the following theorem.

THEOREM 8.12.2 (David Reiner). *If two twelve tone rows are considered the same when one may be obtained from the other using the operations \mathbf{T} , \mathbf{I} and \mathbf{R} , then the total number of tone rows is 9985920.* \square

Further reading:

D. Reiner, *Enumeration in music theory*, Amer. Math. Monthly 92 (1) (1985), 51–54.

8.13. Pólya's enumeration theorem

In this section, we address some more complicated counting problems. For example, suppose we want to know how many of chords there are, consisting of three of the twelve possible pitch classes. Suppose further that we wish to consider two chords to be equivalent if one can be obtained from the other by means of an operation \mathbf{T}^n for some n . This is a typical kind of problem which can be solved using Pólya's enumeration theorem.

A lot of physical counting problems involving symmetry are of a similar nature. A typical example would involve counting how many different necklaces can be made from three yellow beads, two blue beads and five red beads. The symmetry group in this situation is a dihedral group whose order is twice the number of beads.

In the general form of the problem, the configurations being counted are regarded as functions from a set X to a set Y , and the symmetry group G acts on the set X . In the bead problem, the set X would consist of the places in the necklace where we wish to put the beads, and the set Y would consist of the possible colors. A function from X to Y then specifies for each place in the necklace what color bead to use. The group G acts on X by rotating and turning over the necklace.

The action is of G on the set of functions from X to Y is given by the formula

$$g(f)(x) = f(g^{-1}(x)).$$

The reason for the inverse sign is so that composition works right. For a group action, we need $g_1(g_2(f)) = (g_1g_2)(f)$. To see that this holds, we have

$$\begin{aligned} (g_1(g_2(f)))(x) &= (g_2(f))(g_1^{-1}(x)) = f(g_2^{-1}(g_1^{-1}(x))) = f((g_2^{-1}g_1^{-1})(x)) \\ &= f((g_1g_2)^{-1}(x)) = ((g_1g_2)(f))(x), \end{aligned}$$

whereas without the inverse sign the order of g_1 and g_2 would be reversed.

To be continued. . .

8.14. The Mathieu group M_{12}

The combinatorics of twelve tone music has given rise to curious coincidence, which I find worth mentioning. Messiaen, in his *Ile de feu 2* for piano, nearly rediscovered the Mathieu group M_{12} . On pages 409–414 of Berry,⁵ you can read about how Messiaen uses the permutations

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 6 & 8 & 5 & 9 & 4 & 10 & 3 & 11 & 2 & 12 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 7 & 5 & 8 & 4 & 9 & 3 & 10 & 2 & 11 & 1 & 12 \end{pmatrix}$$

⁵Wallace Berry, *Structural function in music*, Prentice-Hall, 1976. Reprinted by Dover, 1987. 447 pages, in print. ISBN 0486253848.

to generate sequences of tones and sequences of durations. These permutations generate a group M_{12} of order 95,040 discovered by Mathieu in the nineteenth century.⁶

A group is said to be *simple* if it has just two normal subgroups, namely the whole group and the subgroup consisting of just the identity element.⁷ One of the outstanding achievements of twentieth century mathematics was the classification of the finite simple groups. Roughly speaking, the classification theorem says that the finite simple groups fall into certain infinite families which can be explicitly described, with the exception of 26 *sporadic* groups. Five of these 26 groups were discovered by Mathieu in the nineteenth century, and the remaining ones were discovered in the nineteen sixties and seventies.

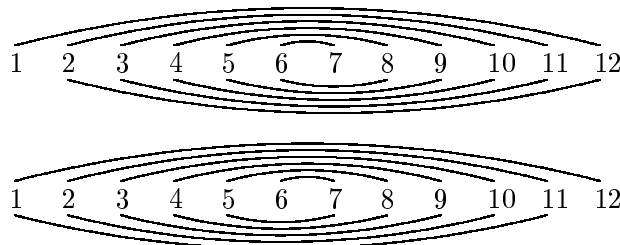
Diaconis, Graham and Kantor discovered that M_{12} was generated by the above two permutations, which they call *Mongean shuffles*. Start with a pack of twelve cards in your left hand, and transfer them to your right hand by placing them alternately under and over the stack you have so far. When you have finished, hand the pack back to your left hand. Since I did not tell you whether to start under or over, this describes two different permutations of the twelve cards. These are the permutations shown above. In cycle notation, these permutations are

$$(1, 7, 10, 2, 6, 4, 5, 9, 11, 12)(3, 8)$$

of order ten, and

$$(1, 6, 9, 2, 7, 3, 5, 4, 8, 10, 11)(12)$$

of order eleven. These permutations can be visualized as follows.



Exercises

1. (Carl E. Linderholm [61]) If this book is read backwards (beginning at the last word of the last page), the last thing read is the introduction (reversed, of course). Thus the introduction acts as a sort of extraduction, and is suggested as a simple form of therapy, used in this way, if the reader gets stuck. Read this exercise backwards, and write an extraduction from it.

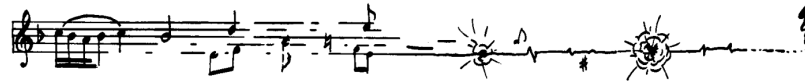
⁶E. Mathieu, *Mémoire sur l'étude des fonctions de plusieurs quantités*, J. Math. Pures Appl. **6** (1861), 241–243; *Sur la fonction cinq fois transitive de 24 quantités*, J. Math. Pures Appl. **18** (1873), 25–46.

⁷So for example the group with only one element is not simple, because it has only one, not two, normal subgroups.

Further reading:

J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Grundlehren der mathematischen Wissenschaften 290, Springer-Verlag, Berlin/New York, 1988. §11.17 of this book contains more information on Mongean shuffles and the Mathieu group M_{12} , as well as a huge amount of information about the sporadic groups in general.

P. Diaconis, R. L. Graham and W. M. Kantor, *The mathematics of perfect shuffles*, Adv. Appl. Math. **4** (1983), 175–196.



Unlike Mozart's *Requiem* and Bartok's *Third Piano Concerto*, the piece that P. D. Q. Bach was working on when he died has never been finished by anyone else.⁸

⁸Professor Peter Schickele, *The definitive biography of P. D. Q. Bach (1807–1742)?*, Random House, New York, 1976.