CHAPTER VII

OCTAVE IDENTIFICATION AND MODULAR ARITHMETIC

Octave identification. As we pointed out before, musical notation often implicitly equates notes which form the interval of m octaves, where m is an integer. In this scenario, the chromatic scale contains all the notes of standard musical notation, of which there are twelve. Starting from C, we can number them 0 through 11 as follows:

(0) C
(1) $C^\sharp = D^\flat$
(2) D
(3) $D^\sharp = E^\flat$
(4) E
(5) F
(6) $F^\sharp = G^\flat$
(7) G
(8) $G^\sharp = A^\flat$
(9) A
(10) $A^\sharp = B^\flat$
(11) B

Similarly, we identify intervals which differ by m octaves, for some integer m. From this perspective, going up an octave is the same as the identity interval. Hence the interval of a fourth followed by the interval of a fifth yields the identity interval. Likewise going up two fifths is the same as going up one step. In this way intervals created between note in the chromatic scale (i.e., those which can be measured as whole multiples of a semitone) are parameterized by the modular group $\mathbb{Z}_{12}$ and iterating intervals amounts to adding or subtracting in this algebraic system. We will now investigate this phenomenon.

Variations On The Well-Ordering Principle. We will shortly give a proof which will appeal to the Well-Ordering Principle. We state four different formulations of that principle, which are easily seen to be equivalent. The first is precisely as it was stated in Chapter I. In the second formulation $\mathbb{Z}^-$ denotes the set of strictly negative integers. A real number y is called a *lower bound* for a set of numbers T if $y \leq t$ for all $t \in T$. The definition of *upper bound* is analogous.

W.-O.P.1. *Any non-empty subset of* $\mathbb{Z}^+$ *has a smallest element.*

W.-O.P.2. *Any non-empty subset of* $\mathbb{Z}^-$ *has a largest element.*

W.-O.P.3. *Any non-empty subset of $\mathbb{Z}$ which has a lower bound has a smallest element.*

W.-O.P.4. *Any non-empty subset of $\mathbb{Z}$ which has an upper bound has a largest element.*

Generalized Division Algorithm. We now state a slightly more general version of the division algorithm than the one presented in Chapter I. Note the generality is that we allow the "dividend" x to be any real number rather than an integer[1].

Generalized Division Algorithm. *Given $m \in \mathbb{Z}^+$ and $x \in \mathbb{R}$ there exist $q \in \mathbb{Z}$ and $r \in \mathbb{R}$ with*

$$0 \leq r < m \tag{1}$$

such that

$$x = qm + r\,. \tag{2}$$

The elements $q \in \mathbb{Z}$ and $r \in \mathbb{R}$ are uniquely determined by (1) *and* (2).

Proof. Consider the set

$$S = \{\ell \in \mathbb{Z} \,|\, \ell m \leq x\} \subset \mathbb{Z}\,.$$

The condition $\ell m \leq x$ is equivalent to $\ell \leq \frac{x}{m}$ (since m is positive), so we see that x is an upper bound for S. By the Well-Ordering Principle (W.-O.P.4 above), S has a largest element q. We must have $q+1 \notin S$ by the maximality of q and hence we have

$$qm \leq x < (q+1)m = qm + m\,. \tag{3}$$

Setting $r = x - qm$, we clearly have $x = qm + r$, and subtracting qm from (3), gives $0 \leq r < m$ as desired.

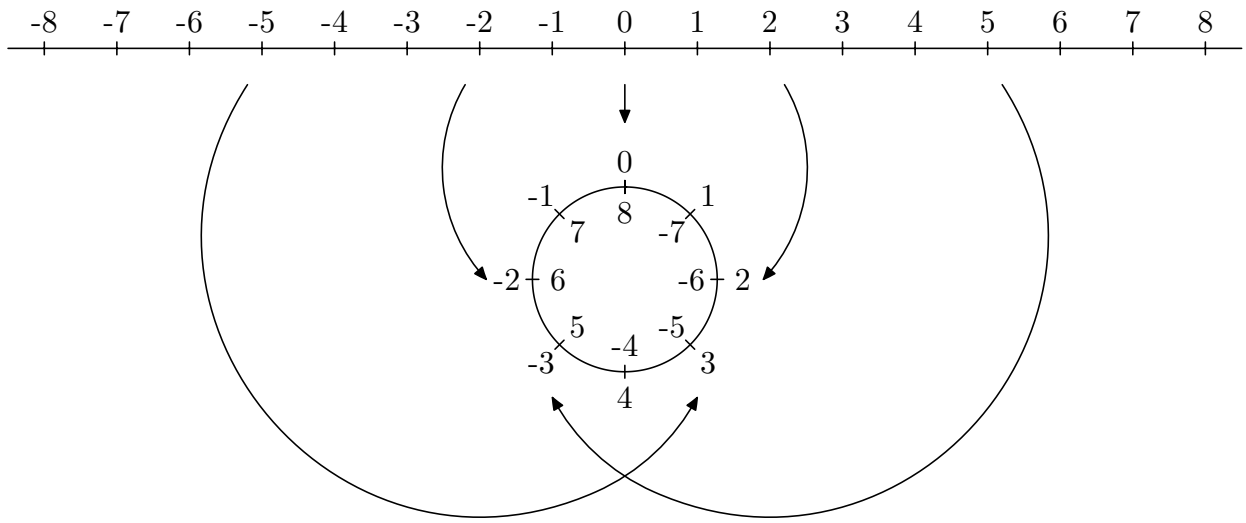
As for the uniqueness of q and r, suppose we have $q' \in \mathbb{Z}$, $r' \in \mathbb{R}$ such that $x = q'm + r'$ and $0 \leq r' < m$. Note that $q'm = x - r' \leq x$ so $q' \in S$. Since $r' < m$ we have $x = q'm + r' < q'm + m = (q'+1)m$. The inequality $(q'+1)m > x$ shows that $q'+1 \notin S$, nor is any larger integer. Therefore q' is the largest element of S, hence $q' = q$. We now have $qm + r' = qm + r$ since both are equal to x. Subtracting qm yields $r' = r$. □

Modular Equivalence on the Real Numbers. Let m be a fixed positive integer. We declare two real numbers x and y to be equivalent if $k - \ell$ is a multiple of m in $\mathbb{Z}$, i.e., there exists $q \in \mathbb{Z}$ such that $x - y = qm$, or equivalently $x = y + qm$. This relationship is denoted by $x \sim y$. Note that this depends on the choice of m.

We leave as an exercise the proof that $\sim$ defines an equivalence relation on the set $\mathbb{R}$, hence it partitions $\mathbb{R}$ into equivalence classes. For $x \in \mathbb{R}$ let us denote by $\bar{x}$ the equivalence class of x. Thus, if $m = 8$ we have $\overline{13} = \overline{53} = \overline{-11}$ and $\overline{6.5} = \overline{-1.5}$.

[1] Actually, you can see from the proof that the "divisor" m in the algorithm can be any element of $\mathbb{R}^+$, not just a positive integer.

Let us denote the set of equivalence classes by $\mathbb{R}/\sim$. The function which associate to $x \in \mathbb{R}$ its equivalence class $\bar{x} \in \mathbb{R}/\sim$ can be seen as the function which wraps the number line around the circle of circumference m in such away that distance is preserved as arc length. We often do this so that the origin $x = 0$ goes to the point at the top of the circle. This is depicted below for the case $m = 8$.



Thus $\mathbb{R}/\sim$ is parameterized by the circle in the same way $\mathbb{R}$ is parameterized by the line.

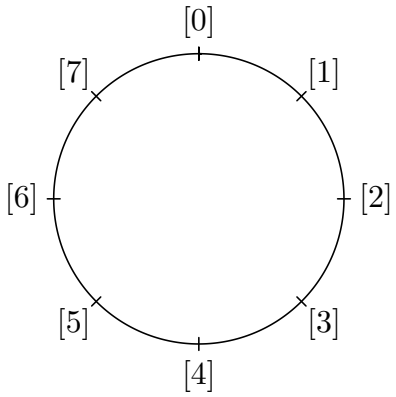
The Generalized Division Algorithm asserts that for each $x \in \mathbb{R}$, there is precisely one equivalence class representative $r \in \bar{x}$ such that $0 \leq r < m$. It is the number r for which $x = qm + r$ in the algorithm. This is reflected in the fact that for any point p on the circle there is precisely one point in the interval $[0, m)$ which wraps onto p.

Modular Equivalence on the Integers. Note that if $x \sim y$ and if $x \in \mathbb{Z}$ then $y \in \mathbb{Z}$ as well. Therefore $\sim$ restricts to an equivalence relation on $\mathbb{Z}$ as well. We denote by $\mathbb{Z}_m$ the set of equivalence classes. For $k, \ell \in \mathbb{Z}$ we express the condition $k \sim \ell$ is now written

$$k \cong \ell \mod m\,.$$

For $k \in \mathbb{Z}$, we write $[k]$ for the equivalence class containing k. Note that the symbol $[\ ]$ does not reference m, so again m must always be established. Bear in mind that $[k] = [\ell]$ if and only if $m \,|\, k - \ell$ in $\mathbb{Z}$. As an example, note that $5 \equiv 19 \mod 7$, and hence $[5] = [19]$ in $\mathbb{Z}_7$.

The set $\mathbb{Z}_m$ is a subset of $\mathbb{R}/\sim$, and it can be seen as the image of $\mathbb{Z}$ by the wrapping function described above. If we place m equally spaced points around the circle, these points will be this image; they correspond to the classes $[0], [1], [2], \ldots, [m-1]$, which is all of $\mathbb{Z}_m$. Hence elements of $\mathbb{Z}_m$ can be seen as "clock" positions" on the "m-hour clock". This is depicted below, again for $m = 8$.



We now introduce some concepts from abstract algebra which will be useful in this discussion.

Monoid. A *monoid* is a set M with an associative law of composition that has an identity element. By "law of composition" we mean a rule which assigns to each ordered pair of elements $(x, y) \in M^2$ an element z of M. This operation is often denoted by choosing some symbol, such as $\cdot$, and writing $x \cdot y = z$. The property of associativity and the existence of an identity element are defined as follows:

(1) Associativity: For any $x, y, z \in M$ we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
(2) Identity: There exists an element $e \in M$, called the *identity element,* having the property that for all $x \in M$, $x \cdot e = e \cdot x = x$.

Note that associative property allows us to drop parenthesies without ambiguity: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ can be written as $x \cdot y \cdot z$.

We claim that the identity element e is the unique element of M having its defining property, justifying our use of the article "the". For if e' is another identity element, then $e = e \cdot e' = e'$.

Examples. Here are some examples of monoids. We leave it as an exercise to verify most the details.

(a) The set $\mathbb{R}$ under the operation $\cdot$ (ordinary multiplication).

(b) The set $\mathbb{Z}$ together with the operation $+$ (addition). The identity element is 0.

(c) Let S be a set and let $\mathcal{F}(S)$ be the set of functions $f : S \to S$. Take the law of composition to be the usual composition of functions: For $f, g \in \{(S)$, $f \circ g$ is the function defined by $(f \circ g)(s) = f(g(s))$ for all $s \in S$. The identity element is the "identity function" id_S defined by $\mathrm{id}_S(s) = s$ for all $s \in S$. A special case is $\mathcal{F}(\mathbb{R})$, the monoid of functions from $\mathbb{R}$ to $\mathbb{R}$.

(d) The set $\mathbb{Z}_m$, for a given $m \in \mathbb{Z}^+$. The law of composition will be denoted $+$ (we'll call it addition), and defined by

$$[k] + [\ell] = [k + \ell]\,.$$

Here we must show that this is well-defined, due to the fact that we have defined the addition using equivalence class representatives. Suppose, then that $[k'] = [k]$ and $[\ell'] = [\ell]$. This means $k' \equiv k \mod m$ and $\ell' \equiv \ell \mod m$. Hence we have $k' = k + pm$ and $\ell' = \ell + qm$ for some $p, q \in \mathbb{Z}$. Therefore $k'+\ell' = (k+pm)+(\ell+qm) = k+\ell+(p+q)m$, which shows $k' + \ell' \equiv k + \ell \mod m$. This means $[k' + \ell'] = [k + \ell]$, and this shows that our definition is well-defined. Note that the identity element is $[0]$.

We sometimes denote a monoid by writing $(M, \cdot)$ to indicate its law of composition. This is necessary when the intended operation is not clear in the context. For example $(\mathbb{Z}, +)$ and $(\mathbb{Z}, \cdot)$ are two different monoid structures having the same underlying set.

Note that a monoid is always a non-empty set, since it contains the element e.

Commutativity. A monoid M is called *commutative* if for all $x, y \in M$ we have $x \cdot y = y \cdot x$.

One will easily verify that the monoids defined in (a), (b), and (d) above are commutative. However, example (c) is not, in general: consider for example the functions $f, g \in \mathcal{F}(\mathbb{R})$ given by $f(x) = x^2$ and $g(x) = x + 1$. Then $(f \circ g)(x) = (x + 1)^2$ and $(g \circ f)(x) = x^2 + 1$. These two are not the same function; they differ at $x = 1$, for example.

By convention, we only use the symbol $+$ for commutative operations.

Group. A *group* is a monoid G with the following property: For every $x \in G$ there is an element x_{inv}, called the *inverse* of x, with the property

$$x \cdot x_{\text{inv}} = x_{\text{inv}} \cdot x = e$$

(where e is the identity element).

The inverse x_{inv} is easily shown to be unique to x. If x'_{inv} were another such element we have

$$x_{\text{inv}} = x_{\text{inv}} \cdot e = x_{\text{inv}} \cdot (x \cdot x'_{\text{inv}}) = (x_{\text{inv}} \cdot x) \cdot x'_{\text{inv}} = e \cdot x'_{\text{inv}} = x'_{\text{inv}}$$

When we are using the symbol $+$ for the law of composition in a commutative group, we denote the inverse of an element x by $-x$, and we write $x - y$ for $x + (-y)$.

Examples. Amongst the examples (a) – (d) above of monoids, note that (b) and (d) are groups: The inverse of $k \in \mathbb{Z}$ is $-k$, and the inverse of $[k] \in \mathbb{Z}_m$ is $[-k]$. Example (a) fails since $0 \in \mathbb{R}$ has no multiplicative inverse. However, if we replace $\mathbb{R}$ by either $\mathbb{R} - \{0\}$ or R^+ we have a group, where the inverse of x is $\frac{1}{x} = x^{-1}$.

Modular Arithmetic. The group $\mathbb{Z}_m$ is called a *modular group,* and operations involving its law of composition, such as $[6] + [13] = [1]$ in $\mathbb{Z}_9$, are called *modular arithmetic.*

Homomorphism. Suppose we have two groups $(G, \cdot)$ and $(G', \circ)$. A function $\varphi : G \to G'$ is called a group *homomorphism* if for all $x, y \in G$ we have

$$\varphi(x \cdot y) = \varphi(x) \circ \varphi(y)\,.$$

We leave it as an exercise to show the if $e \in G$ and $e' \in G'$ are the identity elements and φ is a homomorphism, then $\varphi(e) = e'$.

A homomorphism $\varphi : G \to G'$ is called an *isomorphism* if it is bijective, i.e., one-to-one and onto. In this case there is an inverse function $\varphi^{-1} : G' \to G$, and φ^{-1} will be an isomorphism as well. If such an isomorphism exists we say G and G' are *isomorphic.*

Examples.

(1) Let S be the set $\{\pm 1\} \subset \mathbb{R}$, multiplication. This is a group. The function $\varphi : S \to \mathbb{Z}_m$ defined by $\varphi(1) = [0]$, $\varphi(-1) = [1]$ is a homomorphism, and in fact, an isomorphism.

(2) Consider the function discussed earlier which wraps the real line around the circle. This is the function $w : \mathbb{R} \to \mathbb{R}/\sim$ defined by $w(x) = \bar{x}$. The set $\mathbb{R}/\sim$ inherits from $\mathbb{R}$ the law of composition $+$, by which $\bar{x} + \bar{y} = \overline{x+y}$. (One shows this is well defined by a proof analogous to the proof in (d) that addition is well-defined in $\mathbb{Z}_m$.) Thus we have groups $(\mathbb{R}, +)$ and $(\mathbb{R}/\sim, +)$, and the function w is a group homomorphism. This homomorphism is onto but not one-to-one, hence it is not an isomorphism.

(3) For $b \in \mathbb{R}^+$, we have the encountered the functions $f : \mathbb{R} \to \mathbb{R}^+$ and $g : \mathbb{R}^+ \to \mathbb{R}$ defined by $fr = b^r$ and $g(x) = \log_b x$. These are homomorphisms between the groups $(\mathbb{R}, +)$ and $\mathbb{R}^+, \cdot)$, which are inverse to each other as functions. Hence these two groups are isomorphic. The details are left as an exercise.

The Group of Intervals. The later example is especially relevant since we have identified the set of musical intervals with the sets $\mathbb{R}$ and $\mathbb{R}^+$, the former giving additive measurement (the units depending on the base b), the latter giving multiplicative measurement, or interval ratio. We see by either identification the the set of intervals forms a group, where the law of composition is the usual composition of intervals, i.e., following one interval by the other. We see, then, that the identity element in the group of intervals is the unison interval and the inverse of an interval is its opposite interval. The isomorphisms f and g are precisely the conversion from multiplicative to additive measurement, and back.

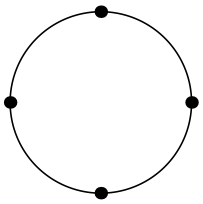
The Group of Modular Intervals. Elements of the group $(\mathbb{R}/\sim, +)$ of (2) can be identified with the set of equivalence classes of intervals modulo octave. Thus the set of these classes becomes a group, which we'll call the group of *modular intervals.* The law of composition, is defined by taking representatives, adding them, and taking the class of the sum. Thus we have, for example third + ninth = tritone, and fourth + fifth = unison.

The Group of Modular Chromatic Intervals. We have noted that the set of keyboard intervals, measured in semitones, can be identified with the group $\mathbb{Z}$. Let us note that the equivalence relation which says intervals of k and ℓ semitones are octave equivalent is just the statement that $k - \ell$ is a multiple of 12, i.e., $k \equiv \ell \mod 12$. We will call equivalence classes *modular chromatic intervals.* Therefore the set of modular chromatic intervals can be indentified with $\mathbb{Z}_{12}$, making it a group whose law of composition is iteration of intervals. Any modular chromatic interval can be has a unique equivalence class representative n semitones, where $0 \leq n \leq 11$. As with performing addition in $\mathbb{Z}_{12}$, the iteration of modular chromatic intervals can be seen as a sequence of rotations on the modular clock.

Example. Consider the iteration of a minor third, an octave, and a fourth. These intervals are represented in semitones as 3, 12, and 5, respectively. However the octave can be represented by 0 semitones. The iteration of the three intervals yields the modular chromatic interval represented by 8 semitones, which is an augmented fifth. This is merely the statement that $[3]+[12]+[5]=[8]$ in $\mathbb{Z}_{12}$, which follows from the fact that $20 \equiv 8 \mod 12$.

Nonstandard Chromatic Intervals. If we divide the octave into m equal intervals an measure intervals by m-chromatic units, the group of intervals is identified with $\mathbb{Z}_m$.

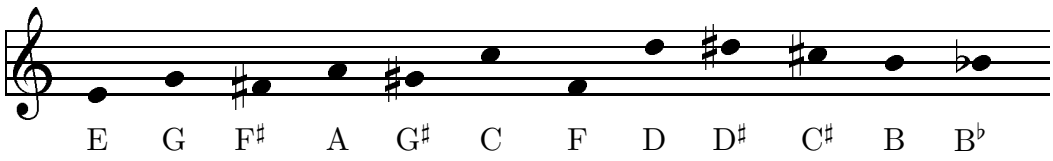
Modular clock. The group $\mathbb{Z}_n$ can be realized as the group of rotations of a regular n-gon, or of a "clock" with n positions, dividing the circle into n equal arcs, with a position at the top of the circle. For example, $\mathbb{Z}_4$ is the group of rotations of the square, or a clock with four positions:



We label a clock position by the group element which rotates the top position to that position. Hence the top position is labeled [0], the first position clockwise from [0] is labeled [1], etc. The positions of the clock are thereby in one-to-one correspondence with the elements of $\mathbb{Z}_n$. With this labeling the addition of elements $[k]$ and $[\ell]$ in $\mathbb{Z}_n$ can be computed by rotating the clock clockwise by k positions (counterclockwise if k is negative), then by ℓ positions. The sum $[k]+[\ell]$ will be where the top position lands after these two rotations.

Creating a Twelve-Tone Chart Using Modular Arithmetic. We can generate a twelve-tone row by designating a note class, then identifying each of the twelve note classes of the row with its modular chromatic interval from the designated note class. This just means we list the elements of $\mathbb{Z}_{12}$ in some order. For what is to follow it will be important to let the designated note be the first note class of the sequence, so that the first modular number is [0].

Example. We revisit the first example in Chapter V, which generates the row chart whose original row is:



As prescribed above, let E be our designated note class. The sequence, given according to

modular interval from E, is then:

$$[0] \quad [3] \quad [2] \quad [5] \quad [4] \quad [8] \quad [1] \quad [10] \quad [11] \quad [9] \quad [7] \quad [6]$$

Provided our sequence starts with [0], the inversion of this row is obtained by replacing each entry in the sequence by its additive inverse, or negative. This is because we want the interval from the first entry to the n^{th} entry in the inversion to be the opposite of the interval from the first entry to the n^{th} entry in the original row. Hence the sequence of intervals for the inversion of our given row is:

$$[0] \quad [9] \quad [10] \quad [7] \quad [8] \quad [4] \quad [11] \quad [2] \quad [1] \quad [3] \quad [5] \quad [6]$$

Let us number the rows an column by the integers 1 through 12 and use the ordered pair (i, j) to refer to the position at row i and column j. We label the entries of the original row as:

$$\begin{array}{cccccc} a_1 = [0] & a_2 = [3] & a_3 = [2] & a_4 = [5] & a_5 = [4] & a_6 = [8] \\ a_7 = [1] & a_8 = [10] & a_9 = [11] & a_{10} = [9] & a_{11} = [7] & a_{12} = [6] \end{array}$$

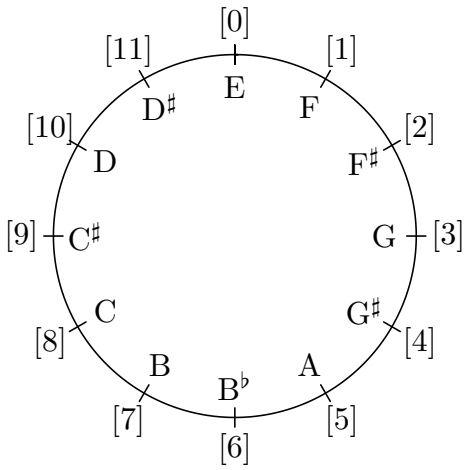
The first column will be the inversion, given by the negatives in $\mathbb{Z}_{12}$:

$$\begin{array}{cccccc} -a_1 = [0] & -a_2 = [9] & -a_3 = [10] & -a_4 = [7] & -a_5 = [8] & -a_6 = [4] \\ -a_7 = [11] & -a_8 = [2] & -a_9 = [1] & -a_{10} = [3] & -a_{11} = [5] & -a_{12} = [6] \end{array}$$

We now proceed to fill in each position of the chart with the element of $\mathbb{Z}_{12}$ corresponding to the appropriate note class. According to the procedure described in Chapter V, the entry in the (i, j) position should make the interval a_j with the leftmost entry in the i^{th} row, which is $-a_i$. Therefore the correct element of $\mathbb{Z}_{12}$ is $a_j - a_i$. For example, the entry in position $(8, 5)$ is $a_5 - a_8 = [4] - [10] = [6]$. Filling in the chart in this fashion yields the row chart:

	1	2	3	4	5	6	7	8	9	10	11	12
1	[0]	[3]	[2]	[5]	[4]	[8]	[1]	[10]	[11]	[9]	[7]	[6]
2	[9]	[0]	[11]	[2]	[1]	[5]	[10]	[7]	[8]	[6]	[4]	[3]
3	[10]	[1]	[0]	[3]	[2]	[6]	[11]	[8]	[9]	[7]	[5]	[4]
4	[7]	[10]	[9]	[0]	[11]	[3]	[8]	[5]	[6]	[4]	[2]	[1]
5	[8]	[11]	[10]	[1]	[0]	[4]	[9]	[6]	[7]	[5]	[3]	[2]
6	[4]	[7]	[6]	[9]	[8]	[0]	[5]	[2]	[3]	[1]	[11]	[10]
7	[11]	[2]	[1]	[4]	[3]	[7]	[0]	[9]	[10]	[8]	[6]	[5]
8	[2]	[5]	[4]	[7]	[6]	[10]	[3]	[0]	[1]	[11]	[9]	[8]
9	[1]	[4]	[3]	[6]	[5]	[9]	[2]	[11]	[0]	[10]	[8]	[7]
10	[3]	[6]	[5]	[8]	[7]	[11]	[4]	[1]	[2]	[0]	[10]	[9]
11	[5]	[8]	[7]	[10]	[9]	[1]	[6]	[3]	[4]	[2]	[0]	[11]
12	[6]	[9]	[8]	[11]	[10]	[2]	[7]	[4]	[5]	[3]	[1]	[0]

In order to convert this to a chart of note classes, it is helpful to draw the modular clock, additionally labeling each position by the note class which has the given interval from E, as follows:



Using this we can translate back to the chart in Chapter V.

Creating an n-Tone Chart Using Modular Arithmetic. This method is equally valid, of course, if we were to create, for some $n \in \mathbb{Z}^+$, an n-tone row chart from an n-tone original row. Given an original row

$$a_1 = [0],\, a_2, \ldots ,\, a_n$$

from $\mathbb{Z}_n$, we form the $n \times n$ row chart by taking:

(1) $$\boxed{\text{entry } (i,j) = a_j - a_i}$$

Here the arithmetic takes place in $\mathbb{Z}_n$.

Example. We will prepare to make a seven-tone composition using this row from $\mathbb{Z}_7$:

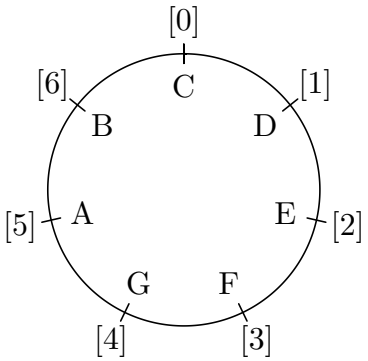
(2) $$a_1 = [0] \quad a_2 = [4] \quad a_3 = [1] \quad a_3 = [6] \quad a_4 = [5] \quad a_6 = [2] \quad a_7 = [3]$$

We begin by detuning the synthesizer to play in seven-tone equal temperament. Suppose we decide to use the white keys on the keyboard, detuned around C. The 7-chromatic interval is given in cents by $1200/7 \approx 171.43$. Using the method described in Chapter V, we detune the white keys as follows:

(3)

C	D	E	F	G	A	B
0	−29	−57	14	−14	−43	−71

We now associate each of these seven redefined note classes to an element of $\mathbb{Z}_7$ according to its modular interval from C. The following modular clock allows us to easily convert from one to the other.



Referring to (1), we fill in the rows of the 7×7 row chart with elements of $\mathbb{Z}_7$ using (2). This gives the chart below on the left, which translates to the chart on the right using the clock above.

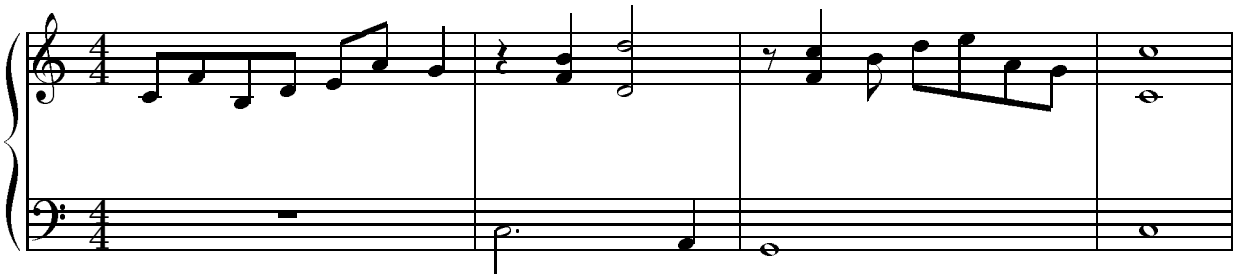
	1	2	3	4	5	6	7
1	[0]	[4]	[1]	[6]	[5]	[2]	[3]
2	[3]	[0]	[4]	[2]	[1]	[5]	[6]
3	[6]	[3]	[0]	[5]	[4]	[1]	[2]
4	[1]	[5]	[2]	[0]	[6]	[3]	[4]
5	[2]	[6]	[3]	[1]	[0]	[4]	[5]
6	[5]	[2]	[6]	[4]	[3]	[0]	[1]
7	[4]	[1]	[5]	[3]	[2]	[6]	[0]

row chart with modular integers

	1	2	3	4	5	6	7
1	C	G	D	B	A	E	F
2	F	C	G	E	D	A	B
3	B	F	C	A	G	D	E
4	D	A	E	C	B	F	G
5	E	B	F	D	C	G	A
6	A	E	B	G	F	C	D
7	G	D	A	F	E	B	C

row chart with note classes

A seven-tone composition based on this row chart might contain the following:



This employs the inversion of the original row, which is the left column of the row chart. The sequence is used three times, first melodically, then twice with some harmonic content. The passage should be played with the detuning given in (3).

Exponential Notation in a Group. Let $(G, \cdot)$ be a group, and let $x \in G, n \in \mathbb{Z}^+$. We define x^n to be the n-fold composition $x \cdot x \cdot \cdots \cdot x$ in G. We define x^0 to be e, the identity element of G. Finally we define x^{-n} to be the n-fold composition $x^{1-} \cdot x^{-1} \cdot \cdots \cdot x^{-1}$. We have now defined x^n for <u>any</u> $n \in \mathbb{Z}$. With these definitions, the following familiar-looking rules of exponents are valid for any $x \in G$, $n, m \in \mathbb{Z}$:

$$\begin{aligned} x^{n+m} &= x^n \cdot x^m \\ (x^n)^m &= x^{nm} \end{aligned} \tag{4}$$

We leave it as an exercise to verify these rules.

In the case where the group is commutative and the group law is denoted by $+$, we usually denote the n-fold sum $x + x + \cdots + x$ by nx rather than x^n. In this situation the rules (4) become:

$$\begin{aligned} (n+m)x &= nx + mx \\ m(nx) &= (nm)x \end{aligned} \tag{5}$$

Generators and Cyclic Groups. Given $t \in G$, G a group, we call t a *generator* for G if every element of G can be written in the form t^n for some $n \in \mathbb{Z}$, in other words,

$$\{t^n \,|\, n \in \mathbb{Z}\} = G\,.$$

If G has a generator, we call G a *cyclic* group.

Suppose G is cyclic and $t \in G$ is a generator. Consider the set

$$S = \{n \in \mathbb{Z}^+ \,|\, t^n = e\}\,.$$

If $S = \emptyset$, then any two powers t^n and t^m of t will be distinct unless $n = m$, and therefore the elements of G are in one-to-one correspondence with elements of $\mathbb{Z}$, and this correspondence defines an isomorphism of G with $\mathbb{Z}$. This assertion will appear as an exercise.

If $s \neq \emptyset$, the S has a smallest element m, by the Well-Ordering Principle. The positive integer m will be called the *order* of t. We claim that any element $x \in G$ has a unique expression $x = t^r$ with $0 \leq r < m$. This follows from the division Algorithm: Writing $n = qm+r$ as in the algorithm, we have $t^n = t^{mq+r} = t^{mq}\cdot t^r = (t^m)^q \cdot t^r = e^q \cdot t^r = e \cdot t^r = t^r$. This uses the rules of exponents in (4). The uniqueness of r is fairly apparent. If two distinct integers r and r', with $0 \leq r < r' < m$ had the property, then we would have $t^{r'-r} = e$ and $r' - r < m$, violating the minimality of m. So the claim is proved, and we see that

$$G = \{e, t, t^2, \ldots, t^{m-1}\}$$

with these elements distinct. Therefore G has precisely m elements.

Example. The group $\mathbb{Z}_m$ is a cyclic group, and $[1]$ is a generator having order m. This is because m is the smallest integer n such that $n[1] = [0]$.

A cyclic group can have more than one generator (and usually does). Consider as an example a group G having a generator t of order 8. In this case G consists of the eight elements

$$e, t, t^2, t^3, t^4, t^5, t^6, t^7\,.$$

Consider $u = t^3 \in G$. We claim that u is also a generator. We show this directly by writing the powers of u as powers of t. We have $u^2 = (t^3)^2 = t^6$ and $u^3 = (t^3)^3 = t^9 = t$. Continuing in this fashion we get

$$e, \quad u = t^3, \quad u^2 = t, \quad u^4 = t^4, \quad u^5 = t^7, \quad u^6 = t^2, \quad u^7 = t^5$$

and this accounts for all the elements of G.

In Chapter VII we will see that if t is a generator having order m, then a power t^n is also a generator precisely when the only positive integer dividing both m and n in $\mathbb{Z}$ is 1, i.e., $\gcd(n, m) = 1$.

Generating Intervals. The group of modular m-chromatic intervals is identified with $\mathbb{Z}_m$. We call such an interval a *generating interval* if it generates the group $\mathbb{Z}_m$. Thes will be the intervals whose iterations give all the m chromatic intervals.

By the criterion advertised above, these coincide with those classes $[n] \in \mathbb{Z}_m$ for which 1 is the only positive integer dividing m and n. Hence there are $\phi(m)$ generators in $\mathbb{Z}_m$, ϕ being the Euler phi function. With this criterion on easily checks that the generating 12-chromatic intervals are the semitone ([1]), the fourth ([5]), the fifth ([7]), and the major seventh ([11]).

Exercises

(1) Show that the functions $f(x) = b^x$ and $g(x) = \log_b(x)$ give isomorphisms between the groups $(\mathbb{R}, +)$ and $(R^+, \cdot)$.

(2) Express the following iterations of chromatic intervals as r semitones with $0 \leq r < 12$. Interpret all these iterations as operations in $\mathbb{Z}_{12}$.
   (a) the iteration of 14 and 23 semitones
   (b) two fifths and a major third
   (c) six fifths
   (d) up three minor thirds, down six steps

(3) Prove using the division algorithm that if I is an interval in the n-chromatic scale, the iteration of I n times is equivalent modulo octave to the unison interval. Restate this as an assertion about elements of the group $\mathbb{Z}_n$.

(4) Prove that $\mathbb{Z}_n$ has exactly n elements by showing that $[0], [1], \ldots, [n-1]$ are distinct, and that these are all of the elements of $\mathbb{Z}_n$.

(5) 6. For each of these choices of n, determine $\phi(n)$ by listing all the generating intervals in the n-chromatic scale. For each generating interval draw the corresponding circle of intervals.

   (a) n=6 (b) n=5 (c) n=9 (d) n=10

(6) Suppose G is a group and $g \in G$. Show that there is a unique group homomorphism $\varphi : \mathbb{Z} \to G$ such that $\varphi(1) = g$.

(7) Create n-tone row charts for the following choices of n and the given sequences of original rows in $\mathbb{Z}_n$:
   (a) $n = 3$; $([2], [0], [1])$
   (b) $n = 5$; $([4], [0], [2], [3], [1])$
   (c) $n = 6$; $([5], [2], [4], [1], [3], [0])$
   (d) $n = 7$; $([3], [5], [6], [0], [2], [1], [4])$