Classification of motives: a mathematical approach

Harald Fripertinger*

November 24, 1999

In this paper we show in a more or less complete way how to apply methods from algebraic combinatorics to the classification of motives. These methods can be described in a very general way so that they can be applied for the classification of objects in different sciences. For instance for the isomer enumeration in chemistry, for spin analysis in physics, for the classification of isometry classes of linear codes, in general for investigating isomorphism classes of objects (cf. [16, 17]). Here we present an application of these methods to music theory.

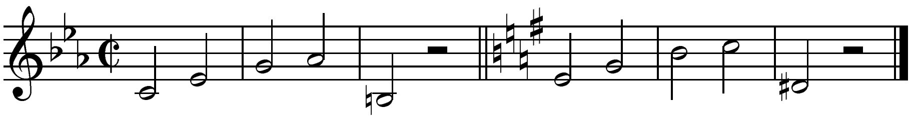
First it should be mentioned that in British English the word "motive" is often spelled as "motif". Sometimes terms like "figure" or "subject" are used as synonyms for it. Moreover there is no unique definition of a motive. The meaning of this word was changing through the centuries so actually there exist many different definitions. In general a motive is the smallest part of a composition which makes some musical sense. In the second half of the eighteenth century such meaningful units of a composition were mentioned for the first time in music theory. The first definitions of motives were given in the first half of the nineteenth century. (Cf. [19, 18].) In H. Riemann's definition [28] a motive includes rhythm, melody, harmony, dynamics and tone colour. ([3])

The concept of motives we are using in this paper was introduced by G. Mazzola in [20]. It is a mathematical precise definition which is useful for investigating both tonal and rhythmical aspects of music. (See section 6.) At the end of section 4 we present some mathematical definitions for operations like transposing, inversion, temporal shift, retrograde inversion etc. They can be applied to a motive such that from a given motive we can construct many other motives. They all will be called *similar* or *equivalent* motives. The exact definition when two motives are called similar will be given in section 6.

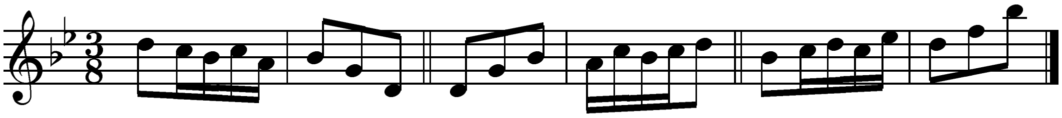
In order to describe the musical meaning of the operations mentioned above we demonstrate their application in the next three examples. We didn't give any formal definitions so far. In some later sections when the corresponding operations are defined in our mathematical model the reader should check that these definitions coincide with the usual meaning in music theory. First three short pieces of music — we call them motives — are shown, which intuitively could be regarded as motives or as collections of motives, together with similar motives which were produced by applying certain of these

*Supported by the Fonds zur Förderung der wissenschaftlichen Forschung, P12642-MAT.

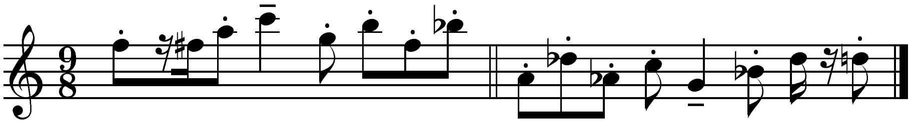
operations. The similar motives are divided from the original motives by 2 vertical lines. The first example demonstrates transposition of a motive from J. S. Bach's *"Musical Offering"*.



The next example shows retrograde inversion and inversion of a motive from *"A Midsummer Night's Dream"* by F. Mendelssohn-Bartholdy.



Finally the last example *"Danse de la chèvre"* by A. Honegger demonstrates a combination of these three operations.



The main aim of this paper is to show how the number of essentially different (i. e. not similar) motives (for the definitions of motives and similarity of motives see section 6) can be computed and how to construct a (complete) system of representatives of motives. In other words, we try to get a list of motives such that motives of this list are pairwise not similar and each possible motive is similar to (exactly) one motive of this list. For the non experienced reader we start with some basic mathematical notions and definitions concerning sets, functions, permutations and elementary number theory. Then the concepts of groups, permutation groups and group actions are introduced. Using these tools it is possible to give a mathematical description of an n-scale Z_n consisting of exactly n pitch-classes, which generalizes the concept of 12 tones in one octave to n tones in one octave. In addition to this, the musical operations of transposing or inversion can be described as permutations of mathematical objects. In order to understand the mathematical meaning of Z_n we will learn some basic facts about rings and fields. Then Mazzola's definition of motives will be presented. The tonal aspects of a motive are described by elements of an n-scale, the rhythmical aspects by elements of an m-bar Z_m. (An m-bar is a collection of m equidistant beats, such that tones are only allowed to start at one of these beats.) The notion of group actions is used for describing which motives are similar. In order to determine the number of different motives a famous theorem by G. Pólya ([24, 23]) will be applied. The last part of this article is dealing with the construction of lists of motives. Strong generators and the Sims-chain of permutation groups will be introduced and Read's method of orderly generation will be described. Combining both algebraic methods and skilled programming techniques it is possible to apply these methods to non trivial problems. Obviously the case $n = m = 12$ is of special interest. For instance in [10, 9] a list of more than 6 millions representatives of 8-motives in that particular situation was computed.

In order to give a complete description of the methods used, all the main definitions and theorems, which are useful for our approach, are mentioned and proved in the next sections.[1] As it is usual in mathematical papers most of the theorems and corollaries are followed by proofs which should prove the correctness of the preceding statements. When the proofs are missing the reader should try to find them by himself. Usually they are not too difficult but sometimes writing down all details can be a lot of work.[2] For the benefit of the reader and in order to make the paper self-contained there are some introductory chapters at the beginning of this article. For that reason it is not necessary to consult different books for understanding the given proofs. On the other hand however the main topic appears rather late in this article which demands some patience of the reader. Nevertheless we chose this way of presentation, since for understanding a mathematical model it is definitely necessary to have some mathematical background information.

1 Sets and functions

In this section basic facts about sets and functions are described and common mathematical notions are introduced. The symmetry operations which will later be applied to motives can be described as permutations of a finite set. These are functions with very particular properties.

A set is a collection of its elements. In order to express that x is an element of the set X we write $x \in X$. Each element of a set occurs exactly once in a set and it does not matter in which sequence the elements of the set are arranged. A set Y is called a *subset* of X if each element of Y also belongs to X. This is indicated by $Y \subseteq X$. Trivial subsets of X are the empty set $\emptyset$ which consists of no elements and the complete set X itself.

The *union* $X \cup Y$ of two sets X and Y consists of all elements which are elements of X or elements of Y. The *intersection* $X \cap Y$ of two sets X and Y consists of all elements which are elements of both X and Y. Two elements X and Y are called *disjoint* if and only if $X \cap Y = \emptyset$. The *difference* $X \setminus Y$ of two sets X and Y consists of all elements which are elements of X and not of Y.

$$X \cup Y := \{z \mid z \in X \text{ or } z \in Y\}, \qquad X \cap Y := \{z \mid z \in X \text{ and } z \in Y\},$$

[1]Nevertheless for the interested reader, who is not familiar with these subjects, it will be necessary to consult some other textbooks for really understanding all the details. As a standard reference for number theory I would suggest to read [22], as an introduction to algebra, groups, rings and fields look at [33] or [21]. Combinatorics under group actions is nicely described in [16, 17], Pólya's Theory of counting in [4]. These are just some suggestions, there exist many other textbooks dealing with these topics as well.

[2]Moreover by doing this the reader can check whether he understood the main ideas of the previous section.

$$X \setminus Y := \{z \mid z \in X \text{ and } z \notin Y\}$$

The *Cartesian product* $X \times Y$ of two sets X and Y is the set of all *pairs* (x, y) for $x \in X$ and $y \in Y$.

$$X \times Y := \{(x, y) \mid x \in X,\ y \in Y\}$$

When writing (x, y) we stress that it is important in which order the elements of a pair occur. In general (x, y) is different from (y, x).

We consider both infinite sets, e. g. the set of all integers

$$\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\},$$

the set of all positive integers

$$\mathbb{N} := \{z \in \mathbb{Z} \mid z \geq 1\},$$

the set of all nonnegative integers $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$, or the set of all rational numbers

$$\mathbb{Q} := \left\{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{N}\right\},$$

and finite sets. E. g. for $n \in \mathbb{N}$ let $\underline{n} := \{1, 2, \ldots, n\}$ and $Z_n := \{0, 1, \ldots, n-1\}$. These sets fulfill

$$\emptyset \subseteq \underline{n} \subseteq \mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q}.$$

Consider two sets X and Y and a subset $f \subseteq X \times Y$ such that for all $x \in X$ there exists exactly one $y \in Y$ such that $(x, y) \in f$, then the triple (X, Y, f) defines a *function* f with *domain* X and *range* Y. Instead of writing $(x, y) \in f$ we usually write $f(x) = y$ and we say that x is *mapped onto* y under f, or y is the *image* of x under f. The *image* of a subset X_1 of X under f is the set

$$f(X_1) := \{f(x) \mid x \in X_1\}.$$

The *pre-image* of a subset Y_1 of Y under f is the set

$$f^{-1}(Y_1) := \{x \in X \mid f(x) \in Y_1\}.$$

From these definitions it is clear that $f(X_1) \subseteq Y$ and $f^{-1}(Y_1) \subseteq X$.

Let f be a function from X to Y and let X_1 be a subset of X then the *restriction* $f|_{X_1}$ of f to the domain X_1 is the triple (X_1, Y, f') where $f' := \{(x, y) \mid x \in X_1,\ (x, y) \in f\}$.

If f is a function from X to Y then we write $f\colon X \to Y$ and the set of all functions from X to Y is indicated by

$$Y^X := \{f \mid f\colon X \to Y\}.$$

A function f is called *injective* if different elements of X are mapped onto different elements in Y. (Or, equivalently, $f(x_1) = f(x_2)$ implies $x_1 = x_2$.) A function f is called *surjective* if each element of Y occurs as the image of an element of X, i. e. $f(X) = Y$. A function f is called *bijective* if f is both injective and surjective.

1.1 Example.

1. Consider $X = \underline{5}$ and $Y = \underline{3}$ and sets $f_1, \dots, f_5$ defined by:

$$\begin{aligned}
f_1 &:= \{(1,2),(2,3),(3,2),(4,2),(5,3)\}\\
f_2 &:= \{(1,2),(2,3),(3,2),(4,2)\}\\
f_3 &:= \{(1,1),(1,2),(2,3),(3,2),(4,2),(5,3)\}\\
f_4 &:= \{(1,2),(2,3),(3,2),(4,2),(5,5)\}\\
f_5 &:= \{(1,2),(2,3),(3,2),(4,2),(5,1)\}.
\end{aligned}$$

   We want to investigate which of these sets define functions from X to Y. f_1 is a function, f_2 is not a function from X to Y because for $x = 5$ there is no $y \in Y$ such that $(5, y) \in f_2$. f_3 is not a function since both $(1,1)$ and $(1,2)$ are in f_3, so there are two different elements (and not exactly one element) $y \in Y$ such that $(1, y)$ belongs to f_3. Furthermore f_4 is not a function from X to Y since $(5,5) \in f_4$ is not an element of $X \times Y$. Finally f_5 defines a function which is surjective since $f_5(X) = Y$. The function f_1 is not surjective since $f_1(X) = \{2,3\}$. Neither f_1 nor f_5 is injective since both functions map the elements 1 and 3 of X to the element $2 \in Y$.

2. Let X be a set, then the *identity function* id_X is given by $\mathrm{id}_X(x) := x$ for all $x \in X$. It is a function from X to X which is both injective and surjective since $\mathrm{id}_X(x_1) = \mathrm{id}_X(x_2)$ implies $x_1 = x_2$ and x is the image $\mathrm{id}_X(x)$ for each $x \in X$. So id_X is bijective. $\diamond$

From two functions $f_1 \colon X_1 \to Y_1$ and $f_2 \colon X_2 \to Y_2$ such that $f_1(X_1) \subseteq X_2$ a new function from X_1 to Y_2 can be constructed by first applying f_1 to $x \in X$ and then f_2 to $f_1(x)$. This *composition* $f_2 \circ f_1$ is defined by $(f_2 \circ f_1)(x) := f_2(f_1(x))$ for all $x \in X_1$.

1.2 Lemma. *For $1 \leq i \leq 3$ let f_i denote a function from X_i to Y_i such that $f_1(X_1) \subseteq X_2$ and $f_2(X_2) \subseteq X_3$. Then the composition of these three functions can be written as $f_3 \circ f_2 \circ f_1$ since*

$$f_3 \circ (f_2 \circ f_1) = (f_3 \circ f_2) \circ f_1.$$

In other words, the composition of functions is associative.

Proof. The function $f_2 \circ f_1$ has domain X_1 and range Y_2. Since $(f_2 \circ f_1)(X_1) = f_2(f_1(X_1)) \subseteq f_2(X_2) \subseteq X_3$ the composition $f_3 \circ (f_2 \circ f_1)$ can be formed and it has X_1 as it's domain and Y_3 as its range. Using similar arguments it is possible to prove that the composition $(f_3 \circ f_2) \circ f_1$ is well defined and has domain X_1 and range Y_3 as well. Thus we only have to decide whether $(f_3 \circ (f_2 \circ f_1))(x) = ((f_3 \circ f_2) \circ f_1)(x)$ for all $x \in X_1$. Let $x \in X_1$ then $(f_3 \circ (f_2 \circ f_1))(x) = f_3((f_2 \circ f_1)(x)) = f_3(f_2(f_1(x)))$ and $((f_3 \circ f_2) \circ f_1)(x) = (f_3 \circ f_2)(f_1(x)) = f_3(f_2(f_1(x)))$, which finishes the proof. $\square$

With the following lemma we characterize the injective and surjective functions.

1.3 Lemma.

1. *A function $f: X \to Y$ is injective if and only if there exists a function $l: f(X) \to X$ such that $l \circ f = \mathrm{id}_X$. The function l is called the* left-inverse *of f.*

2. *A function $f: X \to Y$ is surjective if and only if there exists a function $r: Y \to X$ such that $f \circ r = \mathrm{id}_Y$. The function r is called a* right-inverse *of f.*

Proof.

1. Let f be an injective function, then for each $y \in f(X)$ there exists exactly one $x_y \in X$ such that $f(x_y) = y$, i. e. $f^{-1}(\{y\}) = \{x_y\}$. Consequently we can define a function $l: f(X) \to X$ by $l(y) = x_y$. (This function is even a bijection between X and $f(X)$.) From the construction of l we derive that $l \circ f$ has X as its domain and range and that $(l \circ f)(x) = l(f(x)) = x$ for all $x \in X$. So $l \circ f = \mathrm{id}_X$.

   Conversely, if there is a function $l: f(X) \to X$ such that $l \circ f = \mathrm{id}_X$ then it can be proved that f is injective. Take $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$, then $x_1 = (l \circ f)(x_1) = l(f(x_1)) = l(f(x_2)) = (l \circ f)(x_2) = x_2$, hence f is injective.

2. Let f be a surjective function, then $f^{-1}(\{y\}) \neq \emptyset$ for all $y \in Y$. Define a function $r: Y \to X$ by choosing $r(y)$ as an arbitrary element in $f^{-1}(\{y\})$. Then $(f \circ r)(y) = f(r(y)) = y$ for all $y \in Y$ since $r(y) \in f^{-1}(\{y\})$. Hence $f \circ r = \mathrm{id}_Y$.

   Conversely, if there is a function $r: Y \to X$ such that $f \circ r = \mathrm{id}_Y$ then f is surjective since $Y = (f \circ r)(Y) = f(r(Y)) \subseteq f(X) \subseteq Y$. □

1.4 Corollary. *A function $f: X \to Y$ is bijective if and only if there is a function $f^{-1}: Y \to X$ — the* inverse *of f — such that $f^{-1} \circ f = \mathrm{id}_X$ and $f \circ f^{-1} = \mathrm{id}_Y$. The function f^{-1} is bijective as well.*

Proof. If f is bijective then $f(X) = Y$ and f is injective, consequently its left-inverse function l is a function from Y to X such that $(l \circ f) = \mathrm{id}_X$. From the construction of l it is clear that $f^{-1}(\{y\}) = \{l(y)\}$ for $y \in Y$ so that $(f \circ l)(y) = f(l(y)) = y$, which proves that $f \circ l = \mathrm{id}_Y$. Thus the function l is both a left- and right-inverse of f. Above it was denoted by f^{-1}.

Conversely, if there is a function $f^{-1}: Y \to X$ such that $f^{-1} \circ f = \mathrm{id}_X$ and $f \circ f^{-1} = \mathrm{id}_Y$ then f has a left- and a right-inverse function, therefore f is both injective and surjective, which implies that f is a bijection. □

1.5 Lemma.

1. *The composition of two injective functions is injective.*
2. *If both $f: X \to Y$ and $g: Y \to Z$ are surjective, then $g \circ f: X \to Z$ is surjective.*
3. *If both $f: X \to Y$ and $g: Y \to Z$ are bijective, then $g \circ f: X \to Z$ is bijective.*

A set X is called of *cardinality* $n \in \mathbb{N}$ if and only if there exists a bijection f from X to $\underline{n}$. A set X is called *finite* if and only if either there is some $n \in \mathbb{N}$ such that X is of cardinality n or X is the empty set. For instance the sets $\underline{n}$ and Z_n are of cardinality n. The cardinality of a finite set X is indicated as $|X|$. A subset of a set X of cardinality k is called a *k-subset* of X.

If X and Y are finite and $|X| = |Y|$, then a function $f: X \to Y$ is injective if and only if f is surjective. In this case injectivity, surjectivity and bijectivity are equivalent properties of f.

Bijective functions with the same finite set X as domain and range are called *permutations*. The set of all permutations on X is the *symmetric group* S_X on X.

$$S_X := \{\pi: X \to X \mid \pi \text{ is bijective}\}$$

1.6 Lemma. *The symmetric group $S_{\underline{n}}$ of $\underline{n}$ consists of $n! := n \cdot (n-1) \cdots 2 \cdot 1$ elements.*

Proof. All elements π of $S_{\underline{n}}$ can be constructed in the following way. For defining $\pi(1)$ choose from all elements of $\underline{n}$, so there are n possibilities to choose $\pi(1) \in \underline{n}$. After having defined $\pi(1)$ we choose $\pi(2)$ in the set $\underline{n} \setminus \{\pi(1)\}$, since $\pi(2)$ must be different from $\pi(1)$, thus there are $(n-1)$ possibilities left. Going on like this we see that when π is already defined on $1, 2 \ldots, n-2$ then there are two possibilities left to define $\pi(n-1)$ and finally one possibility for choosing $\pi(n)$ such that π is injective. Multiplying all these possibilities amounts to $n!$ possible elements in $S_{\underline{n}}$. $\square$

For elements of $S_{\underline{n}}$ the following notations are usually used:

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix} \quad \text{or} \quad \pi = [\pi(1), \pi(2), \ldots, \pi(n)].$$

A third form of writing a permutation $\pi \in S_{\underline{n}}$ is the *cycle notation* of π. For $k \in \mathbb{N}_0$ define π^k by

$$\pi^k := \begin{cases} \mathrm{id}_{\underline{n}} & \text{if } k = 0 \\ \pi \circ \pi^{k-1} & \text{if } k > 0, \end{cases}$$

then $\pi^k \in S_{\underline{n}}$. For an arbitrary element $i \in \underline{n}$ compute the sequence $(i, \pi(i), \pi^2(i), \ldots)$ which consists of elements of $\underline{n}$. Since $\underline{n}$ is a finite set, there exists a minimal integer $k \in \mathbb{N}$ such that $\pi^k(i) \in \{i, \pi(i), \ldots, \pi^{k-1}(i)\}$ which means $\pi^j(i) \notin \{i, \pi(i), \ldots, \pi^{j-1}(i)\}$ for $j < k$. Then $\pi^k(i)$ must be equal to i, because otherwise if $\pi^k(i) = \pi^j(i)$ for some $j \in \{1, \ldots, k-1\}$ then $\pi(\pi^{k-1}(i)) = \pi^k(i) = \pi^j(i) = \pi(\pi^{j-1}(i))$. Since π is injective $\pi^{k-1}(i) = \pi^{j-1}(i)$ and $0 \le j-1 \le k-2$ which is a contradiction to the minimality of k.

This proves that the permutation π exchanges the elements $i, \pi(i), \pi^2(i), \ldots$ cyclically.

$$i \mapsto \pi(i) \mapsto \pi^2(i) \mapsto \ldots \mapsto \pi^{k-1}(i) \mapsto \pi^k(i) = i$$

In other words, the elements i, $\pi(i)$, $\ldots$, $\pi^{k-1}(i)$ form a *cycle* of length k. This cycle is indicated as $(i, \pi(i), \ldots \pi^{k-1}(i))$ or in general a cycle of length k as $(i_1, \ldots, i_k)$ with $i_1, \ldots, i_k$ pairwise different elements in $\underline{n}$. The notation of a cycle is not unique since

$$(i_1, \ldots, i_k) = (i_2, \ldots, i_k, i_1) = \ldots = (i_k, i_1, \ldots, i_{k-1}).$$

The element of a cycle of length 1 is called a *fixed point* of π. Cycles of length 2 are usually called *transpositions.* Two cycles are called *disjoint* if the elements which are cyclically permuted form two disjoint sets in $\underline{n}$. Each permutation $\pi \in S_{\underline{n}}$ can be decomposed as a product of pairwise disjoint cycles. A possible method for decomposing a given permutation π is the following. Take an element $i \in \underline{n}$ and determine the cycle $(i, \pi(i), \ldots)$. While there are still elements in $\underline{n}$ which did not occur in the cycles so far take such an element i and determine its cycle $(i, \pi(i), \ldots)$. The following method can be used for making this cycle decomposition of $\pi \in S_{\underline{n}}$ unique. First determine the cycle which contains 1. And then while there are still elements which did not occur in the cycles so far, find the smallest element among them and determine its cycle. This way the *standard cycle decomposition* of π is obtained in the form

$$\pi = \mathop{\circ}_{\nu=1}^{c(\pi)} (i_\nu, \pi(i_\nu), \ldots, \pi^{l_\nu - 1}(i_\nu)) :=$$

$$(i_1, \pi(i_1), \ldots, \pi^{l_1-1}(i_1)) \circ \ldots \circ (i_{c(\pi)}, \pi(i_{c(\pi)}), \ldots, \pi^{l_{c(\pi)}-1}(i_{c(\pi)})),$$

where $c(\pi)$ is the number of cycles in π, $1 = i_1 < \ldots < i_{c(\pi)}$, l_ν is the length of the ν-th cycle, and i_ν is the smallest element in the ν-th cycle. Cycles of length one are often omitted in cycle decompositions. For example these are four different possibilities to write down the permutation

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

The cycle decomposition of $\pi \in S_{\underline{n}}$ determines its *cycle type* $\lambda(\pi)$. It is a sequence of non-negative integers $\lambda_i(\pi)$

$$\lambda(\pi) = (\lambda_1(\pi), \lambda_2(\pi), \ldots, \lambda_n(\pi))$$

where $\lambda_i(\pi)$ is the number of cycles of length i in the decomposition of π, i. e.

$$\lambda_i(\pi) = |\{\nu \mid 1 \leq \nu \leq c(\pi),\ l_\nu = i\}|\,.$$

From the definition it is clear that $\sum_{i=1}^n i \cdot \lambda_i(\pi) = n$. For example the above permutation σ is of cycle type $(2,1,1)$.

2 Divisors, primes and congruences

For the next sections we need some knowledge from elementary number theory. For that reason some of the basic facts are collected in this paragraph. First it should be mentioned that the elements in $\mathbb{Z}$ are *totally ordered* by

$$\ldots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \ldots.$$

In several places we will need the following version of division in $\mathbb{Z}$.

2.1. Division algorithm. *For each $z \in \mathbb{Z}$ and each $n \in \mathbb{N}$ there exist exactly one integer $q \in \mathbb{Z}$ and exactly one nonnegative integer $r < n$ such that $z = nq + r$. The integer r is called the* residue *of z divided by n.*

Proof. First we show that for given integers z and n we can find integers q and r as indicated above. Determine q as the greatest integer less than or equal to the real number $\frac{z}{n}$. Then $q \leq \frac{z}{n} < q + 1$ and $nq \leq z < nq + n$. When setting $r = z - nq$ then $0 \leq r < n$, thus we found q and r as required.

In order to prove the uniqueness statement, assume that z can be expressed as $z = nq_1 + r_1$ and as $z = nq_2 + r_2$ such that $0 \leq r_1, r_2 < n$. Without loss of generality let $r_2 \geq r_1$. Then the difference $r_2 - r_1 = n(q_1 - q_2)$ is a multiple of n. According to the special choice of r_1 and r_2 this is only possible for $r_2 - r_1 = 0$, which means $r_2 = r_1$ and finally $q_1 = q_2$. $\square$

An element $d \in \mathbb{Z}$ is called a *divisor* of $a \in \mathbb{Z}$ (or a a *multiple* of d) if and only if there is an element $b \in \mathbb{Z}$ such that $db = a$, which is indicated by $d \mid a$. Otherwise d does not divide a, which is denoted by $d \nmid a$. Obviously for any $a \in \mathbb{Z}$ it is true that $\pm 1 \mid a$, $\pm a \mid a$ and $a \mid 0$. Moreover each $a \in \mathbb{Z} \setminus \{0\}$ is not a multiple of 0. For $a \in \mathbb{Z}$ the *absolute value of a* is defined by

$$|a| := \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0. \end{cases}$$

If d is a divisor of $a \neq 0$, then $|d| \leq |a|$ and the set $D(a) := \{d \in \mathbb{Z} \mid d \text{ is a divisor of } n\}$ is a subset of the (finite) set $\{z \in \mathbb{Z} \mid -|a| \leq z \leq |a|\}$ for $a \neq 0$. For two integers $a, b \in \mathbb{Z}$, not both of them equal to zero, the *greatest common divisor of a and b* is the maximal element in the intersection $D(a) \cap D(b)$.

$$\gcd(a, b) := \max(D(a) \cap D(b))$$

This intersection is not empty since 1 is an element both of $D(a)$ and $D(b)$. This set is finite (since at least one of these two sets is finite) hence the maximum exists, it is uniquely defined and it is positive. Another characterization of the greatest common divisor is given by

2.2. Bezout's Identity. *The greatest common divisor of two integers a and b, not both of them equal to zero, is given as*

$$\min\{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}.$$

Especially, $\gcd(a, b) = 1$ *if and only if there exist integers u and v such that $au + bv = 1$.*

Proof. Define the positive integer m as the minimum of the set

$$\{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}.$$

This set is bounded from below and $a^2 + b^2$ is an element of this set. Therefore the minimum exists, and let $m = au + bv$ be this minimum. Since $\gcd(a, b)$ is a positive divisor of $m > 0$, it is true that $\gcd(a, b) \leq m$. If we can prove that m is a divisor of both a and b then $m \leq \gcd(a, b)$ must hold, so finally we get $m = \gcd(a, b)$. Assuming in contrary that m is not a divisor of b, an application of 2.1 leads to $b = qm + r$ with integers q, r such that $0 < r < m$. Then r can be written as

$$r = b - qm = b - q(au + bv) = -auq + b(1 - qv).$$

Hence r is a positive integer less than m which can be expressed as a linear combination of a and b. This is a contradiction to choosing m as the smallest positive element with this property. This contradiction was caused by the assumption $m \nmid b$, consequently m divides b. The same arguments can be used in order to prove that $m \mid a$ and the proof is finished. □

Two elements $a, b \in \mathbb{Z}$ are called *relatively prime* if and only if $\gcd(a, b) = 1$.

The *least common multiple of* $a, b \in \mathbb{Z} \setminus \{0\}$ is the smallest integer $n \in \mathbb{N}$ such that both a and b are divisors of n.

$$\operatorname{lcm}(a, b) := \min \left\{ n \in \mathbb{N} \;\middle|\; a \mid n \text{ and } b \mid n \right\}$$

Since $|ab| > 0$ is a common multiple of a and b and $\mathbb{N}$ is bounded from below, this minimum exists and it is uniquely defined.

The following propositions will be useful in various places:

2.3 Lemma. *Let $a, b \in \mathbb{Z}$ such that not both of them are equal to zero.*

1. *Then* $\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$.
2. *Let $c \in \mathbb{N}$ then* $c \gcd(a, b) = \gcd(ac, bc)$.
3. *If $a \neq 0 \neq b$ and $c \in \mathbb{N}$ then* $c \operatorname{lcm}(a, b) = \operatorname{lcm}(ac, bc)$.
4. *If* $\gcd(a, b) = 1$ *and $c \in \mathbb{Z}$ such that $a \mid bc$ then $a \mid c$.*
5. $\gcd(a, b) = \gcd(a + cb, b)$ *for $c \in \mathbb{Z}$.*

The next lemma describes an interesting relationship between $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$.

2.4 Lemma. *For $a, b \in \mathbb{Z} \setminus \{0\}$ it is always true that*

$$|ab| = \operatorname{lcm}(a, b) \gcd(a, b).$$

Proof. Without loss of generality we can assume that both a and b are positive. Consider first the case that $\gcd(a, b) = 1$. From $a \mid \operatorname{lcm}(a, b)$ it is obvious that $\operatorname{lcm}(a, b) = ac$ for some $c \in \mathbb{N}$. Since $b \mid \operatorname{lcm}(a, b) = ac$ and $\gcd(a, b) = 1$ it follows from 2.3 that

$b \mid c$, i. e. there is some $d \in \mathbb{N}$ such that $c = bd$. Finally we derive that $\operatorname{lcm}(a,b) = abd$ for some $d \in \mathbb{N}$, but $\operatorname{lcm}(a,b) \leq ab$, therefore $d = 1$ and $\operatorname{lcm}(a,b) = ab$.

For the general case let $g := \gcd(a,b)$, then from 2.3 it follows that $\gcd(\frac{a}{g}, \frac{b}{g}) = 1$. The first part of this proof shows that

$$\operatorname{lcm}(\frac{a}{g}, \frac{b}{g}) = \frac{ab}{g^2}.$$

Multiplying this equation by g^2 and applying 2.3 yields

$$g^2 \operatorname{lcm}(\frac{a}{g}, \frac{b}{g}) = g \operatorname{lcm}(a,b) = ab,$$

which completes the proof since $g = \gcd(a,b)$. □

An integer $p > 1$ is called a *prime number* if and only if the set of divisors of p is given by $D(p) = \{\pm 1, \pm p\}$. For a prime p it is obvious that $\gcd(a,p) \neq 1$ if and only if a is a multiple of p and in that case $\gcd(a,p) = p$.

2.5 Lemma. *For an integer $p > 1$ the following two statements are equivalent:*

1. *p is a prime number.*
2. *If p divides the product of two integers a and b then $p \mid a$ or $p \mid b$.*

Proof. If p is a prime, $p \mid ab$ and $p \not| a$ then $\gcd(a,p) = 1$. According to 2.3 $p \mid b$.

For proving that 2. implies 1., assume that p is not a prime, whence p can be written as $p = ab$ such that $1 < a, b < p$. Moreover since p divides ab we deduce from 2. that $p \mid a$ or $p \mid b$, but this is not possible because of $a < p$ and $b < p$. Thus we end up with a contradiction which was caused by the assumption that p is not prime. □

The next theorem describes the important role of prime numbers.

2.6. Fundamental theorem of arithmetics. *Any integer $n > 1$ can be expressed as a product of finitely many primes. If there exist two representations of n as a product of prime numbers $n = p_1 \cdots p_k = q_1 \cdots q_l$ then $l = k$ and there is a permutation $\pi \in S_{\underline{k}}$ such that $p_i = q_{\pi(i)}$.*

Proof. We apply induction on n in order to show that each $n > 1$ can be expressed as a product of primes. In the case $n = 2$ it is possible to set $k = 1$ and $p_1 = 2$ and we are done. Let $n > 2$ and assume that each integer m (such that $2 \leq m < n$) can be expressed as a product of finitely many primes. Now two cases must be distinguished. Either there is a non-trivial divisor a of n, thus $n = ab$ for $1 < a, b < n$. According to the assumption both a and b can be expressed as products of finitely many primes, therefore the same holds for $n = ab$. Or in the second case there does not exist a non-trivial divisor of n, hence the positive divisors of n are just 1 and n, so n is a prime and similar to the case $n = 2$ we can put $k = 1$ and $p_1 = n$.

Now assume that there are two possibilities to write n as a product of primes: $n = p_1 \cdots p_k = q_1 \cdots q_l$. Here we apply induction on k. If $k = 1$ then $p_1 = q_1 \cdots q_l$, hence $q_i \mid p_1$ for all i. Since p_1 is prime, $l = 1$ and $p_1 = q_1$. Now assume that $k > 1$ and that each product of $k-1$ primes is unique with exception of the ordering of the factors in this product. Then $l > 1$ and the prime number p_k divides $q_1 \cdots q_l$. According to 2.5 there exists $j \in \underline{l}$ such that $p_k \mid q_j$. Since q_j is a prime, $p_k = q_j$. Without loss of generality $j = l$ and therefore $p_k = q_l$. As a consequence

$$\frac{n}{p_k} = p_1 \cdots p_{k-1} = q_1 \cdots q_{l-1}$$

can be written as a product of $k-1$ primes. From the induction assumption we deduce that $k-1 = l-1$ and that there is a permutation $\rho \in S_{\underline{k-1}}$ such that $p_i = q_{\rho(i)}$ for $i < k$. Immediately we have $k = l$. Now define $\pi \in S_{\underline{k}}$ by $\pi(i) = \rho(i)$ for $1 \le i < k$ and $\pi(k) = k$, then $p_i = q_{\pi(i)}$ for $1 \le i \le k$. □

As a consequence of 2.6 each integer $n > 1$ can uniquely be written as

2.7
$$n = \prod_{i=1}^{r} p_i^{a_i}$$

for some integer $r \in \mathbb{N}$, prime numbers $p_1 < p_2 < \ldots < p_r$ and integers $a_i > 0$.

As we will see in 4.2 the elements in Z_n relatively prime to n are of particular interest. Their number is expressed by the *Euler function* φ. For $n \in \mathbb{N}$ it is defined by

$$\varphi(n) := |\{i \mid 0 \le i < n,\ \gcd(i,n) = 1\}| = |\{i \in Z_n \mid \gcd(i,n) = 1\}|.$$

2.8 Lemma. *The Euler function has the following properties:*

1. $\varphi(1) = 1$.
2. $\varphi(p^a) = p^{a-1}(p-1)$ *for any prime* p *and any integer* $a \in \mathbb{N}$.
3. *Let* p *be a prime and* n *a positive integer. Then*

$$\varphi(np) = \begin{cases} (p-1)\varphi(n) & \text{if } p \nmid n \\ p\varphi(n) & \text{if } p \mid n. \end{cases}$$

4. *If the integer* $n > 1$ *has the (unique) factorization 2.7 into primes then*

$$\varphi(n) = \prod_{i=1}^{r} p_i^{a_i - 1}(p_i - 1).$$

Proof. The first item follows directly from the definition of φ. In order to prove the second item let $a \in \mathbb{N}$, then $\gcd(i, p^a) \ne 1$ for an integer i if and only if i is a multiple of p. The set of non-negative multiples of p less than p^a is given by $\{jp \mid 0 \le j < p^{a-1}\}$.

It is of cardinality p^{a-1}. Consequently there are $p^a - p^{a-1} = p^{a-1}(p-1)$ elements $i \in \{0, 1, \ldots, p^a - 1\}$ such that $\gcd(i, p^a) = 1$.

In order to prove the third item we have to investigate two cases. If p is not a divisor of n then the set of all divisors of np is the disjoint union of $D(n)$, the set of all divisors of n, and $p \cdot D(n) = \{pd \mid d \in D(n)\}$. And $\gcd(i, np)$ is different from 1 if and only if i is a multiple of p or $\gcd(i, n)$ is different from 1. (This can be proved in the following way: If $\gcd(i, np) = d \neq 1$ and $p \not| \, i$ then $p \not| \, d$, hence d is a divisor of n which implies that $\gcd(i, n) = d \neq 1$. Conversely, if i is a multiple of p then p divides $\gcd(i, np)$. Finally from $\gcd(i, n) \neq 1$ it follows immediately that $\gcd(i, np) \neq 1$.) For that reason let S be the set $\{i \in Z_n \mid \gcd(i, n) \neq 1\}$ then 2.3 shows that

$$\{i \in Z_{np} \mid \gcd(i, np) = 1\} = Z_{np} \setminus (\{kp \mid 0 \leq k < n\} \cup \{kn + i \mid 0 \leq k < p, \ i \in S\}).$$

After having subtracted from Z_{np} all the n multiples of p and the $p(n - \varphi(n))$ elements in Z_{np} which are not relatively prime to n we have to add those elements of Z_{np} again which are both multiples of p and which are not relatively prime to n. These are the $n - \varphi(n)$ elements of $\{ip \mid i \in S\}$, such that we finally get

$$\varphi(np) = np - n - p(n - \varphi(n)) + (n - \varphi(n)) = (p-1)\varphi(n).$$

If p is a divisor of n then $\gcd(i, np) = 1$ if and only if $\gcd(i, n) = 1$. (If $\gcd(i, np) = 1$ then it is obvious that $\gcd(i, n) = 1$. Conversely, if $\gcd(i, n) = 1$ it is clear that $p \not| \, n$ which implies that i is not a multiple of p, so $\gcd(i, p) = 1$ and $\gcd(i, np) = 1$.) Hence $\varphi(pn)$ is the cardinality of the set $\{kn + i \mid 0 \leq k < p, \ i \notin S\}$ which is $p\varphi(n)$. Induction over r (the number of different prime divisors of n) proves the last item of this lemma. In the second item the proof was given for $r = 1$. Let $r > 1$ and let $n' = \prod_{i=1}^{r-1} p_i^{a_i}$. From the third item we know that $\varphi(p_r n') = (p_r - 1)\varphi(n')$ and by induction on k it follows that $\varphi(p_r^k n') = p_r^{k-1}(p_r - 1)\varphi(n') = \varphi(p_r^k)\varphi(n')$. Applying the induction hypothesis to $\varphi(n')$ finishes the proof. □

2.9 Corollary. *Let d be a positive divisor of $n \in \mathbb{N}$ then the number of elements $i \in Z_n$ such that* $\gcd(i, n) = d$ *is* $\varphi(\frac{n}{d})$.

Proof. Since $\gcd(i, n) = d$ if and only if $\gcd(\frac{i}{d}, \frac{n}{d}) = 1$ (cf. 2.3) the number of integers $i \in Z_n$ such that $\gcd(i, n) = d$ is equal to

$$\left| \left\{ i \in Z_n \mid \gcd(\frac{i}{d}, \frac{n}{d}) = 1 \right\} \right| = \left| \left\{ j \in Z_{n/d} \mid \gcd(j, \frac{n}{d}) = 1 \right\} \right| = \varphi(\frac{n}{d})$$

and the proof is finished. □

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then *a is congruent to b modulo n* if and only if n is a divisor of the difference $a - b$.

$$a \equiv b \bmod n :\Longleftrightarrow n \mid (a - b)$$

This is an equivalence relation on $\mathbb{Z}$. (An *equivalence relation* on a set X is a subset R of $X \times X$ with the following properties. *Reflexivity*: $(x, x) \in R$ for all $x \in R$. *Symmetry*: If $(x, y) \in R$ then $(y, x) \in R$. *Transitivity*: If (x, y) and $(y, z) \in R$ then $(x, z) \in R$. Usually we write $x\, R\, y$ instead of $(x, y) \in R$ in order to indicate that x and y are *equivalent*. The *equivalence class* of x is the set of all y such that $(x, y) \in R$. The equivalence classes of two elements x_1, x_2 are either equal (then $(x_1, x_2) \in R$, i. e. x_1 and x_2 are equivalent), or they are disjoint (when x_1 is not equivalent to x_2).)

The equivalence classes of congruence modulo n are the sets $i+n\mathbb{Z} = \{i + nz \mid z \in \mathbb{Z}\}$. It follows from the Division Algorithm 2.1 that the elements of $Z_n = \{0, 1, \ldots, n-1\}$ form a complete set of representatives of these equivalence classes.

2.10 Lemma. *For $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$ the* cancellation law *holds:*

$$ac \equiv bc \bmod n \iff a \equiv b \bmod \frac{n}{\gcd(c, n)}.$$

Proof. An application of 2.3 yields: $ac \equiv bc \bmod n \iff n \mid (ac - bc) \iff n \mid (a-b)c \iff \frac{n}{\gcd(c,n)} \mid (a-b)\frac{c}{\gcd(c,n)} \iff \frac{n}{\gcd(c,n)} \mid (a-b) \iff a \equiv b \bmod \frac{n}{\gcd(c,n)}$. □

Next we solve *linear congruences* of the form $a \cdot x \equiv c \bmod n$ for $a, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. An integer b is a solution of this congruence if and only if $ab \equiv c \bmod n$. If b is a solution of this congruence then each integer of the form $b + zn$ for $z \in \mathbb{Z}$ is also a solution of it. Therefore we are mainly interested in *incongruent* solutions modulo n. These are the solutions in a complete set of representatives modulo n, for instance the solutions in Z_n.

2.11 Theorem. *Let $a, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. The linear congruence $a \cdot x \equiv c \bmod n$ has a solution if and only if $\gcd(a, n)$ divides c.*

If the linear congruence has a solution then there exist $\gcd(a, n)$ solutions which are incongruent modulo n. (In other words, if $\gcd(a, n) \mid c$ then there exist $\gcd(a, n)$ different solutions in Z_n.)

Proof. If the linear congruence has a solution, i. e. $ab \equiv c \bmod n$ for $b \in \mathbb{Z}$, then n divides $ab-c$. So there is $d \in \mathbb{Z}$ such that $nd = ab-c$ or $nd-ab = -c$. Since $\gcd(a, n)$ divides the left-hand side it must divide the right-hand side as well, consequently $\gcd(a, n)$ is a divisor of c.

Conversely, if $\gcd(a, n)$ divides c, then define $a' := \frac{a}{\gcd(a,n)}$, $c' := \frac{c}{\gcd(a,n)}$ and $n' := \frac{n}{\gcd(a,n)}$. Due to this construction (see 2.3) $\gcd(a', n') = 1$ and from 2.10 we conclude that for $z \in \mathbb{Z}$

2.12 $$az \equiv c \bmod n \iff a'z \equiv c' \bmod n'.$$

An application of Bezout's Identity 2.2 to $\gcd(a', n') = 1$ shows that there exist integers u, v such that $a'u + n'v = 1$, thus there exists $a'' \in \{1, 2, \ldots, n'-1\}$ such that $a'a'' \equiv 1 \bmod n'$. The second congruence in 2.12 has a solution of the form $a''c'$, since $a'a''c' \equiv 1c' = c' \bmod n'$. The set of all solutions (in Z_n) of the congruence on the left side of 2.12 is then given as

$$\{a''c' + kn' \mid k = 0, 1, \ldots, \gcd(a, n) - 1\}.$$

□

Finally we solve systems of simultaneous congruences: Before doing this we introduce for $r > 2$ the least common multiple of numbers $n_1, \ldots, n_r \in \mathbb{Z} \setminus \{0\}$. It is recursively defined by

$$\mathrm{lcm}(n_1, \ldots, n_r) = \mathrm{lcm}(\mathrm{lcm}(n_1, \ldots, n_{r-1}), n_r).$$

2.13 Lemma. *Let $r \geq 2$ and $n_1, \ldots, n_r \in \mathbb{N}$, such that $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Then $n_1 \cdots n_r = \mathrm{lcm}(n_1, \ldots, n_r)$.*

2.14 Lemma. *Let $n_1, \ldots, n_r \in \mathbb{N}$ and $z, z' \in \mathbb{Z}$ then*

$$z \equiv z' \bmod n_i \textit{ for } i = 1, \ldots, r \Longleftrightarrow z \equiv z' \bmod \mathrm{lcm}(n_1, \ldots, n_r).$$

2.15 Theorem. *Let $n_1, \ldots, n_r \in \mathbb{N}$ and $a_1, \ldots, a_r \in \mathbb{Z}$ such that $\gcd(n_i, n_j) = 1$ for all $i \neq j$, then the following system of congruences*

2.16 $$x \equiv a_i \bmod n_i \textit{ for } i = 1, \ldots, r$$

has a solution. Moreover two different solutions of 2.16 are congruent modulo $n_1 \cdots n_r$.

Proof. Let $n := n_1 \cdots n_r$ then $\gcd(\frac{n}{n_j}, n_j) = 1$ for all j. Bezout's Identity 2.2 guarantees that there exist integers b_j such that $\frac{n}{n_j} b_j \equiv 1 \bmod n_j$. Since furthermore $\frac{n}{n_j} b_j \equiv 0 \bmod n_i$ for $i \neq j$ the integer

$$z := \sum_{j=1}^{r} \frac{n}{n_j} b_j a_j$$

is a solution of 2.16. If z' is an arbitrary solution of 2.16, then $z' \equiv z \bmod n_i$ for all i. In 2.13 and 2.14 it is shown that

$$z' \equiv z \bmod n \Longleftrightarrow z' \equiv z \bmod n_i \text{ for } i = 1, \ldots, r.$$

$\square$

3 Groups and group actions

In this section the very important notion of groups is introduced. We learn some basic facts about groups, subgroups, permutation groups and group actions. As was already mentioned the notion of group actions is later used for introducing the n-scale Z_n and for describing when motives are regarded to be similar or equivalent. In general the set of all (symmetry) operations on a set X forms a group called the symmetry group of X.

An *inner composition* on a set X is a mapping $\star$ from $X \times X$ to X. For $x_1, x_2 \in X$ we usually write $x_1 \star x_2$ instead of $\star(x_1, x_2)$. For instance addition $+$ and multiplication $\cdot$ are inner compositions on sets like $\mathbb{N}$, $\mathbb{Z}$ or $\mathbb{Q}$.

A set G together with an inner composition $\star$ is a *group* $(G, \star)$ if and only if the following axioms hold.

- $\star$ is an associative composition, i. e. $g_1 \star (g_2 \star g_3) = (g_1 \star g_2) \star g_3$ for all $g_1, g_2, g_3 \in G$.
- There exists an *identity element* $e \in G$ such that $e \star g = g \star e = g$ for all $g \in G$.
- For all $g \in G$ there exists an *inverse element* g' such that $g \star g' = g' \star g = e$.

If moreover this composition is *commutative*, i. e. $g_1 \star g_2 = g_2 \star g_1$ for all $g_1, g_2 \in G$, then G is called a *commutative group* or an *Abelian group*.

3.1 Examples.

1. The set $\mathbb{Z}$ together with $+$ is a commutative group. The identity element is 0, the inverse of $z \in \mathbb{Z}$ is $-z$. Using the same arguments you can show that $(\mathbb{Q}, +)$ is a commutative group.

2. The set $\mathbb{Q} \setminus \{0\}$ together with $\cdot$ is a commutative group. The identity element is 1, the inverse of $q \in \mathbb{Q} \setminus \{0\}$ is $q^{-1} = 1/q$. Why is $(\mathbb{Q}, \cdot)$ not a group?

3. Define on Z_n an inner composition (an sum) by
$$a \oplus b := \begin{cases} a+b & \text{if } a+b < n \\ a+b-n & \text{if } a+b \geq n \end{cases} \qquad \text{for } a, b \in Z_n,$$
then $(Z_n, \oplus)$ is a commutative group. From the definition it is clear that $a \oplus b \equiv a + b \bmod n$. For the rest of this paper we rather use $+$ instead of $\oplus$ for indicating this composition.

4. The symmetric group S_X together with $\circ$, the composition of mappings, is a group. (Hence it makes sense to call it a group.) In general this group is not commutative. $\diamond$

For simplifying the notation we usually use the notation of a multiplicative group $(G, \cdot)$ or just G. Instead of $g \cdot h$ we write gh, for $g, h \in G$. Then the identity element is denoted by 1 and the inverse of g by g^{-1}.

A subset U of a group $(G, \cdot)$ is called a *subgroup* of G if and only if $(U, \cdot)$ is a group as well, which will be indicated as $U \leq G$. Since U must contain an identity element, U is different from $\emptyset$. Moreover the identity element of G is the same as the identity element of U. Trivial subgroups of G are G or the group consisting of the identity element only. For instance $(\mathbb{Z}, +)$ is a non-trivial subgroup of $(\mathbb{Q}, +)$.

The set of all subgroups of a group G is indicated by $L(G)$. This set is called the *subgroup lattice* of G.
$$L(G) := \{U \mid U \leq G\}$$
The cardinality $|U|$ of a (finite) subgroup U of G is called the *order of* U. The following characterization of subgroups of G is often very useful.

3.2 Lemma. *A subset U of a group G is a subgroup of G if and only if U is not empty and for all $g, h \in U$ the element $g^{-1}h$ is also in U.*

Proof. Let U be a subgroup of G then the identity element 1 of G also belongs to U, therefore $U \neq \emptyset$. The inverse of $g \in U$ must belong to U, so the product $g^{-1}h$ is in U as well.

Let U be a non-empty subset of G then there exists some $g \in U$. According to the assumption $g^{-1}g = 1 \in U$, i. e. the identity element of G is in U and it is the identity element of U. For each $g \in U$ the inverse of g is also in U, since $g^{-1}1 = g^{-1} \in U$. The multiplication is an inner composition on U since for all $g, h \in U$ the element $g^{-1} \in U$ and (since the inverse of g^{-1} is g) the product $gh \in U$. The multiplication is associative in U, since it is associative in G. This proves that U is a group, whence U is a subgroup of G. □

3.3 Lemma. *For $\mathcal{U} \subseteq L(G)$, the intersection*

$$V := \bigcap_{U \in \mathcal{U}} U$$

of subgroups U of a group G is again a subgroup of G. (In other words, the intersection $\cap$ is an inner composition on $L(G)$.)

Proof. The characterization 3.2 can be applied in order to show that V is a subgroup of G. The set V is not empty since the identity element 1 of G lies in each of the subgroups U, thus $1 \in V$. Take two elements g, h of V, then $g, h \in U$ for all $U \in \mathcal{U}$. Since these U are subgroups, $g^{-1}h$ is also an element of U for all $U \in \mathcal{U}$, consequently $g^{-1}h \in V$. □

For a given subset S of a group G the subgroup $\langle S \rangle$ generated by S is defined by

$$\langle S \rangle := \bigcap_{\substack{U \leq G \\ S \subseteq U}} U.$$

From this definition it is clear that $\langle S \rangle$ is the intersection of all subgroups of G which contain S. According to 3.3 it is the smallest subgroup of G which contains S. If S consists of only one element, i. e. $S = \{g\}$ for some $g \in G$, then the group $\langle g \rangle := \langle \{g\} \rangle$ is called a *cyclic group* generated by g.

3.4 Example.

1. The cyclic group $U := \langle g \rangle \leq G$ is given by

   $$U = \{g^z \mid z \in \mathbb{Z}\},$$

   where g^z is defined by

   $$g^z := \begin{cases} 1 & \text{if } z = 0 \\ g^{z-1}g & \text{if } z \geq 1 \\ (g^{-z})^{-1} & \text{if } z < 0. \end{cases}$$

This set U is a subgroup of G by 3.2 since $1 \in U$ and $g^{-z_1} g^{z_2} = g^{-z_1+z_2} \in U$ for all $z_1, z_2 \in \mathbb{Z}$. And U is the smallest subgroup of G containing g, since together with g all the powers g^n (for $n \in \mathbb{N}_0$) of g and all the powers $(g^{-1})^n = g^{-n}$ of g^{-1} must belong to U.

If G is finite then it is enough to consider the positive powers g^n of g. Since the set $\{g^n \mid n \in \mathbb{N}\}$ is a subset of the finite set G, there must be some natural numbers $i, j \in \mathbb{N}$ such that $i < j$ and $g^i = g^j$. Multiplying both sides with g^{-i} we get $1 = g^0 = g^{j-i}$. Let k be the smallest positive integer such that $g^k = 1$,

$$k := \min \{n \in \mathbb{N} \mid g^n = 1\},$$

then $\langle g \rangle$ is of order k and the elements of this subgroup are given as $\langle g \rangle = \{g, g^2, \ldots, g^k\}$. The identity element is g^k and the inverse of g^i for $1 \leq i \leq k-1$ is g^{k-i}. The integer k is called the *order of g* in G.

2. The permutation group $C_n := \langle (1, 2, \ldots, n) \rangle$ is a *cyclic group* of order n. It is generated by the cyclic permutation $\pi := (1, 2, \ldots, n)$. The elements of C_n can be seen as all possibilities of rotating a regular n-gon.

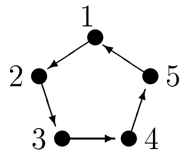


Figure 1: Cyclic shifts in a regular 5-gon.

3. For $n \geq 3$ the group $D_n := \langle (1, 2, \ldots, n), (1, n)(2, n-1) \ldots \rangle$ is called a *dihedral group*. It is of order $2n$. Let π and σ denote the two generators of D_n, where π is the cycle of length n, then depending on n the permutation σ is of the form

$$\sigma = \begin{cases} (1, n)(2, n-1) \ldots (\frac{n-1}{2}, \frac{n+3}{2})(\frac{n+1}{2}) & \text{if } n \text{ is odd} \\ (1, n)(2, n-1) \ldots (\frac{n}{2}, \frac{n}{2} + 1) & \text{if } n \text{ is even.} \end{cases}$$

Since $\sigma \circ \pi = \pi^{-1} \circ \sigma$, each element in D_n can be written as $\pi^k \sigma^j$ such that $k \in \{0, 1, \ldots, n-1\}$ and $j \in \{0, 1\}$. The elements of D_n can be seen as all possibilities of rotating and reflecting a regular n-gon. The reflections are the elements of the form $\pi^k \sigma$. If n is odd then each reflection consists of exactly 1 fixed point and $\frac{n-1}{2}$ transpositions. If n is even then there are $\frac{n}{2}$ reflections consisting of $\frac{n}{2}$ transpositions, and $\frac{n}{2}$ reflections consisting of two fixed points and $\frac{n}{2} - 1$ transpositions. (For more details see the proof of 5.7.) $\diamond$

A mapping $\phi\colon G \to H$ from a group $(G, \star)$ to a group $(H, *)$ is a *group homomorphism* if and only if for all $g_1, g_2 \in G$ the following identity holds:

$$\phi(g_1 \star g_2) = \phi(g_1) * \phi(g_2).$$

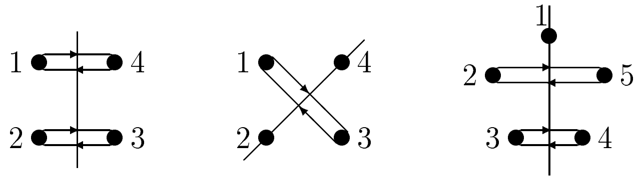


Figure 2: Reflections in regular 4- and 5-gons.

The image $\phi(U)$ of a subgroup U of G is a subgroup of H. A bijective group homomorphism $G \to H$ is called a *group isomorphism*. If there exists an isomorphism from G to H then the groups G and H are called *isomorphic*. If $G = H$ then a homomorphism is called an *endomorphism*, and bijective endomorphisms are called *automorphisms*.

3.5 Lemma. *The symmetric group S_X of a set of cardinality n is isomorphic to the symmetric group $S_{\underline{n}}$.*

Proof. Since $|X| = n$ there is a bijection $f: X \to \underline{n}$. For $\pi \in S_{\underline{n}}$ the composition $f^{-1} \circ \pi \circ f$ is a bijective mapping from X to X, whence it is an element of S_X. For that reason the mapping

$$\phi: S_{\underline{n}} \to S_X, \qquad \pi \mapsto \phi(\pi) := f^{-1} \circ \pi \circ f$$

is well defined. We show that it is a group isomorphism between $S_{\underline{n}}$ and S_X. It is a homomorphism since $\phi(\pi_1 \circ \pi_2) = f^{-1} \circ (\pi_1 \circ \pi_2) \circ f = f^{-1} \circ \pi_1 \circ \mathrm{id}_{\underline{n}} \circ \pi_2 \circ f = (f^{-1} \circ \pi_1 \circ f) \circ (f^{-1} \circ \pi_2 \circ f) = \phi(\pi_1) \circ \phi(\pi_2)$ for $\pi_1, \pi_2 \in S_{\underline{n}}$. It is bijective since the mapping

$$\psi: S_X \to S_{\underline{n}}, \qquad \pi \mapsto \psi(\pi) := f \circ \pi \circ f^{-1}$$

fulfils $\phi \circ \psi = \mathrm{id}_{S_X}$ and $\psi \circ \phi = \mathrm{id}_{S_{\underline{n}}}$. □

From the last lemma we deduce that the symmetric group S_X of a set X of cardinality n is already described by the symmetric group $S_{\underline{n}}$.

There are various possibilities to construct new groups from given groups. A very simple and basic construction is the following:

3.6 Lemma. *The Cartesian product $H \times G$ of two groups $(G, \star)$ and $(H, *)$ together with the following composition*

$$(h_1, g_1)(h_2, g_2) := (h_1 * h_2, g_1 \star g_2)$$

is a group, the direct product *of H and G.*

Now when discussing group actions of a group G on a set X we meet another kind of composition an *outer composition*. A group element g is composed with an element $x \in X$ in order to get a new element gx of X. This composition of g and x must follow certain rules in order to be a group action. The identity element $1 \in G$ may not change an element of X; and when applying the product $g_2 g_1$ (of two group elements) to an element x it must be the same as first applying g_1 to x (in order to get $g_1 x$) and then g_2 to $g_1 x$. These properties are collected in the next definition. A *group action* ${}_G X$ of the group G on the set X is given by a mapping

$$G \times X \to X, \qquad (g, x) \mapsto gx,$$

which fulfils $1x = x$ and $(g_2 g_1)x = g_2(g_1 x)$ for all $x \in X$ and $g_1, g_2 \in G$. A group action is called *finite* if both G and X are finite.

3.7 Lemma. *A group action ${}_G X$ determines a group homomorphism ϕ from G to the symmetric group S_X by*

$$\phi\colon G \to S_X, \qquad g \mapsto \phi(g) := [x \mapsto gx],$$

which is called a permutation representation *of G on X.*

Usually $\phi(g)$ is abbreviated by $\bar{g}$, which is the permutation of X that maps x to gx. For instance $\bar{1}$ is always the identity on X. Accordingly the image $\phi(G)$ is indicated by $\bar{G}$. It is a *permutation group* on X, i. e. a subgroup of S_X. If X is finite then $\bar{G}$ is finite since it is a subgroup of the symmetric group S_X which is of cardinality $|X|!$. Hence whenever X is finite we can speak of a finite group action.

3.8 Examples.

1. A trivial action of an arbitrary group G on a set X is given by $(g, x) \mapsto gx := x$ for all $g \in G$ and $x \in X$. In this situation $\bar{G} = \{\mathrm{id}_X\}$.
2. Another trivial example of an action of a subgroup U of S_X on X is given by $(\pi, x) \mapsto \pi x := \pi(x)$ for all $\pi \in U$. In this situation $\bar{U} = U$. $\diamond$

Before describing some more interesting examples of group actions we investigate certain structures which are induced by group actions. A group action ${}_G X$ defines the following equivalence relation on X. $x_1 \sim_G x_2$ if and only if there is some $g \in G$ such that $x_2 = g x_1$. The equivalence classes $G(x)$ with respect to $\sim_G$ are the *orbits* of G on X,

$$G(x) = \{gx \mid g \in G\}\,.$$

The *set of all orbits* is denoted by

$$G\backslash\backslash X := \{G(x) \mid x \in X\}\,.$$

For each $x \in X$ the *stabilizer* G_x of x

$$G_x := \{g \in G \mid gx = x\}$$

is a subgroup of G. Finally the *set of all fixed points* of $g \in G$ is denoted by

$$X_g := \{x \in X \mid gx = x\}\,.$$

Here are some more examples of group actions.

3.9 Examples.

1. A subgroup U of G acts on G by multiplication from the left

$$U \times G \to G, \qquad (u,g) \mapsto ug.$$

The orbit $U(g)$ is the *right-coset* $Ug := \{ug \mid u \in U\}$ and G is the disjoint union of the different orbits Ug in $U\backslash\backslash G$ which is usually written as $U\backslash G$. If G is finite then each orbit Ug consists of $|U|$ elements and $|G| = |U\backslash\backslash G| \cdot |U|$. This way we proved that *the order of any subgroup U of a finite group G is a divisor of* $|G|$. Moreover the order of $g \in G$ equals the order of the subgroup $\langle g \rangle$, thus it is also a divisor of $|G|$.

The subgroup U also acts from the right on G,

$$U \times G \to G, \qquad (u,g) \mapsto gu^{-1},$$

the orbits are the *left-cosets* gU and $U\backslash\backslash G = G/U$.

2. A group G acts on itself by *conjugation*

$$G \times G \to G, \qquad (g,h) \mapsto ghg^{-1}.$$

The orbit $G(h) = \{ghg^{-1} \mid g \in G\}$ is the *conjugacy class* of h. The stabilizer of h is the set $\{g \in G \mid gh = hg\}$. The set of fixed points of g is $\{h \in G \mid gh = hg\}$.

3. A group G acts on the subgroup lattice $L(G)$ by *conjugation*

$$G \times L(G) \to L(G), \qquad (g,U) \mapsto gUg^{-1} := \left\{gug^{-1} \mid u \in U\right\}.$$

The orbit $G(U)$ is the *conjugacy class* $\widetilde{U} := \{gUg^{-1} \mid g \in G\}$. The stabilizer of U is the *normalizer* $N_G(U) := \{g \in G \mid gU = Ug\}$ of U.

4. Let ${}_GX$ be a group action, then G acts on Y^X by

3.10 $$G \times Y^X \to Y^X, \qquad (g,f) \mapsto f \circ \bar{g}^{-1},$$

where $\bar{g}$ is the permutation representation of g acting on X. $f \circ \bar{g}^{-1}$ is again a function from X to Y, since $(f \circ \bar{g}^{-1})(x) = f(\bar{g}^{-1}(x)) = f(g^{-1}x)$ for $x \in X$. The set of fixed points of g is the set of all functions f which are constant on the cycles (in the cycle decomposition) of $\bar{g}$.

5. Let ${}_HY$ be a group action, then H acts on Y^X by

$$H \times Y^X \to Y^X, \qquad (h,f) \mapsto \bar{h} \circ f,$$

where $(\bar{h} \circ f)(x) = \bar{h}(f(x)) = hf(x)$ for all $x \in X$.

6. Let ${}_GX$ and ${}_HY$ be group actions, then the direct product $H \times G$ acts on Y^X by

$$(H \times G) \times Y^X \to Y^X, \qquad ((h,g), f) \mapsto \bar{h} \circ f \circ \bar{g}^{-1}.$$

The orbits of $f \in Y^X$ defined by the last three group actions are usually called *symmetry types* of mappings. ◇

Often these group actions occur in a very natural way.

3.11 Lemma. *Let ${}_GX$ be a group action. Then the stabilizer of $y = gx$ is of the form gG_xg^{-1}, i. e. it is conjugate to G_x. Moreover the stabilizers of all elements in the orbit $G(x)$ of x form the complete conjugacy class $\widetilde{G}_x$ of the subgroup G_x of G.*

There is an interesting connection between stabilizers and orbits under a given group action.

3.12 Lemma. *If G acts on X then the mapping*

$$f\colon G(x) \to G/G_x, \qquad gx \mapsto f(gx) := gG_x$$

is a bijection between $G(X)$ and the set of all left-cosets of G_x. If G is a finite group then

$$|G(X)| = |G/G_x| = \frac{|G|}{|G_x|}.$$

Proof. First we have to prove that f is well defined, i. e. the definition of f does not depend on the special way of describing an element of $G(x)$ in the form gx. Assume that $g, h \in G$ such that $gx = hx$. Then the following chain of equivalent statements holds:

$$gx = hx \iff h^{-1}gx = x \iff h^{-1}g \in G_x \iff gG_x = hG_x \iff f(gx) = f(hx).$$

Reading this sequence from left to right we deduce that f is well defined and reading it from right to left we get that f is injective. By definition f is surjective, which finishes the proof. □

Now we can prove the *Cauchy-Frobenius-Lemma*. It is the main tool for enumeration under group actions.

3.13. Cauchy-Frobenius-Lemma. *The number of orbits under a finite group action ${}_GX$ is the average number of fixed points.*

$$|G \backslash\backslash X| = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

Proof. An application of 3.12 yields

$$\sum_{g\in G}|X_g| = \sum_{g\in G}\sum_{x\in X_g} 1 = \sum_{x\in X}\sum_{g\in G_x} 1 = \sum_{x\in X}|G_x| = \sum_{x\in X}\frac{|G|}{|G(x)|} =$$

$$= |G| \sum_{\omega\in G\backslash\backslash X}\sum_{x\in\omega}\frac{1}{|G(x)|} = |G| \sum_{\omega\in G\backslash\backslash X}\sum_{x\in\omega}\frac{1}{|\omega|} = |G| \sum_{\omega\in G\backslash\backslash X} 1 = |G|\,|G\backslash\backslash X|\,.$$

In order to understand the last line it is important to remember that when $x \in \omega$ and $\omega \in G\backslash\backslash X$ then ω is the orbit $G(x)$. □

Since we are mainly interested in the group action on Y^X in the form 3.10 we compute the numbers of mapping patterns in this situation.

3.14 Corollary. *Let ${}_GX$ be a finite group action and Y a finite set. Then the number of mapping patterns under the induced action of G on Y^X is given by*

$$\left|G\backslash\backslash Y^X\right| = \frac{1}{|G|}\sum_{g\in G}|Y|^{c(\bar{g})}\,,$$

where $c(\bar{g})$ is the number of cycles (in the cycle decomposition) of $\bar{g}$.

Proof. A function $f \in Y^X$ is a fixed point of g, if and only if $f(g^{-1}x) = f(x)$ for all $x \in X$, i. e. f is constant on each cycle of $\bar{g}$ on X. Since $\bar{g}$ decomposes into $c(\bar{g})$ cycles the proof is finished. □

Two group actions ${}_GX$ and ${}_HY$ are called *isomorphic* if and only if there is a bijection $f\colon X \to Y$ and a group isomorphism $\phi\colon G \to H$ such that $f(gx) = \phi(g)f(x)$ for all $g \in G$ and $x \in X$.

4 The n-scale Z_n

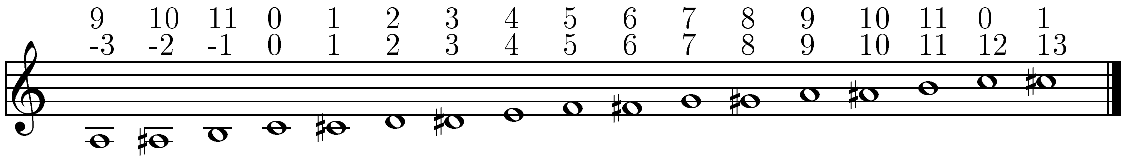
In this section we give a mathematical description of an n-scale (where n is an arbitrary positive integer) which is a generalization of the tempered 12-scale that is commonly used in western music. In our model of an n-scale in each octave there are exactly n tones, which are equally distributed over each octave. We label these tones with the integer numbers in $\mathbb{Z}$. For doing this first choose an arbitrary tone (for instance c^1) and label it with 0. Then stepping up from one tone to the next we increase the labels by one, and stepping down we decrease them. This way we get a bijection between the set of all tones and the set of all integer numbers $\mathbb{Z}$. (It is important to mention that there is no difference between tones like *c-sharp* or *d-flat*. They are considered to be the same tones.) When speaking about tones we use their labels for identifying them.

Often for investigations in music theory it is not important which octave a special tone belongs to, for that reason all tones, which are any number of octaves apart, are collected into one *pitch-class*, ending up in exactly n pitch-classes in an n-scale. This can be done by introducing a group action on $\mathbb{Z}$. It is already known that $(\mathbb{Z},+)$ is a group. The set $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$ is a subgroup of it. As was described in the first item of 3.9 the subgroup $n\mathbb{Z}$ can be used for defining a group action on $\mathbb{Z}$. The orbits correspond to the cosets of the form $i + n\mathbb{Z} = \{i + nz \mid z \in \mathbb{Z}\}$. Consequently all tones with labels in this set are collected to one class, a pitch-class. These are just the tones which differ from the tone i any number of octaves. Since the action above is not a finite group action the Cauchy-Frobenius-Lemma cannot be applied for determining the number of these orbits. But it is not difficult to deduce that the set of orbits (we introduced the notation $\mathbb{Z}/n\mathbb{Z}$) consists of exactly n elements. To be more precise

4.1
$$\mathbb{Z}/n\mathbb{Z} = \{i + n\mathbb{Z} \mid 0 \leq i < n\}$$

and as a standard representative of $z + n\mathbb{Z}$ we choose $i \in z + n\mathbb{Z}$ such that $0 \leq i < n$.

The following figure shows a part of the chromatic scale, together with the labelling of the tones in $\mathbb{Z}$ and with the pitch-class numbers at the top.



On the set $\mathbb{Z}/n\mathbb{Z}$ an inner composition $\oplus$ is defined by setting $i + n\mathbb{Z} \oplus j + n\mathbb{Z} := (i + j) + n\mathbb{Z}$. First we have to prove that $\oplus$ is well defined, i. e. this definition does not depend on the special choice of i and j in $i + n\mathbb{Z}$ or $j + n\mathbb{Z}$. Let $i' \in i + n\mathbb{Z}$ and $j' \in j + n\mathbb{Z}$ then there are $z_1, z_2 \in \mathbb{Z}$ such that $i' = i + nz_1$ and $j' = j + nz_2$. From the following computations we see that $\oplus$ is well defined. $i' + n\mathbb{Z} \oplus j' + n\mathbb{Z} = (i' + j') + n\mathbb{Z} = (i + nz_1 + j + nz_2) + n\mathbb{Z} = (i + j) + n(z_1 + z_2) + n\mathbb{Z} = (i + j) + n\mathbb{Z} = i + n\mathbb{Z} \oplus j + n\mathbb{Z}$. It is possible to prove that $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ is a group. Moreover the mapping

$$\phi\colon \mathbb{Z}/n\mathbb{Z} \to Z_n, \qquad i + n\mathbb{Z} \mapsto \phi(i + n\mathbb{Z}) := i$$

is a bijection and $\phi(i + n\mathbb{Z} \oplus j + n\mathbb{Z}) = \phi(i + n\mathbb{Z}) + \phi(j + n\mathbb{Z})$. In the third item of 3.1 it was shown that $(Z_n, +)$ is a group, therefore ϕ is a group isomorphism, and it is possible to identify these two groups. This way we proved that the n-scale has the structure of Z_n.

There is also another inner composition on $\mathbb{Z}/n\mathbb{Z}$, a multiplication $i + n\mathbb{Z} \odot j + n\mathbb{Z} := ij + n\mathbb{Z}$. Using the same methods as above it is possible to show that this multiplication is well defined, i. e. it does not depend on the special choice i of the representative of $i + n\mathbb{Z}$. The standard representative of $ij + n\mathbb{Z}$ can be computed as $ij \bmod n$. Via the bijection ϕ we can transport this multiplication $\odot$ on $\mathbb{Z}/n\mathbb{Z}$ to a multiplication $\cdot$ in Z_n.

As a matter of fact the structure of Z_n is richer than just the structure of a group. A set $(R, +, \cdot)$ with two inner compositions $+$ and $\cdot$ is called a *ring* if the following axioms are satisfied:

- $(R, +)$ is a commutative group.

- The multiplication $\cdot$ is associative, i. e. $r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$ for all $r_1, r_2, r_3 \in R$.
- The two distributivity laws hold for all $r_1, r_2, r_3 \in R$.

$$(r_1 + r_2) \cdot r_3 = (r_1 \cdot r_3) + (r_2 \cdot r_3) \qquad r_1 \cdot (r_2 + r_3) = (r_1 \cdot r_2) + (r_1 \cdot r_3)$$

Instead of writing $r_1 \cdot r_2$ we usually use $r_1 r_2$. And as we are used from normal computations in $\mathbb{Q}$ we assume that first we have to do all the multiplications, later the summation. Thus $r_1 r_2 + r_1 r_3$ stands for $(r_1 \cdot r_2) + (r_1 \cdot r_3)$.

If there exists an identity element with respect to $\cdot$, this element is usually called 1, we say that the ring R has a *1-element*. If the multiplication is commutative, R is called a *commutative ring*. An element $r \in R \setminus \{0\}$ is called a *zero-divisor* if there exists an $r' \in R \setminus \{0\}$ such that $rr' = r'r = 0$. (It is important to note that 0 is the identity element in the group $(R, +)$.) An element a of a ring R with 1 is called a *unit element* if and only if there is an element $b \in R$ such that $ab = ba = 1$. The set of all units in R is denoted by R^*.

A trivial example of a ring is the 0-ring, it consists only of one element, $R = \{0\}$. It has a 1-element, which is the same as the 0-element, it is commutative and has no zero-divisors. Other well known examples of commutative rings with 1 are $(\mathbb{Z}, +, \cdot)$ or $(\mathbb{Q}, +, \cdot)$.

A subset S of a ring R is called a *sub-ring* if and only if S together with the two compositions defined for R is a ring. For instance $\mathbb{Z}$ is a sub-ring of $\mathbb{Q}$ and the 0-ring is sub-ring of any ring R.

A mapping ϕ from a ring $(R, +, \cdot)$ to a ring $(S, \oplus, \odot)$ is a *ring homomorphism* if and only if $\phi(r_1 + r_2) = \phi(r_1) \oplus \phi(r_2)$ and $\phi(r_1 \cdot r_2) = \phi(r_1) \odot \phi(r_2)$ for all $r_1, r_2 \in R$. If ϕ is bijective it is called a *ring isomorphism*.

4.2 Lemma. *The set Z_n together with the two inner compositions $+$ and $\cdot$ is a commutative ring with 1. It is called the* residue-class-ring *of $\mathbb{Z}$ modulo $n\mathbb{Z}$. The set of units in Z_n can be characterized as*

$$Z_n^* = \{a \in Z_n \mid \gcd(a, n) = 1\}.$$

4.3 Example. The ring Z_{12}. For obvious reason we are mainly interested in the ring Z_{12}. Now we take a closer look to its elements and the two inner compositions on Z_{12}. In finite rings it is possible to write down composition tables for the different inner compositions. In the upper left corner of these tables the inner composition $*$ is indicated. The columns and rows of these tables are labelled by the elements of the ring. The entry in the line labelled by r and in the column labelled by s is given by $r * s$. Here are these tables for addition and multiplication in Z_{12}.

+	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

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

From the second table we deduce that the elements 1, 5, 7 and 11 are the unit elements in Z_{12}, since there is a 1 in the corresponding rows and columns of the multiplication table. Moreover we realize that in each of these rows or columns all elements of Z_{12} occur. The other elements are zero-divisors, since $2 \cdot 6 = 0$, $3 \cdot 4 = 0$, $8 \cdot 9 = 0$ and $10 \cdot 6 = 0$. The columns or rows corresponding to zero-divisors do not contain all elements of Z_{12}. $\diamond$

4.4 Lemma. *The Cartesian product $R \times S$ of two rings R and S is together with the two compositions*

$$(r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_2) \text{ and } (r_1, s_1) \cdot (r_2, s_2) := (r_1 r_2, s_1 s_2)$$

for all $r_1, r_2 \in R$ and $s_1, s_2 \in S$ a ring. It has a 1-element if and only if both R and S have a 1-element and then it is of the form $(1_R, 1_S)$. If $R \times S$ has a 1-element then the set of unit elements is given by

$$(R \times S)^* = R^* \times S^*.$$

This product of two rings can be generalized to a product of finitely many rings.

Let $n > 1$ then in 2.6 it was proved that each $n > 1$ can uniquely be written as a product of primes of the form 2.7.

4.5 Lemma. *The following mapping ϕ defines a ring isomorphism from Z_n to the product of the rings $Z_{p_i^{a_i}}$.*

$$\phi\colon Z_n \to Z_{p_1^{a_1}} \times Z_{p_2^{a_2}} \times \ldots \times Z_{p_r^{a_r}} =: \bigtimes_{i=1}^{r} Z_{p_i^{a_i}}$$

$$j \mapsto \phi(j) := (j \bmod p_1^{a_1}, j \bmod p_2^{a_2}, \ldots, j \bmod p_r^{a_r})$$

Proof. ϕ is a ring homomorphism since $\phi(j_1 + j_2) = \phi(j_1) + \phi(j_2)$ and $\phi(j_1 j_2) = \phi(j_1)\phi(j_2)$ for all $j_1, j_2 \in Z_n$. Here is the proof for the second statement:

$$\phi(j_1 j_2) = (j_1 j_2 \bmod p_1^{a_1}, j_1 j_2 \bmod p_2^{a_2}, \ldots, j_1 j_2 \bmod p_r^{a_r}) =$$

$$= ((j_1 \bmod p_1^{a_1})(j_2 \bmod p_1^{a_1}), (j_1 \bmod p_2^{a_2})(j_2 \bmod p_2^{a_2}), \ldots, (j_1 \bmod p_r^{a_r})(j_2 \bmod p_r^{a_r})) =$$

$$= (j_1 \bmod p_1^{a_1}, j_1 \bmod p_2^{a_2}, \ldots, j_1 \bmod p_r^{a_r})(j_2 \bmod p_1^{a_1}, j_2 \bmod p_2^{a_2}, \ldots, j_2 \bmod p_r^{a_r}) =$$

$$= \phi(j_1)\phi(j_2).$$

In order to prove that ϕ is surjective 2.15 is applied. Since $\gcd(p_i^{a_i}, p_j^{a_j}) = 1$ for $i \neq j$, for each choice $(j_1, \ldots, j_r) \in \bigtimes_{i=1}^{r} Z_{p_i^{a_i}}$ there exists exactly one $j \in Z_n$ such that $j \equiv j_i \bmod p_i^{a_i}$ for $1 \leq i \leq r$, thus $\phi(j) = (j_1, \ldots, j_r)$. Moreover $\bigtimes_{i=1}^{r} Z_{p_i^{a_i}}$ is of cardinality $\prod_{i=1}^{r} p_i^{a_i} = n$, the cardinality of Z_n, consequently ϕ is also injective and the proof is finished. □

From the mathematical point of view the rings Z_p for a prime number p are very interesting. According to 4.2 the set of units in Z_p is $Z_p \setminus \{0\}$. In general rings R with 1 and with the additional property that each element in $R \setminus \{0\}$ is a unit element are called *fields*. Consequently a set F with two inner compositions $+$ and $\cdot$ is a field if and only if the following axioms hold:

- $(F, +)$ is an commutative group.
- $(F \setminus \{0\}, \cdot)$ is a group.
- For $r_1, r_2, r_3 \in F$ the distributivity laws hold:

$$(r_1 + r_2)r_3 = r_1 r_3 + r_2 r_3 \text{ and } r_1(r_2 + r_3) = r_1 r_2 + r_1 r_3.$$

If the multiplication is also commutative, then F is called a *commutative field*.

As we realized above for $n \in \mathbb{N}$ the ring Z_n is a commutative field if and only if n is a prime number. From the prime number decomposition of 12 we get that

$$Z_{12} = Z_3 \times Z_4,$$

where Z_3 is a field, but Z_4 is not a field.

At the end of this section we are coming back to some objects from music theory. To be more precise, it is described how the musical operators *transposing* and *inversion* can be defined on an n-scale. First we realize that transposing by k tones up or down means replacing each tone by the tone which is exactly k tones higher or lower. Since we agreed to speak about tones by using their labels, the operation of transposing by k tones is described by exchanging all labels $z \in \mathbb{Z}$ by $z+k$ or $z-k$ respectively. Furthermore transposing by k tones is the same as transposing k times by one tone. For that reason the operator T *transposing by one tone* is introduced as the following bijection

$$T\colon \mathbb{Z} \to \mathbb{Z}, \qquad z \mapsto T(z) := z+1$$

on $\mathbb{Z}$, the set of all labels of tones. Applying this operator to the elements of a pitch-class $i+n\mathbb{Z}$ we get all the elements in the pitch-class $(i+1)+n\mathbb{Z}$. In other words, $T(i+n\mathbb{Z}) = (i+1)+n\mathbb{Z}$. For that reason it is possible to introduce the operator *transposing by one pitch-class* on the set Z_n, which will also be denoted by T. Then T is the following mapping

$$T\colon Z_n \to Z_n, \qquad i \mapsto T(i) := i+1.$$

It should be mentioned that $i+1$ in Z_n means $i+1 \bmod n$. This mapping is a bijection on Z_n, in other words it is a permutation of Z_n and its standard cycle decomposition is of the form $(0,1,\ldots,n-1)$. Hence T is a cycle of length n.

The musical operator inversion means that tone-steps (in a motive, in a melody or in a tone-row) or just intervals of given size up or down, are exchanged by steps or intervals of the same size but exchanged direction, i. e. down or up. There are two cases to be distinguished: Either there exists a reference tone which is not changed, tones higher than this tone are exchanged into tones lower than this tone and vice versa. Or there are two adjacent tones which are exchanged, and simultaneously tones higher than these two tones are exchanged into tones lower than these two tones and vice versa. Let z_0 be the label of the reference tone, which is not changed, or let z_0 and z_0+1 be the labels of the two adjacent tones which are exchanged. In the first case let $r := z_0$ in the second case let $r := z_0 + \frac{1}{2}$. Then the operator *inversion with respect to* r is defined as the following bijection

$$I_r\colon \mathbb{Z} \to \mathbb{Z}, \qquad z \mapsto I_r(z) := r-(z-r) = 2r-z$$

on $\mathbb{Z}$, the set of all labels of tones. If $r = z_0$ then $I_r(z_0) = 2z_0 - z_0 = z_0$ and $I_r(z_0+k) = 2z_0-(z_0+k) = z_0-k$. If $r = z_0+\frac{1}{2}$ then $I_r(z_0) = 2z_0+1-z_0 = z_0+1$, $I_r(z_0+1) = z_0$ and $I_r(z_0+k) = 2z_0+1-(z_0+k) = z_0-(k-1)$. Applying I_r to all elements of the pitch-class $(2r-i)+n\mathbb{Z}$ we get all the elements in the pitch-class $i+n\mathbb{Z}$. In other words, $I_r((2r-i)+n\mathbb{Z}) = i+n\mathbb{Z}$. Especially for $r = z_0 = 0$ the operator I, *inversion at pitch-class 0,* is defined by

$$I\colon Z_n \to Z_n, \qquad i \mapsto I(i) := -i.$$

It should be mentioned that $-i$ in Z_n means $-i \bmod n$. This mapping is a bijection on Z_n, hence it is a permutation of Z_n and its standard cycle decomposition is of the form $(0)(1, n-1)(2, n-2)\ldots$. Depending on n the permutation I decomposes into 2 fixed points and $\frac{n-2}{2}$ transpositions if n is even, or 1 fixed point and $\frac{n-1}{2}$ transpositions if n is odd.

With these two operators we define two symmetry groups on the n-scale Z_n. First consider the permutation group $\langle T \rangle$. According to 3.4 it consists of all powers T^i for $1 \leq i \leq n$, and the operator T^n is the identity element. Since T stands for transposing by one pitch-class, T^i stands for transposing by i pitch-classes. Thus the group $\langle T \rangle$ describes all the possibilities to transpose in an n-scale. Since the mapping $f: Z_n \to \underline{n}$ given by $f(i) := i + 1$ is a bijection, it defines by 3.5 an isomorphism ϕ from S_{Z_n} to $S_{\underline{n}}$, and $\phi(T) = \pi$ from the second item in 3.4. Consequently the image $\phi(\langle T \rangle)$ is isomorphic to the permutation group C_n. Moreover the action of $\langle T \rangle$ on Z_n is isomorphic to the action of C_n on $\underline{n}$.

The group $\langle T, I \rangle$ consists of all possibilities to combine powers of T with the inversion operator I. Applying the isomorphism ϕ from above we realize that $\phi(I) = \sigma$ from the third item of 3.4. This means that $\langle T, I \rangle$ is isomorphic to the permutation group D_n and the action of $\langle T, I \rangle$ on Z_n is isomorphic to the action of D_n on $\underline{n}$. From 3.4 we derive that $I \circ T = T^{-1} \circ I$ and that all elements of $\langle T, I \rangle$ can be written as $T^k \circ I^j$ such that $k \in \{0, 1, \ldots, n-1\}$ and $j \in \{0, 1\}$.

Sometimes a symmetry of another type is applied in Z_{12}, it is the so called *quart-circle symmetry* Q, which is defined by

$$Q: Z_{12} \to Z_{12}, \qquad i \mapsto Q(i) := 5i.$$

It should be mentioned that $5i$ in Z_{12} means $5i \bmod 12$. In 4.3 it was shown that this mapping is a bijection on Z_{12} since 5 is a unit element in Z_{12}, hence Q is a permutation of Z_{12}. Its standard cycle decomposition is of the form $(0)(1,5)(2,10)(3)(4,8)(6)(7,11)(9)$. Applying Q to the chromatic scale yields a sequence of quarts 0, 5, 10, 3, ... Together with Q usually the other operators T and I are taken into consideration as well, such that we end up with the permutation group $\langle T, I, Q \rangle$ acting on Z_{12}. The product $I \circ Q$ equals $Q \circ I$ which is called the *quint-circle symmetry*. Since $Q \circ T = T^5 \circ Q$ all the elements of this group can be expressed as $T^k \circ I^j \circ Q^l$ such that $k \in \{0, 1, \ldots, 11\}$ and $j, l \in \{0, 1\}$. Therefore the group $\langle T, I, Q \rangle$ consists of 48 permutations.

From 4.3 we know that Z_{12}^*, the set of units in Z_{12}, is given by $\{1, 5, 7, 11\}$. The multiplication $i \mapsto 1i$ is the identity operator, $i \mapsto 5i$ the quart-circle symmetry Q, $i \mapsto 7i$ the quint-circle symmetry $I \circ Q$ and $i \mapsto 11i$ the inversion I. Thus there is a second possibility to describe the action of this permutation group on Z_{12}. Each permutation in $\langle T, I, Q \rangle$ can be expressed as a mapping $i \mapsto ai + b$ such that $a \in Z_{12}^*$ and $b \in Z_{12}$ and each such mapping is an element of $\langle T, I, Q \rangle$.

This approach can be generalized in order to define a symmetry group on the n-scale Z_n for arbitrary n. For $a \in Z_n^*$ and $b \in Z_n$ the mapping

4.6 $$\pi_{a,b}: Z_n \to Z_n, \qquad i \mapsto \pi_{a,b}(i) := ai + b$$

is a bijection on Z_n. The set $\mathrm{Aff}_1(Z_n) := \{\pi_{a,b} \mid a \in Z_n^*,\ b \in Z_n\}$ is a permutation group on Z_n. It is called the group of all *affine mappings* from Z_n to Z_n. The set $\mathrm{Aff}_1(Z_n)$ is not empty since $\pi_{1,0}$, the identity on Z_n, is in $\mathrm{Aff}_1(Z_n)$. Let $\pi_{a,b} \in \mathrm{Aff}_1(Z_n)$, then the inverse (in the symmetric group S_{Z_n}) of $\pi_{a,b}$ is again in $\mathrm{Aff}_1(Z_n)$ since it can be expressed as $\pi_{a^{-1},-a^{-1}b}$. Finally for $c \in Z_n^*$, $d \in Z_n$ the product $\pi_{c,d} \circ \pi_{a,b}$ is again in $\mathrm{Aff}_1(Z_n)$, since $(\pi_{c,d} \circ \pi_{a,b})(i) = \pi_{c,d}(\pi_{a,b}(i)) = \pi_{c,d}(ai+b) = c(ai+b)+d = (ca)i+(cb+d) = \pi_{ca,cb+d}(i)$ and $ca \in Z_n^*$ and $cb+d \in Z_n$. From 3.2 we deduce that $\mathrm{Aff}_1(Z_n)$ is a permutation group and it acts on Z_n as was defined in 4.6. For $n = 12$ the group $\mathrm{Aff}_1(Z_{12})$ coincides with $\langle T, I, Q\rangle$.

5 Pólya's Theorem and cycle indices

In this section we come back to enumeration under group actions. In order to get some more information about the G-orbits on X we introduce *weight functions* on X. Then the number of G-orbits of given weight is determined. This approach will be applied for the enumeration of orbits of k-chords in an n-scale and later for the enumeration of k-motives.

A weight function is a function $w\colon X \to R$ where R is a commutative ring, such that $\mathbb{Q}$ is a sub-ring of R. The function w must be constant on each G-orbit on X, i. e. $w(x) = w(gx)$ for all $g \in G$ and $x \in X$. Then it makes sense to define the weight of an orbit $G(x)$ as the weight of an arbitrary element, say x, of $G(x)$.

5.1
$$w(G(x)) := w(x)$$

When summing up weights of G-orbits instead of counting them we derive the *weighted version* of the *Cauchy-Frobenius-Lemma*.

5.2 Theorem. *The sum of weights of G-orbits defined by the weight function 5.1 under a finite group action ${}_GX$ is given by*

$$\sum_{\omega \in G\backslash\backslash X} w(\omega) = \frac{1}{|G|} \sum_{g \in G} \sum_{x \in X_g} w(x).$$

Proof. An application of 3.12 yields

$$\sum_{g \in G} \sum_{x \in X_g} w(x) = \sum_{x \in X} \sum_{g \in G_x} w(x) = \sum_{x \in X} |G_x|\, w(x) = \sum_{x \in X} \frac{|G|}{|G(x)|} w(x) =$$

$$= |G| \sum_{\omega \in G\backslash\backslash X} \sum_{x \in \omega} \frac{w(x)}{|G(x)|} = |G| \sum_{\omega \in G\backslash\backslash X} \sum_{x \in \omega} \frac{w(\omega)}{|\omega|} = |G| \sum_{\omega \in G\backslash\backslash X} w(\omega).$$

In order to understand the last line it is important to remember that when $x \in \omega \in G\backslash\backslash X$ then ω is the orbit $G(x)$ and $w(x) = w(\omega)$. □

The original version 3.13 of this theorem can be obtained by setting $w(x) = 1$ for all $x \in X$.

A group action ${}_GX$ induces an action of G an the set Y^X as was described in 3.10. Let R be a commutative ring such that $\mathbb{Q}$ is a sub-ring of R and let $W : Y \to R$ be an arbitrary function. Then the function $w\colon Y^X \to R$ defined by

5.3 $$w(f) := \prod_{x\in X} W(f(x))$$

is a weight function. It is constant on each G-orbit on Y^X, since multiplication in R is commutative, and applying any group element g to a function f just leads to a reordering of the terms in the product caused by the permutation $\bar{g}$ on X, since for any $g \in G$ we have

$$w(gf) = \prod_{x\in X} W(f(\bar{g}^{-1}x)) = \prod_{x\in X} W(f(x)) = w(f).$$

For this situation 5.2 is rewritten in order to derive the famous theorem by G. Pólya [24, 23].

5.4. Pólya's Theorem. *The sum of weights of G-orbits on Y^X induced by a finite group action ${}_GX$ is given by*

$$\sum_{\omega\in G\backslash\backslash Y^X} w(\omega) = \frac{1}{|G|}\sum_{g\in G}\prod_{i=1}^{|X|}\left(\sum_{y\in Y} W(y)^i\right)^{\lambda_i(\bar{g})},$$

where $(\lambda_1(\bar{g}), \ldots, \lambda_{|X|}(\bar{g}))$ is the cycle type of the permutation $\bar{g}$.

Proof. According to 5.2 for each $g \in G$ we have to compute $\sum_{f\in Y_g^X} w(f)$. We already know that a function f is a fixed point of g if and only if f is constant on the cycles of $\bar{g}$. As a consequence we get

$$\sum_{f\in Y_g^X} w(f) = \sum_{f\in Y^{\langle g\rangle\backslash\backslash X}} \prod_{\omega\in\langle g\rangle\backslash\backslash X} W(f(\omega))^{|\omega|} =$$

$$= \prod_{\omega\in\langle g\rangle\backslash\backslash X}\sum_{y\in Y} W(y)^{|\omega|} = \prod_{i=1}^{|X|}\left(\sum_{y\in Y} W(y)^i\right)^{\lambda_i(\bar{g})}$$

and the proof is finished. □

Setting $W(y) = 1$ for all $y \in Y$ Pólya's Theorem reduces to 3.14.

The result above motivates the following definition of the *cycle index* of an action ${}_GX$. It is a polynomial over $\mathbb{Q}$ in indeterminates $z_1, z_2, \ldots, z_{|X|}$ which collects for all $g \in G$ the information about the cycle types of the induced permutations $\bar{g}$ on X in a useful way. It is given by

$$C(G, X) := \frac{1}{|G|}\sum_{g\in G}\prod_{i=1}^{|X|} z_i^{\lambda_i(\bar{g})}.$$

Comparing this definition with the formula in 5.4 we realize that the sum of weights of G-orbits on Y^X can be computed from $C(G,X)$ by replacing each variable z_i by $\sum_{y\in Y} W(y)^i$. This substitution is indicated as follows:

$$C(G,X;z_i := \sum_{y\in Y} W(y)^i).$$

Using this notation we can reformulate Pólya's Theorem again. For a given a finite group action ${}_GX$, a finite set Y, a function $W\colon Y \to R$, where R is a commutative ring, such that $\mathbb{Q}$ is a sub-ring of R, and for a weight function $w\colon Y^X \to R$ defined by 5.3, the sum of weights of G-orbits for the action defined by 3.10 on Y^X is

$$\sum_{\omega\in G\backslash\backslash Y^X} w(\omega) = C(G,X;z_i := \sum_{y\in Y} W(y)^i).$$

In order to apply Pólya's Theorem the cycle indices of the acting groups must be determined. Actually there is no general routine for computing cycle indices, it depends on the group and the action of the group which method to use. For groups of small order it is possible to compute the cycle type of all the induced permutations. Often it is not necessary to compute the cycle type of $\bar{g}$ for each element $g \in G$. In the second item of 3.9 the action of G on G in form of the conjugation was introduced. The orbits under this action are the conjugacy classes in G. In 5.6 we are going to prove that conjugate permutations $\bar{g} \in \bar{G}$ are of the same cycle type, therefore it is possible to compute the cycle index in the form

$$C(G,X) = \frac{1}{|G|}\sum_{C\in\mathcal{C}} |C| \prod_{i=1}^{|X|} z_i^{\lambda_i(\bar{g}_C)},$$

where $\mathcal{C}$ is the set of all conjugacy classes of elements of G and g_C is an arbitrary element of the conjugacy class $C \in \mathcal{C}$.

The next lemma describes a connection between the conjugacy classes of $S_{\underline{n}}$ and the cycle types of the permutations in $S_{\underline{n}}$.

5.5 Lemma. *Two permutations $\pi,\sigma \in S_{\underline{n}}$ are conjugate if and only if they have the same cycle type, i. e. $\lambda_i(\pi) = \lambda_i(\sigma)$ for all $1 \le i \le n$.*

Proof. Let $\rho \in S_{\underline{n}}$ then it is easy to show that

$$\rho \circ (i_1,\ldots,i_r) \circ \rho^{-1} = (\rho(i_1),\ldots,\rho(i_r))$$

for any cycle $(i_1,\ldots,i_r)$ of length $r \le n$ in $S_{\underline{n}}$. Using this result one can prove that

$$\rho \circ \left(\mathop{\circ}_{\nu=1}^{c(\pi)} (i_\nu,\pi(i_\nu),\ldots,\pi^{l_\nu-1}(i_\nu))\right) \circ \rho^{-1} = \mathop{\circ}_{\nu=1}^{c(\pi)} (\rho(i_\nu),\rho(\pi(i_\nu)),\ldots,\rho(\pi^{l_\nu-1}(i_\nu))).$$

In other words π and $\rho\circ\pi\circ\rho^{-1}$ are of the same cycle type.

Conversely, if π and σ are of the same cycle type then there is a bijection B between the sets of cycles in the decompositions of π and σ which maps a cycle in the decomposition of π to a cycle of the same length in the decomposition of σ. This bijection can be used for defining a permutation $\rho \in S_{\underline{n}}$ such that $\rho \circ \pi \circ \rho^{-1} = \sigma$ in the following way. Let $(i_1, \ldots, i_r)$ be a cycle of π and let $B(i_1, \ldots, i_r) = (j_1, \ldots, j_r)$ then ρ can be defined on this cycle by $\rho(i_k) := j_k$ for $1 \leq k \leq r$. Now it is easy to check that ρ has the desired property and the proof is finished. □

5.6 Corollary. *Let ${}_GX$ be a group action. If g and h are conjugate elements of G then $\bar{g}$ and $\bar{h}$ are of the same cycle type.*

In the next lemma we compute the cycle indices of the permutation groups C_n and D_n.

5.7 Lemma. *The cycle indices of the permutation groups C_n and D_n (cf. the second and third item of 3.4) are given by*

$$C(C_n, \underline{n}) = \frac{1}{n} \sum_{d|n} \varphi(n/d) z_{n/d}^d$$

and

$$C(D_n, \underline{n}) = \frac{1}{2} C(C_n, \underline{n}) + \begin{cases} \frac{1}{2} z_1 z_2^{(n-1)/2} & \text{if } n \text{ is odd,} \\ \frac{1}{4}(z_1^2 z_2^{(n-2)/2} + z_2^{n/2}) & \text{if } n \text{ is even,} \end{cases}$$

where φ is the Euler function.

Proof. Let $\pi = (1, 2, \ldots, n)$ be the generator of C_n. For each $j \in \{0, 1, \ldots, n-1\}$ the cycle type of π^j must be computed. The element $i \in \underline{n}$ belongs to a cycle of length k of the permutation π^j if and only if $(\pi^j)^k(i) = i$ and $(\pi^j)^l(i) \neq i$ for all $1 \leq l < k$. Consequently for determining the cycle length of i we have to find the smallest positive solution of the linear congruence $i + jx \equiv i \bmod n$ which is the same as $jx \equiv 0 \bmod n$. According to 2.11 this congruence has always a solution and the smallest positive solution is given by $\frac{n}{\gcd(n,j)}$. Since the second congruence does not depend on the special choice of i all elements of $\underline{n}$ belong to cycles of this length. Thus π^j decomposes into $\gcd(n, j)$ cycles of length $\frac{n}{\gcd(n,j)}$. Furthermore $\gcd(n, j)$ is a divisor of n. According to 2.9, for any divisor d of n the number of $j \in \{0, 1, \ldots, n-1\}$ such that $\gcd(n, j) = d$ is equal to $\varphi(n/d)$, which proves the formula for the cycle index of C_n.

The cycle types of reflections in D_n can be computed in the following way. Let $\sigma = (1, n) \circ (2, n-1) \circ \ldots$, i. e. $\sigma(i) = n + 1 - i$. Since $\pi \circ \sigma = \sigma \circ \pi^{-1}$ each reflections $\pi^k \circ \sigma \in D_n$ is a permutation of order 2, i. e. $(\pi^k \circ \sigma) \circ (\pi^k \circ \sigma) = \mathrm{id}$. Consequently the length of each cycle in its cycle decomposition is a divisor of 2. And there is at least one cycle of length 2 in this decomposition. For finding the fixed points of $\pi^k \circ \sigma$ the congruence $2x \equiv k + 1 \bmod n$ must be solved, since $(\pi^k \circ \sigma)(i) = i$ if and only if $n + 1 - i + k \equiv i \bmod n$. According to 2.11 this congruence has a solution if and only if $\gcd(2,n)$ is a divisor of $k+1$. And if it has a solution then there exist $\gcd(2,n)$ incongruent solution modulo n. If n is odd then $\gcd(2,n)=1$ and $\pi^k \circ \sigma$ has exactly one fixed point. If n is even then $\gcd(2,n)=2$. In the case $k+1$ is even there are two fixed points and in the other case no fixed points of $\pi^k \circ \sigma$. Since all the other elements belong to cycles of length two the proof is finished. □

Let ${}_GX$ and ${}_HY$ be two group actions then a natural action of the direct product $G \times H$ on $X \times Y$ can be described by

$$(G \times H) \times (X \times Y) \to X \times Y \qquad ((g,h),(x,y)) \mapsto (gx, hy).$$

If x belongs to a cycle of $\bar{g}$ of length k the elements of which are the element of $X' := \{x, x_2, \ldots, x_k\}$ and y belongs to a cycle of $\bar{h}$ of length l the elements of which are the elements of $Y' := \{y, y_2, \ldots, y_l\}$ then we determine the length of the cycle of (g,h) containing (x,y) and furthermore we determine all (g,h)-cycles on $X' \times Y'$.

All the elements of the cycle of (g,h) containing (x,y) belong to $X' \times Y'$. The length of this cycle is the smallest positive integer which is a multiple of k and l, hence it is equal to $\mathrm{lcm}(k,l)$. This length does not depend on the special choice of $(x,y) \in X' \times Y'$. Since each element of X' belongs to a cycle of length k and each element of Y' to a cycle of length l each pair $(x,y) \in X' \times Y'$ belongs to a cycle of length $\mathrm{lcm}(k,l)$. Since there are kl elements in the set $X' \times Y'$ it decomposes into $\frac{kl}{\mathrm{lcm}(k,l)} = \gcd(k,l)$ cycles of length $\mathrm{lcm}(k,l)$.

This motivates the following definition of a product operator, which can be found in [14]. Let A and B be polynomials in indeterminates $z_1, z_2, \ldots$ over $\mathbb{Q}$ given by

$$A(z_1, z_2, \ldots, z_n) = \sum_{(j)} a_{(j)} \prod_{i=1}^{n} z_i^{j_i},$$

$$B(z_1, z_2, \ldots, z_m) = \sum_{(k)} b_{(k)} \prod_{i=1}^{m} z_i^{k_i},$$

where the first sum is taken over finitely many n-tuples $(j) = (j_1, \ldots, j_n) \in \mathbb{N}_0^n$ and the second sum over finitely many m-tuples $(k) = (k_1, \ldots, k_m) \in \mathbb{N}_0^m$. Then

$$A(z_1, \ldots, z_n) \times B(z_1, \ldots, z_m) := \sum_{(j)} \sum_{(k)} a_{(j)} b_{(k)} \left(\prod_{i=1}^{n} z_i^{j_i} \right) \times \left(\prod_{i=1}^{m} z_i^{k_i} \right),$$

where

$$\left(\prod_{i=1}^{n} z_i^{j_i} \right) \times \left(\prod_{i=1}^{m} z_i^{k_i} \right) := \prod_{i=1}^{n} \prod_{l=1}^{m} (z_i^{j_i} \times z_l^{k_l})$$

and

$$z_i^{j_i} \times z_l^{k_l} := z_{\mathrm{lcm}(i,l)}^{j_i k_l \gcd(i,l)}.$$

5.8 Lemma. *The cycle index of the natural action of $G \times H$ on $X \times Y$ induced by two finite actions ${}_GX$ and ${}_HY$ can be expressed as*

$$C(G \times H, X \times Y) = C(G, X) \times C(H, Y).$$

Applying the ring isomorphism ϕ between Z_n and $\times_{i=1}^{r} Z_{p_i^{a_i}}$ from 4.5 to the action of $\mathrm{Aff}_1(Z_n)$ on Z_n we realize that $\phi(\mathrm{Aff}_1(Z_n)) = \times_{i=1}^{r} \mathrm{Aff}_1(Z_{p_i^{a_i}})$ acts on $\times_{i=1}^{r} Z_{p_i^{a_i}}$ where $\mathrm{Aff}_1(Z_{p_i^{a_i}})$ acts in a natural way on $Z_{p_i^{a_i}}$ for $i = 1, 2, \ldots, r$. A consequence of 5.8 is

$$C(\mathrm{Aff}_1(Z_n), Z_n) = \bigtimes_{i=1}^{r} C(\mathrm{Aff}_1(Z_{p_i^{a_i}}), Z_{p_i^{a_i}}).$$

In [34] the following formulae are given for these cycle indices.

5.9 Lemma. *Let p be a prime and $a \in \mathbb{N}$. Then the cycle index of the natural action of $\mathrm{Aff}_1(Z_{p^a})$ on Z_{p^a} is of the following form: If $p = 2$ then*

$$C(\mathrm{Aff}_1(Z_2), Z_2) = \frac{1}{2}(z_1^2 + z_2)$$

$$C(\mathrm{Aff}_1(Z_4), Z_4) = \frac{1}{8}(z_1^4 + 2z_1^2 z_2 + 3z_2^2 + 2z_4).$$

and for $a \geq 3$

$$C(\mathrm{Aff}_1(Z_{2^a}), Z_{2^a}) = \frac{1}{2^{2a-1}} \Bigg(2^{2(a-1)-1} z_{2^a} + \sum_{i=1}^{a-1} \left(2^{2(i-1)} + \varphi(2^{i-1}) 2^{a-1}\right) z_{2^i}^{2^{a-i}} +$$

$$+ \sum_{i=0}^{a-2} \varphi(2^i) \left(2^i z_1^{2^{a-i}} + 2^{a-1} z_1^2 z_2^{2^{a-i-1}-1}\right) \left(\prod_{j=1}^{i} z_{2^j}\right)^{2^{a-i-1}} \Bigg).$$

If p is a prime number different from 2 then for $a \geq 1$

$$C(\mathrm{Aff}_1(Z_{p^a}), Z_{p^a}) = \frac{1}{p^{2a-1}(p-1)} \Bigg(\sum_{i=1}^{a} p^{2(i-1)}(p-1) z_{p^i}^{p^{a-i}} +$$

$$+ \sum_{i=0}^{a-1} \sum_{d|p-1} p^{i+\delta(d)(a-i)} \varphi(p^i d) z_1 z_d^{(p^{a-i-1}-1)/d} \left(\prod_{j=0}^{i} z_{p^j d}\right)^{p^{a-i-1}(p-1)/d} \Bigg),$$

where

$$\delta(d) = \begin{cases} 1 & \textit{if } d > 1 \\ 0 & \textit{if } d = 1. \end{cases}$$

Now we apply Pólya's Theorem for the enumeration of G-orbits of subsets of X.

5.10 Example. Let ${}_GX$ be a finite group action, then G acts in a natural way on $\mathcal{P}(X) := \{S \mid S \subseteq X\}$, which is the set of all subsets of X. For $g \in G$ and $S \in \mathcal{P}(X)$ the subset gS of X is defined as $gS := \{gx \mid x \in S\}$. It is possible to identify each $S \subseteq X$ with its *characteristic function* χ_S. This is a function from X to $\{0,1\}$ defined by

$$\chi_S(x) := \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{if } x \notin S. \end{cases}$$

Moreover each function $f: X \to \{0,1\}$ can be interpreted as the characteristic function of the subset $S = f^{-1}(\{1\})$ of X. If the weight function W on $Y = \{0,1\}$ is defined by $W(0) = 1$ and $W(1) = z$, where z is an indeterminate over $\mathbb{Q}$, then a function $f: X \to \{0,1\}$ is the characteristic function of a k-subset of X if and only if the weight $w(f)$ defined by 5.3 is equal to z^k. These functions are called functions of weight k.

The group action of G on $\mathcal{P}(X)$ can be translated into a group action of G on $\{0,1\}^X$ in the form of 3.10 since $\chi_{gS}(x) = 1$ if and only if $x \in gS$ or equivalently $g^{-1}x \in S$ which means that $\chi_S(g^{-1}x) = 1$. As was described in 3.10 $\chi_S(g^{-1}x) = g\chi_S(x)$ for all $x \in X$, which proves that these two actions are isomorphic. From Pólya's Theorem we deduce that the number of G-orbits of k-subsets of X is the coefficient of z^k in

$$C(G, X; z_i := 1 + z^i).$$

$\diamond$

Now this method will be applied in order to compute the number of different k-chords in the n-scale Z_n.

5.11 Example. Any k-subset of Z_n is called a *k-chord* in Z_n. Especially 2-chords are called *intervals*. As was shown in section 4 the action of the permutation groups $\langle T \rangle$, $\langle T, I \rangle$ or $\mathrm{Aff}_1(Z_n)$ can be motivated from music theory. Therefore it makes sense to apply the elements of these groups to k-chords. Let G be one of these groups, then the G-orbit $G(S)$ of a k-chord $S \subseteq Z_n$ is the collection of all k-chords which are G-equivalent to S. Consequently the number of different k-chords is the number of G-orbits on the set of all k-subsets of Z_n which is the coefficient of z^k in

$$C(G, Z_n; z_i := 1 + z^i).$$

As a matter of fact for different choices of G we get different classes of G-equivalent chords, consequently different numbers of G-orbits. The numbers of different G-orbits of k-chords in Z_{12} for $k = 1, 2, \ldots, 12$ and G being one of the groups C_{12}, D_{12} or $\mathrm{Aff}_1(Z_{12})$ can be found in [27, 8, 26]. $\diamond$

Finally we enumerate the $H \times G$-orbits for the action on Y^X introduced in the last item of 3.9. Let ${}_GX$ and ${}_HY$ be two finite group actions. For a function $f \in Y^X$ and for $(h, g) \in H \times G$ the following statements are equivalent.

1. f is a fixed point of (h, g).

2. $\bar{h} \circ f \circ \bar{g}^{-1} = f$.
3. $\bar{h} \circ f = f \circ \bar{g}$.
4. f maps each cycle of $\bar{g}$ of length k onto a cycle of $\bar{h}$ of length l such that l is a divisor of k.

Moreover each function f which is a fixed point of (h, g) is completely determined on the elements of the cycle $\langle g\rangle(x)$ by choosing $f(x)$ in a cycle of $\bar{h}$ of the right length, since

$$f(\bar{g}(x)) = \bar{h}(f(x)),\ f(\bar{g}^2(x)) = \bar{h}^2(f(x)),\ \ldots,\ f(\bar{g}^i(x)) = \bar{h}^i(f(x)),\ \ldots$$

If x belongs to a cycle of length k then $f(x) = f(\bar{g}^k(x)) = \bar{h}^k(f(x))$, which shows that $f(x)$ must belong to a cycle of length l dividing k.

From these characterizations it is clear that the number of all fixed points of (h, g) in Y^X is

$$\left|Y^X_{(h,g)}\right| = \prod_{i=1}^{|X|} |Y_{h^i}|^{\lambda_i(\bar{g})},$$

where $(\lambda_1(\bar{g}), \ldots, \lambda_{|X|}(\bar{g}))$ is the cycle type of $\bar{g}$. The number of fixed points of h^i in Y is just the number of elements in Y which belong to cycles of length j dividing i, thus

$$|Y_{h^i}| = \sum_{j|i} j \cdot \lambda_j(\bar{h}).$$

This is the sum of $j \cdot \lambda_j(\bar{h})$ over all positive divisors j of i. Combining these results with 3.13 we get

5.12 Lemma. *The number of $H \times G$-orbits on Y^X is given by*

$$\left|H \times G \backslash\backslash Y^X\right| = \frac{1}{|H \times G|} \sum_{(h,g)\in H\times G} \prod_{i=1}^{|X|} |Y_{h^i}|^{\lambda_i(\bar{g})} = \frac{1}{|H|} \sum_{h\in H} C(G, X; z_i := \sum_{j|i} j \cdot \lambda_j(\bar{h})).$$

The action of $H \times G$ induces the following action of H on $G\backslash\backslash Y^X$, the set of all G-orbits on Y^X.

$$H \times (G\backslash\backslash Y^X) \to G\backslash\backslash Y^X, \qquad (h, G(f)) \mapsto G(\bar{h} \circ f).$$

This definition does not depend on the special choice of a representative of the orbit $G(f)$. For $h \in H$ the G-orbit $G(f)$ is called *h-invariant* if and only if $G(f) = G(\bar{h} \circ f)$, in other words, $G(f)$ is h-invariant if $G(f)$ is a fixed point of h under the action above. If $G(f)$ is h-invariant then for each $f' \in G(f)$ there exists a $g \in G$ such that $\bar{h} \circ f' = f' \circ \bar{g}$. Conversely, if there exists some $g \in G$ such that $\bar{h} \circ f = f \circ \bar{g}$ for a function $f \in Y^X$ then the orbit $G(f)$ is h-invariant. Thus the number of h-invariant orbits is the number of G-orbits on the set

$$\left\{f \in Y^X \mid \text{exists } g \in G \text{ such that } \bar{h} \circ f = f \circ \bar{g}\right\}$$

which can be computed by using 3.13 as

$$\frac{1}{|G|}\sum_{g\in G}\prod_{i=1}^{|X|}|Y_{h^i}|^{\lambda_i(\bar{g})} = C(G,X; z_i := \sum_{j|i} j\cdot\lambda_j(\bar{h})).$$

(Compare this result with [5].)

5.13 Example. The *complement* of a k-chord S in Z_n is the the $n-k$-chord $Z_n \setminus S$. If S is given by its characteristic function χ_S then the characteristic function of the complement of S is $1-\chi_S$ which means that each 1 in the characteristic function of S must be replaced by 0 and each 0 must be replaced by 1. This operation can also be described by multiplying χ_S from the left with the transposition $(0,1) \in S_{\{0,1\}}$. This permutation is of cycle type $(0,1)$.

If n is an even positive integer, then the $n/2$-chord S is called *self-complementary* if and only if it is G-equivalent to its complement $Z_n\setminus S$, where G is a (musically motivated) group acting on Z_n. In mathematical terms the orbits of self-complementary $n/2$-chords are just the $(0,1)$-invariant orbits of $n/2$-chords. Their number is equal to

$$C(G, Z_n; z_{2k} := 2,\ z_{2k+1} := 0)$$

which means that the indeterminates z_i in $C(G, Z_n)$ must be replaced by 0 if i is odd, and by 2 if i is even. Especially, for G being one of the groups C_{12}, D_{12} or $\mathrm{Aff}_1(Z_{12})$ the numbers of self-complementary 6-chords in Z_{12} were computed in [8]. ◇

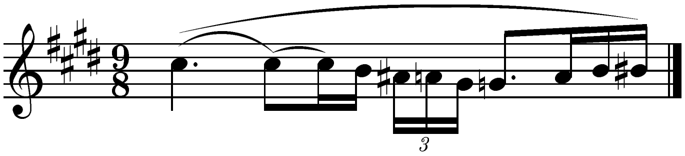
6 Motives

Now we come to the main topic of this article. G. Mazzola introduced in [20] the notion of *motives* in order to describe both tonal and rhythmical aspects of music. The easiest form of describing a rhythm is to find a very dense subdivision of the rhythm into equidistant beats such that all rhythmical events coincide with some of these beats. Collecting $m \in \mathbb{N}$ beats into a bar we are speaking of an *m-bar*. In order to make investigations easier we restrict our attention just to one bar. And if for some reason a given rhythm exceeds one bar then we assume that it continues from the beginning of this bar again. In other words, an m-bar has a cyclic structure, hence the set Z_m can be used as a model of an m-bar. The same way as we introduced symmetry operations for pitch-classes they can be introduced on an m-bar. For instance the standard operators are the *cyclic shift by one beat* S and the *retrograde inversion* R, which reverses a given rhythm. They can be defined as the following permutations on Z_m.

$$S\colon Z_m \to Z_m,\quad i \mapsto S(i) := i+1 \qquad R\colon Z_m \to Z_m,\quad i \mapsto R(i) := -i$$

The permutation groups $\langle S\rangle$ and $\langle S, R\rangle$ and their actions on Z_m are isomorphic to C_m and D_m and to their actions on $\underline{m}$ (cf. the second and third item of 3.4).

For instance the rhythm of C. Debussy's *"Prélude a l'Après-Midi d'un Faune"* could be coded in a 54-bar



as $\{0, 27, 30, 32, 34, 36, 45, 48, 51\}$.

Bach's example from the beginning of this article could be coded in a 6-bar as $\{0, 1, 2, 3, 4\}$, whereas the motive by Mendelssohn has the rhythm $\{0, 2, 3, 4, 5, 6, 8, 10\}$ in a 12-bar. Finally the rhythm in Honegger's motive is the subset $\{0, 3, 4, 6, 10, 12, 14, 16\}$ of Z_{18}.

A *k-rhythm* in an m-bar (for $1 \leq k \leq m$) is defined as a k-subset of Z_m. The actions of the groups $G = \langle S \rangle$ or $G = \langle S, R \rangle$ are motivated by music theory. Applying the same methods as in 5.11 it is possible to determine the number of non-G-equivalent k-rhythms.

When speaking about motives we first have to find all possible combinations of beats in an m-bar Z_m and pitch-classes in an n-scale Z_n. The set of all these combinations is the product $Z_m \times Z_n$. Then for $1 \leq k \leq nm$ each k-subset S of this set is a *k-motive* in $Z_m \times Z_n$. When $(i, j) \in Z_m \times Z_n$ belongs to the motive S it means that a tone of pitch-class j occurs at the beat i in the motive S. So the first parameter describes the rhythmical aspects the second the tonal aspects. Usually when drawing pairs (i, j) on a sheet of paper the first component describes the position on a horizontal axis the second component the position on a vertical axis. This point of view coincides with the musical notation where rhythmical aspects are described horizontally and tonal aspects vertically.

In order to describe suitable symmetry operators on $Z_m \times Z_n$ we first have to investigate the structure of all group endomorphisms of $(Z_m \times Z_n, +)$.

Let A be a function from $Z_m \times Z_n$ to $Z_m \times Z_n$ then for $x \in Z_m \times Z_n$ we can write $A(x)$ in the form $(A_1(x), A_2(x))$ where $A_1(x) \in Z_m$ and $A_2(x) \in Z_n$. Now let A be a group homomorphism then $A((i, j) + (k, l)) = A(i, j) + A(k, l)$ for $(i, j), (k, l) \in Z_m \times Z_n$, or when distinguishing between the two components of A

$$(A_1((i, j) + (k, l)), A_2((i, j) + (k, l))) = (A_1(i, j), A_2(i, j)) + (A_1(k, l), A_2(k, l)) =$$

$$(A_1(i, j) + A_1(k, l), A_2(i, j) + A_2(k, l))$$

which means that both $A_1\colon Z_m \times Z_n \to Z_m$ and $A_2\colon Z_m \times Z_n \to Z_n$ are group homomorphisms. Furthermore each element $(i, j) \in Z_m \times Z_n$ can be written as $(i, 0) + (0, j)$. Thus $A_r(i, j) = A_r((i, 0) + (0, j)) = A_r(i, 0) + A_r(0, j)$ for $r = 1, 2$. Define $A_{11}(i) := A_1(i, 0)$, $A_{12}(j) := A_1(0, j)$, $A_{21}(i) := A_2(i, 0)$ and $A_{22}(j) := A_2(0, j)$, then since A is a homomorphism the four functions $A_{11}\colon Z_m \to Z_m$, $A_{12}\colon Z_n \to Z_m$, $A_{21}\colon Z_m \to Z_n$ and $A_{22}\colon Z_n \to Z_n$ are group homomorphisms as well.

Therefore it remains to describe all the group homomorphisms from Z_m to Z_n. Before doing this we should remember that $(Z_n, +)$ is a cyclic group. A generator of Z_n is for instance 1, since each element $k \in Z_n$ can be computed by k-times summing the element 1 of Z_n. I. e.,

$$k = \underbrace{1 + \ldots + 1}_{k-\text{times}} = \sum_{i=1}^{k} 1 = k \cdot 1.$$

In this context $k \cdot 1$ stands for k-times summing the element 1. But we must take care that $k \in Z_n$ has many different representations as a sum of 1's in Z_n since $k = (k+zn) \cdot 1$ for all $z \in \mathbb{Z}$. Furthermore the order of $k \in Z_n$ is the smallest positive integer i such that $i \cdot k = 0$.

6.1 Lemma. *A mapping $A\colon Z_m \to Z_n$ is a group homomorphism if and only if $A(k) = k \cdot A(1)$ for all $k \in Z_m$ and the order of $A(1)$ divides m.*

Proof. If A is a group homomorphism then $A(k) = A(k \cdot 1) = k \cdot A(1)$ for $k \in Z_m$. Moreover the order of $1 \in Z_m$ equals m, therefore $0 = A(0) = A(m \cdot 1) = m \cdot A(1)$ and the order of $A(1)$ divides m.

Conversely, the mapping $A(k) := k \cdot A(1)$ is well defined on Z_m because $k \cdot A(1) = (k + zm) \cdot A(1)$ since $m \cdot A(1) = 0$. In other words, the value $A(k)$ does not depend on the special way of describing $k \in Z_m$ as a sum of 1's in Z_m. And the mapping A is a group homomorphism since $A(i+j) = (i+j) \cdot A(1) = i \cdot A(1) + j \cdot A(1) = A(i) + A(j)$ for all $i, j \in Z_m$. □

A group homomorphism $A\colon Z_m \to Z_n$ is uniquely given by $A(1)$. In the case $n = m$ $A(1)$ can be any element i of Z_n since the order of i is always a divisor of n. When n is different from m it was explained in 4.5 how Z_n can be decomposed as a product of Z_{p^a} for prime numbers p and integers $a \geq 1$. Consequently it is enough to describe the group homomorphisms from Z_{p^a} to Z_{q^b} where q is a prime number and $b \geq 1$. If $p \neq q$ then $A(1) = 0$, since each non-zero element of Z_{q^b} is of order q^r for some $1 \leq r \leq b$, which implies that it is not a divisor of p^a. If $p = q$ we have to investigate the two cases $a > b$ and $b > a$. Let $a > b$ then the order of $A(1)$ divides p^b thus it also divides p^a and there are no restrictions for $A(1)$. If $a < b$ the order of $A(1)$ must be a divisor of p^a. Hence $A(1)$ must be chosen from

$$p^{b-a} Z_{p^b} = \left\{ p^{b-a} i \mid i \in Z_{p^b} \right\}.$$

Summing all these details up we have shown that each group endomorphism A of $Z_m \times Z_n$ is uniquely determined by giving the values of

$$A_{11}(1) \in Z_m,\ A_{12}(1) \in \frac{m}{\gcd(m,n)} Z_m,\ A_{21}(1) \in \frac{n}{\gcd(m,n)} Z_n,\ A_{22}(1) \in Z_n,$$

which are usually written in a system of the following form.

6.2 $$A = \begin{pmatrix} A_{11}(1) & A_{12}(1) \\ A_{21}(1) & A_{22}(1) \end{pmatrix} =: \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

The meaning of this notation will become clear soon. And the image of $(i, j) \in Z_m \times Z_n$ under the endomorphism A is $A(i, j) = (a_{11}i + a_{12}j, a_{21}i + a_{22}j)$.

In the case $n = m$ some more details can be obtained because in this case all the components of A are elements of the same ring $R = Z_n$.

In general a system of n rows and m columns of elements of a ring R is called an $n \times m$-matrix over R. The set of all $n \times m$-matrices over R is indicated by $M_{n,m}(R)$. The elements $A \in M_{n,m}(R)$ are usually written as $A = (a_{ij})_{\substack{1 \le i \le n \\ 1 \le j \le m}}$ or when explicitly writing down all the components of A as

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}.$$

The first index is the row-index the second the column-index. The *sum* $A + B$ of two matrices $A, B \in M_{n,m}(R)$ is the matrix $C = (c_{ij}) \in M_{n,m}(R)$ given by $c_{ij} = a_{ij} + b_{ij}$. Let $A \in M_{n,m}(R)$ and $B \in M_{m,r}(R)$ (take care that m is both the number of columns of A and number of rows in B) then the product AB of these two matrices is the matrix $C \in M_{n,r}(R)$ given by

$$c_{ik} = \sum_{j=1}^{m} a_{ij} b_{jk}.$$

In the case the matrices have the same number of rows and columns they are called *quadratic matrices* and the set of all $n \times n$-matrices over R is indicated as $M_n(R)$. In this case the two operations sum and product of matrices are inner compositions on $M_n(R)$ and the following lemma holds.

6.3 Lemma. *Let R be a ring, then $M_n(R)$ together with the two operations defined above is a ring. If R has a 1-element then $M_n(R)$ has a 1-element which is given by*

$$I_n := \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

In general $M_n(R)$ is not a commutative ring.

Let R be a ring with 1. The set of unit elements in $M_n(R)$ is indicated by

$$\mathrm{GL}_n(R) := \{A \in M_n(R) \mid \exists A' \in M_n(R) : AA' = A'A = I_n\}.$$

We are especially interested in the ring of all 2×2 matrices over Z_n. All the following results will be presented for 2×2-matrices, usually they hold for higher dimensions as well. For the rest of this section let R be a commutative ring with 1. In order to characterize the unit elements in $M_2(R)$ (or more general in $M_n(R)$) we introduce the determinant of a matrix. The *determinant* of a 2×2-matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is defined by

$$\det(A) := ad - bc.$$

For matrices of higher dimension the definition of the determinant is a little bit more complicated.

6.4 Lemma. *The determinant of the product AB of two matrices $A, B \in M_2(R)$ is the product of the two determinants of A and B, i. e.*

$$\det(AB) = \det(A)\det(B).$$

Proof. Let $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B := \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ then $AB = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$ and $\det(AB) = (ae+bg)(cf+dh) - (af+bh)(ce+dg) = acef + bcfg + adeh + bdgh - acef - bceh - adfg - bdgh = (ad-bc)(eh-fg) = \det(A)\det(B)$. □

6.5 Lemma. *A 2×2 matrix A over R belongs to* $\mathrm{GL}_2(R)$ *if and only if* $\det(A)$ *is a unit element in R.*

Proof. If A belongs to $\mathrm{GL}_2(R)$ then there is a matrix $A' \in M_2(R)$ such that $AA' = I_2$. From 6.4 it follows that $\det(A)\det(A') = \det(AA') = \det(I_2) = 1$ which implies that $\det(A)$ is a unit element in R.

Now let A be the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $\det(A) = ad - bc = e$ belongs to R^*. Then there exists $f \in R^*$ such that $ef = fe = 1$. When we define the matrix A' by

$$A' := \begin{pmatrix} fd & -fb \\ -fc & fa \end{pmatrix}$$

then

$$A'A = \begin{pmatrix} fda - fbc & fbd - fbd \\ -fac + fac & -fcb + fad \end{pmatrix} = \begin{pmatrix} fe & 0 \\ 0 & fe \end{pmatrix} = I_2,$$

i. e. $A'A = I_2$ and by analogy $AA' = I_2$. This means that $A \in \mathrm{GL}_2(R)$ and the proof is finished. □

Each matrix $A \in M_2(Z_n)$ defines a group endomorphism ϕ_A of Z_n^2 of the form

$$\phi_A(i,j) := A \begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} a_{11}i + a_{12}j \\ a_{21}i + a_{22}j \end{pmatrix}.$$

This means that we have to compute the product of two matrices, namely the product of the matrix A and the 2×1-matrix $\begin{pmatrix} i \\ j \end{pmatrix}$. (Matrices consisting of only one row or only one column are usually called *vectors*. Sometimes, as was just seen above, a row-vector must be identified with the corresponding column-vector.) Then ϕ_A is a group automorphism of Z_n^2 if and only if A belongs to $\mathrm{GL}_2(Z_n)$ which is equivalent to $\det(A)$ is a unit element in Z_n.

In the case $m = n$ G. Mazzola suggested to investigate the following group G acting on Z_n^2.

$$G := \langle \{T, \phi_A \mid A \in \{U, P, D_l \mid l \in Z_n^*\}\} \rangle,$$

where

$$T \colon Z_n^2 \to Z_n^2, \qquad (i,j) \mapsto T(i,j) := (i, j+1)$$

$$\phi_A \colon Z_n^2 \to Z_n^2, \qquad (i,j) \mapsto \phi_A(i,j) = A \begin{pmatrix} i \\ j \end{pmatrix}$$

and

$$U := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},\ P := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ D_l := \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}.$$

T stands for transposing by one pitch-class, the matrix U describes an *arpeggio* since for $k \le n$ the k-chord $\{(x, y_1), (x, y_2), \ldots, (x, y_k)\}$, which is played at beat x is transformed into

$$\{(x + y_1, y_1), (x + y_2, y_2), \ldots, (x + y_k, y_k)\}.$$

The matrices D_l define an *augmentation* since the rhythm $\{(x_1, y), (x_2, y), \ldots, (x_k, y)\}$, which is played at pitch-class y is replaced by the rhythm

$$\{(lx_1, y), (lx_2, y), \ldots, (lx_k, y)\}.$$

The matrix P describes the exchange of rhythmical and tonal properties. Moreover the product $\phi_P \circ T \circ \phi_P$ is the cyclic shift S by one beat, $S(i,j) = (i+1, j)$.

The three matrices U, P and D_l are elements of $\mathrm{GL}_2(Z_n)$ so they define group automorphisms of Z_n^2 and the group $\langle \{U, P, D_l \mid l \in Z_n^*\} \rangle$ is a subgroup of $\mathrm{GL}_2(Z_n)$.

6.6 Lemma. *The group $\langle \{U, P, D_l \mid l \in Z_n^*\} \rangle$ is the general linear group* $\mathrm{GL}_2(Z_n)$.

Proof. Simple computations show that

$$U^k = \begin{pmatrix} k & 1 \\ 1 & 0 \end{pmatrix},\ U^k P = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix},\ P U^k = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix},\ P D_l P = \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}.$$

Let $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(Z_n)$, such that one component of A equals zero. Without loss of generality $c = 0$. (Otherwise in one of the products PA, AP or PAP the first component in the second row is zero.) Then $\det(A) = ad - bc = ad \in Z_n^*$, whence $a, d \in Z_n^*$. Furthermore we realize that

$$A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = P D_d P U^b P D_a.$$

In other words, the matrix A is an element of $\langle\{U, P, D_l \mid l \in Z_n^*\}\rangle$.

In the case that all components of A are different from 0, consider a, b, c, d as integers. Without loss of generality assume that $c \geq d$. An application of the division algorithm 2.1 yields $c = qd + r$ with integers q and r such that $0 \leq r < d$. Multiplying A with the matrix PU^{-q} we get

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} = \begin{pmatrix} a - qb & b \\ c - qd & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} =: A',$$

where $a' = a - qb$, $b' = b$, $c' = c - qd = r < d \leq c$, $d' = d$ and $\det(A) = \det(A')$. If there is at least one component of A' which is zero we are done, because in this case it is already proved that A' belongs to $\langle\{U, P, D_l \mid l \in Z_n^*\}\rangle$ and for that reason A belongs to this group as well. Otherwise $c' < c$ and the first component in the second row of $A'P = \begin{pmatrix} b' & a' \\ d' & c' \end{pmatrix}$ is greater than the second component in the second row of this matrix. Repeating this method finitely many times yields a matrix A'' of the form

$$\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$$

such that $c'' = 0$. Because of 6.4 $\det(A) = \det(A'')$, since $\det(P) = 1$ and $\det(PU^{-q}) = 1$ for all q. □

Each mapping of the form

$$(i, j) \mapsto \pi_{A,b}(i, j) := A \begin{pmatrix} i \\ j \end{pmatrix} + b$$

for A in $\mathrm{GL}_2(Z_n)$ and $b \in Z_n^2$ is called an *affine mapping* from Z_n^2 to Z_n^2. The set of all affine mappings is indicated by

$$\mathrm{Aff}_2(Z_n) := \left\{\pi_{A,b} \mid A \in \mathrm{GL}_2(Z_n),\ b \in Z_n^2\right\}.$$

6.7 Lemma. *The group G of symmetry operations of motives introduced above is the group $\mathrm{Aff}_2(Z_n)$ of all affine mappings from Z_n^2 to Z_n^2.*

Proof. It is obvious that G is a subgroup of $\mathrm{Aff}_2(Z_n)$. In order to prove the other inclusion let $A \in \mathrm{GL}_2(Z_n)$ and $b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$, then the mapping $\pi_{A,b}$ can be described as $S^{b_1} \circ T^{b_2} \circ \phi_A$ and together with 6.6 the proof is finished. □

Now we investigate which group to use as the symmetry group of motives in $Z_m \times Z_n$ for $m \neq n$. Generalizing the approach above the group of all symmetries of $Z_m \times Z_n$ could be described as the set of all mappings of the form

$$Z_m \times Z_n \ni (i, j) \mapsto \pi_{A,b}(i, j) := A \begin{pmatrix} i \\ j \end{pmatrix} + b := \begin{pmatrix} a_{11}i + a_{12}j + b_1 \\ a_{21}i + a_{22}j + b_2 \end{pmatrix} \in Z_m \times Z_n,$$

where A is a matrix representing a group automorphism of $Z_m \times Z_n$ as in 6.2, and b is an arbitrary element of $Z_m \times Z_n$.

In order to determine the number of non G-equivalent k-motives by applying Pólya's Theorem 5.4 the cycle index of the acting group G must be computed. Again in the general case $n \neq m$ we do not have enough information in order to get nice results. Of course it is always possible to apply the ring isomorphism from 4.5 to $Z_m \times Z_n$.

6.8 Lemma. *According to 2.6 let $m = \prod_{i=1}^r p_i^{a_i}$ and $n = \prod_{i=1}^s q_i^{b_i}$ be the decompositions of m and n into primes and let ϕ_m and ϕ_n be the corresponding ring isomorphisms $\phi_m\colon Z_m \to \bigtimes_{i=1}^r Z_{p_i^{a_i}}$ and $\phi_n\colon Z_n \to \bigtimes_{i=1}^s Z_{q_i^{b_i}}$. Then*

$$\phi_{m,n}\colon Z_m \times Z_n \to \left(\bigtimes_{i=1}^r Z_{p_i^{a_i}}\right) \times \left(\bigtimes_{i=1}^s Z_{q_i^{b_i}}\right), \quad (k,l) \mapsto \phi_{m,n}(k,l) := (\phi_m(k), \phi_n(l))$$

is a ring isomorphism. Especially if $m = n$ then $\phi_{n,n}$ is a ring isomorphism from Z_n^2 to $\bigtimes_{i=1}^r Z_{p_i^{a_i}}^2$.

Let furthermore A be an endomorphism of $Z_m \times Z_n$ given as a matrix and $k, l \in Z_m \times Z_n$ then

$$\phi_{m,n}(Ak + l) = \phi_{m,n}(A)\phi_{m,n}(k) + \phi_{m,n}(l),$$

where $\phi_{m,n}(A)$ is the matrix $\begin{pmatrix} \phi_m(a_{11}) & \phi_m(a_{12}) \\ \phi_n(a_{21}) & \phi_n(a_{22}) \end{pmatrix}$. If $m = n$ then $\phi_{n,n}(A)$ is an element of $\bigtimes_{i=1}^r M_2(Z_{p_i^{a_i}})$.

For $n = m$ the action of $\mathrm{Aff}_2(Z_n)$ on Z_n^2 can be replaced by the action of the direct product $\bigtimes_{i=1}^r \mathrm{Aff}_2(Z_{p_i^{a_i}})$ on $\bigtimes_{i=1}^r Z_{p_i^{a_i}}^2$ and the cycle index can be computed as

$$C(\mathrm{Aff}_2(Z_n), Z_n^2) = \bigtimes_{i=1}^r C(\mathrm{Aff}_2(Z_{p_i^{a_i}}), Z_{p_i^{a_i}}^2).$$

In the case $a_i = 1$ the residue-class-ring Z_{p_i} is a field and we can apply a lot of theory about fields, polynomials over fields etc. in order to compute the cycle indices of the natural actions of $\mathrm{GL}_2(Z_{p_i})$ or $\mathrm{Aff}_2(Z_{p_i})$ on $Z_{p_i}^2$. Going into details would carry us too far. See for instance [15, 11]. For small values of n the cycle index of the action of $\mathrm{Aff}_2(Z_n)$ on Z_n^2 are given below:

$$C(\mathrm{Aff}_2(Z_2), Z_2^2) = \frac{1}{24}\left(6z_4 + 3z_2^2 + 8z_1z_3 + 6z_1^2z_2 + z_1^4\right)$$

$C(\mathrm{Aff}_2(Z_3), Z_3^2) = \frac{1}{432}(72z_3z_6 + 56z_3^3 + 108z_1z_8 + 54z_1z_4^2 + 72z_1z_2z_6 + 9z_1z_2^4 + 24z_1^3z_3^2 + 36z_1^3z_2^3 + z_1^9)$

$C(\mathrm{Aff}_2(Z_4), Z_4^2) = \frac{1}{1536}(192z_8^2 + 384z_4^4 + 48z_2^4z_4^2 + 69z_2^8 + 384z_1z_3z_6^2 + 128z_1z_3^5 + 192z_1^2z_2z_4^3 + 48z_1^4z_2^2z_4^2 + 72z_1^4z_2^6 + 18z_1^8z_2^4 + z_1^{16})$

$C(\mathrm{Aff}_2(Z_5), Z_5^2) = \frac{1}{12000}(1200z_5z_{20} + 600z_5z_{10}^2 + 504z_5^5 + 2000z_1z_{24} + 1000z_1z_{12}^2 + 1000z_1z_8^3 + 500z_1z_6^4 + 1200z_1z_4z_{20} + 800z_1z_4^6 + 500z_1z_3^8 + 600z_1z_2^2z_{10}^2 + 1500z_1z_2^2z_4^5 + 25z_1z_2^{12} + 120z_1^5z_5^4 + 300z_1^5z_4^5 + 150z_1^5z_2^{10} + z_1^{25})$

$C(\mathrm{Aff}_2(Z_7), Z_7^2) = \frac{1}{98784}(4704z_7z_{42} + 4704z_7z_{21}^2 + 2352z_7z_{14}^3 + 2064z_7^7 + 16464z_1z_{48} + 8232z_1z_{24}^2 + 8232z_1z_{16}^3 + 4116z_1z_{12}^4 + 4116z_1z_8^6 + 4704z_1z_6z_{42} + 2842z_1z_6^8 + 2058z_1z_4^{12} + 4704z_1z_3^2z_{21}^2 + 10976z_1z_3^2z_6^7 + 2842z_1z_3^{16} + 2352z_1z_2^3z_{14}^3 + 5488z_1z_2^3z_6^7 + 5488z_1z_2^3z_3^2z_6^6 + 49z_1z_2^{24} + 336z_1^7z_7^6 + 784z_1^7z_6^7 + 784z_1^7z_3^{14} + 392z_1^7z_2^{21} + z_1^{49})$

$C(\mathrm{Aff}_2(Z_8), Z_8^2) = \frac{1}{98304}(12288z_{16}^4 + 21504z_8^8 + 1536z_4^8z_8^4 + 6912z_4^{16} + 2304z_2^8z_4^4z_8^4 + 864z_2^{16}z_4^8 + 789z_2^{32} + 16384z_1z_3z_6^2z_{12}^4 + 8192z_1z_3z_6^{10} + 6144z_1z_3^5z_6^8 + 2048z_1z_3^{21} + 6144z_1^2z_2z_4^7z_8^4 + 6144z_1^2z_2z_4^{15} + 1536z_1^4z_2^6z_4^4z_8^4 + 2048z_1^4z_2^6z_4^{12} + 768z_1^4z_2^{14}z_4^8 + 256z_1^4z_2^{30} + 768z_1^8z_2^4z_4^4z_8^4 + 576z_1^8z_2^{12}z_4^8 + 768z_1^8z_2^{28} + 96z_1^{16}z_2^8z_4^8 + 216z_1^{16}z_2^{24} + 18z_1^{32}z_2^{16} + z_1^{64})$

$C(\mathrm{Aff}_2(Z_9), Z_9^2) = \frac{1}{314928}(52488z_9z_{18}^4 + 36936z_9^9 + 5832z_3^3z_6^{12} + 3888z_3^9z_9^6 + 4088z_3^{27} + 69984z_1z_8z_{24}^3 + 8748z_1z_8^{10} + 34992z_1z_4^2z_{12}^6 + 4374z_1z_4^{20} + 17496z_1z_2z_6^4z_{18}^3 + 17496z_1z_2z_6^{13} + 17496z_1z_2^4z_6^3z_{18}^3 + 3888z_1z_2^4z_6^{12} + 2592z_1z_2^{13}z_6^9 + 81z_1z_2^{40} + 5832z_1^3z_3^8z_9^6 + 5832z_1^3z_3^{26} + 11664z_1^3z_2^3z_3^2z_6^{11} + 5832z_1^3z_2^{12}z_3^2z_6^8 + 1944z_1^9z_3^6z_9^6 + 432z_1^9z_3^{24} + 1944z_1^9z_2^9z_6^9 + 972z_1^9z_2^{36} + 96z_1^{27}z_3^{18} + z_1^{81})$

$C(\mathrm{Aff}_2(Z_{11}), Z_{11}^2) = \frac{1}{1597200}(58080z_{11}z_{110} + 58080z_{11}z_{55}^2 + 14520z_{11}z_{22}^5 + 13320z_{11}^{11} + 212960z_1z_{120} + 106480z_1z_{60}^2 + 106480z_1z_{40}^3 + 53240z_1z_{30}^4 + 53240z_1z_{24}^5 + 53240z_1z_{20}^6 + 53240z_1z_{15}^8 + 26620z_1z_{12}^{10} + 58080z_1z_{10}z_{110} + 96316z_1z_{10}^{12} + 26620z_1z_8^{15} + 13310z_1z_6^{20} + 58080z_1z_5^2z_{55}^2 + 255552z_1z_5^2z_{10}^{11} + 96316z_1z_5^{24} + 13310z_1z_4^{30} + 13310z_1z_3^{40} + 14520z_1z_2^5z_{22}^5 + 63888z_1z_2^5z_{10}^{11} + 63888z_1z_2^5z_5^2z_{10}^{10} + 121z_1z_2^{60} + 1320z_1^{11}z_{11}^{10} + 5808z_1^{11}z_{10}^{11} + 5808z_1^{11}z_5^{22} + 1452z_1^{11}z_2^{55} + z_1^{121})$

Now the cycle index of $\mathrm{Aff}_2(Z_{12})$ can be computed as

$$C(\mathrm{Aff}_2(Z_3), Z_3^2) \times C(\mathrm{Aff}_2(Z_4), Z_4^2)$$

which is the following polynomial

$\frac{1}{663552}(z_1^{144} + 18z_1^{72}z_2^{36} + 36z_1^{48}z_2^{48} + 24z_1^{48}z_3^{32} + 72z_1^{36}z_2^{54} + 48z_1^{36}z_2^{18}z_4^{18} + 648z_1^{24}z_2^{60} + 432z_1^{24}z_2^{12}z_3^{16}z_6^8 + 192z_1^{18}z_2^9z_4^{27} + 9z_1^{16}z_2^{64} + 72z_1^{16}z_2^{16}z_6^{16} + 54z_1^{16}z_4^{32} + 108z_1^{16}z_8^{16} + 2592z_1^{12}z_2^{66} + 1728z_1^{12}z_2^{30}z_4^{18} + 1728z_1^{12}z_2^{18}z_3^8z_6^{12} + 1152z_1^{12}z_2^6z_3^8z_4^6z_6^4z_{12}^4 + 128z_1^9z_3^{45} + 384z_1^9z_3^9z_6^{18} + 162z_1^8z_2^{68} + 1296z_1^8z_2^{20}z_6^{16} + 972z_1^8z_2^4z_4^{32} + 1944z_1^8z_2^4z_8^{16} + 6912z_1^6z_2^{15}z_4^{27} + 4608z_1^6z_2^3z_3^4z_4^9z_6^2z_{12}^6 + 648z_1^4z_2^{70} + 432z_1^4z_2^{34}z_4^{18} + 5184z_1^4z_2^{22}z_6^{16} + 3456z_1^4z_2^{10}z_4^6z_6^8z_{12}^4 + 3888z_1^4z_2^6z_4^{32} + 7776z_1^4z_2^6z_8^{16} + 2592z_1^4z_2^2z_4^{34} + 5184z_1^4z_2^2z_4^2z_8^{16} + 4608z_1^3z_2^3z_3^{15}z_6^{15} + 13824z_1^3z_2^3z_3^3z_6^{21} + 3072z_1^3z_3^{47} + 9216z_1^3z_3^{11}z_6^{18} + 1728z_1^2z_2^{17}z_4^{27} + 13824z_1^2z_2^5z_4^9z_6^4z_{12}^6 + 10368z_1^2z_2z_4^{35} + 20736z_1^2z_2z_4^3z_8^{16} + 1152z_1z_2^4z_3^5z_6^{20} + 3456z_1z_2^4z_3z_6^{22} + 9216z_1z_2z_3^5z_6^{21} + 27648z_1z_2z_3z_6^{23} + 6912z_1z_3^5z_4^2z_{12}^{10} + 13824z_1z_3^5z_8z_{24}^5 + 20736z_1z_3z_4^2z_6^2z_{12}^{10} + 41472z_1z_3z_6^2z_8z_{24}^5 + 3174z_2^{72} + 2208z_2^{36}z_4^{18} + 6624z_2^{24}z_6^{16} + 4608z_2^{12}z_4^6z_6^8z_{12}^4 + 3726z_2^8z_4^{32} + 7452z_2^8z_8^{16} + 2592z_2^4z_4^{34} + 5184z_2^4z_4^2z_8^{16} + 7224z_3^{48} + 1008z_3^{24}z_6^{12} + 9288z_3^{16}z_6^{16} + 25536z_3^{12}z_6^{18} + 2688z_3^{12}z_6^6z_{12}^6 + 1296z_3^8z_6^{20} + 10752z_3^6z_6^3z_{12}^9 + 32832z_3^4z_6^{22} + 3456z_3^4z_6^{10}z_{12}^6 + 13824z_3^2z_6^5z_{12}^9 + 38400z_4^{36} + 36864z_4^{12}z_{12}^8 + 41472z_4^4z_8^{16} + 8832z_6^{24} + 6144z_6^{12}z_{12}^6 + 39936z_8^{18} + 18432z_8^6z_{24}^4 + 49152z_{12}^{12} + 24576z_{24}^6)$.

Replacing the indeterminate z_i in $C(\mathrm{Aff}_2(Z_{12}), Z_{12}^2)$ by $1 + z^i$ the coefficient of z^k is the number of different k-motives in $Z_{12} \times Z_{12}$. Here are these numbers of k-motives for small values of k. $1 + z + 5z^2 + 26z^3 + 216z^4 + 2024z^5 + 27806z^6 + 417209z^7 + 6345735z^8 + 90590713z^9 + 1190322956z^{10} + \ldots$ This polynomial must be read in the following way: There is (are) exactly one 1-motive, five 2-motives, twenty six 3-motives etc. The complete list of numbers can be found in [7].

7 Construction of motive representatives

In the last part of this article we describe a method which allows to compute complete lists of representatives of k-motives. A complete list of orbit representatives is usually called a *transversal*. Again this method is described in a more general setting. Consider a finite group action ${}_GX$ which induces a group action by 3.10 on the set of all mappings from X to a finite set Y. Without loss of generality we assume that there is a total order defined both on X and Y. Otherwise there exist integers n and m and bijections from X to $\underline{n}$ and Y to $\underline{m}$ and the sets X and Y can be replaced by the totally ordered sets $\underline{n}$ and $\underline{m}$. A function $f \in \underline{m}^{\underline{n}}$ can be written as an n-tuple of the form $f = (f(1), f(2), \dots f(n))$. There is a total order on the set of all n-tuples over $\underline{m}$ given by the *lexicographic order*. With respect to this order a function f is smaller than a function $h \in \underline{m}^{\underline{n}}$ if and only if there is an index $i_0 \in \underline{n}$ such that $f(i) = h(i)$ for all $i < i_0$ and $f(i_0) < h(i_0)$. As the *canonic representative* of the orbit $G(f)$ we choose that function $h \in G(f)$ such that $h \geq gf = f \circ \bar{g}^{-1}$ for all $g \in G$. In other words, the canonic representative h is given as

$$h = \max \{gf \mid g \in G\} .$$

The same way we could have introduced the canonic representative of an orbit as the minimal element in it. These canonic representatives are useful for computing transversals of motives, for other purposes there probably exist other canonic representatives.

If S is a subset of Y^X and $f \in Y^X$ then when writing $f \geq S$ we mean $f \geq h$ for all $h \in S$. In order to decide whether a given function $f \in \underline{m}^{\underline{n}}$ is the canonic representative of the orbit $G(f)$ it must be tested whether $f \geq G(f)$, i. e. $f \geq gf$ for all $g \in G$. this procedure is called the *maximum-test* of f. For applying this test we first have to find a method to generate all elements of the acting group. So far the group G is just given by a set of generators and there is usually no canonic way of describing the elements of G as products of the generators. (For instance in the last item of 3.4 certain relations between the two generators of the group D_n were described what enabled us to construct all elements of D_n.) In general such rules are not known. Therefore we introduce the Sims-chain of a permutation group, which allows to generate all group elements as a product of the strong generators. Moreover we have to analyse the maximum-test in order to make it shorter. Testing whether $f \geq gf$ for all $g \in G$ depends heavily on the order of G. Often it is possible to find certain shortcuts during this test. It will be shown that in many situations it is not necessary to take all group elements into account, often we can do certain jumps as will be described later. Proceeding this way, we generate all functions $f \in \underline{m}^{\underline{n}}$ starting from the biggest one and stepping from one function f to its successor, which is the function h that fulfils $f > h$ such that there exists no function k with the property $f > k > h$. Each of the functions $f \in \underline{m}^{\underline{n}}$ is tested whether it is maximal in its orbit. If it is maximal then it is a canonic representative, if not then we know that the canonic representative of the orbit $G(f)$ appeared already among those functions which were already tested for maximality since these functions are listed according to the lexicographic order in decreasing way. Finally we will see that it is not necessary to test each function $f \in \underline{m}^{\underline{n}}$ for maximality. In certain situations it will be possible to decide from previous results that f cannot be a canonic representative. In general we are usually not interested in a complete list of all orbit representatives. For instance there are 33.608135.013344.714280.178360.727460.692224 representatives of motives in $Z_{12} \times Z_{12}$. For that reason we fix our attention to k-motives for given k, in other words, we are interested in transversals of functions of given weight.

7.1 Example. For the construction of motives we investigate characteristic functions which are functions form $X := Z_m \times Z_n$ to $Y := \{0,1\}$. On Y there is a natural linear order $0 < 1$. A natural bijection from X to $\underline{mn}$ is given by $Z_m \times Z_n \ni (i,j) \mapsto i + m \cdot j + 1 \in \underline{mn}$. This *labelling* of the elements of $Z_m \times Z_n$ is used for the rest of this section.

In order to give an example of the lexicographic order, here is a list of the characteristic functions of all subsets of a set of cardinality 3 in lexicographic order:

$$(0,0,0) < (0,0,1) < (0,1,0) < (0,1,1) < (1,0,0) < (1,0,1) < (1,1,0) < (1,1,1).$$

$\diamond$

Let ${}_G\underline{n}$ be a group action, and let $\bar{G}$ be the induced permutation representation of G on $\underline{n}$. The *pointwise stabilizer* or the *centralizer* of $\underline{k} \subseteq \underline{n}$ is the subgroup

$$C_{\bar{G}}(\underline{k}) := \left\{ \bar{g} \in \bar{G} \mid \bar{g}(i) = i \text{ for all } i \in \underline{k} \right\}$$

of $\bar{G}$. These pointwise stabilizers form a chain of subgroups of $\bar{G}$ of the form

$$\{\mathrm{id}\} = C_{\bar{G}}(\underline{n}) \leq C_{\bar{G}}(\underline{n-1}) \leq \ldots \leq C_{\bar{G}}(\underline{1}) \leq C_{\bar{G}}(\emptyset) = \bar{G}$$

which is called the *Sims-chain* of $\bar{G}$ (cf. [30, 31]). Let b the smallest element in $\underline{n}$ such that $\{\mathrm{id}\} = C_{\bar{G}}(\underline{b})$ then

$$\{\mathrm{id}\} = C_{\bar{G}}(\underline{b}) \leq \ldots \leq C_{\bar{G}}(\emptyset) = \bar{G}.$$

Then b is called the *length* of the Sims-chain and the set $\underline{b}$ is called a *basis* of the Sims-chain.

For each $i \in \underline{b}$ determine a complete set of left-coset representatives $\pi_j^{(i)} \in C_{\bar{G}}(\underline{i-1})$ (cf. the first item of 3.9) of $C_{\bar{G}}(\underline{i-1})/C_{\bar{G}}(\underline{i})$ then

$$C_{\bar{G}}(\underline{i-1}) = \bigcup_{j=1}^{r(i)} \pi_j^{(i)} C_{\bar{G}}(\underline{i}).$$

These $\pi_j^{(i)}$ are called *strong generators* of $\bar{G}$. Without loss of generality $\pi_1^{(i)} = \mathrm{id} \in C_{\bar{G}}(\underline{i-1})$. Each element $\bar{g} \in C_{\bar{G}}(\underline{b-1})$ can uniquely be written as $\pi_{j_b}^{(b)} \circ \mathrm{id}$ and each element $\bar{g} \in C_{\bar{G}}(\underline{b-2})$ has a unique representation as $\pi_{j_{b-1}}^{(b-1)} \circ \pi_{j_b}^{(b)} \circ \mathrm{id}$ for some $1 \leq j_{b-1} \leq r(b-1)$ and $1 \leq j_b \leq r(b)$. Proceeding like that finally we derive the following result:

7.2 Lemma. *Each element of $\bar{G}$ can uniquely be expressed as a product of strong generators in the form*

$$\pi_{j_1}^{(1)} \circ \pi_{j_2}^{(2)} \circ \ldots \circ \pi_{j_b}^{(b)}$$

for some $1 \leq j_k \leq r(k)$, $1 \leq k \leq b$.

Moreover the uniqueness of this representation allows to determine the order of $\bar{G}$.

7.3 Corollary. *The order of $\bar{G}$ equals*

$$|\bar{G}| = \prod_{i=1}^{b} r(i).$$

Since $\pi_j^{(i)}(k) = k$ for $i > k$ the orbit $G(k)$ equals

$$G(k) = \left\{ \pi_{j_1}^{(1)} \circ \pi_{j_2}^{(2)} \circ \ldots \circ \pi_{j_k}^{(k)}(k) \mid j_1 \in \underline{r(1)}, \ldots, j_k \in \underline{r(k)} \right\}.$$

The elements of $\bar{G}$ can be expressed as the leaves (which are the final nodes) of the following tree.

$$\begin{array}{ccccccc}
 & \pi_1^{(1)} & \cdots & \cdots & \cdots & \pi_{r(1)}^{(1)} & \\
\swarrow & \cdots & \searrow & \cdots & \swarrow & \cdots & \searrow \\
\pi_1^{(1)} \circ \pi_1^{(2)} & \cdots & \pi_1^{(1)} \circ \pi_{r(2)}^{(2)} & \cdots & \pi_{r(1)}^{(1)} \circ \pi_1^{(2)} & \cdots & \pi_{r(1)}^{(1)} \circ \pi_{r(2)}^{(2)} \\
\swarrow \cdots \searrow & \cdots & \swarrow \cdots \searrow & \cdots & \swarrow \cdots \searrow & \cdots & \swarrow \cdots \searrow
\end{array}$$

For testing whether a function $f \in \underline{m}^{\underline{n}}$ is maximal in its orbit or not we have to compute $gf = f \circ \bar{g}^{-1}$ for all g which are the leaves of this tree. But sometimes it is possible to cut certain branches of this tree which will be shown in the next lemma. This method helps to make the maximum-test much faster.

7.4 Lemma. *Assume that $f > f \circ \pi_j^{(i)}$ and $f(i) > (f \circ \pi_j^{(i)})(i)$, then*

$$f > C_{\bar{G}}(\underline{i})(f \circ \pi_j^{(i)}).$$

Proof. Let $\tau \in C_{\bar{G}}(\underline{i})$ and assume that $k \leq i - 1$, then

$$(f \circ \pi_j^{(i)} \circ \tau)(k) = (f \circ \pi_j^{(i)})(k) = f(k)$$

since $\pi_j^{(i)} \in C_{\bar{G}}(\underline{i-1})$, and

$$(f \circ \pi_j^{(i)} \circ \tau)(i) = (f \circ \pi_j^{(i)})(i) < f(i).$$

$\square$

In general the functions $f \in \underline{m}^{\underline{n}}$ are not injective, so there exist non-trivial permutations $\pi, \sigma \in \bar{G}$ such that $f \circ \pi = f \circ \sigma$. This fact can also be used for making the maximum-test faster.

7.5 Lemma. *Let $f \geq C_{\bar{G}}(\underline{i})(f)$ and assume that there exists a permutation $\sigma \in C_{\bar{G}}(\underline{i})$ such that $f \circ \pi_j^{(i)} \circ \sigma = f$, then*

$$C_{\bar{G}}(\underline{i})(f \circ \pi_j^{(i)}) \leq f.$$

Proof. Under the given assumptions the orbit of $f \circ \pi_j^{(i)}$ under $C_{\bar{G}}(\underline{i})$ coincides with the orbit $C_{\bar{G}}(\underline{i})(f)$ since

$$C_{\bar{G}}(\underline{i})(f \circ \pi_j^{(i)}) = \left\{ f \circ \pi_j^{(i)} \circ \tau \mid \tau \in C_{\bar{G}}(\underline{i}) \right\} =$$

$$= \left\{ f \circ \pi_j^{(i)} \circ \sigma \circ \tau \mid \tau \in C_{\bar{G}}(\underline{i}) \right\} = \{ f \circ \tau \mid \tau \in C_{\bar{G}}(\underline{i}) \} = C_{\bar{G}}(\underline{i})(f).$$

Hence each $f' \in C_{\bar{G}}(\underline{i})(f \circ \pi_j^{(i)})$ belongs to $C_{\bar{G}}(\underline{i})(f)$ and consequently $f' \leq f$. □

These results motivate the following recursive algorithm for the maximum-test of f.

7.6 Algorithm. Max-Test. Assume that a Sims-chain of length b and a set of strong generators $\pi_j^{(i)}$ for $1 \leq j \leq r(i)$ and $1 \leq i \leq b$ are known for a given action of a group G on $\underline{n}$. Furthermore it is assumed that $\pi_1^{(i)} = \mathrm{id}$. For testing a function $f \in \underline{m}^{\underline{n}}$ for maximality define a vector $F := (f_0, f_1, \ldots, f_b)$ of functions where $f_0 := f$. Then the maximum-test is invoked by `Max-Test`$(0, F)$.

Input: an index i and a vector F of functions $f_j \in \underline{m}^{\underline{n}}$ such that $f_0 = f$.
Output: `TRUE` if f_0 is maximal in its $C_{\bar{G}}(\underline{i})$-orbit
`FALSE` if f_0 is not maximal in its $C_{\bar{G}}(\underline{i})$-orbit.

`Max-Test`(i, F);
{
$i := i + 1$;
For $j := 1, \ldots, r(i)$ do {
  $f_i := f_{i-1} \circ \pi_j^{(i)}$;
  If $(f_0 < f_i)$ then return `FALSE`;
  else if $\Big[[(f_0 = f_i)$ and $(j = 1)]$ or $[(f_0 > f_i)$ and $(f_0(i) \not> f_i(i))]\Big]$ and $(i < b)$ then
    if (`Max-Test`(i, F) =`FALSE`) return `FALSE`;
  } Return `TRUE`;
}

This way R.C. Read's method of *orderly generation* can be described in the following way. (Cf. [1, 2].)

1. Determine the biggest function (of given weight) $f \in \underline{m}^{\underline{n}}$ with respect to the lexicographic order.
2. Using the maximum-test determine whether f is maximal in its orbit or not. In the case f is maximal add f to the list of canonic representatives.

3. If it is possible determine the successor of f with respect to the lexicographic order and jump to 2. Otherwise return the complete list of all representatives.

The Sims-chain of a permutation group $\bar{G}$ on X depends heavily on the labelling of the elements of X. In general it is more convenient to work with Sims-chains of big length.

7.7 Example. Now we describe the Sims-chain and the strong generators which appear when computing lists of representatives of motives in $Z_n \times Z_n$. (In other words, we restrict our interest to $n = m$.) From the previous section we know that the acting group $G := \mathrm{Aff}_2(Z_n)$ is the set of all affine mappings from Z_n^2 to Z_n^2. Using the labelling of elements of $Z_n \times Z_n$ introduced in 7.1 the stabilizer of the first element $(0,0) \in Z_n^2$ is

$$C_{\bar{G}}(\underline{1}) = \{\pi_{A,0} \mid A \in \mathrm{GL}_2(Z_n)\}.$$

This is obvious since $\pi_{A,b}(0,0) = b$ for all $A \in \mathrm{GL}_2(Z_n)$ and $b \in Z_n^2$. The set of left-coset representatives of $\mathrm{Aff}_2(Z_n)/\mathrm{GL}_2(Z_n)$ is

$$\left\{\pi_{I_2,b} \mid b \in Z_n^2\right\}.$$

In the next step we have to compute the pointwise stabilizer of the first two elements which is the set of stabilizers of $(0,0)$ which also stabilize $(1,0)$. It is easy to see that it is

$$C_{\bar{G}}(\underline{2}) = \left\{\pi_{A,0} \mid A = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix},\ b \in Z_n,\ d \in Z_n^*\right\},$$

since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Longleftrightarrow \begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Longleftrightarrow a = 1 \text{ and } c = 0$$

and the matrix $\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$ belongs to $\mathrm{GL}_2(Z_n)$ if and only if $d \in Z_n^*$. For computing the left-coset representatives of $C_{\bar{G}}(\underline{1})/C_{\bar{G}}(\underline{2})$ the following lemma can be applied.

7.8 Lemma. *Two matrices $A, B \in \mathrm{GL}_2(Z_n)$ belong to the same coset in $C_{\bar{G}}(\underline{1})/C_{\bar{G}}(\underline{2})$ if and only if $a_{11} = b_{11}$ and $a_{21} = b_{21}$. Hence a complete system of left-coset representatives can be constructed from*

$$\left\{(r,t) \in Z_n^2 \mid \text{there exists } (s,u) \in Z_n^2 : ru - st \in Z_n^*\right\}$$

by taking the vector $\begin{pmatrix} r \\ t \end{pmatrix}$ as the first column and a suitable vector $\begin{pmatrix} s \\ u \end{pmatrix}$ as the second column of the matrices.

Proof. Since

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} r & rb + sd \\ t & tb + ud \end{pmatrix}$$

all matrices in a left-coset have the same first column.

Assume that there are matrices with the same first column, $A := \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ and $B := \begin{pmatrix} r & v \\ t & w \end{pmatrix} \in \mathrm{GL}_2(Z_n)$, then

$$A^{-1} = \begin{pmatrix} r & s \\ t & u \end{pmatrix}^{-1} = (ru - st)^{-1} \begin{pmatrix} u & -s \\ -t & r \end{pmatrix}$$

and

$$\begin{aligned} A^{-1}B = (ru-st)^{-1} \begin{pmatrix} u & -s \\ -t & r \end{pmatrix} \begin{pmatrix} r & v \\ t & w \end{pmatrix} &= (ru-st)^{-1} \begin{pmatrix} ru - st & uv - sw \\ -rt + rt & -tv + rw \end{pmatrix} = \\ &= \begin{pmatrix} 1 & (ru-st)^{-1}(uv - sw) \\ 0 & (ru-st)^{-1}(rw - tv) \end{pmatrix} \end{aligned}$$

which is of the form $\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$, where d is a unit element in Z_n. So

$$\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} = A^{-1}B \quad \text{or} \quad A \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} = B.$$

□

For prime-powers $n = p^a$ it is possible to prove that the set of representatives of left-cosets $C_{\bar{G}}(\underline{1})/C_{\bar{G}}(\underline{2})$ can be constructed from the following set of first columns

$$\left\{ (r, t) \in Z_{p^a}^2 \mid p \not| \, r, \text{ or } p \not| \, t \right\}.$$

It is the set of all pairs (r, t) such that at least one of the two components is a unit in Z_{p^a}. Combining this result with the ring isomorphism from 4.5 we derive for instance that there are 8 left-coset representatives $C_{\bar{G}}(\underline{1})/C_{\bar{G}}(\underline{2})$ for $G = \mathrm{Aff}_2(Z_3)$ and 12 left-coset representatives for $G = \mathrm{Aff}_2(Z_4)$ which lead to 96 left-coset representatives for $G = \mathrm{Aff}_2(Z_{12})$.

Coming back to arbitrary n it is easy to realize that

$$C_{\bar{G}}(\underline{2}) = C_{\bar{G}}(\underline{3}) = \ldots = C_{\bar{G}}(\underline{n})$$

since for all $i \in Z_n$

$$\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \begin{pmatrix} i \\ 0 \end{pmatrix} = \begin{pmatrix} i \\ 0 \end{pmatrix}.$$

When computing the pointwise stabilizer $C_{\bar{G}}(\underline{n+1})$ we derive that our Sims-chain is of length $n + 1$ since the only element in $C_{\bar{G}}(\underline{n})$ which stabilizes the pair $(0, 1)$ is the identity-matrix I_2. This can be seen from

$$\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Longleftrightarrow \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Longleftrightarrow b = 0 \text{ and } d = 1.$$

◇

In the next part of this section an iterative method for the construction of a transversal of $k+1$-motives from a transversal of k-motives is described. We had agreed to describe k-motives in $Z_m \times Z_n$ as characteristic functions of k-subsets of $Z_m \times Z_n$. Knowing the characteristic functions of all k-motives, a possible way of constructing all characteristic functions of $k+1$-motives is the following augmentation: Let f be a characteristic function of a k-motive. Find the maximal $i \in \underline{mn}$ such that $f(i) = 1$. The *augmentation* $\mathcal{A}(f)$ consists of all those functions $h: \underline{mn} \to \{0,1\}$ such that $h(j) = f(j)$ for $1 \le j \le i$ and there is exactly one $j > i$ such that $h(j) = 1$. Then each function $h \in \mathcal{A}(f)$ is the characteristic function of a $k+1$-motive. And each characteristic function of a $k+1$-motive belongs to the augmentation of exactly one characteristic function of a k-motive. Furthermore $h(i) \ge f(i)$ for all $i \in \underline{mn}$ and $h > f$ with respect to the lexicographic order.

The next theorem is a special case of *Read's recursion algorithm* (cf. [25]). In this context it is interesting to mention that during the maximum-test we are learning both from positive and from negative results. (For more details see [13].)

7.9 Theorem. *If f is not the canonic representative of the G-orbit $G(f)$ then no h in the augmentation $\mathcal{A}(f)$ is the canonic representative of its orbit $G(h)$.*

Proof. Assume $f: Z_m \times Z_n \to \{0,1\}$ is not a canonic representative of a k-motive, then there exists some $g \in G$ such that $f < f \circ \bar{g}$, i. e. there exists $i_0 \in \underline{mn}$ such that $(f \circ \bar{g})(j) = f(j)$ for $j < i_0$ and $(f \circ \bar{g})(i_0) > f(i_0)$. As a matter of fact $f(\bar{g}(i_0)) = 1$. Furthermore let $i_1 := \max\{i \in \underline{mn} \mid f(i) = 1\}$ then $\bar{g}(i_0) \le i_1$. Moreover $i_0 \le i_1$. (Assume in contrary that $i_0 > i_1$ then the restriction $f|_{\underline{i_1}}$ of f to the set $\underline{i_1}$ equals the restriction $(f \circ \bar{g})|_{\underline{i_1}}$. From the definition of i_1 it is clear that these functions are functions of weight k. Since $i_0 > i_1$ and $(f \circ \bar{g})(i_0) = 1$ the function $f \circ \bar{g}$ is at least of weight $k+1$, which is a contradiction to the main assumption that f and consequently $f \circ \bar{g}$ are characteristic functions of k-motives.) Thus $i_0 \le i_1$ and even $i_0 < i_1$ since $f(i_0) = 0$.

Let h belong to the augmentation of f and let $i_2 > i_1$ be that index where $h(i_2) = 1$ whereas $f(i_2) = 0$. We prove that $h < h \circ \bar{g}$ with the same g as above, hence h is not the canonic representative of its orbit. For doing this we have to consider three cases. Assume first that $\bar{g}^{-1}(i_2) > i_0$ then

$$h(j) = f(j) = (f \circ \bar{g})(j) = (h \circ \bar{g})(j) \text{ for } j < i_0$$

since $i_0 < i_2$ and $\bar{g}(j) \ne i_2$, and

$$h(i_0) = f(i_0) < (f \circ \bar{g})(i_0) = (h \circ \bar{g})(i_0)$$

since $\bar{g}(i_0) \ne i_2$. (Suppose $\bar{g}(i_0) = i_2$ then $i_0 = \bar{g}^{-1}(i_2)$ which is a contradiction to $\bar{g}^{-1}(i_2) > i_0$.)

The second case $\bar{g}^{-1}(i_2) = i_0$ is not possible since $\bar{g}(i_0) \le i_1$ and $i_2 > i_1$. Finally we have to consider the situation that $\bar{g}^{-1}(i_2) < i_0$. Then

$$h(j) = f(j) = (f \circ \bar{g})(j) = (h \circ \bar{g})(j) \text{ for } j < \bar{g}^{-1}(i_2)$$

and

$$h(\bar{g}^{-1}(i_2)) = f(\bar{g}^{-1}(i_2)) = (f \circ \bar{g})(\bar{g}^{-1}(i_2)) = f(i_2) < h(i_2) = (h \circ \bar{g})(\bar{g}^{-1}(i_2)).$$

So in all the possible situations it is proved that $h < h \circ \bar{g}$, so h is not the canonic representative of its orbit and the proof is finished. $\square$

7.10 Example. The following list is a transversal of motives in $Z_3 \times Z_3$. It is computed by using Read's recursion. First the characteristic functions of weight 1 are tested for maximality. Whenever a canonic representative is found the maximum-test is applied to all characteristic functions in its augmentation. Since the characteristic functions are listed in decreasing way the characteristic function $(1, 0, 0, 0, 0, 0, 0, 0, 0)$ is tested first. It is the biggest characteristic function of weight 1 and it is the first representative m_1 in our list. The next lines contain elements m_i of the augmentation $\mathcal{A}(m_{i-1})$ for $2 \leq i \leq 9$. There exist no functions in the augmentation of m_9 and no more functions in the augmentation of m_8. All further functions in the augmentations of m_7 and m_6 are not canonic, so finally the next canonic representative m_{10} is found as an element in the augmentation of m_5, hence it is the characteristic function of a 6-motive. The last three canonic representatives turn out to be characteristic functions of 5-, 3- and 4-motives.

$$\begin{aligned}
m_1 &:= (1, 0, 0, 0, 0, 0, 0, 0, 0)\\
m_2 &:= (1, 1, 0, 0, 0, 0, 0, 0, 0)\\
m_3 &:= (1, 1, 1, 0, 0, 0, 0, 0, 0)\\
m_4 &:= (1, 1, 1, 1, 0, 0, 0, 0, 0)\\
m_5 &:= (1, 1, 1, 1, 1, 0, 0, 0, 0)\\
m_6 &:= (1, 1, 1, 1, 1, 1, 0, 0, 0)\\
m_7 &:= (1, 1, 1, 1, 1, 1, 1, 0, 0)\\
m_8 &:= (1, 1, 1, 1, 1, 1, 1, 1, 0)\\
m_9 &:= (1, 1, 1, 1, 1, 1, 1, 1, 1)\\
m_{10} &:= (1, 1, 1, 1, 1, 0, 1, 0, 0)\\
m_{11} &:= (1, 1, 1, 1, 0, 0, 1, 0, 0)\\
m_{12} &:= (1, 1, 0, 1, 0, 0, 0, 0, 0)\\
m_{13} &:= (1, 1, 0, 1, 1, 0, 0, 0, 0)
\end{aligned}$$

After realizing that only m_3 and m_{12} are canonic representatives in the augmentation of m_2 and that there are no canonic representatives different from m_2 in the augmentation of m_1 we have to test the next characteristic functions of weight 1 for maximality. They all turn out not to be maximal in their orbits.

Of course the empty set is always the canonic representative of the unique 0-motive.

Finally we list all representatives of motives in $Z_4 \times Z_4$. In this example the representatives are not given by their characteristic functions. Instead of writing down the complete function f it is enough to indicate the pre-image $f^{-1}(\{1\})$ for each f. Moreover it is enough to compute all the representatives of k-motives for $1 \leq k \leq 8$ since for $k > 8$ there is a one-to-one connection between the representatives of k- and $16 - k$-orbits.

$\{1\}$, $\{1,2\}$, $\{1,2,3\}$, $\{1,2,3,4\}$, $\{1,2,3,4,5\}$, $\{1,2,3,4,5,6\}$, $\{1,2,3,4,5,6,7\}$, $\{1,2,3,4,5,6,7,8\}$, $\{1,2,3,4,5,6,7,9\}$, $\{1,2,3,4,5,6,7,13\}$, $\{1,2,3,4,5,6,7,14\}$, $\{1,2,3,4,5,6,9\}$, $\{1,2,3,4,5,6,9,10\}$, $\{1,2,3,4,5,6,9,11\}$, $\{1,2,3,4,5,6,9,13\}$, $\{1,2,3,4,5,6,9,14\}$, $\{1,2,3,4,5,6,13\}$, $\{1,2,3,4,5,6,13,14\}$, $\{1,2,3,4,5,6,13,15\}$, $\{1,2,3,4,5,6,13,16\}$, $\{1,2,3,4,5,7\}$, $\{1,2,3,4,5,7,9\}$, $\{1,2,3,4,5,7,9,10\}$, $\{1,2,3,4,5,7,9,11\}$, $\{1,2,3,4,5,7,9,13\}$, $\{1,2,3,4,5,7,9,14\}$, $\{1,2,3,4,5,7,13\}$, $\{1,2,3,4,5,7,13,15\}$, $\{1,2,3,4,5,7,14\}$, $\{1,2,3,4,5,7,14,16\}$, $\{1,2,3,4,5,9\}$, $\{1,2,3,4,5,9,10\}$, $\{1,2,3,4,5,9,10,11\}$, $\{1,2,3,4,5,9,10,14\}$, $\{1,2,3,4,5,9,10,16\}$, $\{1,2,3,4,5,9,11\}$, $\{1,2,3,4,5,9,11,13\}$, $\{1,2,3,4,5,9,11,15\}$, $\{1,2,3,4,5,9,13\}$, $\{1,2,3,4,5,9,14\}$, $\{1,2,3,4,5,9,15\}$, $\{1,2,3,4,5,13\}$, $\{1,2,3,4,5,14\}$, $\{1,2,3,4,9\}$, $\{1,2,3,4,9,10\}$, $\{1,2,3,4,9,10,11\}$, $\{1,2,3,4,9,10,11,12\}$, $\{1,2,3,4,9,11\}$, $\{1,2,3,5\}$, $\{1,2,3,5,6\}$, $\{1,2,3,5,6,7\}$, $\{1,2,3,5,6,7,9\}$, $\{1,2,3,5,6,7,9,10\}$, $\{1,2,3,5,6,7,9,11\}$, $\{1,2,3,5,6,7,9,12\}$, $\{1,2,3,5,6,7,10\}$, $\{1,2,3,5,6,7,10,16\}$, $\{1,2,3,5,6,7,12\}$, $\{1,2,3,5,6,7,12,16\}$, $\{1,2,3,5,6,9\}$, $\{1,2,3,5,6,9,11\}$, $\{1,2,3,5,6,10\}$, $\{1,2,3,5,6,10,11\}$, $\{1,2,3,5,6,10,15\}$, $\{1,2,3,5,6,10,16\}$, $\{1,2,3,5,6,11\}$, $\{1,2,3,5,6,14\}$, $\{1,2,3,5,6,14,15\}$, $\{1,2,3,5,7\}$, $\{1,2,3,5,7,9\}$, $\{1,2,3,5,7,9,10\}$, $\{1,2,3,5,7,9,10,11\}$, $\{1,2,3,5,7,9,11\}$, $\{1,2,3,5,7,9,11,12\}$, $\{1,2,3,5,7,9,12\}$, $\{1,2,3,5,7,10\}$, $\{1,2,3,5,7,12\}$, $\{1,2,3,5,7,13\}$, $\{1,2,3,5,7,13,15\}$, $\{1,2,3,5,7,14\}$, $\{1,2,3,5,9\}$, $\{1,2,3,5,9,11\}$, $\{1,2,3,5,10\}$, $\{1,2,3,5,10,15\}$, $\{1,2,3,5,12\}$, $\{1,2,3,5,12,13\}$, $\{1,2,3,5,14\}$, $\{1,2,3,5,15\}$, $\{1,2,3,9\}$, $\{1,2,3,9,10\}$, $\{1,2,3,9,10,11\}$, $\{1,2,3,9,11\}$, $\{1,2,3,10\}$, $\{1,2,5\}$, $\{1,2,5,6\}$, $\{1,2,5,7\}$, $\{1,2,5,7,10\}$, $\{1,2,5,7,10,11\}$, $\{1,2,5,16\}$, $\{1,2,9\}$, $\{1,2,9,10\}$, $\{1,2,9,12\}$, $\{1,3\}$, $\{1,3,9\}$, $\{1,3,9,11\}$

◇

In situations when the list of orbit representatives is too long, or when the order of the acting group is big such that the computation of a transversal takes too long time, then it is useful and it makes sense to apply probabilistic methods for generating orbit representatives uniformly at random. I. e., for any given orbit the probability that a generated representative belongs to this orbit does not depend on the special choice of the orbit. In other words, for all orbits this probability is the same and it is given as the fraction 1 divided by the number of different orbits. This way it is possible to generate in very short time huge lists of unprejudiced representatives. The method of this random generation is known as the *Dixon-Wilf-algorithm* (cf. [6]) which was originally designed for the random generation of linear graphs. It can be formulated for an arbitrary group action as follows: (The reader should remember the definition of the conjugacy classes of elements of a group G given in the second item of 3.9.)

7.11. The Dixon-Wilf-algorithm. *Let ${}_GX$ be a finite group action. Choose a conjugacy class C of G with the probability*

$$p(C) := \frac{|C|\,|X_g|}{|G|\,|G\backslash\backslash X|}, \text{ for an arbitrary } g \in C.$$

Pick any $g \in C$ and determine at random a fixed point x of g. Then the probability that x belongs to a given orbit $\omega \in G\backslash\backslash X$ is equal to $1/|G\backslash\backslash X|$, i. e. it does not depend on the special choice of ω.

Proof. Let $C_1, \ldots, C_r$ be the conjugacy classes of G with representatives $g_i \in C_i$. From 3.13 we deduce that

$$\sum_{i=1}^{r} p(C_i) = \frac{\sum_{i=1}^{r} |C_i|\,|X_{g_i}|}{\sum_{g\in G} |X_g|} = 1,$$

which means that $p(.)$ is a probability function. Then for an arbitrary orbit $\omega \in G\backslash\backslash X$ the following is true:

$$p(x \in \omega) = \sum_{i=1}^{r} p(C_i) p(x \in X_{g_i} \cap \omega) = \sum_{i=1}^{r} p(C_i) \frac{|X_{g_i} \cap \omega|}{|X_{g_i}|} =$$

$$= \sum_{i=1}^{r} \frac{|C_i|\,|X_{g_i}|}{|G|\,|G\backslash\backslash X|} \frac{|X_{g_i} \cap \omega|}{|X_{g_i}|} = \frac{1}{|G|\,|G\backslash\backslash X|} \sum_{i=1}^{r} |C_i|\,|X_{g_i} \cap \omega| = \frac{1}{|G|\,|G\backslash\backslash X|} \sum_{g\in G} |X_g \cap \omega|\,.$$

The last equality holds because $X_{hgh^{-1}} = hX_g := \{hx \mid x \in X_g\}$ from which we deduce that $|X_g \cap \omega| = |X_{hgh^{-1}} \cap \omega|$ for all $g, h \in G$ and for any orbit $\omega \in G\backslash\backslash X$.

Finally the last sum is equal to $|G|$ since ω is a G-orbit and from 3.11 it follows that elements of the same orbit have conjugate stabilizers. Thus finally we get

$$\sum_{g\in G} |X_g \cap \omega| = \sum_{g\in G} \sum_{x\in X_g\cap\omega} 1 = \sum_{x\in\omega} \sum_{g\in G_x} 1 = \sum_{x\in\omega} |G_x| = |G_x|\,|\omega| = |G_x|\,|G(x)| = |G|\,,$$

which finishes the proof. $\square$

For the random generation of motives we have to find a formulation of this algorithm for group actions of the form 3.10. (The reader should remember that $c(\bar{h})$ denotes the number of cycles in the cycle decomposition of the permutation $\bar{h}$.)

7.12 Corollary. *Let ${}_GY^X$ be the finite group action introduced in 3.10. Choose a conjugacy class C of G with the probability*

$$p(C) := \frac{|C|\,|Y|^{c(\bar{h})}}{\sum_{g\in G} |Y|^{c(\bar{g})}}, \text{ for an arbitrary } h \in C.$$

Pick any $g \in C$ and determine at random a fixed point $f \in Y^X$ of g. Then the output of this algorithm is distributed uniformly at random over all G-orbits on Y^X.

Finally for the random generation of k-motives we should find a weighted version of the Dixon-Wilf-algorithm with weights in a commutative ring R such that $\mathbb{Q}$ is a sub-ring of R.

7.13 Corollary. *Let ${}_GX$ be a finite group action and let $w\colon X \to R$ be a weight function which is constant on each G-orbit $\omega \in G\backslash\backslash X$. In order to generate orbit representatives of weight r uniformly at random choose a conjugacy class C of G with the probability*

$$p(C) := \frac{|C|\,|w^{-1}(\{r\})_g|}{|G|\,|G\backslash\backslash w^{-1}(\{r\})|}, \text{ for an arbitrary } g \in C.$$

Pick any $g \in C$ and determine at random a fixed point x of g of weight r.

Combining the last two corollaries it is possible to implement the Dixon-Wilf-algorithm for generating representatives of k-motives uniformly at random. The conjugacy classes of a group G or their representatives can be computed for instance by using the computer algebra system GAP (cf. [29]). Actually determining the conjugacy classes in G is just the problem of finding representatives under the action of conjugation on G (cf. the second item of 3.9). In order to minimize the amount of work before the algorithm actually starts to generate k-motives it is useful to start the generation at once after having computed the information on the first conjugacy class, and evaluate further conjugacy classes and their probabilities only if required. This means we have to compute $p(C_i)$ only if the random number (lying in $[0,1[$) determining which conjugacy class to choose exceeds $\sum_{j=1}^{i-1} p(C_j)$. The efficiency of this method heavily depends on the numbering of the conjugacy classes. Consequently this numbering should be chosen such that $p(C_i) \geq p(C_{i+1})$ which usually leads to $C_1 = \{\mathrm{id}\}$.

Most of these algorithms for computing cycle indices and enumerating motives, for the construction of transversals of k-motives and for the random generation of k-motives are implemented in the computer algebra system SYMMETRICA [32]. The special C-code for handling motives can be loaded from the author's homepage [12].

Acknowledgement: The author wants to thank Prof. Moisei Boroda for the invitation to publish this paper in Musikometrika and for many useful suggestions and hints while preparing this article. Furthermore he wants to express his thanks to Dr. Thomas Noll who established the contact with Prof. Boroda.

References

[1] C.J. Colbourn and R.C. Read. Orderly algorithms for generating restricted classes of graphs. *Journal of Graph Theory*, 3:187 – 195, 1979.

[2] C.J. Colbourn and R.C. Read. Orderly algorithms for graph generation. *Int. J. Comput. Math.*, 7:167 – 172, 1979.

[3] C. Dahlhaus and H.H. Eggebrecht, editors. *Brockhaus-Riemann-Musiklexikon*. Brockhaus, Wiesbaden, 1978/79. ISBN 3-7653-0303-8.

[4] N.G. de Bruijn. Pólya's theory of counting. In E.F. Beckenbach, editor, *Applied Combinatorial Mathematics*, chapter 5, pages 144 – 184. Wiley, New York, 1964.

[5] N.G. de Bruijn. Color patterns that are invariant under a given permutation of the colors. *Journal of Combinatorial Theory*, 2:418 – 421, 1967.

[6] J.D. Dixon and H.S. Wilf. The random selection of unlabeled graphs. *Journal of Algorithms*, 4:205 – 213, 1983.

[7] H. Fripertinger. Untersuchung über die Anzahl verschiedener Intervalle, Akkorde, Tonreihen und anderer musikalischer Objekte in n-Ton Musik. Master's thesis, Hochschule für Musik und Darstellende Kunst, Graz, 1991.

[8] H. Fripertinger. Enumeration in Musical Theory. *Séminaire Lotharingien de Combinatoire*, 476/S-26:29 – 42, 1992. ISSN 0755-3390.

[9] H. Fripertinger. Endliche Gruppenaktionen auf Funktionenmengen. Das Lemma von Burnside — Repräsentantenkonstruktionen — Anwendungen in der Musiktheorie. *Bayreuther Mathematische Schriften*, 45:19 – 135, 1993. ISSN 0172-1062.

[10] H. Fripertinger. *Endliche Gruppenaktionen in Funktionenmengen. Das Lemma von Burnside — Repräsentantenkonstruktionen — Anwendungen in der Musiktheorie.* PhD thesis, Karl-Franzens-Universität Graz, 1993.

[11] H. Fripertinger. Cycle Indices of Linear, Affine and Projective Groups. *Linear Algebra and Its Applications*, 263:133 – 156, 1997.

[12] H. Fripertinger's homepage `http://bedvgm.kfunigraz.ac.at:8001/frib/`.

[13] R. Grund. Symmetrieklassen von Abbildungen und die Konstruktion von diskreten Strukturen. *Bayreuther Mathematische Schriften*, 31:19 – 54, 1990. ISSN 0172-1062.

[14] M.A. Harrison and R.G. High. On the Cycle Index of a Product of Permutation Groups. *Journal of Combinatorial Theory*, 4:277 – 299, 1968.

[15] M.A. Harrison. On the classification of Boolean functions by the general linear and affine groups. *J. Soc. Appl. Ind. Math.*, 12:285 – 299, 1964.

[16] A. Kerber. *Algebraic Combinatorics via Finite Group Actions.* B.I. Wissenschaftsverlag, Mannheim, Wien, Zürich, 1991. ISBN 3-411-14521-8.

[17] A. Kerber. *Applied Finite Group Actions*, volume 19 of *Algorithms and Combinatorics.* Springer, Berlin, Heidelberg, New York, 1999. ISBN 3-540-65941-2.

[18] J.Chr. Lobe. *Compositions-Lehre oder umfassende Theorie von der thematischen Arbeit und den modernen Instrumentalformen.* Voigt, Weimar, 1844.

[19] A.B. Marx. *Die Lehre von der musikalischen Komposition.* Breitkopf und Härtel, Leipzig, 1837.

[20] G. Mazzola. *Geometrie der Töne*. Birkhäuser, Basel, Boston, Berlin, 1990. ISBN 3-7643-2353-1.

[21] K. Meyberg. *Algebra. Teil 1.* Carl Hanser Verlag, München, Wien, 2nd edition, 1980.

[22] I. Niven, H.S. Zuckerman, and H.L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York etc., 5th edition, 1991. ISBN 0-471-62546-9, ISBN 0-471-54600-3.

[23] G. Pólya and R.C. Read. *Combinatorial Enumeration of Groups, Graphs and Chemical Compounds*. Springer Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo, 1987. ISBN 0-387-96413-4 or ISBN 3-540-96413-4.

[24] G. Pólya. Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen. *Acta Mathematica*, 68:145 – 254, 1937.

[25] R.C. Read. Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations. *Ann. Discrete Mathematics*, 2:107 – 120, 1978.

[26] R.C. Read. Combinatorial problems in the theory of music. *Discrete Mathematics*, 167-168(1-3):543–551, 1997.

[27] D.L. Reiner. Enumeration in Music Theory. *Amer. Math. Monthly*, 92:51 – 54, 1985.

[28] H. Riemann. *System der musikalischen Rhythmik und Metrik*. Breitkopf und Härtel, Leipzig, 1903.

[29] M. Schönert et al. *GAP – Groups, Algorithms, and Programming*. Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, fifth edition, 1995.

[30] C.C. Sims. Computational methods in the study of permutation groups. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 169 – 183. Proc, Conf. Oxford 1967, Pergamon Press, 1970.

[31] C.C. Sims. Computation with permutation groups. In S.R. Petrick, editor, *Proceedings of the Second Symposium on Symbolic and Algebraic Manipulation, Los Angeles 1971*, pages 23 – 28. Assoc. Comput. Mach., 1971.

[32] SYMMETRICA. A program system devoted to representation theory, invariant theory and combinatorics of finite symmetric groups and related classes of groups. Copyright by “Lehrstuhl II für Mathematik, Universität Bayreuth, 95440 Bayreuth”. `http://www.mathe2.uni-bayreuth.de/axel/symneu_engl.html`.

[33] B.L. van der Waerden. *Algebra. Volume I. Based in part on lectures by E. Artin and E. Noether.* Springer-Verlag, New York etc., 1991. ISBN 0-387-97424-5.

[34] Wan-Di Wei and Ju-Yong Xu. Cycle index of direct product of permutation groups and number of equivalence classes of subsets of Z_v. *Discrete Mathematics*, 123:179 – 188, 1993.

Harald Fripertinger
Institut für Mathematik
Karl Franzens Universität Graz
Heinrichstr. 36/4
A–8010 Graz, AUSTRIA
harald.fripertinger@kfunigraz.ac.at