2

Homometry and the Phase Retrieval Problem

Summary. This chapter studies in depth the notion of homometry, i.e. having identical internal shape, as seen from Fourier space, where homometry can be seen at a glance by the size (or magnitude) of the Fourier coefficients. Finding homometric distributions is then a question of choosing the phases of these coefficients, hence this problem is often called *phase retrieval* in the literature. Such a choice of phases is summed up in the objects called *spectral units*, which connect homometric sets together. I included the original proof of the one difficult theorem of this book (Theorem 2.10), which non-mathematicians are quite welcome to skip. Some generalisations of the hexachord theorem are given, followed by the few easy results on higher-order homometry which deserve some room in this book because they rely heavily on DFT machinery. An original method for phase-retrieval with singular distributions (the difficult case) is also given. Some knowledge of basic linear algebra may help in this chapter.

We recall the definition of homometry and its characterisation given above: *Two subsets (or distributions) are homometric iff they share the same intervallic distribution, or equivalently iff they have the same magnitude for all their Fourier coefficients:*

$$\mathrm{IC}(A) = \mathrm{IC}(B) \iff |\mathscr{F}_A| = |\mathscr{F}_B|.$$

See the smallest example in Fig. 2.1 with $\{0,1,3,7\},\{0,1,4,6\}$ and of course their retrogrades. Their intervallic function is $(4,1,1,1,1,1,2,1,1,1,1,1)$.

Though these pc-sets do appear in 20^{th} century music (Elliot Carter's first quartet for instance), they had never been used as systematically as in Tom Johnson's *Intervals* (2013). The edges of the graph in Fig. 2.3 are the 48 homometric tetrachords, organised around common tritones for the eponymous piece. The composer navigates between adjacent tetrachords, each tritone being completed into the four distinct forms (up to transposition) of the tetrachords, as can be seen on the first line of the score in Fig. 2.2 (for instance 2,8 can be completed by 0,3 or 0,6 or 0,9 or 6,9). The other pieces in *Intervals*, seconds, thirds and so forth, similarly explore the same collection of 48 pc-sets with focus on seconds, minor thirds, etc –, since these tetrachords contain all possible intervals. The non-trivial homometry is clearly heard, the music spells the common tritones in the four different pc-sets classified in Fig. 2.1. Since the awakening of his interest in homometric sets, Johnson has worked on

E. Amiot, *Music Through Fourier Space*, Computational Music Science,
DOI 10.1007/978-3-319-45581-5_2

$$\begin{pmatrix} 0 & 1 & 3 & 7 \\ 0 & 1 & 4 & 6 \\ 0 & 2 & 5 & 6 \\ 0 & 4 & 6 & 7 \end{pmatrix}$$

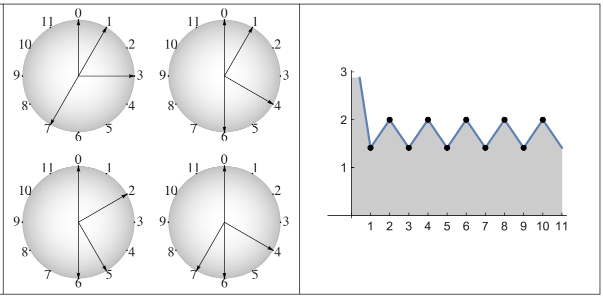


Fig. 2.1. Homometric quadruplets

other compositions using them, notably with homometric heptachords in the septet "Trichords et tetrachords" (2014).

Fig. 2.2. Between common tritones

The Z-relation, as defined by Alan Forte [42] but also previously [49], is homometry in $\mathbb{Z}_{12}$, minus the trivial case of T/I related pc-sets. Non-trivially Z-related sets exist in $\mathbb{Z}_n$ for all $n \geqslant 12$, and also when $n = 8$ or 10.[1]

This notion originated in crystallography (see [75]) and addresses the question of whether an interference picture (say of a crystal under X-ray lighting) provides enough information to identify the geometric structure of the object.[2] The question of finding all (or at least some) homometric sets boils down to finding the *phase* of the Fourier coefficients, since their *magnitude* is common to all homometric distributions. Hence it is often called *the Phase Retrieval Problem* in the literature. Most of this chapter is adapted and simplified from [64, 2] which discuss the finer aspects of this problem and some possible generalisations, especially to non-discrete and/or non commutative groups. We will allude to some of these developments in Section 2.2.1.

[1] Examples in $\mathbb{Z}_n, n \geqslant 12$ are $A = \{0,1,2,6,8,11\}, B = \{0,1,6,7,9,11\}$.

[2] Interferences of lightwaves images are made by summing exponential waves with varying parameters, and the light intensity on the resulting picture varies proportionally to the magnitude of a Fourier transform.

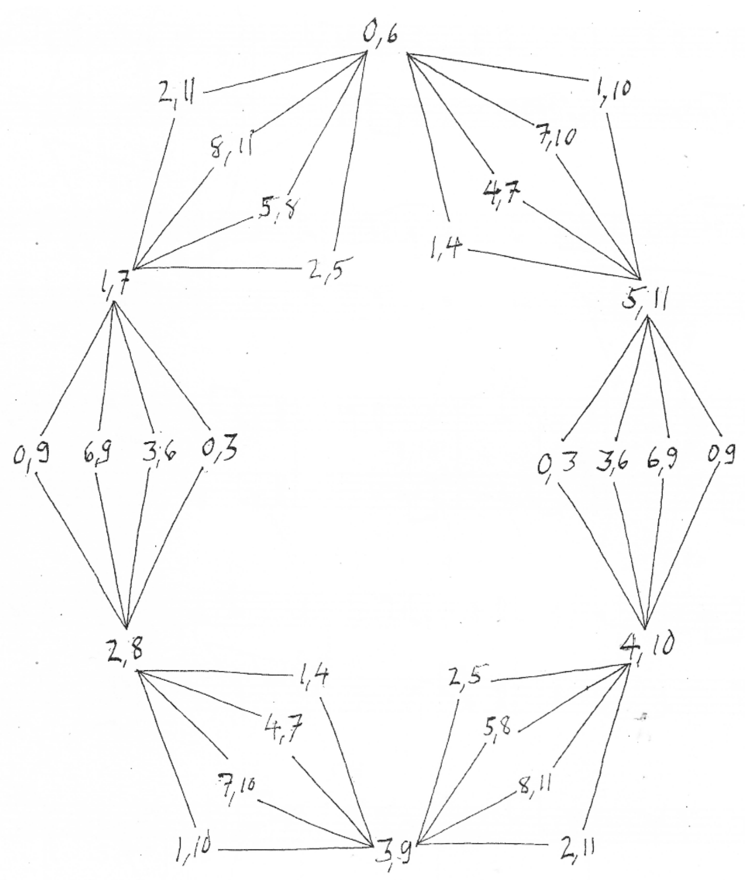


Fig. 2.3. T/I images of 0146 and 0137

2.1 Spectral units

In the most general setting, for a distribution f (recall that this generalizes the characteristic function of a pc-set, for instance) the intervallic function is the convolution product $d^2(f) = f * I(f)$, where $I(f)$ is the inversion of f, i.e. f read backwards, e.g. the traditional musical inversion in the case of a pc-set. This map is called the *Patterson function*; the notation d^2 probably means 'mutual *d*istances between points' for crystallographs. From Lewin's Lemma 1.25 we know that the Patterson function is completely determined by the Fourier transform, since

$$\widehat{d^2(f)} = |\widehat{f}|^2.$$

In this chapter, we will focus on the magnitude of the Fourier transform $|\widehat{f}|$ instead of $d^2(f)$. This is a simpler method, which would fail if $\mathbb{Z}_n$ were to be replaced by a non-commutative group since Fourier analysis is much more complicated in such contexts, but this still works in discrete and locally compact abelian groups as we will point out in Section 2.2.1. For the sake of simplicity, we stick to $\mathbb{Z}_n$ in the present section and refer the more curious readers to the bibliography.

2.1.1 Moving between two homometric distributions

Definition 2.1. *A distribution $u \in \mathbb{C}^{\mathbb{Z}_n} \approx \mathbb{C}^n$ is a* spectral unit *iff its Fourier transform is unimodular:*

$$\forall t \in \mathbb{Z}_n \ |\widehat{u}(t)| = 1.$$

We will denote the set of spectral units on $\mathbb{Z}_n$ as $\mathscr{U}_n$ (or $\mathscr{U}_n(K)$ if we restrict ourselves to coefficients in a subfield $K \subset \mathbb{C}$).

Theorem 2.2. *Two distributions f, g in $\mathbb{C}^{\mathbb{Z}_n} \approx \mathbb{C}^n$ are homometric iff there exists a spectral unit u such that $f = u * g$.*

Proof. This equation is equivalent to $\exists u \in \mathscr{U}_n,\ \widehat{f} = \widehat{u} \times \widehat{g}$ (termwise), which is itself equivalent to $|\widehat{f}| = 1 \times |\widehat{g}|$, i.e. to the homometry of f, g.

Proposition 2.3. *$(\mathscr{U}_n, *)$ is an abelian group.*

Proof. It is the image of the torus $\big((S^1)^n, \times\big)$ by inverse Fourier transform, which is a morphism as we have already established.

Since the Fourier transform is also an isometry (for a $\| \ \|_2$ norm, see Theorem 1.8), this means that the phase retrieval problem is solved and that the set of distributions homometric with f is simply $\mathscr{U}_n * f = \{u * f, u \in \mathscr{U}_n\}$, each orbit exhibiting the shape of a n-dimensional torus. This is true in a way, but deceptively, because we have chosen the smooth setting of the vector space $\mathbb{C}^n$ of *all* distributions. If one wishes to retrieve homometric **pc-sets**, then one must pick in the infinite orbit only those few distributions which are characteristic functions, i.e. with values in $\{0,1\}$. Despite considerable efforts, there is still no known good general method for doing this. Computational methods are by and large the best practical tools but the complexity of their calculations is exponential.

Example 2.4. Consider again the most famous (non-trivial) homometric pc-sets in $\mathbb{Z}_{12}, A = \{0,1,4,6\}$ and $B = \{0,1,3,7\}$.

The spectral unit 'connecting' those two pc-sets, i.e. $\mathbf{1}_B = \mathbf{1}_A * u$, is easily computed using techniques developed in the next . In this case, it is unique:

$$u = (\frac{1}{4}, \frac{1}{4}, 0, \frac{1}{4}, -\frac{1}{4}, -\frac{1}{2}, \frac{1}{4}, \frac{1}{4}, 0, \frac{1}{4}, -\frac{1}{4}, \frac{1}{2}).$$

Since one pc-set is the affine image of the other[3], the Fourier coefficients are actually permutated, following Theorem 1.19. The Fourier coefficients of u are unit-sized as expected:

$$\widehat{u} = \left(1, e^{\frac{i\pi}{6}}, e^{-\frac{i\pi}{3}}, i, 1, e^{\frac{5i\pi}{6}}, -1, e^{-\frac{5i\pi}{6}}, 1, -i, e^{\frac{i\pi}{3}}, e^{-\frac{i\pi}{6}}\right).$$

[3] In $\mathbb{Z}_{12}$, $\{0,1,3,7\} = 5 \times \{0,1,4,6\} - 5$.

2.1.2 Chosen spectral units

The fact that a distribution only takes values 0 or 1 yields *some* information about possible spectral units between this distribution and another homometric one; and we can refine Theorem 2.2:

Theorem 2.5. *If two pc-sets A, B are homometric then there exists a spectral unit u* with rational coefficients *such that $\mathbf{1}_A = u * \mathbf{1}_B$.*

This is an easy case of the more difficult following theorem ([76]):

Theorem 2.6 (Rosenblatt).
Two distributions f, g in $\mathbb{Q}^{\mathbb{Z}_n} \approx \mathbb{Q}^n$ are homometric iff there exists a spectral unit u with values in $\mathbb{Q}$ *such that $f = u * g$.*

This statement is fairly obvious when one distribution is invertible for the convolution product $*$, since the coefficients of the inverse must stay in the same field (actually Rosenblatt's theorem is given for any subfield of $\mathbb{C}$). The difficulty is in the singular case (again Lewin's 'special cases'!) and we will see below that it remains so for higher-level homometry.

Another simple case provides what is probably the most complicated proof of the hexachord theorem so far (no challenge intended):

Proposition 2.7. *Let $h = (\frac{2}{n} - 1, \frac{2}{n}, \frac{2}{n}, \dots)$. Then h is a spectral unit*[4]*, and when n is even, for any set A with $n/2$ elements, $h * \mathbf{1}_A$ is equal to the characteristic function $\mathbf{1}_{\mathbb{Z}_n \setminus A}$ of the complement of A.*

Proof. Left as an exercise.

The question of non-invertible, or singular, distributions, is studied in depth in Section 3.1. For the time being, it will suffice to make a simple observation: if f and g are homometric and $\widehat{f}(k) = 0$ (hence $\widehat{g}(k) = 0$ too) then the value of $\widehat{u}(k)$ can be chosen arbitrarily on the unit circle, with $f = u * g$ in k. In this case there may exist infinitely many different spectral units connecting f and g, even with restrictions on the coefficients. Some examples will be given below after we have developed the matricial technique for computation of spectral units.

Remember the algebra of circulating matrixes $\mathscr{C}_n(\mathbb{C})$ in section 1.2.3. We have the following characterisation of spectral units in this setting (recall that the eigenvalues of the matrix are simply the Fourier coefficients of the distribution listed in its first column):

Proposition 2.8. *$u \in \mathbb{C}^n$ is a spectral unit $\iff$ its circulating matrix has all its eigenvalues on the unit circle. The group of such matrixes is the intersection of $\mathscr{C}_n(\mathbb{C})$ and the group of unitary matrixes (i.e. satisfying $U^{-1} = \overline{U}^T$).*

[4] Using the language of circulating matrixes which appear again *infra*, the matrix of h is $\mathscr{H} = \frac{2}{n}\begin{pmatrix} 1 & 1 & \dots & 1 \\ \vdots & \ddots & & \vdots \\ 1 & \dots & \dots & 1 \end{pmatrix} - I_n$ and its eigenvalues are 1 and -1, this last repeated $n-1$ times.

This makes even more obvious the isomorphism between $\mathscr{U}_n$ and the torus $\mathbb{T}_n$, which appears by diagonalisation. The whole group of rational (or real) spectral unit matrixes can be described implicitly by the equations

$$(E_k) : \sum_{j=0}^{n-1} a_j a_{j+k} = 0, k = 1 \dots \lfloor \frac{n-1}{2} \rfloor \text{ and } \sum_j a_j^2 = 1$$

where indices are taken modulo n. For instance, for $n = 3$ the group of *real* spectral units $\mathscr{U}_3(\mathbb{R})$ is the pair of parallel circles described by the matrixes $\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}$ with $a^2 + b^2 + c^2 = 1$ and $a + b + c = \pm 1$.

Now the computation of a spectral unit between two given homometric distributions is straightforward:[5]

Proposition 2.9.

$$f = u * g \iff \mathscr{F} = \mathscr{U} \times \mathscr{G},$$

where $\mathscr{X}$ stands for the circulating matrix associated with distribution x.

In the example given above, we solved the equation in circulating matrixes (only the first column is provided)

$$\begin{pmatrix} 1 & \dots \\ 1 & \dots \\ 0 & \dots \\ 1 & \dots \\ 0 & \dots \\ 0 & \dots \\ 0 & \dots \\ 1 & \dots \\ 0 & \dots \\ 0 & \dots \\ 0 & \dots \\ 0 & \dots \end{pmatrix} = \mathscr{U} \times \begin{pmatrix} 1 & \dots \\ 1 & \dots \\ 0 & \dots \\ 0 & \dots \\ 1 & \dots \\ 0 & \dots \\ 1 & \dots \\ 0 & \dots \\ 0 & \dots \\ 0 & \dots \\ 0 & \dots \\ 0 & \dots \end{pmatrix}$$

which is done by inverting the right-hand matrix given.

2.1.3 Rational spectral units with finite order

Musical transposition is very simply and universally achieved by convolution with the spectral unit $j = (0,1,0,0,0,0,0,0,0,0,0,0)$ and its powers, e.g. E♭ minor triad is obtained from $\mathscr{S}$ by the matrix product $\mathscr{J}^3\mathscr{S}$, or equivalently $j^3 * s = (0,0,0,1,0,0,1,0,0,0,1,0)$. It is, however, much less straightforward to achieve *inversion* by way of a spectral unit.

Let $\mathscr{S}$ be the matrix of distribution $s = (1,0,0,1,0,0,0,1,0,0,0,0)$ (the C minor triad) and $\mathscr{T}$ defined by $t = (1,0,0,0,1,0,0,1,0,0,0,0)$ (the C major triad). From C major to C minor we must have $\mathscr{U} = \mathscr{S}^{-1}\mathscr{T}$, which yields

$$u = \frac{1}{15}(7,4,-2,1,7,4,-2,1,-8,4,-2,1).$$

[5] With the proviso made above in the case of distributions with some nil Fourier coefficients, which can still be settled but via the arbitrary choice of the corresponding Fourier coefficients in $\widehat{u}$. See Example 2.23.

Contrarily to transposition, the spectral unit achieving inversion *depends on the inverted subset*[6] (or distribution), and even more strangely, in general, such units are of infinite order in the group of units, as in the example above.

On the other hand, iterating convolution by the spectral unit connecting $\{0,1,3,7\}$ and $\{0,1,4,6\}$, which has finite order (all its Fourier coefficient are 12^{th} roots of unity), yields twelve different distributions, eight of which are genuine pc-sets:

$$\begin{bmatrix}
1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & 1 & \frac{1}{2} & \frac{1}{2} & -1 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
\frac{1}{2} & \frac{1}{2} & -1 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 1 & \frac{1}{2} & \frac{1}{2} & -1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
\frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 1 & \frac{1}{2} & \frac{1}{2} & -1 & \frac{1}{2} & \frac{1}{2} & 0
\end{bmatrix}$$

One can interpret the first four distributions in this table as splitting the minor third-down transposition into three identical moves, which are *not* transpositions (the first turns 0137 into 0146, and the next distribution is not a genuine pc-set), e.g. we have defined a non-trivial cubic root of the minor third transposition.

Since the study of rational spectral units with infinite order does not look too promising, it is natural to wonder about rational spectral units with **finite** order. Their set is a subgroup of $\mathscr{U}_n(\mathbb{Q})$. Since there are already, for instance, infinitely many matrixes 2×2 with rational coefficients and finite order, the following result is noteworthy. Moreover it is a practical way for exploring homometric classes in $\mathbb{Z}_n$, when n is not too large (though brute force search may seem more efficient, until more refined applications of this theorem are implemented).

Theorem 2.10. *Any spectral unit (represented as a rational circulating matrix) with finite order is completely determined by the values of the subset $\{\xi_j, j \mid n\}$ of its eigenvalues, the possibilities being listed* infra*:*

- $\xi_0 = \pm 1$*;*
- *When n is odd, for all $j \mid n$, ξ_j OR $-\xi_j$ is any power of* $\mathrm{e}^{2\mathrm{i}j\pi/n}$.
- *When n is even, ξ_j is any power of* $\mathrm{e}^{2\mathrm{i}j\pi/n}$ *if n/j is even, or any power of* $\mathrm{e}^{\mathrm{i}j\pi/n}$ *if n/j is odd.*

Then for any k coprime with n, $\xi_{kj} = \xi_j^k$ (or $-\xi_j^k$ in the specific case when ξ_j is a $\mathrm{e}^{(2p_j+1)\mathrm{i}\pi/n}$ *and k is even).*

As a corollary, we have the structure of the whole group:

---

[6] Matricially, one can write $\mathscr{U} = \mathscr{S}(\mathscr{S}^T)^{-1}$ if $\mathscr{S}$ is not singular.

Theorem 2.11. *The group of all rational spectral units with finite order in dimension n is isomorphic to the product of cyclic groups* $\prod_{d|n} \mathbb{Z}_{\mathrm{lcm}(2,d)}$.

These theorems may perhaps enable computation of all spectral units with, say, small denominators, which occur in practice for homometric subsets of $\mathbb{Z}_n$ and may be a provable condition in general cases.

For instance, for $n = 12$ the structure of this group is $\mathbb{Z}_{12} \times (\mathbb{Z}_6)^2 \times \mathbb{Z}_4 \times (\mathbb{Z}_2)^2$, with 6,912 elements. The denominators of the values of these spectral units are all divisors of 12, a typical one being

$$u = \big(-\frac{1}{12}, -\frac{1}{12}, 0, \frac{1}{4}, -\frac{1}{12}, -\frac{1}{3}, -\frac{3}{4}, \frac{1}{4}, -\frac{1}{3}, -\frac{1}{12}, \frac{1}{4}, 0\big).$$

The proof is quite involved, and non-mathematically inclined readers are invited to skip it.

Proof. We begin by proving two intermediary results, which are contained in the main theorem:

Lemma 2.12. *If $\mathscr{U} \in \mathscr{C}_n$ is a spectral unit (matrix) with finite order and n is even, then all its eigenvalues are n^{th} roots of unity. If n is odd, then the eigenvalues are either n^{th} roots of unity or their opposites (i.e. they are $2n^{th}$ roots of unity).*

This stems from a more precise condition:

Lemma 2.13. *If $\mathscr{U} \in \mathscr{C}_n$ is a rational spectral unit with finite order and n is even, then for all k coprime with n and any Fourier coefficient (= eigenvalue of $\mathscr{U}$) $\xi_j, j \neq 0$, one has $\xi_{kj} = {\xi_j}^k$. For $j = 0$ we have $\xi_0 = \pm 1$.*

The same condition stands when n is odd, with the exception of the case when ξ_j is a $\mathrm{e}^{(2p_j+1)\mathrm{i}\pi/n}$ and k is even: then $\xi_{kj} = -{\xi_j}^k$.

For instance for $k = -1$, this gives the condition that the last Fourier coefficients must be the conjugates of the first ones (thus ensuring that $\mathscr{U}$ is real valued). More generally, given one coefficient ξ_j we know all coefficients with indexes *associated* with j.

Throughout, $\mathscr{U}$ is a circulating matrix which is unitary ($\mathscr{U}^{-1} = {}^t\overline{\mathscr{U}}$), has finite order ($\mathscr{U}^m = I_n$ for some m), and has rational elements. Hence its eigenvalues have magnitude 1 (they are m^{th} roots of unity), and, as discussed above,xx $\mathscr{U}$ diagonalises into $\mathrm{Diag}(\xi_0, \xi_1, \dots \xi_{n-1})$ where the eigenvalues ξ_j are also the Fourier coefficients of the first column of $\mathscr{U}$, seen as a map from $\mathbb{Z}_n$ to $\mathbb{C}$.

We begin by proving an alternative, simpler form of Lemma 2.12, stating that $m = n$ or $m = 2n$:

Lemma 2.14. *All eigenvalues of $\mathscr{U}$ are n^{th} roots of unity for even n, and $2n^{th}$ roots of unity for odd n.*

Already this establishes that the group we are looking for is finite, a non-trivial fact.

Proof. As we assumed that $\mathscr{U}$ has finite order, all its eigenvalues are roots of unity. Moreover, as $\mathscr{U} = P(\mathscr{J}), P \in \mathbb{Q}[X]$ is a polynomial in the matrix $\mathscr{J}$, whose eigenvalues are the n^{th} roots of unity, the eigenvalues of $\mathscr{U}$ are polynomials in these roots, i.e. $\xi_k = P(\mathrm{e}^{2\mathrm{i}k\pi/n})$, and hence lie in the cyclotomic field $\mathbb{Q}_n = \mathbb{Q}[\mathrm{e}^{2\mathrm{i}\pi/n}]$. We need the following:

Lemma 2.15. *Let ξ be a m^{th} root of unity belonging to the cyclotomic field $\mathbb{Q}_n$.*

$$\text{Then} \begin{cases} \xi^n = 1 & \text{when } n \text{ is even,} \\ \xi^{2n} = 1 & \text{when } n \text{ is odd.} \end{cases}$$

In other words, if $\mathbb{Q}_m \subset \mathbb{Q}_n$ then m is a divisor of n or $2n$, according to whether n is even or odd.[7]

Let ξ be such a unit root (say, any eigenvalue of $\mathscr{U}$). Let m be the order of ξ, i.e. the smallest integer satisfying $\xi^m = 1$; we know that ξ, primitive root of order m, generates $\mathbb{Q}_m$. As $\xi \in \mathbb{Q}[\mathrm{e}^{2\mathrm{i}\pi/n}]$ too, $\mathbb{Q}_m \subset \mathbb{Q}_n$. This does not obviously preclude $m > n$. We need still another:

Lemma 2.16. *The multiplicative group of elements of finite order in $\mathbb{Q}_n$ is cyclic.*[8]

This is because given two elements ξ, ξ' with orders m, m' it is possible to construct an element of order $\mathrm{lcm}(m, m')$ (for instance, their product). In other words, the roots of unity in $\mathbb{Q}_n$ have a maximum order, which is the lcm of all possible orders.

Let us call again m this maximal value; to prove Lemma 2.12 we need to prove that $m = n$ or $2n$. Now, any element ξ of $\mathbb{Q}_n$ which is a root of unity must satisfy $\xi^m = 1$.

This is true in particular when ξ is the primitive n^{th} root $\mathrm{e}^{2\mathrm{i}\pi/n}$; hence m is a multiple of n, and it follows that $\mathbb{Q}_n$, generated by a power of $\mathrm{e}^{2\mathrm{i}\pi/m}$, is a subset of $\mathbb{Q}_m$. Finally, by double inclusion,$\mathbb{Q}_n = \mathbb{Q}_m$. Now, in order to clarify the relationship between n and m, we must consider the dimension of $\mathbb{Q}_n$ as a vector space on the rational field $\mathbb{Q}$.

It is $\varphi(n) = \dim[\mathbb{Q}_n/\mathbb{Q}]$, where φ is Euler's totient function[9], it stands that $n \mid m$ and $\varphi(n) = \varphi(m)$.

Since $\varphi(n) = n \times \prod_{p|n \text{ and } p \text{ prime}} \left(1 - \frac{1}{p}\right)$, the only possibility is that $m = \begin{cases} n & \text{for } n \text{ even} \\ 2n & \text{for } n \text{ odd} \end{cases}$.

This proves that all eigenvalues of $\mathscr{U}$ are n^{th} or $2n^{th}$ roots of unity. Let us clarify the case of odd n: $\mathrm{e}^{\mathrm{i}\pi/n} = -\left(\mathrm{e}^{2\mathrm{i}\pi/n}\right)^{\frac{n+1}{2}}$ and hence we do indeed have $\mathbb{Q}_n = \mathbb{Q}_{2n}$. So we can rephrase what we just proved as Lemma 2.12: in the odd case, $\xi^n = \pm 1$.

[7] For instance $\mathbb{Q}_3 = \mathbb{Q}_6$, see exercises.

[8] It is perhaps not obvious that this group is finite, and indeed the group of elements of $\mathbb{Q}_2$ with magnitude one is not; essentially, this holds because for large m the dimension $\varphi(m)$ of the galoisian extension $\mathbb{Q}_m/\mathbb{Q}$ tends to infinity and thus exceeds $\varphi(n)$, dimension of $\mathbb{Q}_n/\mathbb{Q}$ (a more precise computation will be given in the main proof); hence roots of order m for large m cannot exist in $\mathbb{Q}_n$.

[9] This follows from the fact that the minimal polynomial of $\mathrm{e}^{2\mathrm{i}\pi/n}$ over $\mathbb{Q}$ is the cyclotomic polynomial Φ_n with degree $\varphi(n)$.

Remark 2.17. At this point, $\mathscr{U}$ could be constructed as a polynomial in the elementary circulating matrix $\mathscr{J}$ (as all other circulating matrixes) $\mathscr{U} = P(\mathscr{J})$, where P is the interpolating polynomial that sends the Fourier coefficients of $\mathscr{J}$, i.e. the $e^{2ik\pi/n}$, to the Fourier coefficients chosen for $\mathscr{U}$. Such a construction is easy and sometimes practical, using the basis of Lagrange polynomials associated with the $e^{2ik\pi/n}$, since P is a linear combination of these polynomials with coefficients that are precisely the Fourier coefficients of the desired u.

It is now time to prove Lemma 2.13: the possibilities of mapping the n^{th} roots of 1 to m^{th} roots of 1 can be somewhat reduced by noticing that $\mathscr{U}$ is a rational polynomial[10] in $\mathscr{J}$, and such a polynomial is stable under all field automorphisms of $\mathbb{Q}_n$ if we use the following characterisation from Galois theory:

Lemma 2.18. *Any object (number, vector, polynomial, matrix) with coefficients in $\mathbb{Q}_n$ is rational iff it is invariant under all Galois automorphisms of the cyclotomic extension $\mathbb{Q}_n$ over $\mathbb{Q}$.*

We mention the structure of its Galois group without proof either.[11]

Lemma 2.19. *Any field (Galois) automorphism of the cyclotomic extension $\mathbb{Q}_n$ over $\mathbb{Q}$ is defined by $\Psi_k(e^{2i\pi/n}) = e^{2ik\pi/n}$ for some definite $k \in \mathbb{Z}_n^*$, the group of invertible elements of the ring $\mathbb{Z}_n$, e.g. for any integer k coprime with n.*

This is enough to define $\Psi_k(x)$ for any $x \in \mathbb{Q}_n$, since any element of $\mathbb{Q}_n$ can be written $x = \sum a_j e^{2ij\pi/n}$ with rational a_j's, and it follows that $\Psi_k(x) = \sum a_j e^{2ijk\pi/n}$. For instance when $n = 12$, there are exactly four different automorphisms Ψ_k, defined by the possible images of $e^{2i\pi/12} = e^{i\pi/6}$, namely $e^{ik\pi/6}$, $k \in \{1,5,7,11\}$. Their group (the Galois group of the cyclotomic field) is isomorphic with the multiplicative group $\mathbb{Z}_{12}^* = \{1,5,7,11\}$.

If Ψ_k is such an automorphism, notice that $\Psi_k(\xi) = \xi^k$ for any n^{th} root ξ of unity (with one exception: $\Psi_k(-1) = -1\ \forall k \in \mathbb{Z}_n^*$). If n is odd and ξ is a $2n^{th}$ root but not a n^{th}, then $-\xi$ is a n^{th} root, and hence

$$\Psi_k(\xi) = -(-\xi)^k = \begin{cases} \xi_k & \text{for } k \text{ odd} \\ -\xi_k & \text{for } k \text{ even} \end{cases}.$$

For instance $\Psi_2(\xi) = -\xi^2$ for such ξ.

So from Lemma 2.18, we state that $\mathscr{U} \in \mathscr{M}_n(\mathbb{Q})$ iff $\mathscr{U}$ is invariant under all the $\Psi_k, k \in \mathbb{Z}_n^*$.

Now at last we can prove Lemma 2.13.

First case: n **even.**

Consider the eigenvector $X_j = (1, e^{2ij\pi/n}, e^{2i2j\pi/n}, \dots e^{2ij(n-1)\pi/n})^T$ for the eigenvalue ξ_j of $\mathscr{U}$ (for matrix J, the eigenvalue is of course $e^{2ij\pi/n}$). The ^{T} indicates

[10] The coefficients of this polynomial can be read on the first column of $\mathscr{U}$.

[11] These two results can be found in any textbook on Galois theory.

that we consider X_j as a column. We have $\Psi_k(X_j) = X_{jk}$ by direct computation. The case $j = 0$ is straightforward: since the eigenvector is real valued, so must be the eigenvalue, i.e. $\xi_0 = \pm 1$. We shall now set this case aside.

We assume that $\Psi_k(\mathscr{U}) = \mathscr{U}$ (i.e. that $\mathscr{U}$ is rational valued). Applying the Galois automorphism Ψ_k to the equation

$$\mathscr{U} X_j = \xi_j X_j \quad \text{yields} \quad \Psi_k(\mathscr{U})\Psi_k(X_j) = \mathscr{U} X_{kj} = \xi_{kj} X_{kj} = \Psi_k(\xi_j)\Psi_k(X_j) = \xi_j^k X_{kj}.$$

Hence

$$\Psi_k(\xi_j) = \xi_j^k = \xi_{jk} \quad (\sharp)$$

for all $j \neq 0$ and all $k \in \mathbb{Z}_n^*$.

Now for the reciprocal. Assume the above equation $(\sharp)$ between the eigenvalues. We choose one Galois automorphism, Ψ_k (for some k coprime with n). Let us apply $\Psi_k(\mathscr{U})$ to any eigenvector X_j of $\mathscr{U}$; notice that $X_j = \Psi_k(X_{k^{-1}j})$ where $k^{-1}j$ is computed modulo n. Hence

$$\begin{aligned} \Psi_k(\mathscr{U})X_j = \Psi_k(\mathscr{U} X_{k^{-1}j}) = \Psi_k(\xi_{k^{-1}j} X_{k^{-1}j}) &= \Psi_k(\xi_{k^{-1}j})\Psi_k(X_{k^{-1}j}) \\ = \xi_{k^{-1}j}^k X_{kk^{-1}j} \quad &\text{because } \Psi_k \text{ raises any root of 1 to the } k^{th} \text{ power} \\ = \xi_j X_j \quad &\text{by our assumption on the eigenvalues.} \end{aligned}$$

We have proved that $\Psi_k(\mathscr{U})$ does the same thing as $\mathscr{U}$ on any eigenvector. But the eigenvectors of $\mathscr{U}$ constitute a basis, hence $\Psi_k(\mathscr{U}) = \mathscr{U}$ for all k coprime with n, i.e. $\mathscr{U}$ is rational valued.

Last case: *n* odd.

We still get the equation $\Psi_k(\xi_j) = \xi_{jk}$ if $\mathscr{U}$ is assumed to be invariant under Ψ_k.

If ξ is a n^{th} root of unity, the computation is identical.

If $\xi^{2n} = 1$ but $\xi^n \neq 1$, then $(-\xi)^n = 1$ and hence $\Psi_k(\xi) = -\Psi_k(-\xi) = -(-\xi)^k = -\xi^k$ for even k and $\Psi_k(\xi) = \xi^k$ for odd k. The computation above still yields $\xi_{jk} = \Psi_k(\xi_j) = \xi_j^k$ for odd k, and we have also the new case $\xi_{jk} = -\xi_j^k$ for even k.

Say $k = 2$, and $\xi_1 = \xi$ with $\xi_1^{2n} = 1 \neq \xi_1^n$; then $\xi_2 = -\xi^2, \xi_4 = -\xi^4, \dots \xi_{2^m} = -\xi^{2^m}$. Number 2 has finite order in $\mathbb{Z}_n^*$, hence for some m, $\xi_{2^m} = \xi_1$. We get an orbit of m eigenvalues which are all $2n^{th}$ roots of unity, e.g. $\mathscr{O} = \{\xi_1, \xi_2, \xi_4, \xi_8 \dots\}$.

Say now that $k = 2^\nu k', k'$ odd and coprime with n. The formula $(\sharp)$ is then valid and yields $\xi_k = \xi_{2^\nu}^{k'}$. So ξ_k is determined when $\mathscr{O}$ is known. Notice that ξ_k will never be a n^{th} root (because 2 and k' are coprime with n): either all the eigenvalues (with even index) are n^{th} roots, or none (except of course $\xi_0 = \pm 1$).

The reciprocal is similar to the even case:

- it is identical when the eigenvalues are of order n (at most); and
- if ξ_1 has order $2n$, then the values of ξ_k that we have obtained will satisfy the relations $\Psi_k(\mathscr{U})X_j = \xi_j X_j$ for all j, k §k coprime with n, so that $\Psi_k(\mathscr{U})$ is identical to $\mathscr{U}$, i.e. $\mathscr{U}$ is rational-valued.

This ends the proof of Lemma 2.13.

We can now use the cases expounded in Lemma 2.13 to prove Theorem 2.10.

The whole set of eigenvalues is determined if we know ξ_j for a subset of representatives j of all orbits under multiplication by elements of $\mathbb{Z}_n^*$ (so called *associated elements* in the ring $\mathbb{Z}_n$). We can specify the smallest representatives:

Lemma 2.20. *Any element $j \in$ the ring $\mathbb{Z}_n$ is* associated *with a divisor of n, i.e.* $\exists k \in \mathbb{Z}_n^*,\ kj = \gcd(n, j)$.

(We identify integers and classes modulo n here since the distinction is irrelevant).

Proof. This stems from the Bezout identity (in $\mathbb{Z}$): for some $k, \ell, kj + \ell n = \gcd(n, j)$. After division by $\gcd(n, j)$ we see that k and n are coprime. But modulo $n, kj = \gcd(n, j)$.

Example 2.21. For $n = 15$ we have the orbits of equivalent elements

$$(0), (\mathbf{1}, 2, 4, 7, 8, 11, 13, 14), (\mathbf{3}, 6, 9, 12), (\mathbf{5}, 10)$$

indexed by the divisors $1, 3, 5$ and of course 0. This classification will prove useful in Chapter 3.

So it is sufficient to specify ξ_j when j is any divisor of n. We will need a last lemma, interesting in its own right:[12]

Lemma 2.22. *The set of differences $\Delta_n = \mathbb{Z}_n^* - \mathbb{Z}_n^* = \{a - b, (a, b) \in (\mathbb{Z}_n^*)^2\}$ is $\mathbb{Z}_n$ when n is odd, $2\mathbb{Z}_n$ when n is even.*

Proof. It is straightforward for n prime, for n an odd prime power, and we notice that when $n = 2^m$ then $\mathbb{Z}_n^*$ = odd numbers, so that Δ_n = even numbers. The general case now stems from the Chinese remainder theorem, i.e. the Sylow decomposition: if $n = 2^d \dots p^z \dots$ is the prime decomposition of n then $\mathbb{Z}_n^* = (\mathbb{Z}/2^d\mathbb{Z})^* \times \dots (\mathbb{Z}/p^z\mathbb{Z})^* \times \dots$ and the result being true for the factors is true for the product.

We now proceed to prove the theorem. Remember that $\xi_0 = \pm 1$.

- When n is even:
  In this case all eigenvalues are n^{th} roots of unity. Let j be any strict divisor of n.
  - When n/j is even, we can produce $k, k' \in \mathbb{Z}_n^*$ with $k' - k = \dfrac{n}{j} \in 2\mathbb{Z}$ from Lemma 2.22. Hence (noting that $k \equiv k' \mod n$)

$$\xi_j^{k+\frac{n}{j}} = \xi_j^{k'} = \xi_{jk'} = \xi_{jk} = \xi_j^k$$

    which proves that $\xi_j^{\frac{n}{j}} = 1$, i.e. ξ_j is a power of $\mathrm{e}^{2ij\pi/n}$.

[12] Though elementary in nature, the result was previously unknown to the author and does not appear to be readily available in the literature.

– If n/j is odd (meaning that j contains the same power of 2 as n), then Lemma 2.22 only provides $k' - k = \dfrac{2n}{j}$, and the calculation yields $\xi_j^{2n/j} = 1$, i.e. ξ_j is a power of $e^{ij\pi/n}$, which ends the even case of the theorem.

- When n is odd:
  The case when ξ_j is a n^{th} root is identical to the n even (first) case, as from the last Lemma 2.22, we can again produce two elements $k, k' \in \mathbb{Z}_n^*$ such that $k' - k = \dfrac{n}{j}$, and $\xi_j^{k'-k} = 1 = \xi_j^{n/j}$. So the spectral unit is a power of $e^{2i\pi j/n}$, i.e. a n/j^{th} root of unity ξ_j for each divisor j of n.

  Now assume that there is an eigenvalue ξ_j which is *not* a n^{th} root. Then $-\xi_j$ is a n^{th} root, and (as n/j is odd) a similar calculation yields for $k' - k = n/j$, with $k, k' \in \mathbb{Z}_n^*$,
  $$(-\xi_j)^{k'} = -\xi_{jk'} = -\xi_{jk} = (-\xi_j)^k = (-\xi_j)^{k'-\frac{n}{j}}.$$
  Hence $-\xi_j$ is again a n^{th} root of unity, this is the second subcase.
  This ends the proof of the odd case of Theorem 2.10.

Theorem 2.11 follows from the possible independent values for each $\xi_j, j \mid n$: in general each ξ_j lies in a cyclic group with order n/j, while n/j runs over the list of divisors of n. The complicated situation is the case when $-\xi_j$ is also a n/j^{th} root, which explains the lcm in the formula (the group $\{\pm 1\} \times \mathbb{Z}_d$ is isomorphic with $\mathbb{Z}_{2d}$ whenever d is odd).

Example 2.23. This theorem enables us to find alternative spectral units between homometric pc-sets with some nil Fourier coefficients.

An example issued from music theory: consider two melodic minor scales $a = (1,0,1,1,0,1,0,1,0,1,0,1), b = (1,0,1,0,1,0,1,0,1,1,0,1)$. Their Fourier coefficients with indexes 2 and 10 are nil. Let us find a spectral unit u such that $a * u = b$, we have several possible choices for $\mathscr{F}_u(2)$:

- Using Rosenblatt's choice, we choose arbitrarily $\xi_2 = \mathscr{F}_u(2) = \mathscr{F}_u(10) = \xi_{10} = 1$ (the other Fourier coefficients are determined by $\mathscr{F}_u(k) = \mathscr{F}_b(k)/\mathscr{F}_a(k)$). This yields $u = (0,0,0,0,0,0,0,0,0,1,0,0)$. Musically this means that A minor (melodic) is transposed from C minor by a minor third, a foreseeable result!
- We know from Lemma 2.13 that ξ_2 must be some power of $e^{i\pi/3}$, ξ_{10} being its conjugate or inverse. This yields no less than **five** other possible units, e.g.

$$u = \frac{1}{4}(1,0,-1,-1,0,1,1,0,-1,3,0,1) \quad \text{or}$$
$$u = \frac{1}{12}(1,2,1,-1,-2,-1,1,2,1,11,-2,-1) \quad \text{or}$$
$$u = \frac{1}{6}(2,1,-1,-2,-1,1,2,1,-1,4,-1,1) \quad \text{or}$$
$$u = \frac{1}{12}(1,-1,-2,-1,1,2,1,-1,-2,11,1,2) \quad \text{or}$$
$$u = \frac{1}{4}(1,1,0,-1,-1,0,1,1,0,3,-1,0).$$

In a way this can be interpreted as additional, hidden symmetries between those two musical scales.

Example 2.24. Let us elucidate this subgroup of units when $n = 12$. Let u be a spectral unit with finite order, and $\xi_0, \dots \xi_{11}$ its Fourier coefficients, i.e. the eigenvalues of the associated matrix $\mathscr{U}$. From Theorem 2.10 above, the relation $\xi_j^k = \xi_{jk}$ is satisfied for all four values of $k = 1, 5, 7, 11$.

- There are no conditions on ξ_1 which is any 12^{th} root ξ of unity; its value specifies $\xi_5 = \xi^5$ and similarly ξ_7, ξ_{11}.
- ξ_2 must be a power of $e^{2\times 2i\pi/12} = e^{i\pi/3}$. This determines also $\xi_{10} = \overline{\xi}_2$.
- Similarly ξ_3 is a power of $i = e^{i\pi/2}$. We have $\xi_9 = \overline{\xi}_3$.
- Since 12/4 is odd (special case), ξ_4 must be a power of $e^{i\pi/3}$, just like ξ_2. Here also, we find that $\xi_8 = \overline{\xi}_4$.
- $\xi_0 = \pm 1$ and $\xi_6 = \xi_{-6} = \xi_6^{-1}$ is a $12/6^{th}$ root of 1, i.e. $\xi_6 = \pm 1$.

To conclude: ξ_1 is any 12^{th} root of unity, while ξ_2, ξ_3, ξ_4 are limited to subgroups, ξ_0 and $\xi_6 = \pm 1$. The structure of the group is then $\mathbb{Z}_{12} \times (\mathbb{Z}_6)^2 \times \mathbb{Z}_4 \times (\mathbb{Z}_2)^2$, with 6,912 elements like $\big(0, 0, 1/3, -1/3, 0, 0, -2/3, -1/3, 0, 0, 1/3, -1/3\big)$ or $\big(7/12, -1/6, 1/12, 1/12, -1/6, -5/12, -5/12, -1/6, 1/12, 1/12, -1/6, -5/12\big)$. The complete list is available online as a text file:
`http://canonsrythmiques.free.fr/allSpectralUnitsZ_12.txt.`

It can be expanded from the following list of generators:

$$\left(\frac{5}{6}, -\frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}\right)$$
$$\left(\frac{2}{3}, \frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}, \frac{1}{6}, -\frac{1}{3}, \frac{1}{3}, -\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, -\frac{1}{6}, \frac{1}{3}\right)$$
$$\left(\frac{11}{12}, -\frac{1}{6}, -\frac{1}{12}, \frac{1}{12}, \frac{1}{6}, \frac{1}{12}, -\frac{1}{12}, -\frac{1}{6}, -\frac{1}{12}, \frac{1}{12}, \frac{1}{6}, \frac{1}{12}\right)$$
$$\left(\frac{5}{6}, -\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, -\frac{1}{6}, -\frac{1}{6}, \frac{1}{6}, \frac{1}{6}\right)$$
$$\left(\frac{11}{12}, -\frac{1}{12}, \frac{1}{6}, -\frac{1}{12}, -\frac{1}{12}, \frac{1}{6}, -\frac{1}{12}, -\frac{1}{12}, \frac{1}{6}, -\frac{1}{12}, -\frac{1}{12}, \frac{1}{6}\right)$$
$$\left(\frac{5}{6}, \frac{1}{6}, -\frac{1}{6}, \frac{1}{6}, -\frac{1}{6}, \frac{1}{6}, -\frac{1}{6}, \frac{1}{6}, -\frac{1}{6}, \frac{1}{6}, -\frac{1}{6}, \frac{1}{6}\right);$$

one may notice that the first one is the opposite of the complement operator, cf. Proposition 2.7.

2.1.4 Orbits for homometric sets

We have seen that the action of the torus of spectral units describes the most general orbits of homometric classes in the vector space $\mathbb{C}^n$, but fails to elicit the distributions in this space which are actual pc-sets, i.e. distributions with values 0 or 1.[13] Actually there is a deep result behind this failure:

Theorem 2.25. *Let $n \in \mathbb{N}$ with $n \geqslant 2$. If $n = 8$, $n = 10$ or $n \geqslant 12$, then for every field K and for every subgroup H of the linear group $\mathrm{GL}_n(K)$ such that the natural group action of H on $\mathscr{P}(\mathbb{Z}_n)$ identified with $\{0,1\}^n$ is well-defined, the orbits of this group action are not identical with the equivalence classes of the Z-relation.*

This stunning result discovered by John Mandereau [64] needs translation: it means that there is no 'reasonable' group action (that would induce some action on the pcs themselves) whose orbits are the homometric classes.[14]

Of course, it is possible to study the symmetries of *one* class of isometric pc-sets as subgroups of the group of permutations of k-subsets. Such symmetry groups depend on the class and usually include (or coincide with) T/I. The other cases are intriguing: for instance the group of the homometry class of $\{0,1,4,6\}$ in $\mathbb{Z}_{12}$ is isomorphic with the 48-element affine group modulo 12.[15] The drawback of this topdown approach is that the homometry class has to be computed before the symmetry group. On the other hand, elucidating the relationships between the elements of an homometry class is extremely useful for composers: for instance, the aforementioned class is composed of one orbit under the affine group, two orbits under T/I ($\{0,1,4,6\}$ and $\{0,1,3,7\}$) and four under T (adding $\{0,2,5,6\}$ and $\{0,4,6,7\}$, see Fig. 8.13). More about the computations of these groups can be found in [41], hinting at some compositional applications by Tom Johnson. A rich example uses paths between the 108 homometric sets with size 5 in $\mathbb{Z}_{12}$, computed by Franck Jedrzejewski and drawn by Johnson in Fig. 2.4, each line corresponding with one of three generators a,b,c of the symmetry group.

2.2 Extensions and generalisations

2.2.1 Hexachordal theorems

We have stated the original hexachord theorem in modern terms:

Theorem 2.26 (Babbitt's hexachord theorem).
Any hexachord in $\mathbb{Z}_{12}$ is homometric with its complement.

The proof can be easily adapted to a more general statement:

Theorem 2.27. *The intervallic contents of a subset of $\mathbb{Z}_n$ and of its complement differ by a constant distribution, whose value is the difference between the cardinality of the set and of its complement:*

[13] It is possible to get down to $\mathbb{R}^n$ but even the difficult Theorem 2.10 does not completely elucidate homometry in $\mathbb{Q}^n$, leaving aside infinite orbits.

[14] In this light one may remember that moving from a major to a minor triad was a 'local' transformation, depending on both triads.

[15] Actually it *IS* the affine group itself, permutating the interval vector without changing it since these are all-interval sets.

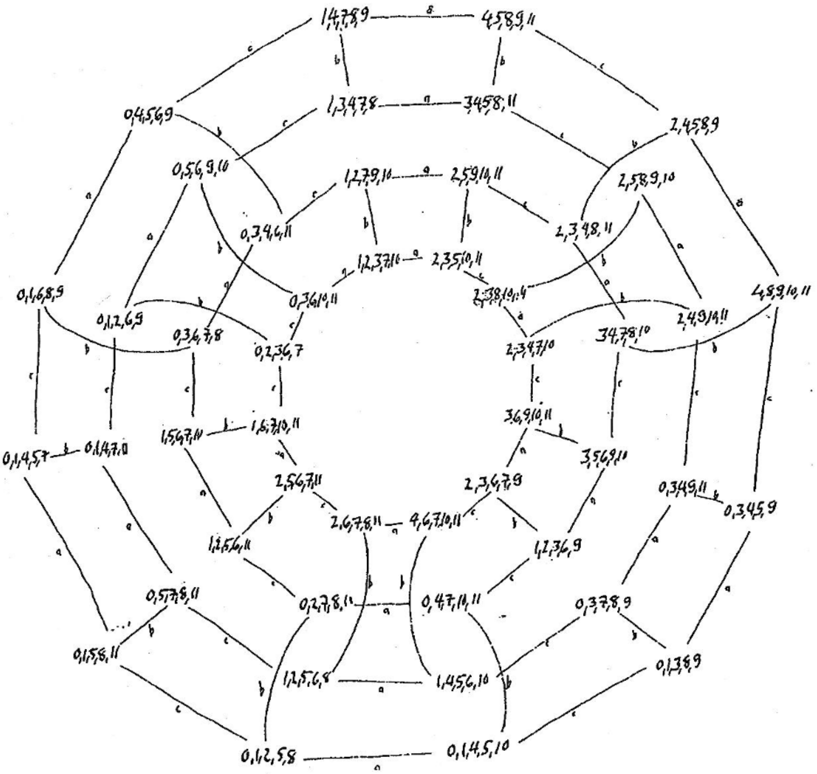


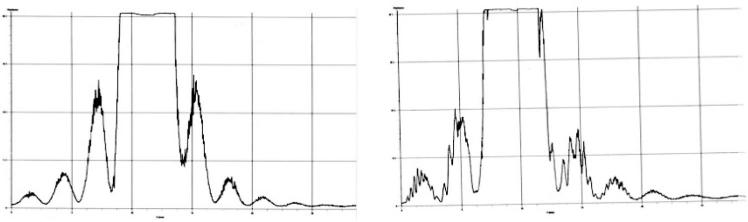
Fig. 2.4. Paths between homometric 5-sets drawn by T. Johnson

$$\mathrm{IC}(A) - \mathrm{IC}(\mathbb{Z}_n \setminus A) = (\#(A) - \#(\mathbb{Z}_n \setminus A)).\mathbf{1} = Constant$$

For instance, the intervallic contents of Tristan's chord $\{3,5,8,11\}$ and its complement are $(4,0,1,2,1,2,0,2,1,2,1,0)$ and $(8,4,5,6,5,6,4,6,5,6,5,4)$; the difference between those two vectors is constant and equal to 4, the cardinality difference. If one is sensitive to the ratios between the interval counts, then the intervallic distribution is clearer on the smaller pc-set. If however one perceives the variation of this interval histogram around a mean value, then perhaps the larger complement set yields a neater intervallic distribution: the theorem says that the two ICs are equal (up to a constant) but the *contrast* differs. In optics this result is actually known as Babinet's theorem:

> The diffraction pattern from an opaque body is identical to that from a hole of the same size and shape except for the overall forward beam intensity.

The difference in contrast means that, for instance, one can estimate the breadth of a hair by carving it out of an opaque sheet and diffracting (ordinary) light with this,



Diffraction for a slit Diffraction for a hair

Fig. 2.5. Two diffraction graphs for a slit and its complement

or estimate the size of red blood cells by comparing the diffraction picture with one obtained from calibrated small holes, see [20] and Fig. 2.5.[16]

This theorem can be further extended to a large class of groups (including mainly compact groups), see [2]. The proof using Fourier transform is still valid for all finite abelian groups and even compact abelian groups (such as the torus $\mathbb{T}_n$), but we will not spell it out here since there is a more general one. The essential point is that the probability of occurrence of an 'interval' g (i.e. the size of $\mathscr{I}_g = \{(a,b) \in G \times G, b = g.a\}$), can still be measured by integral calculus thanks to the existence of a Haar measure.[17]

A nice example in a torus is the following, borrowed from the above paper:

Example 2.28. Musical scales can be modelised as elements of a torus, each note being a point on the continuous unit circle S^1 (see Section 5.1). Say we define the set ITS of 'in-tune' scales as major scales whose maximal deviation from a reference well-tempered major scale does not exceed 10 cents, e.g. the 'in-tune' D major scales would be in $[190,210] \times [390,410] \times [590,610] \times [690,710] \times [890,910] \times [1090,1110] \times [90,110]$ where each pc is given in cents. So ITS is a subset of the torus $\mathbb{T}^7 = (\mathbb{R}/1200\mathbb{Z})^7$, with measure $(20/1200)^7$ of the whole torus, and the complement OTS (out-of-tune' scales) has the same interval content, up to a constant.

The simplest generalisation is to finite abelian groups, which are products of cyclic groups (i.e. discrete torii). Such a group can model for instance:

1. The decomposition $\mathbb{Z}_{12} = \mathbb{Z}_3 \times \mathbb{Z}_4$, so-called torus of thirds: the hexachord theorem (or the notion of homometry in general) can be factored down to this expression of pcs as pairs.
2. Pairs (or $p-$uples) of pcs lie in $\mathbb{Z}_{12} \times \mathbb{Z}_{12}$ (or a larger power), wherein the general hexachord theorems apply.

[16] Obtained by one of my students, Domenech Vianney, in 2015.

[17] This means that there is a way to measure a subset's 'size' which is invariant under translation.

2.2.2 Phase retrieval even for some singular cases

As discussed above, knowledge of $\mathrm{IFunc}(A,B)$ and B enables us to retrieve A, except when $\mathscr{F}_B$ vanishes because $\mathscr{F}_A$ is then indeterminate. It is still possible though to retrieve A, solving Lewin's problem, when $\mathscr{F}_B$ vanishes for a *single* coefficient[18] and when A is known to be a genuine set, i.e. a distribution with only 0's and 1's. This additional information compensates for the missing one. It is perhaps best to describe the somewhat involved process by way of an example:

Example 2.29. The melodic minor scale $B = \{0,2,3,5,7,9,11\}$ is one of Lewin's special cases: $\mathscr{F}_B(2)(= \mathscr{F}_B(10)) = 0$.

Assume $\mathrm{IFunc}(A,B) = (2,2,2,1,2,3,0,3,1,2,2,1)$ where A remains to be found. Adding the number of intervals, i.e. the elements of $\mathrm{IFunc}(A,B)$, one gets 21, meaning that A has three elements to B's seven. Now compute all available values of $\mathscr{F}_A$, i.e. all except $\mathscr{F}_A(2), \mathscr{F}_A(10)$, dividing the coefficients of the DFT of $\mathrm{IFunc}(A,B)$ by the conjugates of those of B. One gets (rounding to the third digit for legibility)

$$\mathscr{F}_A = (3., -0.366-0.366\mathrm{i}, \boxed{\mathbf{X}}, 2+\mathrm{i}, -1.732\mathrm{i}, 1.366+1.366\mathrm{i}, 1, \text{ [and conjugates]}).$$

The secret weapon at this juncture is Parseval-Plancherel's formula:

$$\sum |\mathscr{F}_A(k)|^2 = n\#A$$

in the case of a pc-set. This provides the *magnitude* of the missing Fourier coefficient $\mathbf{X}$, the phase φ being still unknown: let $\mathbf{X} = \mathscr{F}_A(2) = \overline{\mathscr{F}_A(10)} = r\mathrm{e}^{\mathrm{i}\varphi}$, then the difference between the sum of all known $|\mathscr{F}_A(k)|^2$ (here equal to 34) and $n\#A = 3 \times 12 = 36$, is equal to $2r^2$. Hence $r = 1$. Plugging back in this value, we are now down to

$$\mathscr{F}_A = (3., -0.366-0.366\mathrm{i}, \mathrm{e}^{\mathrm{i}\varphi}, 2+\mathrm{i}, -1.732\mathrm{i}, 1.366+1.366\mathrm{i}, 1, \text{ and their conjugates})$$

By inverse Fourier transform, we get (I only quote the first values)

$$\mathbf{1}_A = \left(\frac{\cos(\varphi)}{6} + 0.833, \frac{1}{6}\sin\left(\frac{\pi}{6} - \varphi\right) - 0.083, 0.083 - \frac{1}{6}\sin\left(\varphi + \frac{\pi}{6}\right), \dots\right)$$

Now the only way $\dfrac{\cos(\varphi)}{6} + 0.833333$ can be equal to 0 or 1 is to have $\cos\varphi = 1$, i.e. $\varphi = \pm\dfrac{2\pi}{3}$. The value of φ could be found equally easily from any other coefficient, e.g. $\frac{1}{6}\sin\left(\frac{\pi}{6} - \varphi\right) = 0.08333$ would yield the same solution (in other cases, it might be necessary to examine several equations in order to dispel possible ambiguities – or perhaps find multiple solutions).

Plugging this value of φ in $\mathbf{1}_A$ finally yields (up to rounding errors)

$$\mathbf{1}_A = (1,0,0,0,1,0,0,1,0,0,0,0),$$

i.e. $A = \{0,4,7\}$ which was indeed the pc-set that served to compute $\mathrm{IFunc}(A,B)$ in the first place.

[18] And of course its conjugate.

Of course, in this particular case it might be quicker to proceed by trial and error, but the method is general. To sum up the algorithm, one follows these steps:

1. Compute the cardinality of A: it is the sum of the elements of $\mathrm{IFunc}(A,B)$ divided by $\#B$.
2. Compute $\mathscr{F}_A = \dfrac{\mathscr{F}(\mathrm{IFunc}(A,B))}{\overline{\mathscr{F}_B}}$, with two coefficients still indeterminate.
3. Compute the sum of the squared magnitudes of the $n-2$ known coefficients in the last step; subtract the result from $n\#A$ to get $2r^2$ and hence r, the magnitude of the missing coefficient.
4. Compute the inverse Fourier transform of $\mathscr{F}_A$ as a function of the missing coefficient $r\mathrm{e}^{\mathrm{i}\varphi}$, where only φ remains unknown.
5. Taking into account that all the values computed in the last step must be 0's or 1's, determine φ; complete the computation of $\mathbf{1}_A$.

To some extent, this algorithm could be used even when A is a multiset.

For practical purposes, I will remind the reader of the matricial formalism mentioned in 1.2.3. In [13], we used linear programming to good effect for solving equations like $s * \mathbf{1}_A = \mathbf{1}_B$ (which corresponds to finding a linear combination of translates of A equal to B) and the same procedure could be used for solving $\mathbf{1}_A * \mathbf{1}_{-B} = \mathrm{IFunc}(A,B)$ in A, which is the problem at hand. But though the algorithm seems to work well, it is not formally proved yet that it always provides a solution. For one thing, there may well be multiple solutions (that the algorithm may reach by varying the starting point), e.g. for $B = \{0,2,4,6,8,10\} \subset \mathbb{Z}_{12}$, $\mathrm{IFunc}(A,B)$ does not change when A is replaced by $A+2$. See the reference above or 3.3.3 for a description of this method, which bypasses Fourier transform altogether.

2.2.3 Higher order homometry

IFunc counts intervals, which are pairs of elements. There is no law against counting triplets, quadruplets, and so on. It is necessary to be precise about what is a different ‘occurrence’ of a given triplet. We borrow again some definitions and results from [64], with some modifications.

Let us begin with counting triplets (i.e. 3-subsets of a pc-set) up to translation: if we are looking for copies of $(0,a,b)$, their number in $A \subset \mathbb{Z}_n$ is equal to

$$\mathbf{tv}(a,b) = \sum_{t \in \mathbb{Z}_n} \mathbf{1}_A(t)\mathbf{1}_A(t+a)\mathbf{1}_A(t+b).$$

We redo from scratch the computation of the Fourier transform, here in two variables:[19]

[19] All sums are taken over the whole $\mathbb{Z}_n$.

$$\widehat{\mathbf{tv}}(\omega,\nu) = \sum_t \sum_a \sum_b \mathbf{1}_A(t)\mathbf{1}_A(t+a)\mathbf{1}_A(t+b)\mathrm{e}^{-2\mathrm{i}\pi(\omega a+\nu b)/n}$$
$$= \sum_t \mathbf{1}_A(t)\mathrm{e}^{2\mathrm{i}\pi(\omega t+\nu t)/n} \sum_a \mathbf{1}_A(t+a)\mathrm{e}^{-2\mathrm{i}\pi\omega(t+a)/n} \sum_b \mathbf{1}_A(t+b)\mathrm{e}^{-2\mathrm{i}\pi\nu(t+b)/n}$$
$$= \sum_t \mathbf{1}_A(t)\mathrm{e}^{-2\mathrm{i}\pi(-\omega-\nu)t/n} \sum_x \mathbf{1}_A(x)\mathrm{e}^{-2\mathrm{i}\pi\omega x/n} \sum_y \mathbf{1}_A(y)\mathrm{e}^{-2\mathrm{i}\pi\nu y/n}$$
$$= \mathscr{F}_A(-\omega-\nu)\mathscr{F}_A(\omega)\mathscr{F}_A(\nu).$$

Hence

Proposition 2.30. *The triplet histograms of pc-sets A and B are equal iff for all* $\omega,\nu \in \mathbb{Z}_n$

$$\mathscr{F}_A(-\omega-\nu)\mathscr{F}_A(\omega)\mathscr{F}_A(\nu) = \mathscr{F}_B(-\omega-\nu)\mathscr{F}_B(\omega)\mathscr{F}_B(\nu).$$

Generalizing to k-uplets, we will say that A,B *are* **k-homometric***, i.e. contain the same number of translates of any k-subset, or more generally that two distributions E and F are k-homometric, iff*

$$\widehat{E}(\omega_1)\widehat{E}(\omega_2)\cdots\widehat{E}(\omega_{k-1})\widehat{E}(-\omega_1-\ldots-\omega_{k-1}) =$$
$$= \widehat{F}(\omega_1)\widehat{F}(\omega_2)\cdots\widehat{F}(\omega_{k-1})\widehat{F}(-\omega_1-\ldots-\omega_{k-1})$$

for every $(\omega_1,\ldots,\omega_{k-1}) \in \mathbb{Z}_n^{k-1}$.

It is easily seen from this formula that

1. k-homometry implies $(k-1)-$homometry,[20] and
2. 2-homometry is usual homometry[21]:

$$|\mathscr{F}_A(\omega)|^2 = \mathscr{F}_A(\omega)\mathscr{F}_A(-\omega) = \mathscr{F}_B(\omega)\mathscr{F}_B(-\omega) = |\mathscr{F}_B(\omega)|^2.$$

The study of phase retrieval (find all distributions k-homometric with a given E) is hence very difficult when the Fourier transform vanishes. When it does not, there is a strong result:

Theorem 2.31. *When E is non negative* and if $\widehat{E}$ never vanishes on $\mathbb{Z}_n$, *any distribution* 3*-homometric with E must be a translate of E.*

The proof illustrates the strength and relevancy of the DFT.

Proof. Assume E and F are 3-homometric, $\widehat{E}$ and $\widehat{F}$ never vanishing. Let us denote by ξ the ratio of the DFTs, $\xi(t) = \widehat{E}(t)/\widehat{F}(t)$. Then from Proposition 2.30 we get that

$$\xi(\omega+\nu) = \xi(\omega)\xi(\nu) \quad \forall \omega,\nu \in \mathbb{Z}_n;$$

[20] At least when $\widehat{F}(0) \neq 0$.

[21] By now surely nobody will presume to call it ‘simple homometry’.

meaning that ξ is a group morphism from $(\mathbb{Z}_n, +)$ into $(\mathbb{C}^*, \times)$, a.k.a. a *character*. The characters of $\mathbb{Z}_n$ are well-known: there is[22] an integer k such that $\xi : t \mapsto \mathrm{e}^{-2\mathrm{i}\pi kt/n}$. But this means

$$\forall t \in \mathbb{Z}_n\ \widehat{E}(t) = \widehat{F}(t) \times \mathrm{e}^{-2\mathrm{i}\pi kt/n}.$$

By inverse Fourier transform (or by reversing Proposition 1.16) this means that $E = F + k$.

Here is an example of non-trivial 3-homometry in $\mathbb{Z}_{32}$:

$$A = \{0,7,8,9,12,15,17,18,19,20,21,22,26,27,29,30\},$$
$$B = \{0,1,8,9,10,12,13,15,18,19,20,21,22,23,27,30\}.$$

These sets are 3-homometric – for instance the pattern (0, 10, 20) appears seven times in both – but not translates, cf. Fig. 2.6 (hence their DFT must vanish; indeed all Fourier coefficients with even index are nil).

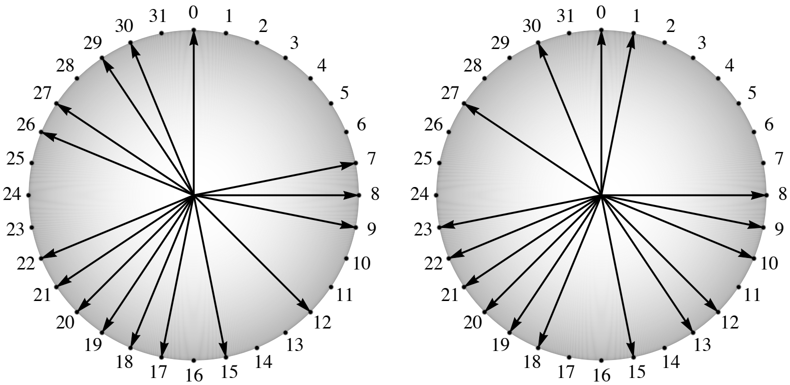


Fig. 2.6. Two 3-homometric subsets

This result narrows the import of the notion of k-homometry of pc-sets: in most cases, this notion is nothing new since it reduces to equivalence under translation.[23] This is probably why the literature usually addresses a broader form of homometry. Indeed a problem appears for $k \geqslant 3$ which did not make sense for $k = 2$, i.e. when

[22] Such a morphism is determined by the image of $1 \in \mathbb{Z}_n$ since one element generates the whole group. We used a stronger form of this result during the proof of Theorem 2.10.

[23] The result is still true even in several cases with vanishing DFT, when n has few factors, though the proof gets really difficult (see [64], Section 4). We will see though in the next chapter that distributions with nil Fourier coefficients play vital roles in some areas of music theory, so perhaps this area deserves further research. For instance, both subsets given in the last example tile (trivially) $\mathbb{Z}_{32}$.

counting intervals: clearly whenever an interval appeared, so did its inverse. But for triplets or larger subsets, the inversion is usually a distinct form. Hence the following, taken again from [64], Section 4:

Definition 2.32. *Let H be a subgroup of the group of permutations of $\mathbb{Z}_n$, $S(\mathbb{Z}_n)$. Let us define a H-copy of a set $S \subset \mathbb{Z}_n$ as any set of the form $h(S)$, with $h \in H$. Their set, the orbit of S under the action of H, will be denoted by $[S]_H$.*

The two most interesting cases are $H = T$, the cyclic group of transpositions, and $H = T/I$, the dihedral group of transpositions and inversions, though other groups, like the affine group, might be of interest for composers.

Definition 2.33. *Let $A \subset \mathbb{Z}_n$; we call k-vector of A the map*

$$S \mapsto \mathbf{mv}^k(A)_S = \#\{S' \in [S]_{T/I}, S' \subset A\}.$$

For of any k-set S, it tallies the number of its T/I-copies embedded in A.

Example 2.34. The set $A = \{0,1,3,4,7\}$ has essentially only six non-zero entries in its 3-vector:

$$\begin{array}{ll} \mathbf{mv}^3(A)_{\{0,1,3\}} = 2 & \mathbf{mv}^3(A)_{\{0,1,4\}} = 3 \\ \mathbf{mv}^3(A)_{\{0,1,6\}} = 1 & \mathbf{mv}^3(A)_{\{0,2,6\}} = 1 \\ \mathbf{mv}^3(A)_{\{0,3,6\}} = 1 & \mathbf{mv}^3(A)_{\{0,3,7\}} = 2 \end{array}$$

Indeed, $\mathbf{mv}^3(A)_{\{0,1,3\}} = 2$ since there are two T/I-copies of $\{0,1,3\}$ embedded in A (they are $\{0,1,3\}$ and $\{1,3,4\}$); $\mathbf{mv}^3(A)_{\{0,1,4\}} = 3$ since there are three T/I-copies of $\{0,1,4\}$ embedded in A (they are $\{0,1,4\}$, $\{0,3,4\}$ and $\{3,4,7\}$); and so on.

This is more general than what we have done with k-homometry.

Definition 2.35. *Sets $A_1,\ldots,A_s$ are k-Homometric (with a capital 'H') iff $\mathbf{mv}^k(A_1)_S = \mathbf{mv}^k(A_2)_S = \ldots = \mathbf{mv}^k(A_s)_S$ for all $S \subset \mathbb{Z}_n$, $\#S = k$.*

Example 2.36. Let us consider, in $\mathbb{Z}_{18}$, the two sets $A = \{0,1,2,3,5,6,7,9,13\}$ and $B = \{0,1,4,5,6,7,8,10,12\}$. They are not related by translation/inversion, but $\mathbf{mv}^3(A)_S = \mathbf{mv}^3(B)_S$ for all $3-$subsets S. For instance the set $S = \{0,1,9\}$ appears once in A and once, inverted, in B (see Fig. 2.7).

Their Fourier transform never vanishes, which shows that Theorem 2.31 works with general homometry (by translation) but not with Homometry (by translation/inversion).

The search for non-trivial k-Homometry is a formidable computational problem, but an example for $k = 4$ was found in 2011 by Daniele Ghisi.

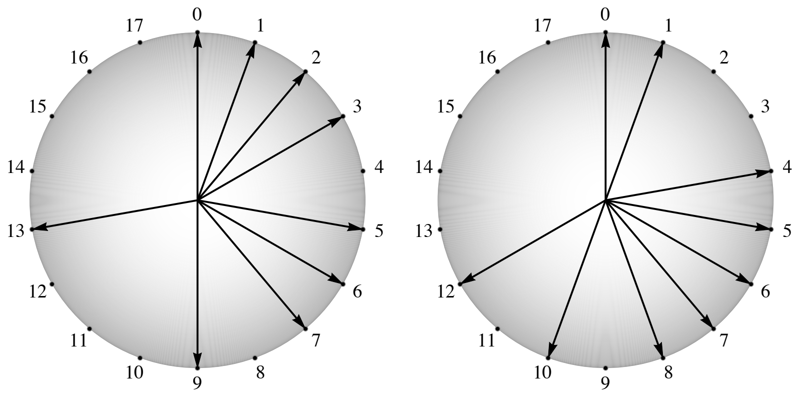


Fig. 2.7. Two non-trivially 3-Homometric subsets of $\mathbb{Z}_{18}$

Exercises

Exercise 2.37. Choose one hexachord, compute its intervallic distribution and that of its complement. Are these two hexachords T/I related?

Exercise 2.38. Compose a melody with four notes in $\{0,1,4,6\}$ in one of its translated forms (say B C E♭ F) spelling eleven distinct intervals. Superimpose another melody with the same intervals, but taken in a homometric pc-set, say $\{0,1,3,7\}$.

Exercise 2.39. Find non-trivially homometric pentachords (two classes). Are they affinely related?

Exercise 2.40. Prove Theorem 2.2 for non-singular distributions (i.e. their DFT never vanishes).

Exercise 2.41. Prove Proposition 2.7 by computing the eigenvalues and eigenspaces and the convolution product with an arbitrary characteristic function.

Exercise 2.42. Compute some non-obvious cubic roots of the circulating matrix of the minor third transposition $mt = (0,0,0,1,0,0,0,0,0,0,0,0) = j^3$ in $\mathscr{C}_n(\mathbb{C})$ (hint: use the matrix formalism and eigenvalues). Which of the solutions belong to $\mathscr{C}_n(\mathbb{R}), \mathscr{C}_n(\mathbb{Q})$?

Exercise 2.43. Cyclotomic fields: find a linear basis of $\mathbb{Q}_3$ over field $\mathbb{Q}$. Same thing with $\mathbb{Q}_6$, checking that $\mathbb{Q}_6 = \mathbb{Q}_3$.

Springer
http://www.springer.com/978-3-319-45580-8

Music Through Fourier Space
Discrete Fourier Transform in Music Theory
Amiot, E.
2016, XV, 206 p. 129 illus., 45 illus. in color., Hardcover
ISBN: 978-3-319-45580-8