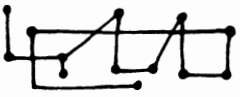
SUPPLEMENTARY SETS AND REGULAR COMPLEMENTARY UNENDING CANONS (PART FOUR)



DAN TUDOR VUZA

8. MULTIPLICATIVE TRANSFORMATIONS OF SUPPLEMENTARY RHYTHMIC CLASSES

IN THIS SECTION we shall study the effect of multiplication by a rational number, as well as the effect of condensed multiplication applied to one of the classes in a pair of suplementary rhythmic classes.

THEOREM 8.1. *Let $R, S \in Rhyt$ and let $k \neq 0$ be an integer relatively prime to* $(\mathrm{Per}\, R \vee \mathrm{Per}\, S)/(\mathrm{Div}\, R \wedge \mathrm{Div}\, S)$. *Then R and S are supplementary iff* $kR + [\mathrm{Per}\, R \vee \mathrm{Per}\, S]$ *and S are supplementary.*

Proof. Set $a = \mathrm{Div}\, R \wedge \mathrm{Div}\, S$, $b = \mathrm{Per}\, R \vee \mathrm{Per}\, S$, $n = b/a$. By Proposition 7.4, R and S are supplementary iff $H_{a,b}(R)$ and $H_{a,b}(S)$ are supplementary translation classes of $\mathbf{Z}_n$. By Proposition 3.7,

$$\operatorname{Per}(kR + [b]) = \operatorname{Per} R\,,$$
$$\operatorname{Div}(kR + [b]) = \operatorname{Div} R\,,$$
$$\mathrm{H}_{a,b}(kR + [b]) = k\mathrm{H}_{a,b}(R).$$

We may therefore again use Proposition 7.4 in order to conclude that $kR + [b]$ and S are supplementary iff $kH_{a,b}(R)$ and $H_{a,b}(S)$ are supplementary translation classes. Now Theorem 2.3 shows that $kH_{a,b}(R)$ and $H_{a,b}(S)$ are supplementary whenever $H_{a,b}(R)$ and $H_{a,b}(S)$ are so. Conversely, suppose that $kH_{a,b}(R)$ and $H_{a,b}(S)$ are supplementary. The map $x \mapsto kx$ is an automorphism of $\mathbf{Z}_n$ and its inverse is $x \mapsto k'x$ where k' is an integer relatively prime to n. Hence $H_{a,b}(R) = k'(kH_{a,b}(R))$ and $H_{a,b}(S)$ are supplementary again by Theorem 2.3, the proof being thus completed.

THEOREM 8.2. *Let R, $S \in Rhyt$ and let r, s be nonzero rational numbers representable as quotients of integers relatively prime to* $(\operatorname{Per} R \vee \operatorname{Per} S)/(\operatorname{Div} R \wedge \operatorname{Div} S)$. *Then R and S are supplementary iff rR and sS are supplementary.*

Proof. By Theorem 8.1, R and S are supplementary iff R and $(-1)S$ are so. We may therefore assume that $r > 0$ and $s > 0$. Write $r = k/k'$ and $s = l/l'$ with k,k',l,l' relatively prime to $n = (\operatorname{Per} R \vee \operatorname{Per} S)/(\operatorname{Div} R \wedge \operatorname{Div} S)$. Remark that whenever R and S are supplementary, then cR and cS are supplementary for every $c \in \mathbf{Q}_+$. Consequently, we are reduced to the consideration of the classes $kl'R$ and $lk'S$; furthermore, by eliminating the common factors of kl' and lk' we see that it suffices to consider the case when r and s are integers relatively prime each to the other and to n.

Set $a = \operatorname{Div} R$, $b = \operatorname{Div} S$, $u = \operatorname{Per} R$, $v = \operatorname{Per} S$, $t = u \vee v$. We consider first the case $s = 1$. In this situation, the conclusion will follow from Theorem 8.1 as soon as we show that rR and S are supplementary iff $rR + [t]$ and S are so. To this purpose we prove first the relations

$$ru \wedge v = u \wedge v\,, \tag{1}$$
$$ra \wedge b = a \wedge b\,, \tag{2}$$
$$ru \vee v = r(u \vee v)\,. \tag{3}$$

Indeed, we have

$$\frac{ru \wedge v}{a \wedge b} = \frac{ru}{a \wedge b} \wedge \frac{v}{a \wedge b}$$

so that $(ru \wedge v)/(a \wedge b)$ is an integer. Moreover,

$$\frac{ru \wedge v}{a \wedge b} \mid \frac{ru}{a \wedge b}, \frac{ru \wedge v}{a \wedge b} \mid \frac{v}{a \wedge b}, \frac{v}{a \wedge b} \mid \frac{u \vee v}{a \wedge b} = n .$$

As $r \wedge n = 1$, it follows from the second and the third of the above relations that $(ru \wedge v)/(a \wedge b)$ is relatively prime to r so that the first of these relations implies

$$\frac{ru \wedge v}{a \wedge b} \mid \frac{u}{a \wedge b},$$

that is $ru \wedge v \mid u$. It follows that $ru \wedge v \mid u \wedge v$ and hence (1) is true. The equality (2) is similarly proved. Finally,

$$ru \vee v = \frac{ruv}{ru \wedge v} = \frac{ruv}{u \wedge v} = r(u \vee v).$$

By Proposition 7.1, rR and S are supplementary iff

$$(\mathrm{Nrp}\ rR)\ (\mathrm{Nrp}\ S) = \frac{\mathrm{Per}\ rR \wedge \mathrm{Per}\ S}{\mathrm{Per}\ (rR + S)}$$

while $rR + [t]$ and S are supplementary iff

$$\mathrm{Nrp}(rR + [t])\ \mathrm{Nrp}\ S = \frac{\mathrm{Per}\ (rR + [t]) \wedge \mathrm{Per}\ S}{\mathrm{Per}\ (rR + [t] + S)} .$$

Obviously $rR + [t] + S = rR + S$ and $\mathrm{Nrp}\ rR = \mathrm{Nrp}\ R$, while Proposition 3.7 gives $\mathrm{Nrp}(rR + [t]) = \mathrm{Nrp}\ R$ and $\mathrm{Per}\ (rR + [t]) = \mathrm{Per}\ R$. Hence the conclusion follows taking into account (1).

We now consider the general case. By the part of the proof above, R and S are supplementary if rR and S are so. As s is relatively prime to r and to n, it is relatively prime to

$$\frac{\mathrm{Per}\ S \vee \mathrm{Per}\ rR}{\mathrm{Div}\ S \wedge \mathrm{Div}\ rR} = rn .$$

(We have used (2) and (3).) By the same part of the proof again, S and rR are supplementary iff sS and rR are so. The proof is complete.

COROLLARY 8.1. *Let $\mathcal{C}$ be a regular complementary canon on l voices and let k be a nonzero integer relatively prime to the modulus of $\mathcal{C}$. Then the canons in the class Can($k\mathrm{Grd}\mathcal{C}$ + [Per Grd $\mathcal{C}$] , Met $\mathcal{C}$) are regular complementary canons on l voices built on kGrd $\mathcal{C}$ + [Per Grd $\mathcal{C}$] and admitting the*

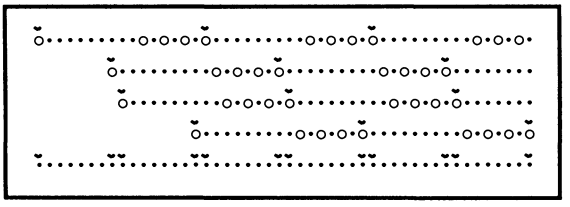
same primary metric class as $\mathcal{C}$, while the canons in the class Can(Grd $\mathcal{C}$, kMet $\mathcal{C}$ + [Per Grd $\mathcal{C}$]) are regular complementary canons on l voices built on the same ground class as $\mathcal{C}$ and admitting kMet $\mathcal{C}$ + [Per Grd $\mathcal{C}$] as the primary metric class and kMet $\mathcal{C}$ as a metric class of order $|k|$.

COROLLARY 8.2. *Let $\mathcal{C}$ be a regular complementary canon on l voices and let k be a nonzero integer relatively prime to the modulus of $\mathcal{C}$. Then the canons in the class Can(kGrd$\mathcal{C}$, Met $\mathcal{C}$) are regular complementary canons on $|k|l$ voices built on kGrd $\mathcal{C}$ and admitting the same primary metric class as $\mathcal{C}$.*

Theorem 8.2 also has the following consequence: Suppose that some regular complementary canon is built on some rhythmic class R. Then there is a regular complementary canon $\mathcal{C}'$ also built on R and admitting a rhythmic class whose period is *arbitrarily close to the period of* R as a metric class. Indeed, elementary number theory shows that for every $a \in \mathbf{Q}_+$ there are integers p, q relatively prime to the modulus of $\mathcal{C}$ so that $|\ (p/q)\ \text{Per}\ \mathit{Met}\ \mathcal{C} - \text{Per}\ R\ | < a$. By Theorem 8.2 it follows that the classes $R = \mathit{Grd}\ \mathcal{C}$ and $(p/q)\ \mathit{Met}\ \mathcal{C}$ are supplementary; hence any canon in the class *Can* (R, (p/q) *Met* $\mathcal{C}$) is a regular complementary canon built on R and admitting (p/q) *Met* $\mathcal{C}$ as a metric class, the period of the latter class differing by less than a from Per R. (Of course, this result has mainly a theoretical character, as the number of voices needed by $\mathcal{C}'$ may become arbitrarily large as a becomes arbitrarily small.) On the other hand, Theorem 7.1 shows that for those regular complementary canons whose ground numbers have the form p^k with p a prime and $k \geq 1$, the words "arbitrarily close" in the above statement cannot be replaced by "equal."

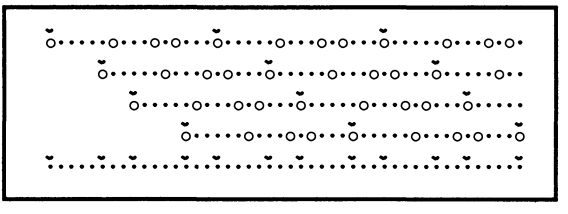
It is by now quite obviously the fact that whenever R and S are supplementary rhythmic classes, then $kR + [b]$ and $kS + [b]$ are also supplementary rhythmic classes for every integer $k \neq 0$ relatively prime to b/a, where $a = \text{Div}\ R \wedge \text{Div}\ S$ and $b = \text{Per}\ R \vee \text{Per}\ S$. Hence Theorem 8.1 brings significative information only in the situation when $kR + [b] \neq R$ and $kS + [b] \neq S$; or equivalently, $kH_{a,b}(R) \neq H_{a,b}(R)$ and $kH_{a,b}(S) \neq H_{a,b}(S)$. We have already mentioned in Section 2 that there are no supplementary translation classes $M, N \in T(\mathbf{Z}_{12})$ so that $kM \neq M$ and $kN \neq N$ for some integer $k \neq 0$ relatively prime to 12. Such classes do exist, for instance in $\mathbf{Z}_{16}$. As an illustration, consider the canon $\mathcal{C}$ of modulus 16 presented in Example 7.10. We have $3\mathit{Grd}\ \mathcal{C} + [1] \neq \mathit{Grd}\ \mathcal{C}$ and $3\mathit{Met}\ \mathcal{C} + [1] \neq \mathit{Met}\ \mathcal{C}$. In the following four examples we shall transform the canon $\mathcal{C}$ by multiplication and by condensed multiplication.

Recall that the class of $\mathcal{C}$ equals *Can*([♩. ♪♪♩ ♩] , [♩.. ♪]).



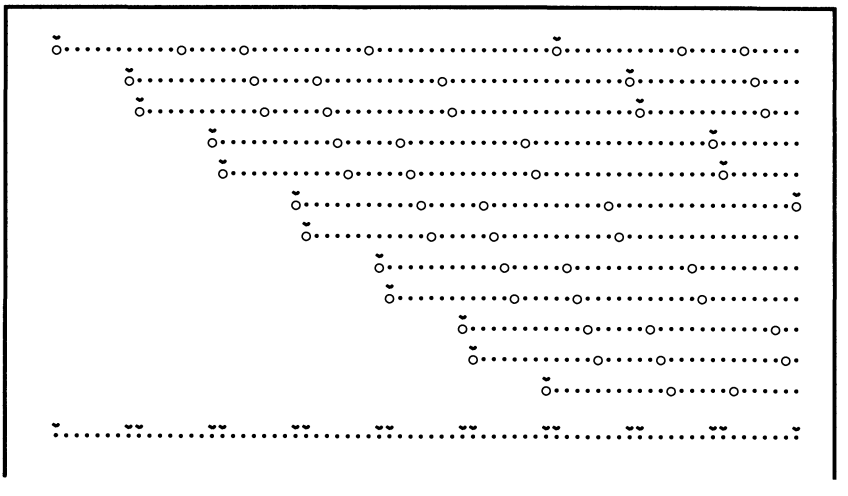
EXAMPLE 8.1: A REGULAR COMPLEMENTARY CANON ON FOUR VOICES OF CLASS

$$Can(3[\ \text{♩.}\ \text{♪}\text{♫}\ \text{♩}\ ] + [1]\,,\,[\ \text{♩..}\ \text{♪}\ ]) = Can([\text{♩}\frown\text{♫}\text{♫}]\,,\,[\ \text{♩..}\ \text{♪}\ ])$$



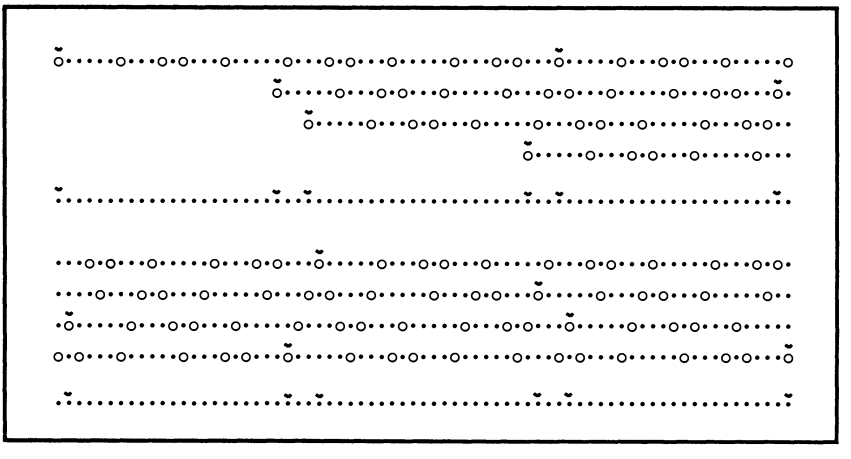
EXAMPLE 8.2: A REGULAR COMPLEMENTARY CANON ON FOUR VOICES OF CLASS

$$Can([\ \text{♩.}\ \text{♪}\text{♫}\ \text{♩}\ ]\,,\,3\,[\ \text{♩..}\ \text{♪}\ ] + [1]) = Can([\ \text{♩.}\ \text{♪}\text{♫}\ \text{♩}\ ]\,,\,[\text{♩}\frown\text{♫.}\ ])$$



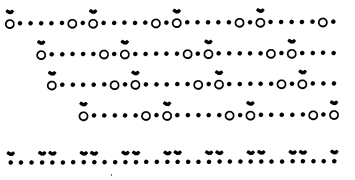
EXAMPLE 8.3: A REGULAR COMPLEMENTARY CANON ON TWELVE VOICES OF CLASS

$$Can((-3)\,[\ \text{♩.}\ \text{♪}\text{♪}\ \text{♩}\ ]\,,[\ \text{♩..}\ \text{♪}\ ])$$
$$= Can(1/16[12,6,12,18]\,,\,1/16[7,1])$$



EXAMPLE 8.4: THE CLASS 3 [♩.. ♪] ADMITTED BY $\mathcal{C}$ AS A METRIC CLASS OF ORDER 3

The following regular complementary canon



outlines an interesting property of the class [♩.♫] : this class together with a multiple of itself (in our case 2 [♩.♫]) form a supplementary pair. There are many other rhythmic classes S with the property that S and aS are supplementary for some $a \in \mathbf{Q} \setminus \{0\}$. For instance, all the classes [♩ ♫. ♫.], [♩ ♫ ♫. ♩], [♩ ♫ ♫♫], [♩. 𝅘𝅥𝅯♫ ♩] have the mentioned property, with $a = 2$.

In order that a rhythmic class S has the property that S and aS are supplementary for some $a \in \mathbf{Q} \setminus \{0\}$, it is necessary that S satisfies the relation

$$(\text{Nrp } S)^2 = \text{Per } S/\text{Div } S\,. \tag{4}$$

Indeed, if S and aS are supplementary, then we must have by Proposition 7.1

$$\begin{aligned}(\text{Nrp } S)^2 = (\text{Nrp } S)(\text{Nrp } aS) &= \frac{\text{Per } S \wedge \text{Per } aS}{\text{Per } (S + aS)} \\ &= \frac{\text{Per } S \wedge \text{Per } aS}{\text{Div } (S + aS)} = \frac{\text{Per } S \wedge \text{Per } aS}{\text{Div}S \wedge \text{Div}aS} \\ &= \frac{\text{Per } S \wedge |a| \text{ Per } S}{\text{Div } S \wedge |a| \text{ Div } S} = \frac{(1 \wedge |a|) \text{ Per } S}{(1 \wedge |a|) \text{ Div } S} = \frac{\text{Per } S}{\text{Div } S}\,.\end{aligned}$$

However, condition (4) is far from sufficient in order to ensure that S and aS are supplementary for some $a \in \mathbf{Q} \setminus \{0\}$, even when combined with the requirement that S should be a member of a supplementary pair.

EXAMPLE 8.5: SUPPLEMENTARY PAIRS OF THE FORM $(aS\,, S)$

Consider the rhythmic class S constructed in Example 7.12. This class admits a supplementary class (the class R in the same example) and verifies (4) because Nrp $S = 12$, Per $S = 144$, Div $S = 1$.

Suppose, if possible, that S and aS are supplementary for some $a \in \mathbf{Q} \setminus \{0\}$. We may assume that $a > 0$. Write $a = p_1/p_2$ with p_1 and p_2 relatively prime integers. It follows that p_1S and p_2S are supplementary. Write $p_i = 2^{k_i}3^{l_i}q_i$ $(i = 1,2)$ where q_i is an integer relatively prime to 2 and to 3. As q_1 and q_2 are relatively prime to the integer

$$\frac{\text{Per } 2^{k_1}3^{l_1}S \vee \text{Per } 2^{k_2}3^{l_2}S}{\text{Div } 2^{k_1}3^{l_1}S \wedge \text{Div } 2^{k_2}3^{l_2}S}\,.$$

it follows by Theorem 8.2 that $2^{k_1}3^{l_1}S$ and $2^{k_2}3^{l_2}S$ are supplementary. As $p_1 \wedge p_2 = 1$ we must have $2^{k_1}3^{l_1} \wedge 2^{k_2}3^{l_2} = 1$. Hence $\text{Div}(2^{k_1}3^{l_1}S + 2^{k_2}3^{l_2}S) = 1$ which implies that the regular class $2^{k_1}3^{l_1}S + 2^{k_2}3^{l_2}S$ must equal $[1]$. Now recall that, by the definition of the isomophism $H_{1,144}$, we have $S = [\varphi_{144}^{-1}(\mathrm{N})]$ where N is the set constructed in Example 7.12. The equality

$$2^{k_1}3^{l_1}S + 2^{k_2}3^{l_2}S = [1]$$

implies therefore

$$2^{k_1}3^{l_1}\varphi_{144}^{-1}(\mathrm{N}) + 2^{k_2}3^{l_2}\varphi_{144}^{-1}(\mathrm{N}) = \mathbf{Z}\,.$$

Applying the homomorphism φ_{144} to both sides of this equality we obtain

$$2^{k_1}3^{l_2}\mathrm{N} + 2^{k_2}3^{l_2} = \mathbf{Z}_{144}\,.$$

In other words, the map $f: 2^{k_1}3^{l_1}\mathrm{N} \times 2^{k_2}3^{l_2}\mathrm{N} \to \mathbf{Z}_{144}$ defined by $f(x_1, x_2) = x_1 + x_2$ is onto. Consequently,

$$144 \leq (\#2^{k_1}3^{l_1}\mathrm{N})\,(\#2^{k_2}3^{l_2}\mathrm{N}) \leq (\#\mathrm{N})^2 = 144$$

which is possible only if

$$\#2^{k_1}3^{l_1}N = \#2^{k_2}3^{l_2}\mathrm{N} = \#\mathrm{N}\,.$$

That is, the maps f_i: $\mathrm{N} \to \mathbf{Z}_{144}$ defined by $f_i(x) = 2^{k_i}3^{l_i}x$ $(i = 1,2)$ must be one-to-one. Observe now that at least one of the integers k_1, l_1, k_2, l_2 is not equal to 0; otherwise we would obtain the contradiction that S and S are supplementary. This implies that at least one of the maps

$$g_2 : \mathbf{N} \to \mathbf{Z}_{144}\,,\ g_2(x) = 2x\,,$$
$$g_3 : \mathbf{N} \to \mathbf{Z}_{144}\,,\ g_3(x) = 3x$$

must be one-to-one. To see this, suppose for instance that $k_1 \neq 0$. Then f_1 equals the composition of the maps

$$\mathbf{N} \overset{g_2}{\to} \mathbf{Z}_{144} \overset{h}{\to} \mathbf{Z}_{144}\,,\ h(x) = 2^{k_1-1}3^{l_1}x$$

so that if f_1 is one-to-one, then g_2 must also be so. We have arrived at a contradiction, as in fact none of the maps is one-to-one. Indeed,

$$g_2(36) = g_2(108)\,,$$
$$g_3(55) = g_3(103)\,.$$

EXAMPLE 8.6: A RHYTHMIC CLASS S WHICH ADMITS A SUPPLEMENTARY CLASS, VERIFIES CONDITION (4), BUT SO THAT S AND aS ARE SUPPLEMENTARY FOR NO $a \in \mathbf{Q} \setminus \{0\}$

9. Completion of the Proofs of Theorems 2.1–2.3. The Role of Convolution and of Fourier Transform in the Analysis of Supplementary Sets

This section contains those parts of the proofs of the theorems indicated in the title which are, from a mathematical viewpoint, above the relatively elementary level at which the proofs presented so far in this paper have been situated. Even if reading the material in this section might cause difficulties to some readers (I do hope that the number of such readers will decrease rapidly in the near future), I finally decided to include it in the concluding part of this study. In making this decision I have been much encouraged by reading and reviewing (Vuza 1988) David Lewin's book (1987), which emphatically marked the introduction of mathematical structures and reasoning into music-theoretic activities, and has set "standards for formal music-theoretical discourse which match those of other disciplines" (Rahn 1987).

In fact, some of the results in the preceding sections, such as Corollary 7.3, are quite intriguing. I thought there might be readers who are not merely satisfied to take notice of the statement of these results, but are also

willing to follow the arguments in rigorous proofs of them. And besides, there are two other serious reasons for presenting those proofs in detail.

Firstly, there is a logical motivation. Most of the musical theories involving algebraic properties of subsets of $\mathbf{Z}_n$ restrict themselves to the case $n = 12$, as this corresponds to the classical and familiar situation of the universe of twelve pitch classes. In such a theory, a formal proof of a theorem concerning subsets of $\mathbf{Z}_{12}$ is not necessary *from a strictly logical point of view*, as the theorem's correctness could be verified by inspecting each of the 2^{12} subsets of $\mathbf{Z}_{12}$, or, if the nature of the theorem allows it, each of the 352 translation classes of $\mathbf{Z}_{12}$, or fewer cases if further reductions are possible: strictly speaking, a job for a computer! (Of course, from the methodological viewpoint, a formal proof could be much more instructive than a proof "by inspection.") The situation is completely different with the rhythmic model employed in this paper. The rhythmic phenomena it describes involve groups $\mathbf{Z}_n$ indexed by unrestricted integers n. For instance, we know that Theorem 0.1 is true for $n = 12$. Is it true for larger values of n? We could (only just) verify its correctness as n ranges from 2 to, say, 70, by inspecting these cases with the aid of a computer. We might be obliged to stop at 70, as larger values would perhaps be beyond the possibilities of the machine. Could this verification be taken as a basis for conjecturing the correctness of Theorem 0.1 for all values of n? By now we already know that such a conjecture would be false: Theorem 0.1 is false for $n = 72$. However, the theorem is again true in the range $72 < n < 120$. That rather curious behavior calls for a precise determination of the set of integers for which the theorem in question is true; this can be achieved only by mathematical reasoning, the resort to formal proofs becoming thus a strong necessity even from the strictly logical point of view.

Secondly, there is a methodological point. The mathematical tools mainly used in the analysis of supplementary sets are convolution and Fourier transform. The use of these tools in connection with the theory of pitch-class sets goes back to Lewin 1959. On page 103 of his book (1987), Lewin insists again on the significance of convolution in studying music-theoretic concepts such as the interval function (defined on page 88 of that book). In fact, Lewin indicates several questions arising from consideration of the interval function, and he concludes that "this is all a vast open ground for mathematical and musical inquiry, even in atonal set-theory." He observes afterwards that when the language of groups and convolution is used, all of his questions "may then be generalized to questions about the interrelations, in a locally compact group, among the characteristic functions of compact subsets." One of his questions, when translated into that language, leads to the formulation of the following very general mathematical problem: "Given compact subsets [of a locally compact group] X_1, X_2, Y_1, and Y_2 with characteristic functions f_1, f_2, g_1, and g_2, under what

conditions will $f_1^* * g_1$ and $f_2^* * g_2$ be the same function?" (Lewin denotes by f^* the function $x \mapsto f(-x)$; the symbol $f * g$ stands for the convolution of f and g.) The theory of supplementary sets may be viewed as subsumed to the above problem, as every couple (X_1, Y_1) , (X_2, Y_2) of pairs of supplementary subsets of $\mathbf{Z}_n$ furnishes an example of sets X_1, X_2, Y_1, and Y_2 satisfying the conditions in that problem (because $f_1^* * g_1(x) = f_2^* * g_2(x) = 1$ for every $x \in \mathbf{Z}_n$; see Lemma 9.1 below, which, in terms of the interval function defined in the setting of the generalized interval system canonically associated to the group $\mathbf{Z}_n$, may be restated as: two subsets X, Y of $\mathbf{Z}_n$ are supplementary iff the X/Y interval function is identically equal to one). The fact that there is, at least for the moment, no obvious way to relate a supplementary pair to another shows how complex the problem stated by Lewin may be, even in the case of finite groups of simple structure such as the groups $\mathbf{Z}_n$.

Convolution also appears, although not explicitly stated, in another of Lewin's articles (1981) devoted this time to the study of a rhythmic problem.[1] Do convolution and Fourier transform "remain outside the grasp of most music theorists," as John Rahn states in his review of Lewin's book (Rahn 1987)? For instance, Fourier transforms is of major importance in the mathematical modelling of phenomena involving periodicity, and periodicity is one of the characteristics of major importance in the class of musical phenomena. It is therefore my conviction that in the near future music theory will integrate convolution and Fourier transform as effective investigation tools, music theorists being able to use them in the same way as presently they make use of groups, homomorphisms, group actions, and so forth; I should be very glad if the material in this section represented a contribution to progress in that direction.

The exposition which follows is (at least in principle) self-contained, with the only exception represented by an appeal to a theorem from higher algebra (an appropriate reference being indicated).

First of all let me recall some facts about convolution.

Let G be a (commutative) finite group and let R be a commutative ring. The *group algebra* R[G] is defined as the set of all functions $F:G \to R$ endowed with the following algebraic operations:

- the addition of two functions F_1 , F_2 defined "pointwise" by the formula

$$(F_1 + F_2)(x) = F_1(x) + F_2(x) \qquad \text{(C1)}$$

for every $x \in G$;

- the multiplication between an element $a \in R$ and a function F also defined pointwise by

$$(aF)(x) = aF(x) \; ; \qquad (C2)$$

- the convolution between F_1 and F_2, denoted $F_1 * F_2$ and defined by the formula

$$(F_1 * F_2)(x) = \sum_{y \in G} F_1(y) F_2(x - y) \; .$$

With respect to these operations, R[G] becomes a commutative algebra over R. If G_1 and G_2 are groups, every group homomorphism φ from G_1 *onto* G_2 gives rise to a map $\overline{\varphi} : R[G_1] \to R[G_2]$ defined by

$$(\overline{\varphi} F)(y) = \sum_{\substack{x \in G_1 \\ \varphi(x) = y}} F(x)$$

for every $F \in R[G_1]$ and $y \in G_2$. By direct computation it is verified that $\overline{\varphi}$ is a homomorphism of algebras; in particular, $\overline{\varphi}(F_1 * F_2) = (\overline{\varphi} F_1) * (\overline{\varphi} F_2)$ for $F_1, F_2 \in R[G_1]$. If G_2 is reduced to the neutral element 0, $R[G_2]$ is canonically identified with R via the map $F \mapsto F(0)$. Hence the unique homomorphism $\varphi : G \to \{0\}$ gives rise, by the preceding construction, to an algebra homomorphism from R[G] onto R, which we denote by S. Explicitly,

$$S(F) = \sum_{x \in G} F(x)$$

The above constructions will be applied in the following, taking some group $\mathbf{Z}_n$ as G, $\mathbf{Z}$ or $\mathbf{Q}$ as R and some homomorphism $\varphi_{n,d}$ as φ. Clearly, $\mathbf{Z}[G]$ is a subalgebra of $\mathbf{Q}[G]$. In addition to the algebraic structure, the group algebra $\mathbf{Q}[G]$ has a structure of a partially ordered set, defined by

$$F_1 \leq F_2 \text{ if } F_1(x) \leq F_2(x) \text{ for every } x \in G.$$

Given an integer k and a function $F \in \mathbf{Z}[G]$, we write $k \mid F$ if $k \mid F(x)$ for every $x \in G$.

Most of the functions in the group algebra $\mathbf{Z}[G]$ to be considered will characteristic functions of subsets of G. We need therefore a notation for

characteristic functions. We shall prefer the notation $<M>$ to the customary notation χ_M as the former offers the typographical advantage of avoiding superposed subscripts. Thus if $M \subset G$, $<M>$ will be the function in [G] defined by $<M>(x) = 1$ if $x \in M$, $<M>(x) = 0$ if $x \in G \setminus M$.

Two characteristic functions will be of particular importance. The first is $<\{0\}>$ and will be denoted by E; the second is $<G>$ and will be denoted by C. To be rigorous we should use notations like E_G and C_G; however, it will always follow from the context which the group is that we are working within, and such complications will not be necessary. The importance of the function E lies in the fact that it is the unit element of $\mathbf{Z}[G]$ and $\mathbf{Q}[G]$; that is, $E * F = F * E = F$ for every $F \in \mathbf{Q}[G]$.

To simplify the notation once again, we shall write $<d>$ (instead of $<(n/d)\mathbf{Z}_n>$) for the characteristic function of the subgroup with d elements of $\mathbf{Z}_n$.

For further references we record here the formulas

$$<d> * <d> = d < d > \tag{C3}$$

for $d|n$;

$$<d_1> * <d_2> = <d_1 d_2> \tag{C4}$$

for $d_1|n$, $d_2|n$ and $d_1 \wedge d_2 = 1$;

$$(<p> * \overline{\varphi_{n,d}}F) \circ \varphi_{n,d} = <pn/d> * F \tag{C5}$$

for $F \in \mathbf{Q}[\mathbf{Z}_n]$, $d|n$ and $p|d$. Here "$\circ$" denotes composition of maps.

We consider next the Fourier transform. For our purposes it will suffice to define it only in the case of the groups $\mathbf{Z}_n$. Denote by $\mathbf{C}$ the field of all complex numbers. A complex number ω is said to be an *n-th root of unity* if $\omega^n = 1$. The set U_n of all n-th roots of unity is a cyclic subgroup with n elements of the multiplicative group of $\mathbf{C}$. For every $\omega \in U_n$, the least integer $k \geq 1$ such that $\omega^k = 1$ is called the *order* of ω. The order of every n-th root of unity divides n; those n-th roots of unity whose orders equal n are called *primitive n-th roots of unity*.

The set of all functions $F: U_n \to \mathbf{C}$ is organized as an algebra over $\mathbf{C}$ in the following way: addition of two functions and the product between a complex number and a function is defined as in (C1) and (C2), while multiplication is this time also defined pointwise, that is, $(F_1F_2)(\omega) = F_1(\omega)F_2(\omega)$ for every $\omega \in U_n$. The algebra so obtained is denoted by $\mathbf{C}(U_n)$ (to be distinguished from $\mathbf{C}[U_n]$!)

Given $n \geq 1$, we define a collection of homomorphisms $\chi_{n,\omega}: \mathbf{Z}_n \to U_n$, the subscript ω ranging over U_n (in Fourier analysis these homomorphisms

are called "the characters of the group $\mathbf{Z}_n$"). Namely, if $x \in \mathbf{Z}_n$, choose $k \in \mathbf{Z}$ so that $x = \varphi_n(k)$ and set $\chi_{n,\omega}(x) = \omega^k$; the correctness of the definition is easily verified. For every $F \in \mathbf{Q}[\mathbf{Z}_n]$, its Fourier transform $\hat{F}$ is defined as the element in $\mathbf{C}(U_n)$ given by the formula

$$\hat{F}(\omega) = \sum_{x \in \mathbf{Z}_n} F(x)\, \chi_{n,\omega}(x).$$

It is well known (or can be verified by direct computation) that *the Fourier transform* (that is, the map $F \mapsto \hat{F}$ from $\mathbf{Q}[\mathbf{Z}_n]$ into $\mathbf{C}(U_n)$) *is an algebra homomorphism from* $\mathbf{Q}[\mathbf{Z}_n]$ *into* $\mathbf{C}(U_n)$; in other words, we have

$$F_1 + F_2 = \hat{F}_1 + \hat{F}_2,$$

$$aF_1 = a\hat{F}_1,$$

$$F_1 * F_2 = \hat{F}_1 \hat{F}_2$$

for every $F_1, F_2 \in \mathbf{Q}[\mathbf{Z}_n]$ and $a \in \mathbf{Q}$. Moreover, it is known that *the Fourier transform is one-to-one.*[2]

The first four lemmas below indicate the close relationship between Fourier analysis and the study of supplementary sets.

LEMMA 9.1. *Two subsets* M,N of $\mathbf{Z}_n$ *are supplementary iff* $<M>*<N> = C$.

The proof is a simple verification and will be omitted.

LEMMA 9.2. *Let d be a divisor of n. The Fourier transform of* $<d> \in \mathbf{Z}[\mathbf{Z}_n]$ *is given by*

$$\hat{<d>}(\omega) = d \text{ if } \omega^{n/d} = 1,$$
$$\hat{<d>}(\omega) = 0 \text{ if } \omega^{n/d} \neq 1.$$

In particular, $\hat{E}(\omega) = 1$ for every $\omega \in U_n$ and $\hat{C}(\omega) = 0$ for every $\omega \in U_n \setminus \{1\}$.

Proof. The map $k \mapsto \varphi_n(kn/d)$ establishes a bijection between $\{0,\ldots,d-1\}$ and $(n/d)\mathbf{Z}_n$. Hence

$$\overset{\wedge}{<d>}(\omega) = \sum_{k=0}^{d-1} (\omega^{n/d})^k$$

and the conclusion is a consequence of the formula for summing a geometric progression.

LEMMA 9.3. *Let $d \neq 1$ be a positive divisor of n. For any $F \in \mathbf{Q}[\mathbf{Z}_n]$ the following conditions are equivalent:*

(i) $\hat{F}$ *vanishes at some primitive d-th root of unity;*

(ii) $\hat{F}$ *vanishes at all primitive d-th roots of unity;*

(iii) $$(E - \frac{1}{p_1} <p_1>)^* \ldots {}^*(E - \frac{1}{p_r} <p_r>)^* \overline{\varphi_{n,d}} F = 0 \qquad (1)$$

where $p_1, \ldots, p_r$ are all the distinct primes which divide d.

Proof. The equation $\hat{F}(\omega) = 0$ is an algebraic equation with rational coefficients in the unknown ω; hence, if some primitive d-th root of unity satisfies it, then every primitive d-th root of unity satisfies it. (This is a consequence of the well-known theorem about the irreducibility over $\mathbf{Q}$ of the d-th cyclotomic polynomial. A short proof of this theorem is presented, for instance, in Exercise 39 on page 23 of Ribenboim 1972.) Thus (i) $\Leftrightarrow$ (ii). To see that (ii) $\Leftrightarrow$ (iii) we need first the formula

$$(\overline{\varphi_{n,d}} F)(\omega) = \hat{F}(\omega) \qquad (2)$$

for every d-th root ω of unity (in the right side, ω is viewed as an n-th root of unity). To prove the formula, observe first that $\chi_{d,\omega}(\varphi_{n,d}(x)) = \chi_{n,\omega}(x)$ for every $x \in \mathbf{Z}_n$ and every d-th root of unity ω. Hence

$$(\overline{\varphi_{n,d}} F)(\omega) = \sum_{y \in \mathbf{Z}_d} (\overline{\varphi_{n,d}} F)(y) \chi_{d,\omega}(y)$$

$$= \sum_{y \in \mathbf{Z}_d} \sum_{\substack{x \in \mathbf{Z}_n \\ \varphi_{n,d}(x) = y}} F(x) \chi_{d,\omega}(y)$$

$$= \sum_{(y) \in \mathbf{Z}_d} \sum_{\substack{x \in \mathbf{Z}_n \\ \varphi_{n,d}(x) = y}} F(x)\, \chi_{n,\omega}(x)$$

$$= \sum_{x \in \mathbf{Z}_n} \mathrm{F}(x)\, \chi_{n,\omega}(x) = \hat{\mathrm{F}}(\omega)\ .$$

Now, the equality (1) holds iff the Fourier transform of its left side vanishes identically on U_d. The transform in question equals the product of the transforms of the factors

$$\mathrm{E} - \frac{1}{p_i} <p_i>$$

multiplied (according to (2)) by the restriction of $\hat{\mathrm{F}}$ to U_d. A d-th root ω of unity is not primitive iff $\omega^{d/p_i} = 1$ for some prime divisor p_i of d. It follows then from Lemma 9.2 that the Fourier transform of

$$(\mathrm{E} - \frac{1}{p_1} <p_1>) * \ldots * (\mathrm{E} - \frac{1}{p_r} <p_r>)$$

vanishes precisely at those d-th roots of unity which are not primitive. Hence the transform of the left side of (1) vanishes identically on U_d iff F vanishes at every primitive d-th root of unity.

In view of subsequent applications of Lemma 9.3 we record here the identity

$$((\mathrm{E} - \frac{1}{p_1} <p_1>) * \ldots * (\mathrm{E} - \frac{1}{p_r} <p_r>) * \overline{\varphi_{n,d}}\mathrm{F}) \circ \varphi_{n,d}$$

$$= <n/d> * \mathrm{F} + \sum_{\substack{\mathrm{P} \subset \{1, \ldots, r\} \\ \mathrm{P} \neq \varnothing}} \frac{(-1)^{\#\mathrm{P}}}{\prod_{i \in \mathrm{P}} p_i} <(n/d) \prod_{i \in \mathrm{P}} p_i> * \mathrm{F}$$

which follows by expanding the left side of (1) and taking into account (C4) and (C5).

Given a divisor $d \neq$ of 1 n, we shall denote by I_d^n the set of all $\mathrm{F} \in \mathbf{Q}[\mathbf{Z}_n]$ satisfying the equivalent conditions of Lemma 9.3.

LEMMA 9.4. *For any* F_1 , $\mathrm{F}_2 \in \mathbf{Q}[\mathbf{Z}_n]$ *the following conditions are equivalent:*

(i) $F_1 * F_2 = aC$ *for some* $a \in \mathbf{Q}$;

(ii) *For every divisor* $d \neq 1$ of n, *at least one of the functions* F_1, F_2 *belongs to* I_d^n.

Proof. (i)=>(ii): Applying the Fourier transform to both sides of $F_1 * F_2 = aC$ yields, according to Lemma 9.2, $\hat{F}_1(\omega)\hat{F}_2(\omega) = 0$ for every $\omega \in U_n \setminus \{1\}$. The conclusion is then a consequence of Lemma 9.3.

(ii) => (i): Set $a = S(F_1)S(F_2)/n$. If $\omega \in U_n \setminus \{1\}$, then $\hat{F}_1(\omega)\hat{F}_2(\omega) = 0$ by hypothesis and $\hat{C}(\omega) = 0$ by Lemma 9.2. Hence

$$F_1 * F_2(\omega) = aC(\omega)$$

in this case. If $\omega = 1$ then

$$F_1 * F_2(1) = S(F_1)S(F_2) = an = aC(1) .$$

The Fourier transforms of $F_1 * F_2$ and aC being equal, it follows that $F_1 * F_2 = aC$.

We are now in position to prove one of the theorems in Section 2.

Proof of Theorem 2.3. Let M,N be two supplementary subsets of $\mathbf{Z}_n$ and let k be relatively prime to n. We prove the formula

$$<kM>(\omega) = <M>(\omega^k) \qquad (1)$$

for every $\omega \in U_n$. Indeed, the map $x \mapsto kx$ is an automorphism of $\mathbf{Z}_n$, which we denote by θ. We have

$$<kM>(\omega) = \sum_{x \in \mathbf{Z}_n} <\theta(M)>(x)\chi_{n,\omega}(x) = \sum_{x \in \mathbf{Z}_n} <M>(\theta^{-1}(x))\chi_{n,\omega}(x)$$

$$= \sum_{x \in \mathbf{Z}_n} <M>(x)\chi_{n,\omega}(\theta(x)) = \sum_{x \in \mathbf{Z}_n} <M>(x)\chi_{n,\omega^k}(x)$$

$$= <M>(\omega^k).$$

As $\omega \mapsto \omega^k$ is an automorphism of the group U_n, it leaves invariant the set of primitive d-th roots of unity. Therefore, it follows from this remark and from (1) that $<M> \in I_d^n$ iff $<kM> \in I_d^n$. Hence $<M>$ and $<N>$ satisfy condition (ii) in Lemma 9.4 iff $<kM>$ and $<N>$ satisfy it. It then follows

from Lemmas 9.1 and 9.4 that $<k\mathrm{M}> * <\mathrm{N}> = a\mathrm{C}$ for some $a \in \mathbf{Q}$. Applying the homomorphism S to both sides of this equality we get

$$an = \mathrm{S}(a\mathrm{C}) = \mathrm{S}(<k\mathrm{M}>) * <\mathrm{N}>) = \mathrm{S}(<k\mathrm{M}>)\mathrm{S}(<\mathrm{N}>)$$
$$= (\#k\mathrm{M})(\#\mathrm{N}) = (\#\mathrm{M})(\#\mathrm{N}) = n.$$

Hence $a=1$ and Lemma 9.1 shows that kM and N are supplementary.

The next series of lemmas are technical steps leading to the proofs of Theorems 2.1 and 2.2.

The stability subgroup of a function $\mathrm{F} \in \mathbf{Q}[\mathbf{Z}_n]$ is defined as the subgroup of those $y \in \mathbf{Z}_n$ with the property that $\mathrm{F}(x + y) = \mathrm{F}(x)$ for every $x \in \mathbf{Z}_n$. Clearly the stability subgroup of $<\mathrm{M}>$ coincides with the stability subgroup of the subset M of $\mathbf{Z}_n$ as defined in Section 1. The function F is called d-periodic if its stability subgroup contains the subgroup with d elements of $\mathbf{Z}_n$.

LEMMA 9.5. *For every divisor d of n and every $\mathrm{F} \in \mathbf{Q}[\mathbf{Z}_n]$ the following conditions are equivalent*:

(i) F *is d-periodic;*

(ii) $(\mathrm{E} - \frac{1}{d}<d>) * \mathrm{F} = 0$;

(iii) *There is* $\mathrm{F}_1 \in \mathbf{Q}[\mathbf{Z}_{n/d}]$ *such that* $\mathrm{F} = \mathrm{F}_1 \circ \varphi_{n,n/d}$;

(iv) *There is* $\mathrm{F}_2 \in \mathbf{Q}[\mathbf{Z}_n]$ *such that* $\mathrm{F} = <d> * \mathrm{F}_2$.

In (iii) *and* (iv) *above, the field* $\mathbf{Q}$ *may be replaced by the ring* $\mathbf{Z}$ *whenever* $\mathrm{F} \in \mathbf{Z}[\mathbf{Z}_n]$.

The proof is an easy consequence of the remark that F is d-periodic iff it is constant on each coset of $\mathbf{Z}_n$ modulo $(n/d)\mathbf{Z}_n$. We omit the details.

LEMMA 9.6. *Let p be a prime and let* $\mathrm{F}_1, \mathrm{F}_2 \in \mathbf{Z}[\mathbf{Z}_{p^r}]$ *be such that* $\mathrm{F}_1 \geq 0$, $\mathrm{S}(\mathrm{F}_1) = p^k$ *for some* $k \geq 0$ *and*

$$\mathrm{F}_1 * \mathrm{F}_2 = m\mathrm{C} \tag{1}$$

with p non$|m$. *Then* $\mathrm{F}_1 \leq \mathrm{C}$.

Proof. We argue by induction on r. For $r = 0$, the relation (1) becomes $\mathrm{F}_1(0)\mathrm{F}_2(0) = m$; as $\mathrm{F}_1(0) = p^k$ and p non$|m$, we necessarily have $\mathrm{F}_1(0) = 1$.

Suppose the result true for $r-1$ and let us prove it for r. By Lemmas 9.3–9.5, the hypothesis (1) implies the existence of $F_3 \in \mathbf{Z}[\mathbf{Z}_{p^{r-1}}]$ such that either $F_1 = F_3 \circ \varphi_{p^r,p^{r-1}}$ or $F_2 = F_3 \circ \varphi_{p^r,p^{r-1}}$. In the first case it follows by applying the homomorphism $\overline{\varphi_{p^r,p^{r-1}}}$ to both sides of (1) that

$$(pF_3) * (\overline{\varphi_{p^r,p^{r-1}}}F_2) = (\overline{\varphi_{p^r,p^{r-1}}}F_1) * (\overline{\varphi_{p^r,p^{r-1}}}F_2) = pmC,$$

hence $F_3 * \overline{\varphi_{p^r,p^{r-1}}}F_2 = mC$; as $F_3 \geq 0$ and $S(F_3) = p^{k-1}$, the induction hypothesis yields $F_3 \leq C$, which implies $F_1 \leq C$. Similarly, in the second case we obtain from (1)

$$(\overline{\varphi_{p^r,p^{r-1}}}F_1) * F_3 = mC\,.$$

As $\overline{\varphi_{p^r,p^{r-1}}}F_1 \geq 0$ and $S(\overline{\varphi_{p^r,p^{r-1}}}F_1) = p^k$, the induction hypothesis yields $\overline{\varphi_{p^r,p^{r-1}}}F_1 \leq C$; taking now into account the fact that $F_1 \geq 0$, the latter relation implies $F_1 \leq C$.

LEMMA 9.7. *Let $p_1, \ldots, p_r$ be some distinct primes dividing n and let $M \subset \mathbf{Z}_n$ be a subset such that $<p_1 \ldots p_r> * <M> \leq C$. Then the function*

$$F = (E - \frac{1}{p_1} <p_1>) * \ldots * (E - \frac{1}{p_r} <p_r>) * <M>.$$

has the property that $F(x) \neq F(y)$ for any $x \in M$ and $y \in \mathbf{Z}_n \setminus M$.

Proof. The conclusion of the lemma will be a consequence of the following more precise statement: for any $x \in \mathbf{Z}_n$ such that $F(x) \neq 0$, there is a partition of $\{1, \ldots, r\}$ into two subsets I , J such that

$$F(x) = (-1)^{\#J} \prod_{i \in I} (1 - \frac{1}{p_i}) \prod_{j \in J} \frac{1}{p_j}\ ; \qquad (1)$$

the case $J = \varnothing$ occurs iff $x \in M$.

Indeed, once this is proved, it follows that F assumes on M the constant value

$$a = \prod_{i=1}^{r} (1 - \frac{1}{p_i}) \qquad (2)$$

while on $\mathbf{Z}_n \setminus M$ it assumes either the value 0 or a value of the form (1) with $J \neq \varnothing$. If $\#J$ is odd, then $F(x) < 0$ while $a > 0$. If $\#J$ is even, then

$$\prod_{j\in J}(1-\frac{1}{p_j}) > \prod_{j\in J}\frac{1}{p_j}$$

as $1-\frac{1}{p_j}\geq\frac{1}{p_j}$ for all $j\in J$ and $1-\frac{1}{p_j}>\frac{1}{p_j}$ for at least one $j\in J$; hence

$$F(x) = \prod_{i\in I}(1-\frac{1}{p_i})\prod_{j\in J}\frac{1}{p_j} < \prod_{i\in I}(1-\frac{1}{p_i})\prod_{j\in J}(1-\frac{1}{p_j}) = a.$$

Now we prove the statement by induction on r; the case $r = 1$ being immediate, we assume the statement true for $r-1$ and we prove it for r. A direct computation based on the identity (C6) (with $d = n$) and on the hypothesis $<p_1\ldots p_r>*<M>\leq C$ shows that F assumes on M the value given by (2). Now let $x\in\mathbf{Z}_n\setminus M$ be such that $F(x)\neq 0$. There is $i_0\in\{1,\ldots,r\}$ such that $<q_{i_0}>*<M>(x) = 0$, where

$$q_i = \prod_{\substack{1\leq j\leq r\\ j\neq i}} p_j$$

for any $i\in\{1,\ldots,r\}$; for otherwise, we would find for every $i\in\{1,\ldots,r\}$ an $x_i\in M$ such that $x - x_i\in(n/q_i)\mathbf{Z}_n$. As $(n/q_i)\mathbf{Z}_n\subset(n/p_1\ldots p_r)\mathbf{Z}_n$ and $<p_1\ldots p_r>*<M>\leq C$, all the x_i's must equal some element $x_0\in M$; consequently,

$$x - x_0\in\bigcap_{i=1}^{r}(n/q_i)\mathbf{Z}_n = \{0\},$$

a contradiction. By changing notation, we may assume that $i_0 = r$. Again the identity (C6) shows that

$$(E-\frac{1}{p_1}<p_1>)*\ldots.*(E-\frac{1}{p_{r-1}}<p_{r-1}>)*<M>(x) = 0\ ;$$

therefore,

$$F(x) = -\frac{1}{p_r}(E-\frac{1}{p_1}<p_1>)*\ldots$$
$$*(E-\frac{1}{p_{r-1}}<(p_{r-1}>)*<p_r>*<M>(x). \quad (3)$$

The induction hypothesis is applicable to the set $N = (n/p_r)\mathbf{Z}_n + M$, as $\langle N\rangle = \langle p_r\rangle * \langle M\rangle$ and $\langle p_1 \dots p_{r-1}\rangle * \langle N\rangle \leq C$; hence, there is a partition of $\{1, \dots, r-1\}$ into two subsets I and J_1 such that

$$(E - \frac{1}{p_1}\langle p_1\rangle) * \dots * (E - \frac{1}{p_{r-1}}\langle p_{r-1}\rangle) * \langle N\rangle(x)$$
$$= (-1)^{\#J_1} \prod_{i\in I} (1 - \frac{1}{p_i}) \prod_{j\in J_1} \frac{1}{p_j}.$$

By letting $J = J_1 \cup \{r\}$, we infer from (3) and (4) that $F(x)$ has the form (1) with $J \neq \emptyset$.

LEMMA 9.8. *Let d_1 and d_2 be two divisors of n and let $M \subset \mathbf{Z}_n$ verify the equality*

$$(E - \frac{1}{d_1}\langle d_1\rangle) * (E - \frac{1}{d_2}\langle d_2\rangle) * \langle M\rangle = 0. \qquad (1)$$

Then M can be written as $M_1 \cup M_2$ with $M_1 \cap M_2 = \emptyset$ and M_i d_i-periodic for $i = 1,2$.

Proof. Set $d = d_1 \vee d_2$. It suffices to prove that for every $x \in M$, the set $M_x = (x + (n/d)\mathbf{Z}_n) \cap M$ is d_1-periodic or d_2-periodic: for then we can define M_1 as the set of those $x \in M$ for which M_x is d_1-periodic and M_2 as $M \setminus M_1$. Suppose that on the contrary, M_x is neigher d_1-periodic nor d_2-periodic for some $x \in M$. It follows that there are four elements u_1, v_1, u_2, v_2 such that $u_i \in M_x$, $v_i \in \mathbf{Z}_n \setminus M_x$ and $u_i - v_i \in (n/d_i)\mathbf{Z}_n$ for $i = 1,2$. Rewrite (1) as

$$\langle M\rangle - \frac{1}{d_1}\langle d_1\rangle * \langle M\rangle - \frac{1}{d_2}\langle d_2\rangle * \langle M\rangle + \frac{1}{d_1 d_2}\langle d_1\rangle * \langle d_2\rangle * \langle M\rangle = 0.$$

By evaluating the left side of the above relation at u_i and v_i and by taking into account the equalities $\langle M\rangle(u_i) = 1$, $\langle M\rangle(v_i) = 0$ for $i = 1,2$, we obtain

$$1 - \frac{1}{d_1}\langle d_1\rangle * \langle M\rangle(u_i) - \frac{1}{d_2}\langle d_2\rangle * \langle M\rangle(u_i) + \frac{1}{d_1 d_2}\langle d_1\rangle * \langle d_2\rangle * \langle M\rangle(u_i) = 0,$$

$$-\frac{1}{d_1} < d_1 > * < \mathrm{M} > (v_i) - \frac{1}{d_2} < d_2 > * < \mathrm{M} > (v_i)$$
$$+ \frac{}{d_1 d_2} < d_1 > * < d_2 > * < \mathrm{M} > (v_i) = 0 .$$

Subtracting these equalities (for $i = 1$, $i = 2$, respectively) and observing that $< d_i > * < \mathrm{M} > (u_i) = < d_i > * < \mathrm{M} > (v_i)$ and $< d_1 > * < d_2 > * < \mathrm{M} > (u_i) = < d_1 > * < d_2 > * < \mathrm{M} > (v_i)$, we get

$$d_1 = < d_1 > * < \mathrm{M} > (u_2) - < d_1 > * < \mathrm{M} > (v_2) ,$$
$$d_2 = < d_2 > * < \mathrm{M} > (u_1) - < d_2 > * < \mathrm{M} > (v_1) ,$$

But $0 \leq < d_i > * < \mathrm{M} > \leq d_i \mathrm{C}$; hence the above equalities can be satisfied only if $< d_1 > * < \mathrm{M} > (u_2) = d_1$, $< d_2 > * < \mathrm{M} > (u_1) = d_2$, $< d_1 > * < \mathrm{M} > (v_2) = < d_2 > * < \mathrm{M} > (v_1) = 0$. From these we infer the inclusions

$$u_2 + (n/d_1)\, \mathbf{Z}_n \subset M ,$$
$$v_1 + (n/d_2)\, \mathbf{Z}_n \subset \mathbf{Z}_n \setminus \mathrm{M} .$$

Consequently,

$$(u_2 + (n/d_1)\, \mathbf{Z}_n) \cap (v_1 + (n/d_2)\, \mathbf{Z}_n) = \varnothing .$$

But this is a contradiction, as can be seen as follows: we may write $u_2 - v_1$ as $x_1 + x_2$ with $x_i \in (n/d_i)\, \mathbf{Z}_n$ for $i = 1,2$. We obtain

$$\begin{aligned}
&(u_2 + (n/d_1)\, \mathbf{Z}_n) \cap (v_1 + (n/d_2)\, \mathbf{Z}_n) \\
&= v_1 + (\, (u_2 - v_1 + (n/d_1)\, \mathbf{Z}_n) \cap (n/d_2)\, \mathbf{Z}_n) \\
&= v_1 + (\, (x_2 + x_1 + (n/d_1)\, \mathbf{Z}_n) \cap (n/d_2)\, \mathbf{Z}_n) \\
&= v_1 + (\, (x_2 + (n/d_1)\, \mathbf{Z}_n) \cap (n/d_2)\, \mathbf{Z}_n) \\
&= v_1 + x_2 + (\, (n/d_1)\, \mathbf{Z}_n) \cap (-x_2 + (n/d_2)\mathbf{Z}_n)) \\
&= v_1 + x_2 + (n/d_1)\mathbf{Z}_n \cap (n/d_2)\, \mathbf{Z}_n \neq \varnothing
\end{aligned}$$

which establishes the announced contradiction.

Proof of the implication (i) => (ii) *in Theorem* 2.1. We distinguish between two cases.

Suppose first that for every $\omega \in \mathrm{U}_n$, the relation $<\mathrm{M}>(\omega) = 0$ implies $\omega^{n/p} = 1$. Then

$$(1 - \frac{1}{p} <p>(\omega))<N>(\omega) = 0 \qquad (1)$$

for every $\omega \in U_n$: indeed, if $\omega^{n/p} = 1$, then $<p>)(\omega) = p$ by Lemma 9.2. If $\omega^{n/p} \neq 1$, then $<\hat{M}>(\omega) = 0$ by our assumption; hence $<\hat{N}>(\omega) = 0$, as it follows from the equality $<\hat{M}>(\omega)<\hat{N}>(\omega) \neq 0$ obtained by applying the Fourier transform to both sides of the equality $<M>*<N> = C$. The relation (1) means that the Fourier transform of

$$(E - \frac{1}{p}<p>)*<N>$$

vanishes identically; hence

$$(E - \frac{1}{p}<p>)*<N> = 0,$$

that is N *is* p-periodic by Lemma 9.5.

In the second case we assume that the set

$$\overline{U}_n = \{ \omega \mid \omega \in U_n , <\hat{M}>(\omega) = 0 , \omega^{n/p} \neq 1 \}$$

is not empty. Write $n = p^r m$ with p non $\mid m$. Let G by the subgroup of $\mathbf{Z}_n$ generated by $(M - M) \cap p^{r-1}\mathbf{Z}_n$. Set $\#G = p^{r_1}m_1$ with p non $\mid m_1$; as $G \subset p^{r-1}\mathbf{Z}_n$ we have $0 \leq r_1 \leq 1$ and $m_1 \mid m$.

By applying the homomorphism $\overline{\varphi_{n,p^r}}$ to the equality $<M>*<N> = C$ we obtain $\overline{\varphi_{n,p^r}}<M>*\overline{\varphi_{n,p^r}}<N> = mC$. As $S(\overline{\varphi_{n,p^r}}<M>) = p^k$ and p non$|m$, Lemma shows that $\overline{\varphi_{n,p^r}}<M> \leq C$; in other words,

$$<m>*<M> \leq C .$$

It follows from (2) that $<d>*<M> \leq C$ for any divisor d of m; consequently, for any such d, the function $\overline{\varphi_{n,n/d}}<M>$ is the characteristic function of the subset $\varphi_{n,n/d}(M)$ of $\mathbf{Z}_{n/d}$, the latter subset being denoted, for the sake of brevity, by $M_{n/d}$.

Consider now an $\omega \in \overline{U}_n$. As $\omega^{n/p} \neq 1$, the order of ω can be written as $p^r d$ with p non $\mid d$ and $d \mid m$. We shall prove that $d \mid m/m_1$ and that $M_{p^r d}$ is p-periodic. Indeed, as ω is a primitive $p^r d$-th root of unity and $<\hat{M}>(\omega) = 0$, it follows from Lemma 9.3 that

$$(E - \frac{1}{p}<p>)*F = 0 \qquad (3)$$

where

$$F = (E - \frac{1}{p_s}<p_1>)* \ldots *(E - \frac{1}{p}<p_s>)*<M_{p^r d}>$$

and $p_1, \ldots, p_s$ are all the distinct prime divisors of d. By Lemma 9.5, it follows from (3) that F is p-periodic. On the other hand, it follows from (2) and (C5) that

$$<p_1 \ldots p_s> * <M_{p^r d}> \leq <d> * <M_{p^r d}> \leq C ; \tag{4}$$

consequently, Lemma 9.7 is applicable to the subset $M_{p^r d}$ yielding that $F(x) \neq F(y)$ for $x \in M_{p^r d}$ and $y \in \mathbf{Z}_{p^r d} \setminus M_{p^r d}$. This fact, combined with the p-periodicity of F, enables us to conclude that $M_{p^r d}$ is p-periodic.

We shall prove now that $d | m/m_1$ (equivalently, $\omega^{n/m_1} = 1$). Let $x_1, x_2 \in M$ be such that $x_1 - x_2 \in p^{r-1}\mathbf{Z}_n$. Set $y_i = \varphi_{n,p^r d}(x_i)$ for $i = 1,2$. We have $y_1, y_2 \in M_{p^r d}$ and $y_1 - y_2 \in p^{r-1}\mathbf{Z}_{p^r d}$; we may therefore write $y_1 - y_2 = u + v$ with $u \in p^{r-1} d\mathbf{Z}_{p^r d}$ and $v \in p^r \mathbf{Z}_{p^r d}$. As $M_{p^r d}$ was seen to be p-periodic, we have $y_2 + u \in M_{p^r d}$. Hence y_1 and $y_2 + u$ are elements in $M_{p^r d}$ lying in the same coset of $\mathbf{Z}_{p^r d}$ modulo $p^r \mathbf{Z}_{p^r d}$. By (4), this is possible only if $y_1 = y_2 + u$. Hence $y_1 - y_2 \in p^{r-1} d\mathbf{Z}_{p^r d}$ so that $x_1 - x_2 \in \varphi^{-1}{}_{n,p^r d}(p^{r-1} d\mathbf{Z}_{p^r d}) = p^{r-1} d\mathbf{Z}_n$. We have thus proved the inclusion $(M - M) \cap p^{r-1}\mathbf{Z}_n \subset p^{r-1} d\mathbf{Z}_n$, which implies $G \subset p^{r-1} d\mathbf{Z}_n$ by the definition of G. Consequently, $p^{r-1} m_1 = \#G | pm/d$ so that $m_1 | m/d$ or equivalently, $d | m/m_1$.

As a consequence of what has just been proved, we learn that M_{n/m_1} is p-periodic. Indeed, observe first that because of $\operatorname{Ker} \varphi_{n,n/m_1} \subset p^{r-1}\mathbf{Z}_n$ we have

$$\begin{aligned}(M_{n/m_1} - M_{n/m_1}) \cap p^{r-1}\mathbf{Z}_{n/m_1} &= \varphi_{n,n/m_1}(M - M) \cap \varphi_{n,n/m_1}(p^{r-1}\mathbf{Z}_n) \\ &= \varphi_{n,n/m_1}((M - M) \cap p^{r-1}\mathbf{Z}_n) \subset \varphi_{n,n/m_1}(G) .\end{aligned}$$

By the definition of m_1 we have $\varphi_{n,n/m_1}(G) \subset (n/pm_1)\mathbf{Z}_{n/m_1}$ so that we finally get

$$(M_{n/m_1} - M_{n/m_1}) \cap p^{r-1}\mathbf{Z}_{n/m_1} \subset (n/pm_1)\mathbf{Z}_{n/m_1} . \tag{5}$$

To prove that M_{n/m_1} is p-periodic, take $x \in M_{n/m_1}$ and $u \in (n/pm_1)\mathbf{Z}_{n/m_1}$; we have to show that $x + u \in M_{n/m_1}$. Take an $\omega_0 \in U_n$ and let $p^r d$ be, as above, the order of ω_0. We have seen that $d | m/m_1$ and that $M_{p^r d}$ is p-periodic. Now remark that $M_{p^r d} = \varphi_{n/m_1,p^r d}(M_{n/m_1})$; as $\varphi_{n/m_1,p^r d}(u) \in p^{r-1} d\mathbf{Z}_{p^r d}$ we obtain $\varphi_{n/m_1,p^r d}(x) + \varphi_{n/m_1,p^r d}(u) \in M_{p^r d}$. Hence there is $y \in M_{n/m_1}$ such that $\varphi_{n/m_1,p^r d}(x + u) = \varphi_{n/m_1,p^r d}(y)$, that is, $x + u - y \in \operatorname{Ker} \varphi_{n/m_1,p^r d} \subset p^r \mathbf{Z}_{n/m_1}$. In conclusion, $x - y = -u + v$ with $x, y \in M_{n/m_1}$, $u \in (n/pm_1)\mathbf{Z}_{n/m_1}$ and $v \in p^r \mathbf{Z}_{n/m_1}$. Because of (5), the latter relation implies $-u + v \in (n/pm_1)\mathbf{Z}_{n/m_1}$ so that $v \in (p^r \mathbf{Z}_{n/m_1}) \cap ((n/pm_1)\mathbf{Z}_{n/m_1}) = \{0\}$ and $x + u = y \in M_{n/m_1}$. In particular, if $m_1 = 1$ then M is already p-periodic and the implication is proved in this case. We shall therefore assume in the following that $m_1 \neq 1$.

We prove now the equality

$$(E - \frac{1}{p}<p>)*(E - \frac{1}{m_1}<m_1>)*<N> = 0 \qquad (6)$$

by verifying that the Fourier transform of its left side vanishes identically. Indeed, by Lemma 9.2, $1 - \frac{1}{p}<p>(\omega) = 0$ if $\omega^{n/p} = 1$, while $1 - \frac{1}{m_1}<m_1>(\omega) = 0$ if $\omega^{n/m_1} = 1$. It remains to consider those $\omega \in U_n$ such that $\omega^{n/p} \neq 1$ and $\omega^{n/m_1} \neq 1$. Applying the Fourier transform to the equality $<M>*<N> = C$ we obtain $<\hat{M}>(\omega)<\hat{N}>(\omega) = 0$. The relation $<M>(\omega) = 0$ combined with $\omega^{n/p} \neq 1$ would imply that $\omega \in \overline{U}_n$. However, we have seen that $\omega^{n/m_1} = 1$ for every $\omega \in \overline{U}_n$, which contradicts our assumption on ω. Hence the only possibility left is $<\hat{N}>(\omega) = 0$ and this completes the verification.

We may now apply Lemma 9.8 in order to derive from (6) the existence of the sets N_1, N_2 such that $N = N_1 \cup N_2$, $N_1 \cap N_2 = \varnothing$, N_1 is p-periodic and N_2 is m_1-periodic. Rewrite $<M>*<N> = C$ as

$$<M>*(<N_1> + <N_2>) = C$$

and apply to both sides the homomorphism $\overline{\varphi_{n,n/m_1}}$; the result is

$$<M_{n/m_1}>*(\overline{\varphi_{n,n/m_1}}<N_1> + \overline{\varphi_{n,m_1}}<N_2>) = m_1 C . \qquad (7)$$

The m_1-periodicity of N_2 implies $\overline{\varphi_{n,n/m_1}}<N_2> = m_1<N_2'>$, where $N_2' = \varphi_{n,n/m_1}(N_2)$. Hence (7) becomes

$$<M_{n/m_1}>*\overline{\varphi_{n,n/m_1}}<N_1> = m_1(C - <M_{n/m_1}>*<N_2'>) . \qquad (8)$$

As $<M_{n/m_1}>$ and $\overline{\varphi_{n,n/m_1}}<N_1>$ are both p-periodic, it follows from Lemma 9.5(iv) and from (C3) that $p \mid <M_{n/m_1}>*\overline{\varphi_{n,n/m_1}}<N_1>$; as p non$|m_1$, the latter relation together with (8) imply that p must divide each value of the function $C - <M_{n/m_1}>*<N_2'>$. But these values are either 0 or 1, as clearly $C - <M_{n/m_1}>*<N_2'> \leq C$ while $C - <M_{n/m_1}>*<N_2'> \geq 0$ by (8); hence we necessarily have $C - <M_{n/m_1}>*<N_2'> = 0$ which implies, by virtue of (8), $N_1 = \varnothing$. In conclusion N is m_1-periodic and the implication (i) => (ii) in Theorem 2.1 is completely proved.

In the course of the proof of the implication (i) =>(ii) in Theorem 2.2 we shall need

LEMMA 9.9. *Let n verify condition* (ii) *in Theorem* 2.2, *let m be a multiple of n and let* M,N *be supplementary subsets of* $\mathbf{Z}_m$ *verifying the following conditions:*

(i) $\#M|<n>*<M>$;

(ii) $<n>*<N> = (n/\#M)C$;

(iii) $n/\#M$ *is a prime.*

Then at least one of the subsets M,N *is periodic.*[3]

Proof. Replacing, if necessary, M by $x + M$ for some $x \in \mathbf{Z}_m$, we may assume that $<n>*<M>(0) = \#M$. The latter means that $M \subset (m/n)\mathbf{Z}_m$. For each $x \in \mathbf{Z}_m$ consider the subset $N_x = (x + N) \cap (m/n)\mathbf{Z}_m$ of $(m/n)\mathbf{Z}_m$. As M and N are supplementary, it follows (Proposition 2.1) that

$$(M - M) \cap (N_x - N_x) \subset (M - M) \cap (N - N) = \{0\} ;$$

from (ii) it follows that $(\#M)(\#N_x) = n$. Consequently, Proposition 2.1 shows that M and N_x are supplementary subsets of $(m/n)\mathbf{Z}_m$; as $(m/n)\mathbf{Z}_m$ is isomorphic to $\mathbf{Z}_n$ and n is supposed to satisfy condition (ii) in Theorem 2.2, we infer that at least one of the subsets M , N_x is periodic. If M is periodic, the proof is concluded. If M is not periodic, then N_x must be periodic for every $x \in \mathbf{Z}_m$. Now (iii) shows that N_x must be in fact $(n/\#M)$-periodic; hence N is also $(n/\#M)$-periodic, as

$$N = \bigcup_{x \in \mathbf{Z}_m} (-x + N_x).$$

Proof of the implication (i) => (ii) *in Theorem* 2.2. During the proof we shall make several uses of Lemmas 9.3–9.5 and of the identity (C6) without explicit references, as the reader who has followed us up to this point should be accustomed with the role played by those technical results.

By virtue of Theorem 2.1, it suffices to do the announced proof only in the cases to be considered below.

CASE A: $n = p^2q^2$, $\#M = \#N = pq$.

We must have $<M> \in I_n^n$ or $<N> \in I_n^n$. To make a choice, let $<M> \in I_n^n$. This is equivalent to

$$(E - \frac{1}{p}<p>)*(E - \frac{1}{q}<q>)*<M> = 0.$$

By Lemma 9.8 we may write $M = M_1 \cup M_2$ with $M_1 \cap M_2 = \varnothing$, M_1 p-periodic and M_2 q-periodic. Hence

$$pq = \#M = \# M_1 + \#M_2 = kp + lq \qquad (1)$$

for some integers k , $l \geq 0$. It follows from (1) that $p|l$ and $q|k$; hence $l = l_1 p$ and $k = k_1 q$ for some integers k_1 , $l_1 \geq 0$. Substituting into (1) and reducing pq yields

$$1 = k_1 + l_1 .$$

Therefore $k_1 = 0$ or $l_1 = 0$, that is, $M = M_2$ or $M = M_1$. Case A is completely proved.

The common principle to be applied in the proofs of cases B and C will be the successive location of <M> and <N> with respect to the I_d^n's.

CASE B: $n = p^2qr$, $\#M = pq$, $\#N = pr$.

We must have $<M> \in I_q^n$ or $<N> \in I_q^n$; but $<N> I_q^n$ would imply $q|\#N$ which is not possible. Hence $<M> \in I_q^n$ which is equivalent to

$$<p^2r> * <M> = pC . \tag{2}$$

Similarly

$$<p^2q> * <N> = pC . \tag{3}$$

Concerning I_p^n , let us suppose that $<M> \in I_p^n$, the discussion of the case $<N> \in I_p^n$ being similar. Hence

$$<pqr> * <M> = qC . \tag{4}$$

We have $<M> \notin I_{p^2}^n$; for otherwise

$$<qr> * <M> = \frac{1}{p} <pqr> * <M> = \frac{q}{p} C$$

and hence $p|q$, a contradiction. Therefore $<N> \in I_{p_2}^n$, that is

$$<qr> * <N> = \frac{1}{p} <pqr> * <N> . \tag{5}$$

We consider now I_{pr}^n , I_{qr}^n , and I_{pq}^n . Suppose first that $<N> \in I_{pr}^n$; then, taking into account (3),

$$\begin{aligned} <pq> * <N> &= \frac{1}{p} <p^2q> * <N> + \frac{1}{r} <pqr> * <N> - \frac{1}{pr} <p^2qr> * <N> \\ &= \frac{1}{r} <pqr> * <N> . \end{aligned}$$

Combining this with (5) we obtain $pr \mid <pqr> * <N>$. Lemma 9.9, which is applicable here due to (4) and to Theorem 2.1, shows then that M or N is periodic. It remains therefore to consider the relation $<M> \in I^n_{pr}$, which, according to (4), may be written as

$$< pq > * < M > = \frac{1}{p} < p^2 q > * < M > . \tag{6}$$

If we had $< M > \in I^n_{qr}$, that is, taking into account (2),

$$< p^2 > * < M > = \frac{1}{q} < p^2 q > * < M > ,$$

then we would obtain from the above relation and from (6) $pq \mid < p^2 q > * < M >$ and Lemma 9.9 would lead to the conclusion. We assume therefore that $< N > \in I^n_{qr}$, which, according to (3), may be written as

$$< p^2 > * < N > = \frac{1}{r} < p^2 r > * < N > . \tag{7}$$

Now if we had $< N > \in I^n_{pq}$ that is,

$$< pr > * <N> = \frac{1}{p} <p^2 r> * <N> + \frac{1}{q} <pqr> * <N> - \frac{r}{q} C ,$$

the above relation together with (7) would imply $pr \mid < p^2 r > * < N >$ and Lemma 9.9 would lead to the conclusion. Hence we may assume that $< M > \in I^n_{pq}$, which, according to (2) and (4), may be written as

$$< pr > * < M > = C . \tag{8}$$

We consider now $I^n_{p^2 q}$ and $I^n_{p^2 r}$. If we had $< N > \in I^n_{p^2 q}$, that is, taking into account (5),

$$< r > * < N > = \frac{1}{p} < pr > * < N >$$

we would obtain $p \mid < pr > * < N >$ and consequently, $p \mid < p^2 r > * < N >$; combining this with (7) would yield $pr \mid < p^2 r > * < N >$ and Lemma 9.9 would lead to the conclusion. We may therefore assume that $< M > \in I^n_{p^2 q}$, which, according to (8), may be written as

$$< r > * < M > = \frac{1}{q} < qr > * < M > . \tag{9}$$

Concerning $I^n_{p^2 r}$, we shall see that $< M > \notin I^n_{p^2 r}$. For otherwise,

$$<q> * <M> = \frac{1}{p} <pq> * <M> + \frac{1}{r} <rq> * <M> - \frac{q}{pr} C .$$

By (8), $< r > * < M > (x_0) = 0$ for some $x_0 \in \mathbf{Z}_n$; by evaluating both sides of (9) and of the above relation at x_0 we would get

$$pr < q > * < M > (x_0) = r < pq > * < M > (x_0) - q$$

and hence $r|q$, a contradiction. Consequently, $< N > \in I^n_{p^2r}$, that is, according to (5),

$$< q > * < N > = \frac{1}{p} < pq > * < N > . \qquad (10)$$

Finally we consider I^n_n . The relation (8) shows, by using Lemma 9.7, that M would be q-periodic if we had $< M > \in I^n_n$. On the other hand, the relation $< N > \in I^n_n$ combined with (10) yields

$$(E - \frac{1}{p} < p >) * (E - \frac{1}{r} < r >) * < N > = 0 . \qquad (11)$$

Now, by the argument employed in the end of the proof of Case A, we infer from (11) that N is p-periodic or r-periodic. Case B is completely proved.

CASE C: $n = pqrs$, $\#M = pq$, $\#N = rs$,

As in the beginning of the proof of Case B, location of $< M >$ and $< N >$ with respect to I^n_p , I^n_q , I^n_r , and I^n_s yields the relations

$$< prs > * < M > = pC , \qquad (12)$$

$$< qrs > * < M > = qC , \qquad (13)$$

$$< pqr > * < N > = rC , \qquad (14)$$

$$< pqs > * < N > = sC . \qquad (15)$$

We observe then that if any of the following relations

$$< M > \in (I^n_{pr} \cap I^n_{qr}) \cup (I^n_{ps} \cap I^n_{qs}) , \qquad (16)$$

$$< N > \in (I^n_{pr} \cap I^n_{ps}) \cup (I^n_{qr} \cap I^n_{qs}) , \qquad (17)$$

holds, then the proof is concluded. Indeed, suppose for instance that $< M > \in I^n_{ps} \cap I^n_{qs}$. By virtue of (12) and (13), this may be written as

$$< pr > * < M > = \frac{1}{q} < pqr > * < M > ,$$

$$< qr > * < \mathrm{M} > = \frac{1}{p} < pqr > * < \mathrm{M} >$$

which entails $pq \mid < pqr > * < \mathrm{M} >$ and the conclusion follows by an application of Lemma 9.9, taking into account (14) and Theorem 2.1.

To make a choice, we shall assume in the following that $< \mathrm{M} > \in \mathrm{I}^n_{qs}$, the discussion of the case $< \mathrm{N} > \in \mathrm{I}^n_{qs}$ being similar. In order that, under the assumption $< \mathrm{M} > \in \mathrm{I}^n_{qs}$, neither (16) nor (17) hold, we must have $< \mathrm{M} > \in \mathrm{I}^n_{pr}$ and $< \mathrm{N} > \in \mathrm{I}^n_{ps} \cap \mathrm{I}^n_{qr}$. By virtue of (12)–(15), all these relations may be written as

$$< pr > * < \mathrm{M} > = \frac{1}{q} < pqr > * < \mathrm{M} >, \tag{18}$$

$$< qs > * < \mathrm{M} > = \frac{1}{p} < pqs > * < \mathrm{M} >, \tag{19}$$

$$< qr > * < \mathrm{N} > = \frac{1}{s} < qrs > * < \mathrm{N} >, \tag{20}$$

$$< ps > * < \mathrm{N} > = \frac{1}{r} < prs > * < \mathrm{N} >. \tag{21}$$

We continue by stating four assertions which allow us to conclude the discussion of some subcases arising during the remaining part of the proof of Case C.

ASSERTION 1. *The relation* $< \mathrm{M} > \in \mathrm{I}^n_{rs}$ *implies* $p > s$ *and* $q > r$. *The relation* $< \mathrm{N} > \in \mathrm{I}^n_{pq}$ *implies* $r > p$ *and* $s > q$.

Indeed, suppose that $< \mathrm{M} > \in \mathrm{I}^n_{rs}$. According to (18) and (19), this yields

$$< pq > * < \mathrm{M} > = \frac{1}{r} < pqr > * < \mathrm{M} > + \frac{1}{s} < pqs > * < \mathrm{M} > - \frac{pq}{rs} \mathrm{C}$$

$$= \frac{q}{r} < pr > * < \mathrm{M} > + \frac{p}{s} < qs > * < \mathrm{M} > - \frac{pq}{rs} \mathrm{C}.$$

If we had $< pr > * < \mathrm{M} > (x_0) = 0$ for some $x_0 \in \mathbf{Z}_n$, we would obtain from the above relation

$$rs < pq > * < \mathrm{M} > (x_0) = pr < qs > * < \mathrm{M} > (x_0) - pq$$

and hence $r \mid pq$, a contradiction. Therefore $< pr > * < \mathrm{M} > \geq \mathrm{C}$, which implies that M contains at least qs elements (at least one in each coset of $\mathbf{Z}_n$ module $qs\mathbf{Z}_n$). Hence $qs \leq \#\mathrm{M} = pq$ and $p > s$. The other parts of the assertion are similarly proved.

ASSERTION 2. *If* $< N > \in I^n_{prs} \cup I^n_{qrs}$ *then* $< pq > * < N > = C$.

Indeed, suppose that $< N > \in I^n_{qrs}$, that is

$$(E - \frac{1}{q} < q >) * (E - \frac{1}{r} < r >) * (E - \frac{1}{s} < s >) * < p > * < N > = 0.$$

As by (21) $< ps > * < N >$ is r-periodic, the above relation reduces to

$$(E - \frac{1}{q} < q >) * (E - \frac{1}{r} < r >) * < p > * < N > = 0,$$

that is, according to (14),

$$rq < p > * < N > = r < pq > * < N > + q < pr > * < N > - rC .$$

From the above we infer that $q| < pq > * < N > - C$. Because of $< pq > * < N > - C \geq -C$, the latter relation implies $< pq > * < N > - C \geq 0$; on the other hand

$$< rs > * (< pq > * < N > - C) = < pqrs > * < N > - rs\, C = 0$$

which is verified only if $< pq > * < N > - C = 0$.

ASSERTION 3. *If any of the relations*

$$< M > \in I^n_n \cap I^n_{pq} \cap (I^n_{prs} \cup I^n_{qrs}) ,$$
$$< N > \in I^n_n \cap I^n_{rs} \cap (I^n_{pqr} \cup I^n_{pqs}) ,$$

holds, then the proof of Case C *is concluded.*

For instance, the relations $< M > \in I^n_n$, $< M > \in I^n_{qrs}$, $< M > \in I^n_{pq}$ are respectively written as

$$(E - \frac{1}{p} < p >) * (E - \frac{1}{q} < q >) * (E - \frac{1}{r} < r >)$$
$$* (E - \frac{1}{s} < s >) * < M > = 0, (E - \frac{1}{q} < q >)$$
$$* (E - \frac{1}{r} < r >) * (E - \frac{1}{s} < s >) * < p >$$
$$* < M > = 0, < rs > * < M > = C.$$

(In deriving the last relation we have used (12) and (13)). Adding to the first relation the second relation multiplied by $1/p$ yields

$$(E - \frac{1}{q}< q >) * (E - \frac{1}{r}< r >) * (E - \frac{1}{s}< s >) * < M > = 0,$$

Now Lemma 9.7, which is applicable here due to the equality $< rs > * < M > = C$, shows that M is q-periodic.

ASSERTION 4. *If any of the relations*

$$< M > \in I^n_{pq} \cap ((I^n_{pqs} \cap I^n_{prs}) \cup (I^n_{pqr} \cap I^n_{qrs})),$$
$$< N > \in I^n_{rs} \cap ((I^n_{prs} \cap I^n_{pqr}) \cup (I^n_{qrs} \cap I^n_{pqs})),$$

holds, then the proof of Case C *is concluded.*

Suppose for instance that $< N > \in I^n_{rs} \cap I^n_{qrs} \cap I^n_{pqs}$. $< N > \in I^n_{rs}$ gives

$$<pq>*<N> = C. \tag{22}$$

$<N> \in I^n_{qrs}$ gives

$$(E - \frac{1}{q}<q>)*(E - \frac{1}{r}<r>)*(E - \frac{1}{s}<s>)*<p>*<N> = 0$$

which, according to (22), reduces to

$$(E - \frac{1}{r}<r>)*(E - \frac{1}{s}<s>)*<p>*<N> = 0. \tag{23}$$

$<N> \in I^n_{pqs}$ gives

$$(E - \frac{1}{p}<p>)*(E - \frac{1}{s}<s>)*(E - \frac{1}{q}<q>)*<r>*<N> = 0$$

which reduces to

$$(E - \frac{1}{p}<p>)*(E - \frac{1}{s}<s>)*<r>*<N> = 0 \tag{24}$$

as $<qr>*<N>$ is s-periodic by (20). From (23) and (24) we infer that

$$\begin{aligned}(sE - <s>)*<r>*<N> &= \frac{1}{p}<p>*(sE - <s>)*<r>*<N> \\ &= \frac{1}{p}<r>*(sE - <s>)*<p>*<N> \\ &= \frac{r}{p}(sE - <s>)*<p>*<N>\end{aligned}$$

which can be verified only if the leftmost and the rightmost sides vanish identically. Hence, by also using (21),

$$rs<p>*<N> = r<ps>*<N> = <prs>*<N>$$

and the conclusion follows by an application of Lemma 9.9.

We combine now Assertions 1–4 in order to conclude the proof of Case C. By Assertion 1, at least one of the relations $<M> \in I^n_{pq}$, $<N> \in I^n_{rs}$ holds; for otherwise we would arrive at the contradiction $pq>rs$ and $rs>pq$. Suppose first that both of the relations mentioned hold. One of the functions <M>, <N>—say <M>—must belong to I^n_n; it follows then from Assertions 3 and 4 that we are successively reduced to the cases $<N> \in I^n_{prs} \cap I^n_{qrs}$ and $<M> \in I^n_{pqr} \cap I^n_{pqs}$. Finally, we have the following requirements imposed to <M>:

$$(E - \frac{1}{p}<p>)*(E - \frac{1}{q}<q>)*(E - \frac{1}{r}<r>) *(E - \frac{1}{s}<s>)*<M> = 0\,, \tag{25}$$

$$(E - \frac{1}{p}<p>)*(E - \frac{1}{q}<q>)*(E - \frac{1}{r}<r>)*<s>*<M> = 0\,, \tag{26}$$

$$(E - \frac{1}{p}<p>)*(E - \frac{1}{q}<q>)*(E - \frac{1}{s}<s>)*<r>*<M> = 0\,. \tag{27}$$

Adding to (25) the equality (26) multiplied by $1/s$, respectively the equality (27) multiplied by $1/r$, yields

$$(E - \frac{1}{r}<r>)*(E - \frac{1}{p}<p>)*(E - \frac{1}{q}<q>)*<M> = 0\,,$$

$$(E - \frac{1}{s}<s>)*(E - \frac{1}{p}<p>)*(E - \frac{1}{q}<q>)*<M> = 0\,.$$

The above means that the function

$$(E - \frac{1}{p}<p>)*(E - \frac{1}{q}<q>)*<M>$$

is r-periodic and s-periodic, hence rs-periodic. Consequently,

$$(E - \frac{1}{rs}<rs>)*(E - \frac{1}{p}<p>)*(E - \frac{1}{q}<q>)*<M> = 0$$

which gives, by using the relation $<rs>*<M> = C$ (which expresses the fact that $<M> \in I^n_{pq}$)

$$(E - \frac{1}{p}<p>)*(E - \frac{1}{q}<q>)*<M> = 0\,.$$

The argument employed in the end of the proof of Case A shows then that M is p-periodic or q-periodic.

We suppose now that one of the relations $<M> \in I^n_{pq}$, $<N> \in I^n_{rs}$ does not hold, say $<N> \notin I^n_{rs}$ (the discussion of the other case being similar). By Assertion 2 it follows that $<M> \in I^n_{prs} \cap I^n_{qrs}$. As we also have $<M> \in I^n_{pq}$, we are reduced via Assertions 3 and 4 to the case $<N> \in I^n_n \cap I^n_{pqr} \cap I^n_{pqs}$. A computation similar to that which was done in the preceding paragraph leads then to

$$(E - \frac{1}{rs}<rs>)^*(E - \frac{1}{p}<p>)^*(E - \frac{1}{q}<q>)^*<N> = 0 . \quad (28)$$

If we had $<pq>^*<N> \geq C$, the argument employed in the proof of Assertion 2 would show that $<pq>^*<N> = C$, that is $<N> \in I^n_{rs}$, which is not the case. On the other hand, $<M> \in I^n_{rs}$; by Assertion 1, this implies

$$pq > rs . \quad (29)$$

If we had $<rs>^*<N> \geq C$, it would follow that N contains at least pq elements (at least one in each coset of $\mathbf{Z}_n$ modulo $pq\mathbf{Z}_n$) and this would contradict (29). Hence there is a coset modulo $pq\mathbf{Z}_n$ and a coset modulo $rs\mathbf{Z}_n$ which do not meet N; let x_0 belong to the intersection of these cosets. (The intersection in question is not empty because of the equality $\mathbf{Z}_n = pq\mathbf{Z}_n + rs\mathbf{Z}_n$, as seen by an argument similar to the one employed in the end of the proof of Lemma 9.8). If we expand the left side of (28), evaluate it at x_0 and use (20) and (21), we get

$$rs = qr <ps>^*<N>(x_0) + ps <qr>^*<N>(x_0) .$$

Writing k for $<ps>^*<N>(x_0)$ and l for $<qr>^*<N>(x_0)$, the above relation becomes $rs = qrk + psl$. It follows that $r \mid l$ and $s \mid k$; writing $k = ts$, $l = ur$ and reducing rs yields $1 = tq + up$ which is a contradiction, as $t \geq 0$ and $u \geq 0$. This concludes the proof of Case C, completing thus the proof of the implication (i) => (ii) in Theorem 2.2.

Notes

1. See formula 5.14 on page 117 of Lewin 1981.
2. If $\hat{F}$ vanishes at all $\omega \in U_n$, the polynomial $\hat{F}(\omega)$ of degree at most $n-1$ in the unknown ω has n distinct roots and must be therefore identically zero; that is, F must be the function identically zero.
3. It can be shown without much difficulty that condition (ii) is in fact a consequence of the other assumptions. We shall not need this stronger version of the lemma.

References

Lewin, David. 1959. "Intervallic Relations between Two Collections of Notes." *Journal of Music Theory* 3:298–301.

_____. 1981. "Some Investigations into Foreground Rhythmic and Metric Patterning." In *Music Theory—Special Topics*, edited by Richmond Browne, 101–37. New York: Academic Press.

_____. 1987. *Generalized Musical Intervals and Transformations*. New Haven and London: Yale University Press.

Rahn, John. 1987. "*Generalized Musical Intervals and Transformations* by David Lewin." (Review). *Journal of Music Theory* 31, no. 2:305–18.

Ribenboim, Paulo. 1972. *Algebraic Numbers*. New York—London—Sydney—Toronto: Wiley—Interscience.

Vuza, Dan. 1988. "Some Mathematical Aspects of David Lewin's Book *Generalized Musical Intervals and Transformations*." *Perspectives of New Music* 26, no. 1 (Winter): 258–87.

References

Re: Intervallic Relations between Two Collections of Notes
David Lewin
Journal of Music Theory, Vol. 3, No. 2. (Nov., 1959), pp. 298-301.
Stable URL:
http://links.jstor.org/sici?sici=0022-2909%28195911%293%3A2%3C298%3ARIRBTC%3E2.0.CO%3B2-C

Review: [Untitled]
Reviewed Work(s):
Generalized Musical Intervals and Transformations by David Lewin
John Rahn
Journal of Music Theory, Vol. 31, No. 2. (Autumn, 1987), pp. 305-318.
Stable URL:
http://links.jstor.org/sici?sici=0022-2909%28198723%2931%3A2%3C305%3AGMIAT%3E2.0.CO%3B2-M

Some Mathematical Aspects of David Lewin's Book: Generalized Musical Intervals and Transformations
Dan Tudor Vuza
Perspectives of New Music, Vol. 26, No. 1. (Winter, 1988), pp. 258-287.
Stable URL:
http://links.jstor.org/sici?sici=0031-6016%28198824%2926%3A1%3C258%3ASMAODL%3E2.0.CO%3B2-2