CIRCULANTS (Extract)

Alun Wyn-jones

Last revised in December 2013.

Chapter 3.
Homomorphisms

3.1 Introduction.

In this chapter, we shall define several ring homomorphisms to or from circulant space or eigenspace. Some of these homomorphisms will be used in later chapters, others will be discussed here just for their intrinsic interest, and a few will be presented because they link the circulants to other mathematical structures.

Since spaces of several dimensions will be under discussion simultaneously, the convention that N be the default dimension is modified: In this chapter, N will be the highest dimension under consideration, and will often equal mn where m and n are dimensions of smaller spaces.

We alert the reader that if we define a homomorphism on circulant vectors, $\mathbf{circ}_N$, then we shall regard them as equally well defined on circulant matrices, $\mathbf{circ}_N$, and *vice versa*.

Likewise, it will often be convenient to define some maps on the eigenspace and other maps on circulant space. Again, this is a matter of convenience because conjugation by λ is a bijection on maps and homomorphisms. All ring homomorphisms defined in this chapter will be linear in the sense of §2.5. Thus, a map $\alpha : \mathbf{circ}_n(R) \to \mathbf{circ}_m(R)$, say, defined on circulants always induces a map $\lambda\alpha\lambda^{-1} : \Lambda_n \to \Lambda_m$ between eigenspaces. The induced eigenvalue map will be denoted with the tilde mark above it. Thus, $\tilde{\alpha} := \lambda\alpha\lambda^{-1}$. Given instead a definition for a map on the eigenspace $\tilde{\alpha} : \Lambda_n(R) \to \Lambda_m(R)$, say, then the map induced on circulants is $\tilde{\alpha}^{\lambda} = \lambda^{-1}\tilde{\alpha}\lambda : \mathbf{circ}_n(R) \to \mathbf{circ}_m(R)$.

The meaning of conjugation by λ might seem clear enough, however, the λ^{-1} map in $\lambda\alpha\lambda^{-1}$ is not necessarily the inverse of the λ map appearing to the left of α. For instance, suppose $\alpha : \mathbf{circ}_m \to \mathbf{circ}_n$, then the leftmost λ, acts on $\mathbf{circ}_n$ whereas the rightmost λ^{-1} acts on Λ_m. When confusion could arise we shall denote λ acting on circulants of dimension n by $\lambda^{(n)}$. The parenthesis are necessary since powers (compositions) of λ occasionally crop up. Since the inverse power is required constantly, we shall simplify the cumbersome $\left(\lambda^{(n)}\right)^{-1}$ to $\lambda^{-(n)}$. Thus, if $\alpha : \mathbf{circ}_n(R) \to \mathbf{circ}_m(R)$ then the induced eigenspace map would be $\alpha^{\lambda^{-1}} = \lambda^{(m)}\alpha\lambda^{-(n)}$, and this maps $\Lambda_n \to \Lambda_m$.

We shall confine ourselves to considering only linear homomorphisms on circulants, that is, those homomorphisms $\alpha : \mathbf{circ}(R) \to \mathcal{A}(R)$ where $\mathcal{A}$ is some algebra over R which satisfy, $\alpha(rv) = r\alpha(v)$, $\forall r \in R$. Still, there are many linear ring endomorphisms on circulant spaces. There is a general construction induced by projection operators on the eigenspace: $\Lambda_N \to \Lambda_N$. Taking $R = \mathbb{C}$ as an example, there are $2^N - 1$ projections of $\mathbb{C}^N$ where one or more eigenvalues are zeroed. By §2.5, all the linear automorphisms on $\mathrm{CIRC}_N(\mathbb{C})$ are induced by the $N!$ permutations of the eigenvalues. The composition of these two sets provide the full set of linear endomorphisms on $\mathrm{CIRC}_N(\mathbb{C})$. Hence, given any linear homomorphism $\alpha : \mathbf{circ}(R) \to \mathcal{A}(R)$, its composition with the set of linear endomorphisms $\eta : \mathbf{circ}(R) \to \mathbf{circ}(R)$ creates many more linear homomorphisms $\alpha\eta : \mathbf{circ}(R) \to A(R)$.

3.2 δ-Idempotents.

The first set of maps are important both for practical calculations and for understanding the structure of circulant spaces. These maps are idempotent endomorphisms on the circulant spaces; they are defined as multiplication by idempotent circulants. The basic construction and properties of such ring endomorphisms is quite general and is our starting point.

We remind the reader that the base rings of the circulant spaces are integral domains whose characteristics do not divide the order of any circulants under discussion. However, in the following proposition, R is a completely arbitrary commutative ring with identity; indeed the proposition is intended for the case that R is a ring of circulant matrices. We use the standard notation R^* for the group of invertible elements, the group of units, in R

3.2.1 Proposition

Let e be an idempotent in a commutative ring R with identity 1. Then,

(i) $1 - e$ is also an idempotent in R, and is complementary to e. That is, $e(1 - e) = 0$.

(ii) The map $e : R \to R$ defined by $e(x) = ex$ is a ring endomorphism, and is idempotent.

(iii) R has a direct sum decomposition given by $R = eR \oplus (1-e)R$.

(iv) $e(1) = e$ is an identity for the subring eR.

(v) e induces an idempotent group homomorphism on the group of units, $e_\times : R^* \to R^*$ given by,

$$e_\times(x) \;=\; 1 \;+\; e(x-1)$$

(vi) $$(eR^*, e) \;\approx\; (e_\times R^*, 1)$$

(vii) $e : R^* \to (eR)^*$ is onto.

(viii) The complement of $e_\times$ is $(1-e)_\times$, and is given by

$$(1-e)_\times(x) \;=\; x - e(x-1)$$

(ix) If e and f are complementary, then so are $e_\times$ and $f_\times$ multiplicatively: $e_\times f_\times(x) = 1$.

Proof. These are elementary results. The only tricky one is *(vii)* which we shall prove. We need to show that $(eR)^* \subset eR^*$. So suppose $e(x) \in (eR)^*$. By part *(vi)*, $e(x) \in (eR)^* \;\Rightarrow\; e_\times(x) \in R^* \;\Rightarrow\; 1 + e(x-1) \in R^*$. Let $u = 1 + e(x-1) \in R^*$. Then, $e(u) = e(1) + e(x-1) = e(x)$. □

The idempotent circulants we have in mind act as Kronecker delta functions on the eigenspace. Recall from Chapter 1 that δ^N_x is 1 if $N \,|\, x$ else 0. Their equivalent maps on the circulants are defined only when all factors of N are invertible in the quotient ring of the base ring of the circulants.

3.2.2 **Definition** Let $N = nm$.

(i) Define $\delta^{n|\,N}$ to be the vector in the eigenspace given by $\delta^{n|\,N} \;:=\; \left(\delta^n_0, \delta^n_1, \ldots, \delta^n_{N-1}\right) \in \Lambda_N$.

(ii) Define the circulant, $\bar\delta^{n|\,N} \;:=\; \mathbf{circ}_N\left(\frac{1}{n}\delta^{m|\,N}\right) \;=\; \frac{1}{n}\sum_{i=0}^{n-1} \mathrm{u}^{im}_{mn}$

The superscript "$n \,|\, N$" is intended to remind the reader that n must divide N. Also, both N and n are needed to fully specify the idempotent although N is not as essential as it first appears. So, when it is clearly understood, the "$|\,N$" will often be omitted.

The $\delta^{n|\,N}$ vector consists of a sequence of zeroes and ones, with a one occurring every time the subscript is divisible by n. That is, every n^{th} component of $\delta^{n|\,N}$ is one, all others are zero. Clearly, $\delta^{n|\,N}$ is idempotent under componentwise multiplication. Following Proposition 3.2.1, for $\mu \in \Lambda_N$, we define the map $\delta^{n|\,N}(\mu)$ to be

$$\delta^{n|\,N} : (\mu_0, \mu_1, \ldots, \mu_{N-1}) \;\mapsto\; \delta^{n|\,N} \cdot (\mu_0, \mu_1, \ldots, \mu_{N-1}) \;=\; (\mu_0, 0, \ldots, 0, \mu_n, 0, \ldots, 0, \ldots, 0, \mu_{in}, 0, \ldots)$$

Let $\mu = \lambda(a)$. Then, $\mu_{in} = \lambda_{in}(a) = a_0 + a_1\zeta^{in} + a_2\zeta^{2in} + \cdots$. We see that δ^n projects out those eigenvalues which are polynomials in ζ^n. Hence, δ^n maps the eigenvalues to the subring of $R(\zeta^n)^N \subset R(\zeta)^N$.

It is not so immediately apparent that $\bar\delta^{n|\,N}$ is idempotent in $\mathbf{circ}_N$. However, we shall show in Proposition 3.2.3, that $\bar\delta^{n|\,N}$ is that unique circulant whose eigenvalues are $\delta^{n|\,N}$, and this immediately implies that $\bar\delta^{n|\,N}$ is idempotent. The $\bar\delta^{n|\,N}(x)$ map is similarly defined as $\bar\delta^{n|\,N}x$ for $x \in \mathbf{circ}_N$.

Any confusion between the componentwise product $\delta^n x$ and the mapping $\delta^n(x)$ is innocuous since they are equal. The same applies to the convolution product $\bar\delta^n x$ and the $\bar\delta^n(x)$ mapping. Nonetheless, we do sometimes need to be clear whether we mean $\{\bar\delta^n, \delta^n\}$ as elements of their respective spaces, or as maps on their spaces. In such cases, we will indicate which we mean by writing (e.g.) $\delta^n \in \Lambda_N$, or $\bar\delta^n : \mathbf{circ}_N \to \mathbf{circ}_N$, or $\bar\delta^n \restriction \mathbf{circ}_N$, the latter notation indicating that $\bar\delta^n$ is a map acting on $\mathbf{circ}_N$, and so is actually $\bar\delta^{n|\,N}$.

3.2.3 **Proposition** $\lambda\left(\bar\delta^n\right) \;=\; \delta^n$ where $\bar\delta^n \in \mathbf{circ}_N$, $\delta^n \in \Lambda_N$.

Proof. Suppose $N = mn$.

$$\lambda^{-1}(\delta^n)_i \;=\; \frac{1}{mn}\sum_{j=0}^{mn-1} \delta^n_j \zeta^{-ij}_{mn} \;=\; \frac{1}{mn}\sum_{j=0}^{m-1} \zeta^{-nij}_{mn} \;=\; \frac{1}{mn}\sum_{j=0}^{m-1} \zeta^{-ij}_m \;=\; \frac{1}{n}\delta^m_i \;:=\; \bar\delta^n_i \;\square$$

3.2.4 **Corollary** $\bar{\delta}^n \in \mathbf{circ}_N$ is an idempotent. □

3.2.5 **Corollary** For $\bar{\delta}^n \mid \mathbf{circ}_N$, $\delta^n \mid \Lambda_N$, $\lambda\,\bar{\delta}^n\,\lambda^{-1} = \delta^n$. □

It is clear that the product of two idempotents elements is idempotent. In the case of $\delta^{a|N}$ and $\delta^{b|N}$, we see by inspection that $\delta^{a|N}\delta^{b|N} = \delta^{\mathrm{lcm}(a,b)|N}$ which is another idempotent of the same type. Applying, λ^{-1}, we obtain $\bar{\delta}^{a|N}\bar{\delta}^{b|N} = \bar{\delta}^{\mathrm{lcm}(a,b)|N}$. From Proposition 3.2.1, we know that $(1-\delta^n) \in \Lambda_N$ and $(1-\bar{\delta}^n) \in \mathbf{circ}_N$ are also idempotents. The closure properties of these idempotents with each other and with the original set is more complicated. Nevertheless, we shall deduce the form of all idempotent elements which can be generated from the combined sets $\{\delta^{n|N} \vdash n \,|\, N\} \cup \{(1-\delta^{n|N}) \vdash n \,|\, N\} =: S$, say. We shall concentrate on S, the idempotent elements of the eigenspace. Of course, our argument will apply equally to $\lambda^{-1}S\lambda$.

Let $\langle S\rangle$ denote the set of all idempotents which can be generated from S by multiplication. Now, all elements of S have the property that their components are either 0 or 1. Also, this property is inherited by products of idempotents having the property. Therefore, this property holds for all of $\langle S\rangle$. Hence, any member of $\langle S\rangle$ is specified uniquely by its subscripts of non-zero components. We call this set the support of the member, $\mathrm{supp}(e) = \{i \in \mathbb{Z}_N \vdash e_i = 1\}$. We make the following observations.

3.2.6 **Lemma** Let $N = mn$.

(i) $\forall e, f \in \langle S\rangle, \quad e = f \;\Leftrightarrow\; \mathrm{supp}(e) = \mathrm{supp}(f)$.

(ii) $\forall e, f \in \langle S\rangle, \quad \mathrm{supp}(ef) = \mathrm{supp}(e) \cap \mathrm{supp}(f)$.

(iii) $\forall e \in \langle S\rangle, \quad \mathrm{supp}(1-e) = \mathbb{Z}_N - \mathrm{supp}(e)$.

(iv) $\mathrm{supp}(\delta^n) = \{ni \bmod N \vdash i = 0, 1, \ldots, m\}$. □

From these observations, we deduce.

3.2.7 **Lemma** If two residues have the same highest common factor mod N, then they are not separated by the supp function acting on $\langle S\rangle$. That is,

$$\gcd(i,N) = \gcd(j,N) \quad \Rightarrow \quad (i \in \mathrm{supp}(e) \;\Leftrightarrow\; j \in \mathrm{supp}(e), \quad \forall e \in \langle S\rangle)$$

Proof. We are given i, j with $\gcd(i,N) = \gcd(j,N)$. Suppose $n \,|\, N$; then, $n \,|\, i \;\Leftrightarrow\; n \,|\, j$. Hence, either both i, j are in $\mathrm{supp}(\delta^n)$ or neither. The same applies to $\mathrm{supp}(1-\delta^n)$. If i, j are either both present or both absent in two sets, then the same holds for the intersection of the two sets. Hence, by part *(ii)* of Lemma 3.2.6, the property holds for all of $\langle S\rangle$. □

To proceed, we need to introduce a class of subsets of congruence classes.

3.2.8 **Notation.**

(i) Let $(i)_N$ denote the principal ideal generated by i in $\mathbb{Z}_N$.

(ii) Let $(i)^*_N := \{ir \bmod N \vdash \gcd(ir,N) = \gcd(i,N)\} \subset \mathbb{Z}_N$.

It is easy to see that $(i)_N$ and $(i)^*_N$ depend only upon the highest common factor of i with N. Letting $h = \gcd(i,N)$, then $(i)_N = (h)_N$ and $(i)^*_N = (h)^*_N$. Indeed these two sets will usually be presented as $(n)_N$ and $(n)^*_N$ where n is a divisor of N.

The set $(i)^*_N$ can be described as those residues mod N which share with i the same highest common factor with N. When $n \,|\, N$, we shall call $(n)^*_N$ the **residue class set** n mod N. We shall now show that each residue class set mod N is the support for an idempotent in $\langle S\rangle$.

3.2.9 **Lemma** Suppose $n \,|\, N$. Let $\delta^{*n} = \delta^n \prod_{n \,||\, d \,|\, N} (1-\delta^d)$. Then, $\mathrm{supp}\,(\delta^{*n}) = (n)^*_N$.

Proof. One views the construction of δ^{*n} as the intersection of the support sets of all the terms appearing in the product. The first such support set is $\mathrm{supp}(\delta^n)$; these are the residues whose common factor with N is at least n. The intersection with the remaining terms remove all residues which have common factors greater than n. This leaves only those residues whose common factor with N is exactly n. □

We formally define δ^{*n} of the lemma.

3.2.10 **Definition** Let $n \,|\, N$.

(i) We define $\delta^{*n|\,N} := \delta^n \prod_{n \,||\, d \,|\, N} (1-\delta^d)$. We shall drop N, and write δ^{*n} if N is understood.

We shall call $\delta^{*n|\,N}$ the eigenspace **residue class idempotent** for n mod N, or more briefly, the δ^*-idempotent for n mod N. Clearly, $(\delta^{*n|\,N})_i = 1 \Leftrightarrow \gcd(i,N) = n$.

(ii) Define the circulant version of this idempotent by $\bar{\delta}^{*n|\,N} = \bar{\delta}^{*n} := \lambda^{-1}\delta^{*n}\lambda$.

We shall call $\bar{\delta}^{*n|\,N}$ the **circulant residue class idempotent** for n mod N, or more briefly, the $\bar{\delta}^*$-idempotent for n mod N.

We have now established the basic building blocks of the δ-idempotents. Let T be the set of residue class idempotents, then one easily sees that $\langle T\rangle = \langle S\rangle$. Furthermore, all members of T are mutually complementary. Hence, their support sets form a partitioning of $\mathbb{Z}_N$. This only restates the standard fact that $\mathbb{Z}_N = \bigcup_{d|\,N} d\mathbb{Z}^*_{N/d}$. Lastly, the members of T are fundamental in the sense that the supports of all other members of $\langle S\rangle$ are unions of the supports of members of T. We state these facts as a proposition for reference.

3.2.11 **Proposition** Let $T = \{\delta^{*n|\,N} \vdash n \,|\, N\}$.

(i) T is a set of idempotents on $\mathbf{circ}_N$.

(ii) $\sum T = 1$

(iii) $\forall s \neq t \in T,\ st = 0$. □

At this point the reader might wonder why we did not start by defining $\delta^{*n|\,N}$ and then deriving $\delta^{n|\,N}$. The derivations would indeed be simpler: The independence of the δ^*-idempotents would be established from the outset, and the derivation of the δ-idempotents would very easy. In fact, here is the formula:

$$\delta^{n|\,N} = \sum_{d|\,n} \delta^{*n|\,N} \tag{1}$$

We started with the δ-idempotents for several reasons. Firstly, the δ-idempotents are intrinsically simpler, being characteristic functions of ideals in $\mathbb{Z}_N$. A second reason is that $\bar{\delta}^{n|\,N}\mathbf{circ}_N$ is isomorphic to $\mathbf{circ}_{N/n}$ (this will be proved in §3.5.2.2) whereas there is no such simple characterization of $\bar{\delta}^{*n|\,N}\mathbf{circ}_N$. Lastly, the formulæ for the $\bar{\delta}$-idempotents are simply geometric series in u, whereas the formulæ for the $\bar{\delta}^*$-idempotents are anything but simple, and in fact, are probably most easily computed using our defining formula in 3.2.10. To demonstrate, we give all the formulæ for $N = 24$; these were derived by computer.

$$
\begin{aligned}
\bar{\delta}^{*1|\,24} &= \tfrac{1}{6}\ (2+\mathrm{u}^4-\mathrm{u}^8)\,(1-\mathrm{u}^{12}) \\
\bar{\delta}^{*2|\,24} &= \tfrac{1}{12}\ (2+\mathrm{u}^2-\mathrm{u}^4)\,(1-\mathrm{u}^6+\mathrm{u}^{12}-\mathrm{u}^{18}) \\
\bar{\delta}^{*3|\,24} &= \tfrac{1}{6}\ (1-\mathrm{u}^4+\mathrm{u}^8)\,(1-\mathrm{u}^{12}) \\
\bar{\delta}^{*4|\,24} &= \tfrac{1}{24}\ (2+\mathrm{u}-\mathrm{u}^2)\,(1-\mathrm{u}^3+\mathrm{u}^6-\mathrm{u}^9+\mathrm{u}^{12}-\mathrm{u}^{15}+\mathrm{u}^{18}-\mathrm{u}^{21}) \\
\bar{\delta}^{*6|\,24} &= \tfrac{1}{12}\ (1-\mathrm{u}^2+\mathrm{u}^4)\,(1-\mathrm{u}^6+\mathrm{u}^{12}-\mathrm{u}^{18}) \\
\bar{\delta}^{*8|\,24} &= \tfrac{1}{24}\ (2-\mathrm{u}-\mathrm{u}^2)\,(1-\mathrm{u}^3+\mathrm{u}^6-\mathrm{u}^9+\mathrm{u}^{12}-\mathrm{u}^{15}+\mathrm{u}^{18}-\mathrm{u}^{21}) \\
\bar{\delta}^{*12|\,24} &= \tfrac{1}{24}\ \sum_{i=0}^{23}(-\mathrm{u})^i \\
\bar{\delta}^{*24|\,24} &= \tfrac{1}{24}\ \sum_{i=0}^{23}\mathrm{u}^i
\end{aligned}
$$

We will make frequent references to functions defined on residue class sets, and most particularly, the eigenvalue functions. So we define these next.

3.2.12 **Definition** Define $L_{n|\,N}$ and $L^*_{n|\,N}$ to be subsets of the maps $\{\lambda_0, \lambda_1, \ldots, \lambda_{N-1}\}$, and

(i) $L_{n|\,N} := \{\lambda_i \vdash i \in (n)_N\} = \{\lambda_n, \lambda_{2n}, \ldots, \lambda_{N-n}\}$

(ii) $L^*_{n|\,N} := \{\lambda_i \vdash i \in (n)^*_N\}$.

These sets can be applied to a circulant, c, giving sets of eigenvalues, thus

$$
\begin{aligned}
L_{n|\,N}(c) &= \{\lambda_n(c), \lambda_{2n}(c), \ldots, \lambda_{N-n}(c)\}, \quad \text{and} \\
L^*_{n|\,N}(c) &= \{\lambda_i(c) \vdash i \in (n)^*_N\}
\end{aligned}
$$

As usual we shall drop the reference to N when there is no danger of ambiguity.

There is an obvious analog of equation (1) which relates $L_{n|\,N}$ to $L^*_{n|\,N}$.

$$
L_{n|\,N} = \bigcup_{d|\,n} L^*_{d|\,N} \tag{2}
$$

The fundamental importance of the residue class sets is demonstrated by the next proposition. To aid in the reading of the theorem, some readers may want consult Appendix A for a summary of facts on the cyclotomic polynomial, and cyclotomic theory in general.

3.2.13 **Proposition** Let $a \in \mathbf{circ}_{_N}(R)$, let ζ be a primitive N^{th} root of unity. Then, $L^*_n(a)$ is a union of orbits under the action of the Galois group of $R(\zeta)/R$. If the cyclotomic polynomial, $\Phi_N(x)$, is irreducible over R, then L^*_n is an orbit.

Proof. If $\zeta \in R$, then the Galois group is trivial, and there is nothing to prove. So we assume $\zeta \notin R$.

Let G be the Galois group of the extension, and let Z be the set of primitive N^{th} roots of unity, $Z = \{\zeta^i \vdash \gcd(i, N) = 1\}$. Then, G is a permutation group on Z. Therefore, any $\alpha \in G$ must map ζ to another primitive N^{th} root of unity, $\alpha : \zeta \mapsto \zeta^j$, say where $j \in \mathbb{Z}^*_N$. Now, suppose $\lambda_i(a) \in L^*_n$. Then, $i \in (n)^*_N$, and $\alpha : \lambda_i(a) \mapsto \lambda_{ij}(a)$. Clearly, $ij \in (n)^*_N$. Therefore, $\alpha : L^*_n \to L^*_n$.

Now, suppose Z is not an orbit under G, then a proper subset of $Z_1 \subset Z$ exists which is invariant under G. Let $p(x)$ be the unique monic polynomial whose roots are the members of Z_1. Then, the coefficients of p are symmetric functions on Z_1, and so are invariant under G, hence must be in the base field, R. That is, $p(x) \in R[x]$. But, $p(x) \,|\, \Phi_N(x)$, and since $Z_1 \neq Z$, $\deg p < \deg \Phi_n$. Therefore, $\Phi_N(x)$ is reducible.

We have shown that if Φ_N is irreducible over R, then Z is an orbit under G. Hence, $f(Z) := \{f(z) \vdash z \in Z\}$ is also an orbit under G for any function $f : R(\zeta) \to R(\zeta)$. Set $f(x) = A(x^n)$ where $A(x)$ is the representer polynomial for the circulant a. Then, $A(\zeta) = \lambda_n(a)$, and $f(z) = \{A(z) \vdash z \in Z\} = L^*_n(a)$. □

The corollary which follows assumes that the integral domain R satisfies the condition $R_\zeta \cap Q = R$ where Q is the field of quotients of R. This condition holds for a large class of rings, including all those which are integrally closed (see Appendix A). For example, $\mathbb{Z}$ is integrally closed. Even if R is not integrally closed, it might neverthess satisfy $Q \cap R_\zeta = R$. For example, one can easily prove that $Q \cap R_\zeta = R$ when $\Phi_n(x)$ is irreducible over Q.

3.2.14 **Corollary** Let Q be the field of quotients for R, and suppose that $R(\zeta_N) \cap Q = R$. Let $a \in \mathbf{circ}_N(R)$. The symmetric functions in $L_{n|\,N}(a)$ with coefficients in R take values in R, and the same applies to symmetric functions in $L^*_{n|\,N}(a)$.

Proof. Let Q be the field of quotients for R. With the given conditions, the proposition implies that $fL^*_{n|\,N}(a) \in Q$ for any symmetric function f having integer coefficients. Now, $\lambda_i(a) \in R(\zeta)$. Therefore, $fL^*_{n|\,N}(a) \in R(\zeta) \cap Q = R$.

The statement for $L_{n|\,N}(a)$ now follows by equation (2). □

The two symmetric functions of most interest to us are the sum and the product. For products it behooves us to define the maps $\bar{\delta}^{*n|\,N}_\times$ as defined for general rings in Proposition 3.2.1.

3.2.15 **Lemma** For $a \in \mathbf{circ}_N$, define the maps $\bar{\delta}^n_\times, \bar{\delta}^{*n}_\times, (1-\bar{\delta}^n)_\times, (1-\bar{\delta}^{*n})_\times : \mathbf{circ}_N{}^* \to \mathbf{circ}_N{}^*$ according to Proposition 3.2.1 *(v)*. Then,

$$\begin{aligned}
\bar{\delta}^n_\times(a) &= 1 + \bar{\delta}^n(a-1) \\
\bar{\delta}^{*n}_\times(a) &= 1 + \bar{\delta}^{*n}(a-1) \\
(1-\bar{\delta}^n)_\times(a) &= a - \bar{\delta}^n(a-1) \\
(1-\bar{\delta}^{*n})_\times(a) &= a - \bar{\delta}^{*n}(a-1)
\end{aligned}$$

Proof. Immediate from Proposition 3.2.1. □

We have almost reached a ring decomposition theorem which summarizes the development so far in this chapter. However, for completeness, we would like to show that the decomposition is the finest possible, and to prove this we need the next proposition.

3.2.16 **Proposition** Let F be a field of characteristic k. If $k > 0$, we suppose $k \nmid n$. Let $E = F(\zeta)$ where ζ is a primitive n^{th} root of unity. Let G be the Galois group for E/F. Let $c \in \mathbf{circ}_n(E)$ with representer polynomial $c(x)$. Then, the eigenvalues of c are $\{\lambda_\xi := c(\xi) \vdash \xi^n = 1\}$, and

$$c \in \mathbf{circ}_n(F) \quad \Leftrightarrow \quad g(\lambda_\xi) = \lambda_{g(\xi)}, \quad \forall g \in G, \quad \forall \xi, \xi^n = 1$$

Proof. ($\Rightarrow$:) Assume $c \in \mathbf{circ}_n(F)$. That is, the components of c are all in the base field, F. For any $g \in G$ and any n^{th} root of unity, ξ, g must map ξ to another n^{th} root of unity. That is, $g : \xi \mapsto \xi^t$ for some t. Hence,

$$g : c_0 + c_1\xi + \ldots + c_i\xi^i + \ldots + c_{n-1}\xi^{n-1} \;\mapsto\; c_0 + c_1\xi^t + \ldots + c_i\xi^{it} + \ldots + c_{n-1}\xi^{(n-1)t}$$

That is, $g : \lambda_\xi(c) \mapsto \lambda_{g(\xi)}(c)$. QED($\Rightarrow$)

($\Leftarrow$:) Now suppose that $g\,(\lambda_\xi(c)) = \lambda_{g(\xi)}(c)$ for all $g \in G$. We shall show that each c_i is invariant under G which implies that $c_i \in F$ thus completing the proof.

$$c_i = n^{-1} \sum_{\xi^n=1} \xi^{-i}\lambda_\xi$$

$$\therefore\; g(c_i) = n^{-1} \sum_{\xi^n=1} g(\xi)^{-i} g(\lambda_\xi) = n^{-1} \sum_{\xi^n=1} g(\xi)^{-i}\lambda_{g(\xi)} = n^{-1} \sum_{g^{-1}(\xi)^n=1} \xi^{-i}\lambda_\xi = c_i \;\square$$

3.2.17 **The Circulant Decomposition Theorem** Let R be an integral domain whose characteristic does not divide n, let Q be its quotient ring, and let $n^{-1}R \subset Q$ be the set of fractions in Q whose denominators divide n.

(i) There is an internal direct sum decomposition of $\mathbf{circ}_n(R)$ into direct summands in $\mathbf{circ}_n(n^{-1}R)$.

$$\mathbf{circ}_n(R) \;=\; \bigoplus_{d|\,n} \bar{\delta}^{*d}\mathbf{circ}_n(R) \tag{3}$$

If furthermore the n^{th} cyclotomic polynomial, Φ_n, is irreducible over Q, then

(ii) The above decomposition has no proper refinement into circulants over Q, and is unique with this property.

(iii) $\bar{\delta}^{*d}\mathbf{circ}_n(R) \overset{\lambda_d}{\approx} \lambda_d\left(\mathbf{circ}_n(R)\right) \;=\; R(\zeta_{n/d})$. In particular, if R is a field then so is $\bar{\delta}^{*d}\mathbf{circ}_n(R)$.

(iv) $\displaystyle\bigoplus_{d|\,n}\lambda_d \;:\; \mathbf{circ}_n(R) \;\approx\; \bigoplus_{d|\,n} R(\zeta_{n/d})$.

Proof. Statement *(i)* and equation (3) follows from Proposition 3.2.1 and Proposition 3.2.11.

(ii) We need only prove that the direct sum in equation (3) cannot be further decomposed. What we shall actually show is that the idempotents $\bar{\delta}^{*d|\,n}$ are **primitive** in the sense that none can be expressed non-trivially as a sum of complementary idempotents in $\mathbf{circ}_n(Q)$.

Hence we need to show that if $\bar{\delta}^{*d} = e + f$ with e, f complementary idempotents in $\mathbf{circ}_n(Q)$, then $e = 0$ or $f = 0$. For this proof it is convenient to temporarily use the matrix point of view. Let $E = \mathrm{CIRC}_n(e)$. Since E is an idempotent matrix, its eigenvalues are either 0 or 1. But E is circulant, therefore $\lambda(E)$ is a diagonal matrix of zeroes and ones. That is, $\tilde{e} = \lambda(e)$ is a vector of zeroes and ones, and likewise, so is $\tilde{f} = \lambda(f)$. Now, $\delta^{*d} = \tilde{e} + \tilde{f}$. Therefore, $\mathrm{supp}(\tilde{e})$ and $\mathrm{supp}(\tilde{f})$ are subsets of $\mathrm{supp}(\delta^{*d}) = (d)^*$. But, $\tilde{e}$, $\tilde{f}$ are complementary, and $\tilde{e} + \tilde{f} = \delta^{*d}$, so $\mathrm{supp}(\tilde{e}) \cap \mathrm{supp}(\tilde{f}) = \emptyset$ and $\mathrm{supp}(\tilde{e}) \cup \mathrm{supp}(\tilde{f}) = (d)^*$. If both e and f are non-zero, we must have $\mathrm{supp}(\tilde{e}) \subsetneq (d)^*$. This means that some non-zero component of δ^{*d} is zero in $\tilde{e}$. That is, there exists $j \in (d)^*$ such that $\tilde{e}_{jd} = \lambda_{dj}(e) = 0$.

We are given that Φ_n is irreducible over Q. By Proposition 3.2.13, the orbit of $\tilde{e}$ under the Galois group is $L_d^*(e) = \{\lambda_{dh}(e) \vdash h \in (d)^*\}$. We note that $0 = \lambda_{dj}(e) \in L_d^*(e)$. Let $g : \zeta \mapsto \zeta^k$ be in the Galois group. We now apply Proposition 3.2.16 to $e \in \mathbf{circ}_n(Q)$, obtaining the condition $0 = g\lambda_{jd}(e) = \lambda_{jkd}(e)$. This is true for all k coprime to n. Hence, $\lambda(e) = 0$ which implies $e = 0$. This shows that $\bar{\delta}^{*d}$ is primitive, and consequently that (3) has no refinement.

To finish the proof of statement *(ii)*, we need to show that there is no other direct sum like (3) into indecomposables. Suppose there was, $\mathbf{circ}(R) \approx \oplus_k A_k$, say, where each A_k is a subring if $\mathbf{circ}(R)$. The projection operators onto A_k must form a set P of primitive idempotents.

Fix $d \,|\, n$. Since $\bar{\delta}^{d*}\mathbf{circ}(R) \neq 0$, there must exist $\pi \in P$ such that $\bar{\delta}^{d*}\pi \neq 0$. Let $e = \bar{\delta}^{d*} - \pi\bar{\delta}^{d*}$, and let $f = \pi\bar{\delta}^{d*}$. Then, e and f are idempotents, $\bar{\delta}^{d*} = e + f$, and $ef = 0$. Since $\bar{\delta}^{d*}$ is primitive, and since $\pi\bar{\delta}^{d*} \neq 0$ by choice of π, this is possible only if $\bar{\delta}^{d*} = \pi\bar{\delta}^{d*}$. Now, let $g = \pi - \pi\bar{\delta}^{d*}$. We have $\pi = f + g$, and $fg = 0$, and as before we conclude that $\pi = \pi\bar{\delta}^{d*}$. But, $\pi\bar{\delta}^{d*} = \bar{\delta}^{d*}$. Therefore, $\bar{\delta}^{d*} = \pi$. Since d was an arbitrary divisor of n, it follows that all the $\bar{\delta}^{d*}$ idempotents are in P. Repeating the argument with the roles of P and $D = \{\bar{\delta}^{d*} \vdash d \,|\, n\}$ reversed shows that $P = D$. QED *(ii)*

(iii) The particular case when R is a field follows from a standard theorem which says that an indecomposable finite dimensional algebra over a field which has no nilpotent elements is a field. (See [FT1].) Statement *(ii)* shows that the components of the direct sum in (3) are indecomposable finite dimensional algebras. Also, since the components of (3) are subalgebras of $\mathbf{circ}_n(R)$, they cannot have nilpotent elements. Thus the standard theorem implies that $\bar{\delta}^{*d}\mathbf{circ}_n(Q)$ is a field.

To see the first statement in *(iii)*, we need to analyze the set $\bar{\delta}^{*d}\mathbf{circ}_n(R)$ more closely. We have that $\bar{\delta}^{*d}\mathbf{circ}_n(R) \approx \lambda\bar{\delta}^{*d}\mathbf{circ}_n(R) = \delta^{*d}\mathbf{circ}_n(R)$. This latter set consists of vectors $\mu \in \Lambda_n$ of the form

$$\mu_i \;=\; \begin{cases} \lambda_i & \text{if } i \in (d)^* \\ 0 & \text{otherwise} \end{cases}$$

The set of non-zero components of μ is L_d^*. By Proposition 3.2.13, L_d^* is an orbit under the Galois group. Hence, all members of L_d^* are determined by any one member of L_d^*, for example, by λ_d. This shows that $\delta^{*d}\mathbf{circ}_n(R)$ must be isomorphic to the set $\{\lambda_d(c) \vdash c \in \mathbf{circ}_n(R)\} = R(\zeta_{n/d})$.

(iv) This decomposition follows trivially from the decomposition of (3). □

Interestingly, there seems to be no easy way to prove statement *(ii)* in the theorem without recourse to treating the circulants as matrices. One wonders how a researcher who first encountered circulants as group rings on cyclic groups (see §3.6) would discover this proof except by effectively rediscovering the circulants as matrices, e.g. by analyzing right translation in the group algebra, $C : a \mapsto ac$ whose matrix representation is in fact $\mathrm{CIRC}(c)$.

3.2.17.1 **Corollary** Given any commutative ring S with identity, write its group of units as $\mathbf{U}(S)$.

(i) Under the conditions of the theorem, the group of invertible circulants over R has a direct sum decomposition given by (written multiplicatively)

$$\mathbf{U}(\mathbf{circ}_n(R)) \;=\; \prod_{d|\,n} \bar{\delta}_\times^{*d}\mathbf{U}(\mathbf{circ}_n(R)) \tag{4}$$

(ii) If $\Phi_n(x)$ is irreducible, then each component in (4) satisfies

$$\bar{\delta}_\times^{*d}\mathbf{U}(\mathbf{circ}_n(R)) \;\overset{\lambda_d}{\approx}\; \lambda_d(\mathbf{U}(\mathbf{circ}_n(R))) \;=\; \mathbf{U}\left(R(\zeta_{n/d})\right).$$

Proof. Apply Proposition 3.2.1 □

We can apply the corollary to derive a factorization of a circulant determinant over an integrally closed ring.

3.2.18 **Proposition** Let Q be the field of quotients for R, and suppose that $R(\zeta_n) \cap Q = R$. Let $a \in \mathbf{circ}_n(R)$. Then,

(i) $\Delta_n\left(\bar{\delta}_\times^{*d}(a)\right) \;=\; \prod L_{d|\,n}^*(a) \;\in\; R.$

(ii) $\Delta_n(a)$ factorizes in R into a product of circulant determinants over $n^{-1}R$:

$$\Delta_n(a) \;=\; \prod_{d|\,n} \Delta_n\left(\bar{\delta}_\times^{*d}(a)\right)$$

(iii) If $\Phi_n(x)$ is irreducible over Q, then $\Delta_n\left(\bar{\delta}_\times^{*d}(a)\right) = \mathcal{N}_d(\lambda_d(a))$, and

$$\Delta_n(a) \;=\; \prod_{d|\,n} \mathcal{N}_{n/d}(\lambda_d(a))$$

where $\mathcal{N}_m(z)$ is the cyclotomic norm of $z \in Q(\zeta_m)$ (see Appendix A).

Proof.

(i) From the definitions: $L_{d|\,n}^*(a)$ is the set of eigenvalues of $\bar{\delta}_\times^{*d}(a)$ which have not been projected to unity. Their product is just $\Delta_n\left(\bar{\delta}_\times^{*d}(a)\right)$. By Corollary 3.2.14, $\prod L_{d|\,n}^*(a) \in R$. QED *(i)*

(ii) Following the decomposition of the corollary, we have

$$\Delta_n(a) \;=\; \prod_{i\in\mathbb{Z}_n} \lambda_i(a) \;=\; \prod_{d|\,n}\prod L_{d|\,n}^* \;=\; \prod_{d|\,n} \Delta_d\left(\bar{\delta}_\times^{d|\,n}(a)\right)$$

(iii) When $\Phi_n(x)$ is irreducible, the eigenvalues of $\bar{\delta}_\times^{d|\,n}(a)$ are the just the conjugates of $\lambda_d(a)$. □

The integrally closed ring of most interest to us is the rational integers, $\mathbb{Z}$. The proposition implies that a circulant determinant of order n over the integers has an integer factor for every divisor of d of n, and each of these factors is itself a circulant determinant over $n^{-1}\mathbb{Z}$.

3.2.18.1 **The Case of Reducible Cyclotomic Polynomials.**

We shall briefly indicate what happens when $\Phi_n(x)$ is not irreducible over the field of quotients, Q. Fix n, and let $\Phi = \Phi_n$, and $\zeta = \zeta_n$. Suppose $\Phi(x) = \Phi_1(x)\cdots\Phi_r(x)$ where each Φ_i is irreducible over Q. Let Z denote the set of primitive n^{th} roots of unity. Then, Z is partitioned into sets $Z_1, Z_2, \ldots, Z_r$ corresponding to the roots of the irreducibles, $\Phi_1, \Phi_2, \ldots, \Phi_r$, respectively. Let us suppose $\zeta \in Z_1$, $\zeta^{e_2} \in Z_2, \ldots, \zeta^{e_r} \in Z_r$ where $1 = e_1, e_2, \ldots, e_r$ are coprime residues modulo n. Then, the splitting field of Φ_1 must also be the splitting field of every other Φ_i.

Let the Galois group be G. G is still cyclic, and permutes the roots of each irreducible. Therefore, there is g coprime to n, such that $\tau_g : \zeta \mapsto \zeta^g$ generates G. So G consists of maps $\tau_g^i : \zeta \mapsto \zeta^{g^i}$. The action of G on Z_i is given by $\tau_g^i : \zeta^{e_j} \mapsto \zeta^{e_j g^i}$. This shows that the action of G on Z_1 is exactly mirrored by its action on Z_i. Hence, $|Z_i| = |Z_1|$ for all $i = 1, \ldots, r$. $\therefore\ |Z_i| = \phi(n)/r$, and $\deg \Phi_i = \phi(n)/r$, and in particular, $r \,|\, \phi(n)$.

If $\Phi(x)$ is reducible, the idempotent $\bar{\delta}^{1*}$ is no longer primitive. It can be decomposed into r idempotents whose support sets are $S_i = \{g^j e_i \vdash j = 0, \ldots, \phi(n)/r\}$ for $i = 1, \ldots, r$. Other idempotents might also decompose. However, $\bar{\delta}^{d*}$ will still be primitive if $\phi(n/d)$ is coprime to r.

3.2.19 **Example** $n = 6$. The circulant residue class idempotents for $n = 6$ are:

$$\begin{array}{rcl}
\bar{\delta}^{1*} &=& 6^{-1}\mathbf{circ}(\ 2,\ \ 1,\ -1,\ -2,\ -1,\ \ 1\ ) \\
\bar{\delta}^{2*} &=& 6^{-1}\mathbf{circ}(\ 2,\ -1,\ -1,\ \ 2,\ -1,\ -1\ ) \\
\bar{\delta}^{3*} &=& 6^{-1}\mathbf{circ}(\ 1,\ -1,\ \ 1,\ -1,\ \ 1,\ -1\ ) \\
\bar{\delta}^{6*} &=& 6^{-1}\mathbf{circ}(\ 1,\ \ 1,\ \ 1,\ \ 1,\ \ 1,\ \ 1\ )
\end{array}$$

Let $c = \mathbf{circ}(1,\ 2,\ -3,\ -2,\ -1,\ 0)$. Then,

$$\begin{array}{rcl}
c &=& \mathbf{circ}(\ \ 1,\ \ 2,\ -3,\ -2,\ -1,\ \ 0\ ) \\
\bar{\delta}^{1*}(c) &=& \mathbf{circ}(\ \ 2,\ \ 1,\ -1,\ -2,\ -1,\ \ 1\ ) \\
\bar{\delta}^{2*}(c) &=& \mathbf{circ}(\ \ 0,\ \ 1,\ -1,\ \ 0,\ \ 1,\ -1\ ) \\
\bar{\delta}^{3*}(c) &=& 2^{-1}\mathbf{circ}(\ -1,\ \ 1,\ -1,\ \ 1,\ -1,\ \ 1\ ) \\
\bar{\delta}^{6*}(c) &=& 2^{-1}\mathbf{circ}(\ -1,\ -1,\ -1,\ -1,\ -1,\ -1\ )
\end{array}$$

$$\begin{array}{rcl}
\bar{\delta}_\times^{1*}(c) &=& 6^{-1}\mathbf{circ}(\ 16,\ \ 5,\ -5,\ -10,\ -5,\ \ 5\ ) \\
\bar{\delta}_\times^{2*}(c) &=& 6^{-1}\mathbf{circ}(\ \ 4,\ \ 7,\ -5,\ \ -2,\ \ 7,\ -5\ ) \\
\bar{\delta}_\times^{3*}(c) &=& 6^{-1}\mathbf{circ}(\ \ 2,\ \ 4,\ -4,\ \ \ 4,\ -4,\ \ 4\ ) \\
\bar{\delta}_\times^{6*}(c) &=& 6^{-1}\mathbf{circ}(\ \ 2,\ -4,\ -4,\ \ -4,\ -4,\ -4\ )
\end{array}$$

$$\begin{array}{rcl}
\Delta(\bar{\delta}_\times^{1*}c) &=& 36 \\
\Delta(\bar{\delta}_\times^{2*}c) &=& 12 \\
\Delta(\bar{\delta}_\times^{3*}c) &=& -3 \\
\Delta(\bar{\delta}_\times^{6*}c) &=& -3 \\
\Delta(c) &=& 3888 \ =\ 3\times 3\times 12\times 36
\end{array}$$

3.3 The Polynomial Wrap-Around Map, $\Gamma^N : R[x] \to \mathbf{circ}_N(R)$.

In this section we study homomorphisms from (or to) $\mathbf{circ}_N(R)$ to (or from) other rings (including $\mathbf{circ}_M(R)$). In other words, we will be looking at some non-endomorphic homomorphisms. Even so we shall see echoes of the idempotent maps of the previous sections in this chapter.

We begin with a map of the polynomial ring $R[x]$ to $\mathbf{circ}_N(R)$.

For an arbitrary polynomial, $A(x) = \sum_{i=0}^{L} a_i x^i \in R[x]$, define $\Gamma^N(A) = \mathbf{circ}(\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_{N-1})$ where $\bar{a}_i = \sum_{j\equiv i \pmod N} a_j$.

Pictorially, one can think of the homomorphism as follows: Take the sequence of polynomial coefficients and wrap them around a circle of N points. The coefficients will go round the circle as many times as N goes into $1 + \deg(A)$. All the coefficients that land on a point i are added up to give the i^{th} component of the circulant vector. Because of this intuitive description, we call this homomorphism the **polynomial wrap-around map**. There is also a simple and convenient algebraic formulation. First recall the standard bases introduced in §1.10, namely,

$$\begin{aligned} \mathbf{circ}(a_0, a_1, \ldots, a_{N-1}) &= \sum_{i \in \mathbb{Z}_N} a_i \mathrm{u}^i \\ \mathrm{CIRC}(a_0, a_1, \ldots, a_{N-1}) &= \sum_{i \in \mathbb{Z}_N} a_i \mathrm{U}^i \end{aligned}$$

The algebraic definition of Γ^N is:

3.3.1 **Definition** Let $a(x) = \sum_{i=0}^{L} a_i x^i \in R[x]$ then $\Gamma^N(a) := a(\mathrm{u})$.

The polynomial $a(\mathrm{u})$ is $a(x)$ regarded as a polynomial in $\mathbf{circ}(R)[x]$ evaluated at $x = \mathrm{u}$. That this defines the same map as before should be fairly clear.

Lastly, we point out that the representer polynomial is a partial inverse of the Γ_N map. That is, if $A(x)$ is the representer polynomial for the circulant $a \in \mathbf{circ}_N(R)$, then $\Gamma(A) = a$.

3.3.2 **Proposition** $\Gamma^N : R[x] \to \mathbf{circ}_N(R)$ is a ring homomorphism with kernel $(x^N - 1)$.

Proof. Definition 3.3.1 shows that Γ^N is just a substitution map. Hence Γ^N is a ring homomorphism. So, we need only show that $\ker \Gamma^N = (x^N - 1)$. That $(x^N - 1) \subset \ker \Gamma^N$ is immediate from $\Gamma^N(x^N - 1) = \mathrm{u}^N - 1 = 0$.

To prove the reverse inclusion, let $a(x) = \sum_{i=0}^{L} a_i x^i \in \ker \Gamma^N$, then $\Gamma^N(A) = 0$. By extending a with zero terms we can assume that $L = mN$ for some m.

$$a(x) = \sum_{i=0}^{N-1} x^i \sum_{j=0}^{m} a_{i+jN}\, x^{jN}$$

Let $b(x^N)$ be the series multiplying x^i in this equation.

$$b_i(t) = \sum_{j=0}^{m} a_{i+jN} t^j \quad \text{where } t = x^N$$

$$\therefore b_i(1) = \sum_{j=0}^{m} a_{i+jN} = \sum_{k \equiv i} a_k = \Gamma^N(a)_i = 0$$

Therefore, 1 is a root of b_i. $\therefore t - 1$ divides $b_i(t)$ $\therefore x^N - 1$ divides $b_i(x^N)$ for every i. $\therefore x^N - 1$ divides $a(x)$. $\therefore a(x) \in (x^N - 1)$. □

Given $a \in \mathbf{circ}_N(R)$ then, by the above proposition, there is only one member of $\left(\Gamma^N\right)^{-1}(a)$ which has degree less than N. It is the representer polynomial, $\sum_{i=0}^{N-1} a_i x^i$, of §1.10.1. We often informally denote it by $a(x)$.

3.4 Homomorphisms to Cyclotomic Fields.

We can use the Γ^N map defined above to induce other homomorphisms on circulants given homomorphisms on $R[x]$. The situation is described by the next, general ring, lemma.

3.4.1 **Lemma**

$$\begin{array}{ccc} A & & \gamma \\ {\scriptstyle\beta}\big\downarrow & \searrow & \\ B & \longrightarrow & C \\ & {\scriptstyle\kappa?} & \end{array}$$

In the diagram, let A, B, C be (possibly non-commutative) rings. If $\ker\beta \subset \ker\gamma$, then $\kappa : B \to C$ exists with $\kappa\beta = \gamma$ and $\ker\kappa = \beta\ker\gamma$.

Proof. We define $\kappa(b) = \gamma\beta^{-1}(b)$. The condition $\ker\beta \subset \ker\gamma$ ensures that $\kappa(b)$ is a single element. The kernel of κ is given by $\ker\kappa = \beta\ker\gamma$ because $\quad \kappa(b) = 0 \;\Leftrightarrow\; \gamma\beta^{-1}(b) = 0 \;\Leftrightarrow\; b \in \beta\ker\gamma$. □

We apply the lemma to the diagram below with $A = R[x]$, $B = \mathbf{circ}(R)$, and with T being any ring.

$$\begin{array}{ccc} R[x] & & \phi \\ {\scriptstyle\Gamma^N}\big\downarrow & \searrow & \\ \mathbf{circ}_N(R) & \longrightarrow & T \\ & {\scriptstyle\phi'?} & \end{array}$$

Hence, ϕ' is well-defined provided $\ker\Gamma^N \subset \ker\phi$. Similarly, in the following diagram, if given an endomorphism ϕ on $R[x]$, and $\gamma : R[x] \to T$, then ϕ' is well-defined whenever $\ker\Gamma^N \subset \phi^{-1}\ker\gamma$.

$$\begin{array}{ccc} R[x] & \xrightarrow{\phi} & R[x] \\ {\scriptstyle\Gamma^N}\big\downarrow & & \big\downarrow{\scriptstyle\gamma} \\ \mathbf{circ}_N(R) & \xrightarrow[\phi']{} & T \end{array} \tag{5}$$

An example of this construction is when ϕ is the power map on polynomials is defined next.

3.4.2 **Definition** Define $\epsilon^i : R[x] \to R[x]$ by $\quad \epsilon^i(f(x)) = f(x^i),\ \forall i \in \mathbb{Z}$.

In diagram (5) set $\phi = \epsilon^i$ for some i, set $T = R(\zeta)$, and set γ to the evaluation map at an N^{th} root of unity, $\gamma : f(x) \mapsto f(\zeta_N)$. We get

$$\begin{array}{ccc} R[x] & \xrightarrow{\epsilon^i} & R[x] \\ {\scriptstyle\Gamma^N}\big\downarrow & & \big\downarrow{\scriptstyle x \mapsto \zeta} \\ \mathbf{circ}_N(R) & \xrightarrow[\lambda_i]{} & R(\zeta) \end{array}$$

We see that we have constructed the eigenvalue maps. Indeed, when R is an integral domain we have constructed **all** the maps from the circulants to any extension of R.

3.4.3 **Proposition** The only ring homomorphisms from $\mathbf{circ}_N(R)$ to an extension of R are the eigenvalue maps, $\lambda_0, \lambda_1, \ldots, \lambda_{N-1}$.

Proof. Let $\alpha : \mathbf{circ}_N(R) \to E \supset R$ be such a homomorphism. We have $\alpha(\mathrm{u}^N) = \alpha(1) = 1$. Therefore $\alpha(\mathrm{u})$ is an N^{th} root of unity; $\alpha(\mathrm{u}) = \zeta_n^i$ for some $n \,|\, N$, i coprime to N, and so $\alpha(\mathrm{u}^j) = \zeta_n^{ij}$. That is, $\alpha = \lambda_{iN/n}$. □

For completeness, we shall also compute the kernel of λ_i. The next lemma shows that in the important case (e.g. $R = \mathbb{Z}$) when $\Phi(x)$ is irreducible, the kernel of λ_i depends only the residue class of $i \pmod N$.

3.4.4 **Lemma** If $\Phi_N(x)$ is irreducible over the ring of quotients of R, then every map in $L^*_{d|\,N}$ has the same kernel.

Proof. Suppose $\lambda_d(a) = 0$ for $d \,|\, N$. Since $\Phi_N(x)$ is irreducible, there is a map in the Galois group which maps $\zeta_N \mapsto \zeta_N^h$ for every h coprime to N. Therefore, for every h coprime to N, there exists $g_h : \zeta_{N/d} \mapsto \zeta_{N/d}^h$ Now, $g_h : \lambda_d(a) \mapsto \lambda_{hd}(a)$. Therefore, $\lambda_d(a) = 0 \;\Rightarrow\; \lambda_{hd}(a) = 0$. The converse is deduced by applying the inverse map, g_h^{-1}. Hence, $i \in (d)^* \;\Rightarrow\; \ker\lambda_i = \ker\lambda_d$ □

We shall continue to assume that $\Phi(x)$ is irreducible to the end of this section. This allows us to restrict our attention to the maps λ_d where $d \,|\, N$ whose kernels we now characterize.

3.4.5 **Proposition** Let R be an integral domain and Q its field of quotients. Let $d \,|\, N$, and suppose that the d^{th} cyclotomic polynomial, $\Phi_d(x)$, is irreducible over Q. Then, $\lambda_{N/d} : \mathbf{circ}_N(R) \to R(\zeta_d)$ is onto, and $\ker\lambda_{N/d} = \big(\Phi_d(\mathrm{u})\big) \subset \mathbf{circ}_N(R)$.

Proof. Let γ be the evaluation map from $R[x]$ to $R(\zeta_d)$ defined by $\gamma(f) = f(\zeta_d)$. Then, $\ker\gamma = (\Phi_d(x))$. Since $d \,|\, N$, $\ker\Gamma^N = (x^N - 1)$ is divisible by $\Phi_d(x)$. Therefore, $\ker\Gamma^N \subset \ker\gamma$. Lastly, note that $\lambda_{N/d}\Gamma^N = \gamma$. Therefore, by Lemma 3.4.1, $\ker\lambda_{N/d} = \Gamma^N \ker\gamma = \big(\Phi(x)|_{x=\mathrm{u}}\big)$. □

3.4.6 **Corollary** Let R be as in 3.4.5 and let $N = p^n$, and suppose $q \parallel N$, then

$$\ker\lambda_q = \Big(\mathbf{circ}_N\Big(\delta^{(N/pq)|\,N}\Big)\Big) = \Big(pq\bar{\delta}^{pq|\,N}\Big)$$

In particular, when $N = p$, $\ker\lambda_1$ is the set of circulants in $\mathbf{circ}_N(R)$ having all elements equal which corresponds to the set of rank 1 circulant matrices.

Proof. See the cyclotomic polynomials for prime powers in Appendix A §A.3. □

3.5 The Homomorphisms $\Gamma^s_r : \mathbf{circ}_r(R) \to \mathbf{circ}_s(R)$.

These homomorphisms are initially defined as maps between circulant spaces of commensurate dimensions. That is, either the dimension of the range divides the dimension of the domain, or vice versa. Later, we shall give a more general definition.

3.5.1 **Definition**

(i) Define the map $\Gamma^n_{mn} : \mathbf{circ}_{mn} \to \mathbf{circ}_n$ by

$$\Gamma^n_{mn}\left(\sum_{i=0}^{mn-1} a_i \mathrm{u}_{mn}^i\right) \;=\; \sum_{i=0}^{mn-1} a_i \mathrm{u}_n^i$$

We call Γ^n_{mn} the **circulant wrap-around** map because of its similarity to the polynomial wrap-around map. By setting $a_i = 0$ for all $i \geq n$, and letting $a_0, a_1, \ldots, a_{n-1}$ be arbitrary, we see that Γ^n_{mn} is onto $\mathbf{circ}_n$.

(ii) Define the map $\Gamma^{mn}_n : \mathbf{circ}_n \to \mathbf{circ}_{mn}$ by

$$\begin{aligned}\Gamma^{mn}_n\left(\sum_{i=0}^{n-1} a_i \mathrm{u}_n^i\right) \;&:=\; \frac{1}{m}\sum_{i=0}^{mn-1} a_{i \bmod n}\mathrm{u}_{mn}^i \\ &=\; \bar{\delta}^{m|\,mn}\sum_{i=0}^{n-1} a_i \mathrm{u}_{mn}^i\end{aligned} \tag{6}$$

The last equation above will be proved in Proposition 3.5.2.

We call Γ^{mn}_n the **circulant repeater** map since the n coefficients of a are repeated m times in the image. We shall see that Γ^{mn}_n is an injection into $\mathbf{circ}_{mn}$.

Remark. As in §2.5.1, these two ring homomorphisms are more simply defined by their action on u. $\Gamma^n_{mn} : \mathrm{u}_{mn} \mapsto \mathrm{u}_n$, and $\Gamma^{mn}_n : \mathrm{u}_n \mapsto \bar{\delta}^m \mathrm{u}_{mn}$.

We should do a couple of checks. Firstly, despite immediate appearances, Γ_n^{mn} maps the identity to the identity because $\bar{\delta}^m$ is the identity element in the ring $\bar{\delta}^m\mathbf{circ}_{mn}$ which is the range of Γ_n^{mn}. Secondly, when $m=1$, Γ_{mn}^n and Γ_n^{mn} are both the identity map on $\mathbf{circ}_n$, and so the two definitions of Γ_n^n agree.

The eigenspace versions of these homomorphisms are defined in the usual way as $\tilde{\Gamma}_{mn}^n := \lambda\Gamma_{mn}^n\lambda^{-1}$, and $\tilde{\Gamma}_n^{mn} := \lambda\Gamma_n^{mn}\lambda^{-1}$. We shall refer to $\tilde{\Gamma}_{mn}^n$ as the **eigenvalue filter** map, and we shall call $\tilde{\Gamma}_n^{mn}$ the **eigenvalue injection** map. The names are justified by the next proposition which gives the actions of these maps on the eigenspaces.

3.5.2 **Proposition**

(i) For $z \in \Lambda_{mn}$, $\tilde{\Gamma}_{mn}^n(z)_i = z_{im}$. (Filter Map)

(ii) For $z \in \Lambda_n$, $\tilde{\Gamma}_n^{mn}(z)_i = \delta_i^m z_{i/m}$. (Injection Map)

(iii) Equation (6) holds.

Proof. Note that, in the interests of clarity, the proof will use the full notation, $\lambda^{(n)}$, for $\lambda|\mathbf{circ}_n$.

(i)
$$\lambda^{(n)}\Gamma_{mn}^n(a) = \lambda^{(n)}\left(\sum_{j=0}^{mn-1} a_j \mathrm{u}_n^j\right)$$

$$\therefore\ \lambda_i^{(n)}\left(\Gamma_{mn}^n(a)\right) = \sum_{j=0}^{mn-1} a_j\zeta_n^{ij} = \sum_{j=0}^{mn-1} a_j\zeta_{mn}^{mij} = \lambda_{im}^{(mn)}(a)$$

$$\therefore\ \lambda_i^{(n)}\left(\Gamma_{mn}^n(\lambda^{-(mn)}(z))\right) = \lambda_{im}^{(mn)}(\lambda^{-(mn)}(z)) = z_{im} \quad \text{QED } \textit{(i)}$$

(ii) We take the first formula for Γ_n^{mn} in equation (6).

$$\begin{aligned}
\lambda^{(mn)}\Gamma_n^{mn}(a) &= \lambda^{(mn)}\left(\frac{1}{m}\sum_{j=0}^{mn-1} a_{j \bmod n}\mathrm{u}_{mn}^j\right)\\
\therefore\ \lambda_i^{(mn)}\Gamma_n^{mn}(a) &= \frac{1}{m}\sum_{j=0}^{mn-1} a_{j \bmod n}\zeta_{mn}^{ij} = \frac{1}{m}\sum_{k=0}^{n-1}\sum_{l=0}^{m-1} a_k\zeta_{mn}^{i(k+ln)} \quad \text{where } j=k+ln\\
&= \frac{1}{m}\sum_{k=0}^{n-1} a_k\zeta_{mn}^{ik}\sum_{l=0}^{m-1}\zeta_m^{il} = \frac{1}{m}\sum_{k=0}^{n-1} a_k\zeta_{mn}^{ik}m\delta_i^m = \delta_i^m\sum_{k=0}^{n-1} a_k\zeta_n^{ki/m}\\
&= \delta_i^m\lambda_{i/m}^{(n)}(a)\\
\therefore\ \left(\lambda\Gamma_n^{mn}\lambda^{-1}(z)\right)_i &= \delta_i^m z_{i/m} \quad \text{QED } \textit{(ii)}
\end{aligned}$$

(iii) Consider, $\lambda^{(mn)}$ operating on the second expression in (6).

$$\lambda_i^{(mn)}\left(\bar{\delta}^{m|mn}\sum_{i=0}^{n-1} a_i\mathrm{u}_{mn}^i\right) = \delta_i^m\left(\sum_{j=0}^{n-1} a_j\zeta_{mn}^{ij}\right) = \delta_i^m\sum_{j=0}^{n-1} a_j\zeta_n^{ij/m} = \delta_i^m\lambda_{i/m}^{(n)}(a) = \tilde{\Gamma}_n^{mn}\lambda^{(n)}(a) \ \square$$

To paraphrase this proposition, let $x = \tilde{\Gamma}_{mn}^n(z)$, then x is the vector of every m^{th} component of z. Whereas, if $z = \tilde{\Gamma}_n^{mn}(x)$, then every m^{th} component of z is set to the successive components of x and all other components of z are set to zero.

3.5.2.1 **Corollary** Γ_n^{mn} is a monomorphism. $\square$

3.5.2.2 **Corollary** $\bar{\delta}^m\mathbf{circ}_{mn} \approx \mathbf{circ}_n$.

Proof. We shall show that the diagram below is commutative and that the vertical map is an isomorphism.

$$\begin{array}{ccc} & \overset{\bar{\delta}^m}{\longrightarrow} & \bar{\delta}^m\mathbf{circ}_{mn} \\ \mathbf{circ}_{mn} & \searrow & \downarrow\Gamma^n_{mn} \\ & \Gamma^n_{mn} & \mathbf{circ}_n \end{array}$$

$\Gamma^n_{mn} : \mathbf{circ}_{mn} \to \mathbf{circ}_n$ onto. From the proposition we see that, $\ker\tilde{\Gamma}^n_{mn} = \{\mu \in \Lambda_{mn} \vdash \mu_{im} = 0,\ \forall i\} = \ker\delta^m$. Hence, $\ker\Gamma^n_{mn} = \ker\bar{\delta}^m$ implying that $\Gamma^n_{mn}\bar{\delta}^m$ is onto. Since $\bar{\delta}^m$ is an idempotent, its image is complementary to its kernel. Therefore, $\ker\Gamma^n_{mn} \cap \bar{\delta}^m\mathbf{circ}_{mn} = 0$ implying $\Gamma^n_{mn}\bar{\delta}^m$ is 1-1. □

The corollary shows that $\mathbf{circ}_n$ is isomorphic to an ideal of $\mathbf{circ}_{mn}$. This is not the only embedding of $\mathbf{circ}_n$ in $\mathbf{circ}_{mn}$. Consider the subalgebra of $\mathbf{circ}_{mn}$ generated by u^m_{mn}. We can identify u^m_{mn} with u_n (this is made precise in the next chapter), so we also have a subalgebra of $\mathbf{circ}_{mn}$ isomorphic to $\mathbf{circ}_n$. To anticipate just a little more, there is an embedding map from $\mathbf{circ}_n$ to $\mathbf{circ}_{mn}$; it is in fact what we currently consider to be an eigenspace map, namely $\tilde{\Gamma}^{mn}_n$.

The Γ maps connect circulant spaces of different dimensions. As such, we can use them to restate the Circulant Decomposition Theorem more naturally. The recast theorem which appears below expresses the decomposition of $\mathbf{circ}_n(R)$ in terms of lower dimensional, and therefore, simpler circulant spaces. As an additional bonus, we can also express the eigenvalues of an $n \times n$ circulant as eigenvalues of lower dimensional circulants. This opens the possibility of a more efficient method of computing eigenvalues.

3.5.2.3 **Theorem Restatement of the Circulant Decomposition Theorem.**
Let R be an integral domain with $n \nmid \mathrm{char}R$.

(i) $$\mathbf{circ}_n(R) \approx \bigoplus_{d|\,n} \bar{\delta}^{*1|\,d}\mathbf{circ}_d(R)$$

(ii) For all $a \in \mathbf{circ}_n(R)$, the eigenvalues of a are given by

$$L_{1|\,n}(a) = \bigcup_{d|\,n} L_{1|\,d}\big(\Gamma^d_n(a)\big) = \biguplus_{d|\,n} L^*_{1|\,d}\big(\Gamma^d_n(a)\big)$$

Proof.

(i) We have $\mathrm{Supp}\,\delta^{*d} \subset \mathrm{Supp}\,\delta^d$, and $\ker\Gamma^n_d \cap \bar{\delta}^d\mathbf{circ}_n = 0$, so $\ker\Gamma^n_d \cap \bar{\delta}^{*d}\mathbf{circ}_n = 0$. So Γ^n_d is also 1-1 on $\bar{\delta}^{*d}\mathbf{circ}_n$. From the definition of $\delta^{*m|\,N}$ in §3.2.10, one easily sees that $\tilde{\Gamma}^n_d\delta^{*d|\,n} = \delta^{*1|\,d}\tilde{\Gamma}^n_d$. Consider a typical factor in the decomposition of $\mathbf{circ}(R)$ in Theorem 3.2.17, namely, $\bar{\delta}^{*d}\mathbf{circ}_n(R)$.

$$\bar{\delta}^{*d|\,n}\mathbf{circ}_n(R) \approx \tilde{\Gamma}^n_d\delta^{*d|\,n}\mathbf{circ}_n(R) = \delta^{*1|\,d}\tilde{\Gamma}^n_d\mathbf{circ}_n(R) = \delta^{*1|\,d}\mathbf{circ}_d(R)$$

Entering the this expression into the decomposition formula of Theorem 3.2.17 gives the desired formula. QED *(i)*

(ii) For $d\,|\,n$, by definition,

$$\begin{aligned} \tilde{\Gamma}^d_n &:= \lambda^{(d)}\,\Gamma^d_n\,\lambda^{-(n)} \\ \therefore \tilde{\Gamma}^d_n\lambda^{(n)} &= \lambda^{(d)}\,\Gamma^d_n \\ \therefore \lambda^{(n)}_{in/d}(a) &= \lambda^{(d)}_i\,\Gamma^d_n(a) \quad \text{for } a \in \mathbf{circ}_n(R) \\ \therefore L_{n/d|\,n}(a) &= L_{1|\,d}\big(\Gamma^d_n(a)\big) \\ \therefore \bigcup_{d|\,n} L_{n/d|\,n}(a) &= \bigcup_{d|\,n} L_{1|\,d}\big(\Gamma^d_n(a)\big) \end{aligned}$$

The second equation follows since it is merely a restatement of the first equation but with overlapping elements removed from the component sets. □

Readers interested in the efficient calculation of the eigenvalues might be struck by the possibilities inherent in the decomposition of $L_{1|n}(a)$. The problem of efficient calculation of the circulant eigenvalues is identical to the problem of efficient calculation of Fourier transforms. There is a large body of work on this question. The method implicit in Theorem 3.5.2.3 is not the most efficient possible. Interested readers should consult Appendix B which contains further references.

3.5.3 $m\Gamma_n^{mn}$ **Acting On** Λ Notice that if we remove the factor of $1/m$ in the definition of Γ_n^{mn} at equation (5), we obtain a vector space map which repeats an n-dimensional vector m times in the space of dimension mn. Thus, if the domain and image vector spaces be endowed with componentwise multiplication, this map would be a ring homomorphism. In other words, it appears that $m\Gamma_n^{mn} : \Lambda_n \to \Lambda_{mn}$ is a ring homomorphism. We shall conclude this indirectly by first showing that $\tilde{\Gamma}_n^{mn}$ is a circulant ring homomorphism induced, through the polynomial wrap-around map, by the ϵ^m map of §3.4.2.

3.5.3.1 **Proposition** The following diagram is commutative. That is, $\tilde{\Gamma}_n^{mn}\Gamma^n = \Gamma^{mn}\epsilon^m$.

$$\begin{array}{ccc} & \epsilon^m & \\ R[x] & \longrightarrow & R[x] \\ \Gamma^n \big\downarrow & & \big\downarrow \Gamma^{mn} \\ \mathbf{circ}_n(R) & \underset{\tilde{\Gamma}_n^{mn}}{\longrightarrow} & \mathbf{circ}_{mn}(R) \end{array}$$

Proof. Let $a \in \mathbf{circ}_n(R)$, and define $a(x) = \sum_{i=0}^{n-1} a_i x^i$. Polynomials mapped to a by Γ^n are of the form $f(x) = a(x) + b(x)(x^n - 1)$.

$$\epsilon^m f(x) = \sum_{i=0}^{n-1} a_i x^{im} + b(x^m)(x^{mn} - 1)$$

$$\therefore \Gamma^{mn}\epsilon^m f(x) = \sum_{i=0}^{n-1} a_i \mathrm{u}_{mn}^{im} + b(\mathrm{u}_{mn}^m)(\mathrm{u}_{mn}^{mn} - 1) = \sum_{i=0}^{n-1} a_i \mathrm{u}_{mn}^{im}$$

$$\text{Now, } \tilde{\Gamma}_n^{mn}\left(\sum_{i=0}^{n-1} a_i \mathrm{u}_n^i\right) = \sum_{i=0}^{mn-1} \delta_i^m a_{i/m}\, \mathrm{u}_{mn}^i = \sum_{i=0}^{n-1} a_i \mathrm{u}_{mn}^{im}$$

$$\therefore \Gamma^{mn}\epsilon^m f(x) = \tilde{\Gamma}_n^{mn}(a) \ \square$$

3.5.4 **Proposition** $\tilde{\Gamma}_n^{mn} : \mathbf{circ}_n(R) \to \mathbf{circ}_{mn}(R)$ is a ring monomorphism and is given by

$$\tilde{\Gamma}_n^{mn}\left(\sum_{i=0}^{n-1} a_i \mathrm{u}_n^i\right) = \sum_{i=0}^{n-1} a_i \mathrm{u}_{mn}^{im}$$

The monomorphism induced by $\tilde{\Gamma}_n^{mn}$ on the eigenspace is $\tilde{\tilde{\Gamma}}_n^{mn} = m\Gamma_n^{mn}$.

Proof. The formula for $\tilde{\Gamma}_n^{mn}$ is immediate from the definition. The formula shows that $\tilde{\Gamma}_n^{mn}$ is 1-1 since $\{\mathrm{u}_{mn}^i\}$ are linearly independent.

It remains to compute the map induced on the eigenspace by $\tilde{\Gamma}_n^{mn}$, that is, the map $\tilde{\tilde{\Gamma}}_n^{mn} = \lambda\tilde{\Gamma}_n^{mn}\lambda^{-1} = \lambda^2\Gamma_n^{mn}\lambda^{-2}$. In order to simplify this expression, we shall take advantage of the fact that the formula for λ is very similar to that for λ^{-1}. For any vector $(x_0, x_1, \ldots, x_{n-1})$ define $\nu_{-1}(x_0, x_1, \ldots, x_{n-1}) = (x_0, x_{n-1}, x_{n-2}, \ldots, x_1)$, that is, $(\nu_{-1}x)_i = x_{-i}$. Clearly, $(\nu_{-1})^2$ is the identity map.

$$\lambda_i^{-1}\left(\sum_{j=0}^{n-1} a_i \mathrm{u}_n^i\right) \;=\; \frac{1}{n}\sum_{j=0}^{n-1} a_j \zeta^{-ij} \;=\; \frac{1}{n}\left(\lambda(\nu_{-1}(a))\right)_i \;=\; \frac{1}{n}\left(\nu_{-1}\lambda(a)\right)_i$$

This shows that $n\lambda^{-1} \;=\; \nu_{-1}\lambda$. $\therefore\; \lambda^2 \;=\; n(\nu_{-1})^{-1} = n\nu_{-1}$, and, in particular, that ν_{-1} and λ commute.

Applying this formula to $\lambda^2\Gamma_n^{mn}\lambda^{-2}$,

$$\lambda^2\Gamma_n^{mn}\lambda^{-2} \;=\; mn\,\nu_{-1}\Gamma_n^{mn}\frac{1}{n}\nu_{-1} \;=\; m\,\nu_{-1}\Gamma_n^{mn}\nu_{-1}$$

Since $(\nu_{-1})^2$ is the identity, all that remains is to show that ν_{-1} commutes with Γ_n^{mn}.

$$\nu_{-1}\Gamma_n^{mn}\left(\sum_{i=0}^{n-1} a_i \mathrm{u}_n^i\right) \;=\; \nu_{-1}\left(\frac{1}{m}\sum_{i=0}^{mn-1} a_{i \bmod n}\mathrm{u}_{mn}^i\right) \;=\; \left(\frac{1}{m}\sum_{i=0}^{mn-1} a_{(mn-i) \bmod n}\mathrm{u}_{mn}^i\right)$$

The final term has coefficients $a_{(mn-i) \bmod n}$. We would have obtained the same term had we started with the circulant $\Gamma_n^{mn}\mathbf{circ}_n(a_0, a_{-1}, a_{-2}, \ldots, a_{-n+1})$. That is, $\nu_{-1}\Gamma_n^{mn}(a) \;=\; \Gamma_n^{mn}\left(\nu_{-1}(a)\right)$. □

From the proof we get the corollary,

3.5.5 **Corollary** $\lambda^2 = n\nu_{-1}$. □

It will be shown that Γ_n^{mn} is a right inverse to Γ_{mn}^n. Curiously, when $m \equiv 1 \pmod{n}$, $\tilde{\Gamma}_n^{mn}$ is a left and right inverse to Γ_{mn}^n. (See §3.7.4ff.) Later in this chapter, we will generalize these maps to Γ_r^s where r, s are any positive integers, but the important cases are the ones already treated. Chapter 6 will offer a different viewpoint on the Γ_r^s maps, and in there the $\tilde{\Gamma}_n^{mn}|\mathbf{circ}$ map turns into an identity map!

We now return to the Γ_m^n and $\tilde{\Gamma}_m^n$ homomorphisms with a view to generalizing them to any positive integers m and n. The proposition which follows is a collection of easily-proved facts on these homomorphisms.

3.5.6 **Proposition** Relations Satisfied by Γ Homomorphisms.

(i) Γ_{mn}^n is a ring epimorphism.

(ii) Γ_n^{mn} is a ring monomorphism.

(iii) $\Gamma_{mn}^n\Gamma^{mn} = \Gamma^n$.

(iv) $\Gamma_{mn}^n\Gamma_{lmn}^{mn} = \Gamma_{lmn}^n$, and $\Gamma_{mn}^{lmn}\Gamma_n^{mn} = \Gamma_n^{lmn}$.

(v) $\Gamma_n^{mn}\Gamma_{mn}^n \;=\; \bar{\delta}^{m|\,mn}$, and $\tilde{\Gamma}_n^{mn}\tilde{\Gamma}_{mn}^n \;=\; \delta^{m|\,mn}$.

(vi) $\Gamma_{mn}^n\Gamma_n^{mn} = \Gamma_n^n$ is the identity map on $\mathbf{circ}_n$.

(vii) $\Gamma_{mn}^m\tilde{\Gamma}_n^{mn}(a) = \lambda_0(a) = \lambda_0^{(n)}(a)\mathrm{u}_m^0 = \lambda_0^{(n)}(a)\bar{\delta}^{1|\,m}$, and

(viii) $\tilde{\Gamma}_{mn}^m\Gamma_n^{mn}(z) \;=\; \frac{1}{m}z_0\delta^{1|\,m}$

Proof. Statements *(i)* through *(vii)* are easily proved. One can prove the eigenspace version of the statement, if that be simpler. Alternatively, one can prove an identity for the generating element of the ring in question ($\mathbf{circ}(R)$, $R[x]$, or $\tilde{\Gamma}(R)$), and then extend the result to the entire ring by linearity. For instance, $\Gamma_{mn}^n(\mathrm{u}_{mn}) = \mathrm{u}_n$ which generates $\mathbf{circ}_n(R)$ proving statement *(i)*.

Statement *(viii)* however is rather subtle. It is the eigenspace version of statement *(vii)* and is derived as follows. We take the third expression given in statement *(vii)*, and conjugate the equation by λ^{-1} getting

$$\tilde{\Gamma}_{mn}^m\tilde{\tilde{\Gamma}}_n^{mn} \;=\; \lambda\lambda_0^{(n)}(a)\bar{\delta}^{1|\,m}\lambda^{-1}$$

$$\therefore\; \tilde{\Gamma}_{mn}^m m\Gamma_n^{mn}(z) \;=\; \lambda_0^{(n)}(a)\delta^{1|\,m} \;=\; z_0\delta^{1|\,m}$$

by propositions 3.5.4 and 3.2.3. □

Statements *(iii)*, *(iv)*, and *(vi)* are cancellation laws for subscripts and superscripts of Γ maps. Mnemonically, subscripts and superscripts can only be cancelled in the ↗ direction, and then only if the dimensions of the two maps (in order of composition, right to left) go up-up, down-down, or up-down. Thus,

$$\Gamma^{n}_{\not m\not h\not l}\Gamma^{\not m\not h\not l}_{lmn} \quad \text{(correct)}$$

$$\Gamma^{m}_{\not m\not h\not l}\Gamma^{\not m\not h\not l}_{n} \quad \text{(correct)}$$

but not $\Gamma^{\not m\not h\not l}_{mn}\Gamma^{mn}_{\not m\not h\not l}$ Wrong: cancellation not in ↗ direction

and not $\Gamma^{mn}_{\not m\not h\not l}\Gamma^{\not m\not h\not l}_{mn}$ Wrong: dimensions proceed (right-to-left) down then up.

We shall later need one corollary of Proposition 3.5.6.

3.5.6.5 **Corollary** $\Gamma^{mn}_{n}\mathbf{circ}_n(R) \;=\; \bar{\delta}^{m|\,mn}\left(\mathbf{circ}_{mn}\right)(R) \;\approx\; \mathbf{circ}_n(R)$

Proof. Statement *(v)* of the Proposition states that $\Gamma^{mn}_{n}\Gamma^{n}_{mn} = \bar{\delta}^{m|\,mn}$. In particular, $\Gamma^{mn}_{n}\Gamma^{n}_{mn}(\mathbf{circ}_{mn}) = \bar{\delta}^{m|\,mn}(\mathbf{circ}_{mn})$. But, Γ^{n}_{mn} is onto $\mathbf{circ}_n$ by Statememt *(i)*. Therefore, $\Gamma^{mn}_{n}(\mathbf{circ}_n) = \bar{\delta}^{m|\,mn}(\mathbf{circ}_{mn})$. The isomorphism is just Corollary 3.5.2.2. □

3.5.7 **Extension of Γ^s_r to general r, s.**

For completeness, we point out that the definition of the Γ homomorphisms can be consistently extended to arbitrary circulant dimensions. The cancellation law, $\Gamma^t_s\Gamma^s_r = \Gamma^t_r$, which on commensurate dimensions, we showed is valid only when $r \,|\, s \,|\, t$, when $t \,|\, s \,|\, r$, or when $r = t \,|\, s$, can also be extended.

3.5.8 **Definition** For all integers $r, s > 0$, define $\tilde{\Gamma}^s_r : \Lambda_r \to \Lambda_s$ and $\Gamma^s_r : \mathbf{circ}_r(R) \to \mathbf{circ}_s(R)$ by

$$\tilde{\Gamma}^s_r(z)_i \;:=\; \delta^s_{ir}\, z_{ir/s}$$

$$\Gamma^s_r \;:=\; \lambda^{-(s)}\tilde{\Gamma}^s_r\lambda^{(r)}$$

3.5.9 **Proposition** For all integers $r, s > 0$,

(i) If $s \,|\, r$ then definition 3.5.8 agrees with definition 3.5.1*(i)*.

(ii) If $r \,|\, s$ then definition 3.5.8 agrees with definition 3.5.1*(ii)*.

(iii) $\Gamma^s_r(a) \;=\; \dfrac{d}{s}\displaystyle\sum_{i=0}^{s-1}\mathrm{u}^i_s \sum_{\substack{j\in\mathbb{Z}_r \\ j\equiv i \pmod d}} a_j \quad$ where $d = \gcd(r, s)$

(iv) $\Gamma^t_s\Gamma^s_r \;=\; \Gamma^t_r$ iff $\gcd(t, r) \,|\, \gcd(t, s)$. (Cancellation Law)

Proof. The proof is routine and is left to the interested reader. □

3.6 Cyclic Group Rings

Some of the homomorphisms on circulants and many of the properties of circulants can be described as special cases of properties of group rings.

A **group ring** over a ring R is formed from an arbitrary group, G, and an arbitrary (commutative with 1) ring, R, and is denoted by $R[G]$. It consists of all finite sums of formal products $r \cdot g$ where $r \in R$ and $g \in G$. The product in $R[G]$ is defined by $(r_1 \cdot g_1)(r_2 \cdot g_2) = (r_1 r_2) \cdot (g_1 g_2)$. We also make the identification $r1_G = r$. Right and left distributivity is assumed. It follows that two arbitrary elements of $R[G]$, $\sum_{g\in G} a_g g$ and $\sum_{g\in G} b_g g$ are equal iff $a_g = b_g,\ \forall g \in G$.

Here are some examples of group rings; all have some relevance to circulants.

(i) The circulant ring $\mathbf{circ}_N(R)$ is easily seen to be isomorphic to the group ring $R[C_{\mathrm{u}}]$ where C_{u} is the cyclic, multiplicative group on the set $\{1, \mathrm{u}, \mathrm{u}^2, \ldots, \mathrm{u}^{N-1}\}$. Hence,

$$\mathbf{circ}_N(R) \;\approx\; R[\mathbb{Z}_N]$$

(ii) Take $G = \langle x \rangle \approx \mathbb{Z}$. Then, $R[G]$ is the Laurent polynomial ring $R[x, x^{-1}]$.

(iii) Take $G = \mathbb{Q}/\mathbb{Z}$. G can be identified with the additive group of all fractions modulo 1. Let R be any commutative ring and define the ring

$$\mathbf{circ}_\infty(R) \;:=\; R[\mathbb{Q}/\mathbb{Z}]$$

Consider the following map from $\mathbf{circ}_n(R)$ to $\mathbf{circ}_\infty(R)$. $\Gamma_n^\infty : \mathrm{u}_n^m \mapsto \{m/n\}$. The domain of Γ_n^∞ is extended to all of $\mathbf{circ}_n(R)$ by requiring it to be R-linear. It easy to show that this map is a ring monomorphism. Therefore, $\mathbf{circ}_\infty(R)$ contains a copy of every circulant ring over R.

The reader might find it easier to visualize the embedding by regarding the group $\mathbb{Q}/\mathbb{Z}$ as the set of points $\{e^{2\pi\imath r} \;\vdash\; r \in \mathbb{Q}\}$ in the complex plane with complex multiplication as the group product. The embedding then becomes $\Gamma_n^\infty : \mathrm{u}_n^m \mapsto \exp(2\pi\imath m/n) = \zeta_n^m$. However, the formal product $r\zeta_n^m$ where $r \in R$ is not complex multiplication. In fact, changing the formal product to complex multiplication is a non-trivial ring homomorphism. Since $\mathbf{circ}_\infty$ contains a copy of every circulant space, we call it the **supercirculant algebra**. We will discuss it in detail in the next chapter.

3.6.1 **Definition** Let $Z = \{z^i : 0 \le i < N\}$ be a cyclic group of order N.

Define $\quad \Upsilon : \mathbf{circ}_N(R) \to R[Z]^N \quad$ by $\quad \Upsilon(a)_i \;:=\; \displaystyle\sum_{j \in \mathbb{Z}_N} a_j \cdot z^{ij}.$

3.6.2 **Proposition** With multiplication in $R[Z]^N$ taken componentwise, Υ is a ring monomorphism.

Proof. Let $a, b \in \mathbf{circ}_N(R)$.

$$\big(\Upsilon(a)\Upsilon(b)\big)_i \;=\; \Upsilon(a)_i\Upsilon(b)_i \;=\; \left(\sum_{j\in\mathbb{Z}_N} a_j \cdot z^{ij}\right)\left(\sum_{k\in\mathbb{Z}_N} b_k \cdot z^{ik}\right) \;=\; \sum_{l\in\mathbb{Z}_N} z^{il} \cdot \sum_{j\in\mathbb{Z}_N} a_j b_{l-j} \;=\; \Upsilon(ab)_i$$

This shows that the map is multiplicative if multiplication is taken componentwise in $R[Z]^N$. The map is obviously additive, so we need only show that it is a monomorphism.

$$\Upsilon(a) = 0 \;\text{ iff }\; \sum_{j\in\mathbb{Z}_N} a_j \cdot z^{ij} = 0,\ \forall i \;\Rightarrow\; \sum_{j\in\mathbb{Z}_N} a_j \cdot z^{j} = 0 \;\Rightarrow\; a_j = 0 \text{ since } Z \text{ is a basis for } R[Z] \;\square$$

3.6.3 **The Υ_c Homomorphisms**

The set $\{\Upsilon_c\}$ is a family of maps from $\mathbf{circ}_N(R) \to R_c^N$ where R is a commutative ring with identity, and c is an N^{th} root of unity in some ring R_c containing $R \cup \{c\}$. A specific Υ_c map is formed from the composition of Υ with the ring homomorphism $V_c : R[Z] \mapsto R_c$ where $V_c : z \mapsto c$. That is, $\Upsilon_c = V_c \circ \Upsilon$. Some examples will follow the next proposition,

3.6.4 **Proposition** Suppose R contains a primitve N^{th} root of unity, c. Then $\Upsilon_c : \mathbf{circ}_N(R) \to R^N$ is a ring monomorphism. If further N is a unit in R then Υ_c is an isomorphism.

Proof. $\Upsilon_c\left(\displaystyle\sum_{j\in\mathbb{Z}_N} a_j \mathrm{u}^j\right)_i \;=\; \sum_{j\in\mathbb{Z}_N} a_j c^{ij}$ where multiplication is the product in R. This homomorphism can be regarded as a vector space endomorphism on R^N given by the matrix $C : a \mapsto Ca^T$ where $C_{i,j} = c^{ij}$,

which is a multiple of the Fourier matrix over R. Since we are assuming throughout that the characteristic of R does not divide N, we see that C is non-singular iff $c^i \neq c^j$ when $i \neq j$. But, $c^N = 1$ is primitive and so $c^i - c^j$ is never zero for $i \not\equiv j \pmod N$. Since R is an integral domain, their product must also be non-zero. Therefore, Υ_c is a monomorphism.

The inverse of the matrix $C : a \mapsto Ca^T$ is $N^{-1}\bar{C}$ where $\bar{C}_{i,j} = c^{-ij}$. If N is unit in R then this matrix is a well-defined transformation on R^N, and so each element in R^N is in $\Upsilon_c(\mathbf{circ}_N(R))$. □

3.6.5 **Examples.**

(i) Take $c = \zeta$, a primitive N^{th} root of unity in $\mathbb{C}$ and take the product to be ordinary complex multiplication then $\Upsilon_\zeta : \mathbf{circ}_N(\mathbb{C}) \to \mathbb{C}^N$ is the eigenspace map, $\Upsilon_\zeta = \lambda^{(N)}$.

(ii) Take $c = \mathrm{u}$. Then $\Upsilon_{\mathrm{u}}(a)_i = \nu_i(a)$ where

$$\nu_i\left(\sum_j a_j \mathrm{u}^j\right) \;=\; \sum_j a_j \mathrm{u}^{ij}$$

(The map ν_{-1} was used in the proof of Proposition 3.5.4.) This family of maps are described in greater detail in §3.7 below.

(iii) Take $R \subset \mathbb{C}$, and let $c = \zeta\mathrm{u}$ where $\zeta = e^{2\pi\iota/N}$. Then, $(\Upsilon_c)_1 = \rho$, a circulant automorphism. The eigenspace version, $\tilde{\rho}$, is simply a rotation of the eigenvalues. Therefore, the map ρ leaves the circulant determinant invariant. If we allow $\tilde{\rho}$ to act on **circ** (which makes it only a vector space map) $\tilde{\rho}$ too leaves the absolute value of the circulant determinant invariant.

(iv) Let $q = tN + 1$ be prime, and let r be a primitive N^{th} root of unity in $\mathbb{Z}_q$. Then, by the proposition, $\Upsilon_r : \mathbf{circ}_N(\mathbb{Z}_q) \to \mathbb{Z}_q^N$ is a ring isomorphism.

(v) Let $N = \phi(p^n) = p^{n-1}(p-1)$, and let $R = \mathbb{Z}_q$ with $q = p^n m$ where p is prime and $p \nmid m$. Then, R contains a primitive N^{th} root of unity. Let c be any such root. Then, $\Upsilon_c : \mathbf{circ}_N(\mathbb{Z}_q) \to \mathbb{Z}_q^N$ is an isomorphism.

3.7 The Position Multiplier Maps.

The position multiplier maps are two overlapping sets of linear maps on vector spaces. The first set is $\nu\mathbb{Z}_N = \{\nu_h \vdash h \in \mathbb{Z}_N\}$ where each ν_h is defined as in §3.6.3 but will be defined again for ease of reference. The second set is $\bar{\nu}\mathbb{Z}_N = \{\bar{\nu}_h \vdash h \in \mathbb{Z}_N\}$ which is defined below.

3.7.1 **Definition** We define two functions, $\nu, \bar{\nu}$ which map $\mathbb{Z}_N$ to rearrangements of the components of N-dimensional vectors. Let R be an integral domain with a field of quotients, Q. We regard $R^N \subset Q^N$. For all $h \in \mathbb{Z}_N$, and for all $x \in R^N$ define

(i) $\nu_{h,N}(x) \;:=\; \nu_h(x) \;:=\; \Upsilon_{\mathrm{u}}(x)_h \;=\; \displaystyle\sum_{i\in\mathbb{Z}_N} x_i \mathrm{u}^{ih}.$

(ii) $\bar{\nu}_{h,N}(x) \;:=\; \bar{\nu}_h(x) \;:=\; \displaystyle\sum_{i\in\mathbb{Z}_N} x_{hi} \mathrm{u}^{i}.$

As usual, we will omit N when there is no danger of ambiguity.

In these definitions, the terms u^i can be regarded as the usual unit vector basis for Q^N provided i is taken modulo N (though we will usually regard u^i as the i^{th} power of the circulant $\mathrm{u} = \mathrm{u}_N$).

It is immediate from the definitions, that ν and $\bar{\nu}$ are both semigroup homomorphisms. That is, $\nu_h\nu_g = \nu_{hg}$ and $\bar{\nu}_h\bar{\nu}_g = \bar{\nu}_{hg}$.

We shall first consider the set $\nu\mathbb{Z}_N$ acting on $a \in \mathbf{circ}_N(R)$. Since Υ_{u} is a ring homomorphism, so is its h^{th} component. Therefore, ν_h is a ring homomorphism on circulants. When h is coprime to N, ν_h is a permutation and since every permutation is invertible, ν_h is a ring automorphism. Contrariwise, suppose h is not coprime to N with $\gcd(h, N) = d > 1$. Then, the only basis terms appearing in $\nu_h(a)$ would be

powers of u^d. Hence, the rank of ν_h would be at most N/d. This shows that ν_h is an isomorphism iff h is coprime to N. This can also be seen from the fact that $\nu_g\nu_h = \nu_{gh}$. Since if h is a divisor of zero, then there exists g with $gh = 0$, and $\nu_g\nu_h = \nu_0$ which is obviously of rank 1; whereas if $\gcd(h, N) = 1$, then there exists $g \in \mathbb{Z}_N$ s.t. $gh = 1$ and hence $\nu_g\nu_h = \nu_{gh} = \nu_1 = 1$. This same argument applied to $\bar{\nu}$ also serves to proves that $\bar{\nu}_h$ is non- singular iff h, N are coprime.

The $\bar{\nu}\mathbb{Z}_N$ maps acting on the space $\mathbf{circ}_N(R)$ are not in general ring homomorphisms. To see this, let $h \in \mathbb{Z}_n - \mathbb{Z}_N^*$ with $\gcd(h, N) = d > 1$, say. Suppose for a contradiction that $\bar{\nu}$ were a multiplicative map on $\mathbf{circ}_N(R)$. But, from the definition, $\bar{\nu}(\mathrm{u}^i) = 0$ unless $d \mid i$. In particular, $\bar{\nu}_h(\mathrm{u}) = 0$. Hence, $\bar{\nu}_h$ is the zero map. Contradiction.

On the other hand, $\bar{\nu}\mathbb{Z}_N^*$ are ring homomorphisms. Suppose $h \in \mathbb{Z}_N^*$. Let $a \in \mathbf{circ}_N(R)$. In terms of the standard basis for $\mathbf{circ}_N$, $\bar{\nu}_h(a)$ is given by

$$\bar{\nu}_h(a) \;=\; \sum_{i=0}^{N-1} a_{ig}\mathrm{u}^i \;=\; \sum_{i=0}^{N-1} a_i \mathrm{u}^{h^{-1}i} \;=\; \nu^{h^{-1}}(a) \;=\; \nu_h^{-1}(a)$$

Therefore, $\bar{\nu}_h = \nu_h^{-1}$, and $\nu\mathbb{Z}_N \cap \bar{\nu}\mathbb{Z}_N$ contains all the invertible maps in $\nu\mathbb{Z}_N \cup \bar{\nu}\mathbb{Z}_N$. Hence,

3.7.2 **Proposition** The non-singular maps in $\nu\mathbb{Z}_N \cup \bar{\nu}\mathbb{Z}_N$ are $\nu\mathbb{Z}_N \cap \bar{\nu}\mathbb{Z}_N \;=\; \nu(\mathbb{Z}_N^*) \;=\; \bar{\nu}(\mathbb{Z}^*)$. □

3.7.3 **The Position Multiplier Map on the Eigenspace.** The induced map on the eigenspace, namely, $\tilde{\nu}_h = \lambda\nu_h\lambda^{-1}$ is as usual extended by linearity to a map on Λ_N and is given by

$$(\lambda\nu_h(a))_i \;=\; \sum_{k\in\mathbb{Z}_N} a_k\zeta^{ihk} \;=\; \lambda_{ih}(a) \;=\; (\bar{\nu}_h\lambda(a))_i$$

$$\therefore\;\; \tilde{\nu}_h \;=\; \bar{\nu}_h$$

Therefore, the map $\bar{\nu}_h$ in $\bar{\nu}\mathbb{Z}_N$ is the eigenspace version of the endomorphism $\nu_h \in \nu\mathbb{Z}_N$, and so $\bar{\nu}_h$ is a ring endomorphism on Λ_N with componentwise multiplication, and is an automorphism iff $h \in \mathbb{Z}_N^*$. But, this means that $\tilde{\nu}_h$ is defined on circulants when $\gcd(h, N) = 1$, which in turn implies that $\tilde{\tilde{\nu}}$ is well-defined. Indeed, we can calculate it using Corollary 3.5.5. $\lambda\bar{\nu}_h\lambda^{-1} = \lambda^2\nu_h\lambda^{-2} = n\nu_{-1}\nu_h\nu_{-1}n^{-1} = \nu_h$. $\therefore\;\; \tilde{\tilde{\nu}}_h \;=\; \nu_h$.

In particular, we see that eigenvalues of $\nu_h(a)$ are a rearrangement of the eigenvalues of a. Hence, the determinant is invariant under the non-singular ν homomorphisms.

$$\Delta_N(\nu_h(a)) \;=\; \Delta_N(a) \qquad \text{(provided } h \text{ is coprime to } N)$$

3.7.4 **Connections with the Γ maps.**

Let ϵ^h be the map $x \mapsto x^h$ as in §3.5.3. Then, $\epsilon^h(\ker\Gamma^N) = (x^{hN} - 1) \subset \ker\Gamma^N$. The map ϵ^h is a ring homomorphism on $R[x]$. Therefore, the following diagram is commutative.

$$\begin{array}{ccc} & \overset{\epsilon^h}{} & \\ R[x] & \longrightarrow & R[x] \\ \Gamma^N\big\downarrow & & \big\downarrow\Gamma^N \\ \mathbf{circ}_N(R) & \underset{\nu_h}{\longrightarrow} & \mathbf{circ}_N(R) \end{array}$$

Using this fact, we can derive a general formula for ν_h in terms of the Γ homomorphisms. By Proposition 3.5.3,

$$\tilde{\Gamma}_n^{mn}\Gamma^n \;=\; \Gamma^{mn}\epsilon^m$$

Multiplying throughout by Γ_{mn}^n, we get

$$\Gamma^n_{mn}\tilde{\Gamma}^{mn}_n\Gamma^n \;=\; \Gamma^n_{mn}\Gamma^{mn}\epsilon^m \;=\; \Gamma^n\epsilon^m \;=\; \nu_m\Gamma^n$$

$$\therefore\;\; \nu_m \;=\; \nu_{m,n} \;=\; \Gamma^n_{mn}\tilde{\Gamma}^{mn}_n$$

In this equation, ν_m acts on $\mathbf{circ}_n$ and so m is an arbitrary residue in $\mathbb{Z}_n$.

There is an another formula for ν_h which holds only when h divides the order of the circulant space. Consider $\tilde{\Gamma}^{mn}_n\Gamma^n_{mn}(a)$.

$$\tilde{\Gamma}^{mn}_n\Gamma^n_{mn}(a) \;=\; \tilde{\Gamma}^{mn}_n\sum_{i=0}^{mn-1} a_i\mathrm{u}^i_n \;=\; \sum_{i=0}^{mn-1} a_i\mathrm{u}^{im}_{mn} \;=\; \nu_m(a)$$

$$\therefore\;\; \nu_m \;=\; \nu_{m,mn} \;=\; \tilde{\Gamma}^{mn}_n\Gamma^n_{mn}$$

This equation gives an expression for ν_m acting on $\mathbf{circ}_{mn}$, and so applies only when m divides the dimension of the domain.

3·7·5 Commutation with Γ Maps.

The commutation relation with Γ^n_{mn} can also be found using the ϵ map.

$$\nu_h\Gamma^n_{mn}\Gamma^{mn} \;=\; \nu_h\Gamma_n \;=\; \Gamma_n\epsilon^h \;=\; \Gamma^n_{mn}\Gamma^{mn}\epsilon^h \;=\; \Gamma^n_{mn}\nu_h\Gamma^{mn}$$

Since Γ^{mn} is onto, this shows that ν_h and Γ^n_{mn} commute.

The maps ν_h and $\tilde{\Gamma}^{mn}_n$ also commute. By Proposition 3·5·3,

$$\nu_h\tilde{\Gamma}^{mn}_n\Gamma^n \;=\; \nu_h\Gamma^{mn}\epsilon^m \;=\; \Gamma^{mn}\epsilon^{h+m} \;=\; \tilde{\Gamma}^{mn}_n\Gamma^n\epsilon^h \;=\; \tilde{\Gamma}^{mn}_n\nu_h\Gamma^n$$

$$\therefore\;\; \nu_h\tilde{\Gamma}^{mn}_n \;=\; \tilde{\Gamma}^{mn}_n\nu_h$$

By conjugating this with λ^{-1}, we see that $\bar{\nu}_h$ and Γ^{mn}_n commute. Therefore, ν_g and Γ^{mn}_n commute for all $g\in\mathbb{Z}^*_{mn}$. However, ν_h and Γ^{mn}_n do not commute in general. This is easiest to see in the eigenspace versions.

$$\Big(\bar{\nu}_h\tilde{\Gamma}^{mn}_n(z)\Big)_i \;=\; \big(\bar{\nu}_h(\delta^m_j z_{j/m})_j\big)_i \;=\; \big((\delta^m_{hj}\, z_{hj/m})_j\big)_i \;=\; \delta^m_{hi}\, z_{hi/m}$$

$$\Big(\tilde{\Gamma}^{mn}_n\bar{\nu}_h(z)\Big)_i \;=\; \Big(\tilde{\Gamma}^{mn}_n(z_{hj})_j\Big)_i \;=\; \delta^m_i\,((z_{hj})_j)_{i/m} \;=\; \delta^m_i z_{hi/m}$$

Hence, $\bar{\nu}_h\tilde{\Gamma}^{mn}_n = \tilde{\Gamma}^{mn}_n\bar{\nu}_h$ iff h is coprime to m iff ν_h and Γ^{mn}_n commute.

We shall summarize the above for easy reference.

3·7·6 Proposition The following identities have been demonstrated. In these statements, m, n, h are arbitrary, positive integers.

(i) $\tilde{\nu}_h \;=\; \bar{\nu}_h, \quad \tilde{\bar{\nu}}_h = \nu_h$

(ii) If g is coprime to N, then $\bar{\nu}_g = \nu_g^{-1}$

(iii) $\nu_{hg} = \nu_h\nu_g, \quad \bar{\nu}_{hg} = \bar{\nu}_h\nu_g, \;\; \forall g, h \in \mathbb{Z}_N.$

(iv) $\Gamma^n_{mn}\nu_h \;=\; \nu_h\Gamma^n_{mn}$

(v) $\tilde{\Gamma}^{mn}_n\nu_h \;=\; \nu_h\tilde{\Gamma}^{mn}_n$

(vi) $\Gamma^{mn}_n\nu_g \;=\; \nu_g\Gamma^{mn}_n$ provided g is coprime to m.

(vii) $\nu_{m,n} \;=\; \Gamma^n_{mn}\tilde{\Gamma}^{mn}_n, \quad m\in\mathbb{Z}_n$

(viii) $\nu_{m,mn} \;=\; \tilde{\Gamma}^{mn}_n\Gamma^n_{mn}$