CIRCULANTS (Extract)

Alun Wyn-jones

Last revised in December 2013.

Chapter 5.
Two Circulant Subalgebras.

There are many subrings of $\mathrm{CIRC}_N(R)$, for instance, the subring whereby any set of eigenvalues are in a subring of $R(\zeta)$, another is the subring $\mathrm{CIRC}_N(S)$ where S is any subring of R, etc. Examples of subalgebras are: the subalgebra whereby any fixed subset of eigenvalues is zero, the subalgebra whereby any fixed set of eigenvalues are equal, the image under Γ^N of any subalgebra of $R[x]$ which includes $(x^N - 1)$, etc.

However, in this chapter only two, very specific, subalgebras are considered. The first will be important later in discussions of circulant ring structure. The second has some historical interest, but is mainly included because it serves as a nice introduction to the next chapter on tensor products. The two subalgebras share a common feature: they are defined by equality conditions between components of the circulant vectors. The two subalgebras also share the property that their eigenspaces satisfy the same type of condition as their circulant vectors.

5.1 Residue Class Circulants.

The residue class circulants are important in discussions of the set of rational circulants, **circ**$(\mathbb{Q})$. Indeed, as will be shown, a rational circulant has rational eigenvalues if and only if it is residue class.

5.1.1 **Definition** Let $(a_0, a_1, \ldots)$ be a sequence of objects. If $\exists N$ s.t. $\forall i,\ a_i = a_d$ where $d = \gcd(i, N)$, then a shall be said to be a **residue class sequence modulo** N. If the number of terms in the sequence is N and the a_i's belong to a ring, then a is said to be a **residue class vector modulo** N. When N is understood, we shall often just say **residue class vector**. If a circulant is a residue class vector, then it is said to be a **residue class circulant**.

Examples The following are residue class vectors. The values of x, y, z, w are arbitrary in all cases.

(a) $(w, y, x, y, x, z, x, y, x, y)$, $N = 10$.

(b) $(z, v, w, x, w, v, y, v, w, x, w, v)$, $N = 12$.

(c) $(x, y, y, \ldots, y)$, any N.

(d) All linear combinations of $\bar{\delta}^d$, $\sum_{d|\,N} c_d \bar{\delta}^d$ where $c_d \in R$.

(e) Let $u = u_0, u_1, \ldots, u_{N-1}$ be a sequence of residues modulo N. Define $c(u)$ † to be the coefficient of the monomial $a_{u_0} a_{u_1} a_{u_2} \cdots a_{u_{N-1}}$ in the algebraic expansion of $\det \mathrm{CIRC}_N(a)$. For any residue $h \in \mathbb{Z}_N$, define hu to be the sequence $(hu_0, hu_1, hu_2, \ldots, hu_{N-1})$. It can be shown that $c(v) = c(hv)$ whenever $h \in \mathbb{Z}_N^*$. Hence, $\big(c(0),\ c(u),\ c(2u),\ \ldots,\ c(hu),\ \ldots,\ c\left((N-1)u\right)\big)$ is a residue class vector.

(f) Let $(z_0, z_1, \ldots, z_{N-1})$ be any N-tuple in an R-module. Define the N-tuple z^+ by $z_i^+ = \sum\{z_{hi} \vdash h \in \mathbb{Z}_N^*\}$. Since $\mathbb{Z}_N^*$ is a group, z_i^+ is the sum of all components of z having subscripts in the same orbit as i under the multiplicative action of the group $\mathbb{Z}_N^*$. All elements in the same orbit have the same residue modulo N, hence we see that z^+ is residue class.

Notice that $z^+ = \sum_{\gcd(h,N)=1} \bar{\nu}_h(z)$ where $\bar{\nu}$ is the reverse position multiplier map defined in §3.7.1. Similarly, if R is a ring, we can define $z^* = \prod_{\gcd(h,N)=1} \bar{\nu}_h(z)$ and z^* too is residue class. Even if z is a circulant, and we take convolution as the product, then z^* is again residue class, though this is not so obvious; the next proposition assures us that this is so.

5.1.2 **Proposition** Let $a = (a_0, a_1, \ldots, a_{N-1})$, and $\lambda = \lambda(a)$. Then a is a residue class circulant iff λ is a residue class vector.

Proof. $(\Rightarrow:)$ We have $\lambda_j = \displaystyle\sum_{i \in \mathbb{Z}_N} a_i \zeta^{ij}$ where a is residue class.

Let $\gcd(j, N) = d$. Then $j = rd$ where r is some residue coprime to N.

† $c(u)$ is called the circulant determinantal coefficient.

$$\therefore\ \lambda_j \;=\; \sum_{i\in\mathbb{Z}_N} a_i\zeta^{ird} \;=\; \sum_{i\in\mathbb{Z}_N} a_{i\bar{r}}\zeta^{id} \quad \text{where } \bar{r}r \equiv 1 \pmod N$$

Since $\bar{r}$ is coprime to N, $\gcd(i\bar{r}, N) = \gcd(i, N)$. $\therefore\ a_{i\bar{r}} = a_i$.

$$\therefore\ \lambda_j \;=\; \sum_{i\in\mathbb{Z}_N} a_i\zeta^{id} \;=\; \lambda_d \quad \text{QED}(\Rightarrow:)$$

The proof of the converse is very similar. □

5.1.3 **Corollary** The residue class circulants form a subalgebra of the circulants.

Proof. Closure under addition and scalar multiplication is obvious. Closure under convolution follows from the obvious closure of $\lambda(\mathbf{circ})$ under componentwise multiplication. □

5.1.4 **Corollary** Let F be a field. A circulant $a \in \mathbf{circ}_n(F)$ is residue class iff $a = \sum_{d|\,n} c_d\, \bar{\delta}^{d*}$ where $c_d \in F$.

Proof. The eigenspace idempotents are obviously residue class, so it is clear that the sum in the statement must also be residue class. Conversely, given a vector of eigenvalues, μ

$$\mu \;=\; \sum_{d|\,n} \delta^{d*}(\mu)$$

If μ is residue class, then $\mu_i = \mu_d$ for all $i \in (d)^*$. In other words, $\delta^{d*}(\mu) = \mu_d\delta^{d*}$. Therefore,

$$\mu \;=\; \sum_{d|\,n} \delta^{d*}(\mu) \;=\; \sum_{d|\,n} \mu_d\delta^{d*}$$

Applying the inverse λ map we obtain the desired conclusion. □

The most important property of residue class circulant matrices is that the circulants are rational iff the eigenvalues are rational. The converse also holds: If both circulants and eigenvalues are rational then the circulant or eigenvalue vectors (and therefore both) are residue class.

5.1.5 **Proposition**
(i) If $\lambda(a) \in \mathbb{Q}^N$ then $a \in \mathbf{circ}_N(\mathbb{Q})$ iff a is residue class.
(ii) If $a \in \mathbf{circ}_N(\mathbb{Z})$ then $\lambda(a) \in \mathbb{Z}^N$ iff a is residue class.

Proof. We shall only prove the second statement the proof for the first is just a simple variation.

Assume that $a \in \mathbf{circ}(\mathbb{Z})$ and is residue class. The Galois group for $\mathbb{Q}(\zeta)/\mathbb{Q}$ is $\{\zeta \mapsto \zeta^i \vdash \gcd(i, N) = 1\}$. The automorphism generated by $\zeta \mapsto \zeta^i$ for $i \in \mathbb{Z}_N^*$ is a permutation on the set of roots of unity, and the orbits of the permutation are the residue classes of powers of ζ. Therefore, since a is residue class, $\zeta \mapsto \zeta^i : \lambda_j(a) \mapsto \lambda_j(a)$. Hence, $\lambda_j(a)$ is invariant under the Galois group and so is in $\mathbb{Q}$. But $\lambda_j \in \mathbb{Z}(\zeta)$. $\therefore\ \lambda_j \in \mathbb{Z}(\zeta) \cap \mathbb{Q} = \mathbb{Z}$.

Now suppose $\lambda(a) \in \mathbb{Z}^N$. Then, each λ_j is invariant under the Galois group. $\therefore\ \lambda_j = \lambda_{ij},\ \forall i \in \mathbb{Z}_N^*$. So, λ is residue class. Therefore, a is residue class by Proposition 5.1.2. □

If $\lambda(a) \in \mathbb{Z}^N$ and is residue class, then the same argument shows that $a \in \mathbf{circ}_N(\mathbb{Q})$, but $a \notin \mathbf{circ}_N(\mathbb{Z})$ in general because of the $1/N$ factor in the inverse Fourier transform, λ^{-1}.

5.1.6 **Eigenvalues of Residue Class Circulants. Ramanujan Sums**

The distinct terms of a residue class vector consists of at most the set $\{a_d \vdash d \mid N\}$. Therefore, the eigenvalues of circulant vectors can depend only on this set.

$$\begin{aligned}
\lambda_i &= \sum_{j\in\mathbb{Z}_N} a_j \zeta^{ij} &= \sum_{d\mid N} a_d \sum_{\{j\,\vdash\,\gcd(j,N)=d\}} \zeta_N^{ij} &= \sum_{d\mid N} a_d \sum_{\{k\,\vdash\,\gcd(k,N)=1\}} \zeta_{N/d}^{ik} \\
a_i &= \frac{1}{N}\sum_{j\in\mathbb{Z}_N} \lambda_j \zeta^{-ij} &= \frac{1}{N}\sum_{d\mid N} \lambda_d \sum_{\{j\,\vdash\,\gcd(j,N)=d\}} \zeta_N^{-ij} &= \frac{1}{N}\sum_{d\mid N} \lambda_d \sum_{\{k\,\vdash\,\gcd(k,N)=1\}} \zeta_{N/d}^{-ik}
\end{aligned}$$

Taking the eigenvalue equation as typical of the two,

$$\lambda_i \;=\; \sum_{n\mid N} a_{N/n} \sum_{j\in\mathbb{Z}_n^*} \zeta_n^{ij} \;=\; \sum_{n\mid N} a_{N/n} r_n(i) \quad \text{where } r_n(i) = \sum_{j\in\mathbb{Z}_n^*} \zeta_n^{ij} \tag{1}$$

In evaluating the functions $r_n(i)$, bear in mind that $\mathbb{Z}_1^* = \{0\}$ and not $\emptyset$. That is, $0 = 1$ in $\mathbb{Z}_1$.

The function $r_n(i\,)$ is a Ramanujan sum. It takes values in $\mathbb{Z}$, and is a multiplicative arithmetic function in its subscript. There is a closed expression for it in terms of the Möbius and Euler functions given in part *(iii)* below.

5.1.7 **Theorem**

(i) If n_1 and n_2 are coprime then $r_{n_1 n_2}(m) = r_{n_1}(m) r_{n_2}(m)\,.$

(ii) $r_n(m) \;=\; \displaystyle\sum_{d\mid\gcd(m,n)} \mu\left(\frac{n}{d}\right) d\,.$

(iii) $r_n(m) \;=\; \mu(h)\,\dfrac{\phi(n)}{\phi(h)} \quad \text{where } h = \dfrac{n}{\gcd(m,n)}$ □

Proof. See Hardy & Wright [HaW1]. □

We recapitulate these results on the eigenvalues of the residue class vectors.

5.1.8 Theorem Let $r_n(m) = \displaystyle\sum_{i\in\mathbb{Z}_M^*} \zeta_n^{im}$. If a is a residue class vector with eigenvalues λ_i, then

$$\lambda_i \;=\; \sum_{n\mid N} a_{N/n} r_n(i) \tag{2}$$

$$a_i \;=\; \frac{1}{N}\sum_{n\mid N} \lambda_{N/n} r_n(i) \tag{3}$$

Proof. This was already proved. We reversed the sign of i in the formula for a_i. This is allowed since $r_n(-i) = r_n(i)$. □

Formulæ (2) and (3) can be made symmetric by the scale change: $a' = a_i/\sqrt{N}$, and $\lambda_i' = \lambda_i/\sqrt{N}$.

We shall give two applications of this development. First we shall prove a theorem on Ramanujan sums.

5.1.9 Theorem Let $r_n(i) = \sum_{j\in\mathbb{Z}_n^*} e^{2\pi\iota ij/n}$ be Ramanujan's sum. Take all the divisors of n in some order $D = (h_1, h_2, \ldots, h_{d(n)})$, say, and define a $d(n)\times d(n)$ matrix R by

$$R_{i,j} \;=\; \frac{1}{\sqrt{n}}\left(r_{n/i}(j)\right)_{i,j\in D}$$

$$\text{Then,} \quad R^2 = I$$

Proof. We use formula (2) to substitute for the term $\lambda_{N/n}$ in formula (3) to obtain an expression for a_i in terms of the vector a.

$$a_i \;=\; \frac{1}{N}\sum_{n|\,N}\left(\sum_{d|\,N} a_{N/d}r_d(N/n)\right) r_n(i) \;=\; \frac{1}{N}\sum_{d|\,N} a_d \sum_{n|\,N} r_{N/d}(N/n)r_n(i)$$

Only the set $\{a_h \vdash h \mid N\}$ are independent so we restrict $i = h \mid N$. Then, we can identify terms on both sides of the equation and we get

$$\sum_{n|\,N} r_{N/d}(N/n)r_n(h) \;=\; N\delta_{h-d}$$

We change variables, $d \to i$, $N/n \to k$, and $h \to j$ giving

$$\sum_{k|\,N} r_{N/i}(k)r_{N/k}(j) \;=\; N\delta_{j-i} \;\; \square$$

The theorem implies an inversion formula: for all $f, g : \mathbb{Z} \to \mathbb{C}$,

$$\text{If} \quad f(d) \;=\; \sum_{h|\,n} r_{n/d}(h)g(h)\,,$$

$$\text{then} \quad g(d) \;=\; \frac{1}{n}\sum_{h|\,n} r_{n/d}(h)f(h)\,.$$

Theorem 5.1.7 suggests that this inversion formula is related somehow to the Möbius Inversion Formula. However, the Möbius Inversion Formula holds only for arithmetic functions whereas the above inversion holds for general, complex-valued functions. Indeed there seems no way to deduce the Möbius formula from the above.

5.1.10 Application to Arithmetic Partitions

Let $P(n,p,m)$ be the number of partitions of n into p distinct, positive parts less than m without regard to order. For example, $P(9,3,6) = 2$ because all the allowable partitions are given by:

$$9 \;=\; 1+3+5 \;=\; 2+3+4$$

One can easily check that the generating function for $P(n,p,m)$ is given by:

$$(1+xy)(1+xy^2)(1+xy^3)\cdots\left(1+xy^{m-1}\right) \;=\; \sum_{n,p\geq 0} x^p y^n P(n,p,m) \tag{4}$$

5.1.11 **Lemma** Let A be any set of $m-1$ elements. There is a bijective correspondence between the subsets of A and the partitions into distinct, positive parts less than m.

Proof. W.l.o.g. let $A = \{1, 2, \ldots, m-1\}$. Given any $B \subset A$, $\sum B$ represents an allowable partition, and vice versa. $\square$

It follows that $\sum_n P(n,p,m) \;=\; \binom{m-1}{p}$.

We now introduce a slight variation on P.

5.1.12 **Definition** For all $n \in \mathbb{Z}_m$, define

(i) $\bar{P}(n,p,m) \; := \sum_{z \equiv n \pmod{m}} P(z,p,m),$ and

(ii) $\bar{P}_{n,m}(x) \; := \sum_{p=0}^{m-1} \bar{P}(n,p,m)x^p.$

Applying Lemma 5.1.11 to the first definition above,

$$\sum_{n \in \mathbb{Z}_m} \bar{P}(n,p,m) \;=\; \binom{m-1}{p}$$

and now applying this to the second definition, we get

$$\sum_{n \in \mathbb{Z}_m} \bar{P}_{n,m}(x) \;=\; \sum_{p=0}^{m-1} \binom{m-1}{p} x^p \;=\; (1+x)^{m-1} \tag{5}$$

Equation (5) leads us to investigate whether there are other formulæ of this kind.

Define $\nu_{*m} : \mathbf{circ}_m(R) \to \mathbf{circ}_m(R)$ by $\nu_{*m}(a) = \prod_{i=1}^{m-1} \nu_i(a)$ where ν_i is the position multiplier map of 3.7. This is very similar to the map, ν_*, briefly described in example *(f)* at the beginning of the chapter, and indeed is the same map when m is prime. As with ν_*, ν_{*m} maps general circulants to residue class circulants. We have,

$$\nu_{*m}(1 + x\mathrm{u}) \;=\; (1+x\mathrm{u})(1+x\mathrm{u}^2)(1+x\mathrm{u}^3)\cdots\left(1+x\mathrm{u}^{m-1}\right) \tag{6}$$

Comparing equations (4) and (6) we see that

$$\nu_{*m}(1+x\mathrm{u}) \;=\; \sum_{p,z=0}^{m-1} \bar{P}(z,p,m)x^p\mathrm{u}^z \;=\; \sum_{z=0}^{m-1} \bar{P}_{z,m}(x)\mathrm{u}^z$$

From this simple derivation, and recalling that $\nu_{*m}(1+x\mathrm{u})$ is residue class, we get the rather startling conclusion that

$$\begin{aligned} \gcd(y,m) = \gcd(z,m) \;\Rightarrow\quad & \bar{P}_{z,m}(x) \;=\; \bar{P}_{y,m}(x) \\ \Rightarrow\quad & \bar{P}(y,p,m) \;=\; \bar{P}(z,p,m) \qquad \text{for } p = 0,1,\ldots,m-1 \end{aligned} \tag{7}$$

5.1.13 **Theorem** Let $r_n(i)$ be Ramanujan's sum, and let $\bar{P}_{n,m}(x)$ be the partition function defined above in §5.1.12. Then, for all $d \,|\, m$, and for all i with $\gcd(i,n) = d$, we have

$$\sum_{t|\,m} r_{m/t}(d)\bar{P}_{t,m}(x) \quad=\quad \frac{\left(1-(-x)^{m/d}\right)^d}{1+x}\,, \quad \text{and} \tag{8a}$$

$$\bar{P}_{i,m}(x) \quad=\quad \bar{P}_{d,m}(x) \quad=\quad \frac{1}{m(1+x)} \sum_{t|\,m} r_{m/t}(d)\left(1-(-x)^{m/t}\right)^t \tag{8b}$$

Proof. To derive the first formula, we compute $\lambda_d \nu_{*m}(1+x\mathrm{u})$ in two ways.

On the one hand, by the definitions of $P(n,p,m)$ and $\bar{P}_{n,m}(x)$,

$$\nu_{*m}(1+x\mathrm{u}) \quad=\quad \sum_{i=0}^{m-1} \bar{P}_{i,m}(x)\mathrm{u}_m$$

and this is a residue class circulant, and so according to Theorem 5.1.8, we have

$$\lambda_d \nu_{*m}(1 + x\mathrm{u}) \quad = \quad \sum_{t|\,m} r_{m/t}(d) \bar{P}_{t,m}(x)$$

On the other hand, letting $\zeta = \zeta_m$, we have

$$\lambda_d \nu_{*m}(1 + x\mathrm{u}) \; = \; \prod_{i=1}^{m-1} \left(1 + x\zeta^{id}\right) \; = \; (1+x)^{-1} \prod_{i=0}^{m/d-1} \left(1 + x\zeta^{i}_{m/d}\right)^{d} \tag{9}$$

Consider the general formula, $F_n(x) = \prod_{i=0}^{n-1} \left(1 + x\zeta_n^i\right)$. Dividing each i^{th} factor in the product by $-\zeta_n^i$, we get,

$$F_n(x) \; = \; (-1)^n \prod_{i=0}^{n} \zeta^i \prod_{i=1}^{n-1} \left(-x - \zeta^{-i}\right) \; = \; (-1)^{n-1}(-1)^n \prod_{i=0}^{n-1} \left((-x) - \zeta^i\right) \; = \; -\prod_{i=0}^{n-1} \left((-x) - \zeta^i\right)$$

Hence, $-F(-x)$ is a monic polynomial of degree n having all n n^{th} roots of unity as its roots. It follows that $-F(-x) = x^n - 1$. Applying this to formula (9),

$$\lambda_d \nu_{*m}(1 + x\mathrm{u}) \quad = \quad \frac{\left(1 - (-x)^{m/d}\right)^{d}}{1 + x}$$

Formula (8b) for $P_{d,m}(x)$ follows from the (8a) by Theorem 5.1.9, and the equation $\bar{P}_{i,m}(x) = \bar{P}_{d,m}(x)$ is just equation (7). □

5.1.14 **Example** Take the simplest case, $m = q$ an odd prime. We have,

$$q\bar{P}_{n,q}(x) \quad = \quad \begin{cases} (1+x)^{q-1} \; + \; (q-1)\left(1 - x + x^2 - \cdots + (-x)^{q-1}\right) \; , & n = 0 \\ (1+x)^{q-1} \; - \; \left(1 - x + x^2 - \cdots + (-x)^{q-1}\right) \; , & \text{otherwise} \end{cases} \qquad \square$$

Summing the above formula for $q\bar{P}_{n,q}(x)$ over $n = 0, 1, 2, \ldots, q-1$ gives $q(1+x)^{q-1}$ which is equivalent to formula (5).

Applying formula (5) to the general formula (8b) of Theorem 5.1.13, we get a pure polynomial formula,

$$m(1+x)^m \quad = \quad \sum_{t|\,m} \left(1 \; - \; (-x)^{m/t}\right)^{t} \sum_{d|\,m} \phi\left(\frac{m}{d}\right) r_{m/t}(d) \tag{10}$$

from which we can derive several relationships between the Euler and Ramanujan functions. For example, identifying constant terms we get

$$m \; = \; \sum_{\substack{d|\,m \\ t|\,m}} \phi\left(\frac{m}{d}\right) r_{m/t}(d) \; = \; \sum_{d|\,m} \phi\left(\frac{m}{d}\right) \sum_{t|\,m} r_t(d)$$

However, this formula is a trivial consequence of $\sum_{t|\,m} r_t(d) = m\delta_d^m$. Identifying the linear terms in (10), we get the well-known

$$m \; = \; \sum_{d|\,m} \phi\left(\frac{m}{d}\right) .$$

When m is odd, the second-order terms in (10) yields the above formula again, but when m is even an extra term appears which must be zero giving

$$\sum_{d|\,m} \phi\left(\frac{m}{d}\right) r_2(d) \; = \; 0 \qquad \text{(for } m \text{ even)}$$

and so on...

5.2 Subrepeating Circulant Matrices.

In the previous section we saw that the residue class circulant matrices form a subalgebra. This was an easy consequence of the fact that their eigenvalues too are residue class. Subrepeating circulant matrices share this property of having the same pattern in both the circulant vectors and their eigenvalues.

5.2.1 Definition

(i) Let $N = nm$. A vector $a = (a_0, a_1, \ldots, a_{N-1})$ is said to be a **subrepeating sequence** of period m if $i \equiv j \not\equiv 0 \pmod{m} \;\Rightarrow\; a_i = a_j$. Hence, a has the form

$$a = (a_0, a_1, \ldots, a_{m-1},\ a_m, a_1, a_2, \ldots, a_{m-1},\ a_{2m}, a_1, a_2, \ldots, a_{m-1}, \ldots, a_{(n-1)m}, a_1, a_2, \ldots, a_{m-1})$$

The sequence is almost periodic, and would be periodic if $a_0 = a_m = \cdots = a_{rm} = \cdots = a_{(n-1)m}$.

Let $A = \mathrm{CIRC}_N(a)$. Notice that if the sequence a is periodic $(i.e$ if $a_0 = \cdots = a_{(n-1)m}.)$ that every m^{th} row of A would be same, and the rank of A would be at most m. Hence, the arbitrariness of the subsequence $(a_0, a_m, a_{2m}, \ldots, a_{N-m})$ is essential for non-singularity.

(ii) If $A = \mathrm{CIRC}_N(a)$ and a is a subrepeating sequence with period $m \mid N$, then A is said to be a **subrepeating circulant matrix** of period m.

5.2.2 Definition

Let QR^m_{mn} denote the set of subrepeating circulants of order mn and of period m over a commutative ring R.

One of the important properties of a subrepeating circulant matrix is that it partitions into an $n \times n$ circulant matrix with entries in the commutative ring CIRC_m of $m \times m$ circulant matrices. This partitioning is most easily seen with an illustration (see Figure 5.2.2.1).

The definition of subrepeating is not only enough to guarantee this partitioning into circulant submatrices, it is also necessary as the next proposition shows.

$$\begin{array}{ccccc@{\quad}ccccc@{\quad}c@{\quad}ccccc}
0 & 1 & 2 & \cdots & m-1 & m & 1 & 2 & \cdots & m-1 & \cdots & N-m & 1 & 2 & \cdots & m-1 \\
m-1 & 0 & 1 & \cdots & m-2 & m-1 & m & 1 & \cdots & m-2 & \cdots & m-1 & N-m & 1 & \cdots & m-2 \\
m-2 & m-1 & 0 & \cdots & m-3 & m-2 & m-1 & m & \cdots & m-3 & \cdots & m-2 & m-1 & N-m & \cdots & m-3 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 2 & 3 & \cdots & 0 & 1 & 2 & 3 & \cdots & m & \cdots & 1 & 2 & 3 & \cdots & N-m \\[1.5em]
N-m & 1 & 2 & \cdots & m-1 & 0 & 1 & 2 & \cdots & m-1 & \cdots & N-2m & 1 & 2 & \cdots & m-1 \\
m-1 & N-m & 1 & \cdots & m-2 & m-1 & 0 & 1 & \cdots & m-2 & \cdots & m-1 & N-2m & 1 & \cdots & m-2 \\
m-2 & m-1 & N-m & \cdots & m-3 & m-2 & m-1 & 0 & \cdots & m-3 & \cdots & m-2 & m-1 & N-2m & \cdots & m-3 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 2 & 3 & \cdots & N-m & 1 & 2 & 3 & \cdots & 0 & \cdots & 1 & 2 & 3 & \cdots & N-2m \\
 & & \vdots & & & & & \vdots & & & & & & \vdots & & \\
 & & \vdots & & & & & \vdots & & & & & & \vdots & & \\
m & 1 & 2 & \cdots & m-1 & 2m & 1 & 2 & \cdots & m-1 & \cdots & 0 & 1 & 2 & \cdots & m-1 \\
m-1 & m & 1 & \cdots & m-2 & m-1 & 2m & 1 & \cdots & m-2 & \cdots & m-1 & 0 & 1 & \cdots & m-2 \\
m-2 & m-1 & m & \cdots & m-3 & m-2 & m-1 & m & \cdots & m-3 & \cdots & m-2 & m-1 & 0 & \cdots & m-3 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 2 & 3 & \cdots & m & 1 & 2 & 3 & \cdots & 2m & \cdots & 1 & 2 & 3 & \cdots & 0
\end{array}$$

Figure 5.2.2.1. Subscripts of a Subrepeating Matrix of Period m.
Sub-matrix blocks are indicated with extra spacing between the blocks.

5.2.3 **Proposition** Let A be the matrix $\mathrm{CIRC}_N(a) \in \mathrm{CIRC}_N(R)$. A can be partitioned into CIRC_m matrices for some $m \mid N$ iff a is a subrepeating sequence of period m.

Proof. Sufficiency was demonstrated above, so we need only show that if $A = \mathrm{CIRC}_N(a)$ can be partitioned into circulant matrices, then a is subrepeating.

Let $N = nm$. We assume that a is arbitrary and impose conditions to satisfy the partitioning requirement. So, the first row is arbitrary and the top row of circulant $m \times m$ submatrices is

$$\big(a_0, a_1, \ldots, a_{m-1}, \quad a_m, a_{m+1}, \ldots, a_{2m-1}, \quad a_{2m}, a_{2m+1}, \ldots, a_{3m-1}, \quad \ldots, \quad a_{N-m}, a_{N-m+1}, \ldots, a_{N-1}\big)$$

The second row of $\mathrm{CIRC}_N(a)$ is the above row rotated to the right. The last entry of each $m \times m$ submatrix row becomes the first entry in its neighbor's second row. Therefore, $a_{jm-1} = a_{(j+1)m-1}$ for $j = 1, \ldots, n-1$. Continuing to the subsequent rows of the top $m \times m$ circulant matrices, we will find that

$$a_{jm-s} = a_{(j+1)m-s} \quad \text{for } j = 1, 2, \ldots, n-1, \text{ and } s = 1, 2, \ldots, m-1$$

$$\text{That is, } a_{m-s} = a_{2m-s} = a_{3m-s} = \cdots = a_{N-m-s} \text{ for } s = 1, 2, \ldots, m-1$$

Therefore, a is a subrepeating sequence. □

5.2.4 **Corollary** The subrepeating matrices, $\mathrm{CIRC}(\mathrm{QR}^m_{mn}(R))$, form an algebra over R, and are equal to $\mathrm{CIRC}_N(R) \cap \mathrm{CIRC}_n(\mathrm{CIRC}_m(R))$.

Proof. $\mathrm{CIRC}_N(R)$ is a ring; so is $\mathrm{CIRC}_n(\mathrm{CIRC}_m(R))$. By the proposition, subrepeating matrices of period m can be regarded as belonging to either, hence so can their sums, products, etc. □

5.2.5 **Decomposition of Subrepeating Circulants.**

The algebraic form of a subrepeating vector can be specified completely using the Γ homomorphisms of chapter 3. Let $N = mn$. Two sub-vectors are required to specify a subrepeating vector of period m: the sequence of $m-1$ terms that repeats n times, and the sequence of terms which fill every m^{th} term. These two subvectors we now define.

5.2.6 **Definition** Let $a \in \mathrm{QR}^m_{mn}$.

(i) Define $a^{(m)}(x) := (x, a_1, a_2, \ldots, a_{m-1}) \in \mathbf{circ}_m(R)$, and define $a^{(m)} := a^{(m)}(0)$.

(ii) Define $a_{(m)}(x) := (a_0 - x, a_m - x, a_{2m} - x, \ldots, a_{mn-m} - x) \in \mathbf{circ}_n(R)$, and define $a_{(m)} := a_{(m)}(0)$.

We call the $a^{(m)}$ the periodic sub-vector, and we call $a_{(m)}$ the basic sub-vector. As a mnemonic, one can think of $a_{(m)}$ as being the vector whose indices are in the ideal (m), and $a^{(m)}$ as being a vector of order m (which is consistent with our notation $\lambda^{(m)}$ for λ operating on circulants of order m.)

The definition of the two subvectors include an arbitrary parameter x. Inspection shows that this parameter is entirely cancelled in the full subrepeating vector, so x can be freely chosen with no effect on the subrepeating vector.

The periodic subvector, $a^{(m)}$, repeats in the full vector with period m. By definition of Γ^{mn}_m in §3.5.1, $n\Gamma^{mn}_m$ applied to $a^{(m)}$ creates a sequence of length mn in which $a^{(m)}$ repeats with period m. (The factor of n is needed to cancel the factor of $1/n$ in the definition of Γ^{mn}_m.) The subvector $a_{(m)}$ is distributed in the full vector at every m^{th} term. By Proposition 3.5.2, $\tilde{\Gamma}^{mn}_n$ applied to $a_{(m)}$ creates a vector of length mn with $a_{(m)}$ so distributed. Hence,

$$a \quad = \quad \tilde{\Gamma}^{mn}_n\left(a_{(m)}(x)\right) \; + \; n \cdot \Gamma^{mn}_m\left(a^{(m)}(x)\right) \tag{4}$$

Formula (4) is merely an algebraic description of Figure 5.2.1.1. It can be interpreted as saying that there is a vector space map, $\tilde{\Gamma}^{mn}_n + n\Gamma^{mn}_m$ which maps $R^n \oplus R^m$ onto $\mathrm{QR}^m_{mn}(R)$. The kernel of the map is the one-dimensional space spanned by $(1, 0, 0, \ldots, 0) \oplus (-1, -1, \ldots, -1)$ corresponding to $x = 1$ and $a_i = 0$ for all i in $a_{(m)}(x)$ and $a^{(m)}(x)$. Equation (4) is therefore a necessary and sufficient condition for a circulant to be subrepeating.

5.2.11 Eigenvalue Decomposition of Subrepeating Circulants.

Apply λ to equation (4).

$$\lambda(a) \;=\; m\Gamma_n^{mn}\left(\lambda a_{(m)}(x)\right) \;+\; n\tilde{\Gamma}_m^{mn}\left(\lambda a^{(m)}(x)\right) \tag{5}$$

This shows that $\lambda(a)$ is also subrepeating but with period n, not m, and

$$\begin{aligned} \lambda(a)^{(n)}(x) \;&=\; \lambda\left(a_{(m)}(x)\right) \\ \lambda(a)_{(n)}(x) \;&=\; n\lambda\left(a^{(m)}(x)\right) \end{aligned} \tag{6}$$

This is confirmation that the subrepeating circulants form a subalgebra since subrepeating sequences are obviously closed under componentwise addition and multiplication. One must take care in interpreting equation (6). Generically, $\lambda_0(a)^{(n)} \neq 0$; that is the periodic sub-vector does not typically have zero first component. So, when inspecting $\lambda(a)$ one should bear in mind that the basic sub-vector has contributions from $\lambda_0(a)^{(n)}$ as well as $n\lambda\left(a^{(m)}(x)\right)$. If one desires pure periodic and basic sub-vectors, then one should set $x = n^{-1}\lambda_0(a_{(m)})$.

Expanding equation (6) using the definition for Γ_n^{mn} and Proposition 3.5.2*(ii)*, the formula for the eigenvalues is

$$\lambda_i^{(mn)}(a) \quad=\quad \lambda_i^{(n)}(a_{(m)}(x)) \;+\; n\delta_i^n\lambda_{i/n}^{(m)}\left(a^{(m)}(x)\right) \tag{7}$$

The arbitrary constant, x, has no effect on any eigenvalue of $a_{(m)}(x)$ except for the $\lambda_0^{(n)}$ eigenvalue which is given by

$$\lambda_0^{(n)}\left(a_{(m)}(x)\right) \;=\; \lambda_0(a_{(m)}) - nx$$

Hence, there is contribution of nx to every n^{th} eigenvalue, $\lambda_{in}^{(mn)}(a)$. However, the effect of x on the eigenvalues of $a^{(m)}$ is to add x to each. Because of the factor of n on $\lambda\left(a^{(m)}(x)\right)$ in equation (6), these exactly cancel the nx from the eigenvalues of $a_{(m)}$.

Given a subrepeating eigenvalue vector, $\mu(y)$, say, of period n with arbitrary constant y, the subrepeating circulant for it is given by reversing equations (6)

$$\begin{aligned} a_{(m)}(y/n) \;&=\; \lambda^{-1}\left(\mu^{(n)}(y)\right) \\ a^{(m)}(y/n) \;&=\; n^{-1}\lambda^{-1}\left(\mu_{(n)}(y)\right) \end{aligned} \tag{8}$$

As an application of these ideas, an example of subrepeating vector is provided by the multiplicative projection, $\bar{a} = \bar{\delta}_\times^n(a)$. This is most simply seen in the eigenvalues of $\bar{a}$. Letting $\mu = \lambda(a)$, by Definition 3.5.5

$$\lambda_i(\bar{a}) \;=\; \begin{cases} \mu_i & \text{if } n\,|\,i \\ 1 & \text{otherwise} \end{cases}$$

$$\therefore\ \lambda(\bar{a}) \;=\; (\mu_0, 1, \ldots, 1,\ \mu_n, 1, \ldots, 1,\ \mu_{2n}, 1, \ldots, \ldots, 1,\ \mu_{mn-m}, 1, \ldots, 1)$$

This is manifestly subrepeating with

$$\begin{aligned} \lambda(\bar{a})^{(n)} \;&=\; (y, 1, 1, \ldots, 1) \\ \lambda(\bar{a})_{(n)} \;&=\; (\mu_0 - y, \mu_n - y, \mu_{2n} - y, \ldots, \mu_{mn-n} - y) \end{aligned}$$

Choose $y = 1$. Then, by equations (8),

$$\bar{a}_{(m)} \;=\; \lambda^{-1}(1, 1, \ldots, 1) \;=\; 1$$

$$\begin{aligned}
\bar{a}^{(m)} &= \frac{1}{n}\lambda^{-1}(\mu_0, \mu_n, \ldots, \mu_{mn-n}) - \frac{1}{n}\lambda^{-1}(1, 1, \ldots, 1) \\
&= \frac{1}{n}\left(\lambda^{-1}\tilde{\Gamma}^m_{mn}(\mu) - 1\right) \\
&= \frac{1}{n}\left(\Gamma^m_{mn}(a) - 1\right)
\end{aligned}$$

We have proved:

5.2.12 **Lemma** Suppose $a \in \mathbf{circ}_{mn}(R)$ and let $\bar{a} = \bar{\delta}^n_\times(a)$, then $\bar{a}$ is a subrepeating sequence with

$$\begin{aligned}
\bar{a}^{(m)} &= \frac{1}{n}\left(\Gamma^m_{mn}(a) - 1\right) \\
\bar{a}_{(m)} &= 1 \qquad \square
\end{aligned}$$

5.2.13 **Determinant Decomposition of Subrepeating Matrices.**
Formula (7) can be used to relate circulant determinants of commensurate orders. The next proposition supplies such a formula for general $N = mn$.

5.2.14 **Proposition** Let $N = mn$ and let $a \in \mathbf{circ}_N(R)$ be subrepeating of period m. Let $b = a_{(m)}$. Then,

$$\Delta_N(a) = \left(\frac{\Delta_n(b)}{\lambda_0(b)}\right)^m \Delta_m\left(\Gamma^m_{mn}(a)\right) \tag{9}$$

Proof. Let $c = a^{(m)}$. By formula (7),

$$\begin{aligned}
\Delta_{mn}(a) &= \prod_{j=0}^{N-1}\left(\lambda^{(n)}_{j \bmod n}(b) \;+\; n\delta^n_j\lambda^{(m)}_{j/n}(c)\right) \\
&= \frac{\prod_{j=0}^{N-1}\lambda^{(n)}_{j \bmod n}(b)}{\prod_{k=0}^{m-1}\lambda^{(n)}_{nk \bmod n}(b)} \cdot \prod_{k=1}^{m-1}\left(\lambda^{(n)}_{nk \bmod n}(b) + n\lambda^{(m)}_k(c)\right) \\
&= \frac{\Delta_n(b)^m}{\lambda_0(b)^m} \cdot \prod_{k=1}^{m-1}\left(\lambda_0(b) + n\lambda^{(m)}_k(c)\right) \\
&= \left(\frac{\Delta_n(b)}{\lambda_0(b)}\right)^m \cdot \prod_{k=0}^{m-1}\lambda^{(m)}_k\left(\mathrm{u}^0\lambda_0(b) + n \cdot c\right) \\
&= \left(\frac{\Delta_n(b)}{\lambda_0(b)}\right)^m \Delta_m\left(\mathrm{u}^0\lambda_0(b) + n \cdot c\right)
\end{aligned}$$

From formula (7) with $x = 0$, the expression $\mathrm{u}^0\lambda_0(b) + n \cdot c$ equals $\Gamma^m_{mn}(a)$. □

One part of formula (9) was published almost a century ago in a book on determinants written by Sir Thomas Muir and W. Metzler. The book devoted quite a long section to circulant determinants. One result appearing in the book was the factorization of the determinant of order $N = 12$; they supplied two factors, of which one was the determinant of order m corresponding to the second factor in formula (9), and the other was a nondescript factor corresponding to the first factor in (9); both factors were shown to be in the base ring of the circulant. Although the authors provided a proof only for $N = 12$, their method clearly applied to general N.

The point of view of the book was purely determinantal; there was no mention of matrices. Possibly as a result of this, the authors failed to notice that their nondescript factor, the first given in formula (9), was also a circulant determinant, albeit divided by the sum of the first row, and raised to the n^{th} power.

The proposition relates the determinants of $mn \times mn$ circulant matrices to the determinants of $n \times n$ and $m \times m$ circulant matrices. Notice that the second factor, $\Delta\left(\Gamma^m_{mn}(a)\right)$ is the determinant of $\bar{\delta}^{n*}_{\times}(a)$. It follows that the first factor, $\left(\Delta(b)/\lambda_0(b)\right)^m$, is the determinant of $(1-\bar{\delta}^{*n})_{\times}(a) = a - \bar{\delta}^{*n}(a-1)$ (see Lemma 3.2.15).

If we take the repeating sub-vector $c = (a_1, a_2, \ldots, a_{m-1})$ to be zero, then formula (9) reduces to

$$\Delta_{mn}(a) = \left(\Delta_n(a_{(m)})\right)^m, \qquad (\forall n, m \text{ with } a^{(m)} = 0)$$

5.2.15 **Example** Let $N = 6$, and $m = 2, n = 3$. The expansion for $\Delta_6(a_0, 0, a_2, 0, a_4, 0)$ can be computed by squaring the expansion for $\Delta_3(a_0, a_2, a_4)$ thus, from §1.11.4,

$$\begin{aligned}
\Delta_6(a_0,0,a_2,0,a_4,0) \quad &= \quad \Delta_3(a_0,a_2,a_4)^2 \quad = \quad (a_0^3 + a_2^3 + a_4^3 - 3a_0a_2a_4)^2 \\
&= \quad a_0^6 + a_2^6 + a_4^6 \; + \; 2(a_0^3a_2^3 + a_2^3a_4^3 + a_0^3a_4^3) \\
&\qquad - \; 6(a_0^4a_2a_4 + a_2^4a_0a_4 + a_4^4a_0a_2) \; + \; 9a_0^2a_2^2a_4^2
\end{aligned}$$

One can check that the above terms are all the even subscript terms in the full expansion for Δ_6 by consulting §1.11.4.