CIRCULANTS

Alun Wyn-jones

Last revised in December 2013.

Preface

The work in this book grew out of a simple discovery which led to other, less simple, discoveries, and eventually to quite complicated discoveries which were all in the service of three assaults (which all failed) on Fermat's Last Theorem. Eventually, I made the really simple discovery that much was already known about the subject of my research, and appeared in the literature under the heading of "circulants" and not " cyclic matrices" as I (and others) had been calling them. I decided that a remedy to working in isolation was to publish what I knew of the subject, and to thereby familiarize the others with "circulants." That effort led to the present book.

The book assumes the reader has an understanding of undergraduate algebra as taught at an American university: linear algebra, introductory group theory, ring theory, and simple Galois Theory. Only Chapter 9 requires some calculus.

The book has been around in various forms for a long time, at least ten years. Shortly before writing the first version, I discovered the formula for the determinantal coefficients of the general circulant. This was (to me) a major accomplishment since there had been attempts since the 19^{th} century to discover such a closed formula which continued up until the early part of the twentieth century. For this reason, the book ends with that formula (Chapter 10), and its immediate consequences (Chapter 11).

Since then, I made some more discoveries. One was already known and published by Hyman Bass, but is independently derived in Chapter 7. This result is the characterization of a group of finite index in the group of units of circulant rings of prime order over the integers. In algebraic terms, the circulants are group rings whose groups are cyclic, and this is how the result was first published by Bass. The latter part of the chapter contains a generalization of this result to prime-power orders which I believe gives a better picture of the units of integral cyclic group rings.

The earlier chapters serve two purposes: to prepare for Chapter 7 which requires quite a bit of ring and cyclotomic theory, and to bring circulants into a ring-theoretic setting. This latter aim has led to much new notation which I hope meets readers' approval.

Chapter 1 introduces the circulants and their most basic properties. It ends with two formulæ for the determinant, the product-of-the-eigenvalues formula, and the rather surprising Resultant Formula.

Chapter 2 considers circulants in their traditional context of a sub-algebra of the matrices. It considers their centralizer and normalizer within the matrices. The chapter calculates the groups of circulant automorphisms over the complex and real numbers.

Chapter 3 is the first to adopt an abstract algebraic view of circulants. The chapter begins by proving a structure theorem which expresses the ring of circulants of order n in terms of the circulants having orders dividing n. The chapter then defines a host of maps between, to, and from circulants, and attempts to impose some order on these maps.

Chapter 4 introduces the "supercirculants." The professional mathematician might recognize them as an inverse limit system in the algebras of circulants. This chapter is probably the prettiest of the book containing some nice simplifications of the plethora of maps in Chapter 3.

Chapter 5 considers two sub-algebras of the circulants which are important in investigations of the circulant determinant. The first of these, the residue class circulants, led to a formula in the theory of partitions which might be new.

Chapter 6 vies with Chapter 4 for prettiness. It investigates possible tensor products over the circulants.

Chapter 7 aims to characterize the unit group of the integer circulants. This succeeds up to a finite index of the group for circulants of prime power order. This is by far the lengthiest and most technical chapter in the book.

Chapter 8 continues the study of the integer circulants from Chapter 7 but from a very different viewpoint. The chapter has a strong ring-theoretic flavor. A circulant norm is defined whose properties are shown to be typical of algebraic norms. The norm is used to find the prime elements of the integer circulants.

Chapter 9 serves as an intermission amidst algebraic abstractions. It discusses a possible application of circulants to physics and statistical mechanics.

Chapter 10 discusses an application to homogenous diophantine equations most particularly, FLT and attempts by Wendt and Sophie Germain at its resolution.

Chapter 11 contains the complete derivation of the formula for the determinantal coefficient. The book ends with an unexpected corollary of this formula which led to a simple conjecture which occupied much of my time in an attempt to prove it until I discovered a theorem of Erdös, Ginzburg, and Ziv, now called the EGZ Theorem which is equivalent to my conjecture. This theorem is proved in full.

Alun Wyn-jones, Carlisle, Pennsylvania
January 2008.

Preface to the Second Edition

I have made minor corrections, and added a small section in Chapter 2 on the projection operator onto the circulants from the set of general matrices.

The biggest changes are the inclusion of a theorem on arithmetical partitions in Chapter 5, the inclusion of the full proof of the formula for the determinantal coefficient in Chapter 11, and the inclusion of a new chapter, Chapter 12, on the case of circulants over finite fields. The material for the new chapter was previously a separate article.

Alun Wyn-jones, New York City
awynjones@verizon.net
December 2013.

Circulants.

Chapter 1.
Circulants.

1.1 **Introduction** Circulants have been known to humanity since at least the beginning of the nineteenth century when they were revealed in their original manifestation as circulant determinants. Later in the century, matrices were invented and circulants were reinterpreted as matrices. Later still, matrices became part of a new, formal, and more abstract algebra of the Twentieth Century. Circulants could then be viewed as a special kind of algebra, a sub-algebra of the matrix algebra.

However circulants retain their basic simplicity. One can understand circulants, study them, discover things about them, and take delight in them with but a little background in college algebra. The primary goal of this book is to describe circulants in an algebraic context. However, the older forms cannot be ignored, else the theory presented herein would be merely a special case of several modern algebraic theories. Therefore, much of the book is concerned with old problems, especially those parts dealing with the circulant determinant. Consequently, the book oscillates between the point of view of circulants as a commutative algebra, and the concrete point of view of circulants as matrices with emphasis on their determinants..

There are many applications of the theory of circulants. Indeed, many researchers have independently rediscovered circulants for this reason. Sometimes a researcher would be unaware of the name "circulant"; indeed one common alternative name was "cyclic matrix."

The applications are mainly in pure mathematics and technology which mysteriously reflects the abstract - concrete dichotomy of the theory of circulants. For instance, modern telecommunications would be impossible without frequency analysis. With the advent of fast digital computing, the main technique of frequency analysis has become the discrete Fourier transform. This transform is also the single most important transform on circulants, so much so, that much of the theory of circulants can be regarded as the theory of the discrete Fourier transform. Circulants are important in digital encoding; this is a wondrous technology --it enables devices ranging from computers to music players to recover from errors in transmission and storage of data, and restore the original data. However, the initial impetus to the study of circulants was not technological but rather stemmed from problems in pure mathematics, particularly number theory. Several other applications to pure mathematics have since been discovered. Prof. D. L. Johnson has used circulants to analyze cyclically presented abelian groups. Prof. P. Davies and others have described properties of nested polygons as circulant transformations. Circulant graphs are an important sub-field of graph theory. As we proceed, we shall point out applications of circulants to homogeneous diophantine equations and combinatorial analysis. Finally, towards the end of the book, we shall return to the physical sciences with an application of circulants to the evolution of density fluctuations.

Given such an imposing collection of applications, it may be a pleasant surprise to discover that the most general circulant matrix can be described very simply. Circulant matrices are always square. Here is the most general circulant matrix of order N.

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{N-1} \\ a_{N-1} & a_0 & a_1 & \dots & a_{N-2} \\ a_{N-2} & a_{N-1} & a_0 & \dots & a_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{pmatrix} \tag{1}$$

We shall explain in a moment why we index the entries in the matrix with the numbers 0 through $N-1$ rather than the more conventional 1 through N. We shall generally reserve the capital letter N to denote the order of circulant matrices.

1.2.1 **How to Construct a Circulant Matrix.** A circulant matrix can be constructed from any sequence of N objects, $a = (a_0, a_1, \dots, a_{N-1})$, say, by the following procedure.

Take the sequence $(a_0, a_1, \dots, a_{N-1})$ as the first row of A. For its second row take the sequence $(a_{N-1}, a_0, a_1, \dots, a_{N-2})$ which is the same sequence but rotated once to the right. For the third row,

take the sequence $(a_{N-2}, a_{N-1}, a_0, \ldots, a_{N-3})$ which is a rotation to the right of the second row. Continue in like manner until all the rows are filled. If the last row were rotated, it would repeat the first row.

We could adopt this contruction as our definition of a circulant matrix by insisting that whatever can be built using the construction is a circulant matrix, and that all circulant matrices can be so constructed. Unfortunately, such heuristic rules do not lend themselves to easy analysis. So, instead, we adopt a formal definition which is easily shown to be equivalent to the construction.

1.2.2 **Definition** Let $A = (a_{i,j})$ be an $N \times N$ matrix. A is a **circulant matrix** if and only if

$$a_{i,j} = a_{k,l} \text{ whenever } j - i \equiv l - k \pmod{N}$$

That is, the value of an entry in a circulant matrix depends only the difference of its column and row position modulo N. You can check that the matrix in (1) above satisfies this criterion.

1.2.3 **Exercise.** Show that this definition guarantees that the matrix is circulant in the sense that it can be constructed from the first row by rotations as described in section 1.2.1.

The construction of §1.2.1 shows that a circulant matrix A is completely defined by any row. For definiteness, we shall always regard A as defined by its top row just as in the construction. Because of its appointed rôle, we shall refer to the top row as the **circulant vector**.

1.3 **Definition**
(i) Let $a = (a_0, a_1, \ldots, a_{N-1})$ then the circulant matrix $A = (a_{i,j})_{i,j}$ where $a_{i,j} = a_{j-i \pmod{N}}$ is denoted by $\mathbf{CIRC}_N(a)$.
(ii) The vector a (the top row of the circulant matrix) is called the **circulant vector**

It is clear that the natural indexing set for entries in $N \times N$ circulant matrices is the set of residues modulo N, that is, remainders after division by N. We shall denote the set of residues modulo N by $\mathbb{Z}_N$, and henceforth, it will be the indexing set for entries in most matrices and vectors. Sometimes, there will be subscripts involving products of residues. So, $\mathbb{Z}_N$ should be regarded as the ring of residues, not just the additive group. The reason we indexed the entries in the circulant matrix from zero to $N-1$ rather than 1 to N is because the remainders modulo N contain 0 but not N.

We shall generally (Chapter §9 is the only exception) assume that the entries in a circulant matrix belong to a commutative ring with identity. If we have no specific ring in mind, we shall usually denote it by R. The order of the circulant matrix, N, should not be a divisor of zero in the ring R else most of the ensuing theory will not work. In fact, R can usually be assumed to be a complex domain, that is, a subring of $\mathbb{C}$, and unless otherwise indicated this can be assumed.

1.4 **Definition** Let R be a (commutative) ring. The set of all $N \times N$ circulant matrices over R will be denoted by $\mathbf{CIRC}_N(R)$. Thus, in terms of Definition 1.3,

$$\mathrm{CIRC}_N(R) \;:=\; \{\mathrm{CIRC}_N(v) \vdash v \in R^N\}$$

1.5 **Examples.**
(i) The first example of a circulant matrix is any matrix of the form cI where c is a scalar and I is the identity matrix. In particular, the identity and zero matrices are circulant.
(ii)

$$\mathrm{CIRC}_3(1,\ 2,\ 3) \;=\; \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \mathrm{CIRC}_3(4,\ 3,\ 2) \;=\; \begin{pmatrix} 4 & 3 & 2 \\ 2 & 4 & 3 \\ 3 & 2 & 4 \end{pmatrix}$$

(iii)

$$\therefore\ \mathrm{CIRC}_3(1,\ 2,\ 3)\mathrm{CIRC}_3(4,\ 3,\ 2) \ = \ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 4 & 3 & 2 \\ 2 & 4 & 3 \\ 3 & 2 & 4 \end{pmatrix} \ = \ \begin{pmatrix} 17 & 17 & 20 \\ 20 & 17 & 17 \\ 17 & 20 & 17 \end{pmatrix}$$
$$= \ \mathrm{CIRC}_3(17,\ 17,\ 20)$$

In example *(iii)*, the product of the two circulant matrices is itself a circulant matrix. This is a general property of circulants as will be proved shortly.

The beginning for most of the ensuing theory is the next theorem (Theorem 1.6). Even though it is easy to prove, its importance to circulant matrices is fundamental, and so some discussion of the theorem is in order.

The theorem is effectively restricted to circulant matrices having entries in a subring of a field which has an extension containing N^{th} roots of unity. The first statement of the theorem says that there is a matrix (denoted by F) which diagonalizes every circulant matrix. That is, given any circulant matrix C, then $F^{-1}CF$ is a diagonal matrix. This is a highly unusual property. A general matrix need not possess any diagonalizing matrix, so the fact that every circulant matrix can be diagonalized is unusual enough. That the single matrix F suffices to diagonalize all circulants is truly exceptional. If we regard the circulant matrices as linear transformations on a complex vector space, then the first statement says that there is a basis for the vector space in which the circulant matrices transform as a set of diagonal matrices. To look ahead a bit, it is easy to see that the set of all diagonal matrices is closed under matrix multiplication, and is also commutative. This shows that multiplication of circulant matrices is commutative, and suggests that it might also be closed. Since circulant matrices are trivially closed under addition, it already emerges that they actually form a commutative ring. We can show that the circulant matrices are closed under multiplication by showing that the set of diagonalized circulant matrices are closed under multiplication. This is effectively accomplished in the third statement of the theorem which shows that inverse diagonalization (whereby diagonal D is mapped to FDF^{-1}) always produces a circulant matrix. To summarize, the transformation $C \mapsto F^{-1}CF = D$ say, acting on circulant matrices, produces a set of diagonal matrices. The property of being a diagonal matrix is obviously preserved by addition and multiplication. The reverse transformation acting on diagonal matrices, $D \mapsto FDF^{-1} = C$ say, produces a set of circulant matrices.

Now, if a matrix C can be diagonalized, the entries down the main diagonal of its diagonalized form are the eigenvalues of C. The second statement of the theorem merely applies this fact to a general circulant matrix to obtain a formula for its eigenvalues. Later, this formula is interpreted as a map, a linear and multiplicative map, on circulants. That the circulant matrices form a ring implies that this map is actually a ring homomorphism. This homomorphism is the single most important map on circulant matrices.

The proof of the theorem uses a notation which will be used throughout the remainder of the book.

$$\delta_x^N \ := \ \begin{cases} 1 & \text{if } x \equiv 0 \pmod{N} \\ 0 & \text{otherwise} \end{cases}$$

When the order, N, is understood or is clear from the context it will often be omitted. (All special terms such as δ_x and N are listed in the Glossary, as well as general notations and conventions.)

1.6 **The Circulant Diagonalization Theorem** Let R be a subring of a field whose characteristic does not divide N, and let ζ be a primitive N^{th} root of unity, if necessary in an extension, R_ζ, of R. Let F be the matrix with entries $F_{i,j} = \sqrt{N^{-1}}\zeta^{ij}$.

(i) F is a simultaneous, unitary, diagonalizing matrix for $\mathrm{CIRC}_N(R)$.

(ii) Let $A = \mathrm{CIRC}_N(a) \in \mathrm{CIRC}_N(R)$ then the eigenvalues of A are

$$\lambda_j \ = \ \lambda_j(A) \ = \ \sum_{i \in \mathbb{Z}_N} a_i \zeta^{ij}, \qquad \forall j \in \mathbb{Z}_N.$$

(iii) If $\mu = (\mu_0, \mu_1, \ldots, \mu_{N-1}) \in R_\zeta^N$ then $F\,\mathrm{Diag}(\mu)F^{-1} \in \mathrm{CIRC}_N(R_\zeta)$.

Proof. Let $A = \mathrm{CIRC}_N(a)$ and let F be as stated. Consider $F^\dagger AF$.

$$\begin{aligned}
(F^\dagger AF)_{i,l} &= N^{-1} \sum_{j,k\in\mathbb{Z}_N} \zeta^{-ij} a_{k-j} \zeta^{kl} \\
&= N^{-1} \sum_{j,s\in\mathbb{Z}_N} a_s \zeta^{(s+j)l-ij} \quad (\text{setting } s = k-j) \\
&= N^{-1} \sum_{s\in\mathbb{Z}_N} a_s \zeta^{sl} \sum_{j\in\mathbb{Z}_N} \zeta^{j(l-i)} \\
&= N^{-1} N \delta_{i-l} \sum_{s\in\mathbb{Z}_N} a_s \zeta^{sl} \\
\therefore F^\dagger AF &= \mathrm{Diag}(\lambda_0, \lambda_1, \ldots, \lambda_{N-1}), \quad \text{where } \lambda_j = \sum_{i\in\mathbb{Z}_N} a_i \zeta^{ij}
\end{aligned} \tag{1}$$

To show that F is a diagonalizing matrix, we shall prove that $F^\dagger = F^{-1}$. Equations (1) are valid for any circulant matrix over R, so substitute the identity matrix, I, for A. It is trivial that I is circulant and that $\lambda_j(I) = 1,\ \forall j \in \mathbb{Z}_N$. Therefore, $F^\dagger F = \mathrm{Diag}(1, 1, \ldots, 1) = I$. QED *(i)* and *(ii)*.

(iii) Let $\mu = (\mu_0, \mu_1, \ldots, \mu_{N-1}) \in R_\zeta^N$ and let $A = (a_{i,j}) = F\,\mathrm{Diag}(\mu)F^{-1}$.

$$a_{i,l} \;=\; N^{-1} \sum_{j,k\in\mathbb{Z}_N} \zeta^{ij} \mu_j \delta_{j-k} \zeta^{-kl} \;=\; N^{-1} \sum_{j\in\mathbb{Z}_N} \zeta^{-j(l-i)} \mu_j$$

which therefore depends only on $l - i \pmod N$ and so, by definition 1.3, A is a circulant matrix. □

We should emphasize that Theorem 1.6 applies only to integral domains whose characteristic does not divide the order of the circulant. So fundamental is the theorem that all ensuing development will be restricted to such rings, and indeed large sections will be further restricted to subrings of the complex numbers.

The matrix F is called the **Fourier matrix**. When the order of the matrix is not clear, we shall denote the Fourier matrix of order $n \times n$ by F_n. Thus, $(F_n)_{i,j} = \sqrt{n^{-1}}\zeta_n^{ij}$ where ζ_n is a primitive n^{th} root of unity. For a given n, there are $\phi(n)$ primitive roots of unity where $\phi(n)$ is the Euler (or totient) function. The choice of ζ_n is arbitrary. In the case of a complex domain, we shall take $\zeta_n = e^{2\pi\iota/n}$. In the case of rings of finite characteristic we just assume that one primitive root can be singled out.

The symbol ζ will be reserved throughout for a primitive root of unity, often an N^{th} primitive root of unity. The symbol λ will be reserved for the eigenvalues of a circulant matrix (though when several circulant matrices are present we might use other Greek letters such as μ). The eigenvalues of a general matrix are not usually presented to us in any natural order. Of course, we can impose an order on them, but this is usually arbitrary. However, once a primitive root of unity has been chosen, the eigenvalues of circulant matrices have a natural order, namely, $\lambda_0, \lambda_1, \ldots, \lambda_{N-1}$, which is the order given in the theorem. We can therefore regard λ as a function acting on a circulant matrix yielding a sequence of N complex numbers --the N eigenvalues of the circulant matrix. Thus, λ is seen to be a map from the set of circulant matrices into an N-dimensional complex vector space. This is formally stated in the next definition.

1.7 **Definition** The following definitions apply to $\mathrm{CIRC}_N(R)$ where R is an integral domain whose characteristic does not divide N.

(i) R_ζ and $R(\zeta)$ will denote same thing, namely, the smallest ring containing both R and a primitive N^{th} root of unity, ζ. Thus, if R contains a primitive N^{th} root of unity, then $R_\zeta = R$

(ii) Let $A = \mathrm{CIRC}_N(a_0, a_1, \ldots, a_{N-1})$. For every $j \in \mathbb{Z}_N$, define the map $\lambda_j : \mathrm{CIRC}_N(R) \to R_\zeta$ by

$$\lambda_j(A) \;:=\; \sum_{i\in\mathbb{Z}_N} a_i \zeta^{ij}$$

$\lambda_j(A)$ is the j^{th} eigenvalue of the circulant matrix A.

(iii) Now define $\lambda(A)$ to be the vector of all the eigenvalues in their natural order.

$$\lambda(A) \;:=\; (\lambda_0(A),\; \lambda_1(A),\; \ldots,\; \lambda_{N-1}(A))$$

In formal notation, λ is the map $\quad \lambda_0 \oplus \lambda_1 \oplus \cdots \oplus \lambda_{N-1} \;:\; \mathrm{CIRC}_N(R) \;\to\; R_\zeta^N$.

With these notations, $\lambda_i(A)$ and $\lambda(A)_i$ denote the same thing: the i^{th} component of $\lambda(A)$ which is the i^{th} eigenvalue of A.

(iv) We shall denote the image of $\mathrm{CIRC}_N(R)$ under λ by $\Lambda_{N,\zeta}(R)$. Thus, λ maps $\mathrm{CIRC}_N(R)$ onto $\Lambda_{N,\zeta}(R)$. We shall almost always omit the ζ in the subscript and write just $\Lambda_N(R)$, or even $\Lambda(R)$.

1.8 **Corollaries of Theorem** 1.6

The theme of the corollaries which follow is that the map λ is a ring homomorphism. However, before showing that λ is a ring homomorphism it is wise to first ensure that the range of λ is a ring.

There is always considerable leeway in choosing the range of a map. Of course, the range must contain the image, which in our case is $\Lambda(R)$, but is otherwise arbitrary. For circulant matrices with complex entries, it would therefore seem natural to take the range of λ as the N-dimensional vector space $\mathbb{C}^N$. However, most circulants of interest have real, algebraic numbers, rational numbers, or integer entries, and not general complex numbers. Let us take the set of integral circulant matrices, $\mathrm{CIRC}(\mathbb{Z})$, as an example. To take $\mathbb{C}^N$ as the range of λ acting on $\mathrm{CIRC}(\mathbb{Z})$ misses all the subtleties of cyclotomic and rational integer arithmetic which makes the set $\mathrm{CIRC}(\mathbb{Z})$ interesting in the first place. So why not take the range as the image itself? One practical reason is that it is not at all easy to characterize the set $\Lambda_N(\mathbb{Z})$. Instead, we could try the set $\mathbb{Z} \oplus \mathbb{Z}_\zeta^{N-1}$ (the direct sum of $\mathbb{Z}$ and $\mathbb{Z}_\zeta$ with itself $N-1$ times). The first component reflects that fact that λ_0 is just the sum of the circulant vector and so is always in the base ring, in this case $\mathbb{Z}$. But this choice is too *ad hoc*. This set does indeed contain $\Lambda_N(\mathbb{Z})$, but it is not homogenous -- the first component differs from all the others. Instead, we prefer to take the even simpler set $\mathbb{Z}_\zeta^N$ as our range. As a range, $\mathbb{Z}_\zeta^N$ has the great advantage that it can be homogenously extended to the vector space, $\mathbb{Q}_\zeta^N$. Lastly, and most importantly, $\mathbb{Q}_\zeta^N$ is the minimum vector space on which the Fourier matrix acts as a linear transform in the case $R = \mathbb{Z}$.

More generally, we take the range of λ acting on $\mathrm{CIRC}(R)$ to be the set R_ζ^N. $\Lambda(R)$ is a subset of the set R_ζ^N. The set R_ζ^N is made into a ring by defining addition and multiplication componentwise. Thus, for $x, y \in R_\zeta^N$,

$$x + y \;:=\; (x_0 + y_0,\; x_1 + y_1,\; \ldots,\; x_{N-1} + y_{N-1})$$
$$xy \;:=\; (x_0 y_0,\; x_1 y_1,\; \ldots,\; x_{N-1} y_{N-1})$$

We can go further and allow scalar multiplication: for all $c \in R_\zeta$, $cx = (cx_0,\; cx_1,\; \ldots,\; cx_{N-1})$. This makes R_ζ^N into an algebra over R_ζ. If R_ζ is a field, then R_ζ^N will be a vector space over R_ζ. If R is not a field, we can still find a range for λ which is a vector space by taking instead the minimum field which contains R. Let Q be this field. Q is called the **quotient field** of R and can always be constructed when R is an integral domain (see [Kap1] or [Lang]). When Q exists, Q_ζ becomes a field extension of Q, and is therefore the quotient field of R_ζ. Thus, given a domain R we can construct a vector space Q_ζ^N which contains $\Lambda(R)$ which in a sense, is the smallest vector space which contains $\Lambda(R)$.

Usually, we take R_ζ^N as the range of λ. When it is important that the range be a vector space then we extend the range to Q_ζ^N. In either case, we refer to the range of λ as the **circulant eigenspace** or just the **eigenspace** of $\mathrm{CIRC}_N(R)$ (strictly it is the "eigenvaluespace", but this is too big a mouthful). In this nomenclature, an element of Q_ζ^N is an "eigenspace vector." The reader should beware of confusing this with the space of eigenvectors which is the space spanned by the common eigenvectors of the circulant matrices. (The circulant eigenvectors are the columns of the Fourier matrix.)

Let us now get to the corollaries of Theorem 1.6. In these corollaries, R is an integral domain, and Q is a field whose characteristic does not divide N, the order of the circulants under discussion.

1.8.1 **Corollary** $\lambda : \mathrm{CIRC}_N(Q_\zeta) \to Q_\zeta^N$ is an algebra isomorphism.

Proof. The map λ is a non-singular, linear map between vector spaces of the same dimension over the same field. Hence, λ is a vector space isomorphism.

By parts *(i)* and *(ii)* of the theorem, λ is equivalent to the map $A \mapsto \mathrm{Diag}^{-1}F^{-1}AF$ where Diag^{-1} is an inverse diagonal map which maps a matrix to the vector of its diagonal entries. The similarity transform $\alpha_F : A \mapsto F^{-1}AF$ is certainly a matrix ring isomorphism. It remains to prove that Diag^{-1} is a ring isomorphism when restricted to the set $\alpha_F(\mathrm{CIRC}_N(Q))$. But this is a set of diagonal matrices by the theorem. It is easy to verify that the map Diag when restricted to diagonal matrices is indeed a ring isomorphism provided addition and multiplication are taken componentwise in its domain. □

1.8.2 **Corollary** $\mathrm{CIRC}_N(Q_\zeta)$ is a commutative algebra over Q_ζ.

Proof. Q_ζ^N with componentwise addition and multiplication is a commutative algebra over Q_ζ. Apply the inverse eigenvalue map, λ^{-1}, and we see that $\mathrm{CIRC}_N(Q_\zeta) = \lambda^{-1}Q_\zeta^N$ is a commutative algebra over Q_ζ with matrix addition and multiplication. □

1.8.3 **Corollary** $\mathrm{CIRC}_N(R)$ is a commutative algebra over R.

Proof. Let $A, B \in \mathrm{CIRC}_N(R)$, and let $c \in R$. Then, clearly, $A + B$, AB, and cA are matrices with entries in R. By the previous corollary, these matrices are also in $\mathrm{CIRC}_N(Q_\zeta)$ where Q is the quotient field for R. Hence, they are in $\mathrm{CIRC}_N(R)$. □

1.8.4 **Corollary** $\lambda : \mathrm{CIRC}_N(R) \to \Lambda_N(R)$ is a ring isomorphism. □

One last, but important, corollary of Corollary 1.8.1 is the existence of the inverse map λ^{-1}.

1.8.5 **Corollary** Let $\mu \in \Lambda_N(R)$. Then, $\lambda^{-1}(\mu) = A$ is a circulant matrix given by

$$A_{i,j} \;=\; \frac{1}{N}\sum_{k=0}^{N-1} \mu_k \zeta^{(i-j)k}$$

Proof. One can verify the formula by direct substitution into the formula for λ. □

1.9 Circulant Vectors.

Recall that the circulant vector of a circulant matrix is simply the top row of the matrix. The question now naturally arises whether the circulant vectors also form a commutative algebra. Specifically, we ask:

> Can we define addition and multiplication on vectors in R^N so that the map
> $\mathrm{CIRC} : R^N \to \mathrm{CIRC}_N(R)$ is a ring isomorphism?

If we construct the circulant matrix with top row $a_0, a_1, \ldots, a_{N-1}$ and add it to the circulant matrix whose top row is $b_0, b_1, \ldots, b_{N-1}$, we should quite obviously get the circulant matrix whose top row is $a_0{+}b_0,\ a_1{+}b_1,\ \ldots,\ a_{N-1}{+}b_{N-1}$. So, we expect that addition be componentwise addition.

However, to agree with the matrix multiplication in $\mathrm{CIRC}_N(R)$, the multiplication of two circulant vectors a and b must be taken as the **convolution** $a * b$ which is defined by

$$(a * b)_i \;:=\; \sum_{j\in\mathbb{Z}_N} a_j b_{i-j} \qquad \forall a, b \in R^N,\ \forall i \in \mathbb{Z}_N$$

In the analysis of power series products, this is sometimes called the Cauchy product, but we shall always call it the convolution.

So the answer to our question is to take addition of circulant vectors as componentwise addition, and multiplication of circulant vectors as the convolution. We shall verify in Proposition 1.9.2 that these operations together with the usual scalar multiplication of vectors makes the circulant vectors into a commutative algebra, and, as required, it makes CIRC into an algebra isomorphism.

To distinguish the set of circulant vectors from the direct sum R^N, we shall denote the set of circulant N-vectors over the ring R by $\mathbf{circ}_N(R)$. Formally,

1.9.1 **Definition** $\mathbf{circ}_N(R)$ is the set of N-tuples over the ring R endowed with componentwise addition, scalar multiplication, and convolution as a product. It is called the **circulant space** of dimension N over the ring R. When R is an integral domain, $\mathbf{circ}(R)$ is sometimes called the **circulant vector space**.

We can now regard CIRC as a map, $\mathrm{CIRC} : \mathbf{circ}_N(R) \to \mathrm{CIRC}_N(R)$.

1.9.2 **Proposition** $\mathbf{circ}_N(R)$ is a ring, and $\mathrm{CIRC} : \mathbf{circ}_N(R) \to \mathrm{CIRC}_N(R)$ is a ring isomorphism.

Proof. We shall first prove that CIRC is an additive and multiplicative bijection. That $\mathbf{circ}_N(R)$ is a ring then follows trivially.

The map CIRC is a bijection because given any vector the algorithm of §1.2.1 shows how to construct the circulant matrix, and given any circulant matrix, its first row is the circulant vector. So it remains to show that CIRC is preserves sums and products.

Although the additivity of CIRC is quite obvious, we nevertheless present a proof since in this chapter the reader is still becoming acquainted with the terminology.

Let a and b be circulant vectors in $\mathbf{circ}_N(R)$.

$$(\mathrm{CIRC}(a+b))_{i,j} \;=\; \big((a+b)_{j-i}\big)_{i,j} \;=\; \big((a_{j-i}+b_{j-i}\big)_{i,j} \;=\; (\mathrm{CIRC}(a)+\mathrm{CIRC}(b))_{i,j}$$

Also $\mathrm{CIRC}(0) = 0$. This shows that CIRC is an additive map.

It is easy to see that the multiplicative identity in $\mathbf{circ}_N(R)$ (that is the identity of the convolution operator) is the vector $(1, 0, 0, \ldots, 0)$, and CIRC maps this vector to the identity matrix. Hence, CIRC maps the identity to the identity.

Again let a and b be circulant vectors in $\mathbf{circ}_N(R)$ and let $A = \mathrm{CIRC}(a)$, and $B = \mathrm{CIRC}(b)$ be their corresponding circulant matrices. We need to show that $\mathrm{CIRC}(a * b) = AB$.

$$(AB)_{i,j} \;=\; \left(\sum_{k\in\mathbb{Z}_N} A_{i,k}B_{k,j}\right)_{i,j} \;=\; \left(\sum_{k\in\mathbb{Z}_N} a_{k-i}b_{j-k}\right)_{i,j}$$

The top row in the matrix on the right is found by setting $i = 0$. It is the vector

$$\left(\sum_{k\in\mathbb{Z}_N} a_k b_{j-k}\right)_j \;=\; (a*b)_j \;\square$$

1.9.3 **Corollary** Let R be a complex domain then $\mathbf{circ}_N(R)$ is a commutative algebra over R.

Proof. $\mathrm{CIRC}_N(R)$ is a commutative algebra with identity. Now CIRC^{-1} is a ring isomorphism and is trivially linear over R. That is, $\mathrm{CIRC}^{-1}(rA) = r\mathrm{CIRC}^{-1}(A)$ for all ring elements r, and circulant matrices, A. Therefore, $\mathbf{circ}_N(R)$ must also be an R-algebra. $\square$

This corollary is true when R is any commutative ring as can easily be proved by direct calculation.

For various reasons it is awkward to use the "$*$" symbol to denote the ring product in circulant vector spaces. For one thing, it is an extra symbol that would appear repeatedly throughout the remainder of the text. For another, repeated convolutions such as $a * a * a$, appear often which we would like to write as a^3. Lastly, the symbol $\mathbf{circ}_N(R)$ means the ring R^N specifically with convolution. For these reasons, the asterisk will be dropped and the ring product in $\mathbf{circ}_N(R)$ will be denoted henceforth by juxtaposition. If this can lead to confusion, the asterisk will be reintroduced but only to remind the reader that the product in $\mathbf{circ}(R)$ is convolution, and not componentwise multiplication.

The connection between a circulant vector and its corresponding circulant matrix is unusually close: either one can very easily be converted to the other, and this conversion is an algebra isomorphism. Therefore, almost any question regarding one can be settled by reference to the other. It is our intention to use whichever provides the most convenient approach for a particular purpose. When we wish to be indiscrimate as to

whether we mean a circulant vector or its circulant matrix, we shall refer to one, both, or either simply as a circulant and we shall refer to the set of circulants as **circulant space**.

So far we have an eigenvalue map defined on circulant matrices but the equivalent map on circulant vectors is the notationally cumbersome $\lambda \circ \mathrm{CIRC} : \mathbf{circ}_N(R) \to R_\zeta^N$. In the spirit of keeping $\mathbf{circ}_N(R)$ and $\mathrm{CIRC}_N(R)$ on par, we shall allow λ to act on $\mathbf{circ}_N(R)$ directly. Thus, $\lambda : \mathbf{circ}_N(R) \to R_\zeta^N$ and is given by

$$\lambda(a) \;=\; \sum_{j \in \mathbb{Z}_N} a_j \zeta^{ij}$$

There will be little danger of confusion between the two uses of λ because we always use capital letters for matrices and lower-case letters for vectors, but if necessary, we can refer to one or the other by $\lambda|\mathbf{circ}$ or $\lambda|\mathrm{CIRC}$.

We are now in a position to appreciate our choice of range for λ. The map $\lambda|\mathbf{circ}_N(Q_\zeta)$ is a vector space endomorphism, $\lambda : Q_\zeta^N \to Q_\zeta^N$, and as such must have a matrix representation. The matrix is obviously $(\zeta^{ij})_{i,j} = \sqrt{N}F$. That is, $\lambda(a) = \sqrt{N}Fa$ where F is the Fourier matrix. The map $\lambda|\mathbf{circ}(\mathbb{C})$ when regarded as a vector space map on $\mathbb{C}^N$ is better known as the **discrete Fourier transform**. (See for instance, [Fla] or [Dav1].) As a simple application of this point of view of circulants as vectors we shall restate Corollary 1.8.5 in more natural language.

1.9.4 Corollary (The Fourier Inversion Formula)

Let $\mu \in \Lambda_N(R)$, then $\lambda = \lambda|_{\mathbf{circ}}$ has an inverse given by $a = \lambda^{-1}(\mu) \in \mathbf{circ}_N(R)$ where

$$a_i \;=\; \frac{1}{N} \sum_{j=0}^{N-1} \mu_j \zeta^{-ij} \qquad \square$$

1.10 Standard Bases for Circulant Space and Eigenspace.

The columns of the Fourier matrix are common eigenvectors of all the circulant matrices. These eigenvectors are

$$e_i \;:=\; \sqrt{N^{-1}}(1, \zeta^i, \zeta^{2i}, \ldots, \zeta^{(N-1)i}) \quad \text{for } i = 0, 1, 2, \ldots, N-1$$

Since the Fourier matrix is unitary, these vectors form an orthonormal basis for the eigenspace R_ζ^N. We shall adopt $e_0, e_1, \ldots, e_{N-1}$ as the standard basis for the eigenspace. But, what should be the standard basis for the circulant space? The natural choice would be circulant vectors which are mapped by λ to the standard basis for R_ζ^N. This basis would be $\lambda^{-1}(e_0), \lambda^{-1}(e_1), \ldots, \lambda^{-1}(e_{N-1})$. Although this would be a perfectly logical choice, there is better. For each $i \in \mathbb{Z}_N$, define $\bar{e}_i = \sqrt{N}e_i$. Hence,

$$\bar{e}_i \;=\; \left(1, \zeta^i, \zeta^{2i}, \ldots, \zeta^{(N-1)i}\right)$$

The set $\{\bar{e}_0, \bar{e}_1, \ldots, \bar{e}_{N-1}\}$ is multiplicatively closed. Recall that the product in the eigenspace is taken componentwise. So, $\bar{e}_i\bar{e}_j = \bar{e}_{i+j}$, and $\bar{e}_1^i = \bar{e}_i$. Of course, all subscripts are residues modulo N. Let $\vec{b}_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbf{circ}_N(R)$ where the 1 occurs in position i. It is very easy to check that $\lambda(\vec{b}_i) = (1, \zeta^i, \zeta^{2i}, \ldots, \zeta^{(N-1)i}) = \bar{e}_i$. Since λ is a ring isomorphism, the set of vectors $\{\vec{b}_0, \vec{b}_1, \ldots, \vec{b}_{N-1}\}$ must also be multiplicatively closed under convolution. Indeed, setting $\mathrm{u} := \vec{b}_1$, we see that $\vec{b}_i = \mathrm{u}^i$, the i^{th} power of u. Since the set $\{\bar{e}_0, \bar{e}_1, \ldots, \bar{e}_{N-1}\}$ is a basis for the eigenspace, the set $\{\mathrm{u}^0, \mathrm{u}, \mathrm{u}^2, \ldots, \mathrm{u}^{N-1}\}$ must be a basis for the circulant vectors. But this is obvious since the vectors u^i are just the usual unit orthonormal basis for R^N.

For these reasons, the best choice for a standard basis for the circulant vectors is the set of powers under convolution of the the circulant vector u, namely, $\{\mathrm{u}^0, \mathrm{u}, \mathrm{u}^2, \ldots, \mathrm{u}^{N-1}\}$. To simplify notation, we shall always identify the zeroth power of u with the identity of the base ring R. Thus, $\mathrm{u}^0 = 1 \in R$. In terms of the basis $1, \mathrm{u}, \mathrm{u}^2, \ldots, \mathrm{u}^{N-1}$, an arbitrary circulant vector $a = (a_0, a_1, \ldots, a_{N-1})$ has the expansion

$$a \;=\; a_0 + a_1\mathrm{u} + a_2\mathrm{u}^2 + \ldots + a_i\mathrm{u}^i + \ldots + a_{N-1}\mathrm{u}^{N-1}$$

Define $\mathrm{U} = \mathrm{CIRC}_N(\mathrm{u})$. Then,

$$\mathrm{U} \;=\; \mathrm{CIRC}_N(0,1,0,\ldots,0) \;=\; \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & & 0 \\ \vdots & \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

By the above, the powers of the U matrix form a natural basis for the circulant matrices. Thus, an arbitrary circulant matrix $A = \mathrm{CIRC}_N(a_0, a_1, \ldots, a_{N-1})$ can be expanded as

$$A \;=\; a_0 I + a_1\mathrm{U} + a_2\mathrm{U}^2 + \ldots + a_i\mathrm{U}^i + \ldots + a_{N-1}\mathrm{U}^{N-1}$$

where I is the $N \times N$ identity matrix.

Calculations involving the standard bases are merely the familiar polynomial additions and multiplications, but with all powers of u and U taken modulo N. For example, let $a, b \in \mathbf{circ}_5(\mathbb{Z})$ with $a = (1, 0, -3, 2, -1)$, and $b = (3, -1, 2, 0, 4)$. Then,

$$\begin{aligned} a \;&=\; 1 - 3\mathrm{u}^2 + 2\mathrm{u}^3 - \mathrm{u}^4 \\ b \;&=\; 3 - \mathrm{u} + 2\mathrm{u}^2 + 4\mathrm{u}^4 \\ \therefore\; ab \;&=\; \left(1 - 3\mathrm{u}^2 + 2\mathrm{u}^3 - \mathrm{u}^4\right)\left(3 - \mathrm{u} + 2\mathrm{u}^2 + 4\mathrm{u}^4\right) \\ &=\; 3 - \mathrm{u} - 7\mathrm{u}^2 + 9\mathrm{u}^3 - 7\mathrm{u}^4 + 5\mathrm{u}^5 - 14\mathrm{u}^6 + 8\mathrm{u}^7 - 4\mathrm{u}^8 \\ &=\; 8 - 15\mathrm{u} + \mathrm{u}^2 + 5\mathrm{u}^3 - 7\mathrm{u}^4 \end{aligned}$$

If the example had been the circulant matrices $A = \mathrm{CIRC}(1, 0, -3, 2, -1)$, and $B = \mathrm{CIRC}(3, -1, 2, 0, 4)$ rather than their circulant vectors, then the same calculation with U substituted throughout for u would have shown that $AB = \mathrm{CIRC}(8, -15, 1, 5, -7)$.

1.10.1 **The Representer Polynomial.** Given a circulant $a = \sum_{i=0}^{N-1} a_i\mathrm{u}^i$, define a polynomial $\vartheta(a)$ by $\vartheta(a)(x) := \sum_{i=0}^{N-1} a_i x^i$. It is clear that $\vartheta(a)(x)$ evaluates to the circulant vector $\mathbf{circ}(a)$ at $x = \mathrm{u}$. That is, $\vartheta(a)(\mathrm{u}) = a$. Similarly, $\vartheta(a)(\mathrm{U}) = A$, the circulant matrix. The polynomial $\vartheta(a)$ is called **representer polynomial** † for the circulant a. The above examples show that we can do calculations on circulants using their representer polynomials, and evaluate the resulting polynomial at u to obtain the result of the calculations on circulants.

To summarize,

1.10.2 **Definition**

(i) Let $\mathrm{u} := (0, 1, 0 \ldots, 0) \in \mathbf{circ}_N(R)$, and let $\mathrm{U} := \mathrm{CIRC}_N(0, 1, 0, \ldots, 0)$.
Then, $\{1, \mathrm{u}, \mathrm{u}^2, \ldots, \mathrm{u}^{N-1}\}$ is the standard orthonormal basis for $\mathbf{circ}_N(R)$.
and $\{I, \mathrm{U}, \mathrm{U}^2, \ldots, \mathrm{U}^{N-1}\}$ is the standard orthonormal basis for $\mathrm{CIRC}_N(R)$.

(ii) Let $e_i := \sqrt{N^{-1}}(1, \zeta^i, \zeta^{2i}, \ldots, \zeta^{(N-1)i}) = \sqrt{N^{-1}}\lambda(\mathrm{u}^i) = F\mathrm{u}^i$.
Then, $(e_0, e_1, \ldots, e_{N-1})$ is the standard orthonormal basis for R_ζ^N.

(iii) Let a be the circulant $\sum_{i=0}^{N-1} a_i\mathrm{u}^i$, then its representer polynomial is $\vartheta(a)(x) = \sum_{i=0}^{N-1} a_i x^i$.

† Some authors call it the Hall polynomial, e.g. [Ham], [Lam].

1.11 The Circulant Determinant.

One of the central questions on circulant matrices is the value of their determinants. Indeed, the study of circulants began as a study of their determinants. There are several formulæ for the determinant, each of which has its advantages and disadvantages. Because of frequent need to refer to the determinant, we give it its own symbol.

1.11.1 Definition Let $a \in R^N$ for some (commutative) ring R. Define

$$\Delta_N(a) \;:=\; \det \mathrm{CIRC}_N(a)$$

The last corollary of Theorem 1.6 is a formula for the determinant.

1.11.2 Corollary Let R_ζ be a complex domain, then $\Delta_N(a) = \prod_{j\in\mathbb{Z}_N} \sum_{i\in\mathbb{Z}_N} a_i\zeta^{ij}$

Proof. The determinant is the product of the eigenvalues. □

The above formula for the circulant determinant is an old result, as is the next formula, (for instance, see [Muir1].) but the formula in the next theorem is no less remarkable for that.

1.11.3 Theorem (The Resultant Formula) †

Let $a \in \mathbf{circ}_N(R)$ where R is an integral domain and let $A(x) = \sum_{i=0}^{N-1} a_i x^i \in R[x]$ be the representer polynomial for a of degree d with roots $\alpha_1, \alpha_2, \ldots, \alpha_d$ if necessary in some extension of R. Then,

$$\Delta_N(a) \quad = \quad a_d^N (-1)^{d(N-1)} \prod_{i=1}^{d} (1 - \alpha_i^N)$$

Proof. By Corollary 1.11.2,

$$\Delta_N \quad = \quad \prod_{i=0}^{N-1} \Big(\sum_{j=0}^{d} a_j \zeta^{ij} \Big) \quad = \quad \prod_{i=0}^{N-1} A(\zeta^i)$$

Decompose A into its linear factors, $A(x) = a_d \prod_{j=1}^{d} (x - \alpha_j)$, then

$$\begin{aligned}
\Delta_N &= a_d^N \prod_{i=0}^{N-1} \prod_{j=1}^{d} (\zeta^i - \alpha_j) \\
&= a_d^N \prod_{j=1}^{d} \prod_{i=0}^{N-1} (\zeta^i - \alpha_j) \\
&= a_d^N \zeta^{\frac{1}{2}dN(N-1)} \prod_{j=1}^{d} \prod_{i=0}^{N-1} (1 - \zeta^{-i}\alpha_j) \\
&= a_d^N (-1)^{d(N-1)} \prod_{j=1}^{d} \prod_{i=0}^{N-1} (1 - \zeta^{-i}\alpha_j)
\end{aligned}$$

The product $\prod_i (1 - \zeta^{-i}\alpha_j)$ can be evaluated. Consider the polynomial $f(x) = x^N - \alpha_j^N$. It has N roots given by $\{\alpha_j \zeta^{-i} \vdash i \in \mathbb{Z}_N\}$. Therefore, the product is $x^N - \alpha_j^N$ evaluated at $x = 1$. Substituting $x = 1$ gives the equation in the theorem statement. □

† This theorem is attributed to M.A.Stern by [FG].

There is another way of stating the theorem when the circulant has integer components. Suppose $R = \mathbb{Z}$ and that A is monic, that is, $a_d = 1$. Let the roots of A be $\alpha_1, \alpha_2, \ldots, \alpha_d$. The roots are a multiset of conjugate algebraic integers. Consequently, so is the multiset of their N^{th} powers, $\alpha_1^N, \alpha_2^N, \ldots, \alpha_d^N$, and this multiset generates a sub-domain of $\mathbb{Z}(\alpha_1, \alpha_2, \ldots, \alpha_d)$. Hence, the polynomial $A_N(x) = \prod_{i=1}^{d}(x - \alpha_i^N)$ is a polynomial in $\mathbb{Z}[x]$, and the formula of the theorem can be written as $\pm\Delta = A_N(1) =$ sum of coefficients of the polynomial A_N.

1.11.4 Circulant Determinant Expansions for $N \leq 6$.

The above formulas can be used to deduce the following expansions for the circulant determinant. (For $N \geq 7$ expansions are more easily obtained from formulæ which will be derived in Chapter 10.)

$$\Delta_1(a_0) = a_0$$

$$\Delta_2(a_0, a_1) = \begin{vmatrix} a_0 & a_1 \\ a_1 & a_0 \end{vmatrix} = a_0^2 - a_1^2 = (a_0 + a_1)(a_0 - a_1)$$

$$\begin{aligned} \Delta_3(a_0, a_1, a_2) &= \begin{vmatrix} a_0 & a_1 & a_2 \\ a_2 & a_0 & a_1 \\ a_1 & a_2 & a_0 \end{vmatrix} \\ &= a_0^3 + a_1^3 + a_2^3 - 3a_0a_1a_2 = (a_0 + a_1 + a_2)(a_0^2 + a_1^2 + a_2^2 - a_0a_1 - a_1a_2 - a_2a_0) \end{aligned}$$

$$\begin{aligned} \Delta_4(a_0, a_1, a_2, a_3) &= \begin{vmatrix} a_0 & a_1 & a_2 & a_3 \\ a_3 & a_0 & a_1 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_1 & a_2 & a_3 & a_0 \end{vmatrix} \\ &= a_0^4 - a_1^4 + a_2^4 - a_3^4 - 4(a_0^2a_1a_3 - a_0a_1^2a_2 + a_1a_2^2a_3 - a_0a_2a_3^2) - 2(a_0^2a_2^2 - a_1^2a_3^2) \\ &= (a_0 + a_1 + a_2 + a_3)(a_0 - a_1 + a_2 - a_3)\left((a_0 - a_2)^2 + (a_1 - a_3)^2\right) \end{aligned}$$

$$\begin{aligned} \Delta_5(a_0, a_1, a_2, a_3, a_4) &= \sum_i a_i^5 + 5\sum_i (a_i^2a_{i+1}^2a_{i+3} + a_i^2a_{i+1}a_{i+2}^2 - a_i^3a_{i+2}a_{i+3} - a_i^3a_{i+1}a_{i+4}) - 5a_0a_1a_2a_3a_4 \\ &= (a_0 + a_1 + a_2 + a_3 + a_4)P(a), \quad \text{where } P(a) \in \mathbb{Z}[a_0, a_1, \ldots, a_4] \end{aligned}$$

$$\begin{aligned} \Delta_6(a_0, a_1, a_2, a_3, a_4, a_5) &= \sum_i (-1)^i \Big\{ a_i^6 + 2a_i^3a_{i+2}^3 - 3a_i^4a_{i+3}^2 \\ &\qquad +6(a_i^3a_{i+1}^2a_{i+4} + a_i^3a_{i+2}a_{i+5}^2 - a_i^4a_{i+1}a_{i+5} - a_i^4a_{i+2}a_{i+4}) \\ &\qquad +12(a_i^3a_{i+1}a_{i+2}a_{i+3} + a_i^3a_{i+3}a_{i+4}a_{i+5}) \\ &\qquad -9a_i^2a_{i+1}^2a_{i+2}^2 \\ &\qquad -18a_i^2a_{i+2}^2a_{i+3}a_{i+5} \\ &\qquad \Big\} \\ &\qquad +9\big(a_0^2a_2^2a_4^2 - a_1^2a_3^2a_5^2\big) \\ &= L_0L_3L_2L_1 \end{aligned}$$

where

$$\begin{aligned} L_0 &= a_0 + a_1 + a_2 + a_3 + a_4 + a_5 = \lambda_0(a_0, a_1, a_2, a_3, a_4, a_5) \\ L_3 &= a_0 - a_1 + a_2 - a_3 + a_4 - a_5 = \lambda_3(a_0, a_1, a_2, a_3, a_4, a_5) \\ L_2 &= (a_0 + a_3)^2 + (a_1 + a_4)^2 + (a_2 + a_5)^2 - (a_0 + a_3)(a_1 + a_4) - (a_1 + a_4)(a_2 + a_5) - (a_2 + a_5)(a_0 + a_3) \\ &= \lambda_2\lambda_4 \\ L_1 &= -2\,a_0a_3 - 2\,a_1a_4 - 2\,a_2a_5 \quad - a_0a_2 - a_1a_3 - a_2a_4 - a_3a_5 - a_4a_0 - a_5a_1 \\ &\quad + a_0a_1 + a_1a_2 + a_2a_3 + a_3a_4 + a_4a_5 + a_5a_0 \quad + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_0^2 \\ &= \lambda_1\lambda_5 \end{aligned}$$

Chapter 2.
Circulant Matrices

This chapter places the circulants in the context of the familiar matrices. Later chapters will focus on circulants almost to the exclusion of the general matrix ring in which they reside. In keeping with this goal, the circulants in this chapter are matrices whereas in subsequent chapters circulants will usually be viewed as vectors with convolution as the ring product. We shall continue to assume that the underlying ring is an integral domain whose characteristic does not divide the order of any circulant matrix under discussion. We usually denote the circulant order by N, and the underlying ring by R. Thus, we are assuming that char $R \nmid N$.

We shall describe circulant matrices as a subring of $\mathrm{M}_N(R)$, or multiplicatively as a subgroup of $\mathrm{GL}_N(R)$. We shall start the study of ring homomorphisms on circulants by describing all those automorphisms on the circulant matrices over the reals and complex numbers which are given by similarity transformations by real and complex non-singular matrices. It will be shown that the similarity transformations (i.e. the inner-automorphisms of $\mathrm{GL}(R)$) account for all of the linear ring automorphisms on $\mathrm{CIRC}_N(R)$ for $R \subset \mathbb{C}$. We can therefore use the general group formula

$$\mathrm{Inn}_G(H) \;\approx\; \mathrm{Norm}_G(H)/C_G(H)$$

to estimate the isomorphism class of the linear automorphisms on circulants. In our case, $G = \mathrm{GL}_N(R)$ and $H = \mathrm{CIRC}_N(R)$. This leads us to calculate the centralizer and normalizer of the circulant matrices in the general linear group.

2.1 The Centralizer of the Circulant Matrices in the General Linear Group.

We begin by determining the centralizer of $\mathrm{CIRC}(R)$. This part proves to be easy to do and easy to state: The largest set of non-singular matrices which commute with the circulants is the circulants themselves.

2.1.1 Proposition Let R be a complex domain. $\mathrm{CIRC}_N(R)$ is its own centralizer in $\mathrm{M}_N(R)$.

Proof. Let A commute with every member of $\mathrm{CIRC}_N(R)$, and pick any $C \in \mathrm{CIRC}_N(R)$ which has distinct eigenvalues. Such a circulant matrix certainly exists, for instance, U, the generator of the standard basis for $\mathrm{CIRC}_N(R)$, has the N distinct eigenvalues $1, \zeta, \zeta^2, \ldots, \zeta^{N-1}$. Let $e_0, e_1, \ldots, e_{N-1}$ be the standard orthonormal basis for the eigenspace. These vectors are also the common eigenvectors of all circulant matrices. (See 1.10.) Multiply e_i by CA.

$$CAe_i \;=\; ACe_i \;=\; A\lambda_i e_i \;=\; \lambda_i A e_i$$

Therefore, Ae_i is an eigenvector of C with eigenvalue λ_i. Since the eigenvalues $\lambda_0, \lambda_1, \ldots, \lambda_{N-1}$ are distinct, this is possible only if Ae_i is a multiple of e_i for every $i \in \mathbb{Z}_N$ which means that A is diagonalized by F. By Theorem 1.5*(iii)*, A must be circulant. □

The above proof can easily be generalized to give the following corollary.

2.1.2 Corollary Let R be a complex domain, and let $A \in \mathrm{M}_N(R)$. Then, A is circulant iff it commutes with any circulant matrix having distinct eigenvalues. In particular, A is circulant iff it commutes with U. □

This corollary has a rather pretty corollary of its own which is the subject of the next exercise.

2.1.3 Exercise For a complex domain R, define a linear map $\tau : \mathrm{M}_n(R) \to \mathrm{M}_n(R)$ by $\tau(M) = n^{-1} \sum_{i=0}^{n-1} \mathrm{U}_n^{-i} M \mathrm{U}_n^i$. Then, τ is a projection map onto $\mathbf{circ}_n(R)$.

2.1.4 Exercise Let A be an $N \times N$ circulant matrix, let P_σ be the permutation matrix corresponding to a cyclic permutation σ on N objects, and let $\tilde{P}_\sigma = F^{-1} P_\sigma F$ where F is the Fourier matrix. Show that $(A\tilde{P}_\sigma)^N = \det(A) I$ where I is the identity matrix.

2.2 The Shift-circulant Matrices.

The next definition introduces a generalization of circulant matrices called the **shift-circulant** or *s*-**circulant** matrices. Like a circulant matrix, an *s*-circulant matrix is completely determined by its first row. Each subsequent row is the prior row rotated $s \pmod N$ columns to the right. The amount, s, that each row is rotated is called the **shift** of the matrix. Thus, a matrix of shift 1 is circulant; that is, 1-circulant means circulant.

2.2.1 Definition The Shift-circulant or *s*-circulant Matrices.

(i) $K_N(R) := \{A \in \mathrm{M}_N(r) \vdash \exists s \in \mathbb{Z}_N,\ A_{i,j} = A_{0,j-si},\ \forall i,j \in \mathbb{Z}_N\}$.

(ii) $K_N^*(R) := \mathrm{GL}_N(R) \cap K_N(R)$.

K_N is the set of all shift-circulant matrices and K_N^* is the set of non-singular shift-circulant matrices.

Example.

$$A = \begin{pmatrix} 1 & -2 & 3 & -4 & 5 \\ -4 & 5 & 1 & -2 & 3 \\ -2 & 3 & -4 & 5 & 1 \\ 5 & 1 & -2 & 3 & -4 \\ 3 & -4 & 5 & 1 & -2 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 3 & -1 & 1 & 4 \\ -1 & 1 & 4 & 0 & 3 \\ 4 & 0 & 3 & -1 & 1 \\ 3 & -1 & 1 & 4 & 0 \\ 1 & 4 & 0 & 3 & -1 \end{pmatrix}$$

$$\therefore AB = \begin{pmatrix} 7 & 25 & -4 & -3 & -4 \\ -4 & 7 & 25 & -4 & -3 \\ -3 & -4 & 7 & 25 & -4 \\ -4 & -3 & -4 & 7 & 25 \\ 25 & -4 & -3 & -4 & 7 \end{pmatrix}, \qquad BA = \begin{pmatrix} 7 & -3 & 25 & -4 & -4 \\ -4 & 7 & -3 & 25 & -4 \\ -4 & -4 & 7 & -3 & 25 \\ 25 & -4 & -4 & 7 & -3 \\ -3 & 25 & -4 & -4 & 7 \end{pmatrix}$$

The matrix A is a 2-circulant, B is a 3-circulant, and the products, AB and BA, are both 1-circulants, that is, circulant. As is clear from this example, shift-circulants do not necessarily commute.

2.2.2 Lemma If $A \in K_N^*(R)$ has shift s, then s is coprime to N.

Proof. Suppose $\gcd(s,N) = d > 1$, then the $(N/d)^{\text{th}}$ row equals the 0^{th} row. So the determinant is zero. □

2.2.3 Proposition $K_N^*(R)$ is a multiplicative group, and is non-abelian for $N > 2$. †

Proof. That it is non-abelian is obvious since for $N > 2$, $K_N^* \not\subset \mathrm{CIRC}_N$, and CIRC_N is its own centralizer. The case of $N = 2$ is semi-trivial, since $K_2^* \subset \mathrm{CIRC}_2$.

Let $A, B \in K_N$ with shifts of s, t respectively.

(i) Closure.

$$\begin{aligned} (AB)_{i,k} &= \sum_{j \in \mathbb{Z}_N} a_{j-si} b_{k-tj} \\ &= \sum_{j \in \mathbb{Z}_N} a_{j-s(i+1)} b_{k+st-tj} \quad \text{by } j \to j - s \\ &= (AB)_{i+1,\ k+st} \\ &\therefore AB \in K_N \text{ with shift } st \end{aligned}$$

(ii) Inverse

Suppose $A \in K_N^*$ with shift s. By the lemma, s is coprime to N, so $s^{-1} \bmod N$ exists. Choose any $B \in K_N^*$ with shift $s^{-1} \bmod N$. By part (i), AB has a shift of 1 and so is circulant. $\therefore F$ diagonalizes AB. $\therefore F^{-1}ABF = D$ where D is diagonal. Since A and $B \in K_N^*$, D is non-singular. $\therefore F^{-1}ABFD^{-1} = We$. $\therefore ABFD^{-1}F^{-1} = We$. By Theorem 1.6*(iii)*, $FD^{-1}F^{-1} \in \mathrm{CIRC}_N$ and by part (i), $BFD^{-1}F^{-1} \in K_N$, $\therefore A^{-1} = BFD^{-1}F^{-1} \in K_N$. □

† The assumption that char R does not divide N is crucial. For example, $K_3^*(\mathbb{Z}_3)$ is abelian.

The above proof can be easily adapted to show that the shift-circulant matrices are multiplicatively closed, that is, form a semigroup. However, the set of shift-circulants is not a ring since they are not additively closed.

The proof showed more than was stated. The implied results are in the next corollary.

2.2.4 Corollary

(i) If $A, B \in K_N$ have shift of s, t respectively, then AB has a shift of st.

(ii) If $A \in K_N^*$ then $A^{-1} = BC$ where $B \in K_N^*$ with $\text{shift}(B) = s^{-1}$ and is otherwise arbitrary, and C (depending on B) is circulant. □

2.2.5 Proposition

$K_N^*(R) \subset \text{Norm}\,\text{CIRC}_N(R)$, the normalizer of $\text{CIRC}_N(R)$ in $\text{GL}_N(R)$.

Proof. Let $\text{shift}(A) = s$. Let $C \in \text{CIRC}_N$. By the corollary Part *(ii)*, we have

$$ACA^{-1} = ACBC_1 \text{ where } \text{shift}(B) = s^{-1},\ \text{shift}(C_1) = 1$$

$$\begin{aligned} \therefore \text{shift}(ACA^{-1}) &= \text{shift}(A)\text{shift}(C)\text{shift}(B)\text{shift}(C_1) \\ &= s \times 1 \times s^{-1} \times 1 \\ &= 1 \ \square \end{aligned}$$

It is clear by now that the shift is a (multiplicative) group homomorphism from $K_N^*(R) \to \mathbb{Z}_N^*$. If $p \,|\, \phi(N)$ there will be a subgroup of order p in $\mathbb{Z}_N^*$ and so its inverse image will be a subgroup in K_N^*. For example, if $N > 2$, the non-singular anticirculant (shift $= -1$) and circulant matrices form a subgroup of K_N^*.

By Theorem 1.6*(iii)* the Fourier matrix diagonalizes a shift-circulant only if the shift is 1. Nevertheless, the Fourier matrix does bring the shift-circulant into a form where each row and column has exactly one non-zero element.

2.2.6 Proposition

Let F be the $N \times N$ Fourier matrix, and let $T \in K_N^*$ with $T_{i,j} = t_{j-si}$, say. Then, $(F^{-1}TF)_{i,h} = \delta_{i-sh}\lambda_h(t)$, and in particular, $\det T = \pm\Delta_N(t)$, the circulant determinant on the same vector.

Proof.

$$\begin{aligned} (F^{-1}TF)_{i,h} &= N^{-1} \sum_{j,k \in \mathbb{Z}_N} \zeta^{-ij} t_{k-sj} \zeta^{kh} \\ &= N^{-1} \sum_{j \in \mathbb{Z}_N} \sum_{m \in \mathbb{Z}_N} t_m \zeta^{(m+sj)h-ij} \quad \text{substituting } m = k - sj \\ &= N^{-1} \sum_{m \in \mathbb{Z}_N} t_m \zeta^{mh} \sum_{j \in \mathbb{Z}_N} \zeta^{j(sh-i)} \\ &= \delta_{i-sh} \sum_{m \in \mathbb{Z}_N} t_m \zeta^{mh} \\ &= \delta_{i-sh} \lambda_h(t) \end{aligned}$$

Since s is coprime to N, δ_{i-sh} has a single 1 in every column and row, and so $\lambda_h(t)$ occurs exactly once and shares no column or row with another. The determinant of T is therefore the product of $\lambda_h(t)$ to within sign. □

Of course, $\det T = \pm\Delta(t)$ is an easy consequence of the fact that T is just a row permutation of $\mathbf{circ}(t)$.

A matrix such as $F^{-1}TF$ in the proposition which has only one non-zero entry in every row and column is called a **monomial** matrix or a **PD-** matrix (for Permutation Diagonal). Note however, that the $F^{-1}TF$ matrix in the proposition is not a completely general PD-matrix: the non-zero entry on each row occurs a fixed displacement from the row above. It will transpire that the full normalizer of the circulants is in fact $FPF^{\dagger}$ where P is the set of PD-matrices (see Proposition 2.5.1).

One might imagine from the proposition that the shift-circulant shares not just its determinant but also its eigenvalues with the circulant having the same top row. This is not the case. Indeed, the eigenvalues of the shift-circulants of order N are not typically in the ring $R(\zeta_N)$. For a simple example, take the vector $t = (1, 0, 0, 0, 0)$ with a shift of 2.

$$T := \begin{pmatrix} 1, & 0, & 0, & 0, & 0 \\ 0, & 0, & 1, & 0, & 0 \\ 0, & 0, & 0, & 0, & 1 \\ 0, & 1, & 0, & 0, & 0 \\ 0, & 0, & 0, & 1, & 0 \end{pmatrix}$$

One easily verifies that $T^4 = I$, and that this is the minimum polynomial for T. Hence, the eigenvalues of T are the fourth roots of unity whereas the eigenvalues of $\mathrm{CIRC}(1, 0, 0, 0, 0)$, which is the 6×6 identity matrix are all 1.

2.4 Normalizer of CIRC_N

We have seen in Proposition 2.2.5 that the shift-circulants are a subgroup of the normalizer group of the circulants. They are not however the entire normalizer subgroup.

2.4.1 Assumptions and Notation.

(i) To characterize the full normalizer group of the circulants, we shall need a notation for the general permutation matrix. We shall denote it by P_σ where σ is any permutation on the symbols $\{0, 1, 2, \ldots, N-1\}$. We denote the set of all such permutations, the full symmetric group on N objects, by $\mathcal{S}_N$.

For all $\sigma \in \mathcal{S}_N$, let P_σ be the permutation matrix given by $(P_\sigma)_{i,j} = \delta_{i-\sigma(j)}$.

Let $u_0, u_1, \ldots, u_{N-1}$ be the unit coordinate vectors. Then, $P_\sigma : u_k \mapsto u_{\sigma(k)}$ which shows that P is a group homomorphism. That is, $P_\sigma P_\tau = P_{\sigma\tau}$.

(ii) In the next few lemmas and propositions, R and S are to represent rings which are subsumed by a larger ring (all integral domains with characteristic not dividing N). The containment by a larger ring guarantees that the ring operations on mixed elements from R and S make sense. This slightly strange requirement allows us to generalize theorems on the normalizer of the circulants to answer natural questions such as, for example, "What is the normalizer within the complex matrices of the real circulants."

(iii) We shall be discussing the normalizer in $\mathrm{GL}_N(S)$ of $\mathbf{circ}_N(R)$ where R and S, as we discussed, are integral domains subsumed in a larger domain.. The standard notation for the normalizer would be the unwieldy $\mathrm{Norm}_{\mathrm{GL}_N(S)} \mathrm{CIRC}_N(R)$. We shall simplify this to $\mathrm{Norm}_S \mathrm{CIRC}_N(R)$.

(iv) To reduce clutter in expressions involving similarity transformations with the Fourier matrix F, we shall denote $F^{-1}AF$ by $\widehat{A}$. Thus, if A is circulant, $\widehat{A} = \mathrm{Diag}\,(\lambda_0, \lambda_1, \ldots, \lambda_{N-1})$ where $\lambda_i = \lambda_i(A)$. Thus, for example, $\widehat{\mathrm{U}} = \mathrm{Diag}(1, \zeta, \zeta^2, \ldots, \zeta^{N-1})$.

Proposition 2.2.6 showed that if T is a shift-circulant, then $\widehat{T}$ is a PD-matrix (one with a single non-zero entry in every row and column). We also know that the shift-circulants normalize the circulants. So it is no surprise to find that the full normalizer of the circulants is in fact all matrices similar to monomial matrices under similarity transformation by F. This is proved in Proposition 2.5.1 below.

Recall that our standard basis for the circulant matrices are powers of the matrix $\mathrm{U} = \mathrm{CIRC}(0, 1, 0, \ldots, 0)$. The next lemma shows that D is in the normalizer of the circulants if and only if U^D is circulant.

2.4.2 Lemma $D \in \mathrm{Norm}_S \mathrm{CIRC}_N(R) \Leftrightarrow D^{-1}\mathrm{U}D \in \mathrm{CIRC}_N(R)$.

Proof. $D^{-1}\mathrm{U}D \in \mathrm{CIRC}_N(R) \Leftrightarrow D^{-1}\mathrm{U}^r D \in \mathrm{CIRC}_N(R) \Leftrightarrow D^{-1}\left(\sum_{r\in\mathbb{Z}_N} a_r \mathrm{U}^r\right) D \in \mathrm{CIRC}_N(R)$. □

2.5.1 **Proposition** A necessary and sufficient condition for $T \in \mathrm{Norm}_S \,\mathrm{CIRC}_N(R_\zeta)$ is that $\widehat{T} = P_\sigma \mathrm{Diag}(\theta)$ for some permutation $\sigma \in \mathcal{S}_N$ and some diagonal matrix $\mathrm{Diag}(\theta_0, \theta_1, \ldots, \theta_{N-1}) \in \mathrm{GL}_N(S)$.

Proof. By the lemma, the proposition need only be proved for U.

Assume $T \in \mathrm{Norm}_S \,\mathrm{CIRC}_N(R)$, then $T^{-1}\mathrm{U}T = C$ for some circulant matrix C. $\therefore \mathrm{U}Te_i = TCe_i = \lambda_i(C)Te_i$. So Te_i is an eigenvector of U. But, the eigenvectors of U are $\{e_0, e_1, \ldots, e_{N-1}\}$. Hence, T maps the set of eigenvectors $\{e_0, e_1, \ldots, e_{N-1}\}$ to itself, possibly with scalar multipliers in S. Since T is non-singular, T must permute $\{e_0, e_1, \ldots, e_{N-1}\}$ within scalar multipliers. Let the permutation be σ, and let the scalar multipliers be $\{\theta_0, \theta_1, \ldots, \theta_{N-1}\} \subset S$. Then, for all j,

$$Te_j = \theta_j e_{\sigma(j)} \tag{1}$$

This says that T maps the eigenspace, columnar, basis vector e_j to θ_j times the columnar basis vector $e_{\sigma(j)}$. So the matrix representation of T in the eigenspace basis, that is $\widehat{T}$, is given by

$$(\widehat{T})_{i,j} = (\theta_j e_{\sigma(j)})_i = \theta_j e_{i-\sigma(j)}$$
$$\therefore \widehat{T} = P_\sigma \mathrm{Diag}(\theta_0, \theta_1, \ldots, \theta_{N-1})$$

QED Necessity.

Let $\widehat{T} = P_\sigma \mathrm{Diag}(\theta)$. Reversing the above proof of sufficiency, we arrive back at equation (1). Thence,

$$\begin{aligned} \therefore T^{-1}\mathrm{U}Te_j &= T^{-1}\theta_j \mathrm{U}e_{\sigma(j)} = T^{-1}\theta_j \zeta^{\sigma(j)} e_{\sigma(j)} = \theta_j \zeta^{\sigma(j)} T^{-1} e_{\sigma(j)} \\ &= \theta_j \zeta^{\sigma(j)} \theta_j^{-1} e_j \qquad \text{applying (1) again} \\ \therefore T^{-1}\mathrm{U}Te_j &= \zeta^{\sigma(j)} e_j \end{aligned} \tag{2}$$

Therefore, e_j is an eigenvector of $T^{-1}\mathrm{U}T$, $\forall j$, and so, the matrix constructed from these eigenvectors, one whose every j^{th} column is e_j, is a diagonalizing matrix for $T^{-1}\mathrm{U}T$. But this diagonalizing matrix is F. Therefore, by Theorem 1.5*(iii)*, $T^{-1}\mathrm{U}T \in \mathrm{CIRC}_N(R_\zeta)$.
QED Sufficiency. □

The PD matrices have interesting algebraic properties beyond those discussed here. For more details on PD-matrices and their use in investigating s-circulants see [Dav3]. The matrices of interest to us are not immediately the PD-matrices but the PD inversely transformed by the Fourier matrix, $F\mathrm{PD}F^{-1}$. Hence, the following definition.

2.5.2 **Definition** For any permutation $\sigma \in \mathcal{S}_N$, and vector $\theta \in \mathbb{C}^N$, define $\widehat{P}(\sigma, \theta) := FP_\sigma \mathrm{Diag}(\theta)F^{-1}$. In the special case when $\mathrm{Diag}(\theta)$ is the identity matrix, we shall write $\widehat{P}_\sigma$. Thus, $\widehat{P}_\sigma = FP_\sigma F^{-1}$.

We shall show that the precise values appearing in the diagonal matrix are irrelevant to automorphisms on circulants; hence, in typifying automorphisms, we can actually take the diagonal matrix to be the identity.

Note that the proof of Proposition 2.5.1 fails to characterize the normalizer of $\mathbf{circ}_N(R)$ because the matrix $T^{-1}\mathrm{U}T$ in general has entries in R_ζ not R. However, Proposition 2.5.1 does determine the normalizer of any subset of $\mathbf{circ}(R_\zeta)$ which is defined by the value of the determinant such as for instance, the non-singular complex circulant matrices. This is because the determinant is unaffected by similarity transformations. That is, $\det A = \det(T^{-1}AT)$. This gives us an easy corollary.

2.5.3 **Corollary** Let $\widehat{P}(\mathcal{S}_N, R^*)$ be the set of all $\widehat{P}(\sigma, \theta)$ where $\sigma \in \mathcal{S}_N$, and $\theta \in R_*^N$ where $R_* = R - \{0\} \subset \mathbb{C}$ --i.e. θ has no zero components. Then,

(i) $\widehat{P}(\mathcal{S}_N, R^*)$ is the normalizer in GL_N of $\mathrm{GL}_N(\mathbb{C}) \cap \mathrm{CIRC}_N(\mathbb{C})$ and $\mathrm{SL}_N(\mathbb{C}) \cap \mathrm{CIRC}_N(\mathbb{C})$, and

(ii) $\widehat{P}(\mathcal{S}_N, R^*)$ is a multiplicative group.

Proof. Part *(i)* is just Proposition 2.5.1 with Definition 2.5.2, and part *(ii)* follows from *(i)* by fact that the normalizer of any set is a group. □

The group product in $\widehat{P}(\mathcal{S}_N, R)$ is not quite as simple as the composition of permutations. There is a twist in the product whenever the matrix on the right of the product is not circulant. Hence, even an abelian group of permutations does not define an abelian subgroup of $\widehat{P}(\mathcal{S}_N, R)$. This is shown next.

2.5.4 **Proposition**
(i) $\widehat{P}(\sigma,\theta)\widehat{P}(\tau,\phi) = \widehat{P}(\sigma\tau,\beta)$ where $\beta_i = \theta_{\tau(i)}\phi_i$.

(ii) $\widehat{P}(\sigma,\theta)$ is unitary iff $|\theta_i| = 1,\ \forall i$.

Proof.
(i) We can determine the product rule by calculating the product $F^{-1}\widehat{P}(\sigma,\theta)\widehat{P}(\tau,\phi)F$ which by definition equals $P_\sigma \mathrm{Diag}(\theta) P_\tau \mathrm{Diag}(\phi)$.

$$\begin{aligned}
\left(P_\sigma \mathrm{Diag}(\theta) P_\tau \mathrm{Diag}(\phi)\right)_{i,m} &= \sum_{j,k,l} \delta_{i-\sigma(j)}\delta_{j-k}\theta_k\delta_{k-\tau(l)}\delta_{l-m}\phi_m \\
&= \sum_{k} \delta_{i-\sigma(k)}\theta_k\delta_{k-\tau(m)}\phi_m \\
&= \delta_{i-\sigma\tau(m)}\theta_{\tau(m)}\phi_m \\
&= \left(P_{\sigma\tau}\mathrm{Diag}(\beta)\right)_{i,m} \qquad \text{where } \beta_m = \theta_{\tau(m)}\phi_m \text{ as required.}
\end{aligned}$$

QED *(i)*.

(ii) $P_\sigma^\dagger = P_\sigma^{-1}$ for all permutation matrices P_σ. Hence, $\widehat{P}(\sigma,\theta)^\dagger = \widehat{P}(\sigma^{-1},\bar{\theta}) = \widehat{P}(\sigma,\theta)^{-1}$ iff $\theta\bar{\theta} = 1$. □

Let $\widehat{P}$ be any member of $\widehat{P}(\mathcal{S}_N, \mathbb{C})$, and let $C = \widehat{P}^{-1}\mathrm{U}\widehat{P}$. Then, C, of course, is circulant. As in the proof of Proposition 2.5.1, we see that $\mathrm{U}\widehat{P}_\sigma e_i = \lambda_i(C)\widehat{P}_\sigma e_i$. which shows that the eigenvalues of C is a permutation of the eigenvalues of U. Since $P_\sigma e_i = e_\sigma(i)$, the permutation of the eigenvalues of U is none other than σ. One can easily generalize this to any matrix of the form $C = \widehat{P}^{-1}B\widehat{P}$ where B is any circulant matrix. If we do so we will find that the eigenvalues of C are again just of those of B permuted by σ. This strongly suggests that the automorphism $B \to \widehat{P}^{-1}B\widehat{P}$ where $\widehat{P} = \widehat{P}(\sigma,\theta)$ is independent of θ.

For any non-singular matrix A, let $\iota A : \mathrm{M}_N \to \mathrm{M}_N$ denote the similarity transformation,

$$\iota A : X \mapsto A^{-1}XA$$

2.5.5 **Lemma** Let $\widehat{P} = \widehat{P}(\sigma,\theta)$ then the automorphism $\iota\widehat{P} : \mathrm{CIRC}_N \to \mathrm{CIRC}_N$ is independent of θ.

Proof. Let $C = (\iota\widehat{P})(\mathrm{U})$. From equation (2) and the above remarks, $\lambda(C)$ and hence C is independent of θ. So, $(\iota\widehat{P})(\mathrm{U})$ is independent of θ, and so is U. Hence, $(\iota\widehat{P})\left(\mathrm{U}^i\right)$ is independent of θ. Therefore, $\iota\widehat{P}$ is independent of θ on CIRC_N. □

However, the vector θ is not wholly arbitrary; it may not contain a zero component otherwise $\widehat{P}(\sigma,\theta)$ would be singular.

Because of Lemma 2.5.5 and Proposition 2.5.4, in dealing with inner-automorphism, $\iota\widehat{P}$, we can take θ as the vector $(1,1,\ldots,1)$ which is tantamount to setting the diagonal matrix in the PD-matrix to be the identity. That is, we can always take $\hat{P}(\sigma,\theta) = \widehat{P}_\sigma$ in similarity transformations on circulants. Hence, the automorphisms of $\mathrm{CIRC}_N(R)$ induced by inner-automorphisms of $\mathrm{GL}_N(R)$ are just permutations of the eigenvalues. The question now is whether distinct permutations lead to distinct automorphisms. But, the answer to this question is obvious. Any subalgebra of $\mathrm{CIRC}(R)$ which contains a matrix with N distinct eigenvalues must be transformed non-trivially by $\hat{P}_\sigma$ unless σ is the identity permutation. This finally gives us the complete characterization of the similarity-induced automorphisms on circulant matrices over rings which contain ζ.

2.5.6 **Proposition** The group of distinct automorphisms of $\mathrm{CIRC}_N(R_\zeta)$ generated by inner automorphisms of $\mathrm{GL}_N(R_\zeta)$ is identical to the group of permutation matrices acting on $\lambda\mathrm{CIRC}_N(R_\zeta)$. In particular, the group is isomorphic to $\mathcal{S}_N$.

2.6 The Linear Automorphisms of $\mathrm{CIRC}_N(R_\zeta)$.

We have seen that all automorphisms on circulants over R_ζ arising from similarity transforms are essentially just permutations of the circulants' eigenvalues. This must apply to any circulant ring. The only difference when $\zeta \notin R$ will be that some eigenvalue permutations will map a circulant into a circulant matrix with some entries not in R. It is an opportune moment to consider what type of automorphisms we might be interested in, regardless of the base ring. We shall argue that we are interested only in linear homomorphisms, and in linear automorphisms in particular.

First we define what we mean by linear. Informally, a homomorphism on $\mathrm{CIRC}_N(R)$ is linear when the homomorphism is a trivial homomorphism on the base ring, R. If the homomorphism maps $\mathrm{CIRC}(R)$ to another algebra over the ring R then the definition of linear is simple: α is linear iff $\alpha(rA) = r\alpha(A)$, $\forall A \in \mathrm{CIRC}(R)$, $\forall r \in R$. Homomorphisms which have a non-trivial action on the base ring are certainly of interest to general ring theory. But, in a study of circulants, as opposed to general ring theory, the description of the linear circulant homomorphisms must be paramount, and so the actions of homomorphisms on general rings R are left to other texts.

The formal definition of linear depends on the following fact: Given R is a subring of S and that $A(R)$ is an R-algebra, then there exists an S-algebra $A(S)$ which contains $A(R)$. Informally, this can be seen by assuming that $A(R)$ has an R-basis $\{v_1, v_2, \ldots, v_n\}$, say. Then, $A(S)$ consists of linear sums $s_1v_1 + \cdots + s_nv_n$ where $s_i \in S$. (Formally, $A(S)$ is identified with the tensor product $S \otimes_R A(R)$.) In the case of circulant algebras, $\mathrm{CIRC}_N(S)$ is defined by Definition 1.2.2 for all rings S, and indeed, it easy to see that $\mathrm{CIRC}_N(S)$ can be constructed as explained above from $\mathrm{CIRC}_N(R)$, for instance, by taking the standard basis $\{I,\ \mathrm{U},\ \mathrm{U}^2,\ \ldots,\ \mathrm{U}^{N-1}\}$ for $\mathrm{CIRC}_N(R)$ and turning it into an S-basis for $\mathrm{CIRC}_N(S)$.

2.6.1 **Definition** Let α be a ring homomorphism from $\mathrm{CIRC}_N(R)$ to an R-algebra, $A(R)$.

(i) α is said to be R-linear if $\alpha(ra) = r\alpha(a)$ for all $r \in R$ and all $a \in \mathrm{CIRC}_N(R)$.

(ii) If R is a subring of S then α is said to be S-linear if there exists an extension $\bar{\alpha}$ of α which is S-linear, and maps $\mathrm{CIRC}_N(S)$ to the S-algebra $A(S)$.

(iii) α is said to be **linear** if α is S-linear for all rings S containing (or equal to) R.

An R-linear ring homomorphism on $\mathrm{CIRC}_N(R)$ is an algebra homomorphism on the algebra of circulant matrices over the base ring R. If the homomorphism maps the identity to the identity then it must map rI to $r1_A$ for all $r \in R$ where 1_A is the identity in $A(R)$. Conversely, any homomorphism which maps every rI to $r1_A$ must be R-linear.

Suppose $\alpha : \mathrm{CIRC}_N(R) \to A(R)$ is an algebra homomorphism, that is, an R-linear ring homomorphism. Let R be a subring of S. Then, α can be extended to $\bar{\alpha} : \mathrm{CIRC}_N(S) \to A(S)$ by defining

$$\bar{\alpha}\left(\sum_{i\in\mathbb{Z}_N} a_i\mathrm{U}^i\right) := \sum_{i\in\mathbb{Z}_N} a_i\alpha(\mathrm{U})^i$$

From this one sees first that $\alpha : \mathrm{CIRC}_N(R) \to A(R)$ is R-linear iff it is linear, and secondly that a linear map is completely specified by its action on U. A good example of an R-linear homomorphism on $\mathrm{CIRC}_N(R)$ is the eigenvalue map, λ.

It is quite easy to invent homomorphisms on $\mathrm{CIRC}_N(R)$ which are not R-linear. For instance, let $R = \mathbb{Q}(\sqrt{2})$ and let α be any linear automorphism on $\mathrm{CIRC}_N(R)$. Define β to be the field automorphism on R given by $\beta(r + s\sqrt{2}) = r - s\sqrt{2}$, $\forall r, s \in \mathbb{Q}$. Finally, define $\gamma : \mathrm{CIRC}_N(R) \to \mathrm{CIRC}_N(R)$ by $\gamma\mathrm{CIRC}_N(a_0, a_1, \ldots, a_{N-1}) = \alpha\mathrm{CIRC}_N(\beta(a_0), \beta(a_1), \ldots, \beta(a_{N-1}))$. The map γ is a ring automorphism but is not linear. For instance, take α as the identity map, then $\gamma((1 + \sqrt{2})C) = (1 - \sqrt{2})\gamma C$.

The proposition which follows essentially proves that the similarity transformations which we have already characterized for $R = \mathbb{C}$ account for all the linear automorphisms on $\mathrm{CIRC}_N(R)$. In this proposition, we introduce a notation which will be used frequently. Given any circulant automorphism α, let $\tilde{\alpha}$ denote the map $\lambda\alpha\lambda^{-1}$. The map $\tilde{\alpha}$ is the automorphism on the eigenspace, $\tilde{\alpha} : R_\zeta^N \to R_\zeta^N$ which agrees with the homomorphism α on the circulant space.

2.6.2 **Theorem** Let R be a complex domain. Let $\alpha : \mathrm{CIRC}_N(R) \to \mathrm{CIRC}_N(R)$ be a linear ring automorphism. Then, α is a similarity transformation, and $\tilde{\alpha} : \lambda \mapsto P_\sigma\lambda$ for some permutation $\sigma \in \mathcal{S}_N$.

Proof. The assumption of linearity implies that α can be extended through linearity to a ring homomorphism $\bar{\alpha} : \mathrm{CIRC}_N(Q) \to \mathrm{CIRC}_N(Q)$ where Q is a subfield of $\mathbb{C}$ which includes R and ζ. We shall drop the bar over $\bar{\alpha}$ and regard α as the map on $\mathbf{circ}_N(Q)$.

We shall temporarily regard the circulants as vectors with convolution as the ring product, and, as usual, componentwise multiplication as the ring product in the eigenspace. The homomorphism $\alpha : \mathbf{circ}_N(Q) \to \mathbf{circ}_N(Q)$ induces the homomorphism $\tilde{\alpha} : Q^N \to Q^N$ on the eigenspace. Since α is linear so is $\tilde{\alpha}$. Therefore $\tilde{\alpha}$ is a vector space map and so can be represented as a matrix transformation. Let the map be $\tilde{\alpha} : \lambda \mapsto M\lambda$ where $M \in \mathrm{M}_N(Q)$. Since this is also a multiplicative map, for all $\lambda, \mu \in Q^N$, we must have

$$M(\lambda\mu) \;=\; (M\lambda)(M\mu)$$

where the vector product is componentwise multiplication. Writing this equation out in terms of components, we get

$$\sum_j m_{i,j}\lambda_j\mu_j \;=\; \sum_j m_{i,j}\lambda_j \sum_k m_{i,k}\mu_k \;=\; \sum_{j,k} m_{i,j}m_{i,k}\lambda_j\mu_k \tag{8}$$

where all summations are over the set $\mathbb{Z}_N$.

Since $\mu \in Q^N$ is arbitrary, we can pick $\mu_j = \delta_{j-s}$ for any $s \in \mathbb{Z}_N$. With this setting, equation (8) becomes

$$\sum_j m_{i,j}\lambda_j\delta_{j-s} \;=\; m_{i,s}\lambda_s \;=\; \sum_{j,k} m_{i,j}m_{i,k}\lambda_j\delta_{s-k} \;=\; m_{i,s}\sum_j m_{i,j}\lambda_j$$

$$\therefore\; m_{i,s}\lambda_s \;=\; m_{i,s}\sum_j m_{i,j}\lambda_j$$

Suppose $m_{i,s} \neq 0$. Cancelling $m_{i,s}$, we get the equation

$$\lambda_s \;=\; \sum_j m_{i,j}\lambda_j \;=\; m_{i,s}\lambda_s + \sum_{j\neq s} m_{i,j}\lambda_j$$

Since λ is also arbitrary, we can pick $\lambda_i = \delta_{i-s}$ which forces $m_{i,s} = 1$. Therefore, $m_{i,s} = 0$ or 1.

Now pick $\mu_j = 1,\ \forall j$, then equation (8) gives

$$\sum_j m_{i,j}\lambda_j \;=\; \sum_{j,k} m_{i,j}m_{i,k}\lambda_j \;=\; \left(\sum_k m_{i,k}\right)\left(\sum_j m_{i,j}\lambda_j\right)$$

Again, λ is arbitrary, so we can deduce that either M is the zero matrix or $\sum_k m_{i,k} = 1$. But the first possibility contradicts the bijectivity of α. Therefore, the sum of every column in M equals 1. This condition together with the condition $m_{i,j} = 0$ or 1, and the fact that α, hence $\tilde{\alpha}$ are bijective implies that M is a permutation matrix. That is, $\tilde{\alpha}$ permutes the components of the eigenvalue vector. The proposition now follows by Proposition 2.5.6. □

2.6.3 **Corollary** The group of linear ring automorphisms on $\mathrm{CIRC}_N(\mathbb{C})$ is induced by the group of permutations of the circulant eigenvalues. □

2.7 The Linear Automorphisms of $\mathrm{CIRC}_N(\mathbb{R})$.

We shall now characterize $\mathrm{Norm}\,\mathrm{CIRC}(R)$ where R no longer necessarily contains ζ.

2.7.1 Proposition $\widehat{P}_\sigma \in \mathrm{Norm}\,\mathrm{CIRC}_N(R)$ iff $\widehat{P}_\sigma \in \mathrm{M}_N(N^{-1}R)$.

Proof. Let $B(k) := \widehat{P}_\sigma^{-1}\mathrm{U}^k\widehat{P}_\sigma$ By equation (6) in Proposition 2.5.1, the eigenvalues of $B(k)$ are $\lambda_i = \zeta^{k\sigma(i)}$. So, $\widehat{B}_{i,j}(k) = \zeta^{k\sigma(i)}\delta_{i-j}$. Applying the inverse eigenvalue map, λ^{-1},

$$NB_{i,l}(k) = \sum_{j,k}\zeta^{ij}\zeta^{k\sigma(j)}\delta_{j-k}\zeta^{-kl} = \sum_j \zeta^{j(i-l)+k\sigma(j)} \tag{1}$$

On the other hand, $\widehat{P}_\sigma = FP_\sigma F^{-1}$.

$$\therefore (\widehat{P}_\sigma)_{i,l} = N^{-1}\sum_{j,k}\zeta^{ij}\delta_{\sigma(j)-k}\zeta^{kl} = N^{-1}\sum_j \zeta^{ij+l\sigma(j)} \tag{2}$$

Therefore,

$$\begin{aligned} P_\sigma \in \mathrm{Norm}\,\mathrm{CIRC}_N(R) &\Leftrightarrow B(k) \in \mathrm{CIRC}_N(R), \quad \forall k \in \mathbb{Z}_N \\ &\Leftrightarrow N\sum_j \zeta^{jr+k\sigma(j)} \in R, \quad \forall r,k \in R, \quad \text{by (1)} \\ &\Leftrightarrow N\widehat{P}_\sigma \in \mathrm{M}_N(R), \quad \text{by (2)} \ \square \end{aligned}$$

Hence, if $F \subset E$ are fields, then the restriction of an inner automorphism of $\mathrm{CIRC}(E)$ to $\mathrm{CIRC}(F)$ is an inner automorphism on $\mathrm{CIRC}(F)$ - - we get no more automorphisms on $\mathrm{CIRC}(F)$ by extending the field to E.

One easy application of the above proposition is to show that the linear automorphism group of $\mathrm{CIRC}_N(\mathbb{R})$ is identical to $\{\widehat{P}_\sigma \vdash \sigma(-i) \equiv -\sigma(i) \pmod N\}$. These are the permutations of the eigenvalues which are odd functions on $\mathbb{Z}_N$. From this we get the next theorem.

2.7.2 Theorem The number of distinct linear automorphisms of $\mathrm{CIRC}_N(\mathbb{R})$ generated by $\mathrm{GL}_N(\mathbb{C})$ is $(\frac{1}{2}(N-1))!$ for N odd and $2\,(\frac{1}{2}N-1)!$ for N even. The group of these automorphisms is isomorphic to the subgroup J_N of $\mathcal{S}_N$ consisting of all those permutations which satisfy $\sigma(-i) = -\sigma(i)$, for all $i \in \mathbb{Z}_N$.

Proof. As discussed above, the set $\{\widehat{P}_\sigma \vdash \sigma \in J_N\}$ is the normalizer of $\mathrm{CIRC}_N(\mathbb{R})$. Since $\alpha_{\widehat{P}_\sigma} = \alpha_{\widehat{P}_\tau} \Leftrightarrow \sigma = \tau$, the automorphism group of $\mathrm{Norm}\,\mathrm{CIRC}_N(\mathbb{R})$ is isomorphic to J_N.

Case I N odd.

The permutation σ which is an odd function on $\mathbb{Z}_N$ is fully specified when one specifies $\sigma(0)$, $\sigma(1)$,..., $\sigma\,(\frac{1}{2}(N-1))$. The remaining values are completely determined by previous choices and the constraint $\sigma(-i) = -\sigma(i)$. The number of free choices is therefore $(\frac{1}{2}(N-1))!$ **QED** Case I.

Case II N even.

In this case, both $\sigma(0)$ and $\sigma\,(\frac{1}{2}N)$ are constrained to the set $\{0, \frac{1}{2}N\}$. Consequently, there are two choices for $\sigma(0)$ and this determines the value of $\sigma\,(\frac{1}{2}N)$.

As in case I, the values of σ on $1, 2, \ldots, \frac{1}{2}N-1$ is free and thereafter all values are determined. Therefore, the number of free choices is $2 \times (\frac{1}{2}N-1)!$

Lastly, since all linear automorphisms are similarity transforms, it follows that the above characterizes all linear ring automorphisms on $\mathrm{CIRC}_N(\mathbb{R})$. $\square$

The theorem can be stated more intuitively. Every linear automorphism of $\mathrm{CIRC}(\mathbb{R})$ is a permutation of the eigenvalues which commutes with complex conjugation.

According to Lemma 2.7.1 if $\widehat{P}_\sigma \in \mathrm{Norm}\,\mathrm{CIRC}_N(\mathbb{R})$ then $\widehat{P}_\sigma$ is a real matrix. Consequently, all the automorphisms of $\mathrm{CIRC}_N(\mathbb{R})$ generated by $\mathrm{GL}_N(\mathbb{C})$ are also generated by $\mathrm{GL}_N(\mathbb{R})$. We get no extra automorphisms by extending the field. Since J_N is a subgroup of $\mathcal{S}_N$, it follows that $\mathrm{Inn}(\mathrm{CIRC}_N(\mathbb{R}))$ is a subgroup of $\mathrm{Inn}(\mathrm{CIRC}_N(\mathbb{C}))$. However, except for $N \leq 2$, $\mathrm{Inn}(\mathrm{CIRC}_N(\mathbb{R}))$ is not normal in $\mathrm{Inn}(\mathrm{CIRC}_N(\mathbb{C}))$. One can for instance easily show that J_N is not normal in $\mathcal{S}_N$ when $N > 2$.

2.8 **The Galois Group and Linear Automorphism of** $\mathrm{CIRC}_N(R)$**.**

We give a preview here of the rôle played by the Galois group of cyclotomic field extensions in subsequent sections. (See Appendix A for a brief overview of cyclotomic theory).

Let R be a complex domain, and let Q be its quotient field. Then, Q_ζ is a cyclotomic extension of Q. Let G be the Galois group for this extension. Concretely, G is the set of field automorphisms of Q_ζ which leave Q fixed. The orbits of G acting on Q_ζ is a partitioning of Q_ζ. Similarity transformation by the matrix $\widehat{P}_\sigma$ is an automorphism of $\mathrm{CIRC}_N(R)$ if and only if the map $\zeta^i \to \zeta^{\sigma(i)}$ maps G-orbits into G-orbits. (Note that the roots of unity is a union of G-orbits.)

For example, take $R = \mathbb{R}$, then $Q = \mathbb{R}$ also, and the Galois group is generated by the map $x+\imath y \leftrightarrow x-\imath y$. Hence, orbits under G consists of the singleton sets of all real numbers and all sets of pairs of conjugate complex numbers. Let $\sigma(i) = j$. By the condition given above for $\widehat{P}_\sigma$ to be an automorphism on $\mathrm{CIRC}_N(\mathbb{R})$, if ζ^i is not real then $\sigma(-i)$ must equal $-j$. This gives the constraint stated in Lemma 2.7.1 part *(i)* except when $i = 0$ or $\frac{1}{2}N$. But, in these latter two cases, $i = -i$ (in $\mathbb{Z}_N$) anyway. Another important case is when $R = \mathbb{Q}$. Automorphisms which preserve rationality must be permutation of the eigenvalues which map eigenvalues into conjugate eigenvalues. Thus, λ_i can be mapped to any λ_{hi} where $h \in {\mathbb{Z}_N}^*$. There will be more on this in later chapters.

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 $\bar\delta^n \,|\, \mathbf{circ}_N$, 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 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**

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

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 $\quad \kappa(b) = 0 \quad \Leftrightarrow \quad \gamma\beta^{-1}(b) = 0 \quad \Leftrightarrow \quad b \in \beta\ker\gamma$. □

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

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

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 $\ker\Gamma^N \subset \phi^{-1}\ker\gamma$.

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

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

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

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.

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

$\Gamma^n_{mn} : \mathbf{circ}_{mn} \to \mathbf{circ}_n$ 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 $\Gamma^{\not m\not l}_{mn}\Gamma^{mn}_{\not m\not l}$ Wrong: cancellation not in ↗ direction

and not $\Gamma^{mn}_{\not m\not l}\Gamma^{\not m\not l}_{mn}$ 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) $\nu_{h,N}(x) \;:=\; \nu_h(x) \;:=\; \Upsilon_{\mathrm{u}}(x)_h \;=\; \sum_{i \in \mathbb{Z}_N} x_i \mathrm{u}^{ih}.$

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

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

Chapter 4.
The Supercirculants, $\mathbf{circ}_\infty$

This chapter describes the algebra $\mathbf{circ}_\infty$ (see example *(iii)* of §3.6).

We hold $\mathbf{circ}_\infty$ (and its extensions) to be the most natural generalization of circulants in that the algebra $\mathbf{circ}_\infty(R)$ subsumes every circulant algebra over a ring R. For this reason, we call $\mathbf{circ}_\infty(R)$ the **supercirculant algebra** over the ring R, and we call its members **supercirculants**.

This is a good point to discuss the supercirculants because many of the homomorphisms between circulants introduced in the last chapter assume particularly simple forms when generalized to the supercirculants. Also, the supercirculant algebra will be useful later in the chapter on tensor products of circulant algebras.

We originally identified $\mathbf{circ}_\infty(R)$ with the group ring $R[\mathbb{Q}/\mathbb{Z}]$. A typical member of $\mathbb{Q}/\mathbb{Z}$ is the fractional part of a rational, $\{m/n\}$ and the group product is addition modulo 1. We shall still use this representation of $\mathbf{circ}_\infty(R)$ where it is useful, but there is a representation which provides a more natural correspondence between the circulant algebras and the supercirculants. For this reason, we shall replace the group $\mathbb{Q}/\mathbb{Z}$ with another (but isomorphic) group consisting of an amalgam of the standard circulant bases $U_\infty := \{\mathrm{u}_m^n \vdash m, n \in \mathbb{Z}\}$.

4.1.1 **Definition** The group U_∞ is the set $\{\mathrm{u}_r^s \vdash r, s \in \mathbb{Z}, r \neq 0\}$ obeying the relations

(i) $\mathrm{u}_r^s \mathrm{u}_t^u = \mathrm{u}_{rt}^{st+ru}$

(ii) $\mathrm{u}_{rs}^{st} = \mathrm{u}_r^t$

(iii) $\mathrm{u}_r^s = 1$ iff $r \,|\, s$.

Clearly, $U_\infty \approx \mathbb{Q}/\mathbb{Z}$.

4.1.2 **Definition** $\mathbf{circ}_\infty(R) := R[U_\infty]$.

There is a copy of $\mathbf{circ}_n(R)$ in $\mathbf{circ}_\infty(R)$ for every n. The embedding is $\Upsilon_{1/n} : \mathbf{circ}_n(R) \hookrightarrow \mathbf{circ}_\infty(R)$ (see Proposition 3.6.4). In replacing $\mathbb{Q}/\mathbb{Z}$ with U_∞ we can identify $\mathbf{circ}_n$ with its copy, $\Upsilon_{1/n}(\mathbf{circ}_n) \subset \mathbf{circ}_\infty$. That is, the embedding is now viewed as a subset map. This identification leads to some intuitive and easily proved observations which follow.

4.1.3 **Proposition** Regarding $\mathbf{circ}_n(R) \subset \mathbf{circ}_\infty(R)$ for all $n = 1, 2, \ldots$,

(i) $\mathbf{circ}_m(R) \cap \mathbf{circ}_n(R) = \mathbf{circ}_{\gcd(m,n)}(R)$

(ii) $\mathbf{circ}_m(R) \vee \mathbf{circ}_n(R) = \mathbf{circ}_m(R)\mathbf{circ}_n(R) = \mathbf{circ}_N(R)$ where $N = \mathrm{lcm}(m, n)$.

(iii) $\mathbf{circ}_{mn}(R)$ is a free $\mathbf{circ}_n(R)$-module of rank m.

□

4.1.4 **Proposition** Every finite subset of $\mathbf{circ}_\infty(R)$ is in $\mathbf{circ}_N(R)$ for some N.

Proof.

The general element of a group ring $R[G]$ is $\sum_{g \in X} a_g g$ where X must be a finite subset of G. Therefore we can write the general element of $\mathbf{circ}_\infty(R)$ as

$$\sum_{m/n \in X} a_{m/n} \mathrm{u}_n^m = b_0 + b_1 \mathrm{u}_N + b_2 \mathrm{u}_N^2 + \cdots + b_i \mathrm{u}_N^i + \cdots + b_{N-1} \mathrm{u}_N^{N-1} \tag{1}$$

where $N = \mathrm{lcm}\,\{n \vdash m/n \in X, \gcd(m, n) = 1\}$, and $b_i = \begin{cases} a_{i/N} & \text{if } i/N \in X \\ 0 & \text{otherwise} \end{cases}$

Let there be a finite subset $\{a, b, c, \ldots\} \subset \mathbf{circ}_\infty$. Then, by the above, there exist $A, B, C, \ldots \in \mathbb{N}$ such that $a \in \mathbf{circ}_A$, $b \in \mathbf{circ}_B$, $c \in \mathbf{circ}_C$, etc. Set $N = \mathrm{lcm}\{A, B, C, \ldots\}$, then by Proposition 4.1.3 *(ii)*, $\{a, b, c, \ldots\} \in \mathbf{circ}_N$. □

4.1.5 **Proposition** Let $R[G]$ be a group ring, let H be a subgroup of G, and let τ be a group endomorphism on G.

(i) τ extends to an R-algebra endomorphism, τ' on $R[G]$
where $\tau'(rf + sg) = r\tau(f) + s\tau(g),\ \forall r, s \in R,\ \ \forall f, g \in G.$

(ii) $\ker \tau' = R[\ker \tau]$

(iii) $R[H]$ is an R-subalgebra of $R[G]$. □

In the case of $R[G] = \mathbf{circ}_\infty(R)$, let us call the endomorphism of the type described in parts *(i)* and *(ii)* an **extended group endomorphism**, and let us call the subring of the type in part *(iii)* a **subgroup ring**. The extended group endomorphisms and the subgroup rings are interesting because they are automatically R-linear and R-subalgebras, respectively. To find all such endomorphisms and subalgebras of $\mathbf{circ}_\infty(R)$ we need more facts on the group U_∞.

4.1.6 **Theorem**

(i) The group U_∞ is pure torsion.

(ii) U_∞ is a divisible group, and so has the injective property.

(iii) $U_\infty = \prod_p \sigma(p^\infty)$ where the direct product is over all p-primary components of U_∞.

Proof. These are standard facts about the group $\mathbb{Q}/\mathbb{Z}$. See [Rot]. □

The injective property on U_∞ assures us that β exists whenever α exists in the map diagram below (where H and K are abelian groups.) Typically, $H \subset K$, and then the theorem says that there is an extension of α to K.

$$\begin{array}{ccccc} & & & & U_\infty \\ & & & \overset{\alpha}{\nearrow} & \uparrow \beta? \\ 0 & \to & H & \to & K \end{array}$$

Part *(iii)* of the theorem is perhaps better illustrated in the group $\mathbb{Q}/\mathbb{Z}$ taking the interval $[0,1) \cap \mathbb{Q}$ as a transversal for the rationals modulo 1. The p-primary component of $\mathbb{Q}/\mathbb{Z}$ is the set of all fractions whose denominators are powers of p. The direct sum decomposition of a general fraction in the interval $[0,1)$ is performed thus: Let $a/mn \in [0,1)$ with m, n coprime. Then, there exists a unique partial fraction decomposition of $a/mn = b/m + c/n$ where $b, c \in \mathbb{N}$ and $b/m,\ c/n \in [0,1)$. We proceed thus until the denominators of all partial fractions are prime powers.

4.1.7 **Proposition**

(i) Each finitely-generated subgroup of U_∞ is cyclic generated by u_n for some n.

(ii) The endomorphisms of U_∞ are direct products of endomorphisms on the p-primary components.

Proof. We shall prove the proposition for the group $\mathbb{Q}/\mathbb{Z}$, and we shall take as representatives the rationals in the interval $[0,1)$.

(i) Let x/y be any reduced fraction in $(0,1)$. Then, $kx/y \bmod 1 \in A$ for all $k \in \mathbb{N}$. Setting k to the inverse residue of $x \pmod y$, we see that $1/v \in A$.

Now, suppose that A is a finitely generated subgroup of $\mathbb{Q}/\mathbb{Z}$. By part *(i)* of the theorem, A is finite; let $u/v \in [0,1) \cap \mathbb{Q}$ be its smallest reduced fraction. By the above, $1/v \in A$. $\therefore u = 1$. Let x/y be any reduced fraction in A, then $1/y \in A$. By considering $a/v + b/y$ where $a, b \in \mathbb{Z}$, we see that $1/\mathrm{lcm}(v,y) \in A$. By the minimality of $1/v$, $\mathrm{lcm}(v,y) \le v$ which means $y \mid v$. That is, A consists entirely of the fractions with denominators dividing v, and hence is cyclic generated by $1/v$. QED *(i)*.

(ii) Let $\alpha : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ be non-trivial with $\alpha(x) \neq 0$. Let P_p be the projection homomorphism onto $\sigma(p^\infty)$ with p chosen so that $P_p(x) \neq 0$. (This must exist since $\alpha(x) \neq 0 \ \Rightarrow\ x \neq 0$.) Let $P_p^\perp = 1 - P_p$ be the complementary projection of P_p. Hence, $x = y \oplus z$ where $y = P_p(x)$, and $z = P_p^\perp(x)$.

Consider first $\alpha(y)$. Since α is a homomorphism, $\alpha(y)$ must have order dividing the order of $y \in \sigma(p^\infty)$. Therefore, $\alpha(y) \in \sigma(p^\infty)$. Similarly, $\alpha(z)$ must have order dividing the order of z which is in the direct product of all q-primary subgroups where $q \neq p$. This means that the order of $\alpha(z)$ cannot be divisible by p.

We have shown that $\alpha = \alpha_p \oplus \alpha_p^\perp$ where $\alpha_p = P_p \alpha P_p$, and $\alpha_p^\perp = P_p^\perp \alpha P_p^\perp$. We now apply the same reasoning to z eventually obtaining a complete decomposition of α into its actions on all the p-primary components of x, and all such actions are endomorphisms of their respective components. □

4.1.8 **Corollary** Each subgroup ring of $\mathbf{circ}_\infty(R)$ with a finite basis is $\mathbf{circ}_n(R)$ for some n. □

The proposition shows that every supercirculant endomorphism is specified by endomorphisms on the p-primary components. Let $\alpha_p : \sigma(p^\infty) \to \sigma(p^\infty)$. How is α_p specified? Let C_n be the subgroup of $\sigma(p^\infty)$ generated by $1/p^n$ (again using the $[0,1] \cap \mathbb{Q}$ representation). One can easily show that α_p must be an endomorphism on C_n for every n. This gives another simple corollary to Proposition 4.1.8.

4.1.9 **Corollary** Every endomorphism of $\mathbb{Q}/\mathbb{Z}$ is an endomorphism of every subgroup $C_n^{(p)} = \{a/p^n \vdash 0 \leq a < p^n\}$, and the action on $C_n^{(p)}$ is $x \to k_n^{(p)} x \bmod 1$ for some integer $k_n^{(p)}$.

Proof. C_n is cyclic since it is generated by $1/p^n$. All endomorphisms of the cyclic group $\mathbb{Z}_N$ are of the form $x \mapsto mx \bmod N$ for some integer m, it follows that the action of α on C_n is multiplication (mod 1) by some constant integer. □

Hence, we can specify α_p by specifying $k_n^{(p)}$ for every n. For consistency on all subgroups of $\sigma(p^\infty)$, we must have $k_{n+i} \equiv k_n \pmod{p^n}$ for $i \geq 0$. We can guarantee consistency by defining k_n p-adically as

$$k_n = k_n^{(p)} = c_0^{(p)} + pc_1^{(p)} + p^2 c_2^{(p)} + \cdots + p^{n-1} c_{n-1}^{(p)} \qquad \text{where } 0 \leq c_i < p \tag{2}$$

This demonstrates that the number of endomorphisms on each p-primary component of U_∞ has the cardinality of $\mathbb{R}$. Furthermore, a complete specification of the full endomorphism, $\alpha : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, requires the independent specifications of an infinity of sequences $\left(k_n^{(p)}\right)_{n=1,2,\cdots}$, one for each prime, p.

4.1.10 **Examples**

(i) Take $c_0^{(p)} = 1$ for some prime p, and set all other $c_i^{(q)} = 0$. We get the projection endomorphism $P_p : \mathbb{Q}/\mathbb{Z} \to \sigma(p^\infty)$.

(ii) Take $k_n^{(p)} = k$, a constant. This specifies the $\mathbb{Q}/\mathbb{Z}$ group endomorphism $\alpha(x) = kx$. On U_∞ the homomorphism is given by $\alpha(\mathrm{u}_n) = \mathrm{u}_n^k$.

(iii) Take $c_i^{(p)} = \pi_i^{(p)}$ where $\pi_i^{(p)}$ is the i^{th} digit of π ($= 3.14159\ldots$) in base p arithmetic. This is an example of a homomorphism which requires an infinity of parameters, but is nevertheless well-defined.

4.2 Supercirculant Endomorphisms.

We have obtained a full description of the endomorphisms of the group U_∞. The next proposition shows that such endomorphisms when extended to $\mathbf{circ}_\infty$ are automatically endomorphisms on the circulant subrings.

4.2.1 **Proposition** Let α be an extended group endomorphism of $\mathbf{circ}_\infty(R)$ then α is also an endomorphism of $\mathbf{circ}_n(R)$ for every n.

Proof. From Corollary 4.1.9, if α is an extended group endomorphism, α must map each p-primary subgroup of the type C_n into itself. Hence, α maps the set $\{\mathrm{u}_n^i \vdash 0 \leq i < n\}$ into itself, and so α must be an endomorphism of $\mathbf{circ}_n(R)$. □

We now return to example *(ii)* of §4.1.10 (where $k_n^{(p)} = k$). As a map on U_∞ this is the endomorphism $\mathrm{u}_n \mapsto \mathrm{u}_n^k$. When extended to $\mathbf{circ}_\infty(R)$ call this map H_k. Observe that $H_n|\mathbf{circ}_{mn}(R)$ maps u_{mn} to u_n, and so it must be the wrap-around map, $\Gamma^m_{mn} : \mathbf{circ}_{mn}(R) \to \mathbf{circ}_m(R)$. More generally, the proposition shows that H_k in an endomorphism on $\mathbf{circ}_n(R)$ for all n. Clearly, H_k can only be the map ν_k of §3.7. In other words, as supercirculant maps, $\Gamma^n_{mn} = \nu_n = H_n|\mathbf{circ}_{mn}(R)$. It is therefore hardly surprising that Γ^n_{mn} and ν_h commute (see Proposition 3.7.6).

Even more drastic is the fate of the injection map, $\tilde{\Gamma}^{mn}_m$, when extended to the supercirculants -- it becomes the identity map ! $\tilde{\Gamma}^{mn}_m : \mathrm{u}_m \to \mathrm{u}^n_{mn} = \mathrm{u}_m$. Hence, all commutation relations of $\tilde{\Gamma}^m_{mn}$ with every circulant map are trivial.

Next, let us consider the idempotent $\bar{\delta}^{n|mn}$ and its associated map, $x \mapsto \bar{\delta}^{n|mn}x$. Trivially, any idempotent in a subring is also an idempotent in the larger ring. So, $\bar{\delta}^{n|mn}$ is a supercirculant idempotent, and hence defines an endomorphism on $\mathbf{circ}_\infty$. By definition,

$$\bar{\delta}^{n|mn} \;:=\; \frac{1}{n}\sum_{i=0}^{n-1} \mathrm{u}^{im}_{mn} \;=\; \frac{1}{n}\sum_{i=0}^{n-1} \mathrm{u}^{i}_{n}$$

and so it is quite unambiguous to write $\bar{\delta}^n$ instead of $\bar{\delta}^{n|mn}$ because as a supercirculant, $\bar{\delta}^n$ truly depends only on n.

The circulant repeater map, Γ^{mn}_m was defined as $\Gamma^{mn}_m(\mathrm{u}_m) = \bar{\delta}^n \mathrm{u}_{mn}$. This definition stands except that Γ^{mn}_m no longer depends upon m. The value of $\Gamma^{mn}_m(x)$ is entirely determined by x and n. Our suspicions are confirmed; indeed, $\Gamma^m_{mn}(x) = \bar{\delta}^n x$. This and the above observations are collected below.

4.2.2 **Proposition** The Γ^s_r homomorphisms of chapter 3 have natural extensions to $\mathbf{circ}_\infty$ which are:

(i) $\Gamma^{mn}_m = \nu_n : \mathrm{u}_i \mapsto \mathrm{u}^n_i, \quad \forall i \in \mathbb{N}.$

(ii) $\tilde{\Gamma}^{mn}_m =$ identity map.

(iii) $\Gamma^m_{mn}(x) = \bar{\delta}^n(x).$

Proof. The first two statements are already clear.

For the third statement, note that $\bar{\delta}^n \mathrm{u}_n = \bar{\delta}^n$. Therefore, $\bar{\delta}^n \mathrm{u}_d = \bar{\delta}^n$ whenever $d \,|\, n$. Whence, $\bar{\delta}^n \mathrm{u}_m = \bar{\delta}^n \mathrm{u}_{m/d}$ where $d = \gcd(m, n)$. We now see that $\bar{\delta}^n \mathrm{u}_{mn} = \bar{\delta}^n \mathrm{u}^n$. But, $\Gamma^{mn}_m(\mathrm{u}_n) = \bar{\delta}^n \mathrm{u}_{mn} = \bar{\delta}^n \mathrm{u}_n$. The rest follows by linearity. □

4.3 Supercirculant Eigenvalues

In the Chapter 2 we saw that the R-linear circulant automorphisms are permutations of the circulant eigenvalues. We would therefore expect that R-linear automorphisms of supercirculants which were also endomorphisms of the circulant algebras would also be permutations of eigenvalues. But, first we must define eigenvalues for the supercirculants. The reader may ponder what definition might be appropriate before reading on, but will conclude that the one given below is the only definition which is an R-linear ring monomorphism from the supercirculant algebra into an algebra having componentwise multiplication and addition.

4.3.1 **Definition** The eigenvalue map $\lambda : \mathbf{circ}_\infty(R) \to \Lambda_\infty(R)$ is defined by $\lambda_i(\mathrm{u}_n) \;:=\; \zeta_n^i, \;\forall i \in \mathbb{N}$, and is then extended by additivity, multiplicativity, and R-linearity to the whole of $\mathbf{circ}_\infty(R)$.

The definition implies that $\Lambda_\infty(R)$ is a space of infinite sequences, and when R is a domain, $\Lambda_\infty(R)$ is an infinite dimensional vector space. That is, given any $c \in \mathbf{circ}_\infty$, $\lambda(c) = (\lambda_0(c), \lambda_1(c), \ldots, \lambda_i(c), \lambda_{i+1}(c), \ldots)$. Also, since $c \in \mathbf{circ}_n(R)$ for some n, the sequence $\lambda(c)$ must be periodic with period n. Informally, $\lambda(c)$ has the frequency spectrum c.

Let $R_{(n)}$ be the set of sequences of period n with entries from $R(\zeta_n)$. Then, $\Lambda_\infty(R)$ is contained in $\bigcup_n R_{(n)}$. In analogy with $\mathbf{circ}_n$, we shall call $\bigcup_n R_{(n)}$ the **supercirculant eigenspace**. That is, we view $\bigcup_n R_{(n)}$ as the range (but it is not the image) of the λ map acting on $\mathbf{circ}_\infty(R)$. Just as all elements must finite sums in group rings so all sequences are periodic in the supercirculant eigenspace.

4.4 The Inverse Transform, λ^{-1}

One can easily prove that λ is a monomorphism. For instance, suppose $\lambda(x) = 0$. W.l.o.g., $x \in \mathbf{circ}_n(R)$. Then, taking a subsequence consisting of one whole period of n terms from $\lambda(x)$ we obtain the vector $\lambda^{(n)}(x)$. Whence $x = 0$.

Therefore, λ must have an inverse on its image. A formula for the inverse should specify the coefficient of u for every $\mathrm{u} \in U_\infty$. (Of course, almost all should turn out to be zero.) It is convenient to use the notation $a_{r/n}$ for the coefficient of u_n^r.

4.4.1 Proposition

Let $\mu = (\mu_0, \mu_1, \ldots) \in \bigcup_n R_{(n)}$, and for definiteness, suppose $\mu \in R_{(m)}$. Define $a = \sum_{0 \le r/n < 1} \{a_{r/n} \mathrm{u}_n^r\}$ where $a_{r/n}$ are defined by

$$a_{r/n} \;:=\; \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} \mu_i \zeta_n^{-ir} \tag{3}$$

Then,

(i) $a \in \mathbf{circ}_M(Q)$ where Q is the ring of quotients of R, and

(ii) $\lambda(a) = \mu$.

Proof.

(i) Fix a typical term $a_{r/n}$, and w.l.o.g., suppose $r < n$ are coprime. The trick to evaluating formula (3) is to group terms within periods of $\mu_i \zeta_n^{-ir}$ which in this case has a period of nm/d where $d = \gcd(n, m)$. Assume for the moment that the series in (3) has a whole number of periods of $\mu_i \zeta_n$, i.e., that $N = Lnm/d$ for some integer L. Then,

$$a_{r/n} \quad = \quad \lim_{L\to\infty} \frac{d}{Lmn} \sum_{l=0}^{L-1} \sum_{i=0}^{mn/d-1} \mu_i \zeta_n^{-ir}$$

The second summation is independent of l. So, the outside factor of $1/L$ cancels with the L repetitions of the second sum. Inside the second sum, the coefficients $\mu_i, \mu_{i+m}, \mu_{i+2m}, \ldots$ are all equal. Group together all such terms. (This is a finite derangement of the series.) We obtain inner sums of the form

$$\begin{aligned}
&\mu_i \zeta_n^{-ir} \;+\; \mu_{i+m} \zeta_n^{-ir-mr} \;+\; \mu_{i+2m} \zeta_n^{-ir-2mr} \;+\; \ldots \;+\; \mu_{i+(n/d-1)m} \zeta_n^{-ir-(n/d-1)mr} \\
&\qquad = \quad \mu_i \zeta_n^{-ir} \left(1 \;+\; \zeta_n^{-mr} \;+\; \zeta_n^{-2mr} \;+\; \ldots \;+\; \zeta_n^{-(n/d-1)mr}\right) \\
&\qquad = \quad \mu_i \zeta_n^{-ir} \left(1 \;+\; \zeta_{n/d}^{-s} \;+\; \zeta_{n/d}^{-2s} \;+\; \ldots \;+\; \zeta_{n/d}^{-(n-d)s}\right) \qquad \text{where } s = rm/d \\
&\qquad = \quad \begin{cases} 1 & \text{if } n/d = 1 \\ 0 & \text{otherwise} \end{cases}
\end{aligned}$$

The final choice of values is comes from the fact that both r and m/d are coprime to n/d. The upshot is that $a_{r/n}$ is zero unless $n \,|\, m$.

Finally, we have to consider the remainder term. This will be the sum over some fractional part of the period of $\mu_i \zeta_n^{-ir}$. Because we have already considered any number of whole periods in the series, we can assume that the remainder contains less terms than a complete period. Therefore, the remainder cannot exceed R in absolute value where

$$R \;=\; \frac{1}{N} \frac{mn}{d} \max\{\mu_i \vdash 0 \le i < m\}$$

and this tends to zero as $N \to \infty$. QED *(i)*

Continuing the above formula, but now assuming $n \,|\, m$. We see that

$$a_{r/n} \;=\; \frac{1}{m}\sum_{i=0}^{m-1} \mu_i \zeta_n^{-ir}$$

which we can rewrite by setting $d = m/n$ as

$$a_{rd/m} \;=\; \frac{1}{m}\sum_{i=0}^{m-1} \mu_i \zeta_m^{-ird}$$

This is the regular formula for $\lambda^{-(m)}$. Since a single period of $\lambda|\mathbf{circ}_m(R)$ agrees with $\lambda^{(m)}$ on $\mathbf{circ}_m(R)$, we have that $\lambda(a) = \mu$. $\square$

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, $\mathbf{circ}(\mathbb{Q})$. 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. That is, a_i depends only on $\gcd(N, i)$. 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) $(w, y, x, y, x, z, x, y, x, y)$, $\quad N = 10$.

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

(c) $(x, y, y, \ldots, y)$, $\quad$ 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, $\big(c(0),\ c(u),\ c(2u),\ \ldots,\ c(hu),\ \ldots,\ c\,((N-1)u)\big)$ 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 $\lambda_j = \sum_{i \in \mathbb{Z}_N} a_i \zeta^{ij}$ 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.

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

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

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

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 $\{a_d \vdash d \,|\, N\}$. Therefore, the eigenvalues of circulant vectors can depend only on this set.

$$\lambda_i = \sum_{j\in\mathbb{Z}_N} a_j\zeta^{ij} = \sum_{d|\,N} a_d \sum_{\{j\vdash \gcd(j,N)=d\}} \zeta_N^{ij} = \sum_{d|\,N} a_d \sum_{\{k\vdash \gcd(k,N)=1\}} \zeta_{N/d}^{ik}$$

$$a_i = \frac{1}{N}\sum_{j\in\mathbb{Z}_N} \lambda_j\zeta^{-ij} = \frac{1}{N}\sum_{d|\,N} \lambda_d \sum_{\{j\vdash \gcd(j,N)=d\}} \zeta_N^{-ij} = \frac{1}{N}\sum_{d|\,N} \lambda_d \sum_{\{k\vdash \gcd(k,N)=1\}} \zeta_{N/d}^{-ik}$$

Taking the eigenvalue equation as typical of the two,

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

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 $r_{n_1n_2}(m) = r_{n_1}(m)r_{n_2}(m)\,.$

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

(iii) $r_n(m) = \mu(h)\,\frac{\phi(n)}{\phi(h)}$ where $h = \frac{n}{\gcd(m,n)}$ □

Proof. See Hardy & Wright [HaW1]. □

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

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

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

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

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

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

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

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 $\{a_h \vdash h \,|\, N\}$ are independent so we restrict $i = h \,|\, N$. 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:

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

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. □

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

We now introduce a slight variation on P.

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

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

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

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

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

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

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

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

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

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

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,

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

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,

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

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_{mn}^m 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.

$$
\begin{array}{ccccccccccccccc}
0 & 1 & 2 & \cdots & m-1 & m & 1 & 2 & \cdots & m-1 & \cdots & N-m & 1 & 2 & \cdots & m-1 \\
m-1 & 0 & 1 & \cdots & m-2 & m-1 & m & 1 & \cdots & m-2 & \cdots & m-1 & N-m & 1 & \cdots & m-2 \\
m-2 & m-1 & 0 & \cdots & m-3 & m-2 & m-1 & m & \cdots & m-3 & \cdots & m-2 & m-1 & N-m & \cdots & m-3 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 2 & 3 & \cdots & 0 & 1 & 2 & 3 & \cdots & m & \cdots & 1 & 2 & 3 & \cdots & N-m \\
 & & & & & & & & & & & & & & & \\
N-m & 1 & 2 & \cdots & m-1 & 0 & 1 & 2 & \cdots & m-1 & \cdots & N-2m & 1 & 2 & \cdots & m-1 \\
m-1 & N-m & 1 & \cdots & m-2 & m-1 & 0 & 1 & \cdots & m-2 & \cdots & m-1 & N-2m & 1 & \cdots & m-2 \\
m-2 & m-1 & N-m & \cdots & m-3 & m-2 & m-1 & 0 & \cdots & m-3 & \cdots & m-2 & m-1 & N-2m & \cdots & m-3 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 2 & 3 & \cdots & N-m & 1 & 2 & 3 & \cdots & 0 & \cdots & 1 & 2 & 3 & \cdots & N-2m \\
 & & \vdots & & & & & \vdots & & & & & & \vdots & & \\
 & & \vdots & & & & & \vdots & & & & & & \vdots & & \\
m & 1 & 2 & \cdots & m-1 & 2m & 1 & 2 & \cdots & m-1 & \cdots & 0 & 1 & 2 & \cdots & m-1 \\
m-1 & m & 1 & \cdots & m-2 & m-1 & 2m & 1 & \cdots & m-2 & \cdots & m-1 & 0 & 1 & \cdots & m-2 \\
m-2 & m-1 & m & \cdots & m-3 & m-2 & m-1 & m & \cdots & m-3 & \cdots & m-2 & m-1 & 0 & \cdots & m-3 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 2 & 3 & \cdots & m & 1 & 2 & 3 & \cdots & 2m & \cdots & 1 & 2 & 3 & \cdots & 0
\end{array}
$$

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 $m \,|\, N$ 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).

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

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^{mn}_n and Proposition 3.5.2*(ii)*, the formula for the eigenvalues is

$$\lambda^{(mn)}_i(a) \quad = \quad \lambda^{(n)}_i(a_{(m)}(x)) \; + \; n\delta^n_i\lambda^{(m)}_{i/n}\left(a^{(m)}(x)\right) \tag{7}$$

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),

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

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

We have proved:

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

$$\begin{aligned} \bar{a}^{(m)} &= \frac{1}{n}\left(\Gamma_{mn}^{m}(a) - 1\right) \\ \bar{a}_{(m)} &= 1 \end{aligned}$$ □

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),

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

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,

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

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.

Chapter 6.
Tensor Products.

6.1 Tensor Circulant Matrices

Tensor products of circulant matrices cannot in general be constructed by substituting circulant matrices for entries in circulant matrices. As Proposition 5.2.3 showed, the Kronecker product of circulant matrices is circulant iff the Kronecker product is subrepeating. In the first section of this chapter, another matrix algebra is constructed which includes the subrepeating circulant matrices as a subalgebra, and so is a generalization of the subrepeating circulants. Although matrices in the new algebra are not necessarily circulant, the algebra nevertheless enjoys some of the key properties of the circulant matrix algebra. In particular, it is simultaneously diagonalizable.

Although the generalization of subrepeating circulants supplies a tensor-like algebra, it suffers from a serious defect. One cannot take two arbitrary circulant matrices of given dimensions, and expect their tensor product to behave like a circulant matrix. Indeed, there is no solution to this requirement, but there is a solution if we restrict the dimensions of the circulants we take into a tensor product. In the second and subsequent sections of this chapter the possibility of a general tensor product is investigated, and a satisfactory tensor product is shown to exist whenever the dimensions of the factors in the tensor product are coprime.

6.1.1 The Kronecker Product.

In this section, a matrix algebra is defined as the intersection of two Kronecker product algebras. This approach is taken from Davies's book (see [Dav4]) and is briefly summarised here.

The **Kronecker product** of a matrix $A = (a_{i,j})_{i,j}$ in $\mathrm{M}_m(R)$ with a matrix $B \in \mathrm{M}_n(R)$ is the matrix $A \times B \in \mathrm{M}_{mn}(R)$ defined by

$$A \times B := \begin{pmatrix} a_{1,1}B & a_{1,2}B & \dots & a_{1,m}B \\ a_{2,1}B & a_{2,2}B & \dots & a_{2,m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1}B & a_{m,2}B & \dots & a_{m,m}B \end{pmatrix}$$

The above definition shows a Kronecker product in block form; each entry is an $n \times n$ matrix.

We proceed by introducing two matrix algebras namely, $\mathrm{CIRC}_m(\mathrm{M}_n(R))$ and $\mathrm{M}_m(\mathrm{CIRC}_n(R))$ which are called respectively the **block circulant** ("circulant in blocks") and the **circulant block** ("blocks of circulants") matrices.

A nice example of a block circulant is a partitioned $mn \times mn$ circulant matrix. For instance, let $m = 3$ and $n = 2$, then the general 6×6 circulant matrix can be partitioned as follows.

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

This matrix is circulant over $\mathrm{M}_2(R)$! Unfortunately, block circulants are not generally circulant. For instance, the matrix below is a block circulant matrix but is not circulant.

$$\begin{pmatrix} a & b & e & f \\ c & d & g & h \\ & & & \\ e & f & a & b \\ g & h & c & d \end{pmatrix}$$

The block circulant $\mathrm{CIRC}_m(0, I_n, 0, \ldots, 0) = \mathrm{U}_m \otimes I_n$ is analagous to the U matrix in the circulants. It can be shown that a matrix is a block circulant iff it commutes with $\mathrm{U}_m \otimes I_n$. This is analogous to Corollary 2.1.1 for ordinary circulants. Also analagous to circulants, is that block circulants are diagonalized by the Kronecker product $F_m \otimes F_n$ where F_n is the $n \times n$ Fourier matrix. However, the diagonal entries are not scalar, rather they are general $n \times n$ matrices.

For the circulant block matrices, on the other hand, the centralizing matrix is $I_m \otimes \mathrm{U}_n$. It is the matrix with U_n blocks down the main diagonal and zeroes elsewhere. It can be shown that a matrix M is a circulant block matrix iff it commutes with $I_m \otimes \mathrm{U}_n$ iff $(F_m \otimes F_n)^\dagger M (F_m \otimes F_n)$ is in $\mathrm{M}_m(\mathrm{Diag}_n(R))$ where $\mathrm{Diag}_n(R)$ is the set of all $n \times n$ diagonal matrices over R.

There is an apparent problem with this development. Block circulants are circulant over a non-commutative ring and hence form a non-commutative algebra. Consequently much of the theory of circulants is inapplicable to block circulants. On the other hand, circulant block matrices do have commutative entries, but they are non-commutative because matrix multiplication is generally non-commutative. However, the intersection of the two algebras, $\mathrm{CIRC}_m(\mathrm{M}_n(R)) \cap \mathrm{M}_m(\mathrm{CIRC}_n(R))$ is commutative and members of this joint algebra are simultaneously diagonalizable by the unitary matrix $F_m \otimes F_n$.

The subrepeating circulants have a special rôle here. From the definitions (see 5.2.2) we have

$$\mathrm{QR}^n_{mn} \subset \mathrm{CIRC}_m(\mathrm{M}_n(R)) \cap \mathrm{M}_m(\mathrm{CIRC}_n(R)) = \mathrm{CIRC}_m(\mathrm{CIRC}_n(R))$$

and by Proposition 5.2.3, we have

$$\begin{aligned} \mathrm{QR}^n_{mn} &= \mathrm{CIRC}_{mn}(R) \cap \mathrm{M}_m(\mathrm{CIRC}_n(R)) \\ \therefore\ \mathrm{QR}^n_{mn} &= \mathrm{CIRC}_{mn}(R) \cap \mathrm{CIRC}_m(\mathrm{M}_n(R)) \cap \mathrm{M}_m(\mathrm{CIRC}_n(R)) \\ &= \mathrm{CIRC}_{mn}(R) \cap \mathrm{CIRC}_m(\mathrm{CIRC}_n(R)) \end{aligned}$$

In summary, the above approach bestows upon suitable Kronecker products all the main properties of circulant matrices. However, the approach still suffers from the problem that the Kronecker product of general circulants is not circulant. The second approach will remedy this at the cost that the tensor product is not defined for all dimensions m and n.

6.2 General Tensor Products of Circulant Matrices.

It is sometimes erroneously assumed that a tensor product of matrices must be a Kronecker product. This is not so, the Kronecker product is merely the simplest tensor product. To find a suitable tensor product for circulants, we shall start with a set of desiderata for such a general tensor product, and then construct a tensor product which satisfy these desiderata.

A tensor product of matrices A and B is a matrix T which is constructed by a rule which assigns to $T_{r,s}$ the product of pairs of entries from A and B, $A_{i,j}B_{k,l}$, say. The rule is a map from pairs of matricial indices $((i,j),(k,l))$ to indices of the tensor product matrix, (r,s). To qualify as a tensor product on A and B, the domain of the map should be the set of all pairs of indices for A and B. For the tensor matrix to be fully defined, the range of the map must be the set of all indices of the tensor product matrix. For the tensor matrix to be well-defined, the map must be one-to-one. There is one other criterion, the so-called product rule: Given matrices A_1, A_2 and B_1, B_2 then $(A_1A_2) \otimes (B_1B_2)$ must equal $(A_1 \otimes B_1)(A_2 \otimes B_2)$.

Now we apply these criteria to circulant matrices. We need to find a tensor product of $\mathrm{CIRC}_m(R)$ and $\mathrm{CIRC}_n(R)$ so that $\mathrm{CIRC}_m(R) \otimes \mathrm{CIRC}_n(R) \subset \mathrm{CIRC}_N(R)$ for some N, and there must be a one-to-one map $\phi : \mathbb{Z}_N^2 \to \mathbb{Z}_m^2 \times \mathbb{Z}_n^2$ such that $T_{x,y} = A_{\phi_1(x,y)}B_{\phi_2(x,y)}$ where $\phi_1 \times \phi_2 = \phi$.

6.2.1 **Theorem** A tensor product $\mathrm{CIRC}_m(R) \otimes \mathrm{CIRC}_n(R)$ can be defined such that $T = A \otimes B$ is circulant in $\mathrm{CIRC}_N(R)$ for some N and for every $A \in \mathrm{CIRC}_m(R)$, $B \in \mathrm{CIRC}_n(R)$ if and only if m and n are coprime. Let $T = \mathrm{CIRC}(t)$, $A = \mathrm{CIRC}(a)$, and $B = \mathrm{CIRC}(b)$. Then, $t_x = a_{\phi_1(x)}b_{\phi_2(x)}$ with $\phi = \phi_1 \oplus \phi_2$ an additive isomorphism, $\phi : \mathbb{Z}_N \to \mathbb{Z}_m \oplus \mathbb{Z}_n$. In particular, $N = nm$.

Proof. Take the most general possible definition of $T = A \otimes B$ and assume that all three matrices are circulant.

$$T_{x,y} \;:=\; A_{\nu_1(x,y),\rho_1(x,y)}B_{\nu_2(x,y),\rho_2(x,y)} \quad \text{where } \nu_1(x,y),\rho_1(x,y)\in\mathbb{Z}_m, \text{ and } \nu_2(x,y),\rho_2(x,y)\in\mathbb{Z}_n.$$

$$\therefore t_{y-x} \;=\; a_{\rho_1(x,y)-\nu_1(x,y)}b_{\rho_2(x,y)-\nu_2(x,y)} \tag{1}$$

$$\therefore t_{y} \;=\; a_{\rho_1(0,y)-\nu_1(0,y)}b_{\rho_2(0,y)-\nu_2(0,y)}$$

$$\therefore t_{y-x} \;=\; a_{\rho_1(0,y-x)-\nu_1(0,y-x)}b_{\rho_2(0,y-x)-\nu_2(0,y-x)} \tag{2}$$

Identifying terms in equations (1) and (2),

$$\therefore \rho_1(x,y)-\nu_1(x,y) \;=\; \rho_1(0,y-x)-\nu_1(0,y-x) \quad \text{with a similar equation for } \rho_2 \text{ and } \nu_2.$$

This shows that $\rho_1(x,y)-\nu_1(x,y)$ is a function of $y-x$. Let $\rho_1(x,y)-\nu_1(x,y)=\phi_1(y-x)$ and let $\rho_2(x,y)-\nu_2(x,y)=\phi_2(y-x)$ then

$$t_x \;=\; a_{\phi_1(x)}b_{\phi_2(x)}$$

We now apply the product rule. Let $t,t'\in\mathbb{Z}_N$ and let $a,a'\in\mathbb{Z}_m,\ b,b'\in\mathbb{Z}_n$.

$$\begin{aligned}
(t*t')_x \;&=\; \sum_{y\in\mathbb{Z}_N} t_y t'_{x-y} \\
&=\; \sum_{y\in\mathbb{Z}_N} a_{\phi_1(y)}b_{\phi_2(y)}a'_{\phi_1(x-y)}b'_{\phi_2(x-y)} \qquad (3)\\
&=\; (a*a')_{\phi_1(x)}\,(b*b')_{\phi_2(x)} \quad \text{by the product rule} \\
&=\; \left(\sum_{j\in\mathbb{Z}_m} a_j a'_{\phi_1(x)-j}\right)\left(\sum_{k\in\mathbb{Z}_n} b_k b'_{\phi_2(x)-k}\right) \\
&=\; \sum_{j\in\mathbb{Z}_m}\sum_{k\in\mathbb{Z}_n} a_j b_k a'_{\phi_1(x)-j}b'_{\phi_2(x)-k} \qquad (4)
\end{aligned}$$

Comparing (3) and (4), we see that the (j,k) subscripts in expression (4) must range over the same set as $(\phi_1(y),\phi_2(y))$ respectively in expression (3).

$$\therefore \phi=\phi_1\times\phi_2:\mathbb{Z}_N\to\mathbb{Z}_m\times\mathbb{Z}_n \;\text{ onto}$$

Since summation order is immaterial, we can substitute $\phi_1(y)$ for j and $\phi_2(y)$ for k in expression (4) and then identify terms with expression (3) showing that,

$$\phi_1(x)-\phi_1(y) \;=\; \phi_1(x-y)$$

$$\phi_2(x)-\phi_2(y) \;=\; \phi_2(x-y)$$

That is, $\phi=\phi_1\times\phi_2$ is a linear map and so is an additive group homomorphism. $\therefore \phi=\phi_1\oplus\phi_2$. It was shown that ϕ must be onto, and by the tensor requirements, ϕ must be one-to-one, therefore, ϕ is an additive isomorphism. But, $\mathbb{Z}_N$ is cyclic, whereas $\mathbb{Z}_m\oplus\mathbb{Z}_n$ cyclic if and only if m,n are coprime. Therefore, m,n are coprime and $N=mn$. □

6.2.2 **Single Residue Definition of ϕ and Tensor Eigenvalues** The ϕ map can be fully defined by a single residue, g, in $\mathbb{Z}^*_{mn}$.

$$\phi_g(x) = (gx \bmod m) \oplus (gx \bmod n)$$

With this definition of the map, the relationship of the eigenvalues of $A \otimes B$ to the eigenvalues of A and B can be found quite easily. Consider a product of arbitrary eigenvalues from A and B.

$$\begin{aligned}
\lambda_i(A)\lambda_j(B) &= \sum_{k\in\mathbb{Z}_m} a_k \zeta_m^{ik} \sum_{l\in\mathbb{Z}_m} b_l \zeta_n^{jl} \\
&= \sum_{k\in\mathbb{Z}_m} \sum_{l\in\mathbb{Z}_m} a_k b_l \zeta_{mn}^{ikn+jlm} \\
&= \sum_{x\in\mathbb{Z}_{mn}} a_{(gx \bmod m)} b_{(gx \bmod n)} \zeta_{mn}^{gxin+gxjm} \\
&= \sum_{x\in\mathbb{Z}_{mn}} t_x \zeta_{mn}^{x(gin+gjm)} \\
&= \lambda(T)_{g(in+jm)}
\end{aligned}$$

The result is a general eigenvalue of $T = A \otimes B$. So (as one would expect), each eigenvalue of the tensor product is the product of eigenvalues of the tensor factors. The map relating the eigenvalues is most simply given by

$$\tilde{\phi}(in + jm) \;=\; (i,\ j)$$

This map can also be defined in terms of a single residue, $h \in \mathbb{Z}_{mn}$.

$$\tilde{\phi}(x) \quad = \quad (hx \bmod m,\ \ hx \bmod n)$$

where $h = g^{-1}(\bar{n}^2 n + \bar{m}^2 m)$, $\bar{n}$ is the inverse residue of $n \pmod m$, and $\bar{m}$ is the inverse residue of $m \pmod n$.

6.2.3 **Example** Let $N = 12$, $m = 3$, $n = 4$, and take $g = 1$. We have,

$$\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \otimes \begin{pmatrix} d & e & f & g \\ g & d & e & f \\ f & g & d & e \\ e & f & g & d \end{pmatrix} = \begin{pmatrix} ad & be & cf & ag & bd & ce & af & bg & cd & ae & bf & cg \\ cg & ad & be & cf & ag & bd & ce & af & bg & cd & ae & bf \\ bf & cg & ad & be & cf & ag & bd & ce & af & bg & cd & ae \\ ae & bf & cg & ad & be & cf & ag & bd & ce & af & bg & cd \\ cd & ae & bf & cg & ad & be & cf & ag & bd & ce & af & bg \\ bg & cd & ae & bf & cg & ad & be & cf & ag & bd & ce & af \\ af & bg & cd & ae & bf & cg & ad & be & cf & ag & bd & ce \\ ce & af & bg & cd & ae & bf & cg & ad & be & cf & ag & bd \\ bd & ce & af & bg & cd & ae & bf & cg & ad & be & cf & ag \\ ag & bd & ce & af & bg & cd & ae & bf & cg & ad & be & cf \\ cf & ag & bd & ce & af & bg & cd & ae & bf & cg & ad & be \\ be & cf & ag & bd & ce & af & bg & cd & ae & bf & cg & ad \end{pmatrix}$$

or, more succinctly,

$$\mathrm{CIRC}_3(a,\ b,\ c) \otimes \mathrm{CIRC}_4(d,\ e,\ f,\ g) \;=\; \mathrm{CIRC}_{12}(ad,\ be,\ cf,\ ag,\ bd,\ ce,\ af,\ bg,\ cd,\ ae,\ bf,\ cg)$$

6.3 **Tensors of Supercirculants.** Within the supercirculants, the tensor product of circulant subalgebras of coprime orders takes a particularly intuitive form. Since the supercirculants contain all circulant

algebras, the tensor product must also be a subalgebra. Clearly, it is one of order mn. Also, in the super-circulants (sticking with the matricial circulants), $\mathrm{U}_{mn}^{nx} = \mathrm{U}_m^x$. So, it is natural to try the map

$$\mathrm{U}_m^i \otimes \mathrm{U}_n^j \;\to\; \mathrm{U}_{mn}^{ni}\mathrm{U}_{mn}^{mj} \;=\; \mathrm{U}_{mn}^{ni+mj}$$

This map works; it is equivalent to that defined by $\phi_g : \mathbb{Z}_{mn} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ where $g = \bar{n}^2 n + \bar{m}^2 m \in \mathbb{Z}_{mn}$, and $\bar{n}$ and $\bar{m}$ are inverse residues modulo m and n respectively. Then, $\phi_g(ni + mj) \mapsto (i, j)$. Hence,

$$\text{if } A = \sum_{i\in\mathbb{Z}_m} a_i \mathrm{U}_m^i \in \mathrm{CIRC}_m, \text{ and } B = \sum_{j\in\mathbb{Z}_n} b_j \mathrm{U}_n^j \in \mathrm{CIRC}_n,$$

$$\text{then } A \otimes B \;=\; \sum_{i\in\mathbb{Z}_m} a_i \left(\mathrm{U}_{mn}^n\right)^i \sum_{j\in\mathbb{Z}_n} b_j \left(\mathrm{U}_{mn}^m\right)^j \;=\; AB \;\in\; \mathrm{CIRC}_{mn}$$

In other words, with this choice of ϕ_g, the tensor product is the circulant product. This applies equally to the eigenvalues with componentwise product, so we also get a simple formula for the tensor product in the eigenspace:

$$\lambda(A \otimes B) \;=\; \lambda(A)\,\lambda(B)$$

In ordinary circulants, this translates to

$$\lambda_x^{(mn)}(A \otimes B) \;=\; \lambda_{(x \bmod m)}^{(m)}(A)\,\lambda_{(x \bmod n)}^{(n)}(B)$$

We have demonstrated the following.

6.3.1 **Theorem** Let m, n be coprime.

(i) $\mathbf{circ}_m(R) \otimes \mathbf{circ}_n(R) \;\approx\; \mathbf{circ}_{mn}(R)$

(ii) The isomorphism is given by $\phi : \mathrm{u}_m^i \otimes \mathrm{u}_n^j \;\mapsto\; \mathrm{u}_{mn}^{in+jm}$.

(iii) In the eigenspace, the map is given by $\tilde{\phi} : \lambda_x^{(mn)}(a \otimes b) \;\mapsto\; \lambda_{(x \bmod m)}^{(m)}(a)\,\lambda_{(x \bmod n)}^{(n)}(b)$. □

A simple consequence of the construction of the tensor product is

6.3.2 **Corollary** Let $A \in \mathrm{CIRC}_m, B \in \mathrm{CIRC}_n$.
If $T = A \otimes B$ is $mn \times mn$ circulant then $\det T = (\det A)^n (\det B)^m$. □

How do we recognize a tensor product matrix? The following lemma gives a necessary condition which is useful for sparse matrices.

6.3.3 **Lemma** Let $T = \mathrm{CIRC}_{mn}(t) = A \otimes B$ be circulant with $A = \mathrm{CIRC}_m(a)$ and $B = \mathrm{CIRC}_n(b)$ and suppose a has x non-zero components and b has y non-zero components. Then, t has xy non-zero components. □

6.3.4 **Corollary** If $T = A \otimes B$ has a prime number, p, say, of non-zero components, then either a has p non-zero components and b has 1 or vice versa. □

6.4 Tensor Products and Polynomials in Several Variables

The homomorphism $\Gamma^n : R[x] \to \mathbf{circ}_n(R)$ of §3.3 will be generalized here to $\Gamma^{m,n} : R[x, y] \to \mathbf{circ}_{mn}(R)$.

The ring $R[x, y]$ is the tensor product $R[x] \otimes_R R[y]$ in a natural way: $(a_i x^i) \otimes (b_j y^i)$ is identified with $a_i x^i b_j y^j$. For m and n coprime, this suggests a definition of the map $\Gamma^{m,n}$ by requiring that it maps tensor products to the tensor products of §6.4. Thus

$$\Gamma^{m,n}\left(x^i \otimes y^i\right) \;=\; \mathrm{u}_m^i \otimes \mathrm{u}_n^j$$

$\Gamma^{m,n}$ is then extended to all of $R[x,y]$ by linearity, so that $\Gamma^{m,n} : \sum_{i\in\mathbb{Z}}\sum_{j\in\mathbb{Z}} a_{i,j}x^iy^j \mapsto \sum_{i\in\mathbb{Z}}\sum_{j\in\mathbb{Z}} a_{i,j}\mathrm{u}_{mn}^{in+jm}$

Here are another two though equivalent descriptions of $\Gamma^{m,n}$.

(i) It can be described as a substitution map

$$\Gamma^{m,n} : a(x,y) \mapsto a\left(\mathrm{u}_{mn}^n, \mathrm{u}_{mn}^m\right)$$

(ii) $\Gamma^{m,n}$ can be defined as the composition of $\tilde{\Gamma}_m^{mn}\Gamma^m$, acting on the variable x, with $\tilde{\Gamma}_n^{mn}\Gamma^n$, acting on the variable y.

$$\tilde{\Gamma}_m^{mn}\Gamma^m|_x\left(\tilde{\Gamma}_n^{mn}\Gamma^n|_y\left(a(x,y)\right)\right) \;=\; \tilde{\Gamma}_n^{mn}\Gamma^n\left(a\left(x,\mathrm{u}_{mn}^m\right)\right) \;=\; a\left(\mathrm{u}_{mn}^n,\mathrm{u}_{mn}^m\right) \;=\; \Gamma^{m,n}(a)$$

By Proposition 3.5.3, $\tilde{\Gamma}_m^{mn}\Gamma^m = \Gamma^{mn}\epsilon_x^m$ where $\epsilon_x^m : x \mapsto x^m$. Therefore, from the above,

$$\Gamma^{m,n} \;=\; \tilde{\Gamma}_m^{mn}\Gamma^m|_x\tilde{\Gamma}_n^{mn}\Gamma^n|_y \;=\; \Gamma^{mn}|_x\Gamma^{mn}|_y\epsilon_x^m\epsilon_y^n \;=\; \Gamma^{mn}S(x,y)\epsilon_x^m\epsilon_y^n$$

where $S(x,y) : f(x,y) \mapsto f(x,x)$.

6.4.1 **Proposition** Let $\Gamma^{m,n} : R[x,y] \to \mathbf{circ}_{mn}(R)$ be the map $\Gamma^{m,n}a(x,y) = a(\mathrm{u}_{mn}^m, \mathrm{u}_{mn}^n)$. Then

(i) $\Gamma^{m,n}$ is a ring homomorphism,

(ii) $\ker\Gamma^{m,n} \;=\; \ker\Gamma^m \vee \ker\Gamma^n \;=\; (x^m-1)+(y^n-1)$, and

(iii) $\Gamma^{m,n}\left(R[x,y]\right) = \tilde{\Gamma}_{mn/d}^{mn}\left(\mathbf{circ}_{mn/d}(R)\right)$ where $d = \gcd(m,n)$.

Proof.

(i) By the description in 6.4*(i)* above, $\Gamma^{m,n}$ is a substitution map, and so must be a ring homomorphism. QED *(i)*

(ii) Denote the ideal $(x^m-1)+(y^n-1)$ by J. It is trivial that $\Gamma^{m,n}(x^m-1) = \Gamma^{m,n}(y^n-1) = 0$,
$\therefore J \subset \ker\Gamma^{m,n}$.

Now assume $a(x,y) \in \ker\Gamma^{m,n}$. Let $\bar{a}(x,y)$ be the polynomial $a(x,y)$ reduced modulo the ideal J so that all powers of x and y in $\bar{a}$ are less than m and n respectively. Since $J \subset \ker\Gamma^{m,n}$, $\bar{a}(x,y) \in \ker\Gamma^{m,n}$. Since $\deg_x(\bar{a}) < m$ and $\deg_y(\bar{a}) < n$, $\Gamma^{m,n}$ maps $\bar{a}$ to the vector in $\mathbf{circ}_{mn}(R)$ whose components equal the coefficients of $\bar{a}$ which are therefore all zero since $\bar{a} \in \ker\Gamma^{m,n}$. Hence, $a \equiv 0 \pmod{J}$. Therefore, $a(x,y) \in \ker\Gamma^{m,n} \;\Rightarrow\; a(x,y) \in J$. QED *(ii)*

(iii) Let $\gcd(m,n) = d$, then $\Gamma^{m,n} : x^iy^j \mapsto \mathrm{u}_{mn}^{ni+mj} = \mathrm{u}_{mn}^{d(in'+jm')}$ where $m' = m/d,\ n' = n/d$. □

Chapter 7.
Circulant Rings over the Integers and the Rationals.

7.1 Introduction: The Group of Units in $\mathbf{circ}_N(\mathbb{Z})$.

This aim of this chapter is to characterize the structure of the integer circulants as a ring, and to do so we shall attempt to determine the group of units in $\mathbf{circ}(\mathbb{Z})$ (that is, the set of integer circulants whose inverses are also integer circulants). We shall not succeed in precisely specifying the group of units, but we shall come close in the case that N is prime and to a lesser extent when N is a prime power.

There are many more references to outside sources in this chapter than any other. This is because the chapter depends heavily on cyclotomic theory which has been an active field of mathematics since Gauss wrote Disquisitiones Arithmeticae in the eighteenth century. As a result, the proofs of several propositions needed in the chapter require too much background that is not germane to circulants. The reader will find that many of the results are taken from Washington's book on cyclotomic field theory [Was]. Edward's book is a very enjoyable historical introduction to cyclotomic integers and ideals [Edw]. In general, we can highly recommend Karpilovsky's book [Kar1] for a lucid exposition of unit groups in rings, and Seghal's book [Seg] has the most relevant results to this chapter, most particularly, it gives a detailed introduction to the Bass Independence Theorem and the Bass units. Finally, Appendix A has a summary of the basic facts on cyclotomic domains.

Section 3.4 gave us the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (x^N-1) & \longrightarrow & R[x] & \xrightarrow{x\to \mathrm{u}} & \mathbf{circ}_N(R) & \longrightarrow & 0 \\ & & & & & \searrow^{x\to\zeta} & \downarrow{\scriptstyle \mathrm{u}\to\zeta} & & \\ & & & & & & R_\zeta & & \\ & & & & & & \downarrow & & \\ & & & & & & 0 & & \end{array}$$

and when $R=\mathbb{Z}$, Proposition 3.4.5 gives the following exact sequence:

$$0 \;\to\; (x^N-1) \;\to\; (\Phi_N(x)) \;\to\; \mathbf{circ}_N(\mathbb{Z}) \;\to\; \mathbb{Z}_\zeta \;\to\; 0$$

So the integer circulants are in a sense sandwiched between the polynomials and the cyclotomics. Many of the properties of circulants are inherited from the polynomial ring, for instance, the convolution product. But many of the properties of integer and rational circulants are also constrained by the homomorphism to the cyclotomics. This is especially so of the group of units within the circulants.

7.2.1 Definition Let R be any commutative ring with 1. Define $\mathbf{U}(R)$ to be the group of units in R.

We shall call the group of units in $\mathbf{circ}(R)$ the (group or set of) R **circulant units** and we shall call any member of the group an R-**circulant unit**, but when $R=\mathbb{Z}$, we shall say simply circulant unit, and we shall call $\mathbf{U}(\mathbf{circ}(\mathbb{Z}))$ simply the circulant units.

7.2.2 Proposition Let R be any commutative ring with 1, and let $a \in \mathbf{circ}_N(R)$. Then,

$$a \in \mathbf{U}(\mathbf{circ}_N(R)) \quad\Leftrightarrow\quad \Delta(a) \in \mathbf{U}(R)$$

Proof. ($\Rightarrow$:) If a is a unit, then $ab=1$ for some $b \in \mathbf{circ}_N(R)$. Therefore, $\Delta(a)\Delta(b)=1$. That is, $\Delta(a) \in \mathbf{U}(R)$.
($\Leftarrow$:) Let $A=\mathrm{CIRC}_N(a)$ be the circulant matrix for a and assume $\det A \in \mathbf{U}(R)$. Let A^* be the cofactor matrix for A; that is, A^*_{ij} is the determinant obtained from A by deleting the i^{th} row and j^{th} column. Then, (for instance, by Cramer's Rule), A^{-1} exists and is given by $A^{-1}=A^*(\det A)^{-1}$. All entries in the cofactor matrix are in R, and $(\det A)^{-1} \in R$, so A^{-1} is in $\mathbf{circ}_N(R)$. □

Therefore, $\mathbf{U}(\mathbf{circ}(\mathbb{Z})) = \{\pm 1\} \times \mathrm{SL} \cap \mathbf{circ}(\mathbb{Z})$, and if R is a field, then $\mathbf{U}(\mathbf{circ}(R))$ is the set of non-singular circulant matrices.

For p prime, there is a close connection between the determinant, $\Delta_p(a)$, and the cyclotomic norm of $\lambda_1(a)$ (see Appendix A for the definition of the norm).

$$\mathcal{N}_p\big(\lambda_1(a)\big) \;=\; \frac{\Delta_p(a)}{\lambda_0(a)}$$

More generally, applying Proposition 3.2.18 Part *(iii)* to $Q = \mathbb{Q}$, we have

7.2.3 **Proposition** If $a \in \mathbf{circ}_N(\mathbb{Q})$, then

$$\Delta_N(a) \;=\; \pm \prod_{d|N} \mathcal{N}_{N/d}\lambda_d(a)$$

where the sign is the sign of $\lambda_0(a)$ if N is odd, and is otherwise the sign of $\lambda_0(a)\lambda_{N/2}(a)$. □

The next proposition on cyclotomic units is analagous to Proposition 7.2.2. One easily sees that the norm is multiplicative, $\mathcal{N}_n(\alpha\beta) = \mathcal{N}_n(\alpha)\mathcal{N}_n(\beta)$, and that $\mathcal{N}_n(1) = 1$. Also, the norm of an irrational is a positive integer. These facts give:

7.2.4 **Proposition** Let $\alpha \in \mathbb{Z}(\zeta_n)$. α is a unit iff $\mathcal{N}_n(\alpha) = 1$.

Proof. We shall first dispense with the case $n \leq 2$. In this case the cyclotomic domain is the (rational) integers whose units are ± 1. The norm in the domain is the absolute value function from which follows the desired result for $n \leq 2$.

Now assume that $n > 2$.
$(\Rightarrow:)$ If α is a unit in $\mathbb{Z}(\zeta_n)$ with inverse β say, then $\alpha\beta = 1$, $\mathcal{N}_n(\alpha)\mathcal{N}_n(\beta) = 1$, and so $\mathcal{N}_n(\alpha) = \mathcal{N}_n(\beta) = 1$.
$(\Leftarrow:)$ If $\mathcal{N}_n(\alpha) = 1$ then either α is rational, in which case $\alpha = \pm 1$ and is clearly a unit, or α is algebraic, in which case, $\alpha\beta = 1$ where β is the product of the algebraic conjugates of α (excluding α). □

From this proposition and Corollary 3.2.17.1 of the Circulant Decomposition Theorem we see that c is a circulant unit iff $\lambda_d(c)$ is a cyclotomic unit for each divisor d of N. This is the next proposition.

7.2.5.1 **Corollary** $c \in \mathbf{U}(\mathbf{circ}_N(\mathbb{Z})) \quad \Leftrightarrow \quad \forall d \,|\, N, \quad \lambda_d(c) \in \mathbf{U}(\mathbb{Z}(\zeta_N))$ □

In a sense, Proposition 7.2.5 has reduced the question of the finding the unit group of the integer circulants to a question in cyclotomic domains. However, even assuming we have knowledge of units in cyclotomic domains, it is still not an easy matter in general to find rational integers $a_0, a_1, \ldots, a_{N-1}$ such that $a_0 + a_1\zeta^d + a_2\zeta^{2d} + \cdots$ for $d \,|\, N$ are all units in the cyclotomic integers.

We can similarly use the Circulant Decomposition Theorem to completely determine the unit group of the rational circulants.

7.2.5.2 **Proposition**

$$\mathbf{U}(\mathbf{circ}_N(\mathbb{Q})) \;\approx\; \prod_{d|\,N} \mathbb{Q}(\zeta_d)^*$$

In particular, if $c \in \mathbf{circ}_N(\mathbb{Q})$, then

$$c \in \mathbf{U}(\mathbf{circ}_N(\mathbb{Q})) \;\Leftrightarrow\; \Delta(c) \neq 0 \;\Leftrightarrow\; \lambda_d(c) \neq 0, \quad \forall d \,|\, N \;\square$$

We conclude this section with the introduction of a useful ring homomorphism, ℓ, defined on cyclotomic domains of prime power order, p^n say, and taking values in $\mathbb{Z}_p$. This is defined next.

7.2.6 **Definition** For $q = p^m$ where p is prime, and for all $\xi \in \mathbb{Z}(\zeta_q)$, define $\ell_p : \mathbb{Z}(\zeta_q) \to \mathbb{Z}_p$ by $\ell_p(\xi) = \lambda_0(x) \bmod p$ where x satisfies $\lambda_1^{(q)}(x) = \xi$.

That is, ℓ_p is defined to agree with λ_1 and λ_0 in the following diagram.

$$\begin{array}{ccc} \mathbf{circ}_q(\mathbb{Z}) & \xrightarrow{\lambda_0} & \mathbb{Z} \\ {\scriptstyle\lambda_1}\downarrow & & \downarrow{\scriptstyle \bmod\ p} \\ \mathbb{Z}(\zeta_q) & \xrightarrow{\ell_p} & \mathbb{Z}_p \end{array} \tag{1}$$

7.2.7 **Proposition** Let $q = p^m$. Then, $\ell_p : \mathbb{Z}(\zeta_q) \to \mathbb{Z}_p$ is a well-defined ring homomorphism and is equivalent to the natural map $\mathbb{Z}(\zeta_q) \to \mathbb{Z}(\zeta_q)/(1-\zeta_q)$; it is arithmetically given by

$$\ell\left(\sum_{i=0}^{p-1} a_i\zeta^i\right) \;=\; \left(\sum_{i=0}^{p-1} a_i\right) \bmod p$$

Proof. Firstly, λ_1 is onto $\mathbb{Z}(\zeta)$, so every cyclotomic integer has a circulant mapped to it by λ_1.

By Corollary 3.4.6, $\ker\lambda_1 = \left(p\bar{\delta}^p\right)$. Now, $\lambda_0\left(p\bar{\delta}^p\right) = p$. Therefore, $\ker\lambda_1$ is contained by the kernel of the map $\lambda_0 \bmod p$. This shows that ℓ_p is well-defined.

The three maps λ_1, λ_0, and mod$p$ are ring homomorphisms, so ℓ_p must also be a ring homomorphism. The formula is obtained by substituting u in $\mathbf{circ}_q(\mathbb{Z})$ for ζ throughout any expression for ξ in terms of powers of ζ.

Lastly, we have to show that $\ell_p : \mathbb{Z}(\zeta_q) \to \mathbb{Z}(\zeta_q)/(1-\zeta_p)$. Each element in the ring $\mathbb{Z}(\zeta)$ can be reduced modulo $(1-\zeta)$ to the sum of the coefficients of its constituent powers of ζ since every power of ζ can be replaced by 1. Now, $\mathcal{N}_q(1-\zeta_q) = p$, therefore by the properties of the algebraic norm, $|\mathbb{Z}(\zeta)/(1-\zeta)| = p$ which can only mean that $\mathbb{Z}(\zeta)/(1-\zeta) \approx \mathbb{Z}_p$. □

Why restrict the definition of the ℓ map to prime powers? The reason is that when N is divisible by two or more distinct primes, diagram (1) might not be commutative. The commutativity of the diagram depends on $\lambda_0 \ker\lambda_1 \in (\Phi_N(1))$. If $N = p^n$, then p divides $\Phi_N(1)$ and diagram (1) is commutative, but when N is divisible by p and other primes, p no longer necessarily divides $\Phi_N(1)$. (See Examples *(v)* to *(viii)* in Appendix A3; also in Example *(iii)* apply L'Hôpital's Rule twice to see that $\Phi_{pq}(1) = 1$.)

7.2.8 **Corollary** Let $q = p^m$ with p prime, and let $a(x) \in \mathbb{Z}[x]$. Then, $\ell_p\left(a(\zeta^i)\right) = \ell_p\left(a(\zeta^j)\right)$ for all i, j.

Proof. $\lambda_0\left(a(\mathrm{u}^i)\right) = \lambda_0\left(a(\mathrm{u}^j)\right)$. □

Using Proposition 3.2.16 we can completely characterize the eigenspace, $\Lambda_p(\mathbb{Z})$, for p prime.

7.2.9 **Proposition** Let $\zeta = \zeta_p$ where p is prime. Let $\mu = (\mu_0, \mu_1, \ldots, \mu_{p-1}) \in \mathbb{Z}_\zeta^p$. Let $c = \lambda^{-1}(\mu)$. Let $G = \{g_h : \zeta \mapsto \zeta^h\}$ be the Galois automorphisms on $\mathbb{Z}_\zeta$. Then,

$$c \in \mathbf{circ}_p(\mathbb{Z}) \quad \Leftrightarrow \quad g_h(\mu_1) = \mu_h,\ \forall g_h \in G, \ \text{ and } \ \mu_0 \in \mathbb{Z} \text{ with } \mu_0 \equiv \ell_p(\mu_1) \pmod p$$

Proof. ($\Rightarrow$:) The implication in this direction follows immediately from propositions 3.2.16 and 7.2.7.
($\Leftarrow$:) We are given that $g_h(\mu_1) = \mu_h$, for all $g_h \in G$. Proposition 3.2.16 implies that $c \in \mathbf{circ}_p(\mathbb{Q})$.

It remains to show that c integral. Since c_i is rational, and since each μ_j is a cyclotomic integer, we have $pc_i \in \mathbb{Q} \cap \mathbb{Z}_\zeta = \mathbb{Z}$. So we need only show that pc_i is divisible by p.

Since $\mu_1 \in \mathbb{Z}_\zeta$, we can write $\mu_1 = a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1} = a(\zeta)$ for some $a(x) \in \mathbb{Z}[x]$. By the given Galois transformations, $\mu_h = a(\zeta^h)$. By Corollary 7.2.8, $\ell_p(\mu_i) = \ell_p(\mu_1)$ for all $i \neq 0$. But, it is given that $\mu_0 \equiv \ell_p(\mu_1)$. Therefore, $\mu_0 \equiv \ell_p(\mu_i)$ for all i. Now consider $\ell_p(pc_i)$. It is given by

$$\ell_p\left(\sum_{j=0}^{p-1} \mu_i\zeta^{-ij}\right) \;=\; \sum_{j=0}^{p-1} \ell_p(\mu_i) \;=\; p\mu_0 \;=\; 0 \quad (\text{in } \mathbb{Z}_p)$$

This shows that p divides pc_i and so $c_i \in \mathbb{Z}$. □

Next is defined a multiplicative endomorphism on circulants which has a close connection with the cyclotomic norm.

7.2.10 **Definition** For any commutative ring R with 1, define $\nu_* : \mathbf{circ}_N(R) \to \mathbf{circ}_N(R)$ by

$$\nu_*(a) \ := \ \prod_{h \in \mathbb{Z}_N^*} \nu_h(a)$$

where ν_h is the position multiplier homomorphism of §3.12.

7.2.11 **Proposition** Let $a \in \mathbf{circ}_N(R)$. Then, $\nu_*(a)$ is a residue class circulant. Furthermore, if $a \in \mathbf{circ}_N(\mathbb{Z})$ then every eigenvalue of $\nu_*(a)$ is a rational integer.

Proof. By §3.12.2, the ν_*-induced map on the eigenspace is

$$\begin{aligned} \bar{\nu}_* : \lambda_i(a) \ \mapsto \ \prod\{\lambda_{ij}(a) \vdash j \in \mathbb{Z}_N^*\} \ &= \ \prod\{\lambda_{dj}(a) \vdash j \in \mathbb{Z}_N^*\} \quad \text{where } d = \gcd(i, N) \\ &= \ \mathcal{N}_N\left(\lambda_d(a)\right) \end{aligned}$$

This shows that $\bar{\nu}_*(a)_i$ depends only on $\gcd(i, N)$. That is, $\lambda(\nu_*(a))$ is a residue class vector. Hence, by Proposition 5.1.2, a is a residue class circulant.

If $R = \mathbb{Z}$ then the above formula shows that $\bar{\nu}_*(a)_i = \mathcal{N}_N\left(\lambda_d(a)\right)$ where $d = \gcd(i, N)$ and this is an integer. □

In certain cases, we can use Propositions 7.2.9 and 7.2.11 to find the residue of a cyclotomic norm with respect to the degree of the cyclotomic domain.

7.2.12 **Proposition** Let $q = p^m$ where p is an odd prime and $m > 0$. Let $\alpha \in \mathbb{Z}(\zeta_q)$. Then,

$$\mathcal{N}_q(\alpha) \ \equiv \ \left\{ \begin{matrix} 0 & \text{if } \ell_p(\alpha) = 0 \\ 1 & \text{otherwise} \end{matrix} \right\} \pmod p$$

Proof. Let $\alpha = a_0 + a_1\zeta + \cdots + a_{q-1}\zeta^{q-1}$, and let $n = a_0 + a_1 + \cdots + a_{q-1}$. Suppose first that $p \,|\, n$. Then, $\ell_p(\alpha_i) = 0$ for all conjugates α_i of α by Proposition 7.2.9. Therefore, $\ell_p\left(\mathcal{N}(\alpha)\right) = 0$. That is, $p \,|\, \mathcal{N}(\alpha)$.

We can now assume that $n \not\equiv 0$. Let $a = a_0 + a_1\mathrm{u} + \cdots + a_{p-1}\mathrm{u}^{p-1} \in \mathbf{circ}_p(\mathbb{Z})$.

$$\lambda(\nu_*(a)) \ = \ \left(\lambda_0(a)^{\phi(q)}, \ \mathcal{N}_q\left(\lambda_1(a)\right), \ \ldots, \ \text{etc.}\right)$$

$$\begin{aligned} 1 \ &\equiv \ \lambda_0(a)^{\phi(q)} && \text{since } \lambda_0(a) = n \not\equiv 0 \pmod p \\ &\equiv \ \ell_p\left(\mathcal{N}\left(\lambda_1(a)\right)\right) && \text{by Corollary 7.2.8} \\ &= \ \ell_p\left(\mathcal{N}(\alpha)\right) && = \ \mathcal{N}(\alpha) \ \square \end{aligned}$$

7.3 Circulant and Cyclotomic Units of Finite Order.

Recall that if G is any group, that the **torsion** of G is the set of elements in G of finite order and is denoted by $\mathrm{t}G$. Thus, $\mathrm{t}\mathbf{U}\left(\mathbf{circ}_N(\mathbb{Z})\right)$ is the set of circulant units of finite order. Since an integer circulant of finite order is necessarily a unit and (i.e. an unimodular matrix), we abuse notation slightly, and simplify $\mathrm{t}\mathbf{U}\left(\mathbf{circ}_N(\mathbb{Z})\right)$ to $\mathrm{t}\mathbf{circ}_N(\mathbb{Z})$.

This section determines the torsion of $\mathbf{circ}_N(\mathbb{Z})$, and section following this one will do the same for the torsion of the rational circulants. It may seem a little strange for us to be treating the torsion subgroup before we describe the full unit group. We do so simply because it much the easiest task; indeed, there is as yet no complete description of the full group of circulants units.

This investigation will require additional facts from cyclotomic theory including one of Kummer's famous results, and some other notable theorems from ring theory.

We shall prove that $\mathbf{tcirc}_N(\mathbb{Z}_N) = \{\pm \mathrm{u}_N^i \vdash i \in \mathbb{Z}_N\}$, and that $\mathbf{U}(\mathbf{circ}_N(\mathbb{Z}))$ is finite and is therefore equal to $\mathbf{tcirc}_N(\mathbb{Z}_N)$ if and only if $N = 1, 2, 3, 4,$ or 6. We shall then characterize $\mathbf{U}(\mathbf{circ}_N(\mathbb{Z}))$ when it is infinite, that is when $N = 5$ or $N > 6$.

7.3.1 **Lemma** If λ is an algebraic integer all of whose (algebraic) conjugates have absolute value 1, then λ is a root of unity.

Proof. [Was2]

Let λ be algebraic of degree n, say, and suppose λ and all its $n-1$ algebraic conjugates have absolute value 1.

If λ is not a root of unity, then the set $\{\lambda^r \vdash r \in \mathbb{N}\}$ is infinite. Therefore, there must be an infinite number of irreducible polynomials with a power of λ as a root. Now, $\lambda^r \in \mathbb{Q}(\lambda)$. Therefore, λ^r is of degree at most n. So, there must be an infinite number of irreducible polynomials of degree n or less with a power of λ as a root.

Let $\alpha_1 = \lambda^r$ for some r, and let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be the conjugates of α_1 where $m \leq n$. Then,

$$f(x) \;=\; \prod_{i=1}^{m}(x - \alpha_i)$$

is the irreducible monic polynomial for α_1. This polynomial must have integer coefficients, so

$$f(x) \;=\; \sum_{i=0}^{m} c_i x^i \quad \text{where } c_i \in \mathbb{Z},\ \forall i$$

$$\text{Now, } c_0 \;=\; \prod_{i=1}^{m} \alpha_i \;=\; 1 \text{ by hypothesis.}$$

$$\text{Similarly, } |c_1| \;=\; \left|\sum_{j=1}^{m}\prod_{i\neq j} \alpha_i\right| \;\leq\; \sum_{j=1}^{m}\prod_{i\neq j} |\alpha_i| \;\doteq\; m$$

Proceeding thus, it is clear that $|c_i| \leq m^i \leq n^i$ for all i. This means that there are only a finite number of polynomials with powers of λ as a root. Contradiction. Therefore, the powers of λ are not all distinct. □

In the case that the algebraic element is in a cyclotomic field, there is a more powerful result.

7.3.2 **Lemma** [Was] If $\alpha \in \mathbb{Q}(\zeta_N)$ and $|\alpha| = r \in \mathbb{Q}$ then $|\alpha_i| = r$ for all algebraic conjugates, α_i, of α.

Proof. Let $\zeta = \zeta_N$. The Galois group for $\mathbb{Q}(\zeta)/\mathbb{Q}$ is $\{\nu_h \vdash \nu_h : \zeta \mapsto \zeta^h \text{ with } h \in \mathbb{Z}_N^*\}$. So, we can label α and its conjugates by $h \in \mathbb{Z}_N^*$. Thus, $\alpha = \alpha_1$.

It is easy to see that complex conjugation commutes with the operations of the Galois group.

$\therefore\ r^2 = \nu_h(r^2) = \nu_h(\alpha\bar{\alpha}) = \nu_h(\alpha)\nu_h(\bar{\alpha}) = \nu_h(\alpha)\overline{\nu_h(\alpha)} = |\alpha_h|^2$. □

7.3.3 **Lemma** Let $\alpha \in \mathbb{Z}(\zeta_N)$. $|\alpha| = 1$ iff α is a root of unity.

Proof. Take $r = 1$ in the previous lemma and apply Lemma 7.3.1. □

7.3.4 **Lemma** Any root of unity in $\mathbb{Q}(\zeta_N)$ is of the form $\pm\zeta_N^i$ for some i.

Proof. Clearly, the rational roots of unity, ± 1, are of the required form. So let ξ be a root of unity which is not rational and is contained in $\mathbb{Q}(\zeta_N)$. From analysis, we know that $\xi = \zeta_M^r = e^{2r\pi\iota/M}$ where r, M are positive integers and w.l.o.g. r is coprime to M. Since r is coprime to M, r has an inverse in $\mathbb{Z}_M$, $\bar{r}$, say. Now, $\xi^{\bar{r}} \in \mathbb{Q}(\zeta_N)$. Therefore, $\zeta_M = (\zeta_M^r)^{\bar{r}}$ must also be a root of unity in $\mathbb{Q}(\zeta_N)$.

Now suppose that ζ_M is not of the form $\pm\zeta_N$. Then M cannot divide N. Let m be the greatest divisor of M which is coprime to N. That is, $m = M/\gcd(M,N)$. Then, $\zeta_M^{M/m} = \zeta_m \in \mathbb{Q}(\zeta_N)$. Therefore, $\zeta_m\zeta_N \in \mathbb{Q}(\zeta_N)$. Since m is coprime to N, the order of $\zeta_m\zeta_N$ is mN. Therefore, $\zeta_{mN} \in \mathbb{Q}(\zeta_N)$. But, $\dim[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \deg\Phi_n(x)$ since, by definition of the cyclotomic polynomial, $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = [\mathbb{Q}[x]:(\Phi_n(x))]$. Therefore, $\phi(mN) = \deg\Phi_{mN} \leq \deg\Phi_N = \phi(N)$. By assumption, M does not divide N and so $m > 1$. This is possible only if N is odd and $m = 2$ in which case $\zeta_{mN} = -\zeta_N$.

Therefore, $M/\gcd(M,N) = 1$ if N is even and is $= 1$ or 2 if N is odd. So if N is even, $M \mid N$ as required. If N is odd, then $\zeta_M = -\zeta_N$ also as required. □

We now have enough facts to deduce results for circulant matrices. The first lemma on circulants looks trivial, and indeed is trivial if $c_i = a_i$ in the lemma statement. But the point is that cyclotomic integers satisfy various linear relationships, therefore there are several ways to represent an eigenvalue of a circulant. For example, if $a = \mathrm{u}^k \in \mathbf{circ}_N(\mathbb{Z})$ then $\lambda_1(a) = \zeta^k = \zeta^k + \sum_{i=0}^{N/d-1}\zeta^{id}$, where d is any divisor of N. The lemma tells us that no matter which representation we take for $\lambda_1(a)$, provided j is coprime to N, we will obtain the correct value for $\lambda_j(a)$ by substituting ζ^j for ζ throughout the chosen expression for $\lambda_1(a)$.

7.3.5 **Lemma** Let $d \mid N$, j be coprime to N, $a \in \mathbf{circ}_N(\mathbb{Q})$, and let $c_0, c_1, \ldots, c_{N-1}$ be rationals.

(i) If $\lambda_d(a) = \sum_{i\in\mathbb{Z}_N} c_i\zeta^i$ then $\lambda_{jd}(a) = \sum_{i\in\mathbb{Z}_N} c_i\zeta^{ij}$

(ii) If $a, b \in \mathbf{circ}_N(\mathbb{Q})$ and $\lambda_d(a) = \lambda_d(b)$ then $\lambda_{jd}(a) = \lambda_{jd}(b)$.

(iii) If $a \in \mathbf{circ}_N(\mathbb{Q})$ then $\lambda_d(a) = 0$ iff $\lambda_{jd}(a) = 0$.

Proof. All three statements are equivalent and are corollaries of Proposition 3.2.13 □

The elements of $\mathbf{circ}_N(R)$ which are of finite multiplicative order are those elements which are roots of unity in $\mathbf{circ}_N(R)$. They form a subgroup of the circulant units and this subgroup is clearly the torsion part of the group of units.

7.3.6 **Definition**

(i) $\mathcal{T}_N := \{\pm\mathrm{u}^i \vdash i \in \mathbb{Z}_N\} \subset \mathbf{circ}_N(\mathbb{Z})$.

(ii) $\hat{\mathcal{T}}_N := \{\pm(2\bar{\delta}^N - \mathrm{u}^i) \vdash i \in \mathbb{Z}_N\} \subset \mathbf{circ}_N(\mathbb{Q})$. (See §3.2 for definition of $\bar{\delta}^N$.)

The set $\mathcal{T}_N$ is a subgroup of $\mathbf{U}(\mathbf{circ}_N(\mathbb{Z}))$ and is called the group of **trivial units** of $\mathbf{circ}_N(\mathbb{Z})$. Although $\hat{\mathcal{T}}_N$ is not a group, the union $\mathcal{T}_N \cup \hat{\mathcal{T}}_N$ is a finite subgroup of $\mathbf{circ}_N(\mathbb{Q})$.

7.3.7 **Lemma** $\mathcal{T}_N \cup \hat{\mathcal{T}}_N$ is a subgroup of $\mathrm{t}\mathbf{U}(\mathbf{circ}_N(\mathbb{Q}))$.

Proof. It is obvious that the eigenvalues of u^k are $\lambda_i(\mathrm{u}^k) = \zeta^{ik}$ and are N^{th} roots of unity.

Now, $\bar{\delta}^N = N^{-1}(1,1,\ldots,1)$. $\therefore \lambda(\bar{\delta}^N) = (1,0,0,\ldots,0)$. $\therefore \lambda(\mp2\bar{\delta}^N \pm \mathrm{u}^i) = \pm(1,-\zeta^i,-\zeta^{2i},\ldots)$. The eigenvalues of a general product $\mathrm{u}^k(\mp2\bar{\delta}^N \pm \mathrm{u}^i)$ are therefore

$$\lambda_j(\mathrm{u}^k(\mp2\bar{\delta}^N \pm \mathrm{u}^i)) = \pm\zeta^{j(k+i)} = \mp\lambda_j(2\bar{\delta}^N \pm \mathrm{u}^{k+i})$$ □

7.3.8 **Lemma**

(i) $\mathrm{t}(\mathrm{GL}_N \cap \mathbf{circ}_N(\mathbb{Q})) = \mathrm{t}\mathbf{U}(\mathbf{circ}_N(\mathbb{Q}))$.

(ii) If $a \in \mathrm{t}\mathbf{U}(\mathbf{circ}_N(\mathbb{Q}))$ then $\lambda(a) = (\pm\zeta_N^{t_0}, \pm\zeta_N^{t_1}, \ldots, \pm\zeta_N^{t_{N-1}})$ for some integers $t_0, t_1, \ldots, t_{N-1}$.

Proof.

(i) The first statement is obvious since a matrix (in this case a circulant matrix) can be of finite order only if it has unit determinant.

(ii) Let $A = \mathrm{CIRC}(a) \in \mathbf{U}(\mathbf{circ}_N(\mathbb{Q}))$. By assumption, A is of finite order, $A^L = I$, say. Therefore, the eigenvalues of A are L^{th} roots of unity. But the eigenvalues of A are in $\mathbb{Q}(\zeta_N)$. By Lemma 7.3.4, this forces $\pm\zeta_L \in \{\zeta_N^i \vdash i \in \mathbb{Z}_N\}$. Therefore, the eigenvalues of A must be $(\pm\zeta_N^{t_0}, \pm\zeta_N^{t_1}, \ldots, \pm\zeta_N^{t_{N-1}})$ for some $t_i \in \mathbb{Z}_N$. □

7.3.9 **Lemma** Let p be an odd prime. Then, $\mathrm{t}\mathbf{U}\left(\mathbf{circ}_p\left(\mathbb{Q}\right)\right) \;=\; \mathcal{T}_p \cup \hat{\mathcal{T}}_p$.

Proof. The inclusion $\mathcal{T}_p \cup \hat{\mathcal{T}}_p \subset \mathrm{t}\mathbf{U}\left(\mathbf{circ}_p\left(\mathbb{Q}\right)\right)$ was proved in Lemma 7.3.7. So we need only prove the reverse inclusion.

Let $a \in \mathrm{t}\mathbf{U}\left(\mathbf{circ}_p\left(\mathbb{Q}\right)\right)$. By the previous lemma, for each $i \neq 0$, $\exists r$ such that $\lambda_i(a) = \pm\zeta^r$. In fact, by takin $k = i^{-1}r \bmod p$, we can suppose w.l.o.g. that $\lambda_i(a) = \pm\zeta^{ik}$ for some $k \in \mathbb{Z}_p$.

$$\sum_j a_j\zeta^{ij} \;=\; \pm\zeta^{ik} \;=\; \sigma\zeta^{ik}, \quad \text{where } \sigma = \pm 1$$

$$\therefore \sum_{j\neq k} a_j\zeta^{ij} \;=\; -(a_k-\sigma)\zeta^{ik} \;=\; (a_k-\sigma)\sum_{j\neq k}\zeta^{ij}$$

Choose as a basis for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$, the set $\{\zeta^s \vdash s \in \mathbb{Z}_p\} - \{\zeta^k\}$. The above equation implies that

$$a_j \;=\; a_k - \sigma, \;\forall j \neq k$$

Using this, we can calculate $\lambda_0 = (p-1)(a_k-\sigma) + a_k = pa_k - \sigma(p-1)$. By hypothesis, $|\lambda_0| = 1$

$$\therefore pa_k - \sigma(p-1) \;=\; \pm 1 \quad (\text{ where } \sigma = \pm 1)$$

$$\therefore a_k \;=\; \sigma \text{ or } \sigma\cdot\left(1-\frac{2}{p}\right)$$

$$\therefore a_j \;=\; 0 \text{ or } -\sigma\frac{2}{p} \quad \text{for } j \neq k$$

$$\therefore a \;=\; \sigma\mathrm{u}^k \text{ or } -\sigma\left(2\bar{\delta}^p - u^k\right)$$

This shows that a is in one of the sets in the statement. □

The next proposition can be deduced immediately from the above for N prime, but since it applies to general N, we must prove it afresh.

7.3.10 **Proposition** $\mathrm{t}\mathbf{circ}_N(\mathbb{Z}) \;=\; \mathcal{T}_N$.

Proof. Let $a \in \mathrm{t}\mathbf{circ}_N(\mathbb{Z})$. From Lemma 7.3.8, $\lambda_j(a) = (\sigma_0\zeta_N^{t_0}, \sigma_1\zeta_N^{t_1}, \ldots, \sigma_{N-1}\zeta_N^{t_{N-1}})$ for some $t_i \in \mathbb{Z}_N$, and $\sigma_i \in \{\pm 1\}$. Applying the map λ^{-1} we see that

$$a_i \;=\; \frac{1}{N}\sum_{j\in\mathbb{Z}_N}\sigma_j\zeta^{t_j-ij}, \quad \forall i \in \mathbb{Z}_N \quad \Rightarrow \quad |a_i| \leq 1 \quad \Rightarrow \quad a_i \in \{0, \pm 1\}$$

So suppose for non-triviality that $|a_k| = 1$ for some k.

$$\text{But, } |a_k| = 1 \;\Leftrightarrow\; \left|\sum_{j\in\mathbb{Z}_N}\sigma_j\zeta^{t_j-kj}\right| \;=\; N \;=\; \sum_{j\in\mathbb{Z}_N}\left|\sigma_j\zeta^{t_j-kj}\right|$$

$$\Leftrightarrow\; \sigma_j\zeta^{t_j-kj} = \varepsilon_k\zeta^{t_0} \text{ for some } t_0 \text{ and where } \varepsilon_k = \pm 1, \;\forall j$$

$$\Leftrightarrow\; t_j - kj \equiv t_0 \pmod N, \text{ and } \sigma_j = \varepsilon_k, \;\forall j \in \mathbb{Z}_N$$

$$\therefore a_k \;=\; \frac{1}{N}\sum_{j\in\mathbb{Z}_N}\sigma_j\zeta^{t_j-kj} \;=\; \frac{1}{N}\sum_{j\in\mathbb{Z}_N}\varepsilon_k\zeta^{t_0} \;=\; \varepsilon_k\zeta^{t_0}$$

$$\therefore \varepsilon_k\zeta^{t_0} = \pm 1 \text{ since } a_k \in \mathbb{Z}. \;\therefore\; \text{W.l.o.g. } \zeta^{t_0} = 1$$

$$\therefore a_i \;=\; \frac{1}{N}\sum_{j\in\mathbb{Z}_N}\varepsilon_k\zeta^{t_0+kj-ij} \;=\; \varepsilon_k\delta_{k-i} \;=\; \pm\delta_{k-i}$$

Therefore, there is at most one non-zero entry in $(a_0, a_1, \ldots, a_{N-1})$ and that entry is ± 1. To be a unit, there must be at least one non-zero entry. $\therefore a = \pm\mathrm{u}^n$ for some i. □

7.3.11 **Theorem** $\mathbf{U}(\mathbf{circ}_N(\mathbb{Z})) = \mathcal{T}_N$ for $N = 1, 2, 3, 4,$ and 6.

Proof. Let $a \in \mathbf{U}(\mathbf{circ}_N(\mathbb{Z}))$ with eigenvalues $\lambda_0, \lambda_1, \ldots, \lambda_{N-1}$. The theorem is trivial for $N = 1$ and 2. For $N = 3$ and 4, notice that there are only two complex eigenvalues, namely λ_1 and λ_{N-1}, and all other eigenvalues are rational integers. Therefore, each of the rational eigenvalues must be ± 1. Since $\Delta_N = \pm 1$ then so must $\lambda_1\lambda_{N-1} = \pm 1$. But, $\lambda_1\lambda_{N-1} = |\lambda_1|$. $\therefore$ $|\lambda_1| = 1$ and so λ must be a root of unity, and in particular, a is of finite order and Proposition 7.3.10 applies.

Lastly, let $N = 6$. In this case, there are four complex eigenvalues, $\lambda_1, \lambda_2, \lambda_4, \lambda_5$. Let $a \in \mathbf{U}(\mathbf{circ}_6(\mathbb{Z}))$ and consider $b = \Gamma_6^3(a)$. By Proposition 3.5.3, $\Delta_3(b) \mid \Delta_6(a)$. $\therefore$ $\Delta(b) = \pm 1$. So, by the previous cases, $|\lambda_1(b)| = |\lambda_2(b)| = 1$. Therefore, by Proposition 3.5.2, $|\lambda_2(a)| = |\lambda_4(a)| = 1$. Therefore, $\lambda_2(a)\lambda_4(a) = 1$ since $\bar{\lambda}_2(a) = \lambda_4(a)$. Now, $\pm 1 = \Delta(a) = (\lambda_0)(\lambda_3)(\lambda_2\lambda_4)(\lambda_1\lambda_5)$. Therefore, $\pm 1 = \lambda_1\lambda_5 = |\lambda_1|^2$, and so all eigenvalues are roots of unity by Lemma 7.3.3 and a has finite order by Lemma 7.3.4. □

The converse of this proposition is also true. That is, $\mathbf{U}(\mathbf{circ}_N(\mathbb{Z}))$ is finite only for the listed values of N, but this is not so easy. One can see that the proof of the proposition breaks down for other N since it depends on there being at most two complex eigenvalues with coprime subscripts. That is, the proof works only when $\phi(N) \leq 2$.

7.3.12 **Corollary** $\Delta_N(a) = \pm 1$ has only trivial solutions in rational integers for $N \in \{1, 2, 3, 4, 6\}$. □

7.3.13 **Corollary** Let $a(x) = \sum_{i=0}^{L} a_i x^i \in \mathbb{Z}[x]$ with $a_0 \neq 0$ and $L < N$ and let $A = \Gamma^N(a) \in \mathrm{CIRC}_N(\mathbb{Z})$. Suppose $\Delta_N(A)$ is prime. If $N \in \{1, 2, 3, 4, 6\}$ then $a(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof.

Suppose a factorizes, $a(x) = f(x)g(x)$, say. Let $F = \Gamma^N(f)$, $G = \Gamma^N(g)$ with $F, G \in \mathrm{CIRC}_N(\mathbb{Z})$. Assuming a non-trivial factorization, then $\deg(f), \deg(g) < L < N$. Therefore, the Γ^N map preserves all coefficients and the circulant matrix A also factorizes $A = FG$. But, by hypothesis, $\Delta(A)$ is prime and $\Delta(A) = \Delta(F)\Delta(G)$. This is possible only if, say, $\Delta(F) = \pm 1$. This means that F is a unit of $\mathrm{CIRC}_N(\mathbb{Z})$. By Theorem 7.3.11 the $F = \pm \mathrm{U}^n$ for some n.

$\therefore$ $f(x) = x^n$, $\therefore$ $a(x) = x^n g(x)$. But, $a_0 \neq 0$, $\therefore$ $n = 0$, $\therefore$ $a = \pm g$. □

7.4 t$\mathbf{circ}_N(\mathbb{Q})$: The Rational Circulants of Finite Order.

In this section, we extend the result of the last section to the rational circulants. We shall find and precisely characterize the torsion subgroup of the non-singular, rational circulants.

The rational circulants of finite order is the torsion part of $\mathbf{U}(\mathbf{circ}_N(\mathbb{Q}))$. That is, t$\mathbf{circ}_N(\mathbb{Q})$ = t$\mathbf{U}(\mathbf{circ}_N(\mathbb{Q}))$. Lemma 7.2.9 showed that the torsion part of $\mathbf{U}(\mathbf{circ}_N(\mathbb{Q}))$ is finite, Lemma 7.2.8 tells us that $\mathcal{T}_N \cup \hat{\mathcal{T}}_N$ is always a subgroup of t$\mathbf{circ}_N(\mathbb{Q})$, and by Lemma 7.2.10 is equal to it when $N = p$ prime.

7.4.1 **Extra Elements.** When N is compound, $\mathcal{T}_N \cup \hat{\mathcal{T}}_N$ does not account for all the elements of finite order in $\mathbf{U}(\mathbf{circ}_N(\mathbb{Q}))$. There are additional elements given by applying the $\bar{\delta}_\times^*$-operators of 3.2.15 to the trivial units $\pm \mathrm{u}^i$. For instance, suppose $N = mn$ is some decomposition of N. From Proposition 3.5.6, we have

$$\bar{\delta}_\times^n(\mathrm{u}^i) = 1 + (\mathrm{u}^i - 1)\,\bar{\delta}^n$$

whose eigenvalues are:

$$\lambda(\bar{\delta}_\times^n(\mathrm{u})) = \Big(1, 1, \ldots, 1, \zeta^{ni}, 1, \ldots, 1, \zeta^{2ni}, 1, \ldots, 1, \ldots, 1, \zeta^{(N-n)i}, 1, \ldots, 1\Big)$$

We also have the complementary projections of u^i:

$$(1 - \bar{\delta}^n)_\times(\mathrm{u}^i) = \mathrm{u}^i - (\mathrm{u}^i - 1)\,\bar{\delta}^n$$

whose eigenvalues are:

$$(1 - \delta^n)_\times(\mathrm{u}^i) = \big(1, \zeta^i, \zeta^{2i}, \ldots, \zeta^{ni-i}, 1, \zeta^{ni+i} \ldots, \zeta^{2ni-i}, 1, \zeta^{2ni+i}, \ldots, \ldots, \zeta^{Ni-i}\big)$$

The circulants $\bar{\delta}^n_\times(\mathrm{u}^i)$ and $(1-\bar{\delta})^n_\times(\mathrm{u}^i)$ are both rational and of finite order. The goal of this section is to show that these additional elements generate all of $\mathrm{t}\mathbf{circ}_N(\mathbb{Q})$. This is achieved in Theorem 7.4.4 below. In fact, the proposition will show that adding $\bar{\delta}^n_\times(\pm\mathrm{u})$ to $\mathcal{T}_N$ is enough.

7.4.2 **Proposition** $\mathrm{t}\mathbf{circ}_N(\mathbb{Q}) \;=\; \prod_{d|\,N} \mathrm{t}\bar{\delta}^{*d}_\times\, \mathbf{U}\left(\mathbf{circ}_d(\mathbb{Q})\right) \;\approx\; \prod_{d|\,N} \mathrm{t}\mathbb{Q}(\zeta_{N/d})$.

Proof. Our starting point is Corollary 3.2.17.1. We have the following facts which are pertinent to its conditions:

(i) $R = Q = \mathbb{Q}$,

(ii) $\Phi_N(x)$ is irreducible over $\mathbb{Q}$ for all N, and

(iii) the non-singular, rational circulants is the group of units, $\mathbf{U}\left(\mathbf{circ}_N(\mathbb{Q})\right)$.

Therefore, we have the following direct sum decomposition for the group of units

$$\mathbf{U}\left(\mathbf{circ}^*_N(\mathbb{Q})\right) \;=\; \prod_{d|\,N} P_d \quad \text{where } P_d \;:=\; \bar{\delta}^{*d}_\times\, \mathbf{U}\left(\mathbf{circ}_d(\mathbb{Q})\right), \quad \text{and}$$

$$\lambda_d \;:\; P_d \;\approx\; \mathbf{U}\left(\mathbb{Q}(\zeta^{N/d})\right) \;=\; \mathbb{Q}(\zeta^{N/d}) - \{0\}$$

Since $\mathrm{t}\mathbf{circ}_N(\mathbb{Q}) \subset \mathbf{U}\left(\mathbf{circ}_N(\mathbb{Q})\right)$, the above implies a decomposition for $\mathrm{t}\mathbf{circ}_N(\mathbb{Q})$ also. Specifically, let $x \in \mathbf{U}\left(\mathbf{circ}_N(\mathbb{Q})\right)$. Then, x has a decomposition $x \;=\; \prod_{d|\,N} x_d$ where $x_d \in P_d$. Clearly, x has finite order iff each x_d has finite order. That is, $x \in \mathrm{t}\mathbf{circ}_N(\mathbb{Q}) \;\Leftrightarrow\; x_d \in \mathrm{t}P_d,\ \forall d \,|\, N$. This is essentially the statement of the proposition. □

The immediate need is to identify $\mathrm{t}\mathbb{Q}(\zeta_{N/d})$. This is easily done.

It is convenient to let $x \parallel y$ mean that the integer x strictly divides the integer y. That is $x \parallel y$ iff $x \,|\, y$ and $x < y$.

7.4.3 **Proposition** $\mathrm{t}\mathbf{circ}_N(\mathbb{Q}) \;\approx\; \mathbb{Z}_2^\nu \oplus \bigoplus_{d\parallel N} \mathbb{Z}_{N/d}$ where ν is the number of odd divisors of N.

Proof. By Lemmas 7.3.3 and 7.3.4, the elements of finite order in $\mathbb{Q}(\zeta_{N/d})$ are $T_d = \{\pm\zeta^i_{N/d}\}$. T_d is clearly a multiplicative group. If N/d is even, then $T_d = \langle\zeta_{N/d}\rangle$, whereas if N/d is odd, $T_d = \{\pm1\} \oplus \langle\zeta_{N/d}\rangle$. Therefore, in the direct sum decomposition of 7.4.2, each component corresponding to N/d odd will contribute two direct summands, one isomorphic to $\mathbb{Z}_2$, and the other to $\mathbb{Z}_{N/d}$ whereas the other components will be isomorphic to $\mathbb{Z}_{N/d}$.

Lastly, we note that the component corresponding to $d = N$ is trivial. □

We can use propositions 7.4.2 and 7.4.3 to construct a basic set of generators for $\mathrm{t}\mathbf{circ}_n(\mathbb{Q})$.

7.4.4 **Theorem** For all $d \,|\, N$, define $u_d := \bar{\delta}^d_\times(\mathrm{u})$, and when N/d is an odd integer, define $s_d := \bar{\delta}^d_\times(-1)$. Then, we have an internal direct product decomposition for the torsion part of the rational circulants,

$$\mathrm{t}\mathbf{circ}_N(\mathbb{Q}) \;=\; \prod_{N/d \text{ odd}} \langle s_d\rangle \;\times\; \prod_{d\parallel N} \langle u_d\rangle, \quad \text{and}$$

$$\text{The order of } s_d \;=\; 2$$

$$\text{The order of } u_d \;=\; \frac{N}{d}$$

Proof. As before, we let $P_d \;:=\; \bar{\delta}^{*d}_\times\, \mathbf{U}\left(\mathbf{circ}_d(\mathbb{Q})\right)$, and let $T_d := \{\pm\zeta^i_{N/d}\} = \mathrm{t}\mathbb{Q}(\zeta_{N/d})$. We have the isomorphism $\lambda_d : P_d \to \mathbb{Q}(\zeta_{N/d})$ which implies the isomorphism $\lambda_d|_{\mathrm{t}P_d} : \mathrm{t}P_d \to \mathrm{t}T_d$.

Consider first the case N/d even. We have $T_d = \{\zeta^i_{N/d}\} = \langle\zeta_{N/d}\rangle$. We easily see that $\lambda_d^{-1}(\zeta_{N/d}) = \bar{\delta}^{*d}_\times(\mathrm{u}) \in P_d$. Therefore, $\mathrm{t}P_d$ is generated by $\bar{\delta}^{*d}_\times(\mathrm{u})$.

Likewise, we find that when N/d is odd, $\mathrm{t}P_d$ is generated by two elements, $\bar{\delta}^{*d}_\times(\mathrm{u})$ and $\bar{\delta}^{*d}_\times(-1)$. □

7·5 Elements of Infinite Order in $\mathbf{U}(\mathbf{circ}_N(\mathbb{Z}))$.

The remainder of this chapter will be devoted to the problem of determining the non-trivial integer circulant units. We shall need to constantly refer to the full unit group of $\mathbf{circ}_N(\mathbb{Z})$, so as to avoid cumbersome formulæ, we shall use the symbol $\mathcal{U}_N$ to stand for $\mathbf{U}(\mathbf{circ}_N(\mathbb{Z}))$, the unit group in the integer circulants of order N.

The problem of determining the elements of infinite order in $\mathcal{U}_N$ is quite difficult, and indeed we shall mostly restrict the discussion to $N = p$, prime. We shall then generalize the results to N a prime power.

Regardless, a set of units in $\mathbf{circ}_N(\mathbb{Z})$ for general N are known which generate a subgroup of finite index in the full unit group. This was shown by Hyman Bass [Bass] and we have reproduced his result as Theorem 7·5.8 below. However, it will be apparent that these units never generate the full unit group, $\mathcal{U}_p$ for prime $p > 3$.

7·5.1 **Reminder** Recall that if R is a ring and G is a group that $R[G]$ denotes the group ring consisting of all formal, finite sums $\sum_i r_i g_i$ where $r_i \in R$ and $g_i \in G$. It is usually assumed that $1 \in R$. Also recall that $\mathrm{t}G$ denotes all elements of G of finite order.

7·5.2 **Theorem (G. Higman)** Let G be an abelian group. Then, $\mathbf{U}(\mathbb{Z}[G]) = \pm\mathrm{t}G \oplus F$ with F a free group whose rank n is given by

$$n = \begin{cases} 0 & \text{if } \mathrm{t}G \text{ consists only of elements of order 1,2,3,4, or 6,} \\ \frac{1}{2}\left(|\mathrm{t}G| - 2d + e + 1\right) & \text{if } \mathrm{t}G \text{ is finite} \\ \infty & \text{otherwise} \end{cases}$$

where d is the number of cyclic subgroups in $\mathrm{t}G$, and e is the number of such subgroups of order 2.

Proof. See Karpilovsky [Kar2]. □

The notation $\pm\mathrm{t}G$ used in the theorem statement means all elements in the group ring of the form $\pm 1g$ with $\pm 1 \in R$, $g \in \mathrm{t}G$.

In all cases of interest to circulant matrices, G is the finite, cyclic group generated by u. In this case, the theorem gives

7·5.3 **Corollary** $\mathcal{U}_N = \mathcal{T}_N \oplus F$ where F is trivial for $N = 1, 2, 3, 4,$ or 6 and otherwise is free abelian of rank $n = \lfloor N/2 \rfloor + 1 - \delta(N)$, where $\delta(N)$ is the number of divisors of N, including 1 and N itself. □

7·5.4 **Corollary** $\mathcal{U}_N$ is finite iff $N \in \{1, 2, 3, 4, 6\}$. □

The key task now is to attempt to find a complete set of units in $\mathbf{circ}_N(\mathbb{Z})$ which generate the free group in $\mathcal{U}_N$.

7·5.5 **Definition** Let R be any ring with identity, and let $X \subset \mathbf{U}(R)$. X is said to be an **independent set of units** if every element in the subgroup generated by X has a unique representation as a product of elements in X.

X is said to be a **set of fundamental units** if X is an independent set which generates the full unit group.

A complex domain always has a finite set of fundamental units (though few of them are known). We start with a general theorem which applies to all finite extensions of the rationals.

Let E be a root field of the polynomial $f(x)$ over the rationals. Define the **signature** of E to be $[r_1, r_2]$ where r_1 is the number of real roots of f, and r_2 is the number of complex conjugate pairs of roots of f. (Thus, $\deg f = r_1 + 2r_2$.)

7·5.6.1 **Dirichlet's Unit Theorem** Let R be a ring of integers of an algebraic number field F with signature $[r_1, r_2]$. Then, $\mathbf{U}(F) \approx \mathrm{t}F^* \oplus A$ where A is free abelian of rank $r_1 + r_2 - 1$.

Proof. See [Kar3]. □

The fundamental units of particular relevance to circulant matrices are those of the cyclotomic domains.

7.5.6.2 **Corollary** $\mathbf{U}(\mathbb{Z}(\zeta_N)) = \langle -\zeta_N \rangle \oplus A$ where A is abelian of rank $\frac{1}{2}\phi(N) - 1$. □

The corollary exactly specifies the isomorphism class of the cyclotomic units. The next theorem gives us a means of constructing nearly all the units if not all of them.

7.5.6.4 **Theorem** (Kummer) Let $N = p^m$ with p prime and $m > 0$, and let $\zeta = \zeta_N$. The following set

$$X_N := \{-1, \zeta\} \cup \left\{ \chi_a \vdash a \in \mathbb{Z}_N^*,\ 1 < a < \tfrac{1}{2}N, \text{ and } \chi_a = \frac{1-\zeta^a}{1-\zeta} \right\}$$

is a set of independent units for $\mathbb{Z}(\zeta)$, and the group generated by this set has finite index in $\mathbf{U}(\mathbb{Z}(\zeta))$. If N is a prime power then this index is h_+, the class number for $\mathbb{R} \cap \mathbb{Q}(\zeta)$.

Proof. See Washington [Was3]. □

7.5.7 **Kummer's Cyclotomic Units.** The reader may wonder why $(1-\zeta^a)/(1-\zeta)$ is a unit of the cyclotomic integers. In fact, given any a and b coprime to N, $\chi_{a,b} = (1-\zeta^a)/(1-\zeta^b)$ is a unit in $\mathbb{Z}(\zeta_N)$, and this is so for any $N > 2$ (not just prime powers). To see this, let $a = bf$ for some $f \in \mathbb{Z}_N$. The residue f must exist because of the coprimality of a and b. Therefore,

$$\chi_{a,b} = \frac{1-\zeta^a}{1-\zeta^b} = \frac{1-\zeta^{fb}}{1-\zeta^b} = 1 + \zeta^b + \zeta^{2b} + \cdots + \zeta^{(f-1)b}$$

The last expression is clearly a cyclotomic integer. By reversing the rôles of a and b, we also deduce that $\chi_{b,a} = (1-\zeta^b)/(1-\zeta^a)$ is an algebraic integer. But, $\chi_{b,a} = \chi_{a,b}^{-1}$. Therefore, $\chi_{a,b}$ is a unit in $\mathbb{Z}_\zeta$.

Let $\zeta = \zeta_N$. Let V be the group generated by $\{\pm\zeta^a(1-\zeta^b) \vdash a, b \in \mathbb{Z}_N - \{0\}\}$. Then, we shall refer to the set $C_N = V \cap \mathbf{U}(\mathbb{Z}(\zeta))$ as the **Kummer group of cyclotomic units**. It can be shown that the Kummer group is generated by the set X_N of the theorem and so we shall call the elements of X_N the **basic Kummer cyclotomic units**. We denote the (full) group of units in $\mathbb{Z}(\zeta_N)$ by E_N. The theorem states that E_N/C_N is finite when N is a prime power; indeed, this is true for all N (see [Was3]), though in the general case, the index $[E_N : C_N]$ only divides h_+.

The following is known: $h_+ = 1$ for all cyclotomic orders N such that $\phi(N) \leq 66$. ([Was1].) This is enough to deduce that the Kummer units account for all the cyclotomic units for all $N \leq 100$ except for $N = 71, 73, 79, 83, 89, 91, 95$.

The reader is warned that in the literature, C_N is often called, confusingly, **the** cyclotomic units, and X_N is called **the** basic cyclotomic units. But, for clarity's sake, when we speak of "cyclotomic units" we always mean the full group of units in the cyclotomic domain of which C_N is in general only a subgroup; when we intend C_N we shall refer to them as the "Kummer units."

7.5.7.1 **Corollary**

(i) $\mathrm{t}\mathcal{U}_N \approx \mathrm{t}\mathbb{Z}(\zeta_N)$.

(ii) When $N = p$, an odd prime, $\mathcal{U}_p \approx \mathbf{U}(\mathbb{Z}(\zeta_p))$.

Proof. *(i)* From the corollary of the Dirichlet Unit Theorem 7.5.6.2

$$\mathrm{t}\mathbb{Z}(\zeta_N) = \begin{cases} \langle -\zeta_N \rangle \approx \mathbb{Z}_2 \oplus \mathbb{Z}_N & \text{if } N \text{ is odd} \\ \langle \zeta_N \rangle \approx \mathbb{Z}_N & \text{if } N \text{ is even} \end{cases}$$

These are precisely the isomorphism classes of $\mathrm{t}\mathcal{U}_N$ by Proposition 7.3.10. QED *(i)*

(ii) Let $\zeta = \zeta_p$. We have that $\mathbf{U}(\mathbb{Z}(\zeta)) = \mathrm{t}(\mathbb{Q}(\zeta)) \oplus F$ where F is free of rank $\frac{1}{2}\phi(p) - 1 = \frac{1}{2}(p-1) - 1$; this is also the rank of $\mathcal{U}_p$ by the Higman Theorem 7.5.2. Therefore, the torsionless components of $\mathcal{U}_N$ and $\mathbf{U}(\mathbb{Z}(\zeta_N))$ are isomorphic. The torsion parts are isomorphic by part *(i)*. □

The next result gives a set of independent units which generate a subgroup of finite index in the unit group of the circulants.

7.5.8 **Theorem**[Bass] Let m be a multiple of $\phi(N)$. For any $d \mid N$, let $\mathrm{u}_d = \mathrm{u}_N^{N/d}$, let $T_d = \{t \in \mathbb{Z} \vdash \gcd(t,d) = 1, \text{ and } 1 < t < \frac{1}{2}d\}$, and for all $t \in T_d$, define

$$b_{t,d} \;:=\; (1 + \mathrm{u}_d + \mathrm{u}_d^2 + \cdots + \mathrm{u}_d^{t-1})^m \;-\; (t^m - 1)\bar{\delta}^{d|N} \;\in\; \mathbf{circ}_N(\mathbb{Z}), \quad \text{and}$$

Let $B = \{b_{t,d} \vdash t \in T_d,\ 2 < d \mid N\}$. Then, B is a set of independent units of infinite order which generates a subgroup of finite index in $\mathbf{U}(\mathbf{circ}_N(\mathbb{Z}))$.

Proof. The most difficult part is proving the independence of the elements of the set B; it is too lengthy and technical to repeat here. We therefore assume independence and refer the reader to the literature for its proof. ([Kar6] and [Seg] †)

Given B consists of independent units, it follows immediately that $\langle B\rangle$ is of finite index in $\mathbf{U}(\mathbf{circ}_N(\mathbb{Z}))$ because $|B| = \frac{1}{2}\phi(N) - 1$, which is precisely the order of the free part of $\mathbf{U}(\mathbf{circ}_N(\mathbb{Z}))$.

Next, we need to show that $B \subset \mathbf{circ}_N(\mathbb{Z})$. We have $\phi(N) \mid m$ and $d \mid N$. $\therefore \phi(d) \mid \phi(N) \mid m$. $\therefore t^m \equiv 1 \pmod{d}$. $\therefore (t^m - 1)\bar{\delta}^d \in \mathbf{circ}(\mathbb{Z})$ as required.

Lastly, we need to show that B consists of units. We note that $b_{t,d}$ consists of a polynomial in $\mathrm{u}_d = \mathrm{u}_N^{N/d}$. So, we can regard $b_{t,d}$ as belonging to $\mathbf{circ}_d \subset \mathbf{circ}_N$ (*à la* Chapter 4). Hence, by Corollary 7.2.5.1, $b_{t,d}$ is a unit iff $\lambda_h(b_{t,d})$ is a cyclotomic unit for all $h \mid d$.

As a member of $\mathbf{circ}_d$, $b_{t,d}$ is a geometric series in u_d plus a member of the ideal $(\bar{\delta}^d)$. But this ideal is mapped to zero by all eigenvalues except λ_0. So applying λ_i to $b_{t,d}$ for non-zero i will result in a basic Kummer unit in $\mathbb{Z}(\zeta_d)$, whereas applying λ_0 we get $t^m - (t^m - 1) = 1$. □

Notice that most of the trivial cases are eliminated by the requirement that $d \mid n$ and $d > 2$. There is no such d for $n = 1, 2, 3$. For $n = 4, 6$, there is no t satisfying $\gcd(t,d) = 1$ and $1 < t < \frac{1}{2}d$.

The basis units in this theorem are not fundamental when N is prime. We shall present a set of units which are basic in the sense that they generate all units which are mapped to the cyclotomic units of Theorem 7.5.6.4. We shall also derive an index for an embedding of the circulant units in the cyclotomic domain.

7.6 Fundamental Units for $\mathcal{U}_p$.

The Bass Theorem is a remarkable achievement: it provides a fundamental basis for a group of circulant units of finite index in the full group, for all circulant orders, N. Furthermore, it provides an infinity of such constructions for each N, one for each $m = k\phi(N),\ k = 1, 2, \ldots$.

Nevertheless, the theorem still leaves important gaps in our knowledge of the circulant units. Firstly, one intuitively feels that larger m leads to a larger index in the full group which is to say that the Bass units omit more circulant units for larger m. Since the least possible m is $\phi(N)$, one has the feeling that a lot of circulant units are missed.

Secondly, the theorem does not provide an estimate of the index of the Bass units in the full group, it states only that the index is finite. For instance, with an estimate of the index, we might better judge how much of the full group is accounted for by the Bass units.

As an example, let us consider the lowest non-trivial order, $N = 5$. The full group is generated by $-1 + \mathrm{u}^2 + \mathrm{u}^3$ ‡. Hence, the index of the Bass group in the circulant units is given by

$$\left(\frac{\log(|b_{2,5}|)}{\log(|-1 + \zeta_5^2 + \zeta_5^3|)}\right)^{\pm 1}$$

We calculated this for $m = k\phi(N) = 4k$ for $k = 1, 2, \ldots 40$ (beyond which rounding errors became significant), and found that the index in all cases equalled $2k$.

† Note that Sehgal's book refers to Karpilovsky's, so both are needed for a complete proof of independence.

‡ For various derivations of this unit, see Example 8.5.7 or Example 7.6.11 following Theorem 7.6.9

The goal of this section is to firstly capture more of the circulant units than is done in the Bass Theorem, and secondly to quantify the index of such discovered circulant units in the full group. We shall exploit the facts that λ_1 maps circulant units to cyclotomic units, and that the cyclotomic units have been the object of intense study for close to two centuries. Thus, the main idea is to use the λ_1 connection and existing corpus of knowledge of the cyclotomic units to discover and describe circulant units.

For the remainder of this chapter N shall be an odd prime power which we shall write as $q = p^n$ where p is an odd prime. We shall first derive results applicable to $q = p$, and then we shall attempt to generalize to $q = p^n$ with $n > 1$. We continue to use the notation $E_q := \mathbf{U}(\mathbb{Z}(\zeta_q))$, the unit group of the q^{th} cyclotomic field.

Since we shall now generally be dealing with homomorphisms on groups of units. So as to be clear we shall write $\ker_*$ for a kernel in a multiplicative group. If α is a ring homomorphism, the ring and the multiplicative kernels are related by $\ker_* \alpha = 1 + \ker \alpha \equiv \{1 + k \vdash k \in \ker \alpha\}$ where $\ker \alpha$ is the ring kernel.

7.6.1 Definition

(i) We define a map which is designed to convert the inverse image under λ_1 of a cyclotomic unit into a circulant of determinant ± 1. Let $\mu : \mathbf{circ}_q(\mathbb{Q}) \to \mathbf{circ}_q(\mathbb{Q})$ be the multiplicative idempotent $(1 - \bar{\delta}^p)_\times$ of §3.2.1. That is, $\mu : c \mapsto c - (c-1)\bar{\delta}^p$. The effect of μ on the eigenvalues is:

$$\lambda_i(\mu(c)) \;=\; \begin{cases} 1 & \text{if } i \equiv 0 \pmod{p} \\ \lambda_i(c) & \text{otherwise} \end{cases}$$

In particular, $\lambda_1 \mu = \lambda_1$.

(ii) We construct two maps $\gamma_+, \gamma_- : E_q \to \mathbf{circ}_q(\mathbb{Q})$ which are designed to pick out a circulant unit belonging to a given cyclotomic unit. We need both maps since they capture two distinct, non-overlapping sets of circulant units. The definition is

$$\begin{aligned} \gamma_+(\xi) &:= \mu\lambda_1^{-1}(\xi) \\ \gamma_-(\xi) &:= -\gamma_+(-\xi) \end{aligned}$$

We extend the notation so that if σ is a variable taking the values ± 1, then γ_σ is to mean γ_+ or γ_- according as $\sigma = 1$ or -1 respectively.

We now list the properties of $\gamma_\pm$.

7.6.2 Lemma

γ_σ is a well-defined map $E_q \to p^{-1}\mathbf{circ}_q(\mathbb{Z})$.

Proof. Let $\xi \in E_q$

We can always pick an integer circulant in $\lambda_1^{-1}(\xi)$; we merely replace powers of ζ_q in ξ with like powers of u. Let us suppose we have done this obtaining the circulant e. Then, $\lambda_1^{-1}(\xi) = e + (p\bar{\delta}^p) \subset \mathbf{circ}_q(\mathbb{Z})$. Pick an arbitrary member of this coset, $e' = e + cp\bar{\delta}^p$ say, where $c \in \mathbf{circ}_p(\mathbb{Z})$ is arbitrary. We have $\gamma_+(\xi) = \mu(e') = e + cp\bar{\delta}^p - (e + cp\bar{\delta}^p - 1)\bar{\delta}^p = e - (e-1)\bar{\delta}^p = \mu(e)$ which shows that γ_+ is well-defined. The proof for γ_- follows from its definition. □

Note that the map γ_σ would not be well-defined if μ were defined along the lines $\mu(e) = e - (e-1)\bar{\delta}^d$ for any $d \,|\, q$ except for $d = p$ (which we adopted) and $d = 1$ which is trivial.

7.6.4 Proposition

(i) $\gamma_\sigma(\sigma\zeta^k) \;=\; \sigma \mathrm{u}^k$. ($\gamma_\sigma$ maps trivial units to trivial units.)

(ii) $\lambda_1\gamma_\sigma$ is the identity map on E_q, and $\gamma_\sigma\lambda_1$ is the identity map on $\gamma_\sigma E_q$.

(iii) $\gamma_+ : E_q \to \mathrm{GL} \cap \mathbf{circ}_q(\mathbb{Q})$ is a group monomorphism.

Proof. *(i)* Trivial! *(ii)* is an easy consequence of the definition.

(iii) γ_+ is a homomorphism because of Lemma 7.6.2 and because μ is a multiplicative homomorphism. Now $\ker \gamma_+ = \lambda_1 \ker \mu$. But, $\ker_* \mu = \ker_*(1 - \bar{\delta}^p)_\times = 1 + (\bar{\delta}^p)$. Therefore, $\ker_* \gamma_+ = \lambda_1\left(1 + (\bar{\delta}^p)\right) = 1$. □

We will need a couple of results pertaining to the ℓ_p map of §7.2.6. The reader is reminded that we are still within the general setting of q being a prime power.

7.6.5 **Lemma** Let $\chi_r = (1-\zeta_q^r)/(1-\zeta_q)$ where $r \in \mathbb{Z}_q^*$. Then, $\chi_r \in E_q$, and $\ell_p(\chi_r) = r \bmod p$.

Proof. This is easily verified. □

Since ℓ_p is a homomorphism, it follows that $\ell_p(\chi_r^{-1}) = r^{-1} \bmod p$, $\ell_p(\chi_r\chi_s) = rs \bmod p$, etc.

7.6.6 **Lemma** $\ell|E_q : E_q \to \mathbb{Z}_p^*$ is a group epimorphism.

Proof. ℓ is a multiplicative homomorphism on E_q by Proposition 7.2.7. To show that $\ell_p|E_q$ is onto, let r be a primitive residue in $\mathbb{Z}_p$. By Lemma 7.6.5, $\ell_p(\chi_r^i) = r^i$, $i = 0, 1, 2, \ldots$ will run through all of $\mathbb{Z}_p^*$. □

7.6.7 **Lemma** Let $c \in \mathbf{circ}_q(\mathbb{Z})$. Then, $\lambda_1(c) = 0 \;\Rightarrow\; \lambda_0(c) \equiv 0 \pmod{p}$.

Proof. $\lambda_1(c) = 0 \;\Rightarrow\; \ell_p\lambda_1(c) = 0 \;\Rightarrow\; \lambda_0(c) \equiv 0 \pmod{p}$ by definition of ℓ_p. □

To state the coming theorem succinctly, we need the following notation.

7.6.8 **Definition**

$$\begin{aligned} \bar{E}_q^+ &:= \mathbf{circ}_q(\mathbb{Z}) \cap \gamma_+(E_q) \\ \bar{E}_q^- &:= \mathbf{circ}_q(\mathbb{Z}) \cap \gamma_-(E_q) \\ \bar{E}_q &:= \bar{E}_q^+ \uplus \bar{E}_q^-, \quad \text{disjoint because } \lambda_0(\bar{E}_q^+) \cap \lambda_0(\bar{E}_q^-) = \{+1\} \cap \{-1\} = \emptyset \end{aligned}$$

7.6.9 **Theorem** Let p be an odd prime, let $\xi \in E_p$, and let $\sigma = \pm 1$. Then,

(i) $\gamma_\sigma(\xi) \in \mathcal{U}_p \;\Leftrightarrow\; \gamma_\sigma(\xi) \in \mathbf{circ}_p(\mathbb{Z}) \;\Leftrightarrow\; \ell(\xi) = \sigma \bmod p$

(ii) $\mathcal{U}_p = \bar{E}_p$

(iii) $\lambda_1 : \mathcal{U}_p \hookrightarrow E_p$

(iv) $\dfrac{E_p}{\lambda_1(\mathcal{U}_p)} \approx \mathbb{Z}_{(p-1)/2}$

Proof.

(i) For this part (and subsequent parts which depend on this), we need Proposition 7.2.9 which is the reason that we must assume $N = p$ prime.

Pick any $c \in \lambda_1^{-1}(\xi)$. By Proposition 7.2.9 and the properties of ℓ_p map (§7.2.6), we have $\gamma_\sigma(\xi) \in \mathcal{U}_p \;\Leftrightarrow\; \mu(\sigma c) \in \mathbf{circ}_p(\mathbb{Z}) \;\Leftrightarrow\; \lambda_0(c) \equiv \sigma \pmod{p} \;\Leftrightarrow\; \ell(\xi) = \sigma$. QED *(i)*

(ii) Suppose we are given $x \in \mathcal{U}_p$, then $\xi = \lambda_1(x) \in E_p$, and $\lambda_0(x) = \sigma = \pm 1$. One easily shows that $\gamma_\sigma(\xi) = x$. QED *(ii)*

(iii) Let $\xi \in E_p$, and suppose $\lambda_1(a) = \lambda_1(b) = \xi$. Then, $b - a \in \ker\lambda_1$. $\therefore \lambda_0(b) \equiv \lambda_0(a) \pmod{p}$ by Lemma 7.6.7. But, any unit of $\mathcal{U}_p$ must satisfy $\lambda_0 = \pm 1$. Since $p > 2$, this is possible for both a and b only if $\lambda_0(b) = \lambda_0(a)$. But now a and b, being rational circulants, share all their eigenvalues, therefore $a = b$. QED *(iii)*

(iv) By the foregoing $\mathcal{U}_p \overset{\lambda_1}{\approx} \lambda_1(\bar{E}_p^+) \uplus \lambda_1(\bar{E}_p^-)$, and in particular $\lambda_1(\bar{E}_p^+) \uplus \lambda_1(\bar{E}_p^-)$ is a group. Let $\xi \in E$, and denote $\ell_p|E$ by ℓ_E. By Part *(i)*, $\xi \in \lambda_1(\bar{E}_p^\sigma)$ iff $\ell_E(\xi) = \sigma$. Therefore,

$$\lambda_1(\bar{E}_p^+) \uplus \lambda_1(\bar{E}_p^-) = \ell_E^{-1}\{\pm 1\}$$

Let $\nu : \mathbb{Z}_p^* \to \mathbb{Z}_p^*/\{\pm 1\}$ be the natural map. By Lemma 7.6.6, ℓ_E is onto $\mathbb{Z}_p^*$. Therefore, $\nu\ell_E$ is onto $\mathbb{Z}_p^*/\{\pm 1\}$. As was shown above, $\ker\nu\ell_E = \lambda_1(\bar{E}_p^+) \uplus \lambda_1(\bar{E}_p^-) = \lambda_1(\mathcal{U}_p)$. Therefore, by the Isomorphism Theorem,

$$\frac{E_p}{\lambda_1(\mathcal{U}_p)} \approx \frac{\mathbb{Z}_p^*}{\{\pm 1\}} \approx \mathbb{Z}_{(p-1)/2}$$

The last isomorphism follows from the fact that $\mathbb{Z}_p^*$ is cyclic and that all quotient groups of cyclic groups are cyclic. □

7.6.10 **Corollary** Let r be a primitive residue in $\mathbb{Z}_p$. Then, $E_p = \lambda_1(\mathcal{U}_p) \vee \{\chi_r\}$.

Proof. Let $\nu : \mathbb{Z}_p^* \to \mathbb{Z}_{(p-1)/2}$ be the map $\nu(r^i) = i \bmod \frac{1}{2}(p-1)$. This is equivalent to the map of the same name used in the theorem proof. Therefore, as in the theorem, $\ker \nu\ell = \lambda_1(\mathcal{U}_p)$. The set $\{\chi_r^i \vdash i \in \mathbb{Z}_{p-1}\}$ contains representatives from all cosets of $\ker \nu\ell$ in E_p. Therefore, $\lambda_1(\mathcal{U}_p)$ together with χ_r generates E_p. □

7.6.11 **Examples of Non-trivial Circulant Units**

(i) We start with the simplest non-trivial case, $N = 5$. Ignoring the torsion part of the circulant and cyclotomic units, by Corollary 7.5.3, the circulant units is a single infinite cyclic group. Let us find its generator. The basic Kummer unit $\chi = 1 + \zeta$ is a generator for the single infinite cyclic subgroup in the cyclotomic units. Although $\gamma_\pm(\chi)$ are not units since $\ell_5(\chi) = 2$, χ^2 fits the bill since $\ell(\chi^2) = 4 \equiv -1 \pmod 5$. Hence, by Theorem 7.6.9, $\gamma_-(\chi^2) \in \mathcal{U}_5$. We have $\gamma_-(\chi^2) = 1 + 2\mathrm{u} + \mathrm{u}^2 - \sum_{i=0}^4 \mathrm{u}^i = \mathrm{u} - \mathrm{u}^3 - \mathrm{u}^4$. Dividing by the trivial unit $-\mathrm{u}$ gives the unit

$$e = -1 + \mathrm{u}^2 + \mathrm{u}^3 \in \mathcal{U}_5$$

The circulant e must be a generator of the circulant units because by Theorem 7.6.9

$$[\,\langle 1+\zeta\rangle : \langle \lambda_1(e)\rangle\,] = 2 = \tfrac{1}{2}\,\phi(N) = [E_5 : \lambda_1(\mathcal{U}_5)]$$

The generator e was originally found by Kaplansky [Kar3].

(ii) Let $N = p = 7$. There are two basic Kummer units, χ_2 and χ_3, By Lemma 7.6.5, the simplest possibility is their product $\chi_2\chi_3 = 1 + 2\zeta + 2\zeta^2 + \zeta^3$. This yields a circulant unit (after dividing by u) of $1 + \mathrm{u} - \mathrm{u}^3 - \mathrm{u}^4 - \mathrm{u}^5$. It so happens that the inverse is simpler; we take it as our first unit.

$$e_1 = 1 - \mathrm{u} + \mathrm{u}^2$$

We need one more generator. The next simplest would appear to be χ_2^3. This yields (ignoring trivial factors)

$$e_2 = 2 + 2\mathrm{u} - \mathrm{u}^4 - \mathrm{u}^5 - \mathrm{u}^6$$

Again we have $\langle e_1, e_2\rangle = \mathcal{U}_7$. We see this by expressing the cyclotomic units $\lambda_1(e_1), \lambda_1(e_2)$ additively in terms of the basic Kummer units:

$$\begin{aligned}\lambda(e_1) &= \chi_2 + \chi_3\\ \lambda(e_2) &= 3\chi_2\end{aligned}$$

Hence,

$$[E_7 : \langle \lambda_1(e_1), \lambda_1(e_2)\rangle\,] = \left\|\begin{matrix}1 & 1\\ 3 & 0\end{matrix}\right\| = 3 = \tfrac{1}{2}\phi(N)$$

The type of construction used in these examples will be exploited in the next theorem which will round-off our knowledge of the circulant units of prime orders by constructing a fundamental set of generators for a subgroup of finite, and in many cases of known, index in the circulant units. The theorem constructs this basis by mapping the fundamental Kummer units to circulant units. It then estimates the index of the resulting subgroup of the circulant units by relating it to the index of the Kummer units in the cyclotomic units. This latter index is well-researched. (See the Kummer Theorem 7.5.6.4 and the notes following in §7.5.7.)

One annoying complication in the theorem needs a note of explanation: the theorem assumes there exists a primitive residue, $r \le \frac{1}{2}(p-1)$, in $\mathbb{Z}_p$. Such a primitive residue always exists because r is primitive iff $p - r$ is primitive. *

* Pf: Let $x \in \mathbb{Z}_q^*$, $x = r^e$, then $x = (-r)^e$ if e is even, else $x = (-r)^{e+\phi(q)/2}$.

7.6.12 **Definition** Let $C_q \subset E_q$ be the group of Kummer units; that is $C_q := \langle \chi_r \vdash 2 \leq r < \frac{1}{2}\phi(q) \rangle$. We define $\overline{C}_q^\sigma$ and $\overline{C}$ analagously to $\overline{E}_q^\sigma$ and $\overline{E}_q$

(i) $\overline{C}_q^\sigma := \mathbf{circ}_q(\mathbb{Z}) \cap \gamma_\sigma(C_q)$, and

(ii) $\overline{C}_q := \overline{C}_q^+ \uplus \overline{C}_q^-$.

7.6.13 **Theorem** Let $p \geq 5$ be prime, and $g = \frac{1}{2}\phi(p)$. Let $X = \{\chi_2, \chi_3, \ldots, \chi_g\}$ be the basis of $C_p / \langle \pm\zeta \rangle$. Let r be a primitive residue in $\mathbb{Z}_p$ satisfying $r < \frac{1}{2}p$. Define the set $Y = \{y_1, y_2, \ldots, y_g\}$ by

$$y_i = \begin{cases} -\mathrm{u} & \text{if } i = 1 \\ \gamma_-(\chi_r^g) & \text{if } i \equiv r \pmod{p} \\ \gamma_+(\chi_i \chi_r^{-n_i}) & \text{otherwise, where } r^{n_i} \equiv i \pmod{p}. \end{cases}$$

Then,

(i) Y_p is a basis for $\overline{C}_p$.

(ii) $\dfrac{C_p}{\lambda_1(\overline{C}_p)} \approx \mathbb{Z}_{\frac{1}{2}\phi(p)}$.

(iii) $\dfrac{\mathcal{U}}{\overline{C}_p} \approx \dfrac{E_p}{C_p}$.

Proof. We shall prove assertions *(i)* and *(ii)* together. Let $r \in \{2, 3, \ldots, g\}$ be the primitive residue mod p. Define $\hat{X}_p := \{x_1, x_2, \ldots, x_g\}$ where $x_i = \lambda_1(y_i)$. By Proposition 7.6.4*(ii)*,

$$x_i = \begin{cases} -\zeta & \text{if } i = 1 \\ \chi_r^g & \text{if } i \equiv r. \\ \chi_i \chi_r^{-n_i} & \text{otherwise, where } r^{n_i} \equiv i \pmod{p}. \end{cases}$$

Then, the set $\hat{X}_p$ generates a subgroup of C_p. By writing the ring product of $\mathbb{Z}_\zeta$ as addition, we can regard C_p as a $\mathbb{Z}$-module with basis elements X_p, and $\hat{X}_p$ defines a basis for a sub-module of C_p defined by the linear transformation:

$$\begin{pmatrix} -\zeta \\ x_2 \\ x_3 \\ \vdots \\ x_r \\ \vdots \\ x_g \end{pmatrix} = \begin{pmatrix} 1 & & & & & 0 & & & \\ & 1 & & & & -n_2 & & & \\ & & 1 & & & -n_3 & & & \\ & & & \ddots & & \vdots & & & \\ & & & & 1 & -n_{r-1} & & & \\ & & & & & g & & & \\ & & & & & -n_{r+1} & 1 & & \\ & & & & & \vdots & & \ddots & \\ & & & & & -n_g & & & 1 \end{pmatrix} \begin{pmatrix} -\zeta \\ \chi_2 \\ \chi_3 \\ \vdots \\ \chi_r \\ \vdots \\ \chi_g \end{pmatrix}$$

(Zero entries are shown as blank for clarity.)

Call the above matrix A. The index of $\langle \hat{X} \rangle$ in C_p is given by the volume of the hyper-parallelepiped defined by the vectors $x_1, x_2, \ldots, x_g$ in the X coordinate system. This in turn is equal to the Jacobian of the transformation. That is, $|\det(A)|$. The determinant can be calculated quite easily because the matrix A can be put in upper-triangular form by merely reordering the basis elements so that the primitive residue, r, appears last.

$$\therefore [C_p : \langle \hat{X} \rangle] = |\det(A)| = g = \tfrac{1}{2}\,\phi(p)$$

$\langle \hat{X} \rangle$ is a subgroup of $\lambda_1(\overline{C}_p)$. $\therefore [C_p : \lambda_1(\overline{C}_p)]$ divides $\frac{1}{2}\phi(p)$. In fact, $\frac{1}{2}\phi(p)$ must also divide $[C_p : \lambda_1(\overline{C}_p)]$ as we shall now show.

$$\begin{aligned}
\chi_r^i \in \lambda_1(\overline{C}_p) &\Leftrightarrow \ell(\chi_r^i) \equiv \pm 1 \pmod{p} && \text{by Theorem 7.6.9} \\
&\Leftrightarrow r^i \equiv \pm 1 \pmod{p} && \text{by Lemma 7.6.5} \\
&\Leftrightarrow \tfrac{1}{2}\,\phi(p) \,|\, i && \text{since } r \text{ is a primitive root of unity.}
\end{aligned}$$

Since X_p consists of independent units, $x_r = \chi_r^g$ is the only element in $\hat{X}_p$ which can generate powers of χ_r. Therefore, the element χ_r has order $\frac{1}{2}\phi(p)$ in the quotient group $C_p/\lambda_1(\overline{C}_p)$.

$$\therefore \quad \tfrac{1}{2}\,\phi(p) \;\mid\; [C_p : \lambda_1(\overline{C}_p)] \;\mid\; \tfrac{1}{2}\,\phi(p)$$

$$\therefore \quad [C_p : \lambda_1(\overline{C}_p)] \;=\; \tfrac{1}{2}\,\phi(p) \;=\; [C_p : \langle \hat{X} \rangle]$$

$$\therefore \quad \lambda_1(\overline{C}_p) \;=\; \langle \hat{X} \rangle$$

$$\therefore \quad \overline{C}_p \;=\; \langle Y \rangle$$

This shows that the coset $\chi_r \lambda_1(\overline{C}_p)$ generates the whole of $C_p/\lambda_1(\overline{C}_p)$ which proves statement *(ii)*. It was also proved that Y generates $\overline{C}_p$. To complete the proof of *(i)*, we need to show that Y is an independent set of generators. Suppose there is a linear relationship

$$0 \;=\; \sum_{i=0}^{g} c_i y_i$$

Applying λ_1 throughout, we get

$$\begin{aligned}
0 \;&=\; -c_1\zeta + c_r g \chi_r + \sum_{i=2, i\neq r}^{g} c_i(\chi_i - n_i\chi_r) \\
&=\; -c_1\zeta + \left(c_r g - \sum_{i=2, i\neq r}^{g} c_i n_i \right) \chi_r + \sum_{i=2, i\neq r}^{g} c_i \chi_i
\end{aligned}$$

The independence of the set X forces $c_i = 0$ for all $i \neq r$. But, this leaves $0 = c_r g \chi_r$ and so $c_r = 0$ also. QED *(i)* and *(ii)*.

(iii) $\lambda_1 | \mathcal{U}_p$ is a group monomorphism (Theorem 7.6.9*(iii)*).

$$\therefore \frac{\mathcal{U}_p}{\overline{C}_p} \;\approx\; \frac{\lambda_1(\mathcal{U}_p)}{\lambda_1(\overline{C}_p)} \;=\; \frac{\lambda_1(\mathcal{U}_p)}{\lambda_1(\mathcal{U}_p) \cap C_p} \;\approx\; \frac{C_p \lambda_1(\mathcal{U}_p)}{C_p} \;\subset\; \frac{E_p}{C_p}$$

We shall now show that the last inclusion is in fact an equality. By Theorem 7.6.9 and Corollary 7.6.10, $E_p/\lambda_1(\mathcal{U}_p)$ is generated by χ_r of order $\frac{1}{2}(p-1)$. That is,

$$E_p \;=\; \bigcup_{i=1}^{(p-1)/2} \chi_r^i \; \lambda_1(\mathcal{U}_p)$$

But, $\chi_r \in C_p$. Therefore, $C_p \lambda_1(\mathcal{U}_p) = E_p$. □

7.6.14 **Corollary** If $h_+ = 1$ for $\mathbb{Z}(\zeta_p)$ then Y_p is a set of fundamental units for $\mathcal{U}_p$. □

7.6.15 Conclusions For The Prime Order Case.

Theorems 7.6.9 and 7.6.13 answer the most important theoretical questions regarding the relationship of the group of circulant units of prime order to the group of units in the cyclotomic domain of the same order. In summary:

The cyclotomic units contain a subgroup isomorphic to the circulant units and the quotient group is cyclic of order $\frac{1}{2}(p-1)$.

There is a map from the cyclotomic units to the rational circulants whose image intersects the integer circulants at precisely the circulant units.

A simple criterion on a cyclotomic unit determines whether it is mapped to a circulant unit or not.

We have constructed a fundamental basis for the circulant units whose index in the full group is also the index of the Kummer units in the cyclotomic units.

We have thus largely reduced the study of the circulant units of prime order to the study of cyclotomic units of prime order, one of the most researched topics in number theory.

7.7 The Prime Power Case

We now assume that the order of the circulants is $q = p^n$ where p is prime; the reader may assume that $n > 1$. As usual N shall represent an arbitrary order of the circulants, not necessarily a prime power.

We shall try to generalize the results in the previous section to prime powers. But the reader is warned that matters are considerably more difficult in the prime power case. Indeed, the first lemma indicates the single biggest obstacle to generalizations of the prime order case. In the $q = p$ case, we found that λ_1 was 1-1 on $\mathcal{U}_q$. Hence, $\mathcal{U}_q$ is embedded in E_q. This is no longer so. The first two lemmas construct a non-trivial unit in $\ker_* \lambda_1$ showing that λ_1 is strictly many-to-one.

7.7.1 Lemma For $p \geq 5$, let $q = p^2$. If there exists $\xi \in E_p$ and $\xi \equiv 1 \pmod{p}$, then $\ker_* \lambda_1^{(q)} \cap \mathcal{U}_q \neq \emptyset$.

Proof. We are given $\xi = 1 + p\lambda_1^{(p)}(a) \in E_p$ where a is an integer circulant of the form

$$a \;=\; a_0 + a_1 \mathrm{u}_p + \cdots + a_{p-1}\mathrm{u}_p^{p-1} \;+\; m\left(\sum_{i=0}^{p-1} \mathrm{u}_p^i\right) \tag{1}$$

The integer m is arbitrary; we shall pick its most propitious value.

Set $c = 1 + p\Gamma_p^q(a)$. Since a is integral, then so is $p\Gamma_p^q(a)$, and hence so is c. We shall show that m can be chosen so that $\lambda_0^{(q)}(c)$, $\lambda_1^{(q)}(c)$, $\lambda_p^{(q)}(c)$ are all units which will imply $c \in \mathcal{U}_q$ by Corollary 7.2.5.1.

First we show that $c \in \ker_* \lambda_1^{(q)}$. From §3.5.1, $\Gamma_p^q(a) \in (\bar{\delta}^p)$ $\therefore$ $\lambda_1^{(q)}(c) = 1$. $\therefore$ $c \in \ker_* \lambda_1^{(q)}$ as claimed, and additionally we have shown that $\lambda_1^{(q)}(c)$ is a cyclotomic unit. Next, $\lambda_p^{(q)}(c) = 1 + \lambda_p^{(q)}(a)\lambda_p^{(q)}(p\bar{\delta}^p) = 1 + p\lambda_1^{(p)}(a) = 1 + p\alpha$ which we are given is a unit. So we need only show that $\lambda_0^{(q)}(c)$ is a unit. Now, $1 + p\alpha$ is a unit in $\mathbb{Z}(\zeta_p)$, and by Corollary 11.15.3 (which is independent of this chapter), this implies that $\ell_p(\alpha) = 0$ which implies $\sum_i a_i = kp$ for some integer k. Therefore, from equation (1), $\lambda_0^{(p)}(a) = kp + mp$. Pick $m = -k$. With this choice, $\lambda_0^{(q)}(c) = 1 + p\left(\tilde{\Gamma}_p^q(a)\right)_0 = 1 + p\lambda_0(a) = 1$, a unit.

So, c is a circulant unit distinct from 1 but which is mapped to 1 by $\lambda_1^{(q)}$. □

The eigenvalue version of the construction used in the above lemma is much easier to picture than the one given in the proof. Given the unit $\xi \in E_p$ with $\xi \equiv 1 \pmod{p}$, let $\xi_1 = \xi, \xi_2, \ldots, \xi_{p-1}$ be the conjugates of ξ. Then, the circulant c is most easily constructed as

$$c \;=\; \lambda^{-1}(\alpha), \quad \text{where } \alpha_i \;=\; \begin{cases} 1 & \text{if } i = 0 \text{ or } p \nmid i \\ \xi_{i/p} & \text{otherwise} \end{cases} \tag{2}$$

(c is actually a rather degenerate type of sub-repeating circulant.)

The next lemma explicity constructs elements of the type required by previous lemma.

7.7.2 **Lemma** Suppose $\xi \in E_p$. Then, $\xi^p \equiv \ell_p(\xi) \pmod p$, and $\xi^{p(p-1)} \equiv 1 \pmod p$.

Proof. Let $\xi = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2}$. By the multinomial theorem, $\xi^p \equiv \sum_i a_i^p \equiv \ell_p(\xi) \pmod p$. Since ξ is a unit, $\ell_p(\xi)$ must be invertible and so is non-zero. $\therefore\ \xi^{p(p-1)} \equiv \ell_p(\xi)^{p-1} \equiv 1 \pmod p$. □

The circulants thus constructed in $\ker_* \lambda_1|\mathcal{U}$ are not easy to express for high values of p. In fact, calculating the eigenvalues of these units using formula (2) is far more economical and less subject to truncation errors than calculating the actual circulants. In one numerical test, we had the eigenvalues of several units of this type at hand, but our attempts to express the results as circulants (by using the Fourier inversion formula, §1.9.4) lost all precision beyond $p = 5$.

In our first calculation, we took the simplest case, $p = 5$, $q = 25$, and $\xi = \chi_2 = 1 + \zeta$. Our computer calculations indicated that

$$\begin{array}{rcl} \lambda_5(c) & = \lambda_{20}(c) & = 15127 \\ \lambda_{10}(c) & = \lambda_{15}(c) & = 1/15127 \end{array}$$

It looked as if the eigenvalues were rational, but this contradicted Proposition 5.1.5. Precise calculations (in large integer arithmetic) revealed that

$$\begin{array}{rcl} \lambda_5(c) & = \lambda_{20}(c) & = 15126.99993389303\ldots \\ \lambda_{10}(c) & = \lambda_{15}(c) & = 1/15126.99993389303\ldots \end{array}$$

The lesson is to check computer calculations with theory. The close approximation of the λ_5 eigenvalue to a rational integer is equivalent to a remarkably accurate approximation (within 5×10^{-9}):

$$\cos\left(2\pi/5\right) \ \sim\ \frac{37 \cdot 113}{2 \cdot 3 \cdot 5 \cdot 11 \cdot 41}$$

A second obstacle in the prime power case is that Lemma 7.6.7 is now false: $\lambda_1(c) = 0$ no longer implies that $\lambda_0(c) \equiv 0 \pmod p$. The upshot is that we no longer have a simple criterion for deciding when $\gamma_\sigma(\xi)$ is a unit circulant. Fortunately, this obstacle we can overcome, and the means of overcoming it will prove useful in analyzing the non-trivial kernel of λ_1

The trick is to restrict the constructions and the maps to the Kummer units and their images in the circulants under the γ_σ maps. This stratagem succeeds because of a fortuitous property of the basic Kummer units. Take any such a unit, $\chi_r = (\zeta^r - 1)/(\zeta - 1)$ say, where r is not divisible by p. If we set $\zeta = \zeta_p$, then $\chi_r \in C_p$. If we set $\zeta = \zeta_{p^2}$, then $\chi_r \in C_{p^2}$, $\zeta = \zeta_{p^3} \ \Rightarrow\ \chi_r \in C_{p^3}$, etc. −− whichever power of p we choose we obtain a unit in the cyclotomic field of that order.

Of course, our confinement to the Kummer units constrains the possible circulants units we can discover to those which are mapped onto C_q by λ_1. But against this, the Kummer units are always of finite index in the cyclotomic units, and for $\phi(q) \leq 66$, they are in fact all the cyclotomic units.

In the prime order case, we were allowed to pick any representative we wished from $\lambda_1^{-1}(\xi)$. However, to take advantage of the nice property of the Kummer units, we need to be more particular. For this reason we define a map γ to be a specific partial inverse to λ_1

7.7.3 **Definition** Define $\gamma : C_N \to \mathbf{circ}_N(\mathbb{Q})$ on the fundamental cyclotomic units, X, as follows †

$$\gamma(-1) = -1, \quad \gamma(-\zeta) \ :=\ -\mathrm{u}, \quad \text{and} \quad \gamma(\chi_r) \ :=\ \sum_{i=0}^{r-1} \mathrm{u}^i, \quad r = 2, \ldots, g = \tfrac{1}{2}\phi(N)$$

Now extend γ to all of C_N by the rule

$$\gamma\left(\chi_2^a \chi_3^b \cdots \chi_g^e\right) \ =\ \gamma(\chi_2)^a \gamma(\chi_3)^b \cdots \gamma(\chi_g)^e \qquad \forall a, b, \ldots, e \in \mathbb{Z}$$

We now show that this definition makes γ into a well-defined homomorphism on the Kummer units.

† When N is odd, the equation $\gamma(-1) = -1$ is redundant but harmless.

7·7·4 **Lemma** $\gamma : C_q \to \mathbf{circ}_q(\mathbb{Q})$ is a multiplicative monomorphism and $\gamma = \lambda_1^{-1}|C_q$.

Proof. We drop the q subscript throughout.

Firstly, $C = \mathrm{t}C \oplus F$ where F is free abelian, so we can verify that γ is a homomorphism separately on each of these direct summands. Theorem 7.3.10 shows $\mathrm{t}\mathcal{U} \approx \mathrm{t}C$ with the correspondence $\mathrm{u} \leftrightarrow \zeta$ and $\pm 1 \leftrightarrow \pm 1$ which is $\gamma|\mathrm{t}C$.

So we need only verify that γ is an monomorphism on F. Let Y be image of the Kummer basis for F under γ:

$$Y \;:=\; \{\gamma(\chi_r) \vdash 2 \le r \le \tfrac{1}{2}\phi(q),\ \gcd(r,N) = 1\}.$$

Assuming that the set generated by Y is a group, then it follows by a standard property of free abelian groups that γ is a homomorphism; the map γ acting on the free part of C -- the non-trivial fundamental units -- extends to a homomorphism on the elements freely generated by them. So we need to verify that Y generates a group in $\mathbf{circ}(\mathbb{Q})$. This must be so unless some member of $\gamma(Y)$ has a zero eigenvalue. Suppose $y = \gamma(\chi_r)$ is such a member. Then $y = \sum_{j=0}^{r-1} \mathrm{u}^j$ and $\lambda_0(y) = r \neq 0$. Therefore, for some $i > 0$, $0 = \lambda_i(\chi_r) = (1-\zeta^{ri})/(1-\zeta^i)$, which is impossible for r coprime to N.

To show that γ is an monomorphism, again by properties of free abelian groups, we need only verify that Y is a set of independent elements in $\mathrm{GL} \cap \mathbf{circ}(\mathbb{Q})$. By construction, $\gamma(\chi_r) \in \lambda_1^{-1}(\chi_r)$, for all $r = 2, ..\tfrac{1}{2}\phi(q)$. Hence, $\gamma(\xi) \in \lambda_1^{-1}(\xi)$ for all $\xi \in C$. Any relationship between the elements of Y, $y_1^{e_1} y_2^{e_2} \cdots y_t^{e_t} = 1$ say, implies the relationship $\lambda_1(y_1)^{e_1}\lambda_1(y_2^{e_2}) \cdots \lambda_1(y_t)^{e_t} = 1$ in C which contradicts the Kummer Theorem (§7.5.6.4). Hence Y is an independent set of generators in $\mathbf{circ}(\mathbb{Q})$. □

7·7·5 **Corollary** $\lambda_1|\gamma(C_q) = \gamma^{-1}$ is an isomorphism. □

In particular, $\lambda_1\gamma$ is well-defined on C_q, and $\gamma\lambda_1$ is well-defined on $\gamma(C_q) \subset \mathcal{U}_q$, but not on $\mathcal{U}_q$.

Here is the lemma which uses the nice property of the Kummer units.

7·7·6 **Lemma** $\lambda_{N/d}\,\gamma : C_N \to C_d$ for all $2 < d \,|\, N$.

Proof. We have $C_N = T \oplus F$ where T is the torsion part and equals the trivial units, and F is free abelian with generators X_N.

The statement is trivial on T, and so since both λ_d and γ are homomorphisms, we need only prove it on F. Let $\chi_r^{(N)} = (1-\zeta_N^r)/(1-\zeta_N) \in X_N$. By definition, $\gamma(\chi_r^{(N)}) \;=\; \sum_{i=0}^{r-1} \mathrm{u}^i$.

$$\therefore\ \lambda_{N/d}\gamma(\chi_r^{(N)}) \;=\; \sum_{i=0}^{r-1} \zeta_d^i \;=\; \chi_r^{(d)} \quad \text{(a Kummer unit)}$$

Hence we have a map $\lambda_d\gamma : X_N \to X_d$. By the free abelian property, this extends to a homomorphism $\lambda_{N/d}\gamma : C_N \to C_d$ as required. □

At this point, mostly for simplicity's sake, we shall assume that N is a prime power, $N = q = p^n$. In the non-prime power case, a fundamental set for the Kummer units is rather complicated. The problem lies not in finding a generating set: all χ_r^d with r coprime to p and $2 < d \,|\, q$ would serve, the problem is in specifying a fundamental set.

Even in the prime power case there is an additional complication: we need to replace the homomorphism ℓ_p with a homomorphism ℓ_q -- one that is defined modulo q instead of modulo p. One can easily check the definition of ℓ_p and the proof that it is a homomorphsim (see §7.2.6 and 7.2.7) and see that it cannot be consistently extended to a map on $\mathbb{Z}_q$. Again, we are saved by our confinement to the Kummer units. We define a new ℓ_q map on the basic Kummer units and extend it using the free property to the entire Kummer group of units.

7·7·7 **Definition** Let $q = p^n$, p an odd prime, $n \ge 1$. Define $\ell_q : C_q \to \mathbb{Z}_q^*$ by

$$\ell_q(-\zeta) \;:=\; -1 \bmod q$$
$$\ell_q(\chi_r) \;:=\; r \bmod q$$

and extend the definition to all of C_q multiplicatively.

7.7.8 **Lemma** ℓ_q is a group homomorphism and it agrees with λ_0 in that $\lambda_0\gamma(\xi) \bmod q = \ell_q(\xi)$.

Proof. That ℓ_q is a homomorphism follows from properties of free abelian groups.

Define $\nu : C_q \to \mathbb{Z}_q^*$ by $\nu(\xi) = (\lambda_0\gamma(\xi))^{-1} \bmod q$. Since λ_0, γ, and the modulus map are all group homomorphisms, and $\mathbb{Z}_q^*$ is an abelian group, ν is also a group homomorphism. Now define $\alpha(\xi) = \nu(\xi)\ell_q(\xi)$. Again since ν, ℓ_q are group homomorphisms to an abelian group, so is α. But, $\alpha(\xi) = 1$ on the basis elements. Therefore, $\alpha(\xi) = 1, \quad \forall \xi \in C_q$. The equation $\lambda_0\gamma(\xi) \bmod q = \ell_q(\xi)$ therefore holds everywhere on C_q. □

Remark The notation ℓ_q is consistent with ℓ_p --if $q = p$, then $\ell_q = \ell_p$. Also, $\ell_q(\xi) \pmod p = \ell_p(\xi)$.

We can now characterize those circulant units which are mapped to the cyclotomic units by λ_1, thus generalizing part *(i)* of Theorem 7.6.9 to the prime power case.

7.7.9 **Definition** Define $\gamma_+ := \mu\gamma : C_q \to \mathbf{circ}_q(\mathbb{Q})$, where $\mu(e) := (1-\bar\delta^q)_\times(e) = e - (e-1)\bar\delta^q$, and define $\gamma_-(\xi) := -\gamma_+(-\xi)$

7.7.10 **Proposition** For $\xi \in C_q$, $\gamma_\sigma(\xi) \in \mathcal{U}_q \Leftrightarrow \ell_q(\xi) \equiv \sigma \pmod q$.

Proof. Let $x = \gamma(\xi)$, and let $x_\sigma = \gamma_\sigma(\xi) = \mu_\sigma(x)$.

$\Rightarrow$ **:** $x_\sigma \in \mathcal{U} \Rightarrow \lambda_0(x_\sigma) = \pm 1 \Rightarrow \lambda_0(x) = \sigma \Rightarrow \ell_q(\lambda_1(x)) \equiv \sigma \pmod q \Rightarrow \ell_q(\xi) \equiv \sigma \pmod q$ by Corollary 7.7.5. QED($\Rightarrow$)

$\Leftarrow$ **:** To show that x_σ is a unit we need to show three things:

(a) $\lambda_0(x_\sigma) = \pm 1$,

(b) $\lambda_{q/d}(x)$ are units for all $p \le d \,|\, q$, and

(c) $x_\sigma \in \mathbf{circ}_q(\mathbb{Z})$.

Now, the eigenvalues of x_σ are identical to those of x except for λ_0 for which $\lambda_0(x_\sigma) = \sigma$. QED (a).

We are given that $\lambda_1(x) = \xi \in C_q$. We deduce immediately from Lemma 7.7.6 that $\lambda_{q/d}(x) \in C_{q/d}$ for $p \,|\, d \,|\, q$. QED (b).

So we are left with proving (c), that x_σ is integral. We are given that $\ell_q(\xi) = \sigma$, so by Lemma 7.7.8 $\lambda_0(x) = \sigma + kq$ for some integer k. By definition $x_\sigma = x - (x-\sigma)\bar\delta^q$. Now $\bar\delta^q$ is a rank 1 circulant; specifically, if c is any circulant, then $c\,\bar\delta^q = \lambda_0(c)\bar\delta^q$. Therefore, $x_\sigma = x - (x-\sigma)\bar\delta^N = x - \lambda_0(x-\sigma)\bar\delta^q = x - kq\bar\delta^q \in \mathbf{circ}_q(\mathbb{Z})$. □

7.7.11 **Definition** Let $\ell_q : C_q \to \mathbb{Z}_q^*$ be the homomorphism of §7.7.7. For $\sigma = \pm 1$, define

(i) $\bar C_q^\sigma := \gamma_\sigma(\ker_* \ell_q)$, and

(ii) $\bar C_q^\pm := \bar C_q^+ \cup \bar C_q^-$

7.7.12 **Proposition** Let $q = p^n$ where prime $p \ge 3$. Then,

(i) $\bar C_q^\pm \subset \mathcal{U}_q$;

(ii) $\bar C^\pm \cap \ker_* \lambda_1 = 1$

Proof. Statement *(i)* is immediate from Proposition 7.7.10. QED *(i)*

(ii) By Lemma 7.7.5, λ_1 is 1-1 on γC, so statement *(ii)* will follow if we can show that $\bar C^\sigma \subset \gamma C$ for $\sigma = \pm 1$. Consider first $\sigma = 1$. $\bar C^+ = \gamma_+ \ker \ell_q$, $\gamma_+ = \mu\gamma$, and μ is a group projection operator. Hence, $\mu\gamma \ker \ell_q \subset \gamma \ker \ell_q \subset \gamma C$ as desired.

In the case of $\sigma = -1$, let $c = \gamma_-(\xi)$ for some $\xi \in -\ker_* \ell_q$. If $\lambda_1(c) = 1$, then $1 = \lambda_1\gamma_-(\xi) = -\lambda_1\mu(-\gamma(\xi))$. Now, μ preserves λ_1. $\therefore 1 = -\lambda_1\mu(-\gamma(\xi)) = -\lambda_1(-\gamma(\xi)) = \xi$ by Corollary 7.7.5. $\therefore \xi = 1 \notin -\ker_* \ell_q$. Contradiction. $\therefore \bar C^- \cap \ker_* \lambda_1 = \emptyset$. □

By adopting the Kummer cyclotomic units as our base of operations as it were, we can concretely construct circulant units. However, when $q > p$, the rank of the full group of cyclotomic units (and therefore also of the Kummer units) is strictly less than the rank of the circulant units; consequently the units we have constructed account for a negligible proportion of the circulant units. To have any chance of describing the full group of circulant units we must account for the missing ranks in $\mathcal{U}_q$. It turns out that the missing ranks are entirely accounted for by $\ker_* \lambda_1$. This is the significance of part *(v)* of the last proposition--the constructed circulant units are all complementary to $\ker_* \lambda_1$.

7.7.13 **Decomposition of the Circulant Units.**

We now address the discrepancy between the ranks of $\mathcal{U}_N$ and E_N, and this will show how we can proceed. We confine ourselves to the prime power case and $q = p^n$ will be the prime power.

We are interested only in non-trivial circulant units, so we focus only on the free part of $\mathcal{U}_q$, call it $\mathcal{U}'_q$, and the free part of E_q, call it E'_q. Likewise let C'_q be the free part of C_q.

Corollary 7.5.6.2 to the Dirichlet Unit Theorem specifies that $\text{rank}E'_1 = \frac{1}{2}\phi(q) - 1 = \frac{1}{2}(p^n - p^{n-1}) - 1$ whereas the Higman Theorem (7.5.2) says that $\text{rank}\mathcal{U}'_q = \frac{1}{2}(p^n - 1) - n$ (where $p \geq 5$). When $n > 1$, $\text{rank}\mathcal{U}'_q > \text{rank}E'_q$ which means that no image of a cyclotomic subgroup can be of finite index in $\mathcal{U}'_q$. So, the method of the last section cannot succeed in the general prime power case, no matter how clever we are about constructing maps from E_q to $\mathcal{U}_q$.

By Proposition 7.7.10, $[C_q : C_q \cap \lambda_1(\mathcal{U}_q)] = \frac{1}{2}\phi(q)$. Now $\text{t}C_q = \text{t}\lambda_1(\mathcal{U}_q)$. $\therefore [C'_q : C'_q \cap \lambda_1(\mathcal{U}'_q)] = \frac{1}{2}\phi(q)$. Also, C'_q is of finite index in E'_q from which it follows that $\lambda_1(\mathcal{U}'_q)$ is of finite index in E'_q. Indeed, $[E'_q : \lambda_1(\mathcal{U}'_q)]$ divides $\frac{1}{2}\phi(q)[E'_q : C_q]$.

7.7.14 **Definition**

(i) Let $\mathcal{K}_q := \ker_* \lambda_1 | \mathcal{U}'_q$,

(ii) Let $\widetilde{U}_q := \lambda_1(\mathcal{U}'_q) \approx E'_q$.

By the theory of free abelian groups ([Rot]), we have the exact split sequence: **WRONG: This is not a split sequence**

$$0 \to \mathcal{K}_q \to \mathcal{U}'_q \to \widetilde{U}_q \to 0 \tag{3}$$

$$\therefore \ \mathcal{U}'_q \ \approx \ \widetilde{U}_q \oplus \mathcal{K}_q, \tag{4}$$

$$\therefore \ \text{rank}\mathcal{K}_q \ = \ \text{rank}\mathcal{U}_q - \text{rank}E_q \ = \ \tfrac{1}{2}\big(p^{n-1}-1\big) - n + 1 \ = \ \text{rank}\mathcal{U}_{q/p}$$

Free abelian groups of equal rank are isomorphic, therefore

$$\mathcal{U}'_q \ \approx \ \widetilde{U}_q \oplus \mathcal{U}'_{q/p} \tag{5}$$

$$\therefore \ \mathcal{U}'_q \ \approx \ \bigoplus_{j=1}^{n} E'_{p^j}, \quad \text{since } \widetilde{U}_q \approx E'_q \tag{6}$$

Isomorphism (6) is quite pretty, but it provides no clue as to its specification. We instead concentrate on formulas (4) and (5), and use them to inductively specify the units in $\mathcal{U}_q$, and to do this we we would like to prove in the general prime power case something along the lines of Lemmas 7.7.1 and 7.7.2.

In order to exploit isomorphism (5), we must find a subgroup of finite index in $\mathcal{U}_{q/p}$ which is somehow related to $\mathcal{K}_q \subset \mathcal{U}_q$. We shall show that $\mathcal{V}_q$ defined below is such a subgroup

7.7.15 **Definition**

(i) Let $\mathcal{V}_q := \{x \in \mathcal{U}'_q \vdash x \equiv 1 \pmod{p}\}$ --cyclotomic units of infinite order congruent to 1 mod p.

(ii) Let $V_q := \{\alpha \in E'_q \vdash \alpha \equiv 1 \pmod{p}\}$ --circulant units of infinite order congruent to 1 mod p.

Clearly, $\mathcal{V}_q$ and V_q are subgroups in the groups which contain them. We can alternatively describe $\mathcal{V}_q$ as the kernel of the modular map $\mathcal{U}_q \to \mathbf{circ}_q^*(\mathbb{Z}_p)$ [†]. This simple observation shows that $\mathcal{V}_q$ is of finite index in $\mathcal{U}_q$, and $[\mathcal{U}_q : \mathcal{V}_q] < q^p$.

The importance of the $\mathcal{V}_q$ subgroup will become apparent in Proposition 7.7.17 below which will demonstrate that $\mathcal{K}_q$ is the isomorphic image of $\mathcal{V}_{q/p}$ under a known map.

[†] These circulants are outside the purview of this book since the characteristic of the base ring divides their order.

Recall that in Lemma 7.7.1, we were given a cyclotomic integer in $\mathbb{Z}(\zeta_p)$ and from this we constructed a unit in $\mathbf{circ}_{p^2}(\mathbb{Z})$. For our present purposes we focus on just one step of that construction, the step which took us from a circulant $1+p\,a \in \mathbf{circ}_p(\mathbb{Z})$ to the circulant $1+p\Gamma_p^{p^2}(a) \in \mathbf{circ}_{p^2}(\mathbb{Z})$. We re-interpret this step as a map

$$\Gamma_{*p}^{p^2} : 1+pa \;\rightarrow\; 1+p\Gamma_p^{p^2}(a)$$

The Γ_* map is a multiplicative monomorphism on units. It is a special case of a general construction described in the next lemma whose proof is routine and is left to the reader.

7.7.16 **Lemma** Let R, S be (possibly non-commutative) rings with identities, and let $\alpha : R \rightarrow S$ be a ring homomorphism. Define $\alpha_* : R \rightarrow S$ by $\alpha_*(x) = 1_S + \alpha(x - 1_R)$. Then, α_* is multiplicative and if $G \subset R$ is a multiplicative group, then $\alpha_*|G$ is a group homomorphism. □

By setting $\alpha = \Gamma_{q/p}^q$ in the lemma, we get $\alpha_* = \Gamma_{*q/p}^q$. Let us consider eigenvalues.

$$\lambda_i^{(q)}\Gamma_{*q/p}^q(b) \;=\; \Big(1+\tilde{\Gamma}_{q/p}^q\big(\lambda^{(q/p)}(b-1)\big)\Big)_i \;=\; \begin{cases} \lambda_{i/p}^{(q/p)}(b) & \text{if } p \,|\, i \\ 1 & \text{otherwise} \end{cases} \tag{7}$$

Intuitively, $\lambda_1^{(q)}$ and its conjugates equal 1, all other eigenvalues are injected from $\lambda(b)$. Regarded as a map on circulant matrices, $\Gamma_{*q/p}^q$ is a monomorphism $\mathcal{U}_{q/p} \rightarrow \pm\mathcal{S}\mathrm{CIRC}_q(\mathbb{Q})$, the improper special rational circulant matrices. So, we need to find criteria which ensure that $\Gamma_{*q/p}^q(b)$ is an integer circulant. One sufficient condition is $b \in \mathcal{V}_{q/p}$.

7.7.17 **Proposition** For $q = p^n$, $p \geq 3$ prime, $\quad \mathcal{K}_q \;=\; \Gamma_{*q/p}^q\left(\mathcal{V}_{q/p}\right)$

Proof. First we show that $\Gamma_{*q/p}^q\left(\mathcal{V}_{q/p}\right) \subset \mathcal{K}_q$.

Let $b \in \mathcal{V}_{q/p}$, $b = 1 + p\,a$, say where $a \in \mathbf{circ}_{q/p}(\mathbb{Z})$. $\Gamma_{*q/p}^q(b)$ is an integer circulant because $\Gamma_{*q/p}^q(b) = 1+p\Gamma_{q/p}^q(a) \in \mathbf{circ}_{q/p}(\mathbb{Z})$ (see the definition of the repeater map, §3.5.1). The Γ_* map is a group homomorphism, therefore $\Gamma_{*q/p}^q(\mathcal{V}_{q/p})$ is a subgroup of $\mathbf{circ}_{q/p}(\mathbb{Z})$, and therefore must be a group of circulant units. Equation (7) shows that $\lambda_1\Gamma_{*q/p}^q(b) = 1$ which means $\Gamma_{*q/p}^q\left(\mathcal{V}_{q/p}\right) \subset \mathcal{K}_q$.

We now show that $\mathcal{K}_q \subset \Gamma_{*q/p}^q\left(\mathcal{V}_{q/p}\right)$.

$$\begin{aligned} c \in \mathcal{K}_q \;&\Rightarrow\; \lambda_1(c) = 1 \;\Rightarrow\; c - 1 \in p(\bar{\delta}^p) \quad \text{by Corollary 3.4.6} \\ &\Rightarrow\; c = 1 \;+\; p\,\Gamma_{q/p}^q(c') \quad \text{where } c' \in \mathbf{circ}_{q/p}(\mathbb{Z}), \text{ by Corollary 3.5.6.5} \\ &\Rightarrow\; c = \Gamma_{*q/p}^q(b), \quad \text{where } b = 1 + pc' \end{aligned}$$

We see from equation (7) that since c is a unit so b must be a unit. Similarly, since c is not torsion, neither is b. Therefore, $b \in \mathcal{V}_{q/p}$. □

A word of caution: the element injected into $\mathcal{K}_q$ from $\mathcal{U}_{q/p}$ by Γ_* is not ready for another injection into $\mathcal{K}_{pq}$. Despite its appearance, $1 + p\Gamma_{q/p}^q(a) \not\equiv 1 \pmod{p}$ in general since $\Gamma_{q/p}^q(a) \in p^{-1}\mathbf{circ}(\mathbb{Z})$.

Proposition 7.7.17 allows us to rewrite the isomorphism (4) as

$$\mathcal{U}_q' \;\approx\; \widetilde{U}_q \;\oplus\; \Gamma_{*q/p}^q\left(\mathcal{V}_{q/p}\right) \tag{8}$$

The above isomorphism is inadequate for the task of characterizing the unit circulants. We really need to find an embedding of established groups into a subgroup of finite index in $\mathcal{U}_q'$. By "established groups," we mean either well-defined subgroups of the cyclotomic units or groups of unit circulants of lower order than q. The point here of course is to describe the so-far unestablished unit circulants of order q in terms of established groups. In Proposition 7.7.17 and equation (8), we have accomplished this for the $\mathcal{K}_q$ component of (4); we must now do the same for the $\widetilde{U}_q$ component in equation (8). So we would like to find a subgroup of low index in $\widetilde{U}_q$. A promising tack is to look for subgroups of $\mathcal{U}_q'$ complementary to $\mathcal{K}_q$ in $\mathcal{U}_q'$. The next lemma provides a characterization of $\mathcal{K}_q$ which will help us in identifying a complementary subgroup.

7.7.18.5 **Lemma** If $\Phi_q(x)$ is irreducible in the domain R, then $\ker_* \lambda_1|\mathbf{circ}_q(R) = \text{Im } \bar{\delta}^p_\times \cap \mathbf{circ}_q(R)$.

Proof. By definition, $\bar{\delta}^p_\times(x) = 1 + \bar{\delta}^p(x-1)$.

First we show that $\ker_* \lambda_1 \supset \text{Im } \bar{\delta}^p_\times \cap \mathbf{circ}(R)$. So suppose that $c = \bar{\delta}^p_\times(x) \in \mathbf{circ}(R)$ for some $x \in \mathbf{circ}(R)$. Then, $\lambda_1(c) = \lambda_1(1 + \bar{\delta}^p(x-1)) = 1$, and $c \in \ker_* \lambda_1$ as required.

It is trivial that $\ker_* \lambda_1|\mathbf{circ}_q(R) \subset \mathbf{circ}_q(R)$. So we need only prove that $\ker_* \lambda_1 \subset \text{Im } \bar{\delta}^p_\times$. Now, $\lambda_1(c) = 1 \Rightarrow \lambda_1(c-1) = 0 \Rightarrow c = 1 + xp\bar{\delta}^p$ for some $x \in \mathbf{circ}(R)$ by Corollary 3.4.6. Consider $\bar{\delta}^p_\times(c) = 1 + \bar{\delta}^p(1 + xp\bar{\delta}^p - 1) = 1 + xp\bar{\delta}^p = c$. That is, $c \in \bar{\delta}^p_\times(\mathbf{circ}(R))$. □

7.7.18.7 **Lemma** $\mathcal{K}_q = \bar{\delta}^p_\times(\mathcal{U}'_q) \cap \mathcal{U}'_q$.

Proof. By definition, $\mathcal{K} = \ker \lambda_1|\mathcal{U}'$, so Lemma 7.7.18.5 implies $\mathcal{K} = \bar{\delta}^p_\times(\mathbf{circ}(\mathbb{Z})) \cap \mathcal{U}'$. $\therefore \mathcal{K} = \bar{\delta}^p_\times(\mathcal{U}') \cap \mathcal{U}'$ because $\bar{\delta}^p_\times$ is an idempotent map. □

7.7.17.1 **Definition** For any subset $S \subset \mathbf{circ}^*_q(\mathbb{Q})$ define $\pi S = (1 - \bar{\delta}^p)_\times(S) \cap S$.

Note that π is a map on the power-set of the rational circulants not on the circulants themselves, and that $\pi^2 = \pi$.

7.7.17.2 **Proposition** $\mathcal{U}'_q = \pi\mathcal{U}'_q \oplus \Gamma^q_{*q/p}(\mathcal{V}_{q/p})$

Proof. Since q is fixed, we shall drop the q-subscripts throughout the proof.

By the exact sequence (3), we have $\mathcal{U}' = X \oplus \mathcal{K}$ where X is an as yet to-be-determined subgroup of $\mathcal{U}$. Since $\mathcal{K} = \Gamma^q_{*q/p}(\mathcal{V}_{q/p})$ by Proposition 7.7.17, we need only find a suitable X.

By Lemma 7.7.18.7, we know that X is complementary to $\mathcal{K} = \bar{\delta}^p_\times(\mathcal{U}') \cap \mathcal{U}'$. The complementary operator to $\bar{\delta}^p_\times$ is $(1-\bar{\delta}^p)_\times$. So, $X \subset (1-\bar{\delta}^p)_\times(\mathbf{circ}(\mathbb{Z}))$. We can be more specific. For any $u \in \mathcal{U}'$, we have $u = xk$ where $x \in X$ and $k \in \mathcal{K} \subset \mathcal{U}'$. $\therefore x \in \mathcal{U}'$. $\therefore X \subset (1-\bar{\delta}^p)_\times(\mathbf{circ}(\mathbb{Z})) \cap \mathcal{U}'$. $\therefore X \subset (1-\bar{\delta}^p)_\times(\mathcal{U}') \cap \mathcal{U}' = \pi\mathcal{U}'$ since $(1-\bar{\delta}^p)_\times$ is an indempotent.

We shall now prove the opposite inclusion. Trivially, $\pi\mathcal{U}' \subset \mathcal{U}'$. By complementarity of the idempotents $\bar{\delta}^p$ and $(1-\bar{\delta}^p)_\times$, we have $1 = \big((1-\bar{\delta}^p)_\times(\mathcal{U}') \cap \mathcal{U}'\big) \cap \big(\bar{\delta}^p_\times(\mathbf{circ}(\mathbb{Z})) \cap \mathcal{U}\big) = \pi\mathcal{U}' \cap \mathcal{K}$. So $\pi\mathcal{U}'$ is complementary to $\mathcal{K}$ in $\mathcal{U}'$ and contains X. But, $\mathcal{U}' = X\mathcal{K}$. This is possible only if $\pi\mathcal{U}' \subset X$. □

Proposition 7.7.17.2 is still unsatisfactory in that the first direct summand is defined in terms of $\mathcal{U}_q$, the very group we are trying to describe. Now, $\text{rank}\pi\mathcal{U}'_q = \text{rank}\widetilde{U}_q = \text{rank}E'_q$, an established group. We therefore look for a "natural" map $E_q \to \pi\mathcal{U}'_q$. A good candidate for such a map is defined next.

7.7.17.5 **Definition** $\gamma_* := (1-\bar{\delta}^p)_\times \lambda_1^{-1} : E_q \to \mathbf{circ}_q(\mathbb{Q})$.

It is easy to verify that γ_* is a well-defined multiplicative homomorphism, and that $\lambda_1\gamma_* = \text{id} : E_q \to E_q$ from which it follows that γ_* is actually a monomorphism.

There is a problem with γ_*; its range is $\mathbf{circ}_q(\mathbb{Q})$ not $\pi\mathcal{U}'_q$ that we were looking for. We can overcome this difficulty it we find a subgroup of E_q that is mapped by γ_* into $\pi\mathcal{U}'_q$. V_q is precisely such a subgroup as we shall show. But first, we need a couple of lemmas.

7.7.18 **Lemma**

Let $x = 1 + pa$ where a is an integer circulant. Then, $\bar{\delta}^p_\times(x)$ and $(1-\bar{\delta}^p)_\times(x)$ are also integer circulants.

Proof. For example, by definition, $\bar{\delta}^p_\times(x) = 1 - \bar{\delta}^p(x-1) = 1 + \bar{\delta}^p pa \in \mathbf{circ}(\mathbb{Z})$. □

The next proposition is key; it shows two things: how the γ_* homomorphism connects the $\mathcal{V}$ and V groups, and that $\mathcal{V}$ has a direct sum decomposition similar to that for $\mathcal{U}$ in (4).

7.7.19 **Proposition** $\mathcal{V}_q \;=\; (\mathcal{K}_q \cap \mathcal{V}_q) \;\oplus\; \gamma_* V_q$

Proof. We fix q and drop the q subscript throughout. We have the following decomposition in $\mathbf{circ}(\mathbb{Q})$:

$$\mathcal{V} \;=\; \bar{\delta}^p_\times(\mathcal{V}) \;\oplus\; (1-\bar{\delta}^p)_\times(\mathcal{V})$$

By Lemma 7.7.18, this is actually a decomposition in $\mathbf{circ}(\mathbb{Z})$.

It is clear from Lemma 7.7.18.5 with $R=\mathbb{Z}$ that $\bar{\delta}^p_\times\mathcal{V} = \ker_*\lambda_1|\mathcal{V} = \mathcal{K}\cap\mathcal{V}$. So all we need show is that $\gamma_* V = (1-\bar{\delta}^p)_\times(\mathcal{V})$.

We first show that $\gamma_* V \subset (1-\bar{\delta}^p)_\times(\mathcal{V})$. Let $\alpha\in V$, $\alpha = 1+pA(\zeta)$ say, for some $A\in\mathbb{Z}[x]$. Let $x = 1+pA(\mathrm{u})$. Then, $\lambda_1(x)=\alpha\in V$, and $\gamma_*(\alpha) = (1-\bar{\delta}^p)_\times(x)\in\mathbf{circ}(\mathbb{Z})$ by Lemma 7.7.18. Since γ_* is a homomorphism, we can apply the same argument to α^{-1} and deduce that $x^{-1}\in\mathbf{circ}(\mathbb{Z})$, which means $x\in\mathcal{U}$, and hence that $x\in\mathcal{V}$. Therefore, $\gamma_*(\alpha)\in(1-\bar{\delta}^p)_\times(\mathcal{V})$.

Now let $x\in\mathcal{V}$. Since x is a unit, so is $\lambda_1(x)=\alpha$ say, and $\alpha\in V$. Now, $\gamma_*(\alpha) = (1-\bar{\delta}^p)_\times\lambda_1^{-1}\lambda_1(x)$. This must have a unique value since γ_* is well-defined; clearly, the value must be $(1-\bar{\delta}^p)_\times(x)$. Therefore, $(1-\bar{\delta}^p)_\times(x) = \gamma_*(\alpha)\in\gamma_* V$. □

7.7.20 **Corollary**

(i) $V_q = \lambda_1\mathcal{V}_q$

(ii) $\gamma_* V_q \subset \mathcal{V}_q$

(iii) $\gamma_* V_q \cap \mathcal{K}_q \;=\; 1$

(iv) $\gamma_* V_q \subset \pi\mathcal{U}'_q$

Proof. Statements *(i)* and *(ii)* are immediate from Proposition 7.7.19.

(iii) Statement *(ii)* and the Proposition imply that $\gamma_* V_q$ and $\mathcal{K}_q\cap\mathcal{V}_q$ are complementary in $\mathcal{V}_q$ QED *(iii)*

(iv) By definition of γ_*, we have $\gamma_* V_q \subset (1-\bar{\delta}^p)_\times(\mathbf{circ}_q(\mathbb{Q}))$, and by Statement *(ii)* $\gamma_* V_q \subset \mathcal{V}_q \subset \mathcal{U}'_q$. $\therefore\ \gamma_* V_q \subset \mathcal{U}'_q \cap (1-\bar{\delta}^p)_\times(\mathbf{circ}_q(\mathbb{Q})) = \pi\mathcal{U}'_q$ since $(1-\bar{\delta}^p)_\times$ is a projection operator. □

The corollary leads to the following subgroup relationships:

$$\mathcal{V}_q\mathcal{K}_q \;=\; (\gamma_* V_q \;\oplus\; (\mathcal{V}_q\cap\mathcal{K}_q))\,\mathcal{K}_q \;=\; \gamma_* V_q \;\oplus\; \mathcal{K}_q \;\subset\; \pi\mathcal{U}'_q \;\oplus\; \mathcal{K}_q \;=\; \mathcal{U}'_q \tag{10}$$

where $\mathcal{K}_q = \Gamma^q_{*q/p}\left(\mathcal{V}_{q/p}\right)$ and $\pi\mathcal{U}'_q = (1-\bar{\delta}^p)_\times\left(\mathcal{U}'_q\right)\cap\mathcal{U}'_q$,

The $\gamma_* V_q\oplus\mathcal{K}_q$ term in the above sequence is an established group in that the first summand is defined in terms of the cyclotomic units, and the second, $\mathcal{K}_q = \Gamma^q_{*q/p}\left(\mathcal{V}_{q/p}\right)$, is defined in terms of lower order circulants. We therefore seek the index of this group in $\mathcal{U}_q$.

We have $[\mathcal{U}'_q : \gamma_* V_q\oplus\mathcal{K}_q] = [\,\pi\mathcal{U}'_q : \gamma_* V_q]$. Now, $\pi\mathcal{U}'_q \subset (1-\bar{\delta}^p)_\times\left(\mathcal{U}'_q\right)\subset\gamma_* E'_q$, so

$$[\mathcal{U}'_q : \gamma_* V_q\oplus\mathcal{K}_q] \;\mid\; [\gamma_* E'_q : \gamma_* V_q]$$

and

$$[\gamma_* E'_q : \gamma_* V_q] \;=\; \frac{[E'_q : V_q]}{[\,\ker\gamma_* \;:\; V_q\cap\ker\gamma_*]} \;=\; [E'_q : V_q]$$

since γ_* is a monomorphism.

$$\therefore\ [\mathcal{U}'_q : \gamma_* V_q\oplus\mathcal{K}_q] \;\mid\; [E'_q : V_q] \tag{11}$$

We need a lemma in order to estimate $[E'_q : V_q]$.

7.7.21 **Lemma** Let $\alpha\in\mathbb{Z}(\zeta_q)$ where $q=p^n$, $n\geq 1$. Then, $\alpha^q \;\equiv\; \ell_p(\alpha) \pmod p$.

Proof. Let $\alpha = a_0 + a_1\zeta_q + \cdots + a_m\zeta_q^m$ for some m and $a_0, a_1, \ldots, a_m\in\mathbb{Z}$. We have

$$(a_0 + a_1\zeta_q + \cdots + a_m\zeta_q^m)^q \;\equiv\; \left(a_0^p + a_1^p\zeta_{q/p} + \cdots + a_m^p\zeta_{q/p}^m\right)^{q/p} \pmod p$$

We proceed to descend through powers of p until we obtain

$$(a_0 + a_1\zeta_q + \cdots + a_m\zeta_q^m)^q \;\equiv\; (a_0^q + a_1^q + \cdots + a_m^q) \pmod p$$

The result follows since any rational integer x satisfies $x^q\equiv x \pmod p$. □

7.7.22 **Definition** We define V^q to be set of units in V_q which are constructed using Lemma 7.7.21. That is, $V^q = \{\xi^q \vdash \xi \in E'_q \ \& \ \ell_p(\xi) = 1\}$. The lemma implies that V^q is a subgroup of V_q.

7.7.23 **Lemma** Let $q = p^n$ with $p \geq 3$, $n \geq 1$. Then, $[E'_q : V^q] \ = \ (p-1)\, q$.

Proof. V^q is the q^{th} power of every element in $\ker \ell_p | E'_q$ and furthermore, $\ell_p | E'_q$ is onto by Lemma 7.6.6. Hence, $[E_q : V^q] = [E'_q : \ker \ell_p]\, q = (p-1)q$. □

7.7.24 **Proposition** $[\mathcal{U}'_q : \gamma_* V_q \oplus \mathcal{K}_q] \,|\, (p-1)q$.

Proof. This is immediate from Proposition 7.7.23 and equation (11). □

We have have obtained an upper bound of $(p-1)q$ on $[\mathcal{U}_q : \mathcal{V}_q\mathcal{K}_q]$ using the equation $\mathcal{V}_q\mathcal{K}_q = \gamma_* V_q \oplus \mathcal{K}_q$, the latter being an established group, and we also used the fact that $[E'_q : V^q]$ is an upper bound on $[E'_q : V_q]$ since $V^q \subset V_q$. Can we not improve this estimate by calculating $[E'_q : V_q]$ itself ? There is a reason to suspect that we cannot, at least in all cases. There is a famous lemma of Kummer which is a partial converse to Lemma 7.7.21 which suggests that $V^q = V_q$ is a possiblity for many q.

7.7.25 **Kummer's Lemma** Let p be a prime that does not divide the class number h_p (that is, p is a "regular prime"). If $\xi \in E_p$, then $\xi = \eta^p$ for some $\eta \in E_p$. □ (See [Was4], [Lang2]).

However, there is another interesting possibility: $\mathcal{V}_q\mathcal{K}_q$ does not wholly contain $\bar{C}^{\pm}$, the elements constructible from the Kummer units as in Proposition 7.7.12. So the question is how much of the index $(p-1)q$ is accounted for by elements in $\bar{C}^{\pm} - \mathcal{V}_q\mathcal{K}_q$.

7.7.26 **Lemma** If $c \in \mathcal{U}_q$ then either $c^q \in \mathcal{V}_q$ or $-c^q \in \mathcal{V}_q$ according as $\lambda_0(c) = +1$ or -1 respectively.

Proof. By Lemma 7.7.21, $\lambda_i(c^q) = \lambda_0(c) + pA(\zeta_q^i)$ where $A \in \mathbb{Z}[x]$ which implies $c^q = \lambda_0(c) + pA(\mathrm{u})$. Since c is a unit, $\lambda_0(c) = \pm 1$. If $\lambda_0(c) = 1$, then $c^q \in \mathcal{V}_q$ else $-c^q \in \mathcal{V}_q$. □

7.7.27 **Corollary** $\forall x \in \bar{C}_q^{\sigma}$, $(\sigma x)^q \in \mathcal{V}_q$. □

7.7.28 **Proposition** Let $\xi \in \ker \ell_q - \{1\}$. Then, $\xi^r \equiv 1 \pmod{p} \ \Leftrightarrow \ q \,|\, r$.

Proof. Let n be the order of $\xi \pmod{p}$. RTP: $n = q$.

Since $\xi \in \ker \ell_q$, $\ell_p(\xi) = 1$; so by Proposition 7.7.21, $\xi^q \equiv 1 \pmod{p}$. $\therefore\ n \,|\, q$. $\therefore\ n = p^r$ for some $r \geq 0$.

Let $\zeta = \zeta_q$ and let $\xi = a_0 + a_1\zeta + a_2\zeta^2 \cdots a_{g-1}\zeta^{g-1}$ where $g = \phi(q) = q - q/p$. Since $\xi \neq 1$, there exists a non-zero coefficient besides a_0 in the expansion for ξ; let this coefficient be a_k where $0 < k < g$. Following the proof of Lemma 7.7.21 we have for $n = p^r$,

$$\xi^n \ \equiv \ a_0 \ + \ \cdots \ + \ a_k\zeta^{nk} \ + \ \cdots \ + \ a_{g-1}\zeta^{n(g-1)} \pmod{p}$$

and this does not become a rational integer modulo p until $n = q$. □

7.7.29 **Corollary** Let ξ be as in Proposition 7.7.28. Then, $\xi^r \in V_q \ \Leftrightarrow \ q \,|\, r$. □

7.7.30 **Proposition** Let $x \in \bar{C}_q^- - \{-1\}$. Then, $x^r \in \mathcal{V}_q\mathcal{K}_q \ \Leftrightarrow \ 2q \,|\, r$.

Proof. By Corollary 7.7.27, $-x^q \in \mathcal{V}_q$. Therefore, $x^{2q} \in \mathcal{V}_q$. So we need only show that $2q$ is the least positive with this property.

Let $\xi = \lambda_1(x)$. Applying Corollary 7.7.29 to ξ^2 we get $\xi^{2q} \in V_q$ and $2q$ is least positive such. But, $\lambda_1(\mathcal{V}_q\mathcal{K}_q) = \lambda_1(\mathcal{V}_q) = V_q$ by Corollary 7.7.20. Therefore, $2q$ is the least positive such that $x^{2q} \in \mathcal{V}_q$. □

7.7.31 **Corollary** Let $H = \langle \gamma_-(\chi_2\chi_{(q-1)/2}) \rangle \subset \mathcal{U}_q$. Then, $[\mathcal{U}_q : H\gamma_*(V_q)\mathcal{K}_q] \mid \frac{1}{2}(p-1)$. □

Chapter 8.
Irreducibles, Primes, and Ideals of $\mathbf{circ}_{N}(\mathbb{Z})$.

This chapter develops a theory of factorization of the integer circulants, $\mathbf{circ}_{N}(\mathbb{Z})$. Divisibility is normally studied in domains, but there is no intrinsic reason why we cannot ask the question whether factorization into irreducibiles is possible in general commutative rings. Even if divisors of zero pose difficulties, we can avoid such ring elements. But, at least in the case of the integer circulants, there is a well-defined factorization possible in all cases.

A theory of factorization is typically applied to number theory, and this is one possible application of factorization of integer circulants.

Although this chapter is focused on the integer circulants, circulants over other rings are also discussed where it seems opportune.

8.1 General Results

Propositions 8.1.2 and 8.1.3 which follow are taken from Kaplansky [Kap] where they were proved for general commutative rings with identity. In fact, they apply to commutative semigroups with identity since they do not require the existence of ring addition. The importance of these propositions in the present context is that they show the intimate connection between the unit group of a ring and its prime and maximal ideals. This chapter complements the previous whose emphasis was the units of $\mathbf{circ}_{N}(\mathbb{Z})$.

8.1.1 **Definition** Let R be a commutative ring with identity. If $S \subset R$ is multiplicatively closed and has the property that every divisor of an element of S is also in S, then S is said to be **multiplicatively saturated**.

8.1.2 **Proposition** Let R be as above and let $S \subset R$. S is multiplicatively saturated iff $R - S$ is a union of prime ideals.

Proof. Suppose first that $R - S$ is a union of prime ideals. $xy \in R - S$ iff $xy \in P$ for some prime ideal P iff x or $y \in P$ by the primality of P. Now apply de Morgan's law to derive the complementary equivalence: $xy \in S$ iff $x, y \in S$. That is, S is multiplicatively saturated.

The converse follows reversing the above proof starting with the definition of multiplicatively saturated. □

8.1.3 **Proposition** Let R be as above. Then, $\mathbf{U}(R)$ is multiplicatively saturated and its complement is the union of all maximal ideals.

Proof. Let $U = \mathbf{U}(R)$. U is obviously multiplicatively closed and if $xy \in U$ then $\exists z$ s.t. $xyz = 1$. $\therefore x^{-1} = yz$, and $y^{-1} = zx$. $\therefore x, y \in U$. $\therefore U$ is saturated.

No ideal can intersect U. Therefore, we can apply Zorn's lemma and take the prime ideals of Lemma 8.1.2 as maximal. □

By Proposition 7.2.2, the unit group of $\mathbf{circ}(\mathbb{Z})$ is all those whose determinant is ± 1, and the unit group of $\mathbf{circ}(F)$ where F is a field is the set of non-singular circulant matrices. Hence,

8.1.4 **Corollary** Let $M(R)$ be the set of maximal ideals in $\mathbf{circ}_{N}(R)$. Then, $\bigcup M(\mathbb{Z}) = \{a \in \mathbf{circ}_{N}(\mathbb{Z}) \vdash \det(a) \neq \pm 1\}$, and if F is a field, then $\bigcup M(F) = \{a \in \mathbf{circ}_{N}(\mathbb{Z}) \vdash \det(a) = 0\}$. □

One of the most useful concepts in ring theory is that of a Noetherian ring. A commutative ring is said to be **Noetherian** if every ascending chain of ideals is finite. That is if $I_1 \subset I_2 \subset \cdots \subset I_i \subset \cdots$ are ideals then $I_i = I_n$ for all $i \geq n$ for some n. It can be shown that a ring is Noetherian iff every ideal in the ring is finitely generated. A ring which contains only principal ideals is called a principal ideal or a P.I. ring. A P.I. ring is trivially Noetherian. Hence, the integers are Noetherian, and so is any field. The next theorem and the proposition which follows provide many more examples of Noetherian rings.

8.1.5 **The Hilbert Basis Theorem** If R is Noetherian then so is $R[x]$.

Proof. See Kaplansky [Kap2]. □

8.1.6 **Proposition** Ring epimorphisms map P.I. rings to P.I. rings, and map Noetherian rings to Noetherian rings.

Proof. Let $\alpha : A \to B$ be a ring epimorphism. Let J be an ideal in B and let $I = \alpha^{-1}(J)$. First assume that A is a P.I. ring. Then, I is an ideal and so is principal, $I = Ac$, say. Therefore, $J = \alpha(A)\alpha(c) = B\alpha(c)$ and is a principal ideal.

Now assume that A is Noetherian. Then, I is finitely generated, $I = Ac_1 + Ac_2 + \cdots + Ac_n$, say.

$$\therefore\ J \ = \ \alpha(A)\alpha(c_1) + \alpha(A)\alpha(c_2) + \cdots + \alpha(A)\alpha(c_n) \ = \ B\alpha(c_1) + B\alpha(c_2) + \cdots + B\alpha(c_n)$$ □

8.1.7 **Corollary** If F is a field then $\mathbf{circ}_{N}(F)$ is a P.I. ring.

Proof. $F[x]$ is P.I. and $\Gamma^N : F[x] \to \mathbf{circ}_{N}(F)$ is onto. □

On the other hand, it will be demonstrated in Proposition 8.4.12 that $\mathbf{circ}_{N}(\mathbb{Z})$ is not a P.I. ring.

8.1.8 **Corollary** If R is Noetherian then so is $\mathbf{circ}_{N}(R)$. In particular, $\mathbf{circ}_{N}(\mathbb{Z})$ is Noetherian. □

8.2 A Circulant Norm

We define a norm function on integer circulants which has most of the nice properties of norms on domains, and also provides the same advantages of such norms: it can be used to limit the possible factorizations of integer circulants.

8.2.1 **Definition** Let $c \in \mathbf{circ}_{N}(R)$. The **circulant norm** of c is denoted by $\mathcal{N}^{\circ}(c)$, and is defined to be the cardinality of the quotient ring $\mathbf{circ}_{N}(R)/(c)$.

Knowledge of the circulant norm places useful constraints on the structure of $\mathbf{circ}(R)$. Take for example the case where $\mathcal{N}^{\circ}(c)$ is a prime number; the quotient ring $\mathbf{circ}(R)/(c)$ must be a field, and the principal ideal generated by c must be a maximal, prime ideal in $\mathbf{circ}(R)$. Fortunately, when $R = \mathbb{Z}$ there is a simple formula for the circulant norm.

8.2.2 **Theorem** Let $a \in \mathbf{circ}(\mathbb{Z})$. Then,

$$\mathcal{N}^{\circ}(a) \ = \ \begin{cases} |\Delta(a)| & \text{if } \Delta(a) \neq 0 \\ \infty & \text{otherwise} \end{cases}$$

Proof. (This proof is similar to that commonly used for the algebraic norm.)

We first take the case where a is a non-singular circulant. Let $a \in \mathbf{circ}_{N}(\mathbb{Z})$. (Henceforth, N is assumed.) Regard $\mathbf{circ}(\mathbb{Z})$ as a subring of $\mathbf{circ}(\mathbb{Q})$, and consider the vector space map on $\mathbb{Q}^N$ which is defined on the standard orthonormal basis by $T_a : \mathrm{u}^i \mapsto a\mathrm{u}^i$. The importance of T_a is that it maps $\mathbf{circ}(\mathbb{Z})$ onto the ideal $a\mathbf{circ}(\mathbb{Z}) = (a)$. Also, the transformation T_a is represented by the matrix $\mathrm{CIRC}(a)$, as one can easily verify. Hence, $\det T_a = \Delta(a)$.

Let $D = \{x \in \mathbf{circ}(\mathbb{Z}) \vdash x = a\sum_i b_i \mathrm{u}^i \text{ where } 0 \leq b_i < 1\} \subset \mathbf{circ}(\mathbb{Q})$.

Claim: D is a transversal for the cosets of (a) in $\mathbf{circ}(\mathbb{Z})$.

Proof of claim:

Since, $\det T_a = \Delta(a) \neq 0$, T_a is non-singular. Therefore, $\{a, a\mathrm{u}, a\mathrm{u}^2, \ldots, a\mathrm{u}^{N-1}\}$ is a basis for $\mathbb{Q}^N$. So, given any $y \in \mathbf{circ}(\mathbb{Z}), \exists g_i \in \mathbb{Q}$ such that

$$y \ = \ a\sum_{i=0}^{N-1} g_i \mathrm{u}^i \ = \ a\sum_i \{g_i\}\mathrm{u}^i + a\sum_i \lfloor g_i \rfloor \mathrm{u}^i \ \equiv \ x \pmod{a\mathbf{circ}(\mathbb{Z})} \quad \text{where } x \in D$$

This shows that $D + (a) = \mathbf{circ}(\mathbb{Z})$. To show that D is a transversal, we must also show that no two elements of D are in the same (a)-coset. So, suppose that $x, y \in D$ with $x - y \in a\mathbf{circ}(\mathbb{Z})$. Then, $x - y \in T_a(\mathbf{circ}(\mathbb{Z}))$. $\therefore x - y = T_a(z)$ for some integer circulant z. But, by construction of D, $x, y \in T_a(I)$ where I is the unit cube at the origin in $\mathbb{Q}^N$ having non-negative coordinates. Therefore, $\exists!\ x', y' \in I$ s.t. $x' = T_a^{-1}x, y' = T_a^{-1}y$, and $x' - y' = z$. This means that z, a point in the lattice $\mathbb{Z}^N$, has coordinates which are the difference of pairs of numbers in the interval $[0, 1)$. This is possible only if $z = 0$. **QED Claim**

We have shown that the cardinality of $\mathbf{circ}(\mathbb{Z})/(a) = |D|$. The number of circulants in D is the number of integral points in D. D is the image of the unit cube under a linear transformation which maps integral points to integral points. Therefore, the count of integral points in D is product of the number of integral points on each coordinate of the basis $\{a, a\mathrm{u}, a\mathrm{u}^2, \ldots, a\mathrm{u}^{N-1}\}$ (the image under T_a of the unit basis). This product is just the absolute value of the area of D as a subset of Euclidean $\mathbb{R}^N$. The absolute area of $D = |\det T_a|$ as desired.

This proves the theorem in the case when $\Delta(a) \neq 0$.

Now suppose $\Delta(a) = 0$. Then, the linear transformation T_a is singular, and its range will have dimension less than N. Therefore, one intuitively sees that there must be a circulant, b, say, which has a component orthogonal to $a\mathbf{circ}(\mathbb{Z})$. Hence, nb are distinct modulo (a) for all integers n. In fact, we can take $b = 1$. That is, the scalar integers are in distinct (a)-cosets. For suppose, $n_1 \equiv n_2 \pmod{(a)}$. Then, $n = n_1 - n_2$ is in (a). So, there exists an integer circulant a' such that $n = aa'$. If n is non-zero, then a has an inverse in $\mathbf{circ}(\mathbb{Q})$, namely, $n^{-1}a'$. Contradiction. Therefore, $n = 0$. □

The theorem tells us a lot about $\mathbf{circ}(\mathbb{Z})/(a)$, and, of course, when $\Delta(a)$ is prime, the isomorphism class of the quotient ring will be completely specified. This specificity can be extended to the case where $|\Delta(a)|$ is square-free because all rings of square-free order are cyclic. Hence, we have

8.2.3 **Corollary** Let $a \in \mathbf{circ}(\mathbb{Z})$. If $D = |\Delta(a)|$ is non-zero and square-free, then $\mathbf{circ}(\mathbb{Z})/(a) \approx \mathbb{Z}_D$. □

The proposition below shows that there is a severe constraint on $\Delta(a)$ being square-free.

8.2.4 **Proposition** Let $a \in \mathbf{circ}(\mathbb{Z})$, let $D = |\Delta(a)|$, and let the ring $\mathbf{circ}(\mathbb{Z})/(a)$ be finite with characteristic c. If D is square-free then $D = c$.

Proof. Let $A = \mathrm{CIRC}(a)$. The scalar $D = |\Delta(A)|$ is in the ideal (A) because $(\det A)I = A^*A$ where A^* is the cofactor matrix for A. Therefore, $c \,|\, D$. The idea behind the proof is to show that if any prime p divides D/c then p^2 divides D.

Suppose $p \,|\, D$ where p is prime. Then, the rank of A over the field $\mathbb{Z}_p$ can be at most $N - 1$. If it is exactly $N-1$ then (recall that the determinant rank equals the matrix rank), there exists a $(N-1)\times(N-1)$ sub-matrix with non-zero determinant mod p. That is, the cofactor matrix, A^*, is non-zero mod p. However, we shall show below that if $p \,|\, (D/c)$ then $A^* = 0$ over $\mathbb{Z}_p$, and this fact forces rank $A \leq N - 2$ over $\mathbb{Z}_p$. Now consider a reduction of A to triangular form using elementary row and column operations. Since the rank of A mod p is at most $N - 2$, at least two diagonal entries will be divisible by p. That is, $p^2 \,|\, D$ as required.

It remains to show that if $p \,|\, (D/c)$ then $A^* \equiv 0 \pmod{p}$.

By definition of a ring characteristic, $c \equiv 0 \pmod{(A)}$. That is, there exists an integer circulant matrix A' such that $AA' = cI$. This implies that $c^{-1}A' = A^{-1} = (\det A)^{-1}A^*$. Therefore, $(c/D)A^* \in \mathrm{CIRC}(\mathbb{Z})$ since $D = |\det A|$. We are given that $p \,|\, (D/c)$. Therefore, $A^* \in p \cdot \mathrm{CIRC}(\mathbb{Z})$. That is, $A^* \equiv 0 \pmod{p}$. □

8.3 Irreducibles

Much of the remainder of the section concerns two circulant analogues of rational primes, namely, prime ideals in an integer circulant ring and irreducible circulants. Given a ring R, $r \in R$ is said to be **irreducible** if r is not a unit and $r = xy$ implies that either x or y is a unit of R. As in the rational integers, the purpose in introducing irreducibles is to factorize ring elements. The rings of current interest are the integer circulant rings and the cyclotomic integers.

In the integers, unique factorization is enforced by requiring *(i)* that the primes be positive, and *(ii)* that the only unit allowed to appear in a prime factorization is a single -1, and then only if the integer is negative. In circulants and in cyclotomic integers, there is no such simple restriction which will eliminate redundant units in the factorization. If c is an irreducible then so is vc where v is any unit. In general, when two ring elements a and b are related by a unit v, $a = vb$, then a and b are said to be **associates**. If we have two factorizations of the same element into irreducibles, they shall be regarded as the same factorization if (possibly after rearrangement) each irreducible in one factorization is an associate of the irreducible in the other at the same position. Even with this association of factorizations, there still may not be unique factorization into irreducibles.

The next four propositions prove simple but basic facts regarding circulant irreducibles. These propositions, and others which follow, use the concept of divisibility in a commutative ring R. The idea is essentially the same as divisibility in $\mathbb{Z}$. Given $\alpha, \beta \in R$, α is said to **divide** β, written $\alpha \,|\, \beta$, if $\beta = \gamma\alpha$ for some $\gamma \in R$. Hence, $\alpha \equiv \beta \pmod{\gamma}$ means γ divides $\alpha - \beta$. In here, R will be either $\mathbf{circ}(\mathbb{Z})$ or $\mathbb{Z}(\zeta)$.

8.3.1 **Proposition** If $z \in \mathbf{circ}_N(\mathbb{Z})$ is a divisor of zero then it is reducible.

Proof. Suppose $zw = 0$ with $w \neq 0$, then $z = z(aw+1)$ for any $a \in \mathbf{circ}_N(\mathbb{Z})$. This shows that z is reducible provided $aw + 1$ is not a unit for some a. We shall show that such an a exists,

Since w is non-zero, it must have a non-zero eigenvalue, and so $\lambda_d(w) \neq 0$ for some $d \mid N$. Let $n = \mathcal{N}_{N/d}(\lambda_d(w)) \neq 0$. Then, $\lambda_d(w) \,|\, n$. Clearly, $\lambda_d(w) \in \mathbb{Z}(\zeta_{N/d})$. $\therefore \lambda_d(w)^{-1} \in \mathbb{Q}(\zeta_{N/d})$. Because $\lambda_d(w) \,|\, n$, we deduce that $n/\lambda_d(w) \in \mathbb{Z}(\zeta_{N/d})$.

Define $\beta = kn/\lambda_d(w)$ where k is an as yet unspecified integer. Then, $\beta \in \mathbb{Z}(\zeta_{N/d})$. Since $\lambda_1^{(N/d)} : \mathbf{circ}_{N/d}(\mathbb{Z}) \to \mathbb{Z}(\zeta_{N/d})$ is onto, we can pick $b \in \mathbf{circ}_{N/d}(\mathbb{Z})$ such that $\lambda_1(b) = \beta$. Again, $\Gamma_N^{N/d} : \mathbf{circ}_N \to \mathbf{circ}_{N/d}$ is onto by Proposition 3.5.6*(i)*, so we can pick $a \in \mathbf{circ}_N(\mathbb{Z})$ such that $\Gamma_N^{N/d}(a) = b$. By Proposition 3.5.2, $\lambda_d(a) = \lambda_1(b) = \beta$.

With these choices, $\lambda_d(aw) = \beta\lambda_d(w) = kn$. $\therefore \lambda_d(aw + 1) = kn + 1$. Pick k equal to the sign of n. Then, $kn + 1 \geq 2$, so $\mathcal{N}_{N/d}(\lambda_d(aw + 1)) \geq 2$. Hence, by Propositions 7.2.4 and 7.2.5, $aw + 1$ is not a unit of $\mathbf{circ}_N(\mathbb{Z})$. □

8.3.2 **Proposition** Let $a \in \mathbf{circ}_N(\mathbb{Z})$. If $\Delta(a)$ is prime then a is irreducible.

Proof. This follows from Proposition 7.2.2. □

The converse of this lemma is false. It will be shown that the scalar prime p is irreducible in $\mathbf{circ}_p(\mathbb{Z})$, whereas obviously $\Delta_p(p) = p^p$ is not prime.

8.3.3 **Proposition** Every non-singular integer circulant has a factorization into a product of irreducibles.

Proof. Let c be an arbitrary non-singular circulant. If c is irreducible, then this is its factorization. Otherwise, $c = c_1c_2$ for some non-unit circulants c_1, c_2. If c_1 is reducible, we split it into factors c_{11}, c_{12}, and likewise we split c_2 if it is reducible. We continue thus until the process stops with all factors being irreducible. The process must stop since otherwise we will get a representation of c as an infinite product of circulants whose determinants have absolute value greater than 1 which is impossible. □

Warning: The factorization is not always unique even to within units.

8.3.4 **Proposition** Let $c \in R$. Then, c is irreducible iff the ideal (c) is maximally principal.

Proof. Suppose first that c is irreducible and $(c) \subset (a)$ for some $a \in R$. Then, $c = xa$ for some x. Since c is irreducible, either x or a is a unit. If x is a unit, then $(c) = (a)$. Otherwise, if a is a unit $(a) = R$. Therefore, (c) is maximally principal.

Now suppose c is maximally principal, and that $c = xy$. Then, $c \in (x)$ and $c \in (y)$. By maximality, $(c) = (x)$ or $(x) = R$, and likewise for (y). If $c = (x)$ then c and x are associates, and y must be a unit as required. If $(x) = R$, then x is a unit. □

8.4 **Primes.** We shall reserve the term "prime" for ring elements which are not zero divisors and which generate principal prime ideals. In the ring of the integers, the three concepts of irreducible, prime, and prime ideal are equivalent: If $p \in \mathbb{Z}$ then, p is irreducible iff p is prime iff (p) is a prime ideal. It is easily shown that a circulant prime (a non-singular generator of a prime ideal) is always irreducible. However, we shall show that there are irreducible circulants which are not prime, and that there are principal prime ideals whose generators are reducible. We shall introduce such prime ideals next.

8.4.1 **Cyclotomic Circulants and Cyclotomic Ideals.** Given any $d \mid N$, let $\Phi_d(x)$ be the d^{th} cyclotomic polynomial. Call the circulant $\Phi_d(\mathrm{u})$ the $d^{\,\text{th}}$ **cyclotomic circulant**. When the context is clear, we shall abbreviate $\Phi_d(\mathrm{u})$ to Φ_d. By Proposition 3.4.5, Φ_d generates a prime ideal in $\mathbf{circ}_N(\mathbb{Z})$ since (Φ_d) is the kernel of the ring homomorphism to the integral domain, $\mathbb{Z}(\zeta_d)$. We shall call this ideal generated by $\Phi_d(\mathrm{u})$ the $d^{\,\text{th}}$ **cyclotomic ideal**. Since the cyclotomic ideals are prime and generated by divisors of zero, they provide the promised examples of principal prime ideals whose generators are reducible by Proposition 8.3.1.

8.4.2 **Lemma** A divisor of zero in $\mathbf{circ}_N(\mathbb{Q})$ is divisible by a cyclotomic circulant.

Proof. Suppose $ab = 0 \in \mathbf{circ}_N(\mathbb{Q})$ with $a, b \neq 0$. Let $a(x)$ and $b(x)$ be the representer polyomials for a and b respectively. Then, $x^N - 1 \,|\, a(x)b(x)$. Therefore $a(x)b(x)$ is divisible by all the cyclotomic polynomials $\Phi_d(x)$ where $d \,|\, N$. These polynomials are all irreducible so either they all divide $a(x)$, they all divide $b(x)$, or some divide $a(x)$ and others divide $b(x)$. The latter case leads to the desired conclusion. So, suppose w.l.o.g., $\Phi_d(x) \,|\, a(x)$ for all $d \,|\, N$. Then, $x^N - 1 \,|\, a(x)$ which implies $a = a(\mathrm{u}) = 0$ contrary to assumption. □

The lemma shows that the divisors of zero in $\mathbf{circ}_N(\mathbb{Q})$ (and also in $\mathbf{circ}_N(\mathbb{Z})$) are essentially the cyclotomic circulants. All other zero divisors are such because they are products involving these.

8.4.3 **Corollary** Let $a \in \mathbf{circ}_N(\mathbb{Q})$. $\Delta_N(a) = 0$ iff a is divisible by a cyclotomic circulant. □

The next proposition shows the relationship between the zero divisors of $\mathbf{circ}_N(\mathbb{Z})$ and its prime ideals.

8.4.4 **Proposition** The cyclotomic ideals in $\mathbf{circ}_N(\mathbb{Q})$ and $\mathbf{circ}_N(\mathbb{Z})$ are minimal prime ideals and all prime ideals of $\mathbf{circ}_N(\mathbb{Q})$ and $\mathbf{circ}_N(\mathbb{Z})$ contain a cyclotomic ideal.

Proof. First we shall prove that every prime ideal contains some cyclotomic circulant. Let $R = \mathbb{Q}$ or $\mathbb{Z}$. Any prime ideal, $K \subset \mathbf{circ}_N(R)$ is the kernel of a homomorphism $\alpha : \mathbf{circ}_N(R) \to S$ where S is an integral domain. That is, $K = \ker \alpha$. Now,

$$\prod_{d \mid N} \Phi_d \;=\; \mathrm{u}^N - 1 \;=\; 0$$

$$\therefore \;\; \prod_{d \mid N} \alpha(\Phi_d) \;=\; 0 \in S$$

Since S is an integral domain, $\alpha(\Phi_d) = 0$ for some $d \,|\, N$. Hence, $\Phi_d \in \ker \alpha = K$.

To prove minimality, let P be a prime ideal in (Φ_d), $P \subset (\Phi_d)$. By the first part, there exists $\Phi_m \in P \subset (\Phi_d)$. So, $\Phi_m = c\Phi_d$ for some $c \in \mathbf{circ}_N(R)$. Let $c(x)$ be the representer polynomial for c. Then, there exists $d(x)$ such that

$$\Phi_m(x) \;=\; c(x)\Phi_d(x) \;+\; d(x)\left(x^N - 1\right)$$

Now, $\Phi_d(x) \,|\, x^N - 1$. Therefore, $\Phi_d(x) \,|\, \Phi_m(x)$. Since the cyclotomic polynomials are irreducible, this is possible only if $d = m$. This implies $\Phi_d \in P$ which implies $P = (\Phi_d)$. □

8.4.5 **Corollary** The only proper ideals of $\mathbf{circ}_N(\mathbb{Q})$ are the principal ideals generated by products of Φ_d where $d \,|\, N$, and in particular, all prime ideals are cyclotomic.

Proof. By Corollary 8.1.7, all ideals of $\mathbf{circ}_N(\mathbb{Q})$ are principal. All non-singular rational circulants are units. Therefore, ideals of $\mathbf{circ}_N(\mathbb{Q})$ must consist of divisors of zero in $\mathbf{circ}_N(\mathbb{Q})$, and so, by Corollary 8.4.3, they must be generated by cyclotomic circulants. Since all ideals are principal, they must be generated by products of cyclotomic circulants as stated. Lastly, it follows immediately that the prime ideals are of the form (Φ_d). □

The following shows what kind of irreducibles are not primes.

8.4.6 **Proposition** If $c \in \mathbf{circ}_N(\mathbb{Z})$ is irreducible but not prime, then c is a member of a maximal ideal which is non-principal, and (c) is not properly contained by any proper principal ideal.

Proof. Let c be irreducible but not prime. Since all maximal ideals are prime, (c) is not maximal. But, by Proposition 8.3.4, it is maximally principal. Hence, (c) must be contained in a non-principal ideal, and is strictly contained in no proper principal ideal. By Corollary 8.1.8, $\mathbf{circ}_N(\mathbb{Z})$ is Noetherian, and so there must be a maximal ideal containing (c) which must therefore be a non-principal maximal ideal. □

8.4.7 **Examples** In all these examples, q is a prime number.

(i) Let $L_q := \{a \in \mathbf{circ}_N(\mathbb{Z}) \vdash q \,|\, \lambda_0(a)\}$, and let $L_1 := \{a \in \mathbf{circ}_N(\mathbb{Z}) \vdash \lambda_0(a) = 0\}$. One can easily see that L_1 and L_q are prime ideals, and indeed, they all contain the first cyclotomic circulant, $\mathrm{u} - 1$. In fact, $L_1 = (\mathrm{u} - 1)$.

(ii) Now suppose that π is prime in $\mathbb{Z}(\zeta_d)$ where $d \,|\, N$, and define $L_{\pi,d} := \{a \in \mathbf{circ}_N(\mathbb{Z}) \vdash \pi \,|\, \lambda_{N/d}(a)\}$. The ideal $L_{\pi,d}$ is obviously prime and contains Φ_d.

(iii) One might be tempted to think that (q) is a prime ideal in $\mathbf{circ}_N(\mathbb{Z})$. It is not. Because suppose it was. Then, by Proposition 8.4.4, $qa(\mathrm{u}) = \Phi_d$ for some polynomial $a(x)$ of degree less than N. Therefore, $qa(x) = \Phi_d(x)$ which is impossible for the monic polynomial $\Phi_d(x)$.

Therefore, (p) is not a prime ideal of $\mathbf{circ}_p(\mathbb{Z})$, but we shall show (Proposition 8.4.15) that p is nevertheless irreducible in $\mathbf{circ}_p(\mathbb{Z})$. This fact is easily demonstrated for $p = 2$.

8.4.8 **Proposition** 2 is irreducible in $\mathbf{circ}_2(\mathbb{Z})$.

Proof. $\lambda(2) = (2, 2)$. The only possible factorization excluding units is $\lambda(2) = (2, 2) = (2, 1)(1, 2)$. But, $\lambda^{-1}(2, 1)$ is not an integer circulant. □

Note that odd primes are reducible in $\mathbf{circ}_2(\mathbb{Z})$ thus: $2n+1 = (n+1+n\mathrm{u})(n+1-n\mathrm{u})$. Hence, to within units, 2 is the only irreducible scalar in $\mathbf{circ}_2(\mathbb{Z})$.

As a consequence of Proposition 8.4.6, it follows that $\mathbf{circ}_2(\mathbb{Z})$ must contain a non-principal ideal. We shall construct such an ideal after the next lemma, and we shall do so for general N afterwards.

8.4.9 **Lemma** Let $a, b \in \mathbf{circ}_N(\mathbb{Z})$. If a is irreducible, $b \notin (a)$, and $\gcd(\lambda_0(a), \lambda_0(b)) > 1$, then (a, b) is non-principal.

Proof. Suppose first that (a, b) is the entire circulant ring. Then, in particular, $\exists x, y \in \mathbf{circ}_N(\mathbb{Z})$ with $ax + by = 1$. Apply λ_0. $\lambda_0(a)\lambda_0(x) + \lambda_0(b)\lambda_0(y) = 1$. This is impossible if $\gcd(\lambda_0(a), \lambda_0(b)) > 1$. Therefore, (a, b) is a proper ideal of $\mathbf{circ}_N(\mathbb{Z})$.

Now suppose $(a, b) = (c)$ for some $c \in \mathbf{circ}_N(\mathbb{Z})$. Then, $a = xc$ for some $x \in \mathbf{circ}_N(\mathbb{Z})$. Since a is irreducible, either x or c is a unit. But, if c is a unit then $(a, b) = (c)$ is the entire circulant ring which was shown impossible. Therefore, x is a unit, and $(a) = (c)$. $\therefore b \in (a)$. Contradiction. □

8.4.10 **Proposition** $(2,\ 1-\mathrm{u}) \subset \mathbf{circ}_2(\mathbb{Z})$ is a non-principal ideal.

Proof. Example 8.4.7*(iii)* shows that $1 - \mathrm{u} \notin (2)$. Now apply the lemma. □

We shall now demonstrate a non-principal ideal in the general case. To do so, we need a lemma on cyclotomic integers. It expresses a rather surprising fact: p is not prime in $\mathbb{Z}(\zeta_p)$. In fact, p is a $(p-1)^{\text{th}}$ power of a prime in $\mathbb{Z}(\zeta_p)$.

8.4.11 **Lemma** Let $p \in \mathbb{Z}$ be prime and let $\zeta = \zeta_p$. Then

(i) p factorizes in $\mathbb{Z}(\zeta)$: $p = v(1-\zeta)^{p-1}$ where v is a unit of $\mathbb{Z}(\zeta)$, and

(ii) $(1-\zeta)$ is a prime ideal of $\mathbb{Z}(\zeta)$.

Proof. *(i)*

$$p = \left(\sum_{i=0}^{p-1} x^i\right)_{x=1} = \lim_{x\to 1}\left(\frac{x^p-1}{x-1}\right) = \left(\prod_{i=1}^{p-1}(x-\zeta^i)\right)_{x=1} = \prod_{i=1}^{p-1}(1-\zeta^i) \tag{1}$$

We now claim that $(1-\zeta^i) = (1-\zeta)$ for all $i \not\equiv 0 \pmod p$. Firstly, $1-\zeta^i = (1-\zeta)(1+\zeta+\zeta^2+\cdots+\zeta^{i-1})$. So, $(1-\zeta^i) \subset (1-\zeta)$. However, we can apply the same argument with $1-\zeta^i$ and $1-\zeta$ reversed since $\zeta = (\zeta^i)^j$ where j is the inverse of $i \pmod p$. Hence, $(1-\zeta^i) = (1-\zeta)$ as claimed.

Therefore, $1-\zeta^i = v_i(1-\zeta)$ for some unit v_i of $\mathbb{Z}(\zeta)$. Substituting into (1) gives the desired factorization of p. QED *(i)*

(ii) Lastly, we need to prove that $(1-\zeta)$ is prime in $\mathbb{Z}(\zeta)$. From equation (1), $\mathcal{N}_p(1-\zeta) = p$. Therefore, the quotient ring $\mathbb{Z}(\zeta)/(1-\zeta)$ has p elements and since $1-\zeta$ divides p, it must be a ring of characteristic dividing p. Since p is prime, this means it is actually the field $\mathbb{Z}_p$. Therefore, $(1-\zeta)$ is maximal and hence prime. □

8.4.12 **Proposition** Let $p \,|\, N$. The ideal $(p,\ \Phi_p)$ is non-principal in $\mathbf{circ}_N(\mathbb{Z})$.

Proof. $\lambda_0(\Phi_p) = \lambda_0(p) = p$. Therefore, all elements of (p, Φ_p) have their λ_0 eigenvalue divisible by p. So, (p, Φ_p) is a proper ideal.

Suppose $(p, \Phi_p) = (c)$ for some $c \in \mathbf{circ}_N(\mathbb{Z})$. Then, in particular, $\exists x, y \in \mathbf{circ}_N(\mathbb{Z})$ such that $xc = \Phi_p$ and $yc = p$. Since (Φ_p) is a prime ideal, $\Phi_p \,|\, x$ or $\Phi_p \,|\, c$. But, if $\Phi_p \,|\, c$ then c is a divisor of zero. Hence, so is $p = yc$. Contradiction. Therefore, $\Phi_p \,|\, x$, and $x = x_1\Phi_p$, say.

$$\therefore\ \Phi_p(x_1c - 1) = 0$$
$$\therefore\ \hat{\Phi}_p \,|\, (x_1c-1)$$

where $\hat{\Phi}_p$ is the product of all cyclotomic circulants in $\mathbf{circ}_N(\mathbb{Z})$ not equal to Φ_p.

$$\therefore\ x_1c = 1 + k\hat{\Phi}_p \quad \text{for some } k \in \mathbf{circ}_N(\mathbb{Z})$$

$$\begin{aligned}\text{Now, } \hat{\Phi}_p(x) &= (x-1)\frac{x^N-1}{x^p-1}\\ &= (x-1)\left(x^{p(m-1)} + x^{p(m-2)} + \cdots + x^p + 1\right) \quad \text{where } m = N/p.\end{aligned}$$

$$\therefore\ \lambda_i(x_1c) = \begin{cases} 1 & \text{if } m \nmid i \\ 1 + (\zeta_N^i - 1)m\kappa_i & \text{if } m \,|\, i \quad \text{where } \kappa = \lambda(k)\end{cases} \tag{2}$$

Therefore, if $i = 0$ or $m \nmid i$ then $\lambda_i(c)$ is a unit of $\mathbb{Z}(\zeta)$. Now suppose $i = m$, and let $d = \lambda_m(c)$. If d is a unit of $\mathbb{Z}(\zeta)$ then all eigenvalues of c are units and so by Proposition 7.2.5, c is a unit in $\mathbf{circ}_N(\mathbb{Z})$. Contradiction. Therefore, d cannot be a unit of $\mathbb{Z}(\zeta)$.

Now, $yc = p$. $\therefore \lambda_m(y)\lambda_m(c) = p$. $\therefore p \in (d)$. By Lemma 8.4.11, p equals a unit times $(1-\zeta_p)^{p-1}$.

$$\therefore\ (1-\zeta_p)^{p-1} \equiv 0 \pmod d$$

Equation (2) shows that d divides $1 + (\zeta_N^m - 1)m\kappa_m = 1 + (\zeta_p - 1)m\kappa_m$.

$$\therefore\ (1-\zeta_p)m\kappa_m \equiv 1 \pmod d$$
$$\therefore\ (1-\zeta_p)^{p-1}m^{p-1}\kappa_m^{p-1} \equiv 1 \pmod d$$
$$\therefore\ 0 \equiv 1 \pmod d$$
$$\therefore\ 1 \in (d). \text{ Contradiction. } \square$$

Proposition 8.4.11 can be used again to show that p is irreducible in $\mathbf{circ}_p(\mathbb{Z})$. First we need a lemma.

8.4.13 **Lemma** In a ring R, if $c \in R$ has a factorization $c = \pi_1\pi_2\cdots\pi_m$ into primes of R then it is the only factorization (to within units) of c into irreducibles.

Proof. Suppose $c = p_1p_2\cdots p_n$ where each p_i is irreducible in R. Since π_1 is prime and divides p, $p_i = v_i\pi_1$ for some i and for some $v_i \in R$. But, p_i is irreducible, so v_i must be a unit. Cancel π_1 on both sides of the factorization. This leaves

$$\prod_{i=2}^{m}\pi_i \;=\; v_i\prod_{j\neq i}p_j$$

Now apply the same argument again to deduce that $p_j = v_j\pi_2$ for some j and some unit v_j, and again cancel π_2 on both sides. Proceeding thus we will eventually cancel all factors of π_i on the left side. What remains on the right side therefore must be units. This shows that each p_j must be an associate of some π_i and vice versa. □

In particular, this lemma shows that the factorization of p in $\mathbb{Z}_\zeta$ as given by Lemma 8.4.11 is unique.

Condensed Notation for Eigenvalues. When specifying eigenvalues of rational circulants, it unnecessary to specify all the eigenvalues, merely the set $\{\lambda_d \vdash d \mid N\}$. All other eigenvalues are conjugates of this basic set and can be deduced using the formula of Lemma 7.3.5. When the circulant order is prime, the basic set is merely two values, λ_0 and λ_1. We will need to consider possible values that eigenvalues can assume, so our task will be greatly simplified if we consider only the basic set.

8.4.14 **Definition** Let $N \equiv 0 < 1 < d_1 < \cdots < d_n < N$ be the distinct divisors of N. For $a \in \mathbf{circ}_N(\mathbb{Q})$ define $\hat{\lambda} := (\lambda_0, \lambda_1, \lambda_{d_1}, \ldots, \lambda_{d_n})$.

Thus, in the case of $N = p$ prime, $\hat{\lambda} : \mathbf{circ}_p(\mathbb{Z}) \to \mathbb{Z}\oplus\mathbb{Z}_\zeta$ and is given by $\hat{\lambda}(a) := (\lambda_0(a), \lambda_1(a))$.

8.4.15 **Proposition** If p is prime then it is irreducible in $\mathbf{circ}_p(\mathbb{Z})$.

Proof. Suppose a factorization of p in $\mathbf{circ}_p(\mathbb{Z})$ yields the factorization $\hat{\lambda}(p) = (\sigma p,\ \xi)(\sigma,\ \xi^{-1}p)$ where $\sigma = \pm 1$ and ξ is a unit of $\mathbb{Z}_\zeta$. Applying Proposition 7.2.9 to the first factor shows that $\ell_p(\xi) = 0$. But this is impossible for a unit. By Lemma 8.4.11*(ii)* and the previous lemma, the only possible factorizations of p remaining are ones that yield

$$\hat{\lambda}(p) \;=\; (\sigma p,\ \xi(1-\zeta)^s)\left(\sigma,\ \xi^{-1}(1-\zeta)^{p-s-1}\right)$$

where again $\sigma = \pm 1$ and ξ is a unit of $\mathbb{Z}_\zeta$. Looking at the second factor, se see that $\ell_p(1-\zeta)^{p-s-1} = 0$ unless $s = p-1$ whereas $\ell_p(\sigma) = \sigma \neq 0$. Therefore, $s = p-1$.

$$\therefore\ \hat{\lambda}(p) \;=\; (\sigma p,\ \xi p)\left(\sigma,\ \xi^{-1}\right)$$

But, $\hat{\lambda}^{-1}(\sigma, \xi^{-1})$ is a circulant unit. □

This proposition raises the question of what are the irreducible elements of $\mathbf{circ}_N(\mathbb{Z})$. We shall restrict the discussion to $N = p$ prime for simplicity.

8.4.16 **Lemma** Given any $r \in \mathbb{Z}_p^*$ there exists a unit $\xi \in \mathbb{Z}(\zeta_p)$ with $\ell_p(\xi) = r$.

Proof. One such unit is

$$\chi_r \;=\; \frac{1-\zeta^r}{1-\zeta} \;=\; 1+\zeta+\zeta^2+\cdots+\zeta^{r-1}$$

To show that this is a unit, we shall construct its inverse. Let $\bar{r}$ be the inverse of r in $\mathbb{Z}_p$, and let

$$\bar{\chi}_r \;=\; \frac{1-\zeta^{r\bar{r}}}{1-\zeta^r} \;=\; 1+\zeta^r+\cdots+\zeta^{r(\bar{r}-1)}$$

Now, $r\bar{r} \equiv 1 \pmod{p}$, so $\zeta^{r\bar{r}} = 1$. Therefore,

$$\chi_r \bar{\chi}_r \;=\; \frac{1-\zeta^r}{1-\zeta}\,\frac{1-\zeta^{\bar{r}r}}{1-\zeta^r} \;=\; 1 \;\square$$

8.5 **Factorizations.** Let $c \in \mathbf{circ}_p(\mathbb{Z})$ and suppose that $\hat{\lambda}(c) = (n_1 n_2,\ \alpha_1\alpha_2)$ where $n_1, n_2 \in \mathbb{Z}$ and $\alpha_1, \alpha_2 \in \mathbb{Z}_\zeta$. (Reminder: $\hat{\lambda}$ is the eigenvalue condensed notation.) Consider the possible factorizations of $\hat{\lambda}(c)$ into factors which involve only $n_1, n_2, \alpha_1, \alpha_2$, the units, $\sigma, \sigma_1 = \pm 1$, and $\xi, \xi_1 \in \mathbf{U}(\mathbb{Z}_\zeta)$. The factorizations are:

$$\begin{aligned}
\hat{\lambda}(c) &= (\sigma n_1 n_2,\ \xi)(\sigma,\ \xi^{-1}\alpha_1\alpha_2) && \textit{(i)}\\
&= (\sigma n_1,\ \xi\alpha_1)(\sigma n_2,\ \xi^{-1}\alpha_2) && \textit{(ii)}\\
&= (\sigma n_1,\ \xi\alpha_2)(\sigma n_2,\ \xi^{-1}\alpha_1) && \textit{(iii)}
\end{aligned}$$

Factorization *(i)* is valid iff $\ell_p(\xi) = \sigma n_1 n_2 \bmod p$ iff $\ell_p(\xi)^{-1}\ell_p(\alpha_1)\ell_p(\alpha_2) = \sigma$. There are similar conditions for the other factorizations. Lemma 8.4.16 shows that we can always pick the unit ξ to satisfy any of these conditions provided no factor has a component whose ℓ_p value is zero but whose other component has non-zero ℓ_p value. For the moment, we shall assume that $\ell_p(n_1 n_2)$ is non-zero, so that all components of all factors have non-zero ℓ_p value.

In this case, all of the above factors factorize again

$$\begin{aligned}
(\sigma n_1 n_2,\ \xi) &= (\sigma\sigma_1 n_1,\ \xi_1)(\sigma_1 n_2,\ \xi_1^{-1}\xi)\\
(\sigma,\ \xi^{-1}\alpha_1\alpha_2) &= (\sigma\sigma_1,\ \xi_1\xi^{-1}\alpha_1)(\sigma,\ \xi_1^{-1}\alpha_2)\\
(\sigma n_1,\ \xi\alpha_1) &= (\sigma\sigma_1 n_1,\ \xi\xi_1)(\sigma_1,\ \xi_1^{-1}\alpha_1)
\end{aligned}$$

and similarly for the other factors of *(ii)* and *(iii)*.

Hence we see that all factorizations terminate in factors of the form (q, ξ) or (σ, π) where q is prime in $\mathbb{Z}$, and π is prime in $\mathbb{Z}_\zeta$. Furthermore, it does not matter how the factorization proceeds -- via *(i)*, *(ii)*, or *(iii)* --it will always end with these same end factors to within units. For instance, suppose $q \equiv \ell_p(\xi)$ where $\xi \in \mathbf{U}(\mathbb{Z}_\zeta))$, then $\xi = \eta\xi_q$ where $\eta = \xi\xi_q^{-1} \in \mathbf{U}(\mathbb{Z}_\zeta)$, and $(q, \xi) = (q, \xi_q)(1, \eta)$. The latter factor is a circulant unit because $\eta^{-1} \in \mathbb{Z}_\zeta$ and $\ell_p(\eta) = \ell_p(\xi)\ell_p(\xi_q)^{-1} = 1 = \ell_p(\eta^{-1})$.

Hence, factorization is unique provided $\lambda_0(c)$ is not divisible by p, and provided factorization is unique in $\mathbb{Z}$, which it is, and in $\mathbb{Z}_\zeta$ which it is for $p < 23$ (but not for $p = 23$).

8.5.1 **Non-unique Factorization in $\mathbf{circ}_p(\mathbb{Z})$.** Factorization is not unique in any $\mathbf{circ}_p(\mathbb{Z})$. For consider the circulant $c = (1-\mathrm{u})^3 + p^2\Phi_p$

$$\begin{aligned}
\hat{\lambda}(c) &= \left(p^3,\ (1-\zeta)^3\right)\\
&= \left(p^2,\ 1-\zeta\right)\left(p,\ (1-\zeta)^2\right) && \text{(irreducible factors)}\\
&= \left(p,\ 1-\zeta\right)^3 && \text{(irreducible factors)}
\end{aligned}$$

The factor $(p^2,\ 1-\zeta)$ cannot be factored because the second component can only be factored into a unit and an associate of $1-\zeta$, and the unit can only accompany a unit in the first component

So even if unique factorization holds in $\mathbb{Z}_\zeta$ unique factorization in $\mathbf{circ}_p(\mathbb{Z})$ holds only for circulants with λ_0 not divisible by p. Suppose $\hat{\lambda}(c) = (n_1 n_2,\ \alpha_1\alpha_2)$ where $n_1 \equiv 0$, $n_2 \not\equiv 0 \pmod{p}$, $\ell_p(\alpha_1) = 0$, and $\ell_p(\alpha_2) \neq 0$. Now, $\ell_p(\alpha_1) = 0$ implies that $p \,|\, \mathcal{N}(\alpha_1)$, and so $1-\zeta \,|\, \mathcal{N}(\alpha_1)$. Since all conjugates of $1-\zeta$ are associates of it, it follows that $1-\zeta \mid \alpha_1$. By the method of §8.5, we can extricate all components whose norms are not divisible by p leaving a circulant c_1 with $\hat{\lambda}(c) = (p^r,\ (1-\zeta)^s)$ for some $r, s > 0$.

Sections 8.5 and 8.5.1 has demonstrated the following.

8.5.2 **Theorem** Let $\zeta = \zeta_p$ where p is prime.

(i) The irreducible elements of $\mathbf{circ}_p(\mathbb{Z})$ are

$$\begin{aligned}\theta_q &:= \hat{\lambda}^{-1}(q,\ \xi_q),\\ \tilde{\theta}_\pi &:= \hat{\lambda}^{-1}(1,\ \xi_\pi \pi),\\ \rho_n &:= \hat{\lambda}^{-1}\left(p^n,\ 1-\zeta\right),\\ \bar{\rho}_n &:= \hat{\lambda}^{-1}(p,\ (1-\zeta)^n)\end{aligned}$$

where $q \neq p$ is a rational prime, π is irreducible in $\mathbb{Z}_\zeta$, $\pi \notin (1-\zeta)$, and $\xi_q, \xi_\pi \in \mathbf{U}(\mathbb{Z}_\zeta)$ with $\ell_p(\xi_q) = q \bmod p$, and $\ell_p(\xi_\pi) = \ell_p(\pi)^{-1}$.

(ii) If $\mathbb{Z}_\zeta$ has unique factorization, then $c \in \mathrm{GL} \cap \mathbf{circ}_p(\mathbb{Z})$ can be uniquely factorized (to within units) into the form $\xi P_{r,s} t_1 t_2 \cdots t_n$ where $P_{r,s} = (p^r,\ (1-\zeta)^s)$, $\xi \in \mathbf{U}(\mathbb{Z}_\zeta)$, and t_i are irreducibles with $\lambda_0(t_i) \not\equiv 0 \pmod{p}$. □

8.5.3 **Proposition** The primes in $\mathbf{circ}_p(\mathbb{Z})$ are associates of irreducibles of the types θ_q or $\tilde{\theta}_\pi$.

Proof. Consider first an irreducible of the type θ_q. We claim that $(\theta_q) = L_q$ where L_q is the prime ideal of Example 8.4.7 *(i)*. Trivially, $(\theta_q) \subset L_q$. Suppose $x \in L_q$. Then, $\hat{\lambda}(x) = (nq, \alpha)$. If x is non-singular then (nq, α) can be factorized into (q, ξ) and other factors, and hence $x \in (\theta_q)$. Otherwise, if x is a divisor of zero, then $x = x_1(1-\mathrm{u})$ or $x = x_1\phi_p$. Since $\phi_p \notin L_q$, and since L_q is a prime ideal, we can assume w.l.o.g. that $x = x_1(1-\mathrm{u})$. RTP: $1-\mathrm{u} \in (\theta_q)$. Now, $\hat{\lambda}(1-\mathrm{u}) = (0,\ 1-\zeta) = \left(0,\ \xi_q^{-1}(1-\zeta)\right)(q,\ \xi_q)$. QED Claim.

We can similarly prove that if π is prime in $\mathbb{Z}_\zeta$ then $\tilde{\theta}_\pi$ generates the ideal $L_{\pi,p}$ of Example 8.4.7*(ii)* and this is a prime ideal. In this case, $1-\mathrm{u} \notin L_{\pi,p}$, and $\Phi_p \in L_{\pi,p}$, and we get $\hat{\lambda}(\Phi_p) = (p,0) = (p,0)(1, \xi_\pi \pi) \in (\tilde{\theta}_\pi)$. □

8.5.4 **Proposition** The primes of $\mathbf{circ}_p(\mathbb{Z})$ generate maximal ideals.

Proof. Since $L_q = (\theta_q)$, and $|\Delta(\theta_q)| = q$, a prime, by Corollary 8.2.3, the quotient ring $\mathbf{circ}_p(\mathbb{Z})/(\theta_q)$ is isomorphic to the field $\mathbb{Z}_q$.

In the case of $L_{\pi,p} = (\tilde{\theta}_\pi)$, we must proceed differently since $\mathcal{N}(\pi)$, and hence $\left|\det(\tilde{\theta}_\pi)\right|$, is not necessarily prime. (It might be a prime power.) All prime ideals of algebraic extensions of the rationals are maximal (see [Kap3]). Therefore, λ_1 maps $L_{\pi,p}$ to a maximal ideal. Therefore, $\lambda_1^{-1}(L_{\pi,p})$ is maximal in $\mathbf{circ}_p(\mathbb{Z})$. Now, $\lambda_1^{-1}(L_{\pi,p}) = (\tilde{\theta}_\pi, \Phi_p)$. But, as was shown in the proof of Proposition 8.5.3, $\Phi_p \in L_{\pi,p}$. Therefore, $L_{\pi,p} = (\tilde{\theta}_\pi, \Phi_p)$ which is maximal. □

8.5.5 **Corollary** Elements of non-principal ideals in $\mathbf{circ}_p(\mathbb{Z})$ are not prime.

Proof. If a non-principal ideal contained a prime, it would contain the maximal ideal generated by the prime. Contradiction. □

It follows from this corollary that if there is unique factorization in $\mathbb{Z}_\zeta$ then all non-principal ideals are contained in the prime ideal L_p. This ideal contains p which is irreducible but not prime. Hence, by Proposition 8.4.6, L_p is non-principal. In fact, $L_p = (\Phi_p, 1-\mathrm{u})$. The quotient ring $\mathbf{circ}_p(\mathbb{Z})/L_p$ can easily be seen isomorphic to $\mathbb{Z}_p$. Hence, L_p is maximal.

We shall return in the next section to the problem of finding the unit circulant group. So we shall end this section with an application of some of the foregoing ideal theory to this quest.

8.5.6 **Proposition** Suppose that c is irreducible in $\mathbf{circ}_N(\mathbb{Z})$, and let $C(x)$ be its representer polynomial. For any $k(x) \in \mathbb{Z}[x]$, let $P(x) = C(x) + k(x)(x^N - 1)$. Then, $P(x) = V(x)Q(x)$ where $V(\mathrm{u})$ is a unit of $\mathbf{circ}_N(\mathbb{Z})$, and $Q(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. Let $P(x) = Q_1(x)Q_2(x)\cdots Q_n(x)$ be the prime factorization of $P(x)$ in $\mathbb{Z}[x]$. By the irreducibility of $P(\mathrm{u}) = C(\mathrm{u}) = c$, we must have that $Q_i(\mathrm{u})$ is a unit for all i but one, $i = 1$, say. Setting $V(x) = Q_2(x)Q_3(x)\cdots Q_n(x)$, and $Q(x) = Q_1(x)$ gives the desired conclusion. □

Although the proposition is simple to prove, it has distinctly non-trivial consequences. For instance, by picking an irreducible circulant with a non-zero scalar term, and by varying $k(x)$, one gets either an irreducible polynomial, or better, an irreducible polynomial and a non-trivial unit in $\mathbf{circ}_{N}(\mathbb{Z})$.

8.5.7 **Example.** Take $N = 5$ with the irreducible element θ_q, and for simplicity, take $q \equiv 1 \pmod 5$. Then, $\theta_q = 1 + (q-1)\bar{\delta}^5$. Taking the smallest such, $q = 11$, and a simple polynomial for $k(x) = x+1$, we get

$$\begin{aligned} P(x) &= (x+1)(x^5-1) + 2x^4 + 2x^3 + 2x^2 + 2x + 2 + 1 \\ &= x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 + x + 2 \end{aligned}$$

One can quickly verify that $-\omega$ is a root of $P(x)$ where ω is as usual the third root of unity. Hence, the 6^{th} primitive roots of unity are roots of $P(x)$, and so $x^2 - x + 1$ must divide $P(x)$. In fact,

$$P(x) = (x^2 - x + 1)(x^4 + 2x^3 + 3x^2 + 3x + 2)$$

It turns out that $V(x)$ is the first factor. That is, $v = V(\mathrm{u}) = 1 - \mathrm{u} + \mathrm{u}^2$ is a unit of $\mathbf{circ}_5(\mathbb{Z})$. This is clearly a non-trivial unit, so, by Proposition 7.3.10, we have shown that $\mathbf{U}(\mathbf{circ}_5(\mathbb{Z}))$ is infinite. From the unit v, others can be derived through multiplications by the trivial units and applications of the ν_h endomorphisms. For instance,

$$w := \nu_2(\mathrm{u}^4 V(\mathrm{u})) = -1 + \mathrm{u}^2 + \mathrm{u}^3$$

We have $\lambda_1(-1 + \mathrm{u}^2 + \mathrm{u}^3) = -\zeta^4(1+\zeta)^2$ which is a product of Kummer's cyclotomic units.

Chapter 9.
Application: Diffusion in Toroidal Spaces.

9.1 **Diffusion of Matter.** Imagine a density of matter in a space, T. Let the density function at time t be $f_t(x)$. Let the quantity of matter in the neighborhood of y moved to a neighborhood of x of equal volume in a small time interval t to $t+h$ be $a_{t,h}(x, y, f_t(y))$. Then the equation for the diffusion in the small time interval t to $t+h$ is

$$f_{t+h}(x) \;=\; \int_T a_{t,h}\left(x, y, f_t(y)\right) dy$$

We shall now make various simplifying assumptions. The first three are crucial and cannot be relaxed.

9.1.1 **The diffusion is linear.**
That is, the quantity of matter in the neighborhood of y moved to a neighborhood of x of equal volume in a small time interval t to $t+h$ is proportional to the density of matter at y at time t.

$$\therefore \;\; a_{t,h}\left(x, y, f_t(y)\right) = a_{t,h}(x, y) f_t(y)$$

9.1.2 **The diffusion is homogenous in space.**
This means that the quantity of matter moved from y to x depends only on the relative positions of x and y.

$$\therefore \;\; a_{t,h}(x, y) = a_{t,h}(x - y)$$

9.1.3 **The diffusion is homogenous in time.**
That is, the diffusion law does not vary with time. Combined with spatial homogeneity of 9.1.2, this implies

$$a_{t,h}(x - y) = a_h(x - y)$$

9.1.4 **Discrete Approximation** If the space is continuous then all distributions of interest and the diffusion law can be approximated as closely as desired with a discrete space and diffusion law.

9.1.5 **The diffusion is non-negative.** That is, if the distribution is initially non-negative then it remains non-negative for all later times. This can be guaranteed only by making the diffusion function non-negative everywhere (and by homogeneity in time, for all times).

$$\therefore \;\; a_h(x - y) \geq 0, \qquad \forall h, x, y$$

9.1.6 **Conservation of Matter**
Conservation means that $\int_T f_t(x)dx$ is constant in time. This is guaranteed if

$$\int_t a_h(y)dy = 1$$

These assumptions simplify the diffusion equation to

$$f_{t+h}(x) \;=\; \int_T a_h(x - y) f_t(y) dy$$
$$\text{with} \quad \int_T a_h(y)dy = 1$$
$$\text{and } a_h(y) \geq 0, \qquad \forall y \in T$$

9.2 **Transitions Between States.**

Another physical system that often satisfies the above assumptions is a collection of transitions between the various states of a system. The distribution now represents a probability density and the $a(x, y)$ represents the transition probability from the state y to the state x. This system automatically satisfies the assumptions 9.1.5 and 9.1.6, and it will satisfy 9.1.1 in a classical system containing only a single particle. Many such systems are inherently discrete and therefore also satisfy assumption 9.1.4.

9.3 **Circulant Matrix Model** An important question is whether any initial distribution eventually becomes equidistributed throughout the space. The special case when the space, T, is toroidal can be treated with circulant matrices. We shall first concentrate on the one-dimensional torus, the circle.

If the space is continuous then we take sufficient points in the space to approximate the continuous distributions and diffusion law. Then, with N points in the space, at the $(n+1)^{\text{th}}$ time step,

$$f_{n+1}(i) \;=\; \sum_{j\in\mathbb{Z}_N} a(i-j)f_n(j) \quad \text{where} \sum_{j\in\mathbb{Z}_N} a(j) = 1$$

Hence, the diffusion is given by multiplying the vector of densities by the circulant matrix $A_{i,j} = a(i-j)$. Normally, we shall represent the diffusion matrix by $a \in \mathbf{circ}_N(\mathbb{R})$ rather than the matrix itself. We shall need to use the matrix only when discussing its effect on the distribution vector, $f \in \mathbb{R}^N$.

Eventual equidistribution now depends on whether

$$A^r f \to f_{eq} \;:=\; (\bar{f}, \bar{f}, \ldots, \bar{f}) \quad \text{as } r \to \infty$$

$$\text{where } \bar{f} \;=\; \text{average value of } f_i \;=\; \frac{1}{N}\left(\sum_i f_i\right)$$

Since the term "eventual equidistribution" refers to a limit on vectors, we need to specify a metric on vectors. We shall adopt the dot inner-product norm since this makes the standard basis orthonormal. The dot inner-product will be written as $x.y$. Recall that the standard basis for the eigenspace is $\{e_i, \vdash i \in \mathbb{Z}_N\}$ which are the orthonormal eigenvectors of the circulant matrices.

In this section, the circulant matrix A is assumed conservative; that it satisfies §9.1.6. Hence, $\lambda_0(A) = 1$.

9.3.1 **Proposition** $A^r f$ approaches equidistribution iff $|\lambda_i(A)| < 1$ whenever $i > 0$ and $e_i.f \neq 0$.

Proof. First suppose that $|\lambda_i(A)| < 1$ whenever $i > 0$ and $e_i.f \neq 0$.

Let $f = \sum_{i\in\mathbb{Z}_N} f'_i e_i$, then $A^r f \;=\; \sum_{i\in\mathbb{Z}_N} \lambda_i^r f'_i e_i$. The stated conditions imply that

$$A^r f \;\to\; \lambda_0^r f'_0 e_0 \;=\; f'_0 e_0 \;\text{ as }\; r \to \infty \tag{1}$$

The eigenvectors $e_0, e_1, \ldots, e_{N-1}$ are an orthonormal set, and $e_0 = \sqrt{N^{-1}}(1, 1, \ldots, 1)$. Therefore, $f'_0 \;=\; f.e_0 \;=\; \frac{1}{\sqrt{N}} \sum_{i\in\mathbb{Z}_N} f_i$.

Hence, $A^r f$ approaches the vector $f_{eq} \;:=\; f'_0 e_0 \;=\; \frac{1}{N}\left(\sum_i f_i\right)(1, 1, \ldots, 1)$. This vector clearly represents an equidistribution. Note that the equidistributed vector, $f_{eq} = \lambda_0(f)\bar{\delta}^N$ where $\bar{\delta}^N$ is the idempotent of §3.5.

Conversely, suppose that $A^r f$ approaches equidistribution. This means that $A^r f \to f_{eq}$ as $r \to \infty$. But, f_{eq} is in the subspace spanned by e_0. Therefore, all components of f orthogonal to this subspace must tend to zero as $r \to \infty$. By equation (1), this is possible only if $\lambda_i^r f'_i \to 0$ which means either $f'_i = 0$ or $|\lambda_i| < 1$. □

The distribution will also approach equidistribution, regardless of the initial distribution, if A^r approaches the matrix O where $O_{i,j} = 1/N,\ \forall i,j$ as $r \to \infty$. If $A = \mathrm{CIRC}_N(a)$, then this is equivalent to $a^r \to \bar{\delta}^N$. We shall now investigate this possibility. We shall say that a is eventually an equidistribution circulant (or operator) if $a^r \to \bar{\delta}^N$ as $r \to \infty$. We shall make one simplifying assumption, namely the condition of 9.1.5 that the diffusion is non-negative: $a_i \geq 0$ for all i.

9.3.2 **Definition** To avoid continually repeating the conditions on a, we shall say that $a \in \mathbf{circ}_N(\mathbb{R})$ is **standard** iff $\sum_j a_j = 1$ and $a_i \geq 0,\ \forall i$. If $a_i > 0,\ \forall i$ then we shall say that a is **standard positive**.

9.3.3 **Definition** For all $c \in \mathbb{R}^N$, let $M(c) := \max_i |c_i|$ and let $m(c) := \min_i |c_i|$.
Of course, as sets, $\mathbf{circ}_N(\mathbb{R}) = \mathbb{R}^N$. So, this definition applies to $c \in \mathbf{circ}_N(\mathbb{R})$.

9.3.4 **Lemma** Let $a, b \in \mathbf{circ}_N(\mathbb{R})$ with a standard. Then, $M(ab) \leq M(b)$ and $m(ab) \geq m(b)$.

Proof. $|(ab)_i| = \left|\sum_{j\in\mathbb{Z}_N} a_j b_{i-j}\right| \leq \sum_{j\in\mathbb{Z}_N} a_j M(b) = M(b)$, and similarly, $|(ab)_i| \geq m(b)$. □

If we regard $M(a) - m(a)$ as a measure of deviation of a from $\bar{\delta}$ then, by setting $b = a^r$ in the lemma, we see that a^r can never deviate further from $\bar{\delta}$ as r increases. The following proposition gives sufficient conditions to ensure that $a^r \to \bar{\delta}$. First, we need to determine when $M(ab) - m(ab)$ is strictly less that $M(b) - m(b)$.

9.3.5 **Lemma** Let $a, b \in \mathbf{circ}_N(\mathbb{R})$. If a is standard positive then

$$M(ab) - m(ab) \ \leq\ (M(b) - m(b))\,(1 - 2m(a))$$

Proof. It is easy to see that $(a^r)_i > 0,\ \forall i \ \Rightarrow\ (a^{r+1})_i > 0$.
Let $c \in \mathbb{R}^N$, let $M(c) = c_g$ and let $m(c) = c_s$ for $g, s \in \mathbb{Z}_N$. Consider the inner-product $a.c$.

$$a.c \ =\ \sum_i a_i(c_i - c_g) + c_g \sum_i a_i \ =\ c_g - \sum_i a_i(c_g - c_i)$$

$$\text{Similarly, } a.c \ =\ c_s + \sum_i a_i(c_i - c_s)$$

Let $G = \{i \in \mathbb{Z}_N \vdash c_i = c_g\}$, and $S = \{i \in \mathbb{Z}_N \vdash c_i = c_s\}$. The components of c achieve their maximum absolute value on G and their minimum absolute value on S.

$$\begin{aligned} a.c \ &=\ c_g - \sum_{i\in\mathbb{Z}_N - G} a_i(c_g - c_i) \\ &=\ c_s + \sum_{i\in\mathbb{Z}_N - S} a_i(c_i - c_s) \end{aligned}$$

If $G \cap S \neq \emptyset$ then $G = S = \mathbb{Z}_N$ and there is nothing to prove. So assume that $G \cap S = \emptyset$. By well-ordering, $G, S \neq \emptyset$. In particular, $s \in \mathbb{Z}_N - G$ and $g \in \mathbb{Z}_N - S$. Therefore,

$$\begin{aligned} a.c \ &\leq\ c_g - m(a)(c_g - c_s) \\ a.c \ &\geq\ c_s + m(a)(c_g - c_s) \end{aligned} \tag{2}$$

Now let $b \in \mathbf{circ}_N(\mathbb{R})$ and set $c_j = b_{i-j}$ for some i. Then, $a.c = (ab)_i$. The inequalities (2) together imply that

$$M(ab) - m(ab) \ \leq\ (M(b) - m(b))\,(1 - 2m(a)) \quad \square$$

9.3.6 **Proposition** Let $a \in \mathbf{circ}_N(\mathbb{R})$. $\exists n > 0$ s.t. a^n is standard positive iff a^{n+i} is standard positive for all $i \geq 0$ iff $\lim_{r\to\infty} a^r = \bar{\delta}^N$.

Proof. That a^n standard positive implies that a^{n+i} is standard positive for all $i \geq 0$ follows easily from Lemma 9.3.4. Its converse is trivial.

So we can complete the proof by demonstrating the equivalence a^n standard positive iff $\lim_{r\to\infty} a^r = \bar{\delta}^N$.

Suppose a^n is standard positive. In the Lemma 9.3.5, setting $a \to a^n$ and $b \to a^r$, we see that $M(a^n a^r) - m(a^n a^r)$ decreases at least geometrically toward zero. Hence, the maximum and minimum components of a^{n+r} converge to a common limit. Since $\lambda_0(a) = 1$, we must have $\lim_{r\to\infty} a = \bar{\delta}^N$.

Conversely, if $\lim_{r\to\infty} a = \bar{\delta}^N$ then by convergence, a must be standard positive for all $r > n$ for some n. □

Proposition 9.3.6 reduces the question of whether a^r approaches the equidistribution operator to the question of whether a^r eventually becomes a standard positive circulant.

A little physical insight will guide us as to how to proceed. Consider the physical meaning of a diffusion law such as

$$a \;=\; a_{-1}\mathrm{u}^{N-1} + a_0 + a_1\mathrm{u}$$

A density of 1 initially at the point x will in the next instant be distributed among the three points $x-1$, x, and $x+1$. At the third instant, it will be distributed at $x-2$, $x-1$, x, $x+1$, and $x+2$. It is clearly spreading out. Intuitively, it seems that if the diffusion law is local and approximately continuous, that a delta-function distribution will eventually become uniformly distributed. Now suppose that the diffusion contains some other terms as well as local diffusion terms. In other words,

$$a \;=\; a_{-1}u^{N-1} + a_0 + a_1u + \text{ other terms}$$

The points in the space which receive matter due to the initial terms in the diffusion will still to do so because of linearity and non-negativity of the diffusion. That is, additional non-negative terms can only increase the number of points which have non-zero densities at a later time instant.

9.3.7 **Lemma** Let $a = a_0 + a_s\mathrm{u}^s \in \mathbf{circ}_N(\mathbb{R})$ be standard with $a_0, a_s > 0$. Then
$\exists R > 0$ s.t. a^r is standard positive for all $r > R$ iff $\gcd(s, N) = 1$.

Proof. Let $\nu = \nu_{\bar{s}}$ where $\bar{s}s \equiv 1 \pmod N$ be the position multiplier homomorphism of §3.12. Then $\nu(a) = a_0 + a_s\mathrm{u}$.

$$\therefore\ \nu(a)^r \;=\; \sum_{i=0}^{r} \binom{r}{i} a_0^{r-i} a_s^{is} \mathrm{u}^i$$

Therefore, when $r \geq N$, all components of $\nu(a)^r$ will be non-zero. Applying ν^{-1} will only derange the components, therefore, all the components of a^r must also be non-zero.

Contrariwise, if $\gcd(s, N) = d > 1$ then a^r can only contain powers of u divisible by d. □

From this lemma and the discussion that preceded it, we deduce:

9.3.8 **Proposition** Let $a \in \mathbf{circ}_N(\mathbb{R})$ be standard. If a contains at least two non-zero components, a_i and a_j, say, such that $\gcd(i - j, N) = 1$ then a^N is standard positive and $\lim_{r\to\infty} a^r = \bar{\delta}^N$. □

9.3.9 **Corollary** Let $a \in \mathbf{circ}_N(\mathbb{R})$ be standard. If a contains at least two non-zero components, a_i and a_j, say, such that $\gcd(i - j, N) = 1$ then $|\lambda_i| < 1, \quad \forall i > 0$.

Proof. Use the above proposition to deduce that $A^r f$ approaches equidistribution for any f, and then use Proposition 9.3.1 with a generic vector f to deduce $\lambda_i < 1$ for $i > 0$. □

The proposition shows that if the circulant a has any two non-zero terms whose subscript difference is coprime to N, then a is eventually an equidistribution operator. What happens if all non-zero terms are separated at even intervals? For instance, suppose a_i is non-zero only for $i \equiv f \pmod{m}$ for some $f \in \mathbb{Z}_m$ and some $m \,|\, N$. Let $N = mn$, then we suppose that

$$a \;=\; \sum_{i=0}^{n-1} x_i \mathrm{u}_{mn}^{f+im} \qquad \text{for some } x_0, x_1, \ldots, x_{n-1} \geq 0$$

Intuitively, one would expect that the circulants a^r would tend to a circulant whose non-zero components were also evenly spaced, and that the non-zero values would be equidistributed among these components. This is so and will be proved in the next section.

The question remains of what happens to a^r when the non-zero components of a are not evenly spaced and yet no two subscripts of non-zero terms are separated by an interval coprime to N. As an example of such a circulant, take $a = 1 + \mathrm{u}^3 + \mathrm{u}^7$ with $N = 84$. A crude solution to this problem is to always to take a prime number of points in the space. This guarantees that a^r becomes an equidistribution operator if and only if a has two or more non-zero components. But this solution is often unavailable. The space might be inherently discrete and so the number of points would not be discretionary, or, as will be seen in section 9.5, approximations to higher dimensional torï demand a compound number of points in the space. These considerations call for a general answer to the question of the eventual form of a^r as $r \to \infty$.

9.4 **Boolean Circulants.** For $a \in \mathbf{circ}_N(\mathbb{R})$ standard, the question of whether a^r tends to $\bar{\delta}^N$ has been reduced to the question of whether a^r ultimately contains all positive components. The actual values of the components are irrevelant, only whether they are zero or not. So it is natural to define a Boolean function H on the non-negative reals by $H(x) = 0$ if $x = 0$ and $H(x) = 1$ otherwise; then extend H to a map on circulant vectors by $H(a) = (H(a_0), H(a_1), \ldots, H(a_{N-1}))$. Similarly, we can define H on real circulant matrices by $H(\mathrm{CIRC}_N(a)) := \mathrm{CIRC}_N(H(a))$. The circulant map H maps $\mathbf{circ}_N(\mathbb{R})$ to $\mathbf{circ}_N(\{0,1\})$. The base "ring" in the range of this map is the set $\{0,1\}$ and is not a ring. It is instead the set of logical truth values with the Boolean operations of disjunction '$\wedge$' and conjunction '$\vee$'. $H(a_i) = 1$ means that "$a_i > 0$ is true". $H(a_i) = 0$ means that "$a_i > 0$ is false" (and hence $a_i = 0$ because a is assumed standard throughout).

The matrices $H(\mathrm{CIRC}_N(\mathbb{R}))$ are examples of **Boolean circulant matrices**, and $H(\mathbf{circ}_N(\mathbb{R}))$ are **Boolean circulant vectors**. In here, we shall need only a few of the simpler properties of Boolean circulants. The interested reader may consult the article by Brink & Pretorius [BaP] for more details.

The operations of Boolean circulants are the same as those of circulants over rings except that the scalar operations are different. The scalar addition is conjunction whose rules are: $0 \vee x = x \vee 0 = x$, $x \vee x = x$ (which is why it is not ring addition). The scalar multiplication is disjunction whose rules are: $0 \wedge x = x \wedge 0 = 0$, $x \wedge x = x$. These rules give the rules for Boolean circulant operations. There is another way to picture the result of circulant operations on Boolean circulants. Regard the Boolean circulants as real circulants, perform the circulant operations as if on real circulants with real arithmetic, and apply the H function. In other words,

$$H(a) \wedge H(b) \;=\; H(ab), \quad \text{and} \quad H(a) \vee H(b) \;=\; H(a+b), \qquad \forall \text{ standard } a, b \in \mathbf{circ}_N(\mathbb{R})$$

Thus, we can investigate the question of whether all the circulant components in a^n become positive for some n by looking at the evolution of the Boolean circulant $H(a^n) = H(a)^{\wedge n}$ (disjunction n times).

Temporarily regard the Boolean circulants as just abstract vectors of zeroes and ones with Boolean operations. We can regard these vectors as representing subsets of $\mathbb{Z}_N$ as follows. The subset corresponding to the Boolean vector v is defined to be the subscripts of all the non-zero components of v. Formally, the correspondence is given by: $\varsigma : v \mapsto \{i \in \mathbb{Z}_N \;\vdash\; v_i = 1\}$. This is clearly a two-way correspondence: Given $A \subset \mathbb{Z}_N$, we can construct $v = \varsigma^{-1}(A)$ by setting $v_i = 1$ for all $i \in A$ and all other components to zero. Hence, ς is a bijection,

$$\varsigma : \mathbf{circ}_N(\{0,1\}) \to 2^{\mathbb{Z}_N}$$

What operation on the power set $2^{\mathbb{Z}_N}$ corresponds to the disjunction of circulants in $\mathbf{circ}_N(\{0,1\})$?

To answer this question, let $a, b \in \mathbf{circ}_N(\{0,1\})$. Then, as for ordinary circulants, a and b can be represented in the standard circulant basis thus,

$$\begin{aligned} a &= a_0 + a_1\mathrm{u} + a_2\mathrm{u}^2 + \cdots + a_{N-1}\mathrm{u}^{N-1} \\ b &= b_0 + b_1\mathrm{u} + b_2\mathrm{u}^2 + \cdots + b_{N-1}\mathrm{u}^{N-1} \end{aligned}$$

where each a_i, b_i is 0 or 1.

Suppose $a_i = b_j = 1$ for some i, j. Then, the term $1\mathrm{u}^i$ appears in the expansion for a, and the term $1\mathrm{u}^j$ appears in the expansion for b. Therefore, the term $1\mathrm{u}^{i+j}$ must appear in the expansion for the product $a \wedge b$. Since Boolean addition can never turn a non-zero value to a zero, it follows that the $(i+j)^{\text{th}}$ component of $a \wedge b$ must be 1. Hence, if $i \in \varsigma(a)$ and $j \in \varsigma(b)$ then $i + j \in \varsigma(a \wedge b)$. It is easy to see that the converse also holds. If $k \in \varsigma(a \wedge b)$, then there must be some $i, j \in \mathbb{Z}_N$ with $i + j = k$ and $a_i = b_i = 1$.

Therefore, $\varsigma(a \wedge b) = \varsigma(a) + \varsigma(b)$ where the addition is the addition of subsets in the additive group of $\mathbb{Z}_N$. That is, if G is an abelian group with addition, and $X, Y \subset G$, then $X + Y$ is defined to be the subset $\{x + y \vdash x \in X,\ y \in Y\}$ of G.

To avoid needlessly repeating definitions, given any subset $X \subset \mathbb{Z}_N$, define the sequence $X_1, X_2, \ldots$ by $X_1 = X$, $X_2 = X + X$, and in general, $X_{i+1} = X + X_i$. Then $X_{i+j} = X_i + X_j,\ \forall i, j$.

9.4.1 **Lemma** Let $a \in \mathbf{circ}_N(\mathbb{R})$ be standard, let $A = \varsigma H(a)$ be its corresponding subset of $\mathbb{Z}_N$, and let $d = \gcd(A \cup \{N\})$. If $0 \in A$, then there exists n such that $A_r = d\,\mathbb{Z}_N$ for all $r \geq n$.

Proof. Let $A = \{0, c_1, c_2, \ldots, c_t\}$. The set $\{N, c_1, c_2, \ldots, c_t\}$ has highest common divisor of d. Therefore, given any integer x, there exist integers $n_0, n_1, \ldots, n_t$ such that

$$n_0 N + n_1 c_1 + n_2 c_2 + \cdots + n_t c_t \ = \ dx$$

Therefore, given any $x \in \mathbb{Z}_N$, there exist $n_1, n_2, \ldots, n_t \in \mathbb{Z}_N$ such that

$$n_1 c_1 + n_2 c_2 + \cdots + n_t c_t \ \equiv \ dx \pmod{N} \tag{3}$$

Let $r = n_1 + n_2 + \cdots + n_t$ and consider the set $A_r = A + A + \cdots + A$. From the first n_1 summands, take the residue c_1, from the next n_2 summands, take the residue c_2, and so on. Clearly, we will get the sum in congruence (3). Since $0 \in A$, the residue $dx \bmod N$ will occur in every A_{r+i} for $i \geq 0$. This shows that ultimately, every residue of the form dx is in A_r. □

The lemma can be paraphrased as follows. Let $A = \varsigma H(a)$. Suppose $0 \in A$. Let $D \triangleleft \mathbb{Z}_N$ be minimal such that $A \subset D$, then $A_r = D$ for all $r > n$ for some n.

When $d = 1$, that is, when $D = \mathbb{Z}_N$, this shows that $a^r \to \bar{\delta}^N$ as $r \to \infty$ by Proposition 9.3.6. The case when $d > 1$ is dealt with in the next lemma.

9.4.2 **Lemma** Let $a \in \mathbf{circ}_N(\mathbb{R})$ be standard with corresponding subset $A \subset \mathbb{Z}_N$. Let $\gcd(A \cup \{N\}) = d$. If $0 \in A$ then $\lim_{r\to\infty} a^r \ = \ \bar{\delta}^{N/d}$.

Proof. Since $d \,|\, N$ we can write $N = dm$. Since $A \subset d\,\mathbb{Z}_N$ there exist $b_0, b_1, \ldots, b_{m-1} \geq 0$ such that

$$a \ = \ \sum_{i=0}^{m} b_i \mathrm{u}_{dm}^{id}$$

$$\therefore \ a \ = \ \tilde{\Gamma}_m^{dm} \left(\sum_{i=0}^{m-1} b_i \mathrm{u}_m^i \right)$$

$\tilde{\Gamma}_m^{dm}$ is the circulant injection homomorphism of §3.5.2. By Proposition 3.5.4 the circulant $b \in \mathbf{circ}_m(\mathbb{R})$ is standard.

Let n be the number such that $A_n = d\,\mathbb{Z}_N$.

$$a^n \;=\; \tilde{\Gamma}_m^{dm}(b^n)$$

By the Lemma 9.4.1, every $d^{\,\text{th}}$ component of a^n is positive. Therefore, b^n is standard positive. Therefore, $b^s \to \bar{\delta}^{n|n}$ as $s \to \infty$ by Proposition 9.3.6. The formula of Proposition 3.5.4 clearly shows that $\tilde{\Gamma}_m^{dm}$ is continuous. Therefore,

$$a^s \to \tilde{\Gamma}_m^{dm}\left(\bar{\delta}^{m|m}\right) \text{ as } s \to \infty$$

$$\text{Now, } \bar{\delta}^{m|m} \;=\; \frac{1}{m}\sum_{i=0}^{m-1} \mathrm{u}_m^i$$

$$\therefore\;\; \tilde{\Gamma}_m^{dm}\left(\bar{\delta}^{m|m}\right) \;=\; \frac{1}{m}\sum_{i=0}^{m-1} \mathrm{u}_{dm}^{id} \;=\; \bar{\delta}^{m|dm}$$

$$\therefore\;\; a^s \to \bar{\delta}^{m|N} \text{ as } s \to \infty \;\square$$

The final result is all but stated.

9.4.3 **Theorem** Let a be standard. Let $D \lhd \mathbb{Z}_N$ be minimal such that $\varsigma H(a)$ is in some coset $D + f$ where $f \in \mathbb{Z}_d$. Then, $a^r - \mathrm{u}^{fr}\bar{\delta}^{N/d} \to 0$ as $r \to \infty$.

Proof. We are given that $\varsigma H(a)$ is in the f coset of D. Therefore, $\varsigma H(\mathrm{u}^{-f}a)$ is in the subgroup D, and so the circulant $\mathrm{u}^{-f}a$ is in the form of the previous lemma. Hence, $(\mathrm{u}^{-f}a)^r - \bar{\delta}^{N/d} \to 0$ as $r \to \infty$. The theorem statement now follows because we can multiply throughout by u^{fr} without affecting the convergence since $|\mathrm{u}| = 1$. $\square$

To summarize, if a physical system can be accurately represented by the circulant matrix model, then the distribution must eventually become equidistributed at evenly spaced points throughout the space possibly with a constant rotational motion. It is interesting to note that if the distribution is eventually equidistributed throughout the space then any rotational motion is undetectable within the circulant model. This is because the model treats only the evolution of densities and not the motion of the constituents of the densities.

9.5 Higher-dimensional Torï.

Circulant matrices can be applied to higher dimensional torï; we shall illustrate with the two-dimensional torus. In this case, the non-homogenous diffusion law is

$$f_{t+h}(x_1, y_1) \;=\; \int_{T^2} a_h(x_1, y_1, x_2, y_2) f_t(x_2, y_2) d(x_2, y_2)$$

Let this space be approximated with $M \times N$ points, then the diffusion law is approximated by the function $a_h\left((x_1, y_1), (x_2, y_2)\right)$ and the integral becomes a matrix product Af where the matrix A is labelled by pairs of points $(x_1, y_1), (x_2, y_2) \in T^2$. If the space is homogenous then the matrix A must satisfy the condition: For all pairs $(x_1, y_1), (x_2, y_2) \in T^2$, the entry at $(x_1, y_1), (x_2, y_2)$ must equal the entry at $(0, y_1 - x_1), (0, y_2 - x_2)$. That is, A must be a tensor circulant matrix. Therefore, by Theorem 6.2.1, we must take M, N coprime and then $A \in \mathrm{CIRC}_M(\mathbb{R}) \otimes \mathrm{CIRC}_N(\mathbb{R})$.

By Theorem 6.3.1, $\mathrm{CIRC}_M \otimes \mathrm{CIRC}_N \approx \mathrm{CIRC}_{MN}$, so all the development of sections 9.3 and 9.4 apply.

9.6 Relaxation of the Assumptions

The assumptions 9.1.1, 9.1.2, and 9.1.4 cannot be relaxed in any meaningful way.

Assumption 9.1.3 can be abandoned completely by replacing the time sequence $a, a^2, \ldots, a^r, \ldots$ with a sequence

$$a^{(0)}, \quad a^{(0)}a^{(1)}, \quad \ldots, \quad a^{(0)}a^{(1)}\cdots a^{(r)}, \quad \ldots$$

That is, the r^{th} time step is modelled by multiplication by the r^{th} circulant matrix $A^{(r)}$. Obviously, the development of this theory will be a lot more difficult. Most probably, a gradual, perturbative change in $A^{(r)}$ as r increases would be a necessary simplification.

Assumption 9.1.5 that a is non-negative can be eliminated, but most of sections 9.3 and 9.4 become of only indirect use. This theory would probably proceed by considering conditions on a which cause a^r to become non-negative for some r.

Assumption 9.1.6 is probably the least essential provided all others are satisfied. Essentially, the theory proceeds the same but factors are introduced at the beginning to normalize $\lambda_0(a)$. These then are removed when the desired conclusion is derived. In this case, the distribution can become everywhere zero, or everywhere infinite.

Chapter 10.
Formulæ for the Circulant Determinant.

In this chapter, various formulæ for the general circulant determinant in complex fields will be derived, and some immediate conclusions drawn where appropriate. There are many reasons for wanting to evaluate the circulant determinant, but probably the earliest was Kummer's proof that the class groups of the cyclotomic fields of prime order were finite.

For convenience, we restate the resultant formula for the circulant determinant.

1.11.3 **Theorem (The Resultant Formula).** Let $a \in \mathbf{circ}_N(R)$ where R is an integral domain and let $A(x) = \sum_{i=0}^{N-1} a_i x^i \in R[x]$ be the representer polynomial for a of degree d with roots $\alpha_1, \alpha_2, \ldots, \alpha_d$ if necessary in some extension of R. Then,

$$\Delta_N(a) \quad = \quad (-1)^{d(N-1)} a_d^N \prod_{i=1}^{d} (1 - \alpha_i^N) \qquad \square$$

The theorem is easily generalized to any polynomial $A(x) \in \left(\Gamma^N\right)^{-1}(a)$ where $d = \deg A$ and $\alpha_1, \alpha_2, \ldots, \alpha_d$ are the roots of $A(x)$. In fact, the only change required in the proof of the theorem is to use A_i throughout for the coefficients of the polynomial instead of the circulant vector components, a_i.

10.1.1 **Corollary** For a given $a = (a_0, a_1, \ldots, a_d) \in R^d \subset \mathbb{C}^d$ with $a_d \neq 0$, extend a with zeroes to a vector in R^N thus defining $\Delta_N = \Delta_N(a)$, for all $N \geq d$. Let $\mathscr{A}$ be the multiset of the roots of $A(x) = \sum_{i=0}^{d} a_i x^i$. Let S_1 be the unit circle in $\mathbb{C}$, and let $\breve{D}_1$ be the open unit disc.

(i) If $\mathscr{A} \cap S_1 = \emptyset$, then $|\Delta_N| \sim |a_d|^N \prod_{|\alpha|>1} |\alpha|^N$, as $N \to \infty$.

(ii) If $\mathscr{A} \cap \breve{D}_1 = \emptyset$, then $|\Delta_N| \sim |a_d a_0|^N$, as $N \to \infty$.

(iii) If $\mathscr{A} \subset \breve{D}_1$, then $|\Delta_N| \sim |a_d|^N$, as $N \to \infty$. $\square$

In the next proposition the base ring R is the field of residues modulo a prime q and is not a complex domain.

10.1.2 **Proposition** Let $A(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ and extend a with zeroes to a_{N-1} if necessary as in the previous corollary. Let $q = rN + 1$ be prime in $\mathbb{Z}$. Then,

$$\Delta_N(a) \equiv 0 \;\Leftrightarrow\; \exists x \in \mathbb{Z} \text{ s.t. } A(x^r) \equiv 0 \pmod{q}$$

Proof. Take $R = \mathbb{F}_q$. R contains a primitive N^{th} root of unity, ζ, say, so $R_\zeta = R$. The set of N^{th} roots of unity is equal to the set of r^{th} powers of residues, so

RTP: In $\mathbb{F}_q$, $\Delta = 0$ iff $A(\zeta^i) = 0$ for some $i \in \{0, 1, \ldots, N-1\}$

$\Leftarrow$: If $A(\zeta^i) = 0$ in $\mathbb{F}_q$, then $\lambda_i(a) = 0$. QED ($\Rightarrow$)

$\Rightarrow$:

$$\begin{aligned} \Delta = 0 \;&\Rightarrow\; \prod_{A(\alpha)=0} (1 - \alpha^N) = 0 \\ &\Rightarrow\; \alpha^N = 1 \text{ for some root } \alpha \text{ of } A \\ &\Rightarrow\; \alpha = \zeta^i \text{ for some } i \\ &\Rightarrow\; \alpha = x^r \text{ for some } x \in \mathbb{F}_q^* \;\square \end{aligned}$$

10.1.3 **Proposition** Let $A(x) \in \mathbb{Z}[x]$ be monic. Given any element $r \in \mathbb{F}_p$, define $n(r)$ to be the highest power of p dividing $r^{p-1} - 1$ (with $n(1) = \infty$). Let $x_1, x_2, \ldots, x_f$ be the roots of A in $\mathbb{F}_p^*$, and define $e := \sum\{n(x_i) \vdash 0 \le i \le f\}$. Then,

$$p^e \mid \Delta_{p-1}(A(\mathrm{u}_{p-1}))$$

and e is highest such, and $e \ge f$. (Divisibility by p^∞ indicates Δ is zero.)

Proof. Let $E \supset \mathbb{F}_p$ be the root field of A, and let the roots lying in $E - \mathbb{F}_p$ be $x_{f+1}, x_{f+2}, \ldots, x_{f+g}$. (Thus, the zero root has multiplicity $\deg A - f - g$).

We have $n(r) \ge 1$ for every $r \in \{x_1, x_2, \ldots, x_f\}$ which proves $e \ge f$.

We shall apply the theorem to the root field of the polynomial A regarded as a polynomial in $\mathbb{F}_p[x]$.

$$\begin{aligned}\Delta_{p-1}(a) &= \pm \prod_{i=1}^{f} \left(x_i^{p-1} - 1\right) \prod_{i=1}^{g} \left(x_{f+i}^{p-1} - 1\right) \\ &= \pm \prod_{i=1}^{f} H(x_i) \prod_{i=1}^{g} H(x_{f+i}) \quad \text{where } H(x) := x^{p-1} - 1\end{aligned}$$

Since each $x_i \in \mathbb{F}_p^*$, and $\left|\mathbb{F}_p^*\right| = p - 1$, we have $x_i^{p-1} = 1$. Therefore, $H(x) = 0$ at $x = x_1, x_2, \ldots, x_f$ showing that p^f divides $\Delta_{p-1}(a)$.

Now, $(d/dx)H(x) = (p-1)x^{p-2} \neq 0$ for $x \in \mathbb{F}_p^*$. Hence $H(x)$ does not have repeated roots at these values. One would therefore expect that $p^2 \nmid H(x)$. But this mistakes a repeated root mod p for repeated divisibility by p. (See the discussion after the proposition for counterexamples.) A repeated root implies repeated divisibility, but the converse is false. Hence, in general, we must set $e = n(x_1) + n(x_2) + \cdots + n(x_f)$.

It remains to show that the other factors, $H(x_{f+i})$, are not divisible by p. But, we need only note that $H(x) = x^{p-1} - 1$ is a polynomial of degree $p-1$ over the field E, and therefore has exactly $p-1$ roots in E. These are all accounted for by $\mathbb{F}_p^*$. That is, there are no roots of $H(x)$ in $E - \mathbb{F}_p$. □

One wonders: How frequently is $r^{p-1} - 1$ divisible by p^2? Let us call such a residue a second degree residue of p. Heuristically, one would expect most primes to have at least one second degree residue because if $r^p \equiv r + bp \pmod{p^2}$, then $(r + bp)^p \equiv r + bp \pmod{p^2}$. This shows that there are p solutions to $x^p - x \equiv 0 \pmod{p^2}$, so one would expect roughly one solution to fall in the range 0 to $p - 1$.

In fact, as the table below demonstrates, few primes below 100 possess second degree residues.

Prime	2^{nd} Degree Residues
11	3, 9
29	14
37	18
43	19
59	53
71	11, 26
79	31
97	53

In the 182 odd primes to 1093, there are only 169 second degree residues, and only one of these is a third degree residue (at $p = 113$, $r = 68$). Curiously, the first prime for which 2 is a second degree residue is $p = 1093$ which also has the distinction of having all powers of 2 to 1024 as second degree residues. This particular fact is of importance to the traditional analysis of Fermat's Last Theorem. (See [HaW].)

The fact that we know the exact power of p dividing Δ_{p-1} allows us to deduce the existence of roots in a finite field. To take a simple example, let $A(x) = x^2 - 2$, $p = 17$. $\Delta_{16}(\mathrm{u}^2 - 2) = (2^8 - 1)^2 = 65025 = 3^2 \times 5^2 \times 17^2$. So, 2 must be a quadratic residue mod 17.

We now give a slight generalization of the proposition.

10.1.4 **Proposition** Let $A(x) \in \mathbb{Z}[x]$ be monic of degree d, let $N = n(p-1)$ with p prime. Suppose $A(x)$ has roots $x_1, x_2, \ldots, x_f$ in $\mathbb{F}_p^*$. Let $e = \sum\{n(x_i) \vdash 1 \leq i \leq f\}$ where $n(r)$ is the highest power of p dividing $r^N - 1$. Then, for all $n \geq 1$, $p^e \mid \Delta_N(A(\mathrm{u}_N))$.

If n is coprime to $p^{h-1} + p^{h-2} + \cdots + p^2 + p + 1$ for all $h \leq d!$, then e is the largest such.

Proof. As before, let E be the root field for $A(x)$. Following the same reasoning as in the proposition we still deduce $p^e \mid \Delta_N(A(\mathrm{u}))$. However, we can no longer deduce that e is the largest such because it is now possible for $H(x) = x^N - 1 = 0$ when $x = \alpha \notin \mathbb{F}_p$.

Assume $\alpha \in E - \mathbb{F}_p$ is such a root of H. Then, some power of α must be in the base field. Now, we already know that $\alpha^N = 1 \in \mathbb{F}_p$. Therefore, $t \mid N$. Now, $\alpha^{p-1} \neq 1$ since all the $p-1$ roots are accounted for in $\mathbb{F}_p$. Therefore, $\gcd(t, n) > 1$. Let $g = \gcd(t, n)$.

Let $\bar{\alpha}$ be the image of α under the natural map to $E^* \to E^*/\mathbb{F}_p^*$. Then, $\bar{\alpha}$ must satisfy $\bar{\alpha}^t = 1$. Now, the order of any element in a finite group must divide the order of the group. Therefore, $t \mid \left|E^*/\mathbb{F}_p^*\right|$. $\therefore g \mid \left|E^*/\mathbb{F}_p^*\right| = (q-1)/(p-1) = p^{h-1} + p^{h-2} + \cdots + p + 1$. The coprimality of n with respect to this latter expression makes $g \mid n$ impossible for $h \leq d!$. We now recall that the greatest possible dimension of the root field of a polynomial over the base field is $d!$ where d is the degree of the polynomial. But, $\dim E = [E : \mathbb{F}_p] = h$. Hence $h \leq d!$. □

10.1.5 **Wendt's circulant.**

An important application of the proposition is finding factors of "Wendt's circulant," W_N, which is defined as $W_N := \left|\Delta_N\left((\mathrm{u}-1)^N - 1\right)\right|$. (See §10.3 for a fuller discussion of Wendt's circulant.)

10.1.6 **Corollary** Suppose N is divisible by $p-1$ for some prime p. Then, $p^{p-2} \mid W_N$.

Proof. Let $A(x) = (x-1)^N - 1$. Then, $W_N = A(\mathrm{u})$.

It is easy to see that all residues in $\mathbb{F}_p$ are roots of A except for $x = 1$. Hence, the non-zero roots are $2, 3 \ldots, p-1$ giving $p-2$ non-zero roots in all. □

(See §10.3.5 for an improvement of this corollary.)

10.2 **Homogenous Diophantine Equations.**

The above proposition has application to certain homogenous diophantine equations. The next theorem places necessary conditions on a class of diophantine equations for them to have non-trivial solutions. One such diophantine equation is the famous equation of Fermat's Last Theorem which is discussed in more detail.

10.2.1 **Theorem**

Let $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ be a solution to the diophantine equation $a_1 x_1^r + a_2 x_2^r + \cdots + a_n x_n^r = 0$.

Suppose $q = 1 + rN$ is prime for some N. Given any map, $\beta : \{1, 2, \ldots, n\} \mapsto \mathbb{Z}_N$. Define $\beta a \in \mathbf{circ}_N(\mathbb{F}_q)$ by $(\beta a)_i = \sum\{a_j \vdash \beta(j) = i\} \bmod q$. If, for all such maps β, $\Delta_N(\beta a) \not\equiv 0 \pmod q$ then q divides $x_1 x_2 \cdots x_n$.

Proof. We have $\sum_{i \in \mathbb{Z}_N} a_i x_i^r \equiv 0 \pmod q$.

Suppose $x_i \not\equiv 0$ for all i. Let x_i also represent its residue modulo q. Then, each x_i^r is an N^{th} root of unity in $\mathbb{F}_q$, and we can replace x_i^r by $\zeta^{\beta(i)}$ where ζ is a primitive N^{th} root of unity in $\mathbb{F}_q$ and $\beta : \{1, 2, \ldots, n\} \mapsto \mathbb{Z}_N$. Let $b = \beta a$. Then the congruence becomes in $\mathbb{F}_q$,

$$\sum_{i \in \mathbb{Z}_N} b_i \zeta^i = 0$$

Multiplying this equation throughout by successively higher powers of ζ, we get the following system of equations in $\mathbb{F}_q$.

$$\begin{pmatrix} b_0 & b_1 & b_2 & \dots & b_{N-1} \\ b_{N-1} & b_0 & b_1 & \dots & b_{N-2} \\ b_{N-2} & b_{N-1} & b_0 & \dots & b_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_1 & b_2 & b_3 & \dots & b_0 \end{pmatrix} \begin{pmatrix} 1 \\ \zeta \\ \zeta^2 \\ \vdots \\ \zeta^{N-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

For consistency, $\Delta_N(b) \equiv 0 \pmod{q}$. Since this contradicts the assumptions, the only possibility is that x_i^r is not a power of ζ for some i. But, ζ is a primitive residue for all non-zero r^{th} powers in $\mathbb{F}_q$; so, x_i must be divisible by q. □

Remark If the conditions of the theorem hold for an infinity of primes $q = 1 + rN$, then we can deduce $q \,|\, x_1x_2\cdots x_n$ for an infinity of primes and hence $x_1x_2\cdots x_n = 0$. Note also that by a well-known theorem of Dirichlet, that there always are an infinity of primes of the form $1 + rN$ with r fixed. (See for instance [Edw], [HaW]. Washington's book [Was] contains a particularly simple proof.)

10.2.2 **Fermat's Last Theorem** The most famous example of a diophantine equation of the type covered by the above theorem is the equation of Fermat's Last Theorem, $x^n + y^n = z^n$. It states that there are no non-zero solutions to this equation for $n > 2$. The only proof at the time of writing is extremely lengthy since it involves the highly developed theory of elliptic curves. (The ancient Greeks proved that there are an infinity of solutions when $n = 2$. See §8.1.3.) The theorem is often referred to as the "FLT Conjecture" in earlier works, and "FLT" in works after the appearance of the proof by Andrew Wiles. It is easily shown that the theorem is true if and only if it is true for $n = 4$ and all primes $n > 2$, that is for all odd prime exponents.

It is quite easy to prove the theorem for $n = 4$. Therefore, one can assume that the equation is $x^p + y^p = z^p$ where p is an odd prime. Since p is odd, the sign of z can be reversed and the equation written in the more symmetric form $x^p + y^p + z^p = 0$. The theorem naturally falls into two cases traditionally called the First and Second Cases. In the First Case it is assumed that none of the variables x, y, z are divisible by p whereas in the Second Case it is assumed that $p \,|\, xyz$.

If in the statement of Theorem 10.2.1 we set $n = 3$, $r = p$, and $a_1 = a_2 = a_3 = 1$, we get the FLT equation. On the face of it, Theorem 10.2.1 appears insensitive to the conditions of the two traditional FLT cases. It matters not whether $p \,|\, xyz$ since the modulus of importance is not p but the prime $q = Np + 1$. This is so. In fact, the conditions $\Delta(\beta a) \not\equiv 0$ in the theorem naturally fall into the following cases:

$$\left.\begin{array}{ll} (i) & \Delta_N(3,0,\dots,0) \not\equiv 0 \\ (ii) & \Delta_N(2,0,\dots,0,1,0,\dots,0) \not\equiv 0 \\ (iii) & \Delta_N(1,0,\dots,0,1,0,\dots,0,1,0,\dots,0) \not\equiv 0 \end{array}\right\} \pmod{q} \qquad (1)$$

where the 1 in *(ii)* occurs in any position $i \neq 0$, and the latter two 1's in *(iii)* are in any positions $0 < i < j$.

Case *(i)* holds trivially. Theorem 10.1 gives the following value for the determinant in case *(ii)*

$$|\Delta_N| = (2^n - (-1)^n)^d \quad \text{where } d = \gcd(N, i) \text{ and } n = N/d$$

Little is known about the determinant in case *(iii)*. Since the determinant has only three non-zero entries per row, all equal to 1, it is natural to try to evaluate the determinant in this case by direct expansion. Although a general formula for the terms in the determinant expansion is known (see Chapter 11), it has not as yet provided much insight into the residue class of the determinant modulo a prime q. Some insight into the terms appearing in such an expansion came from an article in 2004 by Loehr, Warrington, & Wilf ([LWW]). Whose results which are germane to the FLT question are summarized in the next proposition.

10.2.2.3 **Proposition** Let $c(r, s)$ be the coefficient of $x^r y^s$ in the expansion of $\Delta_N(1 + x\mathrm{u} + y\mathrm{u}^j)$. Then,

(i) $c(r, s) \neq 0$ iff $N \,|\, r + sj$.

(ii) $c(r,s)$ is positive or negative according as $\gcd\left(r,s,(r+sj)/N\right)$ is respectively even or odd. □ ([LWW])

As the authors point out, the above proposition can be easily extended to the expansion of $\Delta_N(1 + x\mathrm{u}^i + y\mathrm{u}^j)$ for any i coprime to N by applying the ν_i map to the circulant $1 + x\mathrm{u} + y\mathrm{u}^j$. It can also be extended to cases where i is not coprime provided j is coprime by applying the ν_j^{-1} map.

In conditions (1), we have simplest possible application of the proposition: $x = y = 1$. Evaluating the determinant is reduced to adding and substracting coefficients according to the odd-even rule given in the proposition. Unfortunately, we still lack a good understanding of the magnitudes of the coefficients. Loehr et al. proved only that coefficients grow exponentially with N.

Should conditions (1) be proved for some p and for an infinity of primes $q = Np + 1$, then FLT would be a consequence for the exponent p since any solution x, y, z would have to satisfy $q \,|\, xyz$ for an infinity of primes which is impossible unless $xyz = 0$. Needless to say this has not been proved.

We obtain some partial results in §10.6 by setting bounds on the circulant determinant which imply $q \,|\, xyz$ for several primes q and for various exponent primes p.

Although the two traditional cases of FLT are not salient in the above approach, there is a theorem of Sophie Germain which makes Theorem 10.2.1 directly relevant to the First Case of FLT. We omit the proof as the theorem is not directly relevant to theory of circulants. The proof and more on FLT including the development of cyclotomic theory in the 19^{th} century can be found in Edwards book [Edw]. Also, see Ribenboim's book [Rib1] for a general exposition of "elementary" approaches to FLT.

10.2.3 **The Theorem of Sophie Germain.** Let $p > 2$ be prime. If there is an auxiliary prime q with the properties that

(i) $x_1^p + x_2^p + x_3^p \equiv 0 \pmod{q}$ implies that $x_1x_2x_3 \equiv 0 \pmod{q}$, and

(ii) $x^p \equiv p \pmod{q}$ is impossible

then the First Case of FLT is true for p.

Proof. See [Edw]. □

When the auxiliary prime q is of the form $Np + 1$, condition *(ii)* of the Sophie Germain Theorem can be stated more powerfully.

10.2.4 **Proposition** $q = Np + 1$ satisfies condition *(ii)* of the Sophie Germain Theorem if and only if

$$N^N \not\equiv 1 \pmod{q}$$

Proof. We shall represent the statement of condition *(ii)* by C_2 and its negation by $\sim C_2$. Thus, $\sim C_2$ means that there is a solution to $x^p \equiv p \pmod{q}$. Throughout this proof all congruences are modulo q.

$$\begin{aligned} \sim C_2 \quad &\Rightarrow \quad p \equiv x^p \pmod{q} \quad \text{for some } x \\ &\Rightarrow \quad p^N \equiv x^{Np} = x^{q-1} \equiv \begin{cases} 0 & \text{if } q \,|\, x \\ 1 & \text{otherwise} \end{cases} \end{aligned}$$

But, $q \,|\, x$ is impossible if $p \equiv x^p$ since p and q are distinct primes so $p \not\equiv 0 \pmod{q}$.

$$\therefore \sim C_2 \quad \Rightarrow \quad p^N \equiv 1$$

Now suppose that $p^N \equiv 1$, then $p = \zeta_N^a$ for some a where ζ_N is a primitive N^{th} root of unity in $\mathbb{F}_q$. But, $\zeta_N = \zeta^p$ for some primitive $(q-1)^{\text{th}}$ root of unity, ζ. $\therefore p \equiv (\zeta^a)^p$ and this is a solution to the congruence $x^p \equiv p$. Therefore, $p^N \equiv 1 \;\Rightarrow \sim C_2$

$$\begin{aligned}\therefore \sim C_2 &\Leftrightarrow p^N \equiv 1\\ &\Leftrightarrow \left(\frac{q-1}{N}\right)^N \equiv 1\\ &\Leftrightarrow (q-1)^N \equiv N^N\\ &\Leftrightarrow (-1)^N \equiv N^N\\ &\Leftrightarrow 1 \equiv N^N \text{ since } N \text{ is even}\end{aligned}$$

In the last step, N is said to be even. This must be so since p is odd, so $q = Np + 1$ can be odd only if N is even. □

Using estimates for the maximum value of the the three-term determinant of §10.2.2, and using these to limit the maximum factor dividing the determinant, it is possible to deduce the first case of FLT for many primes. However, the standard, and more successful approach using a circulant determinant, is that based on Wendt's Theorem which we now turn to.

10.3 **Definition** Define **Wendt's Circulant of order** n as

$$W_n := \mathbf{circ}\left(1, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}\right) = (\mathrm{u}+1)^n - 1$$

10.3.1 **Wendt's Theorem** Let $p > 2$ be prime and assume that $q = Np + 1$ is also prime. Then there exist integers x, y, z, not multiples of q, such that $x^p + y^p + z^p \equiv 0 \pmod{q}$ iff $q \,|\, \det(W_N)$.

Proof. [Rib1]. As in Theorem 10.2.1, we replace each of x^p, y^p, z^p by powers of a primitive N^{th} root of unity in $\mathbb{F}_q$ giving us the equation $1 + \zeta^i = \zeta^j$ in $\mathbb{F}_q$ for some $i, j, 0 \le i, j < N$. Setting $\xi = \zeta^i$ we see that this is equivalent to the equation $(1+\xi)^N = 1$ in $\mathbb{F}_q$. Expanding,

$$1 + \binom{N}{1}\xi + \binom{N}{2}\xi^2 + \cdots + \binom{N}{N-1}\xi^{N-1} = 0$$

Proceeding as in Theorem 10.2.1, we multiply this equation throughout by successively higher powers of ξ obtaining a system of simultaneous equations over $\mathbb{F}_q$ equivalent to $W_N\boldsymbol{\xi} = 0$ where $\boldsymbol{\xi}$ is the vector of powers of ξ. Hence, W_N is singular in $\mathbb{F}_q$. □

Note that Wendt's criterion does not require consideration of cases depending on the residues of $x, y, z \pmod{q}$, and this is its great advantage over the three-term determinant of §10.2.2.

Much work has been done on divisibility properties of Wendt's determinant. Some of this is summarised in the next theorem.

10.3.2 **Theorem** Let $\Delta_n = \det W_n$.

(i) $\Delta_n = 0 \Leftrightarrow 6 \,|\, n$.

(ii) $d \,|\, n \Rightarrow \Delta_d \,|\, \Delta_n$. (E.Lehmer)

(iii) if $p > 2$ is prime then $p^{p-2}\left(\dfrac{2^{p-1}-1}{p}\right) \Big| \Delta_{p-1}$.

(iv) If $n \equiv 2$ or $4 \pmod{6}$, then $\Delta_n = -3\left(\dfrac{2^n-1}{3}\right)^3 w^6$ for some integer w. (J.S.Frame).

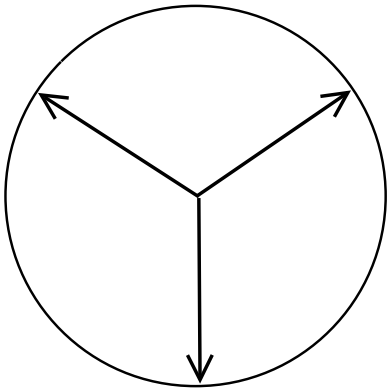
(v) If $2n + 1 = p$ is prime then $p^{\lfloor (n-1)/2 \rfloor} \mid \Delta_n$. (J.S.Frame)

Proof. The proofs of these statements appear in Propositions 10.3.3 through 10.3.6 below. Most of the proofs are adapted from [Rib1] where more details concerning Wendt's determinant can be found. □

Throughout the remaining propositions of this section, $\zeta = \zeta_n$, and $\Delta_n = \det W_n$.

10.3.3 **Proposition** $\Delta_n = 0 \Leftrightarrow 6 \,|\, n$.

Proof. We are given $\Delta\left((1+\mathrm{u})^n - 1\right) = 0$. So, $\exists i$, $(1+\zeta^i)^n = 1$ and so $1+\zeta^i = \zeta^j$ for some j. The diagram below depicts the three terms as vectors in the complex plane. If we think of these vectors as unit forces in balance it is clear that ζ^i and $-\zeta^j$ must be third roots of unity. This is possible only if $6 \,|\, n$. □



Three Unit Forces in Balance

10.3.4 **Proposition** $d \,|\, n \;\Rightarrow\; \Delta_d \,|\, \Delta_n$.

Proof. We have

$$\frac{W_n}{W_d} \;=\; \prod_{i\in\mathbb{Z}_d} \frac{(1+\zeta_d^i)^n - 1}{(1+\zeta_d^i)^d - 1} \;\prod\{(1+\zeta_n^i)^n - 1 \vdash\; i \in \mathbb{Z}_n,\; n/d \nmid i\}$$

The second product ranges over a union of residue classes mod n, and so is a rational; it is also manifestly a cyclotomic integer, and therefore is a rational integer.

The typical term under the first product expands into the geometric series $\sum_{j=0}^{n/d-1}(1+\zeta_d^i)^{dj}$ which is also manifestly an algebraic integer; the product is over all d^{th} roots of unity and so is rational. □

10.3.5 **Proposition** If $p > 2$ is prime then $p^{p-3}\left(2^{p-1}-1\right) \,\big|\, \Delta_{p-1}$.

Proof. We already know from Corollary 10.1.6 that $p^{p-2} \,|\, \Delta_{p-1}$.

By definition, $W_{p-1} := (1+\mathrm{u})^{p-1} - 1$. $\therefore \lambda_0(W_{p-1}) = 2^{p-1} - 1$. Since a determinant of an integer circulant is always divisible by λ_0, it follows that $2^{p-1} - 1 \,|\, \Delta_{p-1}$.

Now $p \,\big|\, 2^{p-1} - 1$, and so p must be removed from $2^{p-1} - 1$ since Proposition 10.1.6 guarantees only that $p^{p-2} \,\big|\, \Delta$ in all cases. Suppose generally that $p^t \,\big|\, 2^{p-1} - 1$ then, in the notation of Proposition 10.1.3, $n(2) = t$, and therefore, $p^{p-3+t} \,\big|\, \Delta$, but we would need to remove a factor of p^t from $2^{p-1} - 1$. Hence, Δ_{p-1} is divisible by

$$p^{p-3+t}\left(\frac{2^{p-1}-1}{p^t}\right) \;=\; p^{p-3}\left(2^{p-1}-1\right) \;\square$$

10.3.6 **Proposition** If $n \equiv 2$ or $4 \pmod 6$, then $\Delta_n \;=\; -3\left(\dfrac{2^n-1}{3}\right)^3 w^6$ for some integer w.

Proof. We term this the "hat trick" proof because three "rabbits" (actually integers) are pulled out of a "hat" (actually a product) leaving an integer still in the hat. The real trick comes at the end when it is revealed that the integer left in the hat is a perfect sixth power.

We let $\rho = \zeta^3$. Since $3 \nmid n$, ρ is a primitive n^{th} root of unity. Hence, $W_n = \prod_{i\in\mathbb{Z}_n}\left((1+\rho^i)^n - 1\right)$. Later in the proof it will be convenient to replace ρ by ζ^3.

Consider the double product $P_n = \prod_{j,k\in\mathbb{Z}_n}(1+\rho^{j+n/2}+\rho^{k+n/2})$.

$$\begin{aligned} P_n &= \prod_{j\in\mathbb{Z}_n}\prod_{k\in\mathbb{Z}_n}(1-\rho^j-\rho^k) \\ &= \prod_{j\in\mathbb{Z}_n}\big((1-\rho^j)^n-1\big) \quad \text{since } \prod_{k\in\mathbb{Z}_n}(x-\zeta^k)=x^n-1 \\ &= W_n \quad \text{since } \{-\rho \vdash \rho^n=1\}=\{\rho\vdash\rho^n=1\} \text{ for } n \text{ even.} \end{aligned}$$

We pull out the following integers from P_n:

(a) All terms with $j=\frac{1}{2}n$ yielding $\pi_a=\prod_{k\in\mathbb{Z}_n}(2-\rho^k) \;=\; 2^n-1.$

(b) All terms with $k=\frac{1}{2}n$ yielding $\pi_b=\prod_{j\in\mathbb{Z}_n}(2-\rho^j) \;=\; 2^n-1.$

(c) All terms with $j=k$ yielding $\pi_c=\prod_{j\in\mathbb{Z}_n}(1-2\rho^j) \;=\; 1-2^n.$

The ranges of the products π_a,π_b,π_c intersect as follows:

$$\mathrm{Ran}(\pi_a)\cap\mathrm{Ran}(\pi_b)=\mathrm{Ran}(\pi_b)\cap\mathrm{Ran}(\pi_c)=\mathrm{Ran}(\pi_c)\cap\mathrm{Ran}(\pi_a) \;=\; 1-\zeta^{n/2}-\zeta^{n/2} \;=\; 3$$

$$\therefore\ \mathrm{Ran}(\pi_a)\cap\mathrm{Ran}(\pi_b)\cap\mathrm{Ran}(\pi_c) \;=\; 3$$

By the intersection-complement principle, we must divide $\pi_a\pi_b\pi_c$ by $3^3\,3^{-1}=9$ to eliminate duplications.

$$\therefore\ P_n \;=\; -\frac{1}{9}(2^n-1)^3H$$

The remaining terms are gathered in H where

$$H \;=\; \prod_{(j,k)\in D}\Big(1+\rho^{j+n/2}+\rho^{k+n/2}\Big) \quad \text{and } D \;:=\; \{(j,k)\in\mathbb{Z}_n^2 \vdash\ j\neq\tfrac{1}{2}n,\ k\neq\tfrac{1}{2}n,\ j\neq k\} \qquad (2)$$

To finish statement *(iii)*, it remains to prove that H is a perfect 6^{th} power.

The geometric mean of the three terms appearing under the product in H is $\rho^{(j+k)/3}=\zeta^{j+k}$. (This is why we started with ρ rather than ζ.) We move this term out of the main product obtaining

$$H \;=\; \prod_{j,k\in D}\zeta^{j+k}\prod_{j,k\in D}\Big(\zeta^{-j-k}+\zeta^{2j-k+n/2}+\zeta^{2k-j+n/2}\Big)$$

The first product in H evaluates to ζ^s where

$$\begin{aligned} s &= \sum_{(j,k)\in D}(j+k) \\ &= \sum_{(j,k)\in\mathbb{Z}_n^2}(j+k) \;-\; \sum_{\substack{(j,k)\in\mathbb{Z}_n^2\\ j=n}}(j+k) \;-\; \sum_{\substack{(j,k)\in\mathbb{Z}_n^2\\ k=n}}(j+k) \;-\; \sum_{\substack{(j,k)\in\mathbb{Z}_n^2\\ j=k}}(j+k) \;+\; 2\sum_{\substack{(j,k)\in\mathbb{Z}_n^2\\ j=k=n}}(j+k) \end{aligned}$$

(The coefficient of 2 on the last sum comes from 3 double intersections − 1 triple intersection.)

$$\equiv\ 0 \pmod n$$

Therefore, the first product is 1, and the second is

$$H \;=\; \prod_{(e,f,g)\in E}\big(\zeta^e+\zeta^f+\zeta^g\big) \qquad (3)$$

where $E \subset \mathbb{Z}_n^3$ consists of distinct triples summing to $0 \pmod{n}$. This follows by the identifications below.

$$\left.\begin{array}{rcl} e &=& -j-k \\ f &=& 2j-k+\frac{1}{2}n \\ g &=& 2k-j+\frac{1}{2}n \end{array}\right\} \text{ in } \mathbb{Z}_n$$

together with the conditions $j \neq \frac{1}{2}n$, $k \neq \frac{1}{2}n$, $j \neq k$, and $3 \nmid n$. For example, $e = f \Leftrightarrow 3j+\frac{1}{2}n = 0 \Leftrightarrow 3 \mid n$.

Define $t(e,f,g) := \zeta^e + \zeta^f + \zeta^g$, the typical term in the product of formula (3). We can separate the product into six factors, $H_1, H_2, \ldots, H_6$ defined by

$$H_1 = \prod_{e<f<g} t(e,f,g), \quad H_2 = \prod_{g<e<f} t(e,f,g), \quad H_3 = \prod_{f<g<e} t(e,f,g),$$
$$H_4 = \prod_{f<e<g} t(e,f,g), \quad H_5 = \prod_{e<g<f} t(e,f,g), \quad H_6 = \prod_{g<f<e} t(e,f,g).$$

where the range of the variables e, f, g is $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with constraints as indicated.

All these factors have the same value since $t(e,f,g)$ is invariant under all permutations of (e,f,g),

$$\therefore \; H \;=\; H_1 H_2 \cdots H_6 \;=\; H_1^6$$

(This implies that $H_1 \in \mathbb{Z}(\zeta_n) \cap \mathbb{R}(\zeta_6)$ with $3 \nmid n$, but is not quite enough to clinch the proof.) Consider the effect of a field automorphism, $\zeta \mapsto \zeta^h$ on H_1. Its effect on a typical term is $t(e,f,g) \mapsto t(eh, fh, gh)$ which is also in H_1 (with (eh, fh, gh) possibly in a different order). Hence, H_1 is rational, is manifestly a cyclotomic integer, and is therefore a rational integer. □

In 1991 Fee and Granville [FG] succeeded in using the Wendt determinant to prove FLT for all primes $p = nq + 1$ where $n \leq 200$ and $6 \nmid n$, a remarkable achievement.

10.4 Formulæ for the Determinantal Coefficients.

The general circulant determinant is

$$\Delta_N(a_0, a_1, \ldots, a_{N-1}) \quad = \quad \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_{N-1} \\ a_{N-1} & a_0 & a_1 & \cdots & a_{N-2} \\ a_{N-2} & a_{N-1} & a_0 & \cdots & a_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{vmatrix}$$

This determinant can obviously be expanded in terms of the entries $a_0, a_1, \ldots, a_{N-1}$ into a sum of monomials thus,

$$\Delta_N(a_0, a_1, \ldots, a_{N-1}) \;=\; \sum_{v_0 \leq v_1 \leq \cdots \leq v_{N-1}} c(v_0, v_1, \ldots, v_{N-1})\, a_{v_0} a_{v_1} a_{v_2} \cdots a_{v_{N-1}} \; .$$

The constraint on the summation ensures that only algebraically distinct terms appear in the summation. The constants or coefficients, $c(v)$, which appear in the summation are called the **circulant determinantal coefficients**. These are functions of the numbers $v_0, v_1, \ldots, v_{N-1}$ which are the subscripts appearing in the monomial $a_{v_0} a_{v_1} a_{v_2} \cdots a_{v_{N-1}}$. By construction, $c(v)$ is a fully symmetric function in its arguments $v_0, v_1, \ldots, v_{N-1}$.

Consider Theorem 10.2.1 when applied to the FLT Conjecture. The circulant vector has only three non-zero components, and all three equal 1. It would appear that the best approach to evaluating the circulant determinant would be to find a formula for the determinantal coefficients as functions of the subscripts $v_0, v_1, \ldots, v_{N-1}$. Even if the general formula was rather complex, it would be reasonable to hope that in special cases such as the FLT conjecture, that the formula would simplify enough to allow an estimate of the determinant. Another instance where a formula would be useful would be the problem of finding the units of the ring $\mathbf{circ}_N(\mathbb{Z})$. In this section, two intermediate expressions are found for the determinantal coefficient which are later used in Chapter 11 to derive an explicit formula.

10.4.1 **Phase Formula** The derivation of the first formula starts with product of the eigenvalues.

$$\Delta_N(a) \;=\; (a_0 + a_1 + \ldots + a_{N-1})(a_0 + a_1\zeta + \ldots)\cdots(a_0 + a_1\zeta^j + a_2\zeta^{2j} + \ldots)\cdots(a_0 + a_1\zeta^{N-1} + \ldots) \quad (4)$$

where ζ is a primitive N^{th} root of unity.

Since we shall be writing formulæ containing fairly complex exponents of ζ, we shall be using $e_N(x)$ (or just $e(x)$, if N is understood) to stand for ζ^x.

Pick a sequence of a_i's, one from each factor of equation (4). Suppose the sequence is $a_{v_0}a_{v_1}\cdots a_{v_{N-1}}$. The coefficient of this particular monomial is

$$\zeta^{0\cdot v_0 + 1\cdot v_1 + 2\cdot v_2 + \cdots + (N-1)\cdot v_{N-1}} \quad = \quad e\Big(\sum_{r\in\mathbb{Z}_N} r v_r\Big)$$

Therefore, $\Delta(a)$ is the sum of all monomials, $a_{v_0}a_{v_1}\cdots a_{v_{N-1}}e\Big(\sum_{r\in\mathbb{Z}_N} r v_r\Big)$ over all sequences of subscripts $(v_0, v_1, \ldots, v_{N-1}) \in \mathbb{Z}_N^N$.

If $(t_0, t_1, \ldots, t_{N-1})$ is a rearrangement of $(v_0, v_1, \ldots, v_{N-1})$ then $a_{t_0}a_{t_1}\cdots a_{t_{N-1}}$ is algebraically the same as $a_{v_0}a_{v_1}\cdots a_{v_{N-1}}$. We wish to collect all such algebraically equal terms into a single term. A sequence of subscripts is therefore naturally a **multiset** since order is immaterial, and multiplicities count.

To distinguish a multiset from a particular sequence defining it, $v = (v_0, v_1, \ldots, v_{N-1})$, say, we shall use the notation $[v]$ for the multiset. Clearly, two multisets are equal iff they have the same elements with the same multiplicities.

To avoid repeated double-subscripts, we shall abbreviate the sequence a_{v_0}, a_{v_1}, …, $a_{v_{N-1}}$ to a_v, and we shall represent the monomial $a_{v_0}a_{v_1}\cdots a_{v_{N-1}}$ by Πa_v. With this new notation, the formula now becomes,

$$\Delta_N(a) \;=\; \sum_{\{[v]\,\vdash\, v\in\mathbb{Z}_N^N\}} \Pi a_v \sum_{\rho} e_N\Big(\sum_{r\in\mathbb{Z}_N} r\rho(v)_r\Big) \quad (5)$$

The ρ summation is over all rearrangements of the sequence v; $\rho(v)$ denotes the rearranged sequence, and $\rho(v)_r$ is the r^{th} component in the rearranged sequence.

Since $[v]$ can have repeated entries, for instance, $v = (0, 0, 0, 1, 1, 4)$, it is not immediately apparent what the set of rearrangements is. Suppose $\rho = (012)$ in cycle notation. Then ρ has no effect on v, merely permuting zeroes in the first three entries. Clearly, all rearrangements of v can be represented by a permutation of the subscripts of v (itself a sequence of subscripts). So, if ρ is any permutation, $\rho : \mathbb{Z}_N \to \mathbb{Z}_N$, then ρ acts on v by:

$$\rho \times v \mapsto (v_{\rho(0)}, v_{\rho(1)}, \ldots, v_{\rho(N-1)})$$

which following the previously introduced convention can be written

$$\rho \times v \mapsto v_\rho$$

Let S_N denote the symmetric group on $\mathbb{Z}_N$. The set of distinct permutations on v corresponds to the set of cosets of the stabilizer subgroup of S_N acting on v through its subscripts. Denote this stabilizer subgroup by $\text{Stab}(v)$ and denote its cardinality by $F(v) := |\text{Stab}(v)|$. Since elements of $\text{Stab}(v)$ leave $e(\sum_r r v_r)$ invariant, it follows that every action of $\rho \in S_N$ on v is one of $F(v)$ permutations which have the same action. Therefore, equation (5) becomes

$$\Delta_N(a) \;=\; \sum_{\{[v]\,\vdash\, v\in\mathbb{Z}_N^N\}} \Pi a_v \frac{1}{F(v)} \sum_{\rho\in S_N} e_N\Big(\sum_{r\in\mathbb{Z}_N} r v_{\rho(r)}\Big)$$

The coefficient of the Πa_v term is therefore,

$$c(v) \;=\; \frac{1}{F(v)} \sum_{\rho \in S_N} e_N\Big(\sum_{r \in \mathbb{Z}_N} \rho(r) v_r \Big) \tag{6}$$

The exponent (argument of $e_N(\cdot)$) has been changed to a more readable form. The change has no effect as ρ is summed over the entire S_N group. The above notation will occur repeatedly in what follows so we provide formal definitions.

10.4.2 **Definition**

(i) Denote by $\mathrm{Stab}(v)$ the group of permutations on the components v which leave v unchanged.

(ii) Define $F(v) := |\mathrm{Stab}(v)|$.

There is a fundamental fact about the determinantal coefficients which can now be proved.

10.4.3 **Proposition** If $c(v) \neq 0$ then $\sum_{r \in \mathbb{Z}_N} v_r \equiv 0 \pmod N$.

Proof. Let $\imath$ be the permutation of $\mathbb{Z}_N$ which increments each residue mod N. That is, $\imath(x) = 1+x \bmod N$. Summing over ρ is the same as summing over $\imath\rho$. Therefore,

$$\begin{aligned} c(v) &= \frac{1}{|F(v)|} \sum_{\rho \in S_N} e\Big(\sum_{r \in \mathbb{Z}_N} \imath\rho(r) v_r \Big) \\ &= \frac{1}{|F(v)|} \sum_{\rho \in S_N} e\Big(\sum_{r \in \mathbb{Z}_N} (1+\rho(r)) v_r \Big) \\ &= e\Big(\sum_{r \in \mathbb{Z}_N} v_r \Big) c(v) \end{aligned}$$

This is possible iff $c(v) = 0$ or $\sum_r v_r \equiv 0 \pmod N$. □

The property of a set of subscripts summing to zero modulo N is a key fact used in the derivation of a formula for the coefficients in Chapter 11.

10.4.4 **Parity Formula** We shall now present a third formula for $\Delta_N(a)$. This one is derived directly from the determinant and is therefore valid over any commutative ring. The formula for expanding the general $N \times N$ determinant $|c_{i,j}|$ by rows and columns is

$$\Delta \;=\; \sum_{\tau \in S_N} (-1)^\tau \prod_{i \in \mathbb{Z}_N} c_{i,\tau(i)}$$

where $\mathbb{Z}_N$ is taken as the index set for both rows and columns, and $(-1)^\tau$ denotes the parity of the permutation $\tau \in S_N$. Substituting values for a circulant determinant, $|a_{j-i}|$, we get

$$\Delta_N(a) \;=\; \sum_{\tau \in S_N} (-1)^\tau \prod_{i \in \mathbb{Z}_N} a_{\tau(i)-i}$$

As before, we rearrange this into algebraic monomials,

$$\Delta_N(a) \;=\; \sum_{[v]} \Pi a_v \sum_{\{\tau \in S_N \vdash [\tau] \equiv [v]\}} (-1)^\tau$$

where $[\tau] := [\tau(0)-0,\ \tau(1)-1,\ \tau(2)-2,\ \ldots,\ \tau(N-1)-(N-1)]$ is the multiset of translations, and the equivalence $[\tau] \equiv [v]$ is modulo N. The above immediately gives the parity formula for the determinantal coefficient.

$$c(v) \;=\; \sum_{\{\tau\in S_N \vdash [\tau]\equiv[v]\}} (-1)^{\tau} \tag{7}$$

Formula (7) provides a reasonably efficient method for calculating all the circulant determinantal coefficients on a computer. However,formula (7) is not practical for calculating individual coefficients as it requires testing $N!$ permutations for each calculation. For single coefficients a recursive algorithm in section 11.2.3 is the simplest for computer calculations, and the coefficient formula of Chapter 11 is amenable to hand reckoning.

10.5.3 **Proposition** If $c(v) \neq 0$ then $[v]$ is the multiset of translations of some permutation of $\mathbb{Z}_N$.

Proof. This is a corollary of the Parity Formula of §10.4.4. □

10.5.4 **When is $c(v)$ non-zero?** We have already shown that if $c(v)$ is non-zero then v is a null multiset. The question is whether the converse is true. It will be shown in Chapter 11 that the converse does hold when N is prime. Even when N is compound Loehr, Warrington, and Wilf ([LWW]), have shown that it holds when

(i) there are only three distinct elements in v,

(ii) v can be transformed by the increment and multiplier maps to a multiset of zeroes, ones, and one other residue.

However, the converse does not always hold as the following examples demonstrate.

Examples

(i) $N = 6,\ v = [0,0,1,3,3,5],\ c(v) = 0$. Note that v is generated by permutations, namely, $\tau = (01)(25)$, and $\tau = (0143)$ in cycle notation.

(ii) $N = 10,\ v = [0,0,0,0,1,1,1,3,6,8],\ c(v) = 0$. Again, v is generated by $\tau = (012)(347)$ and $\tau = (012397)$.

The next proposition could have been proved immediately after Proposition 10.4.3, but with the parity formula in hand, the proof of its first part is slightly easier. Recall that the reverse position multiplier map is the map $\bar{\nu}_h : (a_0, a_1, \ldots, a_{N-1}) \mapsto (a_0, a_h, a_{2h}, \ldots, a_{h(N-1)})$. The effect of $\bar{\nu}_h$ on the monomial Πa_v is to map it to Πa_{hv} where $hv = h(v_0, v_1, \ldots, v_{N-1}) = (hv_0, hv_1, \ldots, hv_{N-1})$. Likewise, the effect of the rotation map σ on Πa_v is to map it to $\Pi a_{\imath v}$ where $\imath$ is the increment map.

10.5.5 **Proposition** Let $\imath$ be the increment map, and let $h \in \mathbb{Z}_N^*$.

(i) $c(\imath v) = (-1)^{N+1} c(v)$

(ii) $c(hv) = c(v)$

Proof.

(i) For the first part, we shall use the parity formula (7). First note that $\langle \imath\tau \rangle_i = \imath\tau(i) - i = \tau(i) + 1 - i$. Secondly, $(\imath \langle\tau\rangle)_i = \imath(\tau(i) - i) = \tau(i) - i + 1 = \langle \imath\tau \rangle_i$. Hence, $[\tau]$ generates $[v]$ iff $[\imath\tau]$ generates $[\imath v]$.

$$c(\imath v) = \sum_{[\tau]=[\imath v]} (-1)^{\tau} = \sum_{[\imath\tau]=[\imath v]} (-1)^{\imath\tau} = (-1)^{\imath} \sum_{[\imath\tau]=[\imath v]} (-1)^{\tau} = (-1)^{\imath} \sum_{[\tau]=[v]} (-1)^{\tau} = (-1)^{\imath} c(v)$$

The parity of the N-cycle $\imath$ is $(-1)^{N+1}$. QED *(i)*

From equation (6),

$$c(hv) \;=\; \frac{1}{F(v)} \sum_{\rho\in S_N} e_N\Big(\sum_{r\in\mathbb{Z}_N} h\rho(r) v_r \Big)$$

Since h is coprime to N, multiplication by h is a permutation of $\mathbb{Z}_N$. Therefore $h\rho$ ranges over all of S_N. Now change the summation variable from ρ to $h\rho$ giving formula (6) for $c(v)$. □

The next proposition is useful for finding divisibility properties of the coefficients.

10.5.6 **Proposition** Let $[v] = [\tau]$. Then $[v]$ is also generated by every permutation in the set $\{\tau^\alpha \vdash \alpha \in \langle \iota, \kappa \rangle\}$ where $\iota, \kappa : \mathbb{Z}_N \to \mathbb{Z}_N$ are maps given by $\iota : x \mapsto x+1$, and $\kappa : x \mapsto -x^{-1}$.

Proof. Very easy. □

10.6 Upper-Bounds on $|\Delta(a)|$.

Since there is no simple computational formula for $\Delta(a)$, it is often convenient to have instead a simple upper-bound on $|\Delta(a)|$. The goal of this section is derive two upper-bounds and compare them. It turns out to be much easier to derive the upper-bounds than to decide which is the better (that is, lower) bound. The first upper-bound is the simpler and the easiest to derive, but the second is more constraining, though we do not demonstrate this here.

10.6.1 **Theorem** Let $a \in \mathbf{circ}_N(\mathbb{R})$. Then, $|\Delta(a)| \le d^N$ where $d = \sqrt{\sum_{i \in \mathbb{Z}_N} a_i^2}$.

Proof. Let $A = \mathrm{CIRC}_n(a)$. Now, $\det(A)$ is the Jacobian of the transformation $A : \mathbb{R}^N \to \mathbb{R}^N$. Therefore, N-dimensional volumes are increased by the factor of $|\det(A)|$. Since $\{\mathrm{u}^i : i \in \mathbb{Z}_N\}$ is an orthonormal basis for $\mathbb{R}^N$, the volume spanned by these vectors equals 1. So what we need is an estimate of the volume enclosed by the transformed vectors $A\mathrm{u}^i$.

Let $\vec{v}_i = A\mathrm{u}^i$, then $\vec{v}_i = (a_i, a_{i-1}, a_{i-2}, \ldots, a_{i+1})^T$. Let V denote the volume spanned by the hyper-parallelepiped $\{\vec{v}_0, \vec{v}_1, \ldots, \vec{v}_{N-1}\}$. The volume of V cannot exceed the volume enlosed by orthogonal vectors of lengths $\{|\vec{v}_0|, |\vec{v}_1|, \ldots, |\vec{v}_{N-1}|\}$. Therefore,

$$|\det(A)| \;=\; |V| \;\le\; \prod_{i=0}^{N-1} |\vec{v}_i| \;=\; \prod_{i=0}^{N-1} \sqrt{\sum_{j \in \mathbb{Z}_N} a_j^2} \;=\; \left(\sum_{j \in \mathbb{Z}_N} a_j^2 \right)^{\frac{1}{2}N} \qquad \square$$

The next theorem provides a different bound on $|\Delta(a)|$. The new bound is not as simple as that of Theorem 10.6.1, nor is it quite as easy to derive.

10.6.2 **Theorem** Let $a \in \mathbf{circ}_N(\mathbb{R})$. Let $d^2 = \sum_{i \in \mathbb{Z}_N} a_i^2$. Then,

$$|\Delta(a)| \;\le\; \begin{cases} |\lambda_0| \left(\dfrac{Nd^2 - \lambda_0^2}{N-1} \right)^{\frac{1}{2}(N-1)} & \text{if } N \text{ is odd} \\ \left| \lambda_0 \lambda_{\frac{1}{2}N} \right| \left(\dfrac{Nd^2 - \lambda_0^2 - \lambda_{\frac{1}{2}N}^2}{N-2} \right)^{\frac{1}{2}N-1} & \text{if } N \text{ is even} \end{cases}$$

Proof. First we estimate the sum of all pairs $\lambda_i \lambda_{-i}$.

$$\sum_{k \in \mathbb{Z}_N} \lambda_k \lambda_{-k} \;=\; \sum_{k \in \mathbb{Z}_N} \left(\sum_{i \in \mathbb{Z}_N} a_i \zeta^{ki} \right) \left(\sum_{j \in \mathbb{Z}_N} a_j \zeta^{-kj} \right) \;=\; \sum_{i \in \mathbb{Z}_N} \sum_{j \in \mathbb{Z}_N} a_i a_j \sum_{k \in \mathbb{Z}_N} \zeta^{k(i-j)} \;=\; N \sum_{i \in \mathbb{Z}_N} a_i^2$$

$$\therefore \;\; \sum_{k \in \mathbb{Z}_N} |\lambda_k|^2 \;=\; Nd^2$$

Case I. N is odd. In the above sum, each eigenvalue except λ_0 is counted twice.

$$\therefore \;\; \lambda_0^2 \;+\; 2 \sum_{k=1}^{\frac{1}{2}(N-1)} |\lambda_k|^2 \;=\; Nd^2$$

On the other hand, the determinant, Δ, is given by

$$\frac{\Delta}{\lambda_0} \;=\; \prod_{j=1}^{N-1} \lambda_j \;=\; \prod_{j=1}^{\frac{1}{2}(N-1)} |\lambda_i|^2$$

The geometric mean of non-negative reals cannot exceed the arithmetic mean. Therefore,

$$\left|\frac{\Delta}{\lambda_0}\right|^{\frac{2}{N-1}} \;=\; \left(\prod_{j=1}^{\frac{1}{2}(N-1)} |\lambda_i|^2\right)^{\frac{2}{N-1}} \;\leq\; \frac{2}{N-1} \sum_{k=1}^{\frac{1}{2}(N-1)} |\lambda_i|^2 \;\doteq\; \frac{2}{N-1}\left(\tfrac{1}{2}\, Nd^2 - \tfrac{1}{2}\,\lambda_0^2\right)$$

$$\therefore\; |\Delta| \;\leq\; |\lambda_0| \left(\frac{Nd^2 - \lambda_0^2}{N-1}\right)^{\frac{1}{2}(N-1)}$$

This completes the proof for N odd. QED(Case I).

Case II. N is even. In this case, there are two real eigenvalues, so

$$\lambda_0^2 \;+\; \lambda_{\frac{1}{2}N}^2 \;+\; 2 \sum_{k=1}^{\frac{1}{2}N-1} |\lambda_k|^2 \;=\; Nd^2$$

Now we estimate instead

$$\frac{\Delta}{\lambda_0 \lambda_{\frac{1}{2}N}} \;=\; \prod_{k=1}^{\frac{1}{2}N-1} |\lambda_i|^2$$

Applying the principle of the geometric mean $\leq$ arithmetic mean again gives the formula of the theorem statement. □

10.6.3 Relative Merits of the Two Bounds.

The bound of Theorem 10.6.1 can be improved if it is known that two vectors $\vec{v}_i = A\mathrm{u}^i$ and $\vec{v}_j = A\mathrm{u}^j$ are close to parallel and their mutual angle can be estimated. (The bound was derived on the worst-case assumption that all vectors $\vec{v}_k$ were orthogonal.) The bound of Theorem 10.6.2 can be improved if $|\lambda_i|$ can be estimated for some i, particularly if the value is close to zero.

It is not immediately apparent which of the two bounds is the best, that is, the lowest. In fact the bound of Theorem 10.6.2 is always at least as good as the bound of Theorem 10.6.1. Ironically, probably the easiest way of demonstrating this is to show that the bound of Theorem 10.6.1 implies that of Theorem 10.6.2. Here is the idea. We add an arbitrary constant to every entry in the circulant vector; so $(a_0, a_1, \ldots, a_N) \mapsto (a_0{+}x, a_1{+}x, \ldots, a_{N-1}{+}x) = a'$, say, This affects only λ_0 leaving all other eigenvalues unchanged. So the determinant of a' is easily computed given the determinant of a. We then use the bound of Theorem 10.6.1 to bound $\det(a')/\lambda_0(a')$ and find the lowest possible value of this by finding its stationary point. But, $\det(a')/\lambda_0(a') = \det(a)/\lambda_0(a)$; so we obtain a new bound on $\det(a)$. The best possible bound over all $x \in \mathbb{R}$ is actually the bound of Theorem 10.6.2!

Bounds on the circulant determinant are important in the theory cyclotomic integers. Suppose momentarily that $N = p$, an odd prime, and that $a \in \mathbf{circ}_p(\mathbb{Z})$. Let $\xi = \lambda_1(a)$, then ξ is an algebraic integer in the domain $\mathbb{Z}(\zeta_p)$. The algebraic norm $\mathcal{N}(\xi)$ of ξ is the product of all algebraic conjugates of ξ. Hence, $\Delta(a) = \lambda_0(a)\mathcal{N}(\xi)$, and so, if given $\lambda_0(a) \neq 0$, a bound on the determinant implies a bound on the norm of ξ, and vice versa. Indeed, assuming $\lambda_0 \neq 0$, the bound Theorem 10.6.2 immediately gives the following bound on the norm:

$$\mathcal{N}(\xi) \;\leq\; \left(\frac{Nd^2 - \lambda_0^2}{p-1}\right)^{\frac{1}{2}(p-1)} \qquad \text{where } d^2 = \sum a_i^2$$

Kummer derived this same bound for the norm using essentially the same argument as we used to derive the bound of Theorem 10.6.2, and with this bound was able to show that the class group of the p^{th} cyclotomic field is finite.

Chapter 11.
Formula for Determinantal Coefficients of Circulant Matrices.

There is a closed formula for the circulant determinantal coefficients which will be derived and proved in this chapter. We offer first a proof by Oystein Ore, and then a new proof of our own. Our proof is rather lengthy, but has some advantages over Ore's derivation as will be discussed.

The determinant of $\mathbf{circ}_n(a)$ can be expanded as a homogenous expression of degree n in the variables $a_0, a_1, \ldots, a_{n-1}$. Thus, we define the circulant determinantal coefficient to be $c_n(v_0, v_1, \ldots, v_{n-1})$ in the following expansion.

$$\det \mathbf{circ}(a_0, a_1, \ldots, a_{n-1}) \;=\; \sum_{v_0 \le v_1 \le \cdots \le v_{n-1}} c_n(v_0, v_1, \ldots, v_{n-1})\; a_{v_0} a_{v_1} \cdots a_{v_{n-1}}$$

The coefficient $c_n(v)$ is a function of the multiset of subscripts appearing in the monomial $\Pi a_v := a_{v_0} a_{v_1} a_{v_2} \cdots a_{v_{n-1}}$ which we write more briefly as $\Pi a_{[v]}$. To state the formula for $c_n(v)$, we need to introduce some notation.

11.1 Notation of the Main Theorem

Let N be the order of the circulant determinant to be expanded.

We regard the subscripts $v_0, v_1, \ldots$ as residues modulo N, and we take the set of residues to be $\{0, 1, 2, \ldots, N-1\}$ which we denote by $\mathbb{Z}_N$.

Given a sequence $v = (v_0, v_1, \ldots, v_{n-1})$. Then, $[v] = [v_0, v_1, \ldots, v_{n-1}]$, denotes the multiset of the elements of v. The symbol $|v|$ denotes the length of the sequence or of its multiset; in this case, $|v| = n$. For $n \le N$, $\bar{v}$ is defined to be $(v_0, v_1, \ldots, v_{n-1}, 0, \ldots, 0)$ which is the sequence v extended by $N - n$ zeroes, so that $|\bar{v}| = N$.

We shall call a sequence v or its multiset $[v]$ a *null multiset* if the sum of its elements is zero (mod N). $\mathcal{P}_0[v]$ denotes the set of partitions of a multiset $[v]$ into null multisets.

For any sequence $w = (w_0, w_1, \ldots)$ of arbitrary objects, we let $F(w)$ denote the order of the group of permutations on the subscripts of w which leave w invariant. $F(w)$ equals $a!\, b! \cdots$ where $a, b, \ldots$ are the multiplicities of the elements in $[w]$.

11.2 Statement of the Main Theorem

Let $\bar{v}$ be a sequence of N subscripts, and let $c(\bar{v})$ be the coefficient of $\Pi a_{\bar{v}}$ in the expansion of $\det \mathbf{circ}_N(a)$. Let v be the sub-sequence of $\bar{v}$ consisting of its non-zero entries. Then,

$$c(\bar{v}) \;=\; (-1)^{|v|} \sum_{[W] \in \mathcal{P}_0[v]} \frac{(-N)^{|W|}}{F(W)} \prod_{[w] \in [W]} \frac{(|w|-1)!}{F(w)} \tag{1}$$

11.2.1 An Example

We illustrate the use of the theorem with an example. Let us compute the coefficient of $a_0^2 a_1^4 a_3 a_7 a_8^2$ in the expansion of the general 10×10 circulant determinant. This is a calculation that would otherwise be practical only by computer.

In the notation of the theorem, we have $N = 10$, and

$$\bar{v} \;=\; (0, 0, 1, 1, 1, 1, 3, 7, 8, 8)$$

$$v \;=\; (1, 1, 1, 1, 3, 7, 8, 8)$$

The computation of the coefficient is summarized in Table 1 below which shows all partitions in $\mathcal{P}_0[v]$. Partitions consisting of two multisets contribute to N^2, those of three multisets contribute to N^3 etc., in accordance with formula (1).

Table 1. Computation of $c(v)$.

Part $\overset{\text{n}}{\cdot\cdot}$	Null Multisets	$\frac{(-1)^{\lvert W\rvert}}{F(W)} \times \prod_{[w]\in[W]} \frac{(\lvert w\rvert-1)!}{F(w)}$		$N^{\lvert W\rvert}$
P_1	[3 7], [1 1 8], [1 1 8]	$-\frac{1}{2!} \times \frac{(2-1)!}{1}\left(\frac{(3-1)!}{2!}\right)^2$	$=-0.5$	N^3
P_2	[1 1 1 7], [1 3 8 8]	$1 \times \frac{(4-1)!}{3!}\frac{(4-1)!}{2!}$	$=3$	N^2
P_3	[3 7], [1 1 1 1 8 8]	$1 \times \frac{(2-1)!}{1}\frac{(6-1)!}{4!2!}$	$=2.5$	N^2
P_4	[1 1 8], [1 1 3 7 8]	$1 \times \frac{(3-1)!}{2!}\frac{(5-1)!}{2!}$	$=12$	N^2
P_5	[1 1 1 1 3 7 8 8]	$-1 \times \frac{(8-1)!}{4!2!}$	$=-105$	N
	Total	$-105N \ + \ 17.5N^2 \ - \ 0.5N^3$		

$$\therefore\ c(v) \ = \ (-1)^8(-105N \ + \ 17.5N^2 \ - \ 0.5N^3) \ = \ 200$$

(There is an algorithm, illustrated in §5(18), which may be used to check this result.)

11.3 **Remarks Concerning Zero Subscripts** Formula (1) requires that v contain only the non-zero elements of $\bar{v}$. The more general version of the theorem in §11.12.1 allows v to contain none, some, or all the zeroes in $\bar{v}$.

We shall use $c(\bar{v})$ interchangeably with $c(v)$. It turns out that the zero subscripts are in a sense irrelevant.

11.4 **The Zero Set Formula.** A proof of the main theorem proceeds by first proving a special form called the Zero Set Formula. The main theorem is then deduced by converting the formula from one involving zero sets to one involving multisets. A zero set is defined as follows:

11.5 **Definition of Zero Set and Zero Set Partition**

For the remainder of this chapter, we shall denote $|v|$ by n.

Let I_n be the set of subscripts appearing in v (in practice, either $I_n = \{0, 1, \ldots, n-1\}$ or $I_n = \{1, 2, \ldots, n\}$).

(i) For any $S \subset I_n$, we define $v:S = \{v_i \vdash i \in S\}$.

(ii) We shall say that S is a zero set on v in the case that $v:S$ is a null multiset.

(iii) Define $\mathcal{P}_0(v)$ to be any partition of I_n such that $v:P$ is a null multiset for every $P \in \mathcal{P}_0(v)$.

11.5.1 **Examples**

(i) Consider $v = (1, 2, 2, 3, 0, 0)$ with $N = 6$. Then, $S_1 = \{0, 1, 3, 5\}$ and $S_2 = \{0, 2, 3, 4\}$ are two distinct zero sets on v, but the null multisets $v:S_1$ and $v:S_2$ are indistinguishable and therefore equal. Note that if v is a null multiset of n elements, then $\mathbb{Z}_n$ is a zero set.

(ii) Let $v = (2, 3, 5, 6),\ N = 8$. Then, $P_1(v) = \{\{0, 3\},\ \{1, 2\}\}$ and $P_2(v) = \{\{0, 1, 2, 3\}\}$ are all the zero-set partitions. They correspond 1-1 to the multiset partitions, $P_1[v] = \big[\,[2, 6],\, [3, 5]\,\big]$ and $P_2[v] = \big[\,[2, 3, 5, 6]\,\big]$ of v.

(iii) Let $v = (1, 1, 2, 2, 4),\ N = 5$. There are the three zero-set partitions: $P_1(v) = \{\{0, 4\},\ \{1, 2, 3\}\}$, $P_2(v) = \{\{1, 4\},\ \{0, 2, 3\}\}$, and $P_3(v) = \{\{0, 1, 2, 3, 4\}\}$, but only two multiset partitions: $P_1[v] = \big[\,[1, 4],\, [1, 2, 2]\,\big]$ and $P_3[v] = \big[\,[1, 1, 2, 2, 4]\,\big]$.

Zero sets allow us to differentiate between like elements of a multiset, and for some mysterious reason drawing such arbitrary distinctions seems necessary to proving the main theorem.

11.6 Ore's Proof of the Zero Set Formula

The Zero Set Formula was first published by Oystein Ore ([Ore]) in 1951. However, Ore's derivation of the formula is telegraphic in the extreme, and requires some interpretation. We provide here an expanded version of Ore's result written using our notation. The general Zero Set Formula allows any number of zeroes in v, the special version proved by Ore assumes v has no zeroes.

11.6.1 **Theorem (Special Form of the Zero Set Formula)** Let v be the sequence of all non-zero subscripts in $\bar{v}$, and let $|v| = n$. Then,

$$c_{N}(\bar{v}) \quad = \quad (-1)^{n}\ F(v)^{-1} \sum_{P \in \mathcal{P}_0(v)} (-N)^{|P|} \prod_{S \in P} (|S|-1)!$$

Proof. (Based on [Ore]).

The eigenvalue formula (Corollary 1.11.2) for the circulant determinant gives

$$\det \mathbf{circ}(a) \ = \prod_{i \in \mathbb{Z}_N} \left(a_0 + a_1\zeta^{i} + a_2\zeta^{2i} + \cdots + a_j\zeta^{ij} + \cdots + a_{N-1}\zeta^{i(N-1)}\right) \tag{2}$$

where $1 = \zeta^0, \zeta, \zeta^2, \ldots, \zeta^{N-1}$ are the N^{th} roots of unity.

Pick a sequence of a_i's, one from each factor of equation (2). Let us suppose that the sequence is $a_0^{N-n} a_{v_1} \cdots a_{v_n}$. (Remember that $v_n = v_0$ if $n = N$.) The coefficient of this particular sequence is

$$\zeta^{1v_1} \cdot \zeta^{2v_2} \cdots \zeta^{n \cdot v_n}$$

(We do not consolidate the powers for reasons that will become plain.)

If $(\bar{t}_0, \bar{t}_1, \ldots, \bar{t}_{N-1})$ is a rearrangement of $(\bar{v}_0, \bar{v}_1, \ldots, \bar{v}_{N-1})$ (with $N-n$ zeroes in both sequences), then $a_0^{N-n} a_{t_1} a_{t_2} \cdots a_{t_n}$ is algebraically the same as $a_0^{N-n} a_{v_1} a_{v_2} \cdots a_{v_n}$. We collect all such algebraically equal terms and obtain

$$\det \mathbf{circ}_{N}(a) \ = \sum_{\{[v] \vdash v \in \mathbb{Z}_N^n\}} \Pi a_v \sum_{\rho \in R(\bar{v})} \zeta^{1\bar{v}_{\rho(0)}} \cdot \zeta^{2\bar{v}_{\rho(1)}} \cdots \zeta^{(N-1)\bar{v}_{\rho(N-1)}} \tag{3}$$

The first summation is over all distinct multisets which can be constructed from arbitrary sequences of n residues modulo N. The second summation is over all distinct rearrangements ρ of the sequence $\bar{v}$, a set which we denote by $R(\bar{v})$. The term $\bar{v}_\rho$ denotes the rearranged sequence, and $\bar{v}_{\rho(r)}$ is the r^{th} component in the rearranged sequence.

The set $R(\bar{v})$ is defined only to within products by permutations in $F_{\bar{v}}$, the stabilizer subgroup of $\bar{v}$ in the full symmetric group S_N on $\bar{v}$. Since permutations act on $\bar{v}$ from the left, $R(\bar{v}) = S_N \backslash F_{\bar{v}}$. A coset in R is fully specified by the resulting sequence of values $\bar{v}_\rho$ where ρ is a representative permutation in the coset.

By definition of the circulant determinantal coefficient,

$$\det \mathbf{circ}_{N}(v) \ = \sum_{0 < v_1 \le v_2 \le \cdots \le v_n} c_{N}(v_1, v_2, \ldots, v_n)\ a_0^{N-n} a_{v_1} \cdots a_{v_n} \tag{4}$$

From (4) and (3), we have

$$\begin{aligned} c(v_1, v_2, \ldots, v_n) \ &= \sum_{\rho \in R(\bar{v})} \zeta^{1\bar{v}_{\rho(1)}} \cdot \zeta^{2\bar{v}_{\rho(2)}} \cdots \zeta^{(N-1)\bar{v}_{\rho(N-1)}} \\ &= \sum_{\tau \in R(\bar{v})} \zeta^{\tau(1)\bar{v}_1} \cdot \zeta^{\tau(2)\bar{v}_2} \cdots \zeta^{\tau(N-1)\bar{v}_{(N-1)}} \\ &= \sum_{\tau \in R(\bar{v})} \zeta^{\tau(1)v_1} \cdot \zeta^{\tau(2)v_2} \cdots \zeta^{\tau(n)v_n} \end{aligned} \tag{5}$$

In the second summation, we reordered the powers of ζ, sorting them left to right by the subscript on $\bar{v}$, and we then set $\tau = \rho^{-1}$. In the last summation, we omitted all zero values of $\bar{v}$, leaving only the non-zero elements $v_1, v_2, \ldots, v_n$.

To see how to proceed, suppose initially that $v_1, v_2, \ldots, v_n$ are distinct. Then, cosets of $F_{\bar{v}}$ correspond to maps $I_n = \{1, 2, , \ldots, n\} \to \mathbb{Z}_N$. Applying this to formula (5), we see that the sequence $(\zeta^{\tau(1)}, \zeta^{\tau(2)}, \ldots, \zeta^{\tau(n)})$ can be any sequence of n distinct N^{th} roots of unity. Thus we see that in this case, the formula for the coefficients assumes a highly symmetric form:

$$c(v_1, v_2, \ldots, v_n) \;=\; \sum_{\substack{\zeta_i^N = 1 \\ \zeta_i \text{ distinct}}} \zeta_1^{v_1} \cdot \zeta_2^{v_2} \cdots \zeta_n^{v_n} \tag{6}$$

To see a general pattern, consider how formula (6) develops for low n.

$$c(v_1) \;=\; \sum_i (\zeta^i)^{v_1} \tag{7a}$$

$$c(v_1, v_2) \;=\; \sum_{i \neq j} (\zeta^i)^{v_1} (\zeta^j)^{v_2} \;=\; c(v_1)c(v_2) - c(v_1 + v_2) \tag{7b}$$

$$c(v_1, v_2, v_3) \;=\; c(v_1)c(v_2)c(v_3) - c(v_1)c(v_2{+}v_3) - c(v_2)c(v_1{+}v_3) - c(v_3)c(v_1{+}v_2) + 2c(v_1{+}v_2{+}v_3) \tag{7c}$$

It is clear that at least when $v_1, v_2, \ldots, v_n$ are distinct that the coefficient $c(v)$ can be reduced to a series of products of power sums over N^{th} roots of unity.

We now suppose that $v_1, v_2, \ldots, v_n$ contains duplicates. Suppose $v_1 = v_2$, then formula (6) becomes

$$c(v_1, v_1, v_3, \ldots, v_n) \;=\; \sum_{\substack{\zeta_i^N = 1 \\ \zeta_i \text{ distinct} \\ \zeta_1 \prec \zeta_2}} \zeta_1^{v_1} \cdot \zeta_2^{v_1} \cdot \zeta_3^{v_3} \cdots \zeta_n^{v_n}$$

where "$\prec$" denotes any well-ordering of the N^{th} roots of unity. In the simplest case, $n = 2$, $v = (a, a)$, we have

$$c(a, a) \;=\; \sum_{0 \leq i < j < N} (\zeta^i)^a (\zeta^j)^a$$

There is a decomposition along the lines of (7b) for $c(a, a)$; it is

$$c(a, a) \;=\; \tfrac{1}{2}\left(c(a)^2 - c(2a)\right) \tag{7d}$$

This is essentially the decomposition of (7b) but divided by $|F_v| = F(v) = 2!$.

The general method of decomposing $c(v_1, v_2, \ldots, v_n)$ appears to be:

(i) Take the leading term to be $c(v_1)c(v_2)\cdots c(v_n)$. We regard this product as a sum over an n-dimensional cube situated at $(0, 0, \ldots, 0)$, the i^{th} side lying along a coordinate which is graduated by the N roots of unity raised to the power of v_i. Each point inside the cube has the value of the product of the coordinate values.

(ii) We remove all diagonal lines, planes, and hyperplanes from the cube by substracting $c(v_1)c(v_2 + \cdots + v_n)$, $c(v_1)c(v_2)c(v_3 + \cdots + v_n)$ etc. with proper adjustments for intersections.

(iii) If x occurs in v with multiplicity k. Then, we regard $c(x)^k$ as a sum over Δ, a k-dimensional simplex in the k-dimensional cube. The simplex Δ is such that permutations of the coordinates applied to Δ tesselate the cube (minus the removed hyperplanes). Thus, when $k = 2$, the simplex is a triangle, and is $1/2$ the area of the square without its diagonal; when $k = 3$, the simplex is a tetrahedron and is $1/6^{\text{th}}$ the volume of the cube without its main diagonals and diagonal planes, etc.

According to Ore, the general result of this process was found by Faà di Bruno ([FB]) and is described as follows.

Let α denote any root of an arbitrary polynomial, $q(x)$, say, of degree N. Define a symmetric function

$$s_{v_1,v_2,\ldots,v_n}(\alpha) \;:=\; \sum \alpha_1^{v_1}\alpha_2^{v_2}\cdots\alpha_n^{v_n} \tag{8}$$

where the sum is extended over all possible sets of distinct $\alpha_1, \alpha_2, \ldots, \alpha_n$ taken from the roots of q. In the event that two or more v_i's are the same, then it is to be understood that their roots be taken in one combination only. As in equations (7a) -(7d), $s_{v_1,v_2,\ldots,v_n}(\alpha)$ can be expressed in terms of $s_t(\alpha)$ where t is an integer; in other words, in terms of sums of the t^{th} powers of the roots of q.

Consider a partition of the set $I_n = \{1, 2, \ldots, n\}$; let us say it is $\mathcal{P} = \{P_1, P_2, \ldots, P_m\}$. We let $p_i = |P_i|$. Thus, $p_1 + p_2 + \cdots + p_m$ is a partition of n.

This partition of I_n implies a multiset partition of the multiset $[v]$.

$$[v] \;=\; [v\!:\!P_1] \;+\; [v\!:\!P_2] \;+\; \cdots \;+\; [v\!:\!P_m]$$

We now fix the integers $p_1, p_2, \ldots, p_m$ and we define

$$A(p) \;:=\; \sum_{\mathcal{P}} s_{\sigma_1}(\alpha)s_{\sigma_2}(\alpha)\cdots s_{\sigma_m}(\alpha)$$

where the sum extends over all partitions $\mathcal{P}$ of I_n into subsets of sizes $p_1, p_2, \ldots, p_m$, and if we suppose $\mathcal{P} = \{P_1, P_2, \ldots, P_m\}$, then $\sigma_i := \sum v\!:\!P_i$, is the sum of all elements in the subsequence $v\!:\!P_i$.

Then, Faà di Bruno's formula gives

$$s_{v_1,v_2,\ldots,v_n}(\alpha) \;=\; \frac{1}{F(v)}\sum_{p}(-1)^{r+m}(p_1-1)(p_2-1)\cdots(p_m-1)A(p)$$

where the sum is over all partitions of $n = p_1 + p_2 + \cdots + p_m$.

We now take the roots α to be the N^{th} roots of unity. Then,

$$s_t \;=\; \begin{cases} N & \text{if } t \equiv 0 \pmod N \\ 0 & \text{otherwise} \end{cases}$$

Thus, we need only consider zero set partitions of I_n, and each set in such a partition contributes exactly a factor of N to $A(p)$, giving the formula of the theorem. □

11.7 **Criticism of the Ore Proof.** Ore found the correct formula for the circulant determinantal coefficient after many before him failed. However, his proof leaves much, indeed too much, to the imagination of the reader. Strictly speaking, Ore proved the formula only in the case of distinct $v_1, v_2, \ldots, v_n$, leaving it entirely to the reader to determine how to proceed in the more general, and indeed, the more difficult case.

Secondly, the proof depends critically on a theorem of Faà di Bruno, a theorem which appeared in a book published in 1881 which is now almost unobtainable outside of Germany. Ordinarily, this would present no difficulties since conventionally a theorem of such critical importance to a proof would be quoted in full. However, Ore did not quote the theorem at all, and as a result, short of visiting a German reference library, and obtaining a translation of the entire book (since no page numbers are given in the reference), it is impossible to verify whether the Faà di Bruno theorem is being correctly used, especially in the case where $v_1, v_2, \ldots, v_n$ are not all distinct.

11.8 New Proof of the Zero Set Formula

For the above reasons, we present an alternative proof of the Zero Set Formula. The proof is self-contained and so is significantly longer than the one above. As a side benefit, a technique will be introduced that can have wider application to evaluating functions defined on permutation groups.

We shall re-derive the Phase Formula of §10.4.1. We now identify our set of subscripts, I_n, with the set $\{0,1,2,\ldots,n-1\} = \mathbb{Z}_n$. Thus, v will now be the sequence $v = (v_0, v_1, \ldots, v_{n-1})$. Also, to avoid subscripting superscripts, we shall denote ζ^x by $e(x)$ as we did in §10.4.

Formula (5) becomes

$$c(v) \;=\; \sum_{\tau \in R(\bar{v})} e\left(\sum_{i\in\mathbb{Z}_n} \tau(i)v_i\right)$$

We can view $R(\bar{v})$ as a transversal in S_N for $S_N \backslash F_{\bar{v}}$. The summand is independent of the choice of representative, τ, from its $F_{\bar{v}}$-coset, $\tau F_{\bar{v}}$. We use this fact to change the summation range to the whole of S_N and compensate by dividing by $F(\bar{v}) = |F_{\bar{v}}|$.

$$c(v) \;=\; \frac{1}{F(\bar{v})} \sum_{\tau \in S_N} e\left(\sum_{i\in\mathbb{Z}_n} \tau(i)v_i\right) \tag{9}$$

We reiterate the fundamental fact that the only non-zero determinantal coefficients are those of null multisets.

10.4.3 **Proposition** If $c(v) \neq 0$ then $\sum_{r\in\mathbb{Z}_N} v_r \equiv 0 \pmod{N}$. □

11.8.1 **Definition** For $n \leq N$, define Z_0^n to be the set of sequences of length n summing to 0 (mod N), in other words, the set of all sequences of length n that are null multisets.

Because of the proposition, we shall henceforth assume that $v \in Z_0^n$.

11.9 Evaluation of the Phase Formula.

One of the problems in evaluating formula (9) is the question of how to sum over all permutations of $\mathbb{Z}_N$. We can represent the general permutation in S_N as a vector of N general but distinct residues from $\mathbb{Z}_N$. Then, we need to sum the exponential in formula (9) over the set of vectors having distinct components. These considerations lead to the next definitions.

11.9.1 **Definition**

(i) Define $D_n \subset \mathbb{Z}_N^n$ to be the set of all sequences of n distinct residues modulo N.

(ii) For any subset X of $\mathbb{Z}_N^n$, and $v \in Z_0^n$ define

$$C(X,v) \;:=\; \sum_{r\in X} e_N\left(\sum_{i=0}^{n-1} r_i v_i\right)$$

We restate formula (9) using these definitions.

11.9.2 **Lemma** Let $v \in Z_0^n$. Then,

$$c(v) \;=\; \frac{(N-n)!}{F(\bar{v})}\, C\left(D_n,\, v\right) \;=\; \frac{C\left(D_n,\, v\right)}{F(v)}$$

Proof. The final expression for $c(v)$ follows from the middle expression due to the fact that $F(\cdot)$ is reduced by $(N-n)!$ by the removal of $N-n$ zeroes from $\bar{v}$.

From formula (9), we have

$$F(\bar{v})c(v) \;=\; \sum_{\rho\in S_N} e_N\left(\sum_{i=1}^{n}\rho(i)v_i\right)$$

Therefore, only n values of ρ contribute to the sum. Fix these n values, $\rho(i)=r_i$, say, for $0\le i\le n-1$. There is a free choice on the remaining $N-n$ values. Given that ρ is a permutation, we get a total of $(N-n)!$ choices. Therefore, we can sum first over the possible choices for $\{r_i \vdash 0\le i\le n-1\}$, and then over all permutations which satisfy $\rho(i)=r_i$. Thus,

$$F(\bar{v})c(\bar{v}) \;=\; \sum_{r\in D_n}\sum_{\substack{\rho\in S_N\\ \rho(i)=r_i}} e\Big(\sum_{i=0}^{n-1}\rho(i)v_i\Big) \;=\; (N-n)!\sum_{r\in D_n} e\Big(\sum_{i=0}^{n-1}r_iv_i\Big)$$

$$=\; (N-n)!\,C\left(D_n,\,v\right)\;\square$$

The immediate goal will be to find a formula for $C\left(D_n,v\right)$ and then use the above lemma to deduce the formula for $c(\bar{v})$. To this end, we would like to find a decomposition of the space D_n into spaces of lower dimension which would open the way to an inductive method of evaluating $C(D_n,v)$. This is provided by the next lemma.

11.9.3 **Lemma** Decomposition of D_n.

(i) $\quad D_n \;=\; D_n^* \;-\; \bigcup_{i=0}^{n-2} D_{n-1}^{(i)}$

$$\text{where } D_n^* \;=\; \{(r_0,r_1,\ldots,r_{n-1})\in\mathbb{Z}_N^n \vdash (r_0,r_1,\ldots,r_{n-2})\in D_{n-1}\}$$
$$=\; D_{n-1}\times\mathbb{Z}_N$$

$$\text{and } D_{n-1}^{(i)} \;=\; \{(r_0,r_1,\ldots,r_{n-1})\in\mathbb{Z}_N^n$$
$$\vdash\; (r_0,r_1,\ldots,r_{n-2})\in D_{n-1},\; r_i=r_{n-1}\},\quad \text{for } i=0,\ldots,n{-}2$$

(ii) $\quad D_{n-1}^{(i)}\cap D_{n-1}^{(j)} \;=\; \emptyset \quad$ for $i\ne j$.

Proof. D_n^* is just D_n except that the last component is allowed to roam freely over $\mathbb{Z}_N$. The sets $D_{n-1}^{(i)}$ must be subtracted because the last component of vectors in D_n must be distinct from all other components. Hence, part *(i)* will follow from part *(ii)* since part *(ii)* implies that adjustments from intersection terms are not required.

To see part *(ii)*, let $r^{(i)}\in D_{n-1}^{(i)}$, and $r^{(j)}\in D_{n-1}^{(j)}$ where $0\le i\ne j\le n-2$. The first $n-1$ components of $r^{(j)}$ are distinct. $\therefore\, r_i^{(j)}\ne r_j^{(j)}$ But, $r_j^{(j)}=r_{n-1}=r_i^{(i)}$. Therefore, $r_i^{(j)}\ne r_i^{(i)}$. That is, $r^{(j)}$ and $r^{(i)}$ differ at their i^{th} components. $\square$

We can apply this lemma to reduce $C(D_n,v)$, but first we need a method of converting sums over $D_{n-1}^{(i)}$ to sums over D_{n-1}. This will then allow an inductive argument. To see the essential idea, let $v\in Z_0^n$, and consider the sum

$$C\left(D_n^{(i)},v\right) \;=\; \sum_{r\in D_{n-1}^{(i)}} e_N\left(\sum_{k=0}^{n-1}r_kv_k\right)$$

The vector r appearing in the inner sum is a member of $D_n^{(i)}$, and so satisfies $r_i=r_{n-1}$. The inner sum is

$$\sum_{k=0}^{n-1}r_kv_k \;=\; \sum_{k=0}^{n-2}r_kv_k+r_iv_{n-1} \;=\; \sum_{k=0}^{n-2}r_kv_k^{(i)}$$

where the vector $v^{(i)}$ is in Z_0^{n-1} and has the same components as v except the i^{th} component is $v_i + v_{n-1}$ and the n^{th} component has been omitted. Since the last component of r has been dropped, there are no restrictions on the remaining $n-1$ components of r except that they must be distinct; that is, $(r_1, r_2, \ldots, r_{n-1}) \in D_{n-1}$. This shows that a simple transformation on v can change a sum over $D_n^{(i)}$ into a sum over D_{n-1}. This motivates the following definition.

11.9.4 **Definition** For $v \in Z_0^n$, define $v^{(i)} \in Z_0^{n-1}$, called the *collapse* of v on i, by

$$v_j^{(i)} := \begin{cases} v_j + v_{n-1} & \text{if } j = i \\ v_j & \text{otherwise} \end{cases}$$

11.9.5 **Lemma** Let $v \in Z_0^n$.

$$C\left(D_n,\, v\right) \quad = \quad \begin{cases} -\displaystyle\sum_{i=0}^{n-2} C\left(D_{n-1},\, v^{(i)}\right) & \text{if } v_{n-1} \not\equiv 0 \pmod N \\ \\ (N-n+1)\, C\left(D_{n-1},\, v^{(0)}\right) & \text{if } v_{n-1} \equiv 0 \pmod N \end{cases}$$

Proof. Apply the decomposition of D_n in Lemma 11.9.3 to the definition of $C\left(D_n, v\right)$.

$$\begin{aligned} C\left(D_n,\, v\right) \;&=\; C\left(D_n^*,\, v\right) \;-\; \sum_{i=0}^{n-2} C\left(D_{n-1}^{(i)},\, v\right) \\ &=\; \sum_{r \in D_n^*} e\left(\sum_{k=0}^{n-1} r_k v_k\right) \;-\; \sum_{i=0}^{n-2} \sum_{r \in D_{n-1}^{(i)}} e\left(\sum_{k=0}^{n-1} r_k v_k\right) \end{aligned}$$

Since $D_n^* = D_{n-1} \times \mathbb{Z}_N$, the first term can be separated:

$$\sum_{r \in D_n^*} e\left(\sum_{k=0}^{n-1} r_k v_k\right) \;=\; \sum_{r_{n-1} \in \mathbb{Z}_N} e\left(v_{n-1} r_{n-1}\right) \sum_{r \in D_{n-1}} e\left(\sum_{k=0}^{n-2} r_k v_k\right)$$

$$\text{Now,} \sum_{r_{n-1} \in \mathbb{Z}_N} e(v_{n-1} r_{n-1}) \;=\; \begin{cases} N & \text{if } v_{n-1} \equiv 0 \pmod N \\ 0 & \text{otherwise} \end{cases}$$

First consider $v_{n-1} \not\equiv 0$. In this case, we get

$$C(D_n, v) \quad = \quad -\sum_{i=0}^{n-2} \sum_{r \in D_{n-1}^{(i)}} e\left(\sum_{k=0}^{n-1} r_k v_k\right) \quad = \quad -\sum_{i=0}^{n-2} \sum_{r \in D_{n-1}} e\left(\sum_{k=0}^{n-2} r_k v_k^{(i)}\right)$$

which, by definition of $C(D_{n-1}, v)$, is the required formula for this case.
When $v_{n-1} \equiv 0$, we get instead,

$$C(D_n, v) \quad = \quad N \sum_{r \in D_{n-1}} e\left(\sum_{k=0}^{n-2} r_k v_k\right) \;-\; \sum_{i=0}^{n-2} \sum_{r \in D_{n-1}} e\left(\sum_{k=0}^{n-2} r_k v_k^{(i)}\right)$$

But, in this case, $v^{(i)} = v^{(0)}$, $\forall i,\ 0 \le i \le n-2$.

$$\therefore\, C(D_n, v) \;=\; NC(D_{n-1}, v^{(0)}) \;-\; \sum_{i=0}^{n-2} C(D_{n-1}, v^{(0)}) \;=\; (N-n+1) C(D_{n-1}, v^{(0)}) \;\square$$

11.9.6 **An Algorithm for Calculating the Determinantal Coefficients.** Using the recursion of the lemma, we demonstrate an algorithm for calculating the determinantal coefficients.

Take $N = 6$, we shall calculate the coefficient of $a_0a_2a_3^2a_5^2$. We have $\bar{v} = (0, 2, 3, 3, 5, 5)$, and we take $v = (2, 3, 3, 5, 5)$. Define $B[u] := C(D_{|u|}, u)$ for any null multiset u. The lemma gives a recursion for B in terms of $|u|$.

$$\begin{aligned}
B[2,3,3,5,5] &= -B[1,3,3,5] - B[2,2,3,5] - B[2,3,2,5] - B[2,3,3,4] \\
\text{(simplify)} &= -B[1,3,3,5] - 2B[2,2,3,5] - B[2,3,3,4] \\
\text{(collapse)} &= B[0,3,3] + B[1,2,3] + B[1,3,2] + 2(B[1,2,3] + B[2,1,3] + B[2,2,2]) \\
&\quad + B[0,3,3] + B[2,1,3] + B[2,3,1] \\
\text{(simplify)} &= 2B[3,3,0] + 8B[1,2,3] + 2B[2,2,2] \\
\text{(collapse)} &= 8B[3,3] - 8(B[4,2] + B[1,5]) - 2(B[4,2] + B[2,4]) \\
\text{(simplify)} &= 8B[3,3] - 12B[2,4] - 8B[1,5] \\
\text{(collapse)} &= -8B[0] + 12B[0] + 8B[0] \\
\text{(simplify)} &= 12 \times N = 72 \qquad (\text{since } B[0] = \textstyle\sum_{r\in\mathbb{Z}_N} e(0) = N) \\
\therefore \text{ by Lemma 11.9.2,} \quad c(\bar{v}) &= \frac{(N-n)!}{F(\bar{v})} \cdot 72 \;=\; 18
\end{aligned}$$

The above calculation is not the fastest; we could have reduced the number of steps by first incrementing all the residues. Let the increment map be $\imath : Z_0^N \mapsto Z_0^N$. Then, $c(\imath\bar{v}) = (-1)^{N+1}c(\bar{v})$. Now $\imath(0, 2, 3, 3, 5, 5) = (1, 3, 4, 4, 0, 0)$ which has two zeroes instead of one. Hence, we could have started the calculation with $-B[1, 3, 4, 4]$ which has only four non-zero elements. This short-cut can be used at any step provided one keeps track of the sign changes.

Another short-cut is to take advantage of the linearity of the algorithm. For instance, if one knows that $B(1, 3, 3, 5) = B(2, 3, 3, 4) = 0$, then these terms can be omitted at the outset giving us $B[2, 3, 3, 5, 5] = -B[2, 2, 3, 5] - B[2, 3, 2, 5] = -2B[2, 2, 3, 5]$.

Despite these short-cuts, this algorithm tends to be less efficient than the formula of the main theorem when $n \gg 1$ because of the explosion of middle terms in the recursion.

We now introduce a formal definition for the numerator of the Zero Set Formula.

11.10.1 **Definition** For all $n \le N$, and $v \in Z_0^n$, define $H_n(v\,;\,x) \in \mathbb{Z}[x]$ by

$$H_n(v\,;\,x) \;:=\; (-1)^n \sum_{P\in\mathcal{P}_0(v)} (-x)^{|P|} \prod_{S\in P} (|S| - 1)!$$

Recall that for $v \in Z_0^n$, $\mathcal{P}_0(v)$ is the set of all partitions of $\mathbb{Z}_n$ into zero sets on v.

In the next three lemmas, we shall show that $H_n(v\,;\,x)$ satisfies the same recurrence relationships as $C(D_n, v)$. We shall then show that $C(D_n, v) = H_n(v\,;\,x)$ when $n = 0$ and $x = N$.

11.10.2 **Lemma** Let $v \in Z_0^n$, and let $v^{(i)}$ be the collapse of v on i. If $v_{n-1} \neq 0$, then

$$H_n(v\,;\,x) \;=\; -\sum_{i=0}^{n-2} H_{n-1}(v^{(i)}\,;\,x)$$

Proof. By definition,

$$H_{n-1}(v^{(i)}, x) \;=\; (-1)^{n-1} \sum_{P^i\in\mathcal{P}_0(v^{(i)})} (-x)^{|P^i|} \prod_{S\in P^i} (|S| - 1)! \tag{10}$$

We now intend to convert this sum over $\mathcal{P}_0(v^{(i)})$ into a sum over $\mathcal{P}_0(v)$ which will allow us to reconstruct the desired formula for H_n. To do so, we shall construct a map from zero set partitions on $v^{(i)}$ (where $i = 0, 1, \ldots, n-2$) to partitions on v:

$$\beta : \bigcup_{i=0}^{n-2} \mathcal{P}_0(v^{(i)}) \;\rightarrow\; \mathcal{P}_0(v)$$

Take any $P^i \in \mathcal{P}_0(v^{(i)})$; let us say $P^i = \{S_1, S_2, \ldots, S_q\}$. Since only the i^{th} component of $v^{(i)}$ disagrees with v, all members of $S_1, S_2, \ldots, S_q$ must also be zero sets on v except the one which contains i. Since the numbering of the sets is arbitrary, we can assume that $i \in S_q$, and that $S_1, S_2, \ldots, S_{q-1}$ are zero sets on v. Let S^c be the complement of $S_1 \cup S_2 \cup \ldots \cup S_{q-1}$ in $\mathbb{Z}_n$. Since $\mathbb{Z}_n$ and each of $S_1, S_2, \ldots, S_{q-1}$ are zero sets on v, then so is S^c. Also,

$$\{i,\ n-1\} \;\subset\; S^c \;=\; S_q \cup \{n-1\} \tag{11}$$

We define β by

$$\beta(P^i) \;=\; \{S_1, S_2, \ldots, S_{q-1}, S^c\} \in \mathcal{P}_0(v)$$

Claim: β is well-defined.

We have shown that all sets in P^i are zero sets on v except possibly for S_q (following our convention that $i \in S_q$). Equation (11) shows that $S_q \cup \{n-1\}$ is a zero set on v and, by assumption, $v_{n-1} \neq 0$. Therefore S_q cannot be a zero set on v. Hence, there is always a unique member of P^i which is not a zero set on v, and this makes the definition of $\beta(P^i)$ unambiguous.

Finally, we need to verify that $\beta|\mathcal{P}_0(v^{(i)})$ agrees with $\beta|\mathcal{P}_0(v^{(j)})$ on the intersection $\mathcal{P}_0(v^{(i)}) \cap \mathcal{P}_0(v^{(j)})$. However, as shown above, there is always a unique member that is not a zero set on v in every partition of $\mathcal{P}_0(v^{(k)})$; this criterion does not depend on k, and determines the image of β. Therefore, β is well-defined on partitions as required. **QED Claim.**

For the remainder of the proof, to save needless repetitions, we shall assume when given a partition $P = \{T_1, T_2, \ldots, T_q\}$ belonging to $\mathcal{P}_0(v)$, that its last element listed, T_q, is the one containing $n-1$.

Claim: $\beta|\mathcal{P}_0(v^{(i)})$ is one-one.

Take any $P = \{T_1, T_2, \ldots, T_q\} \in \mathcal{P}_0(v)$. We have $n-1 \in T_q$. If $i \notin T_q$, then according to (11) no partition of $\mathcal{P}_0(v^{(i)})$ is mapped to P. Otherwise, for $j = 1, 2, \ldots, q-1$, we set $S_j = T_j$, and set $S_q = \mathbb{Z}_n - \bigcup_{j=1}^{q-1} S_j$. Then, $\{S_1, S_2, \ldots, S_q\} \in \mathcal{P}_0(v^{(i)})$, and is uniquely defined. **QED Claim.**

So as to correctly convert the sum of equation (10) into a sum over $\mathcal{P}_0(v)$, it is necessary to know how many partitions there are in $\beta^{-1}P$ for any $P \in \mathcal{P}_0(v)$. Since β is one-one on $\mathcal{P}_0(v^{(i)})$, it follows that each $\mathcal{P}_0(v^{(i)})$ contributes at most one element to $\beta^{-1}P$. Suppose $P = \{T_1, T_2, \ldots, T_q\} \in \mathcal{P}_0(v)$. It is clear from (11) that $\mathcal{P}_0(v^{(i)})$ contains a partition mapped onto P if and only if $i \in T_q - \{n-1\}$.

$$\therefore\ \left|\beta^{-1}(P)\right| \;=\; |T_q| - 1$$

In particular, this shows that β is onto since $P \in \mathcal{P}_0(v)$ is arbitrary, and $|T_q| \geq 2$ for any set in a partition so $i \in T_q - \{n-1\}$ exists.

We are now ready to rewrite the sum in equation (10) as a sum over $\mathcal{P}_0(v)$. Note that β preserves the cardinality of partitions, and it also preserves every set in a partition, and in particular, its cardinality, except for S_q --its cardinality alone is increased by one. That is, for $0 \leq i < q$, $S_i = \beta(S_i)$, and $|S_q| = |\beta(S_q)| - 1$,

So, we have,

$$H_{n-1}(v^{(i)}\,;x) \;=\; (-1)^{n-1} \sum_{P^i \in \mathcal{P}_0(v^{(i)})} (-x)^{|P^i|}\ (|\beta(S_q)| - 2)! \prod_{S \in P^i - \{S_q\}} (|\beta(S)| - 1)!$$

where the sum is over all partitions, $P^i = \{S_1, S_2, \ldots, S_q\}$, in $\mathcal{P}_0(v^{(i)})$.

In the first equation which follows we change the summation to all partitions, $P = \{T_1, T_2, \ldots, T_q\}$, in $\beta(\mathcal{P}_0(v^{(i)})) = \mathcal{P}_0(v)$. We also sum over i. Since the dependence of the R.H.S. on i is entirely in the summation range, the summation over i merely joins the summation ranges. We substitute $|T_q| - 1$ for $\left|\beta^{-1}(P)\right|$ in the third equation.

$$\begin{aligned}
-\sum_{i=0}^{n-2} H_{n-1}(v^{(i)}\,;\,x) &= -(-1)^{n-1}\sum_{i=0}^{n-1}\sum_{P\in\beta(\mathcal{P}_0(v^{(i)}))}(-x)^{|P|}(|T_q|-2)!\prod_{T\in P-\{T_q\}}(|T|-1)! \\
&= (-1)^n\sum_{P\in\mathcal{P}_0(v)}(-x)^{|P|}\left|\beta^{-1}P\right|(|T_q|-2)!\prod_{T\in P-\{T_q\}}(|T|-1)! \\
&= (-1)^n\sum_{P\in\mathcal{P}_0(v)}(-x)^{|P|}(|T_q|-1)!\prod_{T\in P-\{T_q\}}(|T|-1)! \\
&= (-1)^n\sum_{P\in\mathcal{P}_0(v)}(-x)^{|P|}\prod_{T\in P}(|T|-1)! \\
&= H_n(v\,;\,x)\ \square
\end{aligned}$$

The above lemma gives us a recurrence relationship when the element that is combined in the collapse of v to $v^{(i)}$ is non-zero. We now find a recurrence relationship when the collapse removes a zero.

11.10.3 **Lemma** Let $v \in Z_0^n$, and suppose v has at least one zero entry, and let $\hat{v}$ be v without one zero. Then,

$$H_n(v\,;\,x) = (x-n+1)H_{n-1}(\hat{v}\,;\,x)$$

Proof. We shall convert the sum over $\mathcal{P}_0(v)$ in H_n to a sum over partitions of $\mathcal{P}_0(\hat{v})$. To this end we shall construct a map $\alpha : \mathcal{P}_0(v) \to \mathcal{P}_0(\hat{v})$. It is notationally convenient to assume that $v_0 = 0$. This means that $\{0\}$ is a zero set on v.

If given $\hat{P} = \{S_1, S_2, \ldots, S_q\} \in \mathcal{P}_0(\hat{v})$, then for $1 \le j \le q$, $P_j = \{S_1, \ldots, S_j \cup \{0\}, \ldots, S_q\}$ is a partition in $\mathcal{P}_0(v)$ and so is $P_0 = \{S_1, S_2, \ldots, S_q, \{0\}\}$. We shall call the inverse of this correspondence α. By construction, α is onto $\mathcal{P}_0(\hat{v})$.

It is clear that α acts on the sets in a partition by eliminating the zero element or by eliminating the set consisting of only the zero element. Thus, one zero is always eliminated by α. So, α maps into $\mathcal{P}_0(\hat{v})$.

In any zero set partition in $\mathcal{P}_0(v)$ there is exactly one zero set which contains zero. This shows that α is well-defined.

We now take the formula of Definition 22, and convert the sum over partitions of v into one over partitions of $\hat{v}$.

$$\begin{aligned}
H_n(v) &= (-1)^n\sum_{P\in\mathcal{P}_0(v)}(-x)^{|P|}\prod_{T\in P}(|T|-1)! \\
&= (-1)^n\sum_{\widehat{P}\in\mathcal{P}_0(\widehat{v})}\left\{\sum_{j=1}^{\left|\widehat{P}\right|}(-x)^{\left|\widehat{P}\right|}|S_j|\prod_{S\in\widehat{P}}(|S|-1)! + (-x)^{\left|\widehat{P}\right|+1}\prod_{S\in\widehat{P}}(|S|-1)!\right\}
\end{aligned}$$

where the outer summation is over all partitions, $\hat{P} = \{S_1, S_2, \ldots, S_q\}$, in $\mathcal{P}_0(\widehat{v})$.

The $|S_j|$ factor comes from $(|S_j| + 1 - 1)! = |S_j|!$. The extra 1 is due to the extra element, zero, in S_j. We then moved $|S_j|$ out of the product leaving $(|S_j| - 1)!$ in the product. The last term comes from the

extra partition which contains the extra set $\{0\}$. Simplifying,

$$\begin{aligned} H_n(v) &= (-1)^n \sum_{\widehat{P}\in\mathcal{P}_0(\widehat{v})} (-x)^{|\widehat{P}|} \prod_{S\in\widehat{P}} (|S|-1)! \left\{ \sum_{S\in\widehat{P}} |S| - x \right\} \\ &= (-1)^{n-1}(x-n+1) \sum_{\widehat{P}\in\mathcal{P}_0(\widehat{v})} (-x)^{|\widehat{P}|} \prod_{S\in\widehat{P}} (|S|-1)! \quad \text{since } \sum_{S\in\widehat{P}} |S| = n-1 \\ &= (x-n+1)H_{n-1}(\hat{v}) \ \square \end{aligned}$$

11.10.4 **Proposition** For all $v \in Z_0^n$, and for all $n \in \mathbb{N}$, $C(D_n, v) = H_n(v\,;\, N)$.

Proof. Lemmas 11.9.5, 11.10.2 and 11.10.3 show that $C(D_n, v)$ and $H_n(v\,;\, x)$ satisfy the same recurrence relations in n and v. Therefore, if $C(D_0, (\emptyset)) = H_0((\emptyset); x)$, where $(\emptyset)$ is the empty sequence, then they will be equal at $x = N$, for all n and all v because ultimately, the recursion will reduce v to $(\emptyset)$.

So assume that $n = 0$ and $x = N$. Then, $c(\bar{v})$ is the coefficient of the a_0^N term in the determinant expansion. Since a_0 occurs entirely on the main diagonal of the determinant, its coefficient must be 1.

By Lemma 12,

$$C(D_n, v) = \frac{F(\bar{v})}{(N-n)!} c(\bar{v}) = \frac{N!}{N!} \cdot 1 = 1$$

From the definition, $H_n(v\,;\, x)$ at $n = 0$, $x = N$ is

$$H_0((\emptyset)\,;\, N) = (-1)^n \sum_{P\in\mathcal{P}_0((\emptyset))} (-N)^{|P|} \prod_{S\in P} (|S|-1)! \tag{12}$$

The empty sequence, $(\emptyset)$, has one partition, the empty partition. This is the only valid partition since empty zero sets are not allowed by definition. That is, $\mathcal{P}_0(v) = \{\emptyset\}$ and $P \in \mathcal{P}_0(v) \Rightarrow |P| = 0$. Therefore, the sum in formula (12) has a single term, and in this term there is an empty product, which we conventionally take equal to 1. Hence, formula (12) gives the value $(-1)^0(-N)^0 = 1$ as required. $\square$

11.11 Zero Set Formula

We now derive alternate formulæ for the determinantal coefficient.

11.11.1 **Theorem** Let $v \in Z_0^n$, and suppose v has m non-zero entries. Then,

$$c_N(\bar{v}) = (-1)^n \binom{N-m}{N-n}^{-1} F(v)^{-1} \sum_{P\in\mathcal{P}_0(v)} (-N)^{|P|} \prod_{S\in P} (|S|-1)! \tag{13}$$

Proof. Let $s = N - m =$ the number of zeroes in $\bar{v}$, and let $\hat{v}$ denote v stripped of all its zeroes. From Lemma 12,

$$\begin{aligned} C(D_n, v) &= \frac{F(\bar{v})}{(N-n)!}\, c(\bar{v}) \\ &= \frac{F(\hat{v})\, s!}{(N-n)!}\, c(\bar{v}) \\ &= \frac{F(v)\, s!}{(s-(N-n))!\,(N-n)!}\, c(\bar{v}) \\ &= F(v) \binom{s}{N-n} c(\bar{v}) \end{aligned}$$

Finally, by Proposition 11.10.4, we can substitute $H_n(v; N)$ for $C(D_n, v)$. $\square$

11.12 **Multiset Formula** The need to compute zero sets in the formula (13) is undesirable because it is rather prone to error. Not only must one find all the null multiset partitions for v, one must then find all the zero sets representing a given multiset partition. In the theorem which follows, we derive a formula for the coefficient directly in terms of null multiset partitions and thereby entirely eliminate the need to calculate zero sets.

Recall that $\mathcal{P}_0[v]$ denotes the set of all partitions of $[v]$ into null multisets. Note that a partition is a multiset of multisets. For example, $\big[[2,4],[2,4]\big] \in \mathcal{P}_0[2,2,4,4]$ for $N=6$.

11.12.1 **Theorem** Let $v \in Z_0^n$, and suppose v has m non-zero entries. Then,

$$c_{_N}(\bar{v}) \quad = \quad (-1)^n \binom{N-m}{N-n}^{-1} \sum_{[U]\in\mathcal{P}_0[v]} \frac{(-N)^{|U|}}{F(U)} \prod_{[u]\in[U]} \frac{(|u|-1)!}{F(u)} \tag{14}$$

where $F(U) = a!\,b!\cdots f!$ where $a,b,\ldots,f$ are the multiplicities of the multisets in U.

Proof. We define a function $J_n\big([v];\ x\big)$ by

$$J_n\big([v];\ x\big) \ := \ (-1)^n \sum_{[U]\in\mathcal{P}_0[v]} \frac{(-x)^{|U|}}{F(U)} \prod_{[u]\in[U]} \frac{(|u|-1)!}{F(u)}$$

By Theorem 11.11.1,

$$c(\bar{v}) \ = \ \binom{N-m}{N-n}^{-1} F(v)^{-1} H_n(v;\ N)$$

By Theorem 11.11.1, we need only show that $F(v)^{-1}H_n(v;\ N) = J_n([v];N)$.

We make the natural correspondence between zero sets on v and null multisets, namely, we map the zero set S to the multiset $v:S$. We call this map α. The map α also induces a map from $\mathcal{P}_0(v)$ to $\mathcal{P}_0[v]$ in the obvious way, and we call this map α as well. The cardinality of a partition is not changed by α, and neither is the cardinality of each set appearing in the partition. That is, $|\alpha(S)| = |v:S| = |S|$, and the partition $\{S_1,S_2,\ldots,S_r\}$ of $\mathcal{P}_0(v)$ corresponds to the partition $[v:S_1,\ v:S_2,\ \ldots,\ v:S_r]$ of $\mathcal{P}_0[v]$, both of which have cardinality r. Hence, the only adjustment to the zero set formula will be the number of zero sets mapped to a single null multiset.

Let $M \in \mathcal{P}_0[v]$. We need to find $\big|\alpha^{-1}M\big|$. Let $M = \big[[m_1],[m_2],\ldots,[m_r]\big]$ where each m_i is a subsequence of v. There exists $S = \{S_1,S_2,\ldots,S_r\} \in \alpha^{-1}M$. For instance, one such can be constructed by setting S_i to the set of subscripts appearing in m_i for each i. We take S to be this partition.

The defining difference between zero sets and null multisets is that order matters in zero sets but not in null multisets. Hence, we can find all zero sets for a given multiset by acting upon one member of $\alpha^{-1}M$, S say, with permutations on the subscripts of v.

Let G be the stabilizer group of v; specifically, define

$$G \ := \ \{\gamma : \mathbb{Z}_n \to \mathbb{Z}_n \ \vdash \ v = v_\gamma\}$$

Then, $|G| = F(v)$.

Every permutation $\gamma \in G$, maps M to itself, but maps S to a possibly different partition, γS of $\mathcal{P}_0(v)$, where $\gamma S := \{\gamma S_1, \gamma S_2, \ldots, \gamma S_r\}$. However, not all $(\gamma S)_{\gamma\in G}$ will be distinct; there will be duplications whenever $\gamma S = S$. Denote the set of such permutations by R. Clearly, the number of distinct elements in $\big|\alpha^{-1}M\big| = G/R = |G|\,/\,|R|$.

R is that subgroup of G in which each element maps every S_i onto some S_j. To compute $|R|$ we shall factor it into those permutations which permute elements within the S_i's, and those which permute the S_i's among themselves. To this end, define

$$Q \ := \ \{\gamma \in G \ \vdash \ \gamma S_i = S_i, \ \ \forall i = 1,2,\ldots,r\}$$

We know $|Q|$, it is

$$|Q| \;=\; \prod_{i=1}^{r} F(v{:}S_i) \;=\; \prod_{i=1}^{r} F(m_i)$$

One easily sees that $Q \lhd R$. So we can define $R^* = R/Q$. Members of R^* represent permutations of $(S_1, S_2, \ldots, S_r)$. Their number is

$$|R^*| \;=\; F\left(v{:}S_1,\; v{:}S_2,\; \ldots,\; v{:}S_r\right) \;=\; F\left([m_1],[m_2],\ldots,[m_r]\right)$$

$$\therefore\; |R| \;=\; |R^*|\cdot|Q| \;=\; F\left([m_1],[m_2],\ldots,[m_r]\right)\prod_{i=1}^{r} F(m_i) \;=\; F(M)\prod_{m\in M} F(m)$$

$$\therefore\; \left|\alpha^{-1}M\right| \;=\; |G/R| \;=\; \frac{F(v)}{F(M)\prod_{m\in M}F(m)}$$

which is the number of zero set partitions per null multiset partition.

We now apply this to $F(v)^{-1}H_n(v;\,N)$.

$$\begin{aligned}
\frac{(-1)^n}{F(v)}H_n(v;\,N) \;&=\; \frac{1}{F(v)}\sum_{T\in\mathcal{P}_0(v)}(-N)^{|T|}\prod_{S\in T}(|S|-1)!\\
&=\; \sum_{T\in\mathcal{P}_0(v)}(-N)^{|T|}\frac{1}{F(v)}\prod_{S\in T}(|S|-1)!\\
&=\; \sum_{[U]\in\mathcal{P}_0[v]}(-N)^{|U|}\frac{1}{F(v)}\frac{F(v)}{F(U)\prod_{u\in[U]}F(u)}\prod_{[u]\in[U]}(|u|-1)!\\
&=\; \sum_{[U]\in\mathcal{P}_0[v]}\frac{(-N)^{|U|}}{F(U)}\prod_{[u]\in[U]}\frac{(|u|-1)!}{F(u)}\\
&=\; (-1)^n J_n([v];N)\;\square
\end{aligned}$$

We note that the theorem holds for arbitrary $v\in\mathbb{Z}_N^n$ provided we interpret an empty sum as zero, since clearly there are no partitions of v into null multisets if v itself is not a null multiset.

11.13 Power Formula.

The monomials Πa_v would most commonly be expressed as a product of powers of the variables $a_0, a_1, \ldots, a_{N-1}$. Thus, $\Pi a_v = a_0^{k_0}a_1^{k_1}\cdots a_{N-1}^{k_{N-1}}$ where k_i is the multiplicity of v_i in $[v]$. It is quite straightforward to express the determinantal coefficients in terms of the powers $k_0, k_1, \ldots, k_{N-1}$.

$$\det\mathbf{circ}_N(a) \;=\; (-1)^N\sum_{\substack{k\in\mathbb{N}^N\\ \Sigma k=N}} a_0^{k_0}a_1^{k_1}\cdots a_{N-1}^{k_{N-1}}\sum_{\substack{[T]\subset\Delta\\ \Sigma T=k}}\frac{(-N)^{|T|}}{F(T)}\prod_{t\in T}\frac{1}{\Sigma t}\binom{\Sigma t}{t}$$

where $\Delta := \left[t\in\mathbb{Z}^N \vdash t\neq 0 \text{ and } \sum it_i\equiv 0 \pmod N\right]$, and $\binom{s}{t}$ with $s=\Sigma t$ is the multinomial coefficient of the first kind.

The restriction $\sum T = k$ means that the sum of vectors in T must equal the vector k. The condition $\sum k_i = N$ states the degree is N. The condition $[T]\subset\Delta$ means that T is the equivalent of a null multiset partition.

11.14 Application to Permutations

According to Proposition 10.5.3, if $c(v)$ is non-zero, then there exists a permutation, τ, on $\mathbb{Z}_N$ shose multiset of translations equals $[v]$. When $N=p$, prime, the theorem gives a precise criterion for when $c(v)$ is non-zero.

11.14.2 **Proposition** Let p be an odd prime, and let $v \in Z_0^p$. If v consists of only a single residue of multiplicity p, then $c_p(v) = 1$. Otherwise, $F(v) \not\equiv 0 \pmod p$, and

$$c_p(v) \equiv -p\,F(v)^{-1} \pmod{p^2}$$

Proof. The requirement that $v \in Z_0^p$ means that the vector v is of full length. Suppose first that v contains only one distinct residue, r, say, then $c(v)$ is the coefficient of the term a_r^p which one can easily see is 1 for odd order circulants.

Now suppose that v contains at least two distinct residues. By the Zero Set Formula of Proposition 27,

$$c(v) = \frac{(-1)^p}{F(v)} \sum_{W \in \mathcal{P}_0(v)} (-p)^{|W|} \prod_{S \in W} (|S|-1)!$$

Consider first the denominator, $F(v)$. It equals a product of factorials, $a!b!\ldots$ where $a, b, \ldots$ are multiplicities of elements in v. Since v contains at least two distinct elements, no multiplicity can equal or exceed p. Hence, $p \nmid F(v)$, and so $F(v)$ has an inverse in $\mathbb{Z}_{p^2}$ and the formula can be evaluated modulo p^2 by taking the inverse residue. The p term is derived from single set partitions, but there is only one such, namely $W = \{\{\mathbb{Z}_p\}\}$.

$$\therefore c(v) \equiv -F(v)^{-1}(-p)(p-1)! \equiv -pF(v)^{-1} \pmod{p^2}$$

The last congruence follows by Wilson's Theorem. □

Ore also derived the above result from the Zero Set Formula.

11.14.3 **Corollary** For p prime, there exists a permutation $\tau \in S_p$ such that $[\tau] = [v]$ iff v is a null multiset (mod p).

Proof. This is immediate from Proposition 10.5.3 and the proposition when p is odd. The corollary also holds for $p = 2$ because then the determinant is $a_0^2 - a_1^2$. □

This corollary proves a special case of a conjecture of E.T. Parker [Guy]. The full conjecture, if true, would imply that the primality condition in Corollary 11.14.3 is unnecessary.

11.15 Application to Cyclotomic Norms.

We shall apply Proposition 11.14.2 to estimate the congruence class of the determinant modulo p^2.

11.15.1 **Proposition** Let p be an odd prime, and let $A = \mathrm{CIRC}_p(a)$ where $a \in \mathbb{Z}^p$. Then,

$$\det A \equiv (A^p)_{0,0} \equiv p^{-1}\mathrm{tr}A^p \qquad (\mathrm{mod}\ p^2)$$

Proof. Proposition 11.14.2 provides a formula for the determinantal coefficient modulo p^2 unless the monomial is a p^{th} power when the coefficient equals 1. Hence,

$$\det A = \sum_{\Sigma[v] \equiv 0 \pmod p} c(v) \prod a_v \equiv -p\,S(a) + \sum_{j=0}^{p-1} a^p \pmod{p^2} \tag{15}$$

where $S(a) := \sum \left\{ \dfrac{a_1^{i_1} a_2^{i_2} \cdots a_p^{i_p}}{i_1! i_2! \cdots i_p!} \vdash \Sigma i_j = p,\ \Sigma j i_j \equiv 0 \pmod p,\ i_k < p, \forall k \right\}$

We can express $S(a)$ in terms of A^p. We proceed by expanding A in terms of the standard circulant basis $\{I, \mathrm{U}, \mathrm{U}^2, \ldots, \mathrm{U}^{p-1}\}$. Then, by the multinomial theorem,

$$A^p \;=\; \left(\sum_{k=0}^{p-1} a_k \mathrm{U}^k\right)^p \;=\; \sum_{m=0}^{p-1} \mathrm{U}^m \sum_{\substack{\Sigma i_j = p \\ \Sigma j i_j \equiv m \,(\mathrm{mod}\ p)}} \frac{m!}{i_1!\, i_2! \cdots i_m!}\, a_1^{i_1} a_2^{i_2} \cdots a_m^{i_m}$$

Now, the coefficient of $\mathrm{U}^0 = I$ term in the above expansion equals the $(0,0)^{\text{th}}$ entry in A^p. Therefore,

$$\begin{aligned}
\therefore\ (A^p)_{0,0} \;&=\; \sum_{\substack{\Sigma i_j = p \\ \Sigma j i_j \equiv 0 \,(\mathrm{mod}\ p)}} \frac{p!}{i_1!\, i_2! \cdots i_m!}\, a_1^{i_1} a_2^{i_2} \cdots a_m^{i_m} \\
&=\; p!\, S(a) \;+\; \sum_{j=0}^{p-1} a_j^p \\
&\equiv\; -p\, S(a) \;+\; \sum_{j=0}^{p-1} a_j^p \pmod{p^2} && \text{by Wilson's Theorem} \\
&\equiv\; \det A \pmod{p^2} && \text{from (15)}
\end{aligned}$$

This proves the first congruence in the proposition. The second follows because A^p is a circulant, and so its trace is just p times the top left element. □

11.15.2 **Corollary** Let $A = \mathrm{CIRC}(a_0, a_1, \ldots, a_{p-1}) \in \mathrm{CIRC}_p(\mathbb{Z})$ with eigenvalues $\mu_0, \mu_1, \ldots, \mu_{p-1}$, then the cyclotomic norm of μ_1 in $\mathbb{Z}(\zeta_p)$ is

$$\mathcal{N}(\mu_1) \;\equiv\; \frac{(A^p)_{0,0}}{\mu_0} \pmod{p^2} \;\square$$

If $p \,|\, \mu_0$ then the fraction on the right must of course be evaluated before taking of residues.

11.15.3 **Corollary** Let $\xi \in \mathbb{Z}(\zeta_p)$. Then,

$$\mathcal{N}(1 + p\xi) \;\equiv\; 1 - p\,\ell_p(\xi) \pmod{p^2}$$

(See §7.2.6 for the definition of the ℓ_p homomorphism.)

Proof. Let $\xi \in \mathbb{Z}(\zeta_p)$, and let $c \in \lambda_1^{-1}(\xi)$. Following Corollary 11.15.2 we estimate the scalar term in $(1+pc)^p = 1 + p^2(c + \cdots) \equiv 1 \pmod{p^2}$. Hence,

$$\mathcal{N}(1 + p\xi) \;\equiv\; (1 + p\,\lambda_0(c))^{-1} \;\equiv\; 1 - p\,\ell_p \pmod{p^2} \;\square$$

11.16.1 **Application to Combinatorics I.**

Let $n \le N$ but otherwise unrestricted, and we let $v = 0 \in \mathbb{Z}^n$. The coefficient of this subscript vector is 1, and the multiset partitions of v correspond to unordered partitions of the integer n. These are all solutions to

$$\sum_{i=1}^{n} i k_i \;=\; n \quad \text{with } k_i \in \mathbb{N}$$

Each ik_i term represents the multiset $[[0,\ldots,0]\,,\ [0,\ldots,0]\,,\ [0,\ldots,0]]$ which is k_i multisets of i zeroes each. The order of the stabilizer group for each $u = [0,\ldots,0]$ is $F(u) = i!$, and the order of the stabilizer group for a partition is $F(U) = k_1!k_2!\cdots k_n!$. Entering this into the Multiset Formula (see equation (14) in §11.12.1), and multiplying throughout by $\binom{N}{n}$, we get

$$\begin{aligned}\binom{N}{n} &= (-1)^n \sum_{\{k_i \vdash \Sigma i k_i = n\}} \frac{(-N)^{\Sigma k_i}}{k_1!k_2!\cdots k_n!} \prod_{i=1}^{n} \left(\frac{(i-1)!}{i!}\right)^{k_i} \\ &= (-1)^n \sum_{\{k_i \vdash \Sigma i k_i = n\}} \frac{(-N)^{\Sigma k_i}}{k_1!k_2!\cdots k_n!} \left(\prod_{i=1}^{n} i^{-1}\right)\left(\prod_{i=1}^{n} i^{1-k_i}\right)\end{aligned}$$

Cancelling $n!$ with $\prod i^{-1}$,

$$\begin{aligned}\frac{N!}{(N-n)!} &= (-1)^n \sum_{\{k_i \vdash \Sigma i k_i = n\}} (-N)^r \prod_{i=1}^{n} \frac{i^{1-k_i}}{k_i!} \quad \text{where } r = \sum_{i=1}^{n} k_i \\ &= (-1)^n \sum_{r=0}^{n} (-N)^r \sum_{\substack{\Sigma i k_i = n \\ \Sigma k_i = r}} \prod_{i=1}^{n} \frac{i^{1-k_i}}{k_i!}\end{aligned}$$

Both sides of the equation are manifestly polynomials in N with coefficients constant with respect to N. Since the equation holds for general N, and the left has integral coefficients, so must the right.

The Stirling numbers of the first kind, $S_N^{(m)}$, are defined by (see [AbS]),

$$x(x-1)\cdots(x-n+1) = \sum_{m=0}^{n} S_n^{(m)} x^m$$

which gives:

11.16.2 **Proposition** $S_n^{(m)} = (-1)^{n+r} \sum_{\substack{\Sigma i k_i = n \\ \Sigma k_i = r}} \prod_{i=1}^{n} \frac{i^{1-k_i}}{k_i!}$. □

11.16.3 **Application to Combinatorics II.**

In this section, we shall take all subscript vectors v to be of full length, so that $v = \bar{v}$.

It was shown in §5.2.14 that if $N = mn$ then

$$\Delta_N(a_0, 0, \ldots, 0, a_m, 0 \ldots, 0, a_{2m}, 0, \ldots, 0, a_{N-n}, 0, \ldots, 0) = \Delta_n(a_0, a_m, a_{2m}, \ldots, a_{N-m})^m \qquad (16)$$

Since this holds for arbitrary $a_0, a_m, a_{2m}, \ldots, a_{m(n-1)}$, we can deduce relationships between the coefficients using the multinomial theorem which, in our notation, is

$$\left(\sum_{i \in \mathbb{Z}_n} x_i\right)^m = \sum_{v \in \mathbb{Z}_n^m} \frac{m!}{F(v)} \prod x_v$$

In the present case, from equation (16), the x_i's are terms of the form $c_n(u)\Pi a_{mu}$. All terms in $\det \mathbf{circ}_N$ in equation (16) are of the form $c(mv)\Pi a_{mv}$, and can arise from the multinomial expansion only from products of the form

$$c(u_0)\Pi a_{mu_0}\ c(u_1)\Pi a_{mu_1}\ \cdots\ c(u_{m-1})\Pi a_{mu_{m-1}}$$

where $[u_0] \cup [u_1] \cup \cdots \cup [u_{m-1}] = v$. Hence,

$$c_{mn}(mv) = \sum_{U \in \mathcal{P}_0^n(v)} \frac{m!}{F(U)} \prod_{u \in U} c_n(u) \qquad (17)$$

where $\mathcal{P}_0^n(v)$ is all partitions of v into m null multisets modulo n each of length n. That is, $U \in \mathcal{P}_0^n(v) \Rightarrow |U| = m$ and $u \in U \Rightarrow |u| = n$.

We illustrate formula (17) with one example. Let $N = 8,\ n = 4,\ m = 2.\ v = [0\ 1\ 1\ 1\ 1\ 2\ 3\ 3],\ 2v = [0\ 2\ 2\ 2\ 2\ 4\ 6\ 6]$.

$$\begin{aligned} c_8[0\ 2\ 2\ 2\ 2\ 4\ 6\ 6] &= 2c_4[1\ 1\ 1\ 1]c_4[0\ 2\ 3\ 3] \ + \ 2c_4[0\ 1\ 1\ 2]c_4[1\ 1\ 3\ 3] \\ &= 2(-1)(4) + 2(4)(2) \quad \text{from section 1.11} \\ &= 16 \end{aligned}$$

This relationship leads to the following combinatorial statement.

11.16.4 **Proposition** If $c_{mn}(mv) \neq 0$, then v can be split into m sequences of n numbers whose sums are each divisible by n.

Proof. If the left side of equation (17) is non-zero, the sum on the right must have a non-empty range. Hence there must be a partition of the required form. □

11.17 The EGZ Theorem.

The above Proposition 11.16.4 deduces a combinatorial result concerning a multiset v given that its circulant determinantal coefficient is non-zero. This is reminiscent of Proposition 10.5.3.

We believe that in both examples that the non-zero coefficient condition can be replaced by the weaker condition that v be a null multiset. We can prove this assertion in the case of Proposition 11.16.4 using a theorem of Erdös, Ginzburg, and Ziv. First we restate Proposition 11.16.4 with a weaker condition.

11.17.1 **First Assertion** Pick any mn whole numbers, with or without repetitions, whose sum is divisible by mn. Then, the mn numbers can be partitioned into m parts of n numbers each whose sum is divisible by n.

Here is an equivalent and more intuitive form:

Fill a rectangular table of m rows and n columns with arbitrary whole numbers so that their average is also a whole number. Then, the numbers can be rearranged so that the average of each row is a whole number.

In fact we shall prove a slightly different statement which implies the above whereby the requirement of divisibility by mn is weakened to divisibility by only n.

11.17.2 **Second Assertion** Pick any mn whole numbers, with or without repetitions, whose sum is divisible by n. Then, the numbers can be partitioned so that each part contains n numbers whose sum is divisible by n.

11.17.3 **Definition** We shall say that a multiset of integers is n-**null** if the sum of its elements is divisible by n. We shall say that it is an **exact** n-**null** multiset if it n-null and contains exactly n elements.

We now state our third assertion, namely, the EGZ Theorem.

11.17.3 **The EGZ Theorem** Every multiset of $2n-1$ whole numbers contains an exact n-null sub-multiset.

We defer the proof until we have shown that the three assertions are equivalent, and that the theorem need only be proved for n prime.

The theorem statement cannot be strengthened by reducing the size of the given multiset. For instance, the multiset consisting of $n-1$ zeroes and $n-1$ ones has no sub-multiset of the required form.

It is clear that the EGZ Theorem implies the Second Assertion since we can use EGZ to successively remove exact n-null sub-multisets from the mn elements of the second assertion until only n elements are

left. Contrariwise, the Second Assertion with $m = 2$ implies the Second Assertion. Hence, the second and third assertions are equivalent.

In fact, the second and first assertions are also equivalent. To see this we note that both assertions depend only on the congruence class mod n of the multiset members -- we can add any multiple of n to any element without affecting the conditions or conclusions of either assertion.

Suppose that $[v]$ is a multiset satisfying the conditions of the Second Assertion. Then, $\sum[v] \equiv sn \pmod{mn}$ for some integer s. By the foregoing we can subtract sn from any element of v giving an mn-null multiset v' which satisfies the conditions of the First Assertion. Hence, if the First Assertion holds, then so does the Second.

11.17.4 **Definition** We shall call n a **fine** number if the Second Assertion (and therefore, each of the three assertions) holds for modulus n and for all m.

11.17.5 **Proposition** If n is divisible by only fine primes then n is fine.

Proof. The proposition is trivially true for $n = 1$. Assume inductively that it is true for all $n' < n$.

Let v satisfies the conditions of the Second Assersion, and suppose that n is divisible only by fine primes. If n is prime, we are done. So assume that $n = pn_1$ where p is prime and therefore fine. Considering v arranged into a rectangle V of mn_1 rows by p columns, it follows that v can be rearranged within the rectangle V so that each row is p-null. Let the row sums be $s = (s_0, s_1, \ldots, s_{mn_1-1})$, and let r be the sequence s divided throughout by p. Then, $\sum r$ is divisible by n_1. Arrange r into a rectangle R of m rows by n_1 columns. Since n_1 is divisible by only fine primes, by induction hypothesis, n_1 is fine. Hence, r can be rearranged within R so that each row in R is n_1-null. Now replace each r_i by s_i in the rectangle R. We obtain a rectangle whose every row sum is divisible by $pn_1 = n$. But, each s_i is a sum of a row in the rectangle V. Replace each s_i by its corresponding row in V. We obtain a rectangle of m rows and n columns containing the multiset v whose every row sum is divisible by n as required. □

11.17.6 **Corollary** The three assertions hold iff every prime is fine. □

We are now ready to prove the EGZ Theorem. In the propositions which follow, if $X, Y \subset \mathbb{Z}_n$, then $X + Y$ is to mean the set of all sums of pairs from X and Y; that is, $\{x + y \vdash x \in X, y \in Y\} \subset \mathbb{Z}_n$.

11.17.7 **The Cauchy-Davenport Lemma**

If p is a prime, and A, B are two nonempty subsets of $\mathbb{Z}_p$, then $|A + B| \geq \min\{p,\ |A| + |B| - 1\}$.

Proof. [AD]

We do an induction on $|B|$. It is trivial for $|B| = 1$. So we assume it holds for every A' and B' with $|B'| < |B|$.

We can assume we have A and B with $|A| < p$, $2 \leq |B| < p$.

Suppose first that $A \cap B$ is a nonempty proper subset of B. In this case, one can apply the induction hypothesis to $A' = A \cup B$ and $B' = A \cap B$ and obtain the desired result because $A' + B' \subset A + B$ and $|A'| + |B'| = |A| + |B|$. Hence,

$$|A + B| \ \geq\ |A' + B'| \ \geq\ \min\{p,\ |A'| + |B'| - 1\} \ =\ \min\{p,\ |A| + |B| - 1\}$$

In case $A \cap B$ is not a nonempty, proper subset of B we shall show that there is a $c \in \mathbb{Z}_p$ such that $(B+c) \cap A$ is a nonempty proper subset of $(B+c)$ and hence the result follows as before because $|(B + c) + A| = |B + A|$.

Suppose for a contradiction that such an element c does not exist. Then all translates of B in $\mathbb{Z}_p$ are either entirely in A or disjoint from it. So, if $b_1 + c \in A$ for some $b_1 \in B$, then $b + c \in A$ for every $b \in B$. For any $b_1 \in B$, $a \in A$ set $c = a - b_1$. Trivially, $b_1 + c \in A$. Therefore, $b_2 + c = a + b_2 - b_1 \in A$ for all $b_2 \in B$. But $a \in A$ is arbitrary, so $A + d \subset A$ where $d = b_2 - b_1$. Since $|B| \geq 2$, we can pick $b_2 \neq b_1$; that is, we can guarantee $d \neq 0$. So given $a \in A$, then A also contains $\{a, a + d, a + 2d, a + 3d, \ldots\} = \mathbb{Z}_p$ because p is prime. This contradicts our assumption that $|A| < p$. □

11.17.3 **The EGZ Theorem** Every multiset of $2n-1$ whole numbers contains an exact n-null submultiset.

Proof. [AD]

By Proposition 11.17.5 and its corollary, we need only prove the theorem for $n = p$, prime.

Let the multiset be $[a]$ where a is the sequence $(a_1, a_2, \ldots, a_{2p-1})$. Relabel so that the sequence is sorted in ascending order, $a_1 \leq a_2 \leq \ldots < a_{2p-1}$. If $a_i = a_{i+p-1}$ for some $i \leq p-1$, then a_i would have multiplicity of p (in $\mathbb{Z}_p$) and the desired result follows. So we can assume that this is not case. Define $A_i = \{a_i, a_{i+p-1}\}$, for $1 \leq i \leq p-1$. By repeated application of the Cauchy-Davenport Lemma, we conclude that $|A_1 + A_2 + \ldots + A_{p-1}| = p$, and hence every element of $\mathbb{Z}_p$ is a sum of precisely $p-1$ of the first $2p-2$ elements of the sequence a. In particular, $-a_{2p-1}$ is such a sum, supplying the required p-null submultiset. □

There are several other proofs of this celebrated theorem; the above proof using the Cauchy-Davenport Lemma seems to be the simplest and most direct. See for example [AD] and [Pan]; these two papers also suggest various generalizations.

Chapter 12.
Circulants over Finite Fields

The most basic question we can ask in the study of circulants over a finite fields is the structure of the units in the circulant ring. With one exception, we shall provide a complete description of the isomorphism class of the unit group. But, we shall only provide a method of constructing these unit groups assuming generators to the units of various fields are given.

We shall start with the notations to be used here which differ slightly from the main text.

12.1 **Notation.**

(i) Denote the set of units in $\mathbf{circ}_n(F)$ by $\mathbf{circ}_n^*(F)$.

(ii) The symbol p will be reserved for a prime, and q will be reserved for some positive power of p.

(iii) We shall use $\mathbb{F}_p$ (not $\mathbb{Z}_p$) to denote a field of p elements. Likewise, $\mathbb{F}_q$ shall be a field of $q = p^m$ elements.

(iv) $\Phi_n(x)$ will as usual denote the n^{th} cyclotomic polynomial, and $\phi(n)$, the Euler function, will denote its degree.

(v) If an element generates the entire group of units it is called a *primitive* element.

The finite characteristic of the field causes some complications. For example, the Fourier matrix is singular if the characteristic divides n, the order of the circulants. Indeed, we must regrettably exclude this case from the subsequent. However, finite fields do have some compensations. The first theorem, though standard, might be quite surprising to those familiar only with fields of characteristic zero.

12.2 **Theorem**

(i) Any two finite fields having the same number of elements are isomorphic.

(ii) The multiplicative group of non-zero elements of a finite field is cyclic.

Proof. See [Weil] □

As a simple application of part *(i)* of Theorem 12.2, we shall prove a corollary which brings home the difference between finite fields and those of characteristic zero.

12.3 **Corollary** If integers $m, n > 1$ have no square root in $\mathbb{F}_p$, then $\mathbb{F}_p(\sqrt{m}) = \mathbb{F}_p(\sqrt{n})$.

Note: Not only are the two fields isomorphic, they are equal.

Proof. By the theorem, there exists a field isomorphism $\beta : \mathbb{F}_p(\sqrt{m}) \to \mathbb{F}_p(\sqrt{n})$.

$$\therefore 0 = \beta(0) = \beta\left((\sqrt{m})^2 - m\right) = \left(\beta(\sqrt{m})\right)^2 - \beta(m)$$

showing that $x^2 - \beta(m)$ has a solution in $\mathbb{F}_p(\sqrt{n})$. But, $\beta(m) = \beta(1 + 1 + \cdots + 1) = m\beta(1) = m$. □

We shall start by treating some easy cases in order to get an idea of the issues involved. The technique (as in the treatment of the integer circulants) is to concentrate on the eigenvalues since their behavior under circulant multiplication is the easiest to analyze. But to connect the circulants with their eigenvalues uniquely, we need assurance that there is a matrix which diagonalizes the circulants. Recall that in complex domains, we used the Fourier matrix for this purpose. However, the Fourier matrix has an irrational denominator, $\sqrt{n}$, which normalizes the matrix. But we do not need a unitary matrix just for diagonalization, so we avoid the complications of the $\sqrt{n}$ by eliminating it, leaving us with the simpler task of proving that the Vandermonde matrix $V = \left(\zeta^{ij}\right)_{i,j}$ is non-singular.

12.4 **Proposition** Let ζ be a primitive n^{th} root of unity in a field of characteristic p. Let V be the $n \times n$ Vandermonde matrix given by $V_{i,j} = \zeta^{ij}$. If $p \nmid n$, then V is non-singular.

Proof. We compute the determinant of V. The Vandermonde formula gives

$$\det V \;=\; \prod_{i>j}(\zeta^i - \zeta^j)$$

$$\therefore\ \pm\det V^2 \;=\; \prod_{i>j}(\zeta^i-\zeta^j)\prod_{i<j}(\zeta^i-\zeta^j) \;=\; \prod_{i\neq j}(\zeta^i-\zeta^j) \;=\; \prod_{i=0}^{n-1}\zeta^i\prod_{j\neq i}(1-\zeta^{j-i})$$

$$=\; \zeta^{1/2\,n(n-1)}\left(\prod_{k=1}^{n-1}(1-\zeta^k)\right)^n \;=\; \pm\Phi_n(1)^n \;=\; \pm n^n$$

We are given that $p\nmid n$. Therefore, $\det V \not\equiv 0 \pmod p$. □

The first easy case is when $\mathbb{F}_p$ contains a primitive n^{th} root of unity.

12.4.1 **Proposition** Suppose $p\equiv 1 \pmod n$, then $\mathbf{circ}_n^*(\mathbb{F}_p) \;\approx\; \mathbb{Z}_{p-1}^n$.

Proof. In this case, $\mathbb{F}_p$ contains a primitive n^{th} root of unity, ζ, say. The matrix $V=\left(\zeta^{ij}\right)$ consists of eigenvectors of the circulants. Therefore, $\lambda_i(c)=(Vc)_i$ for all $c\in\mathbf{circ}_n(\mathbb{F}_p)$. Clearly, $V\in \mathrm{M}_n(\mathbb{F}_p)$. So, $\lambda_i(c)\in\mathbb{F}_p$.

Now, V is also a diagonalizing matrix for $\mathbf{circ}_n(\mathbb{F}_p)$. and the resulting map, λ, is a bijection iff V is non-singular. By Proposition 12.4, this is so provided $p\nmid n$. But, we are given that $p\equiv 1 \pmod n$, $\therefore p>n,\ \therefore p\nmid n$.

Consequently, F is invertible, and the circulants can be simultaneously diagonalized to $F^{-1}\mathbf{circ}(\mathbb{F}_p)F$ which must be the direct sum, $\mathbb{F}_p^n$, whose unit group is $\mathbb{Z}_{p-1}^n$. □

12.5 **Corollary** For $p\geq 3$, $\mathbf{circ}_2^*(\mathbb{F}_p) \;\approx\; \mathbb{Z}_{p-1}\oplus\mathbb{Z}_{p-1}$. □

Proposition 12.4.1 gives the extreme case where the polynomial x^n-1 completely splits in $\mathbb{F}_p$. We now treat the opposite extreme, where the n^{th} cyclotomic polynomial, $\Phi_n(x)$, is irreducible over $\mathbb{F}_p$.

12.6 **Proposition** If $\Phi_n(x)$ is irreducible over $\mathbb{F}_q$, then the Galois group for the splitting field of Φ_n over $\mathbb{F}_q$ is cyclic of order $\phi(n)$.

Proof. Let ζ be a primitive n^{th} root of unity in the field extension $\mathbb{F}_q(\zeta)$. Let G be the Galois group of this extension. We shall construct G.

Let $\alpha\in G$. Then, α must permute the roots of $\Phi_n(x)$. Therefore, $\alpha:\zeta\mapsto\zeta^t$ for some t coprime to n. Call this map α_t. Extend α_t to all of $\mathbb{F}_q(\zeta)$; we see that its action on a general field element is

$$\alpha_t : c_0+c_1\zeta+c_2\zeta^2+\cdots+c_{n-1}\zeta^{n-1} \;\mapsto\; c_0+c_1\zeta^t+c_2\zeta^{2t}+\cdots+c_{n-1}\zeta^{(n-1)t}$$

$$\text{That is, } \alpha_t:\lambda_1(c)\;\mapsto\;\lambda_t(c)$$

However, the representation $\lambda_1(c)=c_0+c_1\zeta+c_2\zeta^2+\cdots+c_{n-1}\zeta^{n-1}$ is not unique, so we need to verify that α_t is well-defined. Assume there is a linear dependency between $1,\zeta,\zeta^2,\ldots,\zeta^{n-1}$, let us say,

$$1\;+\;f_1\zeta\;+\;f_2\zeta^2\;+\;\cdots\;+\;f_{n-1}\zeta^{n-1}\;=\;0$$

Let $f(x)$ denote the polynomial with coefficients $f_0,f_1,\ldots,f_{n-1}$ so that the linear dependecy is equivalent to $f(\zeta)=0$. Then, $\Phi_n(x)\,|\,f(x)$. Clearly, the converse also holds, $\Phi_n(x)\,|\,f(x)\;\Rightarrow\;f(\zeta)=0$. Hence, all linear dependencies over $\mathbb{F}_q$ between the roots of unity reduce to $\Phi_n(\zeta)=0$.

So suppose $\lambda_1'=\lambda_1+\kappa\Phi_n(\zeta)$ for some $\kappa\in\mathbb{F}_p(\zeta)$. Then,

$$\alpha_t\left(\lambda_1+\kappa\Phi_n(\zeta)\right) \;=\; \alpha_t(\lambda_1)\;+\;\alpha_t(\kappa)\alpha_t(\Phi_n(\zeta)) \;=\; \alpha_t(\lambda_1)\;+\;\alpha_t(\kappa)\Phi_n(\zeta^t) \;=\; \alpha(\lambda_1)$$

The last equation follows from the fact that ζ^t is primitive, and so is a root of $\Phi_n(x)$.

This shows that every α_t is well-defined for every t coprime to n. We can therefore pick t to be a primitive residue mod n. With this choice, α_t becomes a generator for G, and α_t has the same order as t mod n, namely $\phi(n)$. □

12.7 **Proposition** Let n, p be distinct primes, and suppose that the cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{F}_q$, Then, $\mathbf{circ}_n^*(\mathbb{F}_q) \approx \mathbb{Z}_{q-1} \oplus \mathbb{Z}_{q^{n-1}-1}$.

Proof. Proposition 12.6 and its proof showed that the Galois group of the extension $\mathbb{F}_p(\zeta)/\mathbb{F}_p$ is generated by α_t where $\alpha_t : \zeta \mapsto \zeta^t$ and t is coprime to n. Hence, if we are given λ_1 as the eigenvalue of a circulant in $\mathbf{circ}_n(\mathbb{F}_p)$, then by repeatedly applying α_t we can derive $\lambda_t, \lambda_{t^2}, \lambda_{t^3}, \ldots$. Since t is primitive mod n, the set $\{1, t, t^2, t^3, \ldots\}$ equals the set $\{1, 2, \ldots, n-1\}$. Thus, via α_t, λ_1 determines $\{\lambda_1, \lambda_2, \ldots, \lambda_{n-1}\}$.

Now c is in the unit group iff all its eigenvalues are non-zero. By the above, this is equivalent to requiring $\lambda_0(c) \in \mathbb{F}_q^*$, and $\lambda_1(c) \in \mathbb{F}_q(\zeta)^*$. By Theorem 12.2, we can pick primitive elements in g in $\mathbb{F}_q^*$, and γ in $\mathbb{F}_q(\zeta)^*$. Define M to be the set of vectors

$$M \;=\; \left\{ \left(g^a, \gamma^b, \alpha_t(\gamma^b), \ldots, \alpha_t^{n-2}(\gamma^b)\right) \vdash a, b \in \mathbb{N} \right\}$$

By Proposition 7.2.9.1, the eigenvalues of all circulants with components in the base field must be of the above form. Hence, M contains all possible eigenvalue vectors.

$$\therefore\; \mathbf{circ}_n^*(\mathbb{F}_q) \;\approx\; \langle g \rangle \oplus \langle \gamma \rangle$$

Now, $\langle g \rangle \approx \mathbb{Z}_{q-1}$. The field $\mathbb{F}_q(\zeta)$ is of degree $n-1$ over $\mathbb{F}_q$, and so has q^{n-1} elements. Therefore, $|\mathbb{F}_q(\zeta)^*| = q^{n-1} - 1$. Hence, $\langle \gamma \rangle$ is cyclic of order $q^{n-1} - 1$. □

One wonders whether there are congruence fields over which $\Phi_n(x)$ is reducible, but does not completely split into linear factors. The answer is "yes", as will be shown in all generality by Theorem 12.9. However, the theorem gives no indication what the factorization of $\Phi_n(x)$ might be. So that the reader might appreciate seeing a concrete example, we shall present a non-trivial factorization of $\Phi_5(x)$.

12.8 **Proposition**

(i) $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ is reducible over the field $\mathbb{F}_p$ iff $p \equiv \pm 1 \pmod 5$.

(ii) If $p \equiv -1 \pmod 5$ then there exists $e \in \mathbb{Z}$ with $e(e+1) \equiv 1 \pmod p$ such that

$$\Phi_5(x) \;\equiv\; \left(x^2 - ex + 1\right)\left(x^2 + (e+1)x + 1\right) \pmod p$$

Proof. We first eliminate the simplest case: $\Phi_5(x)$ splits into linear factors iff $\mathbb{F}_p$ contains a primitive fifth root of unity iff $p \equiv 1 \pmod 5$.

We now assume that $p \not\equiv 1 \pmod 5$, and that $\Phi_5(x)$ has no linear factor in $\mathbb{F}_p$.

The most general possible factorization remaining is into quadratic factors, $Q_1(x), Q_2(x)$, say.

$$\Phi_5(x) \;\equiv\; Q_1(x)Q_2(x) \;\equiv\; (ax^2 + bx + c)(dx^2 - ex + f) \pmod p$$

Since the coefficient of x^4 is 1, we can divide Q_1 by a, multiply Q_2 by a, and redefine b, c, e, f to obtain

$$\Phi_5(x) \;\equiv\; (x^2 + bx + c)(x^2 - ex + f)$$

Now, c is the product of two roots, both of which are primitive 5^{th} roots of unity. Therefore, $c^5 \equiv 1$. But, by hypothesis, $\mathbb{F}_p$ has no primitive fifth root of unity. Therefore, $c \equiv 1$. Likewise, $f \equiv 1$ which gives us

$$\Phi_5(x) \;\equiv\; (x^2 + bx + 1)(x^2 - ex + 1)$$

Equating coefficients, we get the following equations:

$$\begin{aligned} b \;&\equiv\; e + 1 \\ be \;&\equiv\; 1 \\ \therefore\; e^2 + e - 1 \;&\equiv\; 0 \end{aligned} \tag{2}$$

The discriminant of the quadratic in (2) is $\sqrt{5}$. Hence, a solution to (2) exists iff 5 is a quadratic residue mod p iff $p \equiv \pm 1 \pmod 5$ by the Quadratic Reciprocity Theorem. Since we are assuming $p \not\equiv 1$, we have shown that the quadratic factorization of Φ_n implies $p \equiv -1 \pmod 5$.

The converse follows by reversing the proof. From $p \equiv -1 \pmod 5$ we deduce $\sqrt{5} \in \mathbb{F}_p$, which yields the desired factorization. □

We now state and prove the standard theorem which describes exactly to what degree the cyclotomic polynomial factors over $\mathbb{F}_p$.

12.9 **Theorem**

$\Phi_n(x)$ factors over $\mathbb{F}_q$ into irreducible polynomials of degree w where w is the order of q mod n.

Proof. Let $\mathbb{F}_{q^f}$ be the full splitting field for $\Phi_n(x)$.

We are given $q^w - 1 \equiv 0 \pmod n$ and w is least such. For definiteness, $q^w - 1 = kn$ say. Now, the group of units in $\mathbb{F}_{q^w}$ has a generator, u say. Then, $1 = u^{q^w-1} = (u^k)^n \in \mathbb{F}_{q^w}$. That is, u^k is a primitive n^{th} root of unity in $\mathbb{F}_{q^w}$ which must therefore contain the splitting field for $x^n - 1$, and hence for $\Phi_n(x)$. This shows that $q^f \,|\, q^w$.

Suppose $f < w$. Let v be a primitive n^{th} root of unity in $\mathbb{F}^*_{q^f}$. The subgroup generated by v has order n which must divide the order of the unit group, $q^f - 1$. This contradicts the minimality of w. Therefore, $f = w$.

Let $Q(x)$ be an irreducible factor of $\Phi_n(x)$ (with $Q = \Phi_n$ if Φ_n is irreducible.) Let E be the splitting field of $Q(x)$ over $\mathbb{F}_q$. Obviously, $E \subset \mathbb{F}_{q^f}$. But, E contains a primitive n^{th} root of unity, ζ say. It therefore contains all powers of ζ, and so all n^{th} roots of unity. Hence, $E = \mathbb{F}_{q^f}$. Now, $|E^*| = q^{\deg(Q)} - 1$. So, $q^{\deg(Q)} - 1 = q^f - 1 = q^w - 1$. That is, $\deg(Q) = w$. □

12.10 **Corollaries of the Theorem.**

The dimension of the splitting field of $x^n - 1$ over $\mathbb{F}_q$ is w, and so the splitting field has q^w elements.

Suppose $\Phi_n(x) = Q_1(x)Q_2(x)\cdots Q_r(x) \in \mathbb{F}_q[x]$ where each $Q_i(x)$ is irreducible mod q. Since $\Phi_n(x)$ has no repeated roots, the Q_i polynomials are mutually coprime in pairs, and, by the theorem, they all have the same degree, w, equal to the order of q mod n. Therefore, $\phi(n) = rw$.

The primitive n^{th} roots of unity are partitioned into sets belonging to the different irreducible factors of Φ_n. We shall denote the set to which any one root, ξ say, belongs by $[\xi]$, and we shall relabel the irreducible polynomials with their root sets, thus: $Q_{[\xi]}(x)$. However, we shall usually omit the brackets in which case it is to be understood that Q_ξ stands for $Q_{[\xi]}$.

12.11 **Corollary (The Galois Group).** Let G be the Galois group of the extension $\mathbb{F}_q(\zeta)/\mathbb{F}_q$. With the notation of the theorem, $G \approx \mathbb{Z}_w$.

Proof. G permutes the elements within each partition set, $G \times [\xi] = [\xi]$ for all roots ξ of $\Phi_n(x)$. Let $\tau \in G$. Then, $\tau : \zeta \mapsto \zeta^t$ for some $t > 1$. This action on ζ defines the action of τ on the whole field. For example, given any $j \in \mathbb{Z}_{\phi(n)}$, $\tau : \zeta^j \mapsto \zeta^{ij}$. Hence,

$$\tau : a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{n-1}\zeta^{n-1} \;\mapsto\; a_0 + a_1\zeta^t + a_2\zeta^{2t} + \cdots + a_{n-1}\zeta^{(n-1)t} \tag{3}$$

This is very similar to the case of irreducible $\Phi_n(x)$, the difference being that ζ^t is restricted to be in the same partition as ζ. Applying the τ automorphism successively we see that we generate a set S_τ where

$$S_\tau \;=\; \{\zeta, \tau(\zeta), \tau^2(\zeta), \ldots, \tau^i(\zeta), \ldots\} \;=\; \{\zeta, \zeta^t, \zeta^{t^2}, \ldots, \zeta^{t^i}, \ldots\} \subset [\zeta]$$

and so S_τ consists of at most w elements. Therefore, $t^h \equiv 1 \pmod n$ for some $h \le w$. Let us try the map $\rho(\zeta) = \zeta^q$. By the assumptions of the theorem, the order of q mod n is precisely w, which means, $|S_\rho| = w$, and $G = \langle\rho\rangle \approx \mathbb{Z}_w$. □

We shall continue to use ρ to denote a generating element of G.

12.12 **Finding a Basic Set of Eigenvalues.** In Proposition 12.6, we applied the Galois group to the one eigenvalue λ_1 and derived the values of $\lambda_2, , \ldots, \lambda_{n-1}$. In the more general case of reducible $\Phi_n(x)$, we no longer have enough maps in the Galois group which can be used in equation (3) to derive all eigenvalues from one.

Applying the automorphism ρ to equation (3), we get the sequence,

$$\lambda_1 \xrightarrow{\rho} \lambda_q \xrightarrow{\rho} \lambda_{q^2} \xrightarrow{\rho} \cdots$$

and this defines the w eigenvalues in the set $\{\lambda_i \vdash \zeta^i \in [\zeta]\}$. Let us call such a set an eigenvalue root set, and denote it by $[\lambda_\zeta]$. It is clear that the eigenvalue roots sets are orbits under the Galois group. Therefore, we can no longer deduce all the eigenvalues given only one. In order to see to what degree circulants are constrained by a value for one eigenvalue, we turn to the circulant space. This leads us to consider $\ker \lambda_1$.

Let $a \in \mathbf{circ}_n(\mathbb{F}_q)$, and let $a(x)$ be its representer polynomial. Then,

$$a \in \ker \lambda_1 \quad \Leftrightarrow \quad a(\zeta) = 0 \quad \Leftrightarrow \quad Q_\zeta(x) \,|\, a(x)$$

$$\therefore \ \ker \lambda_1 \ = \ (Q_\zeta(\mathrm{u}))$$

More generally,

$$\ker \lambda_j = (Q_\xi(\mathrm{u})) \quad \Leftrightarrow \quad \zeta^j \in [\xi] \quad \Leftrightarrow \quad \lambda_j \in [\lambda_\xi]$$

Suppose we have picked a value for μ for λ_1. Pick any $a(\mathrm{u}) \in \lambda_1^{-1}(\mu)$ where $a(x)$ is a representer polynomial. Then, taking the remainder of $a(x)$ mod $Q_\zeta(x)$, we see that there exist polynomials $a'(x), a''(x)$ such that

$$a(x) \ = \ a'(x) \ + \ Q_\zeta(x) a''(x) \tag{4a}$$

where $\deg a' < \deg Q_\zeta = w$, and $\deg a'' < n - w$. The polynomial a' satisfying (4a) is the standard representative for the set of circulants, a, which have eigenvalue $\lambda_1(a) = \mu$, and it is standard in the sense that it has the least degree.

The requirement that a is non-singular implies that a' is not the zero polynomial, otherwise the choice of a' is arbitrary, and completely specifies $\lambda_1(a)$, and all others in its eigenvalues root set, $[\lambda_\zeta]$.

If we now consider another eigenvalue, $\lambda_\xi \notin [\lambda_\zeta]$, we arrive at a similar formula,

$$a(x) \ = \ b'(x) \ + \ Q_\xi(x) b''(x) \tag{4b}$$

where $\deg b' < \deg Q_\xi = w$, $\deg b'' < n - w$, and b' is the standard representative for λ_ξ eigenvalue.

All formulæ such as (4a) and (4b) can be combined into a single formula:

$$a(x) \quad = \quad \sum_{[\xi]} L_\xi a_\xi(x) \prod_{[\gamma] \neq [\xi]} Q_\gamma(x) \quad = \quad \sum_{[\xi]} \left(\frac{\Phi_n(x)}{Q_\xi(x)} \right) L_\xi a_\xi(x) \tag{5}$$

The sum in (5) is over all root sets $[\xi]$, and L_ξ and a_ξ actually depend on $[\xi]$. L_ξ is a number to be determined, and a_ξ is the standard representative for the λ_ξ eigenvalue (and so $\deg a_\xi < w$). We now check what happens when we set $x = \eta$, an n^{th} root of unity. Every term but one in (5) is mapped to zero giving

$$\lambda_\eta(a) \ = \ a(\eta) \ = \ L_\eta a_\eta(\eta) \prod_{[\gamma] \neq [\eta]} Q_\gamma(\eta)$$

We now define

$$L_\eta \ := \ \prod_{[\gamma] \neq [\eta]} Q_\gamma(\eta)^{-1} \tag{6}$$

Giving,

$$\lambda_\eta(a) \ = \ a_\eta(\eta)$$

Formula (5) shows that we can simultaneously pick representative circulants $a', b', c', \ldots$ to satisfy independent choices of values for one member from each of r eigenvalue root sets.

Thus, we have our algorithm for picking general, non-zero eigenvalues yielding circulants in $\mathbf{circ}_n(\mathbb{F}_q)$. We pick representative roots from each of the r root sets, $[\xi_1], [\xi_2], \ldots, [\xi_r]$, say. For each ξ_i, we pick a non-zero eigenvalue μ_i, and we compute its standard representative a_i. This determines all other eigenvalues in the same eigenvalue root set. We do this for $i = 1, 2, \ldots, r$, and we construct the circulant $a(\mathrm{u})$ using formulæ (5) and (6).

It is clear from this procedure that there are r independent choices for eigenvalues, each of which can be set to a generator of the units in the field $\mathbb{F}_q(\zeta)$. Thus, we have proved

12.13 **Proposition** Let n, p be distinct primes, $q = p^m$, and let w be the order of q mod n. Then,

$$\mathbf{circ}_n^*(\mathbb{F}_q) \;\approx\; \mathbb{Z}_{q-1} \;\oplus\; \mathbb{Z}_{q^w-1}^{(n-1)/w} \qquad\qquad (n \text{ prime})$$

Proof. The initial summand comes from the direct summand corresponding to the λ_0 eigenvalue.

For the other summands, recall that the field $\mathbb{F}_q(\zeta)$ is of dimension w over $\mathbb{F}_q$, giving $q^w - 1$ non-zero elements.

Using the procedure described above we construct a group generator as follows. We set $\lambda_\xi = g$, a primitive element of $\mathbb{F}_{q^w}$. We apply the Galois map α_t to obtain the values of the other eigenvalues in $[\lambda_\xi]$. The remaining eigenvalues are set to 1.

We repeat this process for each eigenvalue root set, thus creating r independent generators of order $|\mathbb{F}^*(\zeta)| = q^w - 1$. □

We now consider compound n. We again start with a concrete case, namely $n = 6$. This will indicate how to proceed generally.

12.14 **Proposition** Let p be prime, $p \equiv -1 \pmod 6$, then $\mathbf{circ}_6^*(\mathbb{F}_p) \;\approx\; \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^2-1} \oplus \mathbb{Z}_{p^2-1}$.

Proof. The proviso that $p \equiv -1 \pmod 6$ means there is no third root of unity in $\mathbb{F}_p$. We shall denote a primitive root of $x^3 - 1$ by ω. Then, the splitting field of $x^6 - 1$ is $\mathbb{F}(\omega)$, and the primitive root is $-\omega$.

We construct a basis for the group of unit circulants of order 6. We choose circulants, c_0, c_3, c_1, c_2, with the following spectrum of eigenvalues:

$$\begin{aligned} \lambda(c_0) &= (g, 1, 1, 1, 1, 1) \\ \lambda(c_3) &= (1, 1, 1, g, 1, 1) \\ \lambda(c_1) &= (1, x, 1, 1, 1, \bar{x}) \\ \lambda(c_2) &= (1, 1, x, 1, \bar{x}, 1) \end{aligned} \tag{7}$$

where g is a primitive residue mod p, x is primitive in $\mathbb{F}(\omega)$, and $\bar{x}$ is the conjugate of x. These eigenvalues all obey the transformation rule of Proposition 7.2.9.1 which is equivalent to the condition that the circulants be in $\mathbf{circ}_6(\mathbb{F}_p)$. Also, the construction ensures that they generate independent cyclic subgroups of orders (respectively) $p - 1$, $p - 1$, $p^2 - 1$, and $p^2 - 1$. □

Let us describe the method used in the proof in generality.

We shall say that λ_i belongs to **residue class** h whenever $\gcd(i, n) = h$. In particular, λ_h belongs to its eponymous residue class. The importance of the residue class lies in the fact that all eigenvalues in residue class h lie in the same field, a subfield of $\mathbb{F}_q(\zeta^h)$.

In proving the proposition, we set one eigenvalue in each residue class to the generator of the unit group of its range, and we set the others in the residue class to conjugates of the first. The conjugates must be assigned in accordance with Proposition 7.2.9.1 else the circulant components will not be in the base field.

The two eigenvalues λ_0 and $\lambda_{n/2}$ (when n is even) form singleton residue classes, and their range is always the base field. More generally, λ_i has the same range as the first in its residue class, namely λ_d where $d = \gcd(i, n)$, and the range of λ_d is $\mathbb{F}_q\left(\zeta^{n/d}\right)$ where ζ is a primitive n^{th} root of unity.

It is possible that $\zeta^{n/D} \in \mathbb{F}_q$ for some $D \,|\, n$, in which case $\mathbb{F}_q(\zeta^{n/d}) = \mathbb{F}_q$ for all $d \,|\, D$. For example, with $p = 7$, $n = 30$, the sixth roots are in $\mathbb{F}_7$, but the primitive 30^{th} roots are not. This possibility is the reason

why there is a second formula offered in the next theorem. Although formulæ (9a) and (9b) are equivalent, (9b) segregates the terms which are in the base field from those in field extensions.

12.15 **Theorem** Let $q = p^m$ with p prime, $p \nmid n$. For each divisor $d \,|\, n$, define the function $w(d)$ to be the order of q mod d. Then,

$$\mathbf{circ}_n^*(\mathbb{F}_q) \quad = \quad \bigoplus_{d|\,n} \mathbb{Z}_{q^{w(d)}-1}^{\phi(d)/w(d)} \tag{9a}$$

Let e be a maximal integer dividing n such that $\mathbb{F}_q$ contains a primitive e^{th} root of unity. Then, e is greatest such. Define $\delta := \sum_{d|\,e} \phi(d)$. We have

$$\mathbf{circ}_n^*(\mathbb{F}_q) \quad = \quad \mathbb{Z}_{q-1}^{\delta} \,\oplus\, \bigoplus_{d\nmid e,\ d|\,n} \mathbb{Z}_{q^{w(d)}-1}^{\phi(d)/w(d)} \tag{9b}$$

Proof. Formula (9a) is nothing more than an application of Proposition 12.13 to various residue classes of eigenvalues.

Let ζ denote a primitive n^{th} root of unity in $\mathbb{F}$ or some extension of it. Note that, if $r \,|\, n$, $\zeta^{n/r}$ is a primitive r^{th} root of unity.

Let c be an arbitrary circulant, $c \in \mathbf{circ}_n(\mathbb{F}_q)$, and let its eigenvalues be $\lambda_0 = \lambda_0(c)$, $\lambda_1 = \lambda_1(c)$, …, $\lambda_{n-1} = \lambda_{n-1}(c)$.

We start with formula (9a). It consists of direct sums of the cycles generated by the eigenvalues. Let λ_i be an eigenvalue in residue class $\gcd(i,n)$, and let $d = n/\gcd(i,n)$. Then, λ_i is an arbitrary linear combination of powers of $\zeta^{n/d}$. Hence, λ_i lies in the splitting field for $x^d - 1$. By Theorem 12.9, this field is isomorphic to $\mathbb{F}_{q^{w(d)}}$. In particular, it has a multiplicative generator of period $q^{w(d)} - 1$.

As in §12.12, we can pick $r = \phi(d)/w(d)$ independent generators for the residue class of λ_i producing a subgroup of r independent cycles of $q^{w(d)} - 1$ elements each. This completes the proof of formula (9).

Formula (9b) is derived from (9a) by segregating the terms originating from eigenvalues which must take values in the base field. In the first equation, these terms are those having $w(d) = 1$. All that remains to show is that maximality of e implies it is largest.

Let us call r a **base index** if $r \,|\, n$ and $\zeta^{n/r} \in \mathbb{F}_q$ (that is, $\mathbb{F}_q$ contains a primitive r^{th} root of unity). The key observation is that if r and s are base indices, then so is $\operatorname{lcm}(r,s)$. Indeed, we are given $\zeta^{n/r}, \zeta^{n/s} \in \mathbb{F}_q$. Therefore, $\zeta^{in/r}\zeta^{jn/s} = \zeta^{n(jr+is)/rs} \in \mathbb{F}_q$ for all $i,j \in \mathbb{Z}$. Let $\gcd(r,s) = h$. Then, we can pick i,j such that $jr + is = h$. With such a choice of i,j, we have $n(jr+is)/rs = n/\operatorname{lcm}(r,s)$. Hence, $\operatorname{lcm}(r,s)$ is also a base index. Taking the l.c.m. of all base indices yields a unique largest base index, namely e. □

With the information provided by the theorem, we can characterize the entire circulant ring.

12.15.1 **Corollary** With the same notation and conditions of the theorem,

$$\mathbf{circ}_n(\mathbb{F}_q) \quad \overset{\lambda}{\approx} \quad \bigoplus_{d|\,n} \mathbb{F}_{q^{w(d)}}^{\phi(d)/w(d)} \quad \approx \quad \mathbb{F}_q^{\delta} \,\oplus\, \bigoplus_{d\nmid e,\ d|\,n} \mathbb{F}_{q^{w(d)}}^{\phi(d)/w(d)} \ \square$$

We conclude with a digression into cyclotomic theory. It is a question that arose in developing the above results when the author tried some computer computations to verify the theory. Let $\zeta = \zeta_n$ be an n^{th} root of unity, and suppose that $\zeta \notin \mathbb{F}_p$. The question is:

$$\text{When is} \quad \mathbb{F}_p(\zeta) \;\approx\; \mathbb{Z}(\zeta)/(p) \;?$$

It may appear intuitively true to many that $\mathbb{F}_p(\zeta)$ must be the same field as $\mathbb{Z}(\zeta)/(p)$. After all, $\mathbb{F}_p(\zeta)$ can certainly be identified with $\mathbb{Z}_p(\zeta)$ which is the integers reduced modulo p with ζ attached, whereas

$\mathbb{Z}(\zeta)/(p)$ sounds almost like the same thing: the integers with ζ attached reduced modulo p. Readers who find this convincing should consider the following fact: $1 + 5\zeta_5 + \zeta_5^2$ is a divisor of zero in $\mathbb{Z}(\zeta_5)/(19)$. We shall find a simple criterion for when this can happen.

This question is relevant to computation. The field $\mathbb{F}_p(\zeta)$ has no natural embodiment, and so can only be modelled on a computer using symbolic logic, whereas the ring $\mathbb{Z}(\zeta)/(p)$ is realized as a subset of the complex numbers reduced modulo p, and is easily modelled in computer languages that have complex arithmetic.

Denote the norm of z in $\mathbb{Q}(\zeta)/\mathbb{Q}$ by $\mathcal{N}(z)$.

12.16 **Lemma** Let $z \in \mathbb{Z}(\zeta)$, and let $\nu : \mathbb{Z}(\zeta) \to \mathbb{Z}(\zeta)/(p)$ be the natural map . Then, $\nu(z)$ is a divisor of zero iff $p \,|\, \mathcal{N}(z)$.

Proof. First assume that $\nu(z)$ is a divisor of zero. Then, there exists y such that $\nu(zy) = 0$ and $\nu(y) \neq 0$.

Let $\bar{z}$ be the product of the conjugates of z. Then, $0 = \nu(z\bar{z}y) = \nu(\mathcal{N}(z)y) = \mathcal{N}(z)^n\nu(y)$ since $\mathcal{N}(x) \in \mathbb{Z}$. But, if $\mathcal{N}(x)$ is not divisible by p, then it has an inverse mod p given by $\mathcal{N}(x)^{p-2}$. But this would mean that $\nu(y) = 0$. Contradiction. Therefore $p \,|\, \mathcal{N}(z)$. QED($\Rightarrow$).

If $p \,|\, \mathcal{N}(z)$ then $p \,|\, z\bar{z}$ where $\bar{z}$ is the product of the conjugates of z. Then, $\nu(z)\nu(\bar{z}) = 0$. □

12.17 **Lemma** Let $n > 2$, p be prime, $p \not\equiv 1 \pmod{n}$. Let $R = \mathbb{Z}(\zeta)/(p)$ where ζ is an n^{th} primitive root of unity. Then,

(i) R is a field iff if there does not exist $z \in \mathbb{Z}(\zeta) - \{0\}$ such that $p \,|\, \mathcal{N}(z)$.

(ii) When R is a field, it isomorphic to $\mathbb{F}_p(\zeta)$, the root field of $x^n - 1$ over $\mathbb{F}_p$.

Proof.

(i) The implication: field $\Rightarrow$ no divisors of zero is obvious, and no divisors of zero implies no zero norms by the previous lemma.

So assume that there are no zero norms. Then, there are no divisors of zero in R. Take any $z \in R - \{0\}$, and consider the sequence $z, z^2, \ldots, z^i, \ldots$. Since R is finite ($|R| = p^2$), this sequence must eventually repeat. Hence, $z^i = z^j$ for some $i < j$. Since there are no divisors of zero, we can cancel getting $z^{i-j} = 1$. We see that z is invertible with inverse z^{i-j-1}. QED*(i)*

(ii) If $\mathbb{Z}(\zeta)/(p)$ is a field, it is a field having p^2 elements, as is the field $\mathbb{F}_p(\zeta)$. The conclusion follows by Theorem 1.2. □

12.18 **Proposition** Let ζ be an n^{th} primitive root of unity in $\mathbb{C}$. Then,

$$\mathbb{Z}(\zeta)/(p) \text{ is a field} \quad \Leftrightarrow \quad p \text{ is a primitive residue mod } n$$

Proof.

Consider the following diagram.

$$\begin{array}{ccccc} \mathbb{Z}(\zeta) & \xleftarrow{\eta_1} & \mathbb{Z}[x] & \xrightarrow{\nu_2} & \mathbb{F}_p[x] \\ {\scriptstyle \nu_1}\downarrow & & & & \downarrow{\scriptstyle \eta_2} \\ \mathbb{Z}(\zeta)/(p) & ? & \xrightarrow{\alpha} & ? & \mathbb{F}_p(\zeta) \end{array}$$

where η_1, η_2 evaluate polynomials at $x = \zeta$ on their respective polynomial rings, and ν_1, ν_2 are the natural maps modulo the ideal (p) in their respective domains.

The putative map α is well-defined if $\ker \nu_1\eta_1 \subset \ker \eta_2\nu_2$. We compute $\ker \nu_1\eta_1$. We have $\ker \nu_1 = \{pz \vdash z \in \mathbb{Z}(\zeta)\}$. $\therefore$ $\ker \nu_1\eta_1 = \{pz + b(x)\Phi_n(x) \vdash z \in \mathbb{Z}(\zeta), b \in \mathbb{Z}[x]\}$.

Applying ν_2 to this kernel we get $\nu_2(\ker \nu_1\eta_1) = b(x)\Phi_n(x)$, and then, $\eta_2\nu_2(\ker \nu_1\eta_1) = 0$. Hence, α is well-defined, and since all maps are ring homomorphisms, α is also a ring homomorphism.

We now ascertain whether α is an isomorphism. We compute $\ker \eta_2\nu_2$. By Theorem 12.9, $\Phi_n(x)$ factors in $\mathbb{F}_p$ into $r = \phi(n)/w$ irreducible polynomials each of degree w where w is the order of p mod n.

$$\therefore \ \ker \eta_2 \ = \ (Q_1(x), Q_2(x), \ldots, Q_r(x))$$

$$\therefore \ \ker \eta_2\nu_2 \ = \ \big(Q_1(x), Q_2(x), \ldots, Q_r(x)\big) \ + \ pa(x)$$

where $a \in \mathbb{Z}[x]$ is arbitrary.

Clearly, $\nu_1\eta_1(\ker \eta_2\nu_2) = 0$ iff $r = 1$. That is, $\ker \nu_1\eta_1 = 0$ iff $w = \phi(n)$. But, no field can contain a non-trivial ideal. Therefore, $\mathbb{Z}(\zeta)/(p)$ is a field iff $w = \phi(n)$ iff p is a primitive residue mod n. □

12.19 **Corollary** Let $z \in \mathbb{Z}(\zeta_n)$ be a cyclotomic integer. Its norm, $\mathcal{N}(z)$, is divisible only by primes which are not primitive residues mod n. □

Appendix A
Basic Cyclotomic Theory

This appendix assumes knowledge of basic field theory as in Birkoff and McLane's "Survey of Modern Algebra".

A.1 **Cyclotomic Extensions.** Cyclotomic theory studies integral domains which are extended by the addition of a root of unity. The archetypical example is the addition of an n^{th} root of unity to the rational integers.

To extend an integral domain R to include all n^{th} roots of unity is to construct another domain E which is to include R and in which $x^n - 1$ splits. That is, E is contructed so that $x^n - 1$ factorizes into a product of linear factors of the form $x - e$ with $e \in E$.

In this text, we always denote a primitive n^{th} root of unity with ζ_n or ζ if n is understood. A root of unity, ζ, is an n^{th} **primitive root** of unity if $\zeta^n = 1$ and $n > 0$ is least such. There are $\phi(n)$ primitive n^{th} roots of unity where ϕ is the Euler function. The set of all n^{th} roots of unity is a cyclic group under multiplication. Each primitive root is a generator of this group.

When R is extended to include ζ we write the extension as $R(\zeta)$ or R_ζ. R_ζ is called a **cyclotomic** extension of R. If R is a field, then so is R_ζ, and R_ζ is called a **cyclotomic field extension**. Please note that **the** n^{th} cyclotomic field means specifically $\mathbb{Q}(\zeta_n)$, and **the** n^{th} cyclotomic domain means specifically $\mathbb{Z}(\zeta_n)$.

The polynomial $x^n - 1$ always factorizes over any ring. For example,

$$x^{20} - 1 \;=\; (x-1)(x+1)(x^2+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1)(x^8-x^6+x^4-x^2+1)$$

Over the integers, there is no further factorization possible: each of the given factors is irreducible over the rationals. Over other integral domains some, none, or all these factors might be reducible. For instance, when R is the Gaussian integers, $x^2 + 1$ will factorize, but no other.

A.2 **Cyclotomic Polynomials.** The factors appearing in the above reduction of $x^{20}-1$ are examples of **cyclotomic polynomials**. More generally, the n^{th} cyclotomic polynomial is defined to be that polynomial whose roots are exactly the primitive n^{th} roots of unity. In this text it is always denoted by the capital Greek letter phi:

$$\Phi_n(x) \;:=\; \prod\{x - \zeta \vdash \zeta^n = 1 \text{ and } \zeta^r \neq 1 \text{ for } r = 1, 2, \ldots, n-1\}$$

$\Phi_n(x)$ is irreducible over the rationals. Indeed, it is sometimes defined as the unique monic polynomial in $\mathbb{Z}[x]$ irreducible over the rationals which is zero at a complex primitive n^{th} root of unity, for instance at $\zeta_n = e^{2\pi\iota/n}$.

It can be shown that over $\mathbb{Q}$, $\Phi_n(x)$ is the highest degree irreducible monic polynomial dividing $x^n - 1$. In a fortuitous coincidence of notation, the degree of $\Phi_n(x)$ is $\phi(n) = |\mathbb{Z}_n^*|$.

A.3 **Other Examples of Cyclotomic Polynomials.** Let p and q be distinct primes.

(i) $\Phi_p(x) \;=\; x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1.$

(ii) Let $N = p^n$ with $n > 1$.

$$\Phi_N(x) \;=\; x^{N-N/p} \;+\; x^{N-2N/p} \;+\; \cdots \;+\; x^{2N/p} \;+\; x^{N/p} \;+\; 1 \;=\; \frac{x^N - 1}{x^{N/p} - 1}$$

(iii) $\Phi_{pq}(x) \;=\; \dfrac{x^{pq} - 1}{(x^p - 1)(x^q - 1)}(x - 1).$

(iv) (Palindromic) For all $n > 2$, $\quad \Phi_n(0) = 1,$ and $\; x^{\phi(n)}\, \Phi_n\left(x^{-1}\right) \;=\; \Phi_n(x).$

(v) $\Phi_{12}(x) = x^4 - x^2 + 1.$

(vi) $\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1.$

(vii) $\Phi_{75}(x) = x^{40} - x^{35} + x^{25} - x^{20} + x^{15} - x^5 + 1.$

(viii) $\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39}$
$+x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20}$
$+x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1.$

The last example shows that the non-zero coefficients of the cyclotomic polynomials are not necessarily ± 1. (The coefficients of x^{41} and x^7 in $\Phi_{105}(x)$ are both equal to -2.) Indeed, arbitrarily high coefficients are possible if N has enough prime factors.

A.4 **The Galois Group.** Let F be a field, and let $P(x)$ be an irreducible polynomial in $F[x]$ whose roots are primitive n^{th} roots of unity. Then $P \mid \Phi_n$. (If $F = \mathbb{Q}$, then $P = \Phi_n$.) Let ζ be one such root, $P(\zeta) = 0$. By definition, the Galois group of $F(\zeta)/F$, denoted by $\mathcal{G}(F(\zeta)/F)$, is that permutation group on the roots of P which can be extended to automorphisms of $F(\zeta)$.

The Galois groups of cyclotomic extensions are always abelian, and for the fields of interest here, namely, sub-domains of $\mathbb{C}$ and finite fields, they are always cyclic.

Let $G = \mathcal{G}(F(\zeta)/F)$, and let $\alpha \in G$. Then, $\alpha : \zeta \mapsto \zeta^j$ where ζ^j is another primitive n^{th} root of unity. But, ζ^j is a primitive n^{th} root of unity iff $j \in \mathbb{Z}_n^*$. Hence, $G \subset \{\zeta \mapsto \zeta^j \vdash j \in \mathbb{Z}_n^*\}$. In particular, $|G| \le \phi(n)$, and in fact, $|G| \,|\, \phi(n)$.

A.5 **Vector Space Basis.** Let F be a field which does not contain a primitive n^{th} root of unity. Then, F_ζ is an extension of dimension d where d is the degree of an irreducible polynomial dividing $\Phi_n(x)$. For the remainder of this section we shall suppose that $d = \phi(n)$, that is, we assume that $\Phi_n(x)$ is irreducible.

We can regard F_ζ as a vector space over F of dimension $f = \phi(n)$. For a basis, we can take the first f powers of ζ, $\mathcal{B} = \{1, \zeta, \zeta^2, \ldots, \zeta^{f-1}\}$. Let $\lambda_1(c) = \sum_i c_i \zeta^i$ be a linear combination of the n roots of unity. It is also a polynomial in ζ, and it can be reduced to a linear combination in $\mathcal{B}$ by reducing it as a polynomial modulo $\Phi_n(\zeta)$. This process in effect treats R_ζ as the quotient ring $R[x]/(\Phi_n(x))$.

In the special case of $F = \mathbb{Q}$, and $n = p$, prime, all but the highest power of ζ will be in the basis, and the formula for ζ^{p-1} is

$$\zeta^{p-1} = -1 - \zeta - \zeta^2 - \cdots - \zeta^{p-2}$$

A.6 **Cyclotomic Norm.**

The norm of an algebraic integer in an integral domain R plays a fundamental role in algebraic number theory in general and cyclotomic theory in particular. The norm of an algebraic integer z is the number of elements in the quotient ring $R/(z)$. Let Q be the field of quotients of R. It can be shown that the norm is always finite and is the least positive integer in the ideal generated by z, raised to the power of $\dim_Q Q(\zeta)$ divided by $\dim_Q Q(z)$. Arithmetically, this equals the product of z with all its algebraic conjugates all raised to a power $\dim_Q Q(\zeta)/\dim_Q Q(z)$. More simply, the norm is always given by

$$\mathcal{N}(z) = \prod_{\nu \in \mathcal{G}} \nu(z) \quad \text{where } \mathcal{G} \text{ is the Galois group of } Q(\zeta)/Q.$$

The function $\mathcal{N}$ is called the **cyclotomic norm**. The set $\nu(z)$ where $\nu \in \mathcal{G}$ are called the conjugates of z. Given an expression for z as polynomial in ζ, the conjugates can be obtained by substituting the various primitive roots of unity for ζ.

The norm is a multiplicative, non-zero function on R_ζ: $\mathcal{N}(z_1 z_2) = \mathcal{N}(z_1)\mathcal{N}(z_2)$ taking values in $\mathbb{N}$. It is invaluable for determining divisibility properties of cyclotomic integers.

The simplest example of a norm is the norm of an integer. Let $R = \mathbb{Z}(\zeta)$ where $\zeta = \zeta_{15}$, and let $n \in \mathbb{Z}$. We shall calculate $|R/(n)|$. As in §A.5 we take $\{1, \zeta, \zeta^2, \ldots, \zeta^7\}$ as a basis for $\mathbb{Q}(\zeta)$. Then, the

quotient ring $R/(n)$ is the set of all elements of the form $c_0 + c_1\zeta + c_2\zeta^2 + \cdots + c_7\zeta^7$ where each c_i is a residue modulo n. There are clearly n^8 such elements, so $\mathcal{N}(n) = n^8$. We get the same result using the product over the Galois group. There are $\phi(15)$ group elements, $\nu_h : \zeta \mapsto \zeta^h$ where $h \in \mathbb{Z}_{15}^*$. Therefore, $\mathcal{N}(n) = n\nu_2(n)\nu_4(n)\nu_7(n)\nu_8(n)\nu_{11}(n)\nu_{13}(n)\nu_{14}(n) = n^8$.

For a second example, let $\xi = 1+2\zeta^2 \in \mathbb{Z}(\zeta_{15})$. We substitute conjugates for ζ in ξ and multiply obtaining

$$\begin{aligned}
\mathcal{N}(\xi) &= (1+2\zeta^2)(1+2\zeta^4)(1+2\zeta^8)(1+2\zeta^{14})(1+2\zeta^{16})(1+2\zeta^{22})(1+2\zeta^{24})(1+2\zeta^{28}) \\
&= (1+2\zeta^2)(1+2\zeta^4)(1+2\zeta^{-7})(1+2\zeta^{-1})(1+2\zeta)(1+2\zeta^7)(1+2\zeta^{-6})(1+2\zeta^{-2}) \\
&= |1+2\zeta|^2 \cdot \left|1+2\zeta^2\right|^2 \cdot \left|1+2\zeta^4\right|^2 \cdot \left|1+2\zeta^7\right|^2 \\
&= 8.654181830\ldots \times 7.676522425\ldots \times 4.581886146\ldots \times 1.087409597\ldots \\
&= 331
\end{aligned}$$

We cheated at the end by using a computer to evaluate the absolute values. Our only excuse is that it would probably take another page of detailed calculations to derive the result in integer arithmetic.

As a final example, let $\xi = 1 + 2\zeta^5 \in \mathbb{Z}(\zeta_{15})$ then ξ is contained in the subdomain $\mathbb{Z}(\omega)$ where $\omega = \zeta^5 = \frac{1}{2}(-1+\sqrt{3}\iota)$. Hence, its norm can be calculated by taking a single product only and raising it to the power $\dim(\mathbb{Q}(\zeta)/\mathbb{Q}) \;/\; \dim(\mathbb{Q}(\omega)/\mathbb{Q}) = \phi(15)/\phi(3) = 4$.

$$\mathcal{N}(\xi) \;=\; (1+2\zeta^5)^4(1+2\zeta^{10})^4 \;=\; (1+2\omega)^4(1+2\omega^2)^4 \;=\; (5+2\omega+2\omega^2)^4 \;=\; 3^4$$

In general, the norm depends not only on the element but also on the domain and on the base ring. But, in here, the base ring is always the integers, and the domain is always cyclotomic, and so the norm depends only on the element and order of the cyclotomic domain. Hence, we can safely indicate which norm we mean by subscripting the norm symbol by the order of the cyclotomic domain. Thus, in the above example where $\xi = 1 + 2\zeta^5$, $\mathcal{N}_{15}(\xi) = 3^4$ as was shown, whereas $\mathcal{N}_3(\xi) = 3$.

A.7 **Integral Elements** The **integral elements** of a field over the rationals is the set of elements which are roots of a monic polynomial with integer coefficients. We have the following proposition for cyclotomic domains.

A.7.1 **Proposition**

(i) The set of integral elements of $\mathbb{Q}(\zeta_N)$ is $\mathbb{Z}(\zeta_N)$.
(ii) $\mathbb{Z}(\zeta_N) \cap \mathbb{Q} \;=\; \mathbb{Z}$. □ ([Lang1])

An integral domain, R, is said to be **integrally closed** if all its integral elements which are in its ring of quotients are actually in R.

It is known that all principal ideal domains are integrally closed.

Appendix B
The Cooley-Tukey Fast Fourier Transform

B.1 **Fast Fourier Transforms.** This appendix is brief introduction to methods which have been developed in the last 50 years for the efficient computations of Fourier transforms. Since a Fourier transform is just multiplication by the Fourier matrix, all these techniques apply to the computation of circulant eigenvalues.

The entire class of techniques are called Fast Fourier Transforms or FFT for short. Their importance and main application is in calculating frequency distributions from time series. Their commercial applications range from pattern recognition, to analysis of earthquakes, electronic circuit design, electical power transmission, acoustics, automotive engineering, aeronautics, and just about any engineering or scientific analysis involving periodic phenomena.

B.2 **Analysis of the Straightforward Method.** Let us estimate the number of arithmetic operations needed to compute a full set of eigenvalues, that is, the eigenvector, of a general circulant $c \in \mathbf{circ}_n(\mathbb{C})$ using the formula $\lambda(c) = Fc$ of §1.7 where F is the Fourier matrix.

We can suppose that the n^{th} roots of unity, $1, \zeta, \zeta^2, \ldots, \zeta^n$ are given to us; either they have been computed in advance or they are available from tables. We have $\lambda(c) = F_n c$ where F_n is the $n \times n$ Fourier matrix, which when written out is

$$\begin{array}{lllllllll}
\lambda_0 & = & a_0 & + & a_1 & + & \cdots & + & a_{n-1} \\
\lambda_1 & = & a_0 & + & a_1\zeta & + & \cdots & + & a_{n-1}\zeta^{n-1} \\
\lambda_2 & = & a_0 & + & a_1\zeta^2 & + & \cdots & + & a_{n-1}\zeta^{n-2} \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
\lambda_{n-1} & = & a_0 & + & a_1\zeta^{n-1} & + & \cdots & + & a_{n-1}\zeta
\end{array}$$

This method requires $n(n-1)$ additions, and $(n-1)^2$ multiplications. Denote the time required to do a single complex addition by A, and the time to a single complex multiplication by M, then the time required to compute the eigenvector using the Fourier matrix is T_F where

$$T_F \;=\; n(n-1)A + (n-1)^2 M$$

The expression 3.5.2.3*(ii)* (Restatement of the Circulant Decomposition Theorem) for the eigenvalues of the circulant shows a possibility of computing the eigenvector of order n without having to perform this many arithmetic operations. However, when this technique is analyzed we find that although there is improvement, the process is dominated by approximately $(\phi(n)/n)n^2$ operations required to calculate the set $L_{1|n}$ of eigenvalues, and this term still scales as n^2.

*B.*3 **The Cooley-Tukey Algorithm.** There is a much better FFT developed by Cooley following an idea of Tukey, and is now called the Cooley-Tukey FFT. This algorithm will always beat the above circulant decomposition algorithm.

Here is a brief description of the Cooley-Tukey FFT. We suppose that $n = pq$ for some $p, q > 1$. To avoid double subscripting, we shall temporarily write c_i as $c(i)$, ζ_n^x as $e_n(x)$, and $\lambda_i(c)$ as $\lambda[i](c)$.

$$\begin{aligned}
\lambda[i](c) &= \sum_{j=0}^{n-1} e_n(ij)\, c(j) \\
&= \sum_{j_1=0}^{q-1}\sum_{j_2=0}^{p-1} e_n\big((pj_1+j_2)(qi_1+i_2)\big)\; c(pj_1+j_2) \\
&\qquad\qquad \text{where } i_1 = \lfloor i/q \rfloor, i_2 = i \bmod q, j_1 = \lfloor j/p \rfloor, j_2 = j \bmod p \\
&= \sum_{j_1=0}^{q-1}\sum_{j_2=0}^{p-1} e_q(j_1 i_2)\, e_p(i_1 j_2)\, e_n\big(j_2 i_2\big)\; c(pj_1+j_2) \\
&= \sum_{j_2=0}^{p-1} e_n\big(qi_1 j_2 + i_2 j_2\big) \sum_{j_1=0}^{q-1} e_q(j_1 i_2)\, c(pj_1+j_2) \\
&= \sum_{j_2=0}^{p-1} e_n\big(j_2(qi_1+i_2)\big)\; \lambda^{(q)}[i_2](c[j_2])
\end{aligned}$$

where $c[j_2]$ is the circulant vector $\big(c(p+j_2),\, c(2p+j_2),\, \ldots,\, c(pq-p+j_2)\big)$

$$\therefore\ \lambda[qi_1+i_2](c) \;=\; \sum_{j_2=0}^{p-1} e_n\big(j_2(qi_1+i_2)\big)\; \lambda^{(q)}[i_2](c[j_2]) \tag{1}$$

This final formula requires the calculation of $\lambda^{(q)}[i_2](c[j_2])$ for $i_2 = 0, 1, \ldots, q-1$, and $j_2 = 0, 1, \ldots, p-1$. The time required for these calculations will be $pq(q-1)A + p(q-1)^2 M$. The results of these calculations are plugged into the above formula which will require a further time of $(p-1)(A+M)$ for every i, that is, $n(p-1)(A+M)$. When all the operations are tallied we get a total of

$$\begin{aligned}
T_c &= (pq(q-1) + pq(p-1))A \;+\; (p(q-1)^2 + pq(p-1))M \\
&= n(q+p)(A+M) + O(n)
\end{aligned} \tag{2}$$

Already, this beats the decomposition method at all values of $p, q > 2$. But the interesting feature of the Cooley-Tukey FFT is that the process of calculating eigenvalues of lower dimensional circulants can be applied again to the calculation of $\lambda^{(q)}[i_2](c[j_2])$ when q is compound. This opens up the possibility of a recursive calculation which applies the above method to reduce the calculation to circulants of prime dimension. Thus, by taking p to be the smallest prime dividing n at each step, the cost of executing this FFT method will be dominated by the q^2 operations required for the lower-order eigenvalue calculations until q approaches p^2. Thereafter, the process is dominated by qp^2.

Even the last step in the Cooley-Tukey FFT can be viewed as a collection of q calculations of eigenvalues for circulants of order p, and it is therefore also amenable to a recursive reduction when p is compound. To see this, in (1) fix i_2; and define a vector v, and eigenvalues μ (both depending on i_2) by

$$\begin{aligned}
v_j &:= e_n(ji_2)\lambda^{(q)}[i_2](c[j]) \\
\mu_i &:= \lambda[qi+i_2](c)
\end{aligned}$$

Equation (1) becomes

$$\mu_i \;=\; \sum_{j=0}^{p-1} \zeta_n^{qij} v_j \;=\; \sum_{j=0}^{p-1} \zeta_p^{ij} v_j, \quad i = 0, 1, \ldots p-1$$

That is, $\mu = F_p v$, which can also be reduced using the Cooley-Tukey method when p is compound.

Readers interested in frequency analysis of sample data, and who have some measure of control over the value of n, should be aware that there is an especially efficient FFT available when n is a power of 2 called the Bit-Reversal Method. It is based on a finding of Danielson and Lanczos. See [PFTV].

Glossary of Terms

In general, when a subscript or (non-exponent) superscript is omitted, it should be understood to be N unless otherwise indicated in the text.

General Mathematical Terms

Complex Domain	A subring of the complex numbers.
Cyclotomic	Pertaining to $\mathbb{Z}(\zeta)$ or $\mathbb{Q}(\zeta)$. Appendix A, §3.4, Ch.7
Kronecker product	A type of tensor product, §6.1.1
FFT	Fast Fourier Transform, see Appendix B.
Multiset	A set "counting multiplicities", or an "unordered" sequence.
Quotient Field	Fractions created from ring elements. See [KAP1].
Standard residue	$r \in \mathbb{Z}_n$ is standard if $0 \leq r \leq n-1$.
s.t.	such that
w.l.o.g.	Without Loss Of Generality.
w.r.t.	... with respect to ...

General Mathematical Symbols

$(m;\ i_1, \ldots, i_n)$	$m!/(i_1! \cdots i_n!)$. Multinomial coefficient of the first kind.
$(m;\ i_1, \ldots, i_n)_*$	$m!/(1^{i_1} i_1! \cdots n^{i_n} i_n!)$. Multinomial coefficient of the second kind.
$(x_1, x_2, \ldots, x_n)$	Ideal generated by $x_1, x_2, \ldots, x_n$.
$\langle x_1, x_2, \ldots, x_n \rangle$	(Multiplicative) subgroup generated by $x_1, x_2, \ldots, x_n$.
$\lvert S \rvert$	If S is a set or multiset, the number of elements in S.
$a \,\vert\, b$	a divides b.
$a \parallel b$	a strictly divides b. $a \,\vert\, b$ and $a \neq b$
$\alpha\vert A$, $\alpha\vert_A$	A map α restricted to the set A.
$A^\dagger$	The complex transpose of the matrix A; the adjoint matrix
A^T	The transpose of the matrix A
$A \approx B$	(Group or ring) isomorphism from A to B.
$\binom{n}{m}$	The binomial coefficient, $n!/\left((n-m)!m!\right)$.
$\mathbb{C}$	The complex numbers.
$\mathrm{GL}_n(R)$	The non-singular $n \times n$ matrix group over R.
$\imath$	$\sqrt{-1}$.
I, I_n	The $N \times N$ identity matrix, the $n \times n$ identity matrix.
$\ker_*$	A multiplicative group kernel in a ring.
$\mathrm{M}_n(R)$	The $n \times n$ matrix ring over R.
$\mathbb{N}$	The natural numbers.
$\phi(n)$	The Euler or totient function $= \lvert\mathbb{Z}_n^*\rvert$.
$\mathbb{Q}$	The rationals.
$\mathbb{Q}_\zeta$ or $\mathbb{Q}(\zeta)$	The cyclotomic field containing the primitive root of unity, ζ.
$\mathbb{R}$	The reals.
S_n	The symmetric group on $\mathbb{Z}_n$.
$S_N^{(m)}$	Stirling number of the first kind. §11.6.5
$\mathrm{t}G$	The torsion part of a group G.
$\mathbb{Z}$	The (rational) integers.
$\mathbb{Z}_n$	The ring of remainders modulo n.
$\mathbb{Z}_n^*$	The multiplicative group of coprime residues modulo n.
$\mathbb{Z}_\zeta$ or $\mathbb{Z}(\zeta)$	The cyclotomic integers containing the primitive root of unity, ζ.

Special Terms Used in the Book

Boolean circulant	Circulants over Boolean sets. §9.4
Circulant Space	Either the circulant matrices or circulant vectors.
Eigenspace	R_ζ^N, Q_ζ^N, a vector space enclosing all eigenvalue vectors. §1.8

Filter map	The eigenspace filter map , $\tilde{\Gamma}^n_{mn}$, §3.5.2.
τ Generates v	$v_i = \tau(i) - i,\ \forall i \in \mathbb{Z}_N$. §4.3.5
$[\tau]$ Generates $[v]$	$[v] = [\tau]$. (Also, see $[\tau]$ below.) §4.3.5
Injection map	The circulant or eigenspace injection map, $\tilde{\Gamma}^{mn}_n$, §3.5.2.
Null Multiset	$\sum[v] \equiv 0 \pmod N$. §11.1
Multiplier map	ν_h and $\bar{\nu}_h$, §3.12.
Subrepeating circulant	§5.2
Repetition map	The circulant repetition map, Γ^{mn}_n. §3.5.1
Representer	Given $a \in \mathbf{circ}_n(R)$ its representer is $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. §1.10.1
Residue Class	§3.2.
Residue Class Matrix	§5.1.
s-circulant	Shift-circulant §2.2
Standard basis	$1, \mathrm{u}, \mathrm{u}^2, \ldots, \mathrm{u}^{N-1}$ for $\mathbf{circ}_N$, $e_0, e_1, \ldots, e_{N-1}$ for the eigenspace. 1.10.
Standard circulant	$a \in \mathbf{circ}(\mathbb{R})$ is standard if $\sum_i a_i = 1$ and $a_i \geq 0,\ \forall i$. §9.3.2
Standard Positive	a is standard positive if standard and $a_i > 0,\ \forall i$. §9.3.2
Subscript vector	$v \in {\mathbb{Z}_N}^N$ used as subscripts in a monomial expression,$a_v = a_{v_0} \cdots a_{v_{N-1}}$.
Supercirculant	See Chapter 4.
Wrap-around map	The polynomial map, Γ^N, §3.3. Circulant wrap-around map, Γ^n_{mn}, §3.5.1.
Zero set	A subset, S of $\mathbb{Z}_N$, s.t. $\sum_{i \in S} v_i \equiv 0 \pmod N$. §11.2.3

Special Symbols Used in the Book

$(i)_N$	the principal ideal generated by i in $\mathbb{Z}_N$. §3.2.8
$(i)^*_N$	The residue class set of i mod N. §3.2.8
$\langle\tau\rangle$	The sequence of translations of a permutation $\tau \in S_N$. §11.4
$[v]$	The multiset of components of a vector v. §10.2
$[\tau]$	The multiset of translations of a permutation τ. §10.2
$a_{(m)},\ a^{(m)}$	Subrepeating components. §5.2.6
$\tilde{\alpha},\ \alpha^\lambda$	$\lambda\alpha\lambda^{-1}$ if α is a homomorphism on circulants.
$c(v)$	The circulant determinantal coefficient. (Chapters 4 and 10 only) §4.3
$C(S, v)$	(Chapter 10 only) §11.1.4
C_n	The Kummer units (Chapter 7 only). §7.5.6.4ff
$\overline{C}_p$	Circulant units mapped to cyclotomic units. §7.6.18ff
$\mathbf{circ}_n(R)$	The ring of circulant n-vectors over the ring R. §1.9ff
CIRC_n	The circulant isomorphism $\mathrm{CIRC}_n : \mathbf{circ}_n(R) \mapsto \mathrm{CIRC}_n(R)$. §1.3
$\mathrm{CIRC}_n(R)$	The ring of circulant $n \times n$ matrices with base ring R.
$\Delta_n(a)$	The circulant determinant, $\det \mathrm{CIRC}_n(a)$.
$\Delta_n(A)$	Determinant of a circulant $n \times n$ matrix, $\det(A)$.
δ^N_i	0 if $i \not\equiv 0 \pmod N$, 1 otherwise.
δ_i	δ^N_i when N is assumed known.
δ^n	The idempotent vector numerically equal to $(\delta^n_i)_{i=0,1,\ldots,n-1}$
$\delta^n(x)$	The idempotent map numerically equal to $x\delta^n$ (componentwise product)
$\bar{\delta}^n$	The idempotent circulant numerically equal to $(n/N)\delta^n$. §3.2
$\bar{\delta}^n(x)$	The idempotent map on circulants equal to $\bar{\delta}^n x$. §3.2
D_n	§11.9.1
e_i	A vector in the standard basis for the eigenspace. §1.10
$e_N(x),\ e(x)$	$e^{2\pi\imath x/N}$. (Chapters 4 and 10 only) §4.3.1
E_n	The full group of units in the n^{th} cyclotomic field. (Chapter 7 only) §7.5.6.4
$\bar{E}_p,\ \bar{E}^{\pm}_p$	Subgroup of $\mathbf{circ}_p(\mathbb{Z})$ generated by cyclotomic units. (Chapter 7 only) §7.6.9
$F,\ F_n$	The diagonalizing matrix for the circulants. The Fourier matrix. §1.6
$F(v)$	The number of permutations leaving v fixed. (Chapters 4 and 10 only) §4.3.2
γ, γ_+	Inverse λ_1 maps: $\mathbb{Z}_\zeta \to \mathbf{circ}_p(\mathbb{Z})$. §7.6.1, §7.7.3, §7.7.9

γ_-	Related to γ_+. See §7.6.1, §7.7.9
Γ^n	The polynomial wrap-around map. §3.3
Γ_r^s	The circulant wrap-around and/or repeater map. §3.5ff
$\tilde{\Gamma}_r^s$	Injection and/or filter map. §3.5.1 ff
h_+	The class number of the real part of the cyclotomic field.
$H_n(v;\ z)$	The zero-set formula for $c(v)$. §11.2.7
$H_n([v];\ z)$	The multiset formula for $c(v)$. §11.5.3
$K_N(R)$	The shift-circulant matrices over R (Chapter 2 only). §2.2
$L_{n\mid N}$	A subset of the eigenvalue maps, $\{\lambda_n, \lambda_{2n}, \ldots, \lambda_{N-n}\}$ §3.2.12
$L^*_{n\mid N}$	A subset of the eigenvalue maps, $\{\lambda_i \vdash i \in (n)^*_N\}$ §3.2.12
$L_{n\mid N}(c)$	A set of eigenvalues, $\{\lambda_n(c), \lambda_{2n}(c), \ldots, \lambda_{N-n}(c)\}$
$L^*_{n\mid N}(c)$	A set of eigenvalues, $\{\lambda_i(c) \vdash i \in (n)^*_N\}$
$\Lambda_N(R)$	The range of λ which contains $\lambda(\mathbf{circ}_N(R))$. §1.7
λ	The eigenvalue vector map on circulant matrices. §1.7
λ_i	The i^{th} eigenvalue map on circulant matrices. §1.7
	The above can also represent the eigenvalues if the argument is understood.
ℓ_p	A map on $\mathbb{Z}_\zeta \to \mathbb{Z}_p$. §7.2.6
$\bar{\lambda}$	An abbreviated form of the λ map. §7.3.16
μ	A map from $\mathbf{circ}_p(\mathbb{Q})$ to itself. (Chapter 7 only) §7.6.9
N	The default circulant space dimension.
$\mathcal{N}_n(a)$	Algebraic norm in $\mathbb{Q}(\zeta_n)$. §7.2
$\Phi_n(x)$	The n^{th} cyclotomic polynomial of degree $\phi(n)$. §3.4.2
$\mathcal{P}_0(v)$	The set of zero-set partitions of v. §11.2.4
$\mathcal{P}_0([v])$	The set of null multiset partitions of v. §11.5.3
Q	Usually the quotient field of the base ring R of the circulants. §1.8
Q_ζ	The base field of the eigenspace of $\mathbf{circ}_N(R)$. The quotient field of R_ζ. §1.8
$r_n(i)$	Ramanujan sum. §5.1.6 ff.
R	The default symbol for the base ring. Commutative ring with identity.
R_ζ or $R(\zeta)$	The ring formed from R by adding ζ.
R^n	$R \oplus R \oplus \cdots \oplus R$, ($n$ times).
$R[G]$	Group ring formed from the ring R and group G. §3.6
$\mathcal{S}_n$	The full symmetric group on n objects usually taken to be $\{0, 1, \ldots, n-1\}$.
$\mathrm{Stab}(v)$	The set of permutations of a sequence v which leave it fixed.
θ	The defining vector of a $D \in \mathrm{NormCIRC}$. (Chapter 2 only) §2.5
Υ, Υ_c	Ring homomorphism $\mathbf{circ}_N(R) \mapsto R[Z]^N$. §3.6.1
$v : S$	$[v_i \vdash i \in S]$. §11.2.3
U	The circulant matrix $\mathrm{CIRC}(0, 1, 0, \ldots, 0)$. §1.10
u	The circulant vector $(0, 1, 0, \ldots, 0)$ which generates the standard basis. §1.10
$\mathbf{U}(R)$	Group of units of the ring R.
$\mathcal{T}_n$	Trivial units of $\mathbf{circ}_n(\mathbb{Z})$. §7.3.6
$\hat{\mathcal{T}}_n$	$\mathcal{T}_n \cup \hat{\mathcal{T}}_n$ is a finite subgroup of $\mathbf{circ}_n(\mathbb{Q})$. §7.3.6
$\mathcal{U}_n$	The full group of units of $\mathbf{circ}_n(\mathbb{Z})$.
ζ, ζ_n	A primitive N^{th} root of unity, a primitive n^{th} root of unity.
ω	Third root of unity: $\frac{1}{2}(-1 + \imath\sqrt{3})$

Notes and References

[AbS] "Handbook of Mathematical Functions", M. Abramowitz & I.A. Stegun (eds.); Dover Publications, Inc., 1970, (9^{th} printing).

[AD] "Zero-sum sets of prescribed size" by Noga Alon & Moshe Dubiner, pub.at School of Mathematical Sciences, Tel Aviv University, 2006. www.math.tau.ac.il/ nogaa/PDFS/egz1.pdf

[BaP] "Boolean Circulants, Groups, and Relation Algebras" by Chris Brink & Jan Pretorius; American Mathematical Monthly, **99**, 1992, pp 146-152.

[Bass] "The Dirichlet Unit Theorem, Induced Characters, and Whitehead Groups of Finite Groups." by Hyman Bass. Topology, **4**, 1966. pp 391-410.

[Dav] "Circulant Matrices" by Philip J. Davies; John Wiley & Sons, 1979. Available from University Microfilms International, Ann Arbor, Michigan. This is the only other extant book on circulants. It is excellent reading and explains clearly all the basic properties of circulants and much more besides. It has an intriguing chapter on the application of circulants to polygonal geometry.

[Dav1] ibid. §2.5.

[Dav2] ibid. §2.5. Davies derives the basic properties of the Fourier matrix. See also [Fla] below.

[Dav3] ibid. §5.3.

[Dav4] ibid. §5.6.

[EDM] "Encyclopedic Dictionary of Mathematics" by the Mathematical Society of Japan, editors Shôkichi Iyanaga & Yukiyosi Kawada; The MIT Press, 1980, §107G, p350.

[Edw] "Fermat's Last Theorem, a Genetic Introduction to Algebraic Number Theory" by H. M. Edwards; Springer-Verlag, 1977.

[Edw1] ibid. §4.3.

[FB] "Einleitung in die Theorie der binären Formen." by Francois Faà di Bruno; Leipzig (1881).

This is the reference given by Ore in his paper. See [Ore]

[FG] "The Prime Factors of Wendt's Binomial Circulant Determinant" by G. Fee & A. Granville; Mathematics of Computation **57**, 1991, pp 839-848.

[FLA] "Introduction to Number Theory" by Daniel E. Flath; John Wiley & Sons, 1989. The definition of the discrete Fourier transform agrees with that in §6.5 of Flath's book which has more information on the F matrix. The other common definition of the Fourier matrix is $(1/\sqrt{N})\sum_j a_j\zeta^{-ij}$.

[FT] "Algebraic Number Theory" by A. Fröhlich & M.J. Taylor; Cambridge University Press, 1991. §1.44.

[Gauss] "Disquisitiones Arithmeticae" by C.F. Gauss; published in Leipzig, 1801. English translation by A.A. Clarke, Yale University Press, 1966. See ART. 24.

[Guy] "Unsolved Problems." by R. Guy, (ed.); American Mathematical Monthly, **100**, 1993, pp 287-289.

[Ham] "The Friendship Theorem and Love Problem" by J.M. Hammersley; Surveys in Combinatorics (9^{th} British Combinatorial Conference) E. Keith Lloyd(ed.) available in London Mathematical Society Lecture Note Series **82**, Cambridge University Press, 1983, pp 31-54.

[HaW] "Introduction to Theory of Numbers" by G.H. Hardy & E.M. Wright; Oxford University Press, 1960, (4^{th} ed.).

[HaW1] ibid. Theorems 67 and 272.

[Joh] "Presentation of Groups" by D.L. Johnson; London Mathematical Society, Series 22, Cambridge University Press, 1976, Chapter 16.

[Kap] "Commutative Rings" by I. Kaplansky; University of Chicago Press, 1974 (revised edition).

[Kap1] ibid. To see how such a field can constructed from arbitrary commutative rings see §1-4. See also [Lang].

[Kap2] ibid., (Hilbert Basis Theorem) Thm.69

[Kap3] ibid., (Dedekind domains) Thm.98

[Kar1] "Unit Groups of Classical Rings" by G. Karpilovsky; Oxford University Press, 1988.

[Kar2] ibid., §8.9.31.

[Kar3] ibid., §2.2.10.

[Kar4] ibid., §2.2.12

[Kar5] ibid., Attributed to Kaplansky in §8.9.34.

[KW] "Polynomial Equations and Circulant Matrices" by D. Kalman, J.E. White; American Mathematical Monthly, **108**, 2001, pp 821-840.

[Lam] "On rational circulants satisfying $A^2 = dI + \lambda J$." Linear Algebra and Its Applications **12** 1975, pp 139-150.

[Lang] "Algebraic Number Theory" by Serge Lang; Springer-Verlag, 1986.

[Lang1] ibid., Chapter IV, Theorems 3 and 5. The proof in Lang's book is quite general but requires reading and understanding most of the previous sections in the book. The reader may prefer instead to refer to [WAS5] which has a self-contained proof for the case $n =$ prime.

[Lang2] "Cyclotomic Fields I and II" by Serge Lang; Springer-Verlag, 1990 (combined edition). §6.1

[LWW] "The Combinatorics of a Three-Line Circulant Determinant" by N.A. Loehr, G.S. Warrington, H.S. Wilf; Israel Journal of Mathematics, **143**, 2004.

[Muir] "A Treatise on the Theory of Determinants", Sir Thomas Muir & W. Metzler; Longmans, Green, (New York), 1933. This book is an American edition of an earlier work by Muir. It was quite obviously intended as a general textbook on determinants but has a long section on circulants. Muir was active in the development of circulants in the 19^{th} century, and it seems he took the opportunity in this book to (briefly!) summarize the main results known at the time since much of the section would be of interest only to contemporary researchers in circulant determinants.

Please note the typographical error in Exercise 2 on page 443: all negative signs should be changed to plus signs.

[Muir1] ibid., ART.499. Although only the case $N = 4$ is proven, the general method is clear from the context.

[Muir2] ibid. There is a formula derived in ART.491, page 458 which is an apparent generalization to com-

pound n of the formula derived herein at Proposition 10.7.3 which is proved for n prime only. However, the method by which Muir obtains the formula is valid only when n is prime. Indeed, should the reader wish to continue to the subsequent section, the formula should be taken as the definition of the variable S.

[Muir3] ibid. See §503, page 476 where the proposition is demonstrated for $n = 4, m = 3, N = 12$.

[Ore] "Some Studies on Cyclic Determinants" by Oystein Ore; Duke Mathematical Journal, **18**, 1951, pp. 343-354.

[Pan] "On a Congruence Modulo a Prime" by Hao Pan, American Mathematical Monthly, **113**, 2006, pp 652-654.

[Pas1] "The Algebraic Structure of Group Rings" by D.S. Passman; John Wiley & Sons, 1977. This is the standard reference on group rings.

[Pas2] ibid., Chapter 14, Theorem 1.2, attributed by Passman to Perlis & Walker. See also the preceding Lemma 1.1.

[PFTV] "Numerical Recipies. The Art of Scientific Computing" by Wm. H, Press, Brian P. Flannery, Saul A. Teukolsky, Wm. T. Vetterling; Cambridge University Press, London, 1986.

[PP] Preprints and references for various results in this text can be found at www.circulants.org.

[Rib1] "Fermat's Last Theorem for Amateurs" by Paulo Ribenboim; Springer-Verlag, New York, 1999.

[Rib2] "The Little Book of Big Primes" by Paulo Ribenboim; Springer-Verlag, New York, 1991. p15

[Rot] "The Theory of Groups" by Joseph J. Rotman. Allyn & Bacon, 1965.

[Seg] "Units in Integral Group Rings" by Sudarshan K. Seghal. Longman Scientific & Technical, 1993.

[Was] "Introduction to Cyclotomic Fields" by L.C. Washington; Springer-Verlag, 1982.

[Was1] ibid., Appendix §1 and Chapter 12.

[Was2] ibid., §2.4.

[Was3] ibid., Lemma 8.1 and Theorem 8.1. See also the more difficult Theorem 8.3 for general N.

[Was4] ibid., §5.36

[Was5] ibid., §1.2. This proves the integral elements of $\mathbb{Q}(\zeta_p)$ to be $\mathbb{Z}(\zeta_p)$ for p prime.

[Was6] ibid., §5.36

[Weil] "Basic Number Theory" by André Weil, Springer-Verlag, New York, 1973.

[Wyn] "Circulants", A. Wyn-jones. Manuscript for the complete text available at www.circulants.org.