CIRCULANTS (Extract)

Alun Wyn-jones

Last revised in December 2013.

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. $\square$

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. $\square$

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 $\bigcup M(F) = \{a \in \mathbf{circ}_N(\mathbb{Z}) \vdash \det(a) = 0\}$. $\square$

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]. $\square$

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.

$$\therefore\ J \ = \ \alpha(A)\alpha(c_1) + \alpha(A)\alpha(c_2) + \cdots + \alpha(A)\alpha(c_n) \ = \ B\alpha(c_1) + B\alpha(c_2) + \cdots + B\alpha(c_n) \quad \square$$

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. $\square$

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. $\square$

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 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, $n = 0$. $\square$

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 $\mathbf{circ}(\mathbb{Z})/(a) \approx \mathbb{Z}_D$. $\square$

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, $c \mid D$. The idea behind the proof is to show that if any prime p divides D/c then p^2 divides D.

Suppose $p \mid D$ 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 $p \mid (D/c)$ 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, $p^2 \mid D$ as required.

It remains to show that if $p \mid (D/c)$ 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 $p \mid (D/c)$. Therefore, $A^* \in p \cdot \mathrm{CIRC}(\mathbb{Z})$. That is, $A^* \equiv 0 \pmod{p}$. $\square$

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 $\mathcal{N}_{N/d}\left(\lambda_d(aw + 1)\right) \geq 2$. 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^{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^{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, $x^N - 1 \mid a(x)b(x)$. Therefore $a(x)b(x)$ is divisible by all the cyclotomic polynomials $\Phi_d(x)$ where $d \mid N$. 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., $\Phi_d(x) \mid a(x)$ for all $d \mid N$. Then, $x^N - 1 \mid a(x)$ 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 $d \mid N$. 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, $\Phi_d(x) \mid x^N - 1$. Therefore, $\Phi_d(x) \mid \Phi_m(x)$. 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 $d \mid N$, 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 $L_q := \{a \in \mathbf{circ}_N(\mathbb{Z}) \vdash q \mid \lambda_0(a)\}$, 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 $d \mid N$, and define $L_{\pi,d} := \{a \in \mathbf{circ}_N(\mathbb{Z}) \vdash \pi \mid \lambda_{N/d}(a)\}$. 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)*

$$p = \left(\sum_{i=0}^{p-1} x^i\right)_{x=1} = \lim_{x\to 1}\left(\frac{x^p-1}{x-1}\right) = \left(\prod_{i=1}^{p-1}(x-\zeta^i)\right)_{x=1} = \prod_{i=1}^{p-1}(1-\zeta^i) \qquad (1)$$

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. $\square$

8.4.12 **Proposition** Let $p \mid N$. 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, $\Phi_p \mid x$ or $\Phi_p \mid c$. But, if $\Phi_p \mid c$ then c is a divisor of zero. Hence, so is $p = yc$. Contradiction. Therefore, $\Phi_p \mid x$, and $x = x_1\Phi_p$, say.

$$\therefore\ \Phi_p(x_1c - 1) = 0$$
$$\therefore\ \hat{\Phi}_p \mid (x_1c-1)$$

where $\hat{\Phi}_p$ is the product of all cyclotomic circulants in $\mathbf{circ}_N(\mathbb{Z})$ not equal to Φ_p.

$$\therefore\ x_1c = 1 + k\hat{\Phi}_p \quad \text{for some } k \in \mathbf{circ}_N(\mathbb{Z})$$

$$\begin{aligned}\text{Now, } \hat{\Phi}_p(x) &= (x-1)\frac{x^N-1}{x^p-1} \\ &= (x-1)\left(x^{p(m-1)} + x^{p(m-2)} + \cdots + x^p + 1\right) \qquad \text{where } m = N/p.\end{aligned}$$

$$\therefore\ \lambda_i(x_1c) = \begin{cases} 1 & \text{if } m \nmid i \\ 1 + (\zeta_N^i - 1)m\kappa_i & \text{if } m \mid i \quad \text{where } \kappa = \lambda(k)\end{cases} \qquad (2)$$

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. $\square$

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 $a \in \mathbf{circ}_{\scriptscriptstyle N}(\mathbb{Q})$ 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. $\square$

This proposition raises the question of what are the irreducible elements of $\mathbf{circ}_{\scriptscriptstyle N}(\mathbb{Z})$. 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 $c = (1 - \mathrm{u})^3 + p^2\Phi_p$

$$\begin{aligned}
\hat{\lambda}(c) &= \big(p^3,\ (1-\zeta)^3\big)\\
&= \big(p^2,\ 1-\zeta\big)\big(p,\ (1-\zeta)^2\big) && \text{(irreducible factors)}\\
&= (p,\ 1-\zeta)^3 && \text{(irreducible factors)}
\end{aligned}$$

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 $\lambda_0(t_i) \not\equiv 0 \pmod{p}$. $\square$

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 $\hat{\lambda}(\Phi_p) = (p, 0) = (p,0)(1, \xi_\pi \pi) \in (\tilde{\theta}_\pi)$. $\square$

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. $\square$

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. $\square$

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. $\square$

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.