CIRCULANTS (Extract)

Alun Wyn-jones

Last revised in December 2013.

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:

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

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:

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

The circulants $\bar{\delta}_\times^n(\mathrm{u}^i)$ and $(1-\bar{\delta})_\times^n(\mathrm{u}^i)$ 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 $\bar{\delta}_\times^n(\pm\mathrm{u})$ to $\mathcal{T}_N$ is enough.

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

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

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

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

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** $\mathrm{t}\mathbf{circ}_N(\mathbb{Q}) \;\approx\; \mathbb{Z}_2^\nu \oplus \bigoplus_{d\,\|\,N} \mathbb{Z}_{N/d}$ 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 $T_d = \{\pm\zeta_{N/d}^i\}$. 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 $u_d := \bar{\delta}_\times^d(\mathrm{u})$, and when N/d is an odd integer, define $s_d := \bar{\delta}_\times^d(-1)$. Then, we have an internal direct product decomposition for the torsion part of the rational circulants,

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

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

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

Proof. As before, we let $P_d \;:=\; \bar{\delta}_\times^{*d}\,\mathbf{U}\left(\mathbf{circ}_d(\mathbb{Q})\right)$, and let $T_d := \{\pm\zeta_{N/d}^i\} = \mathrm{t}\mathbb{Q}(\zeta_{N/d})$. 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 $T_d = \{\zeta_{N/d}^i\} = \langle\zeta_{N/d}\rangle$. We easily see that $\lambda_d^{-1}(\zeta_{N/d}) = \bar{\delta}_\times^{*d}(\mathrm{u}) \in P_d$. Therefore, $\mathrm{t}P_d$ is generated by $\bar{\delta}_\times^{*d}(\mathrm{u})$.

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

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, $[\mathcal{U}_q : H\gamma_*(V_q)\mathcal{K}_q] \mid \frac{1}{2}(p-1)$. □