

Circulants over Finite Fields

The most basic question we can ask in the study of circulants over a finite fields is the structure of the units in the circulant ring. With one exception, we shall provide a complete description of the isomorphism class of the unit group. But, we shall only provide a method of constructing these unit groups assuming generators to the units of various fields are given.

We shall start with the notations used here which differ slightly from the main text on circulants.

1 Notation.

- (i) Denote the set of units in $\mathbf{circ}_n(F)$ by $\mathbf{circ}_n^*(F)$.
- (ii) The symbol p will be reserved for a prime, and q will be reserved for some positive power of p .
- (iii) We shall use \mathbb{F}_p (not \mathbb{Z}_p) to denote a field of p elements. Likewise, \mathbb{F}_q shall be a field of $q = p^m$ elements.
- (iv) $\Phi_n(x)$ will as usual denote the n^{th} cyclotomic polynomial, and $\phi(n)$, the Euler function, will denote its degree.
- (v) If an element generates the entire group of units it is called a *primitive* element.

The finite characteristic of the field causes some complications. For example, the Fourier matrix is singular if the characteristic divides n , the order of the circulants. Indeed, we must regrettably exclude this case from the subsequent. However, finite fields do have some compensations. The first theorem, though standard, might be quite surprising to those familiar only with fields of characteristic zero.

2 Theorem

- (i) Any two finite fields having the same number of elements are isomorphic.
- (ii) The group of non-zero elements of a finite field is cyclic.

Proof. See [Weil] \square

As a simple application of part (i) of Theorem 1.2, we shall prove a corollary which brings home the difference between finite fields and those of characteristic zero.

3 Corollary If integers $m, n > 1$ have no square root in \mathbb{F}_p , then $\mathbb{F}_p(\sqrt{m}) = \mathbb{F}_p(\sqrt{n})$.

Proof. Note: the claim is not just that the two fields are isomorphic but that they are **equal**.

By the theorem, there exists a field isomorphism $\beta : \mathbb{F}_p(\sqrt{m}) \rightarrow \mathbb{F}_p(\sqrt{n})$.

$$\therefore 0 = \beta(0) = \beta((\sqrt{m})^2 - m) = (\beta(\sqrt{m}))^2 - \beta(m)$$

showing that $x^2 - \beta(m)$ has a solution in $\mathbb{F}_p(\sqrt{n})$. But, $\beta(m) = \beta(1 + 1 + \dots + 1) = m\beta(1) = m$. \square

We shall start by treating some easy cases in order to get an idea of the issues involved. The technique (as in the treatment of the integer circulants) is to concentrate on the eigenvalues since their behavior under circulant multiplication is the easiest to analyze. But to connect the circulants with their eigenvalues uniquely, we need assurance that there is a matrix which diagonalizes the circulants. Recall that in complex domains, we used the Fourier matrix for this purpose. However, the Fourier matrix has an irrational denominator, \sqrt{n} , which normalizes the matrix. But we do not need a unitary matrix just for diagonalization, so we avoid the complications of the \sqrt{n} by eliminating it, leaving us with the simpler task of proving that the Vandermonde matrix $V = (\zeta^{ij})_{i,j}$ is non-singular.

4 Proposition Let ζ be a primitive n^{th} root of unity in a field of characteristic p . Let V be the $n \times n$ Vandermonde matrix given by $V_{i,j} = \zeta^{ij}$. If $p \nmid n$, then V is non-singular.

Proof. We compute the determinant of V . The Vandermonde formula gives

$$\det V = \prod_{i>j} (\zeta^i - \zeta^j)$$

$$\begin{aligned} \therefore \pm \det V^2 &= \prod_{i>j} (\zeta^i - \zeta^j) \prod_{i<j} (\zeta^i - \zeta^j) = \prod_{i \neq j} (\zeta^i - \zeta^j) = \prod_{i=0}^{n-1} \zeta^i \prod_{j \neq i} (1 - \zeta^{j-i}) \\ &= \zeta^{1/2 n(n-1)} \left(\prod_{k=1}^{n-1} (1 - \zeta^k) \right)^n = \pm \Phi_n(1)^n = \pm n^n \end{aligned}$$

We are given that $p \nmid n$. Therefore, $\det V \not\equiv 0 \pmod{p}$. \square

The first easy case is when \mathbb{F}_p contains a primitive n^{th} root of unity.

4.1 Proposition Suppose $p \equiv 1 \pmod{n}$, then $\mathbf{circ}_n^*(\mathbb{F}_p) \approx \mathbb{Z}_{p-1}^n$.

Proof. In this case, \mathbb{F}_p contains a primitive n^{th} root of unity, ζ , say. The matrix $V = (\zeta^{ij})$ consists of eigenvectors of the circulants. Therefore, $\lambda_i(c) = (Vc)_i$ for all $c \in \mathbf{circ}_n(\mathbb{F}_p)$. Clearly, $V \in M_n(\mathbb{F}_p)$. So, $\lambda_i(c) \in \mathbb{F}_p$.

Now, V is also a diagonalizing matrix for $\mathbf{circ}_n(\mathbb{F}_p)$. and the resulting map, λ , is a bijection iff V is non-singular. By Proposition 4, this is so provided $p \nmid n$. But, we are given that $p \equiv 1 \pmod{n}$, $\therefore p > n$, $\therefore p \nmid n$.

Consequently, F is invertible, and the circulants can be simultaneously diagonalized to $F^{-1} \mathbf{circ}(\mathbb{F}_p) F$ which must be the direct sum, \mathbb{F}_p^n , whose unit group is \mathbb{Z}_{p-1}^n . \square

5 Corollary For $p \geq 3$, $\mathbf{circ}_2^*(\mathbb{F}_p) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p-1}$. \square

Proposition 4.1 gives the extreme case where the polynomial $x^n - 1$ completely splits in \mathbb{F}_p . We now treat the opposite extreme, where the n^{th} cyclotomic polynomial, $\Phi_n(x)$, is irreducible over \mathbb{F}_p .

6 Proposition If $\Phi_n(x)$ is irreducible over \mathbb{F}_q , then the Galois group for the splitting field of Φ_n over \mathbb{F}_q is cyclic of order $\phi(n)$.

Proof. Let ζ be a primitive n^{th} root of unity in the field extension $\mathbb{F}_q(\zeta)$. Let G be the Galois group of this extension. We shall construct G .

Let $\alpha \in G$. Then, α must permute the roots of $\Phi_n(x)$. Therefore, $\alpha : \zeta \mapsto \zeta^t$ for some t coprime to n . Call this map α_t . Extend α_t to all of $\mathbb{F}_q(\zeta)$; we see that its action on a general field element is

$$\alpha_t : c_0 + c_1\zeta + c_2\zeta^2 + \cdots + c_{n-1}\zeta^{n-1} \mapsto c_0 + c_1\zeta^t + c_2\zeta^{2t} + \cdots + c_{n-1}\zeta^{(n-1)t}$$

$$\text{That is, } \alpha_t : \lambda_1(c) \mapsto \lambda_t(c)$$

However, the representation $\lambda_1(c) = c_0 + c_1\zeta + c_2\zeta^2 + \cdots + c_{n-1}\zeta^{n-1}$ is not unique, so we need to verify that α_t is well-defined. Assume there is a linear dependency between $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$, let us say,

$$1 + f_1\zeta + f_2\zeta^2 + \cdots + f_{n-1}\zeta^{n-1} = 0$$

Let $f(x)$ denote the polynomial with coefficients f_0, f_1, \dots, f_{n-1} so that the linear dependency is equivalent to $f(\zeta) = 0$. Then, $\Phi_n(x) \mid f(x)$. Clearly, the converse also holds, $\Phi_n(x) \mid f(x) \Rightarrow f(\zeta) = 0$. Hence, all linear dependencies over \mathbb{F}_q between the roots of unity reduce to $\Phi_n(\zeta) = 0$.

So suppose $\lambda'_1 = \lambda_1 + \kappa\Phi_n(\zeta)$ for some $\kappa \in \mathbb{F}_p(\zeta)$. Then,

$$\alpha_t(\lambda_1 + \kappa\Phi_n(\zeta)) = \alpha_t(\lambda_1) + \alpha_t(\kappa)\alpha_t(\Phi_n(\zeta)) = \alpha_t(\lambda_1) + \alpha_t(\kappa)\Phi_n(\zeta^t) = \alpha_t(\lambda_1)$$

The last equation follows from the fact that ζ^t is primitive, and so is a root of $\Phi_n(x)$.

This shows that every α_t is well-defined for every t coprime to n . We can therefore pick t to be a primitive residue mod n . With this choice, α_t becomes a generator for G , and α_t has the same order as t mod n , namely $\phi(n)$. \square

7 Proposition Let n, p be distinct primes, and suppose that the cyclotomic polynomial $\Phi_n(x)$ is irreducible over \mathbb{F}_q . Then, $\mathbf{circ}_n^*(\mathbb{F}_q) \approx \mathbb{Z}_{q-1} \oplus \mathbb{Z}_{q^{n-1}-1}$.

Proof. Proposition 6 and its proof showed that the Galois group of the extension $\mathbb{F}_p(\zeta)/\mathbb{F}_p$ is generated by α_t where $\alpha_t : \zeta \mapsto \zeta^t$ and t is coprime to n . Hence, if we are given λ_1 as the eigenvalue of a circulant in $\mathbf{circ}_n(\mathbb{F}_p)$, then by repeatedly applying α_t we can derive $\lambda_t, \lambda_{t^2}, \lambda_{t^3}, \dots$. Since t is primitive mod n , the set $\{1, t, t^2, t^3, \dots\}$ equals the set $\{1, 2, \dots, n-1\}$. Thus, via α_t , λ_1 determines $\{\lambda_1, \lambda_2, \dots, \lambda_{n-1}\}$.

Now c is in the unit group iff all its eigenvalues are non-zero. By the above, this is equivalent to requiring $\lambda_0(c) \in \mathbb{F}_q^*$, and $\lambda_1(c) \in \mathbb{F}_q(\zeta)^*$. By Theorem 2, we can pick primitive elements in g in \mathbb{F}_q^* , and γ in $\mathbb{F}_q(\zeta)^*$. Define M to be the set of vectors

$$M = \{ (g^a, \gamma^b, \alpha_t(\gamma^b), \dots, \alpha_t^{n-2}(\gamma^b)) \mid a, b \in \mathbb{N} \}$$

By Proposition 7.2.9.1, the eigenvalues of all circulants with components in the base field must be of the above form. Hence, M contains all possible eigenvalue vectors.

$$\therefore \mathbf{circ}_n^*(\mathbb{F}_q) \approx \langle g \rangle \oplus \langle \gamma \rangle$$

Now, $\langle g \rangle \approx \mathbb{Z}_{q-1}$. The field $\mathbb{F}_q(\zeta)$ is of degree $n-1$ over \mathbb{F}_q , and so has q^{n-1} elements. Therefore, $|\mathbb{F}_q(\zeta)^*| = q^{n-1} - 1$. Hence, $\langle \gamma \rangle$ is cyclic of order $q^{n-1} - 1$. \square

One wonders whether there are congruence fields over which $\Phi_n(x)$ is reducible, but does not completely split into linear factors. The answer is “yes”, as will be shown in all generality by Theorem 9. However, the theorem gives no indication what the factorization of $\Phi_n(x)$ might be. So that the reader might appreciate seeing a concrete example, we shall present a non-trivial factorization of $\Phi_5(x)$.

8 Proposition

- (i) $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ is reducible over the field \mathbb{F}_p iff $p \equiv \pm 1 \pmod{5}$.
- (ii) If $p \equiv -1 \pmod{5}$ then there exists $e \in \mathbb{Z}$ with $e(e+1) \equiv 1 \pmod{p}$ such that

$$\Phi_5(x) \equiv (x^2 - ex + 1)(x^2 + (e+1)x + 1) \pmod{p}$$

Proof. We first eliminate the simplest case: $\Phi_5(x)$ splits into linear factors iff \mathbb{F}_p contains a primitive fifth root of unity iff $p \equiv 1 \pmod{5}$.

We now assume that $p \not\equiv 1 \pmod{5}$, and that $\Phi_5(x)$ has no linear factor in \mathbb{F}_p .

The most general possible factorization remaining is into quadratic factors, $Q_1(x), Q_2(x)$, say.

$$\Phi_5(x) \equiv Q_1(x)Q_2(x) \equiv (ax^2 + bx + c)(dx^2 - ex + f) \pmod{p}$$

Since the coefficient of x^4 is 1, we can divide Q_1 by a , multiply Q_2 by a , and redefine b, c, e, f to obtain

$$\Phi_5(x) \equiv (x^2 + bx + c)(x^2 - ex + f)$$

Now, c is the product of two roots, both of which are primitive 5th roots of unity. Therefore, $c^5 \equiv 1$. But, by hypothesis, \mathbb{F}_p has no primitive fifth root of unity. Therefore, $c \equiv 1$. Likewise, $f \equiv 1$ which gives us

$$\Phi_5(x) \equiv (x^2 + bx + 1)(x^2 - ex + 1)$$

Equating coefficients, we get the following equations:

$$\begin{aligned} b &\equiv e + 1 \\ be &\equiv 1 \\ \therefore e^2 + e - 1 &\equiv 0 \end{aligned} \tag{2}$$

The discriminant of the quadratic in (2) is $\sqrt{5}$. Hence, a solution to (2) exists iff 5 is a quadratic residue mod p iff $p \equiv \pm 1 \pmod{5}$ by the Quadratic Reciprocity Theorem. Since we are assuming $p \not\equiv 1$, we have shown that the quadratic factorization of Φ_n implies $p \equiv -1 \pmod{5}$.

The converse follows by reversing the proof. From $p \equiv -1 \pmod{5}$ we deduce $\sqrt{5} \in \mathbb{F}_p$, which yields the desired factorization. \square

We now state and prove the standard theorem which describes exactly to what degree the cyclotomic polynomial factors over \mathbb{F}_p .

9 Theorem

$\Phi_n(x)$ factors over \mathbb{F}_q into irreducible polynomials of degree w where w is the order of $q \pmod{n}$.

Proof. Let \mathbb{F}_{q^f} be the full splitting field for $\Phi_n(x)$.

We are given $q^w - 1 \equiv 0 \pmod{n}$ and w is least such. For definiteness, $q^w - 1 = kn$ say. Now, the group of units in \mathbb{F}_{q^w} has a generator, u say. Then, $1 = u^{q^w - 1} = (u^k)^n \in \mathbb{F}_{q^w}$. That is, u^k is a primitive n^{th} root of unity in \mathbb{F}_{q^w} which must therefore contain the splitting field for $x^n - 1$, and hence for $\Phi_n(x)$. This shows that $q^f | q^w$.

Suppose $f < w$. Let v be a primitive n^{th} root of unity in $\mathbb{F}_{q^f}^*$. The subgroup generated by v has order n which must divide the order of the unit group, $q^f - 1$. This contradicts the minimality of w . Therefore, $f = w$.

Let $Q(x)$ be an irreducible factor of $\Phi_n(x)$ (with $Q = \Phi_n$ if Φ_n is irreducible.) Let E be the splitting field of $Q(x)$ over \mathbb{F}_q . Obviously, $E \subset \mathbb{F}_{q^f}$. But, E contains a primitive n^{th} root of unity, ζ say. It therefore contains all powers of ζ , and so all n^{th} roots of unity. Hence, $E = \mathbb{F}_{q^f}$. Now, $|E^*| = q^{\deg(Q)} - 1$. So, $q^{\deg(Q)} - 1 = q^f - 1 = q^w - 1$. That is, $\deg(Q) = w$. \square

10 Corollaries of the Theorem.

The dimension of the splitting field of $x^n - 1$ over \mathbb{F}_q is w , and so the splitting field has q^w elements.

Suppose $\Phi_n(x) = Q_1(x)Q_2(x) \cdots Q_r(x) \in \mathbb{F}_q[x]$ where each $Q_i(x)$ is irreducible mod q . Since $\Phi_n(x)$ has no repeated roots, the Q_i polynomials are mutually coprime in pairs, and, by the theorem, they all have the same degree, w , equal to the order of $q \pmod{n}$. Therefore, $\phi(n) = rw$.

The primitive n^{th} roots of unity are partitioned into sets belonging to the different irreducible factors of Φ_n . We shall denote the set to which any one root, ξ say, belongs by $[\xi]$, and we shall relabel the irreducible polynomials with their root sets, thus: $Q_{[\xi]}(x)$. However, we shall usually omit the brackets in which case it is to be understood that Q_ξ stands for $Q_{[\xi]}$.

11 Corollary (The Galois Group). Let G be the Galois group of the extension $\mathbb{F}_q(\zeta)/\mathbb{F}_q$. With the notation of the theorem, $G \approx \mathbb{Z}_w$.

Proof. G permutes the elements within each partition set, $G \times [\xi] = [\xi]$ for all roots ξ of $\Phi_n(x)$. Let $\tau \in G$. Then, $\tau : \zeta \mapsto \zeta^t$ for some $t > 1$. This action on ζ defines the action of τ on the whole field. For example, given any $j \in \mathbb{Z}_{\phi(n)}$, $\tau : \zeta^j \mapsto \zeta^{tj}$. Hence,

$$\tau : a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{n-1}\zeta^{n-1} \mapsto a_0 + a_1\zeta^t + a_2\zeta^{2t} + \cdots + a_{n-1}\zeta^{(n-1)t} \quad (3)$$

This is very similar to the case of irreducible $\Phi_n(x)$, the difference being that ζ^t is restricted to be in the same partition as ζ . Applying the τ automorphism successively we see that we generate a set S_τ where

$$S_\tau = \{\zeta, \tau(\zeta), \tau^2(\zeta), \dots, \tau^i(\zeta), \dots\} = \{\zeta, \zeta^t, \zeta^{t^2}, \dots, \zeta^{t^i}, \dots\} \subset [\zeta]$$

and so S_τ consists of at most w elements. Therefore, $t^h \equiv 1 \pmod{n}$ for some $h \leq w$. Let us try the map $\rho(\zeta) = \zeta^q$. By the assumptions of the theorem, the order of $q \pmod{n}$ is precisely w , which means, $|S_\rho| = w$, and $G = \langle \rho \rangle \approx \mathbb{Z}_w$. \square

We shall continue to use ρ to denote a generating element of G .

12 Finding a Basic Set of Eigenvalues. In Proposition 6, we applied the Galois group to the one eigenvalue λ_1 and derived the values of $\lambda_2, \dots, \lambda_{n-1}$. In the more general case of reducible $\Phi_n(x)$, we no longer have enough maps in the Galois group which can be used in equation (3) to derive all eigenvalues from one.

Applying the automorphism ρ to equation (3), we get the sequence,

$$\lambda_1 \xrightarrow{\rho} \lambda_q \xrightarrow{\rho} \lambda_{q^2} \xrightarrow{\rho} \dots$$

and this defines the w eigenvalues in the set $\{\lambda_i \mid \zeta^i \in [\zeta]\}$. Let us call such a set an eigenvalue root set, and denote it by $[\lambda_\zeta]$. It is clear that the eigenvalue roots sets are orbits under the Galois group. Therefore, we can no longer deduce all the eigenvalues given only one. In order to see to what degree circulants are constrained by a value for one eigenvalue, we turn to the circulant space. This leads us to consider $\ker \lambda_1$.

Let $a \in \mathbf{circ}_n(\mathbb{F}_q)$, and let $a(x)$ be its representer polynomial. Then,

$$\begin{aligned} a \in \ker \lambda_1 &\Leftrightarrow a(\zeta) = 0 \Leftrightarrow Q_\zeta(x) \mid a(x) \\ \therefore \ker \lambda_1 &= (Q_\zeta(x)) \end{aligned}$$

More generally,

$$\ker \lambda_j = (Q_\xi(x)) \Leftrightarrow \zeta^j \in [\xi] \Leftrightarrow \lambda_j \in [\lambda_\xi]$$

Suppose we have picked a value for μ for λ_1 . Pick any $a(u) \in \lambda_1^{-1}(\mu)$ where $a(x)$ is a representer polynomial. Then, taking the remainder of $a(x)$ mod $Q_\zeta(x)$, we see that there exist polynomials $a'(x), a''(x)$ such that

$$a(x) = a'(x) + Q_\zeta(x)a''(x) \tag{4a}$$

where $\deg a' < \deg Q_\zeta = w$, and $\deg a'' < n - w$. The polynomial a' satisfying (4a) is the standard representative for the set of circulants, a , which have eigenvalue $\lambda_1(a) = \mu$, and it is standard in the sense that it has the least degree.

The requirement that a is non-singular implies that a' is not the zero polynomial, otherwise the choice of a' is arbitrary, and completely specifies $\lambda_1(a)$, and all others in its eigenvalues root set, $[\lambda_\zeta]$.

If we now consider another eigenvalue, $\lambda_\xi \notin [\lambda_\zeta]$, we arrive at a similar formula,

$$a(x) = b'(x) + Q_\xi(x)b''(x) \tag{4b}$$

where $\deg b' < \deg Q_\xi = w$, $\deg b'' < n - w$, and b' is the standard representative for λ_ξ eigenvalue.

All formulæ such as (4a) and (4b) can be combined into a single formula:

$$a(x) = \sum_{[\xi]} L_\xi a_\xi(x) \prod_{[\gamma] \neq [\xi]} Q_\gamma(x) = \sum_{[\xi]} \left(\frac{\Phi_n(x)}{Q_\xi(x)} \right) L_\xi a_\xi(x) \tag{5}$$

The sum in (5) is over all root sets $[\xi]$, and L_ξ and a_ξ actually depend on $[\xi]$. L_ξ is a number to be determined, and a_ξ is the standard representative for the λ_ξ eigenvalue (and so $\deg a_\xi < w$). We now check what happens when we set $x = \eta$, an n^{th} root of unity. Every term but one in (5) is mapped to zero giving

$$\lambda_\eta(a) = a(\eta) = L_\eta a_\eta(\eta) \prod_{[\gamma] \neq [\eta]} Q_\gamma(\eta)$$

We now define

$$L_\eta := \prod_{[\gamma] \neq [\eta]} Q_\gamma(\eta)^{-1} \tag{6}$$

Giving,

$$\lambda_\eta(a) = a_\eta(\eta)$$

Formula (5) shows that we can simultaneously pick representative circulants a', b', c', \dots to satisfy independent choices of values for one member from each of r eigenvalue root sets.

Thus, we have our algorithm for picking general, non-zero eigenvalues yielding circulants in $\mathbf{circ}_n(\mathbb{F}_q)$. We pick representative roots from each of the r root sets, $[\xi_1], [\xi_2], \dots, [\xi_r]$, say. For each ξ_i , we pick a non-zero eigenvalue μ_i , and we compute its standard representative a_i . This determines all other eigenvalues in the same eigenvalue root set. We do this for $i = 1, 2, \dots, r$, and we construct the circulant $a(u)$ using formulæ (5) and (6).

It is clear from this procedure that there are r independent choices for eigenvalues, each of which can be set to a generator of the units in the field $\mathbb{F}_q(\zeta)$. Thus, we have proved

13 Proposition Let n, p be distinct primes, $q = p^m$, and let w be the order of q mod n . Then,

$$\mathbf{circ}_n^*(\mathbb{F}_q) \approx \mathbb{Z}_{q-1} \oplus \mathbb{Z}_{q^w-1}^{(n-1)/w} \quad (n \text{ prime})$$

Proof. The initial summand comes from the direct summand corresponding to the λ_0 eigenvalue.

For the other summands, recall that the field $\mathbb{F}_q(\zeta)$ is of dimension w over \mathbb{F}_q , giving $q^w - 1$ non-zero elements.

Using the procedure described above we construct a group generator as follows. We set $\lambda_\xi = g$, a primitive element of \mathbb{F}_{q^w} . We apply the Galois map α_t to obtain the values of the other eigenvalues in $[\lambda_\xi]$. The remaining eigenvalues are set to 1.

We repeat this process for each eigenvalue root set, thus creating r independent generators of order $|\mathbb{F}^*(\zeta)| = q^w - 1$. \square

We now consider compound n . We again start with a concrete case, namely $n = 6$. This will indicate how to proceed generally.

14 Proposition Let p be prime, $p \equiv -1 \pmod{6}$, then $\mathbf{circ}_6^*(\mathbb{F}_p) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^2-1} \oplus \mathbb{Z}_{p^2-1}$.

Proof. By the condition $p \equiv -1 \pmod{6}$, there is no third root of unity in \mathbb{F}_p . We shall denote a primitive root of $x^3 - 1$ by ω . Then, the splitting field of $x^6 - 1$ is $\mathbb{F}(\omega)$, and the primitive root is $-\omega$.

We construct a basis for the group of unit circulants of order 6. We choose circulants, c_0, c_3, c_1, c_2 , with the following spectrum of eigenvalues:

$$\begin{aligned} \lambda(c_0) &= (g, 1, 1, 1, 1, 1) \\ \lambda(c_3) &= (1, 1, 1, g, 1, 1) \\ \lambda(c_1) &= (1, x, 1, 1, 1, \bar{x}) \\ \lambda(c_2) &= (1, 1, x, 1, \bar{x}, 1) \end{aligned} \tag{7}$$

where g is a primitive residue mod p , x is primitive in $\mathbb{F}(\omega)$, and \bar{x} is the conjugate of x . These eigenvalues all obey the transformation rule of Proposition 7.2.9.1 which is equivalent to the condition that the circulants be in $\mathbf{circ}_6(\mathbb{F}_p)$. Also, the construction ensures that they generate independent cyclic subgroups of orders (respectively) $p - 1$, $p - 1$, $(p^2 - 1)$, and $(p^2 - 1)$. \square

Let us describe the method used in the proof in generality.

We shall say that λ_i belongs to **residue class** h whenever $\gcd(i, n) = h$. In particular, λ_h belongs to its eponymous residue class. The importance of the residue class lies in the fact that all eigenvalues in residue class h lie in the same field, a subfield of $\mathbb{F}_q(\zeta^h)$.

In proving the proposition, we set one eigenvalue in each residue class to the generator of the unit group of its range, and we set the others in the residue class to conjugates of the first. The conjugates must be assigned in accordance with Proposition 7.2.9.1 else the circulant components will not be in the base field.

The two eigenvalues λ_0 and $\lambda_{n/2}$ (when n is even) form singleton residue classes, and their range is always the base field. More generally, λ_i has the same range as the first in its residue class, namely λ_d where $d = \gcd(i, n)$, and the range of λ_d is $\mathbb{F}_q(\zeta^{n/d})$ where ζ is a primitive n^{th} root of unity.

It is possible that $\zeta^{n/D} \in \mathbb{F}_q$ for some $D | n$, in which case $\mathbb{F}_q(\zeta^{n/d}) = \mathbb{F}_q$ for all $d | D$. For example, with $p = 7$, $n = 30$, the sixth roots are in \mathbb{F}_7 , but the primitive 30th roots are not. This possibility is the reason

why there is a second formula offered in the next theorem. Although formulæ (9a) and (9b) are equivalent, (9b) segregates the terms which are in the base field from those in field extensions.

15 **Theorem** Let $q = p^m$ with p prime, $p \nmid n$. For each divisor $d \mid n$, define the function $w(d)$ to be the order of q mod d . Then,

$$\mathbf{circ}_n^*(\mathbb{F}_q) = \bigoplus_{d \mid n} \mathbb{Z}_{q^{w(d)}-1}^{\phi(d)/w(d)} \quad (9a)$$

Let e be a maximal integer dividing n such that \mathbb{F}_q contains a primitive e^{th} root of unity. Then, e is greatest such. Define $\delta := \sum_{d \mid e} \phi(d)$. We have

$$\mathbf{circ}_n^*(\mathbb{F}_q) = \mathbb{Z}_{q-1}^\delta \oplus \bigoplus_{d \nmid e, d \mid n} \mathbb{Z}_{q^{w(d)}-1}^{\phi(d)/w(d)} \quad (9b)$$

Proof. Formula (9a) is nothing more than an application of Proposition 13 to various residue classes of eigenvalues.

Let ζ denote a primitive n^{th} root of unity in \mathbb{F} or some extension of it. Note that, if $r \mid n$, $\zeta^{n/r}$ is a primitive r^{th} root of unity.

Let c be an arbitrary circulant, $c \in \mathbf{circ}_n(\mathbb{F}_q)$, and let its eigenvalues be $\lambda_0 = \lambda_0(c)$, $\lambda_1 = \lambda_1(c)$, \dots , $\lambda_{n-1} = \lambda_{n-1}(c)$.

We start with formula (9a). It consists of direct sums of the cycles generated by the eigenvalues. Let λ_i be an eigenvalue in residue class $\gcd(i, n)$, and let $d = n/\gcd(i, n)$. Then, λ_i is an arbitrary linear combination of powers of $\zeta^{n/d}$. Hence, λ_i lies in the splitting field for $x^d - 1$. By Theorem 9, this field is isomorphic to $\mathbb{F}_{q^{w(d)}}$. In particular, it has a multiplicative generator of period $q^{w(d)} - 1$.

As in §12, we can pick $r = \phi(d)/w(d)$ independent generators for the residue class of λ_i producing a subgroup of r independent cycles of $q^{w(d)} - 1$ elements each. This completes the proof of formula (9).

Formula (9b) is derived from (9a) by segregating the terms originating from eigenvalues which must take values in the base field. In the first equation, these terms are those having $w(d) = 1$. All that remains to show is that maximality of e implies it is largest.

Let us call r a **base index** if $r \mid n$ and $\zeta^{n/r} \in \mathbb{F}_q$ (that is, \mathbb{F}_q contains a primitive r^{th} root of unity). The key observation is that if r and s are base indices, then so is $\text{lcm}(r, s)$. Indeed, we are given $\zeta^{n/r}, \zeta^{n/s} \in \mathbb{F}_q$. Therefore, $\zeta^{in/r} \zeta^{jn/s} = \zeta^{n(jr+is)/rs} \in \mathbb{F}_q$ for all $i, j \in \mathbb{Z}$. Let $\gcd(r, s) = h$. Then, we can pick i, j such that $jr + is = h$. With such a choice of i, j , we have $n(jr + is)/rs = n/\text{lcm}(r, s)$. Hence, $\text{lcm}(r, s)$ is also a base index. Taking the l.c.m. of all base indices yields a unique largest base index, namely e . \square

With the information provided by the theorem, we can characterize the entire circulant ring.

15.1 **Corollary** With the same notation and conditions of the theorem,

$$\mathbf{circ}_n(\mathbb{F}_q) \stackrel{\lambda}{\approx} \bigoplus_{d \mid n} \mathbb{F}_{q^{w(d)}}^{\phi(d)/w(d)} \approx \mathbb{F}_q^\delta \oplus \bigoplus_{d \nmid e, d \mid n} \mathbb{F}_{q^{w(d)}}^{\phi(d)/w(d)} \quad \square$$

We conclude with a digression into cyclotomic theory. It is a question that arose in developing the above results when the author tried some computer computations to verify the theory. Let $\zeta = \zeta_n$ be an n^{th} root of unity, and suppose that $\zeta \notin \mathbb{F}_p$. The question is:

When is $\mathbb{F}_p(\zeta) \approx \mathbb{Z}(\zeta)/(p)$?

It may appear intuitively true to many that $\mathbb{F}_p(\zeta)$ must be the same field as $\mathbb{Z}(\zeta)/(p)$. After all, $\mathbb{F}_p(\zeta)$ can certainly be identified with $\mathbb{Z}_p(\zeta)$ which is the integers reduced modulo p with ζ attached, whereas $\mathbb{Z}(\zeta)/(p)$ sounds almost like the same thing: the integers with ζ attached reduced modulo p . Readers who find this convincing should consider the following fact: $1 + 5\zeta_5 + \zeta_5^2$ is a divisor of zero in $\mathbb{Z}(\zeta_5)/(19)$. We shall find a simple criterion for when this can happen.

This question is relevant to computation. The field $\mathbb{F}_p(\zeta)$ has no natural embodiment, and so can only be modelled on a computer using symbolic logic, whereas the ring $\mathbb{Z}(\zeta)/(p)$ is realized as a subset of the complex numbers reduced modulo p , and is easily modelled in computer languages that have complex arithmetic.

Denote the norm of z in $\mathbb{Q}(\zeta)/\mathbb{Q}$ by $\mathcal{N}(z)$.

16 Lemma Let $z \in \mathbb{Z}(\zeta)$, and let $\nu : \mathbb{Z}(\zeta) \rightarrow \mathbb{Z}(\zeta)/(p)$ be the natural map. Then, $\nu(z)$ is a divisor of zero iff $p \mid \mathcal{N}(z)$.

Proof. First assume that $\nu(z)$ is a divisor of zero. Then, there exists y such that $\nu(z)y = 0$ and $\nu(y) \neq 0$.

Let \bar{z} be the product of the conjugates of z . Then, $0 = \nu(z\bar{z}y) = \nu(\mathcal{N}(z)y) = \mathcal{N}(z)^n \nu(y)$ since $\mathcal{N}(x) \in \mathbb{Z}$. But, if $\mathcal{N}(x)$ is not divisible by p , then it has an inverse mod p given by $\mathcal{N}(x)^{p-2}$. But this would mean that $\nu(y) = 0$. Contradiction. Therefore $p \mid \mathcal{N}(z)$. QED (\Rightarrow).

If $p \mid \mathcal{N}(z)$ then $p \mid z\bar{z}$ where \bar{z} is the product of the conjugates of z . Then, $\nu(z)\nu(\bar{z}) = 0$. \square

17 Lemma Let $n > 2$, p be prime, $p \not\equiv 1 \pmod{n}$. Let $R = \mathbb{Z}(\zeta)/(p)$ where ζ is an n^{th} primitive root of unity. Then,

- (i) R is a field iff if there does not exist $z \in \mathbb{Z}(\zeta) - \{0\}$ such that $p \mid \mathcal{N}(z)$.
- (ii) When R is a field, it is isomorphic to $\mathbb{F}_p(\zeta)$, the root field of $x^n - 1$ over \mathbb{F}_p .

Proof.

(i) The implication: field \Rightarrow no divisors of zero is obvious, and no divisors of zero implies no zero norms by the previous lemma.

So assume that there are no zero norms. Then, there are no divisors of zero in R . Take any $z \in R - \{0\}$, and consider the sequence $z, z^2, \dots, z^i, \dots$. Since R is finite ($|R| = p^2$), this sequence must eventually repeat. Hence, $z^i = z^j$ for some $i < j$. Since there are no divisors of zero, we can cancel getting $z^{i-j} = 1$. We see that z is invertible with inverse z^{i-j-1} . QED (i)

(ii) If $\mathbb{Z}(\zeta)/(p)$ is a field, it is a field having p^2 elements, as is the field $\mathbb{F}_p(\zeta)$. The conclusion follows by Theorem 1.2. \square

18 Proposition Let ζ be an n^{th} primitive root of unity in \mathbb{C} . Then,

$$\mathbb{Z}(\zeta)/(p) \text{ is a field} \iff p \text{ is a primitive residue mod } n$$

Proof.

Consider the following diagram.

$$\begin{array}{ccccc} \mathbb{Z}(\zeta) & \xleftarrow{\eta_1} & \mathbb{Z}[x] & \xrightarrow{\nu_2} & \mathbb{F}_p[x] \\ \nu_1 \downarrow & & ? & \xrightarrow{\alpha} & ? \\ \mathbb{Z}(\zeta)/(p) & & ? & & \mathbb{F}_p(\zeta) \end{array}$$

where η_1, η_2 evaluate polynomials at $x = \zeta$ on their respective polynomial rings, and ν_1, ν_2 are the natural maps modulo the ideal (p) in their respective domains.

The putative map α is well-defined if $\ker \nu_1 \eta_1 \subset \ker \eta_2 \nu_2$. We compute $\ker \nu_1 \eta_1$. We have $\ker \nu_1 = \{pz + z \in \mathbb{Z}(\zeta)\}$. $\therefore \ker \nu_1 \eta_1 = \{pz + b(x)\Phi_n(x) + z \in \mathbb{Z}(\zeta), b \in \mathbb{Z}[x]\}$.

Applying ν_2 to this kernel we get $\nu_2(\ker \nu_1 \eta_1) = b(x)\Phi_n(x)$, and then, $\eta_2 \nu_2(\ker \nu_1 \eta_1) = 0$. Hence, α is well-defined, and since all maps are ring homomorphisms, α is also a ring homomorphism.

We now ascertain whether α is an isomorphism. We compute $\ker \eta_2 \nu_2$. By Theorem 9, $\Phi_n(x)$ factors in \mathbb{F}_p into $r = \phi(n)/w$ irreducible polynomials each of degree w where w is the order of $p \bmod n$.

$$\therefore \ker \eta_2 = (Q_1(x), Q_2(x), \dots, Q_r(x))$$

$$\therefore \ker \eta_2 \nu_2 = (Q_1(x), Q_2(x), \dots, Q_r(x)) + pa(x)$$

where $a \in \mathbb{Z}[x]$ is arbitrary.

Clearly, $\nu_1 \eta_1(\ker \eta_2 \nu_2) = 0$ iff $r = 1$. That is, $\ker \nu_1 \eta_1 = 0$ iff $w = \phi(n)$. But, no field can contain a non-trivial ideal. Therefore, $\mathbb{Z}(\zeta)/(p)$ is a field iff $w = \phi(n)$ iff p is a primitive residue mod n . \square

19 Corollary Let $z \in \mathbb{Z}(\zeta_n)$ be a cyclotomic integer. Its norm, $\mathcal{N}(z)$, is divisible only by primes which are not primitive residues mod n . \square

References

[Weil] André Weil, "Basic Number Theory," Springer-Verlag, New York, 1973.