Matrix Representation of Finite Fields

WILLIAM P. WARDLAW*
U.S. Naval Academy
Annapolis, MD 21402

Most undergraduate texts in abstract algebra show how to represent a finite field $\mathbf{F}_q$ over its prime field $\mathbf{F}_p$ by clearly specifying its additive structure as a vector space or a quotient ring of polynomials over $\mathbf{F}_p$ while leaving the multiplicative structure hard to determine, or they explicitly illustrate the cyclic structure of its multiplicative group without clearly connecting it to the additive structure. In this note we suggest a matrix representation that naturally and simply displays both the multiplicative and the additive structures of the field $\mathbf{F}_q$ (with $q = p^d$) over its prime field $\mathbf{F}_p$. Although this representation is known (see [3] p. 65, for example), it does not appear to be widely used in abstract algebra texts.

To illustrate these ideas, let us first consider the field $\mathbf{F}_8$ of eight elements over its prime field $\mathbf{F}_2$. The additive structure of $\mathbf{F}_8$ is that of the three-dimensional vector space $\mathbf{V} = \{(0\ 0\ 0), (1\ 0\ 0), (0\ 1\ 0), (0\ 0\ 1), (1\ 1\ 0), (1\ 0\ 1), (0\ 1\ 1), (1\ 1\ 1)\}$ over $\mathbf{F}_2$. However, it is not at all clear how to define products of these vectors to get the multiplicative structure of $\mathbf{F}_8$! It can be shown that extending the multiplication table

	(1 0 0)	(0 1 0)	(0 0 1)
(1 0 0)	(1 0 0)	(0 1 0)	(0 0 1)
(0 1 0)	(0 1 0)	(0 0 1)	(1 1 0)
(0 0 1)	(0 0 1)	(1 1 0)	(0 1 1)

(1)

for the basis $\mathbf{B} = \{(1\ 0\ 0), (0\ 1\ 0), (0\ 0\ 1)\}$ of $\mathbf{V}$ by bilinearity gives the multiplicative structure of $\mathbf{F}_8$, although a direct proof would be tedious.

A more usual, as well as more useful, treatment (see [1], p. 171 or [3], p. 25, Thm. 1.6.1) is to represent

$$\mathbf{F}_8 \cong \mathbf{F}_2[x]/(x^3 + x + 1) \tag{2}$$

as the ring of all polynomials over $\mathbf{F}_2$ modulo the third-degree irreducible polynomial $x^3 + x + 1$. If we let $a \in \mathbf{F}_8$ denote the residue class of x modulo $x^3 + x + 1$, we have $a^3 + a + 1 = 0$. Recalling that the characteristic is 2, it is then easy to see that $a^3 = a + 1$, $a^4 = a^2 + a$, $a^5 = a^2 + a + 1$, $a^6 = a^2 + 1$, and $a^7 = 1$, so

$$\begin{aligned} \mathbf{F}_8 &= \{0, 1, a, a^2, a^3, a^4, a^5, a^6\} \\ &= \{0, 1, a, a^2, a + 1, a^2 + a, a^2 + a + 1, a^2 + 1\}. \end{aligned} \tag{3}$$

Thus, the multiplicative group $\mathbf{F}_8^* = \langle a \rangle$ of $\mathbf{F}_8$ is simply the cyclic group of order 7 generated by a. The second formulation in (3) makes the additive structure easy to see, although it obscures the multiplicative structure a little. One can use the

*Research supported in part by the U.S. Naval Academy Research Council and by the Naval Research Laboratory, Radar Division, Identification Branch.

abbreviated multiplication table

	1	a	a^2
1	1	a	a^2
a	a	a^2	$a+1$
a^2	a^2	$a+1$	a^2+a

(4)

along with the distributive law to multiply elements of $\mathbf{F}_8$. (Comparing tables (1) and (4) is one fairly easy way to prove that the multiplication given by table (1) satisfies the field axioms.) Alternatively, one can use the relation $a^3 + a + 1 = 0$ to multiply the elements given in the second formulation in (3). This is the standard representation of a finite field, and it is reasonably satisfactory. However, the transition from addition to multiplication still leaves something to be desired.

If we pick any element b of the field $\mathbf{F}_8$, left multiplication by b is a linear transformation L_b on the vector space $\mathbf{V} = \mathbf{F}_8$ over $\mathbf{F}_2$. If we choose any basis $\mathbf{B}'$ of $\mathbf{V} = \mathbf{F}_8$ over $\mathbf{F}_2$, we can find the matrix $[L_b] = [L_b]_{\mathbf{B}'}$ of L_b with respect to that basis. If we fix the basis $\mathbf{B}'$ and find the matrix of each element of $\mathbf{F}_8$ in this way, it is clear that the resulting set of matrices form a field isomorphic to $\mathbf{F}_8$! Thus, each choice of basis gives a different matrix representation of $\mathbf{F}_8$.

It appears at first glance that we must have a multiplication table for the field before we can get the matrix representation. But there is a way to get around this difficulty.

Let

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

be the companion matrix (see [1], p. 264, [2], pp. 229–230, or [5], p. 201, Dfn. 5.2.16) of the irreducible third-degree polynomial $f(x) = x^3 + x + 1$ over the field $\mathbf{F}_2$. Then $f(A) = 0$, so the powers of A satisfy the relations satisfied by a above; in particular, the matrix A generates the cyclic group $\langle A \rangle$ of order 7 isomorphic to $\mathbf{F}_8^*$, and the ring of matrices

$$\mathbf{F}_2[A] = \{0, I, A, A^2, A^3, A^4, A^5, A^6\}$$

is isomorphic to the field $\mathbf{F}_8$. That was easy, wasn't it?

Indeed, a bit too easy, as we shall see. Consider now the irreducible polynomial $g(x) = x^2 + 1$ over the three-element field $\mathbf{F}_3$. We see that its companion matrix B has multiplicative order 4:

$$B = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, B^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, B^3 = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, B^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$$

Not enough elements for $\mathbf{F}_9$! And the powers of B are not closed under addition. Fortunately, there is a fairly simple cure: Adjoin the matrices 0, $I + B$, $I + B^3$, $B + B^2$, and $B^2 + B^3$ to the set of powers of B to obtain the ring $\mathbf{F}_3[B]$ of matrices generated by B. Since $g(B) = B^2 + I = 0$, it is clear that the ring $\mathbf{F}_3[B]$ is isomorphic to the field $\mathbf{F}_9$. Thus, B provides a matrix representation $\mathbf{F}_3[B]$ of the nine-element field, and we say that B is a *generator* of the field $\mathbf{F}_9$.

But we would like to have a *cyclic generator* of $\mathbf{F}_9$; that is, a matrix M such that the multiplicative group $\mathbf{F}_9^*$ of $\mathbf{F}_9$ is isomorphic to the cyclic group $\langle M \rangle$ generated by M. This, too, is not terribly difficult. An eight-element cyclic group has exactly $\varphi(8) = 4$ generators, none of which is a power of an element of order 4. Thus, the multiplicative group $\mathbf{F}_3[B]^* \cong \mathbf{F}_9^*$ is cyclically generated by any of the four nonzero

matrices in $\mathbf{F}_3[B]$ that are not powers of B. The reader can easily verify that the matrix $M = I + B = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$ is a cyclic generator of $\mathbf{F}_9$.

Note that the set $\mathbf{F}_3[B]$ is spanned (over $\mathbf{F}_3$) by the matrices I and B, and also by I and M. That is, $\mathbf{F}_3[B] = L(I, B) = L(I, M)$. If $\mathbf{B}$ and $\mathbf{M}$ are the ordered bases (I, B) and (I, M), respectively, we see that

$$L_B\colon \begin{matrix} I \mapsto B = 0 \cdot I + 1 \cdot B \\ B \mapsto B^2 = 2 \cdot I + 0 \cdot B \end{matrix} \quad \text{so} \quad [L_B]_{\mathbf{B}} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} = B,$$

$$L_M\colon \begin{matrix} I \mapsto M = 1 \cdot I + 1 \cdot B \\ B \mapsto MB = 2 \cdot I + 1 \cdot B \end{matrix} \quad \text{so} \quad [L_M]_{\mathbf{B}} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} = M,$$

and

$$L_M\colon \begin{matrix} I \mapsto M = 0 \cdot I + 1 \cdot M \\ M \mapsto M^2 = 1 \cdot I + 2 \cdot M \end{matrix} \quad \text{so} \quad [L_M]_{\mathbf{M}} = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} = A.$$

Since A is similar to M, it follows that A is another cyclic generator of $\mathbf{F}_9$. Moreover, A is the companion matrix of its characteristic polynomial $f_A(x) = x^2 + x + 2$. We call A a *canonical cyclic generator* of $\mathbf{F}_9$, and call the representation

$$\mathbf{F}_3[A] = \{0, I, A, A^2, A^3, A^4, A^5, A^6, A^7\}$$

a *canonical cyclic representation* of $\mathbf{F}_9$.

Of course, all of these ideas generalize for arbitrary finite fields. (Indeed, they generalize to finite extensions of *any* field, but we restrict the treatment here to finite extensions of fields $\mathbf{F}_p$ with p prime.) Let p be a prime number and let $q = p^e$ be the e^{th} power of p. Then $\mathbf{F}_q$ is a q element field containing $\mathbf{F}_p = \mathbf{Z}_p = \mathbf{Z}/(p)$ (the integers modulo p) as its prime field. Let $m(x)$ be any irreducible polynomial of degree e over $\mathbf{F}_p$, and let B be the companion matrix of $m(x)$. The ring $\mathbf{F}_p[B]$ of sums of powers of B is isomorphic to the field $\mathbf{F}_q$, and is thus a matrix representation of $\mathbf{F}_q$. Locate a matrix M in $\mathbf{F}_p[B]$ that has period (multiplicative order) $q - 1$. M is necessarily a cyclic generator of $\mathbf{F}_q$. The companion matrix A of the minimum polynomial $m_M(x) = m_A(x)$ is a canonical cyclic generator of

$$\mathbf{F}_p[A] = \{0, I, A, A^2, \ldots, A^{q-2}\} \cong \mathbf{F}_q.$$

Note that if C is any $e \times e$ matrix over $\mathbf{F}_p$, then the ring $\mathbf{F}_p[C]$ generated by C is isomorphic to $\mathbf{F}_q$ if, and only if, the characteristic polynomial $f_C(x)$ of C is irreducible, only if the sequence $\mathbf{C} = (I, C, C^2, \ldots, C^{e-1})$ of powers of C is independent. In this case, the matrix $[L_C]_{\mathbf{C}}$ of left multiplication by C, with respect to the basis $\mathbf{C}$, is the companion matrix of $f_C(x)$. C is a cyclic generator of $\mathbf{F}_q$ if, and only if, C is a primitive $(q-1)^{\text{st}}$ root of unity in $\mathbf{F}_p[C]$.

There is another, possibly easier, method of getting a canonical cyclic generator of $\mathbf{F}_q$. Recall that the n^{th} cyclotomic polynomial $\mathbf{c}_n(x)$ is defined to be the product

$$\mathbf{c}_n(x) = \prod (x - a) \tag{5}$$

taken over all $\varphi(n)$ primitive n^{th} roots a of unity. Since every root of $x^n - 1 = 0$ is a primitive d^{th} root of unity for some divisor d of n, it follows from (5) that

$$x^n - 1 = \prod_{d|n} \mathbf{c}_d(x). \tag{6}$$

One can use (6) to obtain the recursive formula

$$\mathbf{c}_n(x) = (x^n - 1) \Big/ \prod_{d|n,\, d<n} \mathbf{c}_d(x). \tag{7}$$

It follows inductively from (7) that $\mathbf{c}_n(x)$ is a monic polynomial with integer coefficients of degree (from (5)) $\varphi(n)$. The cyclotomic polynomials are all irreducible over the rational number field (see [3], p. 61, Thm. 2.4.7, [4], p. 162, or [5], p. 289, Thm. 6.3.13), but they usually factor over finite fields. It will be useful later to note that if $n = r^d$ is a power of a prime r, then it follows inductively from (7) that

$$\mathbf{c}_n(x) = (x^n - 1)/(x^{n/r} - 1), \quad (n = r^d, \ r \text{ prime}). \tag{8}$$

Every element of $\mathbf{F}_q$ (p prime and $q = p^e$) is a root of

$$x^q - x = x(x^{q-1} - 1) = 0, \tag{9}$$

since $\mathbf{F}_q$ is the splitting field of $x^q - x$, and every nonzero element is a $(q-1)$st root of unity. If $m(x)$ is a monic irreducible factor of $\mathbf{c}_{q-1}(x)$, and a is a root of $m(x)$, then a is a primitive $(q-1)$st root of unity. (Note that $m(x)$ is necessarily of degree e.) It follows that if A is the $e \times e$ companion matrix of $m(x)$, then A is a canonical cyclic generator of $\mathbf{F}_q$.

Conversely, if A is a canonical cyclic generator of $\mathbf{F}_q$ over $\mathbf{F}_p$, then its minimum polynomial $m_A(x)$ is an irreducible factor of the cyclotomic polynomial $\mathbf{c}_{q-1}(x)$ in $\mathbf{F}_p[x]$. This observation can lead to a method of factoring cyclotomic polynomials. This is a related but different topic that we will not pursue here.

Let us conclude with two examples that use the method of factoring cyclotomic polynomials to obtain canonical cyclic representations of $\mathbf{F}_8$ over $\mathbf{F}_2$, and of $\mathbf{F}_9$ over $\mathbf{F}_3$. (We have treated these cases more naively above.)

For $\mathbf{F}_8$ over $\mathbf{F}_2$, $e = [\mathbf{F}_8 : \mathbf{F}_2] = 3$, so the factors of $\mathbf{c}_7(x)$ are cubic:

$$\begin{aligned}\mathbf{c}_7(x) &= (x^7 - 1)/(x - 1) \\ &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ &= (x^3 + x + 1)(x^3 + x^2 + 1).\end{aligned}$$

(The factorization of $\mathbf{c}_7(x)$ was particularly easy, since its factors are the only irreducible polynomials of degree three over $\mathbf{F}_2$.) Since $x^3 + x + 1$ and $x^3 + x^2 + 1$ are irreducible factors of $\mathbf{c}_7(x)$, it follows that their companion matrices

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

are canonical cyclic generators of $\mathbf{F}_8$ over $\mathbf{F}_2$.

For $\mathbf{F}_9$ over $\mathbf{F}_3$, we would like to factor

$$\mathbf{c}_8(x) = (x^8 - 1)/(x^4 - 1) = x^4 + 1.$$

Since $e = [\mathbf{F}_9 : \mathbf{F}_3] = 2$, the factors are quadratic. It is not hard to see that the monic irreducible quadratics over $\mathbf{F}_3$ are $x^2 + 1$, $x^2 - x - 1$, and $x^2 + x - 1$. The desired factorization is

$$\mathbf{c}_8(x) = x^4 + 1 = (x^2 + x - 1)(x^2 - x - 1),$$

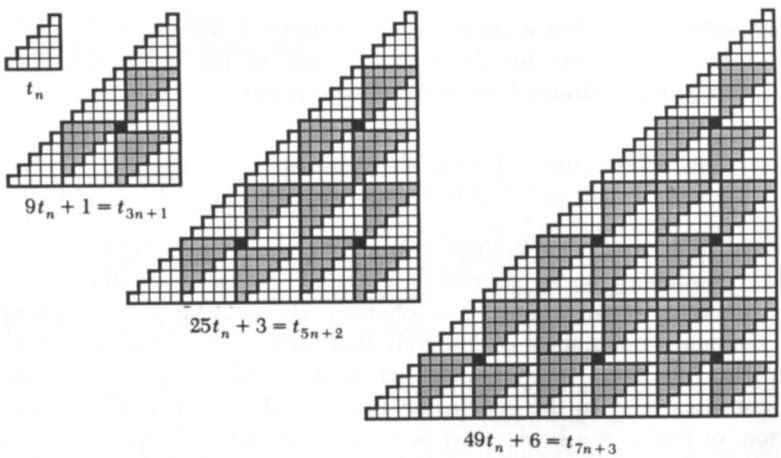
so the canonical cyclic generators of $\mathbf{F}_9$ over $\mathbf{F}_3$ are the corresponding companion matrices,

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

REFERENCES

1. I. N. Herstein, *Topics in Algebra*, Blaisdell, Waltham, MA, 1964.
2. K. Hoffman and R. Kunze, *Linear Algebra*, 2nd edition, Prentice Hall, Inc., Englewood Cliffs, NJ, 1971.
3. R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, New York, 1986.
4. B. L. van der Waerden, *Modern Algebra*, Vol. 1, Ungar, New York, 1969.
5. E. A. Walker, *Introduction to Abstract Algebra*, Random House, Inc., New York, 1987.

Proof without Words: A Triangular Identity



$$t_n = 1 + 2 + \cdots + n \Rightarrow (2k+1)^2 t_n + t_k = t_{(2k+1)n+k}$$

—Roger B. Nelsen
Lewis and Clark College
Portland, OR 97219