Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Linear Algebra and its Applications 403 (2005) 159–164
LINEAR ALGEBRA AND ITS APPLICATIONS
www.elsevier.com/locate/laa

A concrete matrix field description of some Galois fields

Kirby C. Smith [a], Leon van Wyk [b,*]

[a] *Department of Mathematics, Texas A&M University, College Station, TX 77843, USA*
[b] *Department of Mathematics, University of Stellenbosch, P/Bag X1, Matieland 7602, Stellenbosch, South Africa*

Received 8 June 2004; accepted 25 January 2005
Available online 23 March 2005
Submitted by G. Heinig

Abstract

We provide a concrete description of some factor rings of the polynomial ring $k[X]$, k a field, as fields of matrices, namely of the factor rings $k[X]/(X^n - X - 1)$ for which n is such that the polynomial $X^n - X - 1$ is irreducible in $k[X]$. These factor rings include the Galois fields GF(p^n) for which $X^n - X - 1$ is irreducible in $\mathbb{Z}_p[X]$. Both MAGMA and MAPLE show that there are many such fields.

AMS classification: 16S50

Keywords: Galois field; Matrix ring

Although matrix representations of some fields can be found in the literature, in fact in many introductory textbooks on fields, it is the purpose of this sequel to exhibit a concrete and easily explicable description of a rather large class of fields,

* Corresponding author.
E-mail addresses: ksmith@math.tamu.edu (K.C. Smith), lvw@sun.ac.za (L. van Wyk).

0024-3795/$ - see front matter
doi:10.1016/j.laa.2005.01.030

including some Galois fields. Moreover, the particular description holds for all the fields under discussion.

For preliminaries on ring constructions, like quotient rings and various versions of matrix rings, see, for example [2], which is one of the more modern books dealing with these topics.

It is well known that if $f(X)$ is an irreducible polynomial of degree n in the polynomial ring $k[X]$, k any field, and α is a root of $f(X) = 0$, then $k[X]/(f(X))$ is a field and the elements of $k[X]/(f(X))$ can be written as

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \tag{1}$$

with $a_i \in k$, $i = 0, 1, \ldots, n-1$. (Here $(f(X))$ denotes the ideal in $k[X]$ generated by $f(X)$.) Therefore, $k[X]/(f(X))$ is an n-dimensional vector space over k, with $B := \{1, \alpha, \ldots, \alpha^{n-1}\}$ as a basis. Note that if k is the prime field $\mathbb{Z}_p$, then $\mathbb{Z}_p[x]/(f(x))$ is the Galois field $\mathrm{GF}(p^n)$.

For any ring R with identity the ring $\mathscr{L}(R) := \{\lambda_r : r \in R\}$ of left multiplication maps λ_r, with $\lambda_r(s) := rs$, $s \in R$, is isomorphic to R. In particular,

$$\mathscr{L}(k[X]/(X^n - X - 1)) \cong k[X]/(X^n - X - 1)$$

and $\{\lambda_1, \lambda_\alpha, \ldots, \lambda_{\alpha^{n-1}}\}$ is a basis for $\mathscr{L}(k[X]/(X^n - X - 1))$ over k.

Let k be any field, and consider any $n \geqslant 2$ such that $X^n - X - 1$ is irreducible in $k[X]$. If α is a root of $X^n - X - 1 = 0$, then $\alpha^n = 1 + \alpha$ in $k[X]/(X^n - X - 1)$. Hence, if $0 \leqslant i, j \leqslant n-1$ and $i + j \geqslant n$, then

$$\begin{aligned}\alpha^{i+j} &= \alpha^{n+(i+j-n)}\\ &= (1+\alpha)\alpha^{i+j-n}\\ &= \alpha^{i+j-n} + \alpha^{i+j-n+1}\end{aligned}$$

and so

$$\lambda_{\alpha^i}(\alpha^j) = \begin{cases}\alpha^{i+j} & \text{if } i + j \leqslant n-1,\\ \alpha^{i+j-n} + \alpha^{i+j-n+1} & \text{if } i + j \geqslant n.\end{cases} \tag{2}$$

Let $[\lambda_{\alpha^i}]_B$, $i = 0, 1, \ldots, n-1$, denote the matrix of λ_{α^i} with respect to the basis B (for $k[X]/(X^n - X - 1)$ as a vector space over k), and let the n rows and n columns of $[\lambda_{\alpha^i}]_B$ be indexed by $1, \alpha, \ldots, \alpha^{n-1}$. Let I_n denote the $n \times n$ identity matrix, and let E_{α^k,α^ℓ} denote the standard matrix unit with 1 in indexed position (α^k, α^ℓ), $0 \leqslant k, \ell \leqslant n-1$. If no entry in a position in the matrices below means 0, then it follows from (2) that

$$
[\lambda_{\alpha^i}]_B = \begin{array}{c} \begin{array}{cccccccccc} & 1 & \cdots & \alpha^{n-i-1} & & \alpha^{n-i} & & \alpha^{n-i+1} & \cdots & \alpha^{n-1} \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \end{array} \\ \begin{array}{r} 1\rightarrow \\ \alpha\rightarrow \\ \alpha^2\rightarrow \\ \vdots\rightarrow \\ \alpha^{i-1}\rightarrow \\ \alpha^i\rightarrow \\ \vdots\rightarrow \\ \alpha^{n-1}\rightarrow \end{array} \begin{pmatrix} & & & 1 & & & & & \\ & & & 1 & & 1 & & & \\ & & & & & 1 & \ddots & & \\ & & & & & & \ddots & \ddots & \\ & & & & & & & \ddots & 1 \\ 1 & & & & & & & & 1 \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \end{pmatrix} \end{array} \tag{3}
$$

for $i = 1, 2, \ldots, n-1$, i.e.,

$$
[\lambda_1]_B = I_n,
$$

$$
[\lambda_\alpha]_B = (E_{1,\alpha^{n-1}} + E_{\alpha,\alpha^{n-1}}) + (E_{\alpha,1} + E_{\alpha^2,\alpha} + \cdots + E_{\alpha^{n-1},\alpha^{n-2}})
$$

$$
= \begin{array}{c} \begin{array}{cccccc} & 1 & \cdots & \alpha^{n-2} & & \alpha^{n-1} \\ & \downarrow & & \downarrow & & \downarrow \end{array} \\ \begin{array}{r} 1\rightarrow \\ \alpha\rightarrow \\ \vdots\rightarrow \\ \alpha^{n-1}\rightarrow \end{array} \begin{pmatrix} & & & & 1 \\ 1 & & & & 1 \\ & \ddots & & & \\ & & 1 & & \end{pmatrix} \end{array},
$$

$$
[\lambda_{\alpha^2}]_B = (E_{1,\alpha^{n-2}} + E_{\alpha,\alpha^{n-2}}) + (E_{\alpha,\alpha^{n-1}} + E_{\alpha^2,\alpha^{n-1}})
$$

$$
+ (E_{\alpha^2,1} + E_{\alpha^3,\alpha} + \cdots + E_{\alpha^{n-1},\alpha^{n-3}}) \tag{4}
$$

$$
= \begin{array}{c} \begin{array}{cccccc} & 1 & \cdots & \alpha^{n-3} & \alpha^{n-2} & \alpha^{n-1} \\ & \downarrow & & \downarrow & \downarrow & \downarrow \end{array} \\ \begin{array}{r} 1\rightarrow \\ \alpha\rightarrow \\ \alpha^2\rightarrow \\ \vdots\rightarrow \\ \alpha^{n-1}\rightarrow \end{array} \begin{pmatrix} & & & & 1 & \\ & & & 1 & 1 & \\ 1 & & & & 1 & \\ & \ddots & & & & \\ & & 1 & & & \end{pmatrix} \end{array},
$$

$$
\vdots
$$

$$
[\lambda_{\alpha^{n-1}}]_B = (E_{1,\alpha} + E_{\alpha,\alpha}) + (E_{\alpha,\alpha^2} + E_{\alpha^2,\alpha^2}) + \cdots
$$

$$
+ (E_{\alpha^{n-2},\alpha^{n-1}} + E_{\alpha^{n-1},\alpha^{n-1}}) + E_{\alpha^{n-1},1}
$$

$$
= \begin{array}{c} \\ 1\rightarrow \\ \alpha\rightarrow \\ \vdots\rightarrow \\ \alpha^{n-2}\rightarrow \\ \alpha^{n-1}\rightarrow \end{array}
\begin{array}{c}
\begin{array}{ccccc} 1 & \alpha & \cdots & \cdots & \alpha^{n-1} \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \end{array} \\
\begin{pmatrix}
 & 1 & & & \\
 & 1 & \ddots & & \\
 & & \ddots & \ddots & \\
 & & & \ddots & 1 \\
1 & & & & 1
\end{pmatrix}
\end{array}.
$$

Note that the $[\lambda_{\alpha^i}]_B$'s, $i = 1, 2, \ldots, n-1$, can be easily described in terms of the diagonals on which the 1's appear. Let $D^{(0)}$ denote the main diagonal, and let $D^{(i)}$ (respectively $D^{(-i)}$) denote the ith diagonal above (respectively below) the main diagonal. Then $[\lambda_{\alpha^i}]_B$, $i = 1, 2, \ldots, n-1$, has 1's in every position on $D^{(-i)}$ and $D^{(n-i)}$, and in every position on $D^{(n-i-1)}$ that is below a position on $D^{(n-i)}$, and 0's elsewhere.

Keeping in mind that $\{\lambda_1, \lambda_\alpha, \ldots, \lambda_{\alpha^{n-1}}\}$ is a basis for $\mathscr{L}(k[X]/(X^n - X - 1))$ over k, and that the fields $k[X]/(X^n - X - 1)$ and $\mathscr{L}(k[X]/(X^n - X - 1))$ are isomorphic, then (1) and the foregoing arguments prove the following description of $k[X]/(X^n - X - 1)$ as a field of $n \times n$ matrices over k:

Theorem. *If k is a field and n is such that the polynomial $X^n - X - 1$ is irreducible in $k[X]$, then the field $k[X]/(X^n - X - 1)$ is isomorphic to the matrix subfield of the matrix ring $\mathbb{M}_n(k)$ comprising the matrices*

$$
M_{a_0,a_1,\ldots,a_{n-1}} := \begin{bmatrix}
a_0 & a_{n-1} & \cdots & a_3 & a_2 & a_1 \\
a_1 & a_{n-1}+a_0 & a_{n-2}+a_{n-1} & \cdots & a_2+a_3 & a_1+a_2 \\
a_2 & a_1 & a_{n-1}+a_0 & a_{n-2}+a_{n-1} & \cdots & a_2+a_3 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\
a_{n-2} & \cdots & \ddots & a_1 & a_{n-1}+a_0 & a_{n-2}+a_{n-1} \\
a_{n-1} & a_{n-2} & \cdots & a_2 & a_1 & a_{n-1}+a_0
\end{bmatrix},
$$

$a_i \in k,\ i = 0, 1, \ldots, n-1$, *via*

$$
a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mapsto M_{a_0,a_1,\ldots,a_{n-1}}.
$$

Example. Since $X^4 - X - 1$ is irreducible in $\mathbb{Z}_2[X]$, it follows that GF(16) is isomorphic to the matrix subfield

$$
\left\{ \begin{bmatrix}
a_0 & a_3 & a_2 & a_1 \\
a_1 & a_3+a_0 & a_2+a_3 & a_1+a_2 \\
a_2 & a_1 & a_3+a_0 & a_2+a_3 \\
a_3 & a_2 & a_1 & a_3+a_0
\end{bmatrix} : a_0, a_1, a_2, a_3 \in \mathbb{Z}_2 \right\}
$$

of $\mathbb{M}_4(\mathbb{Z}_2)$.

Note that if A denotes the companion matrix of the polynomial $f(X) = X^n - X - 1$ in $k[X]$, then A is precisely the matrix $[\lambda_\alpha]_B$ in (4). In fact, $A^i = [\lambda_{\alpha^i}]_B$ for $i = 0, 1, \ldots, n-1$. Since it is well known in linear algebra (see [1] or [3]) that $f(A) = 0$, i.e., A plays the role of a root of $f(X) = 0$, it follows that if $X^n - X - 1$ is irreducible in $k[X]$, then the polynomials in A over k of degree less than n yield a representation of the elements of $k[X]/(X^n - X - 1)$.

However, the arguments in this sequel provide an alternative way, which uses much less heavy machinery, of obtaining the above theorem.

Moreover, $f(X)$ is both the minimal polynomial and the characteristic polynomial of A, and so the polynomials in A over k of degree less than n, i.e., precisely the matrices $M_{a_0,a_1,\ldots,a_{n-1}}$ in the above theorem, compose the centralizer

$$\mathrm{Cen}(A) := \{C \in \mathbb{M}_n(k) : AC = CA\}$$

of A in $\mathbb{M}_n(k)$.

Of course, one can consider any irreducible polynomial of degree n in $k[X]$ in order to obtain a result analogous to the above theorem. However, it is the purpose of this paper to highlight the fact that the powers of the matrix $[\lambda_\alpha]_B$ in (3), obtained by using the particular polynomial $X^n - X - 1$ in $k[X]$, are very easy to write down because of the pattern (see (4)) involved in obtaining subsequent powers of $[\lambda_\alpha]_B$, which in turn leads to the concrete description of the factor rings $k[X]/(X^n - X - 1)$.

Both MAGMA and MAPLE show (see also, for example, [5]) that the following are precisely all the n's, with $2 \leqslant n \leqslant 25{,}000$, such that $X^n - X - 1$ is irreducible in $\mathbb{Z}_p[X]$, with $p = 2, 3$:

$p = 2$: $n = 2, 3, 4, 6, 7, 9, 15, 22, 28, 30, 46, 60, 63, 127, 153, 172, 303, 471, 532, 865, 900, 1366, 2380, 3310, 4495, 6321, 7447, 10{,}198, 11{,}425, 21{,}846, 24{,}369$;

$p = 3$: $n = 2, 3, 4, 5, 6, 13, 14, 17, 30, 40, 41, 51, 54, 73, 121, 137, 364, 446, 485, 638, 925, 1382, 1478, 2211, 2726, 5581, 5678, 6424, 8524, 10{,}649, 15{,}990, 17{,}174, 18{,}685, 18{,}889$.

The values of n, for $p = 2$ listed above, satisfy no known "magic" pattern, as verified by the extremely helpful database at superseeker@research.att.com.

All the other prime p's that we have tested, using MAGMA as well as MAPLE, yield values of n such that $X^n - X - 1$ is irreducible in $\mathbb{Z}_p[X]$. However, both MAGMA and MAPLE tend to get very slow for large values of n.

Acknowledgments

The authors wish to sincerely thank one of the referees for pointing out that the arguments in this paper are valid for the factor rings $k[X]/(X^n - X - 1)$, k any

field (for which n is such that $X^n - X - 1$ is irreducible in $k[X]$), and not only for $\mathbb{Z}_p[X]/(X^n - X - 1)$, p a prime (for which $X^n - X - 1$ is irreducible in $\mathbb{Z}_p[X]$).

As far as the second author is concerned, this material is based upon work supported by the National Research Foundation of South Africa under Grant No. 2053726. Any opinion, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Research Foundation. This work was initiated while he was visiting Texas A&M University during August 2002–May 2003. He wishes to express his gratitude towards the Department of Mathematics at Texas A&M University for the hospitality bestowed upon him.

References

[1] N. Jacobson, Lectures in Abstract Algebra, in: Vol. II—Linear Algebra, Van Nostrand Company, Princeton, 1953.
[2] A.V. Kelarev, Ring Constructions and Applications, World Scientific, Singapore, 2002.
[3] R. Lidl, H. Niederreiter, Introduction to Finite Fields and their Applications, Cambridge University Press, Cambridge, 1986.
[4] D.A. Suprunenko, R.I. Tyshkevich, Commutative Matrices, Academic Press, New York, 1968.
[5] N. Zierler, On $x^n + x + 1$ over GF(2), Inform. Control 16 (1970) 502–505.