arXiv:2301.05612v1 [math.RA] 13 Jan 2023

有限域与可数域上的伴随弱周期矩阵

Peter Danchev 和 Andrada Pojar

Abstract. 我们研究了域 $\mathbb{F}$ 上所有伴随 $n \times n$ 矩阵均为幂零指数为 2 的弱周期矩阵这一情形，并证明，只有当 $\mathbb{F}$ 是一个正特征可数域，且是其极小简单（有限）子域的代数扩张，同时其所有子域的阶均大于 n 时，这种情形才可能出现。特别地，在交换情形下，我们还证明 $\mathbb{F}$ 是一个阶大于 n 的有限域。

我们的结果在一定程度上推广了 Breaz-Modoi 在《线性代数及其应用》（2016年）中所得的结果。

1. Introduction and Principalities

设 $\mathbb{F}$ 是一个域， n 是任意一个非负整数，记作 $n \geq 1$。我们用 $M_n(\mathbb{F})$表示由 $\mathbb{F}$上的所有方阵 $n \times n$ 组成的矩阵环。对于一个非负整数 $m \geq 2$，我们用 τ 表示循环 $\tau_m = (1\ 2\ \ldots\ m) \in S_m$，用$P_{\tau_m}$ 表示 $\mathbb{F}$上的 $m \times m$ 置换矩阵，其元素只有 0 和 1，即$P_{\tau_m} =(a_{ij})_{1\leq i,\ j\leq m}$，其中若 $j = \tau_m(i)$，则$(a_{ij}) = 1$；若 $j \neq \tau_m(i)$，则$(a_{ij}) = 0$。

若存在一个整数 $k \geq 1$ 使得 $M^{k+1} = M$，则称矩阵 $M \in M_n(\mathbb{F})$是幂等的。因此，令 ST_n为所有幂等伴随矩阵$C \in M_n(\mathbb{F})$的迹的集合。单位根指 $\mathbb{F}$ 上的多项式的一个根，其形式为 $g = X^i - 1$，其中 i 是满足 $i \geq 2$的整数。因此，令 SR_n 为至多 n次单位根之和的集合，这些单位根不必互不相同。

同样，我们用 $L_{m,n}$ 表示次数至多为 m 、系数为单位元的非负整数倍且系数之和不超过 n 的多项式集合。我们还用 $W_m = \cup_{f\in L_{m,n}} Spec(f(P_{\tau_m}))$ 表示，而符号 $d(m)$ 表示 m 的非负因数个数。

设 R 是一个环。若存在一个非负整数 $q \geq 1$ 使得 $x^{q+1} = a$，则称元素 $x \in R$ 为幂等势元；若 x 是 R 中一个幂等势元与一个平方零幂零元之和，则称 $x \in R$ 是幂零指数 2 弱周期的。此外，若环 R 的每个元素 R 都是幂零指数 2 弱周期的，则称环 R 是幂零指数 2 弱周期的。

从历史上看，弱周期性的概念在相关文献中自然地出现了。事实上， [3] 证明了环 x 中的元素R 是周期的，即 $x^n = x^m$ 对于某两个不同的正整数 m， n，当且仅当 x 可以写成一个幂等势元与一个彼此可交换的幂零元素之和。因此，去掉“可交换性”这一条件后，考虑这两个元素的和是很自然的。此外，若环 R 的所有元素都是弱周期的，则称其为弱周期环。

另一方面，Diesl 在 [5] 中定义了幂零清洁环的概念 R：对于每个 $a \in R$，该环中都存在一个幂等元 e 和一个幂零元 b，使得

2010 *Mathematics Subject Classification.* 主要分类号：15A23、15B33；次要分类号：16S50、16U60。*Key words and phrases.* 伴随矩阵、域、幂等幂元、平方零幂零元。

$a = e+b$。此外，Ye 在 [7] 中引入了半洁净环 R的概念：对于每个 $a \in R$，该环中都存在一个幂等 c 元和一个单位 u，使得 $a = c + u$。因此，显然弱周期环介于幂零清洁环和半洁净环之间。所以，确实有必要对它们进行详细探究，这正是本文的主题，也是我们的基本动机。我们的主要目的是确定基域的幂结构：如果该域上的所有伴随矩阵要么都是幂零指数为 2 的交换弱周期矩阵，要么都是幂零指数为 2 的弱周期矩阵，那么该基域分别是什么样的。下文将证明，这样的域分别是有限域或可数无限域。

2. Main Results

我们将基本结果分为以下两个小节：

2.1. 一般情形。我们首先给出一个简单但有用的技术性引理。

引理 2.1. 设 $n \geq 1$ 是一个整数。那么，包含关系 $ST_n \subseteq SR_n$ 成立。

证明。设 $t \in ST_n$ 是幂等伴随矩阵 C 的迹，且 $C^{m+1} =C$，其中 $m \geq 1$ 是某个非负整数。设 λ 是 C 的一个特征值。那么，$\lambda^{m+1} = \lambda$。由此可知，或者 $\lambda = 0$，或者 $\lambda^m = 1$。设 k 是 C 的不同非零特征值的个数，记为 λ_1、λ_2、.....、λ_k。因此可知，存在非负整数 α_1、α_2、.....、α_k、α_{k+1}，其和为 n，以及非零整数 α_1、α_2、.....、α_k，使得

$$t = \alpha_1\lambda_1 + \alpha_2\lambda_2 + \ldots + \alpha_k\lambda_k + \alpha_{k+1} \cdot 0.$$

因此，

$$t = \alpha_1\lambda_1 + \alpha_2\lambda_2 + \ldots + \alpha_k\lambda_k,$$

使得不等式 $\alpha_1 + \alpha_2 + \ldots + \alpha_k \leq n$ 成立。因此，t 是一个.....之和 t 个 n m 次单位根。因此，$t \in SR_n$，正如所需。□

下面继续介绍几条对我们的工作至关重要的结论。

命题 2.2。设 $n \geq 1$ 为一个非负整数，$C \in M_n(\mathbb{F})$ 为域 $\mathbb{F}$上的伴随矩阵。则以下两个断言成立：

(1) 若 C 是幂零指数 2 的弱周期矩阵，则迹 $C \in SR_n$。(2) 若迹 $C \in ST_n$，则 C 是幂零指数 2 的弱周期矩阵。

证明。（1）假设 $C = M + N$ 是幂等元，且 N 是平方零幂零元，使得 trace $C \notin SR_n$。显然，trace$C \notin ST_n$。由于 trace $N = 0$，可得 trace C = trace M。因此可推知，M 与伴随矩阵不相似。现在考虑下面两种情形：

情形 1：M 与两个伴随矩阵的直和相似，其中 C_1 的大小为 l，C_2 的大小为 $n - l$，因此存在一个定义在 $\mathbb{F}$ 上、大小为 n 的可逆矩阵，使得 $M = U(C_1 \oplus C_2)U^{-1}$。因此，trace M = trace C = trace C_1 + trace C_2。由于直和 $C_1 \oplus C_2$ 显然是幂等的，因此可知 trace $C_1 \in ST_l$ 且 trace $C_2 \in ST_{n-l}$。由引理 2.1 可得，trace $C_1 \in SR_l$ 且 trace $C_2 \in SR_{n-l}$。因此，trace C_1+trace $C_2 \in SR_n$，从而 trace $M \in SR_n$。但是 trace C = trace M，所以可得 trace $C \in SR_n$。

情形 2：M 相似于 u 伴随矩阵的直和，其中 $3 \leq u \leq n$。容易通过对 u 进行归纳法得出迹 $C \in SR_n$。

（2）由于迹 $C \in ST_n$，存在一个幂等伴随矩阵 C'，使得迹 $C' =$ 迹 C，因此 $(C - C')^2 = 0$。综上所述，C 是弱周期的，幂零指数为 2，结论得证。□

命题 2.3. 设 $n \geq 2$ 为一个整数。如果所有 $n \times n$ 伴随矩阵都是幂零指数 2 的弱周期矩阵，则 $\mathbb{F} \subseteq SR_n$。

证明。 借助命题 2.2 可立即得到。 □

引理 2.4. 设 $n \geq 2$ 为一个整数。则以下包含关系成立：

$$\cup_{k \leq n, d(m) \geq k} W_m \subseteq \cup_{m \in \mathbb{N}, m \geq 2} W_m.$$

证明。由以下显而易见的事实可直接得到：对于任意非负整数 $m \geq 2$，如果 m 至少有 k 个因数，则 m 至少有一个因数。□

引理 2.5. 设 $n \geq 1$ 为一个非负整数。则以下关系成立：

$$SR_n \subseteq \cup_{m \in \mathbb{N}, m \geq 2} W_m.$$

证明。设 $t \in SR_n$，则存在非零整数 $1 \leq k \leq n$ 和 α_1、α_2、$\ldots \alpha_k$，其和不超过 n；此外，还存在单位根 λ_1、λ_2、$\ldots \lambda_k$ 以及非负整数 m_1、m_2、…、m_k，使得 $\lambda_1^{m_1} = \lambda_2^{m_2} = \ldots = \lambda_k^{m_k} = 1$，并且

$$t = \alpha_1 \lambda_1 + \alpha_2 \lambda_1 + \ldots \alpha_k \lambda_k.$$

若取 m 为 m_1、m_2、…、m_k的公倍数，则对每个$i \in \{1, 2, \ldots, k\}$都有 $\lambda_i^m = 1$。因此，$k \leq m$ 并且

$$\{\lambda_1, \lambda_2, \ldots, \lambda_k\} \subseteq \{\epsilon^{a_1} + \epsilon^{a_2}, \ldots \epsilon^{a_k}\},$$

其中 $\{a_1, a_2, \ldots, a_k\} \subseteq \{0, 1, \ldots, m-1\}$，且 ϵ 使其生成所有 m次单位根。不失一般性，我们可以假设 $a_1 < a_2 < \ldots < a_k$。因此，

$$t = \alpha_1 \epsilon^{a_1} + \alpha_2 \epsilon^{a_2} + \ldots + \alpha_k \epsilon^{a_k}.$$

现在假设

$$f = \alpha_1 X^{a_1} + \alpha_2 X^{a_2} + \ldots + \alpha_k X^{a_k}.$$

由于 α_1、α_2、…、α_k 是和不超过 n 的非负整数，因此 1 可知 $f \in L_{m,\ n}$。我们还可以得到等式

$$t = f(\epsilon).$$

由于 ϵ 是一个本原 m 次单位根，因此可推出 ϵ 是 P_{τ_m} 的特征值，进而 $f(\epsilon)$ 是 $f(P_{\tau_m})$ 的特征值。

此外，由于 m 是 k 的一个公倍数，m_1，m_2、…、m_k，必有 $m \geq 2$ 是一个非负整数。现在，由于 m 是一个非负整数，m 是数 k 的因数的公倍数，当且仅当 m 至少有 k 个因数，因此结合引理2.4，可得

$$SR_n \subseteq \cup_{k \leq n, d(m) \geq k} W_m \subseteq \cup_{m \in \mathbb{N}, m \geq 2} W_m,$$

如所述。 □

引理 2.6. 设 $m \geq 2$ 和 $n \geq 1$ 是整数。若 $\omega \in W_m$，则存在两个单位元的整数倍 $u = u(\omega)$和 $\alpha = \alpha(\omega)$，使得 $(\omega - \alpha)^m = u$。

证明. 给定 $\omega \in W_m$。那么，对于每个 $f \in L_{m,n}$，我们有 $\omega \in Spec(f(P_{\tau_m})$。由此可知， ω 是多项式 $det(XI_m - f(P_{\tau_m})$的一个根。但是，由于 $f \in L_{m,n}$，存在 $1 \leq k \leq m$ 和非零整数 $\alpha_1, \alpha_2, \ldots, \alpha_k$，以及取值不超过 $n-1$ 的非负且两两不同的整数 $a_1, a_2, \ldots, a_k$，使得

$$f = \alpha_1 X^{a_1} + \alpha_2 X^{a_2} + \ldots + \alpha_k X^{a_k}.$$

因此，

$$f(P_{\tau_m}) = \alpha_1 (P_{\tau_m})^{a_1} + \alpha_2 (P_{\tau_m})^{a_2} + \ldots + \alpha_k (P_{\tau_m})^{a_k}.$$

由于 τ_m 是 S_m中的一个循环，且 $\tau_m = (1\ 2 \ldots\ m)$，因此 τ_m 是由$m-1$ 个对换构成的乘积，故 τ_m 和 m 显然具有不同的奇偶性。

此外，假设 m 为偶，则可知 τ_m 为奇，因此对于每个 $i \in \{1, 2, \ldots, k\}$， $\tau_m^{a_i}$和 a_i 具有相同的奇偶性。现在，令 $(b_{ij})_{1 \leq i,\ j \leq m} = XI_m - f(P_{\tau_m})$ 和 $\alpha_i = f(0)$。因此，

$$det(f(P_{\tau_m}) - XI_m) = (\alpha_i - XI_m)^m + \sum_{\sigma \neq e, \sigma even} b_{1\sigma(1)} \cdots b_{m\sigma(m)} - \sum_{\sigma odd} b_{1\sigma(1)} \cdots b_{m\sigma(m)} =$$

$$= (\alpha_i - X)^m + (-1)^{a_1+1}\alpha_1^m + (-1)^{a_2+1}\alpha_2^m + \ldots + (-1)^{a_k+1}\alpha_k^m - (-1)^{a_i+1}\alpha_i^m.$$

因此，对于偶数 m，我们得到：

$$(\alpha_i - \omega)^m = (-1)^{a_1}\alpha_1^m + (-1)^{a_2}\alpha_2^m + \ldots + (-1)^{a_k}\alpha_k^m - (-1)^{a_i}\alpha_i^m.$$

假设现在 m 为奇，则可推知 τ_m 为偶，因此对每个 $i \in \{1, 2, \ldots, k\}$， $\tau_m^{a_i}$ 均为偶。现在，令 $(b_{ij})_{1 \leq i,\ j \leq m} = f(P_{\tau_m}) - XI_m$和 $\alpha_i = f(0)$。因此，

$$det(f(P_{\tau_m}) - XI_m) = (\alpha_i - X)^m + \sum_{\sigma \neq e, \sigma even} b_{1\sigma(1)} \cdots b_{m\sigma(m)} - \sum_{\sigma odd} b_{1\sigma(1)} \cdots b_{m\sigma(m)} =$$

$$= (\alpha_i - X)^m + \alpha_1^m + \alpha_2^m + \ldots + \alpha_k^m - 0 - \alpha_i^m.$$

因此，对于奇数 m，我们得出：

$$(\omega - \alpha_i)^m = \alpha_1^m + \alpha_2^m + \ldots + \alpha_k^m - \alpha_i^m.$$

最后，存在多个单位根，例如 $\alpha = \alpha_i$ 和 u，使得 $(\omega - \alpha)^m = u$，如所要求。□

下一个断言与 [4]中的断言密切相关。

引理 2.7. 对于某个 $l \geq 1$，有限伽罗瓦域 $GF(p^l)$ 上任意没有重特征值的可对角化矩阵都是非亏损幂等矩阵。

证明。由于 $x \in GF(p^l)$ 中的每个元素都满足方程 $x^{p^l} = x$，因此 $GF(p^l)$ 上的每个对角矩阵都是幂等的。因此， $GF(p^l)$ 上的任意可对角化矩阵必然是幂等矩阵。

由于该矩阵没有重特征值，每个特征值的代数重数都恰好为 1。又由于该矩阵可对角化，任意特征值的几何重数等于其代数重数，因此也为 1。因此，该矩阵也是非亏损的。

总之，该矩阵是一个非亏损幂等矩阵，正如预期。 □

以下域论中的技术性断言，是我们证明下文主要结果的关键。

命题 2.8. 每个作为其极小简单（有限）子域的代数扩张的无限域，都是其有限子域的无限可数并，因此它是可数的。此外，这些有限子域可以取为 GF(p^{l_i}) 这样的形式，使得 GF(p^{l_i}) 包含于 GF($p^{l_{i+1}}$)，且对于每个 $i \geq 1$， l_i 整除 l_{i+1}。

证明。给定 $\mathbb{F}$，它是特征为 $p > 0$ 的无限域，是其含有 p 个元素的简单子域 $\mathbb{F}_p$ 的代数扩张； u 是 $\mathbb{F}$ 中的任意元素。因此，每个 $\mathbb{F}_p(u)$（即由 u 生成的 $\mathbb{F}_p$ 的扩张）都是 $\mathbb{F}_p$ 的有限扩张，因而是 $\mathbb{F}$ 的有限子域。具体而言， $\mathbb{F}$ 的所有有限子域都属于这种类型，因为对于 $\mathbb{F}_p$ 的有限扩张，经典的“本原元”定理成立。我们还知道， $\mathbb{F}_p(u) \cong F_p[X]/(g_u(X))$，其中 X 是关于 $\mathbb{F}_p$ 的超越元，而 $g_u(X)$ 是 u 关于 $\mathbb{F}_p$ 的最小多项式。为确保 $g_u(X)$ 的唯一性，通常我们假设它是首一的，也就是说，它的首项系数恰好为 1。此外，扩张 $\mathbb{F}_p(u)/\mathbb{F}_p$ 的次数 $[\mathbb{F}_p(u) : \mathbb{F}_p]$ 与多项式 $g_u(X)$ 的次数相同。

此外，扩张 $\mathbb{F}_p(u)/\mathbb{F}_p$ 是正规扩张，其伽罗瓦群为循环群。此外，对于每个正整数 n，形如 $\mathbb{F}_p(u)$ 的域至多（恰好）有一个是域 $\mathbb{F}_p$ 的次数为 n 的扩张。换言之，形如 $\mathbb{F}_p(u)$ 的 $\mathbb{F}$ 的所有子域，与集合 $\mathbb{N}$ 的某个子集之间存在双射；集合 $\mathbb{N}$ 由所有自然数组成。具体而言，这个子集由 $\mathbb{N}$ 中那些等于某个元素 $u \in \mathbb{F}$ 的次数 $[\mathbb{F}_p(u) : \mathbb{F}_p]$ 的元素组成。由于 $\mathbb{N}$ 的任意子集要么有限，要么可数无限，因此迄今为止的论证使我们能够得出结论： $\mathbb{F}$ 可以表示为有限个或可数无限个有限（子）域的并。当且仅当 $\mathbb{F}$ 是可数无限域时，这个并才是可数的，正如后文所述。

接下来，根据我们已经证明的结果，基域 $\mathbb{F}$ 是可数的，因此 $\mathbb{F}$ 中的元素可以线性排序为 $f_1, \ldots, f_n, \ldots$。对每个 $n \in \mathbb{N}$，令 $\mathbb{F}_n = \mathbb{F}_p(f_1, \ldots, f_n)$。现在很容易看出， $\mathbb{F}$ 等于其所有子域 $\mathbb{F}_n$ 的可数并，其中 $n \geq 1$。此外，由于 $\mathbb{F}_n/\mathbb{F}_p$ 同时是代数扩张且有限生成，因此很容易推出它是有限扩张。同样，对于每个自然数 $n \geq 1$，显然 $\mathbb{F}_n$ 是 $\mathbb{F}_{n+1}$ 的子域。因此，我们得出结论： $\mathbb{F}_n$ 是一个阶为 p^{l_n} 的有限域，其中 $l_n = [\mathbb{F}_n : \mathbb{F}_p]$。由于 $\mathbb{F}_n \leq \mathbb{F}_{n+1}$，可推得 l_{n+1} 可被 l_n 整除，并且对所有 $n \in \mathbb{N}$，等式 $l_{n+1}/l_n = [\mathbb{F}_{n+1} : \mathbb{F}_n]$ 成立，证毕。

至于第二部分，即这样的域必然是.....，现在可由第一部分立即得出。□

以下评论值得一提，以说明前述结论中的条件不能弱化。

注 2.9. 已知 $\mathbb{F}_p$ 是特征为 p 的简单（有限）域，运用常规论证可知，有理函数域 $\mathbb{F}_p(X)$ 是一个可数域，其变量为 X ，系数取自 $\mathbb{F}_p$；该域实际上是 $\mathbb{F}_p$ 的超越扩张，也是一个特征为 p 、无法表示为可数个有限域之并的可数域。此外，用同样的方法可以看出，有理数域 $\mathbb{Q}$ 也无法表示为可数个有限域之并。

现在我们得出了本文的第一个主要结果。具体而言，以下结论成立：

定理 2.10. 设 $n \geq 1$ 是一个整数， $\mathbb{F}$ 是一个域。那么以下两个条件等价:

(1) 每个 $n \times n$ 上的伴随矩阵都是一个幂等元与一个平方为零的幂零元之和。
（2） $\mathbb{F}$ 是一个正特征可数域，它是其极小简单（有限）子域的代数扩张，且所有子域的阶都大于 n。

证明。 (1) $\Longrightarrow$ (2)。假设每个 $n \times n$ 伴随矩阵 C 在 $\mathbb{F}$ 上都是幂零指数为 2 的弱周期矩阵。根据命题 2.5，可得$\mathbb{F} \subseteq \cap_{m\in\mathbb{N},\ m\geq 2} W_m$。但是，对于每个 $\omega \in W_m$，都存在单位元的整数倍，记为 α 和 u，使得 $(\omega - \alpha)^m = u$，这是由引理 2.6得到的。

反设 $\mathbb{F}$ 的特征为零。于是，每个非零的单位元整数倍 s 都是可逆的。令 $\omega = r \cdot s^{-1}$，并设 r 和 ω 是单位元的整数倍。因此，$r \cdot s^{-1} \in \cap_{m\in\mathbb{N},\ m\geq 2} W_m$。取一个 $m \geq 2$。于是，存在单位元的整数倍 α 和 u，使得 $(r \cdot s^{-1} - \alpha)^m = u$。根据经典牛顿二项式公式，可得

$$(r \cdot s^{-1})^m + (-1)^1 \binom{m}{1} (r \cdot s^{-1})^{m-1}\alpha + (-1)^2 \binom{m}{2} (r \cdot s^{-1})^{m-2}\alpha^2 + \ldots$$
$$+(-1)^{m-1} \binom{m}{m-1} (r \cdot s^{-1})^1 \alpha^{m-1} + \alpha^m = u$$

因此

$$r^m + (-1)^1 \binom{m}{1} r^{m-1}s\alpha + (-1)^2 \binom{m}{2} r^{m-2}s^2\alpha^2 +$$
$$\ldots + (-1)^{m-1} r^1 s^{m-1}\alpha^{m-1} + \alpha^m \cdot s^m = u \cdot s^m,$$

这等价于

$$r^m = ((-1)^0 \binom{m}{1} r^{m-1} \cdot \alpha + (-1)^1 \binom{m}{2} r^{m-2}\alpha^2 s +$$
$$\ldots + (-1)^{m-2} r\alpha^{m-1}s^{m-2} + \alpha^m \cdot s^{m-1} + us^{m-1}) \cdot s.$$

由于假设该域的特征为零，我们不失一般性地认为上述方程在 $\mathbb{Z}$ 中成立，由此可得 s 整除r^m 对任意 $s \in \mathbb{Z}^*$， $r \in \mathbb{Z}$，这显然是错误的；例如，考虑$s = 2$ 和 $r = 3$即可。因此，该域的特征必为某个非零素数，记作 $p > 0$。此外，命题 2.3 表明该域必为可数域，因为 SR_n 可数且 $\mathbb{F} \subseteq SR_n$。

现在，假设对于某个整数 l，满足不等式 $2^t \neq p^l - 1 \leq n - 1$（对任意非负整数 t），包含关系 $GF(p^l) \subseteq \mathbb{F}$ 成立。因此， $p^l - 1$存在一个奇真因子 d。进一步，取一个非负奇整数 q，使得 q 和 $p^l - 1$ 互素。于是， $m = d \cdot q$ 为奇数，且$d = gcd(p^l - 1, m)$。设方程 $x^m - 1 = 0$ 在 $\mathbb{F}$上成立。它在 $GF(p^l)$中有 d 个解，即 $1, h, h^2, \ldots, h^{d-1}$，其中 g 是域 $GF(p^l)$的乘法循环群的生成元。由于 $h^d = 1$，我们有

$$1 + h + h^2 + \ldots + h^{d-1} = 0.$$

因此，

$$-1 = h + h^2 + \ldots + h^{d-1}.$$

因此，-1 是若干个 $d-1$ m次单位根之和，且它们都不等于 1。由于 $d-1 < d \leq p^l - 1 \leq n-1$，我们发现

$$-1 = \alpha_1 h + \alpha_2 h^2 + \ldots + \alpha_{d-1} h^{d-1}$$

with

$$\alpha_1 = \alpha_2 = \ldots = \alpha_{d-1} = 1,$$

因此，根据引理的2.6 证明可知

$$(-1-0)^m = \alpha_1^m + \alpha_2^m + \ldots + \alpha_{d-1}^m - 0.$$

此外，$(-1)^m = d-1$，且由于 m是奇数，我们推知 p整除 d。但是， d整除$p^l - 1$。因此，根据传递律， p 必定整除 $p^l - 1$ ，从而整除 $p = 1$，这就产生了矛盾。

因此，对于某个整数 l ，有 $GF(p^l) \subseteq \mathbb{F}$ ，其中 $2^t = p^l - 1 \leq n-1$ ，且 t是某个非负整数。由此可知， $p-1$ 和 $r = p^{l-1} + p^{l-2} + \ldots + p + 1$是 2 的幂，并且 $p-1$ 整除 r。但是，由于 $p-1$ 整除 $r-l$，我们得到 $p-1$ 整除 l。因此，由于 $p \neq 2$，我们推知 $l = 2u$ ，其中 u 是一个正整数。也就是说，$(p^u - 1)(p^u + 1) = 2^t$ ，从而 $p^u - 1$ 整除 $p^u + 1$。最后， $p^u - 1$整除 2，且由于 $p \neq 2$，我们得到 $p = 3$ 和 $u = 1$。

因此， $l = 2u = 2$ 和 $GF(p^l) = GF(3^2)$。令 g 为 $GF(9)$ 乘法群的生成元。由于 $gcd(3^2 - 1, 12) = 4$，域 $GF(3^2)$ 中有四个 12 次单位根。它们是 ϵ^0、 ϵ^6、ϵ^{a_3}和 ϵ^{a_4}，其中 ϵ是本原 12 次单位根，而 a_3 和 a_4 是小于 12 且不等于 6 的两个不同正整数。然而，由于 $\frac{3^2-1}{4} = 2$，我们有

$$\{1, -1, \epsilon^{a_3}, \epsilon^{a_4}\} = \{1, g^2, (g^2)^2, (g^2)^3\}.$$

由于 $(g^2)^4 = 1$，可得

$$1 + g^2 + (g^2)^2 + (g^2)^3 = 0.$$

因此，

$$-1 = -1 + \epsilon^{a_3} + \epsilon^{a_4}.$$

由此我们得到两点：$\epsilon^{a_3} = -\epsilon^{a_4}$，且 -1 是至多 n 12–次单位根之和，因为 $3 < 3^2 \leq n$。因此，仿照引理2.6的证明，并考虑到 12 是偶数，可得

$$(0-(-1))^{12} = (-1)^6 \cdot 1^{12} + (-1)^{a_3} \cdot 1^{12} + (-1)^{a_4} \cdot 1^{12}.$$

由此可知，数 a_3 和 a_4 不可能同时为奇数或同时为偶数。因此，不失一般性，我们可以假设 a_3 为偶数， a_4 为奇数。又由于 $\epsilon^{a_3} = -\epsilon^{a_4}$，我们得到 $(-\epsilon)^{a_3} = (-\epsilon)^{a_4}$。然而，由于 ϵ 不属于集合 $\{-1, 0, 1\}$，而 a_3 和 a_4 是小于 12 的正整数，因此必然有 $a_3 = a_4$，这又产生了一个矛盾。

现在，为了证明 $\mathbb{F}$ 是其极小简单（有限）子域的代数扩张，我们将证明 $\mathbb{F}$ 的每个非零元素都是单位根。事实上，根据命题 2.3，我们有 $\mathbb{F} \in SR_n$，即至多由 n 个单位根构成的所有和的集合。此外，根据引理 2.5，我们得到 $SR_n \subseteq \cup_{m \in \mathbb{N},\ m \geq 2} W_m$；而引理 2.6 使我们得知，若 $x \in W_m$，则存在 $u \in \mathbb{F}_p$ 和 $\alpha \in \mathbb{F}_p$ ，使得 $(x-\alpha)^m = u$。同样，前述引理的证明告诉我们，若 x 是其中恰有 α 个 1 的至多由 n m 次单位根构成的和，则 $(x-\alpha)^m \in \mathbb{F}_p$。因此，我们可以假设

满足 $x=\alpha$。若 $x\neq 0$，则 $x^{p-1}=1$，因而 x 是单位根。然而，若 x 是其中没有 1 的、至多由 n 个单位根构成的和，则 $(x-\alpha)^m\in\mathbb{F}_p-\{0\}$。因此，$x=\alpha+y$，其中 $\alpha^{p-1}=1$ 且 $y^{m(p-1)}=1$。若 $\alpha\neq 1$，则 x 是两个不等于 1 的单位根之和。因此，$x^{m(p-1)}\in\mathbb{F}_p-\{0\}$，从而 $x^{m(p-1)^2}=1$。于是，x 是单位根。现在取 $\alpha=1$。但是，由于

$$x=1\cdot 1+y=(p-1)\cdot(-1)+y=((n-1)\cdot(-1)+y)+(p-n)\cdot(-1),$$

我们有 $(n-1)(-1)+y$ 是 $n-1$ 个单位根之和，等于 (-1)，并且有一个 $m(p-1)-th$ 单位根不等于 1。由此可得 $((n-1)\cdot(-1)+y-1\cdot 0)^{m(p-1)}=1$。此外，如果 $(p-n)\cdot(-1)=1$，那么 p 整除 $n-1$。但是$n-1\leq p-1$，因此 $p\leq p-1$，这是错误的。由此矛盾，我们推得 x 是两个不等于 1 的 $m(p-1)$ 阶单位根之和。因此，$x^{m(p-1)}\in\mathbb{F}_p-\{0\}$，从而 $x^{m(p-1)^2}=1$。最后，x 是一个单位根，正如所承诺的。总之，$\mathbb{F}$是一个正特征可数域，它是其极小简单（有限）子域的代数扩张，且其所有阶大于 n 的子域均如所求。

(2) $\Longrightarrow$ (1)。设 $GF(p^l)$ 包含于 $\mathbb{F}$。取 C_1 为 $n\times n$ 上的伴随矩阵，定义在 $GF(p^l)$ 上。那么，由于 $p^l\geq n+1$，应用 [4] 中的主要结果可得，我们可以将 $C_1=D_1+N_1$分解为，其中 D_1 是定义在 $GF(p^l)$ 上且没有重特征值的可对角化矩阵，N_1 是定义在 $GF(p^l)$ 上、幂零指数为 2 的幂零矩阵。现在，利用引理 2.7 可知 D_1 是非亏损幂等矩阵，并且由于迹 $N=0$，我们可以得到迹 $C_1=$ 迹 D_1。因此，$GF(p^l)$ 中的任意元素都可以是非亏损幂等矩阵的迹。于是，$GF(p^l)$ 中的每个元素都可以是幂等伴随矩阵的迹。

现在，根据命题 2.8，每个正特征可数域若为其极小简单（有限）子域的代数扩张，则它是其有限子域的可数并，因此立即可知 $\mathbb{F}$ 中的每个元素都可以是定义在 $n\times n$上的幂等伴随矩阵的迹 $\mathbb{F}$。因此，令 C为任意一个$n\times n$ 定义在 $\mathbb{F}$上的伴随矩阵。那么，迹 $C\in ST_n$。总之，应用命题 2.2(2)，可推得 C 可以写成定义在 $\mathbb{F}$上的一个幂等矩阵与一个二阶幂零矩阵之和，如所需。□

现在我们讨论幂等矩阵与平方为零矩阵彼此交换的情形。

2.2. 交换情形。我们将在此研究幂零指数为 2 的伴随矩阵的弱周期情形，其中已有的幂等矩阵与平方零幂零元彼此交换。为此，我们首先需要以下两条技术约定。

引理 2.11. 设 n 为正整数，$\mathbb{F}$ 为域。若对于每个 $\mathbb{F}$ 上的 C 伴随矩阵 $n\times n$，都存在一个整数 $t>1$、一个幂等矩阵 P，使得 $P=P^t$，以及一个平方零幂零元 N，使得 $C=P+N$，其中 $PN=NP$，则以下两点成立：

(1) 若 C 可逆，则 χ_C 整除 $(X^{t-1}-1)^2$。(2) 若 λ_1、λ_2、...、λ_n 是 $\mathbb{F}$ 中的非零元素，则存在一个整数 $t>1$，使得对于每个 $i\in\{1,2,\ldots,n\}$，都有 $\lambda_i^{t-1}=1$。

证明。（1）由于 $C=P+N$和 $PN=NP$，因此 $CP=PC$和$CN=NC$。但我们有 $(C-N)^t=C-N$。由于 $CN=NC$，我们可以应用

牛顿二项式公式，论证存在一个 $n \times n$ 矩阵，其元素取自 $\mathbb{F}$，使得

$$C^t - tCN + MN^2 = C - N.$$

但是，由于 $N^2 = 0$，我们得到

$$C(C^{t-1} - tN) = C - N.$$

两边乘以 $C^{t-1} + tN$，可得

$$C(C^{2t-2} - t^2N^2) = C^t + tCN - C^{t-1}N + tN^2,$$

并利用 $N^2 = 0$，我们写出等式

$$C^{2t-1} = C^t + (tC - C^{t-1})N.$$

但是 C 可逆，因此

$$C^{2t-2} - C^{t-1} = (tId_n - C^{t-2})N.$$

现在，考虑到 $CN = NC$ 和 $N^2 = 0$，我们推得

$$((C^{t-1})^2 - C^{t-1})^2 = 0,$$

并且由于 C 可逆，我们得出

$$(C^{t-1} - 1)^2 = 0.$$

因此， C 的最小多项式整除$(X^{t-1} - 1)^2$。但是， C 的最小多项式就是特征多项式，记作 χ_C，它属于 C。综上所述， χ_C 整除$(X^{t-1} - 1)^2$, , 如所述。

(2) 只需令 C 为特征值为 λ_1、 λ_2、.....、 λ_n 的伴随矩阵，并结合前述(1)以及 λ_1、 λ_2、.....、 λ_n 来自 $\mathbb{F}$这一事实即可。□

引理 2.12. 设 n 为正整数， $\mathbb{F}$ 为域。若对于每个 $n \times n$ ，在 $\mathbb{F}$上的伴随矩阵 C ，都存在一个整数 $t > 1$、一个幂等矩阵 P 使得 $P = P^t$，以及一个平方为零的幂零矩阵 N使得 $C = P + N$且 $PN = NP$，则以下两个条件成立:

(1) 如果 C 可逆，那么存在一个多项式 $q \in \mathbb{F}[X]$，使得 χ_C 整除 $(q(X) - X)^2$。(2) 如果 λ_1、 λ_2、.....、 λ_n 是 $\mathbb{F}$ 的非零元素，那么存在一个多项式 $q \in \mathbb{F}[X]$，使得对每个 $i \in \{1, 2, \ldots, n\}$，都有 $q(\lambda_i) = \lambda_i$。

证明。(1) 由于 $C = P + N$ 和 $PN = NP$，可知 $CP = PC$ 和 $CN = NC$。众所周知，所有与伴随矩阵 C 可交换的矩阵，都可以表示为 $\mathbb{F}$ 上关于 C 的多项式。因此，存在 $q \in \mathbb{F}[X]$ ，使得$C = q(C) + N$。现在，由于 $N^2 = 0$，可知 $(q(C) - C)^2 = 0$。因此， C 的最小多项式显然整除 $(q(X) - X)^2$。但 C 的最小多项式就是其特征多项式，记作 χ_C，其中 C。综上所述， χ_C 整除 $(q(X) - X)^2$, , 正如所需。

(2) 只需令 C 为特征值为 $\lambda_1, \lambda_2, \ldots, \lambda_n$ 的伴随矩阵，并结合前述条件 (1) 以及 $\lambda_1, \lambda_2, \ldots, \lambda_n$ 来自 $\mathbb{F}$ 这一事实。□

以下数论命题是众所周知的民间事实，但我们在此陈述它，仅为完整起见并方便读者。

引理 2.13. 设 a、 b、 c 为三个正整数。则， $gcd(bc, a)$ 整除 $gcd(b, a) \cdot gcd(c, a)$。

证明. 设 $f = gcd(a, bc)$、 $f_1 = gcd(a, b)$ 和 $f_2 = gcd(a, c)$。那么，存在整数 s_1、 s_2、 t_1、 t_2 使得

$$f_1 = s_1a + t_1b$$

and

$$f_2 = s_2a + t_2c.$$

因此,

$$f_1f_2 = s_1s_2a^2 + s_1t_2ac + t_1s_2ba + t_1t_2bc.$$

但 f 整除 a 且 f 整除 bc，所以 f 整除 a^2， f 整除 ac， f 整除 ba 且f整除 bc。因此， f整除 f_1f_2，从而 $gcd(bc, a)$ 整除 $gcd(b, a) \cdot gcd(c, a)$，如上所述。□

接下来的注释旨在解释交换情形下的复杂情况。

注 2.14. 设 $\lambda_1, \lambda_2, \ldots, \lambda_n$ 是 $\mathbb{F}$ 的互不相同的非零元素。由引理2.12(2)，存在 $q \in \mathbb{F}[X]$，使得对每个 $i \in \{1, 2, \ldots, n\}$，都有 $q(\lambda_i) = \lambda_i$。取 $GF(p^{l_1})$，使得 $\lambda_1, \lambda_2, \ldots, \lambda_n$ 属于 $GF(p^{l_1})$ $GF(p^{l_2})$，并且 $q \in GF(p^{l_2})[X]$，其中 $l = max(l_1, l_2)$。于是， $\lambda_1, \lambda_2, \ldots, \lambda_n$ 属于 $GF(p^l)$，而 $q \in GF(p^l)[X]$。

此外，由于 $\lambda_1, \lambda_2, \ldots, \lambda_n$ 均属于 $\mathbb{F}$，根据引理 2.11(2)，存在一个非负整数 $t > 1$ 使得 $\lambda_i^{t-1} = 1$ 对每个 $i \in \{1, 2, \ldots, n\}$都成立。现在，由于 $\lambda_1, \lambda_2, \ldots, \lambda_n$ 均属于 $GF(p^l)$，我们可以推知

$$\{\lambda_1, \lambda_2, \ldots, \lambda_n\} \subseteq \{h, h^2, \ldots, h^d = 1\},$$

其中 $h = g^{\frac{p^l-1}{d}}$， g 是 $GF(p^l)$ 的乘法群的一个生成元，且$d = gcd(p^l - 1, t - 1)$。因此， $n \leq d$，并且存在 $\{j_1, j_2, \ldots, j_n\} \subseteq \{1, 2, \ldots, d\}$ 使得 $\lambda_i = h^{j_i}$。最后，我们得到，对于满足 $h^d = 1$ 的每个 $i \in \{1, 2, \ldots, n\}$， $q(h^{j_i}) = h^{j_i}$，正如预期。

下一个例子展示了我们计算操作的一些具体方面。

例2.15. 若在前一个备注 2.14 中取 $\lambda_1 = g^i$ 和 $\lambda_2 = g^{i+1}$，其中 $i \in \{1, 2, \ldots, p^l - 2\}$，则可以看出

$$\{g^i, g^{i+1}\} \subseteq \{g^{\frac{p^l-1}{d}}, g^{2\frac{p^l-1}{d}}, \ldots, g^{d\frac{p^l-1}{d}}\}.$$

因此,

$$\{i, i + 1\} \subseteq \{\frac{p^l - 1}{d}, 2\frac{p^l - 1}{d}, \ldots, d\frac{p^l - 1}{d}\}.$$

因此，普通分数 $\frac{p^l-1}{d}$ 是 i 和 $i + 1$的公因数，所以它必定为 1。于是我们现在有 $p^l - 1 = d = gcd(p^l - 1, t - 1)$。总之， $p^l - 1$ 整除 $t - 1$，这正是我们要证明的。

现在我们可以证明第二个主要结果了。

定理 2.16. 设 $n \geq 1$ 是一个整数， $\mathbb{F}$ 是一个域。若 $\mathbb{F}$ 上的所有伴随$n \times n$ 矩阵都可以表示为 $\mathbb{F}$ 上的一个幂等矩阵与一个平方零矩阵之和，且这两个矩阵彼此可交换，则 $\mathbb{F}$ 是一个阶大于n的有限域。

证明。 设 $n \geq 1$ 是一个整数， $\mathbb{F}$ 是一个域，并且所有伴随 $n \times n$ 矩阵在$\mathbb{F}$ 上都可以表示为一个幂等矩阵与一个平方零矩阵之和，二者均在 $\mathbb{F}$ 上且彼此可交换。于是，根据定理2.10，可知 $\mathbb{F}$ 是一个具有正特征的可数域（它也是有限域的代数扩张）。现在反设 $\mathbb{F}$ 是无限域。因此，命题2.8 陈述的第二部分适用，从而可写为 $\mathbb{F} = \cup_{i=1}^{\infty} GF(p^{l_i})$，其中 l_i整除 l_{i+1}每个正整数 i。因此，存在一个大于 1 的整数序列，记为（c_i）$_{i\geq 1}$，使得 $l_{i+1} = l_i \cdot c_i$ 且（l_i）$_{i\geq 1}$ 是一个严格递增的正整数无限序列。

取 g_1 为 $GF(p^{l_1})$ 的乘法群的生成元，并令

$$\lambda_1 = g_1^{[\frac{p^{l_1}-1}{n}]}, \lambda_2 = g_1^{2\cdot[\frac{p^{l_1}-1}{n}]}, \ldots, \lambda_n = g_1^{n\cdot[\frac{p^{l_1}-1}{n}]}.$$

因此，引理 2.11 使我们能够得到一个正整数 $t > 1$满足

$$\lambda_1^{t-1} = \lambda_2^{t-1} = \cdots = \lambda_n^{t-1} = 1.$$

设 C 为特征值为 λ_1、λ_2、……、λ_n 的伴随矩阵。注意，上述整数 t 具有如下性质： $C = P + N$，其中 $P^t = P$、 $N^2 = 0$ 和 $PN = NP$。如果最终存在多个这样的 C 分解，那么我们可以取 t 为这些整数 t 中的最小值。因此， t 可以选为一个具有上述性质且唯一确定的固定整数。

此外，由于我们是在 $GF(p^{l_1})$ 中工作，注记 2.14 使我们得出 e 关系

$$\{g_1^{[\frac{p^{l_1}-1}{n}]}, g_1^{2\cdot[\frac{p^{l_1}-1}{n}]}, \ldots, g_1^{n\cdot[\frac{p^{l_1}-1}{n}]}\} \subseteq \{g_1^{\frac{p^{l_1}-1}{d_1}}, g_1^{2\frac{p^{l_1}-1}{d_1}}, \ldots, g_1^{d_1\frac{p^{l_1}-1}{d_1}}\},$$

其中 $d_i = gcd(p^{l_i} - 1, t - 1)$。取 $j_i \in \{1, 2, \ldots, d_i\}$ 使得

$$g_1^{[\frac{p^{l_1}-1}{n}]} = g_1^{j_1\cdot\frac{p^{l_1}-1}{d_1}},$$

又由于 g_1 在 $GF(p^{l_1})$ 的乘法群中的阶为 $p^{l_1} - 1$，因此可得

$$[\frac{p^{l_1}-1}{n}] = j_1 \cdot \frac{p^{l_1}-1}{d_1}.$$

类似地，我们得到

$$[\frac{p^{l_1}-1}{n}] = j_i \cdot \frac{p^{l_i}-1}{d_i},$$

对任意正整数 i 均成立。因此，

$$j_i \cdot \frac{p^{l_i}-1}{d_i} = j_{i+1} \cdot \frac{p^{l_{i+1}}-1}{d_{i+1},}$$

因此

$$\frac{j_i}{j_{i+1}} = \frac{d_i}{d_{i+1}} \cdot \frac{(p^{l_i})^{c_i}-1}{p^{l_i}-1}.$$

取 $s_i = (p^{l_i})^{c_i-1} + (p^{l_i})^{c_i-2} + \cdots + p^{l_i} + 1.$。由此可得

$$\frac{j_i}{j_{i+1}} = \frac{gcd(p^{l_i}-1, t-1)}{gcd((p^{l_i})^{c_i}-1, t-1)} \cdot s_i.$$

此外，由引理 2.13 可知，存在一个严格正整数 k_i 使得

$$gcd((p^{l_i})^{c_i} - 1, t - 1) = \frac{gcd(p^{l_i}-1, t-1) \cdot gcd(s_i, t-1))}{k_i}.$$

现在，我们得到

$$\frac{j_i}{j_{i+1}} = k_i \cdot \frac{s_i}{gcd(s_i, t-1)}.$$

然而，由于 $gcd(s_i, t-1)$ 整除 s_i，可知对每个正整数 $i \geq 1$，j_{i+1} 都整除 j_i。但 $j_i \geq 1$，因此存在 $i_0 \geq 1$，使得对每个 $i \geq i_0$，都有 $j_i = j_{i+1}$。于是，我们得到

$$k_i \cdot \frac{s_i}{gcd(s_i, t-1)} = 1,$$

这迫使 $s_i = gcd(s_i, t-1)$。因此，s_i 整除 $t-1$，所以 $s_i \leq t-1$。但是 $p^{l_i} < s_i$，于是 $p^{l_i} < t-1$，对每个 $i \geq i_0$ 都成立，这与以下事实形成鲜明矛盾：$(l_i)_{i \geq 1}$ 是一个严格递增的正整数无限序列。总之，$\mathbb{F}$ 是有限的，正如所声称的那样。接下来，我们再次应用定理 2.10，得到该域的阶大于 n，如前所述。□

秉承上一个结果的精神，我们提出以下猜想。

猜想：给定 $n \geq 1$ 是一个整数，$\mathbb{F}$ 是一个域。那么，$\mathbb{F}$ 上的所有伴随 $n \times n$ 矩阵都可以表示为一个幂等矩阵与一个平方零矩阵之和，且这两个矩阵彼此可交换，当且仅当 $\mathbb{F}$ 是一个有限（因而也是幂等）域且 $n = 1$。

另一方面，关于 [1] 和 [6], ，我们以如下一个颇有意思的问题作为本文的结尾。

问题 2.17. 设 D 是一个除环，$n \geq 1$ 是一个整数。那么，矩阵环 $M_n(D)$ 是弱周期的，当且仅当 D 是一个有限（因而也是幂等）域吗?

资助：Peter V. Danchev 的科研工作部分得到了保加利亚国家科学基金 KP-06 号 32/1 项目（2019年12月7日）的资助，以及安达卢西亚自治区 Junta de Andalucía 的 FQM 264 项目的资助。

References

[1] S. Breaz、G. Calugareanu、P. Danchev 和 T. Micu, *Nil-clean matrix rings*, 《线性代数及其应用》439(10) (2013), 3115–3119。[2] S. Breaz 和 G.C. Modoi, *Nil-clean companion matrices*, 《线性代数及其应用》489(2) (2016年), 50–60。[3] J. Cui 和 P. Danchev, *Some new characterizations of periodic rings*, 《代数与应用杂志》19(12) (2020)。[4] P. Danchev、E. Garc´ıa 和 M. G. Lozano, *Decompositions of matrices into diagonalizable and square-zero matrices* **71** 3 2023 , 《线性与多重线性代数》( ) ( )。[5] A.J. Diesl, *Nil-clean rings*, 《代数杂志》383(11) (2013), 197–211。[6] M.T. Kosan、T.-K. Lee 和 Y. Zhou, *When is every matrix over a division ring a sum of an idempotent and a nilpotent?* **450** 11 2014 7 12 , 《线性代数及其应用》( ) ( ), –。[7] Y. Ye, *Semi-clean rings*, 《代数通讯》31(11) (2003), 5609–5625。

Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, "Acad. G. Bonchev" str., bl. 8, 1113 Sofia, Bulgaria*Email address*: danchev@math.bas.bg; pvdanchev@yahoo.com

The Technical University of Cluj-Napoca, Departament of Mathematics, Str. Memorandumului 28, 400114, Cluj-Napoca, Romania*Email address*: andradapojar@gmail.com