

49(3)

# 有限域上互反本原正规元的存在性

田甜, 戚文峰

郑州信息工程大学应用数学系

收稿日期 2004-10-26 修回日期 2005-3-23 网络版发布日期 接受日期

摘要 设 $q$ 是素数方幂,  $n$ 是正整数,

$\text{trm}\{\mathbf{F}\}_{q^n}$ 是 $q^n$ 个元素的有限域. 本文证明了:

当正整数 $n \geq 3$ 时, 对任意的素数方幂 $q$ ,

存在 $\text{trm}\{\mathbf{F}\}_{q^n}$ 中的本原元 $\xi$ 满足 $\xi$ 和 $\xi^{-1}$ 都是 $\text{trm}\{\mathbf{F}\}_{q^n}$ 在 $\text{trm}\{\mathbf{F}\}_q$ 上的正规元,

也即 $\{\xi, \xi^{-1}, \dots, \xi^{q^{n-1}}\}$ 和 $\{\xi^{-1}, \xi^{-q}, \dots, \xi^{-q^{n-1}}\}$ 都构成 $\text{trm}\{\mathbf{F}\}_{q^n}$

在 $\text{trm}\{\mathbf{F}\}_q$ 上的本原正规基.

关键词 [有限域, 本原元, 正规基, 正规元](#)

分类号

## Primitive Normal Element and Its Inverse in Finite Fields

Tian TIAN, Wen Feng QI

(Department of Applied Mathematics, Zhengzhou Information Engineering University, P.O. Box 1001-745, Zhengzhou, 450002, People's Republic of China)

**Abstract** Let  $q$  be a prime power,  $n$  be a positive integer,  $\text{trm}\{\mathbf{F}\}_{q^n}$  denote a finite field with  $q^n$  elements. We prove that if  $n \geq 3$ , then there exists a primitive element  $\xi$  of  $\text{trm}\{\mathbf{F}\}_{q^n}$  satisfying that  $\xi$  and  $\xi^{-1}$  are normal elements of  $\text{trm}\{\mathbf{F}\}_{q^n}$  over  $\text{trm}\{\mathbf{F}\}_q$ , i.e., both  $\{\xi, \xi^q, \dots, \xi^{q^{n-1}}\}$  and  $\{\xi^{-1}, \xi^{-q}, \dots, \xi^{-q^{n-1}}\}$  are primitive normal bases over  $\text{trm}\{\mathbf{F}\}_q$ .

**Key words** [finite fields](#) [primitive element](#) [normal basis](#) [normal element](#)

DOI:

通讯作者 戚文峰 [wenfeng.qi@263.net](mailto:wenfeng.qi@263.net)

### 扩展功能

#### 本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(0KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [参考文献](#)

#### 服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [复制索引](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

#### 相关信息

- ▶ [本刊中 包含“有限域, 本原元, 正规基, 正规元”的 相关文章](#)
- ▶ 本文作者相关文章

- [田甜](#)
- [戚文峰](#)