中南大學
CENTRAL SOUTH UNIVERSITY

本科生毕业论文

题目：基于有理变换的一些不可约多项式的构造

姓　　名：彭奇

学　　号：8201210220

院　　系：数学与统计学院

专　　业：信息与计算科学

研究方向：代数学

导　　师：胡志

二〇二五 年 六 月

版权声明

摘要

不可约多项式在代数学与密码学中有诸多应用，其构造理论与生成算法的研究始终是数论与代数学的前沿课题。本文将从有理变换的视角，探讨不可约多项式生成的理论框架及其在有限域上的一种实现方法。

自 Cohen 提出有理变换构造不可约多项式的条件以来，多项式不可约性的研究取得了重要进展。Varshamov 在此基础上提出了一种具体的多项式构造方法，本文针对该构造定理的证明条件进行了补充与完善。进一步地，针对 Cohen 和 Meyn 提出的由 $Q = \frac{1}{2}\left(x + \frac{1}{x}\right)$ 定义的 Q 变换，我们补充了原证明中未提及的必要条件，结合已有理论，完整给出了该变换下多项式不可约性的充分必要条件。此外，基于分圆类理论及粟景昱的相关研究，我们对有限域 F_q 上特定形式的一次多项式个数进行了重新梳理与计算。

为验证理论结果的正确性与实用性，本文通过编程实现了上述两种构造方法的输入设定，并进行了数值实验与结果检验。实验数据表明，理论推导与计算结果具有良好的一致性，进一步验证了所提条件的完备性。本研究为不可约多项式的构造提供了更完善的理论支持，同时为相关计算提供了可行的实现方案。

关键词：有限域；不可约多项式；有理变换；群作用

Construction of Some Irreducible Polynomials Based on Rational Transformations

ABSTRACT

Irreducible polynomials have numerous applications in algebra and cryptography, and the study of their construction theory and generation algorithms remains a cutting-edge topic in number theory and algebra. This paper explores the theoretical framework for generating irreducible polynomials from the perspective of rational transformations and presents an implementation method over finite fields.

Since Cohen proposed the conditions for constructing irreducible polynomials via rational transformations, significant progress has been made in the study of polynomial irreducibility. Building upon this, Varshamov introduced a specific polynomial construction method. In this paper, we supplement and refine the proof conditions for this construction theorem. Furthermore, regarding the Q-transformation defined by $Q = \frac{1}{2}\left(x + \frac{1}{x}\right)$ as proposed by Cohen and Meyn, we supplement the necessary conditions omitted in the original proof. By integrating existing theories, we provide a complete proof of the necessary and sufficient conditions for polynomial irreducibility under this transformation. Additionally, based on cyclotomic class theory and related research by Jingyu Su, we systematically reorganize and compute the number of certain linear polynomials over the finite field F_q.

To validate the correctness and practicality of the theoretical results, we implemented the input settings for the aforementioned construction methods through programming and conducted numerical experiments and result verification. The experimental data demonstrate strong consistency between theoretical derivations and computational results, further confirming the completeness of the proposed conditions. This study provides more robust theoretical support for the construction of irreducible polynomials and offers a feasible computational implementation for related applications.

KEY WORDS: Finite field;Irreducible polynomial;Rational transformation;Group action

目录

表格索引

主要符号对照表

$\varphi(x)$	欧拉函数
$\mu(n)$	Möbius 函数
$f^*(x)$	自反多项式
F_q	有限域
$\|\cdot\|$	表示集合的基数（元素个数）
I_k	次数为 k 的齐次多项式的集合
x, y, m, n, t	标量，通常为变量
K, L, D, M, N, T	标量，通常为超参数
$x \in \mathbb{R}^D$	D 维列向量
$(x_1, \cdots, x_D)$	D 维行向量
$(x_1, \cdots, x_D)^T$ or $(x_1; \cdots; x_D)^T$	D 维行向量
$\boldsymbol{A} \in \mathbb{R}^{K \times D}$	大小为 $K \times D$ 的矩阵
$x \in \mathbb{R}^{KD}$	(KD) 维的向量
$\mathbb{M}_i$ or $\mathbb{M}_i(\boldsymbol{x})$	第 i 列为 $\mathbf{1}$(或者 $\boldsymbol{x}$)，其余为 $\mathbf{0}$ 的矩阵
$diag(\boldsymbol{x})$	对角矩阵，其对角元素为 $\boldsymbol{x}$
$\boldsymbol{I}_N$ or $\boldsymbol{I}$	$(N \times N)$ 的单位阵
$diag(\boldsymbol{A})$	列向量，其元素为 $\boldsymbol{A}$ 的对角元素
$\boldsymbol{A} \in \mathbb{R}^{D_1 \times D_2 \times \cdots \times D_K}$	大小为 $D_1 \times D_2 \times \cdots \times D_K$ 的张量
$\{x^{(n)}\}_{n=1}^N$	集合
$\{(x^{(n)}, y^{(n)})\}_{n=1}^N$	数据集
$\mathcal{N}(\boldsymbol{x}; \mu, \sum)$	变量 x 服从均值为 μ，方差为 $\sum$ 的高斯分布

① 本符号对照表内容适用于本文，如遇符号问题可在此查询。

第一章　引论

不可约多项式在代数学与密码学中有诸多应用，其构造理论与生成算法的研究始终是数论与代数学的前沿课题。本文将从有理变换的视角，探讨不可约多项式生成的理论框架及其在有限域上的一种实现方法。

有理变换的数学本质体现为变量替换，例如：

$$x \mapsto \frac{ax+b}{cx+d},$$

其中 a、b、c、d $\in F_q$, 且要求 $ad-bc \neq 0$ 以满足变换的可逆性。通过对已知的不可约多项式，显然采用特别的有理变换，得到的多项式可以继其不可约性质。

我们首先确定一个这样的变换模板：令 $g, h \in F_q[x]$, 且 $g(x), h(x)$ 互素，$g(x) \neq 0$。在多项式环 $F_q[x]$ 上，不可约多项式 $f(x)$ 经有理变换确立多项式：

$$P(x) = g(x)^n f\left(\frac{h(x)}{g(x)}\right).$$

对于该多项式在 F_q 上不可约性的讨论，Cohen 在 1969 年的论文[7] 中给出了不可约的充要性结果的证明（详细定理见第三章）。

而在 Cohen 后, 众多学者构造出了各种满足继承规则的 $f(x), g(x)$，极大丰富了构造的方法，其中 Meyn 从自反多项式的角度出发[9], 构造如下 Q-变换：

$$Q : x \mapsto \frac{x+x^{-1}}{2},$$

并讨论了不可约性质的继承条件。根据该方法迭代生成 $Q-$ 多项式，而该构造也是本文设计不可约多项式的基础。

同时我们也注意到映射：

$$\varphi : f(x) \mapsto \lambda g(x)^n f\left(\frac{h(x)}{g(x)}\right),$$

这种映射（有理变换）对乘法构成了一个同构于 PGL_2 群。对该群的讨论了有助于我们得到 PGL_2 群中元素作用在 n 次首一不可约多项式上生成的不变不可约多项式的数量。Lucas 给出了群 PGL_2 中元素作用下的不变不可约多项式的个数的具体计数方法。[13]

因此我们可以利用不同角度的优点来简化操作，比如利用群作用（如 PGL_2 群的共轭作用）进行轨道分类，方便归纳和计数：比如构造方面，设计特定变换（如 Q-变换）迭代生成不可约多项式，加快生成效率。

近期研究里，栗景昱等学者完成了 Q-变换在低次（一次、二次）下的特性[17]，但

在高次多项式生成及奇数阶 F_q 上的计数问题仍存在理论性缺口。本文深度学习有关的 $Q-$ 变换的构造计数。对于 Meyn 提供的构造，其仅给构造定理的充分性证明，本文将补充必要性的证明，并完整给出了充分必要证明的过程。同时根据 Lucas 的不变不可约多项式的构造研究[13] 对计数方面进行计算。

本论文共分为四个部分：

第二章: 介绍前置知识（包含域论等基础），详细阐述分圆类等概念，PGL_2 群以及部分域论知识；

第三章: 梳理了该问题的历史讨论和已有成果，总结 Cohen、Meyn 和 Lucas 等人的工作，以及粟景昱文章的部分重要成果；

第四章: 对于两种构造方法，第一种给出了充要条件的证明；第二种利用 Q-变换构造不可约多项式，补充了不可约性质的继承的必要证明，并简单计算了 Q-变换构造一次多项式的计数；

第五章： 完成了实验例证，并在附录中补充了相应的代码设计。

第二章　前置知识

在进行多项式构造前，我们需要对基础知识进行回顾与学习。如多项式的所在域要求的基础代数学知识（**见第一节**）；

为对构造的自反多项式进行对称性分类，在此基础下要求的分圆类概念（**见第二节**）；

我们已知这样的有理变换同构于射影群 $PGL_2(\mathbb{F}_q)$，所以我们还需要对这个群进行分析与讨论（**见第三节**）；

通过有理变换构造多项式后，每一次数生成的数目提到的基础公式（**见第四节**）；

最后在**第五节**介绍了密码学上有限域不可约多项式的应用背景。

2.1　有限域及其扩张

定义 2.1.1 (有限域（Galois 域）） 包含有限元素的域，且其中元素运算满足特定性质（如交换律、结合律、分配律等）。其元素个数必是某个素数的幂，即 $q = p^n$，记作 $\mathbb{F}_q$。

定义 2.1.2 (扩域) 若域 K 包含域 F 为子域，则称 K 为 F 的**扩域**（或**域扩张**），记作 K/F。其中 F 称为基域，K 可视为 F 上的线性空间。

命题 2.1.3 (扩域构造方法) 域扩张的两种基本构造方法如下：

1. **添加元素生成扩域**：添加一个元素 α，生成最小扩域 $F(\alpha)$。

根据添加元的性质，分为代数扩张与超越扩张。

2. **利用商环构造扩域**：若 $p(x) \in F[x]$ 在 F 上不可约，则商环 $F[x]/(p(x))$ 构成域扩张，其中：

- 自然同态 $\pi : F[x] \to F[x]/(p(x))$ 将常数项映射为自身
- 元素 $\overline{x} = x + (p(x))$ 是多项式 $p(x)$ 在该扩域中的根[1]

定义 2.1.4 (分裂域) 设 $f(x)$ 为域 F 上的多项式，若存在扩域 E/F 满足：

1.（完全分解）$f(x)$ 在 $E[x]$ 中可分解为一次因式的乘积，即

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \quad (a \in F,\ \alpha_i \in E).$$

2.（最小性）E 是包含所有根 $\alpha_1, \alpha_2, \ldots, \alpha_n$ 的最小扩域，即

$$E = F(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

则称 E 为 $f(x)$ 在 F 上的分裂域（*splitting field*）。

2.2 分圆类及分圆数

分圆类 (cyclotomic classes) 是通过乘法群的子群及其陪集划分的等价类，对元素进行了对称性划分。[2]

定义 2.2.1 (分圆类) 设有限域 $\mathbb{GF}(q)$ 满足 $q = ef+1$，[①] 其中 q 为奇素数的幂，$e, f \in \mathbb{Z}^+$，$\mathbb{GF}(q)^*$ 表示域的乘法群（阶为 $q-1$）构造步骤如下：

1. 取 $\mathbb{GF}(q)$ 的本原元 ω，令 $\epsilon = \omega^e$，则

$$H_e = \langle \epsilon \rangle = \left\{1, \epsilon, \epsilon^2, \ldots, \epsilon^{f-1}\right\}$$

为 $\mathbb{GF}(q)^*$ 的 f 阶循环子群。

2. 将 $\mathbb{GF}(q)^*$ 划分为 e 个陪集：

$$C_a^{(e,q)} = \omega^a \langle \epsilon \rangle = \left\{\omega^a \cdot \epsilon^k \mid 0 \le k < f\right\} \quad (0 \le a < e).$$

每个陪集 $C_a^{(e,q)}$ 称为第 a 个 e **次分圆类**，包含 f 个元素。

例 2.2.1 取 $q = 7$（满足 $q = 2 \cdot 3 + 1$，即 $e = 2, f = 3$），则 $\mathbb{GF}(q)^*$ 的阶为 6。计算如下：

- 本原元 $\omega = 3$（因 $\langle 3 \rangle = \{1, 2, 3, 4, 5, 6\}$）
- 子群 $H_2 = \langle 3^2 \rangle = \langle 2 \rangle = \{1, 2, 4\}$
- 分圆类：

$$C_0^{(2,7)} = H_2 = \{1, 2, 4\}, \quad C_1^{(2,7)} = 3H_2 = \{3, 6, 5\}.$$

例子得证。同时我们引申出分圆数的概念：

定义 2.2.2 (分圆数) 设有限域 $\mathbb{GF}(q)$ 满足 $q = ef + 1$，其分圆类为 $C_a^{(e,q)} = \omega^a H_e$（$0 \le a < e$）。定义分圆数 $N(i,j)^{(e,q)}$ 为方程 $x - y = 1$ 的解数，其中：$x \in C_i^{(e,q)}$，$y \in C_j^{(e,q)}$ 该值可通过集合运算表示为：

$$N(i,j)^{(e,q)} = \left| \left(C_i^{(e,q)} + 1 \right) \cap C_j^{(e,q)} \right|,$$

其中：$C_i^{(e,q)} + 1 := \{x + 1 \mid x \in C_i^{(e,q)}\}$ 表示分圆类中每个元素加 *1* 后的集合。[3]

例 2.2.2 取 $q \equiv 1 (mod 4)$，应用计算工具，我们得到：

$$N(0,0)^{(2,q)} = \frac{q-5}{4}.$$

① 注意隐式表达：q ≡1(mod e)

② 当 $e = 2$ 时，分圆类对应二次剩余（$C_0^{(2,q)}$）与二次非剩余（$C_1^{(2,q)}$）。

2.3　有限域上的特殊群

首先介绍一些常用到的群：

定义 2.3.1 ($\mathbf{GL}_2(\mathbb{F}_q)$ 群) 二阶一般线性群，由所有可逆的 2×2 矩阵构成。

定义 2.3.2 ($\mathbf{PGL}_2(\mathbb{F}_q)$ 群) 二阶一般射影线性群，定义为一般线性群 $GL_2(\mathbb{F}_q)$ 模去其中心（标量矩阵 λI，其中 $\lambda \in \mathbb{F}_q^*$）的商群：$\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{GL}_2(\mathbb{F}_q)/\lambda I$,

对于 $A \in \mathrm{GL}_2(\mathbb{F}_q)$，我们记 $[A]$ 为 A 在商群 $\mathrm{PGL}_2(\mathbb{F}_q)$ 的等价类,i.e.:

$$[A] = \{B \in \mathrm{GL}_2(\mathbb{F}_q) \mid B = \lambda \cdot A, \lambda \in \mathbb{F}_q^*\}.$$

定义 2.3.3 (共轭关系) 设 $A, B, P \in GL_2(\mathbb{F}_q)$，使得 $[B] = [P \cdot A \cdot P^{-1}]$，则 $[A]$ 和 $[B]$ 共轭。

命题 2.3.4 共轭的元素在群作用下表现一致。

因此，我们可通过将元素化为共轭的标准型，以简化计数问题。给出 $\mathrm{PGL}_2(\mathbb{F}_q)$ 群共轭划分 (见表格 3.1)：

表 2.1　$\mathrm{PGL}_2(\mathbb{F}_q)$ 中元素的共轭分类

类型	特征值位置与性质	标准形式	阶数	共轭类代表
类型 1	$\mathbb{F}_q$ 中不同特征值	$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$	整除 $q-1$	$[A(a)]$，$a \in \mathbb{F}_q^* \setminus \{1\}$
类型 2	$\mathbb{F}_q$ 中相同特征值	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	p	$[\mathscr{E}]$
类型 3	$\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ 中互为相反数	$\begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$	2	$[C(b)]$，b 非平方 ①
类型 4	$\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ 中非相反数	$\begin{pmatrix} 0 & 1 \\ c & 1 \end{pmatrix}$	整除 $q+1$	$[D(c)]$，$x^2 - x - c$ 不可约 ②

① “非平方”指 $b \in \mathbb{F}_q^*$ 不是平方数。
② “不可约”指多项式 $x^2 - x - c$ 在 $\mathbb{F}_q$ 上不可约。

接下来，我们探讨一些关于群作用的知识，这在后续分类上作用极大。而可迁性的证明也为不可约多项式的构造提供理论支撑。

定义 2.3.5 (群作用) 群 G 在集合 X 上的作用是一个映射 $G \times X \to X$，满足：

- **单位元作用**：对所有 $x \in X$，有 $e \cdot x = x$（其中 e 是 G 的单位元）。
- **结合律**：对所有 $g, h \in G$ 和 $x \in X$，有 $g \cdot (h \cdot x) = (gh) \cdot x$。

定义 2.3.6 (群作用轨道) 对于 $x \in X$，其轨道 $G \cdot x$ 定义为所有 $g \cdot x$（其中 $g \in G$）的集合，即 $G \cdot x = \{g \cdot x \mid g \in G\}$。集合 X 被划分为互不相交的轨道，每个轨道是 X 的一个等价类。

定义 2.3.7 (轨道可迁性) 若群 G 在 X 上的作用只有一个轨道（即 X 本身），则称该作用是 **可迁的**。即对任意 $x, y \in X$，存在 $g \in G$ 使得 $g \cdot x = y$。

而如何求作用群下的具体的轨道数量，我们可以通过 *Burnside* 引理得到。

引理 1 (*Burnside* 引理) 设有限群 G 作用在有限集合 X 上，轨道数为 N，则：

$$N = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|,$$

其中：$|G|$ 是群 G 的阶（元素个数）。$\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$ 是 g 的不动点集。

例 2.3.1 用 *2* 种颜色（红、蓝）给正方形的 *4* 条边着色，考虑旋转对称性（即旋转 *0°*、*90°*、*180°*、*270°* 的群 G），有多少种本质不同的着色方案？

解答： 首先得到群 G 的阶为 4。然后计算每个群元素的不动点数：旋转 0°：所有 $2^4 = 16$ 种着色方案都不动；旋转 90°：所有边颜色相同，此时有 2 种（全红或全蓝）；旋转 180°：对边颜色相同，此时有 $2^2 = 4$ 种；旋转 270°：同 90°，有 2 种。最后应用 Burnside 引理得到结果：

$$N = \frac{1}{4}(16 + 2 + 4 + 2) = 6.$$

2.4 不可约多项式的存在性与计数讨论

首先给出一些重要的概念，这在后续计算中需要频繁用到：

定义 2.4.1 (欧拉函数 (Euler's totient function)) 欧拉函数 $\varphi(n)$ 定义为：

$$\varphi(n) := \Big|\{k \in [n] \mid \gcd(k, n) = 1\}\Big|,$$

即对于正整数 n，区间 $[1, n]$ 内与 n 互质的正整数个数。

定义 2.4.2 (Möbius 函数（Möbius Function）) *Möbius* 函数 $\mu : \mathbb{N}^+ \to \{-1, 0, 1\}$ 定义为：

$$\mu(n) := \begin{cases} 1 & \text{当} n = 1, \\ (-1)^k & \text{若} n \text{ 无平方因子，且} n = p_1 p_2 \cdots p_k \text{ (其中} p_i \text{ 为不同素数)}, \\ 0 & \text{若} n \text{ 存在大于 } 1 \text{ 的平方因子（即} \exists d > 1,\ d^2 \mid n\text{）}. \end{cases}$$

定义 2.4.3 (自反多项式) 设 $P(x)$ 为域 $\mathbb{F}$ 上一个 n 次多项式，若满足条件：

$$P(x) = x^n P\left(\frac{1}{x}\right) \implies a_k = a_{n-k}, \quad \forall k = 0, 1, \ldots, n$$

则称 $P(x)$ 为**自反多项式**，记为 $P^*(x)$。

命题 2.4.4 令 $[A] \in PGL_2(\mathbb{F}_q)$，$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$，$f(x) \in I_n$，定义

$$[A] \circ f = \lambda(bx + d)^n f\left(\frac{ax + c}{bx + d}\right),$$

其中 λ 是 $\mathbb{F}_q$ 中使得多项式 $[A] \circ f$ 首项系数为 1 的唯一元素。这样，$[A]$ 定义了集合 I_n 上的一个一一变换，称之为由 $[A]$ 确定的集合 I_n 的**有理变换**。[4]

命题 2.4.5 全体这样的有理变换对变换的乘法做成的群同构于 2 阶射影一般线性群 $PGL_2(\mathbb{F}_q)$。

自然地，

$$\mathrm{PGL}_2(\mathbb{F}_q) \times I_n \to I_n, \quad ([A], f) \mapsto [A] \circ f.$$

定义了群 $\mathrm{PGL}_2(\mathbb{F}_q)$ 在集合 I_n 上的一个作用。

2.5　有限域在密码学上的应用

当今的加密体制分为对称密码和公钥密码。对称密码有根据加密方式的不同分为分组密码（block cipher）和流密码（steam cipher）。[5]

对于分组密码，早期研究围绕数据加密标准（Data Encryption Standard，DES）展开，但随着研究的推进，国际数据加密算法（International Data Encryption Algorithm，IDEA）逐渐取代。而千禧年时高级加密标准（Advanced Encryption Standard，AES）的出现引起了新的高潮。在经典的分组密码的算法中，恰恰通过对有限域上的运算来实现的。

对于流密码，也叫做序列密码。业界普遍采用线性反馈移位寄存器 (linear feedback shift register, LFSR) 的设备产生同步密钥流生成器。而实验结果表明对于一个 LFSR 为最长移位寄存器的必要条件是其联接多项式为不可约多项式。而为了保证输出非零序列是 m 序列则要求作用于 GL_2 上。因此，对于一个 n 级 LFSR 为最长移位寄存器的充要条件是它的联接多项式为 GL_2 上的 n 次本原多项式。而当 $2^n - 1$ 为素数时，满足 GL_2 上的 n 次不可约多项式均为本原多项式。

如何巧妙构造出一些次数较大的不可约多项式是密码学中在不断探讨的课题。研究学者们想出如固定某些项系数来简化操作，以及尽可能减少项数的方式来寻找本原或不可约多项式。

为了保证流密码的安全性，通过产生和随机序列相类似的伪随机序列来确保。人们发现 LFSR 的缺陷，通过加入非线性化方式来生成密匙。而通过了解生成器的结构特征，和输入输出的限制，我们发现本质即是在有限域上构造不可约多项式。

第三章　已有研究

多项式可约性问题即讨论多项式在特定数域下能否分解为该域上不可再约的” 最小单元”（即不可约多项式）。这个问题贯穿了代数学的历史发展脉络：从古希腊时期丢番图方程根的存在性探讨，到 19 世纪群论对代数方程根式解的结构性阐释，直至现代密码学中基于不可约多项式构建的抗量子加密体系，在数学的各个分支中都体现着重要的作用。

Gauss 在 1799 年他的博士论文中就如是陈述: 任何一个一元复系数方程，都有至少一个复数根。数学史上后来称作 “**代数基本定理**”，从多项式的角度，揭示了在复数域这一代数闭包上，所有多项式都是 “完全可约” 的。这个代数基本定理的雏形也为后续域论的发展奠定了基石，不可约多项式与代数域扩张密切相关。[6]

对于方程根式问题的研究中，自 Galois 与 Abel 等人创造群论这样的有力的工具后出现了极大进展。通过构造与多项式根对应的伽罗瓦群，Galois 证明了五次及以上方程无根式解的深层原因——当伽罗瓦群不可解时，对应的多项式在有理数域 Q 上不可约且无法通过有限次根式扩张获得全部根。这种将代数结构转化为群论性质的研究范式，意义深远。

可约的概念深入数学的各个分支。比如数论领域中素数与合数的概念：可以被 1 和其自身以外的正整数整除来判定；比如环论中，一个元素称为可约，指它落在某个主理想中，且不能生成该理想；比如拓扑学中，不连通集等概念。包括在代数几何里，代数簇如果可约，则它为一些代数簇的并集。

而可约的意义本身也受所在数域的影响。德国数学家 Eisenstein 就给出了一个判别方法（现被称为 Eisenstein 判别法），该方法给出了多项式可约的判别条件，但该方法仅局限于判断有理数域上整系数多项式的可约性质。

近年来可约性多项式的重要研究方向便是其构造方法，一个自然的思路就是通过已有的不可约多项式生成新的多项式。其中通过有理变换方法来生成也成了探索的手段。而对于生成前后多项式不可约性质的继承问题，也随着具体有理变换方法的不同而不断讨论。且由此衍生的通过计算机连续迭代构造生成不可约多项式，在密码学等领域也有着重要的应用。

3.1　Cohen 的证明

Cohen 主要研究了 n 有限域 GF_2 上三种不可约多项式：

(I) r 多项式：$P(x^r)$, 其中 r 为正整数。

(II) 自反多项式：形如 $x^m P(x+x^{-1})$, 满足

$$Q(x) = x^{2m} + a_{2m-1}x^{2m-1} + \ldots + a_1 x + 1, \quad a_{m-i} = a_{m+i} \quad (i \leq m-1)$$

(III) r 自反多项式：形如 $x^r m P(x+x^{-1})$, 记作 $Q(x^r)$, 其中 $Q(x)$ 同样满足上述规则。

Cohen 在文中[7] 给出了这三种多项式的不可约条件和数量公式。并证明了这样一条关键引理，这给出了有理变换后 $P(x)$ 可约性的继承的充分必要条件:

引理 2 *若 $f(x), g(x) \in GF[q,x]$, 则 $g^n(x)P(\frac{f(x)}{g(x)})$ 不可约当且仅当 $f(x)-\lambda g(x)$ 在 $GF[q^n,x]$ 上不可约，而 $P(\lambda)=0$。*

显然，当存在 $f(x)$ 的根 $\lambda \in F_{q^n}$，使得 $h(x)-\lambda g(x)$ 在 F_{q^n} 不可约时，则有理多项式同样不可约。沿着有理变换的方法，许多学者讨论了不同的构造情况并予以证明。如 Varshamov 讨论了[8]

$$h(x) = x^2 - x - 1, \quad f(x) = 1$$

的情形; Meyn 讨论了[9]

$$h(x) = x^2 + 1, \quad f(x) = x$$

的情形; Menezes 给出了[10]

$$h(x) = x^2, \quad f(x) = 1$$

时 $P(x)$ 在 $\mathbb{F}_q$ 上不可约的充分必要条件；Kyureghyan 给出了 q 为奇数,[11]

$$h(x) = x^2 + ax + b, f(x) = x^2 + cx + d, a, c \neq 0, a^2 = 4bd$$

时, 在特殊情况下 $P(x)$ 在 $\mathbb{F}_q$ 上不可约的一个充分条件; Sergey Abrahamyan 等人讨论了[12] 特征为 q 的有限域上，

$$h(x) = x^2 - ax + b, \quad f(x) = x^2 - ax + c$$

时, 某些特殊情形下多项式 $T(f(x))$ 的不可约性.

这样的例子不会停止，会随着构造的丰富链接产生更多的创新。

3.2 对于 Meyn 方法的研究

我们这里主要研究 Meyn 的工作，因为其构造较为简单。Meyn 从自互多项式入手。自互多项式（Self-Reciprocal Polynomials）是一类满足 $f(x) = x^n f(\frac{1}{x})$ 的多项式, 其系数呈现对称性。由于自互多项式只需定义一半系数，其构造可显著简化编码设计。而如

何在有限域上构造不可约的自互多项式（简称 srim，即首一不可约自互多项式）是正在研究的课题。

Helmut Meyn 的论文系统地研究了[9] 有限域上不可约自反多项式的构造方法，给出了在不同特征域下的不可约性条件，并通过迭代 Q-变换构造了无限序列的不可约自反多项式。

Meyn 的 Q-变换方法，论文提出了一种通过二次变换 $f \to f^Q$ 的构造方法，将次数为 n 的多项式 $f(x)$ 转换为次数为 $2n$ 的自互多项式。该方法的创新在于将不可约性条件从原多项式 f 传递到 f^Q，并区分了偶数阶和奇数阶有限域的情况。对于偶数阶域，条件依赖于迹函数（Trace Function）；对于奇数阶域，则需利用域中二次剩余的性质。

对此我们需要探讨不同特征情况：1）特征为 2：如果 $f(x)$ 的绝对迹 $\mathrm{Tr}(a_1/a_0) = 1$，则 $f_Q(x)$ 是不可约的；2）特征奇数：如果 $f(2)f(-2)$ 是 $\mathbb{F}_q$ 中的非平方元，则 $f_Q(x)$ 是不可约的。

Meyn 的论文里将 Varshamov 和 Garakov 准则从二元域 $\mathbb{F}_2$ 推广到一般有限域，但指出在奇数阶域中，条件提取因涉及未解决的数论问题（如二次剩余分布的复杂性）而尚未完全解决。此外，对于特征为 2 的域，构造无限 srim 序列的准则较为简单；而奇数特征域仍需进一步探索。

自互多项式可用于生成具有反向读取特性的可逆编码。该多项式可通过对任意维数为 n 的多项式 f 通过 Q 变换 $f_Q(x) = x^n f(x + \frac{1}{x})$ 得到。而变换前后的不可约性的继承而根据研究，这其实与所在域的特征数的奇偶性有关。

不可约自互多项式在编码理论中用于构造可逆码，这些码具有读取反向性质，广泛应用于数据存储和传输中。通过自互多项式，可以设计出具有高效纠错能力的编码方案

在密码学中，不可约自互多项式用于生成具有特殊性质的序列，这些序列在加密算法和伪随机数生成器中具有重要应用。自互多项式的对称性和不可约性使其成为构造安全密码系统的重要工具。

命题 3.2.1 *通过自反多项式这种特定结构，定义二次变换（Q-变换）将次数为 n 的多项式转化为次数为 $2n$ 的自反多项式。*

证明： 将 x 替换为 $\frac{1}{x}$，得到：

$$f^Q\left(\frac{1}{x}\right) = \left(\frac{1}{x}\right)^{\deg(f)} f\left(\frac{1}{x} + x\right) = x^{-\deg(f)} f\left(x + \frac{1}{x}\right).$$

两边乘以 $x^{\deg(f^Q)}$（注意 $\deg(f^Q) = 2\deg(f)$）：

$$x^{2\deg(f)} f^Q\left(\frac{1}{x}\right) = x^{\deg(f)} f\left(x + \frac{1}{x}\right) = f^Q(x).$$

引理 3 若 $f(x)$ 是 F_q 上次数 $n>1$ 的不可约多项式，则 $f_Q(x)$ 要么是次数为 $2n$ 的 *srim* 多项式，要么是次数为 n 的非自反多项式的乘积。

定理 3.2.2 (定理 1) 任意次数为 $2n$ 的最简自反多项式都是下列多项式的因式：$H_{q,n} := x^{q^n}+1$。且 $H_{q,n}(x)$ 中所有次数大于 *2* 的不可约因式都是次数为 $2d$ 的最简自反多项式 $(srim)$，其中 d 是 n 的因子，且 $n|d$ 为奇数。

定理 3.2.3 (定理 3) 令 $S_q(n)$ 表示 $\mathbb{F}_q$ 上次数为 $2n$ 的 *srim* 多项式的数量，则有：

$$S_q(n)=\begin{cases}\dfrac{1}{2n}\left(q^n-1\right) & \textit{if } q \textit{ is odd and } n=2^s,\\ \dfrac{1}{2n}\displaystyle\sum_{\substack{d|n\\ d\ odd}}\mu(d)q^{n/d} & \textit{otherwise.}\end{cases}$$

该公式与不可约多项式的经典计数公式 $N_q(n)=\frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}}$ 形式上相似。

在 Q 变换的不可约性保持条件，Meyn 分为两种情况：特征 2 和特征域。

定理 3.2.4 (定理 6（特征 2）) 若 $f(x)=x^n+\cdots+a_1x+a_0\in\mathbb{F}_{2^k}[x](k\geq 1)$ 为一个不可约多项式，则 f^Q 不可约当且仅当 $\frac{a_1}{a_0}$ 的绝对迹等于 *1*。

推论 3.2.5 如果 $f(x)=x^n+\cdots+a_1x+a_0\in F_2[x]$ 不可约，则 f^Q 不可约当且仅当 a_1 等于 *1*。*(arshamov 和 Garakov)*

定理 3.2.6 (定理 8（奇特征域）) 设 q 为奇数幂。如果 f 时 F_q 上次数为 n 的首一不可约多项式，则 f^Q 不可约当且仅当 $f(2)\cdot f(-2)$ 是 F_q 中的非平方数。

而迭代构造思路如下：

对于 $f(x)=\sum_{i=0}^n a_ix^i$ 且 $a_0\neq 0\neq a_n$，定义 Q-变换为：

$$f^Q(x) := x^n f(x+x^{-1})=\sum_{i=0}^{n}a_i(1+x^2)^ix^{n-i}.$$

其中 f 的系数可通过 Andrews 论文中的反演公式唯一得到。

至此，理论支撑完善，Meyn 给出了 F_q 上构造次数为 $2n$ 的 *srim* 多项式的步骤：

1. 生成一个次数为 n 的首一不可约多项式 f。
2. 将 f 变换为 f^Q。
3. 测试结果，如果

$$\gcd(x^{q^n-1}-1, f^Q(x))=1$$

等价于

$$x^{q^n}\equiv x(mod\, f^Q(x)).$$

否则从步骤 1 重新开始。

3.3　Lucas 的证明

有限域上的多项式研究在代数、编码理论和密码学中占据核心地位。近年来，射影线性群（如 $\mathrm{PGL}_2\left(F_q\right)$）在多项式环上的作用引起了广泛关注，尤其是其对不可约多项式结构的对称性影响。Lucas Reis 在 2019 年的工作中，[13] 系统研究了 $\mathrm{PGL}_2\left(F_q\right)$ 作用下不可约多项式的存在性与数量分布，解决了非循环子群不变量的次数限制问题，并给出了精确的计数公式。

Reis 的工作围绕以下两个核心定理展开：

定理 3.3.1 *若 G 为 $\mathrm{PGL}_2\left(F_q\right)$ 的非循环子群，则任何 G-不变量的次数必为 2。*

该定理证明思路可以通过根的置换导出矛盾。假设存在次数 $n \geq 3$ 的 $G-$ 不变量 f，其根集 S 在 G 作用下保持稳定。因 G 非循环，其在 S 上的置换群亦非循环，但 $\mathrm{PGL}_2\left(F_q\right)$ 元素与 Frobenius 自同构 σ （对应 n-循环置换）交换，导致置换群必为循环群，矛盾。

定理 3.3.2 *设 $[A] \in \mathrm{PGL}_2\left(F_q\right)$ 为阶数为 $D = \mathrm{ord}([A])$ 的元素。则对于任意整数 $n > 2$，次数为 n 的 $[A]$-不变多项式的数量 $N_A(n)$ 在 n 不被 D 整除时为零，而对于 $n = Dm$ 且 $m \in \mathbb{N}$，以下成立：*

$$N_A(Dm) = \frac{\varphi(D)}{Dm}\left(c_A + \sum_{\substack{d \mid m \\ \gcd(d,D)=1}} \mu(d)\left(q^{m/d} + \eta_A(m/d)\right)\right),$$

其中 φ 为欧拉函数，μ 为莫比乌斯函数，$\eta_A : \mathbb{N} \to \mathbb{N}$ 和 $c_A \in \mathbb{Z}$ 定义如下：

1. *$c_A = 0$ 且 $\eta_A \equiv \varepsilon$，其中 $\varepsilon = -1$ 或 0，分别对应于 A 在 F_q 中具有不同或相同的特征值；*
2. *$c_A = -1$ 且 η_A 为零函数，如果 A 在 $F_{q^2} \backslash F_q$ 中具有相反的特征值；*
3. *$c_A = 0$ 且 $\eta_A(t) = (-1)^{t+1}$，如果 A 在 $F_{q^2} \backslash F_q$ 中具有非相反的特征值。*

Stichtenoth 与 Topuzoglu[14] 及 Reis[15] 分别针对 $\mathrm{PGL}_2\left(F_q\right)$ 整体和 $p-$ 子群证明了定理 1.3 的特殊情形。Reis 的统一证明通过根置换的群论性质，避免了对具体群结构的依赖，揭示了更深层的对称性约束。

Daykin 曾尝试通过分解多项式 $(ax+b)x^{q^m} - (cx+d)$ 来计数不变量[16]，但其忽略了二次因子的影响，导致结果偏差（如 $q = 2$ 时非整系数）。Reis 通过细致分析各类型元素的 $F_{A,r}$ 因式分解，引入修正项 η_A，解决了这一问题。

粟景昱具体讨论了 $\mathrm{PGL}_2\left(F_q\right)$ 群在 I_n 时的可迁性如下[17]：

n	**可迁性情况**
$n=2$	群作用可迁
$n=3$	对任意有限域 q，群作用可迁
$n=4,5$	仅当 $q=2$ 时群作用可迁
$n>6$	对任意有限域 q，群作用不可迁

表 3.1　$\mathrm{PGL}_2(F_q)$ 在 I_n 上的可迁性

此外，粟的文章还探讨了有理变换 $Q=\frac{1}{2}(x+\frac{1}{x})$ 时的部分计数情况。并探讨了共轭条件下的轨道长度。

这些已有研究为我们的构造提供了理论性的基础。通过 Cohen 的理论，沿着相关学者提供的构造方法，我们给出继承性的证明条件，并利用代码设计迭代构造的程序。

同时，我们沿着粟景昱文章中一次和二次的多项式，重新利用分圆类完成计数，完成相关的学习。

第四章　不可约多项式的构造

4.1　第一种构造

首先给出第一种构造，这由 Varshamov 给出[18]，但并没有给出相关证明。这里我将给出一种证明方式，这里用到了另一篇文章中的一条重要引理[19] 。

引理 4 设 $P(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0$ 为 F_q 上的不可约多项式。则 $P(x^p-x-b)$ 在 F_q 上不可约当且仅当 $\mathrm{Tr}_{q|p}(nb-c_{n-1})\neq 0$。

定理 4.1.1 设 p 为质数，$f(x)=x^n+\sum_{i=0}^{n-1}c_ix^i$ 为在 $\mathbb{F}_p$ 上不可约的多项式。假设存在非零元 $a\in\mathbb{F}_p$ 满足：

$$(na+c_{n-1})f'(a)\neq 0.$$

定义映射多项式 $g(x)=x^p-x+a$，并递归构造：

$$\begin{aligned} f_0(x)&=f(g(x)),\\ f_k(x)&=f_{k-1}^*(g(x))\quad (k\geq 1), \end{aligned}$$

其中 $f^*(x)$ 表示 $f(x)$ 的自反多项式。则对任意 $k\geq 0$，多项式 $f_k(x)$ 在 $\mathbb{F}_p$ 上不可约，其次数为 np^{k+1}。

证明：根据引理 4，多项式 $f_0(x)=f(g(x))$ 不可约当且仅当 $\mathrm{Tr}_{p|p}(a+c_{n-1})=na+c_{n-1}\neq 0$。通过数学归纳法证明：对任意 $k\geq 0$，多项式 $f_k(x)$ 的 x 的系数，记作 $[x]f_k(x)$，要求非零，且 $f_k'(a)\neq 0$。首先我们考虑 f_0:

$$\begin{aligned} [x]f_0(x)&=\frac{d}{dx}f_0(x)\Big|_{x=0}=\frac{d}{dx}\Big(\sum_{i=0}^{n}c_ig^i(x)\Big)\Big|_{x=0}\\ &=\sum_{i=0}^{n}c_ig^{i-1}(x)g'(x)\Big|_{x=0}\\ &=-\sum_{i=0}^{n}c_ia^{i-1}\quad (g(0)=a,\ g'(0)=-1)\\ &=-f'(a). \end{aligned}$$

通过假设非零，类似地，我们有：

$$\begin{aligned} f_0'(a) &= \sum_{i=0}^{n} c_i g^{i-1}(a) g'(a) \\ &= -\sum_{i=0}^{n} c_i i a^{i-1} \quad (g(a) = a,\ g'(a) = -1) \\ &= -f'(a). \end{aligned}$$

设 $f_k(x)$ 为 F_p 上不可约多项式，满足：$[x]f_k(x) \neq 0, f_k'(a) \neq 0$ 成立，归纳法证明对 f_{k+1} 成立。注意到 $f_k, f_k k^*$ 次数都为 $np^{k+1} = n_k$。当 $f_k^*(x)$ 化为首一多项式，x^{n_k-1} 的系数为：$[x](f_k(x)/f_k(0)) \neq 0$ 由引理 4 可以推出 $f_{k+1}(x) = f_k^*$ 在 F_q 上不可约。我们令：

$$f_k(x) = \sum_{i=0}^{n_k} u_i x^i,$$

则有：

$$f_{k+1}(x) = \sum_{i=0}^{n_k} u_i g^{n_k-i}(x)$$

和

$$\begin{aligned} f_{k+1}'(x) &= \sum_{i=0}^{n_k} u_i (n_k - i) g^{n_k-i-1}(x) g'(x) \\ &= -\sum_{i=0}^{n_k} u_i (n_k - i) g^{n_k-i-1}(x). \end{aligned}$$

因为 $f(x)$ 为 F_p 上的常数，所以 f_k, f_k' 也为常数，因此有：

$$[x]f_{k+1}(x) = f_{k+1}'(0) = f_k'(a^{-1})a^{n_k-1} = f_k'(a)a^{n_k-1}.$$

通过归纳法可以证明非零，类似地可以得到：

$$f_{k+1}'(a) = a^{n_k-1} f_k'(a^{-1}) = a^{n_k-1} f_k'(a).$$

同样非零，则命题得证。

4.2 第二种构造

给出第二个构造, 这由 Cohen 给出[20]，Meyn 亦有提到：

定理 4.2.1 设 $f(x)$ 为 $\mathbb{F}_q$ 上的首一不可约多项式，其次数 $n \geq 1$，其中 q 为奇数且当

$q \equiv 3 \pmod 4$ 时 n 为偶数。假设 $f(1)f(-1)$ 是 $\mathbb{F}_q$ 中的非平方元。定义多项式序列：

$$\begin{aligned} f_0(x) &= f(x), \\ f_k(x) &= (2x)^{t_{k-1}} \cdot f_{k-1}\left(\frac{x+x^{-1}}{2}\right) \quad (k \geq 1), \end{aligned}$$

其中 $t_k = n \cdot 2^k$ 表示 $f_k(x)$ 的次数。则对任意 $k \geq 1$，$f_k(x)$ 均为 $\mathbb{F}_q$ 上的不可约多项式，其次数为 $n \cdot 2^k$。

证明： 首先给出充分性的证明：

$$\begin{aligned} f_k(1)f_k(-1) &= \left[2^{t_{k-1}} f_{k-1}(1)\right] \cdot \left[(-2)^{t_{k-1}} f_{k-1}(-1)\right] \\ &= (-1)^{t_{k-1}} \cdot 2^{2t_{k-1}} \cdot f_{k-1}(1)f_{k-1}(-1) \\ &= (-1)^n c^2 \left[(-1)^{t_{k-2}} \cdot 2^{2t_{k-2}} f_{k-2}(1)f_{k-2}(-1)\right] \\ &\ \ \vdots \\ &= (-1)^{n \cdot c_k^2} \cdot f_0(1)f_0(-1). \end{aligned}$$

显然，要么 -1 为 F_q 中的平方元，此时 $q \equiv 1 \pmod 4$；要么 n 为偶数, 也可以构成 $f_k(1)f_k(-1)$ 为 $\mathbb{F}_q$ 中的非平方元。

必要性结论显然（反证法）：当 $q \equiv 3 \pmod 4$，-1 并不是平方元，因此不成立。

命题 4.2.2 对于上述构造 2 的多项式序列，我们称作 $Q-$ 多项式。设 $f(x) = x - a \in F_q[x]$，证明其为 Q-多项式的充要条件并完成 F_q 上该一次多项式的计数。

证明： 粟景昱[17] 充分探讨了一次的充要条件，满足：

- $q \equiv 1 \pmod 4$
- $a^2 - 1 \notin F_q^{*2}$ （或 $a^2 - 1 \notin F_q^{*2}$）

由**定理 4.2.1**，我们知道当 $q \equiv 3 \pmod 4$，要求 n 为偶数，因此不做考虑。于是只有 $q \equiv 1 \pmod 4$ 的情况：等价条件要求了此时 $a^2 - 1$ 不是 F_q 中平方数，根据生成元，我们令 $a^2 - 1 = \alpha t$, 那么根据分圆多项式的知识，我们可以得到：

$$a^2 \in (C_1^{(2,q)} + 1) \cap C_0^{(2,q)},$$

其中：$C_1^{(2,q)} + 1 := \{x + 1 \mid x \in C_1^{(2,q)}\}$。接下来我们计算具体的分圆数，我们将 $q \equiv 1$

(mod 4) 进行参数分解得到：$q = x^2 + 4y^2$, 则二阶分圆数的表达式为

$$(0,1)^{(2,q)} = (1,0)^{(2,q)} = \frac{q-1}{4} + y = \frac{q-1}{4},$$
$$(1,1)^{(2,q)} = \frac{q-1}{4} - y = \frac{q-1}{4}.$$

则此时得到 a^2 的取法共有 $\frac{q-1}{4}$ 种，根据二次剩余的解的对称性，我们得到 a^2 的取法为 a 取法的一半。综合以上我们得到：

$$N(Q,q) = \begin{cases} \frac{q-1}{2}, & \text{如果} q \equiv 1 \pmod 4, \\ 0, & \text{如果} q \equiv 3 \pmod 4. \end{cases}$$
$$= \frac{q-1}{2}.$$

第五章　实例构造与验证

我们选择有限域 $\mathbb{F}_{19} = \{0, 1, \ldots, 18\}$。检验第二种构造并验证其不可约性。$\mathbb{F}_{19}$ 中的平方元和非平方元见附录。

步骤一：验证初始条件

1. **域条件**：$q = 19 \equiv 3 \pmod 4$ 是奇数。
2. **初始多项式条件**: 给定多项式 $f(x) = x^2 + x + 2$ 为二次首一多项式（$n = 2$），其判别式：
$$D = b^2 - 4ac = 1 - 8 = -7 \equiv 12 \pmod{19}$$
为 F_{19} 中非平方元，故在 F_{19} 上满足不可约。
3. **非平方元条件**：计算 $f(1)$ 和 $f(-1)$ 在 $\mathbb{F}_{19}$ 中的值：
$$f(1) = 1^2 + 1 + 2 \equiv 4 \pmod{19},$$
$$f(-1) = (-1)^2 + (-1) + 2 \equiv 2 \pmod{19}.$$
因此 $f(1)f(-1) = 4 \cdot 2 = 8 \pmod{19}$。8 是 F_{19} 中的非平方元，条件满足。

步骤二：构造 $f_1(x)$ 并验证，根据定理定义：
$$f_1(x) = (2x)^{t_0} f_0\left(\frac{x + x^{-1}}{2}\right),$$
其中 $t_0 = n = 2$。在 F_{19} 中计算, 我们发现：

- $(2x)^{t_0} = (2x)^2 = 4x^2 \pmod{19}$.
- $\frac{x+x^{-1}}{2} \equiv 10(x + x^{-1}) = 10x + 10x^{-1} \pmod{19}$.($\because \frac{1}{2} \equiv 10 \pmod{19}$)

令 $y = 10x + 10x^{-1}$。计算 $f_0(y) = y^2 + y + 2$：
$$\begin{aligned} f_0(y) &= (10x + 10x^{-1})^2 + (10x + 10x^{-1}) + 2 (\because 100 \equiv 5 \pmod{19}) \\ &= (5x^2 + 10 + 5x^{-2}) + (10x + 10x^{-1}) + 2 \pmod{19} \\ &= 5x^2 + 10x + (10 + 2) + 10x^{-1} + 5x^{-2} \pmod{19} \\ &= 5x^2 + 10x + 12 + 10x^{-1} + 5x^{-2} \pmod{19}. \end{aligned}$$

于是有：

$$\begin{aligned} f_1(x) &= (4x^2) \cdot f_0(y) \\ &= 4x^2(5x^2 + 10x + 12 + 10x^{-1} + 5x^{-2}) \pmod{19} \\ &= 20x^4 + 40x^3 + 48x^2 + 40x^1 + 20x^0 \pmod{19} \\ &= x^4 + 2x^3 + 10x^2 + 2x + 1 \pmod{19}. \end{aligned}$$

($\because 20 \equiv 1, 40 \equiv 2, 48 \equiv 10 \pmod{19}$)。

步骤三：验证 $f_1(x)$ 的不可约性

1. **一次因子检查**：

$$f_1(1) = 1 + 2 + 10 + 2 + 1 = 16 \not\equiv 0 \pmod{19},$$
$$f_1(-1) = f_1(18) = 1 - 2 + 10 - 2 + 1 = 8 \not\equiv 0 \pmod{19}.$$

为更系统地检查其他根，令 $u = x + x^{-1}$。则 $f_1(x)/x^2 = (x^2 + x^{-2}) + 2(x + x^{-1}) + 10 = (u^2 - 2) + 2u + 10 = u^2 + 2u + 8$。如果 $f_1(x)$ 有根 $x_0 \neq \pm 1$，那么 $u_0 = x_0 + x_0^{-1}$ 必须是 $u^2 + 2u + 8 = 0$ 的根。$u^2 + 2u + 8 = 0$ 的判别式 $D_u = 2^2 - 4(1)(8) = 4 - 32 = -28 \equiv 10 \pmod{19}$。由于 $D_u = 10$ 是 F_{19} 中的非平方元，所以 $u^2 + 2u + 8 = 0$ 在 F_{19} 中没有解。这意味着 $f_1(x)$ 没有形如 x_0, x_0^{-1} (其中 $x_0 \neq \pm 1$) 的成对根。结合 $f_1(1) \neq 0$ 和 $f_1(-1) \neq 0$，可知 $f_1(x)$ 在 F_{19} 中没有根，因此没有线性因子。

2. **二次因子分解检查**：假设 $f_1(x) = (x^2 + ax + 1)(x^2 + cx + 1)$，对比系数：

$$\begin{cases} a + c = 2, \\ ac + 2 = 10, \end{cases}$$

将 $c = 2 - a$ 代入 $ac = 8$：$a(2 - a) = 8 \implies 2a - a^2 = 8 \implies a^2 - 2a + 8 = 0$。该二次方程的判别式 $D_a = (-2)^2 - 4(1)(8) = 4 - 32 = -28 \equiv 10 \pmod{19}$。由于 $D_a = 10$ 是 F_{19} 中的非平方元，所以 $a^2 - 2a + 8 = 0$ 在 F_{19} 中没有解。$f_1(x)$ 不能分解为两个形如 $(x^2 + ax + 1)$ 的二次多项式的乘积。

综上：$f_1(x)$ 在 $\mathbb{F}_{19}$ 上不可约。

得出结论：在 $q = 19$ 的例子中，我们从 $\mathbb{F}_{19}$ 上次数为 2 的首一不可约多项式 $f_0(x) = x^2 + x + 2$ 出发，计算得到 $f_1(x) = x^4 + 2x^3 + 10x^2 + 2x + 1$。我们验证了 $f_1(x)$ 的次数为 4，并且它在 $\mathbb{F}_{19}$ 上是不可约的。这与定理的结论一致。从而构造定理 4.0.2 在此例中成立。

第六章　总结和展望

本文围绕有理变换在不可约多项式构造中的应用展开系统性研究，主要取得以下成果：

1. 理论完善与补充证明：

在 Cohen 提出的有理变换框架下，我们深入分析了 Varshamov 构造方法的充要条件，并对其定理给出了完整的证明过程。针对 Meyn 提出的 Q 变换（$Q = \frac{1}{2}(x + \frac{1}{x})$），本文补充了原证明中未明确阐述的必要条件，结合分圆类理论与有限域扩张性质，完成了计数的讨论，完整建立了 Q 变换下多项式不可约性的充要判别准则。这一工作扩展了了 Meyn 构造的经验，为后续应用提供了严格的理论支撑。

2. 分圆类与计数问题的创新计算：

通过引入分圆类划分和群作用轨道分析，重新梳理了有限域 F_n 上线性不可约多项式的计数方法。沿循粟景昱的研究成果，利用分圆数 $N(i,j)^{(e,q)}$ 的对称性质，优化了传统计数公式的计算复杂度，给出了一次多项式在 Q 变换下的具体构造过程。

3. 算法实现与验证：

针对 Cohen 和 Meyn 的构造方法，设计了基于 Python 的算法框架，实现了从多项式生成、有理变换映射到不可约性检验的全流程自动化验证。通过有限域运算优化和递归迭代设计，为理论结果提供了计算实证。

尽管本文在不可约多项式构造理论中取得了一定进展，但仍存在若干值得深入探索的方向：

1. 密码学应用的实践探索：

不可约多项式在椭圆曲线密码和纠错编码中具有重要应用价值。未来工作可将本文构造方法应用于设计具有特定代数结构的密钥生成算法，并通过安全性分析（如抗量子攻击特性）验证其实际效能。

2. 群作用与轨道分类的优化：

针对 PGL_2 群在不可约多项式集合上的作用，可进一步研究其轨道稳定子群的结构特性，结合 Burnside 引理优化轨道计数算法，为大规模不可约多项式库的生成提供高效分类方法。

本研究为有限域上不可约多项式的系统化构造提供了新的理论工具和计算范式，未来将继续深化代数构造与计算实践的交叉融合，推动该领域在理论与应用层面的双重突破。

参考文献

[1] 聂灵沼, 丁石孙. 代数学引论（第二版）[M]. 高等教育出版社, 2000: 210-229.

[2] DING C S. Designs From Linear Codes[M]. Beijing: World Scientific Publishing, 2018.

[3] 麻常利, 曾丽伟, 刘杨. 一些不可约循环码的权重分布[J]. 中国科学: 数学, 2011, 41(010): 877-884.

[4] PANARIO D, REIS L, WANG Q. Construction of irreducible polynomials through rational transformations[J]. J. Pure Appl. Algebra, 2019, 224(5): 106241.

[5] 王剑涛. 有限域上不可约多项式的若干问题的研究[D]. 上海交通大学, 2018.

[6] 倪佳. 代数基本定理的研究历史[D]. 西北大学, 2021.

[7] COHEN S D. On irreducible polynomials of certain types in finite fields[J]. Math. Proc. Cambridge Philos. Soc., 1969, 66(2): 335-344.

[8] DANIEL P, ALFREDO V. Analysis of Rabin’s polynomial irreducibility test[C]//Lecture Notes in Computer Science: vol. 1380: 1. 1998: 1-10.

[9] MEYN H. On the construction of irreducible self-reciprocal polynomials over finite fields[J]. Applicable Algebra in Engineering, Communication and Computing, 1990, 1: 43-53.

[10] MENEZES A J, BLAKE I F, GAO X H, et al. Applications of Finite Fields[M]. Kluwer Academic Publishers, 1993.

[11] KYUREGHYAN M K. Recurrent methods for constructing irreducible polynomials over Fq of odd characteristics[J]. Finite Fields Appl., 2003, 9(1): 39-58.

[12] ABRAHAMYAN S, ALIZADEH M, KYUREGHYAN M K. Recursive constructions of irreducible polynomials over finite fields[J]. Finite Fields Appl., 2012, 18(4): 738-745.

[13] REIS L. On the existence and number of invariant polynomials[J]. Finite Fields Appl., 2020, 61: 101605.

[14] STICHTENOTH H, TOPUZOĞLU A. Factorization of a class of polynomials over finite fields[J]. Finite Fields Appl., 2012, 18: 108-122.

[15] REIS L. The action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$, revisited[J]. J. Pure Appl. Algebra, 2018, 222: 1087-1094.

[16] DAYKIN D E. The irreducible factors of $(cx+d)x^{q^m}-(ax+b)$ over GF(q)[J]. Quarterly Journal of Mathematics, Oxford Series (2), 1963, 14: 61-64.

[17] 栗景昱. 不可约多项式的相关研究[D]. 河北师范大学, 2023.

[18] VARSHAMOV R. A general method of synthesizing irreducible polynomials over Galois fields[J]. Soviet Math. Dokl., 1984, 29: 334-336.

[19] VARSHAMOV R. A certain linear operator in a Galois field and its applications (Russian)[J]. Studia Sci. Math. Hungar., 1973, 8: 5-19.

[20] COHEN S. The explicit construction of irreducible polynomials over finite fields[J]. Designs, Codes and Cryptography, 1992, 2: 169-174.

附录 A　$\mathbb{F}_{19}$ 中平方元及代码设计

1：$\mathbb{F}_{19}$ 中非零元素的平方运算结果如下（模 19）：

- $1^2 \equiv 1 \pmod{19}$
- $2^2 \equiv 4 \pmod{19}$
- $3^2 \equiv 9 \pmod{19}$
- $4^2 = 16 \pmod{19}$
- $5^2 = 25 \equiv 6 \pmod{19}$
- $6^2 = 36 \equiv 17 \pmod{19}$
- $7^2 = 49 \equiv 11 \pmod{19}$
- $8^2 = 64 \equiv 7 \pmod{19}$
- $9^2 = 81 \equiv 5 \pmod{19}$

综上，我们得到：$\mathbb{F}_{19}$ 中的非零平方元是 $\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$；$\mathbb{F}_{19}$ 中的非平方元是 $\{2, 3, 8, 10, 12, 13, 14, 15, 18\}$ (其中 $18 \equiv -1 \pmod{19}$)。

2：第二种构造的代码设计：

```
# irreducible_poly_constructor.py
class IrreduciblePolyConstructor:
    def __init__(self, q, f_coeffs):
        """
        初始化不可约多项式构造器

        参数:
        q: int - 奇素数，定义有限域 F_q
        f_coeffs: list - 初始不可约多项式的系数列表，从低次到高次排列
        """
        self.q = q
        self.f_coeffs = f_coeffs
        self.iteration_count = 0  # 初始化迭代计数器

        # 转换为字典形式存储多项式 {次数: 系数}
        self.poly = {i: c % q for i, c in enumerate(f_coeffs)}

        # 验证初始条件
        self._validate_initial_conditions()

    def _validate_initial_conditions(self):
```

```
        """ 验证初始多项式满足构造定理条件"""
        # 条件 1: 当 q ≡ 3 mod4 时, 多项式次数必须为偶数
        if self.q % 4 == 3 and self.degree % 2 != 0:
            raise ValueError(f" 当 q≡3 mod4 时, 初始多项式次数必须为偶数,
            当前次数: {self.degree}")

        # 条件 2: f(1)*f(-1) 必须是非平方元
        f1 = sum(self.poly.values()) % self.q
        f_neg1 = sum(c * (-1)**i for i, c in self.poly.items()) % self.q
        product = (f1 * f_neg1) % self.q
        squares = {x**2 % self.q for x in range(self.q)}
        if product in squares:
            raise ValueError(f"f(1)*f(-1) = {product} 是平方元, 违反构造条件")

    @property
    def degree(self):
        """ 获取当前多项式的次数"""
        return max(self.poly.keys()) if self.poly else 0

    @property
    def polynomial(self):
        """ 获取标准形式系数列表 (从 x^0 到 x^n) """
        max_deg = self.degree
        return [self.poly.get(i, 0) for i in range(max_deg + 1)]

    def iterate(self, k=1):
        """
        执行 k 次迭代构造

        参数:
        k: int - 迭代次数, 默认为 1
        """
        for _ in range(k):
            new_poly = {}
            # 变量替换 z = (x + x^-1)/2
            for deg, coeff in self.poly.items():
                # 生成 (x + x^-1)^deg 展开项
                for j in range(deg + 1):
                    new_deg = 2*j - deg
                    term_coeff = coeff * self._comb(deg, j)
                    term_coeff *= pow(2, -deg, self.q)  # 处理 1/2^deg

                    # 合并同类项
                    if new_deg in new_poly:
```

```
                    new_poly[new_deg] = (new_poly[new_deg] + term_coeff) % self.q
                else:
                    new_poly[new_deg] = term_coeff % self.q

        # 消除负次数项 (乘以 x^m)
        min_deg = min(new_poly.keys())
        if min_deg < 0:
            shift = -min_deg
            self.poly = {
                deg + shift: c % self.q
                for deg, c in new_poly.items()
            }
        else:
            self.poly = new_poly

        # 乘以 (2x)^iteration_count
        multiplier = pow(2, self.iteration_count, self.q)
        self.poly = {
            deg + self.iteration_count: (c * multiplier) % self.q
            for deg, c in self.poly.items()
        }

        self.iteration_count += 1  # 更新迭代计数器

    return self

def _comb(self, n, k):
    """ 有限域组合数计算"""
    if k < 0 or k > n:
        return 0
    res = 1
    for i in range(1, k+1):
        res = res * (n - k + i) // i
    return res % self.q
```

致谢

行文至此，落笔为终。值此春深似海之际，回望四年大学生活，感慨良多。在此，谨向所有给予我指导、支持和帮助的老师、同学、家人和朋友致以最诚挚的感谢！

我衷心感谢我的导师胡志老师 。从论文选题、框架设计到研究方法的确定，再到最终的修改完善，他始终以严谨的治学态度和耐心的指导为我指明方向。在任务规划方面提前要求我们准备，这使本该手忙脚乱的最后几个月，变得更从容，更好的规划下一阶段。在学术研究方面，教会我如何做一项基础的研究，在此向您致以最深的敬意与感谢。

回顾我的大学四年岁月，不得不感叹，尽管身为数学系的学生，但数学方面的学习却并不满意，这无疑是个人懒散的缘故。我也时常遗憾，大学里没有再多学一些数学，毕竟在日后的时光中很难再有少年求学时的心境。

我衷心感谢父母和友人，在背后鼓励我，支持我。感谢在我夜深人静，惆怅辗转时，和我的心灵上谈话，支撑着我继续前行。尽管今日这份答卷，或许并不完美，也没那么精彩，但我许诺必携诸君所赐智识德性，步月登云，不负韶华。感谢你们长久的相信，长久的支持。我所有的文章字缝里皆跳动着你们赋予的生命力与光明。

感谢先行者，学长和前辈们给我的经验和鼓励；感谢同行者，四年来的所有课题研究的伙伴们，奋斗岁月永怀在心；感谢后来人，愿这篇稚拙的论文能引起哪怕任何轻微的回响。

恭敬在心，不在虚文。搁笔临窗，海棠未雨，此去经年。谨以此文致谢岁月恩赐的波澜与静好。

最后，对参与论文评审、答辩的各位老师表示衷心的感谢！