Софийски Университет "св. Климент Охридски"
Факултет по Математика и Информатика

Иван Бойчев Маринов

Дзета функции на линейни кодове и локално крайни модули

ДИСЕРТАЦИЯ

за получаване на образователна и научна степен “доктор”
по професионално направление 4.5 “Математика”
(Алгебра и теория на числата)

научен ръководител: проф. д-р Азнив Киркор Каспарян

София
2 0 1 8

Съдържание

Съдържание **2**

1 Увод **2**

2 Предварителни сведения за криви **10**
2.1 Дискретни нормирания 10
2.1.1 Дискретни нормирания и техните пръстени 12
2.1.2 Дискретност на нормиранията на функционално поле на една променлива 15
2.2 Действие на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ върху многообразия 23
2.2.1 $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-действие върху афинно многообразие 23
2.2.2 $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-действие върху проективни пространства и многообразия 29
2.3 Орбити на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ и дискретни нормирания 40
2.3.1 Локален пръстен на точка от крива над алгебрично затворено поле 40
2.3.2 Локален пръстен на точка над крайно поле и орбити на абсолютната група на Галоа на това поле 52
2.4 Теорема на Риман 54
2.4.1 Дивизори и пространства на Риман-Рох 54
2.4.2 Теорема на Риман 65
2.5 Горна граница върху броя на рационалните точки 68

3 Мак Уилямс и дзета полином на код **73**
3.1 Алгебро-геометрични кодове на Гоппа 73
3.2 Тъждества на Мак Уилямс 78
3.3 Дзета полином на линеен код 82
3.4 Свойства на дзета полинома на линеен код 86

4 Редуциран полином на Дуурсма **93**
4.1 Теглови полином на произволен код 94
4.2 Формална самодуалност 101
4.3 Редуциран полином на Дуурсма на функционално поле 109

5 Мак Уилямс и Риман-Рох **118**
5.1 Поляризирани условия на Риман-Рох 119
5.2 Усредняващи и вероятностни интерпретации 125

6 Аналог на хипотезата на Риман **130**
6.1 Елементарни свойства 131
6.2 Локално крайни модули с полиномиално ζ-частно 136
6.3 Крайни неразклонени покрития 144
6.4 Аналог на хипотезата на Риман 156

Библиография **168**

Глава 1

Увод

Настоящият дисертационен труд решава някои комбинаторни задачи чрез пораждащи функции на една променлива, използвайки идеи от алгебричната геометрия. От една страна са развити резултати на Дуурсма за изучаване на тегловото разпределение на линеен код C чрез неговата ζ-функция. От друга страна се определя ζ-функция на локално краен модул M над абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$ и се намира достатъчно условие, при което M изпълнява аналога на хипотезата на Риман относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Разглежданията за линейни кодове установяват, че тъждествата на Мак Уилямс за тегловото разпределение на линеен код C и неговия дуален $C^\perp$ са поляризирано обобщение на Теоремата на Риман-Рох за криви. Нека $C \subset \mathbb{F}_q^n$ е $\mathbb{F}_q$-линеен код с дължина n и размерност $k = \dim_{\mathbb{F}_q}(C)$, а $C^{\mathrm{MDS}} \subset \mathbb{F}_q^n$ е MDS-код със същата дължина n и размерност $k = \dim_{\mathbb{F}_q}(C^{\mathrm{MDS}})$ като C. Коефициентите на редуцирания полином на Дуурсма, който изучаваме се оказват удобни параметри за броя на думите с фиксирано тегло, които трябва да отстраним, съответно, да присъединим към C^{MDS}, за да получим C (или код със същото теглово разпределение като C). Известно е, че от аналога на хипотезата на Риман за гладка неприводима крива X следва границата на Хасе-Вайл за броя на рационалните точки на X. Получените в дисертацията резултати разкриват, че основните предпоставки за изпълнение на аналога на хипотезата на Риман за локално крайни модули M са границата на Хасе-Вайл и наличието на неразклонено покритие $M_o \to L_o$ с обвивка на Галоа за подмодули $M_o \subseteq M$ и $L_o \subseteq \mathbb{P}^1(\overline{\mathbb{F}_q})$ с най-много крайни допълнения.

Ако $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, определена над крайно поле $\mathbb{F}_q$ и $N_m := |X \cap \mathbb{P}^n(\mathbb{F}_{q^m})|$ е броят на $\mathbb{F}_{q^m}$-рационалните точки на X, то формалният степенен ред

$$\zeta_X(t) = \exp\left(\sum_{m=0}^{\infty} N_m \frac{t^m}{m}\right),$$

се нарича ζ-функция на X. Проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ има ζ-функция

$$\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t) = \frac{1}{(1-t)(1-qt)}.$$

Ако $F = \mathbb{F}_q(X)$ е функционалното поле на X над $\mathbb{F}_q$, то

$$\zeta_X(t) = L_F(T)\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t) = \frac{L_F(t)}{(1-t)(1-qt)}$$

за полином $L_F(t) \in \mathbb{Z}[t]$, който се нарича ζ-полином на кривата. По определение, ζ-полиномът и ζ-функцията на крива X съдържат пълна информация за броя на рационалните точки на X.

Изследванията на настоящата дисертационна работа са силно повлияни и вдъхновени от трудовете на Иван Дуурсма [Duursma1] и [Duursma2]. В тези статии той въвежда и изучава ζ-полинома на линеен код C, който задава еднозначно тегловото разпределение на кода. Чрез алгебро-геометрична реализация на C като код на Гоппа върху крива X, Дуурсма свързва ζ полинома на C с този на X. Той представя тегловия полином на линеен код C като линейна комбинация на тегловите полиноми на подходящи MDS-кодове с рационални коефициенти a_i, $0 \leq i \leq r$. Дуурсма определя ζ-полинома на C като

$$P_C(t) = \sum_{i=0}^{r} a_i t^i$$

и ζ-функцията на C като

$$\zeta_C(t) = \frac{P_C(t)}{(1-t)(1-qt)}.$$

Той доказва, че ζ-полиномът $P_C(t)$ на линеен код C е свързан с ζ-полинома $P_{C^\perp}(t)$ на неговия дуален $C^\perp$ посредством функционалното уравнение

$$P_{C^\perp}(t) = P_C\left(\frac{1}{qt}\right) q^g t^{g+g^\perp},$$

което заедно с условието $P_C(1) = P_{C^\perp}(1) = 1$ еквивалентно на тъждествата на Мак Уилямс за тегловото разпределение на C и на $C^\perp$. В частност,

$$P_C\left(\frac{1}{q}\right) = P_{C^\perp}(1)q^{-g} = \frac{1}{q^g}$$

и полиномът $P_C(t) - t^g \in \mathbb{Q}[t]$ се анулира за $t = 1$ и $t = \frac{1}{q}$. Дуурсма забелязва, че

$$D_C(t) := \frac{P_C(t) - t^g}{(1-t)(1-qt)} \in \mathbb{Q}[t]$$

е полином с рационални коефициенти, но не използва този полином за изучаване на тегловото разпределение на C и $C^\perp$. Някои ключови резултати от глави 4 и 5 са свързани със свойствата на $D_C(t)$, който наричаме редуциран полином на Дуурсма.

Мотивацията, както и терминологията на настоящия дисертационен труд са отражение на свойствата на проективните криви, определени над крайно поле. Съгласно статията [PShW] на Пеликаан, Шен и ван Уи, всеки линеен код може да се реализира като алгебро-геометричен код на Гоппа, т.е. като множество от стойности на пространство на Риман-Рох на дивизор върху крива в краен брой точки на тази крива.

При такава реализация, точките от проективизацията на кода могат да се разглеждат като ефективни дивизори от фиксиран клас на линейна еквивалентност. Затова сумата на ζ-функциите на алгебро-геометричните кодове, отговарящи на пълна система представители на класовете на линейна еквивалентност на дивизорите от фиксирана степен, се оказва равна на ζ-функцията на кривата.

Статията [KM1] изучава тегловото разпределение на линеен код C чрез редуцирания полином на Дуурсма $D_C(t)$ на C. Тя установява, че коефициенти на $D_C(t)$ изразяват разликата на тегловия полином на C и тегловия полином на MDS-код C^{MDS} със същата дължина и размерност като C относно мономи на хомогенните линейни полиноми $x-y$ и y. С помощта на $D_C(t)$, работата [KM2] доказва, че тъждествата на Мак Уилямс за тегловото разпределение на C и $C^{\perp}$ са еквивалентни на поляризирани условия на Риман-Рох.

В светлината на [PShW], линейните кодове могат да се разглеждат като комбинаторни разновидности на линейните системи от дивизори върху алгебрична крива X. Абстрахирайки някои свойства на действието на абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$ върху гладка неприводима крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, определена над $\mathbb{F}_q$, въвеждаме понятието локално краен модул M над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Наличието на взаимно еднозначно съответствие между $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитите върху X и класовете дискретни нормирания на функционалното поле $F = \mathbb{F}_q(X)$ на X позволява определянето на ζ-функция $\zeta_M(t)$ на M. Съгласно Теоремата на Хасе-Вайл, частното

$$L_F(t) := \frac{\zeta_X(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = (1-t)(1-qt)\zeta_X(t)$$

на ζ-функцията $\zeta_X(t)$ на X и ζ-функцията $\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)$ на проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ е полином, чиито корени са с модул $\frac{1}{\sqrt{q}}$. Този резултат е еквивалентен на $\mathrm{Re}(s_o) = \frac{1}{2}$ за комплексните корени $s_o \in \mathbb{C}$ на функцията $L_F(q^{-s})$ на комплексна променлива $s \in \mathbb{C}$ и се нарича аналог на хипотезата на Риман. Статията [KM3] доказва достатъчно условие, при което локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул M изпълнява аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Споменатото достатъчно условие се състои от три предположения. Първото предположение е, че частното

$$P_M(t) := \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)}$$

на ζ-функцията $\zeta_M(t)$ на M и ζ-функцията $\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)$ на проективната права е полином $P_M(t)$ с цели коефициенти. Второто предположение изисква съществуването на $\mathfrak{G}$-подмодули $M_o \subseteq M$, съответно, $L_o \subseteq \mathbb{P}^1(\overline{\mathbb{F}_q})$ с най-много крайни допълнения $M \setminus M_o$, $\mathbb{P}^1(\overline{\mathbb{F}_q}) \setminus L_o$, които са свързани с крайно неразклонено покритие $\xi : M_o \to L_o$, притежаващо обвивка на Галоа. Третото изискване е аналог на границата на Хасе-Вайл за броя на рационалните точки на крива X и се формулира като неравенство между порядъка на Хасе.Вайл на M и $\lambda := \log_q \sqrt[d]{|LC(P_M(t))|} \in \mathbb{R}^{\geq 0}$, където $LC(P_M(t)) \in \mathbb{Z} \setminus \{0\}$ е старшият коефициент на $P_M(t)$.

Накратко за съдържанието на настоящия дисертационен труд. Следващите две

глави се състоят от предварителни сведения. Глави 4, 5 и 6 отразяват, съответно, резултатите на публикациите [KM1], [KM2] и [KM3].

Следващата глава 2 съдържа предварителни сведения от областта на алгебричната геометрия. Първият параграф е посветен на взаимно еднозначното съответствие между класовете дискретни нормирания ν на функционалните полета $\mathbb{F}_q(X)$ на алгебричните криви X и техните локални пръстени $\mathcal{O}_\nu$. Напомня се класификацията на дискретните нормирания ν на чисто трансцендентно разширение $\mathbb{F}_q(x)$ на полето от коефициенти $\mathbb{F}_q$ и техните пръстени $\mathcal{O}_\nu$. Доказва се, че всички нормирания на функционално поле $\mathbb{F}_q(X)$ на крива X са дискретни и съответните им полета от остатъци $\mathcal{O}_\nu/\mathfrak{M}_\nu$ са крайни разширения на $\mathbb{F}_q$. Подробно се дискутира Апроксимационната теорема за краен брой дискретни нормирания и краен брой елементи, както и наличието на разлагане в Лоранов ред на произволна рационална функция $f \in \mathbb{F}_q(X)$ относно локален параметър t на $\mathcal{O}_\nu$. Тези факти се използват във втората част на параграф 3 за извеждане на съответствието между пръстените на дискретно нормиране на $\mathbb{F}_q(X)$ и орбитите на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, в четвъртия параграф за изучаване на дивизорите на рационални функции върху крива, както и в параграф 5 за получаване на горна граница върху броя на рационалните точки на крива. Вторият параграф на глава 2 разглежда някои свойства на действието на абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$ върху афинно или проективно пространство или многообразие. Дискутира се топологията на Зариски, структурата на Зариски затворената обвивка и неприводимостта на многообразие. Третият параграф на глава 2 обяснява подробно съответствието между гладките точки на неприводима крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, определена над $\mathbb{F}_q$ и пръстените на дискретно нормиране на $\overline{\mathbb{F}_q}(X)$, както и съответствието между $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитите върху X и пръстените на дискретно нормиране на $\mathbb{F}_q(X)$. Напомнени са основните свойства на дивизорите върху крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ и техните пространства на Риман-Рох. Изложено е доказателството на Теоремата на Риман за дивизор върху крива. Детайлно е разгледан случаят на равенство и е формулирана Теоремата на Риман-Рох. Последният, пети параграф на глава 2 излага доказателството на горна граница върху броя на рационалните точки на гладка неприводима крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, която мотивира даденото в [KM3] определение за порядъка на Хасе-Вайл на локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$.

В глава 3 са събрани някои предварителните сведения от теория на кодирането, които се концентрират около тъждествата на Мак Уилямс. Първият параграф напомня основни определения за линейни кодове и алгебро-геометричните кодове на Гоппа. Вторият параграф дискутира тъждествата на Мак Уилямс за тегловото разпределение на двойка дуални линейни кодове в техния класически вид. Последните два параграфа са посветени на резултати на Дуурсма от [Duursma1], [Duursma2] и [Duursma3]. Третият параграф дава две еквивалентни определения за ζ-полинома $P_C(t)$ на линеен код $C \subset \mathbb{F}_q^n$. Четвъртият параграф доказва връзката между ζ-полиномите $P_{C_i}(t)$ на алгебро-геометричните кодове на Гоппа, асоциирани с пълна система представители G_i на класовете на линейна еквивалентност на дивизорите от подходяща фиксирана степен върху крива X с ζ-полинома $L_{\mathbb{F}_q(X)}$ на X. Тя изразява тъждествата на Мак Уилямс за C и $C^\perp$ във вид на функционално уравнение на техните ζ-полиноми $P_C(t)$,

съответно, $P_{C^\perp}(t)$.

Глава 4 отразява резултатите на статията [KM1]. Тя е посветена на редуцирания полином на Дуурсма

$$D_C(t) := \frac{P_C(t) - t^g}{(1-t)(1-qt)} \in \mathbb{Q}[t]$$

на линеен код C от род g с ζ-полином $P_C(t)$. В своята статия [Duursma3] Дуурсма забелязва съществуването на $D_C(t)$, но не използва този полином за описание на тегловото разпределение на C. Нека C е $\mathbb{F}_q$-линеен код от род g с дуален $C^\perp$ от род $g^\perp$, $\mathcal{W}_C(x,y) \in \mathbb{Z}[x,y]$ е тегловият полином на C, а $\mathcal{M}_{n,n+1-k}(x) \in \mathbb{Z}[x,y]$ е тегловият полином на MDS-код със същата дължина n и размерност k като C. Първият параграф на глава 4 използва коефициентите на редуцирания полином на Дуурсма $D_C(t) \in \mathbb{Q}[t]$ на C за изразяване на $\mathcal{W}_C(x,y) - \mathcal{M}_{n,n+1-k}(x,y) \in \mathbb{Z}[x,y]$ като хомогенен полином на $x-y$ и y от степен n. В резултат, $D_C(t)$ определя еднозначно броя на думите с фиксирано тегло, които трябва да се присъединят, съответно, отстранят от MDS-код C^{MDS} със същата дължина n и размерност k като C, за да се получи C (или код със същото теглово разпределение като C). Във втория параграф се проверява, че линейните кодове C, изпълняващи аналога на хипотезата на Риман са формално самодуални. Тегловото разпределение на формално самодуален код C от род g се характеризира чрез половината на коефициентите на редуцирания полином на Дуурсма $D_C(t)$ на C. Установено е, че тегловото разпределение на формално самодуален код с размерност k и минимално разстояние d се определя напълно от броя на думите на C с тегло $d \le w \le k$. Ако C е формално самодуален код от род g,то редуцираният полином на Дуурсма $D_C(t) \in \mathbb{Q}[t]$ на C е от степен $\deg(D_C(t)) = 2g-2$. Кодовете с постоянен редуциран полином на Дуурсма $D_C(t) = c_o \in \mathbb{Q}$ са почти MDS-кодовете, изучени от Додунеков и Ланджев в [Додунеков, Ланджев]. Резултатите на Ким и Хюн от [Kim, Hyun] характеризират почти MDS-кодовете, изпълняващи аналога на хипотезата на Риман. Параграф 2 от глава 4 дава необходимо и достатъчно условие, при което формално самодуален код с квадратичен полином на Дуурсма изпълнява аналога на хипотезата на Риман. Третият параграф на глава 4 изучава редуцирания полином на Дуурсма, $D_{\mathbb{F}_q(X)}(t) \in \mathbb{Z}[t]$ на функционално поле $\mathbb{F}_q(X)$ на гладка неприводима крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ от род g, определена над $\mathbb{F}_q$. Той доказва, че коефициентите на $D_{\mathbb{F}_q(X)}(t)$ се определят еднозначно от броя на ефективните дивизори върху X от степен $\le g-1$. Частното

$$\frac{D_{\mathbb{F}_q(X)}(t)}{(1-t)(1-qt)}$$

се характеризира с редица свойства на ζ-функцията на гладка неприводима проективна крива от род $g-1$, определена над $\mathbb{F}_q$.

Петата глава на настоящия дисертационен труд е посветена на еквивалентностата на тъждествата на Мак Уилямс за тегловото разпределение на линеен код C и неговия дуален $C^\perp$ с поляризираните условия на Риман-Рох за техните ζ-функции

$$\zeta_C(t) := \frac{P_C(t)}{(1-t)(1-qt)}, \quad \text{съответно,} \quad \zeta_{C^\perp}(t) := \frac{P_{C^\perp}(t)}{(1-t)(1-qt)}.$$

Този резултат разкрива общата природа на споменатите класически резултати от теория на кодирането и алгебричната геометрия. Той позволява разглеждането на тъждествата на Мак Уилямс като поляризиран вариант на Теоремата на Риман-Рох и двойствеността на Сер върху гладка неприводима крива X. Първият параграф на глава 5 въвежда поляризираните условия на Риман-Рох за двойка формални степенни редове и мотивира тяхното определение с условията на Риман-Рох върху крива. Той изразява тъждествата на Мак Уилямс за двойка дуални линейни кодове C, $C^{\perp}$ чрез поляризираните условия на Риман-Рох за съответните ζ-функции $\zeta_C(t)$, $\zeta_{C^{\perp}}(t)$. Вторият параграф на глава 5 предоставя усредняващи и вероятностни интерпретации на коефициентите на редуцирания полином на Дуурсма $D_C(t)$ на линеен код C.

Последната глава 6 дава достатъчно условие за изпълнение на аналога на хипотезата на Риман за локално крайни модули над абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$. Нейните разглеждания обобщават хипотезите на Вайл за гладка неприводима проективна крива X, определена над $\mathbb{F}_q$. Исторически, ζ-функцията $\zeta_X(t)$ на X е въведена от Артин през 1923 г. Теоремата на Хасе-Вайл за X гласи, че

$$\zeta_X(t) = \frac{L_{\mathbb{F}_q(X)}(t)}{(1-t)(1-qt)}$$

за полином $L_{\mathbb{F}_q(X)}(t) \in \mathbb{Z}[t]$, чиито корени се намират върху окръжността в комплексната равнина $\mathbb{C}$ с начало $0 \in \mathbb{C}$ и радиус $\frac{1}{\sqrt{q}}$. Случаят на елиптична крива X е доказан от Хасе през 1936 г. Андре Вайл установява верността на теоремата за произволна гладка неприводима проективна крива X през 1940 г. Разглежданията от глава 6 обобщават доказателството на Бомбиери от [Bombieri] на Теоремата на Хасе-Вайл. Те предоставят критерий или достатъчно условие за изпълнение на аналога на хипотезата на Риман за локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_Q)$-модул M относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Критерият се състои от три предположения. Първо изискваме частното

$$P_M(t) := \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)}$$

на ζ-функцията $\zeta_M(t)$ на M и ζ-функцията $\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)$ на $\mathbb{P}^1(\overline{\mathbb{F}_q})$ да е полином $P_M(t) = \sum_{i=0}^{d} a_i t^i$. Второ, предполагаме съществуването на покритие $\xi : M \dashrightarrow \mathbb{P}^1(\overline{\mathbb{F}_q})$ с обвивка на Галоа. Дефиниционната област M_o на ξ и областта от стойности $\xi(M_o)$ са с крайно допълнение в M, съответно, в $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Обвивката на Галоа се състои от локално краен $\mathfrak{G}_m = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$-модул N за някакво крайно разширение $\mathbb{F}_{q^m} \supset \mathbb{F}_q$ и крайни групи $H_1 < H$ от $\mathfrak{G}_m$-еквивариантни биекции $N \to N$ без фиксирани точки, така че изображението $\xi_H : N \to N/H = \xi(M_o)$, $\xi_H(z) = \mathrm{Orb}_H(z)$, съпоставящо на точка $z \in N$ нейната H-орбита се пропуска през $\xi_{H_1} : N \to N/H_1 = M_o$ и неразклоненото покритие $\xi : M_o \to \xi(M_o)$. Третото предположение на критерия за изпълнение на аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ е горна граница върху относителната скорост на растене на броя на рационалните точки на M относно броя на рационалните точки на $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Споменатата граница зависи от степента и старшия коефициент на

ζ-полинома $P_M(t)$. Тя може да се разглежда като обобщение на класическата граница на Хасе-Вайл за броя на рационалните точки върху гладка неприводима проективна крива, определена над $\mathbb{F}_q$. Конструиран е пример за локално краен модул M над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, изпълняващ предположенията на дискутирания критерий, а оттам и аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$, който не е изоморфен като $\mathfrak{G}$-модул на гладка неприводима проективна крива X, определена над $\mathbb{F}_q$. Установено е, че от аналога на хипотезата на Риман за локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул M относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ следва функционалното уравнение за ζ-полинома $P_M(t)$ на M.

Публикации във връзка с дисертацията

1. Duursma's reduced polynomial, A. Kasparian, I. Marinov, Advances in Mathematics of Communication, vol. 11, № 4, November 2017.

2. Mac Williams identities and polarized Riemann-Roch conditions, A. Kasparian, I. Marinov, Electronic Notes in Discrete Mathematics, vol. 57, 2017.

3. Riemann Hypothesis Analogue for locally finite modules over the absolute Galois group of a finite field, A. Kasparian, I. Marinov, accepted for a publication in Annuaire de l'Université de Sofia "St. Kl. Ohridski"

Апробация на резултатите

Резултатите на дисертацията са докладвани на следните научни форуми:

1. "Tangent codes", A. Kasparian, E. Velikova, I. Marinov, Международна конференция "Дни на математиката в София", 7 - 10 юли 2014 г.

2. "Някои интерпретации на тегловия полином на линеен код", А. Каспарян, И. Маринов, Национален семинар по кодиране "Акад. Стефан Додунеков", 20-23 ноември 2014г.

3. "Редуциран полином на Дуурсма", А. Каспарян, И. Маринов, Юбилейна конференция "125 години математика и природни науки в Софийски университет "Св. Климент Охридски", 5 - 7 декември 2014 г.

4. "Фамилии на Гоппа от линейни кодове", А. Каспарян, И. Маринов, Пролетна научна сесия на Факултета по математика и информатика на Софийски университет "Св. Климент Охридски", 28 март 2015 г.

5. "Нелинейни кодове на Гоппа", А. Каспарян, И. Маринов, Национален семинар по кодиране "Акад. Стефан Додунеков", 19-22 ноември 2015 г.

6. "Mac Williams identities for linear codes as Riemann-Roch conditions", A. Kasparian, I. Marinov, 18-24 юни 2016 г.

7. ”Локално крайни модули над топологично циклична про-крайна група”, А. Каспарян, И. Маринов, Пролетна научна сесия на Факултета по математика и информатика на Софийски университет ”Св. Климент Охридски”, 26 март 2016 г.

8. ”Riemann Hypothesis Analogue for locally finite modules over the absolute Galois group of a finite field”, A. Kasparian, I. Marinov, International Conference ”Groups and Rings - Theory and Applications”, (GRiTA 2016), 11-15 юли 2016 г.

9. ”Унитарни симетрии на локално крайни модули”, А. Каспарян, И. Маринов, Пролетна научна сесия на Факултета по математика и информатика на Софийски университет ”Св. Климент Охридски”, 25 март 2017 г.

Докладите с номера 4, 5, 6, 7, и 9 са изнесени от Иван Маринов, а тези с номера 1, 2, 3 и 8 са изнесени от Азнив Каспарян.

Глава 2

Предварителни сведения за криви

Настоящата глава съдържа предварителни сведения от алгебричната геометрия. Тя дискутира класовете дискретни нормирания на функционално поле на една променлива, както и действието на абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$ върху афинно или проективно неприводимо многообразие X, определено над $\mathbb{F}_q$. Обяснено е подробно съответствието между пръстените на дискретно нормиране на функционалното поле $\mathbb{F}_q(X)$ на X над $\mathbb{F}_q$ и орбитите на $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ върху X. Припомнени са някои свойства на дивизорите върху крива и техните пространства на Риман-Рох. Приведено е доказателството на Теоремата на Риман и е дискутиран случая на равенство. Последният параграф доказва горна граница върху брой на рационалните точки на крива X, определена над $\mathbb{F}_q$. Предварителните сведения от настоящата глава са взети от монографията [Niederreiter, Xing] на Niederreiter и Xing, с изключение на последния параграф, който е взаимстван от книгата [Stichtenoth] на Стичтенот.

2.1 Дискретни нормирания на функционално поле на една променлива

Определение 1. *Разширение $F \supset k$ от крайна ненулева степен на трансцендентност се нарича функционално поле с поле от константи k.*

Ако съществува трансцедентен над k елемент $x \in F$, така че $F \supseteq k(x)$ е крайно разширение, то F е функционално поле на една променлива.

Пример 2. *Ако x е трансцендентно над поле k, то полето*

$$k(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in k[x], \quad g(x) \not\equiv 0 \right\}$$

на рационалните функции на x с коефициенти от k е функционално поле на една променлива с поле от константи k.

Определение 3. *Нормиране на функционално поле $F \supset k$ на една променлива наричаме изображение $\nu : F \to \mathbb{R} \cup \{\infty\}$, за което са изпълнени следните условия:*

(i) $\nu(x) = \infty \Leftrightarrow x = 0$

(ii) $\nu(\alpha) = 0, \forall \alpha \in k^*$

(iii) $\exists \alpha \in F^*, \nu(\alpha) \neq 0$

(iv) $\nu(xy) = \nu(x) + \nu(y), \forall x, y \in F$

(v) $\nu(x+y) \geq \min(\nu(x), \nu(y)), \forall x, y \in F$ *(неархимедово неравенство на триъгълника)*

Аксиома (iv) означава, че нормирането ν се ограничава до хомоморфизъм $\nu : (F^*, .) \to (\mathbb{R}, +)$ на мултипликативната група на полето F в адитивната група на полето $\mathbb{R}$ на реалните числа.

Следващата лема извежда някои непосредствени следствия от аксиомите за нормиране:

Лема 4. *(*Следствия от аксиомите за нормиране*) Ако* $\nu : F \to \mathbb{R} \cup \{\infty\}$ *е нормиране на функционално поле* $F \supset k$ *на една променлива, то*

(i) $\nu\left(\frac{x}{y}\right) = \nu(x) - \nu(y)$ *за* $\forall x, y \in F$, $y \neq 0$;

(ii) $\nu(-x) = \nu(x)$ *за* $\forall x \in F$;

(iii) за $\nu(x) \neq \nu(y)$ *е изпълнено неравенството на триъгълника с равенство*

$$\nu(x + y) = \min(\nu(x), \nu(y))$$

за две събираеми;

(iv) за $x_1, \ldots, x_n \in F$, $n \in \mathbb{N}$, $n \geq 2$ *с* $\nu(x_i) \neq \nu(x_j)$ *за всички* $1 \leq i < j \leq n$ *е изпълнено неравенството на триъгълника с равенство*

$$\nu(x_1 + \ldots + x_n) = \min(\nu(x_i) \,|\, 1 \leq i \leq n)$$

за произволен краен брой събираеми.

Доказателство: (i) Съгласно аксиома (iv) за нормиране,

$$\nu\left(\frac{x}{y}\right) + \nu(y) = \nu\left(\frac{x}{y}.y\right) = \nu(x).$$

(ii) От $-x = (-1)x$ с $-1 \in k^*$ следва, че

$$\nu(-x) = \nu((-1)x) = \nu(-1) + \nu(x) = 0 + \nu(x) = \nu(x).$$

(iii) С точност до пермутация на x с y можем да считаме, че $\nu(y) > \nu(x)$. Ако допуснем, че $\nu(x + y) > \min(\nu(x), \nu(y)) = \nu(x)$, то $x = (x + y) + (-y)$ дава

$$\nu(x) = \nu((x + y) + (-y)) \geq \min(\nu(x + y), \nu(-y)) = \min(\nu(x + y), \nu(y)) > \nu(x),$$

което е противоречие, доказващо неравенството на триъгълника с равенство.

(iv) С индукция по $n \geq 2$, случаят $n = 2$ е доказан в (iii). Без ограничение на общността можем да считаме, че $\nu(x_1) < \nu(x_2) < \ldots, < \nu(x_{n-1}) < \nu(x_n)$. По индукционно продположение имаме

$$\nu(x_1 + \ldots + x_{n-1}) = \min(\nu(x_i) \,|\, 1 \leq i \leq n-1) = \nu(x_1).$$

Това позволява да приложим (iii) към $x = x_1 + \ldots + x_{n-1}$, $y = x_n$ и да получим, че

$$\begin{aligned}\nu(x_1 + \ldots + x_{n-1} + x_n) &= \min(\nu(x_1 + \ldots + x_{n-1}), \nu(x_n)) = \\ &= \min(\nu(x_1), \nu(x_n)) = \nu(x_1) = \min(\nu(x_i) \,|\, 1 \leq i \leq n).\end{aligned}$$

□

2.1.1 Дискретни нормирания на функционално поле на една променлива и пръстени на дискретни нормирания

Определение 5. *Нормиране $\nu : F \to \mathbb{R} \cup \{\infty\}$ на функционално поле наричаме дискретно, ако образът на мултипликативната група на полето F под действието на нормирането ν е дискретна подгрупа на адитивната група на полето на реалните числа.*

Лема 6. *Ненулевите дискретни подгрупи $(D, +)$ на $(\mathbb{R}, +)$ са от вида $(d\mathbb{Z}, +)$ за някакво реално положително $d \in \mathbb{R}^{>0}$.*

Доказателство: Нека $d \in \mathbb{R}^{>0}$ е минималното реално положително число, което принадлежи на $(D, +)$. Съществуването на такова число следва от дискретността на $(D, +)$, защото ако за всяко $r_n \in \mathbb{R}^{>0}$ съществува $0 < r_{n+1} < r_n$, то $0 \in \mathbb{R}$ е точка на сгъстяване на $(D, +)$ в $\mathbb{R}$. Твърдим, че всеки елемент на фактор-групата $(\mathbb{R}, +)/(d\mathbb{Z}, +)$ има единствен представител в $[0, d)$. Наистина, точките dz с $z \in \mathbb{Z}$ разбиват реалната права $\mathbb{R}$ на интервали $[dz, dz + d)$ с дължина d. Всяко реално число $r \in \mathbb{R}$ попада в единствен интервал $dz_r \leq r < d(z_r + 1)$ и $r - dz_r \in [0, d)$ е единствената точка от $[0, d)$, която представя съседния клас $r - dz_r + d\mathbb{Z} = r + d\mathbb{Z}$.

Подгрупата $(D, +)$ на $(\mathbb{R}, +)$ съдържа $(d\mathbb{Z}, +)$, защото $d \in D$. Следователно за всеки съседен клас $\delta + d\mathbb{Z} \in (D, +)/(d\mathbb{Z}, +)$ съществува единствено число $\Delta \in [0, d)$ с $\Delta + d\mathbb{Z} = \delta + d\mathbb{Z}$. Съгласно избора на d като минималното реално положително число от D, имаме $[0, d) \cap D = \{0\}$, така че съществува единствен съседен клас на $(D, +)$ спрямо $(d\mathbb{Z}, +)$ и $(D, +) = (d\mathbb{Z}, +)$.

□

Дискретните нормирания се характеризират със съответните им пръстени. Сега ще въведем понятието пръстен на дискретно нормиране, след което ще представим връзката между двете понятия.

Определение 7. *Комутативна област с единица R наричаме пръстен на дискретно нормиране, ако съществува неразложим елемент $t \in R$, такъв че всеки елемент $z \in R$ има представяне във вида $z = ut^m$ за $m \in \mathbb{Z}^{\geq 0}, u \in R^*$. Елементът t наричаме локален параметър на пръстена на дискретно нормиране R.*

Следващото твърдение показва връзката между дискретните нормирания на функционално поле на една променлива и пръстените на дискретни нормирания.

Твърдение 8. *Нека ν е нормиране на функционално поле на една променлива $F \supset k$ с поле от константи k. Множеството $\mathcal{O}_\nu := \{\alpha \mid \alpha \in F, \nu(\alpha) \geq 0\}$ е комутативна локална област с максимален идеал $\mathfrak{M}_\nu := \{\alpha \mid \alpha \in F, \nu(\alpha) > 0\}$ и поле от частни F. Ако ν е дискретно нормиране, то $\mathcal{O}_\nu$ е пръстен на дискретно нормиране и всеки локален параметър t на $\mathcal{O}_\nu$ поражда максималния идеал $\mathcal{M}_\nu$.*

Доказателство: Доказателството, че множеството $\mathcal{O}_\nu$ е подпръстен на полето F, а оттам и област е тривиално. Същото се отнася и за факта, че $\mathfrak{M}_\nu$ е идеал в тази област. За да докажем, че този идеал е единственият максимален идеал в $\mathcal{O}_\nu$ е достатъчно да отбележим, че множеството на обратимите елементи $\mathcal{O}_\nu^*$ на областта $\mathcal{O}_\nu$ се състои от елементите $x \in \mathcal{O}_\nu$, за които $\nu(x) = 0$, т.е. $\mathcal{O}_\nu^* \equiv \mathcal{O}_\nu \setminus \mathfrak{M}_\nu$.

За да проверим, че полето от частни на областта $\mathcal{O}_\nu$ съвпада с полето F е достатъчно да отбележим, че от една страна полето от частни $F(\mathcal{O}_\nu)$ се влага естествено в полето F. От друга страна, за произволен елемент $z \in F$, имаме две възможности за $\nu(z)$, а именно, $\nu(z) \geq 0$, или $\nu(z) < 0$. Ако $\nu(z) < 0$, то $\nu\left(\frac{1}{z}\right) = -\nu(z) > 0$, така че $\frac{1}{z} \in \mathcal{O}_\nu$ и $z = \left(\frac{1}{z}\right)^{-1} \in F(\mathcal{O}_\nu)$. По този начин, $F \equiv F(\mathcal{O}_\nu)$.

Нека $\nu : F \to \mathbb{R} \cup \{\infty\}$ е дискретно нормиране на функционалното поле на една променлива $F \supset k$. Образът $\nu(F^*)$ е ненулева дискретна подгрупа на $(\mathbb{R}, +)$ и има вида $(d\mathbb{Z}, +)$ за някое положително реално число d. Нека $t \in \mathcal{O}_\nu$ е такъв елемент, че $\nu(t) = d$, т.е. образът на елемента t поражда цялата група $d\mathbb{Z}$. За произволен ненулев елемент $z \in \mathcal{O}_\nu$ имаме $\nu(z) = dm$ за някое цяло число m. Тогава елементът $u = zt^{-m} \in \mathcal{O}_\nu^*$ е такъв, че $z = ut^m$ е търсеното представяне на елемента z. Оттук лесно следва и неразложимостта на елемента t. Поради факта, че $\nu(t) > 0$ лесно се доказва и съвпадението $\langle t \rangle \equiv \mathfrak{M}_\nu$. □

За да докажем пълното съответствие между дискретните нормирания на функционално поле на една променлива и пръстените на дискретно нормиране, ще разгледаме следното твърдение.

Твърдение 9. *Нека $F \supset k$ е функционално поле на една променлива, а $R \subset F$ пръстен на дискретно нормиране с поле от частни F, съдържащо като подпръстен полето от константи k. Тогава съществува дискретно нормиране ν на F, за което $\mathcal{O}_\nu \equiv R$.*

Доказателство: Нека t е локален параметър на R. За произволен елемент $z = \frac{r_1}{r_2} \in F^*, r_1, r_2 \in R, r_1 = ut^m, r_2 = vt^n, u, v \in R^*, m, n \in \mathbb{Z}^{\geq 0}$ полагаме

$$\nu(z) = m - n$$

$$\nu(0) = \infty$$

Така получаваме изображение $\nu : F \to \mathbb{Z} \cup \{\infty\}$. Изображението е коректно, поради единствеността на представянията $z = ut^m, z \in R, u \in R^*, m \in \mathbb{Z}$. Аксиомите за нормиране се проверяват непосредствено, което завършва доказателството. □

Определение 10. *Комутативният пръстен с единица R е нътеров, ако всеки идеал I в R е крайно породен,*

$$I = \langle \alpha_1, \ldots, \alpha_n \rangle = \left\{ \sum_{i=1}^{n} \alpha_i r_i \;\; | \;\; r_i \in R \right\}.$$

Определение 11. *Размерността на Krull на комутативен пръстен с единица R е супремумът на неотрицателните цели числа n, за които съществува редица от $n+1$ различни прости идеала*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

на R.

Твърдение 12. *Всеки пръстен на дискретно нормиране R е нътерова локална област с размерност на Krull* 1.

Доказателство: Достатъчно е да установим, че всеки ненулев собствен идеал I на R е от вида $I = \langle t^n \rangle$ за локален параметър t на R и някое естествено число n. Тогава $\langle t \rangle$ е единственият ненулев прост идеал в R. Височината на $\langle t \rangle$ е 1, защото $\langle t \rangle$ съдържа нулевия идеал $\langle 0 \rangle = \{0\}$, който е прост в областта R. Всеки собствен идеал на R се съдържа в идеала $\langle t \rangle$, така че R е локален пръстен с единствен максимален идеал $\langle t \rangle$.

Произволен идеал $\{0\} \neq I \neq R$ има празно сечение $I \cap R^* = \emptyset$ с мултипликативната група R^* на R, така че $\forall z \in I$ е от вида $z = ut^m$ за някои $m \in \mathbb{N}$, $u \in R^*$. Нека n е минималното естествено число, за което съществува елемент $u_o t^n \in I$ с $u_o \in R^*$. Понеже $u_o^{-1} \in R$, оттук следва, че $t^n \in I$ и идеалът $\langle t^n \rangle$, породен от t^n се съдържа в идеала I. Произволен ненулев елемент $z \in I \setminus \{0\}$ има вида $z = ut^m = (ut^{m-n})t^n$ за някое $m \geq n$ и принадлежи на $\langle t^n \rangle$. Оттук $I \subseteq \langle t^n \rangle$ и $I = \langle t^n \rangle$.

□

Предстои да разгледаме еквивалентността на дискретните нормирания на функционално поле на една променлива. Преди всичко трябва да кажем, кои нормирания наричаме еквивалентни.

Определение 13. *Нормиранията $\nu_1 : F \to \mathbb{R} \cup \{\infty\}, \nu_2 : F \to \mathbb{R} \cup \{\infty\}$ наричаме еквивалентни, ако съществува такава реална положителна константа c, че*

$$\nu_1(x) = c\nu_2(x), \quad за \quad \forall x \in F.$$

Непосредствено се проверява, че еквивалентността на нормирания е релация на еквивалентност. Ако $\nu_1 = c\nu_2$ за $c \in \mathbb{R}^{>0}$, то $\nu_1(x) \geq 0$ тогава и само тогава, когато $\nu_2(x) \geq 0$ и $\nu_1(x) > 0$ точно когато $\nu_2(x) > 0$. Затова пръстените

$$\mathcal{O}_{\nu_1} = \{x \in F \,|\, \nu_1(x) \geq 0\} = \{y \in F \,|\, \nu_2(y) \geq 0\} = \mathcal{O}_{\nu_2}$$

съвпадат, както и максималните им идеали

$$\mathfrak{M}_{\nu_1} = \{x \in F \,|\, \nu_1(x) > 0\} = \{y \in F \,|\, \nu_2(y) > 0\} = \mathfrak{M}_{\nu_2}.$$

Това ни позволява да определим пръстена на даден клас на еквивалентност като пръстена на кой да е от представителите на класа. Ясно е, че произволно дискретно нормиране $\nu : F \to \mathbb{R} \cup \{\infty\}$ с $\nu(F^*) = d\mathbb{Z}$, $d \in \mathbb{R}^{>0}$ е еквивалентно на нормиране $\nu' := \frac{1}{d}\nu$ с $\nu'(F^*) = \mathbb{Z}$, което ще наричаме нормализирано.

Нека $\nu : F \to \mathbb{R} \cup \{\infty\}$ е произволно нормиране на функционално поле на една променлива, а r е произволно реално число от интервала $(0, 1)$. Изображението

$$\varphi : F \to \mathbb{R}^{\geq 0},$$

определено като

$$\varphi(x) = r^{\nu(x)}$$

определя норма на полето F. Така определената норма поражда метрика, която от своя страна задава топология върху F. Две нормирания са еквивалентни тогава и само тогава, когато задават една и съща топология. Накратко, основният момент в доказателството е съвпадението на отворените и затворените единични кълбета относно ν_1 и ν_2, които съвпадат, съответно с пръстените $\mathcal{O}_{\nu_1} = \mathcal{O}_{\nu_2}$ на тези дискретни нормирания и техните максимални идеали $\mathfrak{M}_{\nu_1} = \mathfrak{M}_{\nu_2}$.

2.1.2 Дискретност на нормиранията на функционално поле на една променлива

Изследвайки нормиранията на чисто трансцедентно разширение $k(x) \supset k$ достигаме до изключително интересния факт, че всички нормирания на произволно функционално поле на една променлива са дискретни. Преди всичко, да видим един основен пример, който по същество описва, с точност до еквивалентност, всички нормирания на чисто трансцедентното разширение $k(x) \supset k$.

Лема 14. *Нека $k(x) \supset k$ е чисто трансцедентно разширение на поле k чрез елемент x. Произволен неразложим над k полином $p(x) \in k[x]$ задава дискретно нормиране*

$$\nu_p : k(x) \to \mathbb{Z} \cup \{\infty\}$$

$$\nu_p\left(p(x)^m \frac{f(x)}{g(x)}\right) = m$$

$$\nu_p(0) = \infty$$

за полиноми $f(x), g(x) \in k[x]$, взаимно прости с $p(x)$ и цяло число m. Полиномът $p(x)$ е локален параметър на дискретното нормиране ν_p.

Изображението

$$\nu_\infty : k(x) \to \mathbb{Z} \cup \{\infty\}$$

$$\nu_\infty\left(\frac{f(x)}{g(x)}\right) = \deg(g) - \deg(f), f(x), g(x) \in k[x], g(x) \not\equiv 0$$

$$\nu_\infty(0) = \infty$$

определя дискретно нормиране, съответстващо на безкрайната точка. Рационалната функция $\frac{1}{x}$ е локален параметър на дискретното нормиране ν_∞.

Доказателство: Да означим с $Z(p)$ множеството на полиномите $f(x) \in k[x]$, взаимно прости с $p(x)$. Нека

$$R_p \coloneqq \left\{ p(x)^m \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in Z(p), g(x) \not\equiv 0, m \in \mathbb{Z}^{\geq 0} \right\} \cup \{0\}.$$

Проверката, че R_p е подпръстен в $k(x)$ е тривиална. По определение този подпръстен е пръстен на дискретно нормиране с локален параметър $p(x)$. За да установим този факт е достатъчно да проверим неразложимостта на $p(x)$ като елемент на R_p. Наистина, ако $p = g_1 g_2 = p^{m+n} f_1 f_2$ е разлагане на $p(x)$ и приемем без ограничение на общността, че $m \geq n$, то $m + n = 1$ и $m = 1$, $n = 0$, така че $p^n \frac{f_2}{g_2} = \frac{f_2}{g_2} \in R_p^*$ и p е неразложим.

Пръстенът R_p съдържа основното поле k и има поле от частни $k(x)$. Така, съгласно твърдение 9, дискретното нормиране, отговарящо на пръстена на дискретно нормиране R_p е точно, определеното по-горе дискретно нормиране ν_p.

Нека сега разгледаме изображението ν_∞. За целта ще използваме автоморфизма $\varphi(x) : k(x) \to k(x)$, действащ тъждествено върху k и определен по правилото

$$\varphi\left(\frac{f(x)}{g(x)}\right) = \frac{f(\frac{1}{x})}{g(\frac{1}{x})}.$$

Така, композицията $\nu_x \varphi$ съвпада с определеното по-горе изображение ν_∞, откъдето $\nu_\infty \equiv \nu_x \varphi$ е дискретно нормиране с локален параметър $\varphi(x) = \frac{1}{x}$. Непосредствено се проверява, че композицията на дискретно нормиране с автоморфизъм от групата на Галоа на $Gal(k(x)/k)$ е също дискретно нормиране.

□

Теорема 15. *Всяко нормиране на чисто трансцедентно разширение $k(x) \supset k$ е еквивалентно на нормиране ν_p съответстващо на неразложим над k полином $p(x) \in k[x]$ или на нормирането ν_∞. В частност всяко нормиране на чисто трансцедентно разширение е дискретно.*

Доказателство: Нека ν е произволно нормиране на чисто трансцедентното разширение $k(x) \supset k$. За стойността $\nu(x)$ на елемента x под действието на нормирането ν имаме две възможности, а именно $\nu(x) \geq 0$, или $\nu(x) < 0$. Да разгледаме първо случая $\nu(x) \geq 0$. При тази ситуация $x \in \mathcal{O}_\nu$ и понеже $k \subset \mathcal{O}_\nu$ имаме включването $k[x] \subseteq \mathcal{O}_\nu$, където $\mathcal{O}_\nu$ е пръстенът на нормирането ν. По-нататък, да разгледаме множеството $J \coloneqq \mathfrak{M}_\nu \cap k[x]$. Това множество е собствен идеал в $k[x]$, понеже очевидно $1_k \notin J$. Фактор-пръстенът

$$k[x]/J = k[x]/(k[x] \cap \mathfrak{M}_\nu) \simeq (k[x] + \mathfrak{M}_\nu)/\mathfrak{M}_\nu$$

няма делители на нулата, понеже е подпръстен на полето $\mathcal{O}_\nu/\mathfrak{M}_\nu$, откъдето следва простотата на идеала J. Всички идеали в $k[x]$ са главни и от простотата на идеала J, получаваме съществуването на неразложим над k полином $p(x) \in k[x]$, пораждащ идеаа J, т.е. $J = \langle p(x) \rangle$.

Ако $f(x) \in k[x]$ не се дели на $p(x)$, то $f(x) \notin \langle p(x) \rangle = J \subset \mathfrak{M}_\nu$, откъдето $\nu(f(x)) = 0$. Да разгледаме сега произволна рационална функция $h(x) \in k(x)$, представена във вида

$$p(x)^m \frac{f(x)}{g(x)}$$

за някакви полиноми $f(x), g(x) \in k[x], g(x) \not\equiv 0$, неделящи се на $p(x)$ и някакво цяло число m. Съгласно аксиомите за нормиране, имаме $\nu(h(x)) = m\nu(p(x))$. Вземайки предвид, че образът на рационалната функция $h(x)$ под действието на дискретното нормиране ν_p, съответстващо на неразложимия над k полином $p(x)$ е точно $\nu_p(h(x)) = m$, получаваме еквивалентността на нормиранията ν и ν_p, посредством положителната реална константа $\nu(p(x))$.

За $\nu(x) < 0$ използваме, че $\nu(x^{-1}) \geq 0$ и композицията на нормирането ν с автоморфизма $x \mapsto \frac{1}{x}$ е нормиране, еквивалентно на ν_∞. □

След като се убедихме, че всички нормирания на функционалното поле $k(x)$ на проективната права са дискретни, ще видим, че това свойство е в сила за произволно функционално поле на една променлива.

Теорема 16. *Всяко нормиране на функционално поле на една променлива $F \supset k$ е дискретно.*

Доказателство: Нека $\nu : F \to \mathbb{R} \cup \{\infty\}$ е произволно нормиране на функционалното поле на една променлива $F \supset k$, а $x \in F$ е трансцедентен над k елемент, за който $[F : k(x)] < \infty$. За да докажем дискретността на нормирането ν използваме, че всички нормирания на $k(x)$ са дискретни. Да означим с ξ ограничението на ν върху $k(x)$, т.е. $\xi := \nu \mid_{k(x)}$. Доказателството на теоремата се основава на това, че индексът на подгрупата $\xi(k(x)^*)$ в $\nu(F^*)$ е краен и не надминава степента $[F : k(x)]$ на разширението $F \supset k(x)$. За да докажем този факт ще проверим, че елементите $x_1, x_2, \ldots, x_m \in F^*$ са линейно независими над k, стига образите им $\nu(x_1), \nu(x_2), \ldots, \nu(x_m)$ под действието на ν да са представители на различни съседни класове относно $\xi(k(x^*)$. Да допуснем противното, т.е., че $x_1, x_2, \ldots, x_m \in F^*$ са линейно зависими над $k(x)$, но образите им $\nu(x_1), \nu(x_2), \ldots, \nu(x_m)$ задават различни съседни класове относно подгрупата $\xi(k(x^*))$. Тогава съществуват пермутация на числата от 1 до m, естествено число $1 < l \leq m$ и ненулеви елементи $c_1, c_2, \ldots, c_l \in k(x)^*$, изпълняващи равенството

$$\sum_{i=1}^{l} c_i x_i = 0.$$

Действайки с ν върху това равенство получаваме

$$\nu\left(\sum_{i=1}^{l} c_i x_i\right) = \nu(0) = \infty.$$

Елементите $\nu(c_i x_i) = \xi(c_i) + \nu(x_i)$ са два по два различни, защото $\nu(x_i)$ задават различни съседни класове относно $\xi(k(x^*))$. Използвайки неравенството на триъгълника

с равенство получаваме

$$\min\{\xi(c_i)+\nu(x_i)|1\le i\le l\}=\infty\Leftrightarrow\xi(c_i)+\nu(x_i)=\infty,$$

за някое $1\le i\le l$, което е противоречие, съгласно $c_i\neq 0$ и $x_i\neq 0$.

Защо ни беше необходимо да проверим, че неравенството

$$\mid\nu(F^*):\xi(k(x)^*)\mid\le[F:k(x)]<\infty$$

е изпълнено? Преди всичко, оттук следва, че $\xi(k(x))\neq\{0\}$ (в противен случай, индексът би бил безкраен, заради безкрайността на групата $\nu(F^*)\simeq(\mathbb{Z},+)$), което е достатъчно да твърдим, че $\xi: k(x)\to\mathbb{R}\cup\{\infty\}$) е нормиране на $k(x)$. Освен това, образът $\xi(k(x)^*)=d\mathbb{Z}, d\in\mathbb{R}^{>0}$ на $k(x)^*$ под действие на ξ е дискретна подгрупа на $(\mathbb{R},+)$. Ако $\mid\nu(F^*):\xi(k(x)^*)\mid=n$, то $n\nu(F^*)\subseteq\xi(k(x)^*)\subseteq\nu(F^*)$ и

$$d\mathbb{Z}=\xi(k(x)^*)\subseteq\nu(F^*)\subseteq\frac{1}{n}\xi(k(x)^*)=\frac{d}{n}\mathbb{Z}.$$

Фактор групата $\left(\frac{d}{n}\mathbb{Z}\right)/d\mathbb{Z}$ е от ред n, така че от $\mid\nu(F^*):d\mathbb{Z}\mid=\mid\frac{d}{n}\mathbb{Z}:d\mathbb{Z}\mid$ и $d\mathbb{Z}\subseteq\nu(F^*)\subseteq\frac{d}{n}\mathbb{Z}$ следва $\nu(F^*)=\frac{d}{n}\mathbb{Z}$. Така нормирането ν е дискретно, което завършва доказателството. □

Една важна характеристика на всяко нормиране на функционално поле на една променлива е неговата степен. За да опишем това понятие се нуждаем от някои формулировки и твърдения.

Определение 17. *Нека $\nu: F\to\mathbb{R}\cup\{\infty\}$ е нормиране на функционално поле на една променлива,*

$$\mathcal{O}_\nu:=\{x\mid x\in F,\nu(x)\ge 0\}$$

е пръстенът на нормирането ν, а

$$\mathfrak{M}_\nu:=\{x\mid x\in F,\nu(x)>0\}$$

е съответният му максимален идеал. Полето $\mathcal{O}_\nu/\mathcal{M}_\nu$ наричаме поле от остатъци на нормирането ν.

Твърдение 18. *Нека $\nu: k(x)\to\mathbb{R}\cup\{\infty\}$ е произволно нормиране на чисто трансцедентно разширение $k(x)\supset k$. Ако нормирането ν е еквивалентно на нормиране ν_p, съответстващо на неразложим над k, полином $p(x)\in k[x]$ то полето от остатъци на нормирането ν е изоморфно на $k[x]/\langle p(x)\rangle$. Полето от остатъци на нормиране ν, еквивалентно на ν_∞ е $\mathcal{O}_\nu/\mathfrak{M}_\nu\simeq k$.*

Доказателство: Вече споменахме, че

$$\mathcal{O}_{\nu_p}=\left\{p(x)^m\frac{f(x)}{g(x)}\middle| f(x),g(x)\in k[x],g(x)\not\equiv 0,p(x)\not| f(x),g(x),m\in\mathbb{Z}^{\ge 0}\right\}.$$

За произволен корен α на $p(x)$ в подходящо разширение на k, разглеждаме остойностяващото изображение

$$\varepsilon_\alpha : \mathcal{O}_{\nu_p} \longrightarrow k(\alpha) = k[\alpha],$$

определено по правилото

$$\varepsilon_\alpha \left(p(x)^m \frac{f(x)}{g(x)} \right) = p(\alpha)^m \frac{f(\alpha)}{g(\alpha)}$$

Непосредствено се проверява, че това е хомоморфизъм на пръстени с ядро $\mathfrak{M}_{\nu_p}$, откъдето, съгласно теоремата за хомоморфизмите на пръстени,

$$\mathcal{O}_{\nu_p}/\mathfrak{M}_{\nu_p} \simeq k(\alpha) = k[\alpha].$$

От друга страна, разглеждането остойностяващото изображение

$$\varepsilon_\alpha^{'} : k[x] \to k[\alpha] = k(\alpha),$$

с образ $k[\alpha]$ и ядро $\langle p(x) \rangle$ дава

$$k[x]/\langle p(x) \rangle \simeq k[\alpha] = k(\alpha) \simeq \mathcal{O}_{\nu_p}/\mathfrak{M}_{\nu_p}$$

Вземайки предвид горните разсъждения и факта, че нормирането ν_∞ съвпада с композицията $\nu_x \varphi$ на автоморфизма $\varphi : k(x) \to k(x)$ с $\varphi(x) = \frac{1}{x}$, $\varphi|_k = \mathrm{Id}_k$ и нормирането ν_x, стигаме до извода, че

$$\mathcal{O}_{\nu_\infty}/\mathfrak{M}_{\nu_\infty} = \varphi^{-1}(\mathcal{O}_x/\mathfrak{M}_x) \simeq \mathcal{O}_x/\mathfrak{M}_x \simeq k[x]/\langle x \rangle \simeq k.$$

□

Теорема 19. *Нека $\nu : F \to \mathbb{R} \cup \{\infty\}$ е нормиране на функционално поле на една променлива $F \supset k$. Тогава полето от остатъци $\mathcal{O}_\nu/\mathcal{M}_\nu$ е крайно разширение на k.*

Доказателство: Нека $x \in F$ е трансцедентен над k елемент, за който $[F : k(x)] < \infty$, а $\xi : k(x) \to \mathbb{R} \cup \{\infty\}$ е ограничението $\nu|_{k(x)}$. Както видяхме, ξ е нормиране на $k(x)$ и полето от остатъци $\mathcal{O}_\xi/\mathfrak{M}_\xi$ е крайно разширение на k. Достатъчно е да докажем, че

$$[\mathcal{O}_\nu/\mathfrak{M}_\nu : \mathcal{O}_\xi/\mathfrak{M}_\xi] \leq [F : k(x)] < \infty.$$

За целта ще проверим, че ако $z_1 + \mathfrak{M}_\nu, z_2 + \mathfrak{M}_\nu, \ldots, z_m + \mathfrak{M}_\nu$ са линейно независими над $\mathcal{O}_\xi/\mathfrak{M}_\xi$, то и $z_1, z_2, \ldots, z_m$ са линейно независими над $k(x)$. Да допуснем противното, т.е.

$$\sum_{i=1}^{m} c_i z_i = 0, \quad c_i \in k(x).$$

Нека за подходяща премутация на числата от 1 до m и подходящо $1 < l \leq m$ е изпълнено

$$\sum_{i=1}^{l} c_i z_i = 0, \quad c_i \in k(x)^*,$$

като $\xi(c_1) = min\{\xi(c_i)|1 \leq i \leq l\}$. Умножавайки почленно с c_1^{-1} и редуцирайки двете страни на равенството по модул $\mathfrak{M}_\nu$ получаваме

$$z_1 + \mathfrak{M}_\nu + \sum_{i=2}^{l}(c_i c_1^{-1} + \mathfrak{M}_\xi)(z_i + \mathfrak{M}_\nu) = 0.$$

Съгласно $\xi(c_i c_1^{-1}) = \xi(c_i) - \xi(c_1^{-1}) \geq 0$, елементите $c_i c_1^{-1} \in k(x)$ са от пръстена на дискретно нормиране $\mathcal{O}_\xi$. Така $c_i c_1^{-1} + \mathfrak{M}_\xi \in \mathcal{O}_\xi/\mathfrak{M}_\xi$ и следователно $z_1 + \mathfrak{M}_\nu, z_2 + \mathfrak{M}_\nu, \ldots, z_m + \mathfrak{M}_\nu$ са линейно зависими над $\mathcal{O}_\xi/\mathfrak{M}_\xi$. Достигнатото противоречие доказва неравенството

$$[\mathcal{O}_\nu/\mathfrak{M}_n u : \mathcal{O}_\xi/\mathfrak{M}_\xi] \leq [F : k(x)] < \infty,$$

а с това и твърдението на теоремата. □

Определение 20. *Степента $[\mathcal{O}_\nu/\mathcal{M}_\nu : k] = n$ наричаме степен на нормирането ν или на класа на еквивалентност на нормирането ν. Нормированията от степен 1 и техните класовете на еквивалентност се наричат рационални.*

За да докажем Апроксимационната теорема са ни нужни няколко леми.

Лема 21. *(Отделимост на два класа дискретни нормирания) Нека F е функционално поле на една променлива с поле от константи k, а ν_1, ν_2 са неекивалентни дискретни нормирания на F. Тогава съществува такъв елемент $w \in F$, че $\nu_1(w) > 0$ и $\nu_2(w) \leq 0$.*

Доказателство: Без ограничение на общността можем да считаме, че нормированията ν_1 и ν_2 са нормализирани, т.е. $\nu_1(F^*) = \nu_2(F^*) = \mathbb{Z}$. Избираме $t \in F^*$, $\nu_2(t) = 1$, така че $\nu_2(F^*) = \mathbb{Z}$ се поражда от $\nu_2(t)$ и t е локален параметър на ν_2. Ако допуснем, че съществува $u \in F$, такъв че $\nu_2(u) = 0$, а $\nu_1(u) \neq 0$, то един от елементите u и u^{-1} удовлетворява условията на лемата.

Оттук нататък ще предполагаме, че ако $\nu_2(u) = 0$, то и $\nu_1(u) = 0$, т.е. $\mathcal{O}_{\nu_2}^* \subset \mathcal{O}_{\nu_1}^*$. За произволен елемент $z \in F^*$ с $\nu_2(z) = m$ съществува елемент $u = zt^{-m}$, такъв че $\nu_2(u) = 0$. Тогава $0 = \nu_1(u) = \nu_1(z) - m\nu_1(t)$, или

$$\nu_1(z) = \nu_2(z)\nu_1(t).$$

Оттук $\nu_1(t) < 0$ и t^{-1} удовлетворява условията на лемата. □

Лема 22. *(Ненулева отделимост на два класа дискретни нормирания) Нека F е функционално поле на една променлива с поле от константи k. Тогава съществува елемент $w \in F$, за който $\nu_1(w) < 0$ и $\nu_2(w) > 0$.*

Доказателство: Съгласно предходната лема съществуват елементи $w_1, w_2 \in F$, такива че $\nu_1(w_1) > 0, \nu_2(w_1) \leq 0$ и $\nu_1(w_2) \leq 0, \nu_2(w_2) > 0$ и елементът $w_1 w_2^{-1}$ удовлетворява условията. □

Лема 23. *(Ненулева отделимост на произволен краен брой дискретни нормирания) Нека F е функционално поле на една променлива с поле то константи k, а $\nu_1, \nu_2, \ldots, \nu_n$ са две по две неекивалентни дискретни нормирания на F. Тогава съществува $w \in F$, такъв че $\nu_1(w) > 0$ и $\nu_i(w) < 0$ за $2 \leq i \leq n$.*

Доказателство: Доказателството е индуктивно, като основният момент е конструирането на елемент $w = w_1 + w_2^r$ за естествено число r, такова че $\nu_i(w_1) \neq r\nu_i(w_2)$, $\forall i, 1 \leq i \leq n$. Елементът w отговаря на необходимите условия. □

Теорема 24. *(Апроксимационна теорема) Нека F е функционално поле на една променлива с поле от константи k, $w_1, w_2, \ldots, w_n$ са елементи от F, $\nu_1, \nu_2, \ldots, \nu_n$ са две по две неекивалентни дискретни нормирания, а $m_1, m_2, \ldots, m_n$ са цели числа. Тогава съществува елемент $z \in F$, такъв че $\nu_i(z - w_i) = m_i, \quad \forall \quad i, \quad 1 \leq i \leq n$.*

Доказателство: (Слаб вариант - частен случай) Твърдим, че съществува $x \in F$, такъв че $\nu_1(x-1) > m_1, \nu_2(x) > m_2, \ldots, \nu_n(x) > m_n$. Съгласно лемата за строга отделимост на n класа неекивалентни нормирания, можем да изберем елемент $w \in F$, за който $\nu_1(w) > 0$ и $\nu_2(w) < 0, \ldots, \nu_n(w) < 0$. Използвайки свойствата на дискретните нормирания установяваме, че за произволно естествено число

$$s > \max\left(\frac{m_1}{\nu_1(w)}, \quad \frac{m_i}{-\nu_i(w)} \quad \middle| \quad 2 \leq i \leq n\right)$$

елементът $x = \frac{1}{1+w^s}$ е такъв, че $\nu_1(x-1) > m_1, \nu_2(x) > m_2, \ldots, \nu_n(x) > m_n$.

(Слаб вариант общ случай) Твърдим, че съществува елемент $y \in F$, за който $\nu_i(y - w_i) > m_i$. Избираме $b \in \mathbb{Z}$, така че $\nu_i(w_j) > b, \quad \forall i, j, 1 \leq i, j \leq n$. Полагаме $d_i = m_i - b$ и за всяко $i, 1 \leq i \leq n$ прилагаме частния случай на слабия вариант за елементите $w_1 = 0, w_2 = 0, \ldots, w_{i-1} = 0, w_i = 1, w_{i+1} = 0, \ldots, w_n = 0$. Получаваме елементи $x_i \in F$, такива че $\nu_i(x_i - 1) > d_i$ и $\nu_j(x_i) > d_j, \ \forall j \neq i$. Елементът $y = \sum_{i=1}^{n} w_i x_i$ изпълнява необходимите свойства.

(Силен вариант - общ случай) Нека елементите $t_i \in F$ са локални параметри на $\mathcal{O}_{\nu_i}$ със свойството $\nu_i(t_i) = 1$ и да положим $u_i = t_i^m$. Прилагайки общия случай на слабия вариант към елементите $w_i + u_i$, получаваме елемент $z \in F$, за който

$$\nu_i(z - (w_i + u_i)) > m_i.$$

Посредством неравенството на триъгълника с равенство установяваме, че z удовлетворява условията на Теоремата. □

Като непосредствено следствие от Апроксимационната теорема получаваме развитието на елементите на функционално поле на една променлива в Лоранов ред относно локален параметър на дискретно нормиране.

Твърдение 25. *Нека F е функционално поле на една променлива с поле от константи k, а t е локален параметър на нормализирано дискретно нормиране ν. Тогава всеки елемент $z \in F$ се развива в Лоранов ред*

$$z = \sum_{j=r}^{\infty} a_j t^j \quad c \quad r = \nu(z)$$

и коефициенти a_j от алгебричната обвивка $\overline{k}$ на k, $a_r \neq 0$.

Доказателство: Полето от остатъци $\mathcal{O}_\nu/\mathfrak{M}_\nu$ е крайно разширение на k и можем да считаме, че се съдържа в алгебричната обвивка $\overline{k}$ на k.

Ако $\nu(z) = r$, то $\nu(zt^{-r}) = 0$, така че $zt^{-r} \in \mathcal{O}_\nu^*$. Да означим

$$a_r \coloneqq zt^{-r} + \mathfrak{M}_\nu \in (\mathcal{O}_\nu/\mathfrak{M}_\nu)^* \subset \overline{k}^*.$$

Разликата $zt^{-r} - a_r \in \mathfrak{M}_\nu = \langle t \rangle$, откъдето $\nu(z - a_r t^r) \geq r + 1$ и елементът

$$zt^{-r-1} - a_r t^{-1} \in \mathcal{O}_\nu$$

е регулярен.

С индукция по $m \geq r$, нека $\nu\left(z - \sum_{j=r}^{m} a_j t^j\right) \geq m + 1$. Тогава

$$zt^{-m-1} - \sum_{j=r}^{m} a_j t^{j-m-1} \in \mathcal{O}_\nu$$

и избираме

$$a_{m+1} = zt^{-m-1} - \sum_{j=r}^{m} a_j t^{j-m-1} + \mathfrak{M}_\nu \in \mathcal{O}_\nu/\mathfrak{M}_\nu \subset \overline{k}.$$

Разликата $zt^{-m-1} - \sum_{j=r}^{m} a_j t^{j-m-1} - a_{m+1} \in \mathfrak{M}_\nu = \langle t \rangle$, откъдето

$$\nu\left(z - \sum_{j=r}^{m+1} a_j t^j\right) \geq m + 2.$$

Продължавайки по същия начин достигаме до разлагане $z = \sum_{j=r}^{\infty} a_j t^j$ на $z \in F$ във формален степенен ред на локалния параметър t на ν.

□

2.2 Действие на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ върху афинни и проективни многообразия

Да забележим, че всяко крайно поле $\mathbb{F}_q$ е съвършено, защото произволно крайно разширение $\mathbb{F}_{q^m} \supset \mathbb{F}_q$ на $\mathbb{F}_q$ е сепарабелно. Сепарабелната обвивка $\mathbb{F}_q^{\text{sep}} = \overline{\mathbb{F}_q}$ на $\mathbb{F}_q$ съвпада с алгебричната обвивка $\overline{\mathbb{F}_q}$. Абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \varprojlim Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$ е проективната граница на крайните групи на Галоа

$$Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \Phi_q \rangle = \{\Phi_q^i \,|\, 0 \leq i \leq m-1\},$$

породени от автоморфизма на Фробениус $\Phi_q : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$, $\Phi_q(a) = a^q$ за $\forall a \in \overline{\mathbb{F}_q}$. Поточно,

$$\mathfrak{G} = \left\{ \left(\Phi_q^{l_m (\mathrm{mod}\, m)}\right)_{m\in\mathbb{N}} \in \prod_{m=1}^{\infty} (\mathbb{Z}_m, +) \,\middle|\, l_n \equiv l_m (\mathrm{mod}\, m) \text{ за } m/n \right\}$$

е про-крайната обвивка $\mathfrak{G} = \widehat{\langle \Phi_q \rangle} \simeq (\widehat{\mathbb{Z}}, +)$ на безкрайната циклична група $\langle \Phi_q \rangle \simeq (\mathbb{Z}, +)$.

Множеството

$$\overline{\mathbb{F}_q}^{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)} = \mathbb{F}_q$$

на фиксираните точки на абсолютната група на Galois $Gal(\mathbb{F}_q^{\text{sep}}/\mathbb{F}_q) = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ се изчерпва от $\mathbb{F}_q$. Наистина, нека $a \in \overline{\mathbb{F}_q}^{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}$ има минимален полином $f_a(x) \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$ над $\mathbb{F}_q$ от степен $\deg(f_a) = n$. Полето на разлагане $E = \mathbb{F}_q(a = a_1, \ldots, a_n) \supseteq \mathbb{F}_q$ на $f_a(x)$ над $\mathbb{F}_q$ е крайно разширение на Galois на $\mathbb{F}_q$, съдържащо a. Ограничението $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)|_E$ на абсолютната група на Galois върху E съвпада с групата на Galois $Gal(E/\mathbb{F}_q)$ на E над $\mathbb{F}_q$. Фиксираните точки $E^{Gal(E/\mathbb{F}_q)} = \mathbb{F}_q$ на групата на Galois на E над $\mathbb{F}_q$ се изчерпват от $\mathbb{F}_q$, така че

$$a \in E^{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)} = E^{Gal(E/\mathbb{F}_q)} = \mathbb{F}_q.$$

2.2.1 $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-действие върху афинно пространство и афинно многообразие

Нека $\overline{\mathbb{F}_q}^n$ е n-мерното афинно пространство над алгебричната обвивка $\overline{\mathbb{F}_q}$ на крайно поле $\mathbb{F}_q$. Точките $a \in \mathbb{F}_q^n \subset \overline{\mathbb{F}_q}^n$ се наричат $\mathbb{F}_q$-рационални. Абсолютната група на Galois $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ действа покомпонентно върху $\overline{\mathbb{F}_q}^n$ по правилото

$$\varphi(a_1, \ldots, a_n) = (\varphi(a_1), \ldots, \varphi(a_n)) \quad \text{за} \quad \forall \varphi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q), \;\; \forall a_i \in \overline{\mathbb{F}_q}.$$

Оттук следва, че $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-фиксираните точки на афинното пространство $\overline{\mathbb{F}_q}^n$ са $\mathbb{F}_q$-рационалните,

$$(\overline{\mathbb{F}_q}^n)^{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)} = \mathbb{F}_q^n.$$

По-точно, ако $a = (a_1, \ldots, a_n) \in (\overline{\mathbb{F}_q}^n)^{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}$, то $\varphi(a_i) = a_i$ за всички $1 \leq i \leq n$ и $a_i \in \mathbb{F}_q$ за всички $1 \leq i \leq n$.

Ако $a = (a_1, \ldots, a_n) \in \overline{\mathbb{F}_q}^n$ и $F \supset \mathbb{F}_q$ е крайно разширение на Galois, съдържащо $\mathbb{F}_q(a_1, \ldots, a_n)$, то хомоморфизмът на ограничение $\mathrm{rest}_F : Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to Gal(F/\mathbb{F}_q)$ е епиморфизъм и орбитите

$$Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a) = Orb_{Gal(F/\mathbb{F}_q)}(a)$$

съвпадат, защото $a \in F^n$ и $\varphi(a) = \mathrm{rest}_F(\varphi)(a)$ за $\forall \varphi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. В частност, ако $a \in \overline{\mathbb{F}_q}$, то спрегнатите на $a \in F$ над $\mathbb{F}_q$ образуват орбитата

$$Orb_{Gal(F/\mathbb{F}_q)}(a) = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a).$$

Определение 26. *Дефиниционното поле на точка $a \in \overline{\mathbb{F}_q}^n$ над $\mathbb{F}_q$ е разширението $\mathbb{F}_q(a_1, \ldots, a_n) \supseteq \mathbb{F}_q$ на $\mathbb{F}_q$ чрез компонентите $a_1, \ldots, a_n \in \overline{\mathbb{F}_q}$ на $a = (a_1, \ldots, a_n)$.*

Лема-Определение 27. *Дефиниционното поле на точка*

$$a = (a_1, \ldots, a_n) \in \overline{\mathbb{F}_q}^n$$

над $\mathbb{F}_q$ съвпада с дефиниционното поле на нейния образ

$$\varphi(a) = (\varphi(a_1), \ldots, \varphi(a_n)) \in \overline{\mathbb{F}_q}^n$$

под действие на произволен автоморфизъм $\varphi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ от абсолютната група на Галоа на $\mathbb{F}_q$.

Определяме дефиниционното поле на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита като дефиниционното поле $\mathbb{F}_q(a_1, \ldots, a_n)$ на произволен неин елемент над $\mathbb{F}_q$.

Доказателство: Да забележим, че за произволен елемент $\varphi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ полето

$$\mathbb{F}_q(\varphi(a_1), \ldots, \varphi(a_n)) = \varphi(\mathbb{F}_q(a_1, \ldots, a_n)) = \varphi(L)$$

е образът на $L = \mathbb{F}_q(a_1, \ldots, a_n)$ под действие на φ. Крайното разширение $L \supseteq \mathbb{F}_q$ на крайното поле $\mathbb{F}_q$ е сепарабелно и нормално, т.е. разширение на Galois. Ограничението $\varphi|_L$ на $\varphi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ върху L принадлежи на групата на Galois $Gal(L/\mathbb{F}_q)$ и $\varphi(L) = L$.

□

Твърдение-Определение 28. *(i) Всяка $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита*

$$P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a), \quad a \in \overline{\mathbb{F}_q}^n$$

е крайно множество.

Броят на елементите на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита P се нарича степен на P и се бележи с $\deg(P)$.

(ii) Степента на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$, $a = (a_1, \ldots, a_n) \in \overline{\mathbb{F}_q}^n$ е минималното естествено число m, за което $\mathbb{F}_{q^m}$ съдържа компонентите $a_1, \ldots, a_n$ на a.

(iii) Степента на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$, $a = (a_1, \ldots, a_n) \in \overline{\mathbb{F}_q}^n$ е минималното естествено число m, за което автоморфизмът на Frobenius Φ_{q^m} оставя на място a, $\Phi_{q^m}(a) = a$.

(iv) Степента m на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$, $a = (a_1, \ldots, a_n) \in \overline{\mathbb{F}_q}^n$ съвпада със степента $[\mathbb{F}_q(a_1, \ldots, a_n) : \mathbb{F}_q]$ на дефиниционното поле на P над $\mathbb{F}_q$.

Доказателство: Нека m е минималното естествено число, за което $\mathbb{F}_{q^m}$ съдържа всички компоненти $a_1, \ldots, a_n$ на точката $a = (a_1, \ldots, a_n)$. Доказахме, че $\mathbb{F}_{q^m} \supseteq \mathbb{F}_q$ е крайно разширение на Galois, така че ограничението

$$Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)|_{\mathbb{F}_{q^m}} = Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \Phi_q \rangle \simeq (\mathbb{Z}_m, +)$$

на абсолютната група на Galois на $\mathbb{F}_q$ върху $\mathbb{F}_{q^m}$ съвпада с групата на Galois на $\mathbb{F}_{q^m}$ относно $\mathbb{F}_q$. Оттук, $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитата

$$Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a) = Orb_{Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)}(a) = \{a, \Phi_q(a), \ldots, \Phi_{q^{m-1}}(a)\}$$

съвпада с орбитата на точката a под действие на цикличната група от ред m, породена от автоморфизма на Frobenius Φ_q, действащ по правилото $\Phi_q(x) = (x_1^q, \ldots, x_n^q)$ за всяка точка $x \in \overline{\mathbb{F}_q}^n$. Това доказва, че $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитата $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ е крайно множество. Броят на елементите на $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ е равен на m, защото в противен случай съществува $0 \leq j \leq m-1$ с $\Phi_{q^j}(a) = a$. Следователно всички компоненти a_i на a са корени на полинома $x^{q^j} - x = 0$ за $\forall 1 \leq i \leq n$ и $a_1, \ldots, a_n \in \mathbb{F}_{q^j}$. Това противоречи на избора на m и доказва, че $|Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)| = m$. Междувременно доказахме, че степента m на $\mathbb{F}_q$-затворената точка съвпада с минималното естествено число, за което $\Phi_{q^m}(a) = a$.

От $a_1, \ldots, a_n \in \mathbb{F}_{q^m}$ и $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ следва, че дефиниционното поле $\mathbb{F}_q(a_1, \ldots, a_n)$ на a над $\mathbb{F}_q$ се съдържа в $\mathbb{F}_{q^m}$. Ако $\mathbb{F}_q(a_1, \ldots, a_n) = \mathbb{F}_{q^s} \subseteq \mathbb{F}_{q^m}$, то s дели m и $s \leq m$. Съгласно минималността на m имаме $s = m$ и $\mathbb{F}_q(a_1, \ldots, a_n) = \mathbb{F}_{q^s} = \mathbb{F}_{q^m}$.

□

Твърдение 29. *Нека $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$, $a = (a_1, \ldots, a_n) \in \overline{\mathbb{F}_q}^n$ е $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита от степен $m \in \mathbb{N}$, r е естествено число, а $d = GCD(m, r) \in \mathbb{N}$ е естественият най-голям общ делител на m и r. Тогава P се разлага в непресичащо се обединение*

$$P = \cup_{j=1}^{d} P_j \tag{2.1}$$

на d на брой $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})$-орбити P_j от степен $\deg(P_j) = \frac{m}{d}$.

В частност, $P = \cup_{j=1}^{m} P_j$ се разлага в непресичащо се обединение на m на брой $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})$-орбити от степен 1 точно когато m дели r.

Доказателство: Да отбележим, че алгебричната обвивка $\overline{\mathbb{F}_{q^r}} = \overline{\mathbb{F}_q}$ на $\mathbb{F}_{q^r}$ съвпада с алгебричната обвивка на $\mathbb{F}_q$. От една страна, всеки елемент $\alpha \in \overline{\mathbb{F}_q}$ е алгебричен над $\mathbb{F}_q$. Следователно α е алгебричен над $\mathbb{F}_{q^r}$ и $\alpha \in \overline{\mathbb{F}_{q^r}}$. Това доказва, че $\overline{\mathbb{F}_q} \subseteq \overline{\mathbb{F}_{q^r}}$. От друга страна, $\overline{\mathbb{F}_{q^r}} = \cup_{s=1}^{\infty} \mathbb{F}_{q^{rs}} \subseteq \cup_{t=1}^{\infty} \mathbb{F}_{q^t} \subseteq \overline{\mathbb{F}_q}$, откъдето

$$\overline{\mathbb{F}_{q^r}} = \overline{\mathbb{F}_q}.$$

Абсолютната група на Galois $Gal(\overline{\mathbb{F}_{q^r}}/\mathbb{F}_{q^r}) = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на $\mathbb{F}_{q^r}$ е подгрупа на абсолютната група на Galois $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на $\mathbb{F}_q$ и $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})$-орбитата $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})}(a)$ се съдържа в $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитата $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$. Съгласно Твърдение-Определение 28 (iv), степента

$$|Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})}(a)| = [\mathbb{F}_{q^r}(a_1, \ldots, a_n) : \mathbb{F}_{q^r}]$$

на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})$-орбитата на $a \in \overline{\mathbb{F}_q}^n$ съвпада със степента на дефиниционното поле на a над $\mathbb{F}_{q^r}$ спрямо $\mathbb{F}_{q^r}$. Твърдим, че

$$\mathbb{F}_{q^r}(a_1, \ldots, a_n) = \mathbb{F}_{q^\mu}$$

за естественото най-малко общо кратно $\mu = LCM(m, r) \in \mathbb{N}$ на m и r. От една страна, $\mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^\mu}$, защото r дели μ. От това, че m дели μ получаваме включването $\mathbb{F}_q(a_1, \ldots, a_n) = \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^\mu}$. Следователно $\mathbb{F}_{q^r}(a_1, \ldots, a_n) \subseteq \mathbb{F}_{q^\mu}$. Ако $\mathbb{F}_{q^r}(a_1, \ldots, a_n) = \mathbb{F}_{q^s}$ за някое естествено s, то s дели μ съгласно включването $\mathbb{F}_{q^s} \subseteq \mathbb{F}_{q^\mu}$. От друга страна, $\mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^r}(a_1, \ldots, a_n) = \mathbb{F}_{q^s}$ и

$$\mathbb{F}_{q^m} = \mathbb{F}_q(a_1, \ldots, a_n) \subseteq \mathbb{F}_{q^r}(a_1, \ldots, a_n) = \mathbb{F}_{q^s}$$

изискват r да дели s и m да дели s. Оттук, s е общо кратно на r и m, така че най-малкото общо кратно μ на r и m дели s. Естествените числа s и μ съвпадат, защото s дели μ и μ дели s. В резултат,

$$|Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)| = [\mathbb{F}_{q^\mu} : \mathbb{F}_{q^r}] = \frac{\mu}{r} = \frac{m}{d}$$

за естествения най-голям общ делител $d = GCD(m, r)$ на m и r. Това доказва, че произволна $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ от степен m се разлага в непресичащо се обединение на d на брой $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})$-орбити от степен $\frac{m}{d}$.

В частност, $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ се разлага в обединение на m на брой 1-елементни $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})$-орбити точно когато $d = m$. Последното е в сила тогава и само тогава, когато m дели r.

□

Сега ще въведем афинните алгебрични мнгообразия, определени над $\mathbb{F}_q$ и ще разгледаме действието на абсолютната група на Галоа $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на $\mathbb{F}_q$ върху тях.

Определение 30. *Ако $S \subseteq \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ е множество от полиноми на $x_1, \ldots, x_n$ с коефициенти от $\overline{\mathbb{F}_q}$, то множеството на общите нули*

$$Z(S) = \{a \in \overline{\mathbb{F}_q}^n \mid f(a) = 0 \quad за \quad \forall f \in S\}$$

на S в афинното пространство $\overline{\mathbb{F}_q}^n$ се нарича афинно многообразие.

Ако $S \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ е множество от полиноми с коефициенти от $\mathbb{F}_q$, казваме, че афинното алгебрично множество $Z(S)$ е определено над $\mathbb{F}_q$ и записваме $Z(S)/\mathbb{F}_q$.

Ако $Z(S)/\mathbb{F}_q$ е афинно алгебрично множество, определено над $\mathbb{F}_q$, то сечението

$$Z(S)(\mathbb{F}_q) := Z(S) \cap \mathbb{F}_q^n$$

се нарича множество на $\mathbb{F}_q$-рационалните точки на $Z(S)$.

Действието на $\varphi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ върху коефициентите на полином $f(x) \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ задава действие на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ върху $\overline{\mathbb{F}_q}[x_1, \ldots, x_n]$,

$$\varphi\left(\sum_{i=(i_1,\ldots,i_n)} a_i x_1^{i_1} \ldots x_n^{i_n}\right) = \sum_{i=(i_1,\ldots,i_n)} \varphi(a_i) x_1^{i_1} \ldots x_n^{i_n} \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n].$$

Полиномът $f(x_1, \ldots, x_n) \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ остава на място под действие на групата на Galois $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ тогава и само тогава, когато $f(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ е с коефициенти от $\mathbb{F}_q$.

Ако $f(x_1, \ldots, x_n) \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, $a = (a_1, \ldots, a_n) \in \overline{\mathbb{F}_q}^n$ и $\varphi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, то

$$\varphi(f(a_1, \ldots, a_n)) = \varphi\left(\sum_{i=(i_1,\ldots,i_n)} c_i a_1^{i_1} \ldots a_n^{i_n}\right) =$$

$$= \sum_{i=(i_1,\ldots,i_n)} \varphi(c_i)\varphi(a_1)^{i_1} \ldots \varphi(a_n)^{i_n} = \varphi(f)(\varphi(a)).$$

Ако $Z(S)/\mathbb{F}_q$ е афинно алгебрично множество, определено над $\mathbb{F}_q$, то абсолютната група на Galois $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ действа върху $Z(S)$ и фиксираните точки за това действие са $\mathbb{F}_q$-рационалните. Наистина, за всяко $a \in Z(S)$ и всяко $\varphi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ имаме $\varphi(a) \in Z(S)$, защото произволен полином $f \in S \subset \mathbb{F}_q[x_1, \ldots, x_n]$ има нулева стойност $f(a) = 0$ в a, откъдето $0 = \varphi(f(a)) = f(\varphi(a))$. Точката $a \in Z(S)$ остава на място под действие на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ точно когато $a \in \mathbb{F}_q^n$.

Оттук следва, че ако $Z(S)/\mathbb{F}_q$ е афинно алгебрично множество, определено над $\mathbb{F}_q$ и $a \in Z(S)$, то $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитата $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ върху $\overline{\mathbb{F}_q}^n$, породена от a се съдържа изцяло в $Z(S)$. Затова казваме, че $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ е $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита на $Z(S)$.

Определение 31. *Топологията върху $\overline{\mathbb{F}_q}^n$, чиито затворени подмножества $\mathcal{Z} = \{V(S)\}_{S \subseteq \overline{\mathbb{F}_q}[x_1,\ldots,x_n]}$ са афинните многообразия $Z(S) \subseteq \overline{\mathbb{F}_q}^n$ за произволни множества от полиноми $S \subseteq \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ се нарича топология на Зариски върху $\overline{\mathbb{F}_q}^n$.*

Определение 32. *Затворената обвивка $\overline{M}$ на подмножество M на топологично пространство X е сечението*

$$\overline{M} = \cap_{Z \supseteq M} Z$$

на всички затворени подмножества $Z \subseteq X$, съдържащи M.

Затворената обвивка $\overline{M}$ на M е минималното затворено подмножество на X, съдържащо M. Да отбележим, че подмножеството M е затворено тогава и само тогава, когато $M = \overline{M}$.

Лема 33. *Ако $M \subseteq \overline{\mathbb{F}_q}^n$ е подмножество на афинното пространство $\overline{\mathbb{F}_q}^n$, то Зариски затворената обвивка*

$$\overline{M} = ZI(M)$$

съвпада с афинното многообразие на идеала $I(M) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ на M.

В частност, ако $X \subseteq \overline{\mathbb{F}_q}^n$ е афинно многообразие, то $X = ZI(X)$.

Доказателство: По определение, всеки полином $f \in I(M)$ се анулира върху M, така че $M \subseteq ZI(M)$. Затвореното множество $ZI(M)$ участва в сечението $\cap_{Z \supseteq M} Z = \overline{M}$ и го съдържа, $ZI(M) \supseteq \overline{M}$.

За обратното включване $ZI(M) \subseteq \overline{M} = \cap_{Z \supseteq M} Z$ е достатъчно да проверим, че $ZI(M) \subseteq Z$ за всяко Зариски затворено подмножество $Z \subseteq \overline{\mathbb{F}_q}^n$, съдържащо M. По определение, $Z = Z(S)$ за някакво множество от полиноми $S \subseteq \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$. Условието $M \subseteq Z(S)$ означава анулиране на всички полиноми $f \in S$ в точките $a \in M$, $f(a) = 0$. Следователно $S \subseteq I(M)$, откъдето $Z = Z(S) \supseteq ZI(M)$.

□

Определение 34. *Непразното подмножество M на топологично пространство X е неприводимо, ако за всяко разлагане $M = M_1 \cup M_2$ в обединение на затворени подмножества $M_i \subseteq M$ относно индуцираната от X топология върху M е в сила $M = M_1$ или $M = M_2$.*

Лема 35. *Афинно многообразие $Z(S) \subseteq \overline{\mathbb{F}_q}^n$ е неприводимо тогава и само тогава, когато идеалът му $I(Z(S)) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ е прост.*

Доказателство: Да допуснем, че $X = Z(S) \subseteq \overline{\mathbb{F}_q}^n$ е неприводимо афинно многообразие, чийто идеал $I(X) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ не е прост. Тогава съществуват полиноми $f, g \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n] \setminus I(X)$ с $fg \in I(X)$. Съгласно Лема 33 имаме $X = ZI(X)$. Твърдим, че $Z(f) \not\supseteq ZI(X) = X$ и $Z(g) \not\supseteq ZI(X) = X$, защото предположението $Z(f) \supseteq X$ води до $f|_X = 0$, откъдето $f \in I(X)$, противно на избора на $f \notin I(X)$. От друга страна, $Z(fg) \supseteq ZI(X) = X$, съгласно $fg \in I(X)$. Вземаме предвид, че $Z(fg) = Z(f) \cup Z(g)$ и получаваме

$$X = Z(fg) \cap X = [Z(f) \cup Z(g)] \cap X = [Z(f) \cap X] \cup [Z(g) \cap X].$$

Подмножествата $Z(f) \cap X$ и $Z(g) \cap X$ на X са затворени и различни от X съгласно $X \nsubseteq Z(f)$, $X \nsubseteq Z(g)$. Това противоречи на неприводимостта на X и доказва простотата на идеала на неприводимо афинно алгебрично множество.

Обратно, нека $X = Z(S) \subseteq \overline{\mathbb{F}_q}^n$ е афинно многообразие с прост идеал $I(X) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ и $X = Z_1 \cup Z_2$ за затворени $Z_i \subsetneq X$. Тогава

$$I(X) = I(Z_1 \cup Z_2) = I(Z_1) \cap I(Z_2).$$

От $Z_i \subseteq X$ следва $I(Z_i) \supseteq I(X)$. Допускането $I(X) = I(Z_i)$ и прилагането на Лема 33 водят до $X = ZI(X) = ZI(Z_i) = Z_i$, противно на предположението $Z_i \subsetneq X$. Това доказва $I(Z_i) \supsetneq I(X)$ за $1 \leq i \leq 2$. Избираме полиноми $f_i \in I(Z_i) \setminus I(X)$ и забелязваме, че

$$f_1 f_2 \in I(Z_1) I(Z_2) \subseteq I(Z_i) \cap I(Z_2) = I(X).$$

Това противоречи на простотата на идеала $I(X)$ и доказва неприводимостта на афинните многообразия $X = Z(S)$ с прост идеал $I(X)$.

□

Определение 36. *Ако $Z \subset \overline{\mathbb{F}_q}^n$ е афинно многообразие с идеал $I(Z) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, то фактор-пръстенът*

$$\overline{\mathbb{F}_q}[Z] = \overline{\mathbb{F}_q}[x_1, \ldots, x_n]/I(Z)$$

се нарича афинен координатен пръстен на Z.

Ако $Z/\mathbb{F}_q \subset \overline{k}^n$ е афинно многообразие, определено над $\mathbb{F}_q$, то фактор-пръстенът

$$\mathbb{F}_q[Z] = \mathbb{F}_q[x_1, \ldots, x_n]/I_{\mathbb{F}_q}(Z) \quad с \quad I(Z)_{\mathbb{F}_q} = I(Z) \cap \mathbb{F}_q[x_1, \ldots, x_n]$$

се нарича афинен координатен пръстен на Z над $\mathbb{F}_q$.

Ако $X \subset \overline{\mathbb{F}_q}^n$ е неприводимо афинно многообразие, то афинният координатен пръстен $\overline{\mathbb{F}_q}[X]$ е област и полето от частни $\overline{\mathbb{F}_q}(X)$ на $\overline{\mathbb{F}_q}[X]$ се нарича функционално поле на X. Когато разширението $\overline{\mathbb{F}_q}(X) \supset \overline{\mathbb{F}_q}$ е от степен на трансцендентност 1, казваме, че X е неприводима афинна крива.

2.2.2 $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-действие върху проективни пространства и многообразия

Определение 37. *Множеството $\mathbb{P}^n(\overline{\mathbb{F}_q}) = \left(\overline{\mathbb{F}_q}^{n+1} \setminus \{(0, \ldots, 0)\}\right)/\overline{\mathbb{F}_q^*}$ на правите през началото $(0,0) \in \overline{\mathbb{F}_q}^{n+1}$ в афинното пространство $\overline{\mathbb{F}_q}^{n+1}$ се нарича n-мерно проективно пространство.*

Точките $a \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ представляват класове на пропорционалност на

$$(a_0, a_1, \ldots, a_n) \in \overline{\mathbb{F}_q}^{n+1} \setminus \{(0, \ldots, 0)\},$$

които ще бележим с $a = [a_0 : a_1 : \ldots : a_n]$. Компонентите $a_0, \ldots, a_n$ се наричат хомогенни координати на a и са определени с точност до ненулев множител от $\overline{\mathbb{F}_q}$.

Проективното пространство $\mathbb{P}^n(\overline{\mathbb{F}_q}) = \cup_{i=0}^n U_i$ се покрива от стандартните афинни подмножества

$$U_i = \{x = [x_0 : \ldots : x_i : \ldots : x_n] \in \mathbb{P}^n(\overline{\mathbb{F}_q}) \ \mid \ x_i \neq 0\}.$$

Изображенията

$$\varphi_i : U_i \longrightarrow \overline{\mathbb{F}_q}^n,$$

$$\varphi_i([x_0 : \ldots : x_i : \ldots : x_n]) = \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

са взаимно еднозначни.

Определение 38. *Точките $x \in \mathbb{P}^n(\overline{\mathbb{F}_q})$, които имат представяне от вида*

$$x = [x_0 : \ldots : x_n] \quad с \quad x_i \in \mathbb{F}_q \quad за \quad \forall 0 \leq i \leq n$$

се наричат $\mathbb{F}_q$-рационални.

Точката $x \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ е $\mathbb{F}_q$-рационална точно когато има представяне от вида $x = [a_0 : \ldots : a_{i-1} : 1 : a_{i+1} : \ldots : a_n]$ с $(a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) \in \mathbb{F}_q^n$.

Лема 39. *Броят на $\mathbb{F}_q$-рационалните точки $\mathbb{P}^n(\mathbb{F}_q)$ на проективното пространство $\mathbb{P}^n(\overline{\mathbb{F}_q})$ е*

$$|\mathbb{P}^n(\mathbb{F}_q)| = \frac{q^{n+1}-1}{q-1}.$$

Доказателство: Множеството $\mathbb{F}_q^{n+1} \setminus \{(0, \ldots, 0)\}$ има $q^{n+1} - 1$ елемента. Всяка $\mathbb{F}_q^*$-орбита върху $\mathbb{F}_q^{n+1} \setminus \{(0, \ldots, 0)\}$ се състои от $q-1$ точки и броят на $\mathbb{F}_q^*$-орбитите върху $\mathbb{F}_q^{n+1} \setminus \{(0, \ldots, 0)\}$ е

$$\frac{q^{n+1}-1}{q-1} = |\mathbb{P}^n(\mathbb{F}_q)|.$$

□

Лема 40. *Абсолютната група на Galois $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на $\mathbb{F}_q$ действа върху проективното пространство $\mathbb{P}^n(\overline{\mathbb{F}_q})$.*

Фиксираните точки на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$ са точно $\mathbb{F}_q$-рационалните,

$$\mathbb{P}^n(\overline{\mathbb{F}_q})^{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)} = \mathbb{P}^n(\mathbb{F}_q).$$

Доказателство: Действието на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ върху афинното пространство $\overline{\mathbb{F}_q}^{n+1}$ се ограничава до действие на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ върху $\overline{\mathbb{F}_q}^{n+1} \setminus \{(0, \ldots 0)\}$. По-точно, за $\forall \varphi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ и за $\forall (x_0, \ldots, x_n) \in \overline{\mathbb{F}_q}^{n+1} \setminus \{(0, \ldots, 0)\}$ с $x_i \neq 0$ имаме $\varphi(x_i) \neq 0$ съгласно $\varphi(0) = 0$ и взаимната еднозначност на φ. Следователно

$$\varphi(x_0, \ldots, x_n) = (\varphi(x_0), \ldots, \varphi(x_n)) \in \overline{\mathbb{F}_q}^{n+1} \setminus \{(0, \ldots 0)\}.$$

Ако $(x_0, x_1, \ldots, x_n) \in \overline{\mathbb{F}_q}^{n+1} \setminus \{(0, \ldots, 0)\}$ и $(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) \in \overline{\mathbb{F}_q}^{n+1} \setminus \{(0, \ldots, 0)\}$ с $\lambda \in \overline{\mathbb{F}_q}^*$ са точки от една и съща $\overline{\mathbb{F}_q}^*$-орбита, то за $\forall \varphi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ е изпълнено

$$\varphi(\lambda x_0, \ldots, \lambda x_n) = (\varphi(\lambda)\varphi(x_0), \ldots, \varphi(\lambda)\varphi(x_n))$$

с $\varphi(\lambda) \in \overline{\mathbb{F}_q}^*$, така че $\varphi(x_0, \ldots, x_n)$ и $\varphi(\lambda x_0, \ldots, \lambda x_n)$ са от една и съща $\overline{\mathbb{F}_q}^*$-орбита. По този начин, действието на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ върху $\overline{\mathbb{F}_q}^{n+1} \setminus \{(0, \ldots, 0)\}$ индуцира коректно зададено действие на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ върху множеството $\mathbb{P}^n(\overline{\mathbb{F}_q})$ на $\overline{\mathbb{F}_q}^*$-орбитите върху $\overline{\mathbb{F}_q}^{n+1} \setminus \{(0, \ldots, 0)\}$.

Непосредствено се проверява, че $\varphi_i : U_i \to \overline{\mathbb{F}_q}^n$ са еквивариантни относно действието на абсолютната група на Galois $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. По-точно, $\varphi\varphi_i(a) = \varphi_i\varphi(a)$ за всяка точка $a \in U_i$. Точката $a = [a_0 : a_1 : \ldots : a_n] \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ с $a_i \neq 0$ е неподвижна под действие на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ тогава и само тогава, когато

$$\varphi_i(a) = \left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) \in \overline{\mathbb{F}_q}^n$$

е неподвижна точка на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ за някое $0 \leq i \leq n$ с $a_i \neq 0$. Последното е еквивалентно на $\mathbb{F}_q$-рационалност на $\varphi_i(a)$, а оттам и на a.

□

Разсъжденията от доказателството на Лема 40 доказват следната

Лема 41. *Ако a е точка от стандартното афинно подмножество $U_i \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, то $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитата $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a) \subset U_i$ се съдържа изцяло в U_i и се изобразява изоморфно върху $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитата*

$$\varphi_i Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a) = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}\varphi_i(a) \subset \overline{\mathbb{F}_q}^n$$

на афинното пространство $\overline{\mathbb{F}_q}^n$.

Определение 42. *Дефиниционното поле на точка $a = [a_0 : \ldots : a_n] \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ се определя като разширението*

$$\mathbb{F}_q\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) \supseteq \mathbb{F}_q$$

за някое $a_i \neq 0$.

Лема 43. *Дефиниционното поле $\mathbb{F}_q\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right)$ на точка*

$$a = [a_0 : \ldots : a_n] \in \mathbb{P}^n(\overline{\mathbb{F}_q})$$

над $\mathbb{F}_q$ не зависи от избора на $0 \leq n$ с $a_i \neq 0$.

Доказателство: Достатъчно е да проверим, че ако $a_0 \neq 0$ и $a_1 \neq 0$, то

$$\mathbb{F}_q\left(\frac{a_1}{a_0}, \quad \frac{a_i}{a_0} \;\middle|\; 2 \leq i \leq n\right) = \mathbb{F}_q\left(\frac{a_0}{a_1}, \quad \frac{a_i}{a_1} \;\middle|\; 2 \leq i \leq n\right). \tag{2.2}$$

За целта, полагаме

$$c = \frac{a_1}{a_0}$$

и свеждаме (2.2) към

$$\mathbb{F}_q\left(c, \quad \frac{a_i}{a_0} \;\middle|\; 2 \leq i \leq n\right) = \mathbb{F}_q\left(c^{-1}, \quad c^{-1}\frac{a_i}{a_0} \;\middle|\; 2 \leq i \leq n\right) \tag{2.3}$$

От $c^{-1} \in \mathbb{F}_q\left(c, \quad \frac{a_i}{a_0} \;\middle|\; 2 \leq i \leq n\right)$ и $c^{-1}\frac{a_i}{a_0} \in \mathbb{F}_q\left(c, \frac{a_i}{a_0} \;\middle|\; 2 \leq i \leq n\right)$ следва

$$\mathbb{F}_q\left(c^{-1}, \quad c^{-1}\frac{a_i}{a_0} \;\middle|\; 2 \leq i \leq n\right) \subseteq \mathbb{F}_q\left(c, \quad \frac{a_i}{a_0} \;\middle|\; 2 \leq i \leq n\right).$$

От друга страна, $c \in \mathbb{F}_q\left(c^{-1}, \quad c^{-1}\frac{a_i}{a_0} \;\middle|\; 2 \leq i \leq n\right)$ и

$$\frac{a_i}{a_0} = c\left(c^{-1}\frac{a_i}{a_0}\right) \in \mathbb{F}_q\left(c^{-1}, \quad c^{-1}\frac{a_i}{a_0} \;\middle|\; 2 \leq i \leq n\right)$$

дават $\mathbb{F}_q\left(c, \quad \frac{a_i}{a_0} \;\middle|\; 2 \leq i \leq n\right) \subseteq \mathbb{F}_q\left(c^{-1}, \quad c^{-1}\frac{a_i}{a_0} \;\middle|\; 2 \leq i \leq n\right)$. Това доказва (2.3).

□

От Лема 43 и Лема-Определение 27 следва, че дефиниционното поле на точка $a \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ съвпада с дефиниционното поле на $\sigma(a) \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ за произволен автоморфизъм $\sigma \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Това дава възможност да определим дефиниционното поле на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$ над $\mathbb{F}_q$ като дефиниционното поле на произволен неин елемент над $\mathbb{F}_q$.

Комбинирайки Лема 43 с Твърдение-Определение 28 получаваме следващото

Следствие-Определение 44. *(i) Всяка $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита*

$$P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a),$$

$a \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ е крайно множество.

Броят на елементите в $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита $P \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ се нарича степен на P и се бележи с $\deg(P)$.

(ii) Степента на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ върху проективното пространство $\mathbb{P}^n(\overline{\mathbb{F}_q})$ е минималното естествено $m \in \mathbb{N}$, за което има представяне $a = [a_0 : \ldots : a_n] \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ с $a_0, \ldots, a_n \in \mathbb{F}_{q^m}$.

(iii) Степента на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$ е минималното естествено число m, за което автоморфизмът на Frobenius Φ_{q^m} оставя на място a, $\Phi_{q^m}(a) = a$.

(iv) Степента на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$ съвпада със степента

$$\left[\mathbb{F}_q\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) : \mathbb{F}_q\right]$$

на дефиниционното поле на $a \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ над $\mathbb{F}_q$.

Лема 43 и Твърдение 29 дават следното

Следствие 45. *Ако $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$, $a \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ е $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита върху $\mathbb{F}^n(\overline{\mathbb{F}_q})$, r е естествено число, $d = GCD(m, r)$ е най-големият общ делител на m и r, то*

$$P = \cup_{j=1}^{d} P_j$$

се разлага в непресичащо се обединение от d на брой $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})$-орбити P_j от степен $\deg(P_j) = \frac{m}{d}$.

В частност, $P = \cup_{j=1}^{m} P_j$ се разлага в обединение на m на брой едноелементни $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})$-орбити тогава и само тогава, когато m дели r.

Определение 46. *За произволна фамилия $S \subseteq \overline{\mathbb{F}_q}[x_0, x_1, \ldots, x_n]_h$ от хомогенни полиноми множеството*

$$Z(S) = \{a = [a_0 : \ldots : a_n] \in \mathbb{P}^n(\overline{\mathbb{F}_q}) \quad | \quad f(a) = 0 \quad \text{за всеки} \quad f \in S\}$$

наобщите нули на полиномите от S в $\mathbb{P}^n(\overline{\mathbb{F}_q})$ се нарича проективно многообразие.

Ако $f(x_0,\ldots,x_n)\in\overline{\mathbb{F}_q}[x_0,\ldots,x_n]$ е хомогенен полином от степен d, то за всяка точка $a=[a_0:\ldots:a_i:\ldots:a_n]\in\mathbb{P}^n(\overline{\mathbb{F}_q})$ и $\forall\lambda\in\overline{\mathbb{F}_q}^*$ е в сила $f(\lambda a_0,\lambda a_n)=\lambda^d f(a_0,\ldots,a_n)$. Следователно $f(a_0,\ldots,a_n)=0$ тогава и само тогава, когато $f(\lambda a_0,\ldots,\lambda a_n)=0$ или произволен хомогенен полином $f(x_0,\ldots,x_n)$ се анулира в $(a_0,\ldots,a_n)$ точно когато се анулира във всички точки $(\lambda a_0,\ldots,\lambda a_n)\in\overline{\mathbb{F}_q}^{n+1}\setminus\{(0,\ldots,0)\}$, пропорционални на $(a_0,\ldots,a_n)$. По този начин, анулирането на хомогенен полином $f(x_0,\ldots,x_n)$ в точка $a\in\mathbb{P}^n(\overline{\mathbb{F}_q})$ е коректно определено като анулиране на $f(x_0,\ldots,x_n)$ във всички повдигания на a до точки на $\overline{\mathbb{F}_q}^{n+1}\setminus\{(0,\ldots,0)\}$.

Нехомогенен полином $g(x_0,\ldots,x_n)\in\overline{\mathbb{F}_q}[x_1,\ldots,x_n]$ може да се анулира в някои точки от $\overline{\mathbb{F}_q}^*$-орбита и да не се анулира в други точки от същата орбита. Например $g(x_0,x_1)=x_0-1$ се анулира в $(1,1)\in\overline{\mathbb{F}_q}^2\setminus\{(0,0)\}$, но не се анулира в точките $(\lambda,\lambda)\in Orb_{\overline{\mathbb{F}_q}^*}(1,1)\subset\overline{\mathbb{F}_q}^2\setminus\{(0,0)\}$ с $\lambda\in\overline{\mathbb{F}_q}^*\setminus\{1\}$. Затова не можем да определим нулите на $g(x_0,x_1)=x_0-1$ върху $\mathbb{P}^1(\overline{\mathbb{F}_q})$.

Абсолютната група на Galois $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ действа върху $\overline{\mathbb{F}_q}$-линейното пространство $\overline{\mathbb{F}_q}[x_0,\ldots,x_n]_h$ на хомогенните полиноми с коефициенти от алгебричната обвивка $\overline{\mathbb{F}_q}$ на $\mathbb{F}_q$ и фиксираните точки за това действие са хомогенните полиноми $\mathbb{F}_q[x_0,\ldots,x_n]_h$ с коефициенти от $\mathbb{F}_q$.

Определение 47. *Ако $S\subseteq\mathbb{F}_q[x_1,\ldots,x_n]_h$ се състои от хомогенни полиноми с коефициенти от $\mathbb{F}_q$, то казваче, че проективното многообразие $Z(S)$ е определено над $\mathbb{F}_q$ и записваме $Z(S)/\mathbb{F}_q$.*

Ако $Z(S)/\mathbb{F}_q$ е проективно многообразие, определено над $\mathbb{F}_q$, то сечението

$$Z(S)(\mathbb{F}_q):=Z(S)\cap\mathbb{P}^n(\mathbb{F}_q)$$

се нарича множество на $\mathbb{F}_q$-рационалните точки на $Z(S)$.

Непосредствено се вижда, че $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ действа върху всяко проективно многообразие $Z(S)$, определено над $\mathbb{F}_q$. При това, $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-фиксираните точки на това действие са точно $\mathbb{F}_q$-рационалните,

$$Z(S)^{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}=Z(S)(\mathbb{F}_q).$$

Нека $Z(S)/\mathbb{F}_q$ е проективно многообразие, определено над $\mathbb{F}_q$ и $a\in Z(S)$. Тогава $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитата $P=Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$, породена от a се съдържа изцяло в $Z(S)$.

Множеството $\mathcal{Z}=\{Z(S)\}_{S\subseteq\overline{\mathbb{F}_q}[x_0,\ldots,x_n]_h}$ на проективните многообразия, зададени от фамилия хомогенни полиноми $S\subseteq\overline{\mathbb{F}_q}[x_0,\ldots,x_n]_h$ изпълнява свойствата на съвкупност от затворени подмножества на $\mathbb{P}^n(\overline{\mathbb{F}_q})$, защото $\emptyset=Z(\overline{\mathbb{F}_q}[x_0,\ldots,x_n])\in\mathcal{Z}$, $\mathbb{P}^n(\overline{\mathbb{F}_q})=Z(0)\in\mathcal{Z}$, $\cap_{\alpha\in A}Z(S_\alpha)=Z(\cup_{\alpha\in A}S_\alpha)\in\mathcal{Z}$ за $S_\alpha\subseteq\overline{\mathbb{F}_q}[x_0,\ldots,x_n]_h$, $\alpha\in A$ и $Z(S_1)\cup\ldots\cup Z(S_m)=Z(S_1\ldots S_m)\in\mathcal{Z}$ за $S_j\subseteq\overline{\mathbb{F}_q}[x_0,\ldots,x_n]_h$, $1\le j\le m$.

Определение 48. *Топологията върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$ със затворени подмножества*

$$\mathcal{Z}=\{Z(S)\}_{S\subseteq\overline{\mathbb{F}_q}[x_0,\ldots,x_n]_h}$$

се нарича топология на Зариски върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$.

За произволно множество $S_o \subseteq \overline{\mathbb{F}_q}[x_0, \ldots, x_n]_h$ от хомогенни полиноми, топологията върху $Z(S_o)$, индуцирана от топологията на Зариски върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$ се нарича топология на Зариски върху $Z(S_o)$. Затворените подмножества на топологията на Зариски върху проективно многообразие $Z(S_o)$ са

$$\{Z(S) \cap Z(S_o)\}_{S \subseteq \overline{\mathbb{F}_q}[x_0,\ldots,x_n]_h} = \{Z(S \cup S_o)\}_{S \subseteq \overline{\mathbb{F}_q}[x_0,\ldots,x_n]_h} = \{Z(T)\}_{S_o \subseteq T \subseteq \overline{\mathbb{F}_q}[x_0,\ldots,x_n]_h}.$$

Определение 49. *Проективната обвивка $\overline{W}$ на подмножество $W \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е сечението $\overline{W} = \cap_{F \supseteq W} F$ на всички Зариски затворени подмножества $F \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$, съдържащи W.*

Лема 50. *Проективната обвивка $\overline{M}$ на подмножество $M \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$ е равна на*

$$\overline{M} = Z(I_h(M)_h).$$

В частност, ако M е проективно алгебрични множество, то $M = V_{\mathbb{P}^n}(I_h(M)_h)$.

Доказателство: По определение, $\overline{M} = \cap_{M \subseteq Z} Z$ е сечението на Зариски затворените подмножества $Z \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, съдържащи M. Да забележим, че

$$M \subseteq Z(I_h(M)_h),$$

защото всеки хомогенен елемент f на $I_h(M)$ е хомогенен полином, анулиращ се във всички точки на M. В качеството си на Зариски затворено подмножество на $\mathbb{P}^n(\overline{\mathbb{F}_q})$, съдържащо M, $Z(I_h(M)_h)$ участва в сечението $\cap_{M \subseteq Z} Z = \overline{M}$ и го съдържа.

За обратното включване $Z(I_h(M)_h) \subseteq \overline{M}$ е достатъчно да проверим, че

$$Z(I_h(M)_h) \subseteq Z$$

за всяко Зариски затворено подмножество $M \subseteq Z = Z(S_o) \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$, зададено с множество S_o от хомогенни полиноми. Наистина, от $M \subseteq Z(S_o) = Z$ следва $I_h(M) \supseteq I_h(Z(S_o)) \supseteq S_o$, а оттам и $I_h(M)_h \supseteq I_h(Z(S_o))_h \supseteq S_o$. Това е достатъчно за $Z(I_h(M)_h) \subseteq Z(S_o) = Z$ и доказва $Z(I_h(M)_h) \subseteq_{Z \supseteq M} Z = \overline{M}$.

□

Следващото твърдение установява, че отворените подмножества $U_i \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ са изоморфни на n-мерното афинно пространство $\overline{\mathbb{F}_q}^n$ по такъв начин, че топологията на Зариски върху U_i, наследена от $\mathbb{P}^n(\overline{\mathbb{F}_q})$ съвпада с топологията на Зариски върху $\overline{\mathbb{F}_q}^n$.

Твърдение 51. *За $\forall 0 \leq i \leq n$ изображението*

$$\varphi_i : U_i = \{x \in \mathbb{P}^n(\overline{\mathbb{F}_q}) \ \mid \ x_i \neq 0\} \longrightarrow \overline{\mathbb{F}_q}^n,$$

$$\varphi_i([x_0 : \ldots : x_{i-1} : x_i : x_{i+1} : \ldots : x_n]) = \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

е хомеоморфизъм относно топологията върху U_i, индуцирана от топологията на Зариски върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$ и топологията на Зариски върху $\overline{\mathbb{F}_q}^n$.

Изображението φ_i се нарича афинен координатен хомеоморфизъм на U_i.

Доказателство: Вече споменахме, че изображението φ_i е взаимно еднозначно. Остава да проверим, че $\varphi_i : U_i \to \overline{\mathbb{F}_q}^n$ и $\varphi_i^{-1} : \overline{\mathbb{F}_q}^n \to U_i$ са непрекъснати изображения относно съответните топологии на Зариски. По определение, изображение $f : X \to Y$ на топологични пространства е непрекъснато, ако всяка отвореноо подмножсетво $U \subseteq Y$ се издърпва до отворено подмножество $f^{-1}(U)$. Еквивалентно, $f : X \to Y$ е непрекъснато точно когато издърпва затворените подмножества $Y \backslash U \subseteq Y$ в затворени подмножества $f^{-1}(Y \setminus U) = X \setminus f^{-1}(U) \subseteq X$. Затова е достатъчно да проверим, че за произволно подмножество

$$T \subseteq \overline{\mathbb{F}_q}\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right],$$

афинното многообразие $Z(T) \subseteq \overline{\mathbb{F}_q}^n$ се издърпва в Зариски затворено подмножество $\varphi_i^{-1}Z(T) \subseteq U_i$ и за произволно подмножество $S \subseteq \overline{\mathbb{F}_q}[x_0, \ldots, x_n]_h$ с непразно сечение $Z(S) \cap U_i \neq \emptyset$ на проективното многообразие $Z(S) \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$ със стандартното афинно алгебрично множество $U_i \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, праобразът $(\varphi_i^{-1})^{-1}(Z(S) \cap U_i) = \varphi_i(Z(S) \cap U_i) \subseteq \overline{\mathbb{F}_q}^n$ е Зариски затворен в $\overline{\mathbb{F}_q}^n$.

Въвеждаме i-тата дехомогенизация $f_{[i]}$ на хомогенен полином $f \in \overline{\mathbb{F}_q}[x_0, \ldots, x_n]_h$ от степен d като

$$f_{[i]}\left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right) := x_i^{-d} f(x_0, \ldots, x_n)$$

и забелязваме, че $f_{[i]}$ е полином на $\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}$ от обща степен $\leq d$. Обратно, за произволен полином $g \in \overline{\mathbb{F}_q}\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right]$ от обща степен d определяме i-тата хомогенизация като

$$g^{[i]}(x_0, \ldots, x_n) := x_i^d g\left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

и забелязваме, че $g^{[i]}$ е хомогенен полином на $x_0, \ldots, x_n$ от степен d. Произволен хомогенен полином $f \in \overline{\mathbb{F}_q}[x_0, \ldots, x_n]$ се анулира в точка $a \in U_i$ тогава и само тогава, когато i-тата му дехомогенизация $f_{[i]}$ се анулира в $a_{[i]}$, съгласно

$$f_{[i]}(a_{[i]}) = a_i^{-\deg(f)} f(a_0, \ldots, a_n).$$

За произволно множество $S \subset \overline{\mathbb{F}_q}[x_0, \ldots, x_n]_h$ от хомогенни полиноми означаваме с $S_{[i]}$ множеството на i-тите дехомогенизации на елементите на S получаваме,че

$$\varphi_i(Z(S) \cap U_i) = Z(S_{[i]}).$$

Обратно, полином $g \in \overline{\mathbb{F}_q}\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right]$ се анулира в $a_{[i]}$ точно когато i-тата му хомогенизация се анулира в a, защото $g^{[i]}(a) = a_i^{\deg(g)} g(a_{[i]})$. Ако $T \subset \overline{\mathbb{F}_q}\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right]$ е множество от полиноми и $T^{[i]}$ е множеството на i-тите хомогенизации на елементите на T, то

$$\varphi_i^{-1}Z(T) = Z(T^{[i]}) \cap U_i.$$

□

Определение 52. *Идеалът $I \triangleleft k\mathbb{F}_q[x_1, \ldots, x_n]$ с коефициенти от поле k е хомогенен, ако се поражда от хомогенни полиноми.*

Определение 53. *Идеалът $I_h(Z(S)) \triangleleft \overline{\mathbb{F}_q}[x_0, \ldots, x_n]$, породен от хомогенните полиноми $f(x_0, \ldots, x_n) \in \overline{\mathbb{F}_q}[x_0, \ldots, x_n]_h$, анулиращи се върху $Z(S)$ се нарича хомогенен идеал на проективното алгебрично множество $Z(S) \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$.*

Лема 54. *Идеалът $I \triangleleft k[x_1, \ldots, x_n]$ е хомогенен тогава и само тогава, когато за всеки елемент $f = \sum_{i=0}^{m} f^{[i]}$ на I хомогенните компоненти $f^{[i]}$ на f от степен i принадлежат на I.*

Доказателство: Ако идеалът $I = \langle f_1, \ldots, f_s \rangle$ се поражда от хомогенни полиноми $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, то произволен елемент на I е от вида

$$f = \sum_{j=1}^{s} g_j f_j.$$

Ако $\deg(f_j) = d_j$, то хомогенните компоненти

$$f^{[d]} = \sum_{j=1}^{s} g_j^{[d-d_j]} f_j$$

принадлежат на I.

Обратно, нека $I = \langle g_1, \ldots, g_l \rangle$ се поражда от полиномите $g_1, \ldots, g_l \in k[x_1, \ldots, x_n]$. По предположение, всички хомогенни компоненти $g_i^{[j]}$ на $g_i = \sum_{j=0}^{d_i} g_i^{[j]}$ принадлежат на I, така че идеалът

$$J = \langle g_i^{[j]} \ \mid \ 0 \leq j \leq d_i, \ \ 1 \leq i \leq l \rangle$$

се съдържа в идеала I. От друга страна, $I \subseteq J$, защото за произволни полиноми $h_1, \ldots, h_l \in k[x_1, \ldots, x_n]$ е в сила $\sum_{i=1}^{l} g_i h_i = \sum_{i=1}^{l} \sum_{j=0}^{d_i} g_i^{[j]} h_i \in J$. Следователно $I = J$ се поражда от хомогенните полиноми $g_i^{[j]}$ и I е хомогенен идеал.

□

Лема 55. *Ако I е хомогенен идеал в $k[x_0, \ldots, x_n]$, то идеалът I е прост тогава и само тогава, когато за произволни хомогенни полиноми*

$$f(x_0, \ldots, x_n), g(x_0, \ldots, x_n) \in k[x_0, \ldots, x_n]$$

с $f(x_0, \ldots, x_n)g(x_0, \ldots, x_n) \in I$ е в сила $f(x_0, \ldots, x_n) \in I$ или $g(x_0, \ldots, x_n) \in I$.

Доказателство: Необходимостта на условието следва от определението за прост идеал. Да допуснем, че за произволни хомогенни полиноми $f(x_0, \ldots, x_n)$, $g(x_0, \ldots, x_n) \in$

$k[x_0,\ldots,x_n]$ с $fg \in I$ следва $f \in I$ или $g \in I$, но идеалът I не е прост. Тогава съществуват полиноми $F, G \in k[x_0,\ldots,x_n]$ с $FG \in I$, $F \notin I$, $G \notin I$. Ако

$$F = \sum_{i=0}^{m} F^{[i]} \quad \text{и} \quad G = \sum_{j=0}^{n} G^{[j]}$$

са разлаганията на F и G в сума от хомогенни компоненти, без ограничение на общността можем да предполагаме, че $F^{[m]} \notin I$, $G^{[n]} \notin I$. В противен случай, $F_1 := F - F^{[m]}$ има произведение $F_1 G = FG - F^{[m]}G \in I$ и можем да разглеждаме F_1 и G вместо F и G. Хомогенната компонента от максимална степен

$$(FG)^{[m+n]} = \left[\left(\sum_{i=0}^{m} F^{[i]}\right)\left(\sum_{j=0}^{n} G^{[j]}\right)\right]^{[m+n]} = F^{[m]}G^{[n]} \in I$$

принадлежни на I, защото $FG \in I$ и I е хомогенен идеал. По предположение, от $F^{[m]}G^{[n]} \in I$ следва $F^{[m]} \in I$ или $G^{[n]} \in I$. Противоречието доказва твърдението.

□

Твърдение 56. *Проективното многообразие $Z = Z(S) \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$ за някое $S \subseteq \overline{\mathbb{F}_q}[x_0,\ldots,x_n]_h$ е неприводимо тогава и само тогава, когато хомогенният идеал $I_h(Z) \lhd \overline{\mathbb{F}_q}[x_0,\ldots,x_n]$ е прост.*

Доказателство: Да допуснем, че $Z = Z(S) \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$ е неприводимо проективно многообразие, чийто хомогенен идеал $I_h(Z) \lhd \overline{\mathbb{F}_q}[x_0,\ldots,x_n]$ не е прост. Съгласно Лема 55, съществуват хомогенни полиноми $f(x_0,\ldots,x_n)$ и $g(x_0,\ldots,x_n)$ от $\overline{\mathbb{F}_q}[x_0,\ldots,x_n]_h \setminus I_h(X)$ с $fg \in I_h(Z)_h$. Твърдим, че

$$Z_1 := Z(f) \not\supseteq Z(I_h(Z)_h) = Z, \quad Z_2 := Z(g) \not\supseteq Z(I_h(Z)_h) = Z,$$

защото предположението $Z_1 \supseteq Z$ води до $f|_Z = 0$, откъдето $f \in I_h(X)$, противно на избора на $f \notin I_h(X)$. От друга страна, $Z(fg) \supseteq Z(I_h(Z)_h) = Z$, така че

$$Z = Z(fg) \cap Z = (Z(f) \cup Z(g)) \cap Z = (Z_1 \cap Z) \cup (Z_2 \cap Z).$$

Подмножествата $Z_1 \cap Z$ и $Z_2 \cap Z$ на Z са затворени и различни от Z съгласно $Z \nsubseteq Z_1$, $Z \nsubseteq Z_2$. Това противоречи на неприводимостта на Z и доказва простотата на хомогенния идеал на неприводимо проективно многообразие.

Обратно, нека $Z \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$ е проективно многообразие с прост хомогенен идеал $I_h(Z) \lhd \overline{\mathbb{F}_q}[x_0,\ldots,x_n]$ и $Z = Z_1 \cup Z_2$ за Зариски затворени $Z_i \subsetneq Z$. Тогава

$$I_h(Z) = I_h(Z_1 \cup Z_2) = I_h(Z_1) \cap I_h(Z_2)$$

и $I_h(Z_i) \supsetneq I_h(Z)$ за $1 \leq i \leq 2$. По-точно, от $Z_i \subseteq Z$ следва $I_h(Z_i) \supseteq I_h(Z)$ и предположението $I_h(Z_i) = I_h(Z)$ води до $Z_i = Z(I_h(Z_i)_h) = Z(I_h(Z)_h) = Z$, което противоречи на допускането за приводимост на Z. От $I_h(Z_i) \supsetneq I_h(Z)$ следва $I_h(Z_i)_h \supsetneq I_h(Z)_h$. По-точно, включването $I_h(Z_i)_h \supseteq I_h(Z)_h$ е ясно. Допускането $I_h(Z_i)_h = I_h(Z)_h$ води до

съвпадение $I_h(Z_i) = I_h(Z)$, защото хомогенните идеали $I_h(Z_i)$ и $I_h(Z)$ се пораждат от хомогенните си елементи. Избираме хомогенни полиноми $f_i \in I_h(Z_i)_h \setminus I_h(Z)_h$ и забелязваме, че $f_1 f_2 \in I_h(Z_i)_h \cap I_h(Z_2)_h = I_h(Z)_h$. Това противоречи на простотата на идеала $I_h(Z)$ и доказва неприводимостта на проективните многообразия Z с прост хомогенен идеал $I_h(Z)$.

□

Лема 57. *Нека Z е неприводимо затворено подмножество на топологично пространство X, а $U \subseteq X$ е отворено подмножество с непразно сечение $Z \cap U \neq \emptyset$. Тогава $Z \cap U$ е отворено, навсякъде гъсто в Z и неприводимо подмножество на X.*

Доказателство: Подмножеството $Z \cap U \subseteq Z$ е отворено съгласно определението на индуцираната от X топология върху Z.

За произволни подмножества $A, B \subseteq X$ на топологичното пространство X твърдим, че $\overline{A \cup B} = \overline{A} \cup \overline{B}$. От една страна,

$$\overline{A} \cup \overline{B} = (\cap_{Z_1 \supseteq A} Z_1) \cup (\cap_{Z_2 \supseteq B} Z_2) = \cap_{Z_1 \supseteq A} \cap_{Z_2 \supseteq B} \ (Z_1 \cup Z_2)$$

се съдържа в $\overline{A \cup B} = \cap_{Z \supseteq A \cup B} Z$, защото всяко затворено подмножество $Z \subseteq X$ с $Z \supseteq A \cup B$ може да се представи като $Z = Z \cup Z$ с $Z \supseteq A$, $Z \supseteq B$ и участва в сечението $\cap_{Z_1 \supseteq A} \cap_{Z_2 \supseteq B} \ (Z_1 \cup Z_2) = \overline{A \cup B}$. Обратно, произволни затворени $Z_1, Z_2 \subseteq X$ с $Z_1 \supseteq A$, $Z_2 \supseteq B$ имат затворено обединение $Z_1 \cup Z_2 \supseteq A \cup B$, така че $Z_1 \cup Z_2$ участва в сечението $\cap_{Z \subseteq A \cup B} Z = \overline{A \cup B}$ и $\overline{A \cup B} \subseteq \overline{A} \cup \overline{B}$. Това доказва $\overline{A \cup B} = \overline{A} \cup \overline{B}$.

За гъстотата на $Z \cap U$ в Z разглеждаме разлагането

$$Z = (Z \cap U) \cup (Z \setminus U).$$

Затворената обвивка

$$Z = \overline{Z} = \overline{(Z \cap U) \cup (Z \setminus U)} = \overline{(Z \cap U)} \cup \overline{(Z \setminus U)} = \overline{(Z \cap U)} \cup (Z \setminus U),$$

съгласно затвореността на Z и $Z \setminus U$. Неприводимостта на Z изисква $Z = \overline{Z \cap U}$, защото допускането $Z = Z \setminus U$ противоречи на $Z \cap U \neq \emptyset$. Това доказва, че $Z \cap U$ е навсякъде гъсто в Z.

За неприводимостта на $Z \cap U$ да допуснем, че $Z \cap U = V_1 \cup V_2$ за някакви затворени подмножества $V_j \subseteq Z \cap U$. По определение,

$$V_j = Z'_j \cap (Z \cap U) = (Z'_j \cap Z) \cap U = Z_j \cap U$$

за някакви затворени $Z'_j \subseteq X$ и $Z_j := Z'_j \cap Z \subseteq X$. Затворената обвивка

$$Z = \overline{Z \cap U} = \overline{(Z_1 \cap U) \cup (Z_2 \cap U)} = \overline{(Z_1 \cap U)} \cup \overline{(Z_2 \cap U)} = Z_1 \cup Z_2,$$

съгласно гъстотата на $Z \cap U$ в Z и на $Z_j \cap U$ в Z_j (при $Z_j \cap U \neq \emptyset$). Неприводимостта на Z изисква $Z = Z_1$ или $Z = Z_2$, откъдето $Z \cap U = Z_1 \cap U$ или $Z \cap U = Z_2 \cap U$ и $Z \cap U$ е неприводимо подмножество на X.

□

Твърдение 58. *(i) Ако* $W \subseteq \overline{\mathbb{F}_q}^n \simeq U_i \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ *е неприводимо афинно многообразие, то проективната обвивка* $\overline{W} \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$ *е неприводимо проективно многообразие.*

(ii) Ако афинното многообразие $W/\mathbb{F}_q$ *е неприводимо и определено над полето* $\mathbb{F}_q$*, то проективната обвивка* $\overline{W}/\mathbb{F}_q$ *е определена над* $\mathbb{F}_q$*.*

(iii) Ако $V \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$ *е неприводимо проективно многообразие,*

$$U_i = \{x = [x_0 : \ldots : x_n] \in \mathbb{P}^n(\overline{\mathbb{F}_q}) \ \mid \ x_i \neq 0\}$$

е стандартно афинно отворено подмножество на $\mathbb{P}^n(\overline{\mathbb{F}_q})$ *и сечението* $V \cap U_i \neq \emptyset$ *не е празно, то* $V \cap U_i \subseteq U_i \simeq \overline{k}^n$ *е неприводимо афинно многообразие.*

(iv) Ако $V/\mathbb{F}_q$ *е неприводимо проективно многообразие, определено над* $\mathbb{F}_q$ *и пресичащо стандартното афинно отворено подмножество* U_i *на* $\mathbb{P}^n(\overline{\mathbb{F}_q})$*, то* $V \cap U_i \subseteq U_i \simeq \overline{\mathbb{F}_q}^n$ *е неприводимо афинно многообразие, определено над* $\mathbb{F}_q$*.*

Доказателство: (i) Нека $\overline{W} = Z_1 \cup Z_2$ е разлагане на проективната обвивка $\overline{W} \subseteq \mathbb{P}^n(\overline{k})$ в обединение на затворени подмножества $Z_j \subsetneq \overline{W}$. Тогава сечението

$$W = \overline{W} \cap U_i = (Z_1 \cup Z_2) \cap U_i = (Z_1 \cap U_i) \cup (Z_2 \cap U_i)$$

се представя като обединение на Зариски затворени $Z_j \cap U_i \subseteq U_i$, $1 \leq j \leq 2$. Неприводимото афинно многообразие W съвпада с някое от Зариски затворените подмножества $Z_j \cap U_i \subseteq U_i$. Оттук, проективната обвивка

$$\overline{W} = \overline{Z_j \cap U_i} = Z_j,$$

съгласно гъстотата на $Z_j \cap U_i$ в Z_j. Това доказва неприводимостта на $\overline{W}$.

(ii) Ако $W = Z(T) \subseteq \overline{\mathbb{F}_q}^n \simeq U_i$ е неприводимо афинно многообразие, определено от полиноми

$$T \subseteq \mathbb{F}_q\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right],$$

то проективната обвивка $\overline{W} = Z(T^{[i]})$ се определя от фамилията $T^{[i]} \subseteq k[x_0, \ldots, x_n]_h$ на i-тите хомогенизации на полиномите от T и $\overline{W}$ е неприводимо проективно многообразие , определено над $\mathbb{F}_q$.

(iii) Ако $V \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$ е неприводимо проективно многообразие с $V \cap U_i \neq \emptyset$ за някое стандартно афинно отворено подмножсетво $U_i \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, то $V \cap U_i$ е неприводимо съгласно Лема 57. По определението за индуцирана топология, $V \cap U_i$ е затворено подмножество на $U_i \simeq \overline{\mathbb{F}_q}^n$.

(iv) Ако $V = Z(S)$ с $S \subseteq \mathbb{F}_q[x_0, \ldots, x_n]_h$ е неприводимо проективно многообразие, определено над $\mathbb{F}_q$ и $V \cap U_i \neq \emptyset$, то $V \cap U_i = Z(S_{[i]}) \subseteq \overline{\mathbb{F}_q}^n \simeq U_i$ е неприводимо афинно многообразие, определено от множеството

$$S_{[i]} \subseteq \mathbb{F}_q\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_0}\right]$$

на i-тите дехомогенизации на полиномите от S. В частност, $V \cap U_i$ е определено над $\mathbb{F}_q$.

□

Ако $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е неприводимо проективно многообразие с $X \cap U_i \neq \emptyset$ за някое стандартно афинно отворено подмножество $U_i \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, $0 \leq i \leq n$, то полето $\overline{\mathbb{F}_q}(X)$ на рационалните функции на X се определя като полето от частни на афинния координатен пръстен на $X \cap U_i$. Ако $\overline{\mathbb{F}_q}(X) \supset \overline{\mathbb{F}_q}$ е от степен на трансцендентност 1, казваме, че X е неприводима крива.

2.3 Съответствие между орбити на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ и дискретни нормирания от една и съща степен

2.3.1 Локален пръстен на точка от крива над алгебрично затворено поле

Ако X е неприводима афинна или проективна крива с функционално поле $\overline{\mathbb{F}_q}(X)$ и $p \in X$, то подпръстенът $\mathcal{O}_p(X) < \overline{\mathbb{F}_q}(X)$ на онези рационални функции върху X, които са определени в точката p е локален и се нарича локален пръстен на p в X.

Твърдение 59. *Нека R е нътерова локална област с размерност на Krull 1. В такъв случай, R е пръстен на дискретно нормиране тогава и само тогава, когато $\mathfrak{M}/\mathfrak{M}^2$ е 1-мерно линейно пространство над полето $R/\mathfrak{M}$.*

Доказателство: Нека R е пръстен на дискретно нормиране с локален параметър t. Локалният параметър t принадлежи на максималния идеал $\mathfrak{M}$ на R, така че главният идеал $\langle t \rangle = tR \triangleleft R$, породен от t се съдържа в $\mathfrak{M}$. Всеки ненулев елемент $z \in R \setminus \{0\}$ има единствено представяне $z = ut^m$ с $u \in R^*$ и $m \in \mathbb{Z}^{\geq 0}$. Ако $z = ut^m \in \mathfrak{M}$, то $m \geq 1$ и $z \in \langle t \rangle$, защото в противен случай $z = u \in R^* = R \setminus \mathfrak{M}$. Следователно максималният идеал $\mathfrak{M} = \langle t \rangle = tR$ на R е главен и се поражда от произволен локален параметър t на R.

Твърдим, че умножението

$$\mu_t : R/\mathfrak{M} = R/tR \longrightarrow tR/t^2R = \mathfrak{M}/\mathfrak{M}^2$$

$$\mu_t(r + \mathfrak{M}) = tr + \mathfrak{M}^2$$

с t е изоморфизъм на $R/\mathfrak{M}$-линейни пространства, така че $\dim_{R/\mathfrak{M}} \left(\mathfrak{M}/\mathfrak{M}^2\right) = 1$. Преди всичко, изображението μ_t е коректно зададено, защото от $r + \mathfrak{M} = r_1 + \mathfrak{M}$ следва $tr - tr_1 = t(r - r_1) \in \mathfrak{M}^2$. Съгласно

$$\mu_t((r + \mathfrak{M}) + (s + \mathfrak{M})) = \mu_t(r + s + \mathfrak{M}) = t(r + s) + \mathfrak{M}^2 =$$

$$= tr + ts + \mathfrak{M}^2 = (tr + \mathfrak{M}^2) + (ts + \mathfrak{M}^2) = \mu_t(r + \mathfrak{M}) + \mu_t(s + \mathfrak{M})$$

и

$$\mu_t((\rho + \mathfrak{M})(r + \mathfrak{M})) = \mu_t(\rho r + \mathfrak{M}) = t(\rho r) + \mathfrak{M}^2 =$$

$$= \rho(tr) + \mathfrak{M}^2 = (\rho + \mathfrak{M})(tr + \mathfrak{M}^2) = (\rho + \mathfrak{M})\mu_t(r + \mathfrak{M}),$$

изображението μ_t е $R/\mathfrak{M}$-линейно. За взаимната еднозначност на μ_t да отбележим, че всеки елемент на $\mathfrak{M}/\mathfrak{M}^2 = tR/t^2R$ е от вида $tr + t^2R = tr + \mathfrak{M}^2$ за някое $r \in R$.

Ако $tr + \mathfrak{M}^2 = tr_1 + \mathfrak{M}^2$ за $r, r_1 \in R$, то $t(r - r_1) \in \mathfrak{M}^2 = t^2R$ или съществува $s \in R$ с $t(r - r_1) = t^2s$. В областта R от $t(r - r_1 - ts) = 0$ с $t \neq 0$ следва $r - r_1 - ts$, така че $r - r_1 = ts \in \mathfrak{M}$ и $r + \mathfrak{M} = r_1 + \mathfrak{M}$. Следователно за всеки елемент $tr + \mathfrak{M}^2 = tr_1 + \mathfrak{M}^2$ на $\mathfrak{M}/\mathfrak{M}^2$ съществува единствен праобраз $r + \mathfrak{M} = r_1 + \mathfrak{M}$ от $R/\mathfrak{M}$ с

$$\mu_t(r + \mathfrak{M}) = tr + \mathfrak{M}^2 = tr_1 + \mathfrak{M}^2 = \mu_t(r_1 + \mathfrak{M})$$

и изображението $\mu_t^{-1} : \mathfrak{M}/\mathfrak{M}^2 \to R/\mathfrak{M}$ е коректно зададено. С това установяваме, че $\mu_t : R/\mathfrak{M} \to \mathfrak{M}/\mathfrak{M}^2$ е $R/\mathfrak{M}$-линеен изоморфизъм.

Обратно, нека $\mathfrak{M}/\mathfrak{M}^2$ е 1-мерно линейно пространство над полето $R/\mathfrak{M}$. Съгласно Лемата на Nakayama за $M = \mathfrak{M}$, произволен елемент $t \in \mathfrak{M} \setminus \mathfrak{M}^2$ поражда $\mathfrak{M} = tR$ като идеал в R. За произволен ненулев идеал $\mathfrak{A}$ в ньотерова локална област R с размерност на Krull 1 съществува $k \in \mathbb{N}$ с $\mathfrak{M}^k \subseteq \mathfrak{A} \subseteq \mathfrak{M}$. Без ограничение на общността ще считаме, че k е минималното естествено число с $\mathfrak{M}^k \subseteq \mathfrak{A}$, т.е. $\mathfrak{M}^{k-1} \nsubseteq \mathfrak{A}$. Твърдим, че $\mathfrak{A} = \mathfrak{M}^k = t^kR$. Ако допуснем, че $\mathfrak{M}^k \subsetneq \mathfrak{A}$, то съществува $x \in \mathfrak{A} \setminus \mathfrak{M}^k$. Естествените степени

$$\mathfrak{M} \supsetneq \mathfrak{M}^2 \ldots \supsetneq \mathfrak{M}^{k-1} \supsetneq \mathfrak{M}^k \supsetneq \mathfrak{M}^{k+1} \supsetneq \ldots$$

на максималния идеал $\mathfrak{M}$ на R образуват строго намаляваща редица. По-точно, допускането $t^iR = \mathfrak{M}^i = \mathfrak{M}^{i+1} = t^{i+1}R$ за някое $i \in \mathbb{N}$ води до съществуване на $r \in R$ с $t^i = t^{i+1}r$. В областта R, от $t^i(1 - tr) = 0$ следва $1 = tr$, така че $t \in R^*$ и $\mathfrak{M} = tR = R$. Противоречието доказва $\mathfrak{M}^i \supsetneq \mathfrak{M}^{i+1}$ за $\forall i \in \mathbb{N}$. От $x \notin \mathfrak{M}^k$ следва $x \notin \mathfrak{M}^N$ за всички естествени $N \geq k$. Следователно множеството

$$\mathbb{N}_x := \{n \in \mathbb{N} \mid x \in \mathfrak{M}^n\} \subseteq \{1, 2, \ldots, k-1\}$$

е ограничено отгоре и има максимален елемент $n \leq k - 1$, т.е. $x \in \mathfrak{M}^n = t^nR$, $x \notin \mathfrak{M}^{n+1} = t^{n+1}R$. Оттук получаваме съществуването на $u \in R \setminus tR = R \setminus \mathfrak{M} = R^*$ с $x = t^nu$. В резултат, от $t^n = xu^{-1} \in \mathfrak{A}$ следва $\mathfrak{M}^{k-1} \subseteq \mathfrak{M}^n = t^nR \subseteq \mathfrak{A}$, което противоречи на предположението $\mathfrak{M}^{k-1} \nsubseteq \mathfrak{A}$. Следователно $\mathfrak{A} = \mathfrak{M}^k = t^kR$.

За произволен елемент $x \in R\setminus\{0\}$ идеалът $\langle x \rangle = xR = t^kR = \mathfrak{M}^k$ за някое естествено k. В резултат, съществуват $u, v \in R$ с $x = t^ku$, $t^k = xv$. Сега $t^k - t^kuv = t^k(1 - uv) = 0$ с $t \neq 0$ в областта R дава $1 = uv$, откъдето $u, v \in R^*$. Остава да проверим неразложимостта на t, за да получим, че R е пръстен на дискретно нормиране. Наистина, допускането $t = t_1t_2$ с $t_1, t_2 \in R \setminus R^* = \mathfrak{M} = tR$ води до $t_i = tr_i$ за някои $r_i \in R$, $1 \leq i \leq 2$. В резултат, от $t = t^2r_1r_2$ следва $tr_1r_2 = 1$, така че $t \in R^*$ и $\mathfrak{M} = tR = R$. Противоречието доказва неразложимостта на t.

□

Определение 60. *Нека $V \subseteq \overline{k}^n$ е афинна крива с идеал $I(V) = \langle f_1, \ldots, f_m \rangle$ за някакви полиноми $f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in \overline{k}[x_1, \ldots, x_n]$. Точката $p \in V$ е гладка, ако Якобиевата матрица*

$$\frac{\partial(f_1, \ldots, f_m)}{\partial(x_1, \ldots, x_n)} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \cdots & \cdots & \cdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}$$

има ранг $\mathrm{rk}\frac{\partial(f_1,\ldots,f_m)}{\partial(x_1,\ldots,x_n)}(p) = n-1$ *в* p.

Ако p *е гладка точка на* V, *то правата, съставена от решенията на хомогенната линейна система*

$$\frac{\partial(f_1,\ldots,f_m)}{\partial(x_1,\ldots,x_n)}(p)\begin{pmatrix} x_1 \\ \ldots \\ x_n \end{pmatrix} = 0_{m\times 1}$$

се нарича допирателна към V *в* p.

Точките $p \in V$, *които не са гладки се наричат особени.*

Означаваме с V^{smooth} *множеството на гладките точки, а с* V^{sing} *- множеството на особените точки.*

Кривата V *е гладка, ако всички точки на* V *са гладки,* $V = V^{\mathrm{smooth}}$.

Теорема 61. *Нека* $V \subset \overline{\mathbb{F}_q}^n$ *е афинна крива, а* p *е точка от* V. *В такъв случай, точката* p *е гладка тогава и само тогава, когато локалният пръстен* $\mathcal{O}_p(V)$ *на* p *във* V *е пръстен на дискретно нормиране.*

Доказателство: Изображението

$$\mathrm{grad}_p : \overline{\mathbb{F}_q}[x_1,\ldots,x_n] \longrightarrow \overline{\mathbb{F}_q}^n,$$

$$\mathrm{grad}_p(f(x_1,\ldots,x_n)) = \left(\frac{\partial f}{\partial x_1}(p),\ldots,\frac{\partial f}{\partial x_n}(p)\right) \quad \text{за} \quad \forall f(x_1,\ldots,x_n) \in \overline{\mathbb{F}_q}[x_1,\ldots,x_n]$$

е $\overline{k}$-линейно, т.е. $\mathrm{grad}_p(f+g) = \mathrm{grad}_p(f) + \mathrm{grad}_p(g)$ и $\mathrm{grad}_p(af) = a\,\mathrm{grad}_p(f)$ за $\forall f, g \in \overline{\mathbb{F}_q}[x_1,\ldots,x_n]$, $\forall a \in \overline{\mathbb{F}_q}$. За произволна фиксирана точка $p = (p_1,\ldots,p_n) \in V \subseteq \overline{k}^n$ разглеждаме максималния идеал

$$\mathfrak{N}_p = \langle x_1 - p_1,\ldots,x_n - p_n\rangle = \sum_{i=1}^{n}(x_i - p_i)\overline{\mathbb{F}_q}[x_1,\ldots,x_n]$$

на p в $\overline{\mathbb{F}_q}[x_1,\ldots,x_n]$ и ограничението

$$\mathrm{grad}_p : \mathfrak{N}_p \longrightarrow \overline{\mathbb{F}_q}^n,$$

$$\mathrm{grad}_p\left(\sum_{i=1}^{n}(x_i - p_i)g_i(x_1,\ldots,x_n)\right) = (g_1(p),\ldots,g_n(p)).$$

Ядрото

$$\ker(\mathrm{grad}_p|_{\mathfrak{N}_p}) = \left\{\sum_{i=1}^{n}(x_i - p_i)g_i(x_1,\ldots,x_n) \;\middle|\; g_i(p) = 0 \quad \text{за} \quad \forall 1 \le i \le n\right\} =$$

$$= \left\{\sum_{i=1}^{n}(x_i - p_i)g_i(x_1,\ldots,x_n) \;\middle|\; g_i \in \mathfrak{N}_p\right\} = \mathfrak{N}_p^2,$$

а образът $\mathrm{im}(\mathrm{grad}_p|_{\mathfrak{N}_p}) = \overline{\mathbb{F}_q}^n$, защото за всяко $1 \leq i \leq n$ имаме

$$\mathrm{grad}_p(x_i - p_i) = (0, \ldots, 0, 1, 0, \ldots 0) = e_i$$

за наредените n-торки e_i с единствен ненулев елемент 1 в i-та позиция и $e_1, \ldots, e_n$ образуват базис на $\overline{\mathbb{F}_q}^n$. Епиморфизмът

$$\mathrm{grad}_p : (\mathfrak{N}_p, +) \longrightarrow (\overline{\mathbb{F}_q}^n, +)$$

на адитивните групи индуцира изоморфизъм

$$\overline{\mathrm{grad}_p} : \left(\mathfrak{N}_p/\mathfrak{N}_p^2, +\right) \longrightarrow (\overline{\mathbb{F}_q}^n, +).$$

От съгласуваността на grad_p с умножението по $\lambda \in \overline{\mathbb{F}_q}$ следва $\overline{\mathbb{F}_q}$-линейността на $\overline{\mathrm{grad}_p}$, така че $\mathfrak{N}_p/\mathfrak{N}_p^2$ и $\overline{\mathbb{F}_q}^n$ са изоморфни като линейни пространства над $\overline{\mathbb{F}_q}$.

Да означим с $f_i(x_1, \ldots, x_n) \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, $1 \leq i \leq m$ произволни пораждащи на идеала

$$I(V) = \langle f_1, \ldots, f_m \rangle = \sum_{i=1}^{m} f_i(x_1, \ldots, x_n)\overline{\mathbb{F}_q}[x_1, \ldots, x_n]$$

на кривата V в $\overline{\mathbb{F}_q}[x_1, \ldots, x_n]$. Условието $p \in V$ е еквивалентно на $I(V) \subset \mathfrak{N}_p$. Ограничението

$$\mathrm{grad}_p : I(V) \longrightarrow \overline{\mathbb{F}_q}^n,$$

$$\mathrm{grad}_p\left(\sum_{i=1}^{m} f_i(x_1, \ldots, x_n)g_i(x_1, \ldots, x_n)\right) = \left(\sum_{i=1}^{m} g_i(p)\frac{\partial f_i}{\partial x_1}(p), \ldots, \sum_{i=1}^{m} g_i(p)\frac{\partial f_i}{\partial x_n}(p)\right) =$$

$$\sum_{i=1}^{m} g_i(p)\left(\frac{\partial f_i}{\partial x_1}(p), \ldots, \frac{\partial f_i}{\partial x_n}(p)\right) = \sum_{i=1}^{m} g_i(p)\mathrm{grad}_p(f_i)$$

взема стойности в линейната обвивка

$$\mathrm{Grad}_p(V) = l_{\overline{\mathbb{F}_q}}(\mathrm{grad}_p(f_1), \ldots, \mathrm{grad}_p(f_m))$$

на градиентите на пораждащите на $I(V)$ в $p \in V$. Всеки пораждащ $\mathrm{grad}_p(f_i)$ на $\mathrm{Grad}_p(V)$ е от образа на $\mathrm{grad}_p : I(V) \to \overline{\mathbb{F}_q}^n$, така че

$$\mathrm{grad}_p : I(V) \longrightarrow \mathrm{Grad}_p(V)$$

е линейно изображение върху $\mathrm{Grad}_p(V)$. Ядрото

$$\ker(\mathrm{grad}_p|_{I(V)}) = \ker(\mathrm{grad}_p|_{\mathfrak{N}_p}) \cap I(V) = \mathfrak{N}_p^2 \cap I(V).$$

Следователно

$$(I(V) + \mathfrak{N}_p^2)/\mathfrak{N}_p^2 \simeq I(V)/(I(V) \cap \mathfrak{N}_p^2) \simeq \mathrm{Grad}_p(V) = l_{\overline{k}}(\mathrm{grad}_p(f_1), \ldots, \mathrm{grad}_p(f_m))$$

са изоморфизми на $\overline{\mathbb{F}_q}$-линейни пространства. Якобиевата матрица

$$\frac{\partial(f_1,\ldots,f_m)}{\partial x_1,\ldots,x_n)}(p) = \begin{pmatrix} \mathrm{grad}_p(f_1) \\ \ldots \\ \mathrm{grad}_p(f_m) \end{pmatrix} \in M_{m,n}(\overline{\mathbb{F}_q})$$

се състои по редове от градиентите на пораждащите f_i на $I(V)$, така че рангът

$$\mathrm{rk}\left(\frac{\partial(f_1,\ldots,f_m)}{\partial(x_1,\ldots,x_n)}(p)\right) = \dim_{\overline{\mathbb{F}_q}}\left([I(V)+\mathfrak{N}_p^2]/\mathfrak{N}_p^2\right). \tag{2.4}$$

От друга страна, максималният идеал $N_p = \mathfrak{N}_p/I(V)$ на точката $p \in V$ в афинния координатен пръстен $\overline{\mathbb{F}_q}[V] = \overline{\mathbb{F}_q}[x_1,\ldots,x_n]/I(V)$ на V е фактор на $\mathfrak{N}_p$ по $I(V)$. Локалният пръстен $\mathcal{O}_p(V) = \overline{\mathbb{F}_q}[V]_{N_p}$ на p във V е локализацията на $\overline{\mathbb{F}_q}[V]$ относно N_p, така че максималният идеал на $\mathcal{O}_p(V)$ е

$$\mathfrak{M}_p = (N_p)_{N_p} = \left\{ \frac{\alpha}{\beta} \;\middle|\; \alpha \in N_p, \quad \beta \in \overline{\mathbb{F}_q}[V] \setminus N_p \right\}.$$

Квадратът $\mathfrak{M}_p^2 = (N_p^2)_{N_p}$, откъдето $\mathfrak{M}_p/\mathfrak{M}_p^2 = (N_p)_{N_p}/(N_p^2)_{N_p}$. Да отбележим, че

$$N_p = \left\{ \sum_{j=1}^{n}(x_j - p_j + I(V))(g_j(x_1,\ldots,x_n)+I(V)) \;\middle|\; g_j(x_1,\ldots,x_n) \in \overline{\mathbb{F}_q}[x_1,\ldots,x_n] \right\}.$$

За произволен полином $g_j(x_1,\ldots,x_n) \in \overline{\mathbb{F}_q}[x_1,\ldots,x_n]$ е изпълнено

$$g_j(x_1,\ldots,x_n) - g_j(p) \in \mathfrak{N}_p,$$

откъдето $g_j(x_1,\ldots,x_n) - g_j(p) + I(V) \in N_p$ и $g_j(x_1,\ldots,x_n) + I(V) \equiv g_j(p) + I(V) (\mathrm{mod}\ N_p)$. Следователно

$$N_p/N_p^2 = \left\{ \sum_{j=1}^{n}(x_j - p_j + I(V))g_j(p) + N_p^2 \;\middle|\; g_j(x_1,\ldots,x_n) \in \overline{\mathbb{F}_q}[x_1,\ldots,x_n] \right\}.$$

От друга страна,

$$(N_p)_{N_p} = \left\{ \sum_{j=1}^{n}(x_j - p_j + I(V))h_j \;\middle|\; h_j \in \mathcal{O}_p(V) \right\}$$

с $h_j - h_j(p) \in \mathfrak{M}_p$, откъдето

$$(N_p)_{N_p}/(N_p^2)_{N_p} = \left\{ \sum_{j=1}^{n}(x_j - p_j + I(V))h_j(p) + (N_p^2)_{N_p} \;\middle|\; h_j \in \mathcal{O}_p(V) \right\}$$

В резултат получаваме изоморфизма на $\overline{\mathbb{F}_q}$-линейни пространства

$$\mathfrak{M}_p/\mathfrak{M}_p^2 = (N_p)_{N_p}/(N_p^2)_{N_p} \simeq N_p/N_p^2. \tag{2.5}$$

По-точно, композицията на $\overline{\mathbb{F}_q}$-линейното влагане $N_p \hookrightarrow \mathfrak{M}_p = (N_p)_{N_p}$ с $\overline{\mathbb{F}_q}$-линейния епиморфизъм $\mathfrak{M}_p \to \mathfrak{M}_p/\mathfrak{M}_p^2$ дава $\overline{\mathbb{F}_q}$-линейното изображение

$$\psi : N_p \longrightarrow \mathfrak{M}_p/\mathfrak{M}_p^2,$$

$$\psi\left(\sum_{j=1}^{n}(x_j - p_j + I(V))(g_j(x_1,\ldots,x_n) + I(V))\right) = \sum_{j=0}^{n}(x_j - p_j + I(V))g_j(p) + \mathfrak{M}_p^2.$$

Непосредствено се вижда, че образът на ψ покрива $\mathfrak{M}_p/\mathfrak{M}_p^2$. За да проверим, че ядрото $\ker(\psi) = N_p^2$, да отбележим, че елементите на $\mathfrak{M}_p^2$ са от вида

$$h = \sum_{1\le i\le j\le n}(x_i - p_i + I(V))(x_j - p_j + I(V))h_{ij}$$

за някакви $h_{ij} \in \mathcal{O}_p(V) = \overline{\mathbb{F}_q}[V]_{N_p}$. Съществуват $g_{ij} \in \overline{\mathbb{F}_q}[V]$ и $g'_{ij} \in \overline{\mathbb{F}_q}[V] \setminus N_p$ с

$$\frac{g_{ij}}{g'_{ij}} = h_{ij}.$$

Произведението

$$g_o := \prod_{1\le i\le j\le n} g'_{ij} \in \overline{\mathbb{F}_q}[V] \setminus N_p$$

на знаменателите на h_{ij} е елемент на афинния координатен пръстен $\overline{\mathbb{F}_q}[V]$ извън идеала N_p, защото максималният идеал N_p е прост. Ясно е, че

$$g_o h = \sum_{1\le i\le j\le n}(x_i - p_i + I(V))(x_j - p_j + I(V))g_{ij} \in N_p^2.$$

Остава да покажем, че ако $h \in N_p \cap \mathfrak{M}_p^2$, то $h \in N_p^2$, за да получим, че $\ker(\psi) = N_p^2$. За целта разглеждаме $\overline{\mathbb{F}_q}$-линейното изображение

$$\mathrm{grad}'_p : N_p \longrightarrow \overline{\mathbb{F}_q}^n,$$

$$\mathrm{grad}'_p\left(\sum_{s=1}^{n}(x_s - p_s + I(V))t_s\right) = (t_1(p),\ldots,t_n(p))$$

за произволни $t_1,\ldots,t_n \in \overline{\mathbb{F}_q}[V]$. Ядрото

$$\ker(\mathrm{grad}'_p) = \left\{\sum_{s=1}^{n}(x_s - p_s + I(V))t_s \;\middle|\; t_1,\ldots,t_n \in N_p\right\} = N_p^2.$$

За всяко $h \in N_p \cap \mathfrak{M}_p^2$ съществува $g_o \in \overline{\mathbb{F}_q}[V] \setminus N_p$ с $g_o h \in N_p^2$. Следователно

$$0 = \mathrm{grad}'_p(g_o h) = g_o(p)\mathrm{grad}'_p(h),$$

съгласно $h(p) = 0$. От $g_o(p) \neq 0$ получаваме $\mathrm{grad}'_p(h) = 0$, т.е. $h \in \ker(\mathrm{grad}'_p) = N_p$ и доказваме $\overline{\mathbb{F}_q}$-линейния изоморфизъм (2.5).

Композицията на естествения епиморфизъм $\pi_V : \mathfrak{N}_p \to N_p = \mathfrak{N}_p/I(V)$ с ядро $\ker(\pi_V) = I(V)$ и на естествения епиморфизъм $\pi_2 : N_p \to N_p/N_p^2$ с ядро $\ker(\pi_2) = N_p^2$ дава епиморфизъм

$$\pi = \pi_2\pi_V : \mathfrak{N}_p \longrightarrow N_p/N_p^2$$

с ядро

$$\ker(\pi) = I(V) + \pi_V^{-1}(\ker(\pi_2)) = I(V) + \pi_V^{-1}(N_p^2) = I(V) + \mathfrak{N}_p^2.$$

По този начин получаваме изоморфизъм на пръстени

$$\mathfrak{N}_p/\ker(\pi) = \mathfrak{N}_p/(I(V) + \mathfrak{N}_p^2) \simeq N_p/N_p^2,$$

а оттам и изоморфизъм на $\overline{\mathbb{F}_q}$-линейни пространства

$$\mathfrak{M}_p/\mathfrak{M}_p^2 \simeq \mathfrak{N}_p/(I(V) + \mathfrak{N}_p^2).$$

Вземайки предвид, че $\mathfrak{N}_p^2$ е идеал в $\mathfrak{N}_p$ и $I(V) + \mathfrak{N}_p^2$, представяме

$$\mathfrak{M}_p/\mathfrak{M}_p^2 \simeq \left(\mathfrak{N}_p/\mathfrak{N}_p^2\right) / \left[(I(V) + \mathfrak{N}_p^2)/\mathfrak{N}_p^2\right]. \tag{2.6}$$

Твърдим, че от (2.4) и (2.6) следва

$$\dim_{\overline{\mathbb{F}_q}}\left(\mathfrak{M}_p/\mathfrak{M}_p^2\right) + \mathrm{rk}\left(\frac{\partial(f_1,\ldots,f_m)}{\partial(x_1,\ldots,x_n)}(p)\right) = \dim_{\overline{\mathbb{F}_q}}\left(\mathfrak{N}_p/\mathfrak{N}_p^2\right) = n.$$

Наистина, съгласно $g_j(x_1,\ldots,x_n) \equiv g_j(p) (\mathrm{mod}\ \mathfrak{N}_p)$ за произволен полином $g_j(x_1,\ldots,x_n) \in \overline{\mathbb{F}_q}[x_1,\ldots,x_n]$, елементите на $\mathfrak{N}_p/\mathfrak{N}_p^2$ са от вида

$$\sum_{j=1}^{n}(x_j - p_j)g_j(x_1,\ldots,x_n) + \mathfrak{N}_p^2 = \sum_{j=1}^{n}(x_j - p_j)g_j(p).$$

Хомогенен линеен полином $\sum\limits_{j=1}^{n} a_j(x_j - p_j)$ на $x_j - p_j$ с коефициенти $a_j \in \overline{\mathbb{F}_q}$ принадлежи на $\mathfrak{N}_p^2$ само когато всички $a_i = 0$.

По определение, точката $p \in V$ е гладка точно когато $\mathrm{rk}\frac{\partial(f_1,\ldots,f_m)}{\partial(x_1,\ldots,x_n)}(p) = n - 1$. Следователно гладкостта на $p \in V$ е еквивалентна на $\dim_{\overline{\mathbb{F}_q}}\left(\mathfrak{M}_p/\mathfrak{M}_p^2\right) = 1$. Прилагайки Твърдение 59 стигаме до извода, че p е гладка точка на афинната крива V тогава и само тогава, когато локалният пръстен $\mathcal{O}_p(V)$ е пръстен на дискретно нормиране.

□

Следствие 62. *Нека* $V = Z(f_1, \ldots, f_m) \subseteq \overline{\mathbb{F}_q}^n$ *е неприводима афинна крива с идеал*

$$I(V) = \langle f_1, \ldots, f_m \rangle = \sum_{i=1}^{m} f_i(x_1, \ldots, x_n)\overline{\mathbb{F}_q}[x_1, \ldots, x_n]$$

за някакви полиноми $f_i(x_1, \ldots, x_n) \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, *а* $p = (p_1, \ldots, p_n)$ *е гладка точка на* V *с максимален идеал* $\mathfrak{N}_p = \langle x_1 - p_1, \ldots, x_n - p_n \rangle = \sum_{j=1}^{n} (x_j - p_j)\overline{\mathbb{F}_q}[x_1, \ldots, x_n]$. *Тогава:*

(i) $\dim_{\overline{\mathbb{F}_q}} \left(\mathfrak{N}_p / I(V) + \mathfrak{N}_p^2\right) = 1$ *и произволна* $\overline{\mathbb{F}_q}$*-линейна комбинация*

$$t = \sum_{j=1}^{n} a_j(x_j - p_j)$$

на $x_1 - p_1, \ldots, x_n - p_n$ *извън* $I(V) + \mathfrak{N}_p^2$ *задава локален параметър* $t + I(V)$ *на локалния пръстен* $\mathcal{O}_p(V) = \overline{\mathbb{F}_q}[V]_{(\mathfrak{N}_p/I(V))}$ *на* p *във* V.

(ii) ако

$$\det \frac{\partial(f_1, \ldots, f_{n-1})}{\partial(x_1, \ldots, x_{n-1})}(p) \neq 0,$$

то $x_n - p_n + I(V)$ *е локален параметър на* $\mathcal{O}_p(V)$.

Доказателство: (i) Съгласно Теорема 61, локалният пръстен $\mathcal{O}_p(V)$ на p във V е пръстен на дискретно нормиране. Тогава по Твърдение 59, факторът $\mathfrak{M}_p/\mathfrak{M}_p^2$ е 1-мерно линейно пространство над полето $\mathcal{O}_p(V)/\mathfrak{M}_p = \overline{\mathbb{F}_q}$. В доказателството на Теорема 61 установихме изоморфизма

$$\mathfrak{M}/\mathfrak{M}_p^2 \simeq \mathfrak{N}_p/(I(V) + \mathfrak{N}_p^2)$$

на $\overline{\mathbb{F}_q}$-линейни пространства. Следователно $\dim_{\overline{\mathbb{F}_q}} \left(\mathfrak{N}_p/(I(V) + \mathfrak{N}_p^2)\right) = 1$ и произволен елемент

$$t = \sum_{j=1}^{n} a_j(x_j - p_j) \in l_{\overline{\mathbb{F}_q}}(x_1 - p_1, \ldots, x_n - p_n)$$

с $t + I(V) + \mathfrak{N}_p^2 \neq I(V) + \mathfrak{N}_p^2$ задава $\overline{\mathbb{F}_q}$-базис $t + I(V) + \mathfrak{N}_p^2$ на $\mathfrak{N}_p/(I(V) + \mathfrak{N}_p^2) \simeq \mathfrak{M}_p/\mathfrak{M}_p^2$. От Лемата на Nakayama следва, че ако $t + \mathfrak{M}_p^2 \neq \mathfrak{M}_p^2$, то $t + I(V) \in \mathfrak{M}_p$ е пораждащ на максималния идеал $\mathfrak{M}_p$ на локалния пръстен $\mathcal{O}_p(V)$. Оттук, $t + I(V)$ е локален параметър на класа дискретни нормирания на $\overline{\mathbb{F}_q}(V)$ с пръстен $\mathcal{O}_p(V)$.

(ii) Достатъчно е да докажем, че за всеки полином $f(x_1, \ldots, x_n)$ от идеала $I(V)$ на V е в сила

$$\sum_{j=1}^{n} \frac{\partial f}{\partial x_j}(p)(x_j - p_j) \in I(V) + \mathfrak{N}_p^2. \tag{2.7}$$

Тогава $\sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j}(p)(x_j - p_j) \in I(V) + \mathfrak{N}_p^2$ за $\forall 1 \leq i \leq m$ и

$$\frac{\partial(f_1, \ldots, f_{n-1})}{\partial(x_1, \ldots, x_n)}(p) \begin{pmatrix} x_1 - p_1 \\ \cdots \\ x_{n-1} - p_{n-1} \\ x_n - p_n \end{pmatrix} = 0_{n-1,1}.$$

След ляво умножение с $(n-1)\times(n-1)$-матрицата $\left(\frac{\partial(f_1,\ldots,f_{n-1})}{\partial(x_1,\ldots,x_{n-1})}(p)\right)^{-1}$ получаваме

$$x_1-p_1,\ldots,x_{n-1}-p_{n-1}\in l_{\overline{\mathbb{F}_q}}(x_n-p_n).$$

Ако допуснем, че $x_n-p_n\in I(V)+\mathfrak{N}_p^2$, то

$$\mathfrak{N}_p/(I(V)+\mathfrak{N}_p^2)=l_{\overline{\mathbb{F}_q}}(x_1-p_1,\ldots,x_{n-1}-p_{n-1},x_n-p_n)+I(V)+\mathfrak{N}_p^2=I(V)+\mathfrak{N}_p^2,$$

което противоречи на $\dim_{\overline{\mathbb{F}_q}}\left(\mathfrak{N}_p/(I(V)+\mathfrak{N}_p^2)\right)=1$. Следователно $x_n-p_n\notin I(V)+\mathfrak{N}_p^2$ и $x_n-p_n+I(V)$ е локален параметър на $\mathcal{O}_p(V)$, стига (2.7). За да докажем (2.7) да забележим, че произволен полином $f(x_1,\ldots,x_n)\in I(V)\subset\mathfrak{N}_p$ се разлага в сума

$$f(x_1,\ldots,x_n)=\sum_{s=1}^{d}f(x_1-p_1,\ldots,x_n-p_n)^{(s)}$$

на хомогенни полиноми $f(x_1-p_1,\ldots,x_n-p_n)^{(s)}$ на $x_1-p_1,\ldots,x_n-p_n$ от степен $s\geq 1$. Възоснова на

$$f(x_1,\ldots,x_n)-f(x_1-p_1,\ldots,x_n-p_n)^{(1)}=$$
$$=\sum_{s=2}^{d}f(x_1-p_1,\ldots,x_n-p_n)^{(s)}\in\mathfrak{N}_p^2\subseteq I(V)+\mathfrak{N}_p$$

имаме

$$f(x_1-p_1,\ldots,x_n-p_n)^{(1)}+I(V)+\mathfrak{N}_p^2=f(x_1,\ldots,x_n)+I(V)+\mathfrak{N}_p^2=I(V)+\mathfrak{N}_p^2. \quad (2.8)$$

Стойностите

$$\frac{\partial f}{\partial x_j}(p)=\frac{\partial f}{\partial(x_j-p_j)}(p)=\frac{\partial f(x_1-p_1,\ldots,x_n-p_n)^{(1)}}{\partial(x_j-p_j)}(p)$$

на формалните производни на $f(x_1,\ldots,x_n)$ относно x_j са коефициентите на x_j-p_j в $f(x_1-p_1,\ldots,x_n-p_n)^{(1)}$, така че

$$f(x_1-p_1,\ldots,x_n-p_n)^{(1)}=\sum_{j=1}^{n}\frac{\partial f}{\partial x_j}(p)(x_j-p_j). \quad (2.9)$$

Комбинирайки (2.8) с (2.9) получаваме (2.7).

□

От доказателството на Теорема 61 е ясно, че $\dim_{\overline{\mathbb{F}_q}}(\mathfrak{M}_p/\mathfrak{M}_p^2)\geq 1$. Следователно

$$\mathrm{rk}\frac{\partial(f_1,\ldots,f_m)}{\partial(x_1,\ldots,x_n)}(p)\leq n-1$$

и гладките точки на крива V са точките в общо положение.

Определение 63. *Точката p на неприводима проективна крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка, ако локалният пръстен $\mathcal{O}_p(X)$ във X е пръстен на дискретно нормиране.*

Точките $p \in X$, които не са гладки се наричат особени.

С X^{smooth} означаваме множеството на гладките точки върху X, а с X^{sing} - множеството на особените точки.

Ясно е, че точка p на неприводима проективна крива $X \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка точно когато за всяко стандартно афинно отворено подмножество $U_i \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, съдържащо p, точката p е гладка върху афинната крива $U_i \cap X$.

Твърдение 64. *Особените точки на неприводима алгебрична крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ са краен брой.*

Доказателство: Всяка неприводима проективна крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ има крайно покритие $X = \cup_{i=0}^{n}(X \cap U_i)$ от афинни криви. Достатъчно е да установим, че всяка афинна крива $X_o \subseteq \overline{\mathbb{F}_q}^n$ има краен брой особени точки. Ако идеалът

$$I(X_o) = \langle f_1, \ldots, f_m \rangle \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$$

на X_o се поражда от полиномите $f_i(x_1, \ldots, x_n) \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, то множеството X_o^{sing} на особените точки на V_o е афинното затворено подмножество

$$X_o^{\text{sing}} = Z\left(f_1, \ldots, f_m, \Delta_{j_1,\ldots,j_{n-1}}^{i_1,\ldots,i_{n-1}} \frac{\partial(f_1, \ldots, f_m)}{\partial(x_1, \ldots, x_n)}\right),$$

където

$$\Delta_{j_1,\ldots,j_{n-1}}^{i_1,\ldots,i_{n-1}} \frac{\partial(f_1, \ldots, f_m)}{\partial(x_1, \ldots, x_n)}$$

са минорите от ред $n-1$ на Якобиевата матрица

$$\frac{\partial(f_1, \ldots, f_m)}{\partial(x_1, \ldots, x_n)}.$$

Достатъчно е да проверим, че $X_o^{\text{sing}} \subsetneq X_o$ е собствено Зариски затворено подмножество. Известно е, че кривата X_o е бирационална на афинната права $\overline{\mathbb{F}_q}$ или X_o има афинен равнинен модел $W_o \subseteq \overline{\mathbb{F}_q}^2$. Афинната права е гладка, така че е достатъчно да докажем $W_o^{\text{sing}} \subsetneq W_o$, защото бирационалните изображения запазват размерността. Ако допуснем, че $W_o^{\text{sing}} = W_o = Z(f)$ за някакъв полином $f(x_1, x_2) \in \overline{\mathbb{F}_q}[x_1, x_2]$, то $\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2} \in I(W_o) = \langle f \rangle$. Но общата степен $\deg(f) > \deg\left(\frac{\partial f}{\partial x_i}\right)$ за $1 \leq i \leq 2$, откъдето $\frac{\partial f}{\partial x_1} \equiv 0$ и $\frac{\partial f}{\partial x_2} \equiv 0$ се анулират тъждествено. Това означава, че всички степенни показатели на мономите на $f(x_1, x_2)$ са кратни на характеристиката $p = \text{char}(\overline{\mathbb{F}_q})$ на полето $\overline{\mathbb{F}_q}$ от константи и съществува полином $h(x_1, x_2) \in \overline{\mathbb{F}_q}[x_1, x_2]$ с

$$h(x_1, x_2)^{p^l} = f(x_1, x_2) \quad \text{за някое} \quad l \in \mathbb{N}.$$

Това противоречи на неприводимостта на W_o и доказва $W_o^{\text{sing}} \subsetneq W_o$ е собствено афинно подмногообразие, а оттам и крайно подмножество. Следователно $X_o^{\text{sing}} \subsetneq X_o$ е

крайно подмножество, защото бирационалният модел W_o на X_o се различава от X_o по краен брой точки.

□

Лема 65. *Нека $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е неприводима проективна крива, P и Q са различни гладки точки от X, а ν_P и ν_Q са нормализираните дискретни нормирания на функционалното поле $\overline{\mathbb{F}_q}(X)$ на X, чиито пръстени съвпадат с локалните пръстени $\mathcal{O}_P(X)$ на P, съответно, $\mathcal{O}_Q(X)$ на Q. Тогава нормированията ν_P и ν_Q не са еквивалентни.*

Доказателство: Ако допуснем, че ν_P и ν_Q са еквивалентни, то локалните пръстени $\mathcal{O}_P(X) = \mathcal{O}_Q(X)$ на тези нормирания съвпадат. Ако

$$P = [a_0 : \ldots : a_n] \quad \text{и} \quad Q = [b_0 : \ldots : b_n] \quad \text{с} \quad a_i \neq 0, \quad b_i \neq 0 \quad \text{за някое } 0 \leq i \leq n,$$

то съществува индекс $j \in \{0, \ldots, n\} \setminus \{i\}$ с $\frac{a_j}{a_i} \neq \frac{b_j}{b_i}$. Тогава

$$\frac{x_j}{x_i} - \frac{a_j}{a_i} \in \mathfrak{M}_P(X)$$

е от максималния идеал $\mathfrak{M}_P(X)$ на локалния пръстен $\mathcal{O}_P(X)$ на P, но не и от максималния идеал $\mathfrak{M}_Q(X)$ на локалния пръстен $\mathcal{O}_Q(X)$ на Q. В резултат,

$$\frac{x_j}{x_i} - \frac{a_j}{a_i} \in \mathcal{O}_Q(X) \setminus \mathfrak{M}_Q(X) = \mathcal{O}_Q(X)^*$$

и

$$\left(\frac{x_j}{x_i} - \frac{a_j}{a_i}\right)^{-1} \in \mathcal{O}_Q(X), \quad \text{но} \quad \left(\frac{x_j}{x_i} - \frac{a_j}{a_i}\right)^{-1} \notin \mathcal{O}_P(X).$$

Противоречието доказва, че за всеки индекс $0 \leq i \leq n$ с $a_i \neq 0$ имаме $b_i = 0$.

За произволно $0 \leq i \leq n$ с $a_i \neq 0$ и $b_i = 0$ забелязваме, че $x_i \in \mathfrak{M}_Q(X)$, $x_i \in \mathcal{O}_P(X) \setminus \mathfrak{M}_P(X) = \mathcal{O}_P(X)^*$, откъдето $x_i^{-1} \in \mathcal{O}_P(X)$, $x_i^{-1} \notin \mathcal{O}_Q(X)$. Следователно дискретните нормирания ν_P и ν_Q, чиито пръстени съвпадат с локалните пръстени на различни гладки точки P и Q от проективна крива X не са еквивалентни.

□

Нека $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива. За да докажем, че всеки пръстен на дискретно нормиране R с поле от частни $\overline{k}(X)$ е локален пръстен $R = \mathcal{O}_p(X)$ на точка $p \in X$, ни е нужна следната

Лема 66. *Нека R е пръстен на дискретно нормиране с поле от частни K, а S е пръстен на дискретно нормиране, съдържащ R и съдържащ се строго в K. Тогава $R = S$ съвпадат.*

Доказателство: Допускаме противното и избираме елемент $x \in S \setminus R$. Ако $s \in S$ е локален параметър на S, то съществуват $u \in S^*$ и $m \in \mathbb{Z}^{\geq 0}$, така че $x = s^m u$. Ако $t \in R$ е локален параметър на R, то полето

$$K = \{t^z v \mid z \in \mathbb{Z}, \quad v \in R^*\} \cup \{0\},$$

така че $x = t^z v$ за подходящи $v \in R^*$ и $z \in \mathbb{Z}$, $z < 0$. Съгласно $t \in R \subseteq S$ съществуват $u_o \in S^*$ и $n \in \mathbb{Z}^{\geq 0}$ с $t = s^n u_o$. Ако допуснем, че $n = 0$, то $t \in S^*$ е обратим в S и полето от частни $K = F(R) \subseteq S$ на R се съдържа в S, противно на допускането $S \subsetneq K$. Следователно $n \geq 1$ и $x = s^m u = t^z v = s^{nz} u_o^z v$, откъдето

$$s^{nz-m} = u u_o^{-z} v^{-1} \in S^*,$$

съгласно $R^* \subseteq S^*$. Но $nz - m < 0$, така че $s^{nz-m} \in K \setminus S$ е от допълнението на S в K. Това противоречи на $S^* \cap (K \setminus S) = \emptyset$ и доказва съвпадението $R = S$.

□

Теорема 67. *Нека $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива с функционално поле $\overline{\mathbb{F}_q}(X)$. Тогава всеки пръстен на дискретно нормиране R с поле от частни $\overline{\mathbb{F}_q}(X)$ е локален пръстен $R = \mathcal{O}_p(X)$ на единствена точка $p \in X$.*

Доказателство: Без ограничение на общността можем да считаме, че проективната крива $X \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$ не се съдържа в собствено проективно подпространство на $\mathbb{P}^n(\overline{\mathbb{F}_q})$. (В противен случай, заменяме $\mathbb{P}^n(\overline{\mathbb{F}_q})$ с подходящо $\mathbb{P}^s(\overline{\mathbb{F}_q})$, $s < n$.) Тогава $\frac{x_i}{x_j}$ не се анулират тъждествено върху X и нормализираното дискретно нормиране

$$\nu : \overline{\mathbb{F}_q}(X) \longrightarrow \mathbb{Z} \cup \{\infty\}$$

с пръстен $\mathcal{O}_\nu = \{f \in \overline{\mathbb{F}_q}(X) \ \ |\nu(f) \geq 0\} = R$ достига краен максимум

$$\mu = \max_{0 \leq i,j \leq m} \nu\left(\frac{x_i}{x_j}\right)$$

върху $\frac{x_i}{x_j}$. След евентуална пермутация на хомогенните координати на $\mathbb{P}^n(\overline{\mathbb{F}_q})$ можем да считаме, че

$$\nu\left(\frac{x_0}{x_n}\right) = \mu.$$

Тогава

$$\nu\left(\frac{x_i}{x_n}\right) = \nu\left(\frac{x_0}{x_n} : \frac{x_0}{x_i}\right) = \mu - \nu\left(\frac{x_0}{x_i}\right) \geq 0$$

и афинният координатен пръстен

$$\overline{\mathbb{F}_q}[X \cap U_n] = \overline{\mathbb{F}_q}\left[\frac{x_0}{x_n}, \frac{x_1}{x_n}, \ldots, \frac{x_{n-1}}{x_n}\right] \subseteq R.$$

Максималният идеал $\mathfrak{M}$ на R пресича $\overline{\mathbb{F}_q}[X \cap U_n]$ в прост идеал $\mathfrak{p} = \mathfrak{M} \cap \overline{\mathbb{F}_q}[X \cap U_n]$, защото фактор-пръстенът

$$\overline{\mathbb{F}_q}[X \cap U_n]/\mathfrak{p} = \overline{\mathbb{F}_q}[X \cap U_n]/(\mathfrak{M} \cap \overline{\mathbb{F}_q}[X \cap U_n]) \simeq (\overline{\mathbb{F}_q}[X \cap U_n] + \mathfrak{M})/\mathfrak{M}$$

е подпръстен на полето $R/\mathfrak{M}$ от остатъци на ν. Простият идеал $\mathfrak{p} \lhd \overline{\mathbb{F}_q}[X \cap U_n]$ е ненулев, защото в противен случай $\overline{\mathbb{F}_q}[X \cap U_n]$ е подпръстен на полето $R/\mathfrak{M}$, откъдето и

функционалното поле $\overline{\mathbb{F}_q}(X) = F(\overline{\mathbb{F}_q}[X \cap U_n])$ е подполе на $R/\mathfrak{M}$. Това води до противоречие, защото крайното разширение $R/\mathfrak{M} \supseteq \overline{\mathbb{F}_q}$ е алгебрично, така че $R/\mathfrak{M}$ съвпада с $\overline{\mathbb{F}_q}$ и не може да съдържа разширението $\overline{\mathbb{F}_q}(X) \supset \overline{\mathbb{F}_q}$ от степен на трансцендентност 1.

В областта $\overline{\mathbb{F}_q}[V \cap U_m]$ с размерност на Krull 1 ненулевият прост идеал

$$\mathfrak{p} = \mathfrak{M} \cap \overline{\mathbb{F}_q}[V \cap U_m]$$

е максимален и отговаря на точка $p \in X$, т.е.

$$\mathfrak{p} = \langle x_1 - p_1 + I(X \cap U_m), \ldots, x_n - p_n + I(X \cap U_n) \rangle$$

за $p = (p_1, \ldots, p_n) \in X$. Локалният пръстен $\mathcal{O}_p(X)$ на p във X се съдържа в R, защото $\mathcal{O}_p(X) = \mathcal{O}_p(X \cap U_n) = \overline{\mathbb{F}_q}[X \cap U_n]_{\mathfrak{p}}$ е локализацията на $\overline{\mathbb{F}_q}[X \cap U_n]$ относно $\mathfrak{p}$, $\overline{\mathbb{F}_q}[X \cap U_n]$ е подпръстен на R и допълнението $\overline{\mathbb{F}_q}[X \cap U_n] \setminus \mathfrak{p} \subseteq R \setminus \mathfrak{M} \subseteq R^*$ на простия идеал $\mathfrak{p}$ в $\overline{\mathbb{F}_q}[X \cap U_n]$ се състои от обратими елементи на R. Съгласно Лема 66, от включването $\mathcal{O}_p(X) \subseteq R$ на пръстени на дискретно нормиране с поле от частни $\overline{\mathbb{F}_q}(X)$ следва съвпадението $\mathcal{O}_p(X) = R$. По Твърдение 65, точката $p \in X$ с $\mathcal{O}_p(X) = R$ е единствена.

□

Горните разглеждания установяват следната

Теорема 68. *Нека $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива с функционално поле $\overline{\mathbb{F}_q}(X)$ над алгебричната обвивка $\overline{\mathbb{F}_q}$ на крайно поле $\mathbb{F}_q$. Тогава съществува взаимно еднозначно съответствие между точките p на X и пръстените на дискретно нормиране $\mathcal{O}_p(X)$ с поле от частни $\overline{\mathbb{F}_q}(X)$.*

2.3.2 Локален пръстен на точка над крайно поле и орбити на абсолютната група на Галоа на това поле

Твърдение 69. *Нека $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива, определена над крайно поле $\mathbb{F}_q$, а $x, y \in X$ са точки с локални пръстени $\mathcal{O}_x(X), \mathcal{O}_y(X) \subset \overline{\mathbb{F}_q}(X)$. В такъв случай, x и y са от една и съща $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита върху X тогава и само тогава, когато сеченията $\mathcal{O}_x(X) \cap \mathbb{F}_q(X) = \mathcal{O}_y(X) \cap \mathbb{F}_q(X)$ на локалните пръстени на тези точки с функционалното поле $\mathbb{F}_q(X)$ на X над $\mathbb{F}_q$ съвпадат.*

Доказателство: Ако $y = \sigma(x)$ за $\sigma \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, то

$$\mathcal{O}_y(X) \cap \mathbb{F}_q(X) = \mathcal{O}_{\sigma(x)}(X) \cap \mathbb{F}_q(X) = [\sigma\mathcal{O}_x(X)] \cap \mathbb{F}_q(X) =$$

$$= \sigma[\mathcal{O}_x(X) \cap \mathbb{F}_q(X)] = \mathcal{O}_x(X) \cap \mathbb{F}_q(X).$$

Да допуснем, че $\mathcal{O}_x(X) \cap \mathbb{F}_q(X) = \mathcal{O}_y(X) \cap \mathbb{F}_q(X)$ и x, y лежат върху различни $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$- орбити

$$Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(x) = \{x = x_1, \ldots, x_m\} \quad \text{и} \quad Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(y) = \{y = y_1, \ldots, y_l\}.$$

Съгласно Апроксимационната Теорема 24, съществува $z \in \overline{\mathbb{F}_q}(X)$, така че

$$\nu_{x_i}(z) = -1 \quad \text{за} \quad \forall 1 \leq i \leq m,$$

$$\nu_{y_j}(z) = 1 \quad \text{за} \quad \forall 1 \leq j \leq l,$$

където ν_{x_i}, ν_{y_j} са дискретните нормирания на $\overline{\mathbb{F}_q}(X)$ с пръстени $\mathcal{O}_{x_i}(X)$, съответно, $\mathcal{O}_{y_j}(X)$. Избираме достатъчно голямо $m \in \mathbb{N}$, така че $\mathbb{F}_{q^m}$ да съдържа дефиниционните полета на x, y и $z \in \mathbb{F}_{q^m}(X)$.

За произволен елемент $\sigma \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ от абсолютната група на Galois на $\mathbb{F}_q$ твърдим, че

$$\nu_{\sigma^{-1}(x)}(z) = \nu_x(\sigma(z)).$$

Наистина, нека t е локален параметър на пръстена $\mathcal{O}_{\sigma^{-1}(x)}(X)$ на дискретното нормиране $\nu_{\sigma^{-1}(x)}$. Ако $z = t^m u$ за $m \in \mathbb{Z}$ и $u \in \mathcal{O}_{\sigma^{-1}(x)}(X)^*$, то $\nu_{\sigma^{-1}(x)}(z) = m$. Изоморфизмът на пръстени

$$\sigma : \mathcal{O}_{\sigma^{-1}(x)}(X) \longrightarrow \mathcal{O}_x(X)$$

трансформира максималния идеал $\mathfrak{M}_{\sigma^{-1}(x)} = t\mathcal{O}_{\sigma^{-1}(x)}(X)$ на $\mathcal{O}_{\sigma^{-1}(x)}(X)$, породен от t върху максималния идеал $\mathfrak{M}_x(X) = \sigma(t)\mathcal{O}_x(X)$ на $\mathcal{O}_x(X)$, породен от $\sigma(t)$. Аналогично, $\sigma\mathcal{O}_{\sigma^{-1}(x)}(X)^* = \mathcal{O}_x(X)^*$ за съответните мултипликативни групи, така че $\sigma(z) = \sigma(t)^m\sigma(u)$ с $m \in \mathbb{Z}$ и $\sigma(u) \in \mathcal{O}_x(X)$. Понеже $\sigma(t)$ е локален параметър на $\mathcal{O}_x(X)$, оттук получаваме $\nu_x(\sigma(z)) = m = \nu_{\sigma^{-1}(x)}(z)$.

Ако

$$\alpha = N_{\mathbb{F}_q(X)}^{\mathbb{F}_{q^m}(X)}(z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^m}(X)/\mathbb{F}_q(X))} \sigma(z) = \prod_{\sigma \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(z)$$

е нормата на z относно $\mathbb{F}_q(X)$, то

$$\nu_x(\alpha) = \sum_{\sigma \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)} \nu_x(\sigma(z)) = \sum_{\sigma \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)} \nu_{\sigma^{-1}(x)}(z) = m(-1) = -m,$$

$$\nu_y(\alpha) = \sum_{\sigma \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)} \nu_y(\sigma(z)) = \sum_{\sigma \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)} \nu_{\sigma^{-1}(y)}(z) = m.1 = m.$$

Следователно $\alpha \notin \mathcal{O}_x(X) \cap \mathbb{F}_q(X)$, $\alpha \in \mathcal{O}_q(X) \cap \mathbb{F}_q(X)$. Това противоречи на предположението $\mathcal{O}_x(X) \cap \mathbb{F}_q(X) = \mathcal{O}_y(X) \cap \mathbb{F}_q(X)$ и доказва, че x и y принадлежат на една и съща $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита, стига $\mathcal{O}_x(X) \cap \mathbb{F}_q(X) = \mathcal{O}_y(X) \cap \mathbb{F}_q(X)$.

□

Теорема 70. *Нека $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива, определена над крайно поле $\mathbb{F}_q$. Тогава орбитите на абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на $\mathbb{F}_q$ от степен m са във взаимно еднозначно съответствие с класовете дискретни нормирания от степен m на функционалното поле $\mathbb{F}_q(X)$ на X над $\mathbb{F}_q$.*

Доказателство: Разглеждаме орбита

$$Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(p) = \{p, \Phi_q(p), \ldots, \Phi^{q^{m-1}}(p)\} \subset X$$

от степен m, съответните локални пръстени $\mathcal{O}_{\Phi_{q^i}(p)}(X) = \Phi^{q^i}\mathcal{O}_p(X) \subset \overline{\mathbb{F}_q}(X)$ и сеченията им

$$\mathcal{O}_{\Phi_{q^i}(p)}(X) \cap \mathbb{F}_q(X) = (\Phi^{q^i}\mathcal{O}_p(X)) \cap \mathbb{F}_q(X)$$

с $\mathbb{F}_q(X)$ за $\forall 0 \leq i \leq m-1$. Да напомним, че $\mathcal{O}_p(X)$ е пръстенът на дискретното нормиране ν_p в $\overline{\mathbb{F}_q}(X)$. Следователно $\mathcal{O}_p(X) \cap \mathbb{F}_q(X)$ е пръстенът на ограничението $\nu_p|_{\mathbb{F}_q(X)}$, което е дискретно нормиране на $\mathbb{F}_q(X)$.

Ако $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(p) \neq Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(r)$ са различни, (а оттук и непресичащи се) $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбити, то пръстените $\mathcal{O}_p(X) \cap \mathbb{F}_q(X)$, съответно, $\mathcal{O}_r(X) \cap \mathbb{F}_q(X)$ на нормиранията $\nu_p|_{\mathbb{F}_q(X)}$, $\nu_r|_{\mathbb{F}_q(X)}$ са различни съгласно Твърдение 69. Следователно дискретните нормирания $\nu_p|_{\mathbb{F}_q(X)}$ и $\nu_r|_{\mathbb{F}_q}$ на $\mathbb{F}_q(X)$ са нееквивалентни.

Обратно, нека $\nu : \mathbb{F}_q(X) \to \mathbb{Z} \cup \{\infty\}$ е дискретно нормиране от степен m. Тогава ν се повдига до m класа на еквивалентност $w_1, \ldots, w_m$ на дискретни нормирания от степен 1 на $\mathbb{F}_{q^m}(X)$. Пръстените $\mathcal{O}_{w_j}$ на дискретните нормирания w_j на $\mathbb{F}_{q^m}(X)$ се разширяват до пръстени $\mathcal{O}_{w_j} * \overline{\mathbb{F}_q}$ на дискретни нормирания на $\overline{\mathbb{F}_q}(X)$. Следователно съществуват точки $p_j \in X$, чиито локални пръстени $\mathcal{O}_{p_j}(X) = \mathcal{O}_{w_j} * \overline{\mathbb{F}_q}$ над $\overline{\mathbb{F}_q}$ съвпадат с пръстените на продължения на w_j в $\overline{\mathbb{F}_q}(X)$. Множеството $\{p_1, \ldots, p_m\}$ е $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита, защото

$$\mathcal{O}_{p_j} \cap \mathbb{F}_q(X) = \mathcal{O}_{w_j} \cap \mathbb{F}_q(X) = \mathcal{O}_v = \mathcal{O}_{w_i} \cap \mathbb{F}_q(X) = \mathcal{O}_{p_i}(X) \cap \mathbb{F}_q(X)$$

за произволни $1 \leq i, j \leq m$. Това доказва съществуването на взаимно еднозначно съответствие между $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитите върху X и класовете дискретни нормирания на $\mathbb{F}_q(X)$.

За съвпадението на степените остава да проверим, че произволно дискретно нормиране $\nu : \mathbb{F}_q(X) \to \mathbb{Z} \cup \{\infty\}$ от степен m отговаря на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбита $\{p_1, \ldots, p_m\}$ с точно m различни елемента. Ако $p_i = p_j$ за някои $1 \leq i < j \leq m$, то $\mathcal{O}_{p_i}(X) = \mathcal{O}_{p_j}(X)$ и

$$\mathcal{O}_{w_i} = \mathcal{O}_{p_i}(X) \cap \mathbb{F}_{q^m}(X) = \mathcal{O}_{p_j}(X) \cap \mathbb{F}_{q^m}(X) = \mathcal{O}_{w_j},$$

което противоречи на нееквивалентността на дискретните нормирания w_i и w_j на $\mathbb{F}_{q^m}(X)$.

□

2.4 Дивизори и Теорема на Риман

2.4.1 Дивизори и пространства на Риман-Рох

Определение 71. *Нека $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива, определена над крайно поле $\mathbb{F}_q$, $F = \mathbb{F}_q(X)$ е функционалното поле на X над $\mathbb{F}_q$, а $\mathcal{P}$ е множеството на класовете на еквивалентност на дискретните нормирания на F. Тогава $\mathbb{Z}$-линейните комбинации*

$$D = \sum_{v \in \mathcal{P}} n_v v, \quad n_v \in \mathbb{Z}$$

с краен носител се наричат дивизори на F.

Множеството $Div(F)$ на дивизорите на F е $\mathbb{Z}$-модул или абелева група.

Определение 72. *Дивизорът* $D = \sum_{v \in \mathcal{P}} n_v v$ *е ефективен, ако* $n_v \geq 0$ *за* $\forall v \in \mathcal{P}$.

Определение 73. *Степента на дивизор* $D = \sum_{v \in \mathcal{P}} n_v v$ *е*

$$\deg(D) = \sum_{v \in \mathcal{P}} n_v \deg(v),$$

където $\deg(v) = [\mathcal{O}_v/\mathfrak{M}_v : k]$ *са степените на класовете дискретни нормирания* v *на* F.

Степента на дивизор е хомоморфизъм на $\mathbb{Z}$-модули, защото

$$\deg\left(\sum_{v\in\mathcal{P}} n_v v + \sum_{v\in\mathcal{P}} m_v v\right) = \deg\left(\sum_{v\in\mathcal{P}} (n_v + m_v) v\right) = \sum_{v\in\mathcal{P}} (n_v + m_v)\deg(v) =$$

$$= \sum_{v\in\mathcal{P}} n_v \deg(v) + \sum_{v\in\mathcal{P}} m_v \deg(v) = \deg\left(\sum_{v\in\mathcal{P}} n_v v\right) + \deg\left(\sum_{v\in\mathcal{P}} m_v v\right).$$

Множеството $Div^0(F) = \ker(\deg)$ на дивизорите от степен 0 е $\mathbb{Z}$-подмодул на $Div(F)$.

Дивизорът на нулите на рационална функция $x \in F$ е

$$(x)_0 = \sum_{v\in\mathcal{P}, v(x)>0} v(x) v,$$

а дивизорът на полюсите е

$$(x)_\infty = \sum_{v\in\mathcal{P}, v(x)<0} [-v(x)] v.$$

Лема 74. *Нека* $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ *е гладка неприводима проективна крива, определена над* $\mathbb{F}_q$, $F = \mathbb{F}_q(X)$ *е функционалното поле на* X *над* $\mathbb{F}_q$ *и* $x \in F \setminus \mathbb{F}_q$. *Тогава степента*

$$\deg(x)_0 \leq [F : \mathbb{F}_q(x)]$$

на дивизора на нулите на x *не надминава степента на крайното разширение* $F = \mathbb{F}_q(X) \supseteq \mathbb{F}_q(x)$ *на полето* $\mathbb{F}_q(x)$ *на рационалните функции на* x *с коефициенти от* $\mathbb{F}_q$.

Доказателство: Елементът $x \in F \setminus \mathbb{F}_q$ е трансцендентен над $\mathbb{F}_q$, съгласно алгебричната затвореност на $\mathbb{F}_q$ в $F = \mathbb{F}_q(X)$. Следователно разширението $F \supseteq \mathbb{F}_q(x)$ е крайно и можем да означим степента му с $n = [F : \mathbb{F}_q(x)]$. Да допуснем, че

$$n < \deg(x)_0 = \sum_{v\in\mathcal{P}, v(x)>0} v(x) v.$$

Тогава съществува крайна сума

$$\sum_{j=1}^{r} v_j(x)\deg(v_j) > n, \tag{2.10}$$

защото ако всички крайни суми са $\leq n$, то и границата им е $\leq n$. Съгласно Апроксимационната Теорема 24, за $\forall 1 \leq j \leq r$ съществува $y_j \in F$, така че

$$v_j(y_j) = -1, \quad v_i(y_j) = 0 \quad \text{за} \quad \forall i \in \{1, \ldots, r\} \setminus \{j\}.$$

Тогава $t_j = y_j^{-1}$ са локални параметри на пръстените $\mathcal{O}_{v_j}$ на класовете дискретни нормирания v_j и $v_i(t_j) = 0$ за $\forall i \in \{1, \ldots, r\} \setminus \{j\}$. Избираме базиси

$$\{\alpha_{js} + \mathfrak{M}_{v_j} \mid 1 \leq s \leq \deg(v_j) = \dim_{\mathbb{F}_q}(\mathcal{O}_{v_j}/\mathfrak{M}_{v_j})\}$$

на полетата от остатъци $\mathcal{O}_{v_j}/\mathfrak{M}_{v_j}$ над $\mathbb{F}_q$ с $\alpha_{js} \in \mathcal{O}$ за сечението $\mathcal{O} = \cap_{j=1}^{r}\mathcal{O}_{v_j}$. За целта трябва да проверим, че за всяко $\beta \in \mathcal{O}_{v_j}$ съществува $\alpha \in \mathcal{O}$ с $\beta - \alpha \in \mathfrak{M}_{v_j}$. Това следва от Апроксимационната Теорема 24, съгласно която за произволен елемент $\beta \in \mathcal{O}_{v_j}$ съществува $\alpha \in F$ с

$$v_j(\alpha - \beta) \geq 1 \quad \text{и} \quad v_i(\alpha) \geq 0 \quad \text{за} \quad \forall 1 \leq i \leq r, \quad i \neq j.$$

Достатъчно е да докажем линейната независимост на

$$\{\alpha_{js}t_j^{-i} \mid 1 \leq s \leq \deg(v_j), \quad 1 \leq i \leq v_j(x), \quad 1 \leq j \leq r\}$$

над $\mathbb{F}_q(x)$, за да получим $\sum\limits_{j=1}^{r} v_j(x)\deg(v_j) \leq [F : \mathbb{F}_q(x)]$, противно на (2.10). Да допуснем, че съществуват $h_{j,i,s}(x) \in k(x)$ с

$$\sum_{j=1}^{r}\sum_{s=1}^{\deg(v_j)}\sum_{i=1}^{v_j(x)} h_{j,i,s}(x)\alpha_{js}t_j^{-i} = 0 \tag{2.11}$$

и поне едно $h_{j_o,i_o,s_o}(x) \neq 0$. След почленно умножение с най-малкия общ знаменател на рационалните функции $h_{j,i,s}(x)$ на x можем да считаме, че $h_{j,i,s}(x) \in \mathbb{F}_q[x]$ са полиноми на x. Представяме полиномите

$$h_{j,i,s}(x) = k_{j,i,s} + xg_{j,i,s}(x)$$

като суми на свободните им членове $k_{j,i,s} = h_{j,i,s}(0)$ и полиноми с частни $g_{j,i,s}(x)$ при деление с x. Разбиваме (2.11) в две суми

$$\sum_{j=1}^{r}\sum_{i=1}^{v_j(x)}\sum_{s=1}^{\deg(v_j)} k_{j,i,s}\alpha_{js}t_j^{-i} + x\sum_{j=1}^{r}\sum_{i=1}^{v_j(x)}\sum_{s=1}^{\deg(v_j)} g_{j,i,s}(x)\alpha_{js}t_j^{-i} = 0. \tag{2.12}$$

От $\alpha_{j,s} \in \mathcal{O}_{v_j} \setminus \mathfrak{M}_{v_j} = \mathcal{O}_{v_j}^*$ следва

$$A_{j,i} = \sum_{s=1}^{\deg(v_j)} k_{j,i,s}\alpha_{js} \in \mathcal{O}_{v_j}.$$

Съгласно линейната независимост на $\{\alpha_{js} + \mathfrak{M}_{v_j} \mid 1 \leq s \leq \deg(v_j)\}$ над $\mathbb{F}_q$, допускането $A_{j,i} \in \mathfrak{M}_{v_j}$ води до $k_{j,i,s} = 0$ за $\forall 1 \leq s \leq \deg(v_j)$ и фиксираните $1 \leq j \leq r$, $1 \leq i \leq v_j(x)$. От друга страна,

$$B_{j,i} = \sum_{s=1}^{\deg(v_i)} g_{j,i,s}(x)\alpha_{js} \in \mathcal{O}_{v_j},$$

защото $\alpha_{js} \in \mathcal{O}_{v_j}$ и $g_{j,i,s}(x) \in \mathbb{F}_q[x] \subseteq \mathcal{O}_{v_j}$ за $v_j(x) > 0$. По този начин получаваме

$$\sum_{j=1}^{r}\sum_{i=1}^{v_j(x)} A_{j,i}t_j^{-i} + x\sum_{j=1}^{r}\sum_{i=1}^{v_j(x)} B_{j,i}t_j^{-i} = 0. \tag{2.13}$$

Ако всички $A_{j,i} = 0$, то делим на подходяща степен на x и получаваме (2.13) с поне едно $A_{j_o,i_o} \neq 0$ и $A_{j,i} \in \mathcal{O}_{v_j}^*$ за $\forall A_{j,i} \neq 0$. Тогава $v_j\left(A_{j,i}t_j^{-i}\right) = -i$ за $\forall A_{j,i} \neq 0$ и прилагайки неравенството на триъгълника с равенство за ненулевите събираеми на $\sum_{i=1}^{v_{j_o}(x)} A_{j_o,i}t_{j_o}^{-i}$ получаваме

$$v_{j_o}\left(\sum_{i=1}^{v_{j_o}(x)} A_{j_o,i}t_{j_o}^{-i}\right) = -i_1 < 0$$

за максималното естествено i_1 с $A_{j_o,i_1} \neq 0$. Неравенството на триъгълника за останалите събираеми в лявата сума от (2.13) дава

$$v_{j_o}\left(\sum_{j\neq j_o}\sum_{i=1}^{v_j(x)} A_{j,i}t_j^{-i}\right) \geq 0,$$

съгласно $A_{j,i} \in \mathcal{O} \subseteq \mathcal{O}_{v_{j_o}}$ и $v_{j_o}(t_j) = 0$ за $\forall j \neq j_o$. Общо, стойността на v_{j_o} върху лявата сума от (2.13) е

$$v_{j_o}\left(\sum_{j=1}^{r}\sum_{i=1}^{v_j(x)} A_{j,i}t_j^{-i}\right) = -i_1 < 0,$$

съгласно неравенството на триъгълника с равенство. По-нататък, за $\forall 1 \leq i \leq v_{j_o}(x)$ имаме $v_{j_o}(xt_{j_o}^{-i}) = v_{j_o}(x) - i \geq 0$ и $v_{j_o}(B_{j_o,i}) \geq 0$, откъдето

$$v_{j_o}\left(x\sum_{i=1}^{v_{j_o}(x)} B_{j_o,i}t_{j_o}^{-i}\right) \geq 0.$$

За произволно $j \in \{1, \ldots, r\} \setminus \{j_o\}$ е в сила $v_{j_o}(t_j^{-i}) = 0$, откъдето

$$v_{j_o}(xB_{j,i}t_j^{-i}) = v_{j_o}(x) + v_{j_o}(B_{j,i}) > 0,$$

съгласно $v_{j_o}(x) > 0$ и $v_{j_o}(B_{j,i}) \geq 0$. Прилагайки неравенството на триъгълника получаваме

$$v_{j_o}\left(x \sum_{j \neq j_o} \sum_{i=1}^{v_j(x)} B_{j,i}t_j^{-i}\right) > 0 \quad \text{и} \quad v_{j_o}\left(x \sum_{j=1}^{r} \sum_{i=1}^{v_j(x)} B_{j,i}t_j^{-i}\right) \geq 0.$$

Сега

$$0 > -i_1 = v_{j_o}\left(\sum_{j=1}^{r} \sum_{i=1}^{v_j(x)} A_{j,i}t_j^{-i}\right) = v_{j_o}\left(-\sum_{j=1}^{r} \sum_{i=1}^{v_j(x)} A_{j,i}t_j^{-i}\right) =$$

$$= v_{j_o}\left(x \sum_{j=1}^{r} \sum_{i=1}^{v_j(x)} B_{j,i}t_j^{-i}\right) \geq 0$$

е противоречие, доказващо линейната независимост на

$$\{\alpha_{js}t_j^{-i} \mid 1 \leq s \leq \deg(v_j), \quad 1 \leq i \leq v_j(x), \quad 1 \leq j \leq r\}.$$

□

Следствие 75. *Нека $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива, определена над крайно поле $\mathbb{F}_q$ и $F = \mathbb{F}_q(X)$ е функционалното поле на X над $\mathbb{F}_q$. Тогава всеки елемент $x \in F \setminus \mathbb{F}_q$ има най-много краен брой нули $v \in \mathcal{P}$, $v(x) > 0$ и най-много краен брой полюси $v \in \mathcal{P}$, $v(x) < 0$.*

Доказателство: От

$$\sum_{v \in \mathcal{P}, v(x) > 0} v(x) \deg(v) = \deg(x)_0 \leq [F : \mathbb{F}_q(x)] = n$$

следва, че класовете дискретни нормирания $v \in \mathcal{P}$ с $v(x) > 0$ са не повече от n, защото степените $\deg(v)$ са естествени числа. Вземайки предвид, че $v\left(\frac{1}{x}\right) = -v(x) > 0$ точно когато $v(x) < 0$, стигаме до извода, че полюсите $v \in \mathcal{P}$ на x са точно нулите на $\frac{1}{x}$. От

$$\sum_{v \in \mathcal{P}, v\left(\frac{1}{x}\right) > 0} v\left(\frac{1}{x}\right) \deg(v) = \deg\left(\frac{1}{x}\right)_0 \leq \left[F : \mathbb{F}_q\left(\frac{1}{x}\right)\right]$$

получаваме, че $v \in \mathcal{P}$ с $v(x) < 0$ са краен брой или полюсите на x са краен брой.

□

Следствие 76. *Нека $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива, определена над крайно поле $\mathbb{F}_q$, $F = \mathbb{F}_q(X)$ е функционалното поле на X над $\mathbb{F}_q$ и $x \in F \setminus \mathbb{F}_q$ е неконстантен елемент. Тогава x има поне един полюс и поне една нула.*

Затова изображението

$$div : F^* \longrightarrow Div(F),$$

$$div(x) = \sum_{v\in\mathcal{P}} v(x)v = \sum_{v\in\mathcal{P}, v(x)>0} v(x)v - \sum_{v\in\mathcal{P}, v(x)<0} (-v(x))v = (x)_0 - (x)_\infty$$

е хомоморфизъм на групи с ядро $\ker(div) = \mathbb{F}_q^*$.

Доказателство: Достатъчно е да проверим, че всеки елемент $x \in F\setminus\mathbb{F}_q$ има поне един полюс, защото тогава $\frac{1}{x} \in F\setminus\mathbb{F}_q$ ще има поне един полюс и $x \in F\setminus\mathbb{F}_q$ ще има поне една нула. Да допуснем, че $x \in F\setminus\mathbb{F}_q$ няма полюси, т.е. $v(x) \geq 0$ за $\forall v \in \mathcal{P}$. Тогава за всички класове дискретни нормирания w на $\overline{\mathbb{F}_q}(X) = F*\overline{\mathbb{F}_q}$ е в сила $w(x) \geq 0$, защото $w|_F = v$. Класовете дискретни нормирания w на $\overline{\mathbb{F}_q}(X)$ са във взаимно еднозначно съответствие с точките p на гладката проективна крива X. Следователно $x \in \cap_{p\in X}\mathcal{O}_p(X) = \mathcal{O}_X(X)$. Разглеждаме проективния морфизъм

$$\Phi_x : X \longrightarrow \mathbb{P}^1(\overline{\mathbb{F}_q}),$$

$$\Phi_x(p) = [x(p) : 1].$$

Съгласно Теоремата за образа на проективно многообразие под действие на регулярно изображение, образът $\Phi_x(X)$ е затворено подмножество на $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Вземайки предвид неприводимостта на $\Phi_x(X)$, получаваме, че $\Phi_x(X) = \mathbb{P}^1(\overline{\mathbb{F}_q})$ или $\Phi_x(X)$ е точка. От $[1 : 0] \notin \Phi_x(X)$ става ясно, че $\Phi_x(X) = \{[c : 1]\}$ е точка и $x \equiv c \in \mathbb{F}_q$ е константа. Противоречието доказва, че всеки елемент $x \in F \setminus \mathbb{F}_q$ има поне един полюс.

Изображението $div : F^* \to Div(F)$ е хомоморфизъм на групи, защото

$$div(xy) = \sum_{v\in\mathcal{P}} v(xy)v = \sum_{v\in\mathcal{P}} (v(x) + v(y))v = \sum_{v\in\mathcal{P}} v(x)v + \sum_{v\in\mathcal{P}} v(y)v = div(x) + div(y).$$

Елементите на $\mathbb{F}_q^*$ нямат нито нули, нито полюси, така че $\mathbb{F}_q^* \subseteq \ker(div)$. Ако допуснем, че съществува $x \in \ker(div) \setminus \mathbb{F}_q^*$, то $x \in F \setminus \mathbb{F}_q$ и x има както нула $v \in \mathcal{P}$, $v(x) > 0$, така и полюс $w \in \mathcal{P}$, $w(x) < 0$. В резултат, $div(x) = \sum\limits_{v\in\mathcal{P}} v(x)v \neq 0$, противно на $x \in \ker(div)$. Това доказва, че $\ker(div) = \mathbb{F}_q^*$.

□

Дивизорите върху проективни многообразия са асоцирани с линейни разслоения. Преди да опишем това съответствие да напомним, че векторно разслоение E над многообразие M е фамилия $E = \cup_{x\in M}E_x$ от линейни пространства $E_x \simeq \overline{\mathbb{F}_q}^r$, параметризирана от точките x на M. Тази фамилия има регулярна проекция $\pi : E \to M$, изобразяваща E_x в x и за всяка точка $x_o \in M$ съществуват отворена околност U на x_o върху M и тривиализация $\varphi_U : \pi^{-1}(U) \to U \times \overline{\mathbb{F}_q}^r$ на E върху U с $\varphi_U(E_x) = \{x\} \times \overline{\mathbb{F}_q}^r$. Векторното разслоение $E \to M$ е от ранг r, ако $E_x \simeq \overline{\mathbb{F}_q}^r$ за $\forall x \in M$. Векторните разслоения от ранг 1 се наричат линейни. Ако φ_U и φ_V са тривиализации на векторното разслоение E над пресичащи се отворени подмножества U и V на M,

то изображението $g_{UV} = \varphi_U \varphi_V^{-1} : U \cap V \to GL(r, \overline{\mathbb{F}_q})$ се нарича функция на прехода на от V към U. Функциите на прехода изпълняват тъждествата

$$g_{UV}(x) g_{VU}(x) = E_r \quad \text{за} \quad \forall x \in U \cap V \quad \text{и} \tag{2.14}$$

$$g_{UV}(x) g_{VW}(x) g_{WU}(x) = E_r \quad \text{за} \quad \forall x \in U \cap V \cap W, \tag{2.15}$$

където E_r е единичната матрица от ред r. Обратно, нека $M = \cup_{\alpha \in A} U_\alpha$ е отворено покритие на M с изображения $g_{\alpha,\beta} : U_\alpha \cap U_\beta \to GL(r, \overline{\mathbb{F}_q})$, изпълняващи равенствата (2.14) и (2.15). Твърдим, че съществува единствено векторно разслоение $E \to M$ с ранг r с функции на прехода $\{g_{\alpha,\beta}\}_{\alpha,\beta \in A}$. За целта разглеждаме обединението $\cup_{\alpha \in A}(U_\alpha \times \overline{\mathbb{F}_q}^r)$. Отъждествяваме $(x, v) \in U_\beta \times \overline{\mathbb{F}_q}^r$ с $(x, g_{\alpha,\beta}(x)v) \in U_\alpha \times \overline{\mathbb{F}_q}^r$ за $\forall \alpha, \beta \in A$, $\alpha \neq \beta$ и означаваме полученото пространство с E. Непосредствено се проверява, че E е векторно разслоение от ранг r върху M с функции на прехода $g_{\alpha,\beta}$.

Нека $\pi : L \to M$ е линейно разслоение с тривиализации $\varphi_\alpha : \pi^{-1}(U_\alpha) \to U_\alpha \times \overline{\mathbb{F}_q}$ за $\alpha \in A$. Произволни неанулиращи се регулярни функции $f_\alpha \in \mathcal{O}^*(U_\alpha)$ задават тривиализации $\varphi'_\alpha = f_\alpha \varphi_\alpha : \pi^{-1}(U_\alpha) \to U_\alpha \times \overline{\mathbb{F}_q}$ с функции на прехода $g'_{\alpha,\beta} = \left(\frac{f_\alpha}{f_\beta}\right) g_{\alpha,\beta}$. Обратно, произволни тривиализации $\varphi''_\alpha : \pi^{-1}(U_\alpha) \to U_\alpha \times \overline{\mathbb{F}_q}$ на $\pi : L \to M$ имат частни $\frac{\varphi''_\alpha}{\varphi_\alpha} \in \overline{\mathbb{F}_q}^*$, така че функциите на прехода $\{g_{\alpha,\beta}\}_{\alpha,\beta \in A}$ и $\{g'_{\alpha,\beta}\}_{\alpha,\beta \in A}$ определят едно и също линейно разслоение тогава и само тогава, когато съществуват функции $f_\alpha \in \mathcal{O}^*(U_\alpha)$ с $g'_{\alpha,\beta} = \left(\frac{f_\alpha}{f_\beta}\right) g_{\alpha,\beta}$.

Нека X е крива, определена над крайно поле $\mathbb{F}_q$. Съгласно Теорема 70, класовете дискретни нормирания v на функционалното поле $F = \mathbb{F}_q(X)$ на X над $\mathbb{F}_q$ са във взаимно еднозначно съответствие с орбитите $Orb_{\mathfrak{G}}(p)$, $p \in X$ на абсолютната група на Галоа $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Произволен дивизор $D = \sum\limits_{v \in \mathcal{P}} n_v v$ върху X може да се интерпретира като $\mathbb{Z}$-линейна комбинация на $\mathfrak{G}$-орбити

$$D = \sum_{p \in X} n_p Orb_{\mathfrak{G}}(p),$$

където сумирането е по краен брой представители на $\mathfrak{G}$-орбити върху X. В резултат, съществува отворено покритие $X = \cup_{\alpha \in A} U_\alpha$, така че $U_\alpha \cap D = div(f_\alpha)$ са главни дивизори. Локалните уравнения f_α на D върху U_α имат неанулиращи се регулярни частни

$$g_{\alpha,\beta} = \frac{f_\alpha}{f_\beta}\Big|_{U_\alpha \cap U_\beta}.$$

Непосредствено се проверява, че $g_{\alpha,\beta} = \frac{f_\alpha}{f_\beta}\Big|_{U_\alpha \cap U_\beta}$ изпълняват тъждествата (2.14) и (2.15), така че $\{g_{\alpha,\beta}\}_{\alpha,\beta \in A}$ са функции на прехода на линейно разслоение над X. Това линейно разслоение се бележи с L_D и се нарича асоцирано с дивизора D.

Ако $\pi : L_D \to X$ е проекцията на линейното разслоение, асоцирано с дивизора D, то изображенията $s : X \to L_D$ с $\pi s = \mathrm{Id}_X$ се наричат глобални сечения на L_D. Нека $s_o : X \to L_D$ е глобално рационално сечение с дивизор $div(s_o) = D$, а $\Gamma(X, L_D)$ е множеството на глобалните регуларни сечения на L_D. Множеството

$$\mathcal{L}(D) = \{f \in \mathbb{F}_q(X)^* \ \mid \ div(f) + D \geq 0\} \cup \{0\}.$$

наричаме пространство на Риман-Рох на D. Твърдим, че $\mathcal{L}(D)$ от рационални функции върху X е линейно пространство над $\mathbb{F}_q$. Наистина, условието $\alpha f \in \mathcal{L}(D)$ за $\forall f \in \mathcal{L}(D)$ и $\forall \alpha \in \mathbb{F}_q$ е ясно. Нека $D = \sum\limits_{v\in\mathcal{P}} n_v v$ с $n_v \in \mathbb{Z}$, а $f, g \in \mathcal{L}(D)$. Условието

$$div(f) + D = \sum_{v\in\mathcal{P}} v(f)v + \sum_{v\in\mathcal{P}} n_v v = \sum_{v\in\mathcal{P}} (v(f) + n_v)v \geq 0$$

е еквивалентно на $v(f) + n_v \geq 0$ за всички класове дискретни нормирания $v \in \mathcal{P}$. Аналогично, $v(g) + n_v \geq 0$ за $\forall v \in \mathcal{P}$, съгласно $div(g) + D \geq 0$. За да установим, че $f + g \in \mathcal{L}(D)$ за произволни $f, g \in \mathcal{L}(D)$, оценяваме

$$div(f+g) + D = \sum_{v\in\mathcal{P}} v(f+g)v + \sum_{v\in\mathcal{P}} n_v v =$$

$$= \sum_{v\in\mathcal{P}} (v(f+g) + n_v)v \geq \sum_{v\in\mathcal{P}} [\min(v(f), v(g)) + n_v]v \geq 0$$

с помощта на неравенството на триъгълника $v(f+g) \geq \min(v(f), v(g))$ за произволен клас дискретни нормирания v.

Непосредствено се проверява, че $\Gamma(X, L_D) = s_o\mathcal{L}(D)$.

С известна неточност ще отъждествяваме множеството $\Gamma(X, L_D) = s_o\mathcal{L}(D)$ на глобалните регулярни сечения на L_D с $\mathbb{F}_q$-линейното пространство $\mathcal{L}(D)$, което го параметризира.

Определение 77. *Линейната система $|D|$ на дивизор D върху крива X, определена над крайно поле $\mathbb{F}_q$ е множеството*

$$|D| = \{E \in Div(X) \ \mid \ E = div(f) + D \geq 0, \quad f \in \mathbb{F}_q(X)^*\}$$

на ефективните дивизори върху X, които са линейно еквивалентни с D.

Ефективните дивизори $E = div(f) + D \geq 0$ върху X, които са линейно еквивалентни с D са във взаимно еднозначно съответствие с дивизорите $E - D = div(f)$ на рационалните функции $f \in \mathcal{L}(D)$. Затова имаме изоморфизъм на множества

$$|D| \simeq \{div(f) \ \mid \ f \in \mathbb{F}_q(X)^*, \quad div(f) + D \geq 0\}.$$

Рационалните функции $f, g \in \mathbb{F}_q(X)^*$ имат един и същи дивизор $div(f) = div(g)$ точно когато

$$div\left(\frac{f}{g}\right) = \sum_{v\in\mathcal{P}} v\left(\frac{f}{g}\right)v = \sum_{v\in\mathcal{P}} [v(f) - v(g)]v =$$

$$= \sum_{v\in\mathcal{P}} v(f)v - \sum_{v\in\mathcal{P}} v(g)v = div(f) - div(g) = 0.$$

Последното е еквивалентно на $\frac{f}{g} \in \mathbb{F}_q^*$, съгласно Следствие 76. Следователно линейната система

$$|D| \simeq \{div(f) \ \mid \ f \in \mathcal{L}(D) \setminus \{0\}\} = \mathcal{L}(D) \setminus \{0\}/\mathbb{F}_q^* = \mathbb{P}(\mathcal{L}(D))$$

на дивизор D върху X е изоморфна на проективизацията на пространството на Риман-Рох $\mathcal{L}(D)$.

В следващата лема са събрани някои свойства на пространствата на Риман-Рох $\mathcal{L}(D)$.

Лема 78. *(i) За произволни дивизори $G \geq D$ върху гладка неприводима проективна крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, пространството на Риман-Рох $\mathcal{L}(D)$ на D е $\mathbb{F}_q$-линейно подпространство на пространството на Риман-Рох $\mathcal{L}(G)$ на G.*

(ii) За произволни дивизори $G \geq D$ е в сила

$$\dim_k \left(\mathcal{L}(G)/\mathcal{L}(D)\right) \leq \deg(G) - \deg(D).$$

(iii) $\mathcal{L}(0) = \mathbb{F}_q$.

(iv) Размерността на пространството на Риман-Рох $\mathcal{L}(D)$ на произволен ефективен дивизор $D \geq 0$ е

$$l(D) = \dim_k \mathcal{L}(D) \geq 1.$$

(v) За произволен дивизор D размерността $l(D) = \dim_k \mathcal{L}(D) < \infty$ е крайна.

(vi) За произволен дивизор D и произволна рационална функция $x \in F = \mathbb{F}_q(X)$ е в сила $l(D) = l(D + div(x))$.

Доказателство: (i) По определение, ако $x \in \mathcal{L}(D)$, то $div(x) + D \geq 0$, откъдето

$$div(x) + G = div(x) + D + (G - D) \geq 0,$$

защото дивизорът $G - D \geq 0$ е ефективен.

(ii) Достатъчно е да докажем, че

$$\dim_k \left(\mathcal{L}(D + v)/\mathcal{L}(D)\right) \leq deg(v) \quad \text{за} \quad \forall v \in \mathcal{P}. \tag{2.16}$$

Тогава с индукция по броя на събираемите в $G - D \geq 0$, ако $G = G' + v$ и допуснем, че

$$\dim_k \left(\mathcal{L}(G')/\mathcal{L}(D)\right) \leq \deg(G') - \deg(D) \quad \text{за} \quad G' \geq D, \quad \text{то}$$

$$\dim_k \left(\mathcal{L}(G' + v)/\mathcal{L}(G')\right) \leq \deg(v) \quad \text{дава}$$

$$\dim_k \left(\mathcal{L}(G' + v)/\mathcal{L}(D)\right) \leq [\deg(G') + \deg(v)] - \deg(D).$$

Тук използваме, че ако $A_1 \subset A_2 \subset A_3$ са крайномерни линейни пространства над поле k, то $\dim_k(A_3/A_1) = \dim_k(A_3/A_2) + \dim_k(A_2/A_1)$. За да проверим (2.16) за

$$D = \sum_{w \in \mathcal{P}} n_w w$$

избираме $u \in F$ с $v(u) = n_v + 1$. Тогава всяко $x \in \mathcal{L}(D + v)$ има регулярно във v произведение $xu \in \mathcal{O}_v$, защото $v(xu) = v(x) + v(u) = v(x) + n_v + 1 \geq 0$. Това ни дава възможност да разгледаме изображението

$$\psi : \mathcal{L}(D + v) \longrightarrow \mathcal{O}_v/\mathfrak{M}_v,$$

$$\psi(x) = xu + \mathfrak{M}_v.$$

Съгласно $\psi(x_1 + x_2) = (x_1 + x_2)u + \mathfrak{M}_v = (x_1u + \mathfrak{M}_v) + (x_2u + \mathfrak{M}_v) = \psi(x_1) + \psi(x_2)$ за $\forall x_1, x_2 \in \mathcal{L}(D+v)$ и $\psi(\lambda x) = \lambda xu + \mathfrak{M}_v = \lambda(xu + \mathfrak{M}_v) = \lambda\psi(x)$ за $\forall \lambda \in k$, $\forall x \in \mathcal{L}(D+v)$, изображението ψ е k-линейно. Ядрото

$$\ker(\psi) = \{x \in \mathcal{L}(D+v) \ \mid \ xu \in \mathfrak{M}_v\} =$$

$$= \{x \in \mathcal{L}(D+v) \ \mid \ v(x) + v(u) = v(x) + n_v + 1 \geq 1\} =$$

$$= \{x \in \mathcal{L}(D+v) \ \mid \ v(x) + n_v \geq 0\} = \mathcal{L}(D).$$

Следователно образът $\mathcal{L}(D+V)/\mathcal{L}(D) \simeq \mathrm{im}(\psi)$ има размерност

$$\dim_k (\mathcal{L}(D+v)/\mathcal{L}(D)) = \dim_k \mathrm{im}(\psi) \leq \dim_k (\mathcal{O}_v/\mathfrak{M}_v) = \deg(v).$$

(iii) По определение,

$$\mathcal{L}(0) = \{x \in \mathbb{F}_q(X)^* \ \mid \ div(x) \geq 0\} \cup \{0\} = \mathbb{F}_q^* \cup \{0\} = \mathbb{F}_q,$$

защото единствените нетъждествено нулеви рационални функции $x \in \mathbb{F}_q(X)^*$ без полюси са константите от $\mathbb{F}_q^*$.

(iv) Ако $D \geq 0$, то съгласно (i) и (iii) имаме $\mathcal{L}(D) \supseteq \mathcal{L}(0) = \mathbb{F}_q$, откъдето

$$l(D) = \dim_{\mathbb{F}_q} \mathcal{L}(D) \geq 1.$$

(v) Ако дивизорът $D \geq 0$ е ефективен, то съгласно (ii) имаме

$$\dim_{\mathbb{F}_q} (\mathcal{L}(D)/\mathcal{L}(0)) = \dim_{\mathbb{F}_q} (\mathcal{L}(D)/\mathbb{F}_q) \leq \deg(D),$$

откъдето $l(D) = \dim_{\mathbb{F}_q} \mathcal{L}(D) \leq \deg(D) + 1 < \infty$.

В общия случай избираме ефективен дивизор $G \geq 0$, който доминира D, т.е. $G \geq 0$, $G \geq D$. Тогава $l(G) < \infty$. Прилагайки (i) получаваме, че $l(D) \leq l(G) < \infty$.

(vi) За произволен дивизор D и произволна рационална функция $x \in \mathbb{F}_q(X)$ твърдим, че $x\mathcal{L}(D + div(x)) = \mathcal{L}(D)$. Наистина, ако $y \in \mathcal{L}(D + div(x))$, то

$$div(y) + div(x) + D = div(xy) + D \geq 0$$

и $xy \in \mathcal{L}(D)$. Обратно, ако $z \in \mathcal{L}(D)$, то $y = \frac{z}{x} \in \mathcal{L}(D + div(x))$, защото

$$div\left(\frac{z}{x}\right) + div(x) + D = div(z) + D \geq 0.$$

Оттук

$$l(D) = \dim_{\mathbb{F}_q} \mathcal{L}(D) = \dim_{\mathbb{F}_q} \mathcal{L}(D + div(x)) = l(D + div(x)).$$

□

Твърдение 79. *Нека $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива, определена над крайно поле $\mathbb{F}_q$, $F = \mathbb{F}_q(X)$ е функционалното поле на X над $\mathbb{F}_q$ и $x \in F \setminus \mathbb{F}_q$ е непостоянна рационална функция върху X. Тогава броят на нулите*

$$\deg(x)_0 = [F : \mathbb{F}_q(x)]$$

на x съвпада със степента на функционалното поле F над чисто трансцендентното разширение $\mathbb{F}_q(x)$ на $\mathbb{F}_q$ чрез x.

Доказателство: Вече доказахме, че $n = [F : \mathbb{F}_q(x)] \geq \deg(x)_0$. За $n \leq \deg(x)_0$ избираме базис $y_1, \dots y_n$ на F над $\mathbb{F}_q(x)$ и разглеждаме ефективния дивизор $E = \sum_{j=1}^{n} (y_j)_\infty$. За $\forall m \in \mathbb{N}$, $\forall 0 \leq i \leq m$ и $\forall 1 \leq j \leq n$, рационалните функции $x^{-i}y_j \in \mathcal{L}(m(x)_0 + E)$, защото

$$div(x^{-i}y_j) + m(x)_0 + E = -i(x)_0 + i(x)_\infty + (y_j)_0 - (y_j)_\infty + m(x)_0 + \sum_{j=1}^{n} (y_j)_\infty \geq 0,$$

съгласно $(m-i)(x)_0 \geq 0$, $E - (y_j)_\infty = \sum_{i \neq j} (y_i)_\infty$, $i(x)_\infty \geq 0$ и $(y_i)_0 \geq 0$. Освен това, $\{x^{-i}y_j \mid 0 \leq i \leq m, \quad 1 \leq j \leq n\}$ са линейно независими над $\mathbb{F}_q$, защото $y_1, \dots, y_n$ са линейно независими над чисто трансцендентното разширение $\mathbb{F}_q(x)$ на $\mathbb{F}_q$ чрез x. Следователно броят на тези рационални функции

$$(m+1)n \leq l(m(x)_0 + E) \tag{2.17}$$

не надминава размерността на $\mathcal{L}(m(x)_0 + E)$ над $\mathbb{F}_q$. Прилагаме Лема 78(ii) към дивизорите $m(x)_0 + E \geq 0$ и получаваме

$$l(m(x)_0 + E) - 1 = \dim_{\mathbb{F}_q}(\mathcal{L}(m(x)_0 + E)/\mathcal{L}(0)) \leq m \deg(x)_0 + \deg(E).$$

Комбинирането с 2.17 дава

$$mn + n \leq m \deg(x)_0 + \deg(E) + 1.$$

Оттук $m[\deg(x)_0 - n] \geq n - \deg(E) - 1$ за $\forall m \in \mathbb{N}$. Следователно коефициентът $\deg(x)_0 - n \geq 0$ на m е неотрицателен и $\deg(x)_0 = n$.

□

Следствие 80. *Нека $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива, определена над крайно поле $\mathbb{F}_q$, $F = \mathbb{F}_q(X)$ е функционалното поле на X над $\mathbb{F}_q$ и $x \in F \setminus \mathbb{F}_q$. Тогава*

$$\deg(x)_\infty = \deg(x)_0 = [F : \mathbb{F}_q(x)].$$

В частност, $\deg(div(x)) = 0$ за $\forall x \in F$.

Доказателство: Съгласно $\mathbb{F}_q(x) = \mathbb{F}_q\left(\frac{1}{x}\right)$,

$$\deg(x)_0 = [F : \mathbb{F}_q(x)] = \left[F : \mathbb{F}_q\left(\frac{1}{x}\right)\right] = \deg\left(\frac{1}{x}\right)_0 = \deg(x)_\infty.$$

□

Следствие 81. *Ако D е дивизор от степен $\deg(D) < 0$, то $\mathcal{L}(D) = \{0\}$.*

Доказателство: При допускане на противното съществува рационална функция $x \in \mathcal{L}(D) \setminus \{0\}$ с $div(x) + D \geq 0$. Оттук $\deg(D) = \deg(div(x)) + \deg(D) \geq 0$, противно на предположението $\deg(D) < 0$. Това доказва $\mathcal{L}(D) = \{0\}$ за $\deg(D) < 0$.

□

Дивизорите $div(x)$ на рационални функции $x \in F = \mathbb{F}_q(X)$ се наричат главни дивизори и образуват подгрупа $div(F)$ на свободната абелева група $Div(F)$ на всички дивизори на функционалното поле $F = \mathbb{F}_q(X)$. Групата $div(F)$ на главните дивизори е подгрупа на дивизорите $Div^0(F)$ от степен 0. Фактор-групата $Div(F)/div(F)$ се нарича група на класовете дивизори.

2.4.2 Теорема на Риман

Теорема 82. (Теорема на Риман) *За произволна гладка неприводима проективна крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, определена над крайно поле $\mathbb{F}_q$, съществува цяла константа $g \geq 0$, наречена род на X, така че за всеки дивизор $D \in Div(F)$ на функционалното поле $F = \mathbb{F}_q(X)$ е в сила неравенството*

$$l(D) \geq \deg(D) - g + 1.$$

Доказателство: Разглеждаме функцията

$$s : Div(F) \longrightarrow \mathbb{Z},$$

$$s(D) = \deg(D) - l(D) + 1.$$

Твърдим съществуването на цяла константа $g \geq 0$, така че $s(D) \leq g$ за всички дивизори $D \in Div(F)$. Избираме $x \in F \setminus k$ и базис $y_1, \ldots, y_n$ на F над $k(x)$. По аналогия с доказателството на $[F : k(x)] \leq \deg(x)_0$ фиксираме ефективния дивизор

$$E = \sum_{j=1}^{n} (y_j)_\infty.$$

За произволно естествено $m \in \mathbb{N}$ рационалните функции

$$\{x^{-i} y_j \ \mid \ 0 \leq i \leq m, \ \ 1 \leq j \leq n\}$$

образуват линейно независимо над k подмножество на $\mathcal{L}(m(x)_0 + E)$. Оттук следва (2.17). Прилагаме Лема 78(ii) към $m(x)_0 + E \geq m(x)_0$ и получаваме, че

$$l(m(x)_0 + E) - l(m(x)_0) \leq \deg(E).$$

Комбинирайки последното неравенство с (2.17) извеждаме

$$mn + n \leq l(m(x)_0) + \deg(E).$$

В резултат,

$$s(m(x)_0) = \deg(m(x)_0) - l(m(x)_0) + 1 = mn - l(m(x)_0) + 1 \leq \deg(E) - n + 1,$$

съгласно $\deg(x)_0 = n$. Следователно редицата $\{s(m(x)_0)\}_{m=1}^{\infty}$ е ограничена отгоре и можем да изберем

$$g := \sup_{m \in \mathbb{N}} s(m(x)_0).$$

Супремумът g на редицата $\{s(m(x)_0)\}_{m=1}^{\infty}$ се достига, защото $\{s(m(x)_0)\}_{m=1}^{\infty} \subseteq \mathbb{Z}$ е дискретна редица.

За произволен дивизор $D \in Div(F)$ съществува ефективен дивизор $H \in Div(F)$, $H \geq 0$, който доминира D, т.е. $D \leq H$. Прилагаме Лема 78(ii) към $m(x)_0 \geq m(x)_0 - H$ и получаваме

$$l(m(x)_0) - l(m(x)_0 - H) \leq \deg(H). \tag{2.18}$$

От $s(m(x)_0) = \deg(m(x)_0) - l(m(x)_0) + 1 \leq g$ следва $l(m(x)_0) \geq m\deg((x)_0) - g + 1$. Комбинирайки с (2.18) получаваме

$$l(m(x)_0 - H) \geq l(m(x)_0) - \deg(H) \geq m\deg((x)_0) - g + 1 - \deg(H) = mn - g + 1 - \deg(H).$$

За достатъчно големи $n = \deg(x)_0 \in \mathbb{N}$ имаме $mn - g + 1 - \deg(H) > 0$, откъдето $l(m(x)_0 - H) > 0$. За такива $n \in \mathbb{N}$ съществува $z \in \mathcal{L}(m(x)_0 - H) \setminus \{0\}$ с дивизор $div(z) + m(x)_0 - H \geq 0$. Оттук

$$m(x)_0 \geq H - div(z).$$

Ако $D_1 \leq D_2$ за дивизори $D_1, D_2 \in Div(F)$, то

$$s(D_2) - s(D_1) = [\deg(D_2) - \deg(D_1)] - [l(D_2) - l(D_1)] \geq 0$$

съгласно Лема 78(ii). Освен това,

$$s(D + div(y)) = \deg(D) - l(D) + 1 = s(D),$$

защото $\deg(div(y)) = 0$ и $l(D + div(y)) = l(D)$ по Лема 78(vi). В резултат,

$$g \geq s(m(x)_0) \geq s(H - div(z)) = s(H) \geq s(D),$$

поради $m(x)_0 \geq H - div(z)$ и $H \geq D$. За $D = 0$, доказаната Теорема на Риман дава

$$1 = l(0) \geq \deg(0) - g + 1 = 1 - g,$$

откъдето $g \geq 0$.

□

Следствие 83. *Нека $F = \mathbb{F}_q(X)$ е функционално поле на гладка неприводима крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ от род $g \geq 0$. Тогава съществува $r_o \in \mathbb{Z}^{\geq 0}$, така че за всеки дивизор $D \in Div(F)$ от степен $\deg(D) \geq r_o$ е в сила Теоремата на Риман с равенство*

$$l(D) = \deg(D) - g + 1.$$

Доказателство: Първо ще проверим, че ако дивизор $D \in Div(F)$ изпълнява Теоремата на Риман с равенство $l(D) = \deg(D) - g + 1$, то всеки дивизор $G \geq D$ изпълнява Теоремата на Riemann с равенство, $l(G) = \deg(G) - g + 1$. За целта, прилагаме Лема 78(ii) към $G \geq D$ и получаваме

$$l(G) - l(D) \leq \deg(G) - \deg(D).$$

Съгласно Теоремата на Riemann $l(D) = \deg(D) - g + 1$ за D с равенство, оттук следва $l(G) \leq \deg(G) - g + 1$. Заедно с Теоремата на Riemann $l(G) \geq \deg(G) - g + 1$ за G, това дава $l(G) = \deg(G) - g + 1$.

Както в доказателството на Теоремата на Riemann 82 избираме $x \in F \setminus k$ и такова $\mu \in \mathbb{N}$, че $s(\mu(x)_0) = \deg(\mu(x)_0) - l(\mu(x)_0) + 1 = g$ достига точната горна граница g на $\{s(m(x)_0)\}_{m=1}^{\infty}$. Полагаме

$$r := g + \deg(\mu(x)_0).$$

Тогава за всеки дивизор $D \in Div(F)$ от степен $\deg(D) \geq r$ дивизорът $D - \mu(x)_0 \in Div(F)$ е от степен $\deg(D - \mu(x)_0) \geq g$. По Теоремата на Riemann за $D - \mu(x)_0$ имаме

$$l(D - \mu(x)_0) \geq \deg(D - \mu(x)_0) - g + 1 \geq 1.$$

Следователно съществува $z \in \mathcal{L}(D - \mu(x)_0) \setminus \{0\}$ с $div(z) + D - \mu(x)_0 \geq 0$. С други думи, $D + div(z) \geq \mu(x)_0$ и дивизорът $D + div(z)$ изпълнява Теоремата на Riemann с равенство $s(D + div(z)) = g$. Комбинирайки с $s(D + div(z)) = s(D)$ получаваме Теоремата на Riemann с равенство $s(D) = g$ за всеки дивизор $D \in Div(F)$ от степен $\deg(D) \geq r$.

□

Използвайки резидууми на диференциални форми върху гладка неприводима проективна крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, определена над $\mathbb{F}_q$ или свойствата на аделното пространство на функционалното поле $\mathbb{F}_q(X)$, може да се докаже следната

Теорема 84. (Теорема на Риман-Рох:) *За произволна гладка неприводима проективна крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ от род g съществува дивизор K_X, определен с точност до линейна еквивалентност, така че за всеки дивизор D на функционалното поле $\mathbb{F}_q(X)$ е в сила равенството*

$$l(D) - l(K_X - D) = \deg(D) - g + 1$$

за размерностите $l(G) := \dim_{\mathbb{F}_q} \mathcal{L}(G)$ на пространствата на Риман-Рох

$$\mathcal{L}(G) := \{f \in \mathbb{F}_q(X)^* \mid \operatorname{div}(f) + G \geq 0\} \cup \{0\}$$

на съответните дивизори G.

Дивизорът K_X от степен $\deg(K_X) = 2g-2$ *с пространство на Риман-Рох $\mathcal{L}(K_X)$ с размерност $l(K_X) = g$ се нарича каноничен дивизор на X.*

В частност, за всеки дивизор D от степен $\deg(D) \geq 2g-1$ *е в сила*

$$l(D) = \deg(D) - g + 1.$$

2.5 Горна граница върху броя на рационалните точки на гладка проективна крива над крайно поле

Следващото твърдение дава горна граница (2.19) върху броя на рационалните точки на гладка неприводима крива $X/\mathbb{F}_{q_o} \subset \mathbb{P}^n(\overline{\mathbb{F}_{q_o}})$р която е необходимо условие за изпълнението на аналога на хипотезата на Риман за X относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Обобщавайки (2.19), статията [KM3] въвежда понятието порядък на Хасе-Вайл на локално краен модул M над абсолютната група на Галоа $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$ относно друг локално краен модул L над $\mathfrak{G}$. Достатъчното условие от [KM3] за изпълнение на аналога на хипотезата на Риман за M относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ включва ограничение върху порядъка на Хасе-Вайл на M относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$. В терминология на [KM3], Твърдение 85 установява, че порядъкът на Хасе-Вайл на крива относно проективната права не надминава $\frac{1}{2}$.

Твърдение 85. *(*Stichtenoth - Твърдение V.2.6*) Нека $X/\mathbb{F}_{q_o} \subset \mathbb{P}^n(\overline{\mathbb{F}_{q_o}})$ е гладка неприводима проективна крива от род $g \in \mathbb{Z}^{\geq 0}$, определена над $\mathbb{F}_{q_o}$. Тогава съществува $r_o \in \mathbb{N}$, така че за всяко естествено число $r \geq r_o$ е в сила*

$$\left|X(\mathbb{F}_{q_o^{2r}})\right| < q_o^{2r} + 1 + (2g+1)q_o^r. \tag{2.19}$$

Доказателство: Нека

$$q := q_o^{2r}, \quad m := q_o^r - 1, \quad n := 2g + q_o^r, \quad s := q_o^{2r} - 1 + (2g+1)q_o^r = m + nq_o^r$$

и $Q \in X(\mathbb{F}_q)$ е $\mathbb{F}_q$-рационална точка на X. Да означим с T множеството на онези $0 \leq i \leq m$, за които съществува $x \in \mathbb{F}_q(X)$ с дивизор на полюсите $\mathrm{div}(x)_\infty = iQ$. За всяко $i \in T$ избираме $u_i \in \mathcal{L}_X(mQ)$ с $\mathrm{div}(u_i)_\infty = iQ$ и твърдим, че $\{u_i \,|\, i \in T\}$ е базис на $\mathcal{L}_X(mQ)$ над $\mathbb{F}_q$. Наистина, за $\forall y \in \mathcal{L}_X(mQ)$ дискретното нормиране

$$\nu_Q : \mathbb{F}_q(X) \longrightarrow \mathbb{Z} \cup \{\infty\},$$

отговарящо на $Q \in X(\mathbb{F}_q)$ взема стойност $\nu_Q(y) = -i$ за някое $i \in T$. Това означава, че дивизорът на полюсите $\mathrm{div}(y)_\infty = iQ$ и ако t е локален параметър на ν_Q, то y се развива в Лоранов ред

$$y = \sum_{j=-i}^{\infty} a_j t^j \in \mathbb{F}_q[[t]] \quad \text{с} \quad a_{-i} \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}.$$

От друга страна,

$$u_i = \sum_{j=-i}^{\infty} b_j t^j \quad \text{с} \quad b_{-i} \in \mathbb{F}_q^*$$

и

$$y' := y - \frac{a_{-i}}{b_{-i}} u_j \in \mathcal{L}_X(mQ)$$

се задава с Лоранов ред

$$y' = \sum_{j=-i+1}^{\infty} \left(a_j - \frac{a_{-i}}{b_{-i}} b_j \right) t^j.$$

С други думи, $\operatorname{div}(y')_\infty = jQ$ за някое $j < i$. Продължавайки по същия начин, модифицираме y' с $\mathbb{F}_q$-линейна комбинация на u_j с $j < i$, докато получим рационална функция върху X без полюси, т.е. константа от $\mathbb{F}_q$. Това доказва, че $\mathcal{L}_X(mQ)$ се съдържа в $\mathbb{F}_q$-линейната обвивка на $\{u_i \,|\, i \in T\}$. Ако допуснем, че съществуват $\lambda_i \in \mathbb{F}_q$ с $\sum\limits_{i \in T} \lambda_i u_i = 0$ и поне едно $\lambda_{i_o} \neq 0$, то за максималното $i_o \in T$ с $\lambda_{i_o} \neq 0$ получаваме представяне

$$u_{i_o} = \sum_{i<i_o} \left(-\frac{\lambda_i}{\lambda_{i_o}} \right) u_i.$$

Без ограничение на общността считаме, че $\lambda_i \neq 0$ за всички записани събираеми и забелязваме, че $\nu_Q \left(-\frac{\lambda_i}{\lambda_{i_o}} u_i \right) = \nu_Q(u_i)$ са различни за различни $i < i_o$. Прилагаме неравенството на триъгълника с равенство и получаваме

$$i_o = \nu_Q(u_{i_o}) = \nu_Q \left(\sum_{i<i_o} \left(-\frac{\lambda}{\lambda_o} \right) u_i \right) =$$

$$= \min \left(\nu_Q \left(\left(-\frac{\lambda_i}{\lambda_{i_o}} \right) u_i \right) \,\middle|\, i \in T,\, \lambda_i \neq 0,\, i < i_o \right) < i_o.$$

Полученото противоречие доказва линейната независимост на $\{u_i \,|\, i \in T\}$ над $\mathbb{F}_q$ и установява, че $\{u_i \,|\, i \in T\}$ е базис на $\mathcal{L}_X(mQ)$ над $\mathbb{F}_q$.

Нека $\mathcal{L}$ е множеството на крайните суми от вида

$$z = \sum_{\alpha=1}^{l} x_\alpha y_\alpha^{q_o^r} \quad \text{с} \quad x_\alpha \in \mathcal{L}_X(mQ) \quad \text{и} \quad y_\alpha \in \mathcal{L}_X(nQ).$$

Ясно е, че те принадлежат на $\mathcal{L}_X((m + nq_o^r)Q) = \mathcal{L}_X(sQ)$. Достатъчно е да проверим съществуването на елемент $z \in \mathcal{L} \setminus \{0\}$ с $z(P) = 0$ за $\forall P \in X(\mathbb{F}_q) \setminus \{Q\}$, за да завършим доказателството на твърдението. Наистина, тогава

$$|X(\mathbb{F}_q)| - 1 \leq \deg \operatorname{div}(z)_0 = \deg \operatorname{div}(z)_\infty \leq s = q_o^{2r} - 1 + (2g+1)q_o^r,$$

откъдето

$$\left| X(\mathbb{F}_{q_o^{2r}}) \right| = |X(\mathbb{F}_q)| < q_o^{2r} + 1 + (2g+1)q_o^r$$

и верността на твърдението е установена.

За целта забелязваме, че всеки елемент на $\mathcal{L}$ има единствено представяне

$$z = \sum_{i \in T} u_i y_i^{q_o^r} \quad \text{с} \quad y_i \in \mathcal{L}_X(nQ). \tag{2.20}$$

По-точно, автоморфизмът на Фробениус

$$\Phi_{q_o}^r : \mathbb{F}_q = \mathbb{F}_{q_o^{2r}} \longrightarrow \mathbb{F}_{q_o^{2r}} = \mathbb{F}_q, \quad \Phi_{q_o}^r(\lambda) = \lambda^{q_o^r}$$

е обратим и за $\forall \mu \in \mathbb{F}_q$ съществува единствено $\sqrt[q_o^r]{\mu} = \lambda \in \mathbb{F}_q$ с $\lambda^{q_o^r} = \mu$. Ако

$$x_\alpha = \sum_{i \in T} \mu_{\alpha,i} u_i$$

за някакви $\mu_{\alpha,i} \in \mathbb{F}_q$ и $\sqrt[q_o^r]{\mu_{\alpha,i}} = \lambda_{\alpha,i} \in \mathbb{F}_q$, то

$$z = \sum_{\alpha=1}^{l} x_\alpha y_\alpha^{q_o^r} = \sum_{\alpha=1}^{l} \sum_{i \in T} \mu_{\alpha,i} u_i y_\alpha^{q_o^r} = \sum_{\alpha=1}^{l} \sum_{i \in T} u_i \lambda_{\alpha,i}^{q_o^r} y_\alpha^{q_o^r} =$$

$$= \sum_{i \in T} u_i \left(\sum_{\alpha=1}^{l} (\lambda_{\alpha,i} y_\alpha)^{q_o^r} \right) = \sum_{i \in T} u_i \left(\sum_{\alpha=1}^{l} \lambda_{\alpha,i} y_\alpha \right)^{q_o^r} = \sum_{i \in T} u_i y_i^{q_o^r}$$

за $y_i := \sum\limits_{\alpha=1}^{l} \lambda_{\alpha,i} y_\alpha \in \mathcal{L}_X(nQ)$. Това доказва съществуването на представяне (2.20) за $\forall z \in \mathcal{L}$. Да допуснем, че има елемент на $\mathcal{L}$ с две представяния. Тогава разликата на тези две представяния изпълнява равенството $\sum\limits_{i \in T_1} u_i y_i^{q_o^r} = 0$ за някакви елементи $y_i \in \mathcal{L}_X(nQ) \setminus \{0\}$ и някакво подмножество $T_1 \subseteq T$. Целите числа

$$\nu_Q \left(u_i y_i^{q_o^r} \right) = \nu_Q(u_i) + q_o^r \nu_Q(y_i) = i + q_o^r \nu_Q(y_i)$$

имат различни остатъци $0 \leq i \leq m = q_o^r - 1$ при деление с q_o^r и следователно са различни. Това позволява прилагането на неравенството на триъгълника с равенство и получаването на

$$\infty = \nu_Q(0) = \nu_Q \left(\sum_{i \in T_1} u_i y_i^{q_o^r} \right) = \min \left(\nu_Q \left(u_i y_i^{q_o^r} \right) \,\middle|\, i \in T_1 \right) =$$

$$= \min \left(i + q_o^r \nu_Q(y_i) \,|\, i \in T_1 \right).$$

Ненулевите елементи $y_i \in \mathcal{L}_X(nQ) \setminus \{0\}$ имат $\nu_Q(y_i) \neq \infty$, така че горното равенство е противоречие, доказващо единствеността на представянето $z = \sum\limits_{i \in T} u_i y_i^{q_o^r}$ с $y_i \in \mathcal{L}_X(nQ)$ за всеки елемент z на $\mathcal{L}$.

Подмножеството $\mathcal{L}$ на $\mathcal{L}_X(sQ)$ е подгрупа на адитивната група $(\mathcal{L}_X(sQ), +)$, съгласно

$$\left(\sum_{i \in T} u_i y_i^{q_o^r} \right) - \left(\sum_{i \in T} u_i z_i^{q_o^r} \right) = \sum_{i \in T} u_i \left(y_i^{q_o^r} - z_i^{q_o^r} \right) = \sum_{i \in T} u_i (y_i - z_i)^{q_o^r} \in \mathcal{L}$$

за всички $\sum\limits_{i\in T} u_i y_i^{q_o^r}, \sum\limits_{i\in T} u_i z_i^{q_o^r} \in \mathcal{L}$. За произволни $z = \sum\limits_{i\in T} u_i y_i^{q_o^r} \in \mathcal{L}$ и $\mu \in \mathbb{F}_q$ с $\sqrt[q_o^r]{\mu} = \lambda \in \mathbb{F}_q$ е в сила

$$\mu z = \sum_{i\in T} u_i \lambda^{q_o^r} y_i^{q_o^r} = \sum_{i\in T} u_i (\lambda y_i)^{q_o^r} \in \mathcal{L}.$$

С това проверихме, че $\mathcal{L}$ е $\mathbb{F}_q$-линейно подпространство на $\mathcal{L}_X(sQ)$.

Ако $\{v_j \,|\, j \in J\}$ е $\mathbb{F}_q$-базис на $\mathcal{L}_X(nQ)$, твърдим че $\left\{ u_i v_j^{q_o^r} \,\middle|\, i \in T, j \in J \right\}$ е $\mathbb{F}_q$-базис на $\mathcal{L}$. Всеки елемент на $\mathcal{L}$ е от вида

$$\sum_{i\in T} u_i y_i^{q_o^r} = \sum_{i\in T} u_i \left(\lambda_{i,j} v_j\right)^{q_o^r} = \sum_{i\in T} \lambda_{i,j}^{q_o^r} u_i v_j^{q_o^r} \quad \text{с} \quad \lambda_{i,j}^{q_o^r} \in \mathbb{F}_q,$$

така че $\mathbb{F}_q$-линейната обвивка на $\left\{ u_i v_j^{q_o^r} \,\middle|\, i \in T, j \in J \right\}$ покрива $\mathcal{L}$. Ако допуснем, че

$$0 = \sum_{i\in T}\sum_{j\in J} \mu_{i,j} u_i v_j^{q_o^r} = \sum_{i\in T} u_i \left(\sum_{j\in J} \left(\sqrt[q_o^r]{\mu_{i,j}} v_j \right) \right)^{q_o^r},$$

то $\sum\limits_{j\in J} \sqrt[q_o^r]{\mu_{i,j}} v_j = 0$ за $\forall i \in T$, откъдето $\sqrt[q_o^r]{\mu_{i,j}} = 0$ за $\forall i \in T$, $\forall j \in J$. В резултат, $\mu_{i,j} = 0^{q_o^r}$ за $\forall i \in T, \forall j \in J$ и системата $\left\{ u_i v_j^{q_o^r} \,\middle|\, i \in T,\, j \in J \right\} \subset \mathcal{L}$ е линейно независима над $\mathbb{F}_q$. С това установихме, че $\left\{ u_i v_j^{q_o^r} \,\middle|\, i \in T,\, j \in J \right\}$ е базис на $\mathcal{L}$ над $\mathbb{F}_q$ и

$$\dim_{\mathbb{F}_q} \mathcal{L} = l(mq) l(nQ).$$

Изображението

$$\Psi : (\mathcal{L}, +) \longrightarrow (\mathcal{L}_X((q_o^r m + n)Q), +), \quad \Psi\left(\sum_{i\in T} u_i y_i^{q_o^r} \right) := \sum_{i\in T} u_i^{q_o^r} y_i \quad \text{за} \quad \forall y_i \in \mathcal{L}_X(nQ)$$

е коректно определен хомоморфизъм на адитивните групи, но не и $\mathbb{F}_q$-линейно изображение. Наистина,

$$\begin{aligned} \Psi\left(\sum_{i\in T} u_i y_i^{q_o^r} + \sum_{i\in T} u_i z_i^{q_o^r} \right) &= \Psi\left(\sum_{i\in T} u_i (y_i + z_i)^{q_o^r} \right) = \sum_{i\in T} u_i^{q_o^r} (y_i + z_i) = \\ &= \sum_{i\in T} u_i^{q_o^r} y_i + \sum_{i\in T} u_i^{q_o^r} z_i = \Psi\left(\sum_{i\in T} u_i y_i^{q_o^r} \right) + \Psi\left(\sum_{i\in T} u_i z_i^{q_o^r} \right) \end{aligned}$$

за произволни $y_i, z_i \in \mathcal{L}_X(nQ)$. За $\forall i \in T$ и $\forall \lambda \in \mathbb{F}_q \setminus \mathbb{F}_{q_o^r} = \mathbb{F}_{q_o^{2r}} \setminus \mathbb{F}_{q_o^r}$ заблязваме, че

$$\Psi\left(\lambda^{q_o^r} u_i y_i^{q_o^r} \right) = \Psi\left(u_i (\lambda y_i)^{q_o^r} \right) = \lambda u_i^{q_o^r} y_i \neq \lambda^{q_o^r} u_i^{q_o^r} y_i = \lambda^{q_o^r} \Psi\left(u_i y_i^{q_o^r} \right),$$

така че Ψ не е $\mathbb{F}_q$-линейно изображение.

Твърдим, че от предположението $r > 2\log_q(g+1)$ следва $\dim_{\mathbb{F}_q} \mathcal{L} > l((q_o^r m+n)Q)$, така че съществува ненулев елемент $z \in \ker(\lambda)$ от ядрото на $\lambda : (\mathcal{L}, +) \to (\mathcal{L}_X(sQ), +)$. Наистина, $q_o^r m+n = q+2g > 2g-2$. Съгласно Следствие 83, съществува $r_1 \in \mathbb{Z}^{\geq 0}$, така че за всяко $a \in \mathbb{Z}^{\geq 0}$, $a \geq r_o$ е в сила Теоремата на Риман с равенство $l(aQ) = a-g+1$. Без ограничение, можем да считаме, че $r_1 > m(g+1)^2 + n \geq m+n$ и да фиксираме естествено число $r_o \geq \log_{q_o}\left(\frac{r_1-n}{m}\right) \in \mathbb{R}^{>0}$. Тогава за $\forall r \geq r_o$ е в сила $q_o^r m + n \geq r_1$ и

$$l((q_o^r m+n)Q) = q+2g-g+1 = q+g+1.$$

От друга страна, Теоремата на Риман 82 дава

$$l(mQ) \geq m-g+1, \quad l(nQ) \geq n-g+1,$$

откъдето

$$\begin{aligned}\dim_{\mathbb{F}_q} \mathcal{L} = l(mQ)l(nQ) \geq (m-g+1)(n-g+1) = (q_o^r - g)(q_o^r + g + 1) = \\ = q - g^2 + q_o^r - g > q+g+1 = l((q_o^r m+n)Q),\end{aligned}$$

защото $q_o^r \geq q_o^{r_o} \geq \frac{r_1-n}{m} > (g+1)^2$. С това доказахме, че броят на елементите на $\mathcal{L}$ е

$$|\mathcal{L}| = q^{l(mQ)l(nQ)} > q^{l((q_o^r m+n)Q)} = |\mathcal{L}_X((q_o^r m+n)Q)|\,.$$

Ако допуснем, че хомоморфизмът $\Psi : (\mathcal{L}, +) \to (\mathcal{L}_X((q_o^r m+n)Q), +)$ има $\ker(\Psi) = \{0\}$, то Ψ е инективен и $|\mathcal{L}| = |\Phi(\mathcal{L})| \leq |\mathcal{L}_X((q_o^r m+n)Q)|$, защото $\Psi(\mathcal{L})$ е подмножество на $\mathcal{L}_X((q_o^r m+n)Q)$. Противоречието доказва съществуването на ненулев елемент $z = \sum\limits_{i\in T} u_i y_i^{q_o^r} \in \ker(\Psi) \setminus \{0\}$. В произволна точка $P \in X(\mathbb{F}_q) \setminus \{Q\}$ е изпълнено

$$\begin{aligned}z(P)^{q_o^r} = \left(\sum_{i\in T} u_i(P) y_i(P)^{q_o^r}\right)^{q_o^r} = \sum_{i\in T} u_i(P)^{q_o^r} y_i(P)^q = \\ = \left(\sum_{i\in T} u_i^{q_o^r} y_i\right)(P) = \Psi(z)(P) = 0(P) = 0,\end{aligned}$$

защото $y_i(P) \in \mathbb{F}_q$ за произволно $y_i \in \mathcal{L}_X(nQ) \subset \mathbb{F}_q(X)$. Това установява анулирането на $z \in \ker(\Psi) \setminus \{0\}$ върху $X(\mathbb{F}_q) \setminus \{Q\}$ и завършва доказателството на твърдението.

□

Глава 3

Тъждества на Мак Уилямс и дзета полином на линеен код

Настоящата глава съдържа някои предварителни сведения от теория на кодирането. Първият параграф определя понятията линеен код и алгебро-геометричен код на Гопа. Вторият параграф е посветен на тъждествата на Мак Уилямс за тегловото разпределение на линеен код C и неговия дуален $C^{\perp}$. Изложението е взаимствано от доказателството на Уорд от [Ward]. Третият параграф дискутира ζ-полинома $P_C(t)$ на линеен код C, въведен и изучен от Дуурсма в [Duursma1], [Duursma2], [Duursma3]. Дадени са две определения за $P_C(t)$ и е доказана тяхната еквивалентност. Нека $X/\mathbb{F}_q \subset \mathbb{P}^m(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива от род g, определена над $\mathbb{F}_q$, $G_1, \ldots, G_h$ е пълна система представители на класовете на линейна еквивалентност на дивизорите върху X от степен $2g-2 < m < n$, а $C_1, \ldots, C_h$ са алгебро-геометричните кодове на Гоппа, построени с помощта на $G_1, \ldots, G_h$. За да обясним етимилогията на понятието "ζ-полином на линеен код"напомняме резултат на Дуурсма, свързващ ζ-полиномите $P_{C_i}(t)$ на C_i с ζ-полинома $L_{\mathbb{F}_q(X)}(t)$ на функционалното поле $\mathbb{F}_q(X)$ на X над $\mathbb{F}_q$. Дискутираме подробно формулировката на тъждествата на Мак Уилямс за тегловото разпределение на двойка дуални линейни кодове C, $C^{\perp}$ на езика на ζ-полиномите $P_C(t), P_{C^{\perp}}(t) \in \mathbb{Q}[t]$ на тези кодове.

3.1 Алгебро-геометрични кодове на Гоппа

Кодовете са схеми за предаване на информация, които позволяват коригирането на определен брой грешки, възникнали от шума по канала за предаване. Математически, кодовете са крайни множества от думи C с фиксирана дължина n, които могат да се възстановяват еднозначно при смущение на не повече от t символа. Азбуката на тези думи е най-често крайно поле $\mathbb{F}_q$ с q елемента. Ако C е линейно пространство над $\mathbb{F}_q$, казваме, че C е линеен код.

Определение 86. *Разстоянието на Hamming $d(x,y)$ между $x, y \in \mathbb{F}_q^n$ е броят на различните компоненти $x_i \neq y_i$ за $1 \leq i \leq n$.*

Лема 87. *Разстоянието на Hamming* $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ *е метрика.*

Доказателство: Ясно е, че $d(x, y) \geq 0$ с равенство $d(x, y) = 0$ точно когато $x = y$. Освен това $d(x, y) = d(y, x)$. Остава да се провери неравенството на триъгълника $d(x^{(1)}, x^{(3)}) \leq d(x^{(1)}, x^{(2)}) + d(x^{(2)}, x^{(3)})$ за произволни $x^{(1)}, x^{(2)}, x^{(3)} \in \mathbb{F}_q^n$. Да означим

$$I_{ij} = \{1 \leq k \leq n \ \mid \ x_k^{(i)} \neq x_k^{(j)}\} \quad \text{за всички} \quad 1 \leq i < j \leq 3.$$

С допускане на противното проверяваме, че $I_{13} \subseteq I_{12} \cup I_{23}$. Следователно

$$d(x^{(1)}, x^{(3)}) = |I_{13}| \leq |I_{12}| + |I_{23}| = d(x^{(1)}, x^{(2)}) + d(x^{(2)}, x^{(3)})$$

и $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ е метрика, Q.E.D.

Определение 88. *Минималното разстояние* $d(C)$ *на код* $C \subset \mathbb{F}_q^n$ *е най-малкото разстояние между две различни думи на* C.

При фиксирана дължина n и минимално разстояние $d(C)$ се търсят кодове $C \subset \mathbb{F}_q^n$ с възможно най-голям брой думи $|C|$ или с възможно най-висока ефективност при предаване на информация.

При фиксирана дължина n и брой на думите $|C|$ се максимизира минималното разстояние $d = d(C)$. Причина за това е еднозначността на декодиране при не повече от цялата част $\left[\frac{d-1}{2}\right]$ на $\frac{d-1}{2}$ грешни символа в процеса на предаване на информация. Нека $B_n(x, r) = \{y \in \mathbb{F}_q^n \ \mid \ d(x, y) \leq r\}$ е затвореното кълбо с център x и радиус r в $\mathbb{F}_q^n$ относно разстоянието на Hamming. Ако $C \subset \mathbb{F}_q^n$ е код с минимално разстояние $d = d(C)$, твърдим, че кълбата $B_n\left(x, \left[\frac{d-1}{2}\right]\right)$ с центрове $x \in C$ не се пресичат две по две. В противен случай, за различни $x, y \in C$ и $z \in B_n\left(x, \left[\frac{d-1}{2}\right]\right) \cap B_n\left(y, \left[\frac{d-1}{2}\right]\right)$, неравенството на триъгълника дава

$$d \leq d(x, y) \leq d(x, z) + d(y, z) \leq 2\left[\frac{d-1}{2}\right] < d.$$

Ако C е не само подмножество, но и линейно подпространство на $\mathbb{F}_q^n$, то броят на думите в C е q^k, където k е размерността на C над $\mathbb{F}_q$. В такъв случай казваме, че думите $x = (x_1, \ldots, x_n) \in C$ от кода имат k информационни и $n - k$ проверочни символа. Определяме минималното тегло $w(C)$ на C като най-малкият брой ненулеви компоненти в ненулева дума от C. За линейни кодове $w(C) = d(C)$. По-точно, ако $d(C) = d(x, y)$, то $d(C) = w(x - y) \geq w(C)$. В сила е и обратното неравенство $w(C) = w(z) = d(z, \mathbb{O}) \geq d(C)$, откъдето $w(C) = d(C)$.

Определение 89. *Ако* $g^{(i)} = (g_{i1}, \ldots, g_{in})$, $1 \leq i \leq k$ *е базис на линейния код* $C \subset \mathbb{F}_q^n$ *над* $\mathbb{F}_q$, *то матрицата* $G = (g_{ij})_{i=1 \ \ j=1}^{k \ \ n} \in (\mathbb{F}_q)_{k \times n}$, *образувана по редове от* $g^{(1)}, \ldots, g^{(k)}$ *се нарича пораждаща матрица на* C.

Определение 90. *Ако* $H \in M_{m,n}(\mathbb{F}_q)$ *е матрица с* m *реда,* n *стълба и елементи от крайното поле* $\mathbb{F}_q$, *а* $C \subset \mathbb{F}_q^n$ *е пространството от решения на хомогенната система линейни уравнения* $Hx^t = \mathbb{O}$, *то* H *се нарича проверочна матрица на* C.

Ако $\dim_{\mathbb{F}_q}(C) = k$, то H е от ранг $\mathrm{rk}H = n - k$. Следователно H има $m \geq n - k$ реда. Без ограничение на общността можем да изпуснем зависимите уравнения и да считаме, че H има $m = n - k$ реда.

В $\mathbb{F}_q$-линейното пространство $\mathbb{F}_q^n$ въвеждаме вътрешно произведение

$$\langle x, y\rangle = x_1y_1 + x_2y_2 + \ldots + x_ny_n \quad \text{за} \quad x, y \in \mathbb{F}_q^n.$$

Непосредствено се вижда, че вътрешното произведение е симетрична билинейна билинейна форма с максимален ранг n.

Определение 91. *Нека $C \subset \mathbb{F}_q$ е код. Ортогоналното допълнение*

$$\{x \in \mathbb{F}_q^n \mid \langle x, c\rangle = 0 \quad за \quad \forall c \in C\}$$

на C относно $\langle\ ,\ \rangle$ се нарича дуален код на C и се бележи с $C^\perp$.

Ако $C \subset \mathbb{R}^n$ е $\mathbb{R}$-линейно подпространство на $\mathbb{R}^n$, то $\mathbb{R}^n = C \oplus C^\perp$ се разлага в директна сума на C и $C^\perp$, т.е. $\mathbb{R}^n = C + C^\perp$ и $C \cap C^\perp = \{0^n\}$. За $\mathbb{F}_q$-линейни подпространства $C \subset \mathbb{F}_q^n$ това не винаги е вярно, защото C може да има непразно сечение с $C^\perp$.

Ако $G \in M_{k,n}(\mathbb{F}_q)$ е пораждаща матрица на кода $C \subset \mathbb{F}_q^n$, то пространството от решения на хомогенната линейна система $Gx = 0_{k\times 1}$ съвпада с $C^\perp$ и G е проверочна матрица на $C^\perp$. Още повече,

$$\dim C + \dim C^\perp = \mathrm{rk}G + \dim C^\perp = n.$$

Да отбележим, че $C \subseteq (C^\perp)^\perp$, защото за $\forall c \in C$ и за $\forall c' \in C^\perp$ е изпълнено $\langle c, c'\rangle = 0$. Съгласно $\dim C = n - \dim C^\perp = \dim(C^\perp)^\perp$ имаме съвпадение

$$C = (C^\perp)^\perp.$$

Ако G е проверочна матрица на $C^\perp$, то линейната обвивка на вектор-редовете на G се съдържа, а оттам и съвпада с $(C^\perp)^\perp = C$, защото $\mathrm{rk}G = n - \dim C^\perp = \dim C$. С това проверихме, че $G \in M_{k,n}(\mathbb{F}_q)$ е пораждаща матрица на C точно когато е проверочна матрица на $C^\perp$. Вземайки предвид $(C^\perp)^\perp = C$ получаваме, че H е пораждаща матрица на $C^\perp$ точно когато е проверочна матрица на C.

Лема 92. *(i) Нека $H \in M_{n-k,n}(\mathbb{F}_q)$ е проверочна матрица на линеен код $C \subset \mathbb{F}_q^n$. В такъв случай, C има минимално разстояние d тогава и само тогава, когато произволни $d-1$ стълба на H са линейно независими и съществуват d линейно зависими стълба на H.*

(ii) Граница на Сингълтън: *Ако $C \subset \mathbb{F}_q^n$ е линеен код с дължина n, размерност $\dim C = k$ и минимално разстояние d, то $k + d \leq n + 1$.*

Доказателство: (i) Линейната система уравнения $Hx^t = \mathbb{O}$ има решение c с тегло $w = w(c)$ тогава и само тогава, когато w стълба на H изпълняват линейна зависимост,

чиито всички коефициенти са ненулеви. Минималното разстояние d на линеен код C е минималното естествено число, за което съществува ненулева дума на C с тегло d.

(ii) Ако $C \subset \mathbb{F}_q^n$ е линеен код с размерност k, то произволна проверочна матрица H на C е от ранг $n-k$. Следователно произволни $n-k+1$ стълба на H са линейно зависими и $d \leq n-k+1$.

Ето втори начин за доказване на границата на Сингълтън. Ако линейният код $C \subset \mathbb{F}_q^n$ има минимално разстояние d, то координатното подпространство

$$W = \mathbb{F}_q^{d-1} \times \{(0^{n-d+1}\} \subset \mathbb{F}_q^{d-1} \times \mathbb{F}_q^{n-d+1}$$

има тривиално сечение $W \cap C = \{0^n\} \subset \mathbb{F}_q^n$ с кода C. По теоремата за размерност на сума и сечение,

$$k + (d-1) = \dim C + \dim W = \dim(C+W) + \dim(C \cap W) = \dim(C+W) \leq n,$$

Q.E.D.

Определение 93. *Линейният код C с дължина n, размерност k и минимално разстояние d се нарича MDS-код (Maximum Distance Separable), ако параметрите му изпълняват границата на Сингълтън с равенство, $k+d = n+1$.*

Линеен код $C \subset \mathbb{F}_q^n$ е MDS точно когато е в общо положение спрямо координатните оси в $\mathbb{F}_q^n$.

Пример 94. (Кодове на Рееd-Соломон) *За произволно крайно поле $\mathbb{F}_q$ с q елемента и произволни естествени числа $k \leq n \leq q$ нека*

$$\mathbb{F}_q[x]^{(k)} := \{f(x) \in \mathbb{F}_q[x] \quad | \quad \deg(f) \leq k-1\}$$

е k-мерното линейно пространство на полиномите на x от степен не по-голяма от $k-1$ с коефициенти от $\mathbb{F}_q$, а $a_1, \ldots, a_n \in \mathbb{F}_q$ са различни точки. Разглеждаме остойностяващото изображение

$$\mathcal{E} : \mathbb{F}_q[x]^{(k)} \longrightarrow \mathbb{F}_q^n,$$

$$\mathcal{E}(f) = (f(a_1), \ldots, f(a_n)) \quad за \quad \forall f \in \mathbb{F}_q[x]^{(k)}.$$

Непосредствено се проверява, че $\mathcal{E}$ е $\mathbb{F}_q$-линейно влагане, защото полином $f \in \mathbb{F}_q[x]^{(k)}$ от степен $\deg(f) \leq k-1$ може да има най-много $k-1$ различни корена. Образът $C := \mathrm{im}\mathcal{E} = \mathcal{E}(\mathbb{F}_q[x]^{(k)})$ на $\mathcal{E}$ е линеен код с дължина n и размерност k, който се нарича код на Рееd-Соломон. Всяка ненулева дума $\mathcal{E}(f) \in C \setminus \{0^n\}$ има най-много $k-1$ нулеви компоненти, откъдето най-малко $n-k+1$ ненулеви координати. Комбинирайки с границата на Сингълтън $d \leq n+1-k$ получаваме, че минималното разстояние на кода C е $d = n+1-k$. Следователно кодът $C = \mathcal{E}(\mathbb{F}_q[x]^{(k)}) \subset \mathbb{F}_q^n$ на е максимално отделим.

Кодовете на Рееd-Соломон се обобщават от алгебро-геометричните кодове на Гопа, чиято конструкция е изложена в следващото твърдение.

Теорема-Определение 95. (Алгебро-геометричен код на Гоппа) *Нека*

$$D = P_1 + \ldots + P_n$$

е сума на $\mathbb{F}_q$-рационални точки от гладка проективна крива X, определена над $\mathbb{F}_q$, $G \in Div(F)$ е ефективен дивизор, чийто носител

$$\mathrm{Supp}(G) = \mathrm{Supp}\left(\sum_Q n_Q Q\right) = \{Q \mid n_Q > 0\}$$

не се пресича с $\{P_1, \ldots, P_n\}$, а

$$\mathcal{E}_D : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n,$$

$$\mathcal{E}_D(f) = (f(P_1), \ldots, f(P_n))$$

е остойностяващото изображение на пространството на Риман-Рох $\mathcal{L}(G)$ на G върху D. Тогава образът $C(X, D, G) = \mathcal{E}_D(\mathcal{L}(G)) \subset \mathbb{F}_q^n$ е линеен код с размерност

$$k = l(G) - l(G - D)$$

и минимално разстояние

$$d \geq n - \deg(G).$$

Думата $\mathcal{E}_D(f) \in C(X, D, G)$ е с тегло $r > 0$ точно когато съществува пермутация $\sigma \in S_n$, така че $f \in \mathcal{L}(G - P_{\sigma(r+1)} - \ldots - P_{\sigma(n)})$. Затова минималното разстояние d е минималното естествено число, за което съществува дивизор $D' \leq D$ от степен $\deg(D') = n - d$.

Доказателство: Остойностяващото изображение $\mathcal{E}_D$ е $\mathbb{F}_q$-линейно и

$$k = \dim(\mathrm{im}(\mathcal{E}_D) = l(G) - \dim(\ker(\mathcal{E}_D)).$$

Условието $f \in \mathcal{L}(G)$ означава, че $div(f) + G = (f)_0 - (f)_\infty + G \geq 0$ и е еквивалентно на $G - (f)_\infty \geq 0$. Ако $f \in \mathcal{L}(G)$ се анулира в $P_1, \ldots, P_n$, то $P_1 + \ldots + P_n \leq (f)_0$ и $div(f) + G - D = (f)_0 - D + G - (f)_\infty \geq 0$. Следователно $f \in \mathcal{L}(G) \cap \ker(\mathcal{E}_D) = \mathcal{L}(G - D)$.

Минималното разстояние d на $C(X, D, G)$ се достига от някаква дума $\mathcal{E}_D(f) = (f(P_1), \ldots, f(P_n))$. Съществува пермутация $\sigma \in S_n$, така че

$$P_{\sigma(d+1)} + \ldots + P_{\sigma(n)} \leq (f)_0$$

и $f \in \mathcal{L}(G - (P_{\sigma(d+1)} + \ldots + P_{\sigma(n)})) \setminus \{0\}$. Ако $\mathcal{L}(H) \neq 0$, то $\deg(H) \geq 0$. Да напомним, че всяка рационална функция $f \in F$ има равен брой нули и полюси, броени с техните кратности или $deg(f) = 0$. Ако съществува $f \in \mathcal{L}(H) \setminus \{0\}$, то $div(f) + D \geq 0$. Ефективността на дивизора $div(f) + D$ означава неотрицателност на всичките му цели коефициенти, така че степента $\deg((f) + D) \geq 0$ като сума на коефициентите. Затова от $f \in \mathcal{L}(G - (P_{\sigma(d+1)} + \ldots + P_{\sigma(n)})) \setminus \{0\}$ следва $\deg(G - (P_{\sigma(d+1)} + \ldots + P_{\sigma(n)})) \geq 0$ или $\deg(G) \geq n - d$.

Дума $\mathcal{E}_D(f) \in C(X, D, G)$ има тегло $w(\mathcal{E}_D(f)) = r \in (0, d]$ точно когато съществува $\sigma \in S_n$, така че $f(P_{\sigma(r+1)}) = \ldots = f(P_{\sigma(n)}) = 0$. С други думи, съществува дивизор $D' = \sum_{j=r+1}^{n} P_{\sigma(j)}$ от степен $\deg(D') = n - r$, така че $D \geq D'$ и $f \in \mathcal{L}(G - D')$. Минималното разстояние d на $C(X, D, G)$ е минималното естествено $d = r$ с това свойство

□

3.2 Тъждества на Мак Уилямс за тегловото разпределение на двойка дуални линейни кодове

Настоящият параграф припомня доказателството на Уорд от [Ward] на тъждествата на Мак Уилямс за линеен код C и неговия дуален $C^\perp$. Ако C и $C^\perp$ са с дължина n, $k = \dim_{\mathbb{F}_q}(C)$ и $\mathcal{W}_C(x, y)$, съответно, $\mathcal{W}_{C^\perp}(x, y)$ са тегловите полиноми на тези кодове, то тъждествата на Мак Уилямс се свеждат до равенството

$$\mathcal{W}_{C^\perp}(x, y) = \frac{1}{q^k}\mathcal{W}_C(x + (q-1)y, x - y) \tag{3.1}$$

на хомогенни полиноми на x, y от степен n с рационални коефициенти.

За да докажем (3.1) с индукция по дължината n, за $\forall 1 \leq i \leq n$ разглеждаме пунктираните кодове $P_i(C) \subset \mathbb{F}_q^{n-1}$ и скъсените кодове $S_i(C) \subset \mathbb{F}_q^{n-1}$. По определение, пунктирането

$$P_i : C \longrightarrow P_i(C),$$

$$P_i(c_1, \ldots, c_n) = (c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n)$$

в i-тата компонента е изтриването на тази компонента. Образът на C под действие на пунктирането P_i се означава с $P_i(C)$. Ако

$$Z(x_i) := \{a \in \mathbb{F}_q^n \mid a_i = 0\}$$

е хиперравнината в $\mathbb{F}_q^n$ с уравнение $x_i = 0$, то образът $P_i(C \cap Z(x_i))$ на думите $c \in C \cap Z(x_i)$ на C с нулева i-та компонента, под действие на пунктирането P_i се нарича скъсяване на C и се бележи с $S_i(C)$. Пунктирането и скъсяването са съгласувани с вътрешното произведение, съгласно следната лема.

Лема 96. *Нека $C \subset \mathbb{F}_q^n$ е $\mathbb{F}_q$-линеен код с дуален $C^\perp$ и $1 \leq i \leq n$. Тогава i-тото пунктиране $P_i(C)$ на C и i-тото скъсяване $S_i(C^\perp)$ на $C^\perp$ са взаимно дуални, т.е.*

$$P_i(C)^\perp = S_i(C^\perp).$$

Още повече, ако C е с минимално разстояние $d > 1$, то $C^\perp$ не се съдържа в координатна хиперравнина $Z(x_i)$ и

$$\dim_{\mathbb{F}_q}(P_i(C)) = \dim_{\mathbb{F}_q}(C), \quad \dim_{\mathbb{F}_q}(P_i(C)^\perp) = \dim_{\mathbb{F}_q}(S_i(C^\perp)) = \dim_{\mathbb{F}_q}(C^\perp) - 1.$$

Доказателство: За включването $S_i(C^\perp) \subseteq P_i(C)^\perp$ да изберем $c^* \in S_i(C^\perp) \subset \mathbb{F}_q^{n-1}$. Ако $c^* = (c_1, \ldots, c_{i-1}, c_i, \ldots, c_{n-1})$, то $c := (c_1, \ldots, c_{i-1}, 0, c_i, \ldots, c_{n-1}) \in C^\perp \cap Z(x_i)$ и за всяка дума $x \in C$ е в сила

$$0 = \langle x, c\rangle = \langle P_i(x), c^*\rangle.$$

Следователно $c^* \in P_i(C)^\perp$ и $S_i(C^\perp) \subseteq P_i(C)^\perp$.

Обратно, ако $a = (a_1, \ldots, a_{i-1}, a_i, \ldots, a_{n-1}) \in P_i(C)^\perp$ и

$$\widehat{a} := (a_1, \ldots, a_{i-1}, 0, a_i, \ldots, a_{n-1}),$$

то за всяка дума $x \in C$ е в сила

$$0 = \langle P_i(x), a\rangle = \langle x, \widehat{a}\rangle.$$

Следователно $\widehat{a} \in C^\perp$ и вземайки предвид $\widehat{a} \in Z(x_i)$, получаваме $a \in P_i(C^\perp \cap Z(x_i)) = S_i(C^\perp)$. Това доказва $P_i(C)^\perp \subseteq S_i(C^\perp)$ и $P_i(C)^\perp = S_i(C^\perp)$.

Непосредствено се проверява, че пунктирането $P_i : C \to P_i(C)$ е $\mathbb{F}_q$-линейно изображение. Ако C е с минимално растояние $d > 1$, то P_i има нулево ядро $\ker(P_i|_C) = 0$ и $P_i : C \to P_i(C)$ е $\mathbb{F}_q$-линеен изоморфизъм. В частност, $\dim_{\mathbb{F}_q}(P_i(C)) = \dim_{\mathbb{F}_q}(C) = k$. Следователно $\dim_{\mathbb{F}_q}(S_i(C^\perp)) = \dim_{\mathbb{F}_q}(P_i(C)^\perp) = n - 1 - \dim_{\mathbb{F}_q}(P_i(C)) = n - 1 - k$. Да забележим, че пунктирането P_i се ограничава до $\mathbb{F}_q$-линеен изоморфизъм

$$P_i : C^\perp \cap Z(x_i) \to P_i(C^\perp \cap Z(x_i)) = S_i(C^\perp).$$

Затова $\dim_{\mathbb{F}_q}(C^\perp \cap Z(x_i)) = \dim_{\mathbb{F}_q}(S_i(C^\perp)) = n - 1 - k$. Съгласно

$$\dim_{\mathbb{F}_q}(C^\perp) = n - \dim_{\mathbb{F}_q}(C) = n - k > \dim_{\mathbb{F}_q}(C^\perp \cap Z(x_i)),$$

кодът $C^\perp$ не се съдържа в хиперравнината $Z(x_i)$. Това завършва доказателството на лемата.

□

Линеен код $C \subset \mathbb{F}_q^n$ е разложим, ако съществуват естествено число $1 \leq k \leq n-1$ и линейни кодове $C_1 \subseteq \mathbb{F}_q^k$, $C_2 \subseteq \mathbb{F}_q^{n-k}$, така че

$$C = C_1 \times C_2 = \{(c', c'') \in \mathbb{F}_q^n \,|\, c' \in C_1,\, c'' \in C_2\}.$$

Ако $C = C_1 \times C_2$ е разложим, то дуалният код $C^\perp$ се състои от думите $a = (a', a'') \in \mathbb{F}_q^k \times \mathbb{F}_q^{n-k}$ с

$$0 = \langle a, c\rangle = \langle a', c'\rangle + \langle a'', c''\rangle, \quad \forall c = (c', c'') \in C_1 \times C_2 = C.$$

В частност, за $c'' = 0_{\mathbb{F}_q}^{n-k}$ следва $a' \in C_1^\perp \subseteq \mathbb{F}_q^k$, а за $c' = 0_{\mathbb{F}_q}^k$ получаваме $a'' \in C_2^\perp \subseteq \mathbb{F}_q^{n-k}$. Следователно $(C_1 \times C_2)^\perp \subseteq C_1^\perp \times C_2^\perp$. Обратно, ако $(a', a'') \in C_1^\perp \times C_2^\perp$, то за $\forall c' \in C_1$ и $\forall c'' \in C_2$ е в сила

$$\langle (a', a''), (c', c'')\rangle = \langle a', c'\rangle + \langle a'', c''\rangle = 0.$$

Това доказва $C_1^\perp \times C_2^\perp \subseteq (C_1 \times C_2)^\perp$ и

$$(C_1 \times C_2)^\perp = C_1^\perp \times C_2^\perp.$$

С други думи, дуалният на разложим код е разложим. Ако $\mathcal{W}_{C_1}(x,y) \in \mathbb{Z}[x,y]^{(k)}$ е тегловият полином на $C_1 \subseteq \mathbb{F}_q^k$ и $\mathcal{W}_{C_2}(x,y) \in \mathbb{Z}[x,y]^{(n-k)}$ е тегловият полином на $C_2 \subseteq \mathbb{F}_q^{n-k}$, то тегловият полином на $C_1 \times C_2 \subseteq \mathbb{F}_q^n$ е

$$\mathcal{W}_{C_1 \times C_2}(x,y) = \mathcal{W}_{C_1}(x,y)\mathcal{W}_{C_2}(x,y),$$

защото броят на думите на $C_1 \times C_2$ с тегло w е

$$\mathcal{W}_{C_1 \times C_2}^{(w)} = \sum_{s=0}^{w} \mathcal{W}_{C_1}^{(s)} \mathcal{W}_{C_2}^{(w-s)}$$

за броя $\mathcal{W}_{C_1}^{(s)}$ на думите на C_1 с тегло s и броя $\mathcal{W}_{C_2}^{(w-s)}$ на думите на C_2 с тегло $w-s$. Аналогично,

$$\mathcal{W}_{(C_1 \times C_2)^\perp}(x,y) = \mathcal{W}_{C_1^\perp \times C_2^\perp}(x,y) = \mathcal{W}_{C_1^\perp}(x,y)\mathcal{W}_{C_2^\perp}(x,y),$$

така че е достатъчно да проверим (3.1) за неразложим код C и неговия дуален $C^\perp$, за да получим тъждествата на Мак Уилямс за произволна двойка дуални линейни кодове,

$$\begin{aligned} \mathcal{W}_{(C_1 \times C_2)^\perp}(x,y) &= \mathcal{W}_{C_1^\perp}(x,y)\mathcal{W}_{C_2^\perp}(x,y) = \\ = \frac{1}{|C_1|}\mathcal{W}_{C_1}(x+(q-1)y, x-y)\frac{1}{|C_2|}\mathcal{W}_{C_2}(x+(q-1)y, x-y) &= \\ = \frac{1}{|C_1 \times C_2|}\mathcal{W}_{C_1 \times C_2}(x+(q-1)y, x-y). & \end{aligned}$$

В частност, можем да предполагаме, че линейният код $C \subset \mathbb{F}_q^n$ има минимално разстояние $d > 1$, защото ако C има дума $c = (0^{i-1}, c_i, 0^{n-i}) \in C$ с тегло $\mathrm{wt}(c) = 1$, то C се разлага в директно произведение на $0^{i-1} \times \mathbb{F}_q \times 0^{n-i}$ и $C \cap Z(x_i)$.

Теорема 97. *Ако $C \subset \mathbb{F}_q^n$ е $\mathbb{F}_q$-линеен код с размерност $k = \dim_{\mathbb{F}_q}(C)$, а $C^\perp \subset \mathbb{F}_q^n$ е дуалният код на C, то тегловите полиноми на C и $C^\perp$ изпълняват равенството*

$$\mathcal{W}_{C^\perp}(x,y) = \frac{1}{q^k}\mathcal{W}(x+(q-1)y, x-y)$$

на хомогенни полиноми на x, y от степен n.

Доказателство: С индукция по дължината n, в случая $n = 1$ имаме $k = \dim_{\mathbb{F}_q}(C) = 0$ или 1. Ако $k = 0$ и $C = \{0_{\mathbb{F}_q}\}$, то $\mathcal{W}_C(x,y) = x$, $C^\perp = \mathbb{F}_q$ и

$$\mathcal{W}_{C^\perp}(x,y) = x + (q-1)y = \frac{1}{q^0}\mathcal{W}_C(x+(q-1)y, x-y).$$

В случая $k = 1$ е изпълнено $C = \mathbb{F}_q$ с $\mathcal{W}_C(x, y) = x + (q-1)y$ и $C^\perp = \{0_{\mathbb{F}_q}\}$ с

$$\mathcal{W}_{C^\perp}(x, y) = x = \frac{1}{q}\mathcal{W}_C(x + (q-1)y, x - y).$$

Да предположим, че тъждествата на Мак Уилямс са изпълнени за всички линейни кодове C с дължина $< n$. Съгласно забележката преди Теорема 97, можем да считаме че линейният код $C \subset \mathbb{F}_q^n$ с дължина n е неразложим. В частност, има минимално разстояние $d > 1$. Тогава пунктираният $P_i(C) \subseteq \mathbb{F}_q^{n-1}$ са с размерност $\dim_{\mathbb{F}_q}(P_i(C)) = \dim_{\mathbb{F}_q}(C) = k$. Ако към дума $c \in C$ с тегло $\mathrm{wr}(c) = w$ приложим пунктираният $P_1, \ldots, P_n$, то в резултат получаваме w думи с дължина $n-1$ и тегло $w-1$, както и $n-w$ думи с дължина $n-1$ и тегло w. Следователно сумата на тегловите полиноми на $P_i(C)$ за $1 \leq i \leq n$ може да се изрази като

$$\begin{aligned}\sum_{i=1}^{n} \mathcal{W}_{P_i(C)}(x, y) &= \sum_{w=0}^{n} \mathcal{W}_C^{(w)}[wx^{n-w}y^{w-1} + (n-w)x^{n-1-w}y^w] = \\ &= \sum_{w=1}^{n} \mathcal{W}_C^{(w)} \left(\frac{\partial}{\partial x} + \frac{\partial}{\partial y}\right)(x^{n-w}y^w) = \left(\frac{\partial}{\partial x} + \frac{\partial}{\partial y}\right)\mathcal{W}_C(x, y),\end{aligned}$$

където $\frac{\partial}{\partial x}$ и $\frac{\partial}{\partial y}$ са диференцираният относно x и y. Аналогично, пунктираният $S_1, \ldots, S_n$, приложени към дума $c \in C$ с тегло $\mathrm{wt}(c) = w$ дават $n-w$ думи с дължина $n-1$ и тегло w. В резултат, сумата на тегловите полиноми на $S_i(C)$ е

$$\sum_{i=1}^{n} \mathcal{W}_{S_i(C)}(x, y) = \sum_{w=0}^{n} \mathcal{W}_C^{(w)}(n-w)x^{n-1-w}y^w = \sum_{w=0}^{n} \mathcal{W}_C^{(w)} \frac{\partial}{\partial x}(x^{n-w}y^w) = \frac{\partial}{\partial x}(\mathcal{W}_C(x, y)).$$

По индукционно предположение,

$$\mathcal{W}_{P_i(C)^\perp}(x, y) = \frac{1}{q^k}\mathcal{W}_{P_i(C)}(x + (q-1)y, x - y)$$

за линейните кодове $P_i(C) \subset \mathbb{F}_q^{n-1}$ с дължина $n-1$ и размерност k. Комбинирайки с $P_i(C)^\perp = S_i(C^\perp)$ от Лема 96 получаваме

$$\begin{aligned}\frac{\partial}{\partial x}\mathcal{W}_{C^\perp}(x, y) &= \sum_{i=1}^{n} \mathcal{W}_{S_i(C)}(x, y) = \sum_{i=1}^{n} \mathcal{W}_{P_i(C)^\perp}(x, y) = \\ &= \frac{1}{q^k}\left(\sum_{i=1}^{n} \mathcal{W}_{P_i(C)}(x + (q-1)y, x - y)\right) = \\ &= \frac{1}{q^k}\left[\left(\frac{\partial}{\partial x} + \frac{\partial}{\partial y}\right)\mathcal{W}_C(x, y)\right](x + (q-1)y, x - y).\end{aligned}$$

Прилагайки правилото за диференциране на сложна функция

$$\begin{aligned}\frac{\partial}{\partial x}\mathcal{W}_C(x+(q-1)y,x-y) &= \\ = \left[\frac{\partial}{\partial x}\mathcal{W}_C(x,y)\right](x+(q-1)y,x-y) + \left[\frac{\partial}{\partial y}\mathcal{W}_C(x,y)\right](x+(q-1)y,x-y) &= \\ = \left[\left(\frac{\partial}{\partial x}+\frac{\partial}{\partial y}\right)\mathcal{W}_C(x,y)\right](x+(q-1)y,x-y),&\end{aligned}$$

получаваме

$$\frac{\partial}{\partial x}\mathcal{W}_{C^\perp}(x,y) = \frac{\partial}{\partial x}\left[\frac{1}{q^k}\mathcal{W}_C(x+(q-1)y,x-y)\right].$$

С други думи, хомогенният полином

$$\mathcal{W}_o(x,y) := \mathcal{W}_{C^\perp}(x,y) - \frac{1}{q^k}\mathcal{W}_C(x+(q-1)y,x-y)$$

от степен n не зависи от x и $\mathcal{W}_o(x,y) = ay^n$ за някаква константа $a \in \mathbb{Q}$. Да забележим, че $\mathcal{W}_{C^\perp}(1,1) = |C^\perp| = q^{n-k}$ е броят на думите в $C^\perp$, а $\mathcal{W}_C(q,0) = q^n$. Затова полагането $x = y = 1$ в

$$\mathcal{W}_{C^\perp}(x,y) - \frac{1}{q^k}\mathcal{W}_C(x+(q-1)y,x-y) = ay^n$$

дава $0 = q^{n-k} - \frac{q^n}{q^k} = a$ и доказва тъждествата на Мак Уилямс

$$\mathcal{W}_{C^\perp}(x,y) = \frac{1}{q^k}\mathcal{W}_C(x+(q-1)y,x-y).$$

□

3.3 Дзета полином на линеен код

Следващото понятие, на което трябва да обърнем внимание е самият дзета полином на линеен код. Той е въведен и изследван от Дуурсма в статиите [Duursma1] и [Duursma2]. Мотивацията за това понятие, както и неговото определение се съдържат в следното твърдение.

Твърдение 98. (Duursma - [Duursma1], [Duursma2]) *За произволен $\mathbb{F}_q$ - линеен $[n,k,d]$ код C, несъдържащ се в координатна хиперравнина $Z(x_i) := \{\ x \in \mathbb{F}_q^n \mid x_i = 0\ \}$ на $\mathbb{F}_q^n$ съществуват еднозначно определени рационални числа $a_0, a_1, \ldots, a_r$, такива че тегловият полином $\mathcal{W}_C(x,y)$ на кода C се изразява като следната линейна комбинация на хомогенните теглови полиноми $\mathcal{M}_{n,d+i}(x,y)$ на MDS-кодове с дължина n и минимални разстояния $d+i$*

$$\mathcal{W}_C(x,y) = a_0\mathcal{M}_{n,d}(x,y) + a_1\mathcal{M}_{n,d+1}(x,y) + \ldots + a_r\mathcal{M}_{n,d+r}(x,y). \tag{3.2}$$

и

$$\sum_{i=0}^{r} a_i = 1. \tag{3.3}$$

Полиномът $P_C(t) = \sum_{i=0}^{r} a_i t^i$ *се нарича* ζ*-полином на кода* C *и е еднозначно определен от равенството*

$$\frac{\mathcal{W}_C(x,y) - x^n}{q-1} = Coeff_{t^{n-d}} \left(\frac{P_C(t)}{(1-t)(1-qt)} [y(1-t) + xt]^n \right), \tag{3.4}$$

където с $Coeff_{t^{n-d}}(f(t))$ *означаваме коефициента пред* t^{n-d} *на формалния степенен ред* $f(t) \in \mathbb{C}[[t]]$.

Доказателство: Да забележим, че

$$\mathcal{M}_{n,d}(x,y) - x^n = \sum_{s=d}^{n} \mathcal{M}_{n,d}^{(s)} x^{n-s} y^s$$

има ненулев коефициент $\mathcal{M}_{n,d}^{(d)} = \binom{n}{d}(q-1)$ пред $x^{n-d}y^d$, така че полиномите

$$\mathcal{M}_{n,d}(x,y) - x^n, \mathcal{M}_{n,d+1}(x,y) - x^n, \ldots, \mathcal{M}_{n,n}(x,y) - x^n$$

образуват $\mathbb{Q}$-базис на линейното пространство $\mathbb{Q}[x,y]_{\geq d}^{(n)}$ на хомогенните полиноми на x и y от степен n, в чиито едночлени y участва от степен поне d. Тъй като $\mathcal{W}_C(x,y) - x^n \in \mathbb{Q}[x,y]_{\geq d}^{(n)}$, то съществуват еднозначно определени числа $a_i \in \mathbb{Q}$, $0 \leq i \leq n-d$, такива че

$$\mathcal{W}_C(x,y) - x^n = \sum_{i=0}^{n-d} a_i (\mathcal{M}_{n,d+i}(x,y) - x^n),$$

или с други думи

$$\mathcal{W}_C(x,y) = \left(1 - \sum_{i=0}^{n-d} a_i\right) x^n + \sum_{i=0}^{n-d} a_i \mathcal{M}_{n,d+i}(x,y). \tag{3.5}$$

По същия начин и

$$\mathcal{W}_{C^\perp}(x,y) = \left(1 - \sum_{j=0}^{n-d^\perp} a_j^\perp\right) x^n + \sum_{j=0}^{n-d^\perp} a_j^\perp \mathcal{M}_{n,d^\perp+j}(x,y), \tag{3.6}$$

за еднозначно определени числа $a_j^\perp \in \mathbb{Q}$, $0 \leq j \leq n - d^\perp$.

Ако кодът $C_{n,d} \in \mathbb{F}_q^n$ е MDS-код, то неговият дуален код $C_{n,d}^\perp = C_{n,d^\perp}$, също е MDS-код. В такъв случай $d^\perp = n + 2 - d$ и от тъждествата на МакУилямс имаме

$$q^{n-q-d} \mathcal{M}_{n,n+2-d}(x,y) = \mathcal{M}_{n,d}(x + (q-1)y, x - y). \tag{3.7}$$

Заместваики (3.5) и (3.6) в (97) и прилагайки (3.7), получаваме

$$\begin{aligned} q^k\left(1-\sum_{j=0}^{n-d^\perp} a_j^\perp\right)x^n + q^k\sum_{j=0}^{n-d^\perp} b_j\mathcal{M}_{n,d^\perp+j}(x,y) = \\ = \left(1-\sum_{i=0}^{n-d} a_i\right)[x+(q-1)y]^n + \sum_{i=0}^{n-d} a_i q^{n+1-d-i}\mathcal{M}_{n,n+2-d-i}(x,y). \end{aligned} \tag{3.8}$$

Спрямо индексите на сумиране $d^\perp \le \alpha := d^\perp + j \le n$ и $2 \le \beta := n+2-d-i \le n-2-d$, изразяваме

$$\begin{aligned} q^k\left(1-\sum_{j=0}^{n-d^\perp} a_j^\perp\right)x^n + q^k\sum_{\alpha=d^\perp}^{n} a^\perp_{\alpha-d^\perp}\mathcal{M}_{n,\alpha}(x,y) = \\ = \left(1-\sum_{i=0}^{n-d} a_i\right)[x+(q-1)y]^n + \sum_{\beta=2}^{n+2-d} q^{\beta-1}a_{n+2-d-\beta}\mathcal{M}_{n,\beta}(x,y). \end{aligned} \tag{3.9}$$

Ако $d^\perp > 1$, сравнявайки коефициентите пред $x^{n-1}y$ от двете страни на равенството, получаваме

$$\left(1-\sum_{i=0}^{n-d} a_i\right)n(q-1) = 0,$$

откъдето $\sum_{i=0}^{n-d} a_i = 1$. Още повече, сравнявайки коефициентите пред x^n, получаваме $\sum_{j=0}^{n-d^\perp} a_j^\perp = 1$ и равенство (3.9) се свежда до

$$q^k\sum_{j=d^\perp}^{n} a^\perp_{j-d^\perp}\mathcal{M}_{n,j}(x,y) = \sum_{i=2}^{n+2-d} q^{i-1}a_{n+2-d-i}\mathcal{M}_{n,i}(x,y). \tag{3.10}$$

Да забележим, че $d^\perp = 1$ тогава и само тогава когато съществуват индекс i, $1 \le i \le n$ и дума $c' \in C^\perp$, такива че $\mathrm{Supp(c')} = \{\mathrm{i}\}$. Това се случва точно когато $C \subseteq \mathrm{Span}_{\mathbb{F}_q}(c') = Z(x_i)$, което противоречи на предположението, че кодът C не се съдържа в никоя координатна хиперравнина $Z(x_i)$ и следователно $d^\perp > 1$.

Сравнявайки коефициентите пред $\mathcal{M}_{n,2}(x,y), \ldots, \mathcal{M}_{n,d^\perp-1}(x,y)$ в (3.10), заключаваме, че $a_{n+2-d-i} = 0$ за $2 \le i \le d^\perp - 1$, или $a_i = 0$ за $r+1 = n+2-d-d^\perp+1 \le i \le n-d$. Така равенство (3.5) приема вида (3.2). Освен това, $1 = \sum_{i=0}^{n-d} a_i$. Прилагайки (3.2) за $\mathbb{F}_q$ - линейния код $C^\perp \subset \mathbb{F}_q^n$, получаваме

$$\mathcal{W}_{C^\perp}(x,y) = \sum_{j=0}^{r} a_j^\perp \mathcal{M}_{n,d^\perp+j}(x,y)$$

и свеждаме (3.10) до

$$q^k \sum_{j=d^\perp}^{r+d^\perp} a^\perp_{j-d^\perp} \mathcal{M}_{n,j}(x,y) = \sum_{i=d^\perp}^{r+d^\perp} q^{i-1} a_{n+2-d-i} \mathcal{M}_{n,i}(x,y). \tag{3.11}$$

За доказателството на (3.4) ще използваме следното равенство

$$\frac{\mathcal{M}_{n,d}(x,y) - x^n}{q-1} = \mathrm{Coeff}_{t^{n-d}} \left(\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)} \right). \tag{3.12}$$

Използвайки $\mathrm{Coeff}_{t^{n-d}}(\alpha f(t) + \beta g(t)) = \alpha \mathrm{Coeff}_{t^{n-d}}(f(t)) + \beta \mathrm{Coeff}_{t^{n-d}}(g(t))$ за произволни изрази α и β, независещи от t и произволни $f(t)$, $g(t) \in \mathbb{C}[[t]]$, забелязваме че

$$\mathrm{Coeff}_{t^{n-d}} \left(\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)} \right) = \mathrm{Coeff}_{t^{n-d}} \left(\frac{\sum_{s=0}^{n} \binom{n}{s} t^{n-s}(1-t)^s x^{n-s} y^s}{(1-t)(1-qt)} \right) =$$

$$= \sum_{s=0}^{n} \binom{n}{s} x^{n-s} y^s \mathrm{Coeff}_{t^{n-d}} \left(\frac{t^{n-s}(1-t)^{s-1}}{1-qt} \right) = \sum_{s=0}^{n} \binom{n}{s} x^{n-s} y^s \mathrm{Coeff}_{t^{s-d}} \left(\frac{(1-t)^{s-1}}{1-qt} \right).$$

Да забележим, че формалните степенни редове

$$\frac{1}{(1-t)(1-qt)} \quad \text{и} \quad \frac{(1-t)^{s-1}}{1-qt}$$

нямат полюси в $t=0$. Следователно коефициентите пред t^{s-d} се нулират при $s < d$ и

$$\mathrm{Coeff}_{t^{n-d}} \left(\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)} \right) = \sum_{s=d}^{n} \binom{n}{s} x^{n-s} y^s \mathrm{Coeff}_{t^{s-d}} \left(\frac{(1-t)^{s-1}}{1-qt} \right).$$

Развивайки

$$\frac{1}{1-t} = \sum_{i=0}^{\infty} t^i \quad \text{и} \quad \frac{1}{1-qt} = \sum_{j=0}^{\infty} q^j t^j$$

като суми на геометрични прогресии, пресмятаме

$$\mathrm{Coeff}_{t^{s-d}} \left(\frac{(1-t)^{s-1}}{1-qt} \right) = \mathrm{Coeff}_{t^{s-d}} \left(\frac{(1-t)^{s}}{(1-t)(1-qt)} \right) =$$

$$= \mathrm{Coeff}_{t^{s-d}} \left(\left(\sum_{l=0}^{s} (-1)^l \binom{s}{l} t^l \right) \left(\sum_{i=0}^{\infty} t^i \right) \left(\sum_{j=0}^{\infty} q^j t^j \right) \right) = \sum_{l=0}^{s-d} (-1)^l \binom{s}{l} \left(\sum_{j=0}^{s-d-l} q^j \right) =$$

$$= \sum_{l=0}^{s-d} (-1)^l \binom{s}{l} \frac{q^{s-d-l+1}-1}{q-1} = \frac{\mathcal{M}^{(s)}_{n,d}}{\binom{n}{s}(q-1)}.$$

В резултат,

$$\text{Coeff}_{t^{n-d}}\left(\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right)=\sum_{s=d}^{n}\binom{n}{s}x^{n-s}y^s\text{Coeff}_{t^{s-d}}\left(\frac{(1-t)^{s-1}}{1-qt}\right)=$$
$$=\frac{\sum_{s=d}^{n}\mathcal{M}_{n,d}^{(s)}x^{n-s}y^s}{q-1}=\frac{\mathcal{M}_{n,d}(x,y)-x^n}{q-1},$$

което доказва (3.12).

Сега за $P_C(t)=\sum_{i=0}^{r}a_it^i$ имаме

$$\text{Coeff}_{t^{n-d}}\left(\frac{P_C(t)[y(1-t)+xt]^n}{(1-t)(1-qt)}\right)=\text{Coeff}_{t^{n-d}}\left(\sum_{i=0}^{r}a_i\frac{t^i[y(1-t)+xt]^n}{(1-t)(1-qt)}\right)=$$
$$=\sum_{i=0}^{r}a_i\text{Coeff}_{t^{n-d-i}}\left(\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right)=\sum_{i=0}^{r}a_i\frac{\mathcal{M}_{n,d+i}(x,y)-x^n}{q-1}=$$
$$=\frac{\sum_{i=0}^{r}a_i\mathcal{M}_{n,d+i}(x,y)-\left(\sum_{i=0}^{r}a_i\right)x^n}{q-1}=\frac{\mathcal{W}_C(x,y)-x^n}{q-1},$$

съгласно (3.12), (3.2) и (3.3)

□

3.4 Свойства на дзета полинома на линеен код

Твърдение 99. (Дуурсма - [Duursma3], Теорема 12.1) *Нека $X/\mathbb{F}_q\subset\mathbb{P}^N(\overline{\mathbb{F}_q})$ е гладка неприводима крива от род g, определена над $\mathbb{F}_q$, а $G_1,\ldots,G_h$ е пълна система ефективни представители на класовете на линейна еквивалентност на дивизорите на $F=\mathbb{F}_q(X)$ от степен $2g-2<m<n$. Да предположим, че съществуват n различни $\mathbb{F}_q$-рационални точки $P_1,\ldots,P_n\in X(\mathbb{F}_q)$, такива че $D=P_1+\ldots+P_n\in\text{Div}(F)$ имат носител $\text{Supp}(D)$, не пресичащ носителите на G_i, т.е. $\text{Supp}(D)\cap\text{Supp}(G_i)=\{P_1,\ldots,P_n\}\cap\text{Supp}(G_i)=\emptyset$ за $\forall 1\le i\le h$. Ако*

$$\mathcal{L}(G_i)=H^0(X,\mathcal{O}_X([G_i])):=\{f\in F^*\ \mid\ (f)+G_i\ge 0\}\cup\{0\}$$

са пространства на Риман-Рох на G_i,

$$\mathcal{E}_D:\mathcal{L}(G_i)\longrightarrow\mathbb{F}_q^n,$$

$$\mathcal{E}_D(f)=(f(P_1),\ldots,f(P_n))\quad\text{за}\quad\forall f\in\mathcal{L}(G_i)$$

са остойностяващите изображения в D, а $C_i := \mathcal{E}_D\mathcal{L}(G_i)$ са съответните алгебро-геометрични кодове на Гопа с теглови полиноми $\mathcal{W}_{C_i}(x,y)$, то

$$\sum_{i=1}^{h} \frac{\mathcal{W}_{C_i}(x,y) - x^n}{q-1} = \mathrm{Coeff}_{t^m}\left(\frac{L_F(t)}{(1-t)(1-qt)}[y(1-t)+xt]^n\right) \tag{3.13}$$

за ζ-полинома $L_F(t)$ на F. Еквивалентно,

$$L_F(t) = \sum_{i=1}^{h} t^{g-g_i} P_{C_i}(t) \tag{3.14}$$

за ζ-полиномите $P_{C_i}(t)$ на C_i.

Доказателство: Да забележим, че $\mathcal{E}_D : \mathcal{L}(G_i) \to \mathbb{F}_q^n$ са инективни, така че числата $\mathcal{W}_{C_i}^{(s)}$ са равни на броя на функциите $f \in \mathcal{L}(G_i)$, анулиращи се в точно $n-s$ от точките $P_1, \ldots, P_n$. За всяка s-торка $\alpha = \{\alpha_1, \ldots, \alpha_s\} \subset \{1, \ldots, n\}$, $1 \le \alpha_1 < \ldots < \alpha_s \le n$, да означим с $\mathcal{W}_{C_i}(\alpha)$ броят на рационалните функции $f \in \mathcal{L}(G_i)$ с $f(P_{\alpha_1}), \ldots, f(P_{\alpha_s}) \in \mathbb{F}_q^*$ и $f(P_j) = 0$ за $\forall j \in \{1, \ldots, n\} \setminus \alpha$. Тези $f \in \mathcal{L}(G_i)$ отговарят на ефективните дивизори $(f)+G_i = (f)_0 - (f)_\infty + G_i$ с $(f)_0 \ge D - (P_{\alpha_1} + \ldots + P_{\alpha_s})$ и $\mathrm{Supp}(f)_0 \cap \{P_{\alpha_1}, \ldots, P_{\alpha_s}\} = \emptyset$, които са линейно еквивалентни на G_i. Съгласно $(f)_\infty \le G_i$, условието

$$(f)_0 \ge D - (P_{\alpha_1} + \ldots + P_{\alpha_s})$$

е еквивалентно на $E := (f) + G_i - \left(\sum_{j \notin \alpha} P_j\right) \ge 0$. В такъв случай,

$$\mathrm{Supp}(f)_0 \cap \{P_{\alpha_1}, \ldots, P_{\alpha_s}\} = \emptyset$$

тогава и само тогава, когато $\mathrm{Supp}(E) \cap \{P_{\alpha_1}, \ldots, p_{\alpha_s}\} = \emptyset$, съгласно избора на $D = P_1 + \ldots + P_n$ с $\mathrm{Supp}(D) \cap \mathrm{Supp}(G_i) = \emptyset$. Затова $f \in \mathcal{L}(G_i)$ се анулира върху носителя на $D - (P_{\alpha_1} + \ldots + P_{\alpha_1})$ и не се анулира върху $P_{\alpha_1}, \ldots, P_{\alpha_s}$ точно когато

$$E := (f) + G_i - \left(\sum_{j \notin \alpha} P_j\right)$$

е ефективен дивизор на F с $\mathrm{Supp}(E) \cap \{P_{\alpha_1}, \ldots, P_{\alpha_s}\} = \emptyset$, който е линейно еквивалентен на $G_i - \left(\sum_{j \notin \alpha} P_j\right)$. Дивизорите на рационалните функции от $F = \mathbb{F}_q(X)$ са във взаимно еднозначно съответствие с $\mathbb{F}_q^*$-орбитите върху F. Ако $G_1, \ldots, G_h$ е пълна система представители на класовете на линейна еквивалентност на дивизорите на F от степен m, то

$$G_1 - \left(\sum_{j \notin \alpha} P_j\right), \ldots, G_h - \left(\sum_{j \notin \alpha} P_j\right)$$

е пълна система представители на дивизорите на F от степен $m-(n-s)=m-n+s$. Затова

$$\sum_{i=1}^{h}\mathcal{W}_{C_i}(\alpha)=(q-1)|\{E\in \mathrm{Div}(F)^{\geq 0}\ \mid\ \deg(E)=m-n+s,\ \ \mathrm{Supp}(E)\cap\{P_{\alpha_1},\ldots,P_{\alpha_s}\}=\emptyset\}|. \tag{3.15}$$

Да напомним ζ-функцията на Хасе-Вайл

$$\zeta_F(t)=\frac{L_F(t)}{(1-t)(1-qt)}=\prod_{\nu\in \mathrm{Orb}_{\mathfrak{G}}(X)}\frac{1}{(1-t^{\deg\nu})}=\sum_{j=0}^{\infty}\mathcal{A}_j t^j,$$

където $\mathfrak{G}=Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ е абсолютната група на Галоа на $\mathbb{F}_q$, $\mathrm{Orb}_{\mathfrak{G}}(X)$ е множеството на $\mathfrak{G}$-орбитите върху X, а $\mathcal{A}_j$ е броят на ефективните дивизори на $F=\mathbb{F}_q(X)$ от степен j. Да забележим, че $\mathbb{F}_q$-рационалните точки $P_{\alpha_1},\ldots,P_{\alpha_s}$ са $\mathfrak{G}$-орбити от степен 1, така че

$$\zeta_F(t)(1-t)^s=\frac{(1-t)^s}{\prod\limits_{\nu\in \mathrm{Orb}_{\mathfrak{G}}(X)}(1-t^{\deg\nu})}=\prod_{\nu\in \mathrm{Orb}_{\mathfrak{G}}(X)\setminus\{P_{\alpha_1},\ldots,P_{\alpha_s}\}}\frac{1}{(1-t^{\deg\nu})}=\sum_{j=0}^{\infty}\mathcal{B}_j(\alpha)t^j$$

е пораждащата функция за броя $\mathcal{B}_j(\alpha)$ на ефективните дивизори на F от степен j, чийто носител не пресича $\{P_{\alpha_1},\ldots,P_{\alpha_s}\}$. Следователно, (3.15) може да се запише като

$$\sum_{i=1}^{h}\mathcal{W}_{C_i}(\alpha)=(q-1)\mathcal{B}_{m-n+s}(\alpha).$$

Да забележим, че формалният степенен ред $\zeta_F(t)(1-t)^s$ не зависи от $\alpha=\{\alpha_1,\ldots,\alpha_s\}$, $1\leq\alpha_1<\ldots<\alpha_s\leq n$, така че всеки от коефициентите $\mathcal{B}_j(\alpha)$ е независим от α. Ако $\binom{[n]}{s}$ е множеството на всички s-торки $\alpha=\{\alpha_1,\ldots,\alpha_s\}\subset\{1,\ldots,n\}$, то

$$\sum_{\alpha\in\binom{[n]}{s}}\mathcal{W}_{C_i}(\alpha)=\mathcal{W}_{C_i}^{(s)},$$

откъдето

$$\sum_{i=1}^{h}\mathcal{W}_{C_i}^{(s)}=\sum_{i=1}^{h}\sum_{\alpha\in\binom{[n]}{s}}\mathcal{W}_{C_i}(\alpha)=\sum_{\alpha\in\binom{[n]}{s}}\left(\sum_{i=1}^{h}\mathcal{W}_{C_i}(\alpha)\right)=$$

$$\sum_{\alpha\in\binom{[n]}{s}}(q-1)\mathcal{B}_{m-n+s}=(q-1)\binom{n}{s}\mathcal{B}_{m-n+s}=(q-1)\binom{n}{s}\mathrm{Coeff}_{t^{m-n+s}}(\zeta_F(t)(1-t)^s). \tag{3.16}$$

От друга страна,

$$\mathrm{Coeff}_{t^m}\left(\frac{L_F(t)}{(1-t)(1-qt)}[y(1-t)+xt]^n\right) =$$
$$\mathrm{Coeff}_{t^m}\left(\zeta_F(t)\sum_{s=0}^{n}\binom{n}{s}t^{n-s}(1-t)^s x^{n-s}y^s\right) =$$
$$\sum_{s=0}^{n}\binom{n}{s}x^{n-s}y^s\mathrm{Coeff}_{t^{m-n+s}}(\zeta_F(t)(1-t)^s).$$

Степенният ред

$$\zeta_F(t)(1-t)^s = \frac{L_F(t)}{(1-t)(1-qt)}(1-t)^s$$

е холоморфен в околност на $t=0$, така че $\mathrm{Coeff}_{t^{m-n+s}}(\zeta_F(t)(1-t)^s)=0$ за $m-n+s<0$ и

$$\mathrm{Coeff}_{t^m}\left(\frac{L_F(t)}{(1-t)(1-qt)}[y(1-t)+xt]^n\right) = \sum_{s=n-m}^{n}\binom{n}{s}x^{n-s}y^s\mathrm{Coeff}_{t^{m-n+s}}(\zeta_F(t)(1-t)^s) =$$
$$\sum_{s=n-m}^{n}\left(\frac{\sum\limits_{i=1}^{h}\mathcal{W}_{C_i}^{(s)}}{q-1}\right)x^{n-s}y^s = \sum_{i=1}^{h}\left(\frac{\sum\limits_{s=n-m}^{n}\mathcal{W}_{C_i}^{(s)}x^{n-s}y^s}{q-1}\right) = \sum_{i=1}^{h}\frac{\mathcal{W}_{C_i}(x,y)-x^n}{q-1}.$$

Произволна ненулева дума $c=(f(P_1),\ldots,f(P_n))\in C_i=\mathcal{E}_D\mathcal{L}(G_i)$ с $f\in\mathcal{L}(G_i)$ има най-много $m=\deg(G_i)$ ненулеви компоненти. Следователно c е с тегло $\mathrm{wt}(c)\geq n-m$. В частност, минималното разстояние d_i на C_i изпълнява неравенството

$$d_i\geq n-m.$$

Остойностяващото изображение $\mathcal{E}_D:\mathcal{L}(G_i)\to C_i$ е влагане, защото съществува нетъждествено нулева рационална функция $f\in\mathcal{L}(G_i)\setminus\{0\}$, която се анулира в $n>m=\deg(G_i)$ точки. Следователно

$$\dim_{\mathbb{F}_q}(C_i)=\dim_{\mathbb{F}_q}(\mathcal{L}(G_i))=\deg(G_i)-g+1=m-g+1,$$

съгласно Теорема 84 на Риман-Рох за дивизора G_i от степен $\deg(G_i)=m\geq 2g-1$. Оттук, родът на линейния код C_i е

$$g_i=n+1-\dim_{\mathbb{F}_q}(C_i)-d_i=n-m-d_i+g\leq g,$$

съгласно $d_i\geq n-m$. В частност, $\sum\limits_{i=1}^{h}t^{g-g_i}P_{C_i}(t)\in\mathbb{Q}[t]$ е полином с рационални коефициенти.

Достатъчно е да проверим, че полиномът $P(t) := L_F(t) - \sum_{i=1}^{h} t^{g-g_i} P_{C_i}(t) \in \mathbb{Q}[t]$ изпълнява условието

$$\mathrm{Coeff}_{t^m}\left(P(t)\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right) = 0, \tag{3.17}$$

за да получим, че $P(t) \equiv 0$ се анулира тъждествено. По-точно, ако $P(t) = \sum_{i\geq 0} \nu_i t^i \in \mathbb{Z}[t]$, то съгласно (3.12) е в сила

$$0 = \mathrm{Coeff}_{t^m}\left(P(t)\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right) = \mathrm{Coeff}_{t^m}\left(\left(\sum_{i\geq 0}\nu_i t^i\right)\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right) =$$
$$= \sum_{i\geq 0}\nu_i \mathrm{Coeff}_{t^{m-i}}\left(\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right) = \sum_{i\geq 0}\nu_i \frac{\mathcal{M}_{n,n-m+i}(x,y) - x^n}{q-1}.$$

Тук $n-m+i > 0$ поради $n > m$. Последователното сравняване на коефициентите на $x^{m-i}y^{n-m+i}$ за $i = 0, 1, \ldots$ в горното равенство дава $\nu_i = 0$ за всички $i = 0, 1, \ldots$.

Съгласно (3.13), (3.4) и $m - g + g_i = n - d_i$ е в сила

$$\mathrm{Coeff}_{t^m}\left(P(t)\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right) =$$
$$= \mathrm{Coeff}_{t^m}\left(L_F(t)\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right) - \mathrm{Coeff}_{t^m}\left(\sum_{i=1}^{h} t^{g-g_i}P_{C_i}(t)\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right) =$$
$$= \sum_{i=1}^{h}\frac{\mathcal{W}_{C_i}(x,y) - x^n}{q-1} - \sum_{i=1}^{h}\mathrm{Coeff}_{t^{m-g+g_i}}\left(P_{C_i}(t)\frac{[y(qt)+xt]^n}{(1-t)(1-qt)}\right) = 0,$$

което доказва (3.17) и (3.14).

□

Твърдение 100. (Дуурсма - [Duursma2]) *Нека $C \subset \mathbb{F}_q^n$ е линеен код от род g с минимално разстояние $d \geq 2$ и ζ-полином $P_C(t)$, а $C^\perp \subset \mathbb{F}_q^n$ е дуалният код на C от род $g^\perp$ с ζ-полином $P_{C^\perp}(t)$. Тогава тъждествата на Мак Уилямс за тегловото разпределение на C и $C^\perp$ са еквивалентни на функционалното уравнение*

$$P_{C^\perp}(t) = P_C\left(\frac{1}{qt}\right) q^g t^{g+g^\perp}. \tag{3.18}$$

Доказателство: Съгласно (3.2) от Твърдение 98, съществуват еднозначно определени рационални числа $a_i, a_i^\perp \in \mathbb{Q}$ за $0 \leq i \leq r := g + g^\perp$, изразяващи тегловите полиноми

$$\mathcal{W}_{C^\perp}(x,y) = \sum_{i=0}^{r} a_i^\perp \mathcal{M}_{n,d^\perp+i}(x,y), \quad \mathcal{W}_C(x,y) = \sum_{i=0}^{r} a_i \mathcal{M}_{n,d+i}(x,y)$$

на $C^\perp$, C чрез MDS-теглови полиноми. Дуалният на MDS-код с дължина n и минимално разстояние $d+i$ е MDS-код с дължина n и минимално разстояние $n+2-d-i = r + d^\perp - i$. Тъждествата на Мак Уилямс за такива кодове гласят, че

$$\mathcal{M}_{n,r+d^\perp-i}(x,y) = \frac{1}{q^{n+1-d-i}}\mathcal{M}_{n,d+i}(x+(q-1)y, x-y).$$

Комбинирайки с тъждествата на Мак Уилямс

$$\mathcal{W}_{C^\perp}(x,y) = \frac{1}{q^k}\mathcal{W}_C(x+(q-1)y, x-y)$$

за C, $C^\perp$ с $k = \dim_{\mathbb{F}_q}(C)$, получаваме

$$\begin{aligned}\sum_{i=0}^{r} a_i^\perp \mathcal{M}_{n,d^\perp+i}(x,y) = \mathcal{W}_{C^\perp}(x,y) = \frac{1}{q^k}\mathcal{W}_C(x+(q-1)y, x-y) = \\ = \frac{1}{q^k}\left(\sum_{i=0}^{r} a_i \mathcal{M}_{n,d+i}(x+(q-1)y, x-y)\right) = \sum_{i=0}^{r} q^{g-i} a_i \mathcal{M}_{n,r+d^\perp-i}(x,y),\end{aligned} \tag{3.19}$$

вземайки предвид определението $g := n+1-d-k$ за род на C с минимално разстояние d. Полагането $y = 0$ в горното равенство и (3.3) за $C^\perp$ дават

$$x^n = \left(\sum_{i=0}^{r} a_i^\perp\right) = \sum_{i=0}^{r} a_i^\perp \mathcal{M}_{n,d^\perp+i}(x,0) = \sum_{i=0}^{r} q^{g-i} a_i \mathcal{M}_{n,r+d^\perp-i}(x,0) = \left(\sum_{i=0}^{r} q^{g-i} a_i\right) x^n,$$

откъдето

$$\sum_{i=0}^{r} q^{g-i} a_i = \sum_{i=0}^{r} a_i^\perp = 1. \tag{3.20}$$

След смяна $j = r - i$ на индекса на сумиране в (3.19) и (3.20) извеждаме, че

$$\sum_{i=0}^{r} a_i^\perp \mathcal{M}_{n,d^\perp+i}(x,y) = \sum_{j=0}^{r} q^{j-g^\perp} a_{r-j} \mathcal{M}_{n,d^\perp+j}(x,y)$$

и

$$\sum_{j=0}^{r} q^{j-g^\perp} a_{r-j} = \sum_{i=0}^{r} q^{g-i} a_i = \sum_{i=0}^{r} a_i^\perp = 1.$$

В резултат,

$$\sum_{i=0}^{r} a_i^\perp \left[\mathcal{M}_{n,d^\perp+i}(x,y) - x^n\right] = \sum_{j=0}^{r} q^{j-g^\perp} a_{r-j} \left[\mathcal{M}_{n,d^\perp+j}(x,y) - x^n\right]. \tag{3.21}$$

Да забележим, че $\{\mathcal{M}_{n,d^\perp+i}(x,y) = x^n \,|\, 0 \le i \le n - d^\perp\}$ е базис на $\mathbb{Q}$-линейното пространство $\mathbb{Q}[x,y]^{(n)}_{\ge d^\perp}$ на хомогенните полиноми на x и y от степен n, които са от степен $\ge d^\perp$ относно y. За $d \ge 2$ е в сила $r = n + 2 - d - d^\perp \le n - d^\perp$, така

че $\{\mathcal{M}_{n,d^\perp+i}(x,y) - x^n \,|\, 0 \leq i \leq r\}$ е линейно независима система и равенството на полиноми (3.21) е еквивалентно на павенствата на рационални числа

$$a_i^\perp = q^{i-g^\perp} a_{r-i} \quad \text{за} \quad 0 \leq i \leq r. \tag{3.22}$$

От друга страна, полиномите $P_C(t) = \sum\limits_{i=0}^{r} a_i t^i$, $P_{C^\perp}(t) = \sum\limits_{i=0}^{r} a_i^\perp t^i \in \mathbb{Q}[t]$ изпълняват функционалното уравнение (3.18) точно когато

$$\sum_{i=0}^{r} a_i^\perp t^i = P_{C^\perp}(t) = P_C\left(\frac{1}{qt}\right) q^g t^{g+g^\perp} = \left(\sum_{i=0}^{r} a_i q^{-i} t^{-i}\right) q^g t^r = \\ = \sum_{i=0}^{r} q^{g-i} a_i t^{r-i} = \sum_{j=0}^{r} q^{j-g^\perp} a_{r-j} t^j$$

след смяна на сумационния индекс i с $j = r - i$. Горното равенство на полиноми на една променлива t е равносилно на равенствата (3.22) на съответните коефициенти. □

Глава 4

Редуциран полином на Дуурсма

Нека $C \subset \mathbb{F}_q^n$ е линеен код от род g с дуален $C^\perp \subset \mathbb{F}_q^n$ от род $g^\perp$, $P_C(t)$ е ζ-полиномът на C. В настоящата глава използваме,че

$$D_C(t) := \frac{P_C(t) - t^g}{(1-t)(1-qt)} \in \mathbb{Q}[t]$$

е полином $D_C(t) = \sum_{i=0}^{r-2} c_i t^i$ от степен $r - 2 = g + g^\perp - 2$. Теорема 11.1 от статията на Дуурсма [Duursma3] изразява пораждащата функция

$$\zeta_{C,j}(t) = D_{C,j}(t) + \frac{t^{g+j-1}}{(1-t)(1-qt)\dots(1-q^j t)}$$

на j-тото обобщено тегло на C чрез полином $D_{C,j}(t)$. За $j = 1$ полиномът $D_{C,j}(t)$ съвпада с въведения по-горе полином $D_C(t)$. Въпреки, че Дуурсма забелязва съществуването на $D_C(t)$, той не използва този полином за описание на тегловото разпределение на C. Ние наричаме $D_C(t)$ редуциран полином на Дуурсма. Основният резултат на настоящата глава и статията [KM1] е изразяването на разликата

$$\mathcal{W}_C(x,y) - \mathcal{M}_{n,n+1-k}(x,y) = (q-1)\sum_{i=0}^{r-2} c_i \binom{n}{d+i} (x-y)^{n-d-i} y^{d+i}$$

на тегловият полином $\mathcal{W}_C(x,y)$ на C и тегловия полином $\mathcal{M}_{n,n+1-k}(x,y)$ на MDS-код със същата дължина n и размерност k като C чрез коефициентите c_i на $D_C(T)$. По този начин, c_i определят еднозначно броя на думите, които трябва да се присъединят, съответно, отстранят от MDS-код със същата дължина и размерност като C, за да получим C (или код със същото теглово разпределение като C).

Дуурсма казва, че линеен код $C \subseteq \mathbb{F}_q^n$ удовлетворява аналога на хипотезата на Риман ако всички корени на неговия ζ-полином

$$P_C(t) = \sum_{i=0}^{r} a_i t^i \in \mathbb{Q}[t]$$

лежат върху окръжността

$$S\left(\frac{1}{\sqrt{q}}\right) = \left\{ z \in \mathbb{C} \,|\, |z| = \frac{1}{\sqrt{q}} \right\}.$$

Втория параграф на настоящата глава проверява, че произволен линеен код $C \subseteq \mathbb{F}_q^n$, изпълняващ аналога на хипотезата на Риман е формално-самодуален. Тя изразява хомогенния теглови полином $\mathcal{W}_C(x, y)$ на формално самодуален код C чрез чрез първите g коефициента $c_0, \ldots, c_{g-1} \in \mathbb{Q}$ на $D_C(t)$ или чрез броя $\mathcal{W}_C^{(d)}, \ldots, \mathcal{W}_C^{(k)}$ на кодовите думи на C с тегло между минималното разстояние d и размерността на кода k.

В своя труд [Додунеков, Ланджев] Додунеков и Ланджев определят почти MDS-кодовете като онези линейни кодове $C \subset \mathbb{F}_q^n$, за които родът на C е равен на рода на $C^\perp$ и е равен на 1. Статията [Kim, Hyun] на Kim и Hyun намира необходимо и достатъчно условие, при което почти MDS-код C изпълнява аналога на хипотезата на Риман. Съгласно Теорема 3 от [Duursma2], ζ-полиномът $P_C(t)$ на формално самодуален код C е от четна степен. Вторият параграф на глава 4 извежда необходимо и достатъчно условие, при което формално самодуален код $C \subset \mathbb{F}_q^n$ с ζ-полином $P_C(t)$ от степен 4 изпълнява аналога на хипотезата на Риман.

Последният, трети параграф е посветен на редуцирания полином на Дуурсма $D_F(t)$ на функционалното поле $F = \mathbb{F}_q(X)$ на крива $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$ от род g над $\mathbb{F}_q$. В Следствие 5.2 от [Duursma1] Дуурсма установява съществуването на $D_F(t)$. Обяснявайки формула (10.1) от [Duursma3] той споменава, че $D_F(t)$ отразява приносът на специалните дивизори на F към ζ-функцията $\zeta_F(t)$. Настоящата глава доказва, че $D_F(t) \in \mathbb{Z}[t]$ се определя напълно от първите си g коефициента, които са равни на броя $\mathcal{A}_i$ на ефективните дивизори на F от степен $0 \leq i \leq g-1$. Твърдение 106 установява, че ζ-функцията

$$\frac{D_F(t)}{(1-t)(1-qt)} = \sum_{i=0}^{\infty} \mathcal{B}_i t^i,$$

отговаряща на $D_F(t)$ има свойствата на пораждаща функция за броя $\mathcal{B}_i$ на ефективните дивизори от степен $i \geq 0$ на виртуално функционално поле от род $g-1$ над $\mathbb{F}_q$.

4.1 Теглови полином на произволен код

Нека $C \subset \mathbb{F}_q^n$ е линеен код с размерност $k = \dim_{\mathbb{F}_q} C$, минимално разстояние d и род $g = n + 1 - k - d \geq 1$, чийто дуален $C^\perp \subset \mathbb{F}_q^n$ има минимално разстояние $d^\perp$ и род $g^\perp = k+1-d^\perp \geq 1$. Съгласно Твърдение 100, ζ-полиномите на C и $C^\perp$ удовлетворяват функционалното уравнение

$$P_{C^\perp}(t) = P_C\left(\frac{1}{qt}\right) q^g t^{g+g^\perp} \tag{4.1}$$

и $P_C(1) = P_{C^\perp}(1) = 1$. Следователно

$$P_C\left(\frac{1}{q}\right) = P_{C^\perp}(1)q^{-g} = \left(\frac{1}{q}\right)^g$$

и полиномът $P_C(t) - t^g \in \mathbb{Q}[t]$ се анулира в $t = 1$ и $t = \frac{1}{q}$. В резултат, съществува полином

$$D_C(t) = \frac{P_C(t) - t^g}{(1-t)(1-tq)} = \sum_{i=0}^{r-2} c_i t^i \in \mathbb{Q}[t], \tag{4.2}$$

който ще наричаме редуциран полином на Дуурсма на C. Ако $g = 0$, кодът C е MDS-код и $\mathcal{W}_C(x,y) = \mathcal{M}_{n,n+1-k}(x,y)$. Следващото твърдение представя $\mathcal{W}_C(x,y)$ чрез $\mathcal{M}_{n,n+1-k}(x,y)$ и редуцирания полином на Дуурсма на C.

Твърдение 101. *Нека $C \subset \mathbb{F}_q^n$ е линеен код с размерност $k = dim_{\mathbb{F}_q} C$, минимално разстояние d и род $g = n + 1 - k - d \geq 1$, чийто дуален $C^\perp \subset \mathbb{F}_q^n$ има минимално разстояние $d^\perp$ и род $g^\perp = k + 1 - d^\perp \geq 1$. Ако*

$$D_C(t) = \sum_{i=0}^{g+g^\perp+2} c_i t^i \in \mathbb{Q}[t]$$

е редуцираният полином на Дуурсма на кода C, а $\mathcal{M}_{n,n+1-k}(x,y)$ е MDS*-теглови полином с дължина n, размерност k и минимално разстояние $n+1-k$, то хомогенният теглови полином на C е*

$$\mathcal{W}_C(x,y) = \mathcal{M}_{n,n+1-k}(x,y) + (q-1)\sum_{i=0}^{g+g^\perp-2} c_i \binom{n}{d+i}(x-y)^{n-d-i}y^{d+i}. \tag{4.3}$$

По-точно, редуцираният полином на Дуурсма $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i$ определя еднозначно тегловото разпределение на C по формулите

$$\mathcal{W}_C^{(w)} = (q-1)\binom{n}{w}\sum_{i=0}^{\min(w-d,n-d-d^\perp)} (-1)^{w-d-i}\binom{w}{d+i}c_i, \forall d \leq w \leq d+g-1, \tag{4.4}$$

$$\begin{aligned}\mathcal{W}_C^{(w)} &= (q-1)\binom{n}{w}\sum_{i=0}^{\min(w-d,n-d-d^\perp)} (-1)^{w-d-i}\binom{w}{d+i}c_i + \\ &+\binom{n}{w}\sum_{j=0}^{w-n-1+k}(-1)^j\binom{w}{j}(q^{w-n+k-j}-1), \quad \forall d+g \leq w \leq n.\end{aligned} \tag{4.5}$$

Обратно, за всички цели $0 \leq i \leq g + g^\perp - 2$ числата $\mathcal{W}_C^{(d)}, \mathcal{W}_C^{(d+1)}, \ldots, \mathcal{W}_C^{(d+i)}$ определят еднозначно коефициентите c_i на редуцирания полином на Дуурсма $D_C(t) =$

$\sum_{i=0}^{g+g^\perp-2} c_i t^i$, *чрез равенствата*

$$c_i = (q-1)^{-1}\binom{n}{d+i}^{-1}\sum_{w=d}^{d+i}\binom{n-w}{n-d-i}\mathcal{W}_C^{(w)} \quad \textit{за} \quad 0 \le i \le g-1 \quad \textit{и} \tag{4.6}$$

$$\begin{aligned} c_i = (q-1)^{-1}\binom{n}{d+i}^{-1}\Bigg\{ & \sum_{w=d}^{d+g-1}\binom{n-w}{n-d-i}\mathcal{W}_C^{(w)} + \\ & + \sum_{w=d+g}^{d+i}\binom{n-w}{n-d-i}\left[\mathcal{W}_C^{(w)} - \binom{n}{w}\sum_{j=0}^{w-n-1+k}(-1)^j\binom{w}{j}(q^{w-n+k-j}-1)\right]\Bigg\} \end{aligned} \tag{4.7}$$

за $g \le i \le g+g^\perp-2$.

В частност, числата

$$(q-1)\binom{n}{d+i}c_i$$

са цели за всяко $0 \le i \le g+g^\perp-2$.

Гореспоменатите формули показват, че $\mathcal{W}_C^{(d)}, \mathcal{W}_C^{(d+1)}, \ldots, \mathcal{W}_C^{(d+g+g^\perp-2)}$ *определят еднозначно хомогенния теглови полином* $\mathcal{W}_C(x,y)$ *на кода* C, *съгласно равенството*

$$\mathcal{W}_C(x,y) = \sum_{w=d}^{d+g+g^\perp-2}\mathcal{W}_C^{(w)}\lambda_w(x,y) + \Lambda(x,y), \tag{4.8}$$

където

$$\lambda_w(x,y) \coloneqq \sum_{s=w}^{d+g+g^\perp-2}\binom{n-w}{n-s}(x-y)^{n-s}y^s \quad \textit{за} \quad d \le w \le d+g+g^\perp-2 \tag{4.9}$$

и

$$\Lambda(x,y) \coloneqq \mathcal{M}_{n,n+1-k}(x,y) - \sum_{w=d+g}^{d+g+g^\perp-2}\mathcal{M}_{n,n+1-k}^{(w)}\lambda_w(x,y). \tag{4.10}$$

Доказателство: Полагаме $r \coloneqq g+g^\perp$ и прилагайки (3.2), изразяваме $\mathcal{W}_C(x,y)$ чрез коефициентите на $P_C(t)-t^g = \sum_{i=0}^{r} b_i t^i$,

$$\mathcal{W}_C(x,y) = \mathcal{M}_{n,d+g}(x,y) + \sum_{i=0}^{r} b_i \mathcal{M}_{n,d+i}(x,y).$$

Сравнявайки коефициентите в двете страни на

$$P_C(t) - t^g = (1-t)(1-qt)D_C(t), \tag{4.11}$$

получаваме

$$b_i = c_i - (q+1)c_{i-1} + qc_{i-2},$$

където $c_{-2} = c_{-1} = c_{r-1} = c_r = 0$. Следователно

$$\mathcal{W}_C(x,y) = \mathcal{M}_{n,d+g}(x,y) + \sum_{i=0}^{r} c_i \mathcal{M}_{n,d+i}(x,y) -$$
$$-(q+1)\sum_{i=0}^{r} c_{i-1}\mathcal{M}_{n,d+i}(x,y) + q\sum_{i=0}^{r} c_{i-2}\mathcal{M}_{n,d+i}(x,y).$$

Полагайки $j = i-1$, съответно $j = i-2$ в последните две суми, получаваме

$$\mathcal{W}_C(x,y) = \mathcal{M}_{n,d+g}(x,y) + \sum_{i=0}^{r} c_i \mathcal{M}_{n,d+i}(x,y) -$$
$$-(q+1)\sum_{j=-1}^{r-1} c_j \mathcal{M}_{n,d+j+1}(x,y) + q\sum_{j=-2}^{r-2} c_j \mathcal{M}_{n,d+j+2}(x,y),$$

откъдето

$$\mathcal{W}_C(x,y) = \mathcal{M}_{n,d+g}(x,y) +$$
$$+\sum_{j=0}^{r-2} c_j \left[\mathcal{M}_{n,d+j}(x,y) - (q+1)\mathcal{M}_{n,d+j+1}(x,y) + q\mathcal{M}_{n,d+j+2}(x,y)\right]. \tag{4.12}$$

Да означим

$$\mathcal{W}_{n,d+j}(x,y) \coloneqq \mathcal{M}_{n,d+j}(x,y) - (q+1)\mathcal{M}_{n,d+j+1}(x,y) + q\mathcal{M}_{n,d+j+2}(x,y)$$

и да напомним, че тегловият полином на MDS–код с дължина n и минимално разстояние $d+j$ е

$$\mathcal{M}_{n,d+j}(x,y) = x^n + \sum_{w=d+j}^{n} \mathcal{M}_{n,d+j}^{(w)} x^{n-w} y^w,$$

където

$$\mathcal{M}_{n,d+j}^{(w)} = \binom{n}{w} \sum_{i=0}^{w-d-j} (-1)^i \binom{w}{i} (q^{w+1-d-j-i} - 1) \tag{4.13}$$

Следователно

$$\mathcal{W}_{n,d+j}(x,y) = \mathcal{M}_{n,d+j}^{(d+j)} x^{n-d-j} y^{d+j} + \left[\mathcal{M}_{n,d+j}^{(d+j+1)} - (q+1)\mathcal{M}_{n,d+j+1}^{(d+j+1)}\right] x^{n-d-j-1} y^{d+j+1} +$$
$$+ \sum_{w=d+j+2}^{n} \left[\mathcal{M}_{n,d+j}^{(w)} - (q+1)\mathcal{M}_{n,d+j+1}^{(w)} + q\mathcal{M}_{n,d+j+2}^{(w)}\right] x^{n-w} y^w.$$

Използвайки тегловото разпределение на MDS-код (4.13) и полагайки

$$\mathcal{W}^{(w)}_{n,d+j} \coloneqq \mathcal{M}^{(w)}_{n,d+j} - (q+1)\mathcal{M}^{(w)}_{n,d+j+1} + q\mathcal{M}^{(w)}_{n,d+j+2} \text{ за } d+j+2 \leq w \leq n,$$

изразяваме

$$\mathcal{W}_{n,d+j}(x,y) = \binom{n}{d+j}(q-1)x^{n-d-j}y^{d+j} -$$

$$-\binom{n}{d+j+1}(q-1)(d+j+1)x^{n-d-j-1}y^{d+j+1} + \sum_{w=d+j+2}^{n} \mathcal{W}^{(w)}_{n,d+j}x^{n-w}y^{w}.$$

За всяко $d+j+2 \leq w \leq n$ имаме

$$\mathcal{W}^{(w)}_{n,d+j} = \binom{n}{w}\binom{w}{d+j}(q-1)(-1)^{w-d-j}.$$

Вземайки предвид

$$\binom{n}{w}\binom{w}{d+j} = \binom{n-d-j}{w-d-j}\binom{n}{d+j},$$

получаваме

$$\mathcal{W}_{n,d+j}(x,y) =$$

$$= \binom{n}{d+j}(q-1)x^{n-d-j}y^{d+j} - \binom{n}{d+j+1}(q-1)(d+j+1)x^{n-d-j-1}y^{d+j+1} +$$

$$+ \sum_{w=d+j+2}^{n} \binom{n}{d+j}\binom{n-d-j}{w-d-j}(q-1)(-1)^{w-d-j}x^{n-w}y^{w}.$$

Прилагайки

$$(d+j+1)\binom{n}{d+j+1} = (n-d-j)\binom{n}{d+j},$$

извеждаме

$$\mathcal{W}_{n,d+j}(x,y) = \binom{n}{d+j}(q-1)\Bigg[x^{n-d-j}y^{d+j} - (n-d-j)x^{n-d-j-1}y^{d+j+1} +$$

$$+ \sum_{w=d+j+2}^{n} (-1)^{w-d-j}\binom{n-d-j}{w-d-j}x^{n-w}y^{w}\Bigg].$$

Означавайки $s \coloneqq w-d-j$, изразяваме

$$\sum_{w=d+j+2}^{n} (-1)^{w-d-j}\binom{n-d-j}{w-d-j}x^{n-w}y^{w} = \sum_{s=2}^{n-d-j} (-1)^{s}\binom{n-d-j}{s}x^{n-d-j-s}y^{d+j+s}$$

и получаваме

$$\mathcal{W}_{n,d+j}(x,y) = \binom{n}{d+j}(q-1)(x-y)^{n-d-j}y^{d+j}. \tag{4.14}$$

Да отбележим, че тъждеството $\mathcal{W}_{n,n-k}(x,y) = \binom{n}{k}(q-1)(x-y)^k y^{n-k}$ е точно равенство (c) от Лема 1 на [Kim, Hyun]. Замествайки (4.14) в (4.12) и вземайки предвид, че $d+g = n+1-k$, получаваме равенство (4.3). За да изведем равенства (4.4) и (4.5), да означим

$$\mathcal{V}_C(x,y) \coloneqq \mathcal{W}_C(x,y) - \mathcal{M}_{n,n-k+1}(x,y)$$

и да забележим, че $\mathcal{V}_C(x,y) = \sum\limits_{w=d}^{n} \mathcal{V}_C^{(w)} x^{n-w} y^w$, където $\mathcal{V}_C^{(w)} = \mathcal{W}_C^{(w)}$ за всички $w, d \leq w \leq n-k$ и

$$\mathcal{V}_C^{(w)} = \mathcal{W}_C^{(w)} - \mathcal{M}_{n,n-k+1}^{(w)} = \mathcal{W}_C^{(w)} - \binom{n}{w} \sum_{i=0}^{w-n-1+k} (-1)^i \binom{w}{i} (q^{w-n+k-i} - 1)$$

за $d+g = n+1-k \leq w \leq n$. Използвайки (4.3) можем да изразим

$$\mathcal{V}_C(x,y) = (q-1) \sum_{i=0}^{g+g^\perp-2} c_i \binom{n}{d+i} \sum_{s=0}^{n-d-i} \binom{n-d-i}{s} (-1)^{n-d-i-s} x^s y^{n-s} =$$

$$= (q-1) \sum_{s=0}^{n-d} \left[\sum_{i=0}^{\min(n-d-s, g+g^\perp-2)} c_i \binom{n}{d+i} \binom{n-d-i}{s} (-1)^{n-d-i-s} \right] x^s y^{n-s},$$

променяйки реда на сумиране. Полагайки $w \coloneqq n-s$, получаваме

$$\mathcal{V}_C(x,y) = (q-1) \sum_{w=d}^{n} \left[\sum_{i=0}^{\min(w-d, n-d-d^\perp)} c_i \binom{n}{d+i} \binom{n-d-i}{n-w} (-1)^{w-d-i} \right] x^{n-w} y^w.$$

Сега равенството

$$\binom{n}{d+i} \binom{n-d-i}{n-w} = \binom{n}{w} \binom{w}{d+i}$$

ни позволява да изразим

$$\mathcal{V}_C^{(w)} = (q-1) \binom{n}{w} \sum_{i=0}^{\min(w-d, n-d-d^\perp)} c_i \binom{w}{d+i} (-1)^{w-d-i}, \forall d \leq w \leq n,$$

което доказва развенствата (4.4) и (4.5). Отправяйки се към равенства (4.6) и (4.7), полагаме $z \coloneqq x-y$ и изразяваме равенство (4.3) във вида

$$\mathcal{V}_C(y+z,y) = (q-1) \sum_{i=0}^{g+g^\perp-2} c_i \binom{n}{d+i} z^{n-d-i} y^{d+i} \tag{4.15}$$

От друга страна,

$$\mathcal{V}_C(y+z,y) = \sum_{w=d}^{n} \mathcal{V}_C^{(w)} (y+z)^{n-w} y^w =$$

$$= \sum_{w=d}^{n} \sum_{s=0}^{n-w} \binom{n-w}{s} \mathcal{V}_C^{(w)} y^{n-s} z^s = \sum_{s=0}^{n-d} \left[\sum_{w=d}^{n-s} \binom{n-w}{s} \mathcal{V}_C^{(w)} \right] y^{n-s} z^s,$$

след смяна на реда на сумиране. Сравнявайки коефициентите на $z^{n-d-i}y^{d+i}$ в двете равенства за $\mathcal{V}_C(y+z,y)$, получаваме

$$\sum_{w=d}^{d+i}\binom{n-w}{n-d-i}\mathcal{V}_C^{(w)}=(q-1)c_i\binom{n}{d+i},$$

откъдето

$$c_i=(q-1)^{-1}\binom{n}{d+i}^{-1}\sum_{w=d}^{d+i}\binom{n-w}{n-d-i}\mathcal{V}_C^{(w)}.$$

Комбинирайки това равенство с (4.13) получаваме (4.6) и (4.7). Тези формули, показват също, че числата $(q-1)\binom{n}{d+i}c_i$ са цели за всички $0\le i\le g+g^{\perp}-2$. Замествайки (4.6), (4.7) и (4.13) в (4.3), получаваме

$$\mathcal{W}_C(x,y)=\mathcal{M}_{n,n+1-k}(x,y)+\sum_{i=0}^{g+g^{\perp}-2}\sum_{w=d}^{d+i}\binom{n-w}{n-d-i}\mathcal{W}_C^{(w)}(x-y)^{n-d-i}y^{d+i}-$$
$$-\sum_{i=g}^{g+g^{\perp}-2}\sum_{w=d+g}^{d+i}\binom{n-w}{n-d-i}\mathcal{M}_{n,n+1-k}^{(w)}(x-y)^{n-d-i}y^{d+i}.$$

Чрез размяна на реда на сумиране в двойните суми изразяваме

$$\mathcal{W}_C(x,y)=\mathcal{M}_{n,n+1-k}(x,y)+\sum_{w=d}^{d+g+g^{\perp}-2}\mathcal{W}_C^{(w)}\sum_{i=w-d}^{g+g^{\perp}-2}\binom{n-w}{n-d-i}(x-y)^{n-d-i}y^{d+i}-$$
$$-\sum_{w=d+g}^{d+g+g^{\perp}-2}\mathcal{M}_{n,n+1-k}^{(w)}\sum_{i=w-d}^{g+g^{\perp}-2}\binom{n-w}{n-d-i}(x-y)^{n-d-i}y^{d+i}.$$

Полагайки $s\coloneqq d+i$, получаваме (4.8) с (4.9) и (4.10). □

Сравнявайки коефициентите на $x^{n-d}y^d$ в двете страни на равенство (4.3), получаваме

$$\mathcal{W}_C^{(d)}=(q-1)\binom{n}{d}c_0$$

за линеен код C с минимално разстояние d. Твърдим, че ако C е от род $g\ge 1$, то $c_0<1$. За тази цел, да забележим, че за произволна d-орка $\{i_1,i_2,\dots,i_d\}\in\binom{[n]}{d}$, съставена от индексите на ненулевите компоненти на кодова дума $c\in C$ с тегло d съществуват точно $q-1$ думи $c'\in C$, такива че носителят $Supp(c)=Supp(c')=\{i_1,i_2,\dots,i_d\}$. Това е така, понеже стълбовете $H_{i_1},H_{i_2},\dots,H_{i_d}$ на произволна проверочна матрица H на кода C имат ранг $d-1$ и в пространството от решенията на хомогенната система линейни уравнения с матрица $(H_{i_1},H_{i_2},\dots,H_{i_d})$ няма дума с тегло по-малко от d. Ако v е броят на носителите на думи от C с тегло d, то $\mathcal{W}_C^{(d)}=v(q-1)$, откъдето

$$c_0=\frac{\mathcal{W}_C^{(d)}}{(q-1)\binom{n}{d}}=\frac{v}{\binom{n}{d}}\le 1.$$

Ако допуснем, че $c_0 = 1$, то всеки d на брой стълба на H са линейно зависими. Вземайки предвид, че рангът на матрицата H е $n-k$, заключаваме, че $d > n-k$. Комбинирайки това неравенство с границата на Сингълтън $d \leq n+1-k$, получаваме $d = n+1-k$. Това противоречи на допускането, че C не е MDS-код и доказва, че $c_0 < 1$ за всеки $\mathbb{F}_q$-линеен код C от род $g \geq 1$. Да отбележим, че по този начин числото c_0 може да бъде разглеждано като вероятността дадена d-орка да бъде носител на дума от C с тегло d.

4.2 Аналог на хипотезата на Риман и формална самодуалност на линеен код

Да припомним, че линеен код C с дуален $C^\perp$ е формално самодуален, ако броят на думите с тегло w на C съвпада с броя на думите с тегло w на $C^\perp$, за всяко цяло число $0 \leq w \leq n$, т.е.

$$\mathcal{W}_C^{(w)} = \mathcal{W}_{C^\perp}^{(w)}, \quad \forall 0 \leq w \leq n$$

Да споменем някои тривиални свойства на формално самодуалните кодове. Преди всичко, кодът C и неговият дуален код $C^\perp$ имат едно и също минимално разстояние $d = d(C) = d(C^\perp) = d^\perp$. Освен това, тези два кода имат равен брой елементи, понеже

$$q^{\dim C} = \sum_{w=0}^{n} \mathcal{W}_C^{(w)} = \sum_{w=0}^{n} \mathcal{W}_{C^\perp}^{(w)} = q^{\dim C^\perp}.$$

Оттук, размерностите $k := \dim C$ и $k^\perp := \dim C^\perp$ съвпадат. В резултат получаваме, че дължината $n = k + k^\perp = 2k$ е четно число. Родовете

$$g = n + 1 - k - d = n + 1 - k^\perp - d^\perp = g^\perp$$

също съвпадат. Ако

$$P_C(t) = \sum_{i=0}^{2g} a_i t^i, \quad P_{C^\perp} = \sum_{i=0}^{2g} a_i^\perp t^i$$

са ζ-полиномите на C, $C^\perp$, то сравняването на коефициентите пред $x^{n-d}y^d$, $x^{n-d-1}y^{d+1}$, ..., $x^{n-d-2g}y^{d+2g}$ в хомогенния теглови полином

$$\sum_{i=0}^{2g} a_i \mathcal{M}_{2k,d+i}(x,y) = \mathcal{W}_C(x,y) = \mathcal{W}_{C^\perp}(x,y) = \sum_{i=0}^{2g} a_i^\perp \mathcal{M}_{2k,d+i}(x,y).$$

дава $a_i = a_i^\perp$ за $\forall 0 \leq i \leq 2g$. От друга страна условието $a_i = a_i^\perp, \forall 0 \leq i \leq 2g$ е достатъчно, за да твърдим, че $\mathcal{W}_C(x,y) \equiv \mathcal{W}_{C^\perp}(x,y)$. По този начин, формалната самодуалност на кода C е равносилна на съвпадението

$$P_C(t) = P_{C^\perp}(t)$$

на ζ-полиномите на C и $C^{\perp}$. Твърдение 100 доказва, че тъждествата на МакУилямс за тегловото разпределение $\{\mathcal{W}_C^{(w)}\}_{w=1}^n$ на C, съответно $\{\mathcal{W}_{C^{\perp}}^{(w)}\}_{w=1}^n$ на $C^{\perp}$ са еквивалентни на функционалното уравнение (4.1). Затова $\mathbb{F}_q$-линеен код C е формално самодуален тогава и само тогава, когато неговият ζ-полином удовлетворява функционалното уравнение

$$P_C(t) = P_C\left(\frac{1}{qt}\right) q^g t^{2g} \tag{4.16}$$

на полинома на Хасе-Вайл на функционалното поле на крива от род g над $\mathbb{F}_q$,

Твърдение 102. *Ако линеен код $C \subset \mathbb{F}_q^n$ удовлетворява аналога на хипотезата на Риман, то той е формално-самодуален.*

Доказателство: Нека кодът C удовлетворява аналога на хипотезата на Риман, т.е. неговият ζ-полином $P_C(t)$ от степен $r = g + g^{\perp}$ има вида

$$P_C(t) = a_r \prod_{j=1}^{r} (t - \alpha_j) \in \mathbb{Q}[t]$$

за някакви числа $\alpha_j \in \mathbb{C}$ с модул $|\alpha_j| = \frac{1}{\sqrt{q}}$ за всички $1 \leq j \leq r$. Твърдим, че когато ζ-полиномът $P_C(t)$ е от четна степен $r = 2m$, то той има вида

$$P_C(t) = a_{2m} \prod_{i=1}^{m} (t - \alpha_i)(t - \overline{\alpha_i}), \tag{4.17}$$

или

$$P_C(t) = a_{2m} \left(t^2 - \frac{1}{q}\right) \prod_{i=1}^{m-1} (t - \alpha_i)(t - \overline{\alpha_i}), \tag{4.18}$$

докато при нечетена степен $r = 2m + 1$ е в сила

$$P_C(t) = a_{2m+1} \left(t - \frac{\varepsilon}{\sqrt{q}}\right) \prod_{i=1}^{m} (t - \alpha_i)(t - \overline{\alpha_i}) \quad \text{с} \quad \varepsilon \in \{\pm 1\}. \tag{4.19}$$

Наистина, ако $\alpha_i \in \mathbb{C}\backslash\mathbb{R}$ е комплексен нереален корен на $P_C(t)$, то неговият комплексно спрегнат $\overline{\alpha_i} \neq \alpha_i$ също е корен на $P_C(t) \in \mathbb{Q}[t]$, така че $P_C(t)$ се дели на $(t-\alpha_i)(t-\overline{\alpha_i})$. Ако полиномът $P_C(t)$ има поне три реални корена $\alpha_1, \alpha_2, \alpha_3 \in \left\{-\frac{1}{\sqrt{q}}, \frac{1}{\sqrt{q}}\right\}$, то поне два от тях съвпадат. Ако $\alpha_1 = \alpha_2 \in \mathbb{R}$, то $(t - \alpha_1)(t - \alpha_2) = (t - \alpha_1)(t - \overline{\alpha_1})$. Така $P_C(t)$ има най-много два реални корена, които не са комплексно спрегнати и следователно изглежда по един от описаните начини (4.17), (4.18) или (4.19). Ако ζ-полиномът $P_C(t)$ има вида (4.17), той може да бъде записан като

$$P_C(t) = a_{2m} \prod_{i=1}^{m} \left(t^2 - 2Re(\alpha_i)t + \frac{1}{q}\right)$$

и равенство (4.1) придобива вида

$$P_{C^\perp}(t) = a_{2m}\left[\prod_{i=1}^{m}\left(\frac{1}{q} - 2Re(\alpha_i)t + t^2\right)\right] q^{g-m} = P_C(t)q^{g-m}. \tag{4.20}$$

Ако $D_C(t)$ и $D_{C^\perp}(t)$ са редуцираните полиноми на Дуурсма на C, съответно, $C^\perp$, то

$$(1-t)(1-qt)D_{C^\perp}(t) + t^{g^\perp} = P_{C^\perp}(t) = P_C(t)q^{g-m} = (1-t)(1-qt)q^{g-m}D_C(t) + q^{g-m}t^g.$$

Следователно

$$(1-t)(1-qt)\left[D_{C^\perp}(t) - q^{g-m}D_C(t)\right] = q^{g-m}t^g - t^{g^\perp}.$$

Полагането $t = 1$ дава $q^{g-m} = 1$, откъдето $g = m$. Вземайки предвид $g + g^\perp = 2m$, получаваме $g = g^\perp$. Тогава от равенство (4.20) следва $P_C(t) = P_{C^\perp}(t)$, което е еквивалентно на формалната самодуалност на кода C.

Ако $P_C(t)$ има вида (4.18), равенство (4.1) се свежда до

$$P_{C^\perp}(t) = a_{2m}\left(\frac{1}{q} - t^2\right)\left[\prod_{i=1}^{m-1}\left(\frac{1}{q} - 2Re(\alpha_i)t + t^2\right)\right] q^{g-m} = -P_C(t)q^{g-m}. \tag{4.21}$$

Изразено чрез $D_C(t)$ и $D_{C^\perp}(t)$, това равенство придобива вида

$$\begin{aligned}(1-t)(1-qt)D_{C^\perp}(t) + t^{g^\perp} = P_{C^\perp}(t) = \\ = -P_C(t)q^{g-m} = -(1-t)(1-qt)q^{g-m}D_C(t) - q^{g-m}t^g,\end{aligned}$$

откъдето

$$(1-t)(1-qt)\left[D_{C^\perp}(t) + q^{g-m}D_C(t)\right] = -t^{g^\perp} - q^{g-m}t^g.$$

Заместваики $t = 1$ получаваме $-1 - q^{g-m} = 0$, което е противоречие, показващо, че ζ-полином, удовлетворяващ аналога на хипотезата на Риман не може да има вида (4.18).

Ако ζ-полиномът $P_C(t)$ има нечетна степен $2m+1$, то равенства (4.19) и (4.1) дават

$$\begin{aligned}P_{C^\perp}(t) = -\varepsilon\sqrt{q}a_{2m+1}\left(t - \frac{\varepsilon}{\sqrt{q}}\right)\left[\prod_{i=1}^{m}\left(\frac{1}{q} - 2Re(\alpha_i)t + t^2\right)\right] q^{g-m-1} = \\ = -\varepsilon\sqrt{q}P_C(t)q^{g-m-1}\end{aligned}$$

след умножаване на $\frac{1}{qt} - \frac{\varepsilon}{\sqrt{q}}$ с $-\frac{\varepsilon}{\sqrt{q}}qt$ и всяко $\frac{1}{q^2t^2} - \frac{2Re(\alpha_i)}{qt} + \frac{1}{q}$ с qt^2. Изразявайки това равенство чрез редуцираните полиноми на Дуурсма получаваме

$$\begin{aligned}(1-t)(1-qt)D_{C^\perp}(t) + t^{g^\perp} = P_{C^\perp}(t) = -\varepsilon q^{g-m-\frac{1}{2}}P_C(t) = \\ = -\varepsilon q^{g-m-\frac{1}{2}}(1-t)(1-qt)D_C(t) - \varepsilon q^{g-m-\frac{1}{2}}t^g,\end{aligned}$$

откъдето

$$(1-t)(1-qt)\left[D_{C^\perp}(t) + \varepsilon q^{g-m-\frac{1}{2}}D_C(t)\right] = -t^{g^\perp} - \varepsilon q^{g-m-\frac{1}{2}}t^g.$$

Замествайки с $t = 1$, достигаме до $-1 - \varepsilon q^{g-m-\frac{1}{2}} = 0$, което е невъзможно, понеже $g - m - \frac{1}{2} \neq 0$ за всеки две цели числа g и m. Така ζ-полином от нечетна степен не може да удовлетворява аналога на хипотезата на Риман. □

Твърдение 103. *Следните условия са еквивалентни за линеен код $C \subset \mathbb{F}_q^n$:*

(i) кодът C е формално самодуален, т.е. ζ-полиномът $P_C(t)$ на C удовлетворява функционалното уравнение

$$P_C(t) = P_C\left(\frac{1}{qt}\right) q^g t^{2g};$$

(ii) редуцираният полином на Дуурсма $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i$ удовлетворява функционалното уравнение

$$D_C(t) = D_C\left(\frac{1}{qt}\right) q^{g-1} t^{2g-2}; \tag{4.22}$$

(iii) коефициентите на редуцирания полином на Дуурсма $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i$ на кода C удовлетворяват равенствата

$$c_{g-1+i} = q^i c_{g-1-i} \quad за \quad \forall 1 \leq i \leq g-1; \tag{4.23}$$

(iv) дуалният код $C^\perp \subset \mathbb{F}_q^n$ на C има размерност k, род g и хомогенният теглови полином на кода C има вида

$$\mathcal{W}_C(x,y) = \mathcal{M}_{2k,k+1}(x,y) + \sum_{j=0}^{g-1} c_{g-1-j} w_j(x,y), \tag{4.24}$$

където

$$w_j(x,y) \coloneqq (q-1)\binom{2k}{k+j}\left[(x-y)^{k+j}y^{k-j} + q^j(x-y)^{k-j}y^{k+j}\right] \tag{4.25}$$

за $1 \leq j \leq g-1$ и

$$w_0(x,y) \coloneqq (q-1)\binom{2k}{k}(x-y)^k y^k. \tag{4.26}$$

(v) дуалният код $C^\perp \subset \mathbb{F}_q$ на C има размерност k, род g и хомогенният теглови полином на кода C има вида

$$\mathcal{W}_C(x,y) = \mathcal{M}_{2k,k+1}(x,y) + \sum_{w=d}^{k-1} \mathcal{W}_C^{(w)} \varphi_w(x,y) + \mathcal{W}_C^{(k)}(x-y)^k y^k, \tag{4.27}$$

където

$$\varphi_w(x,y) \coloneqq \sum_{s=w}^{k-1} \binom{2k-w}{s-w} \left[(x-y)^{2k-s}y^s + q^{k-s}(x-y)^s y^{2k-s}\right] + \\ + \binom{2k-w}{k}(x-y)^k y^k, \quad \forall d \le w \le k-1. \tag{4.28}$$

По този начин кодът C може да бъде получен от MDS-код, имащ същата дължина $2k$ и размерност k, чрез добавяне и премахване на подходящи думи, зависещи само от броя $\mathcal{W}_C^{(d)}, \mathcal{W}_C^{(d+1)}, \ldots, \mathcal{W}_C^{(k)}$ на кодовите думи на C с тегло не по-голямо от размерността на кода C.

Доказателство: Първо ще се заемем с посоката $(i) \Rightarrow (ii)$. За тази цел, да заместим $P_C(t) = (1-t)(1-qt)D_C(t) + t^g$ в равенство (4.16). Така получаваме

$$(1-t)(1-qt)D_C(t) + t^g = (qt-1)(t-1)\left[D_C\left(\frac{1}{qt}\right)q^{g-1}t^{2g-2}\right] + t^g,$$

откъдето непосредствено следва (4.22).

Обратно, $(ii) \Rightarrow (i)$ извеждаме по следния начин:

$$\begin{aligned} P_C(t) &= (1-t)(1-qt)D_C(t) + t^g = \\ &= (1-t)(1-qt)\left[D_C\left(\frac{1}{qt}\right)q^{g-1}t^{2g-2}\right] + t^g = \\ &= \left[\left(1-\frac{1}{t}\right)t\right]\left[\left(1-\frac{1}{qt}\right)qt\right]\left[D_C\left(\frac{1}{qt}\right)q^{g-1}t^{2g-2}\right] + \frac{q^g t^{2g}}{q^g t^g} = \\ &= \left[\left(1-\frac{q}{qt}\right)\left(1-\frac{1}{qt}\right)D_C\left(\frac{1}{qt}\right) + \frac{1}{(qt)^g}\right]q^g t^{2g} = P_C\left(\frac{1}{qt}\right)q^g t^{2g}. \end{aligned}$$

Това доказва еквиваленстността на (i) и (ii).

За да докажем $(ii) \Leftrightarrow (iii)$ да забележим, че функционалното уравнение на $D_C(t)$ може да бъде разглеждано по следния начин

$$\begin{aligned} \sum_{i=0}^{2g-2} c_i t^i = D_C(t) = D_C\left(\frac{1}{qt}\right)g^{g-1}t^{2g-2} &= \left(\sum_{i=0}^{2g-2}\frac{c_i}{q^i t^i}\right)q^{g-1}t^{2g-2} = \\ &= \sum_{i=0}^{2g-2} c_i q^{g-i-1}t^{2g-2-i} = \sum_{j=0}^{2g-2} c_{2g-2-j}q^{-g+1+j}t^j. \end{aligned}$$

Сравнявайки коефициентите, можем да изразим формалната самодуалност на кода C, чрез зависимостите

$$c_j = q^{-g+j+1}c_{2g-2-j} \quad \text{за} \quad 0 \le j \le 2g-2.$$

За да опростим това равенство, полагаме $i \coloneqq j+1-g$ и изразяваме

$$c_{g-1+i} = q^i c_{g-1-i} \quad \text{за} \quad -g+1 \le i \le g-1. \tag{4.29}$$

Да забележим, че за всички $-g+1 \leq i \leq -1$, равенството $c_{g-1+i} = q^i c_{g-1-i}$ е еквивалентно на $c_{g-1-i} = q^{-i} c_{g-1+i}$, което е в сила за $1 \leq i \leq g-1$. При $i = 0$, горното равенство е тривиално. По този начин установяваме еквивалентността на твърденията (ii) и (iii).

За да докажем $(iii) \Rightarrow (iv)$ въвеждаме нова променлива $z \coloneqq x - y$ и изразяваме (4.3) По следния начин

$$\mathcal{V}_C(y+z,y) = \mathcal{W}_C(y+z,y) - \mathcal{M}_{2k,k+1}(y+z,y) = (q-1)\sum_{i=0}^{2g-2} c_i \binom{2k}{d+i} y^{d+i} z^{2k-d-i} =$$
$$= (q-1)\sum_{i=0}^{g-1} c_i \binom{2k}{d+i} y^{d+i} z^{2k-d-i} + (d-1)\sum_{i=g}^{2g-2} c_i \binom{2k}{d+i} y^{d+i} z^{2k-d-i}.$$

Заменяме индекса на сумиране в първата сума с $0 \leq j \coloneqq g-1-i \leq g-1$, полагаме $1 \leq j \coloneqq i-g+1 \leq g-1$ във втората сума и използваме $d+g = k+1$, за да получим

$$\mathcal{V}_C(y+z,y) =$$
$$= (q-1)\sum_{j=0}^{g-1} c_{g-1-j} \binom{2k}{k-j} y^{k-j} z^{k+j} + (q-1)\sum_{j=1}^{g-1} c_{j+g-1} \binom{2k}{k+j} y^{k+j} z^{k-j} \tag{4.30}$$

Отделяйки от първата сума монома, съответстващ на $j = 0$, изразяваме

$$\mathcal{V}_C(y+z,y) = (q-1)c_{g-1}\binom{2k}{k} y^k z^k +$$
$$+\sum_{j=1}^{g-1}(q-1)\binom{2k}{k+j}\left[c_{g-1-j} y^{k-j} z^{k+j} + c_{g-1+j} y^{k+j} z^{k-j}\right] \tag{4.31}$$

за произволен $\mathbb{F}_q$-линеен код $C \subset \mathbb{F}_q$. Ако C е формално-самодуален, то замествайки (4.23) в горното равенство, и ползвайки означенията от (iv), получаваме

$$\mathcal{V}_C(y+z,y) = \sum_{j=0}^{g-1} c_{g-1-j} w_j(y+z,y).$$

Замествайки $z \coloneqq x-y$ и $\mathcal{V}_C(x,y) \coloneqq \mathcal{W}_C(x,y) - \mathcal{M}_{2k,k+1}(x,y)$, достигаме до търсеното равенство.

За да покажем, че (iv) е достатъчно условие за формалната самодуалност на C, използваме, че равенствата от (iv) са еквивалентни на

$$\mathcal{V}_C(y+z,y) = \sum_{j=1}^{g-1} c_{g-1-j}(q-1)\binom{2k}{k+j} y^{k-j} z^{k+j} +$$
$$+c_{g-1}(q-1)\binom{2k}{k} y^k z^k + \sum_{j=1}^{g-1} c_{g-1-j}(q-1)\binom{2k}{k+j} q^j y^{k+j} z^{k-j} \tag{4.32}$$

за

$$\mathcal{V}_C(y+z,y) := \mathcal{W}_C(y+z,y) - \mathcal{M}_{2k,k+1}(y+z,y).$$

Сравнявайки коефициентите на $y^{k+j}z^{k-j}$ в (4.31) и (4.32) за $1 \leq j \leq q-1$, стигаме до извода, че

$$c_{g-1+j} = c_{g-1-j}q^j, \forall 1 \leq j \leq g-1.$$

Това са точно равенствата (4.23) от (iii), които са еквивалентни на формалната самодуалност на C.

За да докажем $(iv) \Leftrightarrow (v)$, достатъчно е да положим

$$\mathcal{E}(x,y) \coloneqq \sum_{j=0}^{g-1} c_{g-1-j}w_j(x,y)$$

и да изведем, че

$$\mathcal{E}(x,y) = \sum_{w=d}^{k-1} \mathcal{W}_C^{(w)}\varphi_w(x,y) + \mathcal{W}_C^{(k)}(x-y)^k y^k.$$

За целта, полагаме $i \coloneqq g-1-j$ и изразяваме

$$\mathcal{E}(x,y) = \sum_{i=0}^{g-2} c_i(q-1)\binom{2k}{d+i}\left[(x-y)^{2k-d-i}y^{d+i} + q^{g-1-i}(x-y)^{d+i}y^{2k-d-i}\right] + \\ + c_{g-1}(q-1)\binom{2k}{k}(x-y)^k y^k.$$

Заместваме с (4.6) и променяме реда на сумиране, за да получим

$$\mathcal{E}(x,y) = \sum_{w=d}^{k-1}\sum_{i=w-d}^{g-2}\binom{2k-w}{d+i-w}\mathcal{W}_C^{(w)}[(x-y)^{2k-d-i}y^{d+i} + q^{g-1-i}(x-y)^{d+i}y^{2k-d-i}] + \\ + \sum_{w=d}^{k}\binom{2k-w}{k}\mathcal{W}_C^{(w)}(x-y)^k y^k.$$

Въвеждаме $s \coloneqq d+i$ и изнасяме $\mathcal{W}_C^{(w)}$ като коефициент, за да представим

$$\mathcal{E}(x,y) = \sum_{w=d}^{k-1} \mathcal{W}_C^{(w)}\varphi_w(x,y) + \mathcal{W}_C^{(k)}(x-y)^k y^k.$$

□

Нека $C \subset \mathbb{F}_q^n$ е $\mathbb{F}_q$-линеен код от род g. В [Додунеков, Ланджев] Додунеков и Ланджев изучават кодовете с ζ-полином $P_C(t) \in \mathbb{Q}[t]$ от степен $g+g^\perp = 2$ и ги наричат почти MDS-кодове. Това са кодовете с постоянен редуциран полином на Дуурсма

$D_C(t) = c_0 \in \mathbb{Q}$. Ким и Хюн доказват в [Kim, Hyun], че почти MDS-код удовлетворява аналога на хипотезата на Риман тогава и само тогава, когато

$$\frac{1}{(\sqrt{q}+1)^2} \leq c_0 \leq \frac{1}{(\sqrt{q}-1)^2}.$$

Следващото твърдение характеризира формално-самодуалните кодове C от род 2, които удовлетворяват аналога на хипотезата на Риман. Съгласно предишното твърдение, формално самодуален код C е от род 2 точно когато редуцираният му полином на Дуурсма

$$D_C(t) = c_0 + c_1 t + q c_0 t^2,$$

е квадратен тричлен с рационални коефициенти $c_0, c_1 \in \mathbb{Q}, 0 < c_0 < 1$.

Твърдение 104. *Формално самодуален код $C \subset \mathbb{F}_q^{2k}$ с редуциран полином на Дуурсма $D_C(t) = c_0 + c_1 t + q c_0 t^2 \in \mathbb{Q}[t], 0 < c_0 < 1$ удовлетворява аналога на хипотезата на Риман тогава и само тогава, когато*

$$[(q+1)c_0 + c_1]^2 \geq 4c_0 \tag{4.33}$$

$$q - 4\sqrt{q} + 1 \leq \frac{c_1}{c_0} \leq q + 4\sqrt{q} + 1 \tag{4.34}$$

$$c_1 \leq \min\left(\frac{1}{(\sqrt{q}-1)^2} - 2\sqrt{q}c_0, \frac{1}{(\sqrt{q}+1)^2} + 2\sqrt{q}c_0\right) \tag{4.35}$$

Доказателство: Съгласно равенство (4.17) от доказателството на Твърдение 23, ζ-полиномът

$$P_C(t) = (1-t)(1-qt)(qc_0t^2 + c_1 t + c_0) + t^2$$

удовлетворява аналога на хипотезата на Риман, точно когато съществуват $\varphi, \psi \in [0, 2\pi)$ с

$$P_C(t) = q^2 c_0 \left(t - \frac{e^{i\varphi}}{\sqrt{q}}\right)\left(t - \frac{e^{-i\varphi}}{\sqrt{q}}\right)\left(t - \frac{e^{i\psi}}{\sqrt{q}}\right)\left(t - \frac{e^{-i\psi}}{\sqrt{q}}\right).$$

Сравнявайки коефициентите пред t и t^2, получаваме равенствата

$$c_1 - (q+1)c_0 = -2\sqrt{q}c_0[\cos(\varphi) + \cos(\psi)],$$

$$1 + 2qc_0 - (q+1)c_1 = 2qc_0[1 + 2\cos(\varphi)\cos(\psi)].$$

Те от своя страна са еквивалентни на

$$\cos(\varphi) + \cos(\psi) = \frac{(q+1)c_0 - c_1}{2\sqrt{q}c_0},$$

$$\cos(\varphi)\cos(\psi) = \frac{1 - (q+1)c_1}{4qc_0}.$$

С други думи, квадратното уравнение

$$f(t) := t^2 + \frac{c_1 - (q+1)c_0}{2\sqrt{q}c_0}t + \frac{1-(q+1)c_1}{4qc_0} \in \mathbb{Q}[t]$$

има корени $-1 \leq t_1 = \cos(\varphi) \leq t_2 = \cos(\psi) \leq 1$. Това е в сила, точно когато дискриминантата е неотрицателна, върхът е в интервала $[-1,1]$ и стойностите на $f(t)$ в краищата на този интервал са неотрицателни, т.е.

$$D(f) = \left[\frac{c_1 - (q+1)c_0}{2\sqrt{q}c_0}\right]^2 - \frac{4[1-(q+1)c_1]}{4qc_0} \geq 0, \tag{4.36}$$

$$-1 \leq \frac{(q+1)c_0 - c_1}{4\sqrt{q}c_0} \leq 1 \tag{4.37}$$

и

$$f(-1) \geq 0, f(1) \geq 0. \tag{4.38}$$

Непоредствено се проверява, че равенства (4.33) и (4.36) са еквивалентни. Тъй като минималното разстояние на кода C е $d = k-1$ и

$$\mathcal{W}_C^{(k-1)} = (q-1)\binom{2k}{k-1}c_0 \in \mathbb{N},$$

свободният член c_0 на $D_C(t)$ е положително рационално число. При това положение можем да умножим (4.37) с $-4\sqrt{q}c_0 < 0$, да прибавим почленно $(q+1)c_0$ и да го запишем във вида

$$(q - 4\sqrt{q} + 1)c_0 \leq c_1 \leq (q + 4\sqrt{q} + 1)c_0.$$

Чрез деление на $c_0 > 0$ получаваме (4.34). Накрая, неравенствата

$$4qc_0 f(1) = 4qc_0 + 2\sqrt{q}[c_1 - (q+1)c_0] + 1 - (q+1)c_1 = (-c_1 - 2\sqrt{q}c_0)(\sqrt{q}-1)^2 + 1 \geq 0$$

и

$$4qc_0 f(-1) = 4qc_0 - 2\sqrt{q}[c_1 - (q+1)c_0] + 1 - (q+1)c_1 = (2\sqrt{q}c_0 - c_1)(\sqrt{q}+1)^2 + 1 \geq 0$$

могат да бъдат изразени като (4.35). □

4.3 Редуциран полином на Дуурсма на функционално поле на крива

Нека $F = \mathbb{F}_q(X)$ е функционалното поле на крива X от род g, определена над $\mathbb{F}_q$, а $h_g = h(F)$ е броят на класовете дивизори на F, т.е. броят на класовете на линейна еквивалентност на дивизорите на F от степен 0. В този параграф ще разгледаме адитивно разлагане на полинома на Хасе-Вайл $L_F(t) \in \mathbb{Z}[t]$ на F, което съпоставя на F редица $\{h_i\}_{i=1}^{g-1}$ от виртуален брой класове дивизори h_i на функционални полета на криви от род i, определени над $\mathbb{F}_q$.

Лема 105. *За полином $L_g(t) \in \mathbb{Q}[t]$ от степен $\deg L_g(t) = 2g$, следните условия са еквивалентни:*

(i) $L_g(t)$ *удовлетворява функционалното уравнение на полинома на Хасе-Вайл на функционалното поле на крива от род* g*, определена над* $\mathbb{F}_q$*,*

$$L_g(t) = L_g\left(\frac{1}{qt}\right) q^g t^{2g}$$

(ii)

$$L_{g-1}(t) \coloneqq \frac{L_g(t) - L_g(1)t^g}{(1-t)(1-qt)}$$

е полином с рационални коефициенти от степен $2g-2$*, удовлетворяващ функционалното уравнение на полинома на Хасе-Вайл на функционалното поле на крива от род* $g-1$*, определена над* $\mathbb{F}_q$*,*

$$L_{g-1}(t) = L_{g-1}\left(\frac{1}{qt}\right) q^{g-1} t^{2g-2}$$

(iii)

$$L_g(t) = \sum_{i=0}^{g} h_i t^i (1-t)^{g-i} (1-qt)^{g-i}$$

за някакви рационални числа $h_i \in \mathbb{Q}$*.*

Доказателство: За $(i) \Rightarrow (ii)$ да забележим, че полиномът

$$M_g(t) \coloneqq L_g(t) - L_g(1)t^g$$

се анулира за $t = 1$. Следователно $M_g(t)$ се дели на $1 - t$. Освен това,

$$M_g(t) = L_g(t) - L_g(1)t^g = \left[L_g\left(\frac{1}{qt}\right) - \frac{L_g(1)}{q^g t^g}\right] q^g t^{2g} = M_g\left(\frac{1}{qt}\right) q^g t^{2g}.$$

В частност, $M_g\left(\frac{1}{q}\right) = M_g(1)\frac{q^g}{q^{2g}} = 0$, така че $M_g(t)$ се дели на линейния полином $q\left(\frac{1}{q} - t\right) = 1 - qt$, който е взаимно прост с $1 - t$. В резултат

$$L_{g-1}(t) = \frac{M_g(t)}{(1-t)(1-qt)} \in \mathbb{Q}[t]$$

е полином от степен $2g - 2$. Непосредствено се проверява, че

$$L_{g-1}\left(\frac{1}{qt}\right) q^{g-1} t^{2g-2} = \left[M_g\left(\frac{1}{qt}\right) : \left(1 - \frac{1}{qt}\right)\left(1 - \frac{1}{t}\right)\right] q^{g-1} t^{2g-2} =$$
$$= \frac{M_g(t)}{qt^2} : \frac{(qt-1)(t-1)}{qt^2} = \frac{M_g(t)}{(1-t)(1-qt)} = L_{g-1}(t).$$

Обратно, $(ii) \Rightarrow (i)$ следва от функционалното уравнение за $L_{g-1}(t)$, приложено към $L_g(t) = (1-t)(1-qt)L_{g-1}(t) + L_g(1)t^g$. По-точно,

$$\begin{aligned} L_g\left(\frac{1}{qt}\right) t^g t^{2g} = \\ = \left[\left(1-\frac{1}{qt}\right)qt\right]\left[\left(1-\frac{1}{t}\right)t\right]\left[L_{g-1}\left(\frac{1}{qt}\right)q^{g-1}t^{2g-2}\right] + \frac{L_g(1)}{q^g t^g}q^g t^{2g} = \\ = (qt-1)(t-1)L_{g-1}(t) + L_g(1)t^g = L_g(t). \end{aligned}$$

Извеждаме $(i) \Rightarrow (iii)$ с индукция по g, използвайки (ii). По-точно, за $g = 1$ имаме

$$L_0(t) \coloneqq \frac{L_1(t) - L_1(1)t}{(1-t)(1-qt)} \in \mathbb{Q}[t]$$

от степен $\deg L_0(t) = 0$, т.е. $L_0(t) \in \mathbb{Q}$. Тогава

$$L_1(t) = (1-t)(1-qt)L_0 + L_1(1)t = \sum_{i=0}^{1} h_i t^i (1-t)^{1-i}(1-qt)^{1-i}$$

за $h_0 = L_0 \in \mathbb{Q}$ и $h_1 = L_1(1) \in \mathbb{Q}$. В общия случай, от (ii) получаваме полином

$$L_{g-1}(t) = \frac{L_g(t) - L_g(1)t^g}{(1-t)(1-qt)},$$

удовлетворяващ функционалното уравнение на полинома на Хасе-Вайл на крива от род $g-1$, определена над $\mathbb{F}_q$,

$$L_{g-1}(t) = L_{g-1}\left(\frac{1}{qt}\right)q^{g-1}t^{2g-2}.$$

Съгласно индукционното предположение, съществуват $h_i^{'} \in \mathbb{Q}, 0 \leq i \leq g-1$, така че

$$L_{g-1}(t) = \sum_{i=0}^{g-1} h_i^{'} t^i (1-t)^{g-1-i}(1-tq)^{g-1-i}.$$

Оттук,

$$L_g(t) = (1-t)(1-qt)L_{g-1}(t) + L_g(1)t^g = \sum_{i=0}^{g} h_i t^i (1-t)^{g-i}(1-qt)^{g-i},$$

за $h_i = h_i^{'} \in \mathbb{Q}$ за $0 \leq i \leq g-1$ и $h_g = L_g(1) \in \mathbb{Q}$.

За да проверим $(iii) \Rightarrow (i)$, нека $L_g(t) = \sum_{i=0}^{g} h_i t^i (1-t)^{g-i}(1-qt)^{g-i}$. Тогава

$$L_g\left(\frac{1}{qt}\right) q^g t^{2g} = \left[\sum_{i=0}^{g} \frac{h_i}{q^i t^i}\left(1-\frac{1}{qt}\right)^{g-i}\left(1-\frac{1}{t}\right)^{g-i}\right] q^g t^{2g} =$$

$$= \sum_{i=0}^{g}\left[\frac{h_i}{q^i t^i} q^i t^{2i}\right]\left[\left(1-\frac{1}{qt}\right)qt\right]^{g-i}\left[\left(1-\frac{1}{t}\right)t\right]^{g-i} =$$

$$= \sum_{i=0}^{g} h_i t^i (1-t)^{g-i}(1-qt)^{g-i} = L_g(t).$$

Следователно $L_g(t)$ удовлетворява функционалното уравнение на полинома на Хасе-Вайл на крива от род g, определена над $\mathbb{F}_q$. □

Твърдение 106. *Нека $F = \mathbb{F}_q(X)$ е функционалното поле на гладка неприводима крива $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$ от род g, определена над $\mathbb{F}_q$, $h(F)$ е броят на класовете на линейна еквивалентност на дивизорите на F от степен 0, $\mathcal{A}_i$ е броят на ефективните дивизори на F от степен $i \geq 0$, $L_F(t) \in \mathbb{Q}[t]$ е полиномът на Хасе-Вайл на F, а $D_F(t) \in \mathbb{Q}[t]$ е редуцираният полином на Дуурсма на F, определен чрез равенството*

$$L_F(t) = (1-t)(1-qt)D_F(t) + h(F)t^g$$

Тогава:

(i) $D_F(t) = \sum_{i=0}^{g-2} \mathcal{A}_i(t^i + q^{g-1-i}t^{2g-2-i}) + \mathcal{A}_{g-1}t^{g-1} \in \mathbb{Z}[t]$ *е полином с цели коефициенти, който е еднозначно определен от* $\mathcal{A}_0 = 1, \mathcal{A}_1, \ldots, \mathcal{A}_{g-1}$.

(ii) равенството

$$\frac{D_F(t)}{(1-t)(1-qt)} = \sum_{i=0}^{\infty} \mathcal{B}_i t^i \tag{4.39}$$

на формални степенни редове на t е в сила за числата

$$\mathcal{B}_i = \sum_{j=0}^{i} \mathcal{A}_j \left(\frac{q^{i-j+1}-1}{q-1}\right) \tag{4.40}$$

при $0 \leq i \leq g-1$,

$$\mathcal{B}_i = \sum_{j=0}^{g-1} \mathcal{A}_j \left(\frac{q^{i-j+1}-1}{q-1}\right) + \sum_{j=g}^{i} \mathcal{A}_{2g-2-j}\left(\frac{q^{i-g+2}-q^{j-g+1}}{q-1}\right), \tag{4.41}$$

при $g \leq i \leq 2g-3$ и

$$\mathcal{B}_i = D_F(1)\left(\frac{q^{i-g+2}-1}{q-1}\right), \tag{4.42}$$

при $i \geq 2g-2$;

(iii) естествените числа $\mathcal{B}_i$ *удовлетворяват следните зависимости*

$$\mathcal{B}_i = q^{i-g+2}\mathcal{B}_{2g-4-i} + D_F(1)\left(\frac{q^{i-g+2}-1}{q-1}\right) \text{ за } g-1 \le i \le 2g-4; \tag{4.43}$$

$$\mathcal{B}_i = D_F(1)\left(\frac{q^{i-g+2}-1}{q-1}\right) \text{ за } i \ge 2g-3; \tag{4.44}$$

(iv) броят $h(F)$ *на класовете на линейна еквивалентност на дивизорите на* F *от степен* 0 *удовлетворява неравенствата*

$$(\sqrt{q}-1)^{2g} \le h(F) \le (\sqrt{q}+1)^{2g}.$$

Доказателство: (i) Съгласно Теорема 4.1.6(ii) и Теорема 4.1.11 от [Niederreiter, Xing], дзета функцията на Хасе-Вайл на F е пораждащата функция

$$\zeta_F(t) = \frac{L_F(t)}{(1-t)(1-qt)} = \sum_{j=0}^{\infty}\mathcal{A}_j t^j$$

на редицата $\{\mathcal{A}_i\}_{i=0}^{\infty}$. От Лема 105 и $L_F(1) = h(F)$ получаваме полином

$$D_F(t) \coloneqq \frac{L_F(t) - h(F)t^g}{(1-t)(1-qt)}$$

от степен $\deg D_F(t) = 2g-2$, удовлетворяващ функционалното уравнение на полинома на Хасе-Вайл на крива от род $g-1$, определена над $\mathbb{F}_q$. Следователно

$$\zeta_F(t) = D_F(t) + \frac{h(F)t^g}{(1-t)(1-qt)} = \sum_{j=0}^{\infty}\mathcal{A}_j t^j. \tag{4.45}$$

Нека $l(G)$ е размерността на пространството на Риман-Рох $\mathcal{L}(G)$, асоциирано с дивизора $G \in div(F)$. Теоремата на Риман-Рох гласи, че

$$l(G) = l(K_X - G) + deg(G) - g + 1$$

за каноничен дивизор K_X на X. За произволно $j \ge g-1$, нека $G_1, G_2, \ldots, G_{h(F)}$ е пълно множество от представители на класовете на линейна еквивалентност на дивизорите на F от степен j. Тогава

$$\mathcal{A}_j = \sum_{\nu=1}^{h(F)}\frac{q^{l(G_\nu)}-1}{q-1} = q^{j-g+1}\sum_{\nu=1}^{h(F)}\left(\frac{q^{l(K_X-G_\nu)}-1}{q-1}\right) + h(F)\left(\frac{q^{j-g+1}-1}{q-1}\right) \tag{4.46}$$

за $g \le j \le 2g-2$ и

$$\mathcal{A}_j = h(F)\left(\frac{q^{j-g+1}-1}{q-1}\right) \tag{4.47}$$

за всички $j \geq 2g-1$. Да забележим, че $K_X - G_1, K_X - G_2, \ldots, K_X - G_{h(F)}$ е пълна система от представители на класовете на линейна еквивалентност на дивизорите на F от степен $2g-2-j$, така че

$$\mathcal{A}_{2g-2-j} = \sum_{\nu=1}^{h(F)} \frac{q^{l(K_X-G_\nu)}-1}{q-1}. \tag{4.48}$$

Замествайки (4.48) в (4.46), получаваме

$$\mathcal{A}_j = q^{j-g+1}\mathcal{A}_{2g-2-j} + h(F)\left(\frac{q^{j-g+1}-1}{q-1}\right), \text{ за } g \leq j \leq 2g-2, \tag{4.49}$$

откъдето

$$Z_F(t) = \sum_{j=0}^{g-1} \mathcal{A}_j t^j + \sum_{j=g}^{2g-2} q^{j-g+1}\mathcal{A}_{2g-2-j}t^j + h(F)\sum_{j=g}^{\infty}\left(\frac{q^{j-g+1}-1}{q-1}\right)t^j.$$

Полагайки $i \coloneqq 2g-2-j$ във втората сума и $i \coloneqq j-g$ във третата сума, изразяваме

$$\begin{aligned} Z_F(t) = &\sum_{i=0}^{g-2} \mathcal{A}_i(t^i + q^{g-1-i}t^{2g-2-i}) + \mathcal{A}_{g-1}t^{g-1} + \\ &+h(F)\left[\frac{qt^g}{q-1}\left(\sum_{i=0}^{\infty} q^i t^i\right) - \frac{t^g}{q-1}\left(\sum_{i=0}^{\infty} t^i\right)\right]. \end{aligned} \tag{4.50}$$

Сумирайки геометричните прогресии

$$\sum_{i=0}^{\infty} q^i t^i = \frac{1}{1-qt} \quad \text{и} \quad \sum_{i=0}^{\infty} t^i = \frac{1}{1-t}$$

получаваме

$$\zeta_F(t) = \sum_{i=0}^{g-2} \mathcal{A}_i(t^i + q^{g-1-i}t^{2g-2-i}) + \mathcal{A}_{g-1}t^{g-1} + h(F)\frac{t^g}{(1-t)(1-qt)},$$

откъдето

$$D_F(t) = \sum_{i=0}^{g-2} \mathcal{A}_i(t^i + q^{g-1-i}t^{2g-2-i}) + \mathcal{A}_{g-1}t^{g-1}.$$

В частност, $D_F(t)$ има целочислени коефициенти.

(*ii*) Да развием

$$\frac{1}{1-t} = \sum_{i=0}^{\infty} t^i, \quad \frac{1}{1-qt} = \sum_{i=0}^{\infty} q^i t^i.$$

като суми на геометрични прогресии и да забележим, че

$$\frac{1}{(1-t)(1-qt)} = \sum_{i=0}^{\infty}(1+q+\ldots+q^i)t^i = \sum_{i=0}^{\infty}\left(\frac{q^{i+1}-1}{q-1}\right)t^i.$$

Да представим редуцирания полином на Дуурсма по следния начин

$$D_F(t) = \sum_{j=0}^{g-1} \mathcal{A}_j t^j + \sum_{j=g}^{2g-2} \mathcal{A}_{2g-2-j} q^{j-g+1} t^j.$$

Сега, сравнявайки коефициентите пред $t^i, i \geq 0$ от двете страни на (4.39), получаваме (4.40), (4.41) и

$$\mathcal{B}_i = \sum_{j=0}^{g-1} \mathcal{A}_j \left(\frac{q^{i-j+1}-1}{q-1} \right) + \sum_{j=g}^{2g-2} \mathcal{A}_{2g-2-j} q^{j-g+1} \left(\frac{q^{i-j+1}-1}{q-1} \right) \text{ за } i \geq 2g-2.$$

Последната формула можем да изразим като

$$\begin{aligned} \mathcal{B}_i = \\ = \frac{q^{i+1}}{q-1} \left(\sum_{j=0}^{q-1} \mathcal{A}_j q^{-j} + \sum_{j=g}^{2g-2} \mathcal{A}_{2g-2-j} q^{j-g+1} q^{-j} \right) - \frac{1}{q-1} \left(\sum_{j=0}^{g-1} \mathcal{A}_j + \sum_{j=g}^{2g-2} \mathcal{A}_{2g-2-j} q^{j-g+1} \right) = \\ = \frac{q^{i+1}}{q-1} D_F\left(\frac{1}{q}\right) - \frac{1}{q-1} D_F(1). \end{aligned}$$

Съгласно предишната лема, редуцираният полином на Дуурсма удовлетворява функционалното уравнение

$$D_F(t) = D_F\left(\frac{1}{qt}\right) q^{g-1} t^{2g-2}.$$

В частност, $D_F(1) = D_F\left(\frac{1}{q}\right) q^{g-1}$, откъдето следва и (4.42).

(iii) Тъй като $\mathcal{A}_i \geq 0, \forall i \geq 0$, числата $\mathcal{B}_i$ са суми на неотрицателни цели числа. Още повече, $\mathcal{B}_i \geq \mathcal{A}_0 \left(\frac{q^{i+1}-1}{q-1} \right) \geq \mathcal{A}_0 = 1$, така че числата $\mathcal{B}_i$ са естествени. За да докажем (4.43), да въведем полинома $\psi(t) \coloneqq \sum_{j=0}^{g-2} \mathcal{A}_j t^j \in \mathbb{Z}[t]$ и да изразим

$$\begin{aligned} D_F(t) = \sum_{j=0}^{g-2} \mathcal{A}_j t^j + q^{g-1} t^{2g-2} \left[\sum_{j=0}^{g-2} \mathcal{A}_j (qt)^{-j} \right] + \mathcal{A}_{g-1} t^{g-1} = \\ = \psi(t) + \psi\left(\frac{1}{qt}\right) q^{g-1} t^{2g-2} + \mathcal{A}_{g-1} t^{g-1}. \end{aligned}$$

В частност,

$$D_F(1) = \psi(1) + \psi\left(\frac{1}{q}\right) q^{g-1} + \mathcal{A}_{g-1}$$

Непосредствено проверяваме, че

$$\begin{aligned}\mathcal{B}_{g-1} - q\mathcal{B}_{g-3} = \\ = \frac{q^g}{q-1}\left(\sum_{j=0}^{g-2}\mathcal{A}_j q^{-j}\right) - \frac{1}{q-1}\left(\sum_{j=0}^{g-2}\mathcal{A}_j\right) + \mathcal{A}_{g-1} - \frac{q^{g-1}}{q-1}\left(\sum_{j=0}^{g-2}\mathcal{A}_j q^{-j}\right) + \frac{q}{q-1}\left(\sum_{j=0}^{g-2}\mathcal{A}_j\right) = \\ = \psi\left(\frac{1}{q}\right)q^{g-1} + \psi(1) + \mathcal{A}_{g-1} = D_F(1).\end{aligned}$$

Това доказва (4.43) за $i = g-1$. В случая $g \le i \le 2g-4$, да забележим, че $0 \le 2g-4-i \le g-4$ и

$$\begin{aligned}(q-1)(\mathcal{B}_i - q^{i-g+2}\mathcal{B}_{2g-4-i}) = \\ = \sum_{j=0}^{g-1}\mathcal{A}_j(q^{i-j+1}-1) + \sum_{j=g}^{i}\mathcal{A}_{2g-2-j}(q^{i-g+2} - q^{j-g+1}) - \sum_{j=0}^{2g-4-i}\mathcal{A}_j(q^{g-1-j} - q^{i-g+2}).\end{aligned}$$

Променяйки индекса на сумиране във втората сума на $s := 2g-2-j$, получаваме

$$\begin{aligned}(q-1)(\mathcal{B}_i - q^{i-g+2}\mathcal{B}_{2g-4-i}) = \\ = q^{i+1}\left(\sum_{j=0}^{g-1}\mathcal{A}_j q^{-j}\right) - \left(\sum_{j=0}^{g-1}\mathcal{A}_j\right) + q^{i-g+2}\left(\sum_{s=2g-2-i}^{g-2}\mathcal{A}_s\right) - \\ -q^{g-1}\left(\sum_{s=2g-2-i}^{g-2}\mathcal{A}_s q^{-s}\right) - q^{g-1}\left(\sum_{j=0}^{2g-4-i}\mathcal{A}_j q^{-j}\right) + q^{i-g+2}\left(\sum_{j=0}^{2g-4-i}\mathcal{A}_j\right)\end{aligned}$$

Посредством подходящо групиране на сумите получаваме

$$\begin{aligned}(q-1)(\mathcal{B}_i - q^{i-g+2}\mathcal{B}_{2g-4-i}) = \\ = \psi\left(\frac{1}{q}\right)q^{i+1} + \mathcal{A}_{g-1}q^{i-g+2} - \psi(1) - \mathcal{A}_{g-1} + q^{i-g+2}\psi(1) - \psi\left(\frac{1}{q}\right)q^{g-1} = \\ = (q^{i-g+2}-1)\left[\psi(1) + \psi\left(\frac{1}{q}\right)q^{g-1} + \mathcal{A}_{g-1}\right] = D_F(1)(q^{i-g+2}-1).\end{aligned}$$

Това доказва (4.43)

Да забележим, че (4.44) при $i \ge 2g-2$ съвпада с (4.42). В случая $i = 2g-3$,

$$(q-1)\mathcal{B}_{2g-3} = \sum_{j=0}^{g-1}\mathcal{A}_j(q^{2g-2-j}-1) + \sum_{s=1}^{g-2}\mathcal{A}_s(q^{g-1} - q^{g-1-s}),$$

след смяна на индекса на сумиране във втората сума на $s \coloneqq 2g-2-j$. В резултат,

$$\begin{aligned}(q-1)\mathcal{B}_{2g-3} &= \\ &= q^{2g-2}\left(\sum_{j-0}^{g-2}\mathcal{A}_j q^{-j}\right) - \left(\sum_{j=0}^{g-2}\mathcal{A}_j\right) + \mathcal{A}_{g-1}(q^{g-1}-1) + \\ &\quad + q^{g-1}\left(\sum_{j=0}^{g-2}\mathcal{A}_j\right) - q^{g-1}\left(\sum_{j=0}^{g-2}\mathcal{A}_j q^{-j}\right) = \\ &= (q^{g-1}-1)\left[\psi(1) + \psi\left(\frac{1}{q}\right)q^{g-1} + \mathcal{A}_{g-1}\right] = D_F(1)(q^{g-1}-1),\end{aligned}$$

което е точно (4.44) за $i = 2g-3$.

(iv) Съгласно теоремата на Хасе-Вайл, всички корени на $L_F(t)$ лежат върху окръжността $S\left(\frac{1}{\sqrt{q}}\right) = \left\{ \; z \;\middle|\; z \in \mathbb{C}, |z| = \frac{1}{\sqrt{q}} \; \right\}$. От доказателството на Твърдение 102 знаем, че

$$L_F(t) = a_{2g}\prod_{j=1}^{g}\left(t - \frac{e^{i\varphi_j}}{\sqrt{q}}\right)\left(t - \frac{e^{-i\varphi_j}}{\sqrt{q}}\right)$$

за някакви $\varphi_j \in [0, 2\pi)$. От функционалното уравнение

$$L_F(t) = L_F\left(\frac{1}{qt}\right)q^g t^{2g}$$

следва, че $a_{2g} = q^g a_0$. Комбинирайки с $a_0 = L_F(0) = 1$, получаваме

$$L_F(t) = \prod_{j=1}^{g}(\sqrt{q}t - e^{i\varphi_j})(\sqrt{q}t - e^{-i\varphi_j}) = \prod_{j=1}^{g}(qt^2 - 2\sqrt{q}\cos\varphi_j t + 1).$$

Заместването $t = 1$ дава

$$h(F) = L_F(1) = \prod_{j=1}^{g}(q - 2\sqrt{q}\cos\varphi_j + 1).$$

От друга страна, $\cos\varphi_j \in [-1, 1]$ изисква

$$(\sqrt{q}-1)^2 \leq q - 2\sqrt{q}\cos\varphi_j + 1 \leq (\sqrt{q}+1)^2,$$

откъдето

$$(\sqrt{q}-1)^{2g} \leq h(F) = L_F(1) = \prod_{j=1}^{g}(q - 2\sqrt{q}\cos\varphi_j + 1) \leq (\sqrt{q}+1)^{2g}.$$

□

Глава 5

Тъждествата на Мак Уилямс като поляризирани условия на Риман-Рох

Настоящата глава доказва, че тъждествата на Мак Уилямс за тегловото разпределение на линеен код C и неговия дуален $C^{\perp}$ са еквивалентни на поляризираните условия на Риман-Рох за ζ-функциите

$$\zeta_C(t) := \frac{P_C(t)}{(1-t)(1-qt)}, \quad \zeta_{C^{\perp}}(t) := \frac{P_{C^{\perp}}(t)}{(1-t)(1-qt)}$$

на тези кодове. По този начин, тъждествата на Мак Уилямс могат да се разглеждат като поляризирана версия на Теоремата на Риман-Рох и двойствеността на Сер върху гладка неприводима проективна крива X, определена над $\mathbb{F}_q$. Съдържанието на глава 5 отразява резултатите на статията [KM2]. След извеждане на условията на Риман-Рох върху крива, параграф 1 определя поляризираните условия на Риман-Рох за формални степенни редове $\zeta(t) = \sum\limits_{m=0}^{\infty} \mathcal{A}_m t^m$ и $\zeta^{\perp}(t) = \sum\limits_{m=0}^{\infty} \mathcal{A}_m^{\perp} t^m$. Основният резултат на глава 5 е еквивалентността на тъждествата на Мак Уилямс за тегловото разпределение на C и $C^{\perp}$ с поляризираните условия на Риман-Рох за ζ-функциите на тези кодове. Вторият параграф е посветен на усредняващи и вероятностни интерпретации на коефициентите c_i на редуцирания полином на Дуурсма

$$D_C(t) = \sum_{i=0}^{r-2} c_i t^i \in \mathbb{Q}[t]$$

на линеен код $C \subset \mathbb{F}_q^n$ от род g. За $0 \leq i \leq g-1$ коефициентът c_i е средно аритметично на броя на точките в сечение на проективизацията $\mathbb{P}(C)$ на C с $n-d-i$ координатни хиперравнини в $\mathbb{P}(\mathbb{F}_q^n) = \mathbb{P}^{n-1}(\mathbb{F}_q)$. За същия диапазон от индекси $0 \leq i \leq g-1$ и за минималното разстояние d на C, коефициентът c_i е изразен чрез вероятностите $\pi^{(w)}_{\mathbb{P}(C)}$ за дума $[b] \in \mathbb{P}(\mathbb{F}_q^n)^{(w)} := \{[b] \in \mathbb{P}(\mathbb{F}_q^n) \,|\, \mathrm{wt}([b]) = w\}$ с тегло $d \leq w \leq d+i$ да принадлежи

на $\mathbb{P}(C)$. Ако дуалният код $C^\perp$ на C има род $g^\perp$ и минимално раздстояние $d^\perp$, то за $g \leq i \leq g + g^\perp - 2$ коефициентът c_i на $D_C(t)$ зависи от вероятностите $\pi^{(w)}_{\mathbb{P}(C^\perp)}$ за дума $[b] \in \mathbb{P}(\mathbb{F}_q^n)^{(w)}$ с тегло $d^\perp \leq w \leq n - d - i$ да принадлежи на проективизацията $\mathbb{P}(C^\perp)$ на $C^\perp$. От друга страна, за $0 \leq i \leq g - 1$ коефициентът c_i е равен на сумата на вероятностите $\overline{\pi}^{(d+i)}_{[a]}$ подмножество $\beta \subset \{1, \ldots, n\}$ с $|\beta| = d + i$ елемента да съдържа носителя на фиксирана дума $[a] \in \mathbb{P}(C)$. За $g \leq i \leq g + g^\perp - 2$ коефициентът c_i се изразява чрез сумата на вероятностите $\overline{\pi}^{(n-d-i)}_{[b]}$ подмножество $\gamma \subset \{1, \ldots, n\}$ с $|\gamma| = n - d - i$ елемента да съдържа носителя на дума $[b] \in \mathbb{P}(C^\perp)$.

5.1 Тъждествата на МакУилямс за двойка дуални линейни кодове като поляризирани условия на Риман-Рох

Условията на Риман-Рох за формален степенен ред са мотивирани следната лема.

Лема 107. *Нека $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива от род g, определена над крайно поле $\mathbb{F}_q$, а $\zeta_X(t) = \sum_{m=0}^{\infty} \mathcal{A}_m(X) t^m$ е ζ-функцията на X. Тогава от Теоремата на Риман-Рох за X следват условията на Риман-Рох*

$$\mathcal{A}_m(X) = q^{m-g+1}\mathcal{A}_{2g-2-m}(X) + (q^{m-g+1} - 1)Res_1(\zeta_X(t)) \quad \forall m \geq g$$

за броя $\mathcal{A}_m(X)$ на ефективните дивизори на функционалното поле $\mathbb{F}_q(X)$ и за резидуума $Res_1(\zeta_X(t))$ на $\zeta_X(t)$ в $t = 1$.

Доказателство: За произволен дивизор G на $\mathbb{F}_q(X)$, нека $\mathcal{L}(G)$ е пространството на Риман-Рох на G и $l(G) := \dim_{\mathbb{F}_q} \mathcal{L}(G)$ е размерността на $\mathcal{L}(G)$. По Теоремата на Риман-Рох съществува каноничен дивизор K_X от степен $\deg K_X = 2g - 2$, така че

$$l(G) = l(K_X - G) + \deg G - g + 1 \tag{5.1}$$

за всички дивизори G на $\mathbb{F}_q(X)$. В частност, ако $\deg G > 2g-2$, то $l(G) = \deg G - g + 1$.

Да напомним, че ζ-функцията на функционалното поле $\mathbb{F}_q(X)$ на X над $\mathbb{F}_q$ е от вида

$$\zeta_X(t) = \frac{L_{\mathbb{F}_q(X)}(t)}{(1-t)(1-qt)}$$

за полином $L_{\mathbb{F}_q(X)}(t) \in \mathbb{Z}[t]$ от степен $\deg L_{\mathbb{F}_q(X)}(t) = 2g$. Ако h е броят на класовете на линейна еквивалентност на дивизорите на $\mathbb{F}_q(X)$ от степен 0, то резидуумът

$$Res_1(\zeta_X(t)) = \frac{L_{\mathbb{F}_q(X)}(1)}{q-1} = \frac{h}{q-1}.$$

Нека $G_1, G_2, \ldots, G_h$ е пълна система представители на класовете на линейна еквивалентност на дивизорите от степен $m \in \mathbb{Z}^{\geq 0}$. Тогава $K_X - G_1, K_X - G_2, \ldots, K_X - G_h$

е пълна система от представители на класовете на линейна еквивалентност на дивизорите на $\mathbb{F}_q(X)$ от степен $\deg(K_X - G_i) = 2g - 2 - m$. Ефективните дивизори на $\mathbb{F}_q(X)$, които са линейно еквивалентни с G_i образуват проективното пространство $\mathbb{P}(\mathcal{L}(G_i)) = \mathbb{P}^{l(G_i)-1}(\mathbb{F}_q)$. Така броят на ефективните дивизори на $\mathbb{F}_q(X)$ от степен m е

$$\mathcal{A}_m(X) = \sum_{i=1}^{h} \left| \mathbb{P}^{l(G_1)-1}(\mathbb{F}_q) \right| = \sum_{i=1}^{h} \frac{q^{l(G_i)} - 1}{q - 1} \tag{5.2}$$

Замествайки (5.1) в (5.2), получаваме

$$\mathcal{A}_m(X) = q^{m-g+1} \sum_{i=1}^{h} \left(\frac{q^{l(K_X - G_i)} - 1}{q - 1} \right) + h \left(\frac{q^{m-q+1} - 1}{q - 1} \right).$$

Вземайки предвид

$$\sum_{i=1}^{h} \left(\frac{q^{l(K_X - G_i)} - 1}{q - 1} \right) = \mathcal{A}_{2g-2-m}(X),$$

извеждаме

$$\mathcal{A}_m(X) = q^{m-g+1} \mathcal{A}_{2g-2-m}(X) + h \left(\frac{q^{m-g+1} - 1}{q - 1} \right), \quad \forall m \geq 0. \tag{5.3}$$

Да отбележим, че в случая $g \geq 2$ условията (5.3) за $0 \leq m \leq g-2$ са еквивалентни на същите равенства за $g \leq m = 2g - 2 - i \leq 2g - 2$, след умножение с q^{i-g-1}. Непосредствено се вижда, че (5.3) е тривиално изпълнено за $m = g - 1$. Ако $g = 0$, то $X = \mathbb{P}^1(\overline{\mathbb{F}_q})$, е проективната права и горните равенства се свеждат до

$$\mathcal{A}_m(X) = \frac{q^{m+1} - 1}{q - 1}, \forall m \geq 0.$$

Когато $g = 1$, кривата X е елиптична и

$$\mathcal{A}_m(X) = h \left(\frac{q^m - 1}{q - 1} \right), \forall m \geq 1.$$

□

Определение 108. *Формалният степенен ред* $\zeta(t) = \sum_{m=0}^{\infty} \mathcal{A}_m t^m \in \mathbb{C}[[t]]$ *удовлетворява условията на Риман-Рох* $RRC_q(g)$ *с основа* q *от род* $g \in \mathbb{Z}^{\geq 0}$, *ако*

$$\mathcal{A}_m = q^{m-g+1} \mathcal{A}_{2g-2-m} + (q^{m-g+1} - 1) Res_1(\zeta(t)), \quad \forall m \geq g$$

и за резидуума $\mathrm{Res}_1(\zeta(t))$ *на* $\zeta(t)$ *в* $t = 1$.

Определяме и поляризирана версия на условията на Риман-Рох.

Определение 109. *Формалните степенни редове* $\zeta(t) = \sum_{m=0}^{\infty} \mathcal{A}_m t^m$ *и* $\zeta^{\perp}(t) = \sum_{m=0}^{\infty} \mathcal{A}_m^{\perp} t^m$ *удовлетворяват поляризираните условия на Риман-Рох* $\mathrm{PRRC}_q(g, g^{\perp})$ *с основа* q *от род* $g, g^{\perp} \in \mathbb{Z}^{\geq 0}$, *ако*

$$\mathcal{A}_m = q^{m-g+1}\mathcal{A}^{\perp}_{g+g^{\perp}-2-m} + (q^{m-g+1} - 1)Res_1(\zeta(t)), \quad \forall m \geq g,$$

$$\mathcal{A}_{g-1} = \mathcal{A}^{\perp}_{g^{\perp}-1} \quad и$$

$$\mathcal{A}^{\perp}_m = q^{m-g^{\perp}+1}\mathcal{A}_{g+g^{\perp}-2-m} + (q^{m-g^{\perp}+1} - 1)Res_1(\zeta^{\perp}(t)), \quad \forall m \geq g^{\perp}.$$

Да отбележим, че от поляризираните условия на Риман-Рох $\mathrm{PRRC}_q(g, g^{\perp})$ следва

$$\mathcal{A}_m = \kappa_1 q^m + \kappa_2 \quad \text{и} \quad \mathcal{A}^{\perp}_m = \kappa_1^{\perp} q^m + \kappa_2^{\perp}$$

за всички $m \geq g + g^{\perp} - 1$ и някакви константи $\kappa_j, \kappa_j^{\perp} \in \mathbb{C}$. Тези равенства са еквивалентни на рекурентните зависимости

$$\mathcal{A}_{m+2} - (q+1)\mathcal{A}_{m+1} + q\mathcal{A}_m = \mathcal{A}^{\perp}_{m+2} - (q+1)\mathcal{A}^{\perp}_{m+1} + q\mathcal{A}^{\perp}_m = 0$$

за всички $m \geq g + g^{\perp} - 1$ и са в сила, точно когато

$$\zeta(t) = \frac{P(t)}{(1-t)(1-qt)} \quad \text{и} \quad \zeta^{\perp}(t) = \frac{P^{\perp}(t)}{(1-t)(1-qt)}$$

за някакви полиноми $P(t)$ и $P^{\perp}(t)$.

Основният резултат на настоящата глава е следната теорема.

Теорема 110. *Тъждествата на МакУилямс за* $\mathbb{F}_q$*-линеен* $[n, k, d]$ *код* C *от род* g *и неговия дуален код* $C^{\perp}$ *от род* $g^{\perp}$ *са еквивалентни на поляризираните условия на Риман-Рох* $\mathrm{PRRC}_q(g, g^{\perp})$ *за техните* ζ*-функции* $\zeta_C(t)$ *и* $\zeta_{C^{\perp}}(t)$.

Доказателство: В [Duursma1], [Duursma2] Дуурсма доказва, че тъждествата на Мак Уилямс за C и $C^{\perp}$ са еквивалентни на функционалното уравнение

$$P_{C^{\perp}}(t) = P_C\left(\frac{1}{qt}\right) q^g t^{g+g^{\perp}} \tag{5.4}$$

за техните ζ-полиноми (виж Твърдение 100). В глава 4 въведохме редуцирания полином на Дуурсма

$$D_C(t) \coloneqq \frac{P_C(t) - t^g}{(1-t)(1-qt)} = \sum_{i=0}^{g+g^{\perp}-2} c_i t^i \in \mathbb{Q}[t]$$

от степен $\deg D_C(t) = g + g^{\perp} - 2$ за всички двойки дуални кодове $C, C^{\perp} \subset \mathbb{F}_q^n$, с изключение на MDS-кодовете.

Първо ще докажем твърдението за $g, g^{\perp} \in \mathbb{N}$. Твърдим, че равенството (5.4) е еквивалентно на

$$D_{C^{\perp}}(t) = D_C\left(\frac{1}{qt}\right) q^{g-1} t^{g+g^{\perp}-2}, \tag{5.5}$$

за редуцираните полиноми на Дуурсма $D_C(t)$ и $D_{C^\perp}(t) = \sum_{i=0}^{g+g^\perp-2} c_i^\perp t^i \in \mathbb{Q}[t]$. Наистина, от една страна,

$$D_C\left(\frac{1}{qt}\right) q^{g-1}t^{g+g^\perp-2} = \left[\frac{P_C\left(\frac{1}{qt}\right) - \left(\frac{1}{qt}\right)^g}{\left(1-\frac{1}{qt}\right)\left(1-\frac{1}{t}\right)}\right] q^{g-1}t^{g+g^\perp-2} =$$
$$= \left[\frac{P_C\left(\frac{1}{qt}\right) - \frac{1}{q^g t^g}}{(1-qt)(1-t)}\right] q^g t^{g+g^\perp} = \frac{P_C\left(\frac{1}{qt}\right) q^g t^{g+g^\perp} - t^{g^\perp}}{(1-t)(1-qt)},$$

а от друга страна,

$$D_{C^\perp}(t) = \frac{P_{C^\perp}(t) - t^{g^\perp}}{(1-t)(1-qt)}.$$

Ако представим ζ -функцията $\zeta_C(t) \coloneqq \frac{P_C(t)}{(1-t)(1-qt)}$ на линеен код $C \subset \mathbb{F}_q^n$ като формален степенен ред $\zeta_C(t) = \sum_{m=0}^{\infty} \mathcal{A}_m(C)t^m$, то

$$D_C(t) = \sum_{m=0}^{\infty} \mathcal{A}_m(C)t^m - \sum_{m=g}^{\infty} \left(\frac{q^{m-g+1}-1}{q-1}\right) t^m, \tag{5.6}$$

понеже

$$\frac{t^g}{(1-t)(1-qt)} = t^g \left(\sum_{i=0}^{\infty} t^i\right)\left(\sum_{j=0}^{\infty} q^j t^j\right) =$$
$$= \sum_{m=g}^{\infty} (q^{m-g} + q^{m-g-1} + \ldots + q + 1)t^m = \sum_{m=g}^{\infty} \left(\frac{q^{m-g+1}-1}{q-1}\right) t^m \in \mathbb{Z}[[t]].$$

Така

$$\begin{aligned} D_C(t) &= \sum_{m=0}^{g-2} \mathcal{A}_m(C)t^m + \mathcal{A}_{g-1}(C)t^{g-1} + \sum_{i=g}^{g+g^\perp-2} c_i t^i = \\ &= \sum_{m=0}^{g-2} \mathcal{A}_m(C)t^m + \mathcal{A}_{g-1}(C)t^{g-1} + \left(\sum_{m=0}^{g^\perp-2} c_{g+g^\perp-2-m} t^{-m}\right) t^{g+g^\perp-2} \end{aligned} \tag{5.7}$$

и съответно,

$$D_{C^\perp}(t) = \sum_{m=0}^{g^\perp-2} \mathcal{A}_m(C^\perp)t^m + \mathcal{A}_{g^\perp-1}(C^\perp)t^{g^\perp-1} + \left(\sum_{m=0}^{g-2} c^\perp_{g+g^\perp-2-m} t^{-m}\right) t^{g+g^\perp-2},$$

за

$$\zeta_{C^\perp}(t) = \frac{P_{C^\perp}(t)}{(1-t)(1-qt)} = \sum_{m=0}^{\infty} \mathcal{A}_m(C^\perp)t^m.$$

Съгласно

$$D_C\left(\frac{1}{qt}\right) q^{g-1}t^{g+g^\perp-2} =$$

$$= \sum_{m=0}^{g-2} \mathcal{A}_m(C) q^{g-1-m} t^{g+g^\perp-2-m} + \mathcal{A}_{g-1}(C) t^{g^\perp-1} + \sum_{m=0}^{g^\perp-2} c_{g+g^\perp-2-m} q^{m-g^\perp+1} t^m =$$

$$= \sum_{m=0}^{g^\perp-2} c_{g+g^\perp-2-m} q^{m-g^\perp+1} t^m + \mathcal{A}_{g-1}(C) t^{g^\perp-1} + \left(\sum_{m=0}^{g-2} q^{-m+g-1} \mathcal{A}_m(C) t^{-m} \right) t^{g+g^\perp-2},$$

тъждествата на МакУилямс за редуцираните полиноми на Дуурсма на двойка взаимно дуални линейни кодове $C, C^\perp \subset \mathbb{F}_q^n$ от род $g \geq 1$, съответно $g^\perp \geq 1$ дават

$$c_{g+g^\perp-2-m} = q^{-m+g^\perp-1} \mathcal{A}_m(C^\perp) \text{ за } 0 \leq m \leq g^\perp - 2 \tag{5.8}$$

$$\mathcal{A}_{g^\perp-1}(C^\perp) = \mathcal{A}_{g-1}(C) \text{ и} \tag{5.9}$$

$$c^\perp_{g+g^\perp-2-m} = q^{-m+g-1} \mathcal{A}_m(C) \text{ за } 0 \leq m \leq g-2. \tag{5.10}$$

Замествайки $m = g + g^\perp - 2 - i$ и използвайки (5.6), виждаме че (5.8) е еквивалентно на

$$\mathcal{A}_i(C) = q^{i-g+1} \mathcal{A}_{g+g^\perp-2-i}(C^\perp) + \left(\frac{q^{i-g+1}-1}{q-1} \right), \quad g \leq i \leq g + g^\perp - 2.$$

Разменяйки местата на C и $C^\perp$, изразяваме (5.10) във вида

$$\mathcal{A}_i(C^\perp) = q^{i-g^\perp+1} \mathcal{A}_{g+g^\perp-2-i}(C) + \left(\frac{q^{i-g^\perp+1}-1}{q-1} \right), \quad g^\perp \leq i \leq g + g^\perp - 2.$$

Съгласно (5.6) е в сила

$$\mathcal{A}_i(C) = \frac{q^{i-g+1}-1}{q-1}, \quad \forall i \geq g + g^\perp - 1.$$

Аналогично,

$$\mathcal{A}_i(C^\perp) = \frac{q^{i-g^\perp+1}-1}{q-1}, \quad \forall i \geq g + g^\perp - 1.$$

Имайки предвид, че $\zeta_C(t)$ и $\zeta_{C^\perp}(t)$ нямат полюси в $t = 0$, въвеждаме $\mathcal{A}_{-j}(C) = 0$ и $\mathcal{A}_{-j}(C^\perp) = 0$, $\forall j \in \mathbb{N}$ и изразяваме тъждествата на МакУилямс във вида

$$\mathcal{A}_i(C) = q^{i-g+1} \mathcal{A}_{g+g^\perp-2-i}(C^\perp) + \left(\frac{g^{i-g+1}-1}{q-1} \right) \quad , \quad \forall i \geq g, \tag{5.11}$$

$$\mathcal{A}_{q^\perp-1}(C^\perp) = \mathcal{A}_{g-1}(C) \text{ и} \tag{5.12}$$

$$\mathcal{A}_i(C^\perp) = q^{i-g^\perp+1} \mathcal{A}_{g+g^\perp-2-i}(C) + \left(\frac{q^{i-g^\perp+1}-1}{q-1} \right), \quad \forall i \geq g^\perp. \tag{5.13}$$

Да отбележим също, че рационалната функция

$$\zeta_C = \frac{P_C(t)}{(1-t)(1-qt)}$$

има резидиум

$$Res_1(\zeta_C(t)) = \frac{P_C(1)}{q-1} = \frac{1}{q-1}$$

в $t = 1$. Така, при $g \geq 1$, $g^\perp \geq 1$, тъждествата на МакУилямс за $C, C^\perp \subset \mathbb{F}_q^n$ са еквивалентни на поляризираните условия на Риман-Рох.

Когато $g = 0$, линейният код C, както и неговият дуален $C^\perp$ са MDS-кодове. Съответните ζ-функции

$$\zeta_C(t) = \zeta_{C^\perp}(t) = \frac{1}{(1-t)(1-qt)} = \zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)$$

съвпадат с ζ-функцията на проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ и удовлетворяват условията на Риман-Рох от род 0, които са еквивалентни на поляризираните условия на Риман-Рох. □

Следствие 111. *Половината от събираемите*

$$\varphi_C(t) = \sum_{i=0}^{g-2} c_i t^i, \quad \textit{съответно,} \quad \varphi_{C^\perp}(t) = \sum_{i=0}^{g^\perp-2} c_i^\perp t^i$$

на редуцираните полиноми на Дуурсма

$$D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i, \quad \textit{съответно,} \quad D_{C^\perp}(t) = \sum_{i=0}^{g+g^\perp-2} c_i^\perp t^i$$

на двойка взаимно дуални линейни кодове C, $C^\perp \subset \mathbb{F}_q^n$ с род $g \geq 1$, съответно $g^\perp \geq 1$ и числата c_{g-1} и $c^\perp_{g^\perp-1} \in \mathbb{Q}$ определят напълно

$$D_C(t) = \varphi_C(t) + c_{g-1}t^{g-1} + \varphi_{C^\perp}\left(\frac{1}{qt}\right) q^{g^\perp-1} t^{g+g^\perp-2}, \tag{5.14}$$

$$D_{C^\perp}(t) = \varphi_{C^\perp}(t) + c_{g-1}t^{g^\perp-1} + \varphi_C\left(\frac{1}{qt}\right) q^{g-1} t^{g+g^\perp-2}. \tag{5.15}$$

Доказателство: Заместваики (5.8) в (5.7), получаваме

$$D_C(t) = \varphi_C(t) + c_{g-1}t^{g-1} + \left(\sum_{m=0}^{g^\perp-2} c_m^\perp q^{-m} t^{-m}\right) q^{g^\perp-1} t^{g+g^\perp-2},$$

откъдето следва (5.14). Разменяйки C с $C^\perp$, $C^\perp$ с C и $c^\perp_{g^\perp-1}$ с c_{g-1} получваме равенство (5.15). □

5.2 Усредняващи и вероятностни интерпретации на коефициентите на редуцирания полином на Дуурсма

Нека $C \subset \mathbb{F}_q^n$ е линеен код с редуцуран полином на Дуурсма $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i$ и $\mathbb{P}(C) \subset \mathbb{P}(\mathbb{F}_q^n) = \mathbb{P}^{n-1}(\mathbb{F}_q)$ е проективизацията на C, разглеждана като подпространство на проективизацията на $\mathbb{F}_q^n$. Да забележим, че тегловата функция

$$wt : \mathbb{F}_q^n \longrightarrow \{0, 1, \ldots, n\},$$

$$wt(a) = |\{\ \ 1 \leq i \leq n\ \ |\ \ a_i \neq 0\ \ \}| \quad \text{за } a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n,$$

индуцира коректно определена теглова функция

$$wt : \mathbb{P}(\mathbb{F}_q^n) \longrightarrow \{0, 1, \ldots, n\},$$

$$wt([a]) = wt([a_1 : a_2 : \ldots : a_n]) = |\{\ \ 1 \leq i \leq n\ \ |\ \ a_i \neq 0\ \ \}|.$$

и да определим носителя на $[a] \in \mathbb{P}^{n-1}(\mathbb{F}_q)$ като $Supp([a]) = \{\ \ 1 \leq i \leq n\ \ |\ \ a_i \neq 0\ \ \}$.

Да означим с

$$\mathbb{P}^{n-1}(\mathbb{F}_q)^{(s)} \coloneqq \left\{\ \ [a] \in \mathbb{P}^{n-1}(\mathbb{F}_q)\ \ \middle|\ \ wt([a]) = s\ \ \right\}$$

множеството на думите от $\mathbb{P}^{n-1}(\mathbb{F}_q)$ с тегло $1 \leq s \leq n$ и да положим

$$\mathbb{P}(C)^{(s)} \coloneqq \{\ \ [a] \in \mathbb{P}(C)\ \ |\ \ wt([a]) = s\ \ \} = \mathbb{P}^{n-1}(\mathbb{F}_q)^{(s)} \cap \mathbb{P}(C).$$

За произволно $1 \leq s \leq n$, нека $\binom{[n]}{s}$ е фамилията на подмножествата $\alpha = \{\alpha_1, \ldots, \alpha_s\} \subseteq \{1, \ldots, n\}$ с $|\alpha| = s$ елемента.

Да напомним, че линеен код $C \subset \mathbb{F}_q^n$ е неизроден, ако не се съдържа в координатна хиперравнина $V(x_i) = \{a \in \mathbb{F}_q^n \,|\, a_i = 0\}$ за някое $1 \leq i \leq n$.

Твърдение 112. *Нека C е неизроден $\mathbb{F}_q$-линеен $[n, k, d]$-код от род $g \geq 1$, чийто дуален код $C^\perp \subset \mathbb{F}_q^n$ има минимално разстояние $d^\perp$ и род $g^\perp \geq 1$. Разглеждаме редуцирания полином на Дуурсма $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i$ на C и множеството*

$$\mathbb{P}(C)^{\subseteq\beta} \coloneqq \{\ \ [a] \in \mathbb{P}(C)\ \ |\ \ Supp([a]) \subseteq \beta\ \ \}$$

на думите от $\mathbb{P}(C)$, чийто носител се съдържа в $\beta \in \binom{[n]}{s}$. Тогава:

(i) $c_i \binom{n}{d+i} \in \mathbb{Z}^{\geq 0}$ *за всички* $0 \leq i \leq g + g^\perp - 2$;

(ii) $c_i = \binom{n}{d+i}^{-1} \left(\sum_{\beta \in \binom{[n]}{d+i}} \left| \mathbb{P}(C)^{\subseteq\beta} \right| \right)$ *за* $0 \leq i \leq g-1$ *е средното аритметично на броя на точките в сечението на $\mathbb{P}(C)$ с $n-d-i$ координатни хиперравнини в $\mathbb{P}(\mathbb{F}_q^n) = \mathbb{P}^{n-1}(\mathbb{F}_q)$.*

Доказателство: (i) За всяко $d \leq w \leq n$, нека $\mathcal{W}_C^{(w)}$ е броят на думите $a \in C$, с тегло $wt(a) = w$. Съгласно равенство (4.6),

$$c_i = (q-1)^{-1}\binom{n}{d+i}^{-1} \sum_{w=d}^{d+i} \binom{n-w}{n-d-i} \mathcal{W}_C^{(w)} \quad \text{за} \quad 0 \leq i \leq g-1.$$

Да отбележим, че

$$\frac{\mathcal{W}_C^{(w)}}{q-1} = \left|\mathbb{P}(C)^{(w)}\right| \in \mathbb{Z}^{\geq 0}$$

е броят на думите от $\mathbb{P}(C)$ с тегло w. Затова $c_i\binom{n}{d+i} \in \mathbb{Z}^{\geq 0}$ са неотрицателни цели числа за $0 \leq i \leq g-1$. От равенство (5.14) имаме

$$\sum_{i=g}^{g+g^\perp-2} c_i t^i = \sum_{j=0}^{g^\perp-2} c_j^\perp q^{g^\perp-1-j} t^{g+g^\perp-2-j},$$

откъдето

$$c_i = q^{i-g+1} c_{g+g^\perp-2-i}^\perp \quad \text{за} \quad g \leq i \leq g+g^\perp-2. \tag{5.16}$$

Прилагайки равенство (4.6) за дуалния код $C^\perp$, получаваме

$$c_{g+g^\perp-2-i}^\perp \binom{n}{d^\perp+g+g^\perp-2-i} = c_{g+g^\perp-2-i}^\perp \binom{n}{n-d-i} = c_{g+g^\perp-2-i}^\perp \binom{n}{d+i} \in \mathbb{Z}^{\geq 0}.$$

за $g \leq i \leq g+g^\perp-2$. Комбинирайки с равенство (5.16), стигаме до извода че

$$c_i\binom{n}{d+i} = q^{i-g+1} c_{g+g^\perp-2-i}^\perp \binom{n}{d+i} \in \mathbb{Z}^{\geq 0} \quad \forall i, \quad g \leq i \leq g+g^\perp-2.$$

(ii) Всяка проективна $[n,k,d]$-система $\mathcal{P} = \{P_1, P_2, \ldots, P_n\} \subset \mathbb{P}^{k-1}(\mathbb{F}_q) = \mathbb{P}(C^*)$, отговаряща на неизроден $\mathbb{F}_q$-линеен код C е подмножество на проективизацията на пространството $C^* = Hom_{\mathbb{F}_q}(C, \mathbb{F}_q)$ на линейните функционали на C. По-точно, всяка точка P_j се повдига до ограничението $\widetilde{P_j} = x_j|_C$ на координатния функционал $x_j : \mathbb{F}_q^n \to \mathbb{F}_q$. Хиперравнинвата H_j, асоциирана с P_j можем да отъждествим с $C \cap Z(x_j)$, където $Z(x_j) = \{ \ x \in \mathbb{F}_q^n \ \mid \ x_j = 0 \ \}$. За произволно $\alpha \in \binom{[n]}{i}$ с допълнение $\neg\alpha = [n] \setminus \alpha$ забелязваме, че

$$C \cap \left(\cap_{s=1}^i Z(x_{\alpha_s})\right) = \{ \ a \in C \ \mid \ Supp(a) \subseteq \neg\alpha \ \} = C^{(\subseteq \neg\alpha)}$$

се състои от думите на C, чийто носител се съдържа в $\neg\alpha$. Означавайки $l(\alpha) := \dim_{\mathbb{F}_q} C \cap \left(\cap_{s=1}^i Z(x_{\alpha_s})\right)$, забелязваме че $\mathbb{P}(C)^{(\subseteq\neg\alpha)}$ има мощност

$$\left|\mathbb{P}(C)^{(\subseteq\neg\alpha)}\right| = \frac{q^{l(\alpha)}-1}{q-1}.$$

Съгласно теорема 1.1.28 и Задача 1.1.29 от [Tsafman, Vladut, Nogin], тегловият полином на C може да бъде записан във вида

$$\mathcal{W}_C(x,y) = x^n + \sum_{i=0}^{n-d} B_i (x-y)^i y^{n-i}, \tag{5.17}$$

където

$$B_i = (q-1) \sum_{\alpha \in \binom{[n]}{i}} \left| \mathbb{P}(C)^{(\subseteq \neg\alpha)} \right|.$$

От друга страна от равенство (4.3) имаме

$$\mathcal{W}_C(x,y) = \mathcal{M}_{n,n+1-k}(x,y) + (q-1) \sum_{i=0}^{g+g^\perp-2} c_i \binom{n}{d+i} (x-y)^{n-d-i} y^{d+i},$$

където $\mathcal{M}_{n,n+1-k}(x,y)$ е тегловият полином на MDS-код с дължина n и минимално разстояние $n+1-k$. Прилагайки Теорема 1.1.28 от монографията [Tsafman, Vladut, Nogin] към $\mathcal{M}_{n,n+1-k}(x,y)$, извеждаме

$$\mathcal{M}_{n,n+1-k}(x,y) = x^n + \sum_{i=0}^{k-1} \binom{n}{i} (q^{k-i}-1)(x-y)^i y^{n-i}.$$

Комбинирайки равенства (5.17) и (4.3) с горния резултат, получаваме

$$\sum_{i=0}^{k-1} \binom{n}{i} (q^{k-i}-1)(x-y)^i y^{n-i} + (q-1) \sum_{i=0}^{g+g^\perp-2} c_i \binom{n}{d+i} (x-y)^{n-d-i} y^{d+i} = \\ = \sum_{i=0}^{n-d} B_i (x-y)^i y^{n-i}.$$

Полагаме $z := x - y$ и сравнявайки коефициентите пред $z^i y^{n-i}$ за $k \le i \le n-d$, пресмятаме, че

$$(q-1) c_{n-d-i} \binom{n}{n-i} = B_i \quad \text{за} \quad k \le i \le n-d.$$

С други думи,

$$c_j = \binom{n}{d+j}^{-1} (q-1)^{-1} B_{n-d-j} = \binom{n}{d+j}^{-1} \sum_{\alpha \in \binom{[n]}{n-d-j}} \left| \mathbb{P}(C)^{(\subseteq \neg\alpha)} \right|$$

за всички $0 \le j \le g-1$. Вземайки предвид факта, че $\beta = \neg\alpha$ пробягва $\binom{[n]}{d+j}$, когато α пробягва $\binom{[n]}{n-d-j}$, заключаваме че

$$c_j = \binom{n}{d+j}^{-1} \sum_{\beta \in \binom{[n]}{d+j}} \left| \mathbb{P}(C)^{(\subseteq \beta)} \right| \quad \text{за} \quad 0 \le j \le g-1.$$

□

Твърдение 113. *Нека C е $\mathbb{F}_q$-линеен $[n,k,d]$-код от род $g \geq 1$, чийто дуален код $C^\perp$ е $[n, n-k, d^\perp]$-код от род $g^\perp \geq 1$, а $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i$ е редуцираният полином на Дуурсма на кода C. За произволно $1 \leq w \leq n$ да означим с $\pi^{(w)}_{\mathbb{P}(C)}$ вероятността $[b] \in \mathbb{P}^{n-1}(\mathbb{F}_q)^{(w)} := \{ \ [b] \in \mathbb{P}^{n-1}(\mathbb{F}_q) \ \mid \ wt([b]) = w \ \}$ да принадлежи на $\mathbb{P}(C)^{(w)} := \{ \ [a] \in \mathbb{P}(C) \ \mid \ wt([a]) = w \ \}$, а с $\overline{\pi}^{(w)}_{[a]}$ - вероятността $\beta \in \binom{[n]}{w}$ да съдържа носителя на някое $[a] \in \mathbb{P}(C)$. Тогава:*

(i)

$$c_i = \sum_{w=d}^{d+i} \pi^{(w)}_{\mathbb{P}(C)} \binom{d+i}{w} (q-1)^{w-1} \quad \textit{за} \quad 0 \leq i \leq g-1 \tag{5.18}$$

$$c_i = q^{i-g+1} \left[\sum_{w=d^\perp}^{n-d-i} \pi^{(w)}_{\mathbb{P}(C)} \binom{n-d-i}{w} (q-1)^{w-1} \right] \quad \textit{за} \quad g \leq i \leq g+g^\perp-2, \tag{5.19}$$

(ii)

$$c_i = \sum_{[a] \in \mathbb{P}(C)} \overline{\pi}^{(d+i)}_{[a]} \quad \textit{за} \quad 0 \leq i \leq g-1 \tag{5.20}$$

$$c_i = q^{i-g+1} \left(\sum_{[b] \in \mathbb{P}(C^\perp)} \overline{\pi}^{(n-d-i)}_{[b]} \right) \quad \textit{за} \quad g \leq i \leq g+g^\perp-2 = n-d-d^\perp \tag{5.21}$$

Доказателство: Ако $C^{(w)} := \{ \ a \in C \ \mid \ wt(a) = w \ \}$ е множеството от думите на C с тегло w, то $\mathbb{P}(C)^{(w)} = C^{(w)}/\mathbb{F}_q^*$, откъдето

$$\left| \mathbb{P}(C)^{(w)} \right| = \frac{\left| C^{(w)} \right|}{\left| \mathbb{F}_q^* \right|} = \frac{\mathcal{W}_C^{(w)}}{q-1} \quad \text{за} \quad 1 \leq w \leq n.$$

Вземайки предвид

$$\left| \mathbb{P}^{n-1}(\mathbb{F}_q)^{(w)} \right| = \binom{n}{w} \frac{\left| (\mathbb{F}_q^*)^w \right|}{\left| \mathbb{F}_q^* \right|} = \binom{n}{w} (q-1)^{w-1},$$

пресмятаме, че

$$\pi^{(w)}_{\mathbb{P}(C)} = \frac{\mathcal{W}_C^{(w)}}{\binom{n}{w}(q-1)^w} \quad \text{за} \quad 1 \leq w \leq n.$$

След заместване на горното равенство в (4.6) получаваме

$$c_i = \sum_{w=d}^{d+i} \binom{n}{d+i}^{-1} \binom{n}{w} \binom{n-w}{n-d-i} \pi^{(w)}_{\mathbb{P}(C)} (q-1)^{w-1} \quad \text{за} \quad 0 \leq i \leq g-1.$$

Комбинирайки с

$$\binom{n}{d+i}^{-1}\binom{n}{w}\binom{n-w}{n-d-i}=\binom{d+i}{w} \quad \text{за} \quad d\leq w\leq d+i,$$

извеждаме (5.18) за произволен $\mathbb{F}_q$-линеен $[n,k,d]$-код C. Прилагайки това равенство за дуалния код $C^\perp$, получаваме

$$c_i^\perp=\sum_{w=d^\perp}^{d^\perp+i}\pi^{(w)}_{\mathbb{P}(C^\perp)}\binom{d^\perp+i}{w}(q-1)^{w-1} \quad \text{за} \quad 0\leq i\leq g^\perp-1.$$

Замествайки полученото равенство в (5.16) и използвайки

$$d^\perp+g+g^\perp-2-i=n-d-i, \tag{5.22}$$

извеждаме (5.19).

(*ii*) За произволни $[a]\in\mathbb{P}(C)$ и $1\leq w\leq n$, вероятността $\beta\in\binom{[n]}{w}$ да съдържа $Supp([a])\in\binom{[n]}{s}$ е

$$\overline{\pi}^{(w)}_{[a]}=\begin{cases}\frac{\binom{n-s}{w-s}}{\binom{n}{w}} & \text{при} \quad s=wt([a])\leq w\leq n,\\ 0 & \text{при} \quad s=wt([a])>w.\end{cases}$$

Това ни позволява да изразим (4.6) във вида

$$c_i=\sum_{w=d}^{d+i}\frac{\binom{n-w}{d+i-w}}{\binom{n}{d+i}}\left|\mathbb{P}(C)^{(w)}\right|=\sum_{w=d}^{d+i}\sum_{[a]\in\mathbb{P}(C)^{(w)}}\frac{\binom{n-w}{d+i-w}}{\binom{n}{d+i}}=$$

$$=\sum_{w=d}^{d+i}\sum_{[a]\in\mathbb{P}(C)^{(w)}}\overline{\pi}^{(d+i)}_{[a]}=\sum_{[a]\in\mathbb{P}(C)}\overline{\pi}^{(d+i)}_{[a]}$$

за $0\leq i\leq g-1$. Аналогично,

$$c_j^\perp=\sum_{[b]\in\mathbb{P}(C^\perp)}\overline{\pi}^{(d^\perp+j)}_{[b]} \quad \text{за} \quad 0\leq j\leq g^\perp-1.$$

Комбинирайки с (5.16) и (5.22), получаваме

$$c_i=q^{i-g+1}\left(\sum_{[b]\in\mathbb{P}(C^\perp)}\overline{\pi}^{(n-d-i)}_{[b]}\right) \quad \text{за} \quad g\leq i\leq g+g^\perp-2.$$

□

Глава 6

Аналог на хипотезата на Риман за локално крайни модули над абсолютната група на Галоа на крайно поле

През 1923 г. Артин въвежда ζ-функцията $\zeta_X(t)$ на гладка неприводима крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, за да изучи броя $N_m(X) := |X(\mathbb{F}_{q^m})|$ на $\mathbb{F}_{q^m}$-рационалните точки на хиперелиптична крива. Хасе разглежда случая на елиптична крива през 1936 г., а Андре Вайл обобщава известните резултати за произволна гладка неприводима крива X през 1940 г., доказвайки че $\zeta_X(t)$-функцията е рационална функция, чийто числител има корени единствено върху окръжността с център $0 \in \mathbb{C}$ и радиус $\frac{1}{\sqrt{q}}$. Настоящата глава въвежда понятията локално краен модул M над абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$ и ζ-функция $\zeta_M(t)$ на M, описваща броя на орбитите на $\mathfrak{G}$ върху M с фиксиран брой точки. Обобщавайки идеята на доказателството на Бомбиери на Теоремата на Хасе-Вайл от [Bombieri] е намерено достатъчно условие, при което M изпълнява аналога на хипотезата на Риман относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Достатъчното условие се състои от три предположения, които са изпълнени за гладка неприводима проективна крива $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$ от род $g \geq 1$. Първо предполагаме, че частното

$$P_M(t) := \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)}$$

на ζ-функцията $\zeta_M(t)$ на M с ζ-функцията $\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)$ на $\mathbb{P}^1(\overline{\mathbb{F}_q})$ е полином $P_M(t) == \sum_{i=0}^{d} a_i t^i$. Второто предположение е съществуването на покриващо изображение на $\mathbb{P}^1(\overline{\mathbb{F}_q})$ чрез M с обвивка на Галоа. Покритието $\xi : M \dashrightarrow \mathbb{P}^(\overline{\mathbb{F}_q})$ е определено върху допълнението M_o на краен брой точки от M. Обвивката на Галоа $\xi_H : N \to \xi(M_o) = N/H$ на ξ свива в точка орбитите на крайна група H от $\mathfrak{G}_m = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$-еквивариантни биекции $h : N \to N$ без фиксирани точки за някакво $m \in \mathbb{N}$ и се пропуска през

$\xi : M_o \to \xi(M_o)$. Третото условие е горна граница върху относителната скорост на растеж на броя на рационалните точки на M относно броя на рационалните точки на $\mathbb{P}^1(\overline{\mathbb{F}_q})$. То може да се разглежда като обобщение на границата на Хасе-Вайл за броя на рационалните точки на гладка неприводима проективна крива X, определена над $\mathbb{F}_q$.

Съдържанието на настоящата глава отразява резултатите на статията [KM3]. В параграф 1 са събрани някои непосредствени свойства на локално-крайните $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули M и техните морфизми. Параграф 2 дава няколко израза за ζ-функцията $\zeta_M(t)$ на M и изучава частното

$$P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} \in \mathbb{Z}[[t]]$$

на ζ- функциите на M и $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Тя дава необходимо и достатъчно условие, при което $P_M(t) \in \mathbb{Z}[t]$ е полином. По аналогия с някои свойства на крайните неразклонени покрития на квази-проективни многообразия или топологични пространства, параграф 3 въвежда понятието за крайно неразклонено покритие $\xi : M \to L$ на локално крайни $\mathfrak{G}$-модули. Дискутирани са покритията на Галоа $\xi : M \to L$, както и крайните неразклонени покрития $\xi : M \to L$, които имат обвивка на Галоа. Последният, четвърти параграф е посветен на основния резултат на тази глава - Теорема 142. В него се въвеждат понятията порядък $\mathrm{ord}_{\mathfrak{G}}(M/L)$ на локално краен $\mathfrak{G}$-модул M относно локално краен $\mathfrak{G}$-модул L и H-порядък $\mathrm{ord}^H_{\mathfrak{G}}(M/L)$ на M относно L за крайна група H от $\mathfrak{G}$-еквивариантни биекции $M \to M$ без фиксирани точки. Тези определения обобщават класическата граница на Хасе-Вайл върху броя на рационалните точки на гладка неприводима крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$. С конкретен пример е установено, че предположенията на Теорема 142 са изпълнени за клас от локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули, който съдържа строго гладките неприводими криви $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ от род $g \geq 1$. От аналога на хипотезата на Риман за M относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ е изведено функционално уравнение за ζ-полинома $P_M(t) := \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} \in \mathbb{Z}[t]$ на M.

6.1 Елементарни свойства на локално крайните модули над $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ и техните морфизми

Множество M с действие на група G ще наричаме G-модул. В преобладаваща част от тази глава разглеждаме модули над абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$.

Определение 114. *Казваме, че $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул M е локално краен, ако всички $\mathfrak{G}$-орбити върху M са крайни и за всяко $n \in \mathbb{N}$ съществуват най-много краен брой $\mathfrak{G}$-орбити върху M с n точки.*

Броят на елементите на $\mathfrak{G}$-орбита $\mathrm{Orb}_{\mathfrak{G}}(x)$, $x \in M$ се нарича нейна степен и се бележи с $\deg \mathrm{Orb}_{\mathfrak{G}}(x)$.

Гладките неприводими криви $X/\mathbb{F}_q \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$, определени над $\mathbb{F}_q$ са примери за локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули.

Определение 115. *Ако M е локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул, то формалният степенен ред*

$$\zeta_M(t) := \prod_{\nu \in \mathrm{Orb}_{\mathfrak{G}}(M)} \left(\frac{1}{1 - t^{\deg \nu}} \right) \in \mathbb{C}[[t]]$$

се нарича ζ-функция на M.

От определението следва непосредствено, че $\zeta_M(0) = 1$. За гладка неприводима крива $X/\mathbb{F}_q \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$, ζ-функцията $\zeta_X(t)$ на X като локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул съвпада с локалната ζ-функция на Вайл на X. Фиксираме проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ като основен модел, с който сравняваме разглежданите локално крайни $\mathfrak{G}$-модули M и напомняме найната ζ-функция

$$\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t) = \frac{1}{(1-t)(1-qt)}.$$

Определение 116. *Локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул M изпълнява аналога на хипотезата на Риман относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$, ако частното*

$$P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = \sum_{i=0}^{d} a_i t^i = \prod_{i=1}^{d} (1 - \omega_i t) \in \mathbb{C}[t]$$

е полином с $|\omega_1| = \ldots = |\omega_d| = \sqrt[d]{|\omega_1| \ldots |\omega_d|} = \sqrt[d]{|a_d|}$ за $\forall 1 \leq i \leq d$.

За да обясним етимологията на понятието, да заместим q^{-s}, $s \in \mathbb{C}$ в ζ-функцията $\zeta_M(t) = \zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t) \prod_{i=1}^{d} (1 - \omega_i t)$ на M и да разгледаме

$$\zeta_M\left(q^{-s}\right) = \frac{\prod_{i=1}^{d} (q^s - \omega_i)}{q^{sd-2s+1}(1-q^s)(1-q^{s-1})}$$

като мероморфна функция на $s \in \mathbb{C}$ с полюси $2\pi i\mathbb{Z} \cup (1 + 2\pi i\mathbb{Z})$. Ако $\lambda := \log_q \sqrt[d]{|a_d|} \in \mathbb{R}^{\geq 0}$, то M изпълнява аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ точно когато комплексните корени $s_o \in \mathbb{C}$ на $\zeta_M\left(q^{-s}\right)$ имат $\mathrm{Re}(s_o) = \lambda$. Всички гладки неприводими криви $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ от род $g \geq 1$ изпълняват аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$, съгласно Теоремата на Хасе-Вайл (вж.[Bombieri] или [Stichtenoth]). По-точно,

$$P_X(t) = \frac{\zeta_X(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = \prod_{i=1}^{2g} (1 - \omega_i t) \quad \text{с} \quad |\omega_i| = q^{\frac{1}{2}}, \quad \forall 1 \leq i \leq 2g,$$

което е еквивалентно на $\mathrm{Re}(s_o) = \frac{1}{2}$ за всички комплексни корени $s_o \in \mathbb{C}$ на $\zeta_X(q^{-s})$. Това прилича на оригиналната хипотеза на Риман $\mathrm{Re}(z_o) = \frac{1}{2}$ за нетривиалните корени $z_o \in \mathbb{C} \setminus (-2\mathbb{N})$ на Римановата ζ-функция

$$\zeta(z) := \sum_{n=1}^{\infty} \frac{1}{n^z}, \quad z \in \mathbb{C}.$$

Следват някои тривиални свойства на локално крайните $\widehat{\mathbb{Z}}$-действия.

Лема 117. *Нека $\mathfrak{G} = \widehat{\langle\varphi\rangle}$ е про-крайната обвивка на безкрайната циклична група $\langle\varphi\rangle \simeq (\mathbb{Z}, +)$, M е локално краен $\mathfrak{G}$-модул със затворени стабилизатори $\mathrm{Stab}_{\mathfrak{G}}(x) < \mathfrak{G}$ за всички $x \in M$, $\mathrm{Orb}_{\mathfrak{G}}(x) \subseteq M$ е $\mathfrak{G}$-орбита върху M от степен $m = \deg \mathrm{Orb}_{\mathfrak{G}}(x)$ и $\mathfrak{G}_m = \widehat{\langle\varphi^m\rangle}$ е про-крайната обвивка на $\langle\varphi^m\rangle \simeq (\mathbb{Z}, +)$. Тогава :*

(i) всяка точка $y \in \mathrm{Orb}_{\mathfrak{G}}(x)$ има стабилизатор

$$\mathrm{Stab}_{\mathfrak{G}}(y) = \mathrm{Stab}_{\mathfrak{G}}(x) = \mathfrak{G}_m;$$

(ii) орбитите

$$\mathrm{Orb}_{\mathfrak{G}}(x) = \mathrm{Orb}_{\langle\varphi\rangle}(x) = \{x, \varphi(x), \ldots, \varphi^{m-1}(x)\}$$

съвпадат;

(iii) за $\forall r \in \mathbb{N}$ с най-голям общ делител $\mathrm{GCD}(r, m) = d \in \mathbb{N}$, $\mathfrak{G}$-орбитата

$$\mathrm{Orb}_{\mathfrak{G}}(x) = \coprod_{j=1}^{d} \mathrm{Orb}_{\mathfrak{G}_r}(\varphi^{i_j}(x))$$

на x се разлага в непресичащо се обединение на d орбити от степен $m_1 = \frac{m}{d}$ относно действието на $\mathfrak{G}_r = \widehat{\langle\varphi^r\rangle}$.

Доказателство: Ако $\mathfrak{G}' := Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \widehat{\langle\Phi_q\rangle}$ е абсолютната група на Галоа на крайно поле $\mathbb{F}_q$, то изоморфизмът на групи $f : \langle\varphi\rangle \longrightarrow \langle\Phi_q\rangle$, $f(\varphi^s) = \Phi_q^s$ за $\forall s \in \mathbb{N}$ има единствено продължение до изоморфизъм на групи

$$f : \mathfrak{G} = \widehat{\langle\varphi\rangle} \longrightarrow \widehat{\langle\Phi_q\rangle} = \mathfrak{G}', \quad f(\varphi^{l_s(\mathrm{mod}\, s)})_{s\in\mathbb{N}} = (\Phi_q^{l_s(\mathrm{mod}\, s)})_{s\in\mathbb{N}} \in \prod_{s\in\mathbb{N}} (\langle\Phi_q\rangle/\langle\Phi_q^s\rangle)$$

на съответни про-крайни обвивки. Затова е достатъчно да докажем лемата за $\mathfrak{G}' = \widehat{\langle\Phi_q\rangle}$.

(i) По предположение, $\mathrm{Stab}_{\mathfrak{G}}(x)$ е затворена подгрупа на $\mathfrak{G}$ с индекс

$$[\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(x)] = \deg \mathrm{Orb}_{\mathfrak{G}}(x) = m.$$

Възоснова на

$$Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)/Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m}) = \mathfrak{G}'/\mathfrak{G}'_m$$

за $\mathfrak{G}'_m = \widehat{\langle\Phi_q^m\rangle}$, затворената подгрупа $\mathfrak{G}'_m$ на $\mathfrak{G}'$ е с индекс m и затворената подгрупа $\mathfrak{G}_m$ на $\mathfrak{G}$ е с индекс $[\mathfrak{G} : \mathfrak{G}_m] = m$. Ако $\mathcal{H}$ е затворена подгрупа на $\mathfrak{G}$ с индекс $[\mathfrak{G} : \mathcal{H}] = m$, то $\mathfrak{G}/\mathcal{H}$ е абелева група от ред m и $\varphi^m \in \mathcal{H}$ за $\forall\varphi \in \mathfrak{G}$. Следователно затворената обвивка $\mathfrak{G}_m = \widehat{\langle\varphi^m\rangle}$ на $\langle\varphi^m\rangle$ в $\mathfrak{G}$ се съдържа в $\mathcal{H}$ и

$$[\mathcal{H} : \mathfrak{G}_m] = \frac{[\mathfrak{G} : \mathfrak{G}_m]}{[\mathfrak{G} : \mathcal{H}]} = 1.$$

Следователно $\mathcal{H} = \mathfrak{G}_m$ е единствената затворена подгрупа на $\mathfrak{G}$ от индекс m и $\mathrm{Stab}_{\mathfrak{G}}(x) = \mathfrak{G}_m$. Понеже $\mathfrak{G}$ е абелева група, всяко $y \in \mathrm{Orb}_{\mathfrak{G}}(x)$ има същият стабилизатор $\mathrm{Stab}_{\mathfrak{G}}(y) = \mathrm{Stab}_{\mathfrak{G}}(x) = \mathfrak{G}_m$ като x.

(ii) От включването на групи $\langle\varphi\rangle \subset \widehat{\langle\varphi\rangle} = \mathfrak{G}$ следва включването $\mathrm{Orb}_{\langle\varphi\rangle}(x) \subseteq \mathrm{Orb}_{\mathfrak{G}}(x)$ на съответните орбити. Достатъчно е да докажем, че $x, \varphi(x), \ldots, \varphi^{m-1}(x)$ са две по две различни точки, за да стигнем до заключението, че $\deg \mathrm{Orb}_{\langle\varphi\rangle}(x) \geq m = \deg \mathrm{Orb}_{\mathfrak{G}}(x)$, откъдето $\mathrm{Orb}_{\langle\varphi\rangle}(x) = \mathrm{Orb}_{\mathfrak{G}}(x)$. Наистина, ако $\varphi^i(x) = \varphi^j(x)$ за някои $0 \leq i < j \leq m-1$, то от $x = \varphi^{j-i}(x)$ следва, че $\varphi^{j-i} \in \mathrm{Stab}_{\mathfrak{G}}(x) \cap \langle\varphi\rangle = \widehat{\langle\varphi^m\rangle} \cap \langle\varphi\rangle = \langle\varphi^m\rangle$ и m дели $0 < j - i \leq m - 1$. Това е противоречие, доказващо $\mathrm{Orb}_{\langle\varphi\rangle}(x) = \mathrm{Orb}_{\mathfrak{G}}(x)$.

(iii) Достатъчно е да проверим, че $\forall y \in \mathrm{Orb}_{\mathfrak{G}}(x)$ има стабилизатор $\mathrm{Stab}_{\mathfrak{G}_r}(y) = \mathfrak{G}_{rm_1}$, за да приложим (i) и да стигнем до извода, че $\deg \mathrm{Orb}_{\mathfrak{G}_r}(y) = m_1$. Вземайки предвид, че $\mathrm{Stab}_{\mathfrak{G}_r}(y) = \mathrm{Stab}_{\mathfrak{G}}(y) \cap \mathfrak{G}_r = \mathfrak{G}_m \cap \mathfrak{G}_r$ и най-малкото общо кратно на m и r е $\mathrm{LCM}(m, r) = rm_1 = mr_1 \in \mathbb{N}$ за $r_1 = \frac{r}{d}$, редуцираме твърдението към $\mathfrak{G}_m \cap \mathfrak{G}_r = \mathfrak{G}_{\mathrm{LCM}(m,r)}$. Възоснова на

$$\mathfrak{G}_r/(\mathfrak{G}_m \cap \mathfrak{G}_r) \simeq \mathfrak{G}_r\mathfrak{G}_m/\mathfrak{G}_m < \mathfrak{G}/\mathfrak{G}_m,$$

индексът

$$s := [\mathfrak{G} : \mathfrak{G}_m \cap \mathfrak{G}_r] = [\mathfrak{G} : \mathfrak{G}_r][\mathfrak{G}_r : (\mathfrak{G}_m \cap \mathfrak{G}_r)] \leq rm$$

е краен и $\mathfrak{G}_m \cap \mathfrak{G}_r = \mathfrak{G}_s$. От $\mathfrak{G}_s < \mathfrak{G}_m < \mathfrak{G}$ и $\mathfrak{G}_s < \mathfrak{G}_r < \mathfrak{G}$, цялото число $s \in \mathbb{N}$ е общо кратно на m, r, така че $\mathrm{LCM}(m, r) \in \mathbb{N}$ дели s. Понеже $\mathfrak{G}_{\mathrm{LCM}(m,r)} = \mathfrak{G}_{rm_1} = \mathfrak{G}_{r_1 m}$ се съдържа в $\mathfrak{G}_m$ и $\mathfrak{G}_r$, следва $\mathfrak{G}_{\mathrm{LCM}(m,r)} \leq \mathfrak{G}_m \cap \mathfrak{G}_r = \mathfrak{G}_s$, така че s дели $\mathrm{LCM}(m, r)$ и $s = \mathrm{LCM}(m, r)$.

□

Ако M и L са модули над група G, то G-еквивариантните изображения

$$\xi : M \longrightarrow L, \quad g\xi(x) = \xi(gx) \quad \text{за} \quad \forall g \in G, \quad \forall x \in M$$

се наричат морфизми на G-модули . Нека $\xi : M \to L$ е морфизъм на локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули. Следващото твърдение дава числено описание на ограничението на ξ върху праобраза на $\mathfrak{G}$-орбита чрез индексите на инерция на ξ. Да забележим, че образът $\xi(M)$ е $\mathfrak{G}$-инвариантен и за произволно пълно множество $\Sigma_{\mathfrak{G}}(\xi(M)) \subseteq \xi(M)$ от представители на $\mathfrak{G}$-орбити върху $\xi(M)$, разлагането $\xi(M) = \coprod_{x \in \Sigma_{\mathfrak{G}}(\xi(M))} \mathrm{Orb}_{\mathfrak{G}}(x)$ на $\mathfrak{G}$-орбити се изтегля до непресичащо се разлагане

$$M = \coprod_{x \in \Sigma_{\mathfrak{G}}(\xi(M))} \xi^{-1}\mathrm{Orb}_{\mathfrak{G}}(x) \tag{6.1}$$

на $\mathfrak{G}$-подмодули на M. По този начин, морфизмът $\xi : M \to L$ на $\mathfrak{G}$-модули е напълно определен от сюрективните морфизми

$$\xi : \xi^{-1}\mathrm{Orb}_{\mathfrak{G}}(x) \longrightarrow \mathrm{Orb}_{\mathfrak{G}}(x)$$

на $\mathfrak{G}$-модули за $\forall x \in \Sigma_{\mathfrak{G}}(\xi(M))$.

Твърдение 118. *Нека $\xi : M \to L$ е морфизъм на локално крайни модули със затворени стабилизатори над про-крайната обвивка $\mathfrak{G} = \widehat{\langle\varphi\rangle}$ на безкрайна циклична група $\langle\varphi\rangle \simeq (\mathbb{Z}, +)$,*

$$\delta = \deg \mathrm{Orb}_{\mathfrak{G}} : L \longrightarrow \mathbb{N}, \quad \delta(x) = \deg \mathrm{Orb}_{\mathfrak{G}}(x) \quad \textit{за} \quad \forall x \in L \quad \textit{и}$$

$$e_\xi : M \longrightarrow \mathbb{Q}^{>0}, \quad e_\xi(y) = \frac{\deg \mathrm{Orb}_{\mathfrak{G}}(y)}{\deg \mathrm{Orb}_{\mathfrak{G}}(\xi(y))} \quad \textit{за} \quad \forall y \in M.$$

Тогава :

(i) $\mathrm{Stab}_{\mathfrak{G}}(y)$ *е подгрупа на* $\mathrm{Stab}_{\mathfrak{G}}(\xi(y))$ *за всички точки* $y \in M$*, така че* $e_\xi(y) = [\mathrm{Stab}_{\mathfrak{G}}(\xi(y)) : \mathrm{Stab}_{\mathfrak{G}}(y)] \in \mathbb{N}$ *взема естествени стойности;*

(ii) за всяка точка $x \in \xi(M)$ *съществува подмножество* $S_x \subseteq \xi^{-1}(x)$*, така че*

$$\xi^{-1}\mathrm{Orb}_{\mathfrak{G}}(x) = \coprod_{y \in S_x} \mathrm{Orb}_{\mathfrak{G}}(y) \quad c \quad \deg \mathrm{Orb}_{\mathfrak{G}}(y) = \delta(x) e_\xi(y); \tag{6.2}$$

(iii) за $\forall x \in \xi(M)$ *слоят* $\xi^{-1}(x)$ *е* $\mathfrak{G}_{\delta(x)}$*-модул с разлагане в орбити*

$$\xi^{-1}(x) = \coprod_{y \in S_x} \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y) \quad \textit{от} \quad \deg \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y) = e_\xi(y). \tag{6.3}$$

Съответствието $e_\xi : M \to \mathbb{N}$ *се нарича инерционно изображение на* $\xi : M \to L$*. Стойностите* $e_\xi(y)$*,* $y \in M$ *на* e_ξ *се наричат инерционни индекси на* ξ*.*

Доказателство: (i) От $\mathfrak{G}$-еквивариантността на ξ следва че $\mathrm{Stab}_{\mathfrak{G}}(y) \leq \mathrm{Stab}_{\mathfrak{G}}(\xi(y)) \leq \mathfrak{G}$. Комбинирайки с Лема 117 (i), изразяваме

$$e_\xi(y) = \frac{[\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(y)]}{[\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(\xi(y))]} = [\mathrm{Stab}_{\mathfrak{G}}(\xi(y)) : \mathrm{Stab}_{\mathfrak{G}}(y)] \in \mathbb{N}.$$

(ii) Твърдим, че за $\forall x \in \xi(M)$ всички $\mathfrak{G}$-орбити върху $\xi^{-1}\mathrm{Orb}_{\mathfrak{G}}(x)$ пресичат слоя $\xi^{-1}(x)$. Предполагайки $\xi(z) = \varphi^s(x)$ за някои $z \in M$ и $0 \leq s \leq \delta(x) - 1$, забелязваме че $\xi(\varphi^{\delta(x)-s} z) = \varphi^{\delta(x)-s}\xi(z) = x$, откъдето $y := \varphi^{\delta(x)-s}(z) \in \xi^{-1}(x)$ с $\mathrm{Orb}_{\mathfrak{G}}(z) = \mathrm{Orb}_{\mathfrak{G}}(y)$. Това позволява избора на пълна система $S_x \subseteq \xi^{-1}(x)$ от $\mathfrak{G}$-орбити върху $\xi^{-1}\mathrm{Orb}_{\mathfrak{G}}(x)$ и установяването на (6.2) от определението за $e_\xi(y)$ с $y \in S_x \subseteq \xi^{-1}(x)$.

(iii) Ако $x \in \xi(M)$, $y \in \xi^{-1}(x)$ то от $\xi(\varphi^{\delta(x)} y) = \varphi^{\delta(x)}\xi(y) = \varphi^{\delta(x)}(x) = x$ следва $\varphi^{\delta(x)}(y) \in \xi^{-1}(x)$, така че върху $\xi^{-1}(x)$ действа $\mathfrak{G}_{\delta(x)} = \widehat{\langle\varphi^{\delta(x)}\rangle}$. С това проверихме включването $\cup_{y \in S_x} \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y) \subseteq \xi^{-1}(x)$. За произволни $y, y' \in S_x$, от предположението $y' \in \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y) \subseteq \mathrm{Orb}_{\mathfrak{G}}(y)$ следва че $y' = y$, така че обединението $\coprod\limits_{y \in S_x} \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y)$ е непресичащо се. По определнието на S_x, произволно

$$z \in \xi^{-1}(x) \subset \xi^{-1}\mathrm{Orb}_{\mathfrak{G}}(x) = \coprod_{y \in S_x} \mathrm{Orb}_{\mathfrak{G}}(y)$$

е от вида $z = \varphi^s(y)$ за някое $y \in S_x$ и $0 \leq s < \delta(x) e_\xi(y) - 1$. Възоснова на $x = \xi(z) = \xi(\varphi^s(y)) = \varphi^s\xi(y) = \varphi^s(x)$ получаваме, че $\varphi^s \in \mathrm{Stab}_{\mathfrak{G}}(x) \cap \langle\varphi\rangle = \widehat{\langle\varphi^{\delta(x)}\rangle} \cap \langle\varphi\rangle = \langle\varphi^{\delta(x)}\rangle$,

откъдето $s = \delta(x)r$ за някое $r \in \mathbb{Z}^{\geq 0}$. Следователно $z = \varphi^{\delta(x)r}(y) \in \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y)$ и $\xi^{-1}(x) \subseteq \coprod\limits_{y \in S_x} \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y)$. С това проверихме, разлагането в $\mathfrak{G}_{\delta(x)}$-орбити (6.3). От (ii) и доказателството на Лема 117 (iii) имаме

$$\mathrm{Stab}_{\mathfrak{G}_{\delta(x)}}(y) = \mathrm{Stab}_{\mathfrak{G}}(y) \cap \mathfrak{G}_{\delta(x)} = \mathfrak{G}_{\delta(x)e_\xi(y)} \cap \mathfrak{G}_{\delta(x)} = \mathfrak{G}_{\delta(x)e_\xi(y)},$$

защото $\mathrm{LCM}(\delta(x)e_\xi(y), \delta(x)) = \delta(x)e_\xi(y)$. Прилагаме Лема 117(i) и получаваме, че $\deg \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y) = e_\xi(y)$.

□

6.2 Локално крайни модули с полиномиално ζ-частно

За да дадем още две представяния за ζ-функцията на локално краен модул M над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, да напомним, че върху произволна гладка неприводима крива $X/\mathbb{F}_q \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$, определена над $\mathbb{F}_q$, фиксираните точки

$$X^{\Phi_q^r} := \{x \in X \mid \Phi_q^r(x) = x\} = X(\mathbb{F}_{q^r})$$

на произволна степен Φ_q^r, $r \in \mathbb{N}$ на автоморфизма на Фробениус Φ_q съвпадат с $\mathbb{F}_{q^r}$-рационалните. Затова за произволен локално краен модул M над про-крайната обвивка $\mathfrak{G} = \widehat{\langle\varphi\rangle}$ на безкрайна циклична група $\langle\varphi\rangle \simeq (\mathbb{Z}, +)$, фиксираните точки

$$M^{\varphi^r} := \{x \in M \mid \varphi^r(x) = x\}$$

на φ^r с $r \in \mathbb{N}$ се наричат φ^r-рационални. Да забележим, че ако $\deg \mathrm{Orb}_{\mathfrak{G}}(x) = m$, то $x \in M^{\varphi^r}$ тогава и само тогава, когато $\varphi^r \in \mathrm{Stab}_{\mathfrak{G}}(x) = \mathfrak{G}_m = \widehat{\langle\varphi^m\rangle}$ и това е в сила точно когато m дели r. Понеже всяко фиксирано $r \in \mathbb{N}$ има краен брой естествени делители m и за всяко $m \in \mathbb{N}$ съществуват най-много краен брой $\mathfrak{G}$-орбити върху M от степен m, множествата M^{φ^r} са крайни.

Да разгледаме свободната абелева група $(\mathrm{Div}(M), +)$, породена от $\mathfrak{G}$-орбитите $\nu \in \mathrm{Orb}_{\mathfrak{G}}(M)$. Нейните елементи се наричат дивизори върху M и са крайни линейни комбинации $D = a_1\nu_1 + \ldots + a_s\nu_s$ на орбити $\nu_j \in \mathrm{Orb}_{\mathfrak{G}}(M)$ с цели коефициенти $a_j \in \mathbb{Z}$. Терминологията възниква от случая на гладка неприводима крива $X/\mathbb{F}_q \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$, в който $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитите ν са във взаимно еднозначно съответствие с класовете дискретни нормирания $\widetilde{\nu}$ на функционалното поле $\mathbb{F}_q(X)$ на X над $\mathbb{F}_q$. Ако $R_{\widetilde{\nu}}$ е пръстенът на дискретно нормиране, отговарящ на класа дискретни нормирания $\widetilde{\nu}$, то полето от остатъци $R_{\widetilde{\nu}}/\mathfrak{M}_{\widetilde{\nu}}$ на $R_{\widetilde{\nu}}$ е от степен $[R_{\widetilde{\nu}}/\mathfrak{M}_{\widetilde{\nu}} : \mathbb{F}_q] = \deg \nu$.

Да забележим, че степента на $\mathfrak{G}$-орбита се продължава до хомоморфизъм на групи

$$\deg : (\mathrm{Div}(M), +) \longrightarrow (\mathbb{Z}, +), \quad \deg\left(\sum_{\nu \in \mathrm{Orb}_{\mathfrak{G}}(M)} a_\nu \nu\right) = \sum_{\nu \in \mathrm{Orb}_{\mathfrak{G}}(M)} a_\nu \deg \nu.$$

Дивизор $D = a_1\nu_1 + \ldots + a_s\nu_s \geq 0$ е ефективен ако всичките му ненулеви коефициенти са положителни. Нека $\mathrm{Div}_{\geq 0}(M)$ е множеството на ефективните дивизори върху M.

Ефективните дивизори $D = a_1\nu_1 + \ldots + a_s\nu_s \geq 0$ върху M с фиксирана степен $\deg D = a_1 \deg \nu_1 + \ldots + a_s \deg \nu_s = m \in \mathbb{Z}^{\geq 0}$ имат ограничени коефициенти $1 \leq a_j \leq m$ и огпаничени степени $\deg \nu_j \leq m$ на $\mathfrak{G}$-орбитите от носителя на D. Вземайки предвид, че M има най-много краен брой $\mathfrak{G}$-орбити ν_j от степен $\deg \nu_j \leq m$, стигаме до извода, че съществуват най-много краен брой ефективни дивизори върху M от степен $m \in \mathbb{Z}^{\geq 0}$ и означаваме техния брой с $\mathcal{A}_m(M)$.

Следващата лема обобщава две от добре известните представяния на локалната ζ-функция на Вайл $\zeta_X(t)$ на гладка неприводима крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ за ζ-функцията на произволен локално краен $\mathfrak{G} = \widehat{\langle\varphi\rangle}$-модул M. Доказателствата са подобни на тези за $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, дадени в [Niederreiter, Xing] или в [Stichtenoth].

Твърдение 119. *Нека $\mathfrak{G} = \widehat{\langle\varphi\rangle}$ е про-крайната обвивка на безкрайна циклична група $\langle\varphi\rangle$ и M е локално краен $\mathfrak{G}$-модул. Тогава ζ-функцията на M е равна на*

$$\zeta_M(t) = \exp\left(\sum_{r=1}^{\infty} \left|M^{\varphi^r}\right| \frac{t^r}{r}\right) = \sum_{m=0}^{\infty} \mathcal{A}_m(M) t^m,$$

където $\left|M^{\varphi^r}\right|$ е броят на φ^r-рационалните точки върху M и $\mathcal{A}_m(M)$ е броят на ефективните дивизори върху M от степен $m \in \mathbb{Z}^{\geq 0}$.

Доказателство: Ако $B_k(M)$ е броят на $\mathfrak{G}$-орбити върху M от степен k, то

$$\zeta_M(t) := \prod_{\nu \in \mathrm{Orb}_{\mathfrak{G}}(M)} \left(\frac{1}{1 - t^{\deg \nu}}\right) = \prod_{k=1}^{\infty} \left(\frac{1}{1-t^k}\right)^{B_k(M)}.$$

Следователно

$$\log \zeta_M(t) = -\sum_{k=1}^{\infty} B_k(M) \log(1-t^k) = \sum_{k=1}^{\infty} B_k(M) \left(\sum_{n=1}^{\infty} \frac{t^{kn}}{n}\right) = \sum_{r=1}^{\infty} \left(\sum_{k/r} k B_k(M)\right) \frac{t^r}{r},$$

съгласно равенството на формални степенни редове

$$\log(1-z) = -\sum_{r=1}^{\infty} \frac{z^r}{r} \in \mathbb{Q}[[z]]. \tag{6.4}$$

Ако $M^{\varphi^r} = \coprod_{\deg \mathrm{Orb}_{\mathfrak{G}}(x)/r} \mathrm{Orb}_{\mathfrak{G}}(x)$ е разлагането на M^{φ^r} в непресичащо се обединение на $\mathfrak{G}$-орбити, то броят на φ^r-рационалните точки на M е

$$\left|M^{\varphi^r}\right| = \sum_{k/r} k B_k(M), \tag{6.5}$$

откъдето $\log \zeta_M(t) = \sum_{r=1}^{\infty} \left|M^{\varphi^r}\right| \frac{t^r}{r}$.

От друга страна, имаме равенство на формални степенни редове

$$\zeta_M(t) = \prod_{\nu \in \mathrm{Orb}_{\mathfrak{G}}(M)} \left(\sum_{n=0}^{\infty} t^{\deg(n\nu)} \right) = \sum_{D \in \mathrm{Div}_{\geq 0}(M)} t^{\deg D} = \sum_{m=0}^{\infty} \mathcal{A}_m(M) t^m.$$

□

За произволна група G, биективните морфизми $\xi : M \to L$ на G-модули се наричат изоморфизми на G-модули.

Следствие 120. *За локално крайните $\mathfrak{G} = \widehat{\langle\varphi\rangle}$-модули M, L със затворени стабилизатори съществува изоморфизъм на $\mathfrak{G}$-модули $\xi : M \to L$ тогава и само тогава, когато техните ζ-функции $\zeta_M(t) = \zeta_L(t)$ съвпадат.*

Доказателство: Нека $\xi : M \to L$ е изоморфизъм на $\mathfrak{G}$-модули и $x \in L$ е точка с орбита от степен $\deg \mathrm{Orb}_{\mathfrak{G}}(x) = \delta(x)$. Тогава (6.3) от Твърдение-Определние 118 (iii) дава разлагане $\xi^{-1}(x) = \coprod\limits_{y \in S_x} \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y)$ на слоя $\xi^{-1}(x)$ в непресичащо се обединение на $\mathfrak{G}_{\delta(x)}$-орбити от степен $\deg \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y) = e_\xi(y)$. Следователно $|S_x| = 1$ за $\forall x \in L$, $e_\xi(y) = 1$ за $\forall y \in M$ и $\xi^{-1}\mathrm{Orb}_{\mathfrak{G}}(x) = \mathrm{Orb}_{\mathfrak{G}}\xi^{-1}(x)$ е от степен $\delta(x)$ съгласно (6.2) от Твърдение-Определение 118 (ii). В резултат, (6.1) приема вида $M = \coprod\limits_{x \in \Sigma_{\mathfrak{G}}(L)} \mathrm{Orb}_{\mathfrak{G}}\xi^{-1}(x)$ за произволна пълна система $\Sigma_{\mathfrak{G}}(L)$ от представители на $\mathfrak{G}$-орбитите върху L и

$$\zeta_M(t) = \prod_{x \in \Sigma_{\mathfrak{G}}(L)} \left(\frac{1}{1 - t^{\delta(x)}} \right) = \zeta_L(t).$$

Обратно, да предположим, че локално крайните $\mathfrak{G}$-модули M и L имат една и съща ζ-функция $\zeta_M(t) = \zeta_L(t)$. Тогава от Твърдение 119 следва равенството

$$\sum_{r=1}^{\infty} \left| M^{\varphi^r} \right| \frac{t^r}{r} = \log \zeta_M(t) = \log \zeta_L(t) = \sum_{r=1}^{\infty} \left| L^{\varphi^r} \right| \frac{t^r}{r} \in \mathbb{Q}[[t]]$$

на формални степенни редове на t, а оттам и равенствата

$$\sum_{d/r} dB_d(M) = \left| M^{\varphi^r} \right| = \left| L^{\varphi^r} \right| = \sum_{d/r} dB_d(L)$$

на техните коефициенти за $\forall r \in \mathbb{N}$. С индукция по r извеждаме, че $B_d(M) = B_d(L)$ за $\forall d \in \mathbb{N}$. За всяко $k \in \mathbb{N}$ да забележим, че $M^{(\leq k)} := \{x \in M \mid \deg \mathrm{Orb}_{\mathfrak{G}}(x) \leq k\}$ е краен $\mathfrak{G}$-подмодул на M и локално крайният $\mathfrak{G}$-модул $M = \cup_{k=1}^{k} M^{(\leq k)}$ се изчерпва от $M^{(\leq k)}$. Ако $L^{(\leq k)} := \{y \in L \mid \deg \mathrm{Orb}_{\mathfrak{G}}(y) \leq k\}$, то с индукция по $k \in \mathbb{N}$ конструираме изоморфизми $\xi : M^{(\leq k)} \to L^{(\leq k)}$ на $\mathfrak{G}$-модули и намираме изоморфизъм на $\mathfrak{G}$-модули $\xi : M = \cup_{k=1}^{\infty} M^{(\leq k)} \to \cup_{k=1}^{\infty} L^{(\leq k)} = L$. □

Лема 121. *Ако M е локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул с ζ-функция $\zeta_M(t) \in \mathbb{Z}[[t]]$, то частното*

$$P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = \sum_{i=0}^{\infty} a_i t^i \in \mathbb{Z}[[t]]^*$$

е формален степенен ред с цели коефициенти $a_m \in \mathbb{Z}$, който е обратим в $\mathbb{Z}[[t]]$. Неговите коефициенти $a_m \in \mathbb{Z}$ изпълняват равенствата

$$\mathcal{A}_m(M) = \sum_{i=0}^{m} a_i \left|\mathbb{P}^{m-i}(\mathbb{F}_q)\right|$$

и могат да се интерпретират като "кратности" на проективните пространства $\mathbb{P}^{m-i}(\mathbb{F}_q)$, "изчерпващи" ефективните дивизори върху M от степен m.

Доказателство: Ако $P_M(t) = \sum\limits_{m=0}^{\infty} a_m t^m \in \mathbb{C}[[t]]$ е формален степенен ред с комплексни коефициенти $a_m \in \mathbb{C}$, то сравняването на коефициенти на

$$\sum_{m=0}^{\infty} a_m t^m = P_M(t) = \zeta_M(t)(1-t)(1-qt) = \left(\sum_{m=0}^{\infty} \mathcal{A}_m(M) t^m\right)[1-(q+1)t+qt^2]$$

дава

$$a_m = \mathcal{A}_m(M) - (q+1)\mathcal{A}_{m-1}(M) + q\mathcal{A}_{m-2}(M) \in \mathbb{Z} \quad \text{за} \quad \forall m \in \mathbb{Z}^{\geq 0}, \tag{6.6}$$

защото $\mathcal{A}_m(M) \in \mathbb{Z}^{\geq 0}$ за $\forall m \in \mathbb{Z}^{\geq 0}$ и $\mathcal{A}_{-1}(M) = \mathcal{A}_{-2}(M) = 0$. В частност, $a_0 = \mathcal{A}_0(M) = \zeta_M(0) = 1$ и $P_M(t) = 1 + \sum\limits_{i=1}^{\infty} a_i t^i \in \mathbb{Z}[[t]]^*$ е обратим чрез формален степенен ред $P_M^{-1}(t) = 1 + \sum\limits_{m=1}^{\infty} b_m t^m \in \mathbb{Z}[[t]]$ с цели коефициенти. (Съществуването на $b_m \in \mathbb{Z}$ с $[1 + \sum\limits_{m=1}^{\infty} a_m t^m][1 + \sum\limits_{m=1}^{\infty} b_m t^m] = 1$ следва от $b_m + \sum\limits_{i=1}^{m-1} b_i a_{m-i} + a_m = 0$ с индукция по $m \in \mathbb{N}$.)

Сравняването на коефициентите на

$$\sum_{m=0}^{\infty} \mathcal{A}_m(M) t^m = \zeta_M(t) = P_M(t)\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t) = \left(\sum_{m=0}^{\infty} a_m t^m\right)\left(\sum_{s=0}^{\infty} t^s\right)\left(\sum_{r=0}^{\infty} q^r t^r\right)$$

дава

$$\mathcal{A}_m(M) = \sum_{i=0}^{m} a_i \left(\sum_{j=0}^{m-i} q^j\right) = \sum_{i=0}^{m} a_i \left(\frac{q^{m-i+1}-1}{q-1}\right) = \sum_{i=0}^{m} a_i \left|\mathbb{P}^{m-i}(\mathbb{F}_q)\right|. \tag{6.7}$$

□

Съгласно Теоремата на Риман-Рох за дивизор D от степен $\deg D = n \geq 2g-1$ върху гладка неприводима крива $X/\mathbb{F}_q \subseteq \mathbb{P}^n(\overline{\mathbb{F}_q})$ от род $g \geq 0$, класът на линейна

еквивалентност на D е изоморфен на $\mathbb{P}^{n-g}(\mathbb{F}_q)$. За всяко $n \in \mathbb{Z}^{\geq 0}$ съществуват един и същи брой h класове на линейна еквивалентност на дивизори върху X от степен n. Естественото число $h = P_X(1)$ е равно на стойността на ζ-полинома $P_X(t) = \frac{\zeta_X(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = \sum_{j=0}^{2g} a_j t^j \in \mathbb{Z}[t]$ на X в 1 и се нарича брой на класовете на линейна еквивалентност на дивизорите върху X. За всяко естествено число $n \geq 2g-1$ съществуват

$$\mathcal{A}_n(X) = P_X(1)\left|\mathbb{P}^{n-g}(\mathbb{F}_q)\right| = P_X(1)\left(\frac{q^{n-g+1}-1}{q-1}\right)$$

ефективни дивизора върху X от степен n. Да забележим, че ζ-функцията $\zeta_X(t) = \frac{P_X(t)}{(1-t)(1-qt)}$ има резидууми $\mathrm{Res}_{\frac{1}{q}}(\zeta_X(t)) = \frac{P_X\left(\frac{1}{q}\right)}{1-q}$, $\mathrm{Res}_1(\zeta_X(t)) = \frac{P_X(1)}{q-1}$ в простите си полюси $\frac{1}{q}$, съответно, 1. ζ-полиномът $P_X(t)$ на X изпълнява функционалното уравнение $P_X(t) = P_X\left(\frac{1}{qt}\right) q^g t^{2g}$, съгласно Теорема 4.1.13 от [Niederreiter, Xing] или Теорема V.1.15 (b) от [Stichtenoth]. В частност, $P_X\left(\frac{1}{q}\right) = q^{-g} P_X(1)$ и

$$\mathcal{A}_n(X) = -q^{n+1}\mathrm{Res}_{\frac{1}{q}}(\zeta_X(t)) - \mathrm{Res}_1(\zeta_X(t)) \quad \text{за} \quad \forall n \geq 2g-1.$$

Определение 122. *Локално краен модул M над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ изпълнява общите условия на Риман-Рох, ако M има*

$$\mathcal{A}_n(M) = -q^{n+1}\mathrm{Res}_{\frac{1}{q}}(\zeta_M(t)) - \mathrm{Res}_1(\zeta_M(t))$$

ефективни дивизора от степен n за всички достатъчно големи естествени числа $n \geq n_o$.

Можем да сравним общите условия на Риман-Рох с поляризираните условия на Риман-Рох от глава 5 и глава 5, които са еквивалентни на тъждествата на Мак Уилямс за линейни кодове над крайни полета.

Следващото твърдение хороктеризира локално крайните $\mathfrak{G}$-модули M с полиномиално ζ-частно $P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} \in \mathbb{Z}[t]$.

Твърдение 123. *Следните условия са еквивалентни за ζ-функцията $\zeta_M(t)$ на локално краен модул M над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$:*

(i) $P_M(t) := \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} \in \mathbb{Z}[t]$ е полином от степен $\deg P_M(t) = d \leq \delta \in \mathbb{N}$;

(ii) M изпълнява общите условия на Риман-Рох

$$\mathcal{A}_n(M) = -q^{n+1}\mathrm{Res}_{\frac{1}{q}}(\zeta_M(t)) - \mathrm{Res}_1(\zeta_M(t)) = \frac{q^{n+1}P_M\left(\frac{1}{q}\right) - P_M(1)}{q-1} \tag{6.8}$$

за всички $n \geq \delta - 1$;

$$\text{(iii)} \quad \left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^r}\right| - \left|M^{\Phi_q^r}\right| = \sum_{j=1}^{d} \omega_j^r \quad \textit{за} \quad \forall r \in \mathbb{N} \tag{6.9}$$

за някои $\omega_j \in \mathbb{C}^*$*, за които следва, че изпълняват равенството* $P_M(t) = \prod_{j=1}^{d}(1-\omega_j t)$.

Доказателство: $(i) \Rightarrow (ii)$ Ако $P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = \sum_{j=0}^{d} a_j t^j \in \mathbb{Z}[t]$ е полином от степен $\deg P_M(t) = d \leq \delta \in \mathbb{N}$, то (6.7) се свежда до

$$\mathcal{A}_m(M) = \sum_{i=0}^{d} a_i \left(\frac{q^{m-i+1}-1}{q-1}\right) = \frac{q^{m+1}P_M\left(\frac{1}{q}\right) - P_M(1)}{q-1} \quad \text{за} \quad \forall m \geq \delta.$$

Още повече, от (6.7) получаваме

$$\mathcal{A}_{\delta-1}(M) = \frac{q^\delta\left[P_M\left(\frac{1}{q}\right) - \frac{a_\delta}{q^\delta}\right] - [P_M(1) - a_\delta]}{q-1} = \frac{q^\delta P_M\left(\frac{1}{q}\right) - P_M(1)}{q-1}.$$

Сега (6.8) следва от това, че резидуумите на $\zeta_M(t) = \frac{P_M(t)}{(1-t)(1-qt)}$ в простите полюси са $\operatorname{Res}_{\frac{1}{q}}(\zeta_M(T)) = \frac{P_M\left(\frac{1}{q}\right)}{1-q}$, съответно, $\operatorname{Res}_1(\zeta_M(t)) = \frac{P_M(1)}{q-1}$.

$(ii) \Rightarrow (i)$ Замествайки (6.8) в (6.6), намираме $a_m(M) = 0$ за $\forall m \geq \delta + 1$. Следователно $P_M(t) = \sum_{i=0}^{\delta} a_i(M) t^i \in \mathbb{Z}[t]$ е полином от степен $\deg P_M(t) \leq \delta$.

$(i) \Rightarrow (iii)$ Ако $P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} \in \mathbb{Z}[t]$ е полином от степен $\deg P_M(t) = d \leq \delta$, то $P_M(0) = \frac{\zeta_M(0)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(0)} = 1$ позволява да изразим $P_M(t) = \prod_{j=1}^{d}(1-\omega_j t)$ чрез някакви комплексни числа $\omega_j \in \mathbb{C}^*$. Съгласно Твърдение 119,

$$\zeta_M(t) = \exp\left(\sum_{r=1}^{\infty} \left|M^{\Phi_q^r}\right| \frac{t^r}{r}\right) \quad \text{и} \quad \zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t) = \exp\left(\sum_{r=1}^{\infty} \left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^r}\right| \frac{t^r}{r}\right), \tag{6.10}$$

откъдето

$$\sum_{j=1}^{d} \log(1-\omega_j t) = \log P_M(t) = \log \zeta_M(t) - \log \zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t) = \sum_{r=1}^{\infty} \left(\left|M^{\Phi_q^r}\right| - \left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^r}\right|\right) \frac{t^r}{r}.$$

Съгласно (6.4), намираме

$$-\sum_{r=1}^{\infty}\left(\sum_{j=1}^{d} \omega_j^r\right)\frac{t^r}{r} = \sum_{r=1}^{\infty}\left(\left|M^{\Phi_q^r}\right| - \left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^r}\right|\right)\frac{t^r}{r}.$$

Сравняването на коефициентите на $\frac{t^r}{r}$ за $\forall r \in \mathbb{N}$ дава (6.9).

$(iii) \Rightarrow (i)$ Умножавайки (6.9) с $\frac{t^r}{r}$, сумирайки по $\forall r \in \mathbb{N}$ и използвайки (6.4), пресмятаме $\log \zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t) - \log \zeta_M(t) = -\sum\limits_{j=1}^{d} \log(1-\omega_j t)$. Смяната на знака и прилагането на екпоненциалната функция дават $P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = \prod\limits_{j=1}^{d}(1-\omega_j t) \in \mathbb{Z}[t]$. □

Следствие 124. *Нека M и L са локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули с полиномиални ζ-частни $P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)}$, $P_L(t) = \frac{\zeta_L(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} \in \mathbb{Z}[t]$ от степен $\deg P_M(t) \leq \delta$, $\deg P_L(t) \leq \delta$. В такъв случай, M и L са изоморфни (като $\mathfrak{G}$-модули) отгава и само тогава, когато имат един и същи брой $\mathfrak{G}$-орбити $B_k(M) = B_k(L)$ от степен k за всички $1 \leq k \leq \delta$.*

Доказателство: Съгласно Следствие 120, достатъчно е да докажем, че $B_k(M) = B_k(L)$ за всички $1 \leq k \leq \delta$ е еквивалентно на съвпадението $\zeta_M(t) = \zeta_L(t)$ на съответните ζ-функции. Безкрайните произведения

$$\zeta_M(t) = \prod_{k=1}^{\infty}\left(\frac{1}{1-t^k}\right)^{B_K(M)}, \quad \zeta_L(t) = \prod_{k=1}^{\infty}\left(\frac{1}{1-t^k}\right)^{B_K(L)}$$

показват, че $\zeta_M(t) = \zeta_L(t)$ тогава и само тогава, когато $B_k(M) = B_k(L)$ за $\forall k \in \mathbb{N}$. Остава да се докаже ,че ако $\deg P_M(t) \leq \delta$, то $B_k(M)$ с $1 \leq k \leq \delta$ определят еднозначно $B_k(M)$ за $\forall k \in \mathbb{N}$. Да предположим, че $P_M(t) = \prod\limits_{j=1}^{d}(1-\omega_j t)$ за $d \leq \delta$, $\omega_j \in \mathbb{C}^*$ и да означим $S_r := \sum\limits_{j=1}^{d} \omega_j^r$ за $\forall r \in \mathbb{N}$. Съгласно (6.9) от Твърдение 123 и (6.5) от доказателството на Твърдение 119 имаме

$$S_r = (q^r+1) - \left|M^{\Phi_q^r}\right| = (q^r+1) - \sum_{k/r} kB_k(M) \quad \text{за} \quad \forall r \in \mathbb{N}. \tag{6.11}$$

По този начин, $B_k(M)$ за $1 \leq k \leq \delta$ определят еднозначно S_r за $\forall 1 \leq r \leq \delta$. Понеже $P_M(t)$ е от степен $\deg P_M(t) = d \leq \delta$, S_r за $1 \leq r \leq \delta$ определят еднозначно S_r за $\forall r \in \mathbb{N}$ по формулите на Нютон за степенните сборове. С индукция по $r \in \mathbb{N}$ и използвяйки (6.11), S_r за $r \in \mathbb{N}$ определят еднозначно $B_r(M)$ за $\forall r \in \mathbb{N}$. □

Твърдение 125. *Нека M е локално краен модул над про-крайната обвивка $\mathfrak{G} = \widehat{\langle\varphi\rangle}$ на $\langle\varphi\rangle \simeq (\mathbb{Z},+)$ и M_r е локално крайният $\mathfrak{G}_r = \widehat{\langle\varphi^r\rangle}$-модул с носител M за някое $r \in \mathbb{N}$. Тогава ζ-функциите на M и M_r са свързани с равенството*

$$\zeta_{M_r}(t^r) = \prod_{k=0}^{r-1} \zeta_M\left(e^{\frac{2\pi i k}{r}} t\right). \tag{6.12}$$

В частност, ако M има полиномиално ζ-частно

$$P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = \prod_{j=1}^{d}(1-\omega_j t)$$

от степен $\deg P_M(t) = d$, *то* M_r *има*

$$P_{M_r}(t) := \frac{\zeta_{M_r}(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})_r}(t)} = \prod_{j=1}^{d}(1-\omega_j^r t)$$

от степен $\deg P_{M_r}(t) = d$ *и* M *удовлетворяна аналога на хипотезата на Рима относно* $\mathbb{P}^1(\overline{\mathbb{F}_q})$ *като* $\mathfrak{G}$*-модул тогава и само тогава, когато* M_r *изпълнява аналога на хипотезата на Риман относно* $\mathbb{P}^1(\overline{\mathbb{F}_q})_r$ *като* $\mathfrak{G}_r$*-модул.*

Доказателство: Съгласно (1.7) от параграф V.1 на [Stichtenoth], всички $m, r \in \mathbb{N}$ с най-голям общ делител $\mathrm{GCD}(m,r) = d \in \mathbb{N}$ изпълняват равенството на полиноми

$$\left(1 - t^{r\frac{m}{d}}\right)^d = \prod_{k=0}^{r-1}\left[1 - \left(e^{\frac{2\pi i k}{r}} t\right)^m\right].$$

От Лема 117 (iii), всяка $\mathfrak{G}$-орбита ν от степен $\deg \nu = m$ се разлага в обединение на d орбити $\nu = \nu_1 \coprod \ldots \coprod \nu_d$ над $\mathfrak{G}_r$ от степен $\deg \nu_j = \frac{m}{d}$ за $\forall 1 \leq j \leq d$. Приносът на ν към

$$\left[\prod_{k=0}^{r-1} \zeta_M\left(e^{\frac{2\pi i k}{r}} t\right)\right]^{-1}$$

е

$$\prod_{k=0}^{r-1}\left[1 - \left(e^{\frac{2\pi i k}{r}} t\right)^m\right] = \left(1 - t^{r\frac{m}{d}}\right)^d = \prod_{j=1}^{d}\left(1 - t^{r\deg \nu_j}\right)$$

и е равен на приноса на $\nu_1 \coprod \ldots \coprod \nu_d$ към $\zeta_{M_r}(t^r)^{-1}$. Това доказва равенството на формални степенни редове (6.12).

За всяко $\omega \in \mathbb{C}^*$ да забележим, че

$$\prod_{k=0}^{r-1}\left(1 - e^{\frac{2\pi i k}{r}}\omega t\right) = (\omega t)^r \prod_{k=0}^{r-1}\left(\frac{1}{\omega t} - e^{\frac{2\pi i k}{r}}\right) = (\omega t)^r\left[\frac{1}{(\omega t)^r} - 1\right] = 1 - \omega^r t^r. \tag{6.13}$$

Ако $P_M(t) := \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = \prod\limits_{j=1}^{d}(1-\omega_j t) \in \mathbb{Z}[t]$ с $a_d := \mathrm{LC}(P_M(t)) = (-1)^d \omega_1 \ldots \omega_d$ за някакви $\omega_j \in \mathbb{C}^*$ и $\mathbb{P}^1(\overline{\mathbb{F}_q})_r$ е $\mathfrak{G}_r$-модулът с носител $\mathbb{P}^1(\overline{\mathbb{F}_q}) = \mathbb{P}^1(\overline{\mathbb{F}_{q^r}})$, то (6.12) и (6.13) дават

$$P_{M_r}(t^r) = \frac{\zeta_{M_r}(t^r)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})_r}(t^r)} = \prod_{k=0}^{r-1}\frac{\zeta_M\left(e^{\frac{2\pi i k}{r}} t\right)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}\left(e^{\frac{2\pi i k}{r}} t\right)} = \prod_{k=0}^{r-1} P_M\left(e^{\frac{2\pi i k}{r}} t\right) =$$

$$= \prod_{k=0}^{r-1}\prod_{j=1}^{d}\left(1 - \omega_j e^{\frac{2\pi i k}{r}} t\right) = \prod_{j=1}^{d}\prod_{k=0}^{r-1}\left(1 - \omega_j e^{\frac{2\pi i k}{r}} t\right) = \prod_{j=1}^{d}\left(1 - \omega_j^r t^r\right).$$

Следователно $P_{M_r}(t) = \prod_{j=1}^{d}(1-\omega_j^r t)$ е полином от степен $\deg P_{M_r}(t) = d \in \mathbb{N}$ с $|\mathrm{LC}(P_{M_r}(t))| = |\omega_1 \dots \omega_d|^r = |a_d|^r$ и $|\omega_j| = \sqrt[d]{|a_d|}$ тогава и само тогава, когато $\left|\omega_j^r\right| = \sqrt[d]{|\mathrm{LC}(P_{M_r}(t))|}$. Това доказва еквивалентността на аналога на хипотезата на Риман за M и M_r относно проективната права, когато M има полиномиално ζ-частно $P_M(t)$. $\square$

6.3 Крайни неразклонени покрития на локално крайни модули

Обобщавайки някои свойства на крайнтие неразклонени покрития $f : X \to Y$ на квази-проективни криви X, Y или топологични пространства X, Y, въвеждаме понятието крайно неразклонено покритие на локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули.

Определение 126. *Сюрективен морфизъм $\xi : M \to L$ на $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули е неразклонено покритие от степен $\deg \xi = k$, ако всички слоеве $\xi^{-1}(x)$, $x \in L$ на ξ се състоят от един и същи брой точки $\left|\xi^{-1}(x)\right| = k$.*

Инерционното ицображение $e_\xi : M \to \mathbb{N}$ на неразклонено покритие $\xi : M \to L$ от степен $\deg \xi = k$ взема стойности в множеството $\{1, \dots, k\}$. Това следва от Твърдение-Определение 118 (iii), съгласно което

$$\xi^{-1}(x) = \coprod_{y \in S_x} \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y) \quad \text{за} \quad \forall x \in M, \quad \delta(x) = \deg \mathrm{Orb}_{\mathfrak{G}}(x), \quad \deg \mathrm{Orb}_{\mathfrak{G}_{\delta(x)}}(y) = e_\xi(y),$$

откъдето

$$k = \left|\xi^{-1}(x)\right| = \sum_{y \in S_x} e_\xi(y)$$

с $e_\xi(y) \in \mathbb{N}$.

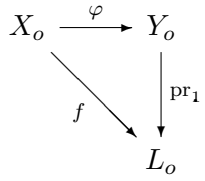
Следващото твърдение установява, че произволна неприводима квази-проективна крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ от род $g \geq 1$ съдържа локално краен $\mathfrak{G}_m = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$-подмодул X_o с най-много крайно допълнение $X \setminus X_o$, който има крайно неразклонено покритие $f : X_o \to f(X_o)$ върху $\mathfrak{G}_m$-подмодул $f(X_o) \subseteq \mathbb{P}^1(\overline{\mathbb{F}_q})$ с $\left|\mathbb{P}^1(\overline{\mathbb{F}_q}) \setminus f(X_o)\right| < \infty$ за някое $m \in \mathbb{N}$.

Твърдение 127. *За всяка неприводима квази-проективна крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ от положителен род съществува $m \in \mathbb{N}$ и локално крайни $\mathfrak{G}_m = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$-подмодули $X_o \subseteq X \cap \overline{\mathbb{F}_q}^n \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, $L_o \subseteq \overline{\mathbb{F}_q} \subset \mathbb{P}^1(\overline{\mathbb{F}_q})$ с най-много крайни допълнения $X \setminus X_o$, $\mathbb{P}^1(\overline{\mathbb{F}_q}) \setminus L_o$, свързани с крайно неразклонено покритие $f : X_o \to L_o$ на $\mathfrak{G}_m$-модули и квази-афинни криви, което индуцира тъждественото влагане*

$$f^* = \mathrm{Id} : \overline{\mathbb{F}_q}(L_o) = \overline{\mathbb{F}_q}(\mathbb{P}^1(\overline{\mathbb{F}_q})) \hookrightarrow \overline{\mathbb{F}_q}(X) = \overline{\mathbb{F}_q}(X_o)$$

на съответните функционални полета. Още повече, съществува равнинна квази-афинна крива $Y_o \subset \overline{\mathbb{F}_q}^2$, която е локално краен $\mathfrak{G}_m$-модул, както и изоморфизъм

$\varphi : X_o \to Y_o$ на квази-афинни криви и $\mathfrak{G}_m$-модули, така че f се пропуска през φ и първата канонична проекция $\mathrm{pr}_1 : Y_o \to L_o$, $\mathrm{pr}_1(u_o, v_o) = u_o$ за $\forall (u_o, v_o) \in Y_o$ по протежение на комутативната диаграма



Доказателство: Съгласно Твърдение 1 от § 4 на Алгебричните предварителни сведения от [Shafarevich], съществуват такива пораждащи u, v на функционалното поле $\overline{\mathbb{F}_q}(X) = \overline{\mathbb{F}_q}(u, v)$ на X над $\overline{\mathbb{F}_q}$, че u е трансцендентен над $\overline{\mathbb{F}_q}$, а v е сепарабелен над $\overline{\mathbb{F}_q}(u)$. Ако

$$\widetilde{g}(x) = \sum_{i=0}^{d} \frac{\alpha_i(u)}{\beta_i(u)} x^i \in \overline{\mathbb{F}_q}(u)[x]$$

с $\alpha_i(u), \beta_i(u) \in \overline{\mathbb{F}_q}[u]$, $\alpha_d(u) = \beta_d(u) \equiv 1$ е минималният полином на v над $\overline{\mathbb{F}_q}(u)$ и $q(u) \in \overline{\mathbb{F}_q}[u]$ е най-малкото общо кратно на знаменателите $\beta_i(u)$ на коефициентите на $\widetilde{g}(x)$, то

$$q(u)\widetilde{g}(x) = \sum_{i=0}^{d} \frac{q(u)\alpha_i(u)}{\beta_i(u)} x^i \in \overline{\mathbb{F}_q}[u, x]$$

е полином на две променливи u, x от положителна степен $k := \deg_x(g(u, x)) \in \mathbb{N}$ относно x. След разделяне на най-големия общ делител на коефициентите

$$\frac{q(u)\alpha_i(u)}{\beta_i(u)} \in \overline{\mathbb{F}_q}[u], \quad 0 \le i \le d$$

на $q(u)\widetilde{g}(x)$, намираме примитивен и неприводим полином $g(u, x) \in \overline{\mathbb{F}_q}[u, x]$. Афинната крива

$$Y := Z(g(u, x)) = \{(u_o, v_o) \in \overline{\mathbb{F}_q}^2 \mid g(u_o, v_o) = 0\}$$

има функционално поле $\overline{\mathbb{F}_q}(Y) = \overline{\mathbb{F}_q}(u, v) = \overline{\mathbb{F}_q}(X)$. Това е достатъчно за съществуването на бирационално изображение $\varphi : X \dashrightarrow Y$, индуциращо тъждественото влагане

$$\varphi^* = \mathrm{Id} : \overline{Y} = \overline{\mathbb{F}_q}(u, v) \to \overline{\mathbb{F}_q}(u, v) = \overline{\mathbb{F}_q}(X)$$

на $\overline{\mathbb{F}_q}$-алгебри. С други думи, съществуват квази-афинни криви $X_1 \subseteq X$, $X_1 \subseteq \overline{\mathbb{F}_q}^n$, съответно $Y_1 \subseteq Y \subset \overline{\mathbb{F}_q}^2$ с изоморфизъм $\varphi : X_1 \to Y_1$ на квази-афинни многообразия. За всяко $1 \le j \le 2$ нека $\mathrm{pr}_j : \overline{\mathbb{F}_q}^2 \to \overline{\mathbb{F}_q}$, $\mathrm{pr}_j(x_1, x_2) = x_j$ е каноничната проекция върху j-тата компонента. Тогава

$$\varphi_j := \mathrm{pr}_j \varphi : X_1 \longrightarrow \overline{\mathbb{F}_q}, \quad 1 \le j \le 2$$

са регулярни функции върху X_1 и съществуват такива полиноми

$$g_j(x_1, \ldots, x_n), h_j(x_1, \ldots, x_n) \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n],$$

че

$$\varphi_j\Big|_{X_1} = \frac{g_j(x_1,\ldots,x_n)}{h_j(x_1,\ldots,x_n)}\Big|_{X_1},$$

след замяна на X_1 с достатъчно малка Зариски отворена околност. Собствените Зариски затворени подмножества на крива са крайните множества, така че $|X\setminus X_1|<\infty$, $|Y\setminus Y_1|<\infty$. Ако $Y\setminus Y_1=\{y_1,\ldots,y_s\}$, то $Y_2:=Y\setminus \mathrm{pr}_1^{-1}\{\mathrm{pr}_1(y_1),\ldots,\mathrm{pr}_1(y_s)\}\subseteq Y_1$ а е квази-афинна крива, върху която слоевете

$$\mathrm{pr}_1^{-1}(u_o)=\{(u_o,v_o)\in\overline{\mathbb{F}_q}^2\,|\,g(u_o,v_o)=0\}\simeq\{v_o\in\overline{\mathbb{F}_q}\,|\,g(u_o,v_o)=0\}$$

на $\mathrm{pr}_1: Y_2\to\mathrm{pr}_1(Y_2)$ съвпадат със съответните слоеве на $\mathrm{pr}_1: Y\to\overline{\mathbb{F}_q}$ и се състоят от $\left|\mathrm{pr}_1^{-1}(u_o)\right|\leq k$ точки. Да забележим, че $X_2:=\varphi^{-1}(Y_2)$ е квази-афинна крива, $|X_1\setminus X_2|<\infty$, $|Y_1\setminus Y_2|<\infty$ и $\varphi: X_2\to Y_2$ е изоморфизъм на квази-афинни криви. Дискриминантата $D_x(g)\in\overline{\mathbb{F}_q}[u]$ на $g(u,x)$ относно x е полином на u и има краен брой корени $Z(D_x(g))\subset\mathrm{pr}_1(Y_2)$. Всички слоеве на

$$\mathrm{pr}_1: Y_o=Y_1\setminus\mathrm{pr}_1^{-1}(Z(D_x(g)))\longrightarrow\overline{\mathbb{F}_q}$$

се състоят от k точки и $\varphi: X_o=\varphi^{-1}(Y_o)\to Y_o$ е изоморфизъм на квази-афинни многообразия с $|X_1\setminus X_o|<\infty$, $|Y_1\setminus Y_o|<\infty$. Ако $X_o=Z(g_1',\ldots,g_s')\setminus Z(h_1',\ldots,h_r')$ се състои от общите нули на полиномите $g_i'(x_1,\ldots,x_n)\in\overline{\mathbb{F}_q}[x_1,\ldots,x_n]$, които не са общи нули на $h_1'(x_1,\ldots,x_n),\ldots,h_r'(x_1,\ldots,x_n)\in\overline{\mathbb{F}_q}[x_1,\ldots,x_n]$, то минималното крайно разширение $\mathbb{F}_{q^\mu}\supseteq\mathbb{F}_q$, което съдържа коефициентите на всички $g_i'(x_1,\ldots,x_n), h_j'(x_1,\ldots,x_n)$ се нарича дефиниционно поле на X_o. Непосредствено се вижда, че за всяко разширение $\mathbb{F}_{q^s}\supseteq\mathbb{F}_{q^\mu}$ квази-афинната крива X_o е локално краен $\mathfrak{G}_s=Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^s})$-модул. Минималното крайно разширение $\mathbb{F}_{q^\nu}\supseteq\mathbb{F}_q$, съдържащо коефициентите на числителите $g_j(x_1,\ldots,x_n)\in\overline{\mathbb{F}_q}[x_1,\ldots,x_n]$ и знаменателите $h_j(x_1,\ldots,x_n)\in\overline{\mathbb{F}_q}[x_1,\ldots,x_n]$ на компонентите φ_j на $\varphi=(\varphi_1,\varphi_2): X_o\to Y_o\subset\overline{\mathbb{F}_q}^2$ се нарича дефиниционно поле на φ. Избираме такова $m\in\mathbb{N}$, че $\mathbb{F}_{q^m}$ съдържа дефиниционните полета на X_2, Y_2, φ и забелязваме, че $\varphi: X_2\to Y_2$ е изоморфизъм на локално крайни $\mathfrak{G}_m=Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$-модули.

Още повече, $L_o:=\mathrm{pr}_1(Y_o)\subseteq\overline{\mathbb{F}_q}\subset\mathbb{P}^1(\overline{\mathbb{F}_q})$ е квази-афинна крива, защото $\left|\overline{\mathbb{F}_q}\setminus L_o\right|<\infty$ и $\mathrm{pr}_1: Y_o\to L_o$ е неразклонено покритие на крази-афинни многообразия. Ако $\mathbb{F}_{q^m}$ съдържа дефиниционното поле на L_o, то $\mathrm{pr}_1: Y_o\to L_o$ е крайно неразклонено покритие на локално крайни $\mathfrak{G}_m$-модули от степен k. Полагаме $f:=\mathrm{pr}_1\varphi: X_o\to L_o$ и забелязваме, че в горните означения $f: X_o\to L_o$ е крайно неразклонено покритие на локално крайни $\mathfrak{G}_m$-модули и квази-афинни многообразия, индуциращо тъждественото влагане

$$f^*=\varphi^*\mathrm{pr}_1^*=\mathrm{pr}_1^*:\overline{\mathbb{F}_q}(L_o)=\overline{\mathbb{F}_q}(u)\hookrightarrow\overline{\mathbb{F}_q}(u,v)=\overline{\mathbb{F}_q}(X_o).$$

□

Автоморфизъм α на $\mathfrak{G}$-модул M е $\mathfrak{G}$-модулен изоморфизъм $\alpha: M\to M$ на M със себе си. Означаваме с $\mathrm{Aut}_{\mathfrak{G}}(M)$ групата на автоморфизмите на M. Понеже $\mathfrak{G}$ е

абелева група, всяко $\varphi \in \mathfrak{G}$ индуцира автоморфизъм $\varphi : M \to M$. По този начин възниква хомоморфизъм на групи $\Psi : \mathfrak{G} \to \mathrm{Aut}_{\mathfrak{G}}(M)$. Ако Ψ е инективно, $\mathfrak{G}$-модулът M се нарича точен и $\mathfrak{G}$ се отъждествява с $\Psi(\mathfrak{G}) \leq \mathrm{Aut}_{\mathfrak{G}}(M)$.

Лема 128. *Локално краен модул M над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ със затворени стабилизатори е точен тогава и само тогава, когато M е безкрайно множество.*

Доказателство: От определението на хомоморфизма $\Psi : \mathfrak{G} \to \mathrm{Aut}_{\mathfrak{G}}(M)$ се вижда, че ядрото му

$$\ker \Psi = \cap_{x \in M} \mathrm{Stab}_{\mathfrak{G}}(x)$$

е сечението на стабилизаторите на всички точки на M. В доказателството на Лема 117 (iii) установихме, че $\mathfrak{G}_m \cap \mathfrak{G}_n = \mathfrak{G}_{\mathrm{LCM}(m,n)}$. Ако $M = \{x_1, \ldots, x_r\}$ е крайно множество, то изображението $\deg \mathrm{Orb}_{\mathfrak{G}} : M \to \mathbb{N}$ взема краен брой стойности $m_1, \ldots, m_\nu$, $\nu \leq r$. В резултат, $\ker \Psi = \cap_{j=1}^{\nu} \mathfrak{G}_{m_j} = \mathfrak{G}_{\mathrm{LCM}(m_j \,|\, 1 \leq j \leq \nu)} \neq \{0\}$ и M не е точен $\mathfrak{G}$-модул.

Да предположим, че M е безкраен локално краен $\mathfrak{G}$-модул и

$$\alpha = (\Phi_q^{l_s (\mathrm{mod}\, s)})_{s \in \mathbb{N}} \in \ker \Psi = \cap_{x \in M} \mathrm{Stab}_{\mathfrak{G}}(x) =$$
$$= \cap_{x \in M} \mathfrak{G}_{\deg \mathrm{Orb}_{\mathfrak{G}}(x)} = \cap_{x \in M} \left\{ \Phi_q^{\deg \mathrm{Orb}_{\mathfrak{G}}(x) m_s (\mathrm{mod}\, s)} \right\}_{s \in \mathbb{N}}.$$

Тогава за всяка точка $x \in M$ и всяко $s \in \mathbb{N}$ степента $\deg \mathrm{Orb}_{\mathfrak{G}}(x)$ на $\mathfrak{G}$-орбитата на x дели l_s. За безкраен локално краен $\mathfrak{G}$-модул M изображението $\deg \mathrm{Orb}_{\mathfrak{G}} : M \to \mathbb{N}$ има безкраен образ, така че всяко l_s се дели на безбройно много различни естествени числа $\deg \mathrm{Orb}_{\mathfrak{G}}(x)$, $x \in M$. Това изисква $l_s = 0$ за $\forall s \in \mathbb{N}$, откъдето $\ker \Psi = \{0\}$. По този начин, всеки безкраен локално краен $\mathfrak{G}$-модул M е точен. □

Определение 129. *Ако $\xi : M \to L$ е крайно неразклонено покритие на локално крайни $\mathfrak{G}$-модули, то автоморфизмите на $\mathfrak{G}$-модули $\alpha : M \to M$ без фиксирани точки с $\xi\alpha = \xi$ се наричат послойни трансформации на ξ.*

Всяка подгрупа H на $\mathrm{Aut}_{\mathfrak{G}}(M)$ без фиксирани точки върху M, която се състои от послойни трансформации на $\xi : M \to L$ се нарича група от послойни трансформации на ξ.

Да забележим, че автоморфизъм $\alpha : M \to M$ на локално краен $\mathfrak{G}$-модул M и крайно неразклонено покритие $\xi : M \to L$ на $\mathfrak{G}$-модули изпълняват равенството $\xi\alpha = \xi$ тогава и само тогава, когато α се ограничава до взаимно еднозначно изображение $\alpha : \xi^{-1}(x) \to \xi^{-1}(x)$ на всеки слой $\xi^{-1}(x)$, $x \in L$ на ξ върху себе си. По-точно, $y \in \xi^{-1}(x)$ се изобразява в $\alpha(y) \in \xi^{-1}(x)$ точно когато $\xi\alpha(y) = x = \xi(y)$. Затова, за всяка група от послойни трансформации H на $\xi : M \to L$ и за всяка точка $x \in L$ възниква хомоморфизъм на групи

$$\Psi_x : H \to \mathrm{Sym}(\xi^{-1}(x)) = \mathrm{Sym}(k),$$

където $k = \deg(\xi)$. Поради липсата на фиксирани точки на H, Ψ_x са инективни и H е крайна група, чиито орбити върху $\xi^{-1}(x)$ са с един и същи брой елементи $|H| \leq k!$. В частност, H действа транзитивно върху някой слой $\xi^{-1}(x_o)$, $x_o \in L$ на крайно неразклонено покритие $\xi : M \to L$ точно когато $|H| = k = \deg(\xi)$. Ако това е в сила, то H действа транзитивно върху всички слоеве $\xi^{-1}(x)$, $x \in L$ на ξ.

Определение 130. *Крайно неразклонено покритие $\xi : M \to L$ на локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули е H-Галоа, ако съществува група от послойни трансформации $H < \mathrm{Aut}_{\mathfrak{G}}(M)$, действаща транзитивно върху един, а оттам и всеки един слой $\xi^{-1}(x)$, $x \in L$ наξ.*

Твърдение 131. *В означенията от Твърдение 127, групата на Галоа*

$$H = Gal(\overline{\mathbb{F}_q}(X)/\overline{\mathbb{F}_q}(\mathbb{P}^1(\overline{\mathbb{F}_q})))$$

на крайното сепарабелно разширение на полета $\overline{\mathbb{F}_q}(\mathbb{P}^1(\overline{\mathbb{F}_q})) \subset \overline{\mathbb{F}_q}(X)$ е група от послойни трансформации на крайното неразклонено покритие $f = \mathrm{pr}_1\varphi : X_o \to L_o$ на локално крайни $\mathfrak{G}_m = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$-модули. Ако $\overline{\mathbb{F}_q}(\mathbb{P}^1(\overline{\mathbb{F}_q})) \subset \overline{\mathbb{F}_q}(X)$ е разширение на Галоа, то $f = \mathrm{pr}_1\varphi : X_o \to L_o$ е H-Галоа покритие . Ако $f = \mathrm{pr}_1\varphi : X_o \to L_o$ има група от послойни трансформации H, която се състои от бирационални изображения $h : X_o \dashrightarrow X_o$ и действа транзитивно върху слоевете на $f : X_o \to L_o$, то крайното сепарабелно разширение на функционални полета $\overline{\mathbb{F}_q}(\mathbb{P}^1(\overline{\mathbb{F}_q})) \subset \overline{\mathbb{F}_q}(X)$ е Галоа и

$$H \simeq Gal(\overline{\mathbb{F}_q}(X)/\overline{\mathbb{F}_q}(\mathbb{P}^1(\overline{\mathbb{F}_q}))).$$

Доказателство: Понеже $\varphi : X_o \to Y_o$ е изоморфизъм на локално крайни $\mathfrak{G}_m$-модули, което индуцира тъждественото изображение

$$\varphi^* = \mathrm{Id} : \overline{\mathbb{F}_q}(Y_o) = \overline{\mathbb{F}_q}(u, v) \to \overline{\mathbb{F}_q}(X_o) = \overline{\mathbb{F}_q}(X)$$

на съответните функционални полета, достатъчно е да докажем съответните твърдения за $\mathrm{pr}_1 : Y_o \to L_o$. По-точно, твърдим, че

$$H = Gal(\overline{\mathbb{F}_q}(Y_o)/\overline{\mathbb{F}_q}(L_o)) \quad \text{с} \quad \overline{\mathbb{F}_q}(\mathbb{P}^1(\overline{\mathbb{F}_q})) = \overline{\mathbb{F}_q}(L_o) = \overline{\mathbb{F}_q}(u)$$

е група от послойни трансформации на крайното неразклонено покритие

$$\mathrm{pr}_1 : Y_o \longrightarrow L_o$$

на локално крайни $\mathfrak{G}_m$-модули. Ако $\overline{\mathbb{F}_q}(u) \subset \overline{\mathbb{F}_q}(u, v)$ е разширение на Галоа, то $\mathrm{pr}_1 : Y_o \to L_o$ е покритие на Галоа. Когато $\mathrm{pr}_1 : Y_o \to L_o$ има група от послойни трансформации H, която се състои от бирационални изображения $h : Y_o \dashrightarrow Y_o$ и действа транзитивно върху слоевете на $\mathrm{pr}_1 : Y_o \to L_o$, то крайното сепарабелно разширение $\overline{\mathbb{F}_q}(u) \subset \overline{\mathbb{F}_q}(u, v)$ на функционалните полета е разширение на Галоа.

Да забележим, че за всяко фиксирано $u_o \in L_o$ групата на Галоа

$$H = Gal(\overline{\mathbb{F}_q}(u, v)/\overline{\mathbb{F}_q}(u))$$

действа без фиксирани точки върху слоя $\mathrm{pr}_1^{-1}(u_o) = \{(u_o, v_o) \in \overline{\mathbb{F}_q}^2 \mid g(u_o, v_o) = 0\}$ на проекцията $\mathrm{pr}_1 : Y_o \to L_o$. Това позволява да разглеждаме H като подгрупа на симетричната група $\mathrm{Sym}(Y_o)$ на Y_o без фиксираните точки. Ако $\deg_x g(u, x) = k$, то $\overline{\mathbb{F}_q}(u, v)$ е k-мерно линейно пространство над $\overline{\mathbb{F}_q}(u)$ с базис $1, v, \ldots, v^{k-1}$. Автоморфизмът на Фробениус $\Phi_{q^m} : \overline{\mathbb{F}_q}(u, v) \to \overline{\mathbb{F}_q}(u, v)$ действа върху коефициентите на рационалните

функции $\frac{g_1(u)}{g_2(u)} \in \overline{\mathbb{F}_q}(u)$ с $g_1(u), g_2(u) \in \overline{\mathbb{F}_q}[u]$, $g_2(u) \not\equiv 0$ и фиксира v^i за $\forall 0 \leq i \leq k-1$. По определение, всяко $h \in H = Gal(\overline{\mathbb{F}_q}(u,v)/\overline{\mathbb{F}_q}(u))$ действа тъждествено върху $\overline{\mathbb{F}_q}(u)$ и индуцира пермутация на корените $x_i \in \overline{\mathbb{F}_q}$ на $g(u,x) = 0$. Затова $h\Phi_{q^m} = \Phi_{q^m}h$ е автоморфизъм на функционалното поле $\overline{\mathbb{F}_q}(u,v) = \overline{\mathbb{F}_q}(Y_o)$ и на афинния координатен пръстен

$$\overline{\mathbb{F}_q}[Y_o] = \overline{\mathbb{F}_q}[u,x]/\langle g(u,x)\rangle = \overline{\mathbb{F}_q}[u,v] = \overline{\mathbb{F}_q}[u] + \overline{\mathbb{F}_q}[u]v + \ldots + \overline{\mathbb{F}_q}[u]v^{k-1}$$

на Y_o. Афинната обвивка $Y = Z(g(u,x)) \subset \overline{\mathbb{F}_q}^2$ of Y_o в $\overline{\mathbb{F}_q}^2$ има същия афинен координатен пръстен $\overline{\mathbb{F}_q}[Y] = \overline{\mathbb{F}_q}[Y_o]$ като Y_o. Автоморфизмите на $\overline{\mathbb{F}_q}[Y]$ като $\overline{\mathbb{F}_q}$-алгебра са във взаимно еднозначно съответствие с автоморфизмите $Y \to Y$ на афинната крива Y с $h\Phi_{q^m} = \Phi_{q^m}h$ съвпадат с автоморфизмите на Y. Съгласно избора на $m \in \mathbb{N}$, квази-афинната крива Y_o е Φ_{q^m}-инвариантна. Възоснова на $Y_o = Y \setminus \mathrm{pr}_1^{-1}\{u_1, \ldots, u_r\}$ за някои $u_1, \ldots, u_r \in \overline{\mathbb{F}_q}$, слоевете на $\mathrm{pr}_1 : Y_o \to \mathrm{pr}_1(Y_o)$ съвпадат със слоевете на $\mathrm{pr}_1 : Y \to \overline{\mathbb{F}_q}$ над $\mathrm{pr}_1(Y_o)$. Понеже h действа върху слоевете на $\mathrm{pr}_1 : Y \to \overline{\mathbb{F}_q}$ без фиксирани точки, кривата Y_o се запазва от h и $h\Phi_{q^m} = \Phi_{q^m}h$ съвпадат като автоморфизми на Y_o. По този начин доказваме, че H е група от послойни трансформации на неразклоненото покритие $\mathrm{pr}_1 : Y_o \to L_o$ на $\mathfrak{G}_m$-модули.

Ако крайното сепарабелно разширение $\overline{\mathbb{F}_q}(u) \subset \overline{\mathbb{F}_q}(u,v)$ е нормално, т.е. крайно разширение на Галоа, то неговата група на Галоа е

$$H = Gal(\overline{\mathbb{F}_q}(u,v)/\overline{\mathbb{F}_q}(u))$$

от ред

$$|H| = [\overline{\mathbb{F}_q}(u,v) : \overline{\mathbb{F}_q}(u)] = \deg_x g(u,x) = k = \deg(\mathrm{pr}_1).$$

Следователно H действа транзитивно върху слоевете на $\mathrm{pr}_1 : Y_o \to L_o$ и $\mathrm{pr}_1 : Y_o \to L_o$ е H-Галоа покритие на локално крайни $\mathfrak{G}_m$-модули.

Нека H е група от послойни трансформации на $\mathrm{pr}_1 : Y_o \to L_o$, която се състои от бирационални изображения $h : Y_o \dashrightarrow Y_o$ и действа транзитивно върху слоевете на pr_1. След замяна на Y_o чрез непрзано Зариски отворено подмножество $Y_1 \subseteq Y_o$, можем да предполагаме, че всички $h \in H$ са инективни морфизми $h : Y_1 \to Y_o$. Всяко такова $h = (h_1, h_2)$ е двойка от регулярни функции $h_i : Y_1 \to \overline{\mathbb{F}_q}$, $1 \leq i \leq 2$. Равенството $\mathrm{pr}_1 h = \mathrm{pr}_1$ за $\forall h = (h_1, h_2)$ е еквивалентно на $h_1(u,v) = u$, така че $h_1 = \mathrm{pr}_1$. Всяко бирационално изображение $h : Y_o \to Y_o$ индуцира изоморфизъм $h^* : \overline{\mathbb{F}_q}(Y_o) = \overline{\mathbb{F}_q}(u,v) \to \overline{\mathbb{F}_q}(u,v) = \overline{\mathbb{F}_q}(Y_o)$ на $\overline{\mathbb{F}_q}$-алгебри. Съгласно $u = \mathrm{pr}_1(u,v)$ имаме $h^*(u) = h^*(\mathrm{pr}_1)(u,v) = \mathrm{pr}_1 h(u,v) = h_1(u,v) = u$ за $\forall h \in H$. Още повече, h^* действа тъждествено върху полето от константи $\overline{\mathbb{F}_q}$ и следователно, фиксира елементите на $\overline{\mathbb{F}_q}(u)$. Това позволява разглеждането на $h^* \in Gal(\overline{\mathbb{F}_q}(u,v)/\overline{\mathbb{F}_q}(u))$ като елемент на групата на Галоа на крайното сепарабелно покритие $\overline{\mathbb{F}_q}(u) \subset \overline{\mathbb{F}_q}(u,v)$. Групата H, действаща транзитивно върху слоевете на $\mathrm{pr}_1 : Y_o \to L_o$ е от ред

$$|H| = \deg(\mathrm{pr}_1) = k = \deg_x g(u,x) = [\overline{\mathbb{F}_q}(u,v) : \overline{\mathbb{F}_q}(u)]$$

и $\overline{\mathbb{F}_q}(u) \subset \overline{\mathbb{F}_q}(u,v)$ е разширение на Галоа. □

Да забележим, че в общия случай, ако крайните покрития $\mathrm{pr}_1 : Y_o \to L_o$, $f = \mathrm{pr}_1\varphi : X_o \to L_o$ на локално крайни $\mathfrak{G}_m$-модули е H-Галоа за някоя група от послойни трансформации H на pr_1 и f, то крайното сепарабелно разширение

$$\overline{\mathbb{F}_q}(L_o) = \overline{\mathbb{F}_q}(u) \subset \overline{\mathbb{F}_q}(u,v) = \overline{\mathbb{F}_q}(Y_o) = \overline{\mathbb{F}_q}(X_o)$$

може да не е разширение на Галоа. Причина за това е, че автоморфизмите $h \in H$ на $\mathfrak{G}_m$-модули Y_o, X_o не са непременно бирационални изображения на Y_o, X_o.

Нека $\xi : M \to L$ е крайно неразклонено покритие на локално крайни $\mathfrak{G}$-модули. Тогава всяка група H от послойни трансформации на ξ е крайна подгрупа без фиксирани точки на групата $\mathrm{Aut}_{\mathfrak{G}}(M)$ на автоморфизмите на M. Следващата лема установява, че множеството на орбитите $\mathrm{Orb}_H(M)$ на произволна крайна подгрупа $H < \mathrm{Aut}_{\mathfrak{G}}(M)$ без фиксирани точки има естествена структура на локално краен $\mathfrak{G}$-модул, относно която изображението $\xi_H : M \to \mathrm{Orb}_H(M)$, $\xi_H(x) = \mathrm{Orb}_H(x)$, съпоставящо на точка $x \in M$ нейната H-орбита $\mathrm{Orb}_H(x)$ е H-Галоа покритие.

Лема 132. *Нека M е безкраен локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул със затворени стабилизатори и H е крайна подгрупа на $\mathrm{Aut}_{\mathfrak{G}}(M)$ без фиксирани точки. Тогава:*

(i) произведението $H\mathfrak{G} \simeq H \times \mathfrak{G}$ на подгрупите H и $\mathfrak{G}$ на $\mathrm{Aut}_{\mathfrak{G}}(M)$ е директно;

(ii) множеството $\mathrm{Orb}_H(M) = \{\mathrm{Orb}_H(x) \,|\, x \in M\}$ на H-орбитите върху M е локално краен $\mathfrak{G}$-модул относно действието

$$\begin{aligned} \mathfrak{G} \times \mathrm{Orb}_H(M) &\longrightarrow \mathrm{Orb}_H(M), \\ (\varphi, \mathrm{Orb}_H(x)) \mapsto \varphi\mathrm{Orb}_H(x) = \mathrm{Orb}_H\varphi(x) \quad &\textit{за} \quad \forall\varphi \in \mathfrak{G}, \quad \forall x \in M; \end{aligned} \tag{6.14}$$

(iii) съответствието

$$\xi_H : M \to \mathrm{Orb}_H(M), \quad \xi_H(x) = \mathrm{Orb}_H(x) \quad \textit{for} \quad \forall x \in M$$

е крайно неразклонено H-Галоа покритие от степен $\deg \xi_H = |H|$.

Доказателство: (i) Съгласно Лема 128, безкрайният локално краен $\mathfrak{G}$-модул M е точен и можем да разглеждаме $\mathfrak{G}$ като подгрупа на $\mathrm{Aut}_{\mathfrak{G}}(M)$. По определение, $\mathrm{Aut}_{\mathfrak{G}}(M)$ централизира $\mathfrak{G}$. В частност, $h\varphi = \varphi h$ за $\forall h \in H$ и $\forall \varphi \in \mathfrak{G}$. Изоморфизмът

$$\mathfrak{G} \simeq (\widehat{\mathbb{Z}}, +) \simeq \prod_{\text{prime } p} (\widehat{\mathbb{Z}}_p, +)$$

с директното произведение на адитивните групи $(\widehat{\mathbb{Z}}_p, +)$ на целите p-адични числа показва, че всяко $\varphi \in \widehat{\mathbb{Z}} \setminus \{0\}$ е от безкраен ред. Понеже всеки елемент h на крайната група H е от краен ред в $\mathrm{Aut}_{\mathfrak{G}}(M)$, следва че $H \cap \mathfrak{G} = \{\mathrm{Id}_M\}$ и произведението $H\mathfrak{G} \simeq H \times \mathfrak{G}$ на подгрупи на $\mathrm{Aut}_{\mathfrak{G}}(M)$ е директно.

(ii) Да забележим, че изображението (6.14) е коректно определено, защото за $\forall x \in M$, $\forall \varphi \in \mathfrak{G}$, $\forall h \in H$ е изпълнено

$$\varphi\mathrm{Orb}_H(hx) = \mathrm{Orb}_H(\varphi h(x)) = \mathrm{Orb}_H(h\varphi(x)) = \mathrm{Orb}_H(\varphi(x)) = \varphi\mathrm{Orb}_H(x).$$

Аксиомите за $\mathfrak{G}$-действие върху $\mathrm{Orb}_H(M)$ следват от тези за действието на $\mathfrak{G}$ върху M. Понеже H централизира $\mathfrak{G}$, $\mathfrak{G}$-орбитите

$$\mathrm{Orb}_{\mathfrak{G}}\xi_H(x) = \mathrm{Orb}_{\mathfrak{G}}\mathrm{Orb}_H(x) = \mathrm{Orb}_H\mathrm{Orb}_{\mathfrak{G}}(x) = \xi_H\mathrm{Orb}_{\mathfrak{G}}(x)$$

върху $\mathrm{Orb}_H(M)$ са образи на $\mathfrak{G}$-орбити върху M под действие на ξ_H и $\deg \mathrm{Orb}_{\mathfrak{G}}\xi_H(x) < \infty$ за $\forall x \in M$. Ако $\deg \mathrm{Orb}_{\mathfrak{G}}\xi_H(x) = |\xi_H\mathrm{Orb}_{\mathfrak{G}}(x)| = m$, то ограничението

$$\xi_H|_{\mathrm{Orb}_{\mathfrak{G}}(x)} : \mathrm{Orb}_{\mathfrak{G}}(x) \to \mathrm{Orb}_{\mathfrak{G}}\xi_H(x)$$

на $\xi_H : M \to \mathrm{Orb}_H(M)$ е от степен

$$\deg(\xi_H|_{\mathrm{Orb}_{\mathfrak{G}}(x)}) \leq \deg(\xi_H) = |H|,$$

така че

$$\deg \mathrm{Orb}_{\mathfrak{G}}(x) = \deg(\xi_H|_{\mathrm{Orb}_{\mathfrak{G}}(x)}) \deg \mathrm{Orb}_{\mathfrak{G}}\xi_H(x) \leq m|H|.$$

По предположение, действието на $\mathfrak{G}$ върху M е локално крайно и съществуват краен брой $\mathfrak{G}$-орбити $\mathrm{Orb}_{\mathfrak{G}}(x)$ върху M от степен $\leq m|H|$. Следователно има краен брой $\mathfrak{G}$-орбити $\mathrm{Orb}_{\mathfrak{G}}\xi_H(x)$ върху $\mathrm{Orb}_H(M)$ от степен m и $\mathrm{Orb}_H(M)$ е локално краен $\mathfrak{G}$-модул.

(iii) Еквивариантността на ξ_H относно действието на $\mathfrak{G}$ е непосредствено следствие от определението на това действие върху $\mathrm{Orb}_H(M)$ □

Нека M е безкраен локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул със затворени стабилизатори. Следващото твърдение описва "усукването"на действието на $\mathfrak{G}$ върху M чрез автоморфизъм $h \in \mathrm{Aut}_{\mathfrak{G}}(M)$ от краен ред без фиксирани точки.

Твърдение 133. *Нека M е безкраен локално краен $\mathfrak{G} = \mathfrak{G}(\Phi_q) = \widehat{\langle\Phi_q\rangle}$-модул със затворени стабилизатори, H е крайна подгрупа на $\mathrm{Aut}_{\mathfrak{G}}(M)$ без фиксирани точки и $\varphi = h\Phi_q^r$ за някое $h \in H$ и някое естествено число $r \in \mathbb{N}$. Тогава:*

(i) про-крайната обвивка $\mathfrak{G}(\varphi) = \widehat{\langle\varphi\rangle}$ на безкрайната циклична група $\langle\varphi\rangle \simeq (\mathbb{Z}, +)$ е подгрупа на $H\mathfrak{G} \simeq H \times \mathfrak{G}$;

(ii) M е локално краен $\mathfrak{G}(\varphi) = \widehat{\langle\varphi\rangle}$-модул;

(iii) втората канонична проекция $\mathrm{pr}_2 : H \times \mathfrak{G} \to \mathfrak{G}$, $\mathrm{pr}_2(h', \gamma) = \gamma$ за $\forall h' \in H$, $\forall \gamma \in \mathfrak{G}$ задава локално крайно $\mathfrak{G}(\varphi)$-действие

$$\mathfrak{G}(\varphi) \times \mathrm{Orb}_H(M) \longrightarrow \mathrm{Orb}_H(M), \quad (\gamma, \mathrm{Orb}_H(x)) \mapsto \mathrm{pr}_2(\gamma)\mathrm{Orb}_H(x) = \mathrm{Orb}_H(\mathrm{pr}_2(\gamma)x);$$

(iv) изображението

$$\xi_H : M \longrightarrow \mathrm{Orb}_H(M), \quad \xi_H(x) = \mathrm{Orb}_H(x) \quad за \quad \forall x \in M$$

е H-Галоа покритие на локално крайни $\mathfrak{G}(\varphi)$-модули.

Доказателство: (i) Преди всичко, $\varphi = h\Phi_q^r$ е от безкраен ред. В противен случай, за h от ред m и φ от ред l имаме $\mathrm{Id}_N = \varphi^{ml} = h^m\Phi_q^{rml} = \Phi_q^{rml}$ и автоморфизмът на Фробениус $\Phi_q : M \to M$ се оказва от краен ред. Това е противоречие, доказващо

$\langle\varphi\rangle \simeq (\mathbb{Z},+)$. Да забележим, че $\varphi = h\Phi_q^r \in H\mathfrak{G}$ е достатъчно за това $\langle\varphi\rangle$ да е подгрупа на компактната група $H\mathfrak{G}$. Про-крайната обвивка $\mathfrak{G}(\varphi) = \widehat{\langle\varphi\rangle}$ е затворената обвивка на $\langle\varphi\rangle$ относно дискретната топология, така че $\mathfrak{G}(\varphi) = \widehat{\langle\varphi\rangle} \leq H\mathfrak{G}$, защото $H\mathfrak{G}$ е затворена относно дискретната топология.

(ii) За да докажем, че всички $\mathfrak{G}(\varphi)$-орбити върху M са крайни, да разгледаме точка $x \in M$ със степен $\deg \mathrm{Orb}_{\mathfrak{G}}(x) = \delta$ на съответната орбита. Ако $h \in H < \mathrm{Aut}_{\mathfrak{G}}(M)$ е от ред m, то

$$\mathfrak{G}(\varphi^{m\delta}) := \widehat{\langle\varphi^{m\delta}\rangle} = \widehat{\langle\Phi_q^{m\delta r}\rangle} = \mathfrak{G}(\Phi_q^{mr\delta}) \leq \mathfrak{G}(\Phi_q^{\delta}) = \mathrm{Stab}_{\mathfrak{G}}(x) \leq \mathrm{Stab}_{H\times\mathfrak{G}}(x),$$

откъдето

$$\mathfrak{G}(\varphi^{m\delta}) \leq \mathfrak{G}(\varphi) \cap \mathrm{Stab}_{H\times\mathfrak{G}}(x) = \mathrm{Stab}_{\mathfrak{G}(\varphi)}(x) \leq \mathfrak{G}(\varphi).$$

Следователно

$$\deg \mathrm{Orb}_{\mathfrak{G}(\varphi)}(x) = [\mathfrak{G}(\varphi) : \mathrm{Stab}_{\mathfrak{G}(\varphi)}(x)] =$$
$$= \frac{[\mathfrak{G}(\varphi) : \mathfrak{G}(\varphi^{m\delta})]}{[\mathrm{Stab}_{\mathfrak{G}(\varphi)}(x) : \mathfrak{G}(\varphi^{m\delta})]} = \frac{m\delta}{[\mathrm{Stab}_{\mathfrak{G}(\varphi)}(x) : \mathfrak{G}(\varphi^{m\delta})]} \in \mathbb{N}$$

и всички $\mathfrak{G}(\varphi)$-орбити върху M са крайни. Нека $n \in \mathbb{N}$ и $y \in M$ е точка с $\deg \mathrm{Orb}_{\mathfrak{G}(\varphi)}(y) = n$ или, еквивалентно, с $\mathrm{Stab}_{\mathfrak{G}(\varphi)}(y) = \mathfrak{G}(\varphi^n)$. Ако $\delta := \deg \mathrm{Orb}_{\mathfrak{G}}(y)$ и $h \in H < \mathrm{Aut}_{\mathfrak{G}}(M)$ е от ред m, то

$$\mathfrak{G}(\varphi^{nm}) = \mathfrak{G}(\Phi_q^{nmr}) < \mathfrak{G} \cap \mathrm{Stab}_{H\times\mathfrak{G}}(y) = \mathrm{Stab}_{\mathfrak{G}}(x) = \mathfrak{G}(\Phi_q^{\delta}).$$

Следователно δ е естествен делител на nmr. По предположение, M съдържа краен брой $\mathfrak{G}$-орбити от степен δ. За всяко фиксирано $n \in \mathbb{N}$ съществуват краен брой естествени делители δ на nmr, откъдето и краен брой $\mathfrak{G}(\varphi)$-орбити върху M от степен n. По този начин проверихме, че действието на $\mathfrak{G}(\varphi)$ върху M е локално крайно.

(iii) е непосредствено следствие от Лема 132 (ii).

(iv) За $\mathfrak{G}(\varphi)$-еквивариантността на $\xi_H : M \to \mathrm{Orb}_H(M)$, $\xi_H(x) = \mathrm{Orb}_H(x)$ за $\forall x \in M$, да разгледаме първата канонична проекция $\mathrm{pr}_1 : H \times \mathfrak{G} \to \mathfrak{G}$, $\mathrm{pr}_1(h',\gamma) = h'$ за $\forall h' \in H$, $\forall \gamma \in \mathfrak{G}$. Произволно $\rho \in \mathfrak{G}(\varphi) < H\mathfrak{G} \simeq H \times \mathfrak{G}$ има единствено разлагане $\rho = \mathrm{pr}_1(\rho)\mathrm{pr}_2(\rho)$ в произведение на $\mathrm{pr}_1(\rho) \in H$ и $\mathrm{pr}_2(\rho) \in \mathfrak{G}$. Сега

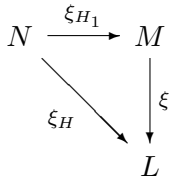
$$\xi_H(\rho x) = \xi_H(\mathrm{pr}_1(\rho)\mathrm{pr}_2(\rho)x) = \xi_H(\mathrm{pr}_2(\rho)x) = \mathrm{pr}_2(\rho)\xi_H(x)$$

за $\forall x \in M$ доказва, че ξ_H е H-Галоа покритие на локално крайни $\mathfrak{G}(\varphi)$-модули. □

Отсега нататък ще отъждествяваме изоморфните локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули, за да избегнем усложнени означения.

Определение 134. *Обвивка на Галоа на крайно неразклонено покритие $\xi : M \to L$ на локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули е тройка (N, H, H_1), съставена от локално краен $\mathfrak{G}_m = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$-модул N за някое $m \in \mathbb{N}$, крайна подгрупа H на $\mathrm{Aut}_{\mathfrak{G}_m}(N)$ без фиксирани точки и такава подгрупа H_1 на H, че пространството $\mathrm{Orb}_{H_1}(N)$ на*

H_1-орбитите е изоморфно на M като $\mathfrak{G}_m$-модул, $\mathrm{Orb}_H(N)$ е изоморфно на L като $\mathfrak{G}_m$-модул и H-Галоа покритието $\xi_H : N \to L$, $\xi_H(x) = \mathrm{Orb}_H(x)$ за $\forall x \in N$ се пропуска през H_1-Галоа покритието $\xi_{H_1} : N \to M$, $\xi_{H_1}(x) = \mathrm{Orb}_{H_1}(x)$ за $\forall x \in N$ и ξ по протежение на комутативната диаграма



от крайни неразклонени покрития на $\mathfrak{G}_m$-модули.

Казваме, че (N, H, H_1) е определено над $\mathbb{F}_{q^m}$.

Твърдение 135. *За всяка неприводима квази-проективна крива X с положителен род над $\overline{\mathbb{F}_q}$ съществува $s \in \mathbb{N}$, локално крайни $\mathfrak{G}_s = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^s})$-подмодули $X' \subseteq X$, $L \subseteq \mathbb{P}^1(\overline{\mathbb{F}_q})$ с най-много крайни допълнения $X \setminus X'$, $\mathbb{P}^1(\overline{\mathbb{F}_q}) \setminus L$, крайно неразклонено покритие $f : X' \to L$ на $\mathfrak{G}_s$-модули и обвивка на Галоа (Z, H, H_1) на f, така че Z е неприводима квази-проективна крива $Z \subseteq \mathbb{P}^r(\overline{\mathbb{F}_q})$, $H = Gal(\overline{\mathbb{F}_q}(Z)/\overline{\mathbb{F}_q}(\mathbb{P}^1(\overline{\mathbb{F}_q})))$, $H_1 = Gal(\overline{\mathbb{F}_q}(Z)/\overline{\mathbb{F}_q}(X))$.*

Доказателство: Нека $f : X_o \to L_o$ е крайното неразклонено покритие на локално крайни $\mathfrak{G}_m$-модули от Твърдение 127. Крайното сепарабелно разширение

$$\overline{\mathbb{F}_q}(X) = \overline{\mathbb{F}_q}(X_o) = \overline{\mathbb{F}_q}(u, v) \supset \overline{\mathbb{F}_q}(u) = \overline{\mathbb{F}_q}(L_o) = \overline{\mathbb{F}_q}(\mathbb{P}^1(\overline{\mathbb{F}_q}))$$

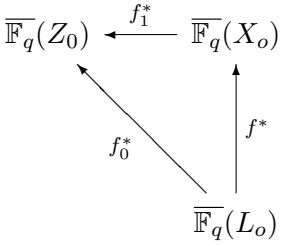
на съответните функционални полета има обвивка на Галоа $K \supseteq \overline{\mathbb{F}_q}(u, v) \supseteq \overline{\mathbb{F}_q}(u)$ с крайна степен $[K : \overline{\mathbb{F}_q}(u)] < \infty$, т.е. K е нормално над $\overline{\mathbb{F}_q}(u)$ и $\overline{\mathbb{F}_q}(u, v)$. Тогава съществува неприводима квази-проективна крива $Z_0 \subset \mathbb{P}^r(\overline{\mathbb{F}_q})$ с функционално поле $\overline{\mathbb{F}_q}(Z_0) = K$ и доминантни рационални изображения $f_0 : Z_0 \dashrightarrow L_0$, $f_1 : Z_0 \dashrightarrow X_0$, индуциращи тъждествените влагания

$$f_0^* = \mathrm{Id} : \overline{\mathbb{F}_q}(L_o) = \overline{\mathbb{F}_q}(u) \hookrightarrow \overline{\mathbb{F}_q}(Z_0),$$

съответно,

$$f_1^* = \mathrm{Id} : \overline{\mathbb{F}_q}(X_o) = \overline{\mathbb{F}_q}(u, v) \hookrightarrow \overline{\mathbb{F}_q}(Z_0)$$

на функционалните полета. Вземайки предвид, че крайното покритие $f : X_o \to L_o$ индуцира тъждественото изображение $f^* = \mathrm{Id} : \overline{\mathbb{F}_q}(L_o) = \overline{\mathbb{F}_q}(u) \hookrightarrow \overline{\mathbb{F}_q}(u, v) = \overline{\mathbb{F}_q}(X_o)$, получаваме комутативната диаграма



от тъждествени влагания на функционалните полета над $\overline{\mathbb{F}_q}$. Следователно, композицията ff_1 съвпада с доминантното рационално изображение f_0. Нека $Z_1' \subset \overline{\mathbb{F}_q}^r$ е квази-афинна крива, съдържаща се в областите на регулярност на f_0 и f_1. Тогава $f_0 : Z_1' \to f_0(Z_1')$ е крайно покритие на афинни криви. Отстранявайки от Z_1' множеството на разклонение на $f_0|_{Z_1'}$, получаваме квази-афинна крива $Z_1'' \subseteq Z_1' \subseteq Z_0$. Крайното множество $Z_0 \setminus Z_1''$ има краен образ $f(Z_0 \setminus Z_1'')$, така че $L_1 := L_o \setminus f_0(Z_0 \setminus Z_1'')$, $X_1 := f^{-1}(L_1)$, $Z_1 := f_0^{-1}(L_1) = f_1^{-1}(X_1) \subseteq Z_1''$ са квази-афинни криви, свързани с комутативна диаграма

$$\begin{array}{ccc} Z_1 & \xrightarrow{f_1} & X_1 \\ & \searrow^{f_0} & \downarrow f \\ & & L_1 \end{array}$$

от крайни неразклонени покрития на квази-афинни криви. В частност, $Z_0 \setminus Z_1$, $X_o \setminus X_1$, $L_o \setminus L_1$ са крайни множества.

Нормалното сепарабелно разширение $\overline{\mathbb{F}_q}(L_o) \subset \overline{\mathbb{F}_q}(Z_0)$ е крайно, така че неговата група на Галоа $H := Gal(\overline{\mathbb{F}_q}(Z_0)/\overline{\mathbb{F}_q}(L_o)) = Gal(\overline{\mathbb{F}_q}(Z_1)/\overline{\mathbb{F}_q}(L_1))$ е крайна. Всяко $h \in H$ трансформира афинните координати z_j, $1 \leq j \leq r$ върху $Z_1 \subset \overline{\mathbb{F}_q}^r$ в рационални функции $h(z_j) \in \overline{\mathbb{F}_q}(Z_1)$. Нека Z_2' е сечението на областите на регулярност на $h(z_j) : Z_1 \dashrightarrow \overline{\mathbb{F}_q}$ за $\forall h \in H$ и $\forall 1 \leq j \leq r$. Тогава за всяко $h \in H$ изображението

$$\widetilde{h} : Z_2' \longrightarrow \widetilde{h}(Z_2') \subseteq Z_1 \subset \overline{\mathbb{F}_q}^r,$$

$$\widetilde{h}(u_1, \ldots, u_r) := (h(z_1)(u_1), \ldots, h(z_r)(u_r)) \quad \text{за} \quad \forall u = (u_1, \ldots, u_r) \in Z_2'$$

е морфизъм на квази-афинни многообразия. Понеже H е крайна група, сечението $Z_2'' := \cap_{h \in H} \widetilde{h}(Z_2')$ е квази-афинна крива, така че $|Z_2' \setminus Z_2''| < \infty$. Още повече, за $\forall u \in Z_2''$ и $\forall h_o, h \in H$ имаме $u \in \widetilde{h_o}^{-1}\widetilde{h}(Z_2')$, откъдето $\widetilde{h_o}(u) \in \widetilde{h}(Z_2')$. Затова, $\widetilde{h_o}(u) \in \cap_{h \in H} \widetilde{h}(Z_2') = Z_2''$ за $\forall u \in Z_2''$, $\forall h_o \in H$ и Z_2'' е H-инвариантна крива. Да забележим, че за всяко $h \in H$ уравнението $\widetilde{h}(u) = u$ има най-много краен брой решения върху Z_2''. Следователно H има най-много краен брой фиксирани точки върху Z_2''. След отстраняване на H-орбитите на H-фиксираните точки върху Z_2'', намираме квази-афинна крива $Z_2 \subseteq Z_2''$ с действие на H без фиксирани точки.

От конструкцията на Z_0 следва, че функционалните полета

$$\overline{\mathbb{F}_q}(Z_0) = \overline{\mathbb{F}_q}(Z_1) = \overline{\mathbb{F}_q}(Z_2) \supseteq \overline{\mathbb{F}_q}(X_1) = \overline{\mathbb{F}_q}(X_o) \quad \text{и}$$

$$\overline{\mathbb{F}_q}(Z_0) = \overline{\mathbb{F}_q}(Z_1) = \overline{\mathbb{F}_q}(Z_2) \supset \overline{\mathbb{F}_q}(L_1) = \overline{\mathbb{F}_q}(L_o)$$

образуват разширения на Галоа. Следователно групите на Галоа

$$H = Gal(\overline{\mathbb{F}_q}(Z_2)/\overline{\mathbb{F}_q}(L_1)) \quad \text{и} \quad H_1 := Gal(\overline{\mathbb{F}_q}(Z_0)/\overline{\mathbb{F}_q}(X_o)) = Gal(\overline{\mathbb{F}_q}(Z_2)/\overline{\mathbb{F}_q}(X_1))$$

имат инвариантни полета $\overline{\mathbb{F}_q}(Z_2)^H = \overline{\mathbb{F}_q}(L_1)$, съответно, $\overline{\mathbb{F}_q}(Z_2)^{H_1} = \overline{\mathbb{F}_q}(X_1)$. Съответствието

$$f_H : Z_2 \longrightarrow \mathrm{Orb}_H(Z_2) = Z_2/H, \quad f_H(z) = \mathrm{Orb}_H(z) \quad \text{за} \quad \forall z \in Z_2,$$

съпоставящо на точка $z \in Z_2$ нейната H-орбита е сюрективен морфизъм на алгебрични криви, който индуцира изоморфизъм $f_H^* : \overline{\mathbb{F}_q}(Z_2/H) \to \overline{\mathbb{F}_q}(Z_2)^H = \overline{\mathbb{F}_q}(L_1)$ на $\overline{\mathbb{F}_q}$-алгебри. Следователно съществува бирационално изображение $\varphi_0 : L_1 \dashrightarrow Z_2/H$ с $\varphi_0^* = f_H^*$. Аналогично,

$$f_{H_1} : Z_2 \longrightarrow \mathrm{Orb}_{H_1}(Z_2) = Z_2/H_1, \quad f_{H_1}(z) = \mathrm{Orb}_{H_1}(z) \quad \text{за} \quad \forall z \in Z_2$$

е сюрективен морфизъм на алгебрични криви, индуциращ изоморфизъм на $\overline{\mathbb{F}_q}$-алгебри $f_{H_1}^* : \overline{\mathbb{F}_q}(Z_2/H_1) \to \overline{\mathbb{F}_q}(Z_2)^{H_1} = \overline{\mathbb{F}_q}(X_1)$. Нека $\varphi_1 : X_1 \dashrightarrow Z_2/H_1$ е бирационалното изображение с $\varphi_1^* = f_{H_1}^*$. Комутативната диаграма

$$\begin{array}{ccc} \overline{\mathbb{F}_q}(Z_2) & & \\ {\scriptstyle \mathrm{Id}}\uparrow & \nwarrow^{f_H^*} & \\ \overline{\mathbb{F}_q}(L_1) & \xleftarrow{\varphi_0^*} & \overline{\mathbb{F}_q}(Z_2/H) \end{array} \quad , \quad \begin{array}{ccc} \overline{\mathbb{F}_q}(Z_2) & & \\ {\scriptstyle \mathrm{Id}}\uparrow & \nwarrow^{f_{H_1}^*} & \\ \overline{\mathbb{F}_q}(X_1) & \xleftarrow{\varphi_1^*} & \overline{\mathbb{F}_q}(Z_2/H_1) \end{array}$$

от влагания Id, f_H^*, $f_{H_1}^*$ на $\overline{\mathbb{F}_q}$-алгебри и изоморфизми φ_0^*, φ_1^* на $\overline{\mathbb{F}_q}$-алгебри индуцира комутативни диаграми

$$\begin{array}{ccc} Z_2 & & \\ {\scriptstyle f_0}\downarrow & \searrow^{f_H} & \\ L_1 & \xrightarrow{\varphi_0} & Z_2/H \end{array} \quad , \quad \begin{array}{ccc} Z_2 & & \\ {\scriptstyle f_1}\downarrow & \searrow^{f_{H_1}} & \\ X_1 & \xrightarrow{\varphi_1} & Z_2/H_1 \end{array}$$

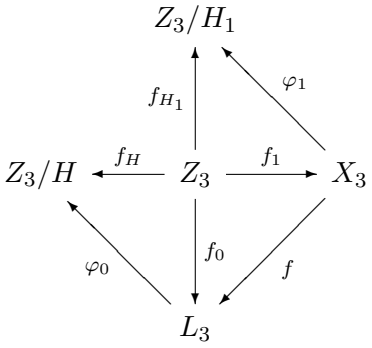
от морфизми f_0, f_H, f_1, f_{H_1} и бирационални изображения φ_0, φ_1.

Съществува квази-афинна крива $L_2' \subseteq L_1$, така че $\varphi_0 : L_1 \dashrightarrow Z_2/H$ се ограничава до изоморфизъм $\varphi_0 : L_2' \to \varphi_0(L_2') \subseteq Z_2/H$ на алгебрични многообразия. Аналогично, можем да изберем такава квази-афинна крива $X_2' \subseteq X_1$, че $\varphi_1 : X_2' \to \varphi_1(X_2') \subseteq Z_2/H_1$ е изиморфизъм на алгебрични криви. Понеже $L_1 \setminus L_2'$ и $X_1 \setminus X_2'$ са крайни множества и $f_0 : Z_1 \to L_1$, $f_1 : Z_1 \to X_1$ са крайни покрития,

$$S := f_0^{-1}(L_1 \setminus L_2') \cup f_1^{-1}(X_1 \setminus X_2')$$

е крайно подмножество на Z_2. Отстранявайки от Z_2 орбитите на H върху S, намираме квази-афинна крива $Z_3 \subseteq Z_2$ с действие на H без фиксирани точки. От разлагането $f_H|_{Z_3} = \varphi_0 f_0|_{Z_3}$ с бирегулярно $\varphi_0 : f_0(Z_3) \to f_H(Z_3)$ следва съвпадението на слоевете на f_H и f_0. Следователно, $f_H : Z_3 \to f_H(Z_3)$ и $f_0 : Z_3 \to L_3 := f_0(Z_3)$ са крайни неразклонени покрития на алгебрични криви от степен $|H|$. Аналогично, $f_{H_1}|_{Z_3} = \varphi_1 f_1|_{Z_3}$ с бирегулярно $\varphi_1 : f_1(Z_3) \to f_{H_1}(Z_3)$ разкрива, че $f_{H_1} : Z_3 \to f_{H_1}(Z_3)$ и $f_1 : Z_3 \to X_3 := f_1(Z_3)$ са крайни неразклонени покрития на алгебрични криви от степен $|H_1|$. Съществува достатъчно голямо $s \in \mathbb{N}$, така че $\mathbb{F}_{q^s}$ съдържа дефиниционните полета на кривите Z_3, X_3, L_3, Z_3/H, Z_3/H_1, както и коефициентите на

компонентите на регулярните изображения f, f_0, f_1, f_H, f_{H_1}. Така получаваме комутативна диаграма



от крайни неразклонение покрития на локално крайни $\mathfrak{G}_s$-модули с биективни φ_0, φ_1, H-Галоа покрития f_H, H_1-Галоа покрития f_{H_1}. Въвеждайки $Z := Z_3$, $X' := X_3$, $L := L_3$, стигаме до извода, че (Z, H, H_1) е обвивка на Галоа на крайното неразклонено покритие $f : X' \to L$. □

6.4 Аналог на хипотезата на Риман за локално крайни модули

Следващото твърдение дава числено необходимо и достатъчно условие, при което локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул с полиномиално ζ-частно изпълнява аналога на хипотезата на Риман относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$.

Твърдение 136. *Следните условия са еквивалентни за локално краен модул M над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ с полиномиално ζ-частно $P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} \in \mathbb{Z}[t]$ от степен $degP_M(t) = d \in \mathbb{N}$ със старши коефициент $\mathrm{LC}(P_M(t)) = a_d \in \mathbb{Z} \setminus \{0\}$ и за $\lambda := \log_q \sqrt[d]{|a_d|} \in \mathbb{R}^{\geq 0}$:*

(i) M изпълнява аналога на хипотезата на Рима относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ като $\mathfrak{G}$-модул;

(ii) $q^r + 1 - dq^{\lambda r} \leq |M^{\Phi_q^r}| \leq q^r + 1 + dq^{\lambda r}$ за $\forall r \in \mathbb{N}$;

(iii) съществуват такива константи $C_1, C_2 \in \mathbb{R}^{>0}$, $\nu, r_1, r_2 \in \mathbb{N}$, че

$$|M^{\Phi_q^{\nu r}}| \leq q^{\nu r} + 1 + C_1 q^{\lambda \nu r} \quad за \quad \forall r \in \mathbb{N}, \quad r \geq r_1 \quad и$$

$$|M^{\Phi_q^{\nu r}}| \geq q^{\nu r} + 1 - C_2 q^{\lambda \nu r} \quad за \quad \forall r \in \mathbb{N}, \quad r \geq r_2.$$

Доказателство: $(i) \Rightarrow (ii)$ Ако $P_M(t) = \prod_{j=1}^{d} (1 - q^{\lambda} e^{i\varphi_j} t)$ за някои $\varphi_j \in [0, 2\pi)$, то

$$\left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^r}\right| - \left|M^{\Phi_q^r}\right| = \sum_{j=1}^{d} q^{\lambda r} e^{ir\varphi_j} \quad \text{за} \quad \forall r \in \mathbb{N},$$

съгласно (6.9) от Твърдение 123. Следователно модулът

$$\left|\left|M^{\Phi_q^r}\right| - (q^r+1)\right| = \left|\sum_{j=1}^{d} q^{\lambda r} e^{ir\varphi_j}\right| \leq \sum_{j=1}^{d} \left|q^{\lambda r} e^{ir\varphi_j}\right| = \sum_{j=1}^{d} q^{\lambda r} = dq^{\lambda r}$$

и е в сила (ii).

$(ii) \Rightarrow (iii)$ е тривиално

$(iii) \Rightarrow (i)$ Нека $P_M(t) = \prod_{j=1}^{d}(1-\omega_j t) \in \mathbb{Z}[t]$. Формалният степенен ред

$$H(t) := \sum_{j=1}^{d} \frac{\omega_j^\nu t}{1-\omega_j^\nu t}$$

има радиус на сходимост

$$\rho = \min\left(\frac{1}{|\omega_1|^\nu}, \ldots, \frac{1}{|\omega_d|^\nu}\right),$$

т.е. редът $H(t) < \infty$ е сходящ за $\forall t \in \mathbb{C}$ с $|t| < \rho$ и $H(t) = \infty$ е разходящ за $\forall t \in \mathbb{C}$ с $|t| > \rho$. Използвайки разлагането

$$\frac{1}{1-\omega_j^\nu t} = \sum_{i=0}^{\infty} \omega_j^{\nu i} t^i$$

във формален степенен ред и разменяйки реда на сумиране, представяме

$$H(t) = \sum_{i=0}^{\infty} \left(\sum_{j=1}^{d} \omega_j^{\nu(i+1)}\right) t^{i+1}.$$

Полагаме $C := \max(C_1, C_2)$, $r_0 := \max(r_1, r_2)$ и забелязваме, че от предположение (iii) следва, че

$$\left|\sum_{j=1}^{d} \omega_j^{\nu r}\right| = \left|\left|M^{\Phi_q^{\nu r}}\right| - (q^{\nu r}+1)\right| \leq Cq^{\lambda\nu r} \quad \text{за} \quad \forall r \in \mathbb{N}, \quad r \geq r_0,$$

съгласно (6.9) от Твърдение 123. По този начин, $\left|\sum_{j=1}^{d} \omega_j^{\nu(i+1)}\right| \leq Cq^{\lambda\nu(i+1)}$ за $\forall i \in \mathbb{Z}$, $i \geq r_0 - 1$ и

$$|H(t)| \leq \sum_{i=0}^{\infty} \left|\sum_{j=1}^{d} \omega_j^{\nu(i+1)}\right| t^{i+1} \leq C \sum_{i=0}^{\infty} q^{\lambda\nu(i+1)} t^{i+1} = C \sum_{i=0}^{\infty} (q^{\lambda\nu} t)^{i+1}.$$

В резултат, $H(t) < \infty$ за $\forall t \in \mathbb{C}$ с $|t| < \frac{1}{q^{\lambda\nu}}$, отъкдето $\frac{1}{q^{\lambda\nu}} \leq \rho \leq \frac{1}{|\omega_j|^\nu}$ за $\forall 1 \leq j \leq d$. Вземайки предвид, че всяко фиксирано $\nu \in \mathbb{N}$ функцията $f(x) = x^\nu$ е ненамаляваща върху $x \in [0, \infty) \subset \mathbb{R}$, стигаме до извода, че $q^\lambda \geq |\omega_j|$. Следователно старшият коефициент $a_d := \mathrm{LC}(P_M(t)) = \prod_{j=1}^{d}(-\omega_j) \in \mathbb{Z} \setminus \{0\}$ има модул

$$|a_d| = \prod_{j=1}^{d} |\omega_j| \leq q^{\lambda d} = |a_d|\,,$$

откъдето $|\omega_j| = q^\lambda$ за $\forall 1 \leq j \leq d$ и M изпълнява аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ като модул над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. □

За гладка неприводима проективна крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ от род g, определена над $\mathbb{F}_q$, условието (ii) от Твърдение 136 се свежда до известната граница на Хасе-Вайл

$$\left|\left|X^{\Phi_q^r}\right| - (q^r + 1)\right| \leq 2g\sqrt{q^r} \quad \text{за} \quad \forall r \in \mathbb{N} \tag{6.15}$$

върху броя $\left|X^{\Phi_q^r}\right| = |X(\mathbb{F}_{q^r})| = |X \cap \mathbb{P}^n(\mathbb{F}_{q^r})|$ на $\mathbb{F}_{q^r}$-рационалните точки на X. Еквивалентността на условията (i) и (iii) от Твърдение (136) е добре известна и доказана от Теорема V.2.3 и Лема V.2.5 от монографията на Стичтенот [Stichtenoth]. Доказателството на аналога на хипотезата на Риман за X относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ от [Stichtenoth] използва границата

$$\left|X^{\Phi_q^{2r}}\right| < q^{2r} + 1 + (2g+1)q^r \quad \text{for} \quad \forall r \in \mathbb{N}, \tag{6.16}$$

доказана в Твърдение 85. Вземайки предвид $\left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^{2r}}\right| = q^{2r} + 1 > q^{2r}$, забелязваме, че от (6.16) следва

$$\left|X^{\Phi_q^{2r}}\right| - \left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^{2r}}\right| < (2g+1)\left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^{2r}}\right|^{\frac{1}{2}} \quad \text{за} \quad \forall r \in \mathbb{N}$$

и разглеждаме $\lambda := \log_q \sqrt[2g]{\mathrm{LC}(P_X(t))} = \log_q \sqrt[2g]{q^g} = \frac{1}{2}$ като порядък на Хасе-Вайл на X относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Това мотивира следното

Определение 137. *Нека M и L са локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули. Ако съществуват константи $\rho \in \mathbb{R}^{\geq 0}$, $C \in \mathbb{R}^{>0}$, $\nu, r_o \in \mathbb{N}$, така че*

$$\left|M^{\Phi_q^{\nu r}}\right| - \left|L^{\Phi_q^{\nu r}}\right| \leq C\left|L^{\Phi_q^{\nu r}}\right|^\rho \quad \textit{за} \quad \forall r \in \mathbb{N}, \quad r \geq r_o, \tag{6.17}$$

казваме, че M има краен порядък на Хасе-Вайл относно L.

Минималното $\rho \in \mathbb{R}^{\geq 0}$, изпълняващо (6.17) за някои $C \in \mathbb{R}^{>0}$, $\nu, r_o \in \mathbb{N}$ се нарича порядък на Хасе-Вайл на M относно L и се означава с $\mathrm{ord}_{\mathfrak{G}}(M/L)$.

В случая $L = \mathbb{P}^1(\overline{\mathbb{F}_q})$, неравенството (6.17) за някое $\rho \geq \mathrm{ord}_{\mathfrak{G}}(M/L)$ може да се разглежда като обобщение на границата на Хасе-Вайл върху броя на рационалните точки на крива.

В следващата лесна лема сме събрали някои свойства на порядъка на Хасе-Вайл на локално краен $\mathfrak{G}$-модул.

Лема 138. *(i) Ако M, L са безкрайни локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули и $M_o \subseteq M$, $L_o \subseteq L$ са $\mathfrak{G}$-подмодули с най-много крайни допълнения $M \setminus M_o$, $L \setminus L_o$, то*

$$\operatorname{ord}_{\mathfrak{G}}(M/L) = \operatorname{ord}_{\mathfrak{G}}(M_o/L_o).$$

(ii) Ако $\xi : M \to L$ е крайно неразклонено покритие на локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули, то $\operatorname{ord}_{\mathfrak{G}}(M/L) \leq 1$.

(iii) Нека M е локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул с $\zeta_M(t) = P_M(t)\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)$ за полином $P_M(t) \in \mathbb{Z}[t]$ от степен $\deg P_M(t) = d \in \mathbb{N}$ с $\mathrm{LC}(P_M(t)) = a_d$ и $\lambda := \log_q \sqrt[d]{|a_d|}$. Ако M изпълнява аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$, то $\operatorname{ord}_{\mathfrak{G}}(M/\mathbb{P}^1(\overline{\mathbb{F}_q})) \leq \lambda$.

Доказателство: (i) Достатъчно е да докажем, че ако съществуват $C \in \mathbb{R}^{>0}$, $\nu, r' \in \mathbb{N}$, изпълняващи неравенството

$$\left|M^{\Phi_q^{\nu r}}\right| \leq \left|L^{\Phi_q^{\nu r}}\right| + C\left|L^{\Phi_q^{\nu r}}\right|^{\rho} \quad \text{за} \quad \forall r \in \mathbb{N}, \quad r \geq r', \tag{6.18}$$

то съществуват $C_o \in \mathbb{R}^{>0}$, $\nu_o, r'_o \in \mathbb{N}$ с

$$\left|M_o^{\Phi_q^{\nu_o r}}\right| \leq \left|L_o^{\Phi_q^{\nu_o r}}\right| + C_o\left|L_o^{\Phi_q^{\nu_o r}}\right|^{\rho} \quad \text{за} \quad \forall r \in \mathbb{N}, r \geq r'_o \tag{6.19}$$

и ако съществуват $\widetilde{C_o} \in \mathbb{R}^{>0}$, $\widetilde{\nu_o}, \widetilde{r'_o} \in \mathbb{N}$, изпълняващи

$$\left|M_o^{\Phi_q^{\widetilde{\nu_o} r}}\right| \leq \left|L_o^{\Phi_q^{\widetilde{\nu_o} r}}\right| + \widetilde{C_o}\left|L_o^{\Phi_q^{\widetilde{\nu_o} r}}\right|^{\rho} \quad \text{за} \quad \forall r \in \mathbb{N}, \quad r \geq \widetilde{r'_o}, \tag{6.20}$$

то съществуват $\widetilde{C} \in \mathbb{R}^{>0}$, $\widetilde{\nu}, \widetilde{r'} \in \mathbb{N}$ с

$$\left|M^{\Phi_q^{\widetilde{\nu} r}}\right| \leq \left|L^{\Phi_q^{\widetilde{\nu} r}}\right| + \widetilde{C}\left|L^{\Phi_q^{\widetilde{\nu} r}}\right|^{\rho} \quad \text{за} \quad \forall r \in \mathbb{N}, \quad r \geq \widetilde{r'}. \tag{6.21}$$

С тази цел, да означим $m := |M \setminus M_o|$, $s := |L \setminus L_o| \in \mathbb{Z}^{\geq 0}$ и да забележим, че

$$\left|L^{\Phi_q^{\nu_o r}}\right| = \left|L_o^{\Phi_q^{\nu_o r}}\right| + \left|L^{\Phi_q^{\nu_o r}} \setminus L_o\right| \leq \left|L_o^{\Phi_q^{\nu_o r}}\right| + s,$$

$$\left|M^{\Phi_q^{\widetilde{\nu} r}}\right| = \left|M_o^{\Phi_q^{\widetilde{\nu} r}}\right| + \left|M^{\Phi_q^{\overline{\nu} r}} \setminus M_o\right| \leq \left|M_o^{\Phi_q^{\widetilde{\nu} r}}\right| + m$$

за $\forall r \in \mathbb{N}$. Понеже L_o е безкраен локално краен $\mathfrak{G}$-модул, изображението

$$\deg \mathrm{Orb}_{\mathfrak{G}} : L_o \to \mathbb{N}, \quad x \mapsto \deg \mathrm{Orb}_{\mathfrak{G}}(x)$$

взема безбройно много стойности и съществува $\sigma_o \in \mathbb{N}$ с $\sigma_o \geq \max\left(s, \sqrt[\ell]{s}\right)$ от образа на $\deg \mathrm{Orb}_{\mathfrak{G}} : L_o \to \mathbb{N}$. С други думи, броят $B_{\sigma_o}(L_o) \geq 1$ на $\mathfrak{G}$-орбитите върху L_o от степен σ_o е положителен. Ако $\nu_o := \nu\sigma_o \in \mathbb{N}$ то съгласно (6.5) е в сила

$$\left|L_o^{\Phi_q^{\nu_o r}}\right| = \sum_{k/\nu_o r} kB_k(L_o) \geq \sigma_o B_{\sigma_o}(L_o) \geq \sigma_o \geq \max\left(s, \sqrt[\ell]{s}\right) \quad \text{за} \quad \forall r \in \mathbb{N}.$$

Аналогично, съществува $\sigma \in \mathbb{N}$ с $\sigma > \sqrt[\rho]{m}$ и $B_\sigma(L_o) \geq 1$. Затова, за $\widetilde{\nu} := \widetilde{\nu_o}\sigma \in \mathbb{N}$ е в сила

$$\left|L_o^{\Phi_q^{\widetilde{\nu}r}}\right| = \sum_{k/\widetilde{\nu}r} kB_k(L_o) \geq \sigma B_\sigma(L_o) \geq \sigma \geq \sqrt[\rho]{m} \quad \text{за} \quad \forall r \in \mathbb{N}.$$

Сега от (6.18) следва

$$\begin{aligned}\left|M_o^{\Phi_q^{\nu_o r}}\right| \leq \left|M^{\Phi_q^{\nu_o r}}\right| \leq \left|L^{\Phi_q^{\nu_o r}}\right| + C\left|L^{\Phi_q^{\nu_o r}}\right|^\rho \leq \left|L_o^{\Phi_q^{\nu_o r}}\right| + s + C\left(\left|L_o^{\Phi_q^{\nu_o r}}\right| + s\right)^\rho \leq \\ \leq \left|L_o^{\Phi_q^{\nu_o r}}\right| + \left|L_o^{\Phi_q^{\nu_o r}}\right|^\rho + C\left(2\left|L_o^{\Phi_q^{\nu_o r}}\right|\right)^\rho = \left|L_o^{\Phi_q^{\nu_o r}}\right| + (2^\rho C + 1)\left|L_o^{\Phi_q^{\nu_o r}}\right|^\rho\end{aligned}$$

за $\forall r \in \mathbb{N}$, $r \geq \frac{r'}{\sigma_o}$, което е еквивалентно на (6.19) за $C_o = 2^\rho C + 1$ и някои $r'_o \in \mathbb{N}$, $r'_o \geq \frac{r'}{\sigma_o}$. Аналогично, (6.20) е достатъчно за

$$\begin{aligned}\left|M^{\Phi_q^{\widetilde{\nu}r}}\right| \leq \left|M_o^{\Phi_q^{\widetilde{\nu}r}}\right| + m \leq \left|L_o^{\Phi_q^{\widetilde{\nu}r}}\right| + \widetilde{C_o}\left|L_o^{\Phi_q^{\widetilde{\nu}r}}\right|^\rho + \left|L_o^{\Phi_q^{\widetilde{\nu}r}}\right|^\rho = \\ = \left|L_o^{\Phi_q^{\widetilde{\nu}r}}\right| + (\widetilde{C_o} + 1)\left|L_o^{\Phi_q^{\widetilde{\nu}r}}\right|^\rho \leq \left|L^{\Phi_q^{\widetilde{\nu}r}}\right| + (\widetilde{C_o} + 1)\left|L^{\Phi_q^{\widetilde{\nu}r}}\right|^\rho\end{aligned}$$

за $\forall r \in \mathbb{N}$, $r \geq \frac{\widetilde{r'_o}}{\sigma}$ и ев сила (6.21) за $\widetilde{C} := \widetilde{C_o} + 1$ и за някои $\widetilde{r'} \in \mathbb{N}$, $\widetilde{r'} \geq \frac{\widetilde{r'_o}}{\sigma}$.

(ii) От $\mathfrak{G}$-еквивариантността на ξ следва $\xi(M^{\Phi_q^r}) \subseteq L^{\Phi_q^r}$ за $\forall r \in \mathbb{N}$. Слоеве $\xi|_{M^{\Phi_q^r}}$ имат не повече от $k := \deg \xi$ елементи, така че

$$\left|L^{\Phi_q^r}\right| \geq \left|\xi(M^{\Phi_q^r})\right| \geq \frac{\left|M^{\Phi_q^r}\right|}{k}$$

и

$$\left|M^{\Phi_q^r}\right| - \left|L^{\Phi_q^r}\right| \leq (k-1)\left|L^{\Phi_q^r}\right|.$$

Това е достатъчно за $\operatorname{ord}_{\mathfrak{G}}(M/L) \leq 1$.

(iii) Съгласно Твърдение 136, ако M изпълнява аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ като $\mathfrak{G}$-модул, то

$$\left|M^{\Phi_q^r}\right| \leq q^r + 1 + dq^{\lambda r} = \left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^r}\right| + d\left(\left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^r}\right| - 1\right)^\lambda < \left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^r}\right| + d\left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^r}\right|^\lambda$$

за $\forall r \in \mathbb{N}$, така че $\operatorname{ord}_{\mathfrak{G}}(M/\mathbb{P}^1(\overline{\mathbb{F}_q})) \leq \lambda$.

□

Определение 139. *Нека M и L са локално крайни $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модули и H е крайна подгрупа на $\operatorname{Aut}_{\mathfrak{G}}(M)$ без фиксирани точки. Ако съществуват такива константи $\rho \in \mathbb{R}^{\geq 0}$, $C \in \mathbb{R}^{>0}$, $\nu, r_o \in \mathbb{N}$, че*

$$\left|M^{h\Phi_q^{\nu r}}\right| - \left|L^{\Phi_q^{\nu r}}\right| \leq C\left|L^{\Phi_q^{\nu r}}\right|^\rho \quad \text{за} \quad \forall r \in \mathbb{N}, \quad r \geq r_o \quad \text{и} \quad \forall h \in H \tag{6.22}$$

то M има краен H-порядък на Хасе-Вайл относно L.

Минималното $\rho \in \mathbb{R}^{\geq 0}$, изпълняващо (6.22) за някое $C \in \mathbb{R}^{>0}$, $\nu, r_o \in \mathbb{N}$ се нарича H-порядък на Хасе-Вайл на M относно L и се означава с $\operatorname{ord}_{\mathfrak{G}}^H(M/L)$.

Твърдение 140. *(i) Ако M е безкраен локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул, $H < \mathrm{Aut}_{\mathfrak{G}}(M)$ е крайна подгрупа без фиксирани точки и $M_o \subset M$ е $H \times \mathfrak{G}$-подмодул M с $|M \setminus M_o| < \infty$, то*

$$\mathrm{ord}_{\mathfrak{G}}^{H}(M/\mathrm{Orb}_H(M)) = \mathrm{ord}_{\mathfrak{G}}^{H}(M_o/\mathrm{Orb}_H(M_o)).$$

(ii) Ако M е локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул и $H < \mathrm{Aut}_{\mathfrak{G}}(M)$ е крайна подгрупа без фиксирани точки, то $\mathrm{ord}_{\mathfrak{G}}^{H}(M/\mathrm{Orb}_H(M)) \leq 1$.

(iii) Нека $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима крива от род $g \geq 1$, а H е крайна подгрупа на $\mathrm{Aut}_{\mathfrak{G}}(X)$ без фиксирани точки. Тогава $\mathrm{ord}_{\mathfrak{G}}^{H}(X/\mathbb{P}^1(\overline{\mathbb{F}_q})) \leq \frac{1}{2}$.

Доказателство: (i) Както в доказателството на Лема 138 (i), трябва да проверим, че ако съществуват $\rho \in \mathbb{R}^{\geq 0}$, $C \in \mathbb{R}^{>0}$, $\nu, r' \in \mathbb{N}$ с

$$\left|M^{h\Phi_q^{\nu r}}\right| \leq \left|\mathrm{Orb}_H(M)^{\Phi_q^{\nu r}}\right| + C\left|\mathrm{Orb}_H(M)^{\Phi_q^{\nu r}}\right|^{\rho} \text{ for } \forall h \in H, \forall r \in \mathbb{N}, r \geq r' \qquad (6.23)$$

то съществуват $C_o \in \mathbb{R}^{>0}$, $\nu_o, r_o' \in \mathbb{N}$ с

$$\left|M_o^{h\Phi_q^{\nu_o r}}\right| \leq \left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\nu_o r}}\right| + C_o\left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\nu_o r}}\right|^{\rho} \text{ за } \forall h \in H, \forall r \in \mathbb{N}, r \geq r_o' \quad (6.24)$$

и ако съществуват $\widetilde{C_o} \in \mathbb{R}^{>0}$, $\widetilde{\nu_o}, \widetilde{r_o} \in \mathbb{N}$ с

$$\left|M_o^{h\Phi_q^{\widetilde{\nu_o} r}}\right| \leq \left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\widetilde{\nu_o} r}}\right| + \widetilde{C_o}\left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\widetilde{\nu_o} r}}\right|^{\rho} \text{ за } \forall h \in H, \forall r \in \mathbb{N}, r \geq \widetilde{r_o} \quad (6.25)$$

то съществуват $\widetilde{C} \in \mathbb{R}^{>0}$, $\widetilde{\nu}, \widetilde{r} \in \mathbb{N}$ с

$$\left|M^{h\Phi_q^{\widetilde{\nu} r}}\right| \leq \left|\mathrm{Orb}_H(M)^{\Phi_q^{\widetilde{\nu} r}}\right| + \widetilde{C}\left|\mathrm{Orb}_H(M)^{\Phi_q^{\widetilde{\nu} r}}\right|^{\rho} \text{ за } \forall h \in H, \forall r \in \mathbb{N}, r \geq \widetilde{r}. \qquad (6.26)$$

Да забележим, че ако $|M \setminus M_o| = m$, то $\mathrm{Orb}_H(M) \setminus \mathrm{Orb}_H(M_o) = \mathrm{Orb}_H(M \setminus M_o)$ има $|\mathrm{Orb}_H(M \setminus M_o)| = \frac{m}{|H|}$ елемента и $\mathrm{Orb}_H(M_o)$ е безкраен локално краен $\mathfrak{G}$-модул. Както в доказателството на Лема 138 (i), имаме

$$\left|\mathrm{Orb}_H(M)^{\Phi_q^{\nu_o r}}\right| \leq \left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\nu_o r}}\right| + \frac{m}{|H|} \quad \text{и} \quad \left|M^{h\Phi_q^{\widetilde{\nu} r}}\right| \leq \left|M_o^{h\Phi_q^{\widetilde{\nu} r}}\right| + m \quad \text{за} \quad \forall r \in \mathbb{N}.$$

По-нататък, съществуват $\nu_o := \nu\sigma_o$ и $\widetilde{\nu} := \widetilde{\nu_o}\sigma$ с $\sigma_o, \sigma \in \mathbb{N}$, така че

$$\left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\nu_o r}}\right| \geq \sigma_o \geq \max\left(\frac{m}{|H|}, \sqrt[\rho]{\frac{m}{|H|}}\right),$$

съответно,

$$\left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\widetilde{\nu} r}}\right| \geq \sigma \geq \sqrt[\rho]{m} \quad \text{за} \quad \forall r \in \mathbb{N}.$$

Тогава

$$\begin{aligned}\left|M_o^{h\Phi_q^{\nu_o r}}\right| \le \left|M^{h\Phi_q^{\nu_o r}}\right| \le \left|\mathrm{Orb}_H(M)^{\Phi_q^{\nu_o r}}\right| + C\left|\mathrm{Orb}_H(M)^{\Phi_q^{\nu_o r}}\right|^\rho \le \\ \le \left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\nu_o r}}\right| + \frac{m}{|H|} + C\left(\left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\nu_o r}}\right| + \frac{m}{|H|}\right)^\rho \le \\ \le \left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\nu_o r}}\right| + \left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\nu_o r}}\right|^\rho + C\left(2\left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\nu_o r}}\right|\right)^\rho\end{aligned}$$

за $\forall r \in \mathbb{N},, r \ge \frac{r'}{\sigma_o}$ доказва (6.24) с $C_o := 2^\rho C + 1$ и

$$\begin{aligned}\left|M^{h\Phi_q^{\widetilde{\nu}r}}\right| \le \left|M_o^{h\Phi_q^{\widetilde{\nu}r}}\right| + m \le \\ \le \left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\widetilde{\nu}r}}\right| + \widetilde{C_o}\left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\widetilde{\nu}r}}\right|^\rho + \left|\mathrm{Orb}_H(M_o)^{\Phi_q^{\widetilde{\nu}r}}\right|^\rho \le \\ \le \left|\mathrm{Orb}_H(M)^{\Phi_q^{\widetilde{\nu}r}}\right| + (\widetilde{C_o}+1)\left|\mathrm{Orb}_H(M)^{\Phi_q^{\widetilde{\nu}r}}\right|^\rho\end{aligned}$$

за $\forall r \in \mathbb{N}$, $r \ge \frac{\widetilde{r_o}}{\sigma}$ установява (6.26) с $\widetilde{C} := \widetilde{C_o} + 1$

(ii) За произволни $h \in H$ и $r \in \mathbb{N}$ изображението $\xi_H : M \to \mathrm{Orb}_H(M)$ е H-Галоа покритие на локално крайни модули над $\mathfrak{G}(h\Phi_q^r) = \widehat{\langle h\Phi_q^r \rangle}$, съгласно Твърдение 133. Ако $y \in M^{h\Phi_q^r}$, то от $\mathfrak{G}(h\Phi_q^r)$-еквивариантността на ξ_H следва $\Phi_q^r \xi_H(y) = \xi_H(\Phi_q^r y) = \xi_H(h\Phi_q^r y) = \xi_H(y)$, така че $\xi_H(y) \in \mathrm{Orb}_H(M)^{\Phi_q^r}$ и $\xi_H(M^{h\Phi_q^r}) \subseteq \mathrm{Orb}_H(M)^{\Phi_q^r}$. Вземайки предвид, че ограничението $\xi_H : M^{h\Phi_q^r} \to \mathrm{Orb}_H(M)^{\Phi_q^r}$ има слоеве с $\le |H|$ елемента, стигаме до извода, че

$$\left|\mathrm{Orb}_H(M)^{\Phi_q^r}\right| \ge \left|\xi_H(M^{h\Phi_q^r})\right| \ge \frac{\left|M^{h\Phi_q^r}\right|}{|H|}.$$

Следователно

$$\left|M^{h\Phi_q^r}\right| - \left|\mathrm{Orb}_H(M)^{\Phi_q^r}\right| \le (|H|-1)\left|\mathrm{Orb}_H(M)^{\Phi_q^r}\right|$$

за $\forall h \in H$, $\forall r \in \mathbb{N}$ и $\mathrm{ord}_{\mathfrak{G}}^H(M/\mathrm{Orb}_H(M)) \le 1$.

(iii) Използваме доказателството на Гротендик на Теоремата на Хасе-Вайл (виж също Теорема 3.6 от книгата на Мустаджа [Mustaţă]). По-точно, нека $S := X \times X$ е Декартовият квадрат на X, $\Delta := \{(x,x) \in S \,|\, x \in X\}$ е диагоналът на S, $L_1 := X \times \{x_2\}$ е общ слой на втората канонична проекция $\mathrm{pr}_2 : S \to X$, $\mathrm{pr}_2(x_1,x_2) = x_2$ и $L_2 := \{x_1\} \times X$ е общ слой на първата канонична проекция $\mathrm{pr}_1 : S \to X$, $\mathrm{pr}_1(x_1,x_2) = x_1$. За произволни $h \in H$ и $r \in \mathbb{N}$ да изберем $\varphi := h\Phi_q^r$ и да означим с $\Gamma(\varphi) := \{(x,\varphi(x)) \,|\, x \in X\}$ графика на $\varphi : X \to X$. Тогава индексът на пресичане $\Gamma(\varphi).\Delta = |X^\varphi|$ е равен на броя на φ-рационалните точки на X. Непосредствено се проверява, че $L_1^2 = L_2^2 = 0$, $L_1.L_2 = 1$, $\Delta.L_1 = \Delta.L_2 = 1$, $\Gamma(\varphi).L_2 = 1$ и $\Gamma(\varphi).L_1 = \Gamma(\Phi_q^r).L_1 = q^r$, понеже уравнението $h\Phi_q^r(x) = x_2$ е еквивалентно на $\Phi_q^r(x) = h^{-1}(x_2)$ и има q^r решения върху гладка неприводима проективна крива X, определена над $\mathbb{F}_q$. Каноничният клас K_S на S е числено еквивалентен на дивизора $(2g-2)(L_1+L_2)$ върху повърхнината S и прилагането на формулата за присъединение към Δ и $\Gamma(\varphi)$ дава

$$2g - 2 = \Delta.(\Delta + K_S) = \Delta^2 + 2(2g-2),$$

$$2g-2=\Gamma(\varphi).(\Gamma(\varphi)+K_S)=\Gamma(\varphi)^2+(q^r+1)(2g-2),$$

откъдето $\Delta^2=-(2g-2)$, $\Gamma(\varphi)^2=-q^r(2g-2)$. Теоремата на Ходж за индекса върху $S=X\times X$ гласи, че ако дивизор $E\subset S$ има нулев индекс на пресичане $E.H=0$ с обилен дивизор $H\subset S$, то E има неположителен индекс на самопресичане $E^2\leq 0$. За произволен дивизор $D\subset S$, полагаме $E:=D-(D.L_1)L_2-(D.L_2)L_1$, $H:=L_1+L_2$ и забелязваме, че H е обилен дивизор върху S с $E.H=0$. Следователно

$$0\geq E^2=D^2-2(D.L_1)(D.L_2). \tag{6.27}$$

Ако $D:=a\Delta+b\Gamma(\varphi)$ за някои $a,b\in\mathbb{Z}$, $b\neq 0$ и

$$f(z):=gz^2+(q^r+1-|X^\varphi|)z+gq^r\in\mathbb{Z}[z],$$

то (6.27) е еквивалентно на $f\left(\frac{a}{b}\right)\geq 0$ за $\forall\frac{a}{b}\in\mathbb{Q}$ и е изпълнено точно когато дискриминантата

$$D(f)=(q^r+1-|X^\varphi|)^2-4q^rg^2\leq 0.$$

Следователно,

$$-2gq^{\frac{r}{2}}\leq|X^\varphi|-(q^r+1)\leq 2gq^{\frac{r}{2}}\quad\text{за}\quad\forall r\in\mathbb{N}$$

и, в частност,

$$\left|X^{h\Phi_q^{2r}}\right|\leq(q^{2r}+1)+2gq^r=\left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^{2r}}\right|+2g\left(\left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^{2r}}\right|-1\right)^{\frac{1}{2}}\leq$$
$$\leq\left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^{2r}}\right|+2g\left|\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^{2r}}\right|^{\frac{1}{2}}\quad\text{за}\quad\forall r\in\mathbb{N}.$$

Това доказва неравенството $\mathrm{ord}_{\mathfrak{G}}^H(X/\mathbb{P}^1(\overline{\mathbb{F}_q}))\leq\frac{1}{2}$. □

Следната лесна лема е ключова за доказателството на основната Теорема 142.

Лема 141. *Нека N и L са безкрайни локално крайни модули над $\mathfrak{G}=Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ със затворени стабилизатори, а $\xi_H:N\to L$ е H-Галоа покритие за някоя крайна подгрупа $H<\mathrm{Aut}_{\mathfrak{G}}(N)$ без фиксирани точки. Тогава*

$$\sum_{h\in H}\left|N^{h\Phi_q}\right|=|H|\left|L^{\Phi_q}\right|.$$

Доказателство: От липсата на фиксирани точки на H следва, че $N^{h_1\Phi_q}\cap N^{h_2\Phi_q}=\emptyset$ за всички $h_1,h_2\in H$, $h_1\neq h_2$. Достатъчно е да проверим, че $\xi_H^{-1}(L^{\Phi_q})=\coprod_{h\in H}N^{h\Phi_q}$, за да стигнем до извода, че

$$|H||L^{\Phi_q}|=\left|\xi_H^{-1}(L^{\Phi_q})\right|=\sum_{h\in H}\left|N^{h\Phi_q}\right|.$$

Ако $y\in\xi_H^{-1}(L^{\Phi_q})$, то от $\xi_H(y)=\Phi_q\xi_H(y)=\xi_H(\Phi_q(y))$ следва съществуването на $h\in H$ с $h(y)=\Phi_q(y)$. Следователно $y\in N^{h^{-1}\Phi_q}$ и $\xi_H^{-1}(L^{\Phi_q})\subseteq\coprod_{h\in H}N^{h\Phi_q}$.

Обратно, за всяко $y \in N^{h\Phi_q}$ е в сила $h^{-1}(y) = \Phi_q(y)$, откъдето

$$\xi_H(y) = \xi_H(h^{-1}(y)) = \xi_H(\Phi_q(y)) = \Phi_q \xi_H(y).$$

Това доказва $N^{h\Phi_q} \subseteq \xi_H^{-1}(L^{\Phi_q})$ и $\xi_H^{-1}(L^{\Phi_q}) = \coprod_{h \in H} N^{h\Phi_q}$.

□

Следва основния резултат на тази глава.

Теорема 142. *Нека M е безкраен локално краен модул над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ със затворени стабилизатори и полиномиално ζ-частно $P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = \sum\limits_{j=0}^{d} a_j t^j \in \mathbb{Z}[t]$ от степен $\deg P_M(t) = d \in \mathbb{N}$ със старши коефициент $\mathrm{LC}(P_M(t)) = a_d \in \mathbb{Z} \setminus \{0\}$, а $\lambda := \log_q \sqrt[d]{|a_d|} \in \mathbb{R}^{>0}$. Да предположим, че съществуват $m \in \mathbb{N}$ и $\mathfrak{G}_m = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$-подмодули $M_o \subseteq M$, $L_o \subseteq \mathbb{P}^1(\overline{\mathbb{F}_q})$ с $|M \setminus M_o| < \infty$, $\left|\mathbb{P}^1(\overline{\mathbb{F}_q}) \setminus L_o\right| < \infty$, които свързани с крайно неразклонено покритие $\xi : M_o \to L_o$ на $\mathfrak{G}_m$-модули с обвивка на Галоа (N, H, H_1), определена над $\mathbb{F}_{q^m}$.*

(i) Ако $\lambda \geq 1$, то M изпълнява аналога на хипотезата на Риман относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ като $\mathfrak{G}$-модул.

(ii) Ако

$$\max\left(\mathrm{ord}_{\mathfrak{G}}(M/\mathbb{P}^1(\overline{\mathbb{F}_q})), \mathrm{ord}^H_{\mathfrak{G}_m}(N/\mathbb{P}^1(\overline{\mathbb{F}_q})\right) \leq \lambda < 1,$$

то M изпълнява аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ като $\mathfrak{G}$-модул.

Доказателство: Достатъчно е да докажем, че ако

$$\max(\mathrm{ord}_{\mathfrak{G}}(M/\mathbb{P}^1(\overline{\mathbb{F}_q})), \mathrm{ord}^H_{\mathfrak{G}_m}(N/\mathbb{P}^1(\overline{\mathbb{F}_q})) \leq \lambda, \tag{6.28}$$

то M изпълнява аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ като $\mathfrak{G}$-модул. Поточно, ако $\lambda \geq 1$, то съгласно Лема 138 (i), (ii) е в сила

$$\mathrm{ord}_{\mathfrak{G}}(M/\mathbb{P}^1(\overline{\mathbb{F}_q})) = \mathrm{ord}_{\mathfrak{G}}(M_o/L_o) \leq 1 \leq \lambda,$$

докато от Твърдение 140 (i), (ii) следва, че

$$\mathrm{ord}^H_{\mathfrak{G}_m}(N/\mathbb{P}^1(\overline{\mathbb{F}_q})) = \mathrm{ord}^H_{\mathfrak{G}_m}(N/L_o) \leq 1 \leq \lambda$$

и е в сила (6.28).

Понеже $f(x) = a^x$ е растяща функция на $x \in \mathbb{R}$ за $a \in \mathbb{N}$, $a \geq 2$, от предположението $\mathrm{ord}_{\mathfrak{G}}(M/\mathbb{P}^1(\overline{\mathbb{F}_q})) \leq \lambda$ следва съществуването на такива константи $C_1 \in \mathbb{R}^{>0}$, $\nu_1, r_1 \in \mathbb{N}$, че

$$\left|M^{\Phi_q^{\nu_1 r}}\right| \leq (q^{\nu_1 r} + 1) + C_1(q^{\nu_1 r} + 1)^{\lambda} < (q^{\nu_1 r} + 1) + C_1(2q^{\nu_1 r})^{\lambda} = (q^{\nu_1 r} + 1) + (2^{\lambda} C_1) q^{\lambda \nu_1 r}$$

за $\forall r \in \mathbb{N}$, $r \geq r_1$. Аналогично, $\mathrm{ord}^H_{\mathfrak{G}_m}(N/\mathbb{P}^1(\overline{\mathbb{F}_q})) \leq \lambda$ дава съществуването на константи $C_2 \in \mathbb{R}^{>0}$, $\nu_2, r_2 \in \mathbb{N}$ с

$$\left|N^{h\Phi_q^{\nu_2 r}}\right| \leq (q^{\nu_2 r} + 1) + C_2(q^{\nu_2 r} + 1)^{\lambda} < (q^{\nu_2 r} + 1) + (2^{\lambda} C_2) q^{\lambda \nu_2 r}$$

за $\forall r \in \mathbb{N}$, $r \geq r_2$. За произволно общо кратно $\nu \in \mathbb{N}$ of ν_1 и ν_2 е изпълнено

$$\left|M^{\Phi_q^{\nu r}}\right| < (q^{\nu r}+1) + (2^\lambda C_1) q^{\lambda \nu r} \quad \text{за} \quad \forall r \in \mathbb{N}, \quad r \geq \frac{r_1 \nu_1}{\nu} \tag{6.29}$$

$$\text{и} \quad \left|N^{h\Phi_q^{\nu r}}\right| < (q^{\nu r}+1) + (2^\lambda C_2) q^{\lambda \nu r} \quad \text{за} \quad \forall r \in \mathbb{N}, \quad r \geq \frac{r_2 \nu_2}{\nu}.$$

Ако $\left|\mathbb{P}^1(\overline{\mathbb{F}_q}) \setminus L_o\right| = s$, то разлагането $\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^{\nu r}} = L_o^{\Phi_q^{\nu r}} \coprod (\mathbb{P}^1(\overline{\mathbb{F}_q})^{\Phi_q^{\nu r}} \setminus L_o)$ в непресичащо се обединение дава неравенството $q^{\nu r}+1 \leq \left|L_o^{\Phi_q^{\nu r}}\right| + s$, откъдето

$$\left|N^{h\Phi_q^{\nu r}}\right| < \left|L_o^{\Phi_q^{\nu r}}\right| + s + (2^\lambda C_2) q^{\lambda \nu r} \leq \left|L_o^{\Phi_q^{\nu r}}\right| + (2^\lambda C_2 + 1) q^{\lambda \nu r} \tag{6.30}$$

за $\forall r \in \mathbb{N}$, $r \geq r_o$ е фиксирано естествено число $r_o \geq \max\left(\frac{r_2\nu_2}{\nu}, \frac{\log_q(s)}{\lambda\nu}\right)$. Съгласно Твърдение 136, достатъчно е да установим съществуването на константи $C \in \mathbb{R}^{>0}$, $r_o \in \mathbb{N}$ с

$$\left|M^{\Phi_q^{\nu r}}\right| \geq (q^{\nu r}+1) - C q^{\lambda \nu r} \quad \text{за} \quad \forall r \in \mathbb{N}, \quad r \geq r_o \tag{6.31}$$

и да комбинираме с (6.29), за да стигнем до извода, че M изпълнява аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ като модул над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$.

За тази цел да забележим, че от Лема 141 следва

$$\sum_{h \in H} \left|N^{h\Phi_q^{\nu r}}\right| = |H| \left|L_o^{\Phi_q^{\nu r}}\right| \quad \text{и} \quad \sum_{h \in H_1} \left|N^{h\Phi_q^{\nu r}}\right| = |H_1| \left|M_o^{\Phi_q^{\nu r}}\right| \quad \text{за} \quad \forall r \in \mathbb{N}.$$

Заедно с (6.30), това дава

$$\begin{aligned} |H_1| \left|M_o^{\Phi_q^{\nu r}}\right| &= \sum_{h \in H_1} \left|N^{h\Phi_q^{\nu r}}\right| + |H| \left|L_o^{\Phi_q^{\nu r}}\right| - \sum_{h \in H} \left|N^{h\Phi_q^{\nu r}}\right| = \\ &= |H| \left|L_o^{\Phi_q^{\nu r}}\right| - \sum_{h \in H \setminus H_1} \left|N^{h\Phi_q^{\nu r}}\right| \geq \\ \geq |H| \left|L_o^{\Phi_q^{\nu r}}\right| - (|H| - |H_1|) \left|L_o^{\Phi_q^{\nu r}}\right| - (|H| - |H_1|)(2^\lambda C_2 + 1) q^{\lambda \nu r} &= \\ = |H_1| \left|L_o^{\Phi_q^{\nu r}}\right| - (|H| - |H_1|)(2^\lambda C_2 + 1) q^{\lambda \nu r} & \end{aligned}$$

за $\forall r \in \mathbb{N}$, $r \geq r_o$. Означаваме $C_3 := \left(\frac{|H|-|H_1|}{|H_1|}\right)(2^\lambda C_2 + 1) \in \mathbb{R}^{\geq 0}$ и делим на $|H_1|$, за да получим

$$\left|M_o^{\Phi_q^{\nu r}}\right| \geq \left|L_o^{\Phi_q^{\nu r}}\right| - C_3 q^{\lambda \nu r} \quad \text{за} \quad \forall r \in \mathbb{N}, \quad r \geq r_o.$$

Вземайки предвид $\left|L_o^{\Phi_q^{\nu r}}\right| \geq (q^{\nu r}+1) - s \geq (q^{\nu r}+1) - q^{\lambda \nu r}$ за $r \geq \frac{\log_q(s)}{\lambda \nu}$, стигаме до извода, че

$$\left|M_o^{\Phi_q^{\nu r}}\right| \geq (q^{\nu r}+1) - (C_3+1) q^{\lambda \nu r} \quad \text{за} \quad \forall r \in \mathbb{N}, \quad r \geq r_o.$$

Комбинирайки с $\left|M^{\Phi_q^{\nu r}}\right| \geq \left|M_o^{\Phi_q^{\nu r}}\right|$, проверяваме (6.31) с $C := C_3 + 1$ и завършваме доказателството на теоремата.

□

Съгласно Твърдение 135, Лема 138 (iv) и Твърдание 140 (iii), произволна гладка неприводима крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ от род $g \geq 1$ изпълнява предположенията на Теорема 142 с $\lambda = \frac{1}{2}$ като локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул. Следващото твърдение дава пример за локално краен $\mathfrak{G}$-модул M, който изпълнява предположенията на Теорема 142 с $\lambda = 0$. Следователно M изпълнява аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ като $\mathfrak{G}$-модул и не е изоморфен (като $\mathfrak{G}$-модул) на гладка неприводима проективна крива, определена над $\mathbb{F}_q$.

Твърдение 143. *За произволно крайно поле $\mathbb{F}_q$ и $\forall x_1 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ квази-афинната крива $M := \overline{\mathbb{F}_q} \setminus \{x_1, x_1^q\}$, определена над $\mathbb{F}_{q^2}$ е локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул с*

$$\zeta_M(t) = \frac{(1-t)(1+t)}{1-qt}, \tag{6.32}$$

който изпълнява предположенията на Теорема 142. По този начин, M изпълнява аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ като модул над $\mathfrak{G}$ и M не е изоморфно (като $\mathfrak{G}$-модул) на гладка неприводима проективна крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ от род $g \geq 1$, определена над $\mathbb{F}_q$.

Доказателство: Тъждественото влагане $\mathrm{Id} : M \hookrightarrow \mathbb{P}^1(\overline{\mathbb{F}_q}) = \overline{\mathbb{F}_q} \cup \{\infty\}$ е крайно неразклонено покритие на $\mathfrak{G}$-модули от степен 1 над образа си. То има обвивка на Галоа $(M, \{\mathrm{Id}_M\}, \{\mathrm{Id}_M\})$. Ако $\zeta_M(t)$ се задава като (6.32), то

$$P_M(t) := \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = (1-t)^2(1+t) \in \mathbb{Z}[t]$$

е полином от степен $\deg P_M(t) = 3$ с $a_3 = \mathrm{LC}(P_M(t)) = 1$, така че $\lambda := \log_q \sqrt[3]{|a_3|} = 0$. Понеже M е $\mathfrak{G}$-подмодул на $\mathbb{P}^1(\overline{\mathbb{F}_q})$ с $\left|\mathbb{P}^1(\overline{\mathbb{F}_q}) \setminus M\right| = 3 < \infty$, относителния порядък $\mathrm{ord}_{\mathfrak{G}}(M/\mathbb{P}^1(\overline{\mathbb{F}_q})) = \mathrm{ord}_{\mathfrak{G}}(M/M) = 0 = \lambda$, съгласно Лема 138 (i) и M изпълнява предположенията на Теорема 142. Ако M е изоморфен на гладка неприводима крива $X/\mathbb{F}_q \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ като модул над $\mathfrak{G}$, то полиномът $P_M(t) = P_X(t) \in \mathbb{Z}[t]$ би трябвало да е от четна степен $\deg P_M(t) = 2g \in \mathbb{N}$ и $\lambda := \log_q \sqrt[2g]{|\mathrm{LC}(P_M(t))|} = \frac{1}{2}$, което противоречи на (6.32).

За пресмятането на $\zeta_M(t)$, да забележим, че $\overline{\mathbb{F}_q}$ е локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул и $\mathrm{Orb}_{\mathfrak{G}}(x_1) = \{x_1, x_1^q\}$, за да стигнем до извода, че M е локално краен $\mathfrak{G}$-модул. Още повече, $x_1, x_1^q \in \overline{\mathbb{F}_q}^{\Phi_q^{2r}} = \mathbb{F}_{q^{2r}}$ и $x_1, x_1^q \notin \overline{\mathbb{F}_q}^{\Phi_q^{2r+1}} = \mathbb{F}_{q^{2r+1}}$ за $\forall r \in \mathbb{Z}^{\geq 0}$. Следователно

$$\left|M^{\Phi_q^{2r}}\right| = \left|\overline{\mathbb{F}_q}^{\Phi_q^{2r}}\right| - 2 = q^{2r} - 2, \quad \forall r \in \mathbb{N}, \quad \left|M^{\Phi_q^{2r+1}}\right| = \left|\overline{\mathbb{F}_q}^{\Phi_q^{2r+1}}\right| = q^{2r+1}, \quad \forall r \in \mathbb{Z}^{\geq 0},$$

откъдето

$$\log \zeta_M(t) = \sum_{r=1}^{\infty} \left|M^{\Phi_q^r}\right| \frac{t^r}{r} = \sum_{r=1}^{\infty} (q^{2r} - 2)\frac{t^{2r}}{2r} + \sum_{r=0}^{\infty} q^{2r+1} \frac{t^{2r+1}}{2r+1} =$$

$$= \sum_{r=1}^{\infty} q^r \frac{t^r}{r} - \sum_{r=1}^{\infty} \frac{t^{2r}}{r} = \log\left(\frac{1}{1-qt}\right) - \log\left(\frac{1}{1-t^2}\right) = \log\left(\frac{1-t^2}{1-qt}\right)$$

съгласно (6.4). Това е достатъчно за (6.32). □

Следващото следствие установява, че от аналога на хипотезата на Риман относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ за локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул M следва функционално уравнение за полиномиалното ζ-частно $P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} \in \mathbb{Z}[t]$.

Следствие 144. *Нека M е безкраен локално краен модул над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, който изпълнява аналога на хипотезата на Рима относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Тогава полиномиалното ζ-частно $P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = \sum_{j=0}^{d} a_j t^j \in \mathbb{Z}[t]$ на M удовлетворява функционалното уравнение*

$$P_M(t) = \operatorname{sign}(a_d) P_M\left(\frac{1}{q^{2\lambda}t}\right) q^{\lambda d} t^d \quad \text{за} \quad \lambda := \log_q \sqrt[d]{|a_d|}.$$

Доказателство: Ако $P_M(t) = \prod_{j=1}^{d}(1 - q^{\lambda} e^{i\varphi_j} t)$ за някакви $\varphi_j \in [0, 2\pi)$, то старшият коефициент $\operatorname{LC}(PM(t)) = a_d = (-1)^d q^{\lambda d} e^{i\left(\sum_{j=1}^{d} \varphi_j\right)}$, откъдето

$$P_M\left(\frac{1}{q^{2\lambda}t}\right) = \frac{a_d}{q^{2\lambda d} t^d} \prod_{j=1}^{d}(1 - q^{\lambda} e^{-i\varphi_j} t).$$

Полиномът $P_M(t) \in \mathbb{Z}[t]$ има реални коефициенти и е инвариантен относно комплексното спрягане. Затова множествата $\left\{e^{i\varphi_j} \,|\, 1 \le j \le d\right\} = \left\{e^{-i\varphi_j} \,|\, 1 \le j \le d\right\}$ съвпадат, броени с кратности и $P_M(t) = \prod_{j=1}^{d}(1 - q^{\lambda} e^{-i\varphi_j} t)$. Това позволява да изразим

$$P_M\left(\frac{1}{q^{2\lambda}t}\right) = \frac{a_d}{q^{2\lambda d}} P_M(t) t^{-d}.$$

Използвайки $|a_d| = q^{\lambda d}$ and $a_d = \operatorname{sign}(a_d)\,|a_d|$, стигаме до извода, че

$$P_M\left(\frac{1}{q^{2\lambda}t}\right) = \frac{\operatorname{sign}(a_d)}{q^{\lambda d}} P_M(t) t^{-d}.$$

□

Библиография

[Bombieri] E. Bombieri, Counting Points on Curves over Finite Fields, Sém. Bourbaki, No. 430, 1972/73.

[Додунеков, Ланджев] S. Dodunekov and I. Landgev, Near MDS-codes, *Journal of Geometry*, **54** (1995), 30–43.

[Duursma1] I. Duursma, From weight enumerators to zeta functions, *Discrete Applied Mathematics*, **111** (2001), 55—73.

[Duursma2] I. Duursma, Weight distribution of geometric Goppa codes, *Transections of the American Mathematical Society*, **351** (1999), 3609–3639.

[Duursma3] I. Duursma Combinatorics of the two-variable zeta function in *In: Mullen G.L., Poli A., Stichtenoth H. (eds) Finite Fields and Applications.* Lecture Notes in Computational Sciences **2948**, Springer, Berlin, Heidelberg (2004), 109–136.

[KM1] A. Kasparian, I. Marinov, Duursma's reduced polynomial, Advances in Mathematics of Communication, vol. 11, № 4, November 2017.

[KM2] A. Kasparian, I. Marinov, Mac Williams identities and polarized Riemann-Roch conditions, Electronic Notes in Discrete Mathematics, vol. 57, 2017.

[KM3] A. Kasparian, I. Marinov, Riemann Hypothesis Analogue for locally finite modules over the absolute Galois group of a finite field, accepted for a publication in Annuaire de l'Université de Sofia "St. Kl. Ohridski"

[Kim, Hyun] D. Ch. Kim and J. Y. Hyun, A Riemann hypothesis analogue for near-MDS codes, *Discrete Applied Mathematics*, **160** (2012), 2440–2444.

[Mustaţă] M. Mustaţă, *Zeta Functions in Algebraic Geometry*, Lecture Notes of Mihnea Popa.

[Niederreiter, Xing] Niederreiter H., Xing Ch., *Algebraic Geometry in Coding Theory And Cryptography*, Princeton University Press, 2009

[PShW] R. Pellikaan, B.-Z. Shen, G. J. M. van Wee, Which linear codes are algebraic geometric?, IEEE Trans. Inform. Theory **IT-37** (1991), 583-602.

[Shafarevich] Shafarevich, I.R., *Basics of Algebraic Geometry*, (Science, Moscow, 1988).

[Stichtenoth] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 1993.

[Tsafman, Vladut, Nogin] M. Tsfasman, S. Vlăduţ, D. Nogin, *Algebraic Geometry Codes: Basic Notions,* Providence, RI: American Mathematical Society, 2007

[Ward] H. K. Ward, The Mac Williams Identity, Preprint.