Глава 3

Крайни полета

3.1 Дефиниция и основни свойства

Дефиниция 3.1.1. *Поле с краен брой елементи се нарича* ***крайно поле.*** *Употребява се и наименованието* ***поле на Галоа.***

Теорема 3.1.2. *Всяко крайно поле F има крайна характеристика $p > 0$ и броят на елементите му е степен на характеристиката, т.е. $|F| = p^n$. Елементите на F се изчерпват с кореният на уравнението $x^q = x$, където $q = |F|$.*

Доказателство. Ако $char\, F = 0$, то $n1 \neq m1$ за всеки естествени $n \neq m$, което противоречи на $|F| < \infty$. Следователно $char\, F = p > 0$. Тогава F съдържа $\mathbb{Z}_p$ като просто подполе и може да се разглежда като линейно пространство над $\mathbb{Z}_p$. Ако $\dim_{\mathbb{Z}_p} F = n$, то $|F| = p^n$.
Следователно мултипликативната група на полето $F^* = F \setminus \{0\}$ се състои от $p^n - 1$ елемента. Но тогава за всеки елемент $\alpha \in F^*$ е изпълнено $\alpha^{p^n-1} = 1$. Следователно $\alpha^{p^n} = \alpha$, за всяко $\alpha \in F$, т.е. елементите на F изчерпват корените на $x^{|F|} = x$. □

Лема 3.1.3. *Всяка крайна подгрупа на мултипликативната група на едно поле е циклична.*

Доказателство. Нека F е произволно поле и G е подгрупа на мултипликативната му група F^*. Нека $|G| = n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, където p_j са различни прости числа. Ако допуснем, че експонентата m на групата (т.е. минималното естествено число m, за което $x^m = 1$ за всяко $x \in G$) е по-малка от $n = |G|$, то всеки елемент на групата е корен на уравнението $x^m - 1 = 0$. Но тъй като това уравнение има най-много m корена, то $n = |G| \leq m$, което противоречи на допускането. Следователно $m = n$.
Тогава за всяко i съществува α_i, такова че $\alpha_i^{\frac{n}{p_i}} \neq 1$, но разбира се $\alpha_i^n = 1$, тъй като противното би означавало, че n/p_i е експонента. В такъв случай $\gamma_i = \alpha_i^{n/p_i^{e_i}}$

има ред точно $p_i^{e_i}$. Тъй като G е комутативна група и p_j са различни прости числа, то $\gamma = \gamma_1\gamma_2\dots\gamma_k$ има ред

$$o(\gamma) = \text{НОК}[p_1^{e_1}, p_2^{e_2}, \dots, p_k^{e_k}] = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k} = n.$$

Следователно $G =< \gamma >$. □

Като непосредствено следствие от лемата получаваме следното свойство на крайните полета.

Теорема 3.1.4. *Мултипликативната група на всяко крайно поле е циклична.*

Доказателство. $G = F^*$ е крайна група. □

Дефиниция 3.1.5. *Примитивен елемент на крайното поле F наричаме всеки образуващ на цикличната група F^*.*

Теорема 3.1.6. *Всяко крайно поле F с характеристика p е просто разширение на $\mathbb{Z}_p$ и степента на разширение $n = [F : \mathbb{Z}_p]$ съвпада със степента на неразложимия полином $m(x)$ на примитивен елемент на полето. Полиномът $m(x)$ е делител на $x^{p^n} - x$.*

Доказателство. Съгласно Теореми 3.1.2 и 3.1.4 съществува α от F, такъв че $F^* = \{1, \alpha, \alpha^2, \dots, \alpha^{p^n-2}\}$, т.е. α е примитивн елемент на F. Но в такъв случай $\mathbb{Z}_p(\alpha) \supset F$. От друга страна F съдържа $\mathbb{Z}_p$ и α, и тъй като по дефиниция $\mathbb{Z}_p(\alpha)$ е сечение на всички полета с това свойство, то $\mathbb{Z}_p(\alpha) \subset F$. Следователно $\mathbb{Z}_p(\alpha) = F$. Тогава, както е добре известно, $n = [F : \mathbb{Z}_p] = \deg \mathbf{irr}_F\alpha, \quad m(x) = \mathbf{irr}_F\alpha$. Но тъй като всички елементи на F са корени на $x^{p^n} - x$, то неразложимият полином $m(x)$ трябва да е негов делител. □

Теорема 3.1.7. *За всяко просто число p и всяко естествено число n съществува единствено с точност до изоморфизъм поле с p^n елемента.*

Доказателство. Съществуване. Нека F е полето на разлагане на полинома $x^{p^n} - x$ над Z_p. Да разгледаме

$$\bar{F} = \{\alpha \in F \mid \alpha^{p^n} = \alpha\}.$$

$\bar{F}$ е подполе. Наистина $(\alpha\pm\beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha\pm\beta$ и $(\alpha\beta^{-1})^{p^n} = \alpha^{p^n}\beta^{-p^n} = \alpha\beta^{-1}$. Но в такъв случай $\bar{F}$ е поле, съдържащо всички корени на $x^{p^n} - x = 0$, откъдето и минималността на полето на разлагане следва, че $F = \bar{F}$. Следователно $|F| = p^n$.

Нека α е корен на $x^{p^n} - x = 0$ и има неразложим полином $m(x)$ от степен $\deg m(x) = n$. Тогава

$$\mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/m(x)$$

и $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n$, т.е. $|\mathbb{Z}_p(\alpha)| = p^n = |F|$. Следователно $F = \mathbb{Z}_p(\alpha)$.

Единственост. Нека F_1 и F_2 са две полета с по p^n елемента. Съгласно Теорема 3.1.6 $F_1 = \mathbb{Z}_p(\alpha)$ за някое $\alpha \in F_1$ и нека $m(x) = \mathbf{irr}_F\alpha$, където $\deg m(x) = n$ и $m(x) \mid (x^{p^n} - x)$. Но елементите на F_2 също са корени на $x^{p^n} - x$. Следователно съществува $\beta \in F_2$, такова че $m(\beta) = 0$. От $F_2 \supset \mathbb{Z}_p(\beta)$ и $[\mathbb{Z}_p(\beta) : \mathbb{Z}_p] = n$, следва че $F_2 = \mathbb{Z}_p(\beta)$. Сега изоморфността на двете полета следва от

$$F_1 = \mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/m(x) \cong \mathbb{Z}_p(\beta) = F_2.$$

Самият изоморфизъм σ се задава с

$$\sigma : \left| \begin{array}{rcl} F_1 = \mathbb{Z}_p(\alpha) & \to & \mathbb{Z}_p(\beta) = F_2 \\ f(\alpha) & \to & f(\beta) \end{array} \right.$$

Напомняме, че действията в F_1 и F_2 се извършват като се има предвид, че $m(\alpha) = m(\beta) = 0$, т.е. по модул $m(x)$. □

Единственото с точност до изоморфизъм крайно поле с p^n елемента бележим с $GF(p^n)$.

Теорема 3.1.8. *Полето $F = GF(p^n)$ съдържа като подполе $L \cong GF(p^m)$ тогава и само тогава, когато $m|n$.*

Доказателство. Необходимост. Нека $L \subset F$. Тогава

$$n = [F : \mathbb{Z}_p] = [F : L][L : \mathbb{Z}_p] = [F : L].m.$$

Следователно $m \mid n$.

Достатъчност. Нека $m \mid n$. Тогава $(p^n - 1) \mid (p^m - 1)$, откъдето получаваме

$$(x^{p^m-1} - 1) \mid (x^{p^n-1} - 1) \quad \text{т. е.} \quad (x^{p^m} - x) \mid (x^{p^n} - x).$$

да разгледаме

$$L = \{\alpha \in F \mid \alpha^{p^m} = \alpha\}.$$

L е поле с p^m елемента (виж Теорема 3.1.7) и следователно $F \supset GF(p^m)$. □

Теорема 3.1.9. *Корените на всеки неразложим полином $f(x)$ с коефициенти от $GF(q)$, $q = p^n$, и степен m се изчерпват с*

$$\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}},$$

където $m = \deg f(x)$.

Доказателство. Нека $f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m$, $a_i \in GF(q)$. Съгласно Теорема 3.1.2 $a_i^q = a_i$, за всяко i. Нека α е корен на $f(x)$. Тогава

$$[f(\alpha)]^q = a_0^q(\alpha^m)^q + a_1^q(\alpha^{m-1})q + \cdots + a_m^q = a_0(\alpha^q)^m + a_1(\alpha^q)^{m-1} + \cdots + a_m.$$

Следователно α^q също е корен на $f(x)$. Твърдението следва от факта, че $\alpha^{q^m} = \alpha$, но $\alpha^{q^j} \neq \alpha$ за $j < m$, тъй като $[F(\alpha) : F] = m$ (т. е. $F(\alpha) = GF(q^m)$) и $f(x)$ неразложим. □

Теорема 3.1.10. *В полето $F = GF(p^n)$ има точно n автоморфизма*

$$\varepsilon, \varphi, \varphi^2, \ldots, \varphi^{n-1},$$

където

$$\varphi : \left| \begin{array}{l} F \longrightarrow F \\ x \longrightarrow x^p \end{array} \right.$$

Доказателство. φ е автоморфизъм, тъй като $(x \pm y)^p = x^p \pm y^p$ и $(xy^{-1})^p = x^p(y^p)^{-1}$.
Нека ψ е произволен автоморфизъм на полето. Тогава $\psi(0) = 0$, $\psi(1) = 1$ и $\psi(k.1) = k.1$, за всяко естествено k. Следователно ψ запазва неподвижни елементите на $\mathbb{Z}_p$. Нека α е примитивен елемент на F. Неговият неразложим полином $m(x)$ е от степен n и $m(x)$ дели $x^{p^n} - x$. Тогава

$$\begin{aligned} m(\psi(\alpha)) &= (\psi(\alpha))^m + a_1(\psi(\alpha))^{m-1} + \cdots + a_m \\ &= \psi(\alpha^m + a_1\alpha^{m-1} + \cdots + a_m) = \psi(0) = 0 \end{aligned}$$

Следователно $\psi(\alpha)$ е корен на $m(x)$ и за подходящо $k = 1, 2, \ldots, n-1$ е в сила $\psi(\alpha) = \alpha^{p^k}$, т. е. $\psi = \varphi^k$. □

Пример 3.1.11. Ще построим полето $GF(2^4)$. Съгласно Теорема 3.1.7

$$GF(2^4) = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_i \in \mathbb{Z}_2\} \cong \mathbb{Z}_2[x]/m(x),$$

където $m(x)$ е неразложим над $\mathbb{Z}_2$ полином от степен 4 и α е негов корен. Има два (реципрочни са) неразложими над $\mathbb{Z}_2$ полинома. Да изберем $m(x) = x^4 + x + 1$. α се явява примитивен елемент на $GF(2^4)$. (Да отбележим, че за по-големи полета това не винаги е така, но може да се избере примитивен елемент, т.е. подходящ полином.) Елементите на полето в мултипликативно (като степен на α) и адитивно представяне (отляво е коефициента a_0) са дадени в таблица 3.1.11. Действията при адитивния запис се извършват като с полиноми на α, но по модул $m(x)$, т.е. при условието $\alpha^4 + \alpha + 1$. Ако разполагаме с мултипликативния и адитивния запис, по-добре е умножението да се извърши чрез събиране на степените по модул 15, а събирането - с двоичните вектори. Например

$$(\alpha^2 + \alpha^3) + (1 + \alpha^2 + \alpha^3) = 1 \text{ или } 0011 + 1011 = 1000,$$

$$(\alpha^2 + \alpha^3).(1 + \alpha^2 + \alpha^3) = \alpha^6\alpha^{13} = \alpha^{19} = \alpha^4 = 1 + \alpha.$$

Степен на α	Полином от α
0	0000
1	1000
α	0100
α^2	0010
α^3	0001
α^4	1100
α^5	0110
α^6	0011
α^7	1101
α^8	1010
α^9	0101
α^{10}	1110
α^{11}	0111
α^{12}	1111
α^{13}	1011
α^{14}	1001

Таблица 3.1: Елементите на полето $GF(16)$.

3.2 Следа и норма при крайни полета

3.2.1 Следа

Дефиниция 3.2.1. ***Следа*** *се нарича функцията* $\mathrm{Tr}_{q^n/q} : GF(q^n) \to GF(q)$ *дефинирана с*

$$\mathrm{Tr}_{q^n/q}(\alpha) \stackrel{def}{=} \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}. \tag{3.1}$$

Казва се, че $\mathrm{Tr}_{q^n/q}(\alpha)$ *е следата на* α *от* $GF(q^n)$ *над* $GF(q)$.

Когато q *е просто число следата се нарича* ***абсолютна следа****.*

За удобство при изписване на математическия текст ще ползваме символа $\mathbb{F}_{q^n}$ вместо $GF(q^n)$.

$\mathrm{Tr}_{q^n/q}(\alpha)$ е елемент на $\mathbb{F}_q$, тъй като $\mathrm{Tr}_{q^n/q}(\alpha)^q = \mathrm{Tr}_{q^n/q}(\alpha)$. Например, ако $\alpha \in \mathbb{F}_{2^4}$ то $\mathrm{Tr}_{2^4/2}(\alpha) = \alpha + \alpha^2 + \alpha^4 + \alpha^8 \in \mathbb{F}_2$ докато $\mathrm{Tr}_{2^4/2^2}(\alpha) = \alpha + \alpha^4 \in \mathbb{F}_{2^4}$.

Ще използваме за краткост означението $\mathrm{Tr}(\alpha)$ вместо $\mathrm{Tr}_{q^n/q}(\alpha)$, когато няма опасност от двусмисленост. Със същата цел ще използваме означението Tr_d вместо Tr_{q^n/q^d} при d делител на n, т. е.

$$\mathrm{Tr}_d(\alpha) = \alpha + \alpha^{q^d} + \alpha^{q^{2d}} + \cdots + \alpha^{q^{(\frac{n}{d}-1)d}}.$$

Теорема 3.2.2. *Функцията следа притежава следните свойства:*

(i) $\mathrm{Tr}_{q^n/q}(a\alpha + b\beta) = a\,\mathrm{Tr}_{q^n/q}(\alpha) + b\,\mathrm{Tr}_{q^n/q}(\beta)$ *за всеки* $\alpha, \beta \in \mathbb{F}_{q^n},\ a, b \in \mathbb{F}_q$;

(ii) $\mathrm{Tr}_{q^n/q^d}(\alpha^{q^{kd}}) = \mathrm{Tr}_{q^n/q^d}(\alpha)$ *за всяко* $\alpha \in \mathbb{F}_{q^n}$ *и* $d|n$;

(iii) $\mathrm{Tr}_{q^n/q}(a) = na = \underbrace{a + a + \cdots + a}_{n}$ *за всяко* $a \in \mathbb{F}_q$;

(iv) *Функцията* $\mathrm{Tr}_{q^n/q}$ *е линейно над* $\mathbb{F}_q$ *изображение от* $\mathbb{F}_{q^n}$ *върху* $\mathbb{F}_q$;

(v) *Нека* $d|n$. *За всяко* $b \in \mathbb{F}_{q^d}$ *броят* $|\{\alpha \in \mathbb{F}_{q^n} \mid \mathrm{Tr}_{q^n/q^d}(\alpha) = b\}| = q^{n-d}$;

(vi) $\mathrm{Tr}_{q^n/q}(\alpha) = \mathrm{Tr}_{q^d/q}(\mathrm{Tr}_{q^n/q^d}(\alpha))$ *за всяко* $d|n$.

(vii) *Ако* $\boldsymbol{irr}_{\mathbb{F}_q}(\alpha) = x^d + a_1x^{d-1} + \cdots + a_d$ *е минималният полином на* $\alpha \in \mathbb{F}_{q^n}$ *над* $\mathbb{F}_q$, *то* $d|n$ *и*

$$\mathrm{Tr}_{q^d/q}(\alpha) = -a_1, \qquad \mathrm{Tr}_{q^n/q}(\alpha) = -\frac{n}{d}\,a_1.$$

Доказателство. **(i):** Следва от $(a\alpha + b\beta)^q = a\alpha^q + b\beta^q$ и $a^q = a,\ b^q = b$.
(ii): Повдигането на α на степен q само завърта циклично надясно събираемите в (3.1).
(iii): $a^q = a$ за всяко $a \in \mathbb{F}_q$.
(iv): Линейността следва от (i). Съществува поне едно $\alpha \in \mathbb{F}_{q^n}$ със следа $\mathrm{Tr}_{q^n/q}(\alpha) = a \neq 0$. В противния случай всички елементи на $\mathbb{F}_{q^n}$ ще бъдат корени на полином от степен $q^{n-1} < q^n$, което е невъзможно. Тогава $\beta = a^{-1}\alpha$ има следа 1 и следователно за всяко $b \in \mathbb{F}_q$ е в сила $\mathrm{Tr}_{q^n/q}(b\beta) = b\,\mathrm{Tr}_{q^n/q}(\beta) = b$.
(v): Множеството $A_0 = \{\alpha \in \mathbb{F}_{q^n} \mid \mathrm{Tr}_{q^n/q^d}(\alpha) = 0\}$ е адитивна подгрупа на $\mathbb{F}_{q^n}$, а $A_b = \{\alpha \in \mathbb{F}_{q^n} \mid \mathrm{Tr}_{q^n/q^d}(\alpha) = b\}$ за $b \neq 0$ са останалите $q^d - 1$ съседни класове по A_0 в $\mathbb{F}_{q^n}$. Следователно $|A_b| = q^n/q^d = q^{n-d}$.
(vi): $\mathrm{Tr}_{q^n/q^d}(\alpha) = \alpha + \alpha^{q^d} + \cdots + \alpha^{q^{n-d)}} = \beta \in \mathbb{F}_{q^d}$. Тогава

$$\mathrm{Tr}_{q^d/q}(\beta) = \sum_{i=0}^{d-1}(\alpha + \alpha^{q^d} + \cdots + \alpha^{q^{n-d}})^{q^i} = \mathrm{Tr}_{q^n/q}(\alpha).$$

(vii): $\alpha \in \mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$, thus $d|n$. От Теорема 3.1.9 и формулите на Виет следва, че $\mathrm{Tr}_{q^d/q}(\alpha) = -a_1$. Тогава съгласно (vi) и (iv)

$$\mathrm{Tr}_{q^n/q}(\alpha) = \mathrm{Tr}_{q^d/q}(\mathrm{Tr}_{q^n/q^d}(\alpha)) = \mathrm{Tr}_{q^d/q}\left(\frac{n}{d}\alpha\right) = \frac{n}{d}\,\mathrm{Tr}_{q^d/q}(\alpha) = -\frac{n}{d}\,a_1.$$

□

Упражнение 3.2.3. *Покажете, че* $\mathrm{Tr}_{q^n/q}(\alpha^{q^k+1}) = \mathrm{Tr}_{q^n/q}(\alpha^{q^{n-k}+1}), \quad \alpha \in \mathbb{F}_{q^n}$.

Упражнение 3.2.4. *Покажете, че* $\mathrm{Tr}_{q^n/q}(ax+bx^q) = \mathrm{Tr}_{q^n/q}((a+c)x), \quad a, b, x \in \mathbb{F}_{q^n}, \quad c^q = b$.

Теорема 3.2.5. *Нека за всяко $\alpha \in \mathbb{F}_{q^n}$ означим с $L_\alpha : \mathbb{F}_{q^n} \to \mathbb{F}_q$ изображението дефинирано с $L_\alpha(x) = \mathrm{Tr}(\alpha x)$. Тогава $L_\alpha \neq L_\beta$ за $\alpha \neq \beta$ и множеството $L = \{L_\alpha \mid \alpha \in \mathbb{F}_{q^n}\}$ съвпада с групата от всички линейни над $\mathbb{F}_q$ изображения от $\mathbb{F}_{q^n}$ в $\mathbb{F}_q$.*

Доказателство. Изображенията L_α и L_β съвпадат точно когато $L_\alpha(x) - L_\beta(x) = 0$ за всяко $x \in \mathbb{F}_{q^n}$. Но $L_\alpha(x) - L_\beta(x) = \mathrm{Tr}(\alpha x) - \mathrm{Tr}(\beta x) = \mathrm{Tr}((\alpha - \beta)x)$, което е нула за всяко x тогава и само тогава, когато $\alpha - \beta = 0$, т. е. $\alpha = \beta$. Следователно $|\{L_\alpha \mid \alpha \in \mathbb{F}_{q^n}\}| = |\mathbb{F}_{q^n}| = q^n$. От друга страна всяко линейно над $\mathbb{F}_q$ изображение на $\mathbb{F}_{q^n}$ в $\mathbb{F}_q$ се определя еднозначно от образите на елементите от базиса на $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$. Следователно броят на всички линейни изображения е q^n, т. е. колкото е и мощността на L. □

Един често използван факт е следната теорема:

Теорема 3.2.6. *Нека $\alpha \in \mathbb{F}_{q^n}$. $\mathrm{Tr}_{q^n/q}(\alpha) = 0$ тогава и само тогава, когато съществува $\beta \in \mathbb{F}_{q^n}$, такова че $\alpha = \beta^q - \beta$.*

Ние ще докажем малко по-общ резултат:

Теорема 3.2.7. *За всяко естествено число k, за което $d = (n, k)$ елементът $\alpha \in \mathbb{F}_{q^n}$ удовлетворява $\mathrm{Tr}_{q^n/q^d}(\alpha) = 0$ тогава и само тогава, когато може да се представи във вида $\alpha = \beta^{q^k} - \beta$ за някое $\beta \in \mathbb{F}_{q^n}$.*

Доказателство. Съгласно (v) на Теорема 3.2.10 $|A_0| = |\{\alpha \in \mathbb{F}_{q^n} \mid \mathrm{Tr}_{q^n/q^d}(\alpha) = 0\}| = q^{n-d}$. От друга страна $\mathrm{Tr}_{q^n/q^d}(\beta^{q^k}) - \mathrm{Tr}_{q^n/q^d}(\beta) = 0$ за всяко $\beta \in \mathbb{F}_{q^n}$. Следователно $\beta^{q^k} - \beta \in A_0$ за всяко $\beta \in \mathbb{F}_{q^n}$, т. е. $B = \{\beta^{q^k} - \beta \mid \beta \in \mathbb{F}_{q^n}\} \subseteq A_0$. Освен това $\beta^{q^k} - \beta = \gamma^{q^k} - \gamma$ тогава и само тогава, когато $(\beta - \gamma)^{q^k} = \beta - \gamma$, т.е. $\beta - \gamma \in \mathbb{F}_{q^k} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^{(n,k)}}$. Следователно $|B| = q^n/q^{(n,k)} = q^{n-d} = |A_0|$. Това означава, че $B \equiv A_0$. □

Непосредствено следствие от предната теорема е следният факт

Теорема 3.2.8. *Уравнението $x^{q^k} - x - \alpha = 0, \quad \alpha \in \mathbb{F}_{q^n}$, има решение в $\mathbb{F}_{q^n}$ тогава и само тогава, когато $\mathrm{Tr}_{q^n/q^d}(\alpha) = 0$, където $d = (n, k)$. В този случай решенията са q^d на брой и представляват множеството $\beta_0 + \mathbb{F}_{q^d}$, където β_0 е едно частно решение.*

Доказателство. От доказателството на предната теорема следва, че $\gamma = \beta - \delta$, където $\delta \in \mathbb{F}_{q^d}$. □

3.2.2 Норма на елемент

Дефиниция 3.2.9. ***Норма*** *се нарича функцията* $\mathrm{N}_{q^n/q} : GF(q^n) \to GF(q)$ *дефинирана с*

$$\mathrm{N}_{q^n/q}(\alpha) \stackrel{def}{=} \alpha\alpha^q\alpha^{q^2}\cdots\alpha^{q^{n-1}} = \alpha^{(q^n-1)/(q-1)}. \tag{3.2}$$

Казва се, че $\mathrm{N}_{q^n/q}(\alpha)$ *е нормата на елемента* α *от* $GF(q^n)$ *над* $GF(q)$.

Когато q *е просто число говорим за* ***абсолютна норма.***

Теорема 3.2.10. *Функцията норма притежава следните свойства:*

(i) $\mathrm{N}_{q^n/q}(\alpha\beta) = \mathrm{N}_{q^n/q}(\alpha)\,\mathrm{N}_{q^n/q}(\beta)$ *за всеки* $\alpha, \beta \in \mathbb{F}_{q^n}$;

(ii) $\mathrm{N}_{q^n/q^d}(\alpha^{q^{kd}}) = \mathrm{N}_{q^n/q^d}(\alpha)$ *за всяко* $\alpha \in \mathbb{F}_{q^n}$ *и* $d|n$, *в частност* $\mathrm{N}_{q^n/q}(\alpha^{q^k}) = \mathrm{N}_{q^n/q}(\alpha)$, $k \neq 0$ *цяло;*

(iii) $\mathrm{N}_{q^n/q}(a) = \underbrace{aa\cdots a}_{n} = a^n$ *за всяко* $a \in \mathbb{F}_q$;

(iv) $\mathrm{N}_{q^n/q}(\alpha) = \mathrm{N}_{q^d/q}(\mathrm{N}_{q^n/q^d}(\alpha))$ *за всяко* $d|n$;

(v) *Ако* $\boldsymbol{irr}_{\mathbb{F}_q}(\alpha) = x^d + a_1x^{d-1} + \cdots + a_d$ *е минималният полином на* $\alpha \in \mathbb{F}_{q^n}$ *над* $\mathbb{F}_q$, *то* $d|n$ *и*

$$\mathrm{N}_{q^d/q}(\alpha) = (-1)^d a_d, \qquad \mathrm{N}_{q^n/q}(\alpha) = (-1)^n\, a_d^{\frac{n}{d}}.$$

(vi) *Нека* $d|n$. *За всяко* $b \in \mathbb{F}_{q^d}^*$ *броят* $|\{\alpha \in \mathbb{F}_{q^n} \mid \mathrm{N}_{q^n/q^d}(\alpha) = b\}| = \dfrac{q^n-1}{q^d-1}$;

Доказателство. **(i):** Следва от $(\alpha\beta)^{(q^n-1)/(q-1)} = \alpha^{(q^n-1)/(q-1)}\beta^{(q^n-1)/(q-1)}$.
(ii): Повдигането на α на степен q (или q^{-1}) само завърта циклично надясно (наляво) множителите в (3.2).
(iii): $a^{q^i} = a$ за всяко $a \in \mathbb{F}_q$.
(iv): $\mathrm{N}_{q^n/q}(\alpha) = \alpha^{\frac{q^n-1}{q-1}} = \alpha^{\frac{q^n-1}{q^d-1}\frac{q^d-1}{q-1}} = (\mathrm{N}_{q^n/q^d}(\alpha))^{\frac{q^d-1}{q-1}} = \mathrm{N}_{q^d/q}(\mathrm{N}_{q^n/q^d}(\alpha))$
(v): Условието дава, че $\alpha \in \mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$, и следователно $d|n$. От Теорема 3.1.9 и формулите на Виет следва, че $\mathrm{N}_{q^d/q}(\alpha) = \alpha\alpha^2\cdots\alpha^{q^{d-1}} = (-1)^d a_d$. Тогава

$$\mathrm{N}_{q^n/q}(\alpha) = \mathrm{N}_{q^d/q}(\alpha)(\mathrm{N}_{q^d/q}(\alpha))^{q^d}\cdots(\mathrm{N}_{q^d/q}(\alpha))^{q^{n-d}} = (\mathrm{N}_{q^d/q}(\alpha))^{\frac{n}{d}} = ((-1)^d a_d)^{\frac{n}{d}},$$

тъй като $\mathrm{N}_{q^d/q}(\alpha) \in \mathbb{F}_q$ и $(\mathrm{N}_{q^d/q}(\alpha))^{q^i} = \mathrm{N}_{q^d/q}(\alpha)$.

(vi): Нека β е примитивен елемент на $\mathbb{F}_{q^n}$. Тогава $\mathrm{N}_{q^n/q^d}(\beta) = \beta^{\frac{q^n-1}{q^d-1}} = \gamma \in \mathbb{F}_{q^d}^*$ има ред q^d-1. Множеството $G = \{\alpha \in \mathbb{F}_{q^n} \mid \mathrm{N}_{q^n/q^d}(\alpha) = 1\} =< \beta^{q^d-1} >$ е мултипликативна подгрупа на $\mathbb{F}_{q^n}^*$ с индекс q^d-1. Множествата $G_b = \{\alpha \in \mathbb{F}_{q^n} \mid \mathrm{N}_{q^n/q^d}(\alpha) = b\} = \beta^k G$ за $b = \gamma^k$ са останалите q^d-1 съседни класове по H в $\mathbb{F}_{q^n}^*$. Следователно $|G_b| = |G| = \frac{q^n-1}{q^d-1}$.

□

3.3 Характери

3.3.1 Общи свойства

Дефиниция 3.3.1. *Нека G е крайна абелева група.* ***Характер*** *на G наричаме всеки хоморфизъм $\chi : G \to \mathbb{C}^*$ на G в мултипликативната група на полето на комплексните числа. Ако G е адитивна група характерът наричаме* ***адитивен****. Съответно при мултипликативна група говорим за* ***мултипликативен*** *характер.*

Дефиницията на хомоморфизъм ни дава, че за адитивен характер е в сила

$$\chi(a+b) = \chi(a)\chi(b), \qquad \chi(0) = 1, \quad \chi(-a) = \chi(a)^{-1}$$

съответно за мултипликативен характер

$$\chi(ab) = \chi(a)\chi(b), \qquad \chi(1) = 1, \quad \chi(a^{-1}) = \chi(a)^{-1}$$

за всяко $a, b \in G$. Характерът $\chi_0 : \chi_0(g) = 1$ за всяко $g \in G$ се нарича ***тривиален***.

Непосредствено следствие от дефиницията е и фактът, че образът $\chi(G)$ е подгрупа на групата $U \subset \mathbb{C}^*$ от комплексните числа с модул единица. Наистина щом G е крайна съществува n (максимален ред на елемент), такова че $g^n = 1$ (в адитивен запис $ng = 0$) за всяко $g \in G$. Следователна $(\chi(g))^n = 1$ за всяко $g \in G$. Това означава, че $\chi(G)$ е *подгрупа на групата от n-ти корени на единицата* $\mathbb{C}_n \subset U$. В частност $\chi(g)^{-1}$ съвпада с комплексно спрегнатото $\overline{\chi(g)}$. Да напомним, че

$$\mathbb{C}_n = \left\{ \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \;\middle|\; k = 0, 1, \ldots, n-1 \right\} = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\},$$

където $\xi = cos(2\pi/n) + i\sin(2\pi/n)$.

С всеки характер χ на G асоциираме друг харатер $\overline{\chi}$ наричан ***спрегнат на*** χ, който се дефинира с $\overline{\chi}(g) \stackrel{def}{=} \overline{\chi(g)}$ за всяко $g \in G$. Следователно $\overline{\chi}(g) = \chi(g^{-1})$ за мултипликативен характер и $\overline{\chi}(g) = \chi(-g)$ за адитивен характер.

Нека $\widehat{G}$ е множеството от всички характери на групата G. Дефинирайки ***произведение на характери*** чрез

$$(\chi_1 \circ \chi_2)(g) \stackrel{def}{=} \chi_1(g)\chi_2(g)$$

задаваме структура на мултипликативна абелева група на $\widehat{G}$ с единичен елемент тривиалният характер χ_0. Тя е и крайна група, тъй като G е крайна и характерите могат да приемат краен брой стойности (n-ти корени на единицата).

Твърдение 3.3.2. *Нека $G =< g >$ е циклична група от ред n, а ξ е n-ти примитивен корен на единицата в $\mathbb{C}$. Тогава $\widehat{G} = \{\phi_0, \phi_1, \ldots, \phi_{n-1}\} =< \phi_1 >$, където*

$$\phi_k(g^j) = (\xi^k)^j = \xi^{kj}, \quad k, j = 0, 1, 2, \ldots, n-1.$$

(При адитивно записана G трябва само да заменим g^j с jg.)

Доказателство. Тривиално се проверява, че така дефинирани ϕ_k са характери на G. Обратно, нека ϕ е произволен елемент на $\widehat{G}$. Тогава $\phi(g)$ трябва да бъде n-ти корен на единицата, т.е. $\phi(g) = \xi^k$, за някое естествено $k < n$. Следователно $\phi = \phi_k$. □

Теорема 3.3.3. *Нека H е подгрупа на крайната абелева група G. Всеки характер ψ на H може да се продължи до характер на G, т.е. съществува $\chi \in \widehat{G}$, такъв че $\chi(h) = \psi(h)$ за всяко $h \in H$.*

Доказателство. Нека $a \in G \setminus H$ и $H_1 =< H, a >$ е подгрупата на G породена от a и H. Всеки елемент $g \in H_1$ се представя еднозначно като $g = a^j h$, за някои $h \in H$, $0 \leq j < m$, където m е минималното естествено число с $a^m \in H$. Дефинираме ψ_1 в H_1 с $\psi_1(a^j h) = \omega^j \psi(h)$, където $\omega \in \mathbb{C}$ такова че $\omega^m = \psi(a^m)$. Функциата ψ_1 е характер на H_1 (провери!). Освен това $\psi_1(h) = \psi(h)$ за всяко $h \in H$. Ако $H_1 = G$ теоремата е доказана. Ако не, продължаваме по същия начин докато достигнем G. □

Следствие 3.3.4. *За всеки два различни елемента $g_1 \neq g_2$ на G съществува $\chi \in \widehat{G}$, такъв че $\chi(g_1) \neq \chi(g_2)$. В частност $\widehat{G}$ е нетривиална група, ако G е нетривиална.*

Доказателство. Достатъчно е да покажем, че за $h = g_1 g_2^{-1} \neq 1$ съществува характер χ, за който $\chi(h) \neq 1$. Но съгласно Твърдение 3.3.2 и Теорема 3.3.3 съществува нетривиален характер на $H =< h >$, който може да бъде продължен до характер на G. □

Лема 3.3.5. *В сила са следните равенства*

$$\sum_{g \in G} \chi(g) = \begin{cases} 0, & \chi \neq \chi_0, \\ |G|, & \chi = \chi_0 \end{cases} \tag{3.3}$$

Доказателство. Случаят $\chi = \chi_0$ е очевиден. Нека χ е нетривиален характер. Тогава съществува $h \in G$, такова че $\chi(h) \neq 1$. Тъй като hg описва G, когато g описва G, то

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(h)\chi(g) = \chi(h) \sum_{g \in G} \chi(g).$$

Следователно

$$(1 - \chi(h)) \sum_{g \in G} \chi(g) = 0,$$

откъдето следва твърдението и в случая $\chi \neq \chi_0$. □

Прилагайки горната лема за $\chi_1 \circ \overline{\chi}_2$ получаваме

Следствие 3.3.6. *Нека χ_1 и χ_2 са характери на G. Тогава*

$$\sum_{g\in G}\chi_1(g)\overline{\chi_2(g)} = \begin{cases} 0, & \chi_1 \neq \chi_2, \\ |G|, & \chi_1 = \chi_2 \end{cases} \tag{3.4}$$

Лема 3.3.7. *В сила са следните равенства*

$$\sum_{\chi\in\widehat{G}}\chi(g) = \begin{cases} 0, & g \neq 1, \\ |\widehat{G}|, & g = 1 \end{cases} \tag{3.5}$$

Доказателство. За всяко $g \in G$ дефинираме функция $\hat{g}(\chi) = \chi(g),\ \chi \in \widehat{G}$.

$$\hat{g}(\chi_1 \circ \chi_2) = (\chi_1 \circ \chi_2)(g) = \chi_1(g)\chi_2(g) = \hat{g}(\chi_1)\hat{g}(\chi_2)$$

и следователно $\hat{g}$ е характер на $\widehat{G}$. Тривиалният характер е $\hat{1}(\chi) = \chi(1) = 1,\ \chi \in \widehat{G}$. Ако $\widehat{G}$ е нетривиална, то съществува χ, така че $\chi(g) \neq 1$ за някое $g \in G$. Следователно $\hat{g}$ е нетривиален. Сега твърдението следва от Лема 3.3.5. □

Аналогично прилагайки горната лема за елемента gh^{-1} получаваме

Следствие 3.3.8. *Нека $g, h \in G$. Тогава*

$$\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi(h)} = \begin{cases} 0, & g \neq h, \\ |G|, & g = h \end{cases} \tag{3.6}$$

Горните две следствия са известни като съотношения за ортогоналност при характери)

Теорема 3.3.9. $|\widehat{G}| = |G|$

Доказателство. Използвайки Леми 3.3.5 и 3.3.7 имаме

$$|\widehat{G}| = \sum_{g\in G}\sum_{\chi\in\widehat{G}}\hat{g}(\chi) = \sum_{g\in G}\sum_{\chi\in\widehat{G}}\chi(g) = \sum_{\chi\in\widehat{G}}\sum_{g\in G}\chi(g) = |G|.$$

□

Нека H е подгрупа на G. Ако за нетривиален характер χ на G е в сила $\chi(h) = 1$ за всяко $h \in H$, то казваме, че χ ***се анулира на*** H. Множеството от всички такива характери се нарича ***анулатор на*** H ***в*** $\widehat{G}$.

Теорема 3.3.10. *Нека H е подгрупа на G. Анулаторът на H е подгрупа на $\widehat{G}$ от ред $|G|/|H|$.*

Доказателство. Нека A е анулаторът на H. От определението и свойствата на характерите веднага следва, че A е група относно въведеното произведение на характери, т.е подгрупа е на $\widehat{G}$. Нека $\chi \in A$. Тогава изображението $\varphi : G/H \to \mathbb{C}^*$ зададено с $\varphi(gH) = \chi(g)$ е характерна G/H (провери!). Обратно, ако $\psi \in \widehat{G/H}$, то ϕ зададено с $\phi(g) = \psi(gH)$ е характер на G, като $\phi(h) = \psi(H) = 1$, т.е. $phi \in A$. Следователно $|A| = |\widehat{G/H}| = |G/H|$. □

3.3.2 Характери на крайни полета

Нека $\mathbb{F}_q$ е крайно поле с $q = p^e$ елементи. В съгласие с общата терминология *адитивен характер на* $\mathbb{F}_q$ се нарича характер на адитивната група, а този на мултипликативната група $\mathbb{F}_q^*$ - съответно *мултипликативен характер*.

$\mathbb{F}_q^*$ е циклична група и съгласно Твърдение 3.3.2 групата ѝ от характери е също циклична от същия ред. По-конкретно, ако α е примитивен елемент на $\mathbb{F}_q$ и ξ е $(q-1)$-ти примитивен корен на единицата в $\mathbb{C}$, то

$$\widehat{\mathbb{F}_q^*} = \{\phi_0, \phi_1, \ldots, \phi_{q-2}\} = \{\phi^0, \phi, \ldots, \phi^{q-2}\}, \qquad \phi(\alpha) = \xi.$$

Очевидно $\overline{\phi}_k = \phi_{q-1-k}$.

Пример 3.3.11. Нека q е нечетно число. Тогава $\xi^{(q-1)/2} = -1$ и характерът $\eta = \phi^{(q-1)/2}$ е от втори ред като

$$\eta(x) = \begin{cases} 1, & x \text{ е квадрат в } \mathbb{F}_q^*, \\ -1, & \text{в противния случай.} \end{cases}$$

Характерът η се нарича ***квадратичен характер***.

Елементите на $\mathbb{F}_q$ имат (относно събирането) максимален ред p и единицата на полето е един такъв елемент с ред p. Следователно всеки адитивен характер $\chi : \mathbb{F}_q \to \mathbb{C}_p$ и е в сила

$$\chi(x) = \zeta^{h(x)}, \qquad h : \mathbb{F}_q \to \mathbb{Z}_p,$$

където ζ е p-ти примитивен корен на единицата в $\mathbb{C}$ и h е адитивен хомоморфизъм, т.е. $h(x+y) = h(x) + h(y)$. Нещо повече h е линейно изображение над $\mathbb{Z}_p$, тъй като $\chi(ax) = \chi(x)^a = \zeta^{ah(x)}$ за всяко $a \in \mathbb{Z}_p$.
Да означим с χ_1 функцията дефинирана с

$$\chi_1(x) \stackrel{def}{=} \zeta^{\mathrm{Tr}(x)},$$

където $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{Z}_p$ е функцията следа. Тъй като следата е адитивен нетривиален хомоморфизъм, то χ_1 е адитивен нетривиален характер и се нарича ***каноничен адитивен характер***.

Теорема 3.3.12. *За всяко $b \in \mathbb{F}_q$ функцията $\chi_b(x) \stackrel{def}{=} \chi_1(bx)$ е адитивен характер на $\mathbb{F}_q$ и*

$$\widehat{\mathbb{F}_q} = \{\chi_b \mid b \in \mathbb{F}_q\}.$$

Доказателство. За всяко $x, y \in \mathbb{F}_q$ имаме

$$\chi_b(x+y) = \chi_1(bx+by) = \chi_1(bx) + \chi_1(by) = \chi_b(x) + \chi_b(y).$$

Следователно $\chi_b : \mathbb{F}_q \to \mathbb{C}_p$ е адитивен характер

Обратно, нека χ е произволен характер на $\mathbb{F}_q$. Тогава $\chi(x) = \zeta^{h(x)}$, където h е линейно над $\mathbb{Z}_p$ изображение на $\mathbb{F}_q$ в $\mathbb{Z}_p$. Но съгласно Теорема 3.2.5 $h(x) = \mathrm{Tr}_{q/p}(bx)$ за подходящо $b \in \mathbb{F}_q$. Но това означава, че $\chi = \chi_b$.

До същият извод може да стигнем и като използваме, че

$$|\widehat{\mathbb{F}_q}| = |\mathbb{F}_q| = |\{\chi_b \mid b \in \mathbb{F}_q\}|.$$

□

Да отбележим, че за адитивните характери е в сила $\bar{\chi}(x) = \chi(-x)$, тъй като

$$\bar{\chi}_b(x) = \bar{\zeta}^{\mathrm{Tr}(bx)} = \zeta^{-\mathrm{Tr}(bx)} = \zeta^{\mathrm{Tr}(-bx)} = \chi_b(-x).$$

Дефиниция 3.3.13. *Нека χ е адитивен, а ψ е мултипликативен характер на $\mathbb{F}_q$. **Повдигане (продължение)** на χ и ψ до адитивен Φ, съответно мултипликативен Ψ характер на разширението $\mathbb{F}_{q^n}$ на $\mathbb{F}_q$ се наричат характерите дефинирани с*

$$\Phi(x) = \chi(\mathrm{Tr}_{q^n/q}(x)), \qquad \Psi(x) = \psi(\mathrm{N}_{q^n/q}(x)).$$

3.3.3 Суми от характери

Дефиниция 3.3.14. *Нека χ е нетривиален характер на $\mathbb{F}_q$ и $a, b \in \mathbb{F}_q$. Сума от вида*

$$K(\chi; a, b) = \sum_{x \in \mathbb{F}_q^*} \chi(ax + bx^{-1})$$

се нарича сума на Клостерман.

Сумите на Клостерман са реални числа, тъй като

$$\overline{K(\chi; a, b)} = \sum_{x \in \mathbb{F}_q^*} \bar{\chi}(ax + bx^{-1}) = \sum_{x \in \mathbb{F}_q^*} \chi(a(-x) + b(-x)^{-1}) = K(\chi; a, b).$$

Тъй като $K(\chi_c; a, b) = K(\chi_1; ca, cb)$ ще считаме, че $\chi = \chi_1$ и ще ползваме означението $K(a, b)$. Освен това с полагане $x = by$ и $x = z/a$ се вижда, че $K(a, b) = K(ab, 1) = K(1, ab)$. Затова много често за означаване на сума на Клостерман се ползва

$$K(a) = K(a, 1) = \sum_{x \in \mathbb{F}_q^*} \chi(ax + x^{-1}) = \sum_{x \in \mathbb{F}_q^*} \zeta^{\mathrm{Tr}(ax + x^{-1})}.$$

Упражнение 3.3.15. *Покажете, че ако характеристиката на полето е 2, то* $K(a,a) = K(a,1)$. *(Използвайте, че* $\mathrm{Tr}(x^2) = \mathrm{Tr}(x)$.*)*

Използвайки методи и резултати от алгебричната геометрия (връзката на сумите на Кластерман с елиптичните криви) се доказва следната теорема за полета с характеристика 2:

Теорема 3.3.16. *Множеството* $\mathcal{K}_e = \{K(a) \mid a \in \mathbb{F}_{2^e}^*\}$ *се състои от всички цели числа* $s \equiv -1 \pmod 4$ *в интервала*

$$[-2^{(e/2)+1},\ 2^{(e/2)+1}].$$

Упражнение 3.3.17. *Проверете верността на горната теорема за* $e = 1, 2, 3$, *т.е. за полета с 2, 4 и 8 елемента.*

Дефиниция 3.3.18. *Нека* χ *е адитивен, а* ψ *е мултипликативен характер на* $\mathbb{F}_q$. *Суми от вида*

$$G(\psi, \chi) = \sum_{x \in \mathbb{F}_q^*} \psi(x)\chi(x)$$

се наричат суми на Гаус.

Неравенството на триъгълника ни дава веднага, че $|G(\psi,\chi)| \leq q-1$, но можем да извлечем и по-точни оценки

Теорема 3.3.19. *Нека* ψ *е мултипликативен, а* χ *е нетривиален адитивен характер на* $\mathbb{F}_q$. *В сила е*

$$G(\psi,\chi) = \begin{cases} q-1, & \psi = \psi_0,\ \chi = \chi_0, \\ -1, & \psi = \psi_0,\ \chi \neq \chi_0, \\ 0 & \psi \neq \psi_0,\ \chi = \chi_0. \end{cases}$$

Ако $\psi \neq \psi_0,\ \chi \neq \chi_0$, *то* $|G(\psi,\chi)| = \sqrt{q}$.

Доказателство. Първият случай е очевиден, а третият е по същество Лема 3.3.5. За втория случай ползвайки отново Лема 3.3.5 имаме

$$G(\psi_0,\chi) = \sum_{x \in \mathbb{F}_q^*} \chi(x) = \sum_{x \in \mathbb{F}_q} \chi(x) - \chi(0) = -1.$$

Нека сега $\psi \neq \psi_0,\ \chi \neq \chi_0$. В такъв случай

$$\begin{aligned}
|G(\psi,\chi)|^2 &= G(\psi,\chi)\overline{G(\psi,\chi)} = \sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*}\psi(x)\chi(x)\overline{\psi(y)\chi(y)} \\
&= \sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*}\psi(xy^{-1})\chi(x-y) = \sum_{y\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\psi(z)\chi(y(z-1) \\
&= \sum_{z\in\mathbb{F}_q^*}\psi(z)\left(\sum_{y\in\mathbb{F}_q}\chi(y(z-1)) - \chi(0)\right) \\
&= \sum_{z\in\mathbb{F}_q^*}\psi(z)\left(\sum_{y\in\mathbb{F}_q}\chi(y(z-1))\right) - \sum_{z\in\mathbb{F}_q^*}\psi(z)
\end{aligned}$$

Използвайки Лема 3.3.5 заключаваме, че $|G(\psi,\chi)|^2 = 0-0 = 0$ при $z \neq 1$ и $|G(\psi,\chi)|^2 = \psi(1)q - 0 = q$ при $z = 1$. □

Гаусовите суми притежават следните свойства

Теорема 3.3.20. *Функцията норма притежава следните свойства:*

(i) $G(\psi,\chi_{ab}) = \overline{\psi(a)}G(\psi,\chi_b)$ *за всеки* $a \in \mathbb{F}_q^*, b \in \mathbb{F}_q$;

(ii) $G(\psi,\bar{\chi}) = \psi(-1)G(\psi,\chi)$;

(iii) $G(\overline{\psi},\chi) = \psi(-1)\overline{G(\psi,\chi)}$;

(iv) $G(\psi,\chi)G(\overline{\psi},\chi) = \psi(-1)q$ *за всяко* $\psi \neq \psi_0,\ \chi \neq \chi_0$;

(v) $G(\psi^p,\chi_b) = G(\psi,\chi_{\sigma(b)})$, *където* $p = char(\mathbb{F}_q)$, *а* $\sigma(b) = b^p$.

Доказателство. **(i):**

$$\begin{aligned}
G(\psi,\chi_{ab}) &= \sum_{x\in\mathbb{F}_q^*}\psi(x)\chi_b(ax) = \sum_{y\in\mathbb{F}_q^*}\psi(a^{-1}y)\chi_b(y) = \psi(a^{-1})\sum_{y\in\mathbb{F}_q^*}\psi(y)\chi_b(y) \\
&= \overline{\psi(a)}G(\psi,\chi_b)
\end{aligned}$$

(ii): $\chi = \chi_b$ за подходящо b и следователно $\bar{\chi}(x) = \chi_b(-x) = \chi_{-b}(x)$. Тогава от (i) получаваме:

$$G(\psi,\bar{\chi}) = G(\psi,\chi_{-b}) = \overline{\psi(-1)}G(\psi,\chi_b) = \psi(-1)G(\psi,\chi)$$

(iii): От (ii) следва

$$G((\bar{\psi},\chi) = \overline{\psi}(-1)G(\bar{\psi},\bar{\chi}) = \psi(-1)\overline{G(\psi,\chi)}$$

(iv):

$$G(\psi,\chi)G(\overline{\psi},\chi) = G(\psi,\chi)\psi(-1)\overline{G(\psi,\chi)} = \psi(-1)|G(\psi,\chi)|^2 = \psi(-1)\,q.$$

(v): Ползвайки свойствата на Tr получаваме

$$\chi_b(x) = \chi_1(bx) = \chi_1(b^p x^p) = \chi_{\sigma(b)}(x^p),$$

и следователно

$$G(\psi^p,\chi_b) = \sum_{x\in\mathbb{F}_q^*} \psi^p(x)\chi_b(x) = \sum_{x\in\mathbb{F}_q^*} \psi(x^p)\chi_{\sigma(b)}(x^p) = \sum_{y\in\mathbb{F}_q^*} \psi(y)\chi_{\sigma(b)}(y) = G(\psi,\chi_{\sigma(b)})$$

тъй като $y = x^p$ описва $\mathbb{F}_q$, когато x описва $\mathbb{F}_q$. □

Теорема 3.3.21 (Davenport-Hasse)**.** *Нека ψ е мултипликативен, а χ е адитивен характер на $\mathbb{F}_q$ не едновременно тривиални. Ако Φ и Ψ са повдиганията им до характери на $\mathbb{F}_{q^n}$, то*

$$G(\Psi,\Phi) = (-1)^{n-1}G(\psi,\chi)^n$$

Теорема 3.3.22. *Нека $q = p^e$, където p е нечетно просто число. Ако η е квадратичният, а χ_1 е каноничният адитивен характер на $\mathbb{F}_q$, то*

$$G(\eta,\chi_1) = \begin{cases} (-1)^{e-1}\sqrt{q}, & p \equiv 1 \pmod 4, \\ (-1)^{e-1}i^e\sqrt{q}, & p \equiv 3 \pmod 4. \end{cases}$$

Упражнение 3.3.23. *Пресметнете $G(\eta,\chi_1)$ за полета с 3 и 9 елемента.*

Сумите на Гаус служат и за представяна на мултипликативните характери и обратно. В сила са следните формули

Твърдение 3.3.24. *Ако ψ и χ означават съответно мултипликативен и адитивен характер на $\mathbb{F}_q$, то*

$$(a):\ \psi(x) = \frac{1}{q}\sum_{\chi\in\widehat{\mathbb{F}}_q} G(\psi,\bar{\chi})\chi(x), \qquad (b):\ \chi(x) = \frac{1}{q-1}\sum_{\psi\in\widehat{\mathbb{F}}_q^*} G(\bar{\psi},\chi)\psi(x)$$

Доказателство. Използвайки съотношението за ортогоналност получаваме

$$\begin{aligned}\psi(x) &= \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\left(\psi(y)\sum_{b\in\mathbb{F}_q}\chi_b(x)\overline{\chi}_b(y)\right) = \frac{1}{q}\sum_{b\in\mathbb{F}_q}\chi_b(x)\sum_{y\in\mathbb{F}_q^*}\psi(y)\bar{\chi}_b(y)\\ &= \frac{1}{q}\sum_{b\in\mathbb{F}_q}\chi_b(x)G(\psi,\bar{\chi}_b)\end{aligned}$$

Аналогично

$$\begin{aligned}\chi(x) &= \frac{1}{q-1}\sum_{y\in\mathbb{F}_q^*}\left(\chi(y)\sum_{\psi\in\widehat{\mathbb{F}}_q}\psi(x)\overline{\psi}(y)\right) = \frac{1}{q-1}\sum_{\psi\in\widehat{\mathbb{F}}_q}\psi(x)\sum_{y\in\mathbb{F}_q^*}\bar{\psi}(y)\chi(y)\\ &= \frac{1}{q-1}\sum_{\psi\in\widehat{\mathbb{F}}_q}\psi(x)G(\bar{\psi},\chi)\end{aligned}$$

□

Горните равенства са известни като аналог на преобразуването на Фурие за характери на крайни полета.

Дефиниция 3.3.25. *Нека χ е нетривиален адитивен характер на $\mathbb{F}_q$ и $f(x)\in\mathbb{F}_q[x]$ е полином от ненулева степен. Суми от вида*

$$\sum_{x\in\mathbb{F}_q}\chi(f(x))$$

се наричат суми на Вейл (Weil).

Теорема 3.3.26. *Нека $p = char\mathbb{F}_q$ и $A(x) = c + L(x) = c + c_0x + c_1x^p + \cdots + c_kx^{p^k}$. Тогава за произволен нетривиален адитивен характер χ_b, $b\in\mathbb{F}_q^*$, на $\mathbb{F}_q$ е изпълнено*

$$\sum_{x\in\mathbb{F}_q}\chi_b(A(x)) = \begin{cases}\chi_b(a)q, & B = bc_k + b^pc_{k-1}^p + \cdots + (bc_0)^{p^k} = 0,\\ 0, & \textit{в останалите случаи.}\end{cases}$$

Доказателство.

$$\sum_{x\in\mathbb{F}_q}\chi_b(c+L(x)) = \sum_{x\in\mathbb{F}_q}\chi_b(c)\chi_b(L(x)) = \chi_b(c)\sum_{x\in\mathbb{F}_q}\chi_1(bL(x))$$

Но

$$\begin{aligned}\chi_1(bL(x)) &= \chi_1(bc_0x + bc_1x^p + \cdots + bc_kx^{p^k})\\ &= \chi_1\left((bc_0)^{p^k}x^{p^k} + (bc_1)^{p^{k-1}}x^{p^k} + \cdots + bc_kx^{p^k}\right) = \chi_1(Bx^{p^k})\end{aligned}$$

Следователно

$$\begin{aligned}\sum_{x\in\mathbb{F}_q}\chi_b(c+L(x)) &= \chi_b(c)\sum_{x\in\mathbb{F}_q}\chi_1(Bx^{p^k})) = \chi_b(c)\sum_{x\in\mathbb{F}_q}\chi_B(x^{p^k})) = \chi_b(c)\sum_{y\in\mathbb{F}_q}\chi_B(y))\\ &= \begin{cases}\chi_b(a)q, & B = 0,\\ 0, & B\neq 0,\end{cases}\end{aligned}$$

тъй като $y = x^{p^k}$ описва $\mathbb{F}_q$, когато x пробягва $\mathbb{F}_q$. □

Прилагайки горната теорема за $p = 2$ и $k = 1$ получаваме

Следствие 3.3.27. *Нека* $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x],\ b \in \mathbb{F}_q^*, \quad q = 2^e$. *Тогава*

$$\sum_{x\in\mathbb{F}_q} \chi_b(f(x)) = \begin{cases} \chi_b(a_0)q, & a_2 = ba_1^2 \\ 0, & \text{в останалите случаи.} \end{cases}$$

Теорема 3.3.28. *Нека* n *е естествено число,* χ *е адитивен характер на* $\mathbb{F}_q$, *а* λ *е мултипликативен характер с ред* $d = (n, q-1)$. *Тогава за* $a, b \in \mathbb{F}_q,\ a \neq 0$

$$\sum_{x\in\mathbb{F}_q} \chi(ax^n + b) = \chi(b) \sum_{j=1}^{d-1} \bar{\lambda}^j(a) G(\lambda^j, \chi).$$

3.4 Уравнения над крайни полета

Друго често използвано следствие от теореми 3.2.7 и 3.2.8 е следната

Теорема 3.4.1. *Полиномът* $f(x) = ax^2 + bx + c \in \mathbb{F}_{2^n}[x]$ *има корен в* $\mathbb{F}_{2^n}$ *тогава и само тогава, когато*

$$\mathrm{Tr}_{2^n/2}(\frac{ac}{b^2}) = 0.$$

Доказателство. Полагайки $x = \dfrac{b}{a}y$ получаваме $\dfrac{b^2}{a}y^2 + \dfrac{b^2}{a}y + c = 0$. След умножение с $\dfrac{a}{b^2}$ получаваме уравнението $y^2 + y + \dfrac{ac}{b^2} = 0$, което има корен в $\mathbb{F}_{2^n}$ тогава и само тогава, когато $\mathrm{Tr}_{2^n/2}(\dfrac{ac}{b^2}) = 0$. □

Като илюстрация за приложенията на предната теорема ще докажем следното твърдение.

Теорема 3.4.2. *Нека* α *е примитивен елемент на* $\mathbb{F}_{2^n}$, *а* $\beta \in \mathbb{F}_{2^{2n}}$ *е елемент от ред* $2^n + 1$. *Тогава*

$$\begin{aligned} \{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(x^{-1}) = 0\} &= \{x = \alpha^i + \alpha^{-i} \mid i = 0, 1, \ldots, 2^{n-1} - 1\}, \\ \{x \in \mathbb{F}_{2^n}^* \mid \mathrm{Tr}(x^{-1}) = 1\} &= \{x = \beta^i + \beta^{-i} \mid i = 1, 2, \ldots, 2^{n-1}\}. \end{aligned}$$

Доказателство. За $x = 0$ твърдението е вярно: $0 = \alpha^0 + \alpha^{-0}$. Считаме, че $x \in \mathbb{F}_{2^n}^*$ и разглеждаме уравнението

$$z^2 + xz + 1 = 0. \tag{3.7}$$

Съгласно Теорема 3.4.1 то има решение в $\mathbb{F}_{2^n}$ тогава и само тогава, когато $\mathrm{Tr}(x^{-2}) = 0$, т.е. когато $\mathrm{Tr}(x^{-1}) = \mathrm{Tr}(x^{-2}) = 0$.

(1): Нека $\mathrm{Tr}(x^{-1}) = \mathrm{Tr}(x^{-2}) = 0$. Уравнението (3.7) има два корена z_1, z_2 в $\mathbb{F}_{2^n}$. От формулите на Виет следва, че $z_2 = z_1^{-1}$ и $x = z_1 + z_1^{-1} = \alpha^i + \alpha^{-i}$ за някое $1 \leq i \leq 2^n - 2$. Но тъй като за i и $2^n - 1 - i$ се получават еднакви стойности за $\alpha^i + \alpha^{-i}$ можем да считаме, че $1 \leq i \leq 2^{n-1} - 1$. Обратно, ако $x = \alpha^i + \alpha^{-i}$, то α^i и α^{-i} са корени на (3.7) и следователно $\mathrm{Tr}(x^{-1}) = \mathrm{Tr}(x^{-2}) = 0$.

(2): Нека $\mathrm{Tr}(x^{-1}) = \mathrm{Tr}(x^{-2}) = 1$. Уравнението (3.7) няма решение в $\mathbb{F}_{2^n}$, но има два корена z_1, z_2 в квадратичното разширение $\mathbb{F}_{2^{2n}}$ и те трябва да са спрегнати: $z_2 = z_1^{2^{2^n}}$ (полиномът е неразложим над $\mathbb{F}_{2^n}$). Тогава от формулите на Виет получаваме

$$x = z_1 + z_1^{-1}, \quad z_1^{2^n+1} = 1.$$

Следователно редът на z_1 е $2^n + 1$ трябва да съществува $j \in \{1, 2, \ldots, 2^{n-1}\}$, такова че $z_1 = \beta^j$. Обратно, нека $x = \beta^i + \beta^{-i}$. Тогава β^i, $\beta^{-i} \notin \mathbb{F}_{2^n}$ са корени на (3.7) и следователно $\mathrm{Tr}(x^{-1}) = \mathrm{Tr}(x^{-2}) = 1$. □

Теорема 3.4.3. *Нека $b \in \mathbb{F}_{q^n}^*$, t е естествено число и $D = (q^n - 1, t)$. Уравнението*

$$x^t = b$$

има и то D решения в $\mathbb{F}_{q^n}$ тогава и само тогава, когато $b^{\frac{q^n-1}{D}} = 1$.

Доказателство. Нека g е примитивен елемент на $\mathbb{F}_{q^n}$ и $b = g^r$. Уравнението има решение тогава и само тогава, когато съществува естествено число y, такова че

$$yt \equiv r \pmod{q^n - 1}.$$

Но това сравнение има и то точно D решения тогава и само тогава, когато D дели r. Последното е еквивалентно с $b^{\frac{q^n-1}{D}} = g^{r\frac{q^n-1}{D}} = 1$. □

Като приложение на горната теорема ще докажем следното твърдение.

Теорема 3.4.4. *Нека $a \in \mathbb{F}_{q^n}^*$, k е естествено число и $d = (n, k)$. За уравнението*

$$a^{q^k} x^{q^{2k}} + ax = 0 \tag{3.8}$$

е в сила:

(i) *Ако n/d е нечетно, то (3.8)*

- *има q^d решения в $\mathbb{F}_{q^n}$, ако q е четно*
- *има единствено решение $x = 0$, ако q е нечетно;*

(ii) *Ако n/d е четно, то (3.8)*

- *има q^{2d} решения, когато* $a^{\frac{q^n-1}{q^d+1}} = \begin{cases} (-1)^{\frac{n}{2d}}, & q \text{ нечетно}, \\ 1, & q \text{ четно}, \end{cases}$
- *има единствено решение $x = 0$ в останалите случаи.*

Доказателство. Съвкупността от решения на (3.8) се състои от тривиалното решение $x = 0$ и решенията на уравнението $x^{q^{2k}} = -a^{1-q^k}$ (при q четно знакът минус липсва). За последното прилагаме Теорема 3.4.3 полагайки $t = q^{2k} - 1$ и $b = -a^{1-q^k}$. Нека $n_1 = n/d$ и $k_1 = k/d$. Ясно, че $(n_1, k_1) = 1$. Най-големият общ делител $D = (q^{2k} - 1,\, q^n - 1) = q^{(2k,n)} - 1$. Но

$$(2k, n) = d(2k_1, n_1) = \begin{cases} d, & n_1 \text{ нечетно} \\ 2d, & n_1 \text{ четно} \end{cases}.$$

Следователно

$$D = \begin{cases} q^d - 1, & n/d \text{ нечетно} \\ q^{2d} - 1, & n/d \text{ четно} \end{cases}$$

Съответно $b^{\frac{q^n-1}{D}} = (-1)^{\frac{q^n-1}{D}} a^{-\frac{(q^k-1)(q^n-1)}{D}}$. Да отбележим, че при q четно, т.е. характеристика 2 на полето, (-1) няма значение.

(i) Нека $\dfrac{n}{d}$ е нечетно. Тогава $b^{\frac{q^n-1}{D}} = (-1)^{\frac{q^n-1}{q^d-1}} a^{-\frac{(q^k-1)(q^n-1)}{q^d-1}} = (-1)^{\frac{q^n-1}{q^d-1}}$, тъй като $q^d - 1$ дели $q^k - 1$. Но

$$\frac{q^n - 1}{q^d - 1} = \underbrace{1 + q^d + \cdots + q^{d(\frac{n}{d}-1)}}_{n/d \text{ събираеми}},$$

което е нечетно число. Следователно съгласно Теорема 3.4.3 уравнението няма ненулево решение за q нечетно и точно $D = q^d - 1$ ненулеви решения при q четно, откъдето получаваме твърдението на теоремата.

(ii) Нека $\dfrac{n}{d}$ е четно. Тогава $D = q^{2d} - 1$ и $k_1 = k/d$ е нечетно число.

$$\frac{q^n - 1}{q^{2d} - 1} = \underbrace{1 + q^{2d} + \cdots + q^{2d(\frac{n}{2d}-1)}}_{n/2d \text{ събираеми}} \equiv \frac{n}{2d} \pmod 2 \quad \text{за } q \text{ нечетно}.$$

Следователно $b^{\frac{q^n-1}{D}} = (-1)^{\frac{n}{2d}} a^{-\frac{(q^k-1)(q^n-1)}{(q^d-1)(q^d+1)}} = (-1)^{\frac{n}{2d}} a^{A\frac{(q^n-1)}{(q^d+1)}}$, където

$$A = \frac{1 - q^k}{q^d - 1} = -(1+q^d+\cdots+q^{d(\frac{k}{d}-1)}) \equiv -(1-1+1-\cdots+1) \equiv -1 \pmod{q^d+1}$$

тъй като k_1 е нечетно число. Но тогава

$$b^{\frac{q^n-1}{D}} = \left[(-1)^{\frac{n}{2d}} a^{\frac{(q^n-1)}{(q^d+1)}}\right]^{-1}.$$

Следователно $b^{\frac{q^n-1}{D}} = 1$ тогава и само тогава, когато $(-1)^{\frac{n}{2d}} a^{\frac{(q^n-1)}{(q^d+1)}} = 1$. Сега Теорема 3.4.3 дава исканото твърдение.

Да отбележи, че за да има (3.8) нетривиално решение трябва $a = g^{s(q^d+1)}$ за някое s, където g е примитивен елемент на $\mathbb{F}_{q^n}$.

□

Забележка. Полиномът $a^{q^k} x^{q^{2k}} + ax$ е линеаризиран полином и като такъв се явява пермутационен полином в $\mathbb{F}_{q^n}$ тогава и само тогава, когато нулата е единственият му корен в $\mathbb{F}_{q^n}$. Доказаната теорема показва, че този полином е пермутационен при характеристика 2 на полето, точно когато n/d четно и $a^{\frac{q^n-1}{q^d+1}} \neq 1$. При нечетна характеристика условието е n/d да е нечетно или ако е четно, то $a^{\frac{q^n-1}{q^d+1}} \neq (-1)^{n/2d}$.

Ще има продължение!