Дзета-функция Артина

Пусть F — поле.

Определим

$$F^n = \mathbb{A}^n(F) = \{(a_1, \ldots, a_n) : a_i \in F\}$$

(афинное пространство).

В $\mathbb{A}^{n+1}(F)$ вводится отношение эквивалентности

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \quad \Longleftrightarrow \quad \exists\, \gamma \in F :\ a_i = \gamma b_i,\ i = 0, \ldots, n.$$

Определим

$$\mathbb{P}^n(F) = \big(\mathbb{A}^{n+1}(F) \setminus \{0\}\big)/\sim = \{[a_0 : \ldots : a_n]\}.$$

Если $F = \mathbb{F}_q$, то

$$|\mathbb{A}^n(\mathbb{F}_q)| = q^n.$$

Можно построить отображение

$$\varphi = \varphi_0 :\ \mathbb{P}^n(F) \longrightarrow \mathbb{A}^n(F), \qquad [x_0 : \ldots : x_n] \longmapsto \left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right),$$

при условии $x_0 \neq 0$.

Лемма. Пусть

$$H_0 = \big\{[x_0 : \ldots : x_n] \in \mathbb{P}^n(F) : x_0 \neq 0\big\}.$$

Тогда ограничение

$$\varphi_0 : H_0 \longrightarrow \mathbb{A}^n(F)$$

является биекцией.

▷ Если $[x_0 : \ldots : x_n] \in H_0$, то

$$[x_0 : \ldots : x_n] = \left[1 : \frac{x_1}{x_0} : \ldots : \frac{x_n}{x_0}\right].$$

Пусть $\varphi_0([x]) = \varphi_0([y])$. Тогда

$$\frac{x_i}{x_0} = \frac{y_i}{y_0} \quad \Longrightarrow \quad x_i y_0 = y_i x_0$$

для всех i, т.е. $x_i = \gamma y_i$ при $\gamma = x_0^{-1} y_0$. Следовательно, $[x] = [y]$. Обратное отображение есть

$$(x_1, \ldots, x_n) \longmapsto [1 : x_1 : \ldots : x_n].$$

■

Таким образом, $H_0 \simeq \mathbb{A}^n(F)$.

Имеем разложение

$$\mathbb{P}^n(F) = \mathbb{A}^n(F) \ \cup \ \mathbb{P}^{n-1}(F).$$

Лемма.

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

▷ Индукция по n, используя разложение $\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$ и то, что $|\mathbb{A}^n(\mathbb{F}_q)| = q^n$. ■

Примеры.

1) $\mathbb{P}^0$ — одна точка.

2) $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$, где ∞ — бесконечно удалённая точка (проективная прямая).

Определение. Многочлен

$$f \in F[x_1, \ldots, x_n]$$

называется *однородным* степени d, если

$$f = \sum a_I x_0^{i_0} \cdots x_n^{i_n}, \qquad i_0 + \cdots + i_n = d.$$

Определение.

$$f \in F[x_1, \ldots, x_n], deg f = d,$$

если возьмем

$$\overline{f} = y_0^d f(\frac{y_1}{y_0}, \ldots, \frac{y_n}{y_n}), \in F[y_1, \ldots, y_n] -$$

соответствующий однородный многочлен. Пример.

$$x_1^2 + x_2^2 - 1$$

не является однородным многочленом, а

$$y_1^2 + y_2^2 - y_3^2$$

— однородный.

Далее $F = \mathbb{F}_q$.

$$E \setminus F - \text{расширение;}$$

$H_f(E) = \{a \in \mathbb{A}^n(E) : f(a) = 0\}-$гиперповерхность над конечным полем.

$$\overline{H}_{\overline{f}(E)} = \{a \in \mathbb{P}^n(E) : \overline{f}(a) = 0\}$$
$$|H_f| \leq |\overline{H}_{\overline{f}}|$$

Пример.

$$f(x_1, x_2) = x_1^2 + x_2^2 - 1 \in \mathbb{F}_p[x_1, x_2].$$

$$|H_f(\mathbb{F}_p)| = \begin{cases} p-1 & \text{, если } p \equiv 1 \pmod 4, \\ p+1 & \text{, если } p \equiv 3 \pmod 4. \end{cases}$$

Проективное множество:

$$H_f(\mathbb{F}_p) = \{[y_0 : y_1 : y_2] \in \mathbb{P}^2(\mathbb{F}_p) : y_1^2 + y_2^2 = y_0^2\}.$$

Если $y_0 = 0$, то

$$[0 : y_1 : y_2] \Rightarrow y_1^2 + y_2^2 = 0 \Leftrightarrow (\frac{y_1}{y_0}) = -1$$

$$p \equiv 1 \pmod 4 \Rightarrow (\frac{-1}{p}) = -1, a^2 = -1$$

$$[0 : 1 : a], [0 : 1; -a] \in \overline{H}_{\overline{f}}$$

$|\overline{H}_{\overline{f}}| = p+1, p \equiv 1 \pmod 4$, иначе$p \equiv 3 \pmod 4-$нет решений$[0 : y_1 : y_2]$

$$\text{Тогда } |\overline{H}_{\overline{f}}| = p + 1$$

Далее рассматривается общий случай.

Пусть f — однородный многочлен степени n над $\mathbb{F}_p$. Тогда проективная кривая $\overline{H}_f$ над $\overline{\mathbb{F}}_p$ имеет число $\mathbb{F}_p$-точек, удовлетворяющее оценке

$$\left||\overline{H}_f(\mathbb{F}_p)| - (p+1)\right| \leq (n-1)(n-2)\sqrt{p}.$$

Теорема (на следующей странице). Пусть $F = \mathbb{F}_q$, $r|q-1$, тогда

$$|\overline{H}_{\overline{f}}| = q^{n-1} + \cdots + 1 + R, \qquad |R| = \frac{1}{q} G(\chi_0) * \cdots * G(\chi_n),$$

$\chi_i -$ характер порядка r : $\chi_i^r = \epsilon -$ главный характер

$|R| = Cq^{\frac{n}{2}-1}$для некоторой константы C

Пусть далее

$$f(y_0, \ldots, y_n) \in \mathbb{F}_q[y_0, \ldots, y_n].$$

Для расширения $\mathbb{F}_{q^m}/\mathbb{F}_q$ обозначим

$$N_m = |\overline{H}_f(\mathbb{F}_{q^m})| = N_m(f).$$

Определение (дзета-функция Артина).
Для $f = 0$ задаётся

$$Z_f(u) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} u^m\right), \qquad u \in \mathbb{C}.$$

Лемма. Функция $Z_f(u)$ определена при $|u| < q^{-n}$.

▷ $|N_m| \leq |\mathbb{P}^n(\mathbb{F}_q^m)| \leq (n+1)q^{mn}$, то тогда ряд $Z_f(u)$ сходится. ■

Почему называется дзета-функцией:
рассмотрим дзето-функцию Римана

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}.$$

Далее рассматриваются многочлены над $\mathbb{F}_q[x]$.

Дзета-функция Артина определяется

$$\zeta_{\mathbb{F}_q[x]}(s) = \prod_f \left(1 - (N_f)^{-s}\right)^{-1},$$

где f - неприводимый многочлен. Рассмотрим $H_f(\overline{\mathbb{F}}_{q^d})$, $\alpha = (a_1, \ldots, a_n) \in \mathbb{F}_q$,

$a_i \in \mathbb{F}_{q^d}, \quad \alpha^q = (a_1^q, \ldots, a_n^q)$
$f(\alpha^q) = f(\alpha)^q = 0$

Определение.

$$\text{Множество} \quad P = \{\alpha_1, \alpha^q, \ldots, \alpha^{q^{d-1}}\} -$$

называется циклом, $\deg \mathrm{P} = \mathrm{d}$ называется степенью цикла $(\alpha_1, \alpha^q, \ldots, \alpha^{q^{d-1}}, \alpha^{q^d}, \alpha^{q^d} = \alpha)$

Лемма. Если обозначить через $n_d = |\{P - \text{циклов} : degP = d\}|$, то

$$N_m = \sum_{d|m} d\, n_d.$$

▷ $H_f(\mathbb{F}_{q^m}) = \bigcup P, \alpha \in \mathbb{F}_{q^d}$. $\mathbb{F}_{q^d}$ подполе $\mathbb{F}_{q^m} \Leftrightarrow d|m$.
$H_f(\mathbb{F}_{q^m}) = \bigcup_{d|m} P, \quad P_1 \bigcap P_2 \neq \emptyset \quad P_1 \neq P_2 . \alpha \in P_1 \bigcap P_2 \Leftrightarrow$
$\alpha^{q^{d_1}-1} = 1, \quad \alpha^{q^{d_2}-1} = 1 \Rightarrow d_1 = d_2 \Rightarrow p_1 = p_2 \quad \perp$ ■

Теорема.

$$Z_p(q^{-s}) = \prod_P (1 - q^{-s \deg P})^{-1}.$$

Теорема.

$$Z_f(u) \in \mathbb{C}(u), \qquad Z_f(u) = \frac{P(u)}{Q(u)}.$$

Теорема.

$$Z_f(u) - \text{рац} \Leftrightarrow N_m = \sum_j p_j^m - \sum_i d_i^m.$$