Глава 17

ζ-функция на Hasse-Weil.

Преди да разгледаме ζ-функцията на Hasse-Weil трябва да въведем някои числови инварианти на крива, определена над крайно поле.

Лема 17.1. *Ако F е функционално поле на една променлива с крайно поле от константи $\mathbb{F}_q$, то за всяко естествено число n съществуват краен брой $A_n(F) \in \mathbb{N}$ ефективни дивизори на F от степен n.*

Доказателство: Нека $D = \sum\limits_{v\mathcal{P}(F)} n_v v$, $n_v \geq 0$ е ефективен дивизор от степен $\deg(D) = \sum\limits_{v\in\mathcal{P}(F)} n_v \deg(v) = n$. Коефициентите $n_v \geq 0$ са неотрицателни, а степените $\deg(v) \geq 1$ са естествени, така че за всички $v \in \mathcal{P}(F)$ с $n_v \neq 0$ имаме $n_v \leq n$ и $\deg(v) \leq n$. Достатъчно е да докажем, че за всяко естествено число d съществуват краен брой $B_d(F)$ класове дискретни нормирания $v \in \mathcal{P}(F)$ от степен d. Еквивалентно, за $\forall d \in \mathbb{N}$ съществуват краен брой $B_d(F)$ $\mathbb{F}_q$-затворени точки на X от степен d. Всички $\mathbb{F}_q$-затворени точки от степен d са $\mathbb{F}_{q^d}$-рационални, така че е достатъчно да установим крайността на броя на $\mathbb{F}_{q^d}$-рационалните точки на X за да докажем лемата. Ако пълната гладка крива X с функционално поле $\mathbb{F}_q(X) = F$ над $\mathbb{F}_q$ се влага в проективното пространство $\mathbb{P}^m(\overline{\mathbb{F}_q})$, то $\mathbb{F}_{q^d}$-рационалните точки $X(\mathbb{F}_{q^d}) \subseteq \mathbb{P}^m(\mathbb{F}_{q^d})$ на X се съдържат в $\mathbb{F}_{q^d}$-рационалните точки на $\mathbb{P}^m(\overline{\mathbb{F}_q})$, чийто брой е

$$|\mathbb{P}^m(\mathbb{F}_{q^d})| = \frac{|(\mathbb{F}_{q^d})^{m+1} \setminus \{(0,\dots,0)\}|}{|\mathbb{F}^*_{q^d}|} = \frac{q^{d(m+1)}-1}{q^d-1} < \infty,$$

Q.E.D.

Да означим с $N(F)$ броят на $\mathbb{F}_q$-рационалните точки на функционалното поле на една променлива F над $\mathbb{F}_q$. Ясно е, че $N(F) = B_1(F)$ съвпада с броя на рационалните класове дискретни нормирания, т.е. с броя на класовете дискретни нормирания от степен 1. За всяко естествено n разглеждаме функционалното поле на една променлива $F_n = F * \mathbb{F}_{q^n}$ над $\mathbb{F}_{q^n}$ и означаваме с $N_n(F) = N(F_n)$ броя на $\mathbb{F}_{q^n}$-рационалните точки на X.

Определение 17.2. *Ако $N_n(F)$ е броят на $\mathbb{F}_{q^n}$-рационалните точки на гладка проективна крива X с функционално поле $\mathbb{F}_q(X) = F$ над $\mathbb{F}_q$, то формалният степенен ред*

$$\zeta(F,t) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n(F)}{n} t^n\right)$$

на t се нарича ζ-функция на Hasse-Weil на F.

Пример 17.3. *Функционалното поле $\mathbb{F}_q(\mathbb{P}^1)$ на проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ има ζ-функцця на Hasse-Weil*

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

Доказателство: За всяко естествено число n проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ има

$$N_n(\mathbb{F}_q(\mathbb{P}^1) = |\mathbb{P}^1(\mathbb{F}_{q^n})| = \frac{|(\mathbb{F}_{q^n})^2 \setminus \{(0,0)\}|}{|\mathbb{F}_{q^n}^*|} = \frac{q^{2n}-1}{q^n-1} = q^n + 1$$

$\mathbb{F}_{q^n}$-рационални точки. По определение,

$$\zeta(\mathbb{F}_q(\mathbb{P}^1), t) = \exp\left(\sum_{n=1}^{\infty} \frac{(q^n+1)}{n} t^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{(qt)^n}{n}\right) \exp\left(\sum_{n=1}^{\infty} \frac{t^n}{n}\right).$$

Използваме развитието в Тейлъров ред

$$-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$$

около $x = 0$, вземайки предвид, че производните

$$(-\log(1-x))^{(n)} = (n-1)!(1-x)^{-n} \quad \text{за} \quad \forall n \in \mathbb{N}.$$

Оттук

$$\frac{1}{1-x} = e^{-\log(1-x)} = \exp\left(\sum_{n=1}^{\infty} \frac{x^n}{n}\right)$$

и

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

Q.E.D.

Лема 17.4. *За произволно функционално поле на една променлива F с поле от константи $\mathbb{F}_q$ е в сила*

$$\zeta(F, t) = \prod_{v \in \mathcal{P}(F)} \frac{1}{1 - t^{\deg(v)}},$$

където произведението е по класовете дискретни нормирания $v \in \mathcal{P}(F)$ на F.

Доказателство: Ако $B_d(F)$ е броят на класовете дискретни нормирания $v \in \mathcal{P}(F)$ от степен $\deg(v) = d$, то

$$\prod_{v \in \mathcal{P}(F)} \frac{1}{1 - t^{\deg(v)}} = \prod_{d=1}^{\infty} \frac{1}{(1-t^d)^{B_d(F)}}.$$

Оттук,

$$\log\left(\prod_{v \in \mathcal{P}(F)} \frac{1}{1 - t^{\deg(v)}}\right) = \sum_{d=1}^{\infty} B_d(F) \log\left(\frac{1}{1-t^d}\right) = \sum_{d=1}^{\infty} \sum_{n=1}^{\infty} B_d(F) \frac{t^{dn}}{n}.$$

Чрез полагането $m = dn$ и размяна на реда на сумиране получаваме

$$\log\left(\prod_{v \in \mathcal{P}(F)} \frac{1}{1 - t^{\deg(v)}}\right) = \sum_{m=1}^{\infty} \left(\sum_{d/m} dB_d(F)\right) \frac{t^m}{m}.$$

Остава да забележим, че

$$\sum_{d/m} dB_d(F) = N_m(F),$$

защото точка $P \in X$ е $\mathbb{F}_{q^m}$-рационална тогава и само тогава, когато принадлежи на $\mathbb{F}_q$-затворена точка от степен d, деляща m и $B_d(F)$ е броят на $\mathbb{F}_q$-затворените точки от степен d, Q.E.D.

ЛЕМА 17.5. *За произволно функционално поле на една променлива F с поле от константи $\mathbb{F}_q$ е в сила*

$$\zeta(F,t) = \sum_{n=0}^{\infty} A_n(F) t^n,$$

където $A_n(F)$ е броят на ефективните дивизори на F от степен n.

Доказателство: Съгласно Лема 17.4, достатъчно е да проверим, че

$$\prod_{v \in \mathcal{P}(F)} \frac{1}{1 - t^{\deg(v)}} = \sum_{n=0}^{\infty} A_n(F) t^n.$$

Представяме множителите на лявата страна като суми на безкрайни геометрични прогресии

$$\frac{1}{1 - t^{\deg(v)}} = \sum_{m=0}^{\infty} t^{m \deg(v)}$$

и получаваме

$$\prod_{v \in \mathcal{P}(F)} \frac{1}{1 - t^{\deg(v)}} = \prod_{v \in \mathcal{P}(F)} \left(\sum_{m=0}^{\infty} t^{m \deg(v)} \right). \tag{17.1}$$

За всяко неотрицателно цяло число n, събираемото t^n на формалния степенен ред (17.1) се получава от класовете дискретни нормирания $v \in \mathcal{P}(F)$ и неотрицателните цели m_v, за които $\sum\limits_{v \in \mathcal{P}(F)} m_v \deg(v) = n$. Оттук, коефициентът на t^n в (17.1) е равен на броя $A_n(F)$ на ефективните дивизори $D = \sum\limits_{V \in \mathcal{P}(F)} m_v v$ от степен $\deg(D) = \sum\limits_{v \in \mathcal{P}(F)} m_v \deg(v) = n$ и

$$\prod_{v \in \mathcal{P}(F)} \frac{1}{1 - t^{\deg(v)}} = \sum_{n=0}^{\infty} A_n(F) t^n,$$

Q.E.D.

ЛЕМА 17.6. *Нека F е функционално поле на една променлива с поле от константи $\mathbb{F}_q$, $\omega_n = e^{\frac{2\pi i}{n}}$ е примитивен n-ти корен на единицата в $\mathbb{C}$, а $F_n = F * \mathbb{F}_{q^n}$. Тогава*

$$\zeta(F_n, t^n) = \prod_{j=0}^{n-1} \zeta(F, \omega_n^j t).$$

Доказателство: Лема 17.4 свежда твърдението на лемата към равенството

$$\prod_{w \in \mathcal{P}(F_n)} \frac{1}{1 - t^{n \deg(w)}} = \prod_{j=0}^{n-1} \prod_{v \in \mathcal{P}(F)} \frac{1}{1 - t^{\deg(v)} \omega_n^{j \deg(v)}}.$$

Произволен клас дискретни нормирания $w \in \mathcal{P}(F_n)$ на F_n се ограничава до клас дискретни нормирания $v \in \mathcal{P}(F)$ на F. Ако $\mathcal{P}_v(F_n)$ е множеството на класовете дискретни нормирания $w \in \mathcal{P}(F_n)$, които се ограничават до $w|_F = v \in \mathcal{P}(F)$, то $\mathcal{P}(F_n) = \cup_{v \in \mathcal{P}(F)} \mathcal{P}_v(F_n)$. Достатъчно е да докажем, че за всяко $v \in \mathcal{P}(F)$ е в сила

$$\prod_{w \in \mathcal{P}_v(F_n)} \frac{1}{1 - t^{n \deg(w)}} = \prod_{i=0}^{n-1} \frac{1}{1 - t^{\deg(v)} \omega_n^{j \deg(v)}}. \tag{17.2}$$

Ако $v \in \mathcal{P}(F)$ е от степен $\deg(v) = d$ и $\delta = GCD(d,n)$ е най-големият общ делител на d и n, токомплексното число $\omega_n^d = e^{\frac{2\pi i d}{n}}$ е примитивен корен на единицата от степен $\frac{n}{GCD(d,n)} = \frac{n}{\delta}$. Следователно множеството $\left\{\omega_n^{jd} \mid 0 \leq j \leq \delta\left(\frac{n}{\delta}\right) - 1\right\}$ се състои от корените на единицата от степен $\frac{n}{\delta}$, всеки от които е записан δ пъти. Достатъчно е да докажем равенството

$$1 - t^{\frac{nd}{\delta}} = \prod_{s=0}^{\frac{n}{\delta}-1} \left(1 - t^d \omega_d^s\right)$$

за $\omega_d = e^{\frac{2\pi i}{d}}$. Наистина,

$$\prod_{s=0}^{\frac{n}{\delta}-1} \left(1 - t^d \omega_d^s\right) = t^{d\frac{n}{\delta}} \prod_{s=0}^{\frac{n}{\delta}-1} \left(t^{-d} - \omega_d^s\right) = t^{d\frac{n}{\delta}} \left(t^{-d\frac{n}{\delta}} - 1\right) = 1 - t^{d\frac{n}{\delta}},$$

съгласно $x^{\frac{n}{\delta}} - 1 = \prod_{s=0}^{\frac{n}{\delta}-1} (x - \omega_d^s)$, Q.E.D.

Да напомним, че дивизорите D_1 и D_2 на функционално поле на една променлива F се наричат линейно еквивалентни, ако разликата им $D_1 - D_2 = div(f)$ е дивизор на рационална функция $f \in F$. Класът на линейна еквивалентност на дивизор D означаваме с $[D]$. Дивизорът $div(f)$ на $f \in F$ е от степен 0, така че групата $(div(F), +)$ на главните дивизори е подгрупа на групата $(Div^{(0)}(F), +)$ на дивизорите на F от степен 0.

Лема 17.7. *Дивизорите $Div^{(0)}(F)$ от степен 0 на функционално поле на една променлива F се разбиват в краен брой $h(F)$ класове на линейна еквивалентност.*
Ако F има дивизор от степен $n \in \mathbb{N}$, то множеството $Div^{(n)}(F)$ на дивизорите на F от степен n се състои от $h(F)$ класа на линейна еквивалентност.

Доказателство: Ако кривата X с функционално поле $\mathbb{F}_q(X) = F$ е от род g, избираме дивизор $D \in Div(F)$ от степен $\deg(D) = d \geq g$. По теоремата на Riemann, $l(D) \geq \deg(D) - g + 1 \geq 1$, така че съществува рационална функция $f \in \mathcal{L}(D) \setminus \{0\}$ и ефективен дивизор $D + div(f) \geq 0$ от степен d, линейно еквивалентен с D. Съгласно Лема 17.1, съществуват краен брой $A_d(F)$ ефективни дивизори на F от степен $d = \deg(D) = \deg(D + div(f))$, така че ефективните дивизори, линейно еквивалентни с D са краен брой.
Ако съществува $D \in Div(F)$ от степен $\deg(D) = m$, то класовете на линейна еквивалентност на дивизорите $D \in Div^{(m)}(F)$ от степен m са във взаимно еднозначно съответствие с класовете на линейна еквивалентност на дивизорите $Div^{(0)}(F)$ от степен 0. По-точно, ако фиксираме класа на линейна еквивалентност $[D]$ на $D \in Div^{(m)}(F)$, то произволен клас на линейна еквивалентност $[H]$ на дивизор H от степен m отговаря на еднозначно определен клас на линейна еквивалентност $[H - D]$ на дивизор $H - D \in Div^{(0)}(F)$ от степен 0. Използвайки споменатото съответствие между класовете на линейна еквивалентност на дивизорите от степен $m \geq g$ и дивизорите от степен 0 получаваме съществуването на краен брой $h(F)$ класове на линейна еквивалентност на дивизорите от степен 0. След това прилагаме споменатото съответствие за прозволно m, за което съществува дивизор $D \in Div(F)$ от степен $\deg(D) = m$, Q.E.D.
Ще изброим ефективните дивизори, които са линейно еквивалентни с D, в зависимост от размерността $l(D)$ на линейната система $\mathcal{L}(D)$ на D. Ако $l(D) \geq 1$, то $f \in \mathcal{L}(D) \setminus \{0\}$ тогава и само тогава, когато $D + div(f)$ е ефективен дивизор, линейно еквивалентен с D. Броят на $f \in \mathcal{L}(D) \setminus \{0\} \simeq \mathbb{F}_q^{l(D)} \setminus \{(0, \dots 0)\}$ е $q^{l(D)} - 1$. Главните дивизори $div(f) = div(g)$ съвпадат тогава и само тогава, когато $div\left(\frac{f}{g}\right) = 0$ и $\frac{f}{g} \in \mathbb{F}_q^*$. Оттук, броят на ефективните дивизори на F,

линейно еквивалентни с D е

$$\frac{q^{l(D)}-1}{q-1}.$$

Ако съществува $D \in Div(F)$ от степен n, то множеството $Div^{(n)}(F)$ на дивизорите на F от степен n се състои от $h(F)$ класа на линейна еквивалентност $[D_1], \ldots, [D_{h(F)}]$ и броят на ефективните дивизори на F от степен n е

$$A_n(F) = \sum_{i=1}^{h(F)} \frac{q^{l([D_i])}-1}{q-1}. \tag{17.3}$$

Ако $\deg(D) = n > 2g-2$, то Теоремата на Riemann е изпълнена с равенство и $l(D) = \deg(D) - g + 1 = n - g + 1$. В резултат,

$$A_n(F) = \frac{h(F)}{q-1}\left(q^{n+1-g}-1\right).$$

Твърдение 17.8. *За произволно функционално поле на една променлива F с крайно поле от константи $\mathbb{F}_q$, ζ-функцията на Hasse-Weil $\zeta(F,t)$ е рационална функция на t, т.е. частно на полиноми на t.*

Доказателство: Да напомним, че степента на дивизор

$$\deg : (Div(F), +) \longrightarrow (\mathbb{Z}, +)$$

е хомоморфизъм на групата $Div(F)$ на дивизорите на F. Образът $\mathrm{im}(\deg)$ е ненулева подгрупа на безкрайната циклична група $(\mathbb{Z},+)$, така че $\mathrm{im}(\deg) = k\mathbb{Z}$ за някое $k \in \mathbb{N}$. Естествените числа n, които не се делят на k не са в образа на $\deg$ и не съществуват ефективни дивизори на F от степен n. Следователно $A_n(F) = 0$ за $\forall n \in \mathbb{N} \setminus k\mathbb{N}$ и

$$\zeta(F,t) = \sum_{m=0}^{\infty} A_{km}(F)t^{km}.$$

съгласно Лема 17.5. Да предположим, че F е от род $g(F) \geq 1$. Заместваме (17.3) в горното равенство и отделяме полинома

$$f_1(t) = \sum_{m=0}^{2g-2}\left(\sum_{i=1}^{h(F)} \frac{q^{l([D_i^{(km)}])}-1}{q-1}\right)t^{km} \in \mathbb{Z}[t]$$

от степен $\deg(f_1) \leq k(2g-2)$, където $[D_1^{(km)}], \ldots, [D_{h(F)}^{(km)}]$ са класовете на линейна еквивалентност на дивизорите на F от степен km. Тогава

$$\zeta(F,t) - f_1(t) = \sum_{m>2g-2} \frac{h(F)}{q-1}\left(q^{km+1-g}-1\right)t^{km}$$

е формален степенен ред с цели коефициенти, който се представя във вида

$$\zeta(F,t) - f_1(t) = \sum_{m=0}^{\infty} \frac{h(F)}{q-1}\left(q^{km+1-g}-1\right)t^{km} - f_2(t)$$

чрез полинома

$$f_2(t) = \sum_{m=0}^{2g-2} \frac{h(F)}{q-1}\left(q^{km+1-g}-1\right)t^{km} \in \mathbb{Z}[t]$$

от степен $\deg(f_2) = k(2g-2)$. Непосредствено се пресмята, че

$$\zeta(F,t) - f_1(t) + f_2(t) = \frac{h(F)}{q-1}q^{1-g}\left(\sum_{m=0}^{\infty}(qt)^{km}\right) - \frac{h(F)}{q-1}\left(\sum_{m=0}^{\infty} t^{km}\right) =$$

$$= \frac{h(F)}{q-1}\left(\frac{q^{1-g}}{1-q^k t^k} - \frac{1}{1-t^k}\right)$$

по формулата за сума на безкрайна геометрична прогресия. Това доказва, че ако F е от род $g(F) \geq 1$, то $\zeta(F,t)$ е частно на полиноми на t. В случая $g(F) = 0$ имаме $A_n(F) = \frac{h(F)}{q-1}(q^{n+1}-1)$ за $\forall n \in \mathbb{N}$, така че

$$\zeta(F,t) = \sum_{m=0}^{\infty} \frac{h(F)}{q-1}\left(q^{km+1}-1\right)t^{km} = \frac{h(F)q}{q-1}\left[\sum_{m=0}^{\infty}(qt)^{km}\right] - \frac{h(F)}{q-1}\left(\sum_{m=0}^{\infty} t^{km}\right) =$$

$$= \frac{h(F)q}{q-1}.\frac{1}{1-q^k t^k} - \frac{h(F)}{q-1}.\frac{1}{1-t^k}$$

и

$$\zeta(F,t) = \frac{\frac{h(F)}{q-1}[t^k(q^k-q)+q-1]}{(1-q^k t^k)(1-t^k)} \tag{17.4}$$

също е рационална функция на t, Q.E.D.

Следствие 17.9. *Ако F е функционално поле на една променлива с поле от константи $\mathbb{F}_q$, то за всяко естествено число n съществува дивизор $D \in Div(F)$ на F от степен* $\deg(D) = n$.

Доказателство: Достатъчно е да установим, че F има дивизор $D \in Div(F)$ от степен $\deg(D) = 1$. В означенията от доказателството на Твърдение 17.8 представяме

$$\zeta(F,t) = f_1(t) - f_2(t) + \frac{h(F)}{q-1}\left(\frac{q^{1-g}}{1-q^k t^k} - \frac{1}{1-t^k}\right),$$

където k е минималната естествена степен на дивизор на F. За да докажем, че $k = 1$ забелязаваме, че $\zeta(F,t)$ има прост полюс в $t = 1$. Понеже $t = 1$ е прост корен на полинома $t^k - 1$, формалният степенен ред $\zeta(F_k, t^k)$ има прост полюс в $t = 1$. Съгласно Лема 17.6 $\zeta(F_k, t^k) = \prod_{j=0}^{n-1} \zeta(F, \omega_k^j t)$, където всички множители

$$\zeta(F, \omega_k^j t) = \sum_{m=0}^{\infty}\left(\sum_{i=1}^{h(F)} \frac{q^{l([D_i^{(km)}])}-1}{q-1}\right)t^{km}$$

са равни помежду си и представляват степенни редове на t^k. В резултат,

$$\zeta(F_k, t^k) = \zeta(F,t)^k,$$

така че $\zeta(F_k, t^k)$ има полюс с кратност k в $t = 1$. Понеже $\zeta(F_k, t^k)$ има прост полюс в $t = 1$, оттук следва $k = 1$ и F има дивизор $D \in Div(F)$ от степен $\deg(D) = 1$, Q.E.D.

Като частен случай на Следствие 14.3, ако функционалното поле на една променлива F е от род $g(F) = 0$, то F има ефективен дивизор $D \in Div(F)$ от степен $\deg(D) = 1$, т.е. клас дискретни нормирания $D = v \in \mathcal{P}(F)$ от степен $\deg(v) = 1$. Наистина, ако $D \in Div(F)$ е (необезателно ефективен) дивизор от степен $\deg(D) = 1$, то по Теоремата на Riemann имаме $l(D) \geq \deg(D) - g(F) + 1 = 2$. Следователно съществува $f \in \mathcal{L}(D) \setminus \{0\}$ и ефективен дивизор $D_0 = D + div(f) \geq 0$ от степен $\deg(D_0) = \deg(D) = 1$. В представянето $D_0 = \sum_{v \in \mathcal{P}(F)} n_v v$ с $n_v \geq 0$ и $\deg(v) \in \mathbb{N}$ има едиствен ненулев коефициент $n_{v_o} = 1$ и $D_0 = v_o$ е клас дискретни нормирания от степен $\deg(v_o) = 1$. Съгласно Следствие 14.14, $F = \mathbb{F}_q(\mathbb{P}^1(\overline{\mathbb{F}_q}))$ е функционалното поле на проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ тогава и само тогава, когато F е от род $g(F) = 0$ и съществува клас дискретни нормирания v_o на F от степен $\deg(v_o) = 1$. Направените разглеждания установяват, че $F = \mathbb{F}_q(\mathbb{P}^1(\overline{\mathbb{F}_q}))$ точно когато F е от род $g(F) = 0$.

Следващото твърдение конкретизира числителя на ζ-функцията на Hasse-Weil при знаменател $(1-qt)(1-t)$.

Твърдение 17.10. *За произволно функционално поле на една променлива F с поле от константи $\mathbb{F}_q$ съществува полином $L(F,t) \in \mathbb{Z}[t]$, така че*

$$\zeta(F,t) = \frac{L(F,t)}{(1-qt)(1-t)},$$

$\deg L(F,t) \leq 2g$, $L(F,0) = 1$ *и* $L(F,1) = h(F)$ *е броят на класовете на линейна еквивалентност на дивизорите на F от степен* 0.

Доказателство: Ако F е от род $g(F) = 0$, то вече знаем, че $\zeta(F,t) = \frac{1}{(1-qt)(1-t)}$, така че твърдението е изпълнено с $L(F,t) \equiv 1 \in \mathbb{Z}[t]$. От (17.4) следва, че функционалното поле $F = \mathbb{F}_q(\mathbb{P}^1(\overline{\mathbb{F}_q}))$ на проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ има $h(F) = 1$ или за всяка естествено число n, дивизорите на $\mathbb{F}_q(\mathbb{P}^1(\overline{\mathbb{F}_q}))$ от степен n са линейно еквивалентни помежду си.
Оттук нататък ще предполагаме, че $g(F) \geq 1$. В означенията от Твърдение 17.8 полагаме $f(t) := f_1(t) - f_2(t) \in \mathbb{Z}[t]$ и представяме

$$\zeta(F,t) = f(t) + \frac{h(F)}{q-1}\left(\frac{q^{1-g}}{1-qt} - \frac{1}{1-t}\right)$$

чрез полинома $f(t)$ от степен $\deg(f) \leq 2g-2$. След привеждане под общ знаменател получаваме

$$\zeta(F,t) = \frac{f(t)(1-qt)(1-t) + \frac{h(F)}{q-1}\left[q^{1-g}(1-t) - (1-qt)\right]}{(1-qt)(1-t)} \tag{17.5}$$

и определяме полинома

$$L(F,t) = f(t)(1-qt)(1-t) + \frac{h(F)}{q-1}[q^{1-g}(1-t) - (1-qt)] = \zeta(F,t)(1-qt)(1-t)$$

на t от степен $\deg L(F,t) \leq 2g$. Да отбележим, че полиномът $L(F,t)$ на t е с цели коефициенти, защото се представя като произведение

$$L(F,t) = (1-qt)(1-t)\zeta(F,t) = (1-qt)(1-t)\left(\sum_{n=0}^{\infty} A_n(F)t^n\right)$$

на полинома $(1-qt)(1-t)$ с цели коефициенти и формалния степенен ред $\zeta(F,t) = \sum\limits_{n=0}^{\infty} A_n(F)t^n$ с цели коефициенти. Непосредствено се пресмята, че

$$L(F,0) = [(1-qt)(1-t)\zeta(F,t)]|_{t=0} = \zeta(F,0) = \exp\left(\sum_{n=1}^{\infty}\frac{N_n(F)}{n}t^n\right)|_{t=0} = \exp(0) = 1,$$

а

$$L(F,1) = \left\{f(t)(1-qt)(1-t) + \frac{h(F)}{q-1}\left[q^{1-g}(1-t) - (1-qt)\right]\right\}|_{t=0} =$$

$$= \frac{h(F)}{q-1}(q-1) = h(F),$$

Q.E.D.
Ще докажем, че L-полиномът $L(F,t)$ на функционално поле на една променлива F от род $g(F)$ или, еквивалентно, ζ-функцията $\zeta(F,t)$ се определят еднозначно от $N_1(F), \ldots, N_{g(F)}(F)$, където $N_i(F) = N(F_i)$ е броят на $\mathbb{F}_{q^i}$-рационалните точки на гладката проективна крива X с $\mathbb{F}_q(X) = F$. За целта ни трябва следната

Лема 17.11. *Ако $\zeta(F,t)$ е ζ-функцията на Hasse-Weil на функционалното поле на една променлива F с род $g(F)=g$, то рационалната функция $t^{1-g}\zeta(F,t)$ се запазва при заместване на t с $\frac{1}{qt}$, т.е.*

$$t^{1-g}\zeta(F,t)=\frac{1}{(qt)^{1-g}}\zeta\left(F,\frac{1}{qt}\right).$$

Доказателство: Съгласно Лема 17.5,

$$t^{1-g}\zeta(F,t)=\sum_{n=0}^{\infty}A_n(F)t^{n+1-g}$$

за броя $A_n(F)$ на ефективните дивизори на F от степен n. Да забележим, че формалният степенен ред

$$\sum_{n>2g-2}A_n(F)t^{n+1-g}=\sum_{n>2g-2}\frac{h(F)}{q-1}(q^{n+1-g}-1)t^{n+1-g}$$

зависи само от рода g на F и броя $h(F)$ на класовете на линейна еквивалентност на дивизорите на F от фиксирана степен, докато първите $2g-1$ събираеми

$$\sum_{n=0}^{2g-2}A_n(F)t^{n+1-g}=\sum_{n=0}^{2g-2}\sum_{i=1}^{h(F)}\frac{q^{[D_i^{(n)}]}-1}{q-1}t^{n+1-g}$$

зависят от размерностите $l([D_i^{(n)}])$ на линейните системи на представителите $D_1^{(n)},\dots,D_{h(F)}^{(n)}$ на класовете на линейна еквивалентност на дивизорите $Div^{(n)}(F)$ от степен n. Полагаме

$$X(t):=\sum_{n=0}^{2g-2}\sum_{i=1}^{h(F)}\frac{q^{l([D_i^{(n)}])}}{q-1}t^{n+1-g}$$

да бъде онази част от $\sum\limits_{n=0}^{2g-2}A_n(F)t^{n+1-g}$, която зависи от $l([D_i^{(n)}])$ за $1\leq i\leq h(F)$, $0\leq n\leq 2g-2$. Означаваме с

$$Y(t):=t^{1-g}\zeta(F,t)-X(t)=\sum_{n=2g-1}^{\infty}\frac{h(F)}{q-1}q^{n+1-g}t^{n+1-g}-\sum_{n=0}^{\infty}\frac{h(F)}{q-1}t^{n+1-g}$$

останалите събираеми на $t^{1-g}\zeta(F,t)$. След сумиране на двете безкрайни геометрични прогресии получаваме

$$Y(t)=\frac{h(F)}{q-1}\left(\frac{q^gt^g}{1-qt}-\frac{t^{1-g}}{1-t}\right).$$

Непосредствено се пресмята, че

$$Y\left(\frac{1}{qt}\right)=\frac{h(F)}{q-1}\left[\frac{q^g}{q^gt^g\left(1-\frac{q}{qt}\right)}-\frac{1}{q^{1-g}t^{1-g}\left(1-\frac{1}{qt}\right)}\right],$$

$$Y\left(\frac{1}{qt}\right)=\frac{h(F)}{q-1}\left[\frac{t}{t^g(t-1)}-\frac{qt}{q^{1-g}t^{1-g}(qt-1)}\right],$$

$$Y\left(\frac{1}{qt}\right)=\frac{h(F)}{q-1}\left(\frac{q^gt^g}{1-qt}-\frac{t^{1-g}}{1-t}\right)=Y(t).$$

Остава да докажем, че $X\left(\frac{1}{qt}\right) = X(t)$, за да получим, че $t^{1-g}\zeta(F,t) = X(t) + Y(t)$ се запазва под действие на трансформацията $t \mapsto \frac{1}{qt}$. За целта представяме

$$X(t) = \frac{1}{q-1} \sum_{[D], 0 \leq \deg[D] \leq 2g-2} q^{l[D]} t^{\deg([D])+1-g}$$

като сума по класовете $[D]$ на линейна еквивалентност на дивизорите $D \in Div(F)$ от степен $0 \leq deg(D) \leq 2g-2$. Замяната на t с $\frac{1}{qt}$ дава

$$X\left(\frac{1}{qt}\right) = \frac{1}{q-1} \sum_{[D], 0 \leq \deg[D] \leq 2g-2} q^{l[D]-\deg[D]-1+g} t^{g-1-deg[D]}.$$

По Теорема 20 на Riemann-Roch, за произволен $\mathbb{F}_q$-линеен диференциал $\omega \in \Omega \setminus \{0\}$ е в сила

$$X\left(\frac{1}{qt}\right) = \frac{1}{q-1} \sum_{[D], 0 \leq \deg[D] \leq 2g-2} q^{l[div(\omega)-D]} t^{\deg[div(\omega)-D]-g+1},$$

съгласно $deg(div(\omega)) = 2g-2$. Непосредствено се проверява, че съответствието $D \mapsto div(\omega) - D$ индуцира пермутация на дивизорите $D \in Div(F)$ от степен $0 \leq \deg(D) \leq 2g-2$, така че

$$X\left(\frac{1}{qt}\right) = \frac{1}{q-1} \sum_{[div(\omega)-D], 0 \leq \deg[div(\omega)-D] \leq 2g-2} q^{l[div(\omega)-D]} t^{\deg[div(\omega)-D]-g+1} =$$

$$= \frac{1}{q-1} \sum_{[H], 0 \leq \deg[H] \leq 2g-2} q^{l[H]} t^{\deg[H]-g+1} = X(t).$$

Това доказва, че $t^{1-g}\zeta(F,t) = \frac{1}{(qt)^{1-g}}\zeta\left(F, \frac{1}{qt}\right)$, Q.E.D.

Лема 17.11 дава функционално уравнение за L-полинома $L(F,t)$ на F. По-точно, от

$$\frac{t^{1-g}L(F,t)}{(1-t)(1-qt)} = t^{1-g}\zeta(F,t) = q^{g-1}t^{g-1}\zeta\left(F, \frac{1}{qt}\right) = \frac{q^g t^{g+1} L\left(F, \frac{1}{qt}\right)}{(qt-1)(t-1)}$$

получаваме, че

$$L(F,t) = q^g t^{2g} L\left(F, \frac{1}{qt}\right).$$

Ако $L(F,t) = \sum\limits_{i=0}^{2g} a_i^i$ с $a_i \in \mathbb{Z}$, то

$$L(F,t) = q^g t^{2g} L\left(F, \frac{1}{qt}\right) = q^g t^{2g} \left(\sum_{i=0}^{2g} a_i q^{-i} t^{-i}\right) = \sum_{i=0}^{2g} a_i q^{g-i} t^{2g-i} = \sum_{j=0}^{2g} a_{2g-j} q^{j-g} t^j$$

след замяна на индекса на сумиране $0 \leq i \leq 2g$ с $0 \leq j = 2g - i \leq 2g$. Сравнявайки коефициентите в

$$\sum_{i=0}^{2g} a_i t^i = L(F,t) = \sum_{j=0}^{2g} a_{2g-j} q^{j-g} t^j$$

получаваме

$$a_i = q^{i-g} a_{2g-i} \quad \text{за} \quad \forall 0 \leq i \leq 2g.$$

В частност, старшият коефициент $a_{2g} = q^g a_0 = q^g$, съгласно $a_0 = L(F,0) = 1$. По този начин, коефициентите $a_0 = 1, a_1, \ldots, a_g$ на $L(F,t)$ определят еднозначно коефициентите $a_{g+1}, \ldots, a_{2g-1}, a_{2g} = q^g$. За определянето на $a_1, \ldots, a_g$

разглеждаме

$$L(F,t) = \zeta(F,t)(1-t)(1-qt) = \exp\left(\sum_{n=0}^{\infty} \frac{N_n(F)}{n} t^n\right)(1-t)(1-qt)$$

и пресмятаме логаритмичната производна

$$\frac{d}{dt} \log L(F,t) = \sum_{n=1}^{\infty} N_n(F) t^{n-1} - \frac{1}{1-t} - \frac{q}{1-qt}.$$

Представяме

$$\frac{1}{1-t} = \sum_{n=0}^{\infty} t^n = \sum_{n=1}^{\infty} t^{n-1} \quad \text{и} \quad \frac{1}{1-qt} = \sum_{n=0}^{\infty} q^n t^n \sum_{n=1}^{\infty} q^{n-1} t^{n-1}$$

като суми на безкрайни геометрични прогресии и получаваме

$$\frac{d}{dt} \log L(F,t) = \sum_{n=1}^{\infty} N_n(F) t^{n-1} - \sum_{n=1}^{\infty} t^{n-1} - q \sum_{n=1}^{\infty} q^{n-1} t^{n-1} =$$

$$= \sum_{n=1}^{\infty} (N_n(F) - q^n - 1) t^{n-1}.$$

Ако положим

$$S_n(F) = N_n(F) - (q^n + 1), \tag{17.6}$$

то получаваме

$$\frac{\frac{d}{dt} L(F,t)}{L(F,t)} = \frac{d}{dt} \log L(F,t) = \sum_{n=1}^{\infty} S_n(F) t^{n-1}. \tag{17.7}$$

Замествайки $L(F,t) = \sum\limits_{i=0}^{2g} a_i t^i$ и $\frac{d}{dt} L(F,t) = \sum\limits_{i=1}^{2g} i a_i t^{i-1}$ представяме

$$\sum_{i=1}^{2g} i a_i t^{i-1} = \frac{d}{dt} L(F,t) = \left(\sum_{i=0}^{2g} a_i t^i\right)\left(\sum_{n=1}^{\infty} S_n(F) t^{n-1}\right).$$

Сравняването на коефициентите на t^{i-1} за $1 \leq i \leq 2g$ дава

$$i a_i = \sum_{j=0}^{i-1} a_j S_{i-j}(F). \tag{17.8}$$

Числата $S_i = N_i(F) - (q^i + 1)$ се определят еднозначно от $N_i(F)$. Следователно $N_1(F), \ldots, N_g(F)$ определят еднозначно $S_1(F), \ldots, S_g(F)$, които от своя страна задават еднозначно $a_1, \ldots, a_g$ по формулите (17.8) за $1 \leq i \leq g$.