Глава 18

Теорема на Hasse-Weil и граница на Hasse-Weil за броя на рационалните точки на крива над крайно поле

Съгласно Твърдение 17.10 и разглежданията след Лема 17.11, ζ-функцията на Hasse-Weil на функционално поле на една променлива F с поле от константи $\mathbb{F}_q$ е

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

където $L(F,t) \in \mathbb{Z}[t]$ е полином от степен $2g$ със старши коефициент q^g и свободен член $L(F,0) = 1$. Ако $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ са корените на $L(F,t)$, броени с техните кратности, то

$$L(F,t) = q^g \prod_{i=1}^{2g} (t - \alpha_i).$$

След изнасяне на $(-\alpha_i)$ от всеки множител $t - \alpha_i$ получаваме

$$L(F,t) = (\alpha_1 \ldots \alpha_{2g}) q^g \prod_{i=1}^{2g} \left(1 - \frac{t}{\alpha_i}\right) = \prod_{i=1}^{2g} \left(1 - \frac{t}{\alpha_i}\right),$$

съгласно формулата на Виет

$$\alpha_1 \ldots \alpha_{2g} = (-1)^{2g} \frac{a_0}{a_{2g}} = q^{-g}.$$

Навсякъде в този въпрос означаваме с

$$\omega_i = \frac{1}{\alpha_i}, \quad 1 \leq i \leq 2g,$$

реципрочните на корените α_i на $L(F,t)$ и изразяваме

$$L(F,t) = \prod_{i=1}^{2g} (1 - \omega_i t). \tag{18.1}$$

Теоеремата на Hasse-Weil твърди, че $|\omega_i| = \sqrt{q}$ за $\forall 1 \leq i \leq 2g$. За да докажем тази теорема започваме със следната

Лема 18.1. *Нека F е функционално поле на една променлива с поле от константи $\mathbb{F}_q$, а $N_k(F)$ е броят на $\mathbb{F}_{q^k}$-рационалните точки на гладка проективна крива X с функционално поле $\mathbb{F}_q(X) = F$ над $\mathbb{F}_q$. Ако съществува естествено число m и реална константа $C > 0$, така че*

$$|N_{2mn}(F) - (q^{2mn} + 1)| \leq C q^{mn}$$

за достатъчно големи естествени n, то $|\omega_i| = \sqrt{q}$ за $\forall 1 \leq i \leq 2g$.

Доказателство: Да напомним означението $S_n = N_n(F) - (q^n + 1)$ от (17.6) и формулата (17.7)

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

за логаритмичната производна на L-полинома. Замествайки (17.1) получаваме

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

Вземайки предвид, че

$$\frac{1}{1-\omega_i t}=\sum_{n=1}^{\infty}\omega_i^{n-1}t^{n-1}$$

са суми на безкрайни геометрични прогресии, извеждаме

$$\sum_{i=1}^{2g}(-\omega_i)\sum_{n=1}^{\infty}\omega_i^{n-1}t^{n-1}=\sum_{n=1}^{\infty}S_n(F)t^{n-1}.$$

Сравняването на коефициентите пред t^{n-1} за $\forall n\in\mathbb{N}$ дава

$$-\sum_{i=1}^{2g}\omega_i^n=S_n(F). \tag{18.2}$$

Оттук, $S_{2mn}(F)=-\sum\limits_{i=1}^{2g}\omega_i^{2mn}$ и степенният ред

$$S(t)=\sum_{n=1}^{\infty}S_{2mn}(F)t^n$$

е равен на

$$S(t)=-\sum_{i=1}^{2g}\left[\sum_{n=1}^{\infty}(\omega_i^{2m}t)^n\right]=-\sum_{i=1}^{2g}\frac{\omega_i^{2m}t}{1-\omega_i^{2m}t}, \tag{18.3}$$

съгласно формулата за сума на безкрайна геометрична прогресия с частно $\omega_i^{2m}t$. По предположение, степенният ред $S(t)$ се оценява отгоре абсолютно и равномерно,

$$|S(t)|\leq\sum_{n=1}^{\infty}|S_{2mn}(F)||t|^n\leq\sum_{n=1}^{\infty}Cq^{mn}|t|^n.$$

Следователно редът $S(t)$ е сходящ за всички $t\in\mathbb{C}$ с $|t|<\frac{1}{q^m}$. Оттук получаваме, че всички геометрични прогресии от дясната страна на (17.3) са сходящи, така че $|\omega_i|\leq\sqrt{q}$ за всички $1\leq i\leq 2g$. По-точно, допускането $|\omega_i|>\sqrt{q}$ за някое $1\leq i\leq 2g$ води до съществуване на $\varepsilon\in\mathbb{R}^{>0}$ с $|\omega_i|=\sqrt{q}+\varepsilon$. Вземайки предвид $\left(\sqrt{q}+\varepsilon\right)^{2m}>(\sqrt{q})^{2m}=q^m$, твърдим съществуването на комплексно число $t\in\mathbb{C}$ с

$$\frac{1}{(\sqrt{q}+\varepsilon)^{2m}}<|t|<\frac{1}{q^m}.$$

Сега $|\omega_i^{2m}t|=(\sqrt{q}+\varepsilon)^{2m}|t|>1$ противоречи на сходимостта на сумата $\frac{1}{1-\omega_i^{2m}t}$ на безкрайната геометрична прогресия с частно $\omega_i^{2m}t$ и доказва $|\omega_i|\leq\sqrt{q}$ за $\forall 1\leq i\leq 2g$. Старшият коефициент на L-полинома е

$$q^g=\prod_{i=1}^{2g}(-\omega_i)=\prod_{i=1}^{2g}\omega_i$$

с модул $q^g=\prod\limits_{i=1}^{2g}|\omega_i|\leq(\sqrt{q})^{2g}=q^g$, така че $|\omega_i|=\sqrt{q}$ за $\forall 1\leq i\leq 2g$, Q.E.D.

Ако в Лема 17.1 заменим крайното поле $\mathbb{F}_q$ с крайното поле $\mathbb{F}_{q^m}$ и функционалното поле на една променлива F над $\mathbb{F}_q$ с функционалното поле на една променлива $F*\mathbb{F}_{q^m}$ над $\mathbb{F}_{q^m}$, то предположението $|S_{2n}(F)| \leq Cq^n$ за достатъчно големи $n \in \mathbb{N}$ се записва като $S_{2n}(F) = O(q^n)$. По този начин,

$$N_{2n}(F) = q^{2n} + O(q^n) \tag{18.4}$$

се оказва достатъчно условие за верността на Теоремата на Hasse-Weil $|\omega_i| = \sqrt{q}$, $\forall 1 \leq i \leq 2g$.

Лема 18.2. *Нека X е гладка проективна крива от род g, определена над крайното поле $\mathbb{F}_{s^2}$ с s^2 елемента, а $F = \mathbb{F}_{s^2}(X)$ е функционалното поле на X над $\mathbb{F}_{s^2}$. Ако $s > (g+1)^2$, то броят $N(F)$ на $\mathbb{F}_{s^2}$-рационалните точки на X изпълнява строгото неравенство*

$$N(F) < s^2 + 1 + s(2g+1).$$

Доказателство: Ако X няма $\mathbb{F}_{s^2}$-рационални точки и $N(F) = 0$, няма какво да се доказва.
Оттук нататък предполагаме, че $N(F) \geq 1$ и фиксираме $\mathbb{F}_{s^2}$-рационална точка $Q \in X(\mathbb{F}_{s^2})$. Съгласно

$$\mathcal{L}((s-1)Q) = \{z \in F^* \ \mid \ div(z) + (s-1)Q \geq 0\} \cup \{0\},$$

ненулевите елементи z на $\mathcal{L}((s-1)Q)$ имат полюс от ред $\leq s-1$ в Q и са регулярни в останалите точки на X. Ако $y, z \in \mathcal{L}((s-1)Q)$ имат един и същи дивизор на полюсите $(y)_\infty = (z)_\infty = jQ$ за някое $0 \leq j \leq s-1$, $\frac{y}{z} \in F$ е рационална функция върху X без полюси, така че $\frac{y}{z} \in \mathbb{F}_{s^2}^*$ и y, z са линейно зависими над $\mathbb{F}_{s^2}$. Оттук следва, че произволен $\mathbb{F}_{s^2}$-базис B на $\mathcal{L}((s-1)Q)$ е от вида $B = \{b_j \ \mid \ j \in J\}$ за рационални функции $b_j \in F$ с дивизори на полюсите $(b_j)_\infty = jQ$ и подмножество $J \subseteq \{0, 1, \ldots, s-1\}$.
Да означим $n = s + 2g$ и да изберем $x \in \mathcal{L}((s-1)Q) \setminus \{0\}$, $y \in \mathcal{L}(nQ) \setminus \{0\}$. Тогава $div(xy^s) + (s-1+ns)Q \geq 0$ и $xy^s \in \mathcal{L}((s-1+ns)Q)$. Нека

$$H = l_{\mathbb{F}_{s^2}}(xy^s \ \mid \ x \in \mathcal{L}((s-1)Q), \ \ y \in \mathcal{L}(nQ))$$

е $\mathbb{F}_{s^2}$-линейната обвивка на всички такива произведения. Произволен базис C на $\mathcal{L}(nQ)$ е от вида $C = \{c_i \ \ |i \in I\}$ за рационални функции $c_i \in F$ с дивизори на полюсите $(c_i)_\infty = iQ$ и подмножество $I \subseteq \{0, 1, \ldots, n\}$. Твърдим, че множеството

$$\{b_j c_i^s \ \mid \ j \in J, \ \ i \in I\}$$

е $\mathbb{F}_{s^2}$-базис на H. Посочените елементи пораждат H като линейно пространство над $\mathbb{F}_{s^2}$, защото всеки елемент $x \in \mathcal{L}((s-1)Q)$ се представя като линейна комбинация $x = \sum\limits_{j \in J} \beta_j b_j$ на b_j с коефициенти $\beta_j \in \mathbb{F}_{s^2}$, а $\forall y \in \mathcal{L}(nQ)$ е $\mathbb{F}_{s^2}$-линейна комбинация $y = \sum\limits_{i \in I} \gamma_i c_i$, $\gamma_i \in \mathbb{F}_{s^2}$. В резултат,

$$xy^s = \left(\sum_{j \in J} \beta_j b_j\right) \left(\sum_{i \in I} \gamma_i c_i\right)^s = \left(\sum_{j \in J} \beta_j b_j\right) \left(\sum_{i \in I} \gamma_i^s c_i^s\right) = \sum_{j \in J} \sum_{i \in I} \beta_j \gamma_i^s b_j c_i^s,$$

защото s е естествена степен на характеристиката на полето F. За линейната независимост на $\{b_j c_i^s \ \mid \ j \in J, i \in I\}$ над $\mathbb{F}_{s^2}$ да разгледаме произволна тяхна линейна комбинация

$$z = \sum_{j \in J} \sum_{i \in I} \alpha_{ji} b_j c_i^s, \quad \alpha_{ji} \in \mathbb{F}_{s^2}.$$

Въвеждаме $d_j = \sum\limits_{i \in I} \alpha_{ji} c_i^s \in \mathcal{L}(snQ)$ за $\forall j \in J$. Понеже s е естествена степен на характеристиката на полето $\mathbb{F}_{s^2}$, степенуването

$$\Phi_s : \mathbb{F}_{s^2} \longrightarrow \mathbb{F}_{s^2},$$

$$\Phi_s(\alpha) = \alpha^s$$

е автоморфизъм и има коректно определен обратен

$$\Phi_s^{-1} : \mathbb{F}_{s^2} \longrightarrow \mathbb{F}_{s^2}.$$

Ако $\Phi_s^{-1}(\alpha_{ji}) = \lambda_{ji} \in \mathbb{F}_{s^2}$, то $\lambda_{ji}^s = \alpha_{ji}$, така че $d_j = \sum\limits_{i\in I} \lambda_{ji}^s c_i^s = \left(\sum\limits_{i\in I} \lambda_{ji} c_i\right)^s = e_j^s$ за $e_j = \sum\limits_{i\in I} \lambda_{ji} c_i \in \mathcal{L}(nQ)$, $\forall j \in J$. В резултат, $z = \sum\limits_{j\in J} b_j e_j^s$. Ако $e_j = \sum\limits_{i\in I} \lambda_{ji} c_i \neq 0$, то класът дискретни нормирания $v_Q \in \mathcal{P}(F)$, отговарящ на $\mathbb{F}_{s^2}$-затворената точка $Q \in X(\mathbb{F}_{s^2})$ от степен 1 има стойност $v_Q(e_j) = -i_o \neq \infty$ за максималния елемент $i_o \in I$ с $\lambda_{ji_o} \neq 0$. Ако съществува $e_j \neq 0$, то

$$v_q(z)(\mathrm{mod}\ \ s) = v_Q\left(\sum_{j\in J} b_j e_j^s\right)(\mathrm{mod}\ \ s) \equiv -j_o(\mathrm{mod}\ \ s)$$

за максималния индекс $j_o \in J$ с $e_{j_o} \neq 0$. По този начин доказахме, че ако $z = 0$ и $v_Q(z) = \infty$, то $e_j = \sum\limits_{i\in I} \lambda_{ji} c_i = 0$ за $\forall j \in J$. Съгласно линейната независимост на $\{c_i \mid i \in I\}$ над $\mathbb{F}_{s^2}$, оттук следва $\lambda_{ji} = 0$ и $\alpha_{ji} = \lambda_{ji}^s = 0$ за $\forall i \in I$, $\forall j \in J$. С това проверихме линейната независимост на $\{b_j c_i^s \ \ j \in J, i \in I\}$ над $\mathbb{F}_{s^2}$ и установихме, че размерността

$$\dim_{\mathbb{F}_{s^2}}(H) = |J||I| = l((s-1)Q)l(nQ).$$

По Теорема 17 на Riemann,

$$l((s-1)Q) \geq \deg((s-1)Q) - g + 1 = s - g, \quad l(nQ) \geq \deg(nQ) - g + 1 = s + g + 1,$$

откъдето

$$\dim_{\mathbb{F}_{s^2}} \geq (s-g)(s+g+1) = s^2 + s - g^2 - g.$$

По предположение, $s > (g+1)^2$, така че

$$\dim_{\mathbb{F}_{s^2}}(H) > s^2 + (g+1)^2 - g^2 - g = s^2 + g + 1.$$

Нека $m = s^2 + 2g$, а ψ е изображението, трансформиращо произволен елемент $z = \sum\limits_{j\in J} \sum\limits_{i\in I} \alpha_{ji} b_j c_i^s H$ в

$$\psi\left(\sum_{j\in J}\sum_{i\in I} \alpha_{ji} b_j c_i^s\right) = \sum_{j\in J}\sum_{i\in I} \alpha_{ji}^s b_j^s c_i.$$

Непосредствено се проверява, че $b_j^s c_i \in \mathcal{L}([s(s-1)+n]Q) = \mathcal{L}(mQ)$, така че

$$\psi : H \longrightarrow \mathcal{L}(mQ)$$

взема стойности в $\mathcal{L}(mQ)$. Съгласно $(\alpha_{ji} + \alpha'_{ji})^s = \alpha_{ji}^s + (\alpha'_{ji})^s$ за $\forall \alpha_{ji}, \alpha'_{ji} \in \mathbb{F}_{s^2}$ изображението ψ е $\mathbb{F}_{s^2}$-линейно. По Теорема 20 на Riemann-Roch,

$$l(mQ) - l(div(\omega) - mQ) = m - g + 1 = s^2 + g + 1.$$

Още повече, степента $\deg(div(\omega) - mQ) = 2g - 2 - m = -s^2 - 2 < 0$, така че $l(div(\omega) - mQ) = 0$ и $l(mQ) = s^2 + g + 1$. Ако допуснем, че ψ е влагане, то

$$s^2 + g + 1 < \dim_{\mathbb{F}_{s^2}}(H) \leq l(mQ) = s^2 + g + 1,$$

което е противоречие. Следователно съществува $z \in \ker(\psi) \setminus \{0\}$. Елементите $y \in H$ се преставят като $\mathbb{F}_{s^2}$-линейни комбинации $y = \sum\limits_{j\in J}\sum\limits_{i\in I} \alpha_{ji} b_j c_i^s$ на $b_j c_i^s$. В произволна точка $P \in X(\mathbb{F}_{s^2}) \setminus \{Q\}$ имаме

$$y(P)^s = \left[\sum_{j \in J} \sum_{i \in I} \alpha_{ji} b_j(P) c_i(P)^s \right]^s = \sum_{j \in J} \sum_{i \in I} \alpha_{ji}^s b_j(P)^s c_i(P)^{s^2},$$

защото s е степен на характеристиката. Елементите $c_i(P)$ на крайното поле $\mathbb{F}_{s^2}$ са корени на уравнението $z^{s^2} = z$, така че

$$y(P)^s = \sum_{j \in J} \sum_{i \in I} \alpha_{ji}^s b_j(P)^s c_i(P) = \psi \left(\sum_{j \in J} \sum_{i \in I} \alpha_{ji} b_j c_i^s \right)(P) = \psi(y)(P).$$

В частност, за $z \in \ker(\psi) \setminus \{0\}$ получаваме $z(P)^s = \psi(z)(P) = 0$ във всяка точка $P \in X(\mathbb{F}_{s^2}) \setminus \{Q\}$. С други думи, дивизорът $(z)_0$ на нулите на z е от степен $\deg(z)_0 \geq N(F) - 1$. От друга страна, $z \in H \subset \mathcal{L}((s-1+ns)Q)$ изисква $(z)_0 - (z)_\infty + (s-1+ns)Q \geq 0$, откъдето

$$\deg(z)_0 = \deg(z)_\infty \leq s - 1 + ns = s^2 - 1 + s(2g+1).$$

В резултат,

$$N(F) \leq s^2 + s(2g+1) < s^2 + 1 + s(2g+1),$$

Q.E.D.

Определение 18.3. *Доминантното рационално изображение на криви*

$$f : Y \longrightarrow X$$

се нарича крайно сепарабелно покритие, ако $k(Y) \supset f^*k(X)$ *е крайно сепарабелно разширение.*

Определение 18.4. *Степента на крайно сепарабелно покритие* $f : Y \to X$ *се определя като степента* $\deg(f) = [k(Y) : f^*k(X)]$ *на функционалното поле* $k(Y)$ *на* Y *над функционалното поле* $f^*k(X) \simeq k(X)$ *на* X.

Определение 18.5. *Индексът на разклонение на крайно сепарабелно покритие* $f : Y \to X$ *на криви в точка* $y \in Y$ *е индексът на разклонение*

$$e_y(f) = e(w_y/v_{f(y)}) = [w_y(k(Y)^*) : v_{f(y)}(f^*k(X)^*)]$$

на класа дискретни нормирания $w_y : k(Y)^* \to \mathbb{Z} \cup \{\infty\}$, *отговарящ на* $Orb_{Gal(\overline{k}/k)}(y)$ *над класа дискретни нормирания* $v_{f(y)} : k(X) \to \mathbb{Z} \cup \{\infty\}$, *съответстващ на* $Orb_{Gal(\overline{k}/k)}(f(y))$, $f(y) \in X$.
Точките $y \in Y$, *в окито* $f : Y \to X$ *има индекс на разклонение* $e_y(f) = 1$ *се наричат неразклонени за* f.

Твърдение 18.6. *Нека* $f : Y \to X$ *е сепарабелно покритие на криви от степен* $\deg(f) = [k(Y) : f^*k(X)] = n$. *Тогава:*
(i) броят $|f^{-1}(x)|$ *на точките в слоя* $f^{-1}(x)$ *на* f *над* $x \in X$ *не надминава* n;
(ii) $|f^{-1}(x)| = n$ *за всички точки* $x \in X$ *с изключение на краен брой;*
(iii) $|f^{-1}(x)| = n$ *тогава и само тогава, когато всички точки* $y \in f^{-1}(x)$ *са неразклонени за* f.

Доказателство: Можем да считаме, че $f : Y_o \to X_o$ е регулярно изображение на афинни криви, което се задава с полиноми. Разглеждаме графика

$$\Gamma_f = \{(y_o, f(y_o)) \ \mid \ y_o \in Y_o\} \subset Y_o \times X_o$$

на f с каноничните му проекции

$$\mathrm{pr}_1 : \Gamma_f \longrightarrow Y_o,$$

$$\mathrm{pr}_1(y_o, f(y_o)) = y_o$$

и

$$\mathrm{pr}_2 : \Gamma_f \longrightarrow X_o,$$
$$\mathrm{pr}_2(y_o, f(y_o)) = f(y_o).$$

В сила е комутативна диагарама

$$\begin{tikzcd} \Gamma_f \arrow[r, "\mathrm{pr}_2"] \arrow[d, "\mathrm{pr}_1"] & X_o \arrow[d, "\mathrm{Id}_{X_o}"] \\ Y_o \arrow[r, "f"] & X_o \end{tikzcd}$$

така че $\mathrm{pr}_2 = f \circ \mathrm{pr}_1$. Проекцията pr_1 е взаимно еднозначна. Слоевете на pr_2 и f съвпадат, така че е достатъчно да докажем твърдението за крайното сепарабелно покритие $\mathrm{pr}_2 : \Gamma_f \to X_o$, което изпуска няколко афинни координати. За произволна композиция $g_1 g_2 : M_2 \to M$ на морфизми $g_2 : M_2 \to M_1$ и $g_1 : M_1 \to M$, степента

$$[k(M_2) : (g_1 g_2)^* k(M)] = [k(M_2) : g_2^* k(M_1)][k(M_1) : g_1^* k(M)]$$

на функционалните полета е мултипликативна функция, както и броят на точките в слоя

$$|(g_1 g_2)^{-1}(x)| = \sum_{x_1 \in g_1^{-1}(x)} |g_2^{-1}(x_1)| = |g_2^{-1}(x_1)||g_1^{-1}(x)| \quad \text{за} \quad x_1 \in g_1^{-1}(x).$$

Затова е достатъчно да установим твърдението за доминантно изпускане

$$\mathrm{pr} : Z_o \longrightarrow X_o,$$
$$\mathrm{pr}(x_0, x_1, \ldots, x_m) = (x_1, \ldots, x_m)$$

на една афинна координата. Функционалното поле $k(Z_o) = \mathrm{pr}^* k(X_o)(x_o)$ на Z_o е примитивно разширение на $\mathrm{pr}^* k(X_o) \simeq k(X_o)$ с елемент x_o, който е от степен n над $\mathrm{pr}^* k(X_o) \simeq k(X_o)$. От друга страна, за всяка фиксирана точка $x = (x_1, \ldots, x_m) \in X_o$ слоят $\mathrm{pr}^{-1}(x)$ на pr е изоморфен на множеството на онези $x'_o \in k$, които са корени на минималния полином $f_{x_o}(z) \in k(X_o)[z]$ на x_o над $k(X_o)$. Броят на тези x'_o не надминава степента n на $f_{x_o}(z)$. Слоят $\mathrm{pr}^{-1}(x)$ съдържа по-малко от n точки тогава и само тогава, когато $f_{x_o}(z)$ има кратен корен или дискриминантата $D(f_{x_o}) = 0 \in k(X_o)$. Условието $D(f_{x_o}) = 0$ е полиномиално уравнение върху кривата X_o и е изпълнено в най-много краен брой точки.

За да докажем, че $|f^{-1}(x)| = n$ е еквивалентно на $e_y(f) = 1$ за $\forall y \in f^{-1}(x)$ да разгледаме локален параметър t на $k(X)$ в $x \in X$ и локален параметър s_y на $k(Y)$ в $y \in f^{-1}(x)$. Тогава $v_x(k(X)^*) = v_x(t)\mathbb{Z}$, $v_y(k(Y)^*) = v_y(s_y)\mathbb{Z}$. Ако $e_y = e_y(f) = [v_y(k(Y)^*) : v_x(k(X)^*)]$, то без ограничение на общността можем да считаме, че $v_y(s_y) = 1$, $v_x(t) = e_y$. Тогава $v_y(t s_y^{-e_y}) = 0$ и $t s_y^{-e_y} = u_y \in \mathcal{O}_y(Y)^*$. Понеже $t = 0$ е локалното уравнение на x в X, $s_y^{e_y} u_y = 0$ е локалното уравнение на слоя $f^{-1}(x)$ в Y. В резултат получаваме

$$t = \alpha \prod_{y \in f^{-1}(y)} s_y^{e_y} \quad \text{с} \quad \alpha \in k^*.$$

По-точно, $s_y^{e_y}$ делят t и s_y са взаимно прости за различните точки $y \in f^{-1}(x)$. Частното

$$\alpha = \frac{t}{\prod_{y \in f^{-1}(x)} s_y^{e_y}}$$

няма нули, откъдето $\alpha \in k^*$.

Ако $|f^{-1}(x)| = n$, то $f^{-1}(x) = \{y_1, \ldots, y_n\}$ и $t = \alpha s_1^{e_1} \ldots s_n^{e_n}$, $\alpha \in k^*$ за локални параметри s_i на $k(Y)$ в y_i и $e_i = e_{y_i}(f)$. Броят на корените на $t = 0$ е $n = e_1 + \ldots + e_n$, откъдето $e_i = 1$ за $\forall 1 \leq i \leq n$ и всички точки $y \in f^{-1}(x)$ са неразклонени за f.
Обратно, нека $e_y(f) = 1$ за $\forall y \in f^{-1}(x)$. Ако допуснем, че $|f^{-1}(x)| = l < n$, то $t = \alpha s_1 \ldots s_l$ с $\alpha \in k^*$. Слоевете с по-малко от n точки са граници на слоевете с n точки. Вече знаем, че за слой с n точки уравнението $t = 0$ има n корена. Следователно върху слоевете с $|f^{-1}(x)| = l < n$ уравнението $t = 0$ има n корена, броени с техните кратности. Това е невъзможно за $t = \alpha s_1 \ldots s_l$ и доказва $|f^{-1}(x)| = n$, когато $e_y(f) = 1$ за $\forall y \in f^{-1}(x)$, Q.E.D.

Теорема 21. (Формула на Riemann-Hurwitz за рода на крайно сепарабелно покритие на крива) *Нека $f : Y \to X$ е сепарабелно покритие на гладки криви от степен n,*

$$R = \sum_{y \in Y} (e_y(f) - 1)$$

е дивизорът на разклонение на f и характеристиката $char(k)$ на основното поле е 0 или просто число $char(k) = p$, което не дели индекстие на разклонение $e_y(f)$ на f във всички точки $y \in Y$. Тогава каноничният дивизор K_Y на Y е линейно еквивалентен на дивизора $f^*K_X + R$, откъдето

$$2g(Y) - 2 = \deg(f)(2g(X) - 2) + \sum_{y \in Y} e_y(f) - 1 \tag{18.5}$$

за рода $g(Y)$ на Y и рода $g(X)$ на X.

Доказателство: Равенството 17.5 следва непосредствено от приравняване на степените на K_Y и $f^*K_X + R$. Преди да докажем $[K_Y] = [f^*K_X + R]$ да отбележим, че носителят на R е краен, понеже $e_y(f) > 0$ за най-много краен брой точки $y \in Y$. Да изберем локален параметър s на $k(Y)$ в $y \in Y$ и локален параметър t на $k(X)$ в $x = f(y) \in X$. Ако $v_y(s) = 1$ и $e_y(f) = e$, то $v_{f(y)}(t) = e$ и $t = s^e u$ за някое $u \in \mathcal{O}_y(Y)^*$. Оттук

$$dt = es^{e-1}uds + s^e du$$

и

$$v_y\left(\frac{dt}{ds}\right) = v_y\left(es^{e-1}u + s^e \frac{du}{ds}\right) = e - 1$$

за $char(k) = 0$ или за проста характеристика $char(k) = p$, не деляща e. Снопът $\Phi_Y / f^*\Phi_X$ на относителните регулярни диференциали има слой

$$(\Phi_Y / f^*\Phi_X)\,|_y = \left(\mathcal{O}_y(Y)ds / f^*\mathcal{O}_{f(y)}(X)dt\right)|_y \simeq$$

$$\simeq \mathcal{O}_y(Y)/f^*\mathcal{O}_{f(y)}(X)\left(\frac{dt}{ds}\right)|_y \simeq \mathcal{L}((e-1)y).$$

Глобално, снопът $\Phi_Y / f^*\Phi_X = \mathcal{A}(R)$ на относителните регулярни диференциали съвпада с аделното простренство на дивизора на разклонение R. За произволни $\omega \in \Phi_Y$ и $\eta \in \Phi_X$ частното $s = \frac{\omega}{f^*\eta}$ е сечение на линейното разслоение, асоцирано с R. Дивизорът $R = div(s) = div(\omega) - f^*div(\eta)$ е линейно еквивалентен на $K_Y - f^*K_X$, Q.E.D.

Пример 18.7. *Прозиволна гладка проективна равнинна кубика*

$$X = \{[x : y : z] \in \mathbb{P}^2(\overline{k}) \quad y^2 z = \prod_{i=1}^{3}(x - x_i z)\}$$

с различни $x_1, x_2, x_3 \in \overline{k}$ е сепарабелно покритие

$$f : X \longrightarrow \mathbb{P}^1(\overline{k}),$$

$$f([x:y:z]) = [x:z]$$

от степен 2, защото минималният полином на y над $k(\mathbb{P}^1)$ е от степен 2 и без кратни корени. Ако $P_i = [x_i : 0 : 1]$ за $1 \leq i \leq 3$ и $\infty = [0:1:0]$, то дивизорът на разклонение

$$R = 2P_1 + 2P_2 + 2P_3 + 2\infty.$$

Над крайно поле $\mathbb{F}_q$ с нечетна характеристика, формулата на Riemann-Hurwitz дава $g(X) = 1$, вземайки предвид, че $g(\mathbb{P}^1) = 0$.

Определение 18.8. *Доменантното рационално изображение на криви $f : Y \to X$, определено над k се нарича покритие на Galois, ако $k(Y) \supset f^*k(X)$ е крайно разширение на Galois.*

Да напомним, че крайното разширение $k(Y) \supset f^*k(X)$ е разширение на Gallois, ако е сепарабелно и нормално. По определение, $k(Y) \supset f^*k(X)$ е сепарабелно, ако минималният полином $g_v(z) \in f^*k(X)[z]$ на произволен елемент $v \in k(Y)$ над $f^*k(X)$ няма кратни корени. Разширението $k(Y) \supset f^*k(X)$ е нормално, ако минималният полином $g_v(z) \in f^*k(X)[z]$ на произволен елемент $v \in k(Y)$ над $f^*k(X)$ се разлага в линейни множители над $k(Y)$.

Определение 18.9. *Групата на Gallois $G_k = Gal(k(Y)/f^*k(X))$ на съответните функционални полета се нарича група на Galois на покритието $f : Y \to X$.*

Да напомним, че действието на група G върху множество M е ефективно, ако всеки елемент $x \in M$ има тривиален стабилизатор $Stab_G(x) = \{e_G\}$ за неутралния елемент e_G на G.
Действието на група G върху множество M е транзитивно, ако за произволни елементи $x, y \in M$ съществува $g \in G$ с $gx = y$.

Твърдение 18.10. *Нека $f : Y \to X$ е покритие на Galois, определено над k с група на Galois $G_k = Gal(k(Y)/f^*k(X))$. Тогава:*
(i) G_k действа транизтивно и ефективно върху неразклонениет солеве $f^{-1}(x)$ над k-рационалните точки $x \in X(k)$;
(ii) G_k действа транзитивно върху разклонените слоеве $f^{-1}(x)$ над k-рационалните точки $x \in X(k)$;
(iii) $X = Y/G_k$ е факторът на Y под действие на G_k;
(iv) за всяко разширение $k_1 \supset k$, групите на Galois $G_{k_1} \simeq G_k$ са изоморфни.

Доказателство: Съгласно Твърдение 17.6 (iii), ако всички точки $y \in f^{-1}(x)$ са неразклонение за f, то

$$|f^{-1}(x)| = \deg(f) = [k(Y) : f^*k(X)].$$

В Твърдение 2.6 установихме равенството

$$[k(Y) : f^*k(X)] = |G_k|$$

за крайното сепаарбелно разширение на Galois $k(Y) \supset f^*k(X)$. За изучаване на действието на G_k върху фиксиран слой $f^{-1}(p)$, $p \in X(k)$ можем да считаме, че $Y \subseteq \overline{k}^n$ и $X \subseteq \overline{k}^m$ са афинни криви, определени над k, а

$$f = (f_1, \ldots, f_m) : Y \longrightarrow X$$

се задава с полиноми $f_i(y_1, \ldots, y_n) \in k[y_1, \ldots, y_n]$ за $\forall 1 \leq i \leq m$. За произволна точка $c = (c_1, \ldots, c_m) \in X \subseteq \overline{k}^m$, слоят $f^{-1}(c) \subset Y$ е множеството на решенията на системата уравнения

$$\left| \begin{array}{c} f_1(y_1, \ldots, y_n) = c_1 \\ \ldots\ldots\ldots\ldots\ldots \\ f_m(y_1, \ldots, y_n) = c_m \end{array} \right. \tag{18.6}$$

в $Y \subseteq \overline{k}^n$. Ако $c = (c_1, \ldots, c_m) \in X(k) \subseteq k^m$ е k-рационална точка на X, то всеки автоморфизъм $\sigma \in G_k = Gal(k(Y)/f^*k(X))$ оставя на място точките $c_i \in k$ и полиномите $f_i(y_1, \ldots, y_n) \in k[y_1, \ldots, y_n]$. В резултат, σ действа върху решенията на (17.6) или върху слоевете $f^{-1}(c)$ на f над k-рационалните точки $c \in X(k)$.

За транзитивността на действието на G_k върху неразклонен слой $f^{-1}(x)$ избираме примитивен елемент θ на $k(Y)$ над $f^*k(X)$, $k(Y) = f^*k(X)(\theta) = f^*k(X)[\theta]$. Точките $y(\theta) = (y_1(\theta), \ldots, y_n(\theta)) \in f^{-1}(x)$ от слоя на f над $x \in X(k)$ са наредени n-торки полиноми $y_j(\theta) \in f^*k(X)[\theta]$. Всеки елемент σ от групата на Galois $G_k = Gal(f^*k(X)[\theta]/f^*k(X))$ се определя еднозначно от $\sigma(\theta) = \theta_i$, където $\theta = \theta_1, \theta_2, \ldots, \theta_d$, $d = \deg(f)$ са корените на минималния полином $g_\theta(z) = \prod_{i=1}^{d}(z - \theta_i) \in f^*k(X)[z]$ на θ над $f^*k(X)$. Полето $k(Y) = f^*k(X)(y_1, \ldots, y_n)$ е разширение на $f^*k(X)$ чрез $y_1, \ldots, y_n$, така че $\theta = \theta(y_1, \ldots, y_n)$ може да се представи като полином на $y_1, \ldots, y_n$. Достатъчно е да докажем, че G_k-орбитата на $(y_1(\theta), \ldots, y_n(\theta))$ се състои от d точки, за да получим транзитивността на G_k върху неразклонен слой $f^{-1}(x)$. При допускане на противното имаме $(y_1(\theta_i), \ldots, y_n(\theta_i)) = (y_1(\theta_j), \ldots, y_n(\theta_j))$ за $1 \leq i < j \leq d$. Тогава

$$\theta_i = \theta(y_1(\theta_i), \ldots, y_n(\theta_n)) = \theta(y_1(\theta_j), \ldots, y_n(\theta_j)) = \theta_j,$$

противно на сепарабелността на елемента θ над $f^*k(X)$. Противоречието доказва транзитивността на действието на G_k върху неразклонен слой $f^{-1}(x)$. Това действие е ефективно, защото групата G_k се състои от d елемента и щом орбитата съдържа d точки, стабилизаторите са тривиални.

Разклонените слоеве на f са граници на неразклонени слоеве, така че транзитивността на действието на G_k се наследява от разклоненията слоеве. Щом слоевете на f представляват G_k-орбити, образът X на f има бирегулярно изображение

$$X \longrightarrow Y/G,$$
$$x \mapsto Orb_{G_k}(y) \quad \text{за} \quad y \in f^{-1}(x).$$

За произволно разширение $k_1 \supset k$, ограничението

$$\rho : G_{k_1} = Gal(k_1(Y)/f^*k_1(X)) \longrightarrow Gal(k(Y)/f^*k(X)) = G_k$$

е хомоморфизъм на групи. Още повече, ρ е влагане, защото ако $\sigma \in G_{k_1}$ действа тъждествено върху $k(Y)$, то σ действа тъждествено върху композита $k_1(Y) = k(Y) * k_1$. Следователно $\rho : G_{k_1} \to \mathrm{im}(\rho) = \rho(G_{k_1})$ е изоморфизъм върху образа си. Броят на елементите на G_k и G_{k_1} е равен на броя на точките в неразклонен слой $f^{-1}(x)$, така че $|G_{k_1}| = |f^{-1}(x)| = |G_k$ и $\mathrm{im}(\rho) = \rho(G_{k_1}) = G_k$. Това доказва, че $\rho : G_{k_1} \to G_k$ е изоморфизъм, Q.E.D.

Съгласно Лема 17.1, достатъчно е да установим, че $N_{2n}(F) = q^{2n} + O(q^n)$, за да получим, че $|\omega_i| = \sqrt{q}$ за $\forall 1 \leq i \leq 2g$ (Теорема на Hasse-Weil). За целта избираме трансцендентен над $\mathbb{F}_q$ елемент $x \in F = \mathbb{F}_q(X)$, така че F да е крайно сепарабелно разширение на $\mathbb{F}_q(x)$. Нека K е обвивката на Galois на F над $\mathbb{F}_q(x)$, т.е. K е минималното разширение на F, което е разширение на Galois на $\mathbb{F}_q(x)$. Ако $\mathbb{F}_{q^m}$ е пълното поле от константи на K, а $F_m = F * \mathbb{F}_{q^m}$, то в сила е следната комутативна диаграма от влагания на полета

$$\begin{tikzcd}
\mathbb{F}_{q^m} \arrow[r] & \mathbb{F}_{q^m}(x) \arrow[r] & F_m \arrow[r] & K \\
\mathbb{F}_q \arrow[r] \arrow[u] & \mathbb{F}_q(x) \arrow[r] \arrow[u] & F \arrow[r] \arrow[u] & K \arrow[u, "\mathrm{Id}"']
\end{tikzcd}.$$

Разширението $F_m \supseteq \mathbb{F}_q(x)$ е крайно и сепарабелно, в качеството си на композит на крайните сепарабелни разширения $F_m \supseteq F$ и $F \supseteq \mathbb{F}_q(x)$. Следователно $F_m \supseteq \mathbb{F}_{q^m}(x)$ е крайно сепарабелно разширение, защото минималните полиноми на $y \in F_m$ над $\mathbb{F}_{q^m}(x)$ делят минималните полиноми на y над $\mathbb{F}_q(x)$. Твърдим, че $K \supseteq \mathbb{F}_{q^m}(x)$ е разширение на Galois. Наистина, $K \supset \mathbb{F}_q(x)$ е крайно сепарабелно разширение. Минималният полином $g_{y,m}(z) \in \mathbb{F}_{q^m}(x)[z]$ на $y \in K$ над $\mathbb{F}_{q^m}(x)$ дели минималния полином $g_y(z) \in \mathbb{F}_q(x)[z]$ на $y \in K$ над $\mathbb{F}_q(x)$, така че винаги $y \in K$ са сепарабелни над $\mathbb{F}_{q^m}(x)$. В резултат, $K \supseteq \mathbb{F}_{q^m}(x)$ е крайно сепарабелно разширение. Освен това, K е нормално над $\mathbb{F}_q(x)$ по построение, така че минималните полиноми $g_y(z)$ на $y \in K$ над $\mathbb{F}_q(x)$ се разлагат в линейни множители над K. Полиномите $g_{y,m}(z)$ са делители на $g_y(z)$ и също се разлагат в линейни множители над K. Това доказва, че $K \supseteq \mathbb{F}_{q^m}(x)$ е крайно сепарабелно и нормално разширение, т.е. крайно разширение на Galois.
Оттук нататък ще бележим $\mathbb{F}_{q^m}$ с $\mathbb{F}_q$ и ще считаме, че $\mathbb{F}_q$ е пълното поле от константи на K. Влаганията $\mathbb{F}_q \subset \mathbb{F}_q(x) \subseteq F \subseteq K$ индуцират доминантни рационални изображения на криви

$$\begin{tikzcd} & Y \arrow[dl, "\varphi"'] \arrow[d, "f"] \\ \mathbb{P}^1(\overline{\mathbb{F}_q}) & X \arrow[l, "h"'] \end{tikzcd},$$

където $K = \mathbb{F}_q(Y)$ и $\varphi : Y \to \mathbb{P}^1(\overline{\mathbb{F}_q})$ е покритие на Galois с група $G_n = Gal(K_{2n}/\mathbb{F}_{q^{2n}})$. Следователно $f : Y \to X$ е покритие на Galois с група $H_n = Gal(K_{2n}/F_{2n})$, защото спрегнатите на $y \in K$ над F са спрегнати над $\mathbb{F}_q(\mathbb{P}^1) = \mathbb{F}_q(x)$ и остават в K. Изображението $h : X \to \mathbb{P}^1(\overline{\mathbb{F}_q})$ е крайно сепарабелно покритие.
Оттук нататък избираме достатъчно голямо $n \in \mathbb{N}$, така че $\varphi : Y \to \mathbb{P}^1(\overline{\mathbb{F}_q})$, $f : Y \to X$ и $h : X \to \mathbb{P}^1(\overline{\mathbb{F}_q})$ да са определени над $\mathbb{F}_{q^{2n}}$. По-точно, покриваме $\mathbb{P}^1(\overline{\mathbb{F}_q})$, X и Y с краен брой афинни координатни карти. Редуцираме φ и h към полином, а f към наредена m-торка полиноми. Обединението на коефициентите на гореспоменатите полиноми за всички афинни карти е крайно множество M. Следователно съществува $n \in \mathbb{N}$, така че $\mathbb{F}_{q^{2n}} \supseteq M$. Тогава f и φ са определени над $\mathbb{F}_{q^{2n}}$. Да отбележим, че $\mathbb{F}_{q^{2n}}$-рационалните точки изпълняват включванията

$$X(\mathbb{F}_{q^{2n}}) \subseteq h^{-1}(\mathbb{P}^1(\mathbb{F}_{q^{2n}})) \quad \text{и} \quad Y(\mathbb{F}_{q^{2n}}) \subseteq \varphi^{-1}(\mathbb{P}^1(\mathbb{F}_{q^{2n}})),$$

защото стойностите на полиномите φ и h с коефициенти от $\mathbb{F}_{q^{2n}}$ в точки от $(\mathbb{F}_{q^{2n}})^m$ принадлежат на $\mathbb{F}_{q^{2n}}$. Да означим с

$$R_n = \varphi^{-1}(\mathbb{P}^1(\mathbb{F}_{q^{2n}}))$$

праобраза на $\mathbb{F}_{q^{2n}}$-рационалните точки на проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ под действие на φ. Множеството R_n е крайно, защото $|\mathbb{P}^1(\mathbb{F}_{q^{2n}})| = q^{2n} + 1 < \infty$ и слоевете на φ съдържат не повече от $\deg(\varphi) \in \mathbb{N}$ точки. Автоморфизмът на Frobenius $\Phi_{q^{2n}}$ действа върху слоевете $\varphi^{-1}(p)$ на g над $p \in \mathbb{P}^1(\mathbb{F}_{q^{2n}})$, защото $\Phi_{q^{2n}}$ фиксира $p \in \mathbb{P}^1(\mathbb{F}_{q^{2n}})$ и полиномите с каефициенти от $\mathbb{F}_{q^{2n}}$, задаващи φ. Оттук $\Phi_{q^{2n}}$ действа върху решенията на полиномиалните системи уравнения, образуващи слоя $\varphi^{-1}(p)$. Съгласно транзитивността на G_n-действието върху $\varphi^{-1}(p)$ с $p \in \mathbb{P}^1(\mathbb{F}_{q^{2n}})$, за всяка точка $y \in \varphi^{-1}(p)$ съществува $\sigma \in G_n$, така че $\Phi_{q^{2n}}(y) = \sigma(y)$. Ако слоят $\varphi^{-1}(p)$ е неразклонен, то множеството $\varphi^{-1}(p) = Orb_{G_n}(y) \simeq G_n$ е изоморфно на групата на Galois G_n и точката $\sigma(y)$ определя еднозначно $\sigma \in G_n$. Разглеждаме множествата

$$R_n(\sigma) = \{y \in R_n \ \mid \ \Phi_{q^{2n}}(y) = \sigma(y)\} \quad \text{за} \quad \forall \sigma \in G_n$$

и разбиваме в (необезателно непресичащо се) обединение

$$R_n = \cup_{\sigma \in G_n} R_n(\sigma).$$

Ако $R_n^o(\sigma)$ е множеството на онези точки от $R_n(\sigma)$, които лежат в неразклонените слоеве на g и

$$R_n^o = \{y \in R_n \ \mid \ e_y(g) = 1 \quad \text{за} \quad \forall z \in g^{-2}g(y)\},$$

то твърдим,че

$$R_n^o = \cup_{\sigma \in G_n} R_n^o(\sigma)$$

е непресичащо се обединение. Наистина, ако $\sigma_1(y) = \Phi_{q^{2n}}(y) = \sigma_2(y)$, то $\sigma_1^{-1}\sigma_2 \in Stab_{G_n}(y) = \{\mathrm{Id}\}$.
За по-нататъшните разглеждания не трябва следната

Лема 18.11. *Нека $\varphi : Y \longrightarrow \mathbb{P}^1$ е покритие на Galois, определено над $\mathbb{F}_q$,*

$$R_n = \varphi^{-1}\mathbb{P}^1(\mathbb{F}_{2n}),$$

$$R_n(\sigma) = \{y \in R_n \ \mid \ \Phi_{q^{2n}}(y) = \sigma(y)\}, \quad \sigma \in \mathrm{Gal}(\varphi) = \mathrm{Gal}(\mathbb{F}_q(Y)/\varphi^*\mathbb{F}_q(\mathbb{P}^1)).$$

Ако n е достатъчно голямо естествено число, така че $q^n > (g(Y)+1)^2$ за рода $g(Y)$ на Y и $R_n(\sigma)$ пресича поне един неразклонен слой на $\varphi : Y \longrightarrow \mathbb{P}^1$, то

$$|R_n(\sigma)| < q^{2n} + 1 + (2g(Y)+1)q^n.$$

Доказателство: Както в доказателството на

$$N_{2n}(K) < q^{2n} + 1 + (2g(Y)+1)q^n$$

за броя $N_{2n}(K)$ на $\mathbb{F}_{q^{2n}}$-рационалните точки на Y, можем да считаме, че множеството $R_n(\sigma) \neq \emptyset$ е непразно и да фиксираме $Q \in R_n(\sigma)$. Всеки базис на $\mathcal{L}((q^n-1)Q)$ е от вида $B = \{b_j \ \mid \ j \in J\}$ с $(b_j)_\infty = jQ$ за някакво подмножество $J \subseteq \{0, 1, \ldots, q^n - 1\}$. Ако слоят $\varphi^{-1}\varphi(Q)$ е неразклонен, $T = \sigma(Q)$ и $y \in \mathcal{L}((q^n+2g)T)$, то $\sigma(y) = y\sigma \in \mathcal{L}((q^n+2g)Q)$, защото $y\sigma(r) = \infty$ точно когато $\sigma(r) = T$ или $r = Q$. Всеки базис на $\mathcal{L}((q^n+2g)T)$ е от вида $C = \{c_i \ \mid \ i \in I\}$ с $(c_i)_\infty = iT$ за подмножество $I \subseteq \{0, 1, \ldots, q^n+2g\}$. Разглеждаме $\mathbb{F}_{q^{2n}}$-линейната обвивка H на xy^{q^n} за $\forall x \in \mathcal{L}((q^n-1)Q)$, $\forall y \in \mathcal{L}((q^n+2g)T)$. Проверяваме, че

$$\{b_j c_i^{q^n} \ \mid \ b_j \in B, \ \ c_i \in C\}$$

е $\mathbb{F}_{q^{2n}}$-базис на H и всеки елемент на H има единствено представяне във вида $y = \sum_{j \in J} b_j e_j^{q^n}$ чрез базиса b_j на $\mathcal{L}((q^n-1)Q)$ и подходящи $e_j \in \mathcal{L}((q^n+2g)T)$.
Размерността

$$\dim_{\mathbb{F}_{q^{2n}}} H = l((q^n-1)Q)l((q^n+2g)T) > q^{2n} + g(Y) + 1,$$

съгласно Теоремата на Riemann-Roch и предположението $q^n > (g(Y)+1)^2$. Нека $m = q^{2n} + 2g(Y)$, а ψ е изображението, трансформиращо $y = \sum_{j \in J} b_j e_j^{q^n}$ в

$$\psi\left(\sum_{j \in J} b_j e_j^{q^n}\right) = \sum_{j \in J} b_j^{q^n} \sigma(e_j).$$

Вземайки предвид $\sigma(e_j) \in \mathcal{L}((q^n+2g)Q)$, забелязваме, че

$$\psi(H) \subseteq \mathcal{L}([q^n(q^n-1) + q^n + 2g(Y)]Q) = \mathcal{L}(mQ).$$

Съгласно $\deg((\omega) - mQ) < 0$,

$$l(mQ) = m - g(Y) + 1 = q^{2n} + g(Y) + 1 < \dim H$$

по Теоремата на Riemann-Roch. Следователно съществува $0 \neq z \in \ker \psi$. Да отбележим, че за $\forall y \in H$ и $\forall P \in R_n(\sigma) \setminus Q$ е изпълнено

$$y(P)^{q^n} = \left(\sum_{j \in J} b_j(P) e_j^{q^n} \right)^{q^n} = \sum_{j \in J} b_j(P)^{q^n} e_j(P)^{q^{2n}} =$$

$$= \sum_{j \in J} b_j(P)^{q^n} \Phi_{q^{2n}}(e_j(P)) = \sum_{j \in J} b_j(P)^{q^n} \sigma(e_j)(P) = \psi(y)(P).$$

В частност,

$$z(P)^{q^n} = \psi(z)(P) = 0 \quad \text{за} \quad \forall P \in R_n(\sigma) \setminus Q,$$

така че $R_n(\sigma) \setminus Q \subseteq \mathrm{Supp}(z)_0$ и $\deg(z)_0 \geq |R_n(\sigma)| - 1$. От друга страна,

$$\deg(z)_0 = \deg(z)_\infty \leq q^n - 1 + q^n(q^n + 2g(Y))$$

за $z \in H \subseteq \mathcal{L}((q^n - 1)Q + q^n(q^n + 2g(Y))T)$, така че

$$|R_n(\sigma)| \leq q^{2n} + (2g(Y) + 1)q^n < q^n + 1 + (2g(Y) + 1)q^n,$$

Q.E.D.

Броят на точките на разклонение на $\varphi : Y \to \mathbb{P}^1(\overline{\mathbb{F}_q})$ е константа, която не зависи от n. Това ни дава възможност да представим

$$|R_n| = \sum_{\sigma \in G_n} |R_n(\sigma)| + O(1), \tag{18.7}$$

където $O(1)$ е поправката, възникваща от пресичанията на $R_n(\sigma_1)$ и $R_n(\sigma_2)$ за $\sigma_1 \neq \sigma_2$ от G_n по протежение на разклонените слоеве на φ. От друга страна, определението $R_n = \varphi^{-1}(\mathbb{P}^1(\mathbb{F}_{q^{2n}}))$ дава

$$|R_n| = \deg(\varphi)(q^{2n} + 1) + O(1) = |G_n|(q^{2n} + 1) + O(1). \tag{18.8}$$

Сравнявайки (17.7) с (17.8) получаваме

$$\sum_{\sigma \in G_n} |R_n(\sigma)| = |G_n|(q^{2n} + 1) + O(1). \tag{18.9}$$

Съгласно Лема 17.11,

$$|R_n(\sigma)| < q^{2n} + 1 + (2g(Y) + 1)q^n. \tag{18.10}$$

Сумирайки по $\forall \sigma \in G_n \setminus \{\sigma_o\}$, стигаме до извода, че

$$\sum_{\sigma \in G_n \setminus \{\sigma_o\}} < (|G_n| - 1)(q^{2n} + 1) + (|G_n| - 1)(2g(Y) + 1)q^n. \tag{18.11}$$

Изваждането на (17.11) от (17.9) дава

$$|R_n(\sigma_o)| > q^{2n} + 1 + (|G_n| - 1)(2g(Y) + 1)q^n + O(1)$$

за произволен елемент $\sigma_o \in G_n$. С други думи,

$$|R_n(\sigma_o)| > q^{2n} + O(q^n), \tag{18.12}$$

къето с $O(q^n)$ сме означили функция на q^n с $|O(q^n)| \leq \mathrm{Const} q^n$. Можем да запишем (17.10) във вида

$$|R_n(\sigma_o)| < q^{2n} + O(q^n). \tag{18.13}$$

От (17.12) и (17.13) получаваме

$$|R_n(\sigma_o)| = q^{2n} + O(q^n) \tag{18.14}$$

за всички $\sigma_o \in G_n$ и достатъчно големи $n \in \mathbb{N}$.

От друга страна, разглеждаме множествата

$$S_n = f^{-1}X(\mathbb{F}_{q^{2n}}),$$

съдържащи $Y(\mathbb{F}_{q^{2n}})$. Нека S_n^o е множеството на точките от S_n, които принадлежат на неразклонените слоеве на f. Твърдим, че

$$S_n^o = \cup_{\sigma \in H_n} R_n^o(\sigma).$$

Да отбележим, че $S_n \supseteq R_n(\sigma)$ за $\forall \sigma \in H_n$, защото за $\forall y \in R_n(\sigma)$ е в сила $\Phi_{q^{2n}}(y) = \sigma(y)$. Сега орбитите $Orb_{H_n}(y) = Orb_{H_n}(\sigma(y)) = Orb_{H_n}(\Phi_{q^{2n}}(y))$ съвпадат. Вземайки предвид, че f изобразява H_n-орбитите на Y върху точките на $X = Y/H_n$, стигаме до извода, че $f(y) \in X$ остава на място под действие на автоморфизма на Frobenius $\Phi_{q^{2n}}$ и $\Phi_{q^{2n}}(y) \in X(\mathbb{F}_{q^{2n}})$ е $\mathbb{F}_{q^{2n}}$-рационална точка. От друга страна твърдим, че $S_n^o \subseteq \cup_{\sigma \in H_n} R_n^o(\sigma)$. Наистина, от $y \in f^{-1}X(\mathbb{F}_{q^{2n}}) = S_n$ следва $Orb_{H_n}(y) \in X(\mathbb{F}_{q^{2n}})$. Следователно $\Phi_{q^{2n}} Orb_{H_n}(y) = Orb_{H_n}(y)$, откъдето $Orb_{H_n}\Phi_{q^{2n}}(y) = Orb_{H_n}(y)$ и съществува $\sigma \in H_n$ с $\Phi_{q^{2n}}(y) = \sigma(y)$. В резултат, от $S_n^o = \cup_{\sigma \in H_n} R_n^o(\sigma)$ следва

$$|S_n| = \sum_{\sigma \in H_n} |R_n(\sigma)| + O(1), \tag{18.15}$$

защото броят на точките в разклонените слоеве на f е константа, не зависеща от $n \in \mathbb{N}$. От друга страна, определението $S_n = f^{-1}X(\mathbb{F}_{q^{2n}})$ дава

$$|S_n| = \deg(f) N_{2n}(F) + O(1) = |H_n| N_{2n}(F) + O(1) \tag{18.16}$$

с поправка $O(1)$ за разклонените слоеве. Комбинирайки (17.15) с (17.16) получаваме

$$\sum_{\sigma \in H_n} |R_n(\sigma)| = |H_n| N_{2n}(F) + O(1). \tag{18.17}$$

Вземайки предвид (17.14) за $\forall \sigma \in H_n \leq G_n$ стигаме до извода, че

$$|H_n| q^{2n} + |H_n| O(q^n) = |H_n| N_{2n}(F) + O(1). \tag{18.18}$$

Оттук следва (17.4) за достатъчно големи $n \in \mathbb{N}$. Съгласно Лема 17.1, условието (17.4) е достатъчно за $|\omega_i| = \sqrt{q}$ за $\forall 1 \leq i \leq 2g$. С това доказахме следната

Теорема 22. (Теорема на Hasse=Weil) *Ако F е функционално поле на една променлива с поле от константи $\mathbb{F}_q$, а*

$$\zeta(F,t) = \frac{L(F,t)}{(1-qt)(1-t)} = \frac{\prod_{i=1}^{2g}(1-\omega_i t)}{(1-qt)(1-t)}$$

е ζ-функцията на Hasse-Weil на F, то

$$|\omega_i| = \sqrt{q} \quad \text{за} \quad \forall 1 \leq i \leq 2g.$$

Следствие 18.12. (Граница на Hasse-Weil) *Нека X е гладка проективна крива от род g, определена над $\mathbb{F}_q$, а $F = \mathbb{F}_q(X)$ е функционалното поле на X над $\mathbb{F}_q$. Тогава за всяко естествено число n, броят $N_n(F)$ на $\mathbb{F}_{q^n}$-рационалните точки на X изпълнява неравенството*

$$|N_n(F) - (q^n + 1)| \leq 2g\sqrt{q}.$$

Доказателство: Съгласно 17.2 имаме

$$N_n(F) - (q^n + 1) = -\sum_{i=1}^{2g} \omega_i.$$

По неравенството на триъгълника оттук следва, че

$$|N_n(F) - (q^n + 1)| \leq \sum_{i=1}^{2g} |\omega_i|.$$

Вземайки предвид, че $|\omega_i| = \sqrt{q}$ за $\forall 1 \leq i \leq 2g$ по Теорема 22 на Hasse-Weil, получаваме, че

$$|N_n(F) - (q^n + 1)| \leq 2g\sqrt{q},$$

Q.E.D.

Следващото твърдение установява, че така наречените ермитови криви достигат границата на Hasse-Weil за броя на рационалните точки.

Твърдение 18.13. *Ако $q = s^2 = p^{2m}$ за просто p, проективната равнинна крива*

$$X = \{[x : y : z] \in \mathbb{P}^2 \ \ | \ \ y^{s+1} = x^s z + x z^s\}$$

от род $g = \frac{s(s-1)}{2}$ достига горната граница

$$N(F) = q + 1 + 2g\sqrt{q} = s^3 + 1$$

на Hasse-Weil за броя на $\mathbb{F}_q$-рационалните точки.

Доказателство: За да пресметнем рода g на X да разгледаме сепарабелното покритие

$$f : X \longrightarrow \mathbb{P}^1,$$
$$f([x : y : z]) = [x : z]$$

от степен $\deg(f) = s + 1$. Дивизорът на разклонение на f е

$$R = (s+1)P_1 + \ldots + (s+1)P_s + (s+1)\infty$$

за $\infty = [1 : 0 : 0]$ и точките $P_i = [\zeta_i : 0 : 1]$, $1 \leq i \leq s$, където $\zeta_1, \ldots, \zeta_s$ са корените на полинома $x^s + x = 0$. Характеристиката $\mathrm{char}\mathbb{F}_q = p$ не дели локалните степени на разклонение $s + 1$, така че можем да приложим формулата на Riemann-Hurwitz и да пресметнем

$$2g(X) - 2 = (s+1)(2g(\mathbb{P}^1) - 2) + (s+1)s = (s+1)(-2) + (s+1)s = s^2 - s - 2.$$

Оттук

$$g = g(X) = \frac{s(s-1)}{2}.$$

Сега $q + 1 + 2g\sqrt{q} = s^3 + 1$ и трябва да проверим, че броят на $\mathbb{F}_q$-рационалните точки на X е $s^3 + 1$. Сечението $X \cap \{z = 0\} = \infty = [1 : 0 : 0]$ се състои от единствена точка, която е $\mathbb{F}_q$-рационална. Остава да докажем, че афинната равнинна крива

$$X \cap \{z = 1\} = \{(x, y) \in \mathbb{F}_q^2 \ \ | \ \ y^{s+1} = x^s + x\}$$

има s^3 на брой $\mathbb{F}_q$-рационални точки. За целта да отбележим, че групата на Galois

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_s) = \langle \Psi_s \rangle \simeq \mathbb{Z}_2$$

е циклична от ред 2 и следата

$$Tr_{\mathbb{F}_s}^{\mathbb{F}_q} : \mathbb{F}_q \longrightarrow \mathbb{F}_s,$$
$$Tr_{\mathbb{F}_s}^{\mathbb{F}_q}(x) = x^s + x.$$

Проверявали сме, че $Tr_{\mathbb{F}_s}^{\mathbb{F}_q}$ е $\mathbb{F}_s$-линейно изображение с ранг 1 и дефект 1. Накратко,

$$\ker(Tr_{\mathbb{F}_s}^{\mathbb{F}_q}) = \{x \in \mathbb{F}_q \ \ | \ \ x^s + x = 0\}$$

има $\leq s$ елемента, защото се съдържа в корените на полинома $x^s + x = 0$. Оттук $\mathrm{im}(Tr_{\mathbb{F}_s}^{\mathbb{F}_q}) \simeq \mathbb{F}_q / \ker(Tr_{\mathbb{F}_s}^{\mathbb{F}_q})$ има $\geq s$ елемента и понеже $\mathrm{im}(Tr_{\mathbb{F}_s}^{\mathbb{F}_q}) \subseteq \mathbb{F}_s$, в сила е $|\mathrm{im}(Tr_{\mathbb{F}_s}^{\mathbb{F}_q})| = s$, $\ker(Tr_{\mathbb{F}_s}^{\mathbb{F}_q})| = s$.
Уравнението $Tr_{\mathbb{F}_s}^{\mathbb{F}_q}(x) = x^s + x = \alpha \in \mathbb{F}_s$ има s различни корена в $\overline{\mathbb{F}_q}$. (Полиномът и производната му нямат общи корени.) Всички те са в $\mathbb{F}_q$, защото остават на място под действие на $\Phi_s^2 = \Phi_q$, $\Phi_s(r) = r^s$.
Уравнението $y^{s+1} = 0$ има единствен корен $y = 0$ и той е от $\mathbb{F}_q$.
За $\forall \alpha \in \mathbb{F}_s^*$ уравнението $y^{s+1} = \alpha$ има $s+1$ различни корена в $\overline{\mathbb{F}_q}$ и всички те са в $\mathbb{F}_q$, защото се стабилизират от $\Phi_q = \Phi_s^2$.
Следователно броят на $\mathbb{F}_q$-рационалните точки на $X \cap \{z = 1\}$ е

$$s + (s-1)s(s+1) = s^3,$$

Q.E.D.