Глава 13

Съответствие между затворени точки и класове дискретни нормирания с една и съща степен

Преди да установим взаимно еднозначно съответствие между $\mathbb{F}_q$-затворените точки от степен m върху гладка проективна крива C и класовете дискретни нормирания на $\overline{\mathbb{F}_q}(C)$ от степен m, ще разгледаме някои общи свойства на попълненията и продълженията на нормирания на полета.
Нормиране v на поле F е изображение $v : F \to \mathbb{R} \cup \{\infty\}$ със свойствата:
(i) $v(x) = \infty$ тогава и само тогава, когато $x = 0_F$;
(ii) $v(xy) = v(x) + v(y)$ за $\forall x, y \in F$;
(iii) $v(x + y) \geq \min(v(x), v(y))$ за $\forall x, y \in F$.
Ако $v : F \to \mathbb{R} \cup \{\infty\}$ е нормиране на поле F, а $r \in (0, 1)$ е реално число между 0 и 1, то

$$| \ |_v : F \longrightarrow \mathbb{R}^{\geq 0},$$

$$|x|_v = r^{v(x)} \quad \text{за} \quad \forall x \in F$$

е норма, за която:
(i) $|x|_v \geq 0$ с $|x|_v = 0$ тогава и само тогава, когато $x = 0_F$;
(ii) $|xy|_v = |x|_v|y|_v$ за $\forall x, y \in F$;
(iii) $|x + y|_v \leq \max(|x|_v, |y|_v)$ за $\forall x, y \in F$.
Нормата $| \ |_v$ определя разстояние

$$\rho_v : F \times F \longrightarrow \mathbb{R}^{\geq 0},$$

$$\rho_v(x, y) = |x - y|_v = r^{\nu(x-y)} \quad \rho \quad \forall x, y \in F,$$

което изпълнява условията:
(i) $\rho_v(x, y) \geq 0$ с $\rho_v(x, y) = 0$ тогава и само тогава, когато $x = y$;
(ii) $\rho_v(x, y) = \rho_v(y, x)$ за $\forall x, y \in F$;
(iii) $\rho_v(x, z) \leq \max(\rho_v(x, y), \rho_v(y, z))$ за $\forall x, y, z \in F$.
Да напомним, че редицата $\{x_n\}_{n=1}^{\infty} \subset F$ е фундаментална относно ρ_v, ако за $\forall \varepsilon > 0$ съществува $n_0 \in \mathbb{N}$, така че $\rho_v(x_m, x_n) < \varepsilon$ за $\forall m, n \in \mathbb{N}$, $m \geq n_0$, $n \geq n_0$.

Определение 13.1. *Полето F е пълно относно метриката ρ_v или нормирането v, ако всяка фундаментална редица относно ρ_v е сходяща относно ρ_v.*

Определение 13.2. *Подмножеството M на метричното пространство (F, ρ_v) е навсякъде гъсто, ако всеки елемент на F е граница на редица $\{x_n\}_{n=1}^{\infty} \subseteq M$ с елементи от M.*

Лема-Определение 13.3. *Нека F е поле с нормиране $v : F \to \mathbb{R} \cup \{\infty\}$. Тогава съществува единствено с точност до изоморфизъм поле F_v с нормиране $v : F_v \to \mathbb{R} \cup \{\infty\}$, което е пълно относно v и съдържа F като навсякъде гъсто подполе.*
Полето F_v се нарича попълнение на F относно v.

Доказателство: Множеството R_v на фундаменталните относно v редици $\{x_n\}_{n=1}^{\infty} \subset F$ е пръстен относно поелементно определените събиране

$$\{x_n\}_{n=1}^{\infty} + \{y_n\}_{n=1}^{\infty} = \{x_n + y_n\}_{n=1}^{\infty}$$

и умножение

$$\{x_n\}_{n=1}^{\infty}\{y_n\}_{n=1}^{\infty} = \{x_n y_n\}_{n=1}^{\infty}.$$

Ако фундаментална относно v редица $\{x_n\}_{n=1}^{\infty} \subset F$ не клони към 0_F, то $x_n \neq 0_F$ за всички $n \in \mathbb{N}$ с изключение на краен брой и $\{x_n^{-1}\}_{n=1}^{\infty} \in R_v$ е фундаментална редица с елементи от F. Следователно необратимите елементи $\{x_n\}_{n=1}^{\infty} \in R_v \setminus R_v^*$ се съдържат в идеала $\mathfrak{M}_v$ на сходящите към 0_F редици $\{x_n\}_{n=1}^{\infty} \subset F$. Вземайки предвид $\mathfrak{M}_v \subseteq R_v \setminus R_v^*$, стигаме до извода, че $\mathfrak{M}_v = R_v \setminus R_v^*$ е единственият максимален идеал на R_v и пръстенът R_v е локален. Определяме

$$F_v = R_v / \mathfrak{M}_v$$

като полето от остатъци на R_v.

Твърдим, че ако $\{x_n\}_{n=1}^{\infty} \subset F$ е фундаментална редица относно ρ_v, то редицата $\{|x_n|_v\}_{n=1}^{\infty} \subset \mathbb{R}$ от съответните норми е сходяща. Преди всичко, редицата от реални числа $\{|x_n|_v\}_{n=1}^{\infty}$ е ограничена, защото в противен случай за $\forall N \in \mathbb{N}$ съществува $n_N \in \mathbb{N}$ с $|x_n|_v \geq N$ за $\forall n \geq n_N$. След перминаване към подредица можем да считаме, че $|x_m|_v \neq |x_n|_v$ за всички различни $m, n \in \mathbb{N}$ от известно място нататък. Съгласно фундаменталността на $\{x_n\}_{n=1}^{\infty} \subset F$, за произволно фиксирано $N \in \mathbb{N}$ съществува $n_0 \in \mathbb{N}$ с $|x_m - x_n|_v < N$ за $\forall m \geq n_0$, $\forall n \geq n_0$. За всички $n \geq n_N$ имаме $|x_m - x_n|_v \neq |x_n|_v$ и неравенството на триъгълника с равенство

$$|x_m|_v = \max(|x_m - x_n|_v, |x_n|_v) = |x_n|_v$$

е изпълнено за $\forall n \geq \max(n_N, n_0)$, $\forall m \geq n_0$. Противоречието доказва ограничеността на $\{|x_n|_v\}_{n=1}^{\infty} \subset \mathbb{R}$.

Да допуснем, че $\{|x_n|_v\}_{n=1}^{\infty}$ има две различни точки на сгъстяване $0 \leq a < b$ и да изберем безкрайни подредици $\{x_{k_n}\}_{n=1}^{\infty}$, съответно, $\{x_{l_m}\}_{n=1}^{\infty}$ с $\lim\limits_{n \to \infty} |x_{k_n}|_v = a$, $\lim\limits_{m \to \infty} |x_{l_m}|_v = b$. За произволно реално $0 < \varepsilon < \frac{a+b}{2}$ съществува $n_0 \in \mathbb{N}$, така че $|x_m - x_n|_v < \varepsilon$ за $\forall m \geq n_0$, $\forall n \geq n_0$. Съществуват $n_1 \in \mathbb{N}$ и $m_1 \in \mathbb{N}$, така че $k_n \geq n_0$ за $\forall n \geq n_1$ и $l_m \geq n_0$ за $\forall m \geq m_1$. Без ограничение на общността можем да считаме, че

$$||x_{l_m}|_v - a| < \frac{b-a}{2} \quad \text{за} \quad \forall m \geq m_1 \quad \text{и} \quad ||x_{k_n}|_v - b| < \frac{b-a}{2} \quad \text{за} \quad \forall n \geq n_1.$$

Тогава

$$|x_{k_n}|_v > b - \frac{b-a}{2} = \frac{a+b}{2} > \varepsilon > |x_m - x_n|_v \quad \text{за} \quad \forall m \geq m_1, \quad \forall n \geq n_1 \quad \text{и}$$

$$|x_{l_m}|_v = \max(|x_m - x_n|_v, |x_{k_n}|_v) = |x_{k_n}|_v.$$

Сега

$$\frac{a+b}{2} = a + \frac{b-a}{2} > |x_{l_m}|_v = |x_{k_n}|_v > b - \frac{b-a}{2} = \frac{a+b}{2}$$

е противоречие, доказващо сходимостта на $\{|x_n|_v\}_{n=1}^{\infty} \subset \mathbb{R}$ за произволна ρ_v-фундаментална редица $\{x_n\}_{n=1}^{\infty} \subset F$.

Проверяваме, че за произволна редица $\{y_n\}_{n=1}^{\infty} \subset F$, която клони към 0_F относно ρ_v е в сила $\lim\limits_{n \to \infty} |x_n|_v = \lim\limits_{n \to \infty} |x_n + y_n|_v$. Грубо казано, ако $\lim\limits_{n \to \infty} |x_n|_v = 0$, то $\{x_n\}_{n=1}^{\infty} \in \mathfrak{M}_v$ и $\{x_n + y_n\}_{n=1}^{\infty} \in \mathfrak{M}_v$, т.е. $\lim\limits_{n \to \infty} |x_n + y_n|_v = 0$. Ако границата $\lim\limits_{n \to \infty} |x_n|_v = a > 0$, то за достатъчно големи $n \in \mathbb{N}$ имаме $|x_n|_v > |y_n|_v$, откъдето

$$|x_n + y_n|_v = \max(|x_n|_v, |y_n|_v) = |x_n|_v$$

и $\lim\limits_{n\to\infty} |x_n + y_n|_v = \lim\limits_{n\to\infty} |x_n|_v$. Това ни дава възможност да въведем норма

$$| \ |_v : F_v \longrightarrow \mathbb{R}^{\geq 0},$$

$$\Big|\{x_n\}_{n=1}^{\infty} + \mathfrak{M}_v\Big|_v = \lim_{n\to\infty} |x_n|_v = \lim_{n\to\infty} r^{v(x_n)} \quad \text{за} \quad \forall \{x_n\}_{n=1}^{\infty} \in R_v$$

или, еквивалентно, нормиране

$$v : F_v \longrightarrow \mathbb{R} \cup \{\infty\},$$

$$v\left(\{x_n\}_{n=1}^{\infty} + \mathfrak{M}_v\right) = \log_r \left(\lim_{n\to\infty} |x_n|_v\right) = \log_r \left(\lim_{n\to\infty} r^{v(x_n)}\right) \quad \text{за} \quad \forall \{x_n\}_{n=1}^{\infty} \in R_v.$$

Аксиомите за нормиране се проверяват непосредствено.

За пълнотата на F_v относно v да разгледаме фундаментална редица $\{\xi_n\}_{n=1}^{\infty} \in F_v$ с $\xi_n = \{x_{n,i}\}_{i=1}^{\infty} + \mathfrak{M}_v$, $x_{n,i} \in F$. За всяко $\varepsilon > 0$ съществува $n_0 \in \mathbb{N}$ с $|\xi_n - \xi_m|_v = \lim\limits_{i\to\infty} |x_{n,i} - x_{m,i}|_v < \varepsilon$ за $\forall n \geq n_0$, $\forall m \geq n_0$. Оттук за $\forall 0 < \varepsilon_1 < \varepsilon$ съществува $i_o \in \mathbb{N}$, така че

$$\varepsilon - \varepsilon_1 < |x_{n,i} - x_{m,i}|_v < \varepsilon + \varepsilon_1 \quad \text{за} \quad \forall i \geq i_o, \quad \forall n \geq n_o, \forall m \geq n_o.$$

В частност, за $\forall i \geq \max(n_0, i_o)$ е в сила

$$\varepsilon - \varepsilon_1 < |x_{n,i} - x_{i,i}|_v < \varepsilon + \varepsilon_1$$

или $|\xi_n - \xi|_v = \lim\limits_{i\to\infty} |x_{n,i} - x_{i,i}| < \varepsilon$ за $\forall n \geq n_0$. Това означава, че $\lim\limits_{n\to\infty} |\xi_n - \xi|_v = 0$ и редицата $\{\xi_n\}_{n=1}^{\infty} \subset F_v$ клони към $\xi = \{x_{i,i}\}_{i=1}^{\infty} + \mathfrak{M}_v \in F_v$. Това проверява пълнотата на F_v относно v.

Полето F се влага в полето F_v чрез постоянните редици $x = \{x_n = x\}_{n=1}^{\infty} + \mathfrak{M}_v \in F_v$. Всяка фундаментална редица $\{x_n\}_{n=1}^{\infty} \in R_v$ с елементи $x_n \in F$ може да се разглежда като границата $\lim\limits_{n\to\infty} x_n$ на постоянните редици $\{x_{n,i} = x_n\}_{i=1}^{\infty} + \mathfrak{M}_v \in F$, така че полето F е навсякъде гъсто в полето F_v.

Полето F_v е единствено с точност до изоморфизъм, защото се състои от границите на фундаменталните редици с елементи от F, Q.E.D.

ЛЕМА 13.4. *Нека F е поле с нормиране $v : F \to \mathbb{R} \cup \{\infty\}$, а $E \supset F$ е алгебрично разширение на F. Тогава съществува нормиране $w : E \to \mathbb{R} \cup \{\infty\}$ на E, продължаващо $w|_F = v$.*
Казваме, че w е нормиране на E над v.

Идея за доказателство: Нека $R = \{x \in F \mid v(x) \geq 0\}$ е локалният пръстен на нормирането v с максимален идеал $\mathcal{M} = \{x \in F \mid v(x) > 0\}$. Разглеждаме цялата обвивка S на R в E. Локализацията $S_{\mathcal{M}}$ на S относно мултипликативно затвореното подмножество $R \setminus \mathcal{M}$ е локален пръстен с макисмален идеал $\mathfrak{M}$, който пресича R в $\mathfrak{M} \cap R = \mathcal{M}$. Твърдим, че нормирането $w : E \to \mathbb{R} \cup \{\infty\}$ с пръстен $S_{\mathcal{M}} = \{x \in E \mid w(x) \geq 0\}$ продължава $v : F \to \mathbb{R} \cup \{\infty\}$. За целта, разглеждаме ограниченията на v и w върху мултипликативните групи F^* и E^* като епиморфизми $v : F^* \to v(F^*) = F^*/R^*$, съответно $w : E^* \to w(E^*) = E^*/S^*_{\mathcal{M}}$. Достатъчно е да докажем съществуването на естествено влагане на групи $i : F^*/R^* \hookrightarrow E^*/S^*_{\mathcal{M}}$, за да получим комутативната диаграма

$$\begin{tikzcd}
F^* \arrow[d, "v"] \arrow[dr, "w"] & \\
F^*/R^* \arrow[r, "i"] & F^* S^*_{\mathcal{M}}/S^*_{\mathcal{M}}
\end{tikzcd} .$$

За целта разглеждаме композицията $\widetilde{i} : F^* \to E^*/S^*_{\mathcal{M}}$ на влагането $F^* \hookrightarrow E^*$ и естествения епиморфизъм $E^* \to E^*/S^*_{\mathcal{M}}$. Вземайки предвид, че полето от частни на R е F, $S^*_{\mathcal{M}} = S_{\mathcal{M}} \setminus \mathcal{M}_{\mathcal{M}}$ и $(S \setminus \mathcal{M}) \cap F = R \setminus \mathcal{M} = R^*$, представяме ядрото

$$\ker(\widetilde{i}) = \left\{ \ \frac{a}{b} = \frac{x}{y} \ \middle| \ a, b \in R, \ \ x \in S \setminus \mathcal{M}, \ \ y \in R \setminus \mathcal{M} = R^* \ \right\}$$

като подмножество на $\left\{ \ \frac{x}{y} \ \middle| \ x \in (S \setminus \mathcal{M}) \cap F = R^*, \ \ y \in R^* \ \right\} = R^*$. Комбинирайки с $R^* \subseteq \ker(\widetilde{i})$ получаваме $\ker(\widetilde{i}) = R^*$. Следователно $\widetilde{i}$ индуцира естествено влагане

$$i : F^*/R^* \longrightarrow E^*/S^*_{\mathcal{M}}$$

и съществува продължение $w : E \to \mathbb{R} \cup \{\infty\}$ на $v : F \to \mathbb{R} \cup \{\infty\}$, Q.E.D.

Лема 13.5. *Нека полето F е пълно поле относно нормиране $v : F \to \mathbb{R} \cup \{\infty\}$, $E \supset F$ е крайно разширение на F с базис $e_1, \ldots, e_n$ над F, а $w : E \to \mathbb{R} \cup \{\infty\}$ е нормиране на E над v. В такъв случай, $\left\{ \ \sum\limits_{i=1}^{n} a_{i,m} e_i \ \right\}_{m=1}^{\infty} \subset E$ с $a_{i,m} \in F$ е фундаментална редица с елементи от E тогава и само тогава, когато за всяко $1 \leq i \leq n$ редицата $\{a_{i,m}\}_{m=1}^{\infty} \in F$ е сходяща.*

Доказателство: Нека $\xi = \left\{ \xi_m = \sum\limits_{i=1}^{n} a_{i,m} e_i \right\}_{m=1}^{\infty} \subset E$ е фундаментална редица. С индукция по $n = [E : F]$ ще докажем, че редиците $\{a_{i,m}\}_{m=1}^{\infty} \subset F$ са сходящи. За $n = 1$ няма какво да се доказва. Да допуснем, че твърдението е вярно за всички разширения $E_o \supset F$ от степен $[E_o : F] = n - 1$, но съществуват разширение $E \supset F$ от степен $[E : F] = n$ и фундаментална редица $\xi = \left\{ \xi_m = \sum\limits_{i=1}^{n} a_{i,m} e_i \right\}_{m=1}^{\infty} \subset E$ с поне една разходяща редица от координати $\{a_{i,n}\}_{n=1}^{\infty} \subset F$. След евентуална пермутация на базиса на E над F можем да считаме, че редицата $\{a_{1,m} - a_{1,k}\}_{m,k=1}^{\infty} \subset F$ не клони към 0_F. Тогава лявата страна на

$$\frac{\xi_m - \xi_k}{a_{1,m} - a_{1,k}} - e_1 = \sum_{i=2}^{n} (a_{i,m} - a_{i,k}) e_i \in E \tag{13.1}$$

клони към $-e_1$, така че редицата $\{\eta_{m,k} = \sum\limits_{i=2}^{n} (a_{i,m} - a_{i,k}) e_i\}_{m,k=1}^{\infty} \subset l_F(e_2, \ldots, e_n)$ е сходяща и клони към $-e_1$. В частност, $\{\eta_{m,k}\}_{m,k=1}^{\infty} \subset l_F(e_2, \ldots, e_n)$ е фундаментална редица в $(n-1)$-мерното разширение $l_F(e_2, \ldots, e_n)$ на F, така че редиците $\{a_{i,m}\}_{m=1}^{\infty} \subset F$ са сходящи за $\forall 2 \leq i \leq n$. Ако $\lim\limits_{m \to \infty} |a_{i,m}|_v = a_i \in F$, то границата на (13.1) е $-e_1 = \sum\limits_{i=2}^{n} a_i e_i$. Това противоречи на линейната независимост на базиса $e_1, e_2, \ldots, e_n$ на E над F и доказва сходимостта на редиците $\{a_{i,m}\}_{m=1}^{\infty} \subset F$ за $\forall 1 \leq i \leq n$.

В частност, ако $\{\xi_m = \sum\limits_{i=1}^{n} a_{i,m} e_i\}_{m=1}^{\infty} \subset E$ е фундаментална редица относно w, то $\lim\limits_{m \to \infty} a_{i,m} = a_i$ и съществува $\lim\limits_{m \to \infty} \left(\sum\limits_{i=1}^{n} a_{i,m} e_i \right) = \sum\limits_{i=1}^{n} a_i e_i \in E$. Това доказва пълнотата на E относно w, Q.E.D.

Следствие 13.6. *Нека полето F е пълно относно нормирането о $v : F \to \mathbb{R} \cup \{\infty\}$, $E \supset F$ е алгебрично разширение на F, а $w_i : E \to \mathbb{R} \cup \{\infty\}$ са нормирания на E над v за $1 \leq i \leq 2$. Тогава w_1 и w_2 са еквивалентни.*

Доказателство: Съгласно Лема 13.5, всеки две продължения

$$w_i : E_o \longrightarrow \mathbb{R} \cup \{\infty\}, \quad 1 \leq i \leq 2$$

на $v : F \to \mathbb{R} \cup \{\infty\}$ до нормирания на крайно разширение $E_o \supset K$ са еквивалентни. По определение, съществува реално положително число $c \in \mathbb{R}$ с $w_2 = cw_1$. Ако $\mathcal{O}_v \subset F$ е пръстенът на нормирането v и $x \in F \setminus \mathcal{O}_v^*$, то $v(x) \neq 0$ и $v(x) = w_2(x) = cw_1(x) = cv(x)$ изисква $c = 1$. Следователно

$$w_1|_{E_o} \equiv w_2|_{E_o}.$$

Да означим със Σ множеството на разширенията $L \supset F$, върху които w_1 съвпада с w_2. Произволно линейно наредено подмножество $\{L_\alpha\}_{\alpha \in A} \subseteq \Sigma$ има точна горна граница $L_\infty = \cup_{\alpha \in A} L_\alpha \in \Sigma$. Съгласно Лемата на Zorn съществува максимален елемент $E' \in \Sigma$. Ако допуснем, че $E' \subsetneq E$, то всеки елемент $y \in E \setminus E'$ е алгебричен над F, така че разширението $F(y) \supset F$ е крайно и $w_1 \equiv w_2 : F(y) \to \mathbb{R} \cup \{\infty\}$. В резултат, w_1 съвпада с w_2 върху $E'(y) \supsetneq E'$, което противоречи на максималността на $E' \in \Sigma$. Следователно $E' = E$ и w_1 съвпада с w_2 върху E, Q.E.D.

Нека E_1 и E_2 са полета с общо подполе F. Ако хомоморфизмът на пръстенни $\varphi : E_1 \to E_2$ се ограничава до тъждественото изображение на F, $\varphi|_F = \mathrm{Id}_F$, то казваме, че φ е хомоморфизъм над F.

Лема 13.7. *Нека $v : \overline{F_v} \to \mathbb{R} \cup \{\infty\}$ е продължението на нормиране v на поле F до алгебричната обвивка $\overline{F_v}$ на попълнението F_v на F относно v, а $E \supset F$ е алгебрично разширение. Тогава:*

(i) всяко влагане $\sigma : E \hookrightarrow \overline{F_v}$ над F задава нормиране $w = v\sigma : E \to \mathbb{R} \cup \{\infty\}$;

(ii) всяко нормиране $w : E \to \mathbb{R} \cup \{\infty\}$ на E над v се индуцира от влагане $\sigma : E \hookrightarrow \overline{F_v}$ над F.

Доказателство: (i) Композицията $w = v\sigma$ на влагане $\sigma : E \hookrightarrow \overline{F_v}$ и нормиране $v : \overline{F_v} \to \mathbb{R} \cup \{\infty\}$ е нормиране.

(ii) Нека $w : E \to \mathbb{R} \cup \{\infty\}$ е нормиране с $w|_F = v$. Разглеждаме произволно влагане $\sigma_o : E \hookrightarrow \overline{F}$ над F в алгебричната обвивка $\overline{F}$ на F. Диагоналното влагане $\Delta : F \hookrightarrow F_v$ на F в попълнението F_v на F относно v се продължава до влагане $\Delta : \overline{F} \to \overline{F_v}$ на съответните алгебрични обвивки. Композицията

$$\sigma = \Delta\sigma_o : E \hookrightarrow \overline{F_v}$$

е влагане на E над F. С помощта на изоморфизма на полета $\sigma : E \to \sigma(E)$ получаваме комутативна диаграма

$$\begin{tikzcd}
E \arrow[r, "\sigma"] \arrow[d, "w"'] & \sigma(E) \arrow[dl, "w\sigma^{-1}"] \\
\mathbb{R} \cup \{\infty\} &
\end{tikzcd}$$

с нормирания w и $w\sigma^{-1}$ над v. Композитът $\sigma(E) * F_v \subseteq \overline{F_v}$ е алгебрично разширение на пълното поле F_v, така че нормирането v на $\sigma(E)$ съвпада с нормирането $w\sigma^{-1}$. Композирайки със σ получаваме $v\sigma|_E = w|_E$, Q.E.D.

Лема 13.8. *Нека F е поле с нормиране $v : F \to \mathbb{R} \cup \{\infty\}$, $E \supset F$ е крайно разширение на F с влагане $\sigma : E \hookrightarrow \overline{F_v}$ над F в алгебричната обвивка $\overline{F_v}$ на попълнението F_v на F относно v, а $w : E \to \mathbb{R} \cup \{\infty\}$ е нормирането над v, което се индуцира от σ. Тогава попълнението $E_w \simeq \sigma(E)_{w\sigma^{-1}}$ на E относно w е изоморфно на композита $\sigma(E) * F_v$ на $\sigma(E)$ и F_v в $\overline{F_v}$.*

Доказателство: Попълнението $\sigma(E)_{w\sigma^{-1}}$ на $\sigma(E)$ относно $w\sigma^{-1}$ съдържа композита $\sigma(E) * F_v$, защото от $F \subset \sigma(E)$ следва $F_v \subset \sigma(E)_{w\sigma^{-1}}$ за нормирането $w\sigma^{-1}$ над v. За съвпадението $\sigma(E)_{w\sigma^{-1}} = \sigma(E) * F_v$ е достатъчно да забележим, че $\sigma(E) * F_v \supset F_v$ е крайно разширение на пълното поле F_v. Съгласно Лема 13.5, $\sigma(E) * F_v$ е пълно относно нормирането $w\sigma^{-1}$ над v. Пълното подполе $\sigma(E) * F_v$ на $\sigma(E)_{w\sigma^{-1}}$ съвпада с попълнението $\sigma(E)_{w\sigma^{-1}}$, $\sigma(E) * F_v = \sigma(E)_{w\sigma^{-1}}$, Q.E.D.

Лема 13.9. *Нека F е поле с нормиране $v : F \to \mathbb{R} \cup \{\infty\}$, а $E \supset F$ е алгебрично разширение с влагания $\sigma : E \hookrightarrow \overline{F_v}$ и $\tau : E \hookrightarrow \overline{F_v}$ над F. Влаганията σ и τ индуцират еквивалентни нормирания на E тогава и само тогава, когато са спрегнати над F_v, т.е. когато съществува $\lambda \in \mathrm{Gal}(\overline{F_v}/F_v)$ с $\tau = \lambda\sigma$,*

$$\begin{tikzcd}
E \arrow[r, "\sigma"] \arrow[dr, "\tau"'] & \overline{F_v} \arrow[d, "\lambda\ ."] \\
& \overline{F_v}
\end{tikzcd}$$

Доказателство: Ако $\tau = \lambda\sigma$ с $\lambda \in Gal(\overline{F_v}/F_v)$, то твърдим, че нормиранията $v\sigma$, $v\tau = v\lambda\sigma$ на E са еквивалентни. Достатъчно е да проверим, че нормиранията $v : \sigma(E) \to \mathbb{R} \cup \{\infty\}$ и $v\lambda : \sigma(E) \to \mathbb{R} \cup \{\infty\}$ са еквивалентни. Разглеждаме изоморфизма на полета

$$\lambda : \sigma(E) * F_v \longrightarrow \tau(E) * F_v$$

над F_v. Разширението $\sigma(E) * F_v \supset F_v$ е алгебрично над пълното поле F_v, така че всички нормирания на $\sigma(E) * F_v$ са еквивалентни помежду си. В частност, $v|_{\sigma(E) * F_v}$ и $v\lambda|_{\sigma(E) * F_v}$ са еквивалентни, откъдето ограниченията им $v|_{\sigma(E)}$ и $v\lambda|_{\sigma(E)}$ са еквивалентни.

Обратно, нека σ и τ задават еквивалентни нормирания $v\sigma$ и $v\tau$. Подполетата $\sigma(E)$ и $\tau(E)$ на $\overline{F_v}$ са изоморфни над F, така че съществува изоморфизъм $\lambda : \sigma(E) \to \tau(E)$ над F, затварящ комутативната диаграма

$$\begin{tikzcd}
E \arrow[r, "\sigma"] \arrow[dr, "\tau"'] & \sigma(E) \arrow[d, "\lambda\quad ."] \\
& \tau(E)
\end{tikzcd}$$

Достатъчно е да продължим λ до изоморфизъм $\lambda : \sigma(E) * F_v \to \tau(E) * F_v$ над F_v. Тогава произволно продължение на λ до изоморэфизъм $\lambda : \overline{F_v} \to \overline{F_v}$ над F_v ще изпълнява условието $\tau = \lambda\sigma$.

Полето $\sigma(E)$ е навсякъде гъсто в попълнението $\sigma(E) * F_v = \sigma(E)_{w\sigma^{-1}}$. Следователно елементите на $\sigma(E) * F_v$ са от вида $x = \lim\limits_{n\to\infty} \sigma(y_n)$ с $y_n \in E$. Съгласно еквивалентността на нормиранията $v\sigma$ и $v\tau$ на E, редицата $\{\tau(y_n)\}_{n=1}^{\infty}$ е сходяща. Полагаме $\lambda(x) = \lim\limits_{n\to\infty} \tau(y_n)$. Ако $\{z_n\}_{n=1}^{\infty} \subset E$ е друга редица с $\lim\limits_{n\to\infty} \sigma(z_n) = x$, то $\lim\limits_{n\to\infty} \sigma(y_n - z_n) = 0$. Следователно $\lim\limits_{n\to\infty} \tau(y_n - z_n) = 0$ и $\lim\limits_{n\to\infty} \tau(y_n) = \lim\limits_{n\to\infty} \tau(z_n)$. С това проверихме, че изображението

$$\lambda : \sigma(E) * F_v \longrightarrow \tau(E) * F_v,$$

$$\lambda\left(\lim_{n\to\infty} \sigma(y_n)\right) = \lim_{n\to\infty} \tau(y_n)$$

е коректно зададено. Непосредствено се проверява, че λ е хомоморфизъм на пръстени. Разменяйки σ с τ получаваме коректно определено изображение λ^{-1}. Следователно λ е изоморфизъм над F_v и се продължава до $\lambda \in Gal(\overline{F_v}/F_v)$ с $\tau = \lambda\sigma$, Q.E.D.

Твърдение 13.10. *Нека F е поле с нормиране $v : F \to \mathbb{R} \cup \{\infty\}$, а $E \supset F$ е крайно сепарабелно разширение. Тогава степента*

$$[E : F] = \sum_{w/v} [E_w : F_v],$$

където w пробягва класовете нормирания на E над v, F_v е попълнението на F относно v, а E_w са попълненията на E относно w.

Доказателство: Нека θ е примитивен елемент на крайното сепарабелно разширение $E \supset F$, т.е. $E = F(\theta)$. Означаваме с $f(x) \in F[x] \setminus F$ минималния полином на θ над F и разлагаме

$$f(x) = f_1(x) \dots f_m(x)$$

в неразложими над F_v множители $f_i(x) \in F_v[x] \setminus F_v$. Класовете нормирания w на алгебричното разширение $E \supset F$ са във взаимно еднозначно съответствие с влаганията $\sigma : E = F(\theta) \hookrightarrow \overline{F_v}$ над F_v. Всяко такова влагане се индуцира от съответствие $\theta \mapsto \theta_{ij}$ за корените θ_{ij} на $f_i(x)$ в $\overline{F_v}$. Влаганията на $E = F(\theta)$ в $\overline{F_v}$, продължаващи съответствията $\theta \mapsto \theta_{ij}$ и $\theta \mapsto \theta_{i_1 j_1}$ задават еквивалентни нормирания върху E тогава и само тогава, когато са спрегнати над F_v. Последното е равносилно на $i = i_1$, така че съществуват точно m класа нормирания w_i над v и всяко от тях отговаря на влагане $E = F(\theta) \hookrightarrow F(\theta_{ij}) \subset \overline{F_v}$ за някой корен θ_{ij} на $f_i(x)$. Да напомним, че попълненията $E_{w_i} = F(\theta_{ij}) * F_v = F_v(\theta_{ij})$, откъдето степените $[E_{w_i} : F_v] = [F_v(\theta_{ij}) : F_v] = \deg(f_i)$. От друга страна, $\deg(f) = [F(\theta) : F] = [E : F]$, така че

$$[E : F] = \deg(f) = \sum_{i=1}^{m} \deg(f_i) = \sum_{i=1}^{m} [E_{w_i} : F_v] = \sum_{w/v} [E_w : F_v],$$

където сумирането е по m-те класа нормирания w на E над v, Q.E.D.

Определение 13.11. *Нека F е поле с дискретно нормиране $v : F \to \mathbb{R} \cup \{\infty\}$, $E \supset F$ е крайно разширение и $w : E \to \mathbb{R} \cup \{\infty\}$ е нормиране на E над v. Тогава*

$$e(w/v) = [w(E^*) : v(F^*)]$$

се нарича индекс на разклонение на w над v.
Полето от остатъци $\mathcal{O}_v/\mathfrak{M}_v$ на v е подполе на полето от остатъци $\mathcal{O}_w/\mathfrak{M}_w$ на w и

$$f(w.v) = [\mathcal{O}_w/\mathfrak{M}_w : \mathcal{O}_v/\mathfrak{M}_v]$$

се нарича относителна степен на w над v.

Непосредствено се вижда, че всички нормирания w на E над дискретното нормиране v на F са дискретни и ако $w : E \to \mathbb{Z} \cup \{\infty\}$ е нормализирано, то $v : F \to e(w/v)\mathbb{Z} \cup \{\infty\}$ взема стойности в единствената адитивна подгрупа $(e(w/V)\mathbb{Z}, +)$ на $(\mathbb{Z}, +)$ с индекс $e(w/v)$.

Лема 13.12. *Нека F е поле с дискретно нормиране $v : F \to \mathbb{R} \cup \{\infty\}$, F_v е попълнението на F относно v, $E \supset F$ е крайно разширение с дискретно нормиране $w : E \to \mathbb{R} \cup \{\infty\}$ над v, а E_w е попълнението на E относно w. Тогава индексът на разклонение*

$$[w(E^*) : v(F^*)] = [w(E_w^*) : v(F_v^*)]$$

не се променя при попълнение.
Ако $\mathcal{O}'_w/\mathfrak{M}'_w$, $\mathcal{O}'_v/\mathfrak{M}'_v$ са полетата от остатъци на w, v в E_w, F_v, то относителната степен

$$[\mathcal{O}_w/\mathfrak{M}_w] = [\mathcal{O}'_w/\mathfrak{M}'_w : \mathcal{O}'_v/\mathfrak{M}'_v]$$

на w над v не се променя при попълнение.

Доказателство: Да означим $e = e(w/v) = [w(E^*) : v(F^*)]$. Без ограничение на общността можем да считаме, че дискретното нормиране w е нормализирано, т.е. $w(E^*) = \mathbb{Z}$, така че $v(F^*) = e\mathbb{Z}$. Попълнението E_w е затворената обвивка на E относно w, така че образът $w(E_w^*)$ на мултипликативната група E_w^* на E_w е попълнението на образа $w(E^*)$ на мултипликатевната група E^* на E в $(\mathbb{R}, +)$. Съгласно дискретността на $w(E^*) = \mathbb{Z}$ имаме $w(E_w^*) = w(E^*) = \mathbb{Z}$. Аналогично, $v(F_v^*) = v(F^*)$ и

$$[w(E_w^*) : v(F_v^*)] = [w(E^*) : v(F^*)].$$

Нека $[\mathcal{O}_w/\mathfrak{M}_w : \mathcal{O}_v/\mathfrak{M}_v] = f(w/v) = f$ и $b_1, \dots, b_f$ е $\mathcal{O}_v/\mathfrak{M}_v$-базис на $\mathcal{O}_w/\mathfrak{M}_w$. Максималният идеал $\mathfrak{M}_w = \mathfrak{M}_v\mathcal{O}_w$ на $\mathcal{O}_w$ се поражда от максималния идеал $\mathfrak{M}_v$ на $\mathcal{O}_v$, така че можем да приложим Лема 12.3 (ii) на Nakayama и да получим, че $\mathcal{O}_w = \mathcal{O}_v b_1 + \ldots + \mathcal{O}_v b_f$ се поражда от $b_1, \dots, b_f$ като $\mathcal{O}_v$-модул. Пръстените на нормиране $\mathcal{O}'_w$, $\mathcal{O}'_v$ са затворените обвивки на $\mathcal{O}_w$, съответно, на $\mathcal{O}_v$ в E_w или в F_v, така че

$$\mathcal{O}'_w = \mathcal{O}'_v b_1 + \ldots + \mathcal{O}'_v b_f.$$

Следователно $b_1 + \mathfrak{M}'_w, \dots, b_f + \mathfrak{M}'_w$ пораждат $\mathcal{O}'_w/\mathfrak{M}'_w$ като линейно пространство над $\mathcal{O}'_v/\mathfrak{M}'_v$. Остава да проверим линейната независимост на елементите $b_1 + \mathfrak{M}'_w, \dots, b_f + \mathfrak{M}'_w$ над $\mathcal{O}'_v/\mathfrak{M}'_v$. При допускане на противното получаваме съществуването на фундаментални редици $r_j = \{r_{j,n}\}_{n=1}^{\infty} \subset \mathcal{O}_v$, така че

$$\sum_{j=1}^{f}(\lim_{n\to\infty} r_{j,n} + \mathfrak{M}'_v)(b_j + \mathfrak{M}'_w) = \mathfrak{M}'_w \quad \text{с} \quad \lim_{n\to\infty} r_{j_o,n} \notin \mathfrak{M}'_v \quad \text{за поне едно} \quad j_o.$$

Оттук $\sum_{j=1}^{f}(\lim_{n\to\infty} r_{j,n})b_j \in \mathfrak{M}'_w$ или $\lim_{n\to\infty}\left(\sum_{j=1}^{f} r_{j,n}b_j\right) \in \mathfrak{M}'_w$. В резултат, $\xi_n = \sum_{j=1}^{f} r_{j,n}b_j \in \mathfrak{M}'_w$ с изключение на краен брой членове ξ_n и

$$\sum_{j=1}^{f}(r_{j,n} + \mathfrak{M}_v)(b_j + \mathfrak{M}_w) = \mathfrak{M}_w \quad \text{с} \quad r_{j_o,n} \notin \mathfrak{M}_v$$

за всички $n \in \mathbb{N}$ с изключение на краен брой. Това противоречи на $\mathcal{O}_v/\mathfrak{M}_v$-линейната независимост на $b_1, \dots, b_f$ и доказва $\mathcal{O}'_v/\mathfrak{M}'_v$-линейната независимост на $b_1 + \mathfrak{M}'_w, \dots, b_f + \mathfrak{M}'_w$. С други думи, $[\mathcal{O}_w/\mathfrak{M}_w : \mathcal{O}_v/\mathfrak{M}_v] = [\mathcal{O}'_w/\mathfrak{M}'_w : \mathcal{O}'_v/\mathfrak{M}'_v]$, Q.E.D.

Твърдение 13.13. *Нека F_v е попълнението на поле F относно дискретно нормиране v, $E \supset F$ е крайно разширение, $w : E \to \mathbb{R} \cup \{\infty\}$ е дискретно нормиране на E над v, а E_w е попълнението на E относно w. Тогава степента*

$$[E_w : F_v] = e(w/v)f(w/v)$$

на попълнението E_w на E относно w над попълнението F_v на F относно v е равна на произведението на индекса на разклонение $e(w/v) = [w(E^*) : v(F^*)]$ и на относителната степен $f(w/v) = [\mathcal{O}_w/\mathfrak{M}_w : \mathcal{O}_v/\mathfrak{M}_v]$.

Доказателство: Съгласно Лема 13.12, $e = e(w/v) = [w(E_w^*) : v(F_v^*)]$. Без ограничение на общността можем да считаме, че $w(E_w^*) = w(E^*) = \mathbb{Z}$. Тогава $v(F_v^*) = v(F^*) = e\mathbb{Z}$. Нека $f = f(w/v) = [\mathcal{O}_w/\mathfrak{M}_w : \mathcal{O}_v/\mathfrak{M}_v]$ и елементите $\alpha_1 + \mathfrak{M}_w, \dots, \alpha_f + \mathfrak{M}_w$ образуват базис на $\mathcal{O}_w/\mathfrak{M}_w$ над $\mathcal{O}_v/\mathfrak{M}_v$. Избираме множество от представители $R \subset \mathcal{O}_v$ на $\mathcal{O}_v/\mathfrak{M}_v$. Тогава всеки елемент на $\mathcal{O}_w/\mathfrak{M}_w$ е от вида

$$\sum_{j=1}^{f}(\alpha_j + \mathfrak{M}_w)r_j = \left(\sum_{j=1}^{f} r_j\alpha_j\right) + \mathfrak{M}_w,$$

така че $R\alpha_1 + \ldots + R\alpha_f \subset \mathcal{O}_w$ е множество от представители на $\mathcal{O}_w/\mathfrak{M}_w$. Ако T е локален параметър на w, то $w(T) = 1$ и $w(T^e) = ew(T) \in e\mathbb{Z} = v(F^*)$. За произволен локален параметър t на v съществува $u \in \mathcal{O}_w^*$, така че $T^e = tu$. Всеки елемент z на E_w се представя с Лоранов ред

$$z = \sum_{i \geq i_0} \eta_i T^i$$

на T с коефициенти $\eta_i \in R\alpha_1 + \ldots + R\alpha_f$, които разглеждаме като елементи на $\mathcal{O}_v/\mathfrak{M}_v$. Представяме $\eta_i = \sum_{j=1}^{f} r_{ij}\alpha_j$ чрез $r_{ij} \in R$. Ако $i = eq + s$ е делението на $i \in \mathbb{Z}$ с $e \in \mathbb{N}$ с частно $q \in \mathbb{Z}$ и остатък $s \in \mathbb{Z}$, $0 \leq s \leq e-1$, то $T^i = T^s t^q$ и

$$z = \sum_{s=0}^{e-1}\sum_{q\in\mathbb{Z}}\sum_{j=1}^{l} r_{s,q,j}\alpha_j T^s t^q.$$

Оттук $\{T^s\alpha_j\}_{s=0,j=1}^{e-1,f}$ пораждат E_w над $\mathcal{O}_v \ni \sum_{q\in\mathbb{Z}} r_{s,q,j}t^q$, а оттам и над F_v. Твърдим, че $\{T^s\alpha_j\}_{s=0,j=1}^{e-1,f}$ са F_v-линейно независими. Да допуснем, че

$$\sum_{s=0}^{e-1}\sum_{j=1}^{f} a_{s,j}T^s\alpha_j = 0 \tag{13.2}$$

с $a_{s,j} \in F_v$ и поне едно $a_{s_o,j_o} \neq 0$. Твърдим, че за $\forall 0 \leq s \leq e-1$ съществува $1 \leq j_s \leq f$ с

$$w\left(\sum_{j=1}^{f} a_{s,j}\alpha_j\right) = v(a_{s,j_s}). \tag{13.3}$$

За целта разглеждаме $m_s = \min(v(a_{s,j}) \ \ |1 \leq j \leq f)$ и избираме j_s с $v(a_{s,j_s}) = m_s$. Достатъчно е да докажем, че $\sum_{j=1}^{f} \frac{a_{s,j}}{a_{s,j_s}}\alpha_j \in \mathcal{O}_w^*$, за да получим (13.3). Да отбележим, че $v\left(\frac{a_{s,j}}{a_{s,j_s}}\right) \geq 0$, така че $\frac{a_{s,j}}{a_{s,j_s}} \in \mathcal{O}_v$. Ако допуснем, че $\sum_{j=1}^{f} \frac{a_{s,j}}{a_{s,j_s}}\alpha_j \in \mathfrak{M}_w$, то линейната независимост на $\alpha_1 + \mathfrak{M}_w, \ldots, \alpha_f + \mathfrak{M}_w$ над $\mathcal{O}_v/\mathfrak{M}_v$ води до $\frac{a_{s,j}}{a_{s,j_s}} \in \mathfrak{M}_v$ за $\forall 1 \leq j \leq f$. При $j = j_s$ получаваме $1 \in \mathfrak{M}_v$, което е противоречие, доказващо $\sum_{j=1}^{f} \frac{a_{s,j}}{a_{s,j_s}}\alpha_j \in \mathcal{O}_w^*$. По този начин, за всички s, за които съществува $1 \leq j \leq f$ с $a_{s,j} \neq 0$, стойността $w\left(\left(\sum_{j=1}^{f} a_{s,j}\alpha_j\right)T^s\right) = v(a_{s,j_s}) + s$ е цяло число с остатък s при деление с e. В частност $w\left(\left(\sum_{j=1}^{f} a_{s,j}\alpha_j\right)T^s\right)$ са различни за всички s с поне едно $a_{s,j} \neq 0$. Това дава възможност са приложим неравенството на триъгълника с равенство към (13.2) и да получим

$$\infty = w(0) = w\left(\sum_{s=0}^{e-1}\left(\sum_{j=1}^{f} a_{s,j}\alpha_j\right)T^s\right) =$$

$$= \min\left(w\left(\sum_{j=1}^{f} a_{s,j}\alpha_j\right) + s \ \mid \ 0 \leq s \leq e-1, \ \ \exists a_{s,j} \neq 0 \right) < \infty.$$

Противоречието доказва линейната независимост на $\{T^s\alpha_j\}_{s=0,j=1}^{e-1,f}$ над F_v, а оттам и $[E_w : F_v] = ef$, Q.E.D.

Следствие 13.14. *Нека F е поле с дискретно нормиране v, а $E \supset F$ е крайно сепарабелно разширение. Тогава степента*

$$[E : F] = \sum_{w/v} e(w/v)f(w/v),$$

където w пробягва класовете дискретни нормирания на E над v,

$$e(w/v) = [w(E^*) : v(F^*)]$$

е индексът на разклонение на w над v, а

$$f(w/v) = [\mathcal{O}_w/\mathfrak{M}_w : \mathcal{O}_v/\mathfrak{M}_v]$$

е относителната степен на w над v.

Доказателство: По Твърдение 13.10 имаме $[E : F] = \sum\limits_{w/v} [E_w : F_v]$ за степените $[E_w : F_v]$ на попълненията E_w на E относно w относно попълнението F_v на F относно v. Достатъчно е да приложим Твърдение 13.13, съгласно което $[E_w : F_v] = e(w/v)f(w/v)$ за всяко дискретно нормиране w на E над v, Q.E.D.
Навсякъде по-нататък разглеждаме гладки проективни криви C, определени над крайно поле $\mathbb{F}_q$. Съгласно Следствие 6.31(iii), $\mathbb{F}_q$ е пълното поле от константи на фунционалното поле $\mathbb{F}_q(C)$ на C над $\mathbb{F}_q$, защото $\mathbb{F}_q$ е съвършено поле.

Лема 13.15. *Нека C е гладка проективна крива, определена над крайно поле $\mathbb{F}_q$, а $\mathbb{F}_{q^n}(C) := \mathbb{F}_q(C) * \mathbb{F}_{q^n}$ е композитът на $\mathbb{F}_q(C)$ и $\mathbb{F}_{q^n}$ в $\overline{\mathbb{F}_q}(C)$. Тогава степента $[\mathbb{F}_{q^n}(C) : \mathbb{F}_q(C)] = n$ и групата на Galois*

$$Gal(\mathbb{F}_{q^n}(C)/\mathbb{F}_q(C)) = Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \Phi_q \rangle \simeq (\mathbb{Z}_n, +).$$

Доказателство: Разширението $\mathbb{F}_{q^n} \supset \mathbb{F}_q$ е крайно и сепарабелно, така че $\mathbb{F}_{q^n} = \mathbb{F}_q(\theta)$ има примитивен елемент θ. Минималният полином $f(x) \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$ на θ над $\mathbb{F}_q$ е от степен $\deg(f) = [\mathbb{F}_q(\theta) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Достатъчно е да се докаже, че полиномът $f(x) \in \mathbb{F}_q(C)[x] \setminus \mathbb{F}_q(C)$ е неразложим над $\mathbb{F}_q(C)$, за да получим, че $\mathbb{F}_{q^n}(C) = \mathbb{F}_q(C) * \mathbb{F}_{q^n} = \mathbb{F}_q(C) * \mathbb{F}_q(\theta)$ е от степен n над $\mathbb{F}_q(C)$. Да допуснем противното, $f(x) = g(x)h(x)$ за $g(x), h(x) \in \mathbb{F}_q(C)[x] \setminus \mathbb{F}_q(C)$. Поради нормалността на разширението $\mathbb{F}_{q^n} \supset \mathbb{F}_q$, всички корени на $f(x)$ са в $\mathbb{F}_{q^n}$, така че и всички корени на $g(x)$ и $h(x)$ са от $\mathbb{F}_{q^n}$. Оттук, коефициентите на $g(x)$ и $h(x)$ са от $\mathbb{F}_{q^n}$ и са алгебрични над $\mathbb{F}_q$ елементи на $\mathbb{F}_q(C)$. Съгласно Следствие 6.31 (iii), $\mathbb{F}_q$ е пълното поле от константи на $\mathbb{F}_q(C)$, така че $g(x), h(x) \in \mathbb{F}_q[x]$. Това противоречи на неразложимостта на $f(x) \in \mathbb{F}_q(C)[x] \setminus \mathbb{F}_q(C)$ над $\mathbb{F}_q$. Следователно $\mathbb{F}_{q^n}(C) = \mathbb{F}_q(C)(\theta) \supset \mathbb{F}_q(C)$ е нормално сепарабелно разширение от степен n, породено от θ. Образите на θ под действие на $\varphi \in Gal(\mathbb{F}_{q^n}(C)/\mathbb{F}_q(C))$ са корени на минималния полином $f(x) \in \mathbb{F}_q[x]$ на θ над $\mathbb{F}_q(C)$. Следователно

$$Gal(\mathbb{F}_{q^n}(C)/\mathbb{F}_q(C)) \subseteq Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \subseteq Gal(\mathbb{F}_{q^n}(C)/\mathbb{F}_q(C))$$

и $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \Phi_q \rangle \simeq (\mathbb{Z}_n, +)$ е циклична група от ред n, породена от автоморфизма на Frobenius $\Phi_q(\alpha) = \alpha^q$ за $\forall \alpha \in \mathbb{F}_{q^n}$, Q.E.D.

Твърдение 13.16. *Нека C е гладка проективна крива, определена над крайно поле $\mathbb{F}_q$, $v : \mathbb{F}_q(C) \to \mathbb{R} \cup \{\infty\}$ е дискретно нормиране от степен d, $n \in \mathbb{N}$, а $GCD(d, n)$ е естественият най-голям общ делител на d и n. Тогава:*

(i) нормиранията w на $\mathbb{F}_{q^n}(C)$ над v са от степен

$$[\mathcal{O}_w/\mathfrak{M}_w : \mathbb{F}_{q^n}] = \frac{d}{GCD(d,n)};$$

(ii) индексите на разклонение

$$e(w/v) = [w(\mathbb{F}_{q^n}(C)^*) : v(\mathbb{F}_q(C)^*)] = 1;$$

(iii) относителните степени

$$f(w/v) = [\mathcal{O}_w/\mathfrak{M}_w : \mathcal{O}_v/\mathfrak{M}_v] = \frac{n}{GCD(d,n)};$$

(iv) съществуват точно $GCD(d,n)$ класа дискретни нормирания w на $\mathbb{F}_{q^n}(C)$ над v.

Идея за доказателство: Твърдим, че ако $w : \mathbb{F}_{q^n}(C) \to \mathbb{Z} \cup \{\infty\}$ е нормализирано дискретно нормиране над $v : \mathbb{F}_q(C) \to \mathbb{Z} \cup \{\infty\}$, то полето от остатъци

$$\mathcal{O}_w/\mathfrak{M}_w = \mathcal{O}_v/\mathfrak{M}_v * \mathbb{F}_{q^n}$$

на w е композитът на полето от остатъци $\mathcal{O}_v/\mathfrak{M}_v$ на v с $\mathbb{F}_{q^n}$ във функционалното поле $\overline{\mathbb{F}_q}(C)$. Избираме базис $\beta_1, \ldots, \beta_n$ на $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$. Съгласно Лема 13.15, от $[\mathbb{F}_{q^n}(C) : \mathbb{F}_q(C)] = n$ следва, че $\beta_1, \ldots, \beta_n$ е базис на $\mathbb{F}_{q^n}(C)$ над $\mathbb{F}_q(C)$. Следователно $\beta_1, \ldots, \beta_n$ пораждат пръстена $\mathcal{O}_w$ на дискретното нормиране w като модул над пръстена $\mathcal{O}_v = \mathcal{O}_w \cap \mathbb{F}_q(C)$ на дискретното нормиране v. Оттук, $\beta_1 + \mathfrak{M}_w, \ldots, \beta_n + \mathfrak{M}_w$ пораждат полето от остатъци $\mathcal{O}_w/\mathfrak{M}_w$ като линейно пространство над $\mathcal{O}_v/\mathfrak{M}_v$ и $\mathcal{O}_w/\mathfrak{M}_w = \mathcal{O}_v/\mathfrak{M}_v(\beta_1, \ldots, \beta_n)$ е разширението на $\mathcal{O}_v/\mathfrak{M}_v$ чрез $\beta_1, \ldots, \beta_n$. Вземайки предвид $\mathcal{O}_v/\mathfrak{M}_v(\beta_1, \ldots, \beta_n) = \mathcal{O}_v/\mathfrak{M}_v * \mathbb{F}_{q^n}$, получаваме $\mathcal{O}_w/\mathfrak{M}_w = \mathcal{O}_v/\mathfrak{M}_v * \mathbb{F}_{q^n}$.

Ако нормирането $v : \mathbb{F}_q(C) \to \mathbb{R} \cup \{0\}$ е от степен $[\mathcal{O}_v/\mathfrak{M}_v : \mathbb{F}_q] = d$, то полето от остатъци $\mathcal{O}_v/\mathfrak{M}_v \simeq \mathbb{F}_{q^d}$ е изоморфно но полето с q^d елемента и степента на нормирането w на $\mathbb{F}_{q^n}(C)$ е

$$[\mathcal{O}_w/\mathfrak{M}_w : \mathbb{F}_{q^n}] = \left[\mathbb{F}_{q^d} * \mathbb{F}_{q^n} : \mathbb{F}_{q^n}\right] = \left[\mathbb{F}_{q^{LCM(d,n)}} : \mathbb{F}_{q^n}\right] = \frac{LCM(d,n)}{n} = \frac{d}{GCD(d,n)},$$

където $LCM(d,n)$ е естественото най-малко общо кратно на d и n.

Ще приемем наготово, че $w\left(\mathbb{F}_{q^n}(C)^*\right) = w\left(\mathbb{F}_q(C) * \mathbb{F}_{q^n}\right) = v\left(\mathbb{F}_q(C)^*\right)$ или индексът на разклонение $e(w/v) = [w(\mathbb{F}_{q^n}(C)^*) : v(\mathbb{F}_q(C)^*)] = 1$. Грубо казано, ако t е локален параметър на v, то максималният идеал $\mathfrak{M}_v = t\mathcal{O}_v$ на $\mathcal{O}_v$ се разклонява в $\mathcal{O}_w$ тогава и само тогава, когато съдържа дискриминантата на $\mathcal{O}_v$-пораждаща система на $\mathcal{O}_w$. Базисът $\beta_1, \ldots, \beta_n$ на $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$ е $\mathcal{O}_v$-пораждаща система на $\mathcal{O}_w$. Дискриминантата на тази система е в $\mathbb{F}_q^*$ и не принадлежи на $\mathfrak{M}_v = t\mathcal{O}_v$. Следователно $\mathfrak{M}_v = t\mathcal{O}_v$ не се разклонява в $\mathcal{O}_w$ и t е локален параметър на w. Относителните степени

$$f(w/v) = [\mathcal{O}_w/\mathfrak{M}_w : \mathcal{O}_v/\mathfrak{M}_v] = \left[\mathbb{F}_{q^{LCM(d,n)}} : \mathbb{F}_{q^d}\right] = \frac{LCM(d,n)}{d} = \frac{n}{GCD(d,n)}.$$

Сега от равенството

$$n = [\mathbb{F}_{q^n}(C) : \mathbb{F}_q(C)] = \sum_{w/v} e(w/v) f(w/v) = N_v \frac{n}{GCD(d,n)}$$

за броя N_v на дискретните нормирания w на $\mathbb{F}_{q^n}(C)$ над v получаваме $N_v = GCD(d,n)$, Q.E.D.

СЛЕДСТВИЕ 13.17. *Нека C е гладка проективна крива, определена над крайно поле $\mathbb{F}_q$, а $v : \mathbb{F}_q(C) \to \mathbb{Z} \cup \{\infty\}$ е дискретно нормиране от степен m. Тогава съществуват m класа дискретни нормирания w на $\mathbb{F}_{q^m}(C)$ над V. Всички* *такива нормирания са от степен* $[\mathcal{O}_w/\mathfrak{M}_w : \mathbb{F}_{q^m}] = 1$ *и относителна степен* $f(w/v) = 1$.

ЛЕМА 13.18. *Нека C е гладка проективна крива, определена над съвършено поле k. Тогава произволен автоморфизъм $\sigma \in Gal(\overline{k}/k)$ от абсолютната група на Galolis на k трансформира локалния пръстен $\mathcal{O}_p(C)$ на точка $p \in C$ в C върху локалния пръстен*

$$\sigma\mathcal{O}_p(C) = \mathcal{O}_{\sigma(p)}(C)$$

а образа $\sigma(p)$ на p под действие на σ.

Доказателство: Без ограничение на общността заменяме C с афинна отворена околност $V \subset C$, съдържаща p и $\sigma(p)$. За целта е достатъчно да изберем проективна хипер-равнина H в проективното пространство $\mathbb{P}^n(\overline{k}) \supset C$, която не минава през p и $\sigma(p)$. Тогава $V = C \setminus H \subseteq \overline{k}^n$ е афинна крива, съдържаща p и $\sigma(p)$. Локалният пръстен $\mathcal{O}_p(C) = \mathcal{O}_p(V) = \overline{k}[V]_{\mathfrak{N}_p}$ съвпада с локализацията на афинния кооридnatен пръстен $\overline{k}[V] = \overline{k}[x_1, \dots, x_n]/I(V)$ по максималния идеал $\mathfrak{N}_p \triangleleft \overline{k}[V]$ на точката p. Произволен елемент $\sigma \in Gal(\overline{k}/k)$ индуцира автоморфизъм $\sigma : \overline{k}[V] \to \overline{k}[V]$ на афинния координатен пръстен $\overline{k}[V]$ на V, изобразяващ $\mathfrak{N}_p$ върху максималния идеал $\sigma(\mathfrak{N}_p) = \mathfrak{N}_{\sigma(p)}$ на $\sigma(p)$ в $\overline{k}[V]$. По-точно, ако $g \in \mathfrak{N}_p$, то

$$\sigma(g)(\sigma(p)) = \sigma(g(p)) = \sigma(0) = 0$$

и $\sigma(g) \in \mathfrak{N}_{\sigma(p)}$. Следователно $\sigma \in Gal(\overline{k}/k)$ индуцира изоморфизъм

$$\sigma : \mathcal{O}_p(V) = \overline{k}[V]_{\mathfrak{N}_p} \longrightarrow \overline{k}[V]_{\mathfrak{N}_{\sigma(p)}} = \mathcal{O}_{\sigma(p)}(V),$$

Q.E.D.

ТВЪРДЕНИЕ 13.19. *Нека C е гладка проективна крива, определена над крайно поле $\mathbb{F}_q$, а $x, y \in C$ са точки с локални пръстени $\mathcal{O}_x(C), \mathcal{O}_y(C) \subset \overline{k}(C)$. В такъв случай, x и y са от една и съща $\mathbb{F}_q$-затворена точка върху C тогава и само тогава, когато сеченията $\mathcal{O}_x(C) \cap \mathbb{F}_q(C) = \mathcal{O}_y(C) \cap \mathbb{F}_q(C)$ на локалните пръстени на тези точки с функционалното поле $\mathbb{F}_q(C)$ на C над $\mathbb{F}_q$ съвпадат.*

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

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

Да допуснем, че $\mathcal{O}_x(C) \cap \mathbb{F}_q(C) = \mathcal{O}_y(C) \cap \mathbb{F}_q(C)$ и x, y лежат върху различни $\mathbb{F}_q$-затворени точки

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

Съгласно Апроксимационната Теорема 8, съществува $z \in \overline{\mathbb{F}_q}(C)$, така че

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

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

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

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

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

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

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

Ако

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

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

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

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

Следователно $\alpha \notin \mathcal{O}_x(C) \cap \mathbb{F}_q(C)$, $\alpha \in \mathcal{O}_q(C) \cap \mathbb{F}_q(C)$. Това противоречи на $\mathcal{O}_x(C) \cap \mathbb{F}_q(C) = \mathcal{O}_y(C) \cap \mathbb{F}_q(C)$ и доказва, че x и y принадлежат на една и съща $\mathbb{F}_q$-затворена точка, стига $\mathcal{O}_x(C) \cap \mathbb{F}_q(C) = \mathcal{O}_y(C) \cap \mathbb{F}_q(C)$, Q.E.D.

ТЕОРЕМА 16. *Нека C е гладка проективна крива, определена над крайно поле $\mathbb{F}_q$. Тогава $\mathbb{F}_q$-затворените точки от степен m върху C са във взаимно еднозначно съответствие с класовете дискретни нормирания от степен m на функционалното поле $\mathbb{F}_q(C)$ на C над $\mathbb{F}_q$.*

Доказателство: Разглеждаме $\mathbb{F}_q$-затворена точка

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

от степен m, съответните локални пръстени $\mathcal{O}_{\Phi_{q^i}(p)}(C) = \Phi^{q^i}\mathcal{O}_p(C)$ и сеченията им $\mathcal{O}_{\Phi_{q^i}(p)}(C) \cap \mathbb{F}_q(C) = \Phi^{q^i}(\mathcal{O}_p(C) \cap \mathbb{F}_q(C))$ с $\mathbb{F}_q(C)$ за $\forall 0 \leq i \leq m-1$. Да напомним, че $\mathcal{O}_p(C)$ е пръстенът на дискретното нормиране ν_p в $\overline{\mathbb{F}_q}(C)$. Следователно $\mathcal{O}_p(C) \cap \mathbb{F}_q(C)$ е пръстенът на ограничението $\nu_p|_{\mathbb{F}_q(C)}$, което е дискретно нормиране на $\mathbb{F}_q(C)$.

Ако $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(p) \neq Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(r)$ са различни, (а оттук и непресичащи се) $\mathbb{F}_q$-затворени точки, то пръстените $\mathcal{O}_p(C) \cap \mathbb{F}_q(C)$, съответно, $\mathcal{O}_r(C) \cap \mathbb{F}_q(C)$ на нормиранията $\nu_p|_{\mathbb{F}_q(C)}$, $\nu_r|_{\mathbb{F}_q(C)}$ са различни съгласно Твърдение 13.19. Следователно дискретните нормирания $\nu_p|_{\mathbb{F}_q(C)}$ и $\nu_r|_{\mathbb{F}_q}$ на $\mathbb{F}_q(C)$ са нееквивалентни.

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

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

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

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

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

което противоречи на нееквивалентността на дискретните нормирания w_i и w_j на $\mathbb{F}_{q^m}(C)$, Q.E.D.
В останалата част от въпроса ще разгледаме някои свойства на рационалните изображения на криви. Ще докажем, че всяко рационално изображение на гладка крива е морфизъм.

ЛЕМА 13.20. *Ако $\varphi : X \dashrightarrow C$ е рационално изображение на алгебрично многообразие X в крива C, то φ е или постоянно, или доминантно.*

Доказателство: Нека $\mathcal{D} \subseteq X$ е областта на регулярност на φ. Твърдим, че затворената обвивка $\overline{\varphi(\mathcal{D})}$ на образа $\varphi(\mathcal{D})$ на $\mathcal{D}$ е неприводимо подмногообразие на C. Наистина, допускането $\overline{\varphi(\mathcal{D})} = Z_1 \cup Z_2$ за затворени подмножества $Z_i \subseteq \overline{\varphi(\mathcal{D})}$ води до разлагане $X = \varphi^{-1}(Z_1) \cup \varphi^{-1}(Z_2)$ на алгебричното многообразие X в обединение на затворени подмножества $\varphi^{-1}(Z_i)$. Съгласно неприводимостта на X имаме $X = \varphi^{-1}(Z_1)$ след евентуална преномерация на Z_1, Z_2. Следователно $\varphi(\mathcal{D}) \subseteq Z_1$ и $\overline{\varphi(\mathcal{D})} \subseteq Z_1$, откъдето $\overline{\varphi(\mathcal{D})}$ е неприводимо алгебрично подмножество на кривата C. В резултат, $\overline{\varphi(\mathcal{D})} = \{p\}$ е точка или $\overline{\varphi(\mathcal{D})} = C$ е цялата крива C. Рационалното изображение $\varphi : X \dashrightarrow C$ е постоянно, ако $\overline{\varphi(\mathcal{D})} = \{p\}$ или доминантно за $\overline{\varphi(\mathcal{D})} = C$, Q.E.D.

ОПРЕДЕЛЕНИЕ 13.21. *Нека k е съвършено поле, C_1 и C_2 са проективни криви, определени над k, а $\varphi : C_1 \dashrightarrow C_2$ е рационално изображение. Ако φ комутира с произволен елемент $\sigma \in Gal(\overline{k}/k)$ от абсолютната група на Galois на k, казваме, че φ е определено над k.*

ТВЪРДЕНИЕ-ОПРЕДЕЛЕНИЕ 13.22. *Нека C_1 и C_2 са проективни криви, определени над съвършено поле k, $\varphi : C_1 \dashrightarrow C_2$ е непостоянно рационално изображение, определено над k. Тогава:*
(i) φ индуцира влагане $\varphi^* : k(C_2) \hookrightarrow k(C_1)$ на функционалните полета над k;
(ii) $k(C_1) \supset \varphi^* k(C_2)$ е крайно разширение, чиято степен

$$\deg(\varphi) = [k(C_1) : \varphi^* k(C_2)]$$

се нарича степен на φ;
(iii) $\varphi(p) = q$ за точка p от областта на регулярност $\mathcal{D}$ на φ тогава и само тогава, когато $\varphi^* \mathcal{O}_q(C_2) \subseteq \mathcal{O}_p(C_1)$ и $\varphi^* \mathfrak{M}_q(C_2) \subseteq \mathfrak{M}_p(C_1)$.

Доказателство: (i) Съгласно Лема 13.20, рационалното изображение

$$\varphi : C_1 \dashrightarrow C_2$$

е доминантно. Прилагаме Твърдение 8.4 и получаваме влагане

$$\varphi^* : \overline{k}(C_2) \hookrightarrow \overline{k}(C_1)$$

на функционалните полета като $\overline{k}$-алгебри. Твърдим, че това влагане се ограничава до влагане

$$\varphi^* : k(C_2) \hookrightarrow k(C_1)$$

на съответните функционални полета над k, стига $\sigma\varphi = \varphi\sigma$ за $\forall \sigma \in Gal(\overline{k}/k)$. За целта използваме $k(C_j) = \overline{k}^{Gal(\overline{k}/k)}$ от Следствие 6.31(ii). За произволна рационална функция $f \in k(C_2)$ имаме $\sigma(f) = f$ за $\forall \sigma \in Gal(\overline{k}/k)$. В произволна точка p от областта на регулярност на φ е изпълнено

$$\varphi\sigma(p) = \sigma(\varphi(p)) = \sigma(\varphi)(\sigma(p)) \quad \text{за} \quad \forall \sigma \in Gal(\overline{k}/k),$$

така че $\sigma(\varphi) = \varphi$. В резултат, $\sigma(\varphi^*(f)) = \sigma(f\varphi) = \sigma(f)\sigma(\varphi) = f\varphi = \varphi^*(f)$ за $\forall f \in k(C_2)$, $\forall \sigma \in Gal(\overline{k}/k)$, така че $\varphi^*(f) \in \overline{k}(C_1)^{Gal(\overline{k}/k)} = k(C_1)$.

(ii) Подполето $\varphi^* k(C_2)$ на $k(C_1)$ е изоморфно на $k(C_2)$, така че $\varphi^* k(C_2)$ е функционално поле на една променлива. За произволен трансцендентен над k елемент $x \in \varphi^* k(C_2)$, полетата $k(C_1) \supset \varphi^* k(C_2)$ са от крайна степен над чисто трансцендентното разширение $k(x)$ на k чрез x. Следователно степента

$$[k(C_1) : \varphi^* k(C_2)] = \frac{[k(C_1) : k(x)]}{[\varphi^* k(C_2) : k(x)]} < \infty$$

е крайна.

(iii) Нека p е точка от областта на регулярност $\mathcal{D}$ на φ, а $q = \varphi(p)$. Тогава всяка афинна околност U'_q на q върху C_2 пресича $\varphi(\mathcal{D})$, защото в противен случай $\varphi(\mathcal{D})$ се съдържа в затвореното подмножество $C_2 \setminus U'_q \subsetneq C_2$ и $\overline{\varphi(\mathcal{D})} \subseteq C_2 \setminus U'_q$, противно на доминантността на φ. Избираме афинна околност $U_q \subseteq U'_q \cap \varphi(\mathcal{D})$ на q върху C_2 и афинна околност $U_p = \varphi^{-1}(U_q)$ на p върху C_1, така че φ ограничава до морфизъм $\varphi : U_p \to U_q$. Индуцираният хомоморфизъм на k-алгебри $\varphi^* : k[U_q] \to k[U_p]$ е влагане с $\varphi^*(k[U_q] \backslash \mathfrak{N}_q) \subseteq k[U_p] \backslash \mathfrak{N}_p$ за максималния идеал $\mathfrak{N}_q$ на q в $k[U_q]$ и максималния идеал $\mathfrak{N}_p$ на p в $k[U_p]$. Следователно φ^* се продължава до инективен хомоморфизъм на k-алгебри

$$\varphi^* : \mathcal{O}_q(C_2) = \mathcal{O}_q(U_q) = k[U_q]_{\mathfrak{N}_q} \longrightarrow k[U_p]_{\mathfrak{N}_p} = \mathcal{O}_p(U_p) = \mathcal{O}_p(C_1),$$

изобразяващ максималния идеал $\mathfrak{M}_q(C_2)$ на $\mathcal{O}_q(C_2)$ в максималния идеал $\mathfrak{M}_p(C_1) \supseteq \varphi^* \mathfrak{M}_q(C_2)$.

Нека p е точка от областта на регулярност $\mathcal{D}$ на φ, $\varphi^* \mathcal{O}_q(C_2) \subseteq \mathcal{O}_p(C_1)$ и $\varphi^* \mathfrak{M}_q(C_2) \subseteq \mathfrak{M}_p(C_1)$. Като в първата част на доказателството, избираме афинни отворени околности U_p върху C_1 и U_q върху C_2, така че φ се ограничава до морфизъм на афинни многообразия $\varphi : U_p \to U_q$. Разглеждаме хомоморфизма $\varphi^* : \overline{k}[U_q] \to \overline{k}[U_p]$ на съответните афинни координатни пръстени. Максималният идеал на локалния пръстен $\mathcal{O}_q(C_2) = \mathcal{O}_q(U_q)$ е локализацията $\mathfrak{M}_q(C_2) = \mathfrak{N}_{q_{\mathfrak{N}_q}}$ на максималния идеал $\mathfrak{N}_q$ на q в $\overline{k}[U_q]$ относно допълнението му $\overline{k}[U_q] \setminus \mathfrak{N}_q$. От $\mathfrak{N}_q \subset \mathfrak{N}_{q_{\mathfrak{N}_q}} = \mathfrak{M}_q(C_2)$ и $\varphi^* \mathfrak{M}_q(C_2) \subseteq \mathfrak{M}_p(C_1)$ получаваме $\varphi^* \mathfrak{N}_q \subseteq \mathfrak{M}_p(C_1)$. Ако $q = (q_1, \ldots, q_m) \in U_q \subseteq \overline{k}^m$, то $x_j - q_j + I(U_q) \in \mathfrak{N}_q$ се изобразява в $\varphi^*(x_j - q_j + I(U_q)) \in \mathfrak{M}_p(C_1)$. Да отбележим, че $\varphi^* I(U_q) \subseteq I(U_p)$. Ако $\varphi = (\varphi_1, \ldots, \varphi_m) : U_p \to U_q \subseteq \overline{k}^m$, то за всяко $1 \leq j \leq m$ получаваме, че $\varphi_j - q_j \in \mathfrak{M}_p(C_1)$ е регулярна функция в p, която се анулира в p. В резултат получаваме $\varphi_j(p) = q_j$ за $\forall 1 \leq j \leq m$, което е равносилно на $\varphi(p) = q$, Q.E.D.

Лема 13.23. *Нека C_1 и C_2 са проективни криви, определени над съвършено поле k, а $\psi : k(C_2) \hookrightarrow k(C_1)$ е влагане на функционалните им полета над k с $\psi|_k = \mathrm{Id}_k$. Тогва съществува рационално изображение $\varphi : C_1 \dashrightarrow C_2$ над k с $\varphi^* = \psi$.*

Доказателство: Продължаваме ψ до влагане

$$\psi : \overline{k}(C_2) = k(C_@) * \overline{k} \hookrightarrow k(C_1) * \overline{k} = \overline{k}(C_1)$$

на съответните функционални полета над $\overline{k}$ с $\psi|_{\overline{k}} = \mathrm{Id}_{\overline{k}}$. Тогава съгласно Твърдение 8.4 съществува рационално изображение $\varphi : C_1 \dashrightarrow C_2$ с $\varphi^* = \psi$. Остава да проверим, че φ е определено над k. Достатъчно е да докажем, че произволно ограничение на φ до морфизъм $\varphi : U_1 \to U_2$ на афинни отворени подмножества $U_i \subset C_i$ е определено над k. За целта разглеждаме индуцираното влагане $\varphi^* = \psi : k(U_2) = k(C_2) \hookrightarrow k(C_1) = k(U_1)$ на функционалните полета над k. Съгласно $k(U_2) = \overline{k}(U_2)^{Gal(\overline{k}/k)}$, елементите f на $k(U_2)$ се характеризират с $\sigma(f) = f$ за $\forall \sigma \in Gal(\overline{k}/k)$. Понеже $f\varphi = \varphi^*(f) = \psi(f) \in k(U_1)$, имаме

$$f\varphi = \sigma(f\varphi) = \sigma(f)\sigma(\varphi) = f\sigma(\varphi) \quad \text{за} \quad \forall \sigma \in Gal(\overline{k}/k).$$

Прилагайки последното равенство към координатните функции $y_1, \ldots, y_m \in k[U_2]$ върху $U_2 \subseteq \overline{k}^m$, получаваме $\varphi = \sigma(\varphi)$. Сега за всяка точка $p \in U_1$ е изпълнено

$$\sigma(\varphi(p)) = \sigma(\varphi)(\sigma(p)) = \varphi(\sigma(p)),$$

така че $\sigma\varphi = \varphi\sigma$ за $\forall \sigma \in Gal(\overline{k}/k)$ и морфизмът $\varphi : U_1 \to U_2$ е определен над k, Q.E.D.

Лема 13.24. *Нека $F \subseteq L$ са функционални полета на една променлива с общо поле от константи k. Тогава всеки подпрьстен $F \subseteq R \subseteq L$ е поле.*

Доказателство: Ще проверим, че всеки ненулев елемент $\alpha \in R \setminus \{0\}$ на R е обратим в R. Щом $F \subseteq L$ са функционални полета на една променлива, разширението $L \supseteq F$ е крайно. Следователно $\forall \alpha \in R \setminus \{0\}$ е алгебрично над F. Ако

$$f(x) = x^m + c_{m-1}x^{m-1} + \ldots + c_1 x + c_0 \in F[x]$$

е минималният полином на $\alpha \in R \setminus \{0\}$ над F, то $c_0 \neq 0$ съгласно неразложимостта на $f(x)$ над F. Следователно

$$\alpha(\alpha^{m-1} + c_{m-1}\alpha^{m-2} + \ldots + c_2\alpha + c_1) = -c_0,$$

откъдето

$$\alpha[(\alpha^{m-1} + c_{m-1}\alpha^{m-2} + \ldots + c_2\alpha + c_1)(-c_0)^{-1}] = 1$$

и съществува

$$\alpha^{-1} = (\alpha^{m-1} + c_{m-1}\alpha^{m-2} + \ldots + c_2\alpha + c_1)(-c_0)^{-1} \in F[\alpha] \subseteq R,$$

Q.E.D.

Твърдение 13.25. *Нека C_1, C_2 са проективни криви, определени над съвършено поле k и $\varphi : C_1 \dashrightarrow C_2$ е непостоянно рационално изображение, определено над k. Тогава множеството C_1^{smooth} на гладките точки на C_1 се съдържа в областта на регулярност $\mathcal{D}$ на φ.*
В частност, ако C_1 е гладка проективна крива, то всяко рационално изображение $\varphi : C_1 \dashrightarrow C_2$ в проекитвна крива C_2 е морфизъм.

Доказателство: Твърдим, че всяка гладка точка $p \in C_1^{\text{smooth}}$ на C_1 е от областта на регулярност $\mathcal{D}$ на φ. Условието $p \in \mathcal{D}$ е еквивалентно на съществуването на точка $q \in C_2$ с $\varphi^*\mathcal{O}_q(C_2) \subseteq \mathcal{O}_p(C_1)$, $\varphi^*\mathfrak{M}_q(C_2) \subseteq \mathfrak{M}_p(C_1)$.
Преди всичко, $\varphi^*k(C_2) \cap \mathcal{O}_p(C_1) \neq \varphi^*k(C_2)$, защото допускането $\varphi^*k(C_2) \cap \mathcal{O}_p(C_1) = \varphi^*k(C_2)$ е еквивалентно на $\varphi^*k(C_2) \subseteq \mathcal{O}_p(C_1)$. Но $\mathcal{O}_p(C_1) \subseteq k(C_1)$, така че по Лема 13.24, локалният пръстен $\mathcal{O}_p(C_1)$ трябва да е поле. Противоречието доказва, че $R = \varphi^*k(C_2) \cap \mathcal{O}_p(C_1)$ е собствен подпръстен на полето $\varphi^*k(C_2)$.
Дискретното нормиране ν_p на $k(C_1)$ с пръстен $\mathcal{O}_p(C_1) \cap k(C_1)$ се ограничава до дискретно нормиране на $\varphi^*k(C_2)$ с пръстен R. Следователно съществува точка $q \in C_2$, така че $R = \varphi^*(\mathcal{O}_q(C_2) \cap k(C_2))$. В резултат, $\varphi^*\mathcal{O}_q(C_2) \subseteq \mathcal{O}_p(C_1)$ и $\varphi^*\mathfrak{M}_q(C_2) \subseteq \mathfrak{M}_p(C_1)$, откъдето $\varphi(p) = q$ и $p \in \mathcal{D}$, Q.E.D.

Следствие 13.26. *Нека C_1, C_2 са гладки проективни криви, определени над съвършено поле k. Тогава следните условия са еквивалентни:*
(i) съществува изоморфизъм $\psi : k(C_2) \to k(C_1)$ на функционалните полета над k с $\psi|_k = \mathrm{Id}_k$;
(ii) съществува бирационално изображение $\varphi : C_1 \dashrightarrow C_2$, определено над k;
(iii) съществува изоморфизъм $\varphi : C_1 \to C_2$, определен над k.