

Локален пръстен на гладка точка на крива

В настоящия въпрос ще въведем понятието гладка точка на афинна крива V . Ще докажем, че дискретните нормирания на функционалното поле $\bar{k}(V)$ на V са във взаимно еднозначно съответствие с гладките точки на V . По-точно, точка $p \in V$ е гладка тогава и само тогава, когато локалният и пръстен $\mathcal{O}_p(V)$ е пръстен на дискретно нормиране с поле от частни $\bar{k}(V)$. Ако кривата V е гладка, то всеки пръстен на дискретно нормиране $R \subset \bar{k}(V)$ с поле от частни $\bar{k}(V)$ е локален пръстен на еднозначно определена точка, $R = \mathcal{O}_p(V)$.

ОПРЕДЕЛЕНИЕ 12.1. Нека $V \subseteq \bar{k}^n$ е афинна крива с идеал $I(V) = \langle f_1, \dots, f_m \rangle$ за някакви полиноми $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n) \in \bar{k}[x_1, \dots, x_n]$. Точката $p \in V$ е гладка, ако Якобиевата матрица

$$\frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \cdots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}$$

има ранг $\text{rk} \frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)}(p) = n - 1$ в p .

Ако p е гладка точка на V , то правата, съставена от решенията на хомогенната линейна система

$$\frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)}(p) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0_{m \times 1}$$

се нарича допирателна към V в p .

Точките $p \in V$, които не са гладки се наричат особенени.

Означаваме с V^{smooth} множеството на гладките точки, а с V^{sing} - множеството на особените точки.

Кривата V е гладка, ако всички точки на V са гладки, $V = V^{\text{smooth}}$.

ЛЕМА 12.2. Локалният пръстен $\mathcal{O}_p(V)$ на точка p от крива V е нютерова локална област с размерност на Krull 1.

Доказателство: Без ограничение на общността можем да заменим кривата V с нейно афинно отворено подмножество и да считаме, че V е афинна крива. Съгласно Лема-Определение 7.8, $\mathcal{O}_p(V)$ е локална област.

Твърдим, че пръстенът $\mathcal{O}_p(V) = \bar{k}[V]_{\mathfrak{m}_p}$ е нютеров. Преди всичко, факторпръстенът $\bar{k}[V] = \bar{k}[x_1, \dots, x_n]/I(V)$ на нютеровия полиномиален пръстен $\bar{k}[x_1, \dots, x_n]$ е нютеров, защото всеки идеал $J \triangleleft \bar{k}[V]$ се повдига до идеал $\tilde{J} \triangleleft \bar{k}[x_1, \dots, x_n]$, който съдържа $I(V)$ и има фактор $\tilde{J}/I(V) = J$. Идеалът $\tilde{J} = \langle f_1, \dots, f_m \rangle$ е крайно породен съгласно Теорема 9 на Hilbert за базиса. Отгук $J = \langle f_1 + I(V), \dots, f_m + I(V) \rangle$ е крайно породен и афинният координатен пръстен $\bar{k}[V]$ е нютеров.

За нютеровостта на $\bar{k}[V]_{\mathfrak{m}_p} = \mathcal{O}_p(V)$ е достатъчно да проверим, че за произволна нютерова комутативна област с единица R и произволен прост идеал \mathfrak{p}

в R локализацията

$$R_{\mathfrak{p}} = \left\{ \frac{\alpha}{\beta} \mid \alpha, \beta \in R, \beta \notin \mathfrak{p} \right\}$$

на R относно \mathfrak{p} е нютерова област. Съгласно Задача 7.13, пръстенът $R_{\mathfrak{p}}$ е локален, с максимален идеал

$$\mathfrak{p}_{\mathfrak{p}} = \left\{ \frac{\alpha}{\beta} \mid \alpha \in \mathfrak{p} \right\}.$$

За произволен собствен идеал $I \triangleleft R_{\mathfrak{p}}$ да означим с

$$\tilde{I} = \left\{ \alpha \in R \mid \exists \frac{\alpha}{\beta} \in I \right\}$$

множеството на числителите на елементите на I . За произволни $\alpha_1, \alpha_2 \in \tilde{I}$ с $\frac{\alpha_1}{\beta_1}, \frac{\alpha_2}{\beta_2} \in I$ имаме $I \ni \frac{\alpha_1}{\beta_1} \cdot \frac{\beta_1}{\beta_2} - \frac{\alpha_2}{\beta_2} = \frac{\alpha_1 - \alpha_2}{\beta_2}$, откъдето $\alpha_1 - \alpha_2 \in \tilde{I}$. Ако $\alpha \in \tilde{I}$ с $\frac{\alpha}{\beta} \in I$ и $\gamma \in R$, то $I \ni \frac{\alpha}{\beta} \cdot \gamma$ с $\alpha\gamma \in \tilde{I}$, така че \tilde{I} е идеал в R . При $I \neq R_{\mathfrak{p}}$ идеалът $\tilde{I} \subseteq \mathfrak{p}$ се съдържа в простия идеал \mathfrak{p} . Непосредствено се вижда, че

$$I = \left\{ \frac{\alpha}{\beta} \mid \alpha \in \tilde{I}, \beta \in R \setminus \mathfrak{p} \right\}.$$

Съгласно нютеровостта на R , идеалът $\tilde{I} = \langle \alpha_1, \dots, \alpha_m \rangle = \left\{ \sum_{i=1}^m \alpha_i \gamma_i \mid \gamma_i \in R \right\}$ е крайно породен. Следователно

$$I = \left\{ \sum_{i=1}^m \alpha_i \frac{\gamma_i}{\beta} \mid \frac{\gamma_i}{\beta} \in R_{\mathfrak{p}} \right\} = \langle \alpha_1, \dots, \alpha_m \rangle$$

е крайно породен и $R_{\mathfrak{p}}$ е също нютеров. Това доказва, че $\mathcal{O}_p(V)$ е нютерова локална област.

Съгласно Твърдение ??, размерността 1 на афинната крива V съвпада с размерността на Krull на афинния координатен пръстен $\bar{k}[V]$. Нулевият идеал на областта $\bar{k}[V]$ е прост. Максималната дължина на редица от прости идеали в $\bar{k}[V]$ е две, така че всеки ненулев прост идеал е максимален. Твърдим, че идеалът $\mathfrak{q} \triangleleft \bar{k}[V]_{\mathfrak{M}_p} = \mathcal{O}_p(V)$ е прост тогава и само тогава, когато повдигането му $\tilde{\mathfrak{q}}$ е прост идеал в $\bar{k}[V]$, съдържащ се в \mathfrak{M}_p . Оттук $\tilde{\mathfrak{q}} = 0$ или $\tilde{\mathfrak{q}} = \mathfrak{M}_p$ и $\mathfrak{q} = 0$ или

$$\mathfrak{q} = (\mathfrak{M}_p)_{\mathfrak{M}_p} = \left\{ \frac{\alpha}{\beta} \mid \alpha \in \mathfrak{M}_p, \beta \in \bar{k}[V] \setminus \mathfrak{M}_p \right\}.$$

Следователно максималната дължина на редица от прости идеали в $\mathcal{O}_p(V) = \bar{k}[V]_{\mathfrak{M}_p}$ е две и нютеровата локална област $\mathcal{O}_p(V)$ е с размерност на Krull 1. Простотата на повдигането $\tilde{\mathfrak{q}} = \left\{ \alpha \in \bar{k}[V] \mid \frac{\alpha}{\beta} \in \mathfrak{q} \right\}$ на прост идеал $\mathfrak{q} \triangleleft \bar{k}[V]_{\mathfrak{M}_p}$ се проверява непосредствено. По-точно, нека $\alpha\gamma \in \tilde{\mathfrak{q}}$ и $\gamma \notin \tilde{\mathfrak{q}}$. Тогава съществува $\beta \in \bar{k}[V] \setminus \mathfrak{M}_p$ с $\frac{\alpha\gamma}{\beta} \in \mathfrak{q}$. Понеже $\gamma \notin \mathfrak{q}$ и идеалът \mathfrak{q} е прост, от $\frac{\alpha}{\beta}\gamma \in \mathfrak{q}$ следва $\frac{\alpha}{\beta} \in \mathfrak{q}$ и $\alpha \in \tilde{\mathfrak{q}}$. Това доказва простотата на $\tilde{\mathfrak{q}}$ и факта, че $\mathcal{O}_p(V)$ е с размерност на Krull 1, Q.E.D.

За да характеризираме локалните пръстени на гладките точки на криви ни е необходимо примарното разлагане на идеал в нютеров комутативен пръстен с единица. Следващите няколко лема са алгебрична подготовка за това.

ЛЕМА 12.3. (Лема на Накауата) *Нека R е локален пръстен с максимален идеал \mathfrak{M} , M е крайно породен R -модул, а N е подмодул на M . Тогава*

- (i) *от $N + \mathfrak{M}M = M$ следва $N = M$;*
- (ii) *ако $x_1 + \mathfrak{M}M, \dots, x_n + \mathfrak{M}M$ пораждат*

$$M/\mathfrak{M}M = l_{R/\mathfrak{M}}(x_1 + \mathfrak{M}M, \dots, x_n + \mathfrak{M}M)$$

като линейно пространство над полето R/\mathfrak{M} , то x_1, \dots, x_n поражда

$$M = RX_1 + \dots + Rx_n$$

като R -модул.

Доказателство: (i) В частния случай на $N = 0$ трябва да докажем, че от $\mathfrak{M}M = M$ следва $M = 0$. Допускаме противното $M \neq 0$ и избираме минимална пораждаща система u_1, \dots, u_r на M като R -модул. Тогава за $u_r \in M = \mathfrak{M}M$ съществуват елементи $\mu_i \in \mathfrak{M}$, така че $u_r = \sum_{i=1}^r \mu_i u_i$. Оттук $(1 - \mu_r)u_r = \sum_{i=1}^{r-1} \mu_i u_i$ с $1 - \mu_r \in R \setminus \mathfrak{M} = R^*$. В резултат, $u_r = \sum_{i=1}^{r-1} (1 - \mu_r)^{-1} \mu_i u_i \in Ru_1 + \dots + Ru_{r-1}$ противоречи на минималността на пораждащата система u_1, \dots, u_r на M като R -модул и доказва, че $M = 0$.

В общия случай, от $N + \mathfrak{M}M = M$ следва, че фактор-модулът

$$M/N = (N + \mathfrak{M}M)/N = \mathfrak{M}(M/N).$$

По-точно, за произволни $\mu_i \in \mathfrak{M}$, $m_i \in M$, $1 \leq i \leq s$ и $n \in N$ имаме

$$n + \sum_{i=1}^s \mu_i m_i + N = \sum_{i=1}^s \mu_i (m_i + N),$$

така че $(N + \mathfrak{M}M)/N \subseteq \mathfrak{M}(M/N)$. Обратно, всяко

$$\sum_{i=1}^s \mu_i (m_i + N) = \sum_{i=1}^s \mu_i m_i + N \in (\mathfrak{M}M + N)/N$$

и $\mathfrak{M}(M/N) \subseteq (N + \mathfrak{M}M)/N$. Съгласно частния случай, от $\mathfrak{M}(M/N) = M/N$ следва $M/N = 0$ или $M = N$.

(ii) За $\forall x \in M$ съществуват $r_i + \mathfrak{M} \in R/\mathfrak{M}$, така че

$$x + \mathfrak{M}M = \sum_{i=1}^n (r_i + \mathfrak{M})(x_i + \mathfrak{M}M) = \sum_{i=1}^n r_i x_i + \mathfrak{M}M.$$

Следователно $M \subseteq \sum_{i=1}^n Rx_i + \mathfrak{M}M \subseteq M$ и $M = \sum_{i=1}^n Rx_i + \mathfrak{M}M$. Прилагаме (i)

към $N = \sum_{i=1}^n Rx_i$ и получаваме, че $M = N = \sum_{i=1}^n Rx_i$, Q.E.D.

СЛЕДСТВИЕ 12.4. Ако R е локален пръстен с максимален идеал \mathfrak{M} и $\mathfrak{M} = \mathfrak{M}^2$, то $\mathfrak{M} = 0$ и R е поле.

Доказателство: Прилагаме частния случай на Лема 12.3 (i) с $N = 0$ за $M = \mathfrak{M}$ и получаваме, че $\mathfrak{M} = 0$. Оттук $R = R/\mathfrak{M}$ е поле, Q.E.D.

СЛЕДСТВИЕ 12.5. Ако R е локален пръстен с максимален идеал \mathfrak{M} и

$$\mathfrak{M}/\mathfrak{M}^2 = l_{R/\mathfrak{M}}(x_1 + \mathfrak{M}^2, \dots, x_n + \mathfrak{M}^2)$$

е R/\mathfrak{M} -линейната обвивка на $x_1 + \mathfrak{M}^2, \dots, x_n + \mathfrak{M}^2$, то

$$\mathfrak{M} = \langle x_1, \dots, x_n \rangle = \sum_{i=1}^n Rx_i$$

се поражда от x_1, \dots, x_n като R -модул.

Доказателство: Прилагаме Лема 12.3 (ii) към R -модула $M = \mathfrak{M}$ и получаваме, че максималният идеал $\mathfrak{M} = \sum_{i=1}^n Rx_i$ се поражда от x_1, \dots, x_n , Q.E.D.

ОПРЕДЕЛЕНИЕ 12.6. Идеалът \mathfrak{A} на комутативен пръстен с единица R е неприводим, ако за произволни идеали \mathfrak{B} и \mathfrak{C} в R с $\mathfrak{A} = \mathfrak{B} \cap \mathfrak{C}$ следва $\mathfrak{A} = \mathfrak{B}$ или $\mathfrak{A} = \mathfrak{C}$.

ЗАДАЧА 12.7. Да се докаже, че за всяко просто p и всяко естествено n идеалът $(p^n) = p^n\mathbb{Z} \triangleleft \mathbb{Z}$ е неприводим.

ОПРЕДЕЛЕНИЕ 12.8. Идеалът \mathfrak{q} на комутативния пръстен с единица R е примарен, ако за произволни $a \in R \setminus \mathfrak{q}$ и $b \in R$ с $ab \in \mathfrak{q}$ следва $b^m \in \mathfrak{q}$ за някое $m \in \mathbb{N}$.

ЗАДАЧА 12.9. Нека \mathbb{Z} е пръстенът на целите числа, а K е произволно поле. Да се докаже, че:

(i) идеалът $\mathfrak{q} \triangleleft \mathbb{Z}$ е примарен тогава и само тогава, когато $\mathfrak{q} = (p^n)$ за просто p и естествено n ;

(ii) идеалът $\mathfrak{q} \triangleleft K[x]$ е примарен тогава и само тогава, когато $\mathfrak{q} = (p(x)^n)$ за неразложим над K полином $p(x) \in K[x]$ и $n \in \mathbb{N}$.

ЗАДАЧА 12.10. Да се опишат неприводимите идеали в пръстена \mathbb{Z} на целите числа.

ТВЪРДЕНИЕ 12.11. Ако R е нютеров комутативен пръстен с единица, то всеки неприводим идеал \mathfrak{A} в R е примарен.

Доказателство: Ако $\mathfrak{A} \triangleleft R$ е неприводим идеал, то нулевият идеал $\bar{0}$ във фактор-пръстена R/\mathfrak{A} е неприводим. По-точно, ако $\bar{\mathfrak{B}} \triangleleft R/\mathfrak{A}$ и $\bar{\mathfrak{C}} \triangleleft R/\mathfrak{A}$ са идеали с $\bar{\mathfrak{B}} \cap \bar{\mathfrak{C}} = \bar{0}$, то повдиганията

$$\mathfrak{B} = \{b \in R \mid b + \mathfrak{A} \in \bar{\mathfrak{B}}\} \quad \text{и} \quad \mathfrak{C} = \{c \in R \mid c + \mathfrak{A} \in \bar{\mathfrak{C}}\}$$

са идеали в R с $\mathfrak{B} \cap \mathfrak{C} \subseteq \mathfrak{A}$. Вземайки предвид $\mathfrak{A} \subseteq \mathfrak{B}$ и $\mathfrak{A} \subseteq \mathfrak{C}$, стигаме до извода, че $\mathfrak{B} \cap \mathfrak{C} = \mathfrak{A}$. Съгласно неприводимостта на \mathfrak{A} , оттук следва $\mathfrak{A} = \mathfrak{B}$ или $\mathfrak{A} = \mathfrak{C}$. В резултат, $\bar{\mathfrak{B}} = \bar{0}$ или, съответно $\bar{\mathfrak{C}} = \bar{0}$.

Достатъчно е да докажем, че ако $\bar{0} \triangleleft R/\mathfrak{A}$ е неприводим идеал, то $\bar{0}$ е примарен. Тогава от $ab \in \mathfrak{A}$ с $a \in R \setminus \mathfrak{A}$, $b \in R$ следва $(a + \mathfrak{A})(b + \mathfrak{A}) = \bar{0}$ с $a + \mathfrak{A} \neq \bar{0}$. Примарността на $\bar{0} \triangleleft R/\mathfrak{A}$ дава $(b + \mathfrak{A})^m = \bar{0}$ за някое $m \in \mathbb{N}$. Следователно $b^m \in \mathfrak{A}$ и идеалът $\mathfrak{A} \triangleleft R$ е примарен.

За да изведем примарността на нулевия идеал $\bar{0} \triangleleft \bar{R} = R/\mathfrak{A}$ от неговата неприводимост, фиксираме $\bar{a} \neq \bar{0}$ и $\bar{b} \in \bar{R}$ с $\bar{a}\bar{b} = \bar{0}$. Разглеждаме анулаторите

$$\text{Ann}_{\bar{R}}(\bar{b}^i) = \{\bar{r} \in \bar{R} \mid \bar{r}\bar{b}^i = \bar{0}\}$$

на естествените степени \bar{b}^i на $\bar{b} = b + \mathfrak{A}$. Непосредствено се проверява, че те образуват ненамаляваща редица

$$\text{Ann}_{\bar{R}}(\bar{b}) \subseteq \text{Ann}_{\bar{R}}(\bar{b}^2) \subseteq \dots \subseteq \text{Ann}_{\bar{R}}(\bar{b}^m) \subseteq \text{Ann}_{\bar{R}}(\bar{b}^{m+1}) \subseteq \dots$$

от идеали в нютеровия пръстен \bar{R} . Обединението $A = \cup_{i=1}^{\infty} \text{Ann}_{\bar{R}}(\bar{b}^i)$ на тези идеали е крайно породен идеал в \bar{R} . Ако $A = \bar{R}\bar{r}_1 + \dots + \bar{R}\bar{r}_k$ с $\bar{r}_j \in \text{Ann}_{\bar{R}}(\bar{b}^{m_j})$ за някои $m_j \in \mathbb{N}$, $1 \leq j \leq k$ и $m = \max(m_1, \dots, m_k)$, то $A \subseteq \text{Ann}_{\bar{R}}(\bar{b}^m) \subseteq A$, откъдето $A = \text{Ann}_{\bar{R}}(\bar{b}^m)$ и редицата $\text{Ann}_{\bar{R}}(\bar{b}^m) = \text{Ann}_{\bar{R}}(\bar{b}^{m+2}) = \dots$ се стабилизира от известно място нататък. Достатъчно е да проверим, че идеалите $\langle \bar{a} \rangle \triangleleft \bar{R}$ и $\langle \bar{b}^m \rangle \triangleleft \bar{R}$ имат нулево сечение $\langle \bar{a} \rangle \cap \langle \bar{b}^m \rangle = \bar{0}$. Тогава от неприводимостта на $\bar{0} \triangleleft \bar{R}$ и $\bar{a} \neq \bar{0}$ следва $\bar{b}^m = \bar{0}$. С това установяваме примарността на $\bar{0} \triangleleft \bar{R}$ и доказваме твърдението. Ако допуснем съществуването на ненулев елемент

$$\bar{0} \neq \bar{x} = \bar{a}\bar{r}_1 = \bar{b}^m \bar{r}_2 \in \langle \bar{a} \rangle \cap \langle \bar{b}^m \rangle,$$

то почленното умножение с \bar{b} дава $\bar{0} = \bar{a}\bar{b}\bar{r}_1 = \bar{b}^{m+1}\bar{r}_2$. Това означава, че $\bar{r}_2 \in \text{Ann}_{\bar{R}}(\bar{b}^{m+1}) = \text{Ann}_{\bar{R}}(\bar{b}^m)$ и $\bar{x} = \bar{b}^m\bar{r}_2 = \bar{0}$. Противоречието доказва $\langle \bar{a} \rangle \cap \langle \bar{b}^m \rangle = \bar{0}$, откъдето $\bar{b}^m = \bar{0}$, съгласно неприводимостта на $\bar{0} \triangleleft \bar{R}$, Q.E.D.

Твърдение 12.12. *Всеки идеал \mathfrak{A} в нютеров комутативен пръстен с единица R се разлага в крайно сечение*

$$\mathfrak{A} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$$

на примарни идеали \mathfrak{q}_i в R .

Доказателство: Съгласно Твърдение 12.11, достатъчно е да докажем, че всеки идеал $\mathfrak{A} \triangleleft R$ се разлага в крайно сечение $\mathfrak{A} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$ на неприводими идеали $\mathfrak{q}_i \triangleleft R$. Допускаме противното и разглеждаме множеството $\Sigma \neq \emptyset$ на идеалите в R , които не се разлагат като крайно сечение на неприводими идеали. Всяко линейно наредено подмножество $\{\mathfrak{B}_\alpha\}_{\alpha \in A} \subseteq \Sigma$ има точна горна граница $\mathfrak{B}_\infty := \cup_{\alpha \in A} \mathfrak{B}_\alpha \in \Sigma$. По-точно, $\mathfrak{B}_\infty = \mathfrak{B}_N$ за някое $N \in \mathbb{N}$, съгласно нютеровостта на R . Отгук $\mathfrak{B}_\infty \in \Sigma$. По Лемата на Zorn, съществува максимален елемент $\mathfrak{B}_o \in \Sigma$. Условието $\mathfrak{B}_o \in \Sigma$ изисква \mathfrak{B}_o да не е неприводим. Следователно съществуват идеали $\mathfrak{A}_1 \triangleleft R$ и $\mathfrak{A}_2 \triangleleft R$ с $\mathfrak{B}_o = \mathfrak{A}_1 \cap \mathfrak{A}_2$, $\mathfrak{B}_o \subsetneq \mathfrak{A}_1$, $\mathfrak{B}_o \subsetneq \mathfrak{A}_2$. Съгласно максималността на $\mathfrak{B}_o \in \Sigma$, идеалите \mathfrak{A}_1 и \mathfrak{A}_2 имат крайни разлагания $\mathfrak{A}_1 = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_l$ и $\mathfrak{A}_2 = \mathfrak{q}_{l+1} \cap \dots \cap \mathfrak{q}_m$ в сечение на неприводими идеали $\mathfrak{q}_j \triangleleft R$. В резултат, $\mathfrak{B}_o = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_l \cap \mathfrak{q}_{l+1} \cap \dots \cap \mathfrak{q}_m$ е крайно сечение на неприводими идеали $\mathfrak{q}_j \triangleleft R$, противно на $\mathfrak{B}_o \in \Sigma$. Това опровергава допускането $\Sigma \neq \emptyset$ и доказва твърдението, Q.E.D.

Задача 12.13. *Нека \mathbb{Z} е пръстенът на целите числа, а K е произволно поле. Да се докаже, че:*

(i) *ако естественото число $n \geq 2$ има разлагане $n = p_1^{a_1} \dots p_k^{a_k}$, $a_i \in \mathbb{N}$ в произведение от прости множители p_i , то идеалът $(n) \triangleleft \mathbb{Z}$, породен от n има примарно разлагане*

$$(n) = (p_1^{a_1}) \cap \dots \cap (p_k^{a_k}).$$

(ii) *ако полиномът $f(x) \in K[x]$ има разлагане $f(x) = p_1(x)^{a_1} \dots p_k(x)^{a_k}$, $a_i \in \mathbb{N}$ в произведение от неразложими над K множители $p_i(x) \in K[x]$, то идеалът $(f(x)) \triangleleft K[x]$, породен от $f(x)$ има примарно разлагане*

$$(f(x)) = (p_1(x)^{a_1}) \cap \dots \cap (p_k(x)^{a_k}).$$

ЛЕМА 12.14. *За произволен идеал \mathfrak{A} в нютеров комутативен пръстен с единица R съществува естествено число $k \in \mathbb{N}$, така че*

$$r(\mathfrak{A})^k \subseteq \mathfrak{A} \subseteq r(\mathfrak{A})$$

за радикала $r(\mathfrak{A}) \triangleleft R$ на \mathfrak{A} .

Доказателство: Идеалът $r(\mathfrak{A}) = Rx_1 + \dots + Rx_n$ е крайно породен, съгласно нютеровостта на R . От $x_i \in r(\mathfrak{A})$ за $\forall 1 \leq i \leq n$ следва съществуването на естествени числа l_i с $x_i^{l_i} \in \mathfrak{A}$. За $l = \max(l_1, \dots, l_n)$ твърдим, че $r(\mathfrak{A})^{nl} \subseteq \mathfrak{A}$. Да забележим, че

$$r(\mathfrak{A})^{nl} = \sum_{d=(d_1, \dots, d_n) \in (\mathbb{Z}^{\geq 0})^n, d_1 + \dots + d_n = nl} Rx_1^{d_1} \dots x_n^{d_n}.$$

Всяка наредена n -торка $d = (d_1, \dots, d_n) \in (\mathbb{Z}^{\geq 0})^n$ с $d_1 + \dots + d_n = nl$ има компонента $d_j \geq l$, защото в противен случай

$$nl = d_1 + \dots + d_n \leq n(l-1) \quad \text{за} \quad \forall d_i \leq l-1$$

води до противоречие. От $d_j \geq l \geq l_j$ следва $x_j^{d_j} \in \mathfrak{A}$, откъдето $x_1^{d_1} \dots x_j^{d_j} \dots x_n^{d_n} \in \mathfrak{A}$ за $\forall d = (d_1, \dots, d_n) \in (\mathbb{Z}^{\geq 0})^n$ с $d_1 + \dots + d_n = nl$. Това доказва съществуването на $k = nl$ с $r(\mathfrak{A})^k \subseteq r(\mathfrak{A})$, Q.E.D.

СЛЕДСТВИЕ 12.15. (i) Нека R е нютеров комутативен пръстен с единица, а \mathfrak{q}_1 и \mathfrak{q}_2 са примарни идеали в R с общ радикал $r(\mathfrak{q}_1) = r(\mathfrak{q}_2)$. Тогава сечението $\mathfrak{q}_1 \cap \mathfrak{q}_2$ е примарен идеал с радикал $r(\mathfrak{q}_1) = r(\mathfrak{q}_2)$.

(ii) Всеки идеал \mathfrak{A} в нютеров комутативен пръстен с единица R е крайно сечение $\mathfrak{A} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$ на примарни идеали \mathfrak{q}_i с различни прости радикали $r(\mathfrak{q}_i)$.

Доказателство: (i) Да напомним, че радикалът $r(\mathfrak{A})$ на идеал $\mathfrak{A} \triangleleft R$ е множеството на онези $r \in R$, за които съществува $m \in \mathbb{N}$ с $r^m \in \mathfrak{A}$. Твърдим, че ако идеалът \mathfrak{q} е примарен, то радикалът му $r(\mathfrak{q}) \triangleleft R$ е прост.

Да допуснем обратното и да разгледаме $a, b \in R \setminus r(\mathfrak{q})$ с $ab \in r(\mathfrak{q})$. Тогава съществува $k \in \mathbb{N}$ с $a^k b^k \in \mathfrak{q}$. От $\mathfrak{q} \subseteq r(\mathfrak{q})$ следва $a \notin \mathfrak{q}$, откъдето $b^k \in \mathfrak{q}$, съгласно примарността на \mathfrak{q} . Това противоречи на $b \notin r(\mathfrak{q})$ и доказва простотата на $r(\mathfrak{q})$. Ако $a, b \in R$ имат произведение $ab \in \mathfrak{q}_1 \cap \mathfrak{q}_2 \subseteq r(\mathfrak{q}_1) = r(\mathfrak{q}_2)$, то $a \in r(\mathfrak{q}_1)$ или $b \in r(\mathfrak{q}_1)$, съгласно простотата на $r(\mathfrak{q}_1) \triangleleft R$. След евентуална замяна на a с b имаме $a \in r(\mathfrak{q}_1)$. По Лема 12.14 съществуват естествени числа k_i с $r(\mathfrak{q})^{k_i} \subseteq \mathfrak{q}_i$ за $1 \leq i \leq 2$. Ако $k = \max(k_1, k_2)$, то $a^k \in r(\mathfrak{q}_1)^k = r(\mathfrak{q}_2)^k \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2$ и идеалът $\mathfrak{q}_1 \cap \mathfrak{q}_2 \triangleleft R$ е примарен.

За произволно крайно сечение $\mathfrak{A} = \mathfrak{A}_1 \cap \dots \cap \mathfrak{A}_n$ на идеали $\mathfrak{A}_i \triangleleft R$ твърдим, че радикалът $r(\mathfrak{A}) = r(\mathfrak{A}_1) \cap \dots \cap r(\mathfrak{A}_n)$ на \mathfrak{A} е сечение на радикалите $r(\mathfrak{A}_i)$ на \mathfrak{A}_i . По-точно, ако $r^k \in \mathfrak{A}$ за някое $r \in R$ и някое $k \in \mathbb{N}$, то $r^k \in \mathfrak{A}_i$ за $\forall 1 \leq i \leq n$ и $r \in r(\mathfrak{A}_1) \cap \dots \cap r(\mathfrak{A}_n)$. Това доказва, че $r(\mathfrak{A}) \subseteq r(\mathfrak{A}_1) \cap \dots \cap r(\mathfrak{A}_n)$. Обратно, ако $r \in r(\mathfrak{A}_1) \cap \dots \cap r(\mathfrak{A}_n)$, то за всяко $1 \leq i \leq n$ съществува $k_i \in \mathbb{N}$ с $r^{k_i} \in \mathfrak{A}_i$. Ако $k = \max(k_1, \dots, k_n)$, то $r^k \in \mathfrak{A}_1 \cap \dots \cap \mathfrak{A}_n = \mathfrak{A}$ и $r(\mathfrak{A}_1) \cap \dots \cap r(\mathfrak{A}_n) \subseteq r(\mathfrak{A})$. В частност, радикалът $r(\mathfrak{q}_1 \cap \mathfrak{q}_2) = r(\mathfrak{q}_1) \cap r(\mathfrak{q}_2) = r(\mathfrak{q}_1) = r(\mathfrak{q}_2)$ и $\mathfrak{q}_1 \cap \mathfrak{q}_2$ съвпада с общия радикал $r(\mathfrak{q}_1) = r(\mathfrak{q}_2)$ на \mathfrak{q}_1 и \mathfrak{q}_2 .

(ii) Съгласно Твърдение 12.12, произволен идеал \mathfrak{A} в нютеров комутативен пръстен с единица R се разлага в крайно сечение $\mathfrak{A} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$ на примарни идеали $\mathfrak{q}_j \triangleleft R$. Въз основа на (i), можем да считаме, че радикалите $r(\mathfrak{q}_1), \dots, r(\mathfrak{q}_m)$ са различни, Q.E.D.

ЗАДАЧА 12.16. Нека $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$ е разлагането на идеал $I \triangleleft \bar{k}[x_1, \dots, x_n]$ в сечение на примарни идеали $\mathfrak{q}_i \triangleleft \bar{k}[x_1, \dots, x_n]$, а $V = Z(I)$ е афинното многообразие, определено от I . Да се докаже, че V се разлага в обединение

$$V = Z(r(\mathfrak{q}_1)) \cup \dots \cup Z(r(\mathfrak{q}_m))$$

на неприводимите си подмногообразия $Z(r(\mathfrak{q}_j))$.

Упътване: Проверете, че $Z(I) = Z(r(I))$. За произволни идеали J_1 и J_2 в $\bar{k}[x_1, \dots, x_n]$ докажете, че $Z(J_1 \cap J_2) = Z(J_1) \cup Z(J_2)$ и приложете това свойство към $r(I) = r(\mathfrak{q}_1) \cap \dots \cap r(\mathfrak{q}_m)$.

ЗАДАЧА 12.17. Нека I е идеал в полиномиалния пръстен $\bar{k}[x_1, \dots, x_n]$, а $Z(I) = Z_1 \cup \dots \cup Z_m$ е разлагане на афинното многообразие $Z(V) \subseteq \bar{k}^n$, породено от I в обединение на неприводими подмногообразия, наречени компоненти. Да се докаже, че радикалът $r(I)$ на I има разлагане

$$r(I) = I(Z_1) \cap \dots \cap I(Z_m)$$

в сечение на прости идеали $I(Z_j) \triangleleft \bar{k}[x_1, \dots, x_n]$.

СЛЕДСТВИЕ 12.18. Нека $\mathfrak{A} \neq 0$ е ненулев идеал в нютерова локална област R с размерност на Krull 1 и максимален идеал \mathfrak{M} . Тогава:

- (i) идеалът \mathfrak{A} е примарен;
(ii) радикалът $r(\mathfrak{A}) = \mathfrak{M}$ на \mathfrak{A} съвпада с максималния идеал \mathfrak{M} на R ;
(iii) съществува естествено число k , така че $\mathfrak{M}^k \subseteq \mathfrak{A} \subseteq \mathfrak{M}$.

Доказателство: Размерността на Krull на R е 1 тогава и само тогава, когато всеки ненулев прост идеал в R е максимален. Ако $0 \neq \mathfrak{A} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$ е сечение на примарни идеали $\mathfrak{q}_i \triangleleft R$ с прости радикали $r(\mathfrak{q}_i) \triangleleft R$, то $\mathfrak{q}_i \subseteq r(\mathfrak{q}_i) \neq 0$. Следователно $r(\mathfrak{q}_1) = \dots = r(\mathfrak{q}_m) = \mathfrak{M}$ и $\mathfrak{A} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$ е примарен идеал в R , съгласно Следствие 12.15. Условието (iii) следва от Лема 12.14, Q.E.D.

Нека R е локален пръстен с максимален идеал \mathfrak{M} . Тогава $\mathfrak{M}/\mathfrak{M}^2$ е идеал във фактор-пръстена R/\mathfrak{M}^2 и, в частност, $(\mathfrak{M}/\mathfrak{M}^2, +)$ е подгрупа на адитивната група $(R/\mathfrak{M}^2, +)$ на фактор-пръстена R/\mathfrak{M}^2 . Твърдим, че съответствието

$$R/\mathfrak{M} \times \mathfrak{M}/\mathfrak{M}^2 \longrightarrow \mathfrak{M}/\mathfrak{M}^2,$$

$$(r + \mathfrak{M})(x + \mathfrak{M}^2) = rx + \mathfrak{M}^2 \quad \text{за } \forall r \in R, \forall x \in \mathfrak{M}$$

задава структура на R/\mathfrak{M} -линейно пространство върху $\mathfrak{M}/\mathfrak{M}^2$. Преди всичко, умножението на елементи $x + \mathfrak{M}^2$ на адитивната група $\mathfrak{M}/\mathfrak{M}^2$ с елементи $r + \mathfrak{M}$ на полето R/\mathfrak{M} е коректно зададено. Ако $r + \mathfrak{M} = r_1 + \mathfrak{M}$ с $r, r_1 \in R$ и $x + \mathfrak{M}^2 = x_1 + \mathfrak{M}^2$ с $x, x_1 \in \mathfrak{M}$, то $rx + \mathfrak{M}^2 = r_1x_1 + \mathfrak{M}^2$, защото

$$r_1x_1 - rx = (r_1x_1 - r_1x) + (r_1x - r) = r_1(x_1 - x) + (r_1 - r)x \in \mathfrak{M}^2.$$

Непосредствено проверяваме дистрибутивния закон над скаларен множител

$$\begin{aligned} [(r + \mathfrak{M}) + (s + \mathfrak{M})](x + \mathfrak{M}^2) &= (r + s + \mathfrak{M})(x + \mathfrak{M}^2) = (r + s)x + \mathfrak{M}^2 = \\ &= rx + sx + \mathfrak{M}^2 = (rx + \mathfrak{M}^2) + (sx + \mathfrak{M}^2) = (r + \mathfrak{M})(x + \mathfrak{M}^2) + (s + \mathfrak{M})(x + \mathfrak{M}^2), \end{aligned}$$

дистрибутивния закон над векторен множител

$$\begin{aligned} (r + \mathfrak{M})[(x + \mathfrak{M}^2) + (y + \mathfrak{M}^2)] &= (r + \mathfrak{M})(x + y + \mathfrak{M}^2) = r(x + y) + \mathfrak{M}^2 = \\ &= rx + ry + \mathfrak{M}^2 = (rx + \mathfrak{M}^2) + (ry + \mathfrak{M}^2) = (r + \mathfrak{M})(x + \mathfrak{M}^2) + (r + \mathfrak{M})(y + \mathfrak{M}^2), \end{aligned}$$

както и останалите две аксиоми

$$\begin{aligned} [(r + \mathfrak{M})(s + \mathfrak{M})](x + \mathfrak{M}^2) &= (rs + \mathfrak{M})(x + \mathfrak{M}^2) = (rs)x + \mathfrak{M}^2 = \\ &= r(sx) + \mathfrak{M}^2 = (r + \mathfrak{M})(sx + \mathfrak{M}^2) = (r + \mathfrak{M})[(s + \mathfrak{M})(x + \mathfrak{M}^2)] \quad \text{и} \\ (1_R + \mathfrak{M})(x + \mathfrak{M}^2) &= 1_Rx + \mathfrak{M}^2 = x + \mathfrak{M}^2 \end{aligned}$$

за произволни $r, s \in R$, $x, y \in \mathfrak{M}$. С това проверихме, че ако R е локален пръстен с максимален идеал \mathfrak{M} , то $\mathfrak{M}/\mathfrak{M}^2$ е линейно пространство над полето R/\mathfrak{M} .

ТВЪРДЕНИЕ 12.19. Нека R е нютерова локална област с размерност на Krull 1. В такъв случай, R е пръстен на дискретно нормиране тогава и само тогава, когато $\mathfrak{M}/\mathfrak{M}^2$ е 1-мерно линейно пространство над полето R/\mathfrak{M} .

Доказателство: Нека R е пръстен на дискретно нормиране с локален параметър t . Съгласно Определение 3.14 и забележка след него, локалният параметър t принадлежи на максималния идеал \mathfrak{M} на R , така че главният идеал $\langle t \rangle = tR \triangleleft R$, породен от t се съдържа в \mathfrak{M} . Всеки ненулев елемент $z \in R \setminus \{0\}$ има единствено представяне $z = ut^m$ с $u \in R^*$ и $m \in \mathbb{Z}^{\geq 0}$. Ако $z = ut^m \in \mathfrak{M}$, то $m \geq 1$ и $z \in \langle t \rangle$, защото в противен случай $z = u \in R^* = R \setminus \mathfrak{M}$. Следователно максималният идеал $\mathfrak{M} = \langle t \rangle = tR$ на R е главен и се поражда от произволен локален параметър t на R .

Твърдим, че умножението

$$\begin{aligned} \mu_t : R/\mathfrak{M} = R/tR &\longrightarrow tR/t^2R = \mathfrak{M}/\mathfrak{M}^2 \\ \mu_t(r + \mathfrak{M}) &= tr + \mathfrak{M}^2 \end{aligned}$$

с t е изоморфизъм на R/\mathfrak{M} -линейни пространства, така че $\dim_{R/\mathfrak{M}}(\mathfrak{M}/\mathfrak{M}^2) = 1$. Преди всичко, изображението μ_t е коректно зададено, защото от $r + \mathfrak{M} = r_1 + \mathfrak{M}$ следва $tr - tr_1 = t(r - r_1) \in \mathfrak{M}^2$. Съгласно

$$\begin{aligned} \mu_t((r + \mathfrak{M}) + (s + \mathfrak{M})) &= \mu_t(r + s + \mathfrak{M}) = t(r + s) + \mathfrak{M}^2 = \\ &= tr + ts + \mathfrak{M}^2 = (tr + \mathfrak{M}^2) + (ts + \mathfrak{M}^2) = \mu_t(r + \mathfrak{M}) + \mu_t(s + \mathfrak{M}) \end{aligned}$$

и

$$\begin{aligned} \mu_t((\rho + \mathfrak{M})(r + \mathfrak{M})) &= \mu_t(\rho r + \mathfrak{M}) = t(\rho r) + \mathfrak{M}^2 = \\ &= \rho(tr) + \mathfrak{M}^2 = (\rho + \mathfrak{M})(tr + \mathfrak{M}^2) = (\rho + \mathfrak{M})\mu_t(r + \mathfrak{M}), \end{aligned}$$

изображението μ_t е R/\mathfrak{M} -линейно. За взаимната еднозначност на μ_t да отбележим, че всеки елемент на $\mathfrak{M}/\mathfrak{M}^2 = tR/t^2R$ е от вида $tr + t^2R = tr + \mathfrak{M}^2$ за някое $r \in R$. Ако $tr + \mathfrak{M}^2 = tr_1 + \mathfrak{M}^2$ за $r, r_1 \in R$, то $t(r - r_1) \in \mathfrak{M}^2 = t^2R$ или съществува $s \in R$ с $t(r - r_1) = t^2s$. В областта R от $t(r - r_1 - ts) = 0$ с $t \neq 0$ следва $r - r_1 - ts$, така че $r - r_1 = ts \in \mathfrak{M}$ и $r + \mathfrak{M} = r_1 + \mathfrak{M}$. Следователно за всеки елемент $tr + \mathfrak{M}^2 = tr_1 + \mathfrak{M}^2$ на $\mathfrak{M}/\mathfrak{M}^2$ съществува единствен праобраз $r + \mathfrak{M} = r_1 + \mathfrak{M}$ от R/\mathfrak{M} с

$$\mu_t(r + \mathfrak{M}) = tr + \mathfrak{M}^2 = tr_1 + \mathfrak{M}^2 = \mu_t(r_1 + \mathfrak{M})$$

и изображението $\mu_t^{-1} : \mathfrak{M}/\mathfrak{M}^2 \rightarrow R/\mathfrak{M}$ е коректно зададено. С това установяваме, че $\mu_t : R/\mathfrak{M} \rightarrow \mathfrak{M}/\mathfrak{M}^2$ е R/\mathfrak{M} -линейен изоморфизъм.

Обратно, нека $\mathfrak{M}/\mathfrak{M}^2$ е 1-мерно линейно пространство над полето R/\mathfrak{M} . Съгласно Лемата на Накауама (ii) (Лема 12.3(ii)) с $M = \mathfrak{M}$, произволен елемент $t \in \mathfrak{M} \setminus \mathfrak{M}^2$ поражда $\mathfrak{M} = tR$ като идеал в R . По Следствие 12.18(iii), за произволен ненулев идеал \mathfrak{A} в нютерова локална област R с размерност на Krull 1 съществува $k \in \mathbb{N}$ с $\mathfrak{M}^k \subseteq \mathfrak{A} \subseteq \mathfrak{M}$. Без ограничение на общността ще считаме, че k е минималното естествено число с $\mathfrak{M}^k \subseteq \mathfrak{A}$, т.е. $\mathfrak{M}^{k-1} \not\subseteq \mathfrak{A}$. Твърдим, че $\mathfrak{A} = \mathfrak{M}^k = t^kR$. Ако допуснем, че $\mathfrak{M}^k \subsetneq \mathfrak{A}$, то съществува $x \in \mathfrak{A} \setminus \mathfrak{M}^k$. Естествените степени

$$\mathfrak{M} \supseteq \mathfrak{M}^2 \dots \supseteq \mathfrak{M}^{k-1} \supseteq \mathfrak{M}^k \supseteq \mathfrak{M}^{k+1} \supseteq \dots$$

на максималния идеал \mathfrak{M} на R образуват строго намаляваща редица. По-точно, допускането $t^iR = \mathfrak{M}^i = \mathfrak{M}^{i+1} = t^{i+1}R$ за някое $i \in \mathbb{N}$ води до съществуване на $r \in R$ с $t^i = t^{i+1}r$. В областта R , от $t^i(1 - tr) = 0$ следва $1 = tr$, така че $t \in R^*$ и $\mathfrak{M} = tR = R$. Противоречието доказва $\mathfrak{M}^i \supsetneq \mathfrak{M}^{i+1}$ за $\forall i \in \mathbb{N}$. От $x \notin \mathfrak{M}^k$ следва $x \notin \mathfrak{M}^N$ за всички естествени $N \geq k$. Следователно множеството

$$\mathbb{N}_x := \{n \in \mathbb{N} \mid x \in \mathfrak{M}^n\} \subseteq \{1, 2, \dots, k-1\}$$

е ограничено отгоре и има максимален елемент $n \leq k-1$, т.е. $x \in \mathfrak{M}^n = t^nR$, $x \notin \mathfrak{M}^{n+1} = t^{n+1}R$. Оттук получаваме съществуването на $u \in R \setminus tR = R \setminus \mathfrak{M} = R^*$ с $x = t^nu$. В резултат, от $t^n = xu^{-1} \in \mathfrak{A}$ следва $\mathfrak{M}^{k-1} \subseteq \mathfrak{M}^n = t^nR \subseteq \mathfrak{A}$, което противоречи на предположението $\mathfrak{M}^{k-1} \not\subseteq \mathfrak{A}$. Следователно $\mathfrak{A} = \mathfrak{M}^k = t^kR$. За произволен елемент $x \in R \setminus \{0\}$ идеалът $\langle x \rangle = xR = t^kR = \mathfrak{M}^k$ за някое естествено k . В резултат, съществуват $u, v \in R$ с $x = t^ku$, $t^k = xv$. Сега $t^k - t^kuv = t^k(1 - uv) = 0$ с $t \neq 0$ в областта R дава $1 = uv$, откъдето $u, v \in R^*$. Остава да порверим неразложимостта на t , за да получим, че R удовлетворява условията от Определение 3.14 за пръстен на дискретно нормиране. Наистина, допускането $t = t_1t_2$ с $t_1, t_2 \in R \setminus R^* = \mathfrak{M} = tR$ води до $t_i = tr_i$ за някои $r_i \in R$, $1 \leq i \leq 2$. В резултат, от $t = t^2r_1r_2$ следва $tr_1r_2 = 1$, така че $t \in R^*$ и $\mathfrak{M} = tR = R$. Противоречието доказва неразложимостта на t , Q.E.D.

ТЕОРЕМА 15. *Нека $V \subset \bar{k}^n$ е афинна крива, а p е точка от V . В такъв случай, точката p е гладка тогава и само тогава, когато локалният пръстен $\mathcal{O}_p(V)$ на p във V е пръстен на дискретно нормиране.*

Доказателство: Изображението

$$\text{grad}_p : \bar{k}[x_1, \dots, x_n] \longrightarrow \bar{k}^n,$$

$$\text{grad}_p(f(x_1, \dots, x_n)) = \left(\frac{\partial f}{\partial x_1}(p), \dots, \frac{\partial f}{\partial x_n}(p) \right) \quad \text{за } \forall f(x_1, \dots, x_n) \in \bar{k}[x_1, \dots, x_n]$$

е \bar{k} -линейно, т.е. $\text{grad}_p(f + g) = \text{grad}_p(f) + \text{grad}_p(g)$ и $\text{grad}_p(af) = a\text{grad}_p(f)$ за $\forall f, g \in \bar{k}[x_1, \dots, x_n], \forall a \in \bar{k}$. За произволна фиксирана точка $p = (p_1, \dots, p_n) \in V \subseteq \bar{k}^n$ разглеждаме максималния идеал

$$\mathfrak{N}_p = \langle x_1 - p_1, \dots, x_n - p_n \rangle = \sum_{i=1}^n (x_i - p_i) \bar{k}[x_1, \dots, x_n]$$

на p в $\bar{k}[x_1, \dots, x_n]$ и ограничението

$$\text{grad}_p : \mathfrak{N}_p \longrightarrow \bar{k}^n,$$

$$\text{grad}_p \left(\sum_{i=1}^n (x_i - p_i) g_i(x_1, \dots, x_n) \right) = (g_1(p), \dots, g_n(p)).$$

Ядрото

$$\begin{aligned} \ker(\text{grad}_p|_{\mathfrak{N}_p}) &= \left\{ \sum_{i=1}^n (x_i - p_i) g_i(x_1, \dots, x_n) \mid g_i(p) = 0 \quad \text{за } \forall 1 \leq i \leq n \right\} = \\ &= \left\{ \sum_{i=1}^n (x_i - p_i) g_i(x_1, \dots, x_n) \mid g_i \in \mathfrak{N}_p \right\} = \mathfrak{N}_p^2, \end{aligned}$$

а образът $\text{im}(\text{grad}_p|_{\mathfrak{N}_p}) = \bar{k}^n$, защото за всяко $1 \leq i \leq n$ имаме $\text{grad}_p(x_i - p_i) = (0, \dots, 0, 1, 0, \dots, 0) = e_i$ за наредените n -торки e_i с единствен ненулев елемент 1 в i -та позиция и e_1, \dots, e_n образуват базис на \bar{k}^n . Епиморфизмът

$$\text{grad}_p : (\mathfrak{N}_p, +) \longrightarrow (\bar{k}^n, +)$$

на адитивните групи индуцира изоморфизъм

$$\overline{\text{grad}_p} : (\mathfrak{N}_p/\mathfrak{N}_p^2, +) \longrightarrow (\bar{k}^n, +).$$

От съгласуваността на grad_p с умножението по $\lambda \in \bar{k}$ следва \bar{k} -линейността на $\overline{\text{grad}_p}$, така че $\mathfrak{N}_p/\mathfrak{N}_p^2$ и \bar{k}^n са изоморфни като линейни пространства над \bar{k} .

Да означим с $f_i(x_1, \dots, x_n) \in \bar{k}[x_1, \dots, x_n], 1 \leq i \leq m$ произволни пораждащи на идеала

$$I(V) = \langle f_1, \dots, f_m \rangle = \sum_{i=1}^m f_i(x_1, \dots, x_n) \bar{k}[x_1, \dots, x_n]$$

на кривата V в $\bar{k}[x_1, \dots, x_n]$. Условието $p \in V$ е еквивалентно на $I(V) \subset \mathfrak{N}_p$. Ограничението

$$\text{grad}_p : I(V) \longrightarrow \bar{k}^n,$$

$$\begin{aligned} \text{grad}_p \left(\sum_{i=1}^m f_i(x_1, \dots, x_n) g_i(x_1, \dots, x_n) \right) &= \left(\sum_{i=1}^m g_i(p) \frac{\partial f_i}{\partial x_1}(p), \dots, \sum_{i=1}^m g_i(p) \frac{\partial f_i}{\partial x_n}(p) \right) = \\ &= \sum_{i=1}^m g_i(p) \left(\frac{\partial f_i}{\partial x_1}(p), \dots, \frac{\partial f_i}{\partial x_n}(p) \right) = \sum_{i=1}^m g_i(p) \text{grad}_p(f_i) \end{aligned}$$

взема стойности в линейната обвивка $\text{Grad}_p(V) = l_{\bar{k}}(\text{grad}_p(f_1), \dots, \text{grad}_p(f_m))$ на градиентите на пораждащите на $I(V)$ в $p \in V$. Всеки пораждащ $\text{grad}_p(f_i)$

на $\text{Grad}_p(V)$ е от образа на $\text{grad}_p : I(V) \rightarrow \bar{k}^n$, така че $\text{grad}_p : I(V) \rightarrow \text{Grad}_p(V)$ е линейно изображение върху $\text{Grad}_p(V)$. Ядрото

$$\ker(\text{grad}_p|_{I(V)}) = \ker(\text{grad}_p|_{\mathfrak{N}_p}) \cap I(V) = \mathfrak{N}_p^2 \cap I(V).$$

Следователно

$$(I(V) + \mathfrak{N}_p^2)/\mathfrak{N}_p^2 \simeq I(V)/(I(V) \cap \mathfrak{N}_p^2) \simeq \text{Grad}_p(V) = l_{\bar{k}}(\text{grad}_p(f_1), \dots, \text{grad}_p(f_m))$$

са изоморфизми на \bar{k} -линейни пространства. Якобиевата матрица

$$\frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)}(p) = \begin{pmatrix} \text{grad}_p(f_1) \\ \dots \\ \text{grad}_p(f_m) \end{pmatrix} \in M_{m,n}(\bar{k})$$

се състои по редове от градиентите на пораждащите f_i на $I(V)$, така че рангът

$$\text{rk} \left(\frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)}(p) \right) = \dim_{\bar{k}} [(I(V) + \mathfrak{N}_p^2)/\mathfrak{N}_p^2]. \quad (12.1)$$

От друга страна, максималният идеал $N_p = \mathfrak{N}_p/I(V)$ на точката $p \in V$ в афинния координатен пръстен $\bar{k}[V] = \bar{k}[x_1, \dots, x_n]/I(V)$ на V е фактор на \mathfrak{N}_p по $I(V)$. Локалният пръстен $\mathcal{O}_p(V) = \bar{k}[V]_{N_p}$ на p във V е локализацията на $\bar{k}[V]$ относно N_p , така че максималният идеал на $\mathcal{O}_p(V)$ е

$$\mathfrak{M}_p = (N_p)_{N_p} = \left\{ \frac{\alpha}{\beta} \mid \alpha \in N_p, \beta \in \bar{k}[V] \setminus N_p \right\}.$$

Квадратът $\mathfrak{M}_p^2 = (N_p^2)_{N_p}$, откъдето $\mathfrak{M}_p/\mathfrak{M}_p^2 = (N_p)_{N_p}/(N_p^2)_{N_p}$. Да отбележим, че

$$N_p = \left\{ \sum_{j=1}^n (x_j - p_j + I(V))(g_j(x_1, \dots, x_n) + I(V)) \mid g_j(x_1, \dots, x_n) \in \bar{k}[x_1, \dots, x_n] \right\}.$$

За произволен полином $g_j(x_1, \dots, x_n) \in \bar{k}[x_1, \dots, x_n]$ имаме $g_j(x_1, \dots, x_n) - g_j(p) \in \mathfrak{N}_p$, откъдето $g_j(x_1, \dots, x_n) - g_j(p) + I(V) \in N_p$ и $g_j(x_1, \dots, x_n) + I(V) \equiv g_j(p) + I(V) \pmod{N_p}$. Следователно

$$N_p/N_p^2 = \left\{ \sum_{j=1}^n (x_j - p_j + I(V))g_j(p) + N_p^2 \mid g_j(x_1, \dots, x_n) \in \bar{k}[x_1, \dots, x_n] \right\}.$$

От друга страна,

$$(N_p)_{N_p} = \left\{ \sum_{j=1}^n (x_j - p_j + I(V))h_j \mid h_j \in \mathcal{O}_p(V) \right\}$$

с $h_j - h_j(p) \in \mathfrak{M}_p$, откъдето

$$(N_p)_{N_p}/(N_p^2)_{N_p} = \left\{ \sum_{j=1}^n (x_j - p_j + I(V))h_j(p) + (N_p^2)_{N_p} \mid h_j \in \mathcal{O}_p(V) \right\}$$

В резултат получаваме изоморфизма на \bar{k} -линейни пространства

$$\mathfrak{M}_p/\mathfrak{M}_p^2 = (N_p)_{N_p}/(N_p^2)_{N_p} \simeq N_p/N_p^2. \quad (12.2)$$

По-точно, композицията на \bar{k} -линейното влагане $N_p \hookrightarrow \mathfrak{M}_p = (N_p)_{N_p}$ с \bar{k} -линейния епиморфизъм $\mathfrak{M}_p \rightarrow \mathfrak{M}_p/\mathfrak{M}_p^2$ дава \bar{k} -линейното изображение

$$\psi : N_p \longrightarrow \mathfrak{M}_p/\mathfrak{M}_p^2,$$

$$\psi \left(\sum_{j=1}^n (x_j - p_j + I(V))(g_j(x_1, \dots, x_n) + I(V)) \right) = \sum_{j=0}^n (x_j - p_j + I(V))g_j(p) + \mathfrak{M}_p^2.$$

Непосредствено се вижда, че образът на ψ покрива $\mathfrak{M}_p/\mathfrak{M}_p^2$. За да проверим, че ядрото $\ker(\psi) = N_p^2$, да отбележим, че елементите на \mathfrak{M}_p^2 са от вида

$$h = \sum_{1 \leq i \leq j \leq n} (x_i - p_i + I(V))(x_j - p_j + I(V))h_{ij}$$

за някакви $h_{ij} \in \mathcal{O}_p(V) = \bar{k}[V]_{N_p}$. Съществуват $g_{ij} \in \bar{k}[V]$ и $g'_{ij} \in \bar{k}[V] \setminus N_p$ с $\frac{g_{ij}}{g'_{ij}} = h_{ij}$. Произведението $g_o := \prod_{1 \leq i \leq j \leq n} g'_{ij} \in \bar{k}[V] \setminus N_p$ на знаменателите на

h_{ij} е елемент на афинния координатен пръстен $\bar{k}[V]$ извън идеала N_p , защото максималният идеал N_p е прост. Ясно е, че

$$g_o h = \sum_{1 \leq i \leq j \leq n} (x_i - p_i + I(V))(x_j - p_j + I(V))g_{ij} \in N_p^2.$$

Остава да покажем, че ако $h \in N_p \cap \mathfrak{M}_p^2$, то $h \in N_p^2$, за да получим, че $\ker(\psi) = N_p^2$. За целта разглеждаме \bar{k} -линейното изображение

$$\text{grad}'_p : N_p \longrightarrow \bar{k}^n,$$

$$\text{grad}'_p \left(\sum_{s=1}^n (x_s - p_s + I(V))t_s \right) = (t_1(p), \dots, t_n(p))$$

за произволни $t_1, \dots, t_n \in \bar{k}[V]$. Ядрото

$$\ker(\text{grad}'_p) = \left\{ \sum_{s=1}^n (x_s - p_s + I(V))t_s \mid t_1, \dots, t_n \in N_p \right\} = N_p^2.$$

За всяко $h \in N_p \cap \mathfrak{M}_p^2$ съществува $g_o \in \bar{k}[V] \setminus N_p$ с $g_o h \in N_p^2$. Следователно

$$0 = \text{grad}'_p(g_o h) = g_o(p) \text{grad}'_p(h),$$

съгласно $h(p) = 0$. От $g_o(p) \neq 0$ получаваме $\text{grad}'_p(h) = 0$, т.е. $h \in \ker(\text{grad}'_p) = N_p$ и доказваме \bar{k} -линейния изоморфизъм (12.2).

Композицията на естествения епиморфизъм $\pi_V : \mathfrak{N}_p \rightarrow N_p = \mathfrak{N}_p/I(V)$ с ядро $\ker(\pi_V) = I(V)$ и на естествения епиморфизъм $\pi_2 : N_p \rightarrow N_p/N_p^2$ с ядро $\ker(\pi_2) = N_p^2$ дава епиморфизъм $\pi = \pi_2 \pi_V : \mathfrak{N}_p \rightarrow N_p/N_p^2$ с ядро

$$\ker(\pi) = I(V) + \pi_V^{-1}(\ker(\pi_2)) = I(V) + \pi_V^{-1}(N_p^2) = I(V) + \mathfrak{N}_p^2.$$

По този начин получаваме изоморфизъм на пръстени

$$\mathfrak{N}_p/\ker(\pi) = \mathfrak{N}_p/(I(V) + \mathfrak{N}_p^2) \simeq N_p/N_p^2,$$

а оттам и изоморфизъм на \bar{k} -линейни пространства

$$\mathfrak{M}_p/\mathfrak{M}_p^2 \simeq \mathfrak{N}_p/(I(V) + \mathfrak{N}_p^2).$$

Вземайки предвид, че \mathfrak{N}_p^2 е идеал в \mathfrak{N}_p и $I(V) + \mathfrak{N}_p^2$, представяме

$$\mathfrak{M}_p/\mathfrak{M}_p^2 \simeq (\mathfrak{N}_p/\mathfrak{N}_p^2) / [(I(V) + \mathfrak{N}_p^2)/\mathfrak{N}_p^2]. \quad (12.3)$$

Твърдим, че от (12.1) и (12.3) следва

$$\dim_{\bar{k}}(\mathfrak{M}_p/\mathfrak{M}_p^2) + \text{rk} \left(\frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)}(p) \right) = \dim_{\bar{k}}(\mathfrak{N}_p/\mathfrak{N}_p^2) = n.$$

Наистина, съгласно $g_j(x_1, \dots, x_n) \equiv g_j(p) \pmod{\mathfrak{N}_p}$ за произволен полином $g_j(x_1, \dots, x_n) \in \bar{k}[x_1, \dots, x_n]$, елементите на $\mathfrak{N}_p/\mathfrak{N}_p^2$ са от вида

$$\sum_{j=1}^n (x_j - p_j)g_j(x_1, \dots, x_n) + \mathfrak{N}_p^2 = \sum_{j=1}^n (x_j - p_j)g_j(p).$$

Хомогенен линеен полином $\sum_{j=1}^n a_j(x_j - p_j)$ на $x_j - p_j$ с коефициенти $a_j \in \bar{k}$ принадлежи на \mathfrak{N}_p^2 само когато всички $a_i = 0$.

По определение, точката $p \in V$ е гладка точно когато $\text{rk} \frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)}(p) = n - 1$. Следователно гладкостта на $p \in V$ е еквивалентна на $\dim_{\bar{k}}(\mathfrak{M}_p/\mathfrak{M}_p^2) = 1$. Прилагайки Твърдение 12.19 стигаме до извода, че p е гладка точка на афинната крива V тогава и само тогава, когато локалният пръстен $\mathcal{O}_p(V)$ е пръстен на дискретно нормиране, Q.E.D.

СЛЕДСТВИЕ 12.20. Нека $V = Z(f_1, \dots, f_m) \subseteq \bar{k}^n$ е неприводима афинна крива с идеал $I(V) = \langle f_1, \dots, f_m \rangle = \sum_{i=1}^m f_i(x_1, \dots, x_n)\bar{k}[x_1, \dots, x_n]$ за някакви полиноми $f_i(x_1, \dots, x_n) \in \bar{k}[x_1, \dots, x_n]$, а $p = (p_1, \dots, p_n)$ е гладка точка на V с максимален идеал $\mathfrak{N}_p = \langle x_1 - p_1, \dots, x_n - p_n \rangle = \sum_{j=1}^n (x_j - p_j)\bar{k}[x_1, \dots, x_n]$. Тогава:

(i) $\dim_{\bar{k}}(\mathfrak{N}_p/I(V) + \mathfrak{N}_p^2) = 1$ и произволна \bar{k} -линейна комбинация

$$t = \sum_{j=1}^n a_j(x_j - p_j)$$

на $x_1 - p_1, \dots, x_n - p_n$ извън $I(V) + \mathfrak{N}_p^2$ задава локален параметър $t + I(V)$ на локалния пръстен $\mathcal{O}_p(V) = \bar{k}[V]_{(\mathfrak{N}_p/I(V))}$ на p във V .

(ii) ако

$$\det \frac{\partial(f_1, \dots, f_{n-1})}{\partial(x_1, \dots, x_{n-1})}(p) \neq 0,$$

то $x_n - p_n + I(V)$ е локален параметър на $\mathcal{O}_p(V)$.

Доказателство: (i) Съгласно Теорема 15, локалният пръстен $\mathcal{O}_p(V)$ на p във V е пръстен на дискретно нормиране. Тогава по Твърдение 12.19, факторът $\mathfrak{M}_p/\mathfrak{M}_p^2$ е 1-мерно линейно пространство над полето $\mathcal{O}_p(V)/\mathfrak{M}_p = \bar{k}$. В доказателството на Теорема 15 установихме изоморфизма

$$\mathfrak{M}/\mathfrak{M}_p^2 \simeq \mathfrak{N}_p/(I(V) + \mathfrak{N}_p^2)$$

на \bar{k} -линейни пространства. Следователно $\dim_{\bar{k}}(\mathfrak{N}_p/(I(V) + \mathfrak{N}_p^2)) = 1$ и произволен елемент

$$t = \sum_{j=1}^n a_j(x_j - p_j) \in l_{\bar{k}}(x_1 - p_1, \dots, x_n - p_n)$$

с $t + I(V) + \mathfrak{N}_p^2 \neq I(V) + \mathfrak{N}_p^2$ задава \bar{k} -базис $t + I(V) + \mathfrak{N}_p^2$ на $\mathfrak{N}_p/(I(V) + \mathfrak{N}_p^2) \simeq \mathfrak{M}_p/\mathfrak{M}_p^2$. Съгласно Следствие 12.5 от Лемата на Накауата, от $t + \mathfrak{M}_p^2 \neq \mathfrak{M}_p^2$ следва, че $t + I(V) \in \mathfrak{M}_p$ е пораждащ на максималния идеал \mathfrak{M}_p на локалния пръстен $\mathcal{O}_p(V)$. Оттук, $t + I(V)$ е локален параметър на класа дискретни нормирания на $\bar{k}(V)$ с пръстен $\mathcal{O}_p(V)$.

(ii) Достатъчно е да докажем, че за всеки полином $f(x_1, \dots, x_n)$ от идеала $I(V)$ на V е в сила

$$\sum_{j=1}^n \frac{\partial f}{\partial x_j}(p)(x_j - p_j) \in I(V) + \mathfrak{N}_p^2. \quad (12.4)$$

Тогава $\sum_{j=1}^n \frac{\partial f_i}{\partial x_j}(p)(x_j - p_j) \in I(V) + \mathfrak{N}_p^2$ за $\forall 1 \leq i \leq m$ и

$$\frac{\partial(f_1, \dots, f_{n-1})}{\partial(x_1, \dots, x_n)}(p) \begin{pmatrix} x_1 - p_1 \\ \dots \\ x_{n-1} - p_{n-1} \\ x_n - p_n \end{pmatrix} = 0_{n-1,1}.$$

След ляво умножение с $(n-1) \times (n-1)$ -матрицата $\left(\frac{\partial(f_1, \dots, f_{n-1})}{\partial(x_1, \dots, x_{n-1})}(p)\right)^{-1}$ получаваме

$$x_1 - p_1, \dots, x_{n-1} - p_{n-1} \in l_{\bar{k}}(x_n - p_n).$$

Ако допуснем, че $x_n - p_n \in I(V) + \mathfrak{N}_p^2$, то

$$\mathfrak{N}_p / (I(V) + \mathfrak{N}_p^2) = l_{\bar{k}}(x_1 - p_1, \dots, x_{n-1} - p_{n-1}, x_n - p_n) + I(V) + \mathfrak{N}_p^2 = I(V) + \mathfrak{N}_p^2,$$

което противоречи на $\dim_{\bar{k}}(\mathfrak{N}_p / (I(V) + \mathfrak{N}_p^2)) = 1$. Следователно $x_n - p_n \notin I(V) + \mathfrak{N}_p^2$ и $x_n - p_n + I(V) + \mathfrak{N}_p^2$ е локален параметър на $\mathcal{O}_p(V)$, стига (12.4). За да докажем (12.4) да забележим, че произволен полином $f(x_1, \dots, x_n) \in I(V) \subset \mathfrak{N}_p$ се разлага в сума

$$f(x_1, \dots, x_n) = \sum_{s=1}^d f(x_1 - p_1, \dots, x_n - p_n)^{(s)}$$

на хомогенни полиноми $f(x_1 - p_1, \dots, x_n - p_n)^{(s)}$ на $x_1 - p_1, \dots, x_n - p_n$ от степен $s \geq 1$. Въз основа на

$$\begin{aligned} f(x_1, \dots, x_n) - f(x_1 - p_1, \dots, x_n - p_n)^{(1)} &= \\ = \sum_{s=2}^d f(x_1 - p_1, \dots, x_n - p_n)^{(s)} &\in \mathfrak{N}_p^2 \subseteq I(V) + \mathfrak{N}_p^2 \end{aligned}$$

имаме

$$f(x_1 - p_1, \dots, x_n - p_n)^{(1)} + I(V) + \mathfrak{N}_p^2 = f(x_1, \dots, x_n) + I(V) + \mathfrak{N}_p^2 = I(V) + \mathfrak{N}_p^2. \quad (12.5)$$

Стойностите

$$\frac{\partial f}{\partial x_j}(p) = \frac{\partial f}{\partial(x_j - p_j)}(p) = \frac{\partial f(x_1 - p_1, \dots, x_n - p_n)^{(1)}(p)}{\partial(x_j - p_j)}$$

на формалните производни на $f(x_1, \dots, x_n)$ относно x_j са коефициентите на $x_j - p_j$ в $f(x_1 - p_1, \dots, x_n - p_n)^{(1)}$, така че

$$f(x_1 - p_1, \dots, x_n - p_n)^{(1)} = \sum_{j=1}^n \frac{\partial f}{\partial x_j}(p)(x_j - p_j). \quad (12.6)$$

Комбинирайки (12.5) с (12.6) получаваме (12.4), Q.E.D.

ЗАДАЧА 12.21. Нека $V_p = \{(x, y) \in \overline{\mathbb{F}_p}^2 \mid y^2 = x^3 - x\}$ е афинна равнинна крива, определена над просто поле \mathbb{F}_p с p елемента. Да се докаже, че:

(i) $y - p_2 + I(V_3)$ е локален параметър на V_3 в произволна точка $p = (p_1, p_2) \in V_3$;

(ii) $y - p_2 + I(V_5)$ е локален параметър на V_5 в произволна \mathbb{F}_5 -рационална точка $p = (p_1, p_2) \in V_5(\mathbb{F}_5) = V_5 \cap \mathbb{F}_5^2$.

От доказателството на Теорема 15 е ясно, че $\dim_{\bar{k}}(\mathfrak{M}_p / \mathfrak{M}_p^2) \geq 1$. Следователно

$$\text{rk} \frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)}(p) \leq n - 1$$

и гладките точки на крива V са точките в общо положение.

ОПРЕДЕЛЕНИЕ 12.22. Точката p на проективна крива V е гладка, ако локалният пръстен $\mathcal{O}_p(V)$ във V е пръстен на дискретно нормиране.

Точките $p \in V$, които не са гладки се наричат особенени.

V^{smooth} означаваме множеството на гладките точки върху V , а с V^{sing} - множеството на особените точки.

Ясно е, че точка p на проективна крива $V \subseteq \mathbb{P}^n(\bar{k})$ е гладка точно когато за всяко стандартно афинно отворено подмножество $U_i \subset \mathbb{P}^n(\bar{k})$, съдържащо p , точката p е гладка върху афинната крива $U_i \cap V$.

ТВЪРДЕНИЕ 12.23. Особените точки на алгебрична крива V са краен брой.

Доказателство: Доколкото всяка проективна крива V има крайно покритие $V = \cup_{i=0}^m (V \cap U_i)$ от афинни криви, достатъчно е да установим, че всяка афинна крива $V_o \subseteq \bar{k}^n$ има краен брой особенени точки. Ако идеалът $I(V_o) = \langle f_1, \dots, f_m \rangle \subset \bar{k}[x_1, \dots, x_n]$ на V_o се поражда от полиномите $f_i(x_1, \dots, x_n) \in \bar{k}[x_1, \dots, x_n]$, то множеството V_o^{sing} на особените точки на V_o е афинното затворено подмножество

$$V_o^{\text{sing}} = Z \left(f_1, \dots, f_m, \Delta_{j_1, \dots, j_{n-1}}^{i_1, \dots, i_{n-1}} \frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)} \right),$$

където $\Delta_{j_1, \dots, j_{n-1}}^{i_1, \dots, i_{n-1}} \frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)}$ са минорите от ред $n-1$ на Якобиевата матрица $\frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)}$. Достатъчно е да проверим, че $V_o^{\text{sing}} \subsetneq V_o$ е собствено Зариски затворено подмножество. Съгласно Следствие ??, V_o е бирационално на афинната прова \bar{k} или V_o има афинен равнинен модел $W_o \subseteq \bar{k}^2$. Афинната права е гладка, така че е достатъчно да докажем $W_o^{\text{sing}} \subsetneq W_o$, защото бирационалните изображения запазват размерността. Ако допуснем, че $W_o^{\text{sing}} = W_o = Z(f)$ за някакъв полином $f(x_1, x_2) \in \bar{k}[x_1, x_2]$, то $\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2} \in I(W_o) = \langle f \rangle$. Но общата степен $\deg(f) > \deg\left(\frac{\partial f}{\partial x_i}\right)$ за $1 \leq i \leq 2$, откъдето $\frac{\partial f}{\partial x_1} \equiv 0$ и $\frac{\partial f}{\partial x_2} \equiv 0$ се анулират тъждествено. Това означава, че всички степенни показатели на мономите на $f(x_1, x_2)$ са кратни на характеристиката $p = \text{char}(\bar{k})$ на полето \bar{k} от константи и съществува полином $h(x_1, x_2) \in \bar{k}[x_1, x_2]$ с $h(x_1, x_2)^{p^l} = f(x_1, x_2)$ за някое $l \in \mathbb{N}$. Това противоречи на неприводимостта на W_o и доказва $W_o^{\text{sing}} \subsetneq W_o$, а оттам и $V_o^{\text{sing}} \subsetneq V_o$, Q.E.D.

ЛЕМА 12.24. Нека V е проективна крива, P и Q са различни гладки точки от V , а ν_P и ν_Q са нормализираните дискретни нормирания на функционалното поле $\bar{k}(V)$ на V , чиито пръстени съвпадат с локалните пръстени $\mathcal{O}_P(V)$ на P и, съответно, $\mathcal{O}_Q(V)$ на Q . Тогава нормиранията ν_P и ν_Q не са еквивалентни.

Доказателство: Ако допуснем, че ν_P и ν_Q са еквивалентни, то локалните пръстени $\mathcal{O}_P(V) = \mathcal{O}_Q(V)$ на тези нормирания съвпадат.

Ако $P = [a_0 : \dots : a_n]$ и $Q = [b_0 : \dots : b_n]$ с $a_i \neq 0$ и $b_i \neq 0$ за някое $0 \leq i \leq n$, то съществува индекс $j \in \{0, \dots, n\} \setminus \{i\}$ с $\frac{a_j}{a_i} \neq \frac{b_j}{b_i}$. Тогава $\frac{x_j}{x_i} - \frac{a_j}{a_i} \in \mathfrak{M}_P(V)$ е от максималния идеал $\mathfrak{M}_P(V)$ на локалния пръстен $\mathcal{O}_P(V)$ на P , но не и от максималния идеал $\mathfrak{M}_Q(V)$ на локалния пръстен $\mathcal{O}_Q(V)$ на Q . В резултат, $\frac{x_j}{x_i} - \frac{a_j}{a_i} \in \mathcal{O}_Q(V) \setminus \mathfrak{M}_Q(V) = \mathcal{O}_Q(V)^*$ и $\left(\frac{x_j}{x_i} - \frac{a_j}{a_i}\right)^{-1} \in \mathcal{O}_Q(V)$, но $\left(\frac{x_j}{x_i} - \frac{a_j}{a_i}\right)^{-1} \notin \mathcal{O}_P(V)$. Противоречието доказва, че за всеки индекс $0 \leq i \leq n$ с $a_i \neq 0$ имаме $b_i = 0$.

За произволно $0 \leq i \leq n$ с $a_i \neq 0$ и $b_i = 0$ забелязваме, че $x_i \in \mathfrak{M}_Q(V)$, $x_i \in \mathcal{O}_P(V) \setminus \mathfrak{M}_P(V) = \mathcal{O}_P(V)^*$, откъдето $x_i^{-1} \in \mathcal{O}_P(V)$, $x_i^{-1} \notin \mathcal{O}_Q(V)$. Следователно дискретните нормирания ν_P и ν_Q , чиито пръстени съвпадат с локалните пръстени на различни гладки точки P и Q от проективна крива V не са еквивалентни, Q.E.D.

Нека V е гладка проективна крива. За да докажем, че всеки пръстен на дискретно нормиране R с поле от частни $\bar{k}(V)$ е локален пръстен $R = \mathcal{O}_p(V)$ на точка $p \in V$, ни е нужна следната

ЛЕМА 12.25. *Нека R е пръстен на дискретно нормиране с поле от частни K , а S е пръстен на дискретно нормиране, съдържащ R и съдържащ се строго в K . Тогава $R = S$ съвпадат.*

Доказателство: Допускаме противното и избираме елемент $x \in S \setminus R$. Ако $s \in S$ е локален параметър на S , то съществуват $u \in S^*$ и $m \in \mathbb{Z}^{\geq 0}$, така че $x = s^m u$. Ако $t \in R$ е локален параметър на R , то полето

$$K = \{t^z v \mid z \in \mathbb{Z}, v \in R^*\} \cup \{0\},$$

така че $x = t^z v$ за подходящи $v \in R^*$ и $z \in \mathbb{Z}$, $z < 0$. Съгласно $t \in R \subseteq S$ съществуват $u_o \in S^*$ и $n \in \mathbb{Z}^{\geq 0}$ с $t = s^n u_o$. Ако допуснем, че $n = 0$, то $t \in S^*$ е обратим в S и полето от частни $K = F(R) \subseteq S$ на R се съдържа в S , противно на допускането $S \subsetneq K$. Следователно $n \geq 1$ и $x = s^m u = t^z v = s^{nz} u_o^z v$, откъдето

$$s^{nz-m} = u u_o^{-z} v^{-1} \in S^*,$$

съгласно $R^* \subseteq S^*$. Но $nz - m < 0$, така че $s^{nz-m} \in K \setminus S$ е от допълнението на S в K . Това противоречи на $S^* \cap (K \setminus S) = \emptyset$ и доказва съвпадението $R = S$, Q.E.D.

ТЕОРЕМА 16. *Нека V е гладка проективна крива с функционално поле $\bar{k}(V)$. Тогава всеки пръстен на дискретно нормиране R с поле от частни $\bar{k}(V)$ е локален пръстен $R = \mathcal{O}_p(V)$ на единствена точка $p \in V$.*

Доказателство: Без ограничение на общността можем да считаме, че проективната крива $V \subseteq \mathbb{P}^m(\bar{k})$ не се съдържа в собствено проективно подпространство на $\mathbb{P}^m(\bar{k})$. (В противен случай, заменяме $\mathbb{P}^m(\bar{k})$ с подходящо $\mathbb{P}^n(\bar{k})$, $n < m$.) Тогава $\frac{x_i}{x_j}$ не се анулират твържествено върху V и нормализираното дискретно нормиране $\nu : \bar{k}(V) \rightarrow \mathbb{Z} \cup \{\infty\}$ с пръстен $\mathcal{O}_\nu = \{f \in \bar{k}(V) \mid \nu(f) \geq 0\} = R$ достига краен максимум

$$\mu = \max_{0 \leq i, j \leq m} \nu \left(\frac{x_i}{x_j} \right)$$

върху $\frac{x_i}{x_j}$. След евентуална пермутация на хомогенните координати на $\mathbb{P}^m(\bar{k})$ можем да считаме, че

$$\nu \left(\frac{x_0}{x_m} \right) = \mu.$$

Тогава

$$\nu \left(\frac{x_i}{x_m} \right) = \nu \left(\frac{x_0}{x_m} : \frac{x_0}{x_i} \right) = \mu - \nu \left(\frac{x_0}{x_i} \right) \geq 0$$

и афинният координатен пръстен

$$\bar{k}[V \cap U_m] = \bar{k} \left[\frac{x_0}{x_m}, \frac{x_1}{x_m}, \dots, \frac{x_{m-1}}{x_m} \right] \subseteq R.$$

Максималният идеал \mathfrak{M} на R пресича $\bar{k}[V \cap U_m]$ в прост идеал $\mathfrak{p} = \mathfrak{M} \cap \bar{k}[V \cap U_m]$, защото фактор-пръстенът

$$\bar{k}[V \cap U_m] / \mathfrak{p} = \bar{k}[V \cap U_m] / (\mathfrak{M} \cap \bar{k}[V \cap U_m]) \simeq (\bar{k}[V \cap U_m] + \mathfrak{M}) / \mathfrak{M}$$

е подпръстен на полето R / \mathfrak{M} от остатъци на ν . Простият идеал $\mathfrak{p} \triangleleft \bar{k}[V \cap U_m]$ е ненулев, защото в противен случай $\bar{k}[V \cap U_m]$ е подпръстен на полето R / \mathfrak{M} , откъдето и функционалното поле $\bar{k}(V) = F(\bar{k}[V \cap U_m])$ е подполе на R / \mathfrak{M} . Това води до противоречие, защото крайното разширение $R / \mathfrak{M} \supseteq \bar{k}$ е алгебрично,

така че R/\mathfrak{M} съвпада с \bar{k} и не може да съдържа разширението $\bar{k}(V) \supset \bar{k}$ от степен на трансцендентност 1.

В областта $\bar{k}[V \cap U_m]$ с размерност на Krull 1 ненулевият прост идеал $\mathfrak{p} = \mathfrak{M} \cap \bar{k}[V \cap U_m]$ е максимален и отговаря на точка $p \in V$, т.е.

$$\mathfrak{p} = \langle x_1 - p_1 + I(V \cap U_m), \dots, x_n - p_n + I(V \cap U_m) \rangle$$

за $p = (p_1, \dots, p_n) \in V$. Локалният пръстен $\mathcal{O}_p(V)$ на p във V се съдържа в R , защото $\mathcal{O}_p(V) = \mathcal{O}_p(V \cap U_m) = \bar{k}[V \cap U_m]_{\mathfrak{p}}$ е локализацията на $\bar{k}[V \cap U_m]$ относно \mathfrak{p} , $\bar{k}[V \cap U_m]$ е подпръстен на R и допълнението $\bar{k}[V \cap U_m] \setminus \mathfrak{p} \subseteq R \setminus \mathfrak{M} \subseteq R^*$ на простия идеал \mathfrak{p} в $\bar{k}[V \cap U_m]$ се състои от обратими елементи на R . Съгласно Лема 12.25, от включването $\mathcal{O}_p(V) \subseteq R$ на пръстени на дискретно нормиране с поле от частни $\bar{k}(V)$ следва съпадението $\mathcal{O}_p(V) = R$. По Твърдение 12.24, точката $p \in V$ с $\mathcal{O}_p(V) = R$ е единствена, Q.E.D.

Разглежданията от настоящия въпрос установяват следната

ТЕОРЕМА 17. *Нека V е гладка проективна крива с функционално поле $\bar{k}(V)$ над алгебричната обвивка \bar{k} на поле k . Тогава съществува взаимно еднозначно съответствие между точките p на V и пръстените на дискретно нормиране $\mathcal{O}_p(V)$ с поле от частни $\bar{k}(V)$.*