

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC VINH

VŨ ĐÌNH QUYẾT

ĐA THỨC DUY NHẤT
CHO HỌ CÁC HÀM PHÂN HÌNH KHÁC HẰNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

Nghệ An - 2021

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC VINH

VŨ ĐÌNH QUYẾT

ĐA THỨC DUY NHẤT
CHO HỌ CÁC HÀM PHÂN HÌNH KHÁC HẰNG

Chuyên ngành: ĐẠI SỐ VÀ LÝ THUYẾT SỐ

Mã số: 8 46 01 04

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học
TS. NGUYỄN THỊ NGỌC DIỆP

Nghệ An - 2021

Mục lục

MỞ ĐẦU	1
Chương 1. KIẾN THỨC CHUẨN BỊ	3
1.1. Đa tạp trong không gian afin và không gian xạ ảnh	3
1.2. Đường cong phẳng trong mặt phẳng afin	6
1.3. Trường định chuẩn	9
Chương 2. ĐA THỨC DUY NHẤT CHO HỌ CÁC HÀM PHÂN HÌNH KHÁC HẰNG	13
2.1. 1-dạng chính quy kiểu Wronski trên một đường cong đại số	13
2.2. Đa thức duy nhất cho họ các hàm phân hình khác hằng	15
KẾT LUẬN	44
TÀI LIỆU THAM KHẢO	45

MỞ ĐẦU

Giả sử $\mathbf{K}$ là trường đóng đại số, đầy đủ với giá trị tuyệt đối không Archimedean. Ký hiệu $\mathfrak{B}^*(\mathbf{K})$ là tập các hàm phân hình khác hằng xác định trên trường $\mathbf{K}$ và $\mathcal{F}$ là tập con khác rỗng của $\mathfrak{B}^*(\mathbf{K})$.

Đa thức một biến P trên trường $\mathbf{K}$ được gọi là đa thức duy nhất cho họ các hàm $\mathcal{F}$ nếu với mọi hàm khác hằng $f, g \in \mathcal{F}$ thỏa mãn $P(f) = P(g)$ thì $f = g$.

Thời gian gần đây, nhiều kết quả thú vị về đa thức duy nhất đã được đưa ra bởi nhiều tác giả như W. Cherry, A. Escassut, J. T. Y. Wang,... Năm 2003, trong bài báo [4], các tác giả T. T. H. An, J. T. Y. Wang và P. M. Wong đã chỉ ra một lớp các đa thức đặc biệt là đa thức duy nhất cho họ các hàm phân hình bằng cách xây dựng các 1-dạng chính quy kiểu Wronski. Tiếp tục hướng nghiên cứu về đa thức duy nhất cho họ các hàm phân hình, năm 2005, nhóm tác giả này xem xét những lớp đa thức tổng quát hơn.

Trong luận văn này, chúng tôi tập trung tìm hiểu về đa thức duy nhất cho họ các hàm phân hình khác hằng.

Nội dung chính của luận văn là tìm hiểu và trình bày một cách chi tiết những kết quả trong bài báo "Unique range sets and uniqueness polynomials in positive characteristic II" của các tác giả T. T. H. An, J. T. Y. Wang và P. M. Wong trên tạp chí Acta Arithmetica [5].

Ngoài các phần mở đầu, kết luận và tài liệu tham khảo, nội dung chính của luận văn được chia thành hai chương.

Chương 1. Kiến thức chuẩn bị

Trong chương này chúng tôi trình bày một số kiến thức cơ bản nhằm mục đích làm cơ sở cho việc trình bày nội dung của chương 2. Ngoài ra

chúng tôi còn trích dẫn một số kết quả đã có nhằm phục vụ cho các chứng minh ở phần sau.

Chương 2. Đa thức duy nhất cho họ các hàm phân hình khác hằng

Trong chương này, chúng tôi tìm hiểu phương pháp xây dựng các 1-dạng chính quy kiểu Wronski trên một đường cong đại số. Đồng thời, chúng tôi tìm hiểu một số điều kiện đủ để một đa thức một biến trên trường $\mathbf{K}$ là đa thức duy nhất, đa thức duy nhất mạnh cho họ các hàm phân hình khác hằng trên $\mathbf{K}$ trong trường hợp đặc số của trường $\mathbf{K}$ chia hết bậc của đa thức.

Tôi xin bày tỏ lòng biết ơn chân thành đến TS. Nguyễn Thị Ngọc Diệp đã luôn quan tâm giúp đỡ tôi trong quá trình học tập, nghiên cứu, hướng dẫn tôi hoàn thành luận văn này.

Tôi xin chân thành cảm ơn các Thầy, Cô khoa Toán và phòng Đào tạo sau Đại học, Trường Đại học Vinh; các bạn học viên cao học Toán khóa 28 cùng gia đình, người thân và bạn bè đã động viên, góp ý và giúp đỡ tôi trong suốt quá trình học tập và thực hiện luận văn.

Nghệ An, tháng 6 năm 2022

Tác giả

Chương 1

KIẾN THỨC CHUẨN BỊ

Trong chương này chúng tôi trình bày những kiến thức cơ bản nhằm mục đích làm cơ sở cho việc trình bày nội dung của chương 2. Ngoài ra chúng tôi còn trích dẫn một số kết quả đã có nhằm phục vụ cho các chứng minh ở phần sau. Những nội dung này chủ yếu được tham khảo trong các tài liệu [1], [2], [3] và [8].

1.1. Đa tạp trong không gian afin và không gian xạ ảnh

Trong toàn bộ chương này ta luôn luôn ký hiệu k là một trường.

1.1.1. Định nghĩa. Cho đa thức $E(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$. Một điểm $W = (w_1, \dots, w_n) \in \mathbb{A}^n(k)$ được gọi là *không điểm* của đa thức $E(x_1, \dots, x_n)$ nếu

$$E(W) = E(w_1, \dots, w_n) = 0.$$

Nếu E không là hằng thì tập hợp các không điểm của E được gọi là *siêu mặt* xác định bởi E , ký hiệu là $Z(E)$. Như vậy

$$Z(E) = \{W \in \mathbb{A}^n(k) \mid E(W) = 0\}.$$

1.1.2. Định nghĩa. Nếu $\mathcal{A}$ là tập hợp các đa thức bất kỳ trong vành đa thức $k[x_1, \dots, x_n]$ thì tập hợp

$$Z(\mathcal{A}) = \{W \in \mathbb{A}^n(k) \mid E(W) = 0, \forall E \in \mathcal{A}\}$$

được gọi là *tập đại số* trong $\mathbb{A}^n(k)$.

1.1.3. Ví dụ. (1) Tập rỗng $\emptyset$ là một tập đại số vì tập rỗng là tập nghiệm

của phương trình $f=0$, với mọi $f \in k$, $f \neq 0$.

(2) Mỗi điểm $W = (w_1, w_2, \dots, w_n)$ trong không gian afin $\mathbb{A}^n(k)$ là một tập đại số vì W là tập nghiệm của hệ phương trình sau

$$\begin{cases} x_1 - w_1 = 0 \\ x_2 - w_2 = 0 \\ \dots \\ x_n - w_n = 0 \end{cases}$$

nghĩa là

$$W = Z(x_1 - w_1, x_2 - w_2, \dots, x_n - w_n).$$

(3) Tập nghiệm của một hệ phương trình tuyến tính là một tập đại số và được gọi là đa tạp tuyến tính.

(4) $\mathbb{A}^n(k)$ là tập đại số trong $\mathbb{A}^n(k)$ vì $\mathbb{A}^n(k)$ là tập nghiệm của phương trình $0=0$.

1.1.4. Mệnh đề (i) Cho $\mathcal{A}_1, \mathcal{A}_2$ là các hệ đa thức trong vành đa thức $k[x_1, \dots, x_n]$. Nếu $\mathcal{A}_2 \subseteq \mathcal{A}_1$ thì $Z(\mathcal{A}_1) \subseteq Z(\mathcal{A}_2)$.

(ii) Hợp của hai tập đại số cũng là tập đại số, nghĩa là: Với các hệ đa thức $\mathcal{A}_1, \mathcal{A}_2$ trong vành đa thức $k[x_1, \dots, x_n]$ ta luôn có

$$Z(\mathcal{A}_1) \cup Z(\mathcal{A}_2) = Z(\mathcal{A})$$

trong đó

$$\mathcal{A} = \{ hg \mid h \in \mathcal{A}_1, g \in \mathcal{A}_2 \}.$$

(iii) Giao của một họ tùy ý các tập đại số là một tập đại số, nghĩa là: Với một họ $\{\mathcal{A}_i\}$ các hệ đa thức trong vành đa thức $k[x_1, \dots, x_n]$ ta luôn có

$$\bigcap_i Z(\mathcal{A}_i) = Z\left(\bigcup_i \mathcal{A}_i\right).$$

1.1.5. Chú ý. Trong không gian afin $\mathbb{A}^n(k)$ ta luôn có hợp của hai tập đại số là một tập đại số, giao của một họ tùy ý các tập đại số là một tập

đại số, tập rỗng và toàn bộ không gian afin $\mathbb{A}^n(k)$ là các tập đại số. Vì vậy ta có thể trang bị một tôpô trên không gian afin $\mathbb{A}^n(k)$ bằng cách coi các tập đại số là các tập đóng. Tôpô này được gọi là tôpô Zariski trên không gian afin $\mathbb{A}^n(k)$.

1.1.6. Định nghĩa. (i) Ta nói tập đại số $M \subset \mathbb{A}^n(k)$ là *khả quy* nếu $M = M_1 \cup M_2$, trong đó M_1, M_2 là các tập đại số trong $\mathbb{A}^n(k)$ và $M_1 \neq M, M_2 \neq M$. Trong trường hợp ngược lại, tập đại số M được gọi là *bất khả quy*.

(ii) Một tập đại số bất khả quy trong không gian afin $\mathbb{A}^n(k)$ được gọi là một *đa tạp afin*.

(iii) Một tập con mở của một đa tạp afin được gọi là *đa tạp tựa afin*.

1.1.7. Định lý. Giả sử M là tập đại số trong không gian afin $\mathbb{A}^n(k)$. Khi đó tồn tại duy nhất các tập đại số bất khả quy $M_1, M_2, \dots, M_m$ sao cho

$$M = M_1 \cup M_2 \cup \dots \cup M_m$$

trong đó $M_i \not\subset M_j$ với mọi $i \neq j$.

Các tập đại số bất khả quy M_i được gọi là các thành phần bất khả quy của tập đại số M và $M = M_1 \cup M_2 \cup \dots \cup M_m$ là sự phân tích M thành các thành phần bất khả quy.

Giả sử S là đa thức thuần nhất bậc s trong vành đa thức $k[x_1, \dots, x_{n+1}]$. Ta có

$$S(\lambda a_1, \lambda a_2, \dots, \lambda a_{n+1}) = \lambda^s S(a_1, a_2, \dots, a_{n+1}),$$

với mọi điểm $a = (a_1, a_2, \dots, a_{n+1}) \in \mathbb{A}^{n+1}(k)$, $\lambda \in k$. Vì vậy nếu a là nghiệm của S thì λa cũng là nghiệm của S .

Lưu ý rằng điểm 0 là nghiệm của mọi đa thức thuần nhất.

Để xét nghiệm của đa thức thuần nhất ta chia tập $\mathbb{A}^{n+1}(k) \setminus \{0\}$ theo quan hệ tương đương

$$a \sim b \text{ nếu tồn tại } \lambda \neq 0 \text{ sao cho } b = \lambda a.$$

Tập hợp các lớp tương đương này được gọi là không gian xạ ảnh n chiều trên trường k và ký hiệu là $\mathbb{P}^n(k)$.

Với mỗi điểm $a \in \mathbb{A}^{n+1}(k) \setminus \{0\}$ ta cũng dùng ký hiệu a để chỉ lớp các điểm tương đương với a . Khi đó ta coi a như là điểm của không gian xạ ảnh $\mathbb{P}^n(k)$.

1.1.8. Định nghĩa. (i) Cho đa thức $R \in k[x_1, \dots, x_{n+1}]$. Một điểm $a \in \mathbb{P}^n(k)$ được gọi là *nghiệm xạ ảnh* của đa thức R nếu $R(\lambda a) = 0$ với mọi $\lambda \in k$.

(ii) Với mỗi tập $\mathfrak{B}$ không rỗng gồm các đa thức thuần nhất trong vành đa thức $k[x_1, \dots, x_{n+1}]$ thì

$$Z(\mathfrak{B}) = \{ a \in \mathbb{P}^n(k) \mid R(a) = 0, \forall R \in \mathfrak{B} \}$$

được gọi là *tập đại số xạ ảnh* trong không gian xạ ảnh $\mathbb{P}^n(k)$.

1.1.9. Định nghĩa. (i) Ta nói tập đại số M trong không gian xạ ảnh $\mathbb{P}^n(k)$ là *bất khả quy* nếu M không là hợp của hai tập đại số bé hơn thực sự.

(ii) Một tập đại số bất khả quy trong $\mathbb{P}^n(k)$ được gọi là một *đa tạp xạ ảnh*.

(iii) Một tập con mở của một đa tạp xạ ảnh gọi là *đa tạp tựa xạ ảnh*.

1.2. Đường cong phẳng trong mặt phẳng afin

1.2.1. Định nghĩa. Đường cong phẳng $\mathcal{L}$ trong $\mathbb{A}^2(k)$ xác định bởi đa thức $R(x, y)$ là

$$\mathcal{L} = \{ (a, b) \in \mathbb{A}^2(k) \mid R(a, b) = 0 \}.$$

Đường cong $\mathcal{L}$ là bất khả quy nếu $R(x, y)$ bất khả quy. Bậc của đường cong xác định bởi đa thức $R(x, y)$ là bậc của đa thức $R(x, y)$.

Giả sử $R = \prod_i R_i^{e_i}$, trong đó R_i là các nhân tử bất khả quy của R và $e_i \geq 1$. Ta gọi các R_i là các thành phần của R và e_i là bội của thành phần R_i . Ta nói R_i là thành phần đơn nếu $e_i = 1$, và là thành phần bội nếu $e_i > 1$.

Do vành đa thức $k[x, y]$ là vành nhân tử hóa nên mọi đa thức $R(x, y) \in k[x, y]$ đều có thể phân tích được một cách duy nhất thành thành phần bất khả quy

$$R = R_1^{s_1} R_2^{s_2} \dots R_l^{s_l},$$

trong đó $R_1, R_2, \dots, R_l$ là các đa thức bất khả quy phân biệt và $s_1, s_2, \dots, s_l$ là các số tự nhiên.

Bây giờ ta ký hiệu

$$\mathcal{L}_i = \left\{ (a, b) \in \mathbb{A}^2(k) \mid R_i(a, b) = 0 \right\}, \quad i = 1, 2, \dots, l.$$

Khi đó $\mathcal{L}_i$ ($i = 1, 2, \dots, l$) là các thành phần bất khả quy của đường cong $\mathcal{L}$. Đồng thời đường cong $\mathcal{L}$ có sự phân tích thành các thành phần bất khả quy

$$\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \dots \cup \mathcal{L}_l.$$

Giả sử $R(x, y)$ là đa thức hai biến trên trường k có bậc n . Đặt $\tilde{R}(x, y, z) = z^n R\left(\frac{x}{z}, \frac{y}{z}\right)$, ta có $\tilde{R}(x, y, z)$ là một đa thức thuần nhất bậc n thuộc vành đa thức $k[x, y, z]$ và được gọi là sự thuần nhất của đa thức $R(x, y)$.

Ta ký hiệu

$$\tilde{\mathcal{L}} = \left\{ [a : b : c] \in \mathbb{P}^2(k) \mid \tilde{R}(a, b, c) = 0 \right\}$$

thì $\tilde{\mathcal{L}}$ được gọi là đường cong xạ ảnh tương ứng của đường cong $\mathcal{L}$. Điểm (a, b) thuộc đường cong $\mathcal{L}$ khi và chỉ khi điểm $(a, b, 1)$ thuộc đường cong

$\tilde{\mathcal{L}}$. Đường cong $\mathcal{L}$ bất khả quy khi và chỉ khi đường cong $\tilde{\mathcal{L}}$ bất khả quy. Nếu đường cong $\mathcal{L}$ có sự phân tích thành các thành phần bất khả quy

$$\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \cdots \cup \mathcal{L}_l$$

thì đường cong $\tilde{\mathcal{L}}$ cũng có sự phân tích thành các thành phần bất khả quy tương ứng

$$\tilde{\mathcal{L}} = \tilde{\mathcal{L}}_1 \cup \tilde{\mathcal{L}}_2 \cup \cdots \cup \tilde{\mathcal{L}}_l.$$

1.2.2. Định nghĩa. Cho đường cong phẳng $\mathcal{L}$ trong không gian afin $\mathbb{A}^2(k)$ xác định bởi phương trình $R(x, y) = 0$ và điểm $N = (u, v) \in \mathcal{L}$. Điểm N được gọi là *điểm đơn* của đường cong $\mathcal{L}$ nếu $\frac{\partial R}{\partial x}(N) \neq 0$ hoặc $\frac{\partial R}{\partial y}(N) \neq 0$. Khi đó đường thẳng xác định bởi phương trình

$$\left. \frac{\partial R}{\partial x} \right|_N (x - u) + \left. \frac{\partial R}{\partial y} \right|_N (y - v) = 0$$

được gọi là *đường tiếp tuyến* với đường cong $\mathcal{L}$ tại điểm N . Một điểm không phải là điểm đơn thì gọi là *điểm kỳ dị*.

Một đường cong được gọi là *trơn* nếu mọi điểm của đường cong đó là điểm đơn.

1.2.3. Định nghĩa. Cho đường cong phẳng $\mathcal{L}$ trong không gian afin $\mathbb{A}^2(k)$ xác định bởi phương trình $R(x, y) = 0$ và điểm $N = (0, 0)$. Ta viết

$$R = R_t + R_{t+1} + \cdots + R_n,$$

trong đó R_i là đa thức thuần nhất bậc i trong vành đa thức $k[x, y]$, $R_t \neq 0$. Ta gọi t là *số bội* của đường cong $\mathcal{L}$ tại $N = (0, 0)$ và viết $t = t_N(R) = t_N(\mathcal{L})$.

Do R_t là đa thức thuần nhất hai biến trên trường đóng đại số nên ta có thể viết $R_t = \prod_i Q_i^{q_i}$ trong đó Q_i các nhân tử tuyến tính. Các Q_i được gọi là các *đường tiếp tuyến* của đường cong $\mathcal{L}$ tại $N = (0, 0)$; q_i gọi là *số bội* của tiếp tuyến. Q_i gọi là *tiếp tuyến đơn* (kép,...) nếu $q_i = 1$ (2, ...).

Nếu đường cong $\mathcal{L}$ có t tiếp tuyến đơn phân biệt tại N thì ta nói N là *điểm kỳ dị chính tắc* của đường cong $\mathcal{L}$.

Giả sử $R = \prod R_i^{e_i}$ là sự phân tích R thành các thành phần bất khả quy. Khi đó

$$t_N(R) = \sum_i e_i t_N(R_i) .$$

Nếu Q là đường tiếp tuyến của R_j với số bội q_j thì Q là tiếp tuyến của R với số bội $\sum_i e_i q_i$.

1.2.4. Nhận xét. Ta có thể mở rộng các định nghĩa trên đây cho điểm $N = (u, v) \neq (0, 0)$ bằng cách thực hiện phép tịnh tiến $S(x, y) = (x + u, y + v)$ biến $(0, 0)$ thành N . Khi đó $R^S = R(x + u, y + v)$ và ta định nghĩa $t_N(R)$ chính là $t_{(0,0)}(R^S)$.

1.3. Trường định chuẩn

1.3.1. Định nghĩa. Trường $\mathbf{K}$ cùng với ánh xạ $\varphi : \mathbf{K} \rightarrow \mathbb{R}$, ký hiệu bởi $(\mathbf{K}, \varphi)$, được gọi là một trường *định chuẩn* hay *trường metric* nếu các điều kiện sau đây thỏa mãn:

- 1) $\varphi(\alpha) \geq 0$; $\varphi(\alpha) = 0 \Leftrightarrow \alpha = 0$, $\forall \alpha \in \mathbf{K}$;
- 2) $\varphi(\alpha + \beta) \leq \varphi(\alpha) + \varphi(\beta)$, $\forall \alpha, \beta \in \mathbf{K}$;
- 3) $\varphi(\alpha\beta) = \varphi(\alpha) + \varphi(\beta)$, $\forall \alpha, \beta \in \mathbf{K}$.

Nếu thay điều kiện 2) bởi điều kiện mạnh hơn sau đây:

- 4) $\varphi(\alpha + \beta) \leq \max\{\varphi(\alpha), \varphi(\beta)\}$, $\forall \alpha, \beta \in \mathbf{K}$

thì trường định chuẩn $(\mathbf{K}, \varphi)$ được gọi là *trường định chuẩn không Acsimet*.

Hàm $\varphi : \mathbf{K} \rightarrow \mathbb{R}$ xác định bởi $\varphi(0) = 0$, $\varphi(\alpha) = 1$, $\forall \alpha \in \mathbf{K}$, $\alpha \neq 0$ là một chuẩn trên trường $\mathbf{K}$ và được gọi là *chuẩn tầm thường* trên $\mathbf{K}$. Như vậy, một chuẩn φ là không tầm thường trên trường $\mathbf{K}$ nếu tồn tại

$\alpha \in \mathbf{K}, \alpha \neq \mathbf{0}$ sao cho $\varphi(\alpha) \neq 1$.

Giả sử φ là một chuẩn trên trường $\mathbf{K}$, khi đó bằng cách đặt

$$d(\alpha, \beta) = \varphi(\alpha - \beta), \quad \forall \alpha, \beta \in \mathbf{K}$$

thì d là một khoảng cách (mêtric) trên trường $\mathbf{K}$. Khoảng cách này sẽ xác định một cấu trúc tôpô trên trường $\mathbf{K}$.

1.3.2. Ví dụ. 1) Hàm giá trị tuyệt đối thông thường $||$ là chuẩn trên trường số hữu tỉ $\mathbb{Q}$.

2) Hàm giá trị tuyệt đối thông thường $||$ là chuẩn trên trường số thực $\mathbb{R}$.

3) Hàm môđun $||$ là chuẩn trên trường số phức $\mathbb{C}$.

1.3.3. Chuẩn p -adic trên trường số hữu tỉ. Cho p là một số nguyên tố cố định. Với mỗi số hữu tỉ $\alpha \neq 0$, ta viết được một cách duy nhất:

$$\alpha = \frac{a}{b} p^n; \quad a, b, n \in \mathbb{Z}, \quad a, b \text{ không chia hết cho } p.$$

Ta định nghĩa chuẩn p -adic $|\cdot|_p$ trên trường số hữu tỉ $\mathbb{Q}$ là hàm số

$$\varphi_p : \mathbb{Q} \rightarrow \mathbb{R} \text{ xác định bởi } \varphi_p(0) = |0|_p = 0; \quad \varphi_p(\alpha) = |\alpha|_p = p^{-n}.$$

Ta có $|\cdot|_p$ là chuẩn không Acsimet trên trường $\mathbb{Q}$.

1.3.4. Các tính chất của trường định chuẩn. Cho $(\mathbf{K}, \varphi)$ là một trường định chuẩn, khi đó ta có:

$$1) \quad \varphi(1) = \varphi(-1) = 1.$$

$$2) \quad \varphi(a) = \varphi(-a), \quad \forall a \in \mathbf{K}.$$

$$3) \quad |\varphi(a) - \varphi(b)| \leq \varphi(a - b), \quad \forall a, b \in \mathbf{K}.$$

$$4) \quad \varphi\left(\sum_{i=1}^n a_i\right) \leq \sum_{i=1}^n \varphi(a_i).$$

$$5) \quad \varphi(a^{-1}) = \varphi(a)^{-1} = \frac{1}{\varphi(a)}, \quad \forall a \in \mathbf{K}, a \neq \mathbf{0}.$$

$$6) \quad \varphi(ab^{-1}) = \frac{\varphi(a)}{\varphi(b)}, \quad \forall a, b \in \mathbf{K}, b \neq \mathbf{0}.$$

1.3.5. Trường định chuẩn đầy đủ. Giả sử $(\mathbf{K}, \varphi)$ là trường định chuẩn.

Khi đó:

- Dãy $\{\alpha_n\}_{n \in \mathbb{N}}$ các phần tử của $\mathbf{K}$, được gọi là *hội tụ về phần tử* $\alpha \in \mathbf{K}$ (theo chuẩn φ) nếu với mỗi số thực $\varepsilon > 0$ tùy ý, tồn tại một số tự nhiên n_0 sao cho $\varphi(\alpha_n - \alpha) < \varepsilon, \forall n > n_0$. Ta kí hiệu: $\lim_{n \rightarrow \infty} \alpha_n = \alpha$.

- Dãy $\{\alpha_n\}_{n \in \mathbb{N}}$ các phần tử của $\mathbf{K}$ được gọi là *dãy không* (theo chuẩn φ) nếu $\lim_{n \rightarrow \infty} \alpha_n = 0$.

- Dãy $\{\alpha_n\}_{n \in \mathbb{N}}$ các phần tử của $\mathbf{K}$ được gọi là *dãy cơ bản* hay *dãy Cauchy* (theo chuẩn φ) nếu với mỗi số thực $\varepsilon > 0$ tùy ý, tồn tại một số tự nhiên n_0 sao cho $\varphi(\alpha_n - \alpha_m) < \varepsilon, \forall n, m > n_0$.

Trường định chuẩn $(\mathbf{K}, \varphi)$ được gọi là *trường định chuẩn đầy đủ* nếu trong nó mọi dãy cơ bản đều là dãy hội tụ (theo chuẩn φ).

1.3.6. Định lý. *Trong trường định chuẩn mọi dãy hội tụ là dãy cơ bản. Tuy nhiên điều ngược lại không đúng.*

1.3.7. Hệ quả. *Trường số hữu tỉ $\mathbb{Q}$ là trường không đầy đủ theo chuẩn giá trị tuyệt đối.*

1.3.8. Định lý. *Chuẩn φ trên trường $\mathbf{K}$ là chuẩn không Asimet khi và chỉ khi $\varphi(n) \leq 1, \forall n \in \mathbb{N}$.*

1.3.9. Sự tương đương giữa các chuẩn. Các chuẩn φ và ψ trên cùng một trường $\mathbf{K}$ được gọi là *tương đương với nhau* và ký hiệu bởi $\varphi \sim \psi$ nếu chúng xác định trên $\mathbf{K}$ cùng một tính hội tụ, nghĩa là $\varphi(x_n - x) \rightarrow 0$ khi và chỉ khi $\psi(x_n - x) \rightarrow 0$ theo chuẩn giá trị tuyệt đối trong trường số thực $\mathbb{R}$.

1.3.10. Định lý. *Giả sử φ và ψ là các chuẩn trên trường $\mathbf{K}$. Khi đó, φ và ψ là tương đương với nhau khi và chỉ khi $\forall x \in \mathbf{K} (\varphi(x) < 1 \Leftrightarrow \psi(x) < 1)$.*

1.3.11. Định lý. *Trên trường hữu hạn chỉ có duy nhất một chuẩn tầm thường.*

1.3.12. Mệnh đề. *Cho φ là chuẩn không Acsimet trên $\mathbf{K}$. Nếu các giá*

trị thực $\varphi(\alpha)$ và $\varphi(\beta)$ khác nhau thì:

$$\varphi(\alpha + \beta) = \max\{\varphi(\alpha), \varphi(\beta)\}, \forall \alpha, \beta \in K.$$

1.3.13. Mệnh đề. Hàm số $\varphi(x) = |x|^\alpha$, với α là một số thực tùy ý thỏa mãn điều kiện $0 < \alpha \leq 1$, là một chuẩn trên trường số hữu tỉ $\mathbb{Q}$.

1.3.14. Định lý Ostrowski. Các chuẩn $\varphi(x) = |x|^\alpha$ với $0 < \alpha \leq 1$ và các chuẩn p -adic $|\cdot|_p$ với tất cả các số nguyên tố p nhận hết các chuẩn không tầm thường của trường số hữu tỉ $\mathbb{Q}$. Nói khác đi, một chuẩn không tầm thường trên trường số hữu tỉ $\mathbb{Q}$ là tương đương với một trong hai chuẩn sau:

- (i) hoặc chuẩn giá trị tuyệt đối $|\cdot|_\infty$
- (ii) hoặc chuẩn p -adic $|\cdot|_p$, với p là số nguyên tố nào đó.

Như vậy Định lý Ostrowski khẳng định trên trường số hữu tỉ chỉ có hai kiểu chuẩn (sai khác nhau một tương đương). Do đó, chỉ có hai hướng mở rộng $\mathbb{Q}$ thành trường đầy đủ như sau:

1 – Nếu xuất phát từ $\mathbb{Q}$ theo chuẩn giá trị tuyệt đối $|\cdot|_\infty$ thì bằng phương pháp Cantor người ta sẽ xây dựng được trường số thực $\mathbb{R}$ là bổ sung đầy đủ của $\mathbb{Q}$ (trường $\mathbb{R}$ là trường đầy đủ bé nhất chứa trường $\mathbb{Q}$).

2 – Nếu xuất phát từ $\mathbb{Q}$ theo chuẩn p -adic $|\cdot|_p$ thì cũng bằng phương pháp Cantor người ta thu được trường các số p -adic $\mathbb{Q}_p$ là mở rộng đầy đủ của $\mathbb{Q}$. Chẳng hạn các trường: $\mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \mathbb{Q}_7, \dots$

Chương 2

ĐA THỨC DUY NHẤT CHO HỌ CÁC HÀM PHÂN HÌNH KHÁC HẰNG

Trong chương này, chúng tôi tìm hiểu phương pháp xây dựng các 1-dạng chính quy kiểu Wronski trên một đường cong đại số. Đồng thời, chúng tôi tìm hiểu một số điều kiện đủ để một đa thức một biến trên trường $\mathbf{K}$ là đa thức duy nhất, đa thức duy nhất mạnh cho họ các hàm phân hình khác hằng trên $\mathbf{K}$ trong trường hợp đặc số của trường $\mathbf{K}$ chia hết bậc của đa thức. Nội dung của chương này được tham khảo trong bài báo [5].

2.1. 1-dạng chính quy kiểu Wronski trên một đường cong đại số

Phương pháp xây dựng các 1-dạng kiểu Wronski được đưa ra dựa trên việc điều chỉnh các 1-dạng hữu tỷ

$$\frac{\begin{vmatrix} t_i & t_j \\ dt_i & dt_j \end{vmatrix}}{t_j^2} = \frac{t_i}{t_j} \begin{vmatrix} 1 & 1 \\ \frac{dt_i}{t_i} & \frac{dt_j}{t_j} \end{vmatrix} = -d\left(\frac{t_i}{t_j}\right), i \neq j$$

trong đó $[t_0, t_1, t_2]$ là các tọa độ đồng nhất của $P^2(\mathbf{K})$, hoặc các 1-dạng hữu tỷ tổng quát hơn có dạng

$$v d\left(\frac{t_j}{t_k}\right) - u d\left(\frac{t_i}{t_k}\right) = \begin{vmatrix} 1 & 1 \\ u d\left(\frac{t_i}{t_k}\right) & v d\left(\frac{t_j}{t_k}\right) \end{vmatrix},$$

với $0 \leq i, j, k \leq 2, u, v \in \mathbf{K}$.

2.1.1. Định nghĩa. Giả sử $\mathcal{D}$ là một đường cong trong $P^2(\mathbf{K})$. 1-dạng δ trên $\mathcal{D}$ gọi là *chính quy* nếu nó là hạn chế của 1-dạng hữu tỷ trên $P^2(\mathbf{K})$ sao cho không có cực điểm nào của δ thuộc $\mathcal{D}$.

1-dạng chính quy trên $\mathcal{D}$ gọi là *1-dạng kiểu Wronski* nếu nó có dạng

$$\frac{U}{V} W(t_i, t_j) \text{ với } W(t_i, t_j) = \begin{vmatrix} t_i & t_j \\ dt_i & dt_j \end{vmatrix},$$

trong đó U và V là các đa thức thuần nhất sao cho $\deg U + 2 = \deg V$.

2.1.2. Phương pháp xây dựng

Giả sử $A(t_0, t_1, t_2)$ là đa thức thuần nhất trên trường $\mathbf{K}$ và $\mathcal{D}$ là đường cong trong $P^2(\mathbf{K})$ xác định bởi đa thức $A(t_0, t_1, t_2)$:

$$\mathcal{D} = \{[t_0, t_1, t_2] \in P^2(\mathbf{K}) : A(t_0, t_1, t_2) = 0\}.$$

Theo định lý Euler, với $[t_0, t_1, t_2] \in \mathcal{D}$, ta có

$$t_0 \frac{\partial A}{\partial t_0}(t_0, t_1, t_2) + t_1 \frac{\partial A}{\partial t_1}(t_0, t_1, t_2) + t_2 \frac{\partial A}{\partial t_2}(t_0, t_1, t_2) = 0. \quad (2.1)$$

Phương trình siêu phẳng tiếp xúc với $\mathcal{D}$ tại điểm $[t_0, t_1, t_2] \in \mathcal{D}$ xác định bởi

$$\frac{\partial A}{\partial t_0}(t_0, t_1, t_2) dt_0 + \frac{\partial A}{\partial t_1}(t_0, t_1, t_2) dt_1 + \frac{\partial A}{\partial t_2}(t_0, t_1, t_2) dt_2 = 0. \quad (2.2)$$

Kết hợp (2.1) và (2.2) ta có hệ phương trình

$$\begin{cases} t_0 \frac{\partial A}{\partial t_0}(t_0, t_1, t_2) + t_1 \frac{\partial A}{\partial t_1}(t_0, t_1, t_2) = -t_2 \frac{\partial A}{\partial t_2}(t_0, t_1, t_2) \\ t_0 \frac{\partial A}{\partial t_0}(t_0, t_1, t_2) dt_0 + t_1 \frac{\partial A}{\partial t_1}(t_0, t_1, t_2) dt_1 = -\frac{\partial A}{\partial t_2}(t_0, t_1, t_2) dt_2. \end{cases}$$

Nếu

$$\frac{\partial A}{\partial t_0}(t_0, t_1, t_2) \neq 0,$$

$$\frac{\partial A}{\partial t_1}(t_0, t_1, t_2) \neq 0,$$

$$\frac{\partial A}{\partial t_2}(t_0, t_1, t_2) \neq 0,$$

thì theo quy tắc Gramer, ta có

$$\frac{\begin{vmatrix} t_0 & t_1 \\ dt_0 & dt_1 \end{vmatrix}}{\frac{\partial A}{\partial t_2}(t_0, t_1, t_2)} = \frac{\begin{vmatrix} t_1 & t_2 \\ dt_1 & dt_2 \end{vmatrix}}{\frac{\partial A}{\partial t_0}(t_0, t_1, t_2)} = \frac{\begin{vmatrix} t_2 & t_0 \\ dt_2 & dt_0 \end{vmatrix}}{\frac{\partial A}{\partial t_1}(t_0, t_1, t_2)} \quad (2.3)$$

là 1-dạng hữu tỷ kiểu Wronski. Hơn nữa mỗi 1-dạng hữu tỷ

$$\begin{aligned} & \frac{\begin{vmatrix} t_0 & t_1 \\ dt_0 & dt_1 \end{vmatrix}}{\frac{\partial A}{\partial t_2}(t_0, t_1, t_2)}, \\ & \frac{\begin{vmatrix} t_1 & t_2 \\ dt_1 & dt_2 \end{vmatrix}}{\frac{\partial A}{\partial t_0}(t_0, t_1, t_2)}, \\ & \frac{\begin{vmatrix} t_2 & t_0 \\ dt_2 & dt_0 \end{vmatrix}}{\frac{\partial A}{\partial t_1}(t_0, t_1, t_2)} \end{aligned}$$

xác định tốt.

2.2. Đa thức duy nhất cho họ các hàm phân hình khác hằng

Trong mục này, chúng tôi tìm hiểu điều kiện đủ để một đa thức một biến trên trường $\mathbf{K}$ là đa thức duy nhất, đa thức duy nhất mạnh cho họ các hàm phân hình khác hằng trên $\mathbf{K}$ trong trường hợp đặc số của trường $\mathbf{K}$ chia hết bậc của đa thức.

Giả sử $\mathbf{K}$ là một trường đóng đại số có đặc số $p \geq 0$, đầy đủ với giá trị tuyệt đối không Acsimet. Cho $\mathfrak{B}^*(\mathbf{K})$ là tập các hàm phân hình khác hằng xác định trên $\mathbf{K}$ và $\mathcal{F}$ là tập con khác rỗng của $\mathfrak{B}^*(\mathbf{K})$.

2.2.1. Định nghĩa. Đa thức một biến P xác định trên trường $\mathbf{K}$ được gọi là *đa thức duy nhất cho họ hàm $\mathcal{F}$* nếu với mọi hàm khác hằng $f, g \in \mathcal{F}$ thỏa mãn điều kiện $P(f) = P(g)$ thì $f = g$.

2.2.2. Định nghĩa. Đa thức một biến P xác định trên trường $\mathbf{K}$ được gọi là *đa thức duy nhất mạnh cho họ hàm $\mathcal{F}$* nếu với mọi hàm khác hằng $f, g \in \mathcal{F}$ và hằng số c khác 0 thỏa mãn điều kiện $P(f) = cP(g)$ thì $c = 1$ và $f = g$.

2.2.3. Định nghĩa. Tập con S của trường $\mathbf{K}$ gọi là *tập cứng affin* nếu không tồn tại phép biến đổi affin $\alpha = ux + v$; $u, v \in \mathbf{K}$ khác phép đồng nhất để $\alpha(S) = S$.

Trong suốt chương này, chúng ta giả thiết rằng $P(X)$ là một đa thức bậc n trong $\mathbf{K}[X]$. Ta ký hiệu l là số nghiệm phân biệt của $P'(X)$, và các nghiệm của $P'(X)$ là $\alpha_1, \dots, \alpha_l$. Ta ký hiệu $m_1, \dots, m_l$ lần lượt là các bội của các nghiệm của $P'(X)$. Như vậy

$$P'(X) = a(X - \alpha_1)^{m_1} \cdots (X - \alpha_l)^{m_l},$$

trong đó a là hằng số khác không.

2.2.4. Định nghĩa. Đa thức $P(X)$ gọi là *thỏa mãn Giả thiết I* nếu:

$$P(\alpha_i) \neq P(\alpha_j) \tag{2.4}$$

với mọi $1 \leq i \neq j \leq l$.

Không mất tính tổng quát, ta giả sử rằng ta có các α_i để m_i không tăng. Chúng ta lưu ý rằng Giả thiết I là một điều kiện chung, và với Giả thiết I thì việc lập luận, tính toán được thuận lợi hơn.

Ta ký hiệu μ_i là số bội của $X - \alpha_i$ trong $P(X) - P(\alpha_i)$. Chúng ta

xác định $b_{i,j}$ bằng cách viết

$$P(X) - P(\alpha_i) = \sum_{j=\mu_i}^n b_{i,j}(X - \alpha_i)^j.$$

Khi đó đa thức thuần nhất $A_{i,\mu_i}(X, Y, Z)$ xác định bởi

$$\begin{aligned} A_{i,\mu_i}(X, Y, Z) = & b_{i,\mu_i} Z \left[\frac{(X - \alpha_i Z)^{\mu_i} - (Y - \alpha_i Z)^{\mu_i}}{X - Y} \right] \\ & + b_{i,\mu_i+1} \left[\frac{(X - \alpha_i Z)^{\mu_i+1} - (Y - \alpha_i Z)^{\mu_i+1}}{X - Y} \right]. \end{aligned}$$

Đặt $m = 1 + \sum_{i=1}^l m_i$. Khi $c \neq 0, 1$ và $m_1 = \dots = m_l = 1$, thì với một hoán vị ϕ của $\{1, \dots, l\}$ sao cho $\phi(i) \neq i$, ta xác định đa thức thuần nhất $B_{i,m}(X, Y, Z)$ bởi

$$B_{i,m}(X, Y, Z) = \sum_{j=2}^m \left[b_{i,j}(X - \alpha_i Z)^j - c b_{\phi(i),j}(Y - \alpha_{\phi(i)} Z)^j \right] Z^{m-j}.$$

Khi đó ta đặt

$$B(i, m) := B_{i,m}(X, Y, 1).$$

2.2.5. Định lý. *Giả sử đa thức $P(X)$ là một đa thức thỏa mãn Giả thiết I và $p|n$. Giả sử S là tập không điểm của $P(X)$ và S là tập cứng afin. Giả sử m_i được sắp xếp theo thứ tự không tăng. Khi đó*

(I) $P(X)$ là một đa thức duy nhất cho họ $\mathfrak{B}^*(\mathbf{K})$ nếu một trong các trường hợp (A), (B) hoặc (C) xảy ra, trong đó:

(A) $l \geq 3$;

(B) $l = 2$ và

(1) $m_2 \geq 2$, hoặc

(2) $m_2 = 1$ và

(a) $\mu_1 \leq m_1$, hoặc

(b) $\mu_1 = m_1 + 1$ và

(i) $(m_1 + 2) \nmid n$, hoặc

- (ii) $(m_1 + 2) \mid n$, $A_{1,m_1}(X, Y, 1)$ không là nhân tử của $[P(X) - P(Y)] / (X - Y)$;
- (C) $l = 1$ và (1), (2) hoặc (3) xảy ra, trong đó:
- (1) $\mu_1 \leq m_1 - 1$,
- (2) $\mu_1 = m_1$ và
- (a) $(m_1 + 1) \nmid n$, hoặc
- (b) $(m_1 + 1) \mid n$, $p \geq 5$, và $A_{1,m_1}(X, Y, 1)$ không phải là nhân tử của $[P(X) - P(Y)] / (X - Y)$,
- (3) $\mu_1 = m_1 + 1$, và
- (a) $u = 2$, $p \geq 5$ và $A_{1,m_1+1}(X, Y, 1)$ không là nhân tử của $P(X) - P(Y)$, hoặc
- (b) $u \geq 3$ và $m_1 \geq 2$, trừ khi $(m_1, p) = (2, 2)$, hoặc $(u, m_1, p) = (3, 2, 5)$ hoặc $(3, 3, 3)$, trong đó u được xác định bằng cách viết $P(X) - P(\alpha_1) = b_{1,m_1+1}(X - \alpha_1)^{m_1+1} + b_{1,m_1+u}(X - \alpha_1)^{m_1+u} + \dots$ với $b_{1,m_1+u} \neq 0$.
- (II) Nếu $P(X)$ là đa thức duy nhất cho họ $\mathfrak{B}^*(\mathbf{K})$ thì $P(X)$ cũng là đa thức duy nhất mạnh cho họ $\mathfrak{B}^*(\mathbf{K})$ ngoại trừ các trường hợp sau:
- (A) $l = 3$, $m_1 = m_2 = m_3 = 1$, $3 \mid n - 1$, $4 \mid n$, tồn tại một hoán vị ϕ của $\{1, 2, 3\}$ sao cho $\phi(i) \neq i$ với $i = 1, 2, 3$ và tồn tại nghiệm w của $w^2 + w + 1 = 0$ sao cho $w = \frac{P(\alpha_i)}{P(\alpha_{\phi(i)})}$ với $i = 1, 2, 3$, và $B(1, 4) = B(2, 4) = B(3, 4)$ và $B(i, 4)$ không là nhân tử của $P(X) - wP(Y)$, với $i = 1, 2, 3$;
- (B) $l = 2$, $m_1 = m_2 = 1$, $3 \mid n$ và tồn tại hằng số $c \neq 0, 1, -1$ sao cho với $\{i, j\} = \{1, 2\}$, ta có $P(\alpha_i) = cP(\alpha_j)$ và $B(i, 3)$ là một nhân tử của $P(X) - cP(Y)$;
- (C) $l=2$, $m_1 = m_2 = 1$, n lẻ, $3 \mid n$, $P(\alpha_1) = -P(\alpha_2)$, $B(1, 3) = B(2, 3)$

và $B(1, 3)/(X + Y - \alpha_1 - \alpha_2)$ là một nhân tử của $P(X) + P(Y)$.

Trong chương này ta xem xét đa thức P có dạng

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0.$$

Ta ký hiệu μ_i là số bội của $X - \alpha_i$ trong $P(X) - P(\alpha_i)$. Khi đó $P(X) - P(\alpha_i)$ có dạng

$$\begin{aligned} P(X) - P(\alpha_i) &= *(X - \alpha_i)^{\mu_i} \\ &+ \cdots + *(X - \alpha_i)^{m_i+1} + \cdots + *(X - \alpha_i)^n \end{aligned} \quad (2.5)$$

trong đó ta sử dụng $*$ để biểu thị phần tử khác không trong $\mathbf{K}$. Chúng ta sẽ sử dụng ký hiệu này trong suốt chương 2. Lưu ý rằng $\mu_i \leq m_i + 1$ kể cả trong trường hợp đặc số của $\mathbf{K}$ bằng 0.

Ký hiệu $F(X, Y, Z)$ là đa thức thuần nhất của đa thức hai biến

$$\frac{P(X) - P(Y)}{X - Y} = \sum_{k=1}^n a_k \sum_{j=0}^{k-1} X^{k-1-j} Y^j,$$

ta có

$$\begin{aligned} F(X, Y, Z) &= \sum_{k=1}^n \sum_{j=0}^{k-1} a_k X^{k-1-j} Y^j Z^{n-k} \\ &= Z^n \frac{P(X/Z) - P(Y/Z)}{X - Y}, \end{aligned} \quad (2.6)$$

Ký hiệu C là đường cong xác định bởi phương trình $F(X, Y, Z) = 0$. Tương tự, giả sử $F_c(X, Y, Z)$ là đa thức thuần nhất của đa thức $P(X) - cP(Y)$ với $c \neq 0, 1$ và C_c là đường cong xác định bởi phương trình $F_c(X, Y, Z) = 0$.

Mục tiêu của chúng ta là xây dựng trên đường cong C và mỗi đường cong C_c , $c \neq 0, 1$, 1-dạng chính quy hoặc tích các 1-dạng chính quy không tầm thường trên mỗi một thành phần của đường cong.

Bây giờ ta xem xét việc xây dựng này trên đường cong xác định bởi phương trình $F(X, Y, Z) = 0$.

Ta có thể biểu thị đa thức $F(X, Y, Z)$ dưới dạng một đa thức theo $X - \alpha_i Z$ và $Y - \alpha_i Z$:

$$\begin{aligned} F(X, Y, Z) = & * \left[\frac{(X - \alpha_i Z)^{\mu_i} - (Y - \alpha_i Z)^{\mu_i}}{X - Y} \right] Z^{n-\mu_i} \\ & + * \left[\frac{(X - \alpha_i Z)^{w_i} - (Y - \alpha_i Z)^{w_i}}{X - Y} \right] Z^{n-w_i} \\ & + \cdots + * \left[\frac{(X - \alpha_i Z)^n - (Y - \alpha_i Z)^n}{X - Y} \right], \end{aligned} \quad (2.7)$$

trong đó w_i là bậc của số hạng không triệt tiêu thứ hai trong (2.5). Từ (2.7) và $F(\varphi_0, \varphi_1, \varphi_2) = 0$ với tham số hóa $\varphi = (\varphi_0, \varphi_1, \varphi_2)$ tại $p_i = (\alpha_i, \alpha_i, 1)$ ta có

$$\text{ord}_{\mathbf{p}_i, \varphi}(X - \alpha_i Z) = \text{ord}_{\mathbf{p}_i, \varphi}(Y - \alpha_i Z), \quad (2.8)$$

do đó

$$\begin{aligned} \text{ord}_{\mathbf{p}_i, \varphi}(X - Y) &= \text{ord}_{\mathbf{p}_i}(X - \alpha_i Z - (Y - \alpha_i Z)) \\ &\geq \text{ord}_{\mathbf{p}_i, \varphi}(X - \alpha_i Z) \end{aligned} \quad (2.9)$$

và

$$\begin{aligned} \text{ord}_{\mathbf{p}_i, \varphi}((X - \alpha_i Z)^{\mu_i-1} + \cdots + (Y - \alpha_i Z)^{\mu_i-1}) \\ \geq (w_i - 1) \text{ord}_{\mathbf{p}_i, \varphi}(X - \alpha_i Z). \end{aligned} \quad (2.10)$$

Theo định lý Euler ta có điều kiện $F(X, Y, Z) = 0$ tương đương với

$$X \frac{\partial F}{\partial X} + Y \frac{\partial F}{\partial Y} + Z \frac{\partial F}{\partial Z} = 0.$$

Không gian tiếp xúc với đường cong C xác định bởi các phương trình $F(X, Y, Z) = 0$ và

$$dX \frac{\partial F}{\partial X} + dY \frac{\partial F}{\partial Y} + dZ \frac{\partial F}{\partial Z} = 0.$$

Theo quy tắc Gramer ta có

$$\gamma := \frac{W(X, Y)}{\frac{\partial F}{\partial Z}} = \frac{W(Y, Z)}{\frac{\partial F}{\partial X}} = \frac{W(Z, X)}{\frac{\partial F}{\partial Y}} \quad (2.11)$$

là 1-dạng hữu tỷ xác định tốt trên $\pi^{-1}(C)$, với $\pi : \mathbf{K}^3 \setminus \{0\} \rightarrow \mathbf{P}^2$ là phép chiếu thông thường, trong đó

$$W(X, Y) = \begin{vmatrix} X & Y \\ dX & dY \end{vmatrix}, W(Y, Z) = \begin{vmatrix} Y & Z \\ dY & dZ \end{vmatrix}, W(Z, X) = \begin{vmatrix} Z & X \\ dZ & dX \end{vmatrix}$$

Để chứng minh định lý 2.2.5 ta cần một số bổ đề sau đây.

2.2.6. Bổ đề [5]. *Giả sử đa thức P thỏa mãn Giả thiết I và m_i được xếp theo thứ tự không tăng. Khi đó thành phần bất khả quy bất kỳ của đường cong C đều chứa 1-dạng chính quy không tầm thường trong các trường hợp sau đây:*

- (i) $l \geq 3$ hoặc $l = 2$ và $m_2 = 2$;
- (ii) $p > 0$, $l = 2$, $m_2 = 1$, $\mu_1 \leq m_1$ và đường cong C không có các thành phần tuyến tính;
- (iii) $p > 0$, $l = 1$, $\mu_1 \leq m_1 - 1$ và đường cong C không có các thành phần tuyến tính.

Bây giờ ta đặt

$$m = 1 + \sum_{i=1}^l m_i. \quad (2.12)$$

Nếu n chia hết cho p thì m là số mũ lớn nhất trong $P(X)$ mà không chia hết cho p .

2.2.7. Bổ đề. *Giả sử rằng $p > 0$ và $p|n$. Ký hiệu $\gcd(n, m) = d$ và ξ_d^j , $0 \leq j \leq d - 1$, là các nghiệm nguyên thủy của $X^d = 1$. Khi đó, các cực điểm có thể có của dạng vi phân*

$$\zeta := \frac{W(Y, Z)}{Z(X - \alpha_1 Z)^{m_1} \dots (X - \alpha_l Z)^{m_l}}$$

trên $\pi^{-1}(C)$ là các điểm $\mathbf{p}_i = (\alpha_i, \alpha_i, 1)$, $1 \leq i \leq l$, và $\mathbf{q}_j = (\xi_d^j, 1, 0)$,

$$0 \leq j \leq d-1.$$

Chứng minh. Với $p|n$, ta có

$$\frac{\partial F}{\partial Z}(X, Y, Z) = a_m(n-m)Z^{n-m-1} \left(\sum_{i=0}^{m-1} X^{m-1-i}Y^i + ZH_{m-2} \right), \quad (2.13)$$

trong đó H_{m-2} là đa thức thuần nhất bậc $m-2$ theo X, Y, Z . Hạn chế $\partial F/\partial X$ và $\partial F/\partial Y$ trên đường cong C xác định bởi phương trình $F(X, Y, Z)=0$ cho ta

$$\frac{\partial F}{\partial X}(X, Y, Z) = \frac{ma_m Z^{n-m} \prod_{i=1}^l (X - \alpha_i Z)^{m_i}}{X - Y},$$

$$\frac{\partial F}{\partial Y}(X, Y, Z) = \frac{-ma_m Z^{n-m} \prod_{i=1}^l (Y - \alpha_i Z)^{m_i}}{X - Y}.$$

Kết hợp (2.13) và (2.11), ta có

$$\begin{aligned} \zeta &= \frac{W(Y, Z)}{Z(X - \alpha_1 Z)^{m_1} \cdots (X - \alpha_l Z)^{m_l}} \\ &\equiv - \frac{W(Z, X)}{Z(Y - \alpha_1 Z)^{m_1} \cdots (Y - \alpha_l Z)^{m_l}} \\ &\equiv - \frac{W(X, Y)}{(X - Y)(X^{m-1} + X^{m-2}Y + \cdots Y^{m-1} + ZH_{m-2})}, \end{aligned} \quad (2.14)$$

là 1-dạng hữu tỉ trên $\pi^{-1}(C)$. Các cực điểm có thể có của ζ trên $\pi^{-1}(C)$ là $\mathfrak{p}_i = (\alpha_i, \alpha_i, 1)$, $1 \leq i \leq l$, và $(x, 1, 0)$ với $x^n = 1$ và $x^m = 1$. Đồng thời ξ_d^j , $0 \leq j \leq d-1$, là các nghiệm thỏa mãn $x^n = 1$ và $x^m = 1$. Do đó, $\mathfrak{q}_j = (\xi_d^j, 1, 0)$, $0 \leq j \leq d-1$, là các cực điểm có thể có của ζ trên $\pi^{-1}(C) \cap [Z = 0]$. $\square$

Giả sử rằng $*(X - \alpha_i Z)^v$ xuất hiện trong biểu thức của (2.5), và giả sử rằng có một số hạng $*(X - \alpha_i Z)^{v_1}$ theo sau nó. Gọi $A_{i,v-1}Z^{n-v}$ là tổng các số hạng trong (2.7) cho đến bậc $v-1$ theo X và Y , tức là,

$$A_{i,v-1} = * \left[\frac{(X - \alpha_i Z)^{\mu_i} - (Y - \alpha_i Z)^{\mu_i}}{X - Y} \right] Z^{v-\mu_i} + \cdots$$

$$+ * \left[\frac{(X - \alpha_i Z)^v - (Y - \alpha_i Z)^v}{X - Y} \right]. \quad (2.15)$$

Chúng ta có các đánh giá sau đây về bậc của $A_{i,v-1}$ tại $\mathbf{p}_i$ và $\mathbf{q}_j$.

2.2.8. Bổ đề. *Ta có*

- (i) $\text{ord}_{\mathbf{p}_i, \varphi}(A_{i,v-1}) \geq v \text{ord}_{\mathbf{p}_i, \varphi}(X - \alpha_i Z)$;
- (ii) $\text{ord}_{\mathbf{p}_r, \varphi}(A_{i,m-1}) \geq (p-1) \text{ord}_{\mathbf{p}_r, \varphi}(X - \alpha_r Z)$ với $1 \leq r \leq l$;
- (iii) $p \mid -m \text{ord}_{\mathbf{q}_j, \varphi} Z + \text{ord}_{\mathbf{q}_j, \varphi}((X - Y)A_{i,m-1})$ với $0 \leq j \leq d-1$.

Chứng minh. Trước tiên, chúng ta lưu ý rằng $\mathbf{p}_i = (\alpha_i, \alpha_i, 1)$, $i=1, \dots, l$, và $\mathbf{q}_j$, $0 \leq j \leq d-1$, là những điểm của C . Hơn nữa, từ (2.7) suy ra

$$\text{ord}_{\mathbf{p}_i, \varphi}(A_{i,v-1}) \geq (v_1 - 1) \text{ord}_{\mathbf{p}_i, \varphi}(X - \alpha_i Z) \geq v \text{ord}_{\mathbf{p}_i, \varphi}(X - \alpha_i Z).$$

Như vậy ta có được (i).

Vì m là số mũ lớn nhất trong $P(X)$ không chia hết cho p và n chia hết cho p , nên ta có thể viết

$$F(X, Y, Z) = A_{i,m-1} Z^{n-m} + (X - Y)^{p-1} H(X, Y, Z),$$

trong đó $H(X, Y, Z)$ là đa thức thuần nhất bậc $n-p$. Vì $\mathbf{p}_r = (\alpha_r, \alpha_r, 1) \in C$ nên $\mathbf{p}_r$ thuộc đường cong xác định bởi phương trình $A_{i,m-1}(X, Y, Z) = 0$ và

$$\text{ord}_{\mathbf{p}_r, \varphi}(A_{i,m-1}) \geq (p-1) \text{ord}_{\mathbf{p}_r, \varphi}(X - Y) \geq (p-1) \text{ord}_{\mathbf{p}_r, \varphi}(X - \alpha_r Z).$$

Điều này suy ra (ii).

Vì $(X - Y) F(X, Y, Z) - (X - Y) A_{i,m-1} Z^{n-m}$ là lũy thừa thứ p , nên đối với những điểm $\mathbf{q}_j \in C$, $j = 0, \dots, d-1$, ta có

$$p \mid (n - m) \text{ord}_{\mathbf{q}_j, \varphi} Z + \text{ord}_{\mathbf{q}_j, \varphi}((X - Y)A_{i,m-1}),$$

tương đương với

$$p \mid -m \text{ord}_{\mathbf{q}_j, \varphi} Z + \text{ord}_{\mathbf{q}_j, \varphi}((X - Y)A_{i,m-1})$$

do n chia hết cho p . Như vậy ta được (iii). $\square$

2.2.9. Bổ đề [5]. Giả sử λ_1, λ_2 là các hằng số khác 0 và b là một số nguyên dương. Đặt

$$A(X, Y, Z) = \lambda_1 \left[\frac{(X - \alpha Z)^b - (Y - \alpha Z)^b}{X - Y} \right] Z + \lambda_2 \left[\frac{(X - \alpha Z)^{b+1} - (Y - \alpha Z)^{b+1}}{X - Y} \right].$$

Khi đó đường cong xác định bởi phương trình $A(X, Y, Z) = 0$ là đường cong bất khả quy có giống 0.

2.2.10. Bổ đề. Giả sử $P(X)$ là đa thức bậc n thỏa mãn Giả thiết I. Giả sử m_i được sắp xếp theo thứ tự không tăng. Giả sử rằng $p > 0$ và $p|n$. Nếu đường cong C không có thành phần tuyến tính thì bất kỳ thành phần bất khả quy nào của C cũng chứa tích các 1-dạng chính quy không tầm thường trong các trường hợp sau đây:

(i) $l \geq 3$; $l = 2$ và $m_2 \geq 2$; $l = 2, m_2 = 1$ và $\mu_1 \leq m_1$; hoặc $l = 1$ và $\mu_1 \leq m_1 - 1$;

(ii) $l = 2, m_2 = 1, \mu_1 = m_1 + 1$ và

(a) $(m_1 + 2) \nmid n$, hoặc

(b) $(m_1 + 2) | n$ và A_{1, m_1+1} không là nhân tử của $F(X, Y, Z)$;

(iii) $l = 1, \mu_1 = m_1$ và

(a) $(m_1 + 1) \nmid n$, hoặc

(b) $(m_1 + 1) | n, p \geq 5$, và A_{1, m_1} là một nhân tử của $F(X, Y, Z)$;

(iv) $l = 1, \mu_1 = m_1 + 1$, và

(a) $u = 2, p \geq 5$ và A_{1, m_1+1} không là nhân tử của $F(X, Y, Z)$, hoặc

(b) $u \geq 3$ và $m_1 \geq 2$, ngoại trừ trường hợp $(m_1, p) = (2, 2)$ hoặc

$(u, m_1, p) = (3, 2, 5), (3, 3, 3)$, trong đó u được xác định bởi khai triển

$P(X) = P(\alpha_1) + *(X - \alpha_1)^{m_1+1} + *(X - \alpha_1)^{m_1+u} + \text{các}$
số hạng có bậc cao hơn.

Chứng minh. Trường hợp (i) được suy ra từ Bổ đề 2.2.6.

Đặt $m = 1 + \sum_{i=1}^l m_i$. Đối với trường hợp (ii), ta có $m = m_1 + 2$, $\mu_1 = m_1 + 1$, $\mu_2 = 2$, do đó $p \nmid m_1 + 2$, $p \nmid m_1 + 1$ và $p \neq 2$. Hơn nữa,

$$A_{1,m_1+1} = *Z \left[\frac{(X - \alpha_1 Z)^{m_1+1} - (Y - \alpha_1 Z)^{m_1+1}}{X - Y} \right] \\ + * \left[\frac{(X - \alpha_1 Z)^{m_1+2} - (Y - \alpha_1 Z)^{m_1+2}}{X - Y} \right],$$

xác định một đường cong bất khả quy có giống 0 theo Bổ đề 2.2.9.

Lấy

$$\omega = \left(\frac{W(Y, Z)}{Z(X - \alpha_1 Z)^{m_1}(X - \alpha_2 Z)} \right)^{m_1+e} ((X - Y)A_{1,m_1+1}Z^{e-2})^{m_1}.$$

Ta có ω xác định tốt trên $\mathbf{P}^2$, trong đó $e = 3$ nếu bậc của số hạng không triệt tiêu sau bậc $m_1 + 2$ trong biểu thức của (2.5) là $m_1 + 3$, và nếu không thì $e = 4$. Trên đường cong C , ω chỉ có các cực điểm tại $\mathbf{p}_j = (\alpha_j, \alpha_j, 1)$, $j = 1, 2$ và $\mathbf{q}_j = (\xi_d^j, 1, 0)$, $0 \leq j \leq d - 1$, với $d = \gcd(n, m_1 + 2)$ và ξ_d là nghiệm nguyên thủy của $X^d = 1$. Theo Bổ đề 2.2.8 (i) ta có ω chính quy tại $\mathbf{p}_1$ và

$$\text{ord}_{\mathbf{p}_1, \varphi} A_{1,m_1+1} \geq (m_1 + e - 1) \text{ord}_{\mathbf{p}_1, \varphi} (X - \alpha_1 Z).$$

Theo Bổ đề 2.2.8 (ii), ta có $\text{ord}_{\mathbf{p}_2, \varphi} A_{1,m_1+1} \geq (p - 1) \text{ord}_{\mathbf{p}_2, \varphi} (X - \alpha_2 Z)$, do đó

$$\text{ord}_{\mathbf{p}_2, \varphi} \omega \geq (m_1 p - m_1 - e) \text{ord}_{\mathbf{p}_2, \varphi} (X - \alpha_2 Z) \geq m_1(p - 1) - 4 \geq 0$$

khi $p \geq 3$ hoặc $p = 3$ và $m_1 \geq 2$. Chúng ta lưu ý rằng nếu $p = 3$ thì $m_1 \neq 1$ vì $p \nmid m_1 + 2$. Do đó, ω là chính quy tại $\mathbf{p}_2$. Đối với các điểm tại

vô cực $\mathfrak{q}_j$, $j = 0, \dots, d-1$, ta có

$$\text{ord}_{\mathfrak{q}_j, \varphi}(A_{1, m_1+1}(X-Y)) + \text{ord}_{\mathfrak{q}_j, \varphi}Z \geq 3, \quad (2.16)$$

vì nếu $\text{ord}_{\mathfrak{q}_j, \varphi}A_{1, m_1+1}(X-Y) = \text{ord}_{\mathfrak{q}_j, \varphi}Z = 1$ thì theo Bổ đề 2.2.8 (iii) suy ra $m-1 = m_1+1$ chia hết cho p , điều này là không thể xảy ra. Tương tự nếu $m_1 = 1$ và $\text{ord}_{\mathfrak{q}_j, \varphi}Z = 1$ thì theo Bổ đề 2.2.8 (iii) suy ra $-3 + \text{ord}_{\mathfrak{q}_j, \varphi}A_{1, m_1+1}(X-Y)$ chia hết cho p , do đó $\text{ord}_{\mathfrak{q}_j, \varphi}A_{1, m_1+1}(X-Y) \geq 3$. Từ đó, nếu $m_1 = 1$ ta thu được

$$\text{ord}_{\mathfrak{q}_j, \varphi}(A_{1, m_1+1}(X-Y)) + 2 \text{ord}_{\mathfrak{q}_j, \varphi}Z \geq 5. \quad (2.17)$$

Hơn nữa, nếu $m_1 = 1$ thì chúng ta có thể lấy $e = 4$ vì bậc của số hạng không triệt tiêu sau số hạng bậc 3 không thể là 4; nếu không thì p sẽ là 2. Trong trường hợp này, ta có

$$\begin{aligned} \text{ord}_{\mathfrak{q}_j, \varphi}\omega &\geq -(m_1 + e) + m_1 \text{ord}_{\mathfrak{q}_j, \varphi}(A_{1, m_1+1}(X-Y)) + m_1(e-2) \text{ord}_{\mathfrak{q}_j, \varphi}Z \\ &\geq m_1 [\text{ord}_{\mathfrak{q}_j, \varphi}(A_{1, m_1+1}(X-Y)) + (e-2) \text{ord}_{\mathfrak{q}_j, \varphi}Z - 1] - e. \end{aligned}$$

Theo (2.16), điều này có nghĩa là $\text{ord}_{\mathfrak{q}_j, \varphi}\omega \geq 2m_1 - 4$ là không âm khi $m_1 \geq 2$. Nếu $m_1 = 1$, thì $e = 4$ và theo (2.17) thì bất đẳng thức trên cho ta

$$\text{ord}_{\mathfrak{q}_j, \varphi}\omega \geq \text{ord}_{\mathfrak{q}_j, \varphi}(A_{1, m_1+1}(X-Y)) + 2 \text{ord}_{\mathfrak{q}_j, \varphi}Z - 5,$$

cũng không âm. Như vậy ω chính quy trên đường cong C . Bây giờ ta cần kiểm tra ω không tầm thường trên mọi thành phần của C . Giả sử rằng $(m_1 + 2) \nmid n$ và $A_{1, m_1+1} \mid F(X, Y, Z)$. Khi đó

$$(X-Y)A_{1, m_1+1} \mid (X-Y)F(X, Y, Z)$$

và

$$(X^{m_1+2} - Y^{m_1+2}) \mid (X^n - Y^n).$$

Giả sử ξ là một nghiệm nguyên thủy của $X^{m_1+2} = 1$ trong $\mathbf{K}$. Nếu $(X^{m_1+2} - Y^{m_1+2}) \mid (X^n - Y^n)$ thì $(\xi, 1)$ cũng là nghiệm của $X^n - Y^n$ và do đó $1 = \xi^n$, điều này không thể xảy ra khi $(m_1 + 2) \nmid n$. Nếu $(m_1 + 2) \mid n$, thì ta cần giả thiết rằng A_{1,m_1+1} không là nhân tử của $F(X, Y, Z)$.

Với trường hợp (iii), ta có $l = 1$ và $\mu_1 = m_1 = m - 1$. Khi đó m_1 chia hết cho p và ta có thể viết $m_1 = p^a b$ với $a, b \geq 1$. Nếu $\gcd(n, m) = 1$ thì

$$\omega := \frac{W(Y, Z)(X - Y)^{p^a-1} \left((X - \alpha_1 Z)^{b-1} + \dots + (Y - \alpha_1 Z)^{b-1} \right)^{p^a}}{Z(X - \alpha_1 Z)^{m_1}}$$

chính quy và không tầm thường trên bất kỳ thành phần nào của đường cong C nếu C không có các thành phần tuyến tính.

Nếu $1 < \gcd(n, m) = d < m$, thì ta có thể viết $m = m_0 d$ với $m_0 \geq 2$ và $d \geq 2$. Khi đó $m - d - 2 = (m_0 - 1)d - 2 \geq 0$. Ta đặt

$$\omega := \left(\frac{W(Y, Z)(X^d - Y^d)}{Z(X - \alpha_1 Z)^{m_1}} \right)^{m_1} A_{1,m_1}^{m_1-d-1}.$$

Vì $\mu_1 = m_1$ nên

$$\begin{aligned} A_{1,m_1} = & *Z \left[\frac{(X - \alpha_1 Z)^{m_1} - (Y - \alpha_1 Z)^{m_1}}{X - Y} \right] \\ & + * \left[\frac{(X - \alpha_1 Z)^{m_1+1} - (Y - \alpha_1 Z)^{m_1+1}}{X - Y} \right], \end{aligned}$$

xác định một đường cong bất khả quy có giống 0. Tương tự, ω chỉ có thể có một cực điểm tại $\mathbf{p}_1$. Vì m_1 chia hết cho p nên bậc của số hạng xuất hiện sau $(X - \alpha_1)^{m_1+1}$ trong (2.5) ít nhất là $m_1 + p$. Lưu ý rằng số hạng như vậy phải tồn tại vì $p \nmid m$ và $p \mid n$. Theo Bổ đề 2.2.8 (i), ta có

$$\text{ord}_{\mathbf{p}_1, \varphi} A_{1,m_1} \geq (m_1 + p) \text{ord}_{\mathbf{p}_1, \varphi} (X - \alpha_1 Z),$$

do đó

$$\text{ord}_{\mathbf{p}_1, \varphi} \omega \geq [(m_1 - d - 1)(m_1 + p) - m_1(m_1 - d)] \text{ord}_{\mathbf{p}_1, \varphi} (X - \alpha_1 Z)$$

$$= [d(pm_0 - m_0 - p) - 2p + 1] \operatorname{ord}_{\mathfrak{p}_1, \varphi}(X - \alpha_1 Z). \quad (2.18)$$

Nếu $p = 2$ thì vì $p \nmid m_1 + 1$ nên ta có $m_0 \geq 3$ và $d \geq 3$. Do đó, theo (2.18) ta có, $\operatorname{ord}_{\mathfrak{p}_1, \varphi} \omega$ không âm. Nếu $m_0 \geq 3$ và $p \geq 3$ thì theo (2.18) ta có, $\operatorname{ord}_{\mathfrak{p}_1, \varphi} \omega \geq 2(2p - 3) - 2p + 1 = 2p - 5$, là số dương. Ta cần kiểm tra trường hợp $m_0 = 2$ và $p \geq 3$. Vì $p \mid m - 1$ nên nếu $m_0 = 2$ và $p \geq 5$ thì $d \geq 3$, và từ (2.18) ta suy ra $\operatorname{ord}_{\mathfrak{p}_1, \varphi} \omega$ là dương. Tương tự, nếu $m_0 = 2$ và $p = 3$, thì d chỉ có thể là 2 hoặc lớn hơn 5. Với $d > 5$ thì $\operatorname{ord}_{\mathfrak{p}_1, \varphi} \omega$ không âm. Ta kiểm tra trường hợp $m_0 = 2$, $p = 3$ và $d = 2$. Trong trường hợp này, chúng ta có

$$\omega = \frac{W(Y, Z)(X^2 - Y^2)}{Z(X - \alpha_1 Z)^3}.$$

Khai triển của $F(X, Y, Z)$ tại $\mathfrak{p}_1 = (\alpha_1, \alpha_1, 1)$ được xác định bởi

$*(X - Y)^2 + * \sum_{i=0}^3 (X - \alpha_1 Z)^{3-i} (Y - \alpha_1 Z)^i +$ số hạng bậc cao hơn,
do đó

$$2 \operatorname{ord}_{\mathfrak{p}_1, \varphi}(X - Y) = 3 \operatorname{ord}_{\mathfrak{p}_1, \varphi}(X - \alpha_1 Z).$$

Điều này có nghĩa là $\operatorname{ord}_{\mathfrak{p}_1, \varphi}(X - \alpha_1 Z) \geq 2$ và

$$\begin{aligned} \operatorname{ord}_{\mathfrak{p}_1, \varphi} \omega &\geq \operatorname{ord}_{\mathfrak{p}_1, \varphi}(X + Y) + \operatorname{ord}_{\mathfrak{p}_1, \varphi}(X - Y) - 2 \operatorname{ord}_{\mathfrak{p}_1, \varphi}(X - \alpha_1 Z) - 1 \\ &\geq \frac{1}{2} \operatorname{ord}_{\mathfrak{p}_1, \varphi}(X - \alpha_1 Z) - 1 \geq 0. \end{aligned}$$

Vì vậy tính chính quy của ω được thiết lập trong mọi trường hợp. Do đường cong xác định bởi phương trình $A_{1, m_1} = 0$ là một đường cong bất khả quy có giống 0 nên ω là không tầm thường trên bất kỳ thành phần nào của C với điều kiện A_{1, m_1} không là nhân tử của $F(X, Y, Z)$. Hơn nữa với $m = m_1 + 1$ và $A_{1, m_1} = A_{1, m-1}$, thì $A_{1, m-1}$ không là nhân tử của $F(X, Y, Z)$ nếu $m \nmid n$.

Đối với trường hợp (iii.b), ta có $m \mid n$ và $\mu_1 = m_1 = m - 1$. Giả sử rằng $p \geq 5$ và $m_1 + u (\geq m_1 + 2)$ là bậc của số hạng triệt tiêu kế tiếp

$(X - \alpha_1)^m$ trong khai triển của $P(X)$ trong (2.5). Vì $p|m_1$ và $p \geq 5$ nên ta có $p|u$, $m_1 \geq 5$ và $u \geq 5$. Khi đó

$$\omega := \left(\frac{W(Y, Z)}{Z(X - \alpha_1 Z)^{m_1}} \right)^{m_1+u} (A_{1,m_1}(X - Y))^{m_1} Z^{(u-2)(m_1-1)-2}$$

chính quy tại $\mathfrak{p}_1$ do các bất đẳng thức

$$(u - 2)(m_1 - 1) - 2 \geq 0,$$

$$\text{ord}_{\mathfrak{p}_1, \varphi} A_{1,m_1} \geq (m_1 + u - 1) \text{ord}_{\mathfrak{p}_1, \varphi} (X - \alpha_1 Z),$$

$$\text{ord}_{\mathfrak{p}_1, \varphi} (X - Y) \geq \text{ord}_{\mathfrak{p}_1, \varphi} (X - \alpha_1 Z).$$

Tại các điểm ở vô cực $\mathfrak{q}_j$, $j = 0, 1, \dots, m - 1$, ta có

$$\begin{aligned} \text{ord}_{\mathfrak{q}_j, \varphi} \omega &\geq ((u - 2)(m_1 - 1) - 2) \text{ord}_{\mathfrak{q}_j, \varphi} Z \\ &\quad + m_1 \text{ord}_{\mathfrak{q}_j, \varphi} (A_{1,m_1}(X - Y)) - m_1 - u \\ &\geq (u - 2)m_1 - u - u = (u - 2)(m_1 - 2) - 4 \geq 0, \end{aligned}$$

khi $u \geq 5$ và $m_1 \geq 5$. Vì đường cong xác định bởi phương trình $A_{1,m_1} = 0$ là một đường cong bất khả quy có giống 0 nên ω là chính quy và không tầm thường trên bất kỳ thành phần nào của C chỉ khi A_{1,m_1} không phải là nhân tử của $F(X, Y, Z)$.

Với trường hợp (iv.a), ta có $l = 1$, $\mu_1 = m_1 + 1 = m$ và $u = 2$, trong đó $m_1 + u$ ($\geq m_1 + 2$) là bậc của số hạng không bị triệt tiêu theo sau $(X - \alpha_1)^m$ trong khai triển của $P(X)$ trong (2.5). Tương tự, trong trường hợp này

$$\begin{aligned} A_{1,m_1+1} &= *Z \left[\frac{(X - \alpha_1 Z)^{m_1+1} - (Y - \alpha_1 Z)^{m_1+1}}{X - Y} \right] \\ &\quad + * \left[\frac{(X - \alpha_1 Z)^{m_1+2} - (Y - \alpha_1 Z)^{m_1+2}}{X - Y} \right], \end{aligned}$$

cũng xác định đường cong bất khả quy có giống 0. Nếu $n = m_1 + 2$ thì $F(X, Y, Z) = A_{1,m_1+1}$. Do đó đường cong C là bất khả quy và có

giống 0. Nếu $n \geq m_1 + 3$ thì tồn tại số hạng không bị triệt tiêu theo sau $(X - \alpha_1)^{m_1+2}$ trong khai triển của $P(X)$ trong (2.5) với bậc $v > m_1 + 2$. Vì $p|m_1 + 2$ và $p|v$ nên $v \geq m_1 + 2 + p$ và

$$d_{\mathbf{p}_1, \varphi} A_{1, m_1+1} \geq (m_1 + 1 + p) \operatorname{ord}_{\mathbf{p}_1, \varphi} (X - \alpha_1 Z)$$

theo Bổ đề 2.2.8 (i). Để ý rằng điều kiện $p|m_1 + 2$ kéo theo $m_1 \geq p - 2$, do đó $m_1 \geq 3$ và $m_1 - 2 \geq p - 4 \geq 1$ nếu $p \geq 5$. Từ đó ta có $(m_1 - 2)(p - 2) \geq 6$ nếu $p \geq 5$ và $(p, m_1) \neq (5, 3)$. Lấy

$$\omega := \left(\frac{W(Y, Z)}{(X - \alpha_1 Z)^{m_1}} \right)^{m_1+1} A_{1, m_1+1}^{m_1-2}.$$

Khi đó

$$\begin{aligned} \operatorname{ord}_{\mathbf{p}_1, \varphi} \omega &\geq [(m_1 + 1 + p)(m_1 - 2) - m_1(m_1 + 1)] \operatorname{ord}_{\mathbf{p}_1, \varphi} (X - \alpha_1 Z) \\ &= [(m_1 - 2)(p - 2) - 6] \operatorname{ord}_{\mathbf{p}_1, \varphi} (X - \alpha_1 Z) \end{aligned}$$

là không âm nếu $p \geq 5$ và $(p, m_1) \neq (5, 3)$. Do đó, ω là chính quy và không tầm thường trên bất kỳ thành phần của C nếu A_{1, m_1+1} không là nhân tử của C . Đối với trường hợp còn lại, tức là, $(p, m_1) = (5, 3)$, ta có

$$\omega := \left(\frac{W(Y, Z)}{Z(X - \alpha_1 Z)^3} \right)^5 A_{1, 4} (X - Y) \left((X - \alpha_1 Z)^4 - (Y - \alpha_1 Z)^4 \right) Z$$

xác định tốt trong $\mathbf{P}^2$ và chỉ có thể có các cực điểm tại $\mathbf{p}_1$ và $\mathbf{q}_i$. Gọi $\mathbf{q}$ là một trong các điểm $\mathbf{q}_i$. Theo Bổ đề 2.2.8 (i), ta có

$$5|\operatorname{ord}_{\mathbf{q}, \varphi} Z + \operatorname{ord}_{\mathbf{q}, \varphi} \left((X - \alpha_1 Z)^4 - (Y - \alpha_1 Z)^4 \right),$$

và do đó $\operatorname{ord}_{\mathbf{q}} Z + \operatorname{ord}_{\mathbf{q}, \varphi} \left((X - \alpha_1 Z)^4 - (Y - \alpha_1 Z)^4 \right) \geq 5$. Vì vậy, ω là chính quy tại các điểm ở vô cực. Tại $\mathbf{p}_1$, từ sự khai triển của $F(X, Y, Z)$ trong (2.7), ta có

$$\operatorname{ord}_{\mathbf{p}_1, \varphi} \left((X - \alpha_1 Z)^4 - (Y - \alpha_1 Z)^4 \right) \geq 5 \operatorname{ord}_{\mathbf{p}_1, \varphi} (X - \alpha_1 Z)$$

và $\text{ord}_{\mathfrak{p}_1, \varphi}(A_{1,4}(X - Y)) \geq 10 \text{ord}_{\mathfrak{p}_1, \varphi}(X - \alpha_1 Z)$, do đó ω cũng chính quy tại $\mathfrak{p}_1$.

Đối với trường hợp (iv.b), ta có $l = 1$, $\mu_1 = m_1 + 1 = m$ và $u \geq 3$. Chúng ta lưu ý rằng trong trường hợp này $p|m_1 + u$ và chúng ta cần loại trừ các trường hợp sau đây: $m_1 = 2$ và $p = 2$; $(u, m_1) = (3, 2)$, $p = 5$; và $(u, m_1) = (3, 3)$, $p = 3$. Hai điều kiện đầu và $p|m_1 + u$ kéo theo $u \geq 5$ nếu $m_1 = 2$. Lấy

$$\omega := \left(\frac{W(Y, Z)}{Z(X - \alpha_1 Z)^{m_1}} \right)^{m_1 + u} (A_{1, m_1}(X - Y))^{m_1} Z^{(u-2)(m_1-1)-2},$$

trong đó $A_{1, m_1}(X - Y) = (X - \alpha_1 Z)^{m_1+1} - (Y - \alpha_1 Z)^{m_1+1}$. Từ giả thiết ta có $m_1 \geq 3$ hoặc $m_1 = 2$ và $u \geq 5$, do đó $(u - 2)(m_1 - 1) - 2 \geq 0$. Vì

$$\text{ord}_{\mathfrak{p}_1, \varphi} A_{1, m_1} \geq (m_1 + u - 1) \text{ord}_{\mathfrak{p}_1, \varphi}(X - \alpha_1 Z)$$

và $\text{ord}_{\mathfrak{p}_1, \varphi}(X - Y) \geq \text{ord}_{\mathfrak{p}_1, \varphi}(X - \alpha_1 Z)$ nên ω là chính quy tại $\mathfrak{p}_1$. Gọi $\mathfrak{q}$ là một trong các cực điểm ở vô cực. Thế thì

$$\begin{aligned} \text{ord}_{\mathfrak{q}, \varphi} \omega &\geq ((u - 2)m_1 - u) \text{ord}_{\mathfrak{q}, \varphi} Z + m_1 \text{ord}_{\mathfrak{q}, \varphi}(A_{1, m_1}(X - Y)) - m_1 - u \\ &\geq (u - 2)m_1 - u - u = (u - 2)(m_1 - 2) - 4, \end{aligned} \quad (2.19)$$

là không âm, trừ khi $m_1 = 2$ hoặc $(u, m_1) = (3, 3), (3, 4), (3, 5), (4, 3), (5, 3)$. Vì $p|u + m_1$ và $p \nmid m_1 + 1$ nên (u, m_1) không thể là $(5, 3)$ hay $(3, 5)$. Tương tự, nếu $(u, m_1) = (3, 3)$ thì $p = 3$. Trường hợp này được loại trừ bởi giả thiết. Chúng ta còn lại các trường hợp: $(u, m_1) = (3, 4), (4, 3)$, hoặc $m_1 = 2$. Vì $p|m_1 + u$, hai trường hợp đầu chỉ xảy ra khi $p = 7$ và $u \geq p - 2$ nếu $m_1 = 2$. Hơn nữa, vì $(m_1, p) \neq (2, 5)$ nên ta phải có $p \geq 7$ nếu $m_1 = 2$. Bất đẳng thức (2.19) trở thành

$$\text{ord}_{\mathfrak{q}, \varphi} Z + 4 \text{ord}_{\mathfrak{q}, \varphi}(A_{1, m_1}(X - Y)) - 7 \quad \text{nếu } (u, m_1) = (3, 4), \quad (2.20)$$

$$\text{ord}_{\mathfrak{q}, \varphi} Z + 3 \text{ord}_{\mathfrak{q}, \varphi}(A_{1, m_1}(X - Y)) - 7 \quad \text{nếu } (u, m_1) = (4, 3), \quad (2.21)$$

$$(p - 6)(\text{ord}_{\mathfrak{q}, \varphi} Z - 1) + 2 \text{ord}_{\mathfrak{q}, \varphi}(A_{1, m_1}(X - Y)) - 6 \quad \text{nếu } m_1 = 2. \quad (2.22)$$

Mặt khác, theo Bổ đề 2.2.8 (iii) ta có

$$7 | \text{ord}_{q,\varphi}(A_{1,m_1}(X-Y)) - 5 \text{ord}_{q,\varphi} Z \quad \text{nếu } (u, m_1) = (3, 4), \quad (2.23)$$

$$7 | \text{ord}_{q,\varphi}(A_{1,m_1}(X-Y)) - 4 \text{ord}_{q,\varphi} Z, \quad \text{nếu } (u, m_1) = (4, 3), \quad (2.24)$$

$$p | \text{ord}_{q,\varphi}(A_{1,m_1}(X-Y)) - 3 \text{ord}_{q,\varphi} Z \quad \text{nếu } m_1 = 2. \quad (2.25)$$

Với $\text{ord}_{q,\varphi}(A_{1,m_1}(X-Y)) \geq 2$, ta có (2.20) là không âm. Nếu $\text{ord}_{q,\varphi}(A_{1,m_1}(X-Y)) = 1$ thì $\text{ord}_{q,\varphi} Z \geq 3$ theo (2.23), do đó (2.20) là không âm. Tương tự, nếu $\text{ord}_{q,\varphi}(A_{1,m_1}(X-Y)) \geq 2$ thì (2.21) không âm; nếu $\text{ord}_{q,\varphi}(A_{1,m_1}(X-Y)) = 1$ thì $\text{ord}_{q,\varphi} Z \geq 2$ theo (2.24), do đó (2.21) là không âm. Nếu $p > 7$ và $m_1 = 2$ thì (2.22) là không âm. Nếu $p = 7$, thì từ (2.25) suy ra $\text{ord}_{q,\varphi} Z \geq 5$ nếu $\text{ord}_{q,\varphi}(A_{1,m_1}(X-Y)) = 1$, và $\text{ord}_{q,\varphi} Z \geq 3$ nếu $\text{ord}_{q,\varphi}(A_{1,m_1}(X-Y)) = 2$. Như vậy (2.22) không âm. Vì đường cong C không có các nhân tử tuyến tính, nên ω chính quy và không tầm thường trên bất kỳ thành phần nào của đường cong C . Như vậy bổ đề được chứng minh. $\square$

Bây giờ ta xem xét đường cong C_c xác định bởi phương trình

$$F_c(X, Y, Z) = 0, \quad c \neq 0, 1.$$

Theo (2.11) ta có

$$\gamma := \frac{W(Y, Z)}{\frac{\partial F_c}{\partial X}} = \frac{W(Z, X)}{\frac{\partial F_c}{\partial Y}} = \frac{W(X, Y)}{\frac{\partial F_c}{\partial Z}}$$

là 1-dạng hữu tỷ xác định tốt trên $\pi^{-1}(C_c)$ với $\pi : \mathbf{K}^3 \setminus \{0\} \rightarrow \mathbf{P}^2$ là phép chiếu thông thường. Ta có

$$\begin{aligned} \frac{\partial F_c}{\partial X}(X, Y, Z) &= aZ^{n-1-\sum_{i=1}^l m_i} \prod_{i=1}^l (X - \alpha_i Z)^{m_i}, \\ \frac{\partial F_c}{\partial Y}(X, Y, Z) &= -caZ^{n-1-\sum_{i=1}^l m_i} \prod_{i=1}^l (Y - \alpha_i Z)^{m_i}. \end{aligned}$$

Đặt

$$l_0 := \# \{(i, j) \mid P(\alpha_i) = cP(\alpha_j)\}.$$

Vì $P(X)$ thỏa mãn Giả thiết I nên $0 \leq l_0 \leq l$ và $l_0 = l$ khi và chỉ khi tồn tại phép hoán vị ϕ của $\{1, \dots, l\}$ sao cho $(\alpha_i, \alpha_{\phi(i)}, 1) \in C_c$ với $i=1, \dots, l$, tức là

$$\frac{P(\alpha_1)}{P(\alpha_{\phi(1)})} = \frac{P(\alpha_2)}{P(\alpha_{\phi(2)})} = \dots = \frac{P(\alpha_l)}{P(\alpha_{\phi(l)})} = c.$$

Để đơn giản ký hiệu, từ đây về sau ta luôn ký hiệu ϕ là hoán vị của $\{1, \dots, l\}$ sao cho $\phi(i) = j$ nếu $P(\alpha_i) = cP(\alpha_j)$.

Giả sử $\mathbf{p}_i = (\alpha_i, \alpha_{\phi(i)}, 1)$ và $\mathbf{p}_j = (\alpha_j, \alpha_{\phi(j)}, 1)$ là các điểm phân biệt trong $\mathbf{P}^2$. Gọi L_{ij} là đường thẳng đi qua $\mathbf{p}_i$ và $\mathbf{p}_j$:

$$L_{ij} := (Y - \alpha_{\phi(j)}Z) - \frac{\alpha_{\phi(i)} - \alpha_{\phi(j)}}{\alpha_i - \alpha_j} (X - \alpha_j Z). \quad (2.26)$$

Thế thì L_{ij} cũng bằng

$$(Y - \alpha_{\phi(i)}Z) - \frac{\alpha_{\phi(i)} - \alpha_{\phi(j)}}{\alpha_i - \alpha_j} (X - \alpha_i Z).$$

Ta có

$$\text{ord}_{\mathbf{p}_i, \varphi} L_{ij} \geq \min \{ \text{ord}_{\mathbf{p}_i, \varphi} (X - \alpha_i Z), \text{ord}_{\mathbf{p}_i, \varphi} (Y - \alpha_{\phi(i)} Z) \} \quad (2.27)$$

và

$$\text{ord}_{\mathbf{p}_j, \varphi} L_{ij} \geq \min \{ \text{ord}_{\mathbf{p}_j, \varphi} (X - \alpha_j Z), \text{ord}_{\mathbf{p}_j, \varphi} (Y - \alpha_{\phi(j)} Z) \} \quad (2.28)$$

2.2.11. Bổ đề [5]. *Giả sử đa thức P thỏa mãn Giả thiết I và m_i được xếp theo thứ tự không tăng. Nếu đường cong C_c không có nhân tử tuyến tính thì mọi thành phần bất khả quy của đường cong C_c đều chứa 1-dạng chính quy không tầm thường trừ các trường hợp sau đây:*

- (i) $l = l_0 = 3$ và $m_1 = m_2 = m_3 = 1$;
- (ii) $l=2$ và $m_1 = m_2 = 1, l_0 = 1, 2$;
- (iii) $l=1$ và $m_1 = 1$.

Ta lưu ý rằng

$$P(X) - P(\alpha_i) = \sum_{j=\mu_i}^n b_{i,j} (X - \alpha_i)^j.$$

Nếu $\mathbf{p}_i = (\alpha_i, \alpha_{\phi(i)}, 1) \in C_c$, thì ta có thể viết

$$F_c(X, Y, Z) = \sum_{j=\mu_i}^n b_{i,j} Z^{n-j} (X - \alpha_i Z)^j - c \sum_{j=\mu_{\phi(i)}}^n b_{\phi(i),j} Z^{n-j} (Y - \alpha_{\phi(i)} Z)^j \quad (2.29)$$

Ta ký hiệu $B_{i,m}$ là tổng sau đây

$$B_{i,m}(X, Y, Z) = \sum_{j=\mu_i}^m b_{i,j} Z^{m-j} (X - \alpha_i Z)^j - c \sum_{j=\mu_{\phi(i)}}^m b_{\phi(i),j} Z^{m-j} (Y - \alpha_{\phi(i)} Z)^j.$$

Nếu $p|n$, thì $m = 1 + \sum_{i=1}^l m_i < n$, do đó tồn tại số nguyên $u_i > m$ sao cho $b_{i,u_i} \neq 0$ hoặc $b_{\phi(i),u_i} \neq 0$, và $b_{i,j} = b_{\phi(i),j} = 0$ với $m < j < u_i$. Nói cách khác, u_i là bậc theo X và Y của các số hạng không bị triệt tiêu trong (2.29) theo sau $B_{i,m}$. Khi đó tại $\mathbf{p}_i$, ta có

$$\text{ord}_{\mathbf{p}_i, \varphi} B_{i,m} \geq u_i \min \{ \text{ord}_{\mathbf{p}_i, \varphi} (X - \alpha_i Z), \text{ord}_{\mathbf{p}_i, \varphi} (Y - \alpha_{\phi(i)} Z) \}; \quad (2.30)$$

và tại $\mathbf{q}_i = (x_i, 1, 0)$ sao cho $x_i^m = c$ và $x_i^n = c$, ta có

$$p | \text{ord}_{\mathbf{q}_i, \varphi} B_{i,m} - m \text{ord}_{\mathbf{q}_i, \varphi} Z. \quad (2.31)$$

Chứng minh Định lý 2.2.5.

Trước hết ta xem xét các trường hợp sau đây:

- (i) $l \geq 4$; $l = 2, 3$ và $\max \{m_i\} \geq 2$; hoặc $l = 1$ và $m_1 \geq 2$;
- (ii) $l = 3$, $m_1 = m_2 = m_3 = 1$ và $B_{1,4}$ không là nhân tử của $F_c(X, Y, Z)$ nếu $l_0 = l = 3$, $3|n - 1$, $4|n$, và $B_{1,4} = B_{2,4} = B_{3,4}$;
- (iii) $l = 2$, $m_1 = m_2 = 1$, $l_0 = 1$ và $B_{i,3}$ không là nhân tử của $F_c(X, Y, Z)$ nếu $3|n$ và $(\alpha_i, \alpha_{\phi(i)}, 1) \in C_c$;
- (iv) $l = 2$, $m_1 = m_2 = 1$, $l_0 = 2$, $B_{1,3} = B_{2,3}$, và $B_{1,3}/(X + Y - (\alpha_1 + \alpha_2)Z)$ không là nhân tử của $F_c(X, Y, Z)$ nếu n là số lẻ và $3|n$.

Ta sẽ chứng minh rằng nếu đường cong C_c không có các thành phần tuyến tính thì mỗi thành phần của C_c chứa tích các 1-dạng không tầm thường trong những trường hợp này.

Lưu ý rằng với trường hợp (ii), ta đặt

$$\widetilde{P}_1(X) = P_0(X) - (P_0(\alpha_1) - cP_0(\alpha_{\phi(1)})) / (1 - c),$$

trong đó $P(X) = \sum_{i=0}^n a_i X^i$ và $P_0(X) = \sum_{i=0}^4 a_i X^i$. Khi đó tổng $B_{1,4}$ là đa thức thuần nhất của $\widetilde{P}_1(X) - c\widetilde{P}_1(Y)$ và $B_{1,4} = B_{2,4} = B_{3,4}$ tương đương với các điều kiện $\widetilde{P}_1(\alpha_i) = c\widetilde{P}_1(\alpha_{\phi(i)})$ với $i = 1, 2, 3$.

Từ Bổ đề 2.2.11 ta có được (i) và (ii) trong trường hợp $l_0 < 3$. Ta cần xem xét trường hợp (ii) với $l_0 = 3$, trường hợp (iii) và trường hợp (iv). Ta có

$$\begin{aligned}\frac{\partial F_c}{\partial X}(X, Y, Z) &= m a_m Z^{n-m} \prod_{i=1}^l (X - \alpha_i Z)^{m_i}, \\ \frac{\partial F_c}{\partial Y}(X, Y, Z) &= -m c a_m Z^{n-m} \prod_{i=1}^l (Y - \alpha_i Z)^{m_i}, \\ \frac{\partial F_c}{\partial Z}(X, Y, Z) &= (n - m) a_m Z^{n-m-1} (X^m - cY^m + ZG_{m-1}),\end{aligned}$$

trong đó G_{m-1} là đa thức thuần nhất bậc $m - 1$. Từ đó ta nhận được

$$\begin{aligned}\frac{W(Y, Z)}{Z \prod_{i=1}^l (X - \alpha_i Z)^{m_i}} &\equiv \frac{W(Z, X)}{-cZ \prod_{i=1}^l (Y - \alpha_i Z)^{m_i}} \\ &\equiv \frac{W(X, Y)}{-(X^m - cY^m + ZG_{m-1})}.\end{aligned}$$

Ta ký hiệu 1-dạng này là θ . Trên đường cong C_c ta có một điểm tại vô cực $\mathfrak{q}_i = (x_i, 1, 0)$ là một cực điểm của θ chỉ khi $x_i^m = c$ và $x_i^n = c$.

Trước hết ta xét trường hợp $l = l_0 = 3$ và $m_1 = m_2 = m_3 = 1$. Ta có $m = 4$ và $p \neq 2, 3$ trong trường hợp này. Chúng ta lưu ý rằng nếu $p = 3$ và $l_0 = l = 3$ thì $c = 1$, điều này không thể xảy ra. Hơn nữa, hằng số c là một nghiệm của phương trình $w^2 + w + 1 = 0$ và các cực điểm có thể có của θ là $\mathfrak{p}_i = (\alpha_i, \alpha_{\phi(i)}, 1)$, $i = 1, 2, 3$ và $\mathfrak{q}_j = (x_j, 1, 0)$ thỏa mãn $x_j^4 = w$ và $x_j^n = w$. Các nghiệm của $X^4 = w$ là $w, -w, w\xi, -w\xi$, trong đó ξ là nghiệm nguyên thủy của $X^4 = 1$. Nếu $3 \nmid n - 1$ thì không có nghiệm nào

trong số các nghiệm này có thể là nghiệm của $X^n = w$, điều này có nghĩa là θ không có cực điểm tại vô cực; nếu $3|n-1$ và $2 \nmid n$, tức là $\gcd(n, m) = 1$, thì $(w, 1, 0)$ là cực điểm của θ tại vô cực; nếu $3|n-1$, $2|n$ và $4 \nmid n$ thì $(w, 1, 0)$ và $(-w, 1, 0)$ là hai cực điểm của θ tại vô cực; nếu $3|n-1$ và $4|n$, thì θ có bốn cực điểm tại vô cực. Đối với hai trường hợp đầu tiên, tức là $3 \nmid n-1$ hoặc $3|n-1$ và $2 \nmid n$, chúng ta có thể lấy

$$\omega = \frac{W(Y, Z)L_{12}L_{30}}{Z(X - \alpha_1 Z)(X - \alpha_2 Z)(X - \alpha_3 Z)},$$

trong đó L_{30} là đường thẳng đi qua $(\alpha_3, \alpha_{\phi(3)}, 1)$ và $(w, 1, 0)$. Tương tự, ta có ω chính quy và không tầm thường trên mỗi thành phần của C_c nếu C_c không có nhân tử tuyến tính. Đối với hai trường hợp còn lại, tức là, $3|n-1$, và $2|n$, ta có

$$\omega = \left(\frac{W(Y, Z)L_{12}}{Z(X - \alpha_1 Z)(X - \alpha_2 Z)(X - \alpha_3 Z)} \right)^p B_{3,4} Z^{p-4},$$

là chính quy tại $\mathfrak{p}_1$ và $\mathfrak{p}_2$. Vì $m_3 = m_{\phi(3)} = 1$ nên ta có

$$\text{ord}_{\mathfrak{p}_3}(X - \alpha_3) = \text{ord}_{\mathfrak{p}_3}(Y - \alpha_{\phi(3)}).$$

Do đó, từ bất đẳng thức (2.30) và $u_i \geq p$ suy ra ω là chính quy tại $\mathfrak{p}_3$. Tại điểm $\mathfrak{q} = (w, 1, 0)$, ta có

$$d_{\mathfrak{q}, \varphi} \omega \geq \text{ord}_{\mathfrak{q}, \varphi} B_{3,4} + (p-4) \text{ord}_{\mathfrak{q}, \varphi} Z - p. \quad (2.32)$$

Theo (2.31) ta có $\text{ord}_{\mathfrak{q}, \varphi} B_{3,4} - 4 \text{ord}_{\mathfrak{q}, \varphi} Z$ chia hết cho p . Hơn nữa, $\text{ord}_{\mathfrak{q}, \varphi} B_{3,4} + (p-4) \text{ord}_{\mathfrak{q}, \varphi} Z$ lớn hơn không vì $p \geq 5$. Do đó,

$$\text{ord}_{\mathfrak{q}, \varphi} B_{3,4} + (p-4) \text{ord}_{\mathfrak{q}, \varphi} Z$$

lớn hơn p và điều này có nghĩa là số nguyên trong (2.32) không âm. Vì vậy ω chính quy trên C_c . Để kiểm tra ω không tầm thường trên mỗi thành phần của C_c , ta phân tích rõ hơn về tổng $B_{i,4}$, $i = 1, 2, 3$. Ta viết $P(X) = P_0(X) + Q(X)$, trong đó

$$P(X) = \sum_{j=0}^n a_j X^j,$$

$$P_0(X) = \sum_{j=0}^4 a_j X^j,$$

và

$$Q(X) = \sum_{j=5}^n a_j X^j.$$

Khi đó

$$P(X) - P(\alpha_i) = P_0(X) - P_0(\alpha_i) + Q(X) - Q(\alpha_i).$$

Tổng $B_{i,4}$ là đa thức thuần nhất của $P_0(X) - P_0(\alpha_i) - c(P_0(Y) - P_0(\alpha_{\phi(i)}))$, vì $p \geq 5$ và bậc của mỗi số hạng trong $Q(X)$ chia hết cho p . Mặt khác, đặt

$$\tilde{P}_i(X) := P_0(X) - \frac{P_0(\alpha_i) - cP_0(\alpha_{\phi(i)})}{1-c};$$

thì

$$\tilde{P}_i(X) - c\tilde{P}_i(Y) = P_0(X) - P_0(\alpha_i) - c(P_0(Y) - P_0(\alpha_{\phi(i)}))$$

và ta có $B_{i,4}$ cũng là đa thức thuần nhất của $\tilde{P}_i(X) - c\tilde{P}_i(Y)$. Vì $\deg P_0 = 4$ và $p \neq 2$, nên ta có mỗi điểm trong số bốn điểm tại vô cực của đường cong xác định bởi $B_{i,4} = 0$ có bội là một và các điểm kỳ dị cũng vậy. Tại các điểm hữu hạn, ta có các điểm kỳ dị có thể có của đường cong xác định bởi $B_{i,4} = 0$ là $(\alpha_j, \alpha_{\phi(j)}, 1)$, $j = 1, 2, 3$, với số bội 2 vì $\tilde{P}'_i(X) = P'(X)$. Rõ ràng, $\mathfrak{p}_i = (\alpha_i, \alpha_{\phi(i)}, 1) \in B_{i,4}$. Nếu tồn tại một $j \neq i$ sao cho $(\alpha_j, \alpha_{\phi(j)}, 1)$ không thuộc đường cong xác định bởi $B_{i,4} = 0$ thì đường cong xác định bởi $B_{i,4} = 0$ bất khả quy và có giống nhỏ nhất bằng 1. Trong trường hợp này, tồn tại 1-dạng chính quy không tầm thường trên đường cong xác định bởi $B_{i,4} = 0$ và ω không tầm thường trên mọi thành phần của đường cong C_c khác đường cong xác định bởi $B_{i,4} = 0$. Bây giờ chúng ta xét trường hợp $\mathfrak{p}_j \in B_{i,4}$ với mỗi $j \neq i$. Khi đó $\tilde{P}_i(\alpha_j) = c\tilde{P}_i(\alpha_{\phi(j)})$, tương đương với $P_0(\alpha_j) - cP_0(\alpha_{\phi(j)}) = P_0(\alpha_i) - cP_0(\alpha_{\phi(i)})$. Vì $B_{i,4}$ là đa thức thuần nhất của $P_0(X) - P_0(\alpha_i) - c(P_0(Y) - P_0(\alpha_{\phi(i)}))$, nên $B_{j,4} = B_{i,4}$. Do

đó, trong trường hợp này chúng ta có $B_{1,4} = B_{2,4} = B_{3,4}$ và đường cong xác định bởi $B_{i,4} = 0$ có ba điểm kỳ dị với số bội 2. Nếu đường cong xác định bởi $B_{i,4} = 0$ là khả quy thì theo định lý Bezout ta có đường cong này chứa một đường thẳng và một đường cong trơn bất khả quy có giống 1; nếu đường cong xác định bởi $B_{i,4} = 0$ là bất khả quy thì đường cong này có giống 0. Với trường hợp thứ nhất thì đường cong C_c không có nhân tử tuyến tính và một thành phần có giống 1 chứa một dạng chính quy không tầm thường. Do đó, ta chỉ cần giả thiết rằng $B_{i,4}$ không là nhân tử của $F_c(X, Y, Z)$ nếu $B_{1,4} = B_{2,4} = B_{3,4}$. Tuy nhiên, nếu $B_{i,4}$ là một nhân tử của $F_c(X, Y, Z)$ thì ta có $(X^4 - wY^4) \mid (X^n - wY^n)$ bằng cách tính $B_{i,4}$ và $F_c(X, Y, Z)$ tại $Z = 0$. Vì $w^3 = 1$ và $3 \mid n - 1$ nên ta có $w^n = 1$. Vì vậy $(X^4 - (wY)^4) \mid (X^n - (wY)^n)$ không thể xảy ra nếu $4 \nmid n$.

Đối với trường hợp (iii), chúng ta có thể giả sử rằng $\mathbf{p}_1 = (\alpha_1, \alpha_2, 1) \in C_c$ và $(\alpha_2, \alpha_1, 1) \notin C_c$. Khi đó các cực điểm có thể có của θ là $\mathbf{p}_1$ và $\mathbf{q} = (x, 1, 0)$ thỏa mãn $x^3 = c$ và $x^n = c$. Giả sử rằng $\xi^3 = c$ thế thì $X^3 = c$ có ba nghiệm ξ , $w\xi$ và $w^2\xi$, trong đó $w^2 + w + 1 = 0$. Do đó, nếu $3 \nmid n$ thì θ có nhiều nhất một cực điểm tại vô cực. Trong trường hợp này, ta lấy

$$\omega = \frac{W(Y, Z)L_{10}}{Z(X - \alpha_1 Z)(X - \alpha_2 Z)} ,$$

trong đó L_{10} là đường thẳng đi qua $\mathbf{p}_1$ và $\mathbf{q}_0$. Nếu $3 \mid n$, thì ta lấy

$$\omega = \left(\frac{W(Y, Z)}{Z(X - \alpha_1 Z)(X - \alpha_2 Z)} \right)^p B_{1,3} Z^{p-3} .$$

Thế thì ω chính quy trên đường cong C_c và $B_{1,3}$ xác định một đường cong bất khả quy có giống 0. Do đó ta cần giả thiết rằng $B_{1,3}$ không là nhân tử của $F_c(X, Y, Z)$.

Đối với trường hợp (iv), $l = l_0 = 2$ và $m_1 = m_2 = 1$ suy ra $p \neq 2, 3$; $c = -1$ và θ có các cực điểm tại vô cực, chẳng hạn là $(x, 1, 0)$, chỉ nếu

$x^3 = -1$ và $x^n = -1$. Ta có θ không có cực điểm vô cực nếu n chẵn. Nếu n lẻ và $3 \nmid n$ thì $(-1, 1, 0)$ là cực điểm của θ ở vô cực. Trong trường hợp này, ta lấy

$$\omega = \frac{W(Y, Z)L_{12}}{Z(X - \alpha_1 Z)(X - \alpha_2 Z)} .$$

Vì đường thẳng L_{12} xác định bởi phương trình $X + Y - (\alpha_1 + \alpha_2)Z = 0$ đi qua các điểm $\mathbf{p}_1 = (\alpha_1, \alpha_2, 1)$, $\mathbf{p}_2 = (\alpha_2, \alpha_1, 1)$ và $(1, -1, 0)$ nên ω chính quy tại các điểm này. Nếu n lẻ và $3|n$ thì $B_{1,3} = B_{2,3}$. Để đơn giản, ta viết

$$P'(X) = (X - \alpha_1)(X - \alpha_2)Q(X) .$$

Khi đó

$$P(X) - P(\alpha_1) = \left(\frac{\alpha_1 - \alpha_2}{2}(X - \alpha_1)^2 + \frac{1}{3}(X - \alpha_1)^3 + \dots \right) R(X) ,$$

trong đó Q và R là các đa thức. Từ đó ta suy ra

$$B_{1,3} = \frac{\alpha_1 - \alpha_2}{2} \left[(X - \alpha_1 Z)^2 - (Y - \alpha_2 Z)^2 \right] Z + \frac{1}{3} \left[(X - \alpha_1 Z)^3 + (Y - \alpha_2 Z)^3 \right] ,$$

$$B_{2,3} = \frac{\alpha_2 - \alpha_1}{2} \left[(X - \alpha_2 Z)^2 - (Y - \alpha_1 Z)^2 \right] Z + \frac{1}{3} \left[(X - \alpha_2 Z)^3 + (Y - \alpha_1 Z)^3 \right] .$$

Ta có $X + Y - (\alpha_1 + \alpha_2)Z$ là nhân tử tuyến tính của $B_{1,3}$ và $B_{2,3}$; hơn nữa, $B_{1,3} = B_{2,3}$ và $B_{1,3}/(X + Y - (\alpha_1 + \alpha_2)Z)$ là bất khả quy và xác định một đường cong có giống 0. Do đó

$$\omega = \left(\frac{W(Y, Z)}{Z(X - \alpha_1 Z)(X - \alpha_2 Z)} \right)^p B_{1,3} Z^{p-3}$$

chính quy trên đường cong C_c và không tầm thường trên mỗi thành phần của đường cong C_c nếu $B_{1,3}/(X + Y - (\alpha_1 + \alpha_2)Z)$ không là nhân tử của $F_c(X, Y, Z)$.

Kết hợp với Bổ đề 2.2.10 ta có Định lý 2.2.5 hoàn toàn được chứng minh. $\square$

2.2.12. Nhận xét. Nếu chúng ta giả thiết rằng $p \geq 7$ và $m_1 \geq 2$ khi $l = 1$, thì các điều kiện trong Định lý 2.2.5 là điều kiện cần và đủ.

Gọi $\mathcal{A}^*(\mathbf{K})$ là tập các hàm nguyên khác hằng. Ta lưu ý rằng một đa thức là đa thức duy nhất mạnh cho họ hàm $\mathcal{A}^*(\mathbf{K})$ nếu và chỉ nếu tập các không điểm của nó là tập xác định duy nhất cho họ hàm $\mathcal{A}^*(\mathbf{K})$. Gọi S là tập các không điểm của $P(X)$. Giả sử rằng b_{1,p^r} và b_{1,p^r-1} trong khai triển của $P(X) - P(\alpha_1)$ đều khác không. Ta xem xét đa thức hai biến có bậc $p^r - 1$

$$\begin{aligned}\mathcal{F}_{p^r-1}(X, Y) &:= A_{1,p^r-1}(X, Y, 1) \\ &= b_{1,p^r}(X - Y)^{p^r-1} + b_{1,p^r-1} \frac{(X - \alpha_1)^{p^r-1} - (Y - \alpha_1)^{p^r-1}}{X - Y}.\end{aligned}$$

Với mỗi s_j trong S , đặt $t_{j,1}, \dots, t_{j,p^r-1}$ là $p^r - 1$ nghiệm theo t của phương trình $\mathcal{F}_{p^r-1}(t, s_j) = 0$. Khi đó

$$T_{\mathcal{F}_{p^r-1}}(S) = \{t_{1,1}, \dots, t_{1,p^r-1}, t_{2,1}, \dots, t_{n,p^r-1}\}.$$

2.2.13. Định nghĩa. Ta nói rằng tập S được bảo toàn bằng phép biến đổi Frobenius $\mathcal{F}_{p^r-1}$ nếu

$$T_{\mathcal{F}_{p^r-1}}(S) = (p^r - 1) S.$$

2.2.14. Hệ quả. Giả sử đa thức $P(X)$ thỏa mãn Giả thiết I và $p|n$. Gọi S là tập các không điểm của $P(X)$.

(I) Trong các trường hợp (A) và (B) sau đây, S là tập xác định duy nhất cho họ hàm $\mathcal{A}^*(\mathbf{K})$ khi và chỉ khi S là tập cứng afin:

(A) $l \geq 2$;

(B) $l = 1$, và

(1) $\mu_1 \leq m_1 - 1$, hoặc

(2) $\mu_1 = m_1$, và

(a) $(m_1 + 1) \nmid n$, hoặc

(b) $(m_1 + 1) \mid n$ và $p \geq 5$,

(3) $\mu_1 = m_1 + 1 \geq 3$, và

(a) $b_{1,m_1+2} = 0$ và $p \geq 7$, hoặc

(b) $b_{1,m_1+2} \neq 0$, $m_1 + 2$ không phải là một lũy thừa của p và $p \geq 5$.

(II) Khi $l = 1$, $\mu_1 = m_1 + 1 \geq 3$, $p \geq 7$, $b_{1,p^r} \neq 0$ và $m_1 + 2 = p^r$ với $r \geq 1$, S là một tập xác định duy nhất cho họ hàm $\mathcal{A}^*(\mathbf{K})$ khi và chỉ khi S là tập cứng affin và S không được bảo toàn bởi phép biến đổi Frobenius $\mathcal{F}_{p^r-1}(X, Y)$.

Chứng minh. Ta lưu ý rằng nếu S không là tập cứng affin thì $P(X)$ không là đa thức duy nhất mạnh cho họ hàm $\mathcal{A}^*(\mathbf{K})$. Từ đây về sau ta luôn giả thiết rằng S là tập cứng affin. Khi $l \geq 3$ ta có $P(X)$ là đa thức duy nhất mạnh cho họ $\mathfrak{B}^*(\mathbf{K})$ trừ khi $l = l_0 = 3$, $m_1 = m_2 = m_3 = 1$, $3 \mid n - 1$, $4 \mid n$, $B_{1,4} = B_{2,4} = B_{3,4}$ và $B_{1,4}$ là một nhân tử của $F_c(X, Y, Z)$. Trong trường hợp này ta đã chứng minh rằng đường cong xác định bởi phương trình $B_{1,4} = 0$ là bất khả quy và có giống 0. Từ phép chứng minh Định lý 2.2.5 ta thấy rằng trên các thành phần của đường cong C_c khác với đường cong xác định bởi phương trình $B_{1,4} = 0$ thì tích các 1-dạng mà chúng ta đã xây dựng là chính quy và không tầm thường. Vì vậy, những thành phần đó phải có giống dương. Mặt khác, chúng ta đã chứng minh được $B_{1,4}(X, Y, 1)$ có thể được viết dưới dạng $\widetilde{P}_1(X) - c\widetilde{P}_1(Y)$ với $\deg \widetilde{P}_1(X) = 4$. Vì $p \neq 2$, $p \nmid 4$ nên $\widetilde{P}_1$ là đa thức duy nhất mạnh cho họ hàm $\mathcal{A}^*(\mathbf{K})$ khi và chỉ khi $\widetilde{P}_1(X) - c\widetilde{P}_1(Y)$ và $(\widetilde{P}_1(X) - \widetilde{P}_1(Y))/(X - Y)$ không có nhân tử tuyến tính. Vì vậy, $B_{1,4}(X, Y, 1) = 0$ không thể chứa nghiệm là cặp hàm nguyên khác hằng. Do đó, $P(X)$ là đa thức duy nhất

mạnh cho họ hàm $\mathcal{A}^*(\mathbf{K})$ nếu $l \geq 3$. Lập luận tương tự cho các trường hợp (I.A), (I.B.1) và (I.B.2) vì các đa thức $A_{1,m_1}(X, Y, 1)$ (trong Định lý 2.2.5 (I.B.2.b.ii) và (I.C.2)) và $B_{1,3}(X, Y, 1)$ (trong Định lý 2.2.5 (II.C)) không chứa bất kỳ nghiệm nào là cặp hàm nguyên khác hằng.

Bây giờ ta xem xét trường hợp $l = 1$ và $\mu_1 = m_1 + 1$. Ta có

$$P(X) - P(\alpha_1) = b_{1,m_1+1}(X - \alpha_1)^{m_1+1} + b_{1,m_1+2}(X - \alpha_1)^{m_1+2} + \dots$$

Nếu $b_{1,m_1+2} = 0$ thì từ Định lý 2.2.5 (I.C.3.b) suy ra $P(X)$ cũng là đa thức duy nhất mạnh cho họ hàm $\mathcal{A}^*(\mathbf{K})$ với điều kiện $m_1 \geq 2$ và $p \geq 7$. Do đó ta có được (I.B.3.a). Nếu $b_{1,m_1+2} \neq 0$, ta đặt

$$P_0(X) = b_{1,m_1+1}(X - \alpha_1)^{m_1+1} + b_{1,m_1+2}(X - \alpha_1)^{m_1+2}.$$

Thế thì $P_0(X)$ là đa thức duy nhất mạnh cho họ hàm $\mathcal{A}^*(\mathbf{K})$ khi và chỉ khi $m_1 + 2 = p^r s$, $p \nmid s$, $s \geq 2$. Trong trường hợp này ta cũng lưu ý rằng

$$\frac{P_0(X) - P_0(Y)}{X - Y} = A_{1,m_1+1}(X, Y, 1).$$

Do đó, $A_{1,m_1+1}(X, Y, 1) = 0$ không có nghiệm trong $\mathcal{A}^*(\mathbf{K}) \times \mathcal{A}^*(\mathbf{K})$ nếu $m_1 + 2$ không là một lũy thừa của p . Vì vậy $P(X)$ là đa thức duy nhất mạnh cho họ hàm $\mathcal{A}^*(\mathbf{K})$ trong trường hợp (I.B.3.b) theo Định lý 2.2.5 (I.C.3.a).

Bây giờ chúng ta chứng minh (II). Ta đặt $m_1 + 2 = p^r$ với r là một số nguyên dương. Từ Định lý 2.2.5 (I.C.3.a) và lập luận như trên ta có $P(X)$ không là đa thức duy nhất mạnh cho họ hàm $\mathcal{A}^*(\mathbf{K})$ khi và chỉ khi $F(X, Y, Z)$ chia hết cho $A_{1,m_1+1} = A_{1,p^r-1}$. Điều kiện này tương đương với $P(X) - P(Y)$ chia hết cho

$$\begin{aligned} A_{1,p^r-1}(X, Y, 1) &= b_{1,p^r-1} \frac{(X - \alpha_1)^{p^r-1} - (Y - \alpha_1)^{p^r-1}}{X - Y} + b_{1,p^r}(X - Y)^{p^r-1} \\ &= \mathcal{F}_{p^r-1}(X, Y). \end{aligned}$$

Nếu $P(X) - P(Y)$ chia hết cho $\mathcal{F}_{p^r-1}(X, Y)$ thì $(p^r - 1)S = T_{\mathcal{F}_{p^r-1}}(S)$. Mặt khác, nếu $(p^r - 1)S = T_{\mathcal{F}_{p^r-1}}(S)$ thì các điểm $\{(t_{ij}, s_i, 1) \mid 1 \leq i \leq n, 1 \leq j \leq p^r - 1\}$ là phần giao của hai đường cong được xác định bởi $P(X) - P(Y)$ và $\mathcal{F}_{p^r-1}(X, Y)$ và tổng các số bội giao là $n(p^r - 1)$. Hơn nữa, các đường cong này có một giao điểm $(1, 1, 0)$ ở vô cực, suy ra chúng phải có một thành phần chung theo định lý Bezout. Vì $A_{1,m_1+1}(X, Y, Z)$ là bất khả quy nên $\mathcal{F}_{p^r-1}(X, Y)$ là một nhân tử của $P(X) - P(Y)$. $\square$

KẾT LUẬN

Trên cơ sở tham khảo các tài liệu, trong luận văn này chúng tôi đã tập trung tìm hiểu và trình bày những nội dung sau đây:

1. Đa tạp trong không gian afin và không gian xạ ảnh, đường cong trong mặt phẳng afin, trường định chuẩn.
2. Phương pháp xây dựng 1-dạng chính quy kiểu Wronski trên một đường cong đại số.
3. Một số điều kiện đủ để một đa thức một biến trên trường $\mathbf{K}$ là đa thức duy nhất cho họ các hàm phân hình khác hằng trên $\mathbf{K}$ trong trường hợp đặc số của trường $\mathbf{K}$ chia hết bậc của đa thức.

TÀI LIỆU THAM KHẢO

TIẾNG VIỆT

- [1] Ngô Thị Hải Lý (2018), *Đa thức duy nhất mạnh cho họ các hàm hữu tỷ*, Luận văn Thạc sĩ toán học, Trường Đại học Vinh.
- [2] Đặng Thị Nghĩa (2020), *Đa thức duy nhất cho họ các hàm nguyên*, Luận văn Thạc sĩ toán học, Trường Đại học Vinh.
- [3] Ngô Việt Trung (2012), *Nhập môn Đại số giao hoán và Hình học đại số*, Nhà xuất bản Khoa học tự nhiên và công nghệ.

TIẾNG ANH

- [4] T. T. H. An, J. T. Y. Wang and P. M. Wong (2003), Unique range sets and uniqueness polynomials in positive characteristic, *Acta Arith.*, 109(3), 259 - 280.
- [5] T. T. H. An, J. T. Y. Wang and P. M. Wong (2005), Unique range sets and uniqueness polynomials in positive characteristic II, *Acta Arith.*, 116(2), 115-143.
- [6] A. Boutabaa, W. Cherry and A. Escassut (2002), Unique range sets in positive characteristic, *Acta Arith.*, 103, 169–189.
- [7] W. Cherry and J. T. Y. Wang (2002), Uniqueness polynomials for entire functions, *Internat. J. Math.*, 13, 323–332.
- [8] W. Fulton (1969), *Algebraic curves, An Introduction to Algebraic Geometry*, W. A. Benjamin, NewYork.
- [9] J. T. Y. Wang (2002), Uniqueness polynomials and bi-unique range sets for rational functions and non-archimedean meromorphic functions, *Acta Arith.*, 104, 183–200.