

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC QUY NHƠN

HÀ DUY NGHĨA

**DẠNG MODUNLAR
VÀ HÀM SỐ HỌC**

TIỂU LUẬN HÌNH HỌC SỐ HỌC

Quy Nhơn, Tháng 5 năm 2010

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC QUY NHƠN

HÀ DUY NGHĨA

**DẠNG MODUNLAR
VÀ HÀM SỐ HỌC**

CAO HỌC TOÁN KHÓA 11
Chuyên ngành: Đại số và lý thuyết số

TIỂU LUẬN HÌNH HỌC SỐ HỌC

Người hướng dẫn khoa học
GS.TSKH HÀ HUY KHOÁI

Quy Nhơn, Tháng 5 năm 2010

MỤC LỤC

Trang phụ bìa	i
Mục lục	ii
Lời mở đầu	1
Chương 1 MỘT SỐ KIẾN THỨC CƠ SỞ	2
1.1 Đặc trưng của nhóm hữu hạn	2
1.2 Quan hệ trực giao của đặc trưng	4
Chương 2 CÁC HÀM SỐ HỌC	7
2.1 Zeta hàm và L hàm	7
2.1.1 Zeta hàm	7
2.1.2 Zêta hàm Rieman	8
2.2 L-Hàm	9
2.2.1 Đặc trưng Modunlar	9
2.2.2 Định nghĩa và tính chất của L-Hàm	9
2.2.3 Tích các L hàm ứng với mọi $\chi \in \widehat{G}(m)$	10
Chương 3 DẠNG MODULAR	11
3.1 Nhóm modular	11
3.2 Miền cơ bản của nhóm modular	12
3.3 Hàm modular	12
3.4 Không gian các dạng Modular	13
Tài liệu tham khảo	17

LỜI MỞ ĐẦU

Số học là bộ môn toán học ra đời từ rất sớm nhưng nó luôn được các nhà toán học quan tâm nghiên cứu, bởi lẽ không vì sự bí ẩn của các con số mà nó còn ứng dụng quan trọng cho cuộc cách mạng khoa học kỹ thuật hiện nay như lý thuyết mật mã, kỹ thuật số,...

chuyên đề hình học số học là chuyên đề nghiên cứu số học dưới công cụ hình học, thiết lập mật mã bởi đường cong Eliptic là thế mạnh của phân môn này. Để làm đề tài tiểu luận kết thúc bộ môn tôi chọn đề tài " Dạng modular và hàm số học" , tiểu luận gồm 3 chương cùng với phần mở đầu và kết luận. Trong mỗi chương cụ thể như sau;

Chương 1: Gồm các kiến thức cơ sở liên quan đến hai chương sau

Chương 2: Giới thiệu hai hàm số học quan trọng đó là Zeta hàm và L hàm cùng với các tính chất của nó.

Chương 3: Nói về các dạng Modular, không gian các dạng Modular .

Mặc dù bản thân đã rất cố gắng trong học tập, nghiên cứu và được sự hướng dẫn nhiệt tình của thầy giáo hướng dẫn, nhưng do năng lực của bản thân và thời gian còn hạn chế nên tiểu luận khó tránh khỏi những thiếu sót. Tôi rất mong nhận được sự góp ý của quý thầy cô và các bạn để tiểu luận được hoàn thiện hơn.

Cuối cùng tôi xin chân thành cảm ơn GS.TSKH Hà Huy Khoái người đã tận tình giúp đỡ, cùng tập thể lớp cao học toán khoá 11 tạo điều kiện cho tôi hoàn thành tiểu luận này.

Quy Nhơn, tháng 5 năm 2010

Hà Duy nghĩa

Chương 1

MỘT SỐ KIẾN THỨC CƠ SỞ

1.1 Đặc trưng của nhóm hữu hạn

Định nghĩa 1.1.1. Một đặc trưng của nhóm G là một đồng cấu từ G vào nhóm nhân các số phức khác không. Nói cách khác, đặc trưng của G là một hàm $\chi : G \rightarrow \mathbb{C}^*$ sao cho $\chi(a.b) = \chi(a)\chi(b), \forall a, b \in G$. Một đặc trưng χ gọi là tầm thường nếu $\chi(g) = 1, \forall g \in G$ được ký hiệu là χ_T

Gọi χ, χ' là hai đặc trưng của nhóm G , tích 2 đặc trưng là một hàm $\chi.\chi' : G \rightarrow \mathbb{C}^*$ xác định bởi $\chi\chi'(g) = \chi(g)\chi'(g)$.

Định lý 1.1.2. Đặc trưng của nhóm tùy ý G là nhóm Abel với phép toán nhân được định nghĩa như trên.

Chứng minh. i) G đóng đối với phép toán nhân, tức là $\chi.\chi'$ là đặc trưng của G , thật vậy $\chi.\chi'(a.b) = \chi(a.b).\chi'(a.b) = \chi(a)\chi(b)\chi'(a)\chi'(b) = \chi.\chi'(a)\chi.\chi'(b)$

ii) Phần tử đơn vị là đặc trưng tầm thường χ_T

iii) Phần tử nghịch đảo của χ là χ^{-1} với $\chi^{-1} : G \rightarrow \mathbb{C}^*$, được xác định $\chi^{-1}(g) = \chi(g^{-1})$ khi đó χ^{-1} là đặc trưng của G và $\chi.\chi^{-1} = \chi_T$ \square

Tập hợp các đặc trưng của G lập thành nhóm, ký hiệu là \widehat{G} gọi là nhóm đặc trưng hay nhóm đối ngẫu của G

Giả sử rằng $h : G_1 \rightarrow G_2$ là một đồng cấu nhóm và χ là đặc trưng của G_2 . Cái nối của χ bởi h ký hiệu là $h^*\chi$ được xác định bởi $h^*\chi = \chi \circ h$, từ định nghĩa ta suy ra $h^*\chi$ là một đồng cấu.

Định lý 1.1.3. Giả sử rằng G_1, G_2 là những nhóm. Khi đó χ là đặc trưng của $G_1 \times G_2$ nếu và chỉ nếu $\chi = \chi_1 \otimes \chi_2, \forall \chi_1 \in \widehat{G}_1, \chi_2 \in \widehat{G}_2$

Hệ quả 1.1.4. Nếu G_1, G_2 là những nhóm thì $\widehat{G_1 \times G_2} = \widehat{G}_1 \otimes \widehat{G}_2$

Giả χ là đặc trưng của G và g là phần tử của G có cấp hữu hạn k . Từ $\chi(g)^k = \chi(g^k) = \chi(1) = 1$. Điều này kéo theo khẳng định rằng, những đặc trưng chuyển những phần tử có cấp hữu hạn vào căn của đơn vị. Cụ thể là : Nếu G là một nhóm và n là số nguyên dương nhỏ nhất sao cho $g^n = 1, \forall g \in G$ khi các đặc trưng của G sẽ cho tương ứng mỗi phần tử của G là căn bậc n của đơn vị .

Từ đó suy ra nếu $\chi \in \widehat{G}$ thì $|\chi(g)| = 1 \forall g \in G$, do đó

$$\overline{\chi(g)} = \overline{\chi(g)} = \frac{1}{\chi(g)} = \chi(g^{-1}) = \chi^{-1}(g)$$

môđun [Proposition 1.1 [2]] Với mọi đặc trưng không tầm thường χ của G thì $\sum_{a \in G} \chi(a) = 0$

Chứng minh. Lấy $b \in G$ sao cho $\chi(b) \neq 1$, gọi $S = \sum_{a \in G} \chi(a)$, khi đó

$$\chi(b).S = \sum_{a \in G} \chi(b)\chi(a) \sum_{ab \in G} \chi(ba) = S$$

do đó $S(\chi(b) - 1) = 0 \Rightarrow S = 0$ □

Từ mệnh đề trên, nếu thay G bằng \widehat{G} ta có kết quả sau:

$$\sum_{x \in \widehat{G}} \chi(x) = 0, \chi \in \widehat{\widehat{G}}$$

Suy ra

$$\sum_{x \in \widehat{G}} \chi(x) = 0, x \in G \cong \widehat{\widehat{G}}$$

môđun [proposition 1.3 , [2]] Gọi ω là căn bậc n của đơn vị, khi đó ánh xạ $\chi_j : \mathbb{Z}_n \rightarrow \mathbb{C}^*$ xác định bởi $\chi_j(a) = \omega^{ja}$ là đặc trưng của $\mathbb{Z}_n \forall j \in \mathbb{Z}$, ngoài ra:

(a) $\chi_j = \chi_k$ nếu và chỉ nếu $j \equiv k \pmod{n}$;

(b) $\chi_j = \chi_1^j$;

(c) $\widehat{\mathbb{Z}} = \{\chi_0, \dots, \chi_{n-1}\}$;

(d) $\widehat{\widehat{\mathbb{Z}}}_n \cong \mathbb{Z}_n$

Chứng minh. Trước hết chứng minh χ_j là đặc trưng của \mathbb{Z}_n .

Ta có $\chi_j(a+b) = \omega^{j(a+b)} = \omega^{ja}\omega^{jb} = \chi_j(a)\chi_j(b)$, Vậy χ_j là đặc trưng của \mathbb{Z}_n .

(a) $\chi_j = \chi_k$ nếu và chỉ nếu $j \equiv k \pmod n$;

(\Rightarrow) Ta có $\chi_j = \chi_k$ nên $\chi_j(1) = \chi_k(1) \Rightarrow \omega^j = \omega^k \Rightarrow j \equiv k \pmod n$.

(\Leftarrow) Nếu $j \equiv k \pmod n \Rightarrow j = k + tn \Rightarrow \omega^j = \omega^{k+tn} = \omega^k \Rightarrow \chi_j = \chi_k$.

(b) Hiển nhiên theo định nghĩa

(c) Theo trên ta đã chứng minh $\widehat{\mathbb{Z}}_n$ là nhóm, nên để chứng minh mệnh đề ta cần chứng minh $\widehat{\mathbb{Z}}_n$ là nhóm cyclic cấp n . Thật vậy, $\forall \chi_j \in \widehat{\mathbb{Z}}_n$ ta có $\chi_j^n(a) = \chi_j(na) = \chi_j(0) = 1 = \chi_0(a)$, $a \in \mathbb{Z}_n$. (Có thể giải thích theo định nghĩa của $\chi_j(a) = \omega^{ja}$), khi đó ta suy ra được (c), (d). \square

Hệ quả 1.1.5. $G \cong \widehat{G}$

Chứng minh. Vì G, \widehat{G} là những nhóm hữu hạn nên $G \cong \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_k}$, và $\widehat{G} \cong \widehat{\mathbb{Z}}_{n_1} \oplus \dots \oplus \widehat{\mathbb{Z}}_{n_k}$, do đó theo Mệnh đề 1.1 ta có $\mathbb{Z}_{n_1} \cong \widehat{\mathbb{Z}}_{n_1}, \dots, \mathbb{Z}_{n_k} \cong \widehat{\mathbb{Z}}_{n_k}$. Suy ra điều phải chứng minh. \square

1.2 Quan hệ trực giao của đặc trưng

Gọi G là nhóm Abelian hữu hạn và H là nhóm con của G , ký hiệu \widehat{G}_H là tập các đặc trưng của G có hạt nhân chứa H , tức là $\forall h \in H, \chi(h) = 1$. Khi đó ta có các kết quả sau:

Định lý 1.2.1. Nếu H là nhóm con của G và $\chi \in \widehat{G}$ thì

$$\sum_{h \in H} \chi(h) = \begin{cases} |H| & \text{Nếu } \chi \in \widehat{G}_H \\ 0 & \text{Nếu } \chi \notin \widehat{G}_H \end{cases}$$

Chứng minh. Gọi $A = \sum_{h \in H} \chi(h)$, khi đó nếu $\chi \in \widehat{G}_H$ thì $\chi(h) = 1, \forall h \in H$ suy ra $A = |H|$, ngoài ra nếu $\chi \notin \widehat{G}_H$ thì tồn tại $h_0 \in H$ sao cho $\chi(h_0) \neq 1$, khi đó $A = \sum_{h \in H} \chi(h.h_0) = \chi(h_0) \sum_{h \in H} \chi(h) \Rightarrow A = 0$ \square

Định lý 1.2.2 (Quan hệ trực giao thứ 1). Gọi χ, ψ là hai đặc trưng của G khi đó

$$\sum_{a \in G} \overline{\chi(a)}\psi(a) = \begin{cases} n & \text{Nếu } \chi = \psi \\ 0 & \text{Nếu } \chi \neq \psi \end{cases}$$

Chứng minh. Trường hợp , nếu $\chi = \psi$ khi đó $\overline{\chi(a)}.\chi(a) = \chi(a)^{-1}\chi(a) = 1$ nên $\sum_{a \in G} \overline{\chi(a)}\psi(a) = n$.

Trường hợp, nếu $\chi \neq \psi$ thì $\overline{\chi}\psi$ là đặc trưng không tầm thường, nên theo Mệnh đề 1.1 ta có điều phải chứng minh. \square

Gọi \mathbb{C}^G là không gian các hàm tuyến tính $f : G \rightarrow \mathbb{C}$. Không gian này là không gian các hàm tuyến tính n chiều trên \mathbb{C} . Với tích vô hướng được định nghĩa

$$(f, g) = \frac{1}{n} \sum_{a \in G} \overline{f(a)}g(a) \quad (f, g \in \mathbb{C}^G)$$

Định lý 1.2.3. \widehat{G} là cơ sở trực giao trong \mathbb{C}^G

Chứng minh. Ta có : $\forall \chi, \psi \in \widehat{G}, (\chi, \psi) = \frac{1}{n} \sum_{a \in G} \overline{\chi(a)}\psi(a) = 0$ (Theo Định lý 1.2.2)

Ngoài ra, theo Hệ quả 1.1.5 ta suy ra $|\widehat{G}| = n = \dim \mathbb{C}^G$. \square

Gọi $\chi_0, \dots, \chi_{n-1}$ là những đặc trưng của $G = \{a_0, a_1, \dots, a_{n-1}\}$. Khi đó ma trận vuông $C = (\chi_i(a_j))$ là bảng đặc trưng của G

Hệ quả 1.2.4. Ma trận $A = \frac{1}{\sqrt{n}}C$ là ma trận đơn vị, hơn nữa $A.A^* = A^*.A = I$ trong đó I là ma trận đơn vị và A^* là ma trận liên hợp của A

Hệ quả 1.2.5 (Quan hệ trực giao thứ 2). Gọi $a, b \in G$ khi đó

$$\sum_{\chi \in \widehat{G}} \overline{\chi(a)}\chi(b) = \begin{cases} n & \text{Nếu } a = b \\ 0 & \text{Nếu } a \neq b \end{cases}$$

Chứng minh. Thật vậy, nếu $a = b$ ta có

$$\sum_{\chi \in \widehat{G}} \overline{\chi(a)}\chi(b) = \sum_{\chi \in \widehat{G}} \overline{\chi(a)}\chi(a) = \sum_{\chi \in \widehat{G}} |\chi(a)|^2 = n$$

nếu $a \neq b$ ta có

$$\sum_{\chi \in \widehat{G}} \overline{\chi(a)} \chi(b) = \sum_{\chi \in \widehat{G}} \chi(a^{-1}) \chi(b) = \sum_{\chi \in \widehat{G}} \chi(a^{-1}b) = 0$$

(Suy ra từ Mệnh đề 1.1)

□

Chương 2

CÁC HÀM SỐ HỌC

2.1 Zeta hàm và L hàm

2.1.1 Zeta hàm

Định nghĩa 2.1.1. Cho $f : \mathbb{N} \rightarrow \mathbb{C}$ là hàm số học, f được gọi là :

Nhân tính nếu : $\forall m, n(m, n) = 1, f(m, n) = f(m).f(n)$

Nhân tính mạnh nếu : $\forall m, n f(m, n) = f(m).f(n)$

Bổ đề 2.1.2. Chuỗi $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ hội tụ tuyệt đối khi $Res > 1$ và biểu diễn thành tích vô hạn $\prod_{p \in \mathcal{P}} (1 + f(p)p^{-s} + f(p^2).p^{-2s} + \dots)$ trong đó $f(n)$ là hàm nhân tính giới nội.

Chứng minh. Vì $f(n)$ là hàm nhân tính giới nội nên $|f(n)| < M \Rightarrow \left| \frac{f(n)}{n^s} \right| < \frac{M}{n^X}, X = Res > 1$ chuỗi hội tụ tuyệt đối khi $Res > 1$.

Lấy một tập hữu hạn $S \subset \{ \text{Tập hợp các số nguyên tố} \}$, gọi $\mathbb{N}(S) \subset \mathbb{N}$ là tập các số mà các ước nguyên tố thuộc S , giả sử $S = p_1, \dots, p_r$, khi đó $\mathbb{N}(S) = \{n = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \alpha_i \geq 0\}$ Khi đó ta có :

$$\sum_{n \in \mathbb{N}(S)} \frac{f(n)}{n^s} = \sum \frac{f(p_1^{\alpha_1} \dots p_k^{\alpha_k})}{(p_1^{\alpha_1} \dots p_k^{\alpha_k})^s}$$

Do f là hàm nhân tính nên $f(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) \dots f(p_k^{\alpha_k})$ do đó :

$$\sum_{n \in \mathbb{N}(S)} \frac{f(n)}{n^s} = \sum_{\alpha_1 \dots \alpha_k} \frac{f(p_1^{\alpha_1}) \dots f(p_k^{\alpha_k})}{(p_1^{\alpha_1} \dots p_k^{\alpha_k})^s} = \prod_{i=1}^k \left(\sum_{\alpha_i=0}^{\infty} \frac{f(p_i^{\alpha_i})}{(p_i^{\alpha_i})^s} \right), S \rightarrow \mathcal{P}$$

Từ đó suy ra: $\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathcal{P}} (1 + f(p)p^{-s} + f(p^2).p^{-2s} + \dots)$ □

Giả sử $f(n)$ là hàm nhân tính mạnh giới nội, khi đó theo bổ đề trên ta cũng có

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{f(n)}{n^s} &= \prod_{p \in \mathcal{P}} (1 + f(p)p^{-s} + f(p^2).p^{-2s} + \dots) \\ &= \prod_{p \in \mathcal{P}} \frac{1}{1-f(p).p^{-s}} = \prod_{p \in \mathcal{P}} (1 - f(p)p^{-s})^{-1}. \end{aligned}$$

Và công thức này gọi là công thức Ôle.

2.1.2 Zêta hàm Rieman

Từ bổ đề trên ta thấy khi $f(n) = 1$ ta luôn có: $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, $\zeta(s) = \prod_{p \in \mathcal{P}} (1 - p^{-s})^{-1}$

ζ là hàm Rieman hội tụ tuyệt đối trên miền $Re s > 1$

Định lý 2.1.3. ζ Hàm Rieman là hàm chỉnh hình trên miền $Re s > 0$. Thác triển được thành hàm phân hình trên miền $Re s > 0$ có cực điểm đơn tại $s = 1$ tức là $\zeta(s) = \frac{1}{s-1} + \Phi(s)$ trong đó $\Phi(s)$ chỉnh hình trong miền $Re s > 0$.

Chứng minh. Ta có: $\frac{1}{s-1} = \int_1^{\infty} t^{-s} dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s} dt$ nên suy ra:

$$\begin{aligned} \zeta(s) - \frac{1}{s-1} &= \sum_{n=1}^{\infty} \frac{1}{n^s} - \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s} dt \\ &= \sum_{n=1}^{\infty} \left(n^{-s} - \int_n^{n+1} t^{-s} dt \right) \\ &= \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s}) dt. \end{aligned}$$

Đặt $\Phi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s}) dt$, $\Phi(s) = \sum_{n=1}^{\infty} \Phi_n(s)$, các hàm $\Phi_n(s)$ chỉnh hình theo s trong miền $Re s > 0$. Để chứng minh $\Phi(s)$ chỉnh hình trong $Re s > 0$ ta chứng minh chuỗi hội tụ tuyệt đối và đều. Thật vậy, ta có:

$$|\Phi_n(s)| = \left| \int_n^{n+1} (n^s - t^{-s}) dt \right| \leq \max_{n \leq t \leq n+1} |n^s - t^{-s}|$$

nên suy ra: $|\Phi_n(s)| \leq \frac{|s|}{n^{X+1}}$, $X = Re s$ Từ đó suy ra $\Phi(s)$ chỉnh hình trong miền $Re s > 0$, ngoài ra khi $s \rightarrow 1$, $\Phi(s)$ giới nội. \square

2.2 L-Hàm

2.2.1 Đặc trưng Modular

Giả sử $m \in \mathbb{Z}, m \geq 1, G(m) = (\mathbb{Z}/m\mathbb{Z})^*$ nhóm các lớp đồng dư khả nghịch theo modulo m , $G(m)$ có m phần tử, gọi χ là đặc trưng của nhóm $G(m)$ gọi là đặc trưng Modular. $\chi G(m) : \rightarrow \mathbb{C}^*$ thác triển lên \mathbb{Z} , khi đó:

- $\chi(n) = 0$ nếu $(n, m) \neq 1$
- $\chi(n) = \chi(n \bmod m)$ nếu $(n, m) = 1$

2.2.2 Định nghĩa và tính chất của L-Hàm

Định nghĩa 2.2.1. Cho $m \geq 1, \chi$ đặc trưng modular m , ta định nghĩa L hàm ứng với đặc trưng χ được xác định bởi công thức

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n).n^{-s}$$

Mệnh đề 2.2.2. Nếu $\chi = 1$ thì $L(s, 1) = F(s).\zeta(s)$ trong đó $F(s) = \prod_{p|m} (1 - p^{-s}), \zeta(s)$ là Zeta hàm Riemann.

Từ mệnh đề trên ta thấy rằng $L(s, 1)$ chỉ khác $\zeta(s)$ khi $(n; m) \neq 1$ và $L(s, 1)$ có thể thác triển thành hàm phân hình trên miền $Re s > 0$ và có cực điểm đơn tại $s = 1$.

Mệnh đề 2.2.3. Với $\chi \neq$ chuỗi $L(s, \chi)$ hội tụ tuyệt đối trong $Re s > 0$ ($Re s > 1$) đồng thời có tích Euler

$$L(s, \chi) = \prod_{p \in \mathcal{P}} (1 - \chi(p).p^{-s})^{-1}, , Re s > 0$$

Chứng minh. $\forall u, v \in \mathbb{N}, u < v$ ta đặt $A_{u,v} = \sum_u^v \chi(n)$, theo tính chất trực giao ta có

$$\sum_u^{u+m} \chi(n) = 0$$

Do đó

$$|A_{u,v}| \leq \Phi(m)$$

và không phụ thuộc vào u, v , nên theo tiêu chuẩn Abel chuỗi hội tụ tuyệt đối.

ngoài ra $\chi(n)$ là hàm nhân tính mạnh nên $L(s, \chi)$ có tính Euler \square

2.2.3 Tích các L hàm ứng với mọi $\chi \in \widehat{G}(m)$

Cho $p \nmid m, \bar{p}$ là ảnh của m trong nhóm $G(m) = (\mathbb{Z}/m\mathbb{Z})^*$ $f(p)$ là cấp của p trong nhóm $G(m)$, $f = f(r)$ là số nhỏ nhất sao cho $p^f \equiv 1 \pmod{m}$ suy ra $f(p) | \Phi(m)$, $G(p) = \Phi(m)/f(p)$ là cấp của nhóm sinh bởi (p)

Mệnh đề 2.2.4.

$$\zeta_m(s) = \prod_{p|m} (1 - p^{-f(p)s})^{-g(p)}$$

Chứng minh. Ta có : $\zeta_m(s) = \prod_{\chi} L(\chi, s) = L(s, 1) \prod_{\chi \neq 1} L(s, \chi)$
 $= \prod_{p|m} (1 - p^{-s}) \zeta(s) \prod_{\chi \neq 1} L(s, \chi)$
 $= \prod_{p|m} (1 - p^{-s}) \prod_{p \in P} (1 - p^{-s})^{-1} \prod_{\chi \neq 1} \prod_{p \in P} (1 - \chi(p)p^{-s})^{-g(p)}$
 $= \prod_{\chi} \prod_{p|m} (1 - \chi(p)p^{-s})^{-1} = \prod_{p|m} (1 - p^{-f(p)s})^{-g(p)} \quad \square$

Định lý 2.2.5. (i) $\forall \chi \neq 1, L(1, \chi) \neq 0$ (ii) $\zeta(s)$ có cực điểm đơn tại $s = 1$.

Chứng minh. (i) giả sử có χ_0 nào đó, $\chi_0 \neq 1, L(1, \chi_0) = 0$ khi đó $L(1, \chi)$ giới nội $\forall \chi \neq 1$, và $L(1, \chi_0)$ có cực điểm đơn tại $s = 1$.

Nếu $L(1, \chi_0) = 0$ thì khử được cực điểm $s = 1$ suy ra hàm $\zeta(s)$ chỉnh hình trong miền $Re s > 0$, ta cần chứng minh chuỗi hội tụ trong miền $Re s > 0$, ta chứng tỏ chuỗi $\zeta(s)$ phân kỳ tại $s = \frac{1}{\Phi(m)}$, thật vậy;

$$\zeta(m) = \prod_{p|m} (1 - \chi(p) \cdot p^{-f(p) \cdot s})^{-g(p)} \cdot (1 - p^{-f(p) \cdot s})^{-g(p)} = \left(\frac{1}{1 - p^{-f(p) \cdot s}} \right)^{g(p)}$$

$$= (1 + p^{-f(p) \cdot s} + \dots + (p^{-f(p) \cdot s})^m + \dots)^{g(p)}$$

mà $\Phi(m) \geq f(p)$ nên chuỗi trên được làm già bởi

$$(1 + p^{-\Phi(m) \cdot s} + \dots + (p^{-\Phi(m) \cdot s}) + \dots) = \left(1 + \frac{1}{p} + \dots \right)$$

mà chuỗi này phân kỳ nên $s = \frac{1}{\Phi(m)}$ là phân kỳ.

(ii) được suy ra trực tiếp từ (i) \square

Chương 3

DẠNG MODULAR

3.1 Nhóm modular

Cho H là nửa mặt phẳng trên của \mathbb{C} Nhóm modular kí hiệu là

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

Tác động của $SL_2(\mathbb{R})$ lên $\mathbb{C} \cup \{\infty\}$:

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}) \quad gz = \frac{az+b}{cz+d} \text{ với } z \text{ là một phần tử trong } \mathbb{C} \cup \{\infty\}.$$

Qua tác động của nhóm $SL_2(\mathbb{R})$, nửa mặt phẳng trên là ổn định. Thật vậy, giả sử $H = \{z / \text{Im } z > 0\}$ và $z \in H$. Khi đó

$$\begin{aligned} \text{Im}(gz) &= \text{Im} \left(\frac{az+b}{cz+d} \right) = \frac{1}{2i} \left(\frac{az+b}{cz+d} - \frac{\overline{az+b}}{\overline{cz+d}} \right) \\ &= \frac{1}{2i} \left(\frac{(ad-bc)z - (ad-bc)\overline{z}}{|cz+d|^2} \right) \\ &= \frac{1}{2i} \frac{(ad-bc)(z-\overline{z})}{|cz+d|^2} \\ &= \frac{z-\overline{z}}{2i|cz+d|^2} = \frac{\text{Im } z}{|cz+d|^2} \end{aligned}$$

Tác động tầm thường trên H :

$$\text{Xét } g = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ ta có } gz = z, \quad \forall z \in \mathbb{C} \cup \{\infty\}.$$

$$\text{Xét nhóm } SL_2(\mathbb{Z}) \subset SL_2(\mathbb{R}). \text{ Ta có } SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

. Kí hiệu $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) / \{\pm 1\}$.

Định nghĩa 3.1.1. Nhóm $G = SL_2(\mathbb{Z})$ gọi là nhóm modular.

3.2 Miền cơ bản của nhóm modular

Định lý 3.2.1. Miền $D = \{|z| \geq 1, |Re z| \leq \frac{1}{2}\}$ là miền cơ bản của nhóm modular G tức là

(i) Với mọi $z \in H$ và với mọi $g \in G$ ta có $gz \in D$.

(ii) Giả sử $z, z' \in D$ tồn tại g sao cho $z' = gz$. Khi đó ta có

$$\text{hoặc } |Re z| = \frac{1}{2}, z' = z \pm 1 \text{ hoặc } |z| = 1, z' = -\frac{1}{z}.$$

(iii) Với mọi $z \in D$ đặt $I(z) = \{g \in G, gz = z\}$

(Nhóm con ổn định của z đối với G).

Khi đó $I(z) = 1$ trừ 3 trường hợp:

- $z = i$: $I(i)$ là nhóm cấp 2 sinh bởi S
- $z = \rho = e^{\frac{2\pi i}{3}}$: G là nhóm cấp 3 sinh bởi S, T .
- $z = \bar{\rho} = e^{\frac{\pi i}{3}}$: $I(z)$ là nhóm cấp 3 sinh bởi TS .

3.3 Hàm modular

Định nghĩa 3.3.1. Cho số nguyên k , $f(z)$ cho trong nửa mặt phẳng trên được gọi là một hàm modular yếu trong số $2k$ nếu $f(z)$ phân hình trên H

đồng thời với mọi $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ ta có

$$f(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right) \quad (3.1)$$

Định lý 3.3.2. Hàm phân hình $f(z)$ trên nửa mặt phẳng H là dạng modular trong số $2k$ khi và chỉ khi $f(z)$ thỏa mãn hai điều kiện sau

$$(i) f(z - 1) = f(z)$$

$$(ii) f\left(-\frac{1}{z}\right) = z^{2k} f(z).$$

Định nghĩa 3.3.3. Hàm modular yếu $f(z)$ gọi là hàm modular nếu $f(z)$ phân hình tại ∞ . Hàm $f(z)$ được gọi là hàm modular trọng số $2k$ nếu $f(z)$ là hàm modular trọng số $2k$ và $f(z)$ làm hàm chỉnh hình trên H kể cả tại ∞ .

Nhận xét: $f(z)$ là dạng modular trọng số $2k$ khi

- (i) f là hàm chỉnh hình trên H .
- (ii) $f(z)$ có khai triển $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$.
- (iii) $f\left(-\frac{1}{z}\right) = z^{2k} f(z)$.

3.4 Không gian các dạng Modular

Cho f và g là các dạng modular trọng số $2k$. Khi đó $f + g$ cũng là một dạng modular.

Đặt M_k là tập hợp các dạng modular trọng số $2k$. Khi đó M_k là không gian tuyến tính phức.

Định nghĩa 3.4.1. Dạng modular f gọi là dạng cusp nếu như $f(\infty) = 0$.

Kí hiệu M_k^0 là không gian các dạng cusp trọng số $2k$. Ta có $M_k^0 \subset M_k$. Xét $\varphi : M_k \rightarrow \mathbb{C}$, $\varphi(f) = f(\infty)$. Ta có $M_k^0 = \text{Ker}\varphi$. Do đó $M_k = M_k^0 \oplus \mathbb{C}G_k$.

Định lý 3.4.2. Giả sử f là hàm modular trọng số $2k$ khác 0. Khi đó ta có

$$\mathcal{U}_{\infty}(f) + \sum_{p \in D} \frac{1}{e_p} \mathcal{U}_p(f) = \frac{k}{6}, (e_p \text{ là cấp của nhóm ổn định tại } p).$$

Viết lại, $\mathcal{U}_{\infty}(f) + \frac{1}{2}\mathcal{U}_i(f) + \frac{1}{3}\mathcal{U}_{\rho}(f) + \sum_{p \in H/G}^* \mathcal{U}_p(f) = \frac{k}{6}$ (*) trong đó \sum^* là tổng theo mọi modun trong H/G khác i, ρ và các điểm đồng dư với i, ρ .

Nhận xét: $\sum^* \mathcal{U}_p(f)$ chỉ là tổng hữu hạn (tức là, chỉ có hữu hạn điểm mà tại đó $\mathcal{U}_{\rho}(f) = 0$). Nếu f là hàm modular thì f phân hình tại ∞ . $q = e^{2\pi i z} : \lim_{q \rightarrow 0} f(q) = \infty$, tồn tại lân cận của 0, chẳng hạn $|q| < r$ trong đó chỉ có q là cực điểm, $z = x + iy$, $|q| = e^{-2\pi y} < r$ suy ra $\frac{1}{r} < e^{2\pi y} = y > \frac{1}{2\pi} \log \frac{1}{r}$. Khi $y > \frac{1}{2\pi} \log \frac{1}{r}$ hàm f chỉ có cực điểm tại ∞ . Miền $D \cap \left\{ y \leq \frac{1}{2\pi} \log \frac{1}{r} \right\}$ compact do đó chỉ có hữu hạn cực điểm và không điểm tức là chỉ có hữu hạn p sao cho $\mathcal{U}_p(H) \neq 0$.

Định lý 3.4.3. (i) $M_k = 0$ với $k < 0$ hoặc $k = 1$.

(ii) Khi $k = 0, 2, 3, 4, 5$ thì M_k là không gian vecto một chiều và cơ sở của

nó là $1, G_2, G_3, G_4, G_5$.

(iii) Ánh xạ
$$\begin{array}{ccc} M_{k-6} & \rightarrow & M_k^0 \\ f & \mapsto & \Delta f \end{array}$$
 là một đẳng cấu.

Chứng minh. (i) Khi $k = 1$ hoặc $k < 0$ thì không có dạng $f \neq 0$ do đó $f = 0$.

(iii) Xét ánh xạ
$$\begin{array}{ccc} M_{k-6} & \rightarrow & M_k^0 \\ f & \mapsto & \Delta f \end{array}.$$

- Trong công thức (*) ta thay f bởi $G_2 : \mathfrak{U}_\infty(G_2) + \frac{1}{2}\mathfrak{U}_i(G_2) + \frac{1}{3}\mathfrak{U}_\rho(G_2) + \sum_{p \in H/G}^* \mathfrak{U}_p(G_2) = \frac{1}{3}$ suy ra $\mathfrak{U}_\rho(G_2) = 1$ và $\mathfrak{U}_p(G_2) = 0$. Do đó G_2 có không điểm đơn duy nhất tại ρ , $G_2(\rho) = 0$, $G_2(p) \neq 0$.

- Trong (*) ta thay f bởi $G_3 : \mathfrak{U}_\infty(G_3) + \frac{1}{2}\mathfrak{U}_i(G_3) + \frac{1}{3}\mathfrak{U}_\rho(G_3) + \sum_{p \in H/G}^* \mathfrak{U}_p(G_3) = \frac{1}{2}$ suy ra $\mathfrak{U}_\rho(G_3) = 1$ và $\mathfrak{U}_p(G_3) = 0$. Do đó G_3 có $\mathfrak{U}_i(G_3) = 1$, $\mathfrak{U}_p(G_3) = 0, \forall p \neq i$ và $G_3(i) = 0$, $G_3(p) \neq 0, \forall p \neq i$.

- Trong (*) ta thay f bởi Δ . Khi đó $\Delta(\infty) = 0$ suy ra $\mathfrak{U}_\infty(\Delta) \geq 1$. Ta có $\mathfrak{U}_\infty(\Delta) + \frac{1}{2}\mathfrak{U}_i(\Delta) + \frac{1}{3}\mathfrak{U}_\rho(\Delta) + \sum_{p \in H/G}^* \mathfrak{U}_p(\Delta) = 1$ suy ra $\mathfrak{U}_\infty(\Delta) = 1$ và $\mathfrak{U}_i(\Delta) = \mathfrak{U}_\rho(\Delta) = \mathfrak{U}_p(\Delta) = 0, \forall p \neq \infty$. Do đó Δ có không điểm đơn tại ∞ . Hiển nhiên ánh xạ trên là đơn ánh.

Lấy g tùy ý thuộc M_k^0 . Ta có $g(\infty) = 0$ và $\Delta(\infty) = 0$ nên g/Δ chỉnh hình kể cả tại ∞ . Tại điểm $p \neq \infty$ thì $\Delta \neq 0$. Vì g/Δ là hàm chỉnh hình nên $g/\Delta \in M_{k-6}$. Đặt $f = g/\Delta$ ta có $f \in M_{k-6}$ và $g = \Delta f$ suy ra ánh xạ trên là một toàn cấu và do đó nó là một đẳng cấu.

(ii) Xét $k = 0$: Vì f là dạng modular nên nó không có cực điểm suy ra $\mathfrak{U}_p(f) \geq 0$. Theo (*) thì $\mathfrak{U}_p(f) = 0$ với mọi p nên f chỉnh hình và khác 0 trên H , kể cả tại ∞ . Do đó f là hàm hằng nên M_k là không gian một chiều có cơ sở là 1.

Xét $k = 2, 3, 4, 5$ ta có $M_k^0 \cong M_{k-6}$. Do $k-6 < 0$ nên theo (i) ta có $M_{k-6} = 0$ suy ra $M_k^0 = 0$. Vì $M_k = M_k^0 \oplus \mathbb{C}G_k$ nên $M_k = \mathbb{C}G_k$ do đó M_k là không gian một chiều cơ sở G_k với $k = 2, 3, 4, 5$. \square

Hệ quả 3.4.4. Số chiều của M_k được cho bởi công thức

$$\dim M_k = \begin{cases} \left[\frac{k}{6} \right] & , k \equiv 1 \pmod{6}, k \geq 0 \\ \left[\frac{k}{6} \right] + 1 & , k \not\equiv 1 \pmod{6} \end{cases}$$

Chứng minh. Ta chứng minh quy nạp theo k :

- $k = 0$ tức là $k \not\equiv 1 \pmod{6}$ thì $\dim M_k = 1$.
- $k = 1$ tức là $k \equiv 1 \pmod{6}$ thì $\dim M_k = \left[\frac{1}{6} \right] = 0$.
- $k = 2, 3, 4, 5$ thì $k \not\equiv 1 \pmod{6}$ do đó $\dim M_k = \left[\frac{1}{6} \right] + 1 = 1$.

Giả sử công thức trên đúng với mọi $k > 5$, ta cần chứng minh công thức đúng với $k + 6$. Khi đó:

$$\begin{aligned} \dim M_{k+6} &= \dim M_{k+6}^0 + 1 = \dim M_k + 1 \\ &= \begin{cases} \left[\frac{k}{6} \right] + 1 & , k \equiv 1 \pmod{6} \\ \left[\frac{k}{6} \right] + 2 & , k \not\equiv 1 \pmod{6} \end{cases} \\ &= \begin{cases} \left[\frac{k+6}{6} \right] & , k \equiv 1 \pmod{6} \\ \left[\frac{k+1}{6} \right] + 1 & , k \not\equiv 1 \pmod{6} \end{cases} \quad \square \end{aligned}$$

Định lý 3.4.5. Không gian M_k có cơ sở gồm họ các đơn thức có dạng sau

$$\{G_2^\alpha G_3^\beta, \alpha, \beta \in \mathbb{Z}, \alpha, \beta \geq 0, 2\alpha + 3\beta = k\}.$$

Chứng minh. Ta chứng minh họ các đơn thức trên sinh ra M_k bằng quy nạp như sau:

Nếu $k = 0$ thì $\alpha = \beta = 0$.

Nếu $k = 2$ thì chọn $\alpha = 2$ và $\beta = 0$ do đó M_2 sinh bởi G_2 .

Nếu $k = 3$ thì chọn $\alpha = 0$ và $\beta = 3$ do đó M_3 sinh bởi G_3 .

Nếu $k \geq 4$ thì ta luôn tìm được γ và δ sao cho $2\gamma + 3\delta = k$. Xét $g = G_2^\gamma G_3^\delta \in M_k$ sao cho $g(\infty) \neq 0$ và $f \in M_k$. Ta phải tìm λ sao cho $f - \lambda g \in M_k^0$ tức là tìm $\frac{f(\infty)}{g(\infty)}$. Vì $M_k^0 \cong M_{k-6}$ nên ta có $f - \lambda g = \Delta h$, $h \in M_{k-6}$. Theo giả thiết quy nạp đúng với $k - 6$ nên ta có $h = \sum_{2\alpha+3\beta=k-6} c_{\alpha\beta} G_2^\alpha G_3^\beta$. Khi đó

$$f = \lambda G_2^\alpha G_3^\beta + \Delta h = \lambda G_2^\alpha G_3^\beta + ((60G_2)^3 - 27(140G_3)^2) h$$

$$= \lambda G_2^\alpha G_3^\beta + \sum (a_{\alpha\beta} G_2^\alpha G_3^{\beta+2} + b_{\alpha\beta} G_2^{\alpha+3} G_3^\beta)$$

và

$$\begin{cases} 2\alpha + 3(\beta + 2) = k \\ 2(\alpha + 3) + 3\beta = k \end{cases}$$

Điều cần chứng minh đúng với k nên $\{G_2^\alpha G_3^\beta, \alpha, \beta \in \mathbb{Z}, \alpha, \beta \geq 0, 2\alpha + 3\beta = k\}$ sinh ra M_k .

Ta cần chứng minh họ $\{G_2^\alpha G_3^\beta, \alpha, \beta \in \mathbb{Z}, \alpha, \beta \geq 0, 2\alpha + 3\beta = k\}$ là hệ độc lập tuyến tính.

Giả sử $\sum_{(\alpha,\beta)} \lambda_{\alpha\beta} G_2^\alpha G_3^\beta = 0$ trong đó $2\alpha + 3\beta = k$. Chọn (α_0, β_0) trong đó α_0 là số nhỏ nhất trong các α và β_0 là số lớn nhất trong các số β sao cho $2\alpha_0 + 3\beta_0 = k$. Từ $2(\alpha - \alpha_0) + 3(\beta - \beta_0) = 0$ ta có $\alpha - \alpha_0 : 3$ và $\beta - \beta_0 : 2$ do đó $\alpha - \alpha_0 = 3m$ và $\beta - \beta_0 = -2n$ suy ra $m = n$. Từ đó $\sum \lambda_{\alpha\beta} G_2^{\alpha-\alpha_0} G_3^{\beta-\beta_0} = 0 \Leftrightarrow \sum \lambda_{\alpha\beta} (G_2^3)^m (G_3^2)^{-n} = 0 \Leftrightarrow \sum \lambda_{\alpha\beta} \left(\frac{G_2^3}{G_3^2}\right)^n = 0$.

Nếu $\lambda_{\alpha\beta}$ không đồng thời bằng không thì $\frac{G_2^3}{G_3^2} = c$. Khi đó

Tại ρ ta có $G_3 = 0$ và $G_2 \neq 0$ (vô lý).

Tại ρ ta có $G_2 = 0$ và $G_3 \neq 0$ (vô lý).

Vậy hệ sinh trên là một hệ độc lập tuyến tính, tức là

$$\{G_2^\alpha G_3^\beta, \alpha, \beta \in \mathbb{Z}, \alpha, \beta \geq 0, 2\alpha + 3\beta = k\}$$

là một cơ sở của M_k . □

TÀI LIỆU THAM KHẢO

- [1] Hà Huy Khoái , *Bài giảng hình học số học* , Trường đại học Quy Nhơn.
- [2] Wolfgang M.Schmidt, *Equation over Finite Fields An Elementary Approach* NewYork 1976.