Giải tích p-adic

Đặng Tuấn Hiệp

Tháng 10 năm 2007

MỤC LỤC

Chương 1

Chuẩn trên trường

1.1 Các khái niệm cơ bản

Định nghĩa 1.1.1. *Cho F là một trường, ánh xạ $|.| : F \to \mathbb{R}$ được gọi là chuẩn trên F nếu nó thỏa mãn ba tính chất sau:*

i. $|x| \geq 0; \quad \forall x \in F$ *và* $|x| = 0 \Leftrightarrow x = 0$

ii. $|xy| = |x||y|; \quad \forall x, y \in F$

iii. $|x + y| \leq |x| + |y|; \quad \forall x, y \in F$

Ví dụ.

1. Lấy $F = \mathbb{Q},\ \mathbb{R},\ \mathbb{C}$; với giá trị tuyệt đối thông thường là chuẩn.

2. Lấy F là trường tùy ý, $\forall x \in F$, ta định nghĩa

$$|x| = \begin{cases} 1 & \text{nếu } x \neq 0 \\ 0 & \text{nếu } x = 0 \end{cases}$$

   là chuẩn tầm thường.

□

Tính chất.

1. $|1| = 1$

2. $|x^{-1}| = \frac{1}{|x|}; \quad \forall x \neq 0$

3. Nếu F là trường hữu hạn thì trên F có duy nhất một chuẩn là chuẩn tầm thường.

□

1.1.1 Chuẩn tương đương

Cho F là trường; $|.|$ là chuẩn trên F. Khi đó, chuẩn $|.|$ cảm sinh ra mêtric $d(x,y) = |x-y|$. Tôpô sinh bởi mêtric này được gọi là tôpô cảm sinh bởi chuẩn $|.|$.

Định nghĩa 1.1.2. *Cho hai chuẩn $|.|_1$, $|.|_2$ trên trường F. Ta nói $|.|_1$ và $|.|_2$ là tương đương với nhau khi và chỉ khi tôpô cảm sinh bởi hai chuẩn này là trùng nhau.*

Ký hiệu $|.|_1 \sim |.|_2$

Định lý 1.1.1 (Các điều kiện tương đương của chuẩn). *Cho F là trường; với $|.|_1$, $|.|_2$ là hai chuẩn trên F, các khẳng định sau tương đương*

1. $|x|_1 < 1 \Leftrightarrow |x|_2 < 1; \quad \forall x \in F.$
2. $|x|_1 \leq 1 \Leftrightarrow |x|_2 \leq 1; \quad \forall x \in F.$
3. *Tồn tại* $c > 0$ *sao cho* $|x|_1 = |x|_2^c; \quad \forall x \in F$
4. *Dãy* $\{x_n\}$ *là dãy Cauchy đối với chuẩn* $|.|_1 \Leftrightarrow$ *dãy* $\{x_n\}$ *là dãy Cauchy đối với chuẩn* $|.|_2$.
5. $|.|_1 \sim |.|_2$

Chứng minh.

$1. \Rightarrow 2.$ Với mọi $x \in F,\ x \neq 0$; ta có $|x|_1 > 1 \Leftrightarrow |1/x|_1 < 1 \Leftrightarrow |1/x|_2 < 1 \Leftrightarrow |x|_2 > 1$. Do đó $|x|_1 \leq 1 \Leftrightarrow |x|_2 \leq 1;\ \forall x \in F,\ x \neq 0$, với $x = 0$ hiển nhiên.

$2. \Rightarrow 1.$ Với $x = 0$ hiển nhiên.
Với mọi $x \in F,\ x \neq 0$; ta có $|x|_1 \geq 1 \Leftrightarrow |1/x|_1 \leq 1 \Leftrightarrow |1/x|_2 \leq 1 \Leftrightarrow |x|_2 \geq 1$. Do đó $|x|_1 < 1 \Leftrightarrow |x|_2 < 1;\ \forall x \in F,\ x \neq 0$

$1. \Rightarrow 3.$

- Nếu chuẩn $|.|_1$ là chuẩn tầm thường thì chuẩn $|.|_2$ cũng là chuẩn tầm thường.
  Thật vậy, với mọi $x \in F,\ x \neq 0$ ta có $|x|_1 = 1$.
  Nếu $|x|_2 > 1$ thì $|1/x|_2 < 1 \Rightarrow |1/x|_1 < 1$ (mâu thuẫn)
  Nếu $|x|_2 < 1$ thì $|x|_1 < 1$ (mâu thuẫn)
  Do đó $|x|_2 = 1$ hay $|.|_2$ là chuẩn tầm thường. Vậy $|.|_1 \equiv |.|_2$
- Nếu $|.|_1$ không là chuẩn tầm thường thì tồn tại $x_0 \in F$ sao cho $|x_0|_1 > 1$, do đó $|x_0|_2 > 1$. Đặt $a = |x_0|_1$ và $b = |x_0|_2$. Khi đó, $\forall x \in F,\ x \neq 0$ ta viết $|x|_1 = a^y,\ y = \log_a |x|_1$. Ta sẽ chứng minh $|x|_2 = b^y$. Thật vậy, lấy $\frac{m}{n} > y$ ta có

$$|x|_1 = a^y < a^{\frac{m}{n}} = |x_0|_1^{\frac{m}{n}} \Rightarrow |x^n|_1 < |x_0^m|_1$$

$$\Rightarrow |x^n/x_0^m|_1 < 1 \Rightarrow |x^n/x_0^m|_2 < 1 \Rightarrow |x|_2 < b^{\frac{m}{n}}$$

cho $\frac{m}{n} \to y$ ta được $|x|_2 \le b^y$.
Tương tự nếu lấy $y > \frac{m}{n}$, thì ta được $|x|_2 \ge b^y$.
Vậy $|x|_2 = b^y$. Do đó

$$|x|_1 = a^y = (b^y)^{\log_b a} = |x|_2^c; \quad \text{với } c = \log_b a > 0$$

Với $x = 0$ hiển nhiên đẳng thức trên cũng thỏa mãn.

3. $\Rightarrow$ 4. Dãy $\{x_n\}$ là dãy Cauchy đối với chuẩn $|.|_1$ khi và chỉ khi

$$|x_n - x_m|_1 \to 0 \quad \text{khi } m, n \to \infty$$

$$\Leftrightarrow |x_n - x_m|_1^{1/c} \to 0 \quad \text{khi } m, n \to \infty \text{ với } c > 0$$

$$\Leftrightarrow |x_n - x_m|_2 \to 0 \quad \text{khi } m, n \to \infty$$

$\Leftrightarrow$ Dãy $\{x_n\}$ là dãy Cauchy đối với chuẩn $|.|_2$.

4. $\Rightarrow$ 1. Giả sử $|x|_1 < 1$ ta cần chứng minh $|x|_2 < 1$. Từ giả thiết $|x|_1 < 1$ ta suy ra $x^n \to 0$ đối với chuẩn $|.|_1$. Do đó $\{x^n\}$ là dãy Cauchy đối với $|.|_1$ hay $\{x^n\}$ là dãy Cauchy đối với $|.|_2$. Điều này có nghĩa là $(x^{n+1} - x^n) \to 0$ đối với chuẩn $|.|_2$ hay $x^n(x-1) \to 0$ đối với chuẩn $|.|_2$. Do đó $|x^n|_2|1-x|_2 \to 0$. Mà $|1-x|_2 \neq 0$ suy ra $|x^n|_2 \to 0$ hay $|x|_2 < 1$.

3. $\Rightarrow$ 5. Gọi τ_1, τ_2 lần lượt là tôpô được cảm sinh từ chuẩn $|.|_1, |.|_2$. Lấy $A \in \tau_1$, $\forall x \in A$ thì tồn tại $B_1(x,r) \subset A$. Khi đó

$$y \in B_1(x,r) \Leftrightarrow |y-x|_1 < r \Leftrightarrow |y-x|_1^{1/c} < r^{1/c}$$

$$\Leftrightarrow |y-x|_2 < r^{1/c} \Leftrightarrow y \in B_2(x, r^{1/c}) \Leftrightarrow B_1(x,r) = B_2(x, r^{1/c})$$

Điều này có nghĩa là tồn tại $B_2(x, r^{1/c}) \subset A$. Do đó $A \in \tau_2$.
Vậy $\tau_1 \equiv \tau_2$

5. $\Rightarrow$ 1. Giả sử $|x|_1 < 1$ suy ra $|x^n|_1 \to 0$. Do $|.|_1 \sim |.|_2$ nên $|x^n|_2 \to 0$. Suy ra $|x|_2 < 1$

$\square$

1.2 Chuẩn phi Archimedean

Định nghĩa 1.2.1. *Cho F là trường và $|.|$ là chuẩn trên F. Khi đó chuẩn $|.|$ được gọi là chuẩn phi Archimedean nếu nó thỏa mãn thêm điều kiện*

iii'. $|x+y| \le \max\{|x|, |y|\}; \quad \forall x, y \in F$

Ví dụ.

1. Chuẩn tầm thường trên trường F là chuẩn phi Archimedean.

2. Nếu F là trường hữu hạn thì mọi chuẩn trên F đều là chuẩn tầm thường. Do đó, mọi chuẩn trên trường hữu hạn F đều là phi Archimedean.

3. Cho p là số nguyên tố. Khi đó $\forall x \in \mathbb{Q},\ x \neq 0$ được biểu diễn dưới dạng

$$x = p^a \frac{m}{n}; \quad \text{với } a, m, n \in \mathbb{Z};\ n \neq 0;\ (m,p) = 1,\ (n,p) = 1$$

Ký hiệu $a = ord_p(x)$
Qui ước $ord_p(0) = \infty$

Bổ đề 1.2.1. *Cho p là số nguyên tố. Khi đó $\forall x, y \in \mathbb{Q}$ ta có*

i. $ord_p(xy) = ord_p(x) + ord_p(y)$

ii. $ord_p(x+y) \geq min\{ord_p(x), ord_p(y)\}$

Lấy $\rho \in (0,1)$. Khi đó chuẩn $|.| : \mathbb{Q} \to \mathbb{R}$ xác định bởi

$$|x| = \begin{cases} \rho^{ord_p(x)} & \text{nếu } x \neq 0 \\ 0 & \text{nếu } x = 0 \end{cases}$$

là chuẩn phi Archimedean trên $\mathbb{Q}$
Lấy $\rho_1, \rho_2 \in (0,1)$ và gọi $|.|_1, |.|_2$ tương ứng là hai chuẩn được xác định theo ρ_1, ρ_2. Khi đó $|.|_1 \sim |.|_2$. Thật vậy $\forall x \in \mathbb{Q},\ x \neq 0$

$$|x|_1 = \rho_1^{ord_p(x)} = (\rho_2^{ord_p(x)})^{log_{\rho_2}\rho_1} = |x|_2^c; \quad \text{với } c = log_{\rho_2}\rho_1 > 0$$

Lấy $\rho = \frac{1}{p}$, ta có chuẩn $|.|_p : \mathbb{Q} \to \mathbb{R}$ xác định bởi

$$|x|_p = \begin{cases} p^{-ord_p(x)} & \text{nếu } x \neq 0 \\ 0 & \text{nếu } x = 0 \end{cases}$$

là chuẩn phi Archimedean trên $\mathbb{Q}$. Ta hay gọi là chuẩn p-adic trên $\mathbb{Q}$.

□

Định lý 1.2.1 (Các điều kiện của chuẩn phi Archimedean). *Cho F là trường với e là phần tử đơn vị và $|.|$ là chuẩn trên F. Các điều kiện sau đây là tương đương.*

1. *Chuẩn $|.|$ là chuẩn phi Archimedean.*

2. $|2| \leq 1$, *với* $2 = 2.e = e + e$.

3. $|n| \leq 1$, *với* $n = n.e = \underbrace{e + e + \cdots + e}_{n}$

4. *Tập* $N = \{n = n.e \mid n \in \mathbb{N}\}$ *bị chặn.*

Chứng minh.

1. $\Rightarrow$ 2. Ta có $|2| = |e + e| \leq \max\{|e|, |e|\} = 1$

2. $\Rightarrow$ 3. Nếu $n \in N$ thì $n = a_0 + a_1 2 + \cdots + a_s 2^s$.
Trong đó $a_i \in \{0, 1\},\ \forall i = 0, 1, \ldots, s;\ a_s = 1$.
Suy ra $|a_i| \leq 1,\ \forall i = 0, 1, \ldots, s$. Do đó

$$|n| = |a_0 + a_1 2 + \cdots + a_s 2^s| \leq |a_0| + |a_1||2| + \cdots + |a_s||2^s|$$
$$\leq 1 + 1 + \cdots + 1 = s + 1$$

Mặt khác, ta có
$$2^s \leq n < 2^{s+1}$$
Suy ra
$$s + 1 \leq \log_2 n + 1$$
Do đó
$$|n| \leq \log_2 n + 1$$
Khi đó, với mọi số nguyên dương k, ta có
$$|n^k| \leq \log_2 n^k + 1 = k \log_2 n + 1 \leq k(\log_2 n + 1)$$
Suy ra
$$|n| \leq k^{1/k}(\log_2 n + 1)^{1/k}$$
Cho $k \to \infty$, ta sẽ có $|n| \leq 1$

3. $\Rightarrow$ 4. Hiển nhiên.

4. $\Rightarrow$ 1. Giả sử tập N bị chặn, tồn tại $a \in \mathbb{R}$ sao cho $|n| \leq a;\ \forall n \in N$. Khi đó

$$|x + y|^n = |(x + y)^n| = |\sum_{k=0}^{n} C_n^k x^k y^{n-k}|$$
$$\leq \sum_{k=0}^{n} |C_n^k||x|^k|y|^{n-k} \leq \sum_{k=0}^{n} a|x|^k|y|^{n-k}$$
$$\leq (n + 1)a(\max\{|x|, |y|\})^n$$

Suy ra
$$|x + y| \leq \sqrt[n]{n + 1}\,\sqrt[n]{a}\max\{|x|, |y|\}$$
Cho $n \to \infty$ thì $\sqrt[n]{n + 1}\,\sqrt[n]{a} \to 1$. Do đó
$$|x + y| \leq \max\{|x|, |y|\}$$
Vậy $|.|$ là chuẩn phi Archimedean.

$\square$

1.2.1 Tính chất cơ bản của chuẩn phi Archimedean

Mệnh đề 1.2.1 (Nguyên lý tam giác cân). *Cho $|.|$ là chuẩn phi Archimedean trên trường F. Nếu $|x| \neq |y|$ thì $|x+y| = \max\{|x|, |y|\}$.*

Chứng minh. Không mất tính tổng quát, ta giả sử $|x| > |y|$. Khi đó, ta có

$$|x| = |x+y-y| \leq \max\{|x+y|, |y|\} \leq \max\{|x|, |y|\} = |x|$$

Suy ra

$$|x| = \max\{|x+y|, |y|\}$$

Mà $|x| > |y|$ nên $|x| = |x+y|$. Vậy $|x+y| = \max\{|x|, |y|\}$. □

Mệnh đề 1.2.2. *Cho $|.|$ là chuẩn phi Archimedean trên trường F. Nếu dãy $\{x_n\} \to x \neq 0$ thì tồn tại $n_0 \in \mathbb{N}$ sao cho $|x_n| = |x|,\ \forall n \geq n_0$*

Chứng minh. Vì $x \neq 0$ nên $|x| > 0$ và do $\{x_n\} \to x$ nên tồn tại $n_0 \in \mathbb{N}$ sao cho $|x_n - x| < |x|;\ \forall n \geq n_0$. theo nguyên lý tam giác cân, ta có $|x_n| = |x_n - x + x| = \max\{|x_n - x|, |x|\} = |x|;\ \forall n \geq n_0$ □

1.3 Chuẩn trên $\mathbb{Q}$

Định lý 1.3.1 (Định lý Ostrowski). *Mọi chuẩn không tầm thường $|.|$ trên $\mathbb{Q}$ đều tương đương với chuẩn giá trị tuyệt đối thông thường hoặc chuẩn $|.|_p$, với p là số nguyên tố nào đó.*

Chứng minh.

1. Nếu $|2| > 1$ thì $|.|$ là chuẩn Archimedean.
   Lấy $n \in \mathbb{N}$, giả sử $n = a_0 + a_1 2 + \cdots + a_s 2^s$, trong đó $a_i \in \{0; 1\}$ và $2^s \leq n < 2^{s+1}$; $|2| = 2^a$, $a = \log_2 |2|$. Ta có

   $$|n| \leq |a_0| + |a_1||2| + \cdots + |a_s||2|^s \leq 1 + 2^a + \cdots + 2^{as} \leq 2^{as}C \leq n^a C$$

   Suy ra
   $$|n^k| \leq n^{ka}C \Rightarrow |n| \leq n^a C^{1/k}$$

   Cho $k \to \infty$ ta được $|n| \leq n^a$
   Mặt khác, do $2^s \leq n < 2^{s+1}$ nên ta có

   $$|2^{s+1}| = |n + 2^{s+1} - n| \leq |n| + |2^{s+1} - n|$$

   Suy ra
   $$|n| \geq |2^{s+1}| - |2^{s+1} - n| \geq 2^{(s+1)a} - (2^{s+1} - n)^a \geq 2^{(s+1)a} - 2^{sa}$$

   Do đó
   $$|n| \geq 2^{(s+1)a}C' \geq n^a C'$$

Suy ra

$$|n^k| \geq n^{ka}C' \Rightarrow |n| \geq n^a C'^{1/k}$$

Cho $k \to \infty$ ta được $|n| \geq n^a$. Vậy $|n| = n^a; \quad \forall n \in \mathbb{N}$.
Do đó $|x| = |x|^a; \quad \forall x \in \mathbb{Q}$

2. Nếu $|2| \leq 1$ thì $|.|$ là chuẩn phi Archimedean.
Từ giả thiết $|2| \leq 1$ ta có $|n| \leq 1; \ \forall x \in \mathbb{N}$. Do đó $|.|$ là chuẩn không tầm thường nên tồn tại $n \in \mathbb{N}^*$ sao cho $|n| < 1$. Gọi $p \neq 0$ là số tự nhiên bé nhất thỏa mãn $|p| < 1$. Khi đó p là số nguyên tố. Lấy $q \neq p$ là số nguyên tố, ta sẽ chứng minh $|q| = 1$. Giả sử $|q| < 1$, vì $(p^k, q^k) = 1$ nên tồn tại $u, v \in \mathbb{Z}$ sao cho $up^k + vq^k = 1$. Ta có

$$1 = |1| = |up^k + vq^k| \leq |u||p^k| + |v||q^k| \leq |p^k| + |q^k|$$

Cho $k \to \infty$ ta được $1 \leq 0$ (vô lý). Vậy $|q| = 1$.
Lấy $n \in \mathbb{N}$, giả sử $n = p^m p_1^{m_1} p_2^{m_2} \dots p_i^{m_i}$. ta có

$$|n| = |p|^m = \left[\left(\frac{1}{p}\right)^{\log_{\frac{1}{p}} |p|}\right]^m = \left(\frac{1}{p}\right)^{m \log_{\frac{1}{p}} |p|} = \left(\frac{1}{p^m}\right)^C = |n|_p^C$$

trong đó $C = \log_{\frac{1}{p}} |p|$. Do đó $|x| = |x|_p^C; \quad \forall x \in \mathbb{Q}$

□

1.4 Xây dựng trường số p-adic $\mathbb{Q}_p$

Từ định lý Oxtropski, ta thấy một chuẩn không tầm thường trên $\mathbb{Q}$ là giá trị tuyệt đối thông thường $|.|$, hoặc là chuẩn phi Archimedean $|.|_p$. Mặt khác, ta biết rằng làm đầy đủ $\mathbb{Q}$ theo $|.|$ ta thu được trường số thực $\mathbb{R}$. Do đó nếu ta làm đầy đủ $\mathbb{Q}$ theo $|.|_p$ ta cũng sẽ thu được trường mới mà ta gọi là trường các số p-adic $\mathbb{Q}_p$. Cụ thể cách xây dựng như sau:
Ký hiệu S là tập tất cả các dãy Cauchy hữu tỷ theo chuẩn $|.|_p$. Trên S ta xác định một quan hệ tương đương như sau:

$$\{x_n\} \sim \{y_n\} \Leftrightarrow \lim_{n \to \infty} |x_n - y_n|_p = 0$$

Ta gọi $\mathbb{Q}_p$ là tập hợp tất cả các lớp tương đương theo quan hệ trên và ta trang bị cho $\mathbb{Q}_p$ hai phép toán cộng và nhân như sau:

- Phép cộng

$$\overline{\{x_n\}} + \overline{\{y_n\}} = \overline{\{x_n + y_n\}}$$

Phần tử không là $0 = \overline{\{0\}}$
Phần tử đối của $x = \overline{\{x_n\}}$ là $-x = \overline{\{-x_n\}}$.
Ta có $(\mathbb{Q}_p, +)$ là một nhóm Abel.

- Phép nhân
$$\overline{\{x_n\}}.\overline{\{y_n\}} = \overline{\{x_n.y_n\}}$$

  Phần tử đơn vị là $1 = \overline{\{1\}}$
  Phần tử nghịch đảo: Ta có nhận xét rằng bất kỳ một lớp khác không $0 \neq x = \overline{\{x_n\}}$ của $\mathbb{Q}_p$ đều có một đại diện là dãy Cauchy mà mọi phần tử đều khác không. Thật vậy, nếu $x_i = 0$ ta có thể thay x_i bởi $x'_i = p^i$. Vậy nếu $x \in \mathbb{Q}_p,\ x \neq 0$ thì $x = \overline{\{x_n\}},\ x_n \neq 0,\ \forall n$. Khi đó $\frac{1}{x} = \overline{\{\frac{1}{x_n}\}}$ là phần tử nghịch đảo của x trong $\mathbb{Q}_p$.
  Ta có $(\mathbb{Q}_p^*, .)$ là một nhóm Abel.

Do đó, ta có thể chứng minh $(\mathbb{Q}_p, +, .)$ là một trường, trường này được gọi là trường số p-adic $\mathbb{Q}_p$. Trường $\mathbb{Q}$ có thể được xem như là trường con của $\mathbb{Q}_p$ nhờ đồng cấu nhúng

$$i : \mathbb{Q} \to \mathbb{Q}_p; \quad x \mapsto \overline{\{x\}}$$

1.4.1 Chuẩn trên $\mathbb{Q}_p$

Định nghĩa 1.4.1. *Chuẩn trên $\mathbb{Q}_p$ được xác định như sau:*

$$x \in \mathbb{Q}_p,\ x = \overline{\{x_n\}}; \quad |x|_p = \lim_{n\to\infty} |x_n|_p$$

Cách định nghĩa như vậy là hợp lý và thực sự cho ta một chuẩn trên $\mathbb{Q}_p$. Ta có thể thấy rõ được điều này qua những lý luận sau đây.

1. $\lim_{n\to\infty} |x_n|_p$ luôn luôn tồn tại.
   Nếu $x = 0$ thì $|x_n|_p \to 0$.
   Nếu $x \neq 0$ thì với $\varepsilon > 0$ nào đó và với $N \in \mathbb{N}$ tồn tại $i_N > N$ sao cho

$$|x_{i_N}|_p > \varepsilon \tag{1.1}$$

   Khi đó với N đủ lớn ta có

$$|x_i - x_{i'}|_p < \varepsilon; \quad \forall i, i' > N$$

   Chọn $i' = i_N$ ta được

$$|x_i - x_{i_N}|_p < \varepsilon; \quad \forall i > N \tag{1.2}$$

   Từ (1.1) và (1.2), áp dụng nguyên lý tam giác cân ta được

$$|x_i|_p = |x_{i_N}|_p; \quad \forall i > N$$

   Suy ra

$$\lim_{n\to\infty} |x_n|_p = |x_{i_N}|_p$$

2. Chuẩn $|x|_p$ không phụ thuộc vào cách chọn phần tử đại diện.
   Giả sử $x = \overline{\{x_n\}} = \overline{\{x'_n\}}$, khi đó $\{x_n\} \sim \{x'_n\}$, suy ra
   $$\lim_{n\to\infty} |x_n - x'_n|_p = 0$$
   Mặt khác, ta có $|x_n - x'_n|_p \geq ||x_n|_p - |x'_n|_p|$. Do đó
   $$\lim_{n\to\infty} ||x_n|_p - |x'_n|_p| = 0$$
   Suy ra
   $$\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |x'_n|_p$$

Chú ý. Khi tiến hành làm đầy đủ $\mathbb{Q}$ để thu được $\mathbb{R}$ thì tập giá trị của chuẩn $|.|$ tăng lên đến tập hợp tất cả các số thực không âm. Nhưng khi làm đầy đủ $\mathbb{Q}$ để thu được $\mathbb{Q}_p$ thì tập giá trị của chuẩn $|.|_p$ vẫn giữ nguyên là $\{p^n | n \in \mathbb{Z}\} \cup \{0\}$. □

1.4.2 Đồng dư trong $\mathbb{Q}_p$

Với $a, b \in \mathbb{Q}_p$, ta nói $a \equiv b \pmod{p^n} \Leftrightarrow |a-b|_p \leq p^{-n}$.
Nếu $a, b \in \mathbb{Z}$ thì định nghĩa đồng dư trong $\mathbb{Q}_p$ sẽ trùng với định nghĩa đồng dư thông thường trên tập hợp số nguyên $\mathbb{Z}$.

1.4.3 Số nguyên p-adic

Tập hợp $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}$ cùng với phép cộng và phép nhân trong $\mathbb{Q}_p$ lập thành một vành. Vành này được gọi là vành các số nguyên p-adic.
Tập hợp tất cả các phần tử khả nghịch của vành $\mathbb{Z}_p$ là
$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p : 1/x \in \mathbb{Z}_p\} = \{x \in \mathbb{Z}_p : |x|_p = 1\}$$
Các phần tử của $\mathbb{Z}_p^*$ còn được gọi là các đơn vị p-adic.

1.5 Biểu diễn p-adic của số x trong $\mathbb{Q}_p$

Ta đã biết rằng, nếu $x \in \mathbb{Q}_p$ thì ta có thể viết $x = \overline{\{x_n\}}$ với $\{x_n\}$ là dãy Cauchy nào đó trong $\mathbb{Q}$. Tuy nhiên nếu x là một số nguyên p-adic thì ta có thể chọn đại diện $\{x_n\}$ thỏa mãn một số điều kiện đặc biệt nào đó. Trước hết, ta cần tới các bổ đề sau đây.

Bổ đề 1.5.1. *Nếu* $x = \overline{\{x_n\}} \in \mathbb{Q}_p$ *thì* $\lim_{n\to\infty} x_n = x$

Chứng minh. Ta có $x - x_n = \overline{\{(x_i - x_n)_i\}}$. Do đó

$$|x - x_n|_p = \lim_{i\to\infty} |x_i - x_n|_p$$

Vì $\{x_n\}$ là dãy Cauchy trong $\mathbb{Q}$ nên với mọi $\varepsilon > 0$ tồn tại $N \in \mathbb{N}$ sao cho $\forall i, i' > N$ ta có $|x_i - x_i'|_p < \varepsilon$. Chọn $n > N$, khi đó $\forall i > N$ ta có $|x_i - x_n|_p < \varepsilon$. Do đó

$$|x - x_n|_p \leq \varepsilon; \quad \forall n > N$$

Vậy

$$\lim_{n\to\infty} x_n = x$$

□

Bổ đề 1.5.2. *Nếu $x \in \mathbb{Q}$ và $|x|_p \leq 1$ thì $\forall i \in \mathbb{N}$, tồn tại $a \in \mathbb{Z}$ sao cho $|a - x|_p \leq p^{-i}$. Hơn nữa, số a có thể chọn trong tập $\{0, 1, \ldots, p^i - 1\}$*

Chứng minh. Giả sử $x = \frac{m}{n} \in \mathbb{Q}$, $(m, n) = 1$. Do $|x|_p \leq 1$ nên $(n, p) = 1 \Rightarrow (n, p^i) = 1$, do đó tồn tại $u, v \in \mathbb{Z}$ sao cho $un + vp^i = 1$. Đặt $b = mu \in \mathbb{Z}$, khi đó

$$|b - x|_p = |x|_p |nu - 1|_p \leq |nu - 1|_p = |vp^i|_p \leq p^{-i}$$

Đặt $b = p^i q + a$ trong đó $0 \leq a \leq p^i - 1$. Khi đó

$$|a - x|_p = |b - x - p^i q|_p \leq \max\{|b - x|_p, |p^i q|_p\} \leq p^{-i}$$

□

Định lý 1.5.1. *Với mỗi $a \in \mathbb{Z}_p$ có duy nhất một đại diện là dãy Cauchy các số nguyên $\{a_i\}$ thỏa mãn*

1. $0 \leq a_i \leq p^i - 1; \quad \forall i = 1, 2, \ldots$
2. $a_i \equiv a_{i+1} \pmod{p^i}$

Chứng minh.

- Sự tồn tại:
  Giả sử dãy Cauchy $\{c_i\}$ là dãy đại diện bất kỳ của a. Ta phải tìm một dãy Cauchy gồm các số nguyên $\{a_i\}$ tương đương với $\{c_i\}$ và thỏa hai điều kiện của định lý.
  Do $\{c_i\}$ là dãy Cauchy nên với mỗi số $j = 1, 2, \ldots$ tồn tại một số $N(j) \in \mathbb{N}$ sao cho

$$|c_i - c_{i'}|_p \leq p^{-j}; \quad \forall i, i' \geq N(j)$$

  Khi đó $\forall j = 1, 2, \ldots$ và $\forall i' \geq N(j)$ ta có

$$|c_{N(j)}|_p = |c_{i'} + c_{N(j)} - c_{i'}|_p \leq \max\{|c_{i'}|_p, |c_{N(j)} - c_{i'}|_p\} \leq \max\{|c_{i'}|_p, p^{-j}\}$$

Vì $|c_{i'}|_p \to |a|_p \leq 1$ khi $i' \to \infty$ nên ta có

$$|c_{N(j)}|_p \leq 1; \quad \forall j = 1, 2, \ldots$$

Áp dụng bổ đề (1.5.2) ta tìm được dãy số nguyên $\{a_j\}$ thỏa mãn

$$\begin{cases} 0 \leq a_j < p^j \\ |a_j - c_{N(j)}|_p \leq p^{-j} \end{cases}$$

Ta chứng minh $\{a_j\}$ là dãy cần tìm:

$$|a_{j+1} - a_j|_p = |a_{j+1} - c_{N(j+1)} + c_{N(j+1)} - c_{N(j)} - (a_j - c_{N(j)})|_p$$

$$\begin{aligned} &\leq \max\{|a_{j+1} - c_{N(j+1)}|_p, |c_{N(j+1)} - c_{N(j)}|_p, |a_j - c_{N(j)}|_p\} \\ &\leq \max\{p^{-(j+1)}, p^{-j}, p^{-j}\} = p^{-j} \end{aligned}$$

Suy ra $\{a_j\}$ là dãy Cauchy và $a_j \equiv a_{j+1} \pmod{p^j}$
Lấy j bất kỳ, khi đó ta có

$$|a_j - c_j|_p = |a_j - c_{N(j)} + c_{N(j)} - c_j|_p$$

$$\begin{aligned} &\leq \max\{|a_j - c_{N(j)}|_p, |c_{N(j)} - c_j|_p\} \\ &\leq \max\{p^{-j}, p^{-j}\} = p^{-j} \end{aligned}$$

Do đó $|a_j - c_j|_p \to 0$ khi $j \to \infty$ hay $\{a_j\} \sim \{c_j\}$

- Sự duy nhất:
  Nếu $\{a'_i\}$ là một dãy số nguyên khác thỏa hai điều kiện của định lý thì tồn tại $i_0 \in \mathbb{N}$ nào đó sao cho $a_{i_0} \neq a'_{i_0}$.
  Vì $0 \leq a_{i_0}, a'_{i_0} < p^{i_0}$ nên $a_{i_0} \not\equiv a'_{i_0} \pmod{p^{i_0}} \Rightarrow |a_{i_0} - a'_{i_0}|_p > p^{-i_0}$.
  Nếu $i \geq i_0$ thì $|a_i - a_{i_0}|_p \leq p^{-i_0}$ và $|a'_i - a'_{i_0}|_p \leq p^{-i_0}$. Do đó theo nguyên lý tam giác cân ta có $|a_i - a_{i'}|_p = |a_{i_0} - a'_{i_0}|_p > p^{-i_0}$; $\forall i \geq i_0$.
  Suy ra $\{a_i\} \nsim \{a'_i\}$

□

Với các số nguyên $\{a_i\}$ thỏa mãn các điều kiện trong định lý (1.5.1), ta có thể viết

$$\begin{aligned} &a_1 = b_0 \\ &a_2 = b_0 + b_1 p \\ &a_3 = b_0 + b_1 p + b_2 p^2 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &a_i = b_0 + b_1 p + \cdots + b_{i-1} p^{i-1} \end{aligned}$$

trong đó $0 \leq b_i \leq p - 1$ với $i = 0, 1, 2, \ldots$. Khi đó với mỗi $a \in \mathbb{Z}_p$ ta có

$$a = \overline{\{b_0 + b_1 p + \cdots + b_{i-1} p^{i-1}\}}$$

Theo bổ đề (1.5.1), ta có thể viết a dưới dạng

$$a = b_0 + b_1 p + \cdots + b_n p^n + \cdots$$

Công thức này được gọi là biểu diễn p-adic của a trong $\mathbb{Z}_p$.
Nếu $x \in \mathbb{Q}_p$ bất kỳ, $|x|_p = p^m$ với $m \in \mathbb{Z}$ thì ta sẽ nhân x với một số p^m sao cho số $x' = xp^m$ thỏa mãn $|x'|_p = 1$. Sau đó áp dụng định lý (1.5.1), ta sẽ chọn được một dãy $\{b_i\}$ sao cho $b_0 \neq 0$, $0 \leq b_i \leq p-1$ và ta có

$$x' = b_0 + b_1 p + \cdots + b_n p^n + \cdots = \sum_{i=0}^{\infty} b_i p^i$$

Suy ra biểu diễn của x sẽ có dạng

$$x = \frac{x'}{p^m} = b_0 p^{-m} + b_1 p^{-m+1} + \cdots + b_n p^{-m+n} + \cdots$$

Đặt $c_i = b_{i+m}, \forall i = -m, \ldots, 0, 1, \ldots$, khi đó $c_{-m} \neq 0$ và ta sẽ có

$$x = c_{-m} p^{-m} + c_{-m+1} p^{-m+1} + \cdots + c_{-m+n} p^{-m+n} + \cdots = \sum_{i=-m}^{\infty} c_i p^i$$

Trong đó $m \in \mathbb{Z}$, $c_{-m} \neq 0$, $0 \leq c_i \leq p-1$ sao cho $|x|_p = p^m$. Công thức này được gọi là công thức biểu diễn p-adic của x trong $\mathbb{Q}_p$.

1.6 Bổ đề Hensel

Các phép toán số học thông thường như: cộng, trừ, nhân và chia trong $\mathbb{Q}_p$ được thực hiện một cách dễ dàng. Tuy nhiên, việc khai căn của một số nguyên và việc tìm nghiệm của một phương trình nào đó trong $\mathbb{Q}_p$ noi chung là vấn đề không phải lúc nào chúng ta cũng thực hiện được. Bổ đề Hensel và bổ đề Hensel mở rộng được trình bày dưới đây sẽ giúp chúng ta giải quyết một phần nào về vấn đề nói trên.

Định lý 1.6.1 (Bổ đề Hensel). *Cho* $F(x) = c_0 + c_1 x + \cdots + c_n x^n \in \mathbb{Z}_p[x]$ *có đạo hàm* $F'(x) = c_1 + 2c_2 x + \cdots + nc_n x^{n-1} \in \mathbb{Z}_p[x]$. *Giả sử có* $a_0 \in \mathbb{Z}_p$ *thỏa* $F(a_0) \equiv 0 \pmod p$ *và* $F'(a_0) \not\equiv 0 \pmod p$. *Khi đó tồn tại duy nhất* $a \in \mathbb{Z}_p$ *sao cho* $F(a) = 0$ *và* $a \equiv a_0 \pmod p$.

Định lý 1.6.2 (Bổ đề Hensel mở rộng). *Cho* $F(x) = c_0 + c_1 x + \cdots + c_n x^n \in \mathbb{Z}_p[x]$ *có đạo hàm* $F'(x) = c_1 + 2c_2 x + \cdots + nc_n x^{n-1} \in \mathbb{Z}_p[x]$. *Giả sử có* $a_0 \in \mathbb{Z}_p$ *thỏa* $F(a_0) \equiv 0 \pmod{p^{2m+1}}$, $F'(a_0) \equiv 0 \pmod{p^m}$ *và* $F'(a_0) \not\equiv 0 \pmod{p^{m+1}}$. *Khi đó tồn tại duy nhất* $a \in \mathbb{Z}_p$ *sao cho* $F(a) = 0$ *và* $a \equiv a_0 \pmod{p^{m+1}}$.

Chứng minh. □

1.7 Nhóm giá trị và trường thặng dư của $\mathbb{Q}_p$

1.8 Một số tính chất tôpô của $\mathbb{Q}_p$

Vì Tôpô trong $\mathbb{Q}_p$ là tôpô cảm sinh bởi chuẩn phi Archimedean nên nó có nhiều tính chất khác lạ so với tôpô thông thường.

Định nghĩa 1.8.1.

- *Hình cầu mở tâm a bán kính r là tập hợp*

$$B(a,r) = \{x \in \mathbb{Q}_p : |x-a|_p < r\}$$

- *Hình cầu đóng tâm a bán kính r là tập hợp*

$$B[a,r] = \{x \in \mathbb{Q}_p : |x-a|_p \leq r\}$$

- *Mặt cầu tâm a bán kính r là tập hợp*

$$D(a,r) = \{x \in \mathbb{Q}_p : |x-a|_p = r\}$$

Từ định nghĩa này ta thấy $\mathbb{Z}_p$ là hình cầu mở tâm 0 bán kính 1 và $\mathbb{Z}_p^*$ là mặt cầu tâm 0 bán kính 1.

Mệnh đề 1.8.1.

1. *Mọi hình cầu, mặt cầu trong $\mathbb{Q}_p$ đều là những tập vừa đóng, vừa mở.*
2. *Hai hình cầu bất kỳ trong $\mathbb{Q}_p$ hoặc lồng nhau hoặc rời nhau.*
3. *Mọi hình cầu, mặt cầu trong $\mathbb{Q}_p$ đều có vô số tâm. Mọi hình cầu đều có vô số bán kính.*
4. *$\mathbb{Q}_p$ chỉ có một số đếm được các hình cầu và mặt cầu.*

Chứng minh.

1.

2.

3.

4.

$\square$

Ta đã biết vành số nguyên p-adic $\mathbb{Z}_p$ chính là hình cầu mở $B(0,1)$ nên $\mathbb{Z}_p$ là tập mở. Hơn thế nữa, ta còn có mệnh đề.

Mệnh đề 1.8.2. *$\mathbb{Z}_p$ là tập compact.*

Chứng minh. Lấy $\{x_n\}$ là một dãy trong $\mathbb{Z}_p$. Ta sẽ xây dựng một dãy con $\{x_{n_k}\}$ hội tụ trong $\mathbb{Z}_p$. Xét các khai triển $p-$adic:

$$x_1 = x_{10} + x_{11}p + \cdots + x_{1k}p^k + \cdots$$

$$x_2 = x_{20} + x_{21}p + \cdots + x_{2k}p^k + \cdots$$

$$\vdots$$

$$x_n = x_{n0} + x_{n1}p + \cdots + x_{nk}p^k + \cdots$$

$$\vdots$$

Do $x_{10}, x_{20}, \ldots, x_{n0}, \ldots$ gồm vô hạn các phần tử nhưng chỉ nhận các giá trị trong tập hữu hạn $\{0, 1, \ldots, p-1\}$ nên tồn tại tập K_0 gồm vô hạn các phần tử của dãy $\{x_n\}$ sao cho chữ số đầu tiên trong khai triển $p-$adic của mỗi phần tử thuộc K_0 đều bằng nhau và bằng b_0. Tương tự, $K_1 \subset K_0$: tập vô hạn các phần tử của dãy $\{x_n\}$ sao cho chữ số thứ hai trong khai triển $p-$adic của mỗi phần tử thuộc K_1 đều bằng nhau và bằng b_1. Cứ thế, tiếp tục quá trình trên ta xây dựng được một dãy các tập vô hạn lồng nhau:

$$K_0 \supset K_1 \supset \cdots \supset K_n \supset \cdots$$

Trong đó K_n là tập con vô hạn các phần tử của dãy $\{x_n\}$ sao cho trong khai triển $p-$adic của mỗi phần tử thuộc K_n chữ số đầu tiên đều bằng b_0, chữ số thứ hai đều bằng $b_1, \ldots,$ chữ số thứ $n+1$ đều bằng b_n.
Lấy $x_{n_0} \in K_0, x_{n_1} \in K_1, \ldots, x_{n_i} \in K_i, \ldots (n_0 < n_1 < \cdots < n_i < \cdots)$.
Đặt $a = b_0 + b_1 p + \cdots + b_i p^i + \cdots \in \mathbb{Z}_p$. Ta có $|x_{n_i} - a|_p \leq p^{-i-1}$.
Cho $i \to \infty$ ta được dãy con $\{x_{n_i}\}$ hội tụ về $a \in \mathbb{Z}_p$.
Vậy $\mathbb{Z}_p$ là tập compact. □

Nhận xét. Như vậy, chúng ta đã chứng minh được $\mathbb{Z}_p$ là tập compact, điều này có nghĩa là $B(0,1)$ là tập compact. Do đó với mọi $a \in \mathbb{Q}_p$ thì $a + \mathbb{Z}_p$ là lân cận compact của a trong $\mathbb{Q}_p$. Vì vậy, $\mathbb{Q}_p$ là tập compact địa phương. □

1.8.1 Khoảng trong $\mathbb{Q}_p$

1.9 Bài tập chương 1

Chương 2

Xây dựng trường số phức p-adic $\mathbb{C}_p$

2.1 Chuẩn trên không gian vectơ

2.2 Trường $\overline{\mathbb{Q}_p}$

2.3 Các tính chất cơ bản của $\mathbb{C}_p$

1. $\mathbb{C}_p$ đầy đủ.

2. $\mathbb{C}_p$ là trường đóng đại số.

   Chứng minh. Đầu tiên, ta sẽ chứng minh bổ đề sau đây.

   Bổ đề 2.3.1. *Lấy $g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0 \in \mathbb{Q}_p[x]$. Khi đó, nếu β là một nghiệm của $g(x)$ thì $|\beta|_p \leq c = \max\{1, |b_i|_p\}$*

   Chứng minh. Giả sử β là nghiệm của $g(x)$ và $|\beta|_p > c$ (*)
   Ta có

$$\beta^n + b_{n-1}\beta^{n-1} + \cdots + b_0 = 0$$

$$\Rightarrow \beta = -b_{n-1} - \frac{b_{n-2}}{\beta} - \cdots - \frac{b_0}{\beta^{n-1}}$$

$$\Rightarrow |\beta|_p \leq \max_{0 \leq i \leq n-1}\{|\frac{b_{n-i-1}}{\beta^i}|_p\} \leq \max_{0 \leq i \leq n-1}\{|b_{n-i-1}|_p\} \quad (\text{do } |\beta^i|_p > 1)$$

$$\leq c \quad (\text{mâu thuẫn với (*)})$$

   Vậy $|\beta|_p \leq c$ ∎

Lấy $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{C}_p[x]$, với $a_i \in \mathbb{C}_p$. Ta sẽ chứng minh $f(x)$ có nghiệm trong $\mathbb{C}_p$.
Với mỗi $i = 0, 1, \ldots, n-1$; lấy $\{a_{ij}\}_j$ là dãy phần tử của $\overline{\mathbb{Q}_p}$ hội tụ về a_i. Đặt

$$g_j(x) = x^n + a_{n-1,j}x^{n-1} + \cdots + a_{1,j}x + a_{0,j} \quad ;\forall j$$

Lấy r_{ij} là nghiệm của $g_j(x)$ trong $\overline{\mathbb{Q}_p}$ $(i = 1, 2, \ldots, n)$. Ta có

$$g_{j+1}(x) = \Pi_{i=1}^n (x - r_{i,j+1})$$

Với mọi j, ta đặt $A_j = \max_{1\le i\le n}\{1, |a_{ij}|^n\}$. Do $a_{ij} \to a_i$ khi $j \to \infty$ nên $a_{ij}^n \to a_i^n$ khi $j \to \infty$. Do đó $|a_{ij}|^n$ bị chặn khi $j \to \infty$, suy ra A_j bị chặn khi $j \to \infty$, tồn tại A sao cho $A_j < A$,$\forall j$.
Theo bổ đề 2.3.1, ta được $\max_{1\le i\le n}\{1, |r_{ij}|^n\} < A$

$\square$

3. $\mathbb{C}_p$ là không gian vectơ vô hạn chiều trên $\mathbb{Q}_p$
4. Nhóm giá trị $|\mathbb{C}_p^*| = \{p^r : r \in \mathbb{Q}\} \le (\mathbb{R}^+, .)$
5. Trường thặng dư của $\mathbb{C}_p$ là bao đóng đại số của $F_p = \mathbb{Z}_p/p\mathbb{Z}_p$
6. $\mathbb{C}_p$ là không gian khả ly.
7. $\mathbb{C}_p$ không compact địa phương.

Chứng minh. Với $m \in \mathbb{N}, (m, p) = 1$, ta kí hiệu

$$\sqrt[m]{1} = \{z \in \mathbb{C}_p : z^m = 1\}$$

Dễ dàng thấy, $z \in \sqrt[m]{1} \Leftrightarrow z^m = 1$. Suy ra $|z|_p^m = 1 \Rightarrow |z|_p = 1$

Bổ đề 2.3.2. *Với* $m \in \mathbb{N}, (m, p) = 1, z \in \sqrt[m]{1}, z \neq 1$ *thì* $|z - 1|_p = 1$

Chứng minh. Ta có $|z-1|_p \le \max\{|z|_p, |1|_p\} = 1$. Giả sử $|z-1|_p < 1$. Đặt $a = z-1 \neq 0$ thì $0 \neq |a|_p < 1$ và $z = a + 1$. Khi đó

$$1 = z^m = (1 + a)^m = 1 + C_m^1 a + \cdots + C_m^{m-1}a^{m-1} + a^m$$

Suy ra

$$C_m^1 a + \cdots + C_m^{m-1}a^{m-1} + a^m = 0$$
$$\Rightarrow a(C_m^1 + \cdots + C_m^{m-1}a^{m-2} + a^{m-1}) = 0$$
$$\Rightarrow |a|_p|m + \cdots + C_m^{m-1}a^{m-2} + a^{m-1}|_p = 0$$

Ta lại có $(m,p) = 1$ nên $|m|_p = 1$ và do $|a|_p < 1$ nên ta cũng có $|C_m^i a^{i-1}|_p = |C_m^i|_p |a|_p^{i-1} \leq |a|_p < 1$, $\forall i = 2, \ldots, m$. Do đó, ta phải có

$$|m + \cdots + C_m^{m-1} a^{m-2} + a^{m-1}|_p = 1$$

Suy ra $|a|_p = 0 \Rightarrow a = 0 \Rightarrow z = 1$. Ta gặp sự mâu thuẫn.
Vậy $|z-1|_p = 1$ □

Bây giờ, ta sẽ đi chứng minh $\mathbb{C}_p$ không compact địa phương. Đặt

$$I = \bigcup_{(m,p)=1} \sqrt[m]{1}$$

Khi đó, I là một tập hợp vô hạn các phần tử nằm trên mặt cầu đơn vị. Lấy $\{z_i\}_{i\in\mathbb{N}} \subset I$ là một dãy bất kỳ gồm các phần tử phân biệt thuộc I. Ta sẽ chứng minh $\{z_i\}_{i\in\mathbb{N}}$ không có dãy con hội tụ. Thật vậy, với $z_i \neq z_j$ bất kỳ, giả sử $z_i \in \sqrt[m]{1}, z_j \in \sqrt[n]{1}$. Khi đó, ta có

$$(|\frac{z_i}{z_j}|_p)^{mn} = \frac{|z_i|_p^{mn}}{|z_j|_p^{mn}} = 1$$

Suy ra

$$\frac{z_i}{z_j} \in \sqrt[mn]{1} \ , \ \frac{z_i}{z_j} \neq 1$$

Do đó, theo bổ đề trên, ta sẽ có

$$|z_i - z_j|_p = |z_j|_p |\frac{z_i}{z_j} - 1|_p = 1$$

Suy ra mọi dãy con của $\{z_i\}_{i\in\mathbb{N}}$ đều không hội tụ. Do đó quả cầu đơn vị là không compact, hay mọi quả cầu trong $\mathbb{C}_p$ đều không compact. Vậy $\mathbb{C}_p$ không compact địa phương. □

8. $\mathbb{C}_p$ có lực lượng continum, nhưng số hình cầu trong $\mathbb{C}_p$ là đếm được.

2.4 Bài tập chương 2

1. Gọi $\mathbb{C}_p^+ = \{z \in \mathbb{C}_p : |z-1|_p < 1\}$ là tập hợp các phần tử dương của $\mathbb{C}_p$. Chứng minh các khẳng định sau là tương đương

   (a) $a \in \mathbb{C}_p^+$

   (b) $\lim_{n\to\infty} a^{p^n} = 1$

   (c) $a^p \in \mathbb{C}_p^+$

Giải. $(a) \Rightarrow (b)$
Lấy $a \in \mathbb{C}_p^+$, đặt $c = \max\{|a-1|_p, 1/p\}$, khi đó $0 < c < 1$. Ta sẽ chứng minh bằng quy nạp khẳng định sau $|a^{p^n} - 1|_p \leq c^{n+1}$.
Với $n = 0$, ta có $|a-1|_p \leq c$, điều này luôn đúng do cách xác định c.
Giả sử, ta đã có $|a^{p^n} - 1|_p \leq c^{n+1}$.
Ta cần chứng minh $|a^{p^{n+1}} - 1|_p \leq c^{n+2}$.
Đặt $b = a^{p^n} - 1$, suy ra $|b|_p \leq c^{n+1} \leq c$. Khi đó

$$\begin{aligned}|a^{p^{n+2}} - 1|_p = |(a^{p^n})^p - 1|_p &= |(b+1)^p - 1|_p \\ &= |b^p + C_p^1 b^{p-1} + \cdots + C_p^{p-1} b|_p \\ &= |b|_p |b^{p-1} + C_p^1 b^{p-2} + \cdots + C_p^{p-1}|_p\end{aligned}$$

Vì $|b|_p \leq c^{n+1} \leq c$ nên $|C_p^k b^{p-k-1}|_p = |C_p^k|_p |b^{p-k-1}|_p \leq |b^{p-k-1}|_p \leq c^{p-k-1} \leq c$;$\forall k = 0, 1, \ldots, p-2$ và $|C_p^{p-1}|_p = |p|_p = 1/p \leq c$. Do đó

$$|b^{p-1} + C_p^1 b^{p-2} + \cdots + C_p^{p-1}|_p \leq c$$

Suy ra

$$|a^{p^{n+1}} - 1|_p \leq c^{n+2}$$

Vậy ta đã chứng minh được $|a^{p^n} - 1|_p \leq c^{n+1}$, với $0 < c < 1$. Do đó

$$\lim_{n\to\infty} |a^{p^n} - 1|_p = 0 \;\Rightarrow\; \lim_{n\to\infty} a^{p^n} = 1$$

$(b) \Rightarrow (a)$
Giả sử $\lim_{n\to\infty} a^{p^n} = 1 \Rightarrow \exists n : |a^{p^n} - 1|_p < 1$. Đặt $x = a - 1$, ta cần chứng minh $|x|_p < 1$. Giả sử $|x|_p \geq 1$, ta có

$$1 > |(x+1)^{p^n} - 1|_p = |x^{p^n} + C_{p^n}^1 x^{p^n - 1} + \cdots + C_{p^n}^{p^n - 1} x|_p$$

Vì $|x|_p \geq 1$ nên với mọi $k = 1, 2, \ldots, p^n - 1$, ta có

$$|C_{p^n}^k x^{p^n - k}|_p = |C_{p^n}^k|_p |x^{p^n - k}|_p < |x|_p^{p^n - k} \leq |x|_p^{p^n}$$

Theo nguyên lý tam giác cân ta phải có

$$1 > |x^{p^n} + C_{p^n}^1 x^{p^n - 1} + \cdots + C_{p^n}^{p^n - 1} x|_p = |x|_p^{p^n} \geq 1$$

Suy ra $1 > 1$ (vô lý)
Ta đã chứng minh được $(a) \Leftrightarrow (b)$
Mặt khác, ta lại có

$$\begin{aligned}a \in \mathbb{C}_p^+ \Leftrightarrow \lim_{n\to\infty} a^{p^n} = 1 &\Leftrightarrow \lim_{n\to\infty} a^{p^{n+1}} = 1 \\ \Leftrightarrow \lim_{n\to\infty} (a^p)^{p^n} = 1 &\Leftrightarrow a^p \in \mathbb{C}_p^+\end{aligned}$$

Vậy ta cũng có được $(a) \Leftrightarrow (c)$ □

Chương 3

Hàm giải tích p-adic

3.1 Chuỗi lũy thừa

Chuỗi $\sum_{n=0}^{\infty} a_n$ hội tụ khi và chỉ khi dãy $S_n = \sum_{i=0}^{n} a_i$ hội tụ $\Leftrightarrow \{S_n\}$ là dãy Cauchy $\Leftrightarrow S_n - S_{n-1} = a_n \to 0$.
Chuỗi $\sum_{n=0}^{\infty} a_n z^n$, $a_n \in \mathbb{C}_p$ gọi là chuỗi lũy thừa (1).
Bán kính hội tụ của chuỗi (1) là

$$r = \frac{1}{\lim_{n\to\infty} \sup |a_n|_p^{1/n}}$$

1. $\forall z \in \mathbb{C}_p, |z|_p < r$: chuỗi (1) hội tụ.
2. $\forall z \in \mathbb{C}_p, |z|_p > r$: chuỗi (1) phân kỳ.
3. $\forall z \in \mathbb{C}_p, |z|_p = r$: chuỗi (1) hội tụ nếu $a_n r^n \to 0$, chuỗi (1) phân kỳ nếu $a_n r^n \not\to 0$.

3.2 Hàm giải tích

Gọi $D = D(0, r) = \{z \in \mathbb{C}_p : |z|_p < r\}$. Hàm $f : D \to \mathbb{C}_p$ gọi là hàm giải tích trên D nếu $f(z)$ biểu diễn được dưới dạng chuỗi lũy thừa hội tụ, tức là

$$f(z) = \sum_{n=0}^{\infty} a_n z^n$$

hội tụ trong $D = D(0, r)$.

Ví dụ.

1. $$\log(1 + z) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1} z^n}{n}$$

Bán kính hội tụ:

$$r = \frac{1}{\lim_{n\to\infty} \sup |1/n|_p^{1/n}} = \lim_{n\to\infty} \sqrt[n]{|n|_p}$$

Ta có $n = p^{ord_p n} m$, $(m,p) = 1 \Rightarrow |n|_p = p^{-ord_p n} \le 1$. Do đó

$$\frac{1}{n} = p^{-ord_p n} \frac{1}{m} \le |n|_p = p^{-ord_p n} \le 1$$

Suy ra

$$\frac{1}{\sqrt[n]{n}} \le \sqrt[n]{|n|_p} \le 1$$

Chuyển qua giới hạn ta được:

$$r = \lim_{n\to\infty} \sqrt[n]{|n|_p} = 1$$

Xét $|z|_p = 1$:
Ta có $|1/n|_p \not\to 0$ vì tồn tại dãy con $\{n_k\}, (n_k, p) = 1$.
Khi đó $|1/n_k|_p = 1 \not\to 0$. Vậy chuỗi không hội tụ nếu $|z|_p = 1$.
Kết luận: $\log(1+z) : D(0,1) \longrightarrow \mathbb{C}_p$

$$z \longmapsto \sum_{n=1}^{\infty} \frac{(-1)^{n+1} z^n}{n}$$

là hàm giải tích trên $D(0,1)$.

2.

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

Bán kính hội tụ:

$$r = \frac{1}{\lim_{n\to\infty} \sup |1/n!|_p^{1/n}} = \lim_{n\to\infty} \sqrt[n]{|n!|_p}$$

Ta có

$$ord_p(n!) = \frac{n - S_n}{p-1} \ , \ S_n = a_0 + a_1 + \cdots + a_s$$

trong đó $a_0, a_1, \ldots, a_s$ là các chữ số của n trong khai triển $p-$adic $n = a_0 + a_1 p + \cdots + a_s p^s$, $0 \le a_i \le p-1, a_s \ne 0$. Ta có

$$S_n = a_0 + a_1 + \cdots + a_s \le (p-1)(s+1) \le (p-1)(\log_p n + 1)$$

Do đó

$$\frac{n - (p-1)(\log_p n + 1)}{n(p-1)} \le \frac{ord_p(n!)}{n} \le \frac{1}{p-1}$$

Chuyển qua giới hạn ta được:

$$\lim_{n\to\infty} \frac{ord_p(n!)}{n} = \frac{1}{p-1}$$

Suy ra

$$r = \lim_{n\to\infty} \sqrt[n]{|n!|_p} = p^{-\lim_{n\to\infty} \frac{ord_p(n!)}{n}} = p^{\frac{1}{1-p}}$$

Xét $|z|_p = p^{\frac{1}{1-p}}$: ta cần kiểm tra $\frac{p^{\frac{n}{1-p}}}{n!} \to 0 \Leftrightarrow |\frac{p^{\frac{n}{1-p}}}{n!}|_p \to 0$

$$\Leftrightarrow \frac{n}{p-1} - \frac{n-S_n}{p-1} \to \infty \Leftrightarrow \frac{S_n}{p-1} \to \infty$$

Thế nhưng, ta có với $n_k = p^k$ thì $S_{n_k} = 1 \not\to \infty$. Vậy chuỗi phân kỳ.
Kết luận: $e^z : D(0, p^{\frac{1}{1-p}}) \longrightarrow \mathbb{C}_p$

$$z \longmapsto \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

là hàm giải tích trên $D(0, p^{\frac{1}{1-p}})$.

□

3.3 Vành các hàm giải tích

3.3.1 Các định nghĩa

- Vành các đa thức:

$$\mathbb{C}_p[z] = \{f = \sum_{i=0}^{n} a_i z^i : a_i \in \mathbb{C}_p\}$$

- Vành các chuỗi lũy thừa hình thức:

$$\mathbb{C}_p[[z]] = \{f = \sum_{n=0}^{\infty} a_n z^n : a_n \in \mathbb{C}_p\}$$

Các phép toán:
Cho

$$f = \sum_{n=0}^{\infty} a_n z^n \quad ; \quad g = \sum_{n=0}^{\infty} b_n z^n$$

  – Phép cộng:

$$f + g = \sum_{n=0}^{\infty} (a_n + b_n) z^n$$

– Phép nhân:

$$fg = \sum_{n=0}^{\infty} c_n z^n$$

trong đó

$$c_n = \sum_{i+j=n} a_i b_j$$

Ta có $\mathbb{C}_p[[z]]$ với hai phép toán cộng và nhân được định nghĩa ở trên lập thành một vành.

- Cho $r > 0$ ($r \in \mathbb{R}$), ta định nghĩa:

$$A_r(\mathbb{C}_p) = \{f = \sum_{n=0}^{\infty} a_n z^n \in \mathbb{C}_p[[z]] : |a_n|_p r^n \to 0\}$$

Ta dễ dàng kiểm tra được $A_r(\mathbb{C}_p)$ là vành con của vành $\mathbb{C}_p[[z]]$.

- Nếu $f(z) = a_0 + a_1 z + \cdots + a_n z^n + \cdots \in A_r(\mathbb{C}_p)$ thì $|a_n|_p r^n \to 0$ khi $n \to \infty$. Đặt

$$\mu(r, f) = \max_n |a_n|_p r^n \ \text{ : hạng tử tối đại của } f$$

$$\nu(r, f) = \max\{n : |a_n|_p r^n = \mu(r, f)\}$$

Ta có $\mu(r, f), \nu(r, f)$ là các hàm tăng đối với r. Thật vậy, giả sử $r_1 \leq r_2$

* $\mu(r_1, f) = |a_{n_0}|_p r_1^{n_0} \leq |a_{n_0}|_p r_2^{n_0} \leq \mu(r_2, f)$
* Giả sử $\nu(r_1, f) = n_1, \nu(r_2, f) = n_2$. Ta có

$$|a_{n_2}|_p r_2^{n_2} \geq |a_{n_1}|_p r_2^{n_1} \quad \text{và} \quad |a_{n_2}|_p r_1^{n_2} \leq |a_{n_1}|_p r_1^{n_1}$$

Suy ra

$$(r_2/r_1)^{n_2} \geq (r_2/r_1)^{n_1} \Rightarrow n_2 \geq n_1$$

3.3.2 Định lý

Cho $r > 0$, $\mu(r, -)$ là chuẩn phi Archimedean trên vành $A_r(\mathbb{C}_p)$, tức là:

1. $\mu(r, f) \geq 0$ và $\mu(r, f) = 0 \Leftrightarrow f = 0$.
2. $\mu(r, fg) = \mu(r, f).\mu(r, g)$.
3. $\mu(r, f + g) \leq \max\{\mu(r, f); \mu(r, g)\}$.

Chứng minh. 1. và 3. Hiển nhiên đúng suy ra từ định nghĩa của $\mu(r, f)$.
Ta chứng minh 2.
Lấy bất kỳ $f, g \in A_r(\mathbb{C}_p)$, khi đó

$$f = \sum_{n=0}^{\infty} a_n z^n \quad ; \quad g = \sum_{n=0}^{\infty} b_n z^n \quad ; \quad fg = \sum_{n=0}^{\infty} c_n z^n$$

trong đó

$$c_n = \sum_{i+j=n} a_i b_j \Rightarrow |c_n|_p \leq \max_{i+j=n} |a_i|_p |b_j|_p$$

Do đó

$$\mu(r, fg) = \max_n |c_n|_p r^n \leq \max_n \max_{i+j=n} \{|a_i|_p |b_j|_p r^n\}$$
$$= \max_n \max_{i+j=n} \{|a_i|_p r^i . |b_j|_p r^j\} \leq \mu(r, f).\mu(r, g)$$

Ngược lại, gọi

$$i_0 = \min\{i : |a_i|_p r^i = \mu(r, f)\} \quad ; \quad j_0 = \min\{j : |b_j|_p r^j = \mu(r, g)\}$$

Với mọi i, j ta có

$$|a_i|_p r^i \leq |a_{i_0}|_p r^{i_0} \quad ; \quad |b_j|_p r^j \leq |b_{j_0}|_p r^{j_0}$$

Nếu $i < i_0$ và $j < j_0$ thì ta có

$$|a_i|_p r^i < |a_{i_0}|_p r^{i_0} \quad ; \quad |b_j|_p r^j < |b_{j_0}|_p r^{j_0}$$

Đặt $n = i_0 + j_0$, ta có

$$|a_{i_0}|_p = r^{-i_0} \mu(r, f) \quad ; \quad |b_{j_0}|_p = r^{-j_0} \mu(r, g)$$

Suy ra

$$|a_{i_0} b_{j_0}|_p = r^{-n} \mu(r, f) \mu(r, g)$$

Nếu $(i, j) \neq (i_0, j_0)$ và $i + j = n$ thì $i < i_0$ hoặc $j < j_0$. Khi đó

$$|a_i b_j|_p < r^{-n} \mu(r, f) \mu(r, g)$$

Do đó

$$|c_n|_p = |\sum_{i+j=n} a_i b_j|_p = |a_{i_0} b_{j_0} + \sum_{i+j=n, i \neq i_0} a_i b_j|_p = |a_{i_0} b_{j_0}|_p = r^{-n} \mu(r, f) \mu(r, g)$$

Suy ra

$$\mu(r, f) \mu(r, g) = |c_n|_p r^n \leq \mu(r, fg)$$

□

3.3.3 Các tính chất

1. $A_r(\mathbb{C}_p)$ đầy đủ đối với chuẩn $\mu(r,-)$.

   Chứng minh. Lấy $\{f_i\}$ là dãy Cauchy trong $A_r(\mathbb{C}_p)$.

$$f_i = a_{0i} + a_{1i}z + \cdots + a_{ni}z^n + \cdots \in A_r(\mathbb{C}_p)$$

   Khi đó $\mu(r, f_i - f_j) \to 0$ khi $i, j \to \infty$

$$\forall \epsilon > 0, \exists N : \forall i, j \geq N : \mu(r, f_i - f_j) < \epsilon$$

$$\Leftrightarrow \max_n |a_{ni} - a_{nj}|_p r^n < \epsilon \quad ; \forall i, j \geq N$$

   Với mỗi n, ta có

$$|a_{ni} - a_{nj}|_p < \frac{\epsilon}{r^n} \quad ; \forall i, j \geq N$$

   Suy ra, với mỗi n, dãy $\{a_{ni}\}_i$ là dãy Cauchy trong $\mathbb{C}_p$. Do $\mathbb{C}_p$ là đầy đủ nên dãy $\{a_{ni}\}_i$ hội tụ trong $\mathbb{C}_p$. Do đó, với mỗi n, ta đặt

$$a_n = \lim_{i\to\infty} a_{ni}$$

$$f = a_0 + a_1 z + \cdots + a_n z^n + \cdots$$

   Ta sẽ chứng minh $f \in A_r(\mathbb{C}_p)$ và $f_i \to f$ khi $i \to \infty$. Thật vậy, ta có

$$\forall \epsilon > 0, \exists N : \max_n |a_{ni} - a_{nj}|_p r^n < \epsilon \quad ; \forall i, j \geq N$$

   Cho $j \to \infty$, ta được

$$\max_n |a_{ni} - a_n|_p r^n \leq \epsilon \quad ; \forall i \geq N$$

   Suy ra

$$\mu(r, f_i - f) = \max_n |a_{ni} - a_n|_p r^n \to 0$$

   Do đó

$$f = \lim_{i\to\infty} f_i$$

   Ta có

$$\forall \epsilon > 0, \exists N : \max_n |a_n - a_{ni}|_p r^n \leq \epsilon \quad ; \forall i \geq N$$

   Chọn $i_0 > N$, do $f_{i_0} \in A_r(\mathbb{C}_p)$ nên $\exists M : |a_{ni_0}|_p r^n < \epsilon \quad ; \forall n \geq M$.
   Khi đó, $\forall n \geq M$, ta có

$$|a_n|_p r^n = |a_n - a_{ni_0} + a_{ni_0}|_p r^n \leq \max\{|a_n - a_{ni_0}|_p r^n, |a_{ni_0}|_p r^n\} \leq \epsilon$$

   Suy ra

$$\lim_{n\to\infty} a_n r^n = 0$$

   Do đó

$$f \in A_r(\mathbb{C}_p)$$

   □

2. $\mathbb{C}_p[z]$ trù mật trong $A_r(\mathbb{C}_p)$.

Chứng minh. Lấy $f = a_0 + a_1 z + \cdots + a_n z^n + \cdots \in A_r(\mathbb{C}_p)$. Khi đó

$$f_n = a_0 + a_1 z + \cdots + a_n z^n \in \mathbb{C}_p[z]$$

Ta sẽ chứng minh $f_n \to f$ theo chuẩn $\mu(r, -)$. Thật vậy, do $f \in A_r(\mathbb{C}_p)$ nên $|a_i|_p r^i \to 0$ khi $i \to \infty$. Tức là, ta có

$$\forall \epsilon > 0, \exists N : |a_i|_p r^i < \epsilon \quad ; \forall i \geq N$$

Khi đó, $\forall n \geq N$, ta có

$$\mu(r, f - f_n) = \max_{i \geq n} |a_i|_p r^i < \epsilon$$

Do đó

$$\lim_{n \to \infty} \mu(r, f - f_n) = 0$$

□

3.4 Định lý chuẩn bị Weierstrass

3.5 Đa giác Newton

3.6 Hàm phân hình p-adic

3.7 Bài tập chương 3

1. Cho f là hàm giải tích trên $\mathbb{C}_p$, f không có không điểm trong $\mathbb{C}_p$. Chứng minh rằng f là hằng số.

Giải. Áp dụng định lý Weierstrass, ta có:

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \quad ; \quad a_n \in \mathbb{C}_p$$

là hàm giải tích trên $\mathbb{C}_p$ thì số không điểm của $f(z)$ trong hình cầu $|z|_p \leq r$ là $\nu(r, f)$. Trở lại bài toán, giả sử f là hàm giải tích trên $\mathbb{C}_p$ và f không có không điểm trong $\mathbb{C}_p$. Ta sẽ chứng minh f là hằng số, giả sử ngược lại f không là hằng số, tức là tồn tại số nguyên dương k sao cho $a_k \neq 0$. Khi đó ta luôn chọn được r sao cho $|a_k|_p r^k > |a_0|_p$. Suy ra $\nu(r, f) > 0$, nghĩa là f có không điểm trong $\mathbb{C}_p$, trái giả thiết. □

2. Cho f là hàm giải tích trên $\mathbb{C}_p$, f có hữu hạn không điểm trong $\mathbb{C}_p$. Chứng minh rằng f là đa thức.

   Giải. Giả sử f là hàm giải tích trên $\mathbb{C}_p$ và f chỉ có đúng k không điểm là $z_1, \ldots, z_k$. Ta sẽ chứng minh f là đa thức bậc k.
   Đặt $r_0 = \max\{|z_1|_p, \ldots, |z_k|_p\}$. Khi đó, theo định lý Weierstrass, ta có $\nu(r, f) = k$ với mọi $r \geq r_0$. Ta sẽ chứng minh $a_n = 0$, $\forall n > k$.
   Thật vậy, giả sử ngược lại tồn tại $n > k$ sao cho $a_n \neq 0$. Khi đó, ta luôn chọn được $r \geq r_0$ đủ lớn để $|a_n|_p r^n > |a_i|_p r^i$, $\forall i = 0, 1, \ldots, k$. Suy ra $\nu(r, f) > k$, mâu thuẫn vì $\nu(r, f) = k$.
   Hơn nữa, do f có đúng k không điểm nên $a_k \neq 0$.
   Vậy f là đa thức bậc k. □

3. Cho $f(z) = \sum a_i z^i \in \mathbb{Z}_p[[z]]$ hội tụ trong $B[0, 1]$ và có ít nhất hai hệ số a_i, a_j không chia hết cho p. Chứng minh rằng f có nghiệm trong $B[0, 1]$.

   Giải. Theo định lý Weierstrass, ta chỉ cần chứng minh $\nu(1, f) > 0$.
   Vì $a_n \in \mathbb{Z}_p$ nên $|a_n|_p \leq 1$. Theo giả thiết, ta có tồn tại $n_0 > 0$ sao cho $|a_{n_0}|_p = 1$. Do đó
   $$\mu(1, f) = \max_n\{|a_n|_p\} = 1$$
   Khi đó
   $$\nu(1, f) = \max\{n : |a_n|_p = 1\} \geq n_0 > 0$$
   □

4. Đặt $E = \{z \in \mathbb{C}_p : |z|_p < p^{\frac{1}{1-p}}\}$: là miền xác định của hàm số mũ e^z. Chứng minh rằng:

   (a) e^z là đẳng mêtric từ E đến $1 + E$.
   (b) $e^{x+y} = e^x + e^y$
   (c) $\log[(1 + x)(1 + y)] = \log(1 + x) + \log(1 + y)$
   (d) $\log(1 + z)$ là đẳng mêtric từ $1 + E$ đến E.
   (e) $\log : B(1, 1) \to \mathbb{C}_p$ là toàn ánh.
   (f) Tập hợp các không điểm của $\log(1 + z)$ là
   $$\bigcup_n (\sqrt[p^n]{1} - 1)$$

   Giải.

   (a) Chứng minh e^z là đẳng mêtric từ E vào $1 + E$

Nhận xét. Nếu $x_1, \ldots, x_{n-1} \in E$ thì $|\frac{x_1 \ldots x_{n-1}}{n!}|_p \leq 1$. Thật vậy:

$$ord_p(\frac{x_1 \ldots x_{n-1}}{n!}) > \frac{n-1}{p-1} - ord_p(n!)$$

$$= \frac{n-1}{p-1} - \frac{n-S_n}{p-1} = \frac{S_n - 1}{p-1} \geq 0$$

Suy ra, nếu $x_1, \ldots, x_n \in E$ thì $\frac{x_1 \ldots x_n}{n!} \in E$, vì :

$$|\frac{x_1 \ldots x_n}{n!}|_p = |\frac{x_1 \ldots x_{n-1}}{n!}|_p |x_n|_p \leq |x_n|_p < p^{\frac{1}{1-p}}$$

□

□

Chương 4

Lý thuyết Nevanlinna

TÀI LIỆU THAM KHẢO

[1] Neal Koblitz , *p-adic numbers, p-adic analysis, and zeta-functions*, Springer-Verlag, 1977.

[2] Chung-Chun Yang and Pei-Chu Hu , *Meromorphic functions over non-Archimedean fields*, Kluwer Academic Publishers, 2000.