BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM TP. HỒ CHÍ MINH

Bùi Minh Tâm

TRƯỜNG SỐ *P*-ADIC VÀ BỔ ĐỀ HENSEL

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thành phố Hồ Chí Minh – 2011

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM TP. HỒ CHÍ MINH

Bùi Minh Tâm

TRƯỜNG SỐ *P*-ADIC VÀ BỔ ĐỀ HENSEL

Chuyên ngành : Đại số và lý thuyết số
Mã số : 60 46 05

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS.TS. MỴ VINH QUANG

Thành phố Hồ Chí Minh – 2011

LỜI CÁM ƠN

Trong quá trình học tập tại trường Đại học Sư phạm Thành phố Hồ Chí Minh, tôi đã được Quý Thầy Cô cung cấp cho tôi những kiến thức chuyên sâu, giúp tôi trưởng thành trong học tập và nghiên cứu khoa học. Tôi xin gửi lời biết ơn đến tất cả Quý Thầy Cô đã tận tình giảng dạy tôi trong suốt thời gian học tại trường.

Tôi xin gửi lời biết ơn sâu sắc đến **PGS. TS Mỵ Vinh Quang** Thầy đã tận tình hướng dẫn tôi trong suốt thời gian thực hiện luận văn. Đặc biệt, tôi đã được học ở Thầy phương pháp làm việc khoa học và sự am hiểu thấu đáo của riêng Thầy.

Xin được phép gửi lời cám ơn đến Quý Thầy trong Hội đồng Bảo vệ Luận văn Thạc sĩ đã đọc, đóng góp ý kiến, nhận xét và đánh giá luận văn.

Tôi cũng xin được phép gửi lời cám ơn đến quý Thầy, Cô công tác tại phòng KHCN và Sau đại học của trường ĐHSP Tp. Hồ Chí Minh, Sở Giáo dục và Đào tạo Tp.Hồ Chí Minh, Ban Giám Hiệu trường THPT Lương Thế Vinh và các đồng nghiệp đã tạo nhiều điều kiện thuận lợi và giúp đỡ tôi trong quá trình học tập, thực hiện luận văn.

Cuối cùng, xin khắc sâu công ơn Cha Mẹ, cảm ơn Ông xã và hai cậu con trai yêu quí, người thân, bạn bè luôn ủng hộ, động viên và giúp đỡ tôi trong suốt khóa học.

TP.Hồ Chí Minh tháng 10 – 2011

Bùi Minh Tâm

MỤC LỤC

MỘT SỐ KÍ KIỆU

$\mathbb{N}$: : Tập số tự nhiên.

$\mathbb{Z}$: Tập số nguyên.

$\mathbb{Q}$: Tập số hữu tỉ.

$\mathbb{R}$: Tập số thực.

$\mathbb{Z}_p$: Tập các số nguyên *p*-adic.

$\mathbb{Z}_p^*$: Tập các phần tử khả nghịch trong $\mathbb{Z}_p$.

$\mathbb{Q}_p$: Trường số *p*-adic.

$|\bullet|$: Chuẩn thông thường.

$|\bullet|_p$: Chuẩn *p*-adic.

ord_p^a : Số mũ của *p* trong sự phân tích a thành thừa số nguyên tố.

$B_a(r)$: Hình cầu mở tâm a bán kính r trong $\mathbb{Q}_p$.

$\overline{B_a}(r)$: Hình cầu đóng tâm a bán kính r trong $\mathbb{Q}_p$.

$S_a(r)$: Mặt cầu tâm a bán kính r trong $\mathbb{Q}_p$.

F_p : Trường thặng dư của trường F.

■ : Kết thúc phép chứng minh.

MỞ ĐẦU

Các số *p*-adic được mô tả đầu tiên vào năm 1897 và chúng dần dần thâm nhập vào nhiều lĩnh vực khác nhau của Toán học như là Lý thuyết số, Hình học đại số, Tôpô đại số…

Vào năm 40 của những thế kỷ 20, giải tích *p*-adic phát triển mạnh mẽ và trở thành một chuyên ngành độc lập nhờ vào việc phát hiện những mối liên hệ sâu sắc của giải tích *p*-adic với những vấn đề lớn của số học và hình học đại số.

Trường các số *p*-adic $\mathbb{Q}_p$ được xem tương tự *p*-adic của trường số thực $\mathbb{R}$, tuy nhiên nó lại có khá nhiều tính chất khác với $\mathbb{R}$. Chính vì vậy, chúng tôi chọn đề tài **"Trường *p*-adic và Bổ đề Hensel"** để có thể nghiên cứu rõ hơn về trường số *p*-adic.

Mục tiêu chính của luận văn là xây dựng và nghiên cứu trường số *p*-adic.
Đặc biệt là xây dựng Bổ đề Hensel và các ứng dụng chúng để nghiên cứu các số *p*-adic. Luận văn gồm hai chương

Chương 1: Các kiến thức cơ bản

Chương này sẽ trình bày các kiến thức cơ bản về chuẩn trên một trường, các tính chất chung, khái niệm chuẩn phi *Archimede,* một số tính chất cần thiết cho chương sau.

Chương 2: Trường số *p*-adic $\mathbb{Q}_p$ và Bổ đề Hensel

Trong chương này sẽ xây dựng chi tiết trường số *p*-adic $\mathbb{Q}_p$. Nghiên cứu khảo sát các tính chất $\mathbb{Q}_p$ và so sánh nó với trường số thực $\mathbb{R}$. Đặc biệt là xây dựng Bổ đề Hensel và tìm tòi các ứng dụng của nó.

Chương 1: CÁC KIẾN THỨC CƠ BẢN

Trong chương này chúng tôi sẽ trình bày các kiến thức cơ bản về giải tích *p*-adic chẳng hạn như chuẩn trên một trường, các tính chất chung, đặc biệt là khái niệm chuẩn phi Archimede, một số tính chất cần thiết cho chương sau.

1.1 Một số định nghĩa và tính chất của chuẩn trên trường

1.1.1 Định nghĩa *Cho F là một trường. Ánh xạ* $|\bullet|: F \to \mathbb{R}$ *được gọi là một chuẩn trên F nếu thỏa các điều kiện sau*:

$i) |x| \geq 0, \forall x \in F. |x| = 0 \Leftrightarrow x = 0;$

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

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

1.1.2 Ví dụ

Trường các số hữu tỉ $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ với giá trị tuyệt đối thông thường thỏa mãn các điều kiện của định nghĩa nên trị tuyệt đối là chuẩn trên $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ và ta gọi là chuẩn giá trị tuyệt đối, kí hiệu $|\bullet|$

1.1.3 Ví dụ

Cho *F* là một trường tùy ý: Ánh xạ

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

Là một chuẩn trên trường *F* và được gọi là chuẩn tầm thường.

1.1.4 Mệnh đề (*Các tính chất của chuẩn*)

Cho $|\bullet|$ *là một chuẩn trên trường F có đơn vị* 1. $\forall x \in F$ *ta có*:

$i) |1| = |-1| = 1$

$ii) |x^n| = |x|^n, \forall n \in \mathbb{N}$

$iii) |x^{-1}| = |x|^{-1}, x \neq 0$

Chứng minh

i) Ta có $1 = |1| = |1^2| = |1|^2$ suy ra $|1| = 1$

Lập luận hoàn toàn tương tự, ta được $|-1|=1$.

ii) $|x^n|=\left|\underbrace{x.x...x}_{n\text{ - thừa số}}\right|=|x|.|x|..|x|=|x|^n$

iii) Ta có $|x|.|x^{-1}|=|x.x^{-1}|=|1|=1\Rightarrow|x^{-1}|=|x|^{-1}$.■

1.1.5 Nhận xét *Nếu F là trường hữu hạn thì trên F chỉ có duy nhất một chuẩn là chuẩn tầm thường.*

Chứng minh Xét $|\bullet|$ là một chuẩn trên trường *F*. Giả sử *F* có *q* phần tử, thế thì nhóm nhân F^* có cấp *q* – 1. Khi đó, $\forall x\in F^*$ ta có $x^{q-1}=1$, suy ra $|x^{q-1}|=|x|^{q-1}=1$ hay $|x|=1$.Vậy $|\bullet|$ là chuẩn tầm thường trên *F*. ■

1.1.6 Định nghĩa (*Hai chuẩn tương đương*)

Cho $|\bullet|_1,|\bullet|_2$ *là hai chuẩn trên trường F. Ta nói rằng hai chuẩn này tương đương nếu* $\{x_n\}$ *là dãy Cauchy theo chuẩn* $|\bullet|_1$ *khi và chỉ khi* $\{x_n\}$ *là dãy Cauchy theo chuẩn* $|\bullet|_2$

Chú ý rằng $\{x_n\}$ là dãy Cauchy theo chuẩn $|\bullet|$, nghĩa là: $|x_m-x_n|\xrightarrow{m,n\to+\infty}0$.

Hay với $\forall\varepsilon>0,\exists n_o\in\mathbb{N}:\forall n,m>n_o,|x_m-x_n|<\varepsilon$

1.1.7 Định lý (*Các điều kiện để chuẩn tương đương)*

Cho F là một trường; $|\bullet|_1,|\bullet|_2$ *là hai chuẩn trên trường F. Các điều sau là tương đương*:

1) $\forall x\in F,|x|_1<1$ *khi và chi khi* $|x|_2<1$

2) $\forall x\in F,|x|_1\le 1$ *khi và chi khi* $|x|_2\le 1$

3)Tồn tại hằng số C >0 sao cho $\forall x\in F,|x|_2=|x|_1^c$

4) *Các tôpô sinh bởi* $|\bullet|_1$ *và* $|\bullet|_2$ *là trùng nhau.*

5) $|\bullet|_1$ *tương đương với* $|\bullet|_2$ ($|\bullet|_1\sim|\bullet|_2$).

Chứng minh

$1 \Rightarrow 2)$ $\forall x \in F, |x|_1 \le 1$, ta sẽ chứng minh $|x|_2 \le 1$. Thật vậy, giả sử ngược lại $|x|_2 > 1$, khi đó $\left|\frac{1}{x}\right|_2 = \frac{1}{|x|_2} < 1$ theo (1) ta có $\frac{1}{|x|_1} < 1$ suy ra $|x|_1 > 1$ (mâu thuẩn với giả thiết) nên $|x|_2 \le 1$.

Lập luận tương tự ta cũng có $|x|_1 \le 1$ nếu $|x|_2 \le 1$

Vậy $|x|_1 \le 1$ khi và chỉ khi $|x|_2 \le 1$

$2 \Rightarrow 1)$ $\forall x \in F, |x|_1 < 1$, ta sẽ chứng minh $|x|_2 < 1$. Giả sử ngược lại $|x|_2 \ge 1$,vì $|x|_1 < 1$ nên theo (2) ta có $|x|_2 \le 1$ suy ra $|x|_2 = 1$. Khi đó $\left|\frac{1}{x}\right|_2 = \frac{1}{|x|_2} = 1$

nên theo (2) ta có $\left|\frac{1}{x}\right|_1 \le 1$ hay $|x|_1 \ge 1$ (mâu thuẩn giả thiết) do đó $|x|_2 < 1$

Tương tự ta cũng có nếu $|x|_2 < 1$ thì $|x|_1 < 1$

Vậy $|x|_1 < 1$ khi và chỉ khi $|x|_2 < 1$

$1 \Rightarrow 3)$ Ta xét hai trường hợp

Trường hợp nếu có một trong hai chuẩn là tầm thường ta sẽ chứng minh chuẩn còn lại cũng tầm thường. Giả sử $|\bullet|_1$ là tầm thường. Khi đó với $\forall x \in F^*, |x|_1 = 1$. Giả sử $|x|_2 \ne 1$, thế thì $|x|_2 > 1$ hoặc $|x|_2 < 1$

Nếu $|x|_2 < 1$ thì theo (1) ta có $|x|_1 < 1$ (mâu thuẩn giả thiết)

Ngược lại nếu $|x|_2 > 1$ thì $\left|\frac{1}{x}\right|_2 = \frac{1}{|x|_2} < 1$, suy ra $\left|\frac{1}{x}\right|_1 < 1$ do đó $|x|_1 > 1$ (mâu thuẩn)

nên $|x|_2 = 1$, tức là $|\bullet|_1 \equiv |\bullet|_2$. Hay $c = 1$.

Trường hợp nếu cả hai chuẩn đều không tầm thường.

Khi đó, $\exists x_0 \in F : |x_0|_1 > 1$ suy ra $\left|\frac{1}{x}\right|_1 < 1$ nên $\left|\frac{1}{x}\right|_2 < 1$ do đó $|x|_2 > 1$

Đặt $a=|x_0|_1, b=|x_0|_2, a>0, b>0$. Với mọi $x\in F^*$, giả sử $|x|_1=a^\alpha(\alpha=\log_a|x|)$. Ta sẽ chứng minh $|x|_2=b^\alpha$. Thật vậy, $\forall r>\alpha(r\in\mathbb{Q})$ ta có $a^r>a^\alpha$. Giả sử $r=\frac{m}{n},(m,n)=1$. Khi đó $|x_0|_1^{\frac{m}{n}}>|x|_1$ suy ra $|x_0|_1^m>|x|_1^n$ nên $\left|\frac{x^n}{x_0^m}\right|_1<1$ theo (1) ta có $\left|\frac{x^n}{x_0^m}\right|_2<1$ do đó $|x^n|_2<|x_0^m|_2$ hay $|x|_2<|x_0|_2^{\frac{m}{n}}=|x_0|_2^r=b^r$.

Chọn dãy $\{r_n\}\subset\mathbb{Q}, r_n>\alpha: r_n\to\alpha$ suy ra $|x_0|_2^{r_n}>|x|_2\Rightarrow|x_0|_2^\alpha\geq|x|_2\Leftrightarrow|x|_2\leq b^\alpha$

Tương tự ta chứng minh được $|x|_2\geq b^\alpha$. Vậy $|x|_2=b^\alpha$

Khi đó, $\forall x\in F^*, |x|_2=b^\alpha=\left(a^{\log_a b}\right)^\alpha=\left(a^\alpha\right)^{\log_a b}=|x|_1^c, c=\log_a b>0$.

$3\Rightarrow 5)$ Giả sử $\{x_n\}$ là dãy Cauchy theo chuẩn $|\bullet|_1$. Khi đó $|x_m-x_n|_1\xrightarrow{m,n\to+\infty}0$ suy ra $|x_m-x_n|_1^c\xrightarrow{m,n\to+\infty}0$

nên $|x_m-x_n|_2\xrightarrow{m,n\to+\infty}0$ hay $\{x_n\}$ là dãy Cauchy theo chuẩn $|\bullet|_2$.

$5\Rightarrow 1)$ $\forall x\in F^*, |x|_1<1$ suy ra $|x^n|_1\to 0$ nên $\{x^n\}$ là dãy Cauchy theo chuẩn $|\bullet|_1$ suy ra $\{x^n\}$ là dãy Cauchy theo chuẩn $|\bullet|_2$ nên $|x^{n+1}-x^n|_2\to 0$ suy ra $|x^n|_2|x-1|_2\to 0$, mà $|x|_1<1$ suy ra $x\neq 1$ do đó $|x-1|_2\neq 0$ hay $|x^n|_2\to 0$

Ta có $|x^n|_2<1$ (với n đủ lớn) suy ra $|x|_2<1$. Tương tự ta cũng có $|x|_2<1\Rightarrow|x|_1<1$

Vậy $|x|_1<1$ khi và chỉ khi $|x|_2<1$

$3\Rightarrow 4)$ Ta có $B_2(a,r)=\{x\in F:|x-a|_2<r\}=\{x\in F:|x-a|_1^c<r\}$

$$=\{x\in F:|x-a|_1<r^{\frac{1}{c}}\}=B_1(a,r^{\frac{1}{c}})$$

Khi đó, $\forall A\in\tau_1,\forall a\in A,\exists r>0: B_1(a,r)\subset A\Leftrightarrow\exists c>0: B_2(a,r^c)\subset A\Leftrightarrow A\in\tau_2$

Vậy $\tau_1 = \tau_2$

$4 \Rightarrow 1)$ Giả sử $x \in F, |x|_1 < 1$. Thế thì $|x^n|_1 \to 0$ suy ra $x^n \to 0$ theo τ_1,

mà $\tau_1 = \tau_2$ nên $x^n \to 0$ theo τ_2. Khi đó, $|x^n|_2 \to 0$ nên $|x|_2 < 1$

Tương tự, nếu $|x|_2 < 1$ thì $|x|_1 < 1$. ■

1.1.8 Hệ quả *Cho $|\bullet|_1, |\bullet|_2$ là hai chuẩn trên trường F. Nếu tồn tại hai số dương c_1, c_2 sao cho $|\bullet|_1 \le c_1 |\bullet|_2$ và $|\bullet|_2 \le c_2 |\bullet|_1$ thì khi đó $|\bullet|_1 = |\bullet|_2$.*

1.2 Chuẩn phi Archimede

1.2.1 Định nghĩa (*chuẩn phi Archimede*)

Cho $|\bullet|$ là một chuẩn trên trường F. Chuẩn $|\bullet|$ được gọi là chuẩn phi Archimede trên F nếu nó thỏa thêm điều kiện:

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

Chuẩn thỏa (iii) nhưng không thỏa (iii') được gọi là chuẩn Archimede.

1.2.2 Ví dụ Chuẩn tầm thường trên trường *F* là chuẩn phi *Archimede*

Thật vậy

Nếu $x + y = 0$ thì $|x+y| = 0 \Rightarrow |x+y| \le \max\{|x|, |y|\}$

Nếu $x + y \neq 0$ thì $x \neq 0$ hoặc $y \neq 0$, do đó: $|x+y| = 1 \le \max\{|x|, |y|\}$.

1.2.3 Ví dụ Nếu *F* là trường hữu hạn có q phần tử với phần tử đơn vị là e thì chuẩn trên trường *F* là phi *Archimede.*

Thật vậy

Nếu $x = 0$ thì $|x| = 0$

Nếu $x \neq 0$ thì $x^{q-1} = e$ từ đó suy ra $|x|^{q-1} = |x^{q-1}| = |e| = 1$ do đó $|x| = 1$

Vậy $|\bullet|$ là chuẩn tầm thường trên trường *F* và do đó nó là chuẩn phi *Archimede.*

1.2.4 Mệnh đề *Cho F là một trường với chuẩn phi Archimede $|\bullet|$*

i) $\forall x, y \in F, |x| \neq |y|$ *thì* $|x+y| = \max\{|x|, |y|\}$. *Nghĩa là, mọi tam giác đều cân trong không gian mêtric sinh bởi chuẩn* $|\bullet|$.

ii) Các tập

$$B_a(r) = \{x \in F : |x-a| < r\}$$
$$\overline{B}_a(r) = \{x \in F : |x-a| \leq r\}$$
$$S_a(r) = \{x \in F : |x-a| = r\}$$

là các tập vừa đóng vừa mở.

iii)Mọi điểm thuộc hình cầu đều là tâm của nó. Nghĩa là, $\forall b \in B_a(r)$, *suy ra* $B_a(r) = B_b(r)$

iv)Dãy $\{x_n\} \subset F$ *là dãy Cauchy* $\Leftrightarrow \lim_{n\to\infty} |x_{n+1} - x_n| = 0$

v)Cho $\{x_n\}$ *là dãy Cauchy. Khi đó, nếu* $x_n \to 0$ *thì* $|x_n| \to 0$ *,còn nếu* $x_n \not\to 0$ *thì* $\{x_n\}$ *là dãy dừng.Nghĩa là,* $\exists N : \forall n \geq N, |x_n| = |x_{n+1}| = |x_{n+2}| = \cdots$

Chứng minh

i) Không mất tính tổng quát, giả sử $|x| > |y|$. Khi đó,

$$|x+y| \leq \max\{|x|, |y|\} = |x| \Leftrightarrow |x+y| \leq |x| \quad (1)$$

Mặt khác, $|x| = |x+y-x| \leq \max\{|x+y|, |x|\}$ mà $|x| > |y|$ nên $\max\{|x+y|, |x|\} = |x+y|$

Do đó $|x| \leq |x+y|$ (2). Từ (1) và (2) suy ra $|x+y| = |x| = \max\{|x|, |y|\}$

ii) Rõ ràng $B_a(r)$ là tập mở. Ta chỉ còn phải chứng minh $B_a(r)$ là tập đóng,

tức $\forall x \notin B_a(r)$, ta chứng minh $\exists \varepsilon > 0, B_a(r) \cap B_x(\varepsilon) = \varnothing$.

Thật vậy, chọn $\varepsilon = \frac{r}{2}$, giả sử $\exists y \in B_a(r) \cap B_x(\frac{r}{2})$ ta suy ra

$$|y-x| < \frac{r}{2} \text{ và } |y-a| < r$$

Khi đó, $|x-a|=|x-y+y-a|\le \max\{|x-y|,|y-a|\}<r \Leftrightarrow |x-a|<r$ suy ra $x\in B_a(r)$ (mâu thuẩn) nên $B_a(r)\cap B_x(\varepsilon)=\varnothing$. Vậy $B_a(r)$ là tập đóng.

iii) $\forall b\in B_a(r)$ ta chứng minh $B_a(r)=B_b(r)$. Thật vậy,

$\forall x\in B_a(r)\Leftrightarrow |x-a|<r\Leftrightarrow |x-b+b-a|<r$ nên $\max\{|x-b|,|b-a|\}<r$

mà $|b-a|<r$ do đó $|x-b|<r$ khi và chỉ khi $x\in B_b(r)$. Vậy $B_a(r)=B_b(r)$

iv) Giả sử $\{x_n\}$ là dãy Cauchy. Khi đó, $\forall\varepsilon>0,\exists N:\forall n>N,|x_{n+1}-x_n|<\varepsilon$

suy ra $\lim_{n\to\infty}|x_{n+1}-x_n|=0$ .Ngược lại, nếu $\lim_{n\to\infty}|x_{n+1}-x_n|=0$ thì

$$\forall\varepsilon>0,\exists N:\forall n>N,|x_{n+1}-x_n|<\varepsilon$$

Với mọi $m,n>N$, giả sử rằng $m>n$ ta có

$|x_m-x_n|=|x_m-x_{m-1}+x_{m-1}-x_{m-2}+\cdots x_{n+1}-x_n|\le \max\{|x_m-x_{m-1}|,\cdots|x_{n+1}-x_n|\}<\varepsilon$

suy ra $|x_m-x_n|<\varepsilon$. Vậy $\{x_n\}$ là dãy Cauchy.

v) Nếu $x_n\to 0$ thì $|x_n-0|=|x_n|\to 0$

Nếu $x_n\not\to 0$ thì $|x_n|\not\to 0$ nên $\exists\varepsilon>0$ và dãy con $\{n_k\}$ sao cho $|x_{n_k}|<\varepsilon$. Mặt khác, $\{x_n\}$ là dãy Cauchy nên $\exists N:\forall m,n>N,|x_n-x_m|<\varepsilon$. Ta sẽ chứng minh $|x_m|=|x_{m+1}|=\cdots,\forall m>N$. Thật vậy, cố định $n_k>N$, ta có $|x_m|=|x_m-x_{n_k}+x_{n_k}|$ $=\max\{|x_m-x_{n_k}|,|x_{n_k}|\}(theo\,i)=|x_{n_k}|,\forall m>N$. Vậy $\{x_n\}$ là dãy dừng. ■

1.2.5 Định lý (*Các điều kiện tương đương của chuẩn phi Archimede*)

Cho F là một trường, $|\bullet|$ là một chuẩn trên F. Các điều sau là tương đương:

i) $|\bullet|$ *là chuẩn phi Archimede*

ii) $|2|\le 1$

iii) $|n|\le 1,\forall n\in N=\{n=n.1/\,n\in\mathbb{N},1\_$ đơn vị của F $\}$

iv) N bị chặn. Nghĩa là, $\exists c > 0 : |n| \le c, \forall n \in N$

Chứng minh

$i \Rightarrow ii)$ Ta có $|2| = |1+1| \le \max\{|1|,|1|\} = 1$ suy ra $|2| \le 1$

$ii \Rightarrow iii)$ Với mọi $n \in N$, giả sử $n = a_0 + a_1 2 + a_2 2^2 + \cdots + a_s 2^s$ với $0 \le a_i \le 1,\ 2^s \le n < 2^{s+1}$. Khi đó,

$$|n| = |a_0 + a_1 2 + a_2 2^2 + \cdots + a_s 2^s| \le |a_0| + |a_1||2| + |a_2||2^2| + \cdots + |a_s||2^s|$$
$$\le 1 + |2| + |2^2| + \cdots + |2^s| \ \le s+1 \text{ (vì } |2| \le 1)$$

Với mọi $k \in \mathbb{N}^*$, giả sử $n^k = b_0 + b_1 2 + b_2 2^2 + \cdots + b_t 2^t, 2^t \le n^k < 2^{s+1}$ thì $|n^k| \le t+1$. Ta có $n < 2^{s+1}$ suy ra $n^k < 2^{(s+1)k}$ mà $n^k \ge 2^t$ nên $2^t < 2^{(s+1)k}$ do đó $t < (s+1)k$

Khi đó $t+1 \le (s+1)k$, mặt khác $|n^k| \le t+1$ nên $|n^k| \le (s+1)k$ suy ra $|n| \le \sqrt[k]{s+1}\sqrt[k]{k}$

Vậy $|n| \le 1$ khi $k \to \infty$

$iii \Rightarrow iv)$ Hiển nhiên

$iv \Rightarrow i)$ Với mọi $n \in \mathbb{N}^*$, ta có

$$|x+y|^n = |(x+y)^n| = \left|\sum_{k=1}^{n} C_n^k x^k y^{n-k}\right| \le \sum_{k=1}^{n} |C_n^k||x^k||y^{n-k}|$$

mà N bị chặn nên có $c > 0 : |C_n^k| \le c$, do đó $|x+y|^n \le (n+1)c\left(\max\{|x|,|y|\}\right)^n$ suy ra

$|x+y| \le \sqrt[n]{(n+1)c}\left(\max\{|x|,|y|\}\right)$ nên $|x+y| \le \max\{|x|,|y|\}(n \to \infty)$.■

1.2.6 Định nghĩa *Cho p là một số nguyên tố cố định. Với mỗi* $x \in \mathbb{Q} \setminus \{0\}$*, ta luôn có*

$$x = p^{\alpha}\frac{m}{n}\begin{pmatrix} m,n \in \mathbb{Z},(m,n)=1 \\ (m,p)=1,(n,p)=1 \end{pmatrix}$$

α *gọi là p – số mũ của x, ký hiệu* $ord_p(x) = \alpha$. *Quy ước:* $ord_p(0) = \infty, \infty \pm a = \infty$.

1.2.7 Mệnh đề *Cho p là một số nguyên tố,* $\forall x, y \in \mathbb{Q}$ *ta có*

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

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

1.2.8 Mệnh đề *Cho* ρ *là một số thực thỏa* $0 < \rho < 1$ *và p là một số nguyên tố. Ánh xạ*

$$\begin{aligned} |\bullet|_\rho &: \mathbb{Q} \to \mathbb{R} \\ x &\mapsto |x|_\rho = \rho^{ord_p(x)} \end{aligned}$$

là một chuẩn phi Archimede trên $\mathbb{Q}$ *với quy ước* $\rho^\infty = 0$

Chú ý

1) $0 < \rho_1, \rho_2 < 1 \Rightarrow |\bullet|_{\rho_1} \sim |\bullet|_{\rho_2}$

Thật vậy, với mọi $x \in \mathbb{Q}$ ta có

$$|x|_{\rho_1} = \rho_1^{ord_p(x)} = \left(\rho_2^{\log_{\rho_2}\rho_1}\right)^{ord_p(x)} = \left(\rho_2^{ord_p(x)}\right)^{\log_{\rho_2}\rho_1} = |x|_{\rho_2}^{\log_{\rho_2}\rho_1}$$

Đặt $c = \log_{\rho_2}\rho_1 > 0$, ta được $|x|_{\rho_1} = |x|_{\rho_2}^c$. Vậy $|\bullet|_{\rho_1} \sim |\bullet|_{\rho_2}$.

2) Với mỗi số nguyên tố *p*, ta có chuẩn

$$|x|_p = \left(\frac{1}{p}\right)^{ord_p(x)}, \forall x \in \mathbb{Q}$$

Chuẩn $|\bullet|_p$ được gọi là chuẩn *p*-adic hay chuẩn *p*. Rõ ràng chuẩn *p* là chuẩn phi *Archimede.*

3) Cho n_o là số tự nhiên lớn hơn 1. Với mỗi $x \in \mathbb{N}$, ta luôn có

$x = a_o + a_1 n_o + \cdots + a_s n_o^s$ (*)

trong đó, $0 \leq a_i < n_o - 1$, $a_s \neq 0$. Biểu diễn (*) được gọi là biểu diễn n_o- phân của *x*. Ta dễ dàng chứng minh được $n_o^s \leq x < n_o^{s+1}$ và do đó, $s \leq \log_{n_o} x < s+1$ nên $s = \left[\log_{n_o} x\right]$.■

1.2.9 Định lý (*Ostrowski*) *Mọi chuẩn không tầm thường trên trường* $\mathbb{Q}$ *hoặc tương đương với chuẩn* $|\bullet|_p$ (*p là một số nguyên tố*) *hoặc tương đương với giá trị tuyệt đối thông thường trên* $\mathbb{Q}$.

Chứng minh Giả sử $\|\ \|$ là một chuẩn không tầm thường trên $\mathbb{Q}$. Ta xét hai trường hợp

1.Nếu $\|2\|>1$ thì $\|\ \|$ là chuẩn *Archimede*.

Lấy $n\in\mathbb{N}$, giả sử $n=a_o+a_1 2+\cdots a_r 2^r+\cdots a_s 2^s$, trong đó

$a_i\in\{0,1\}$ và $2^s\le n<2^{s+1}$ .Ta viết $\|2\|=2^\alpha$ với $\alpha=\log_2\|2\|$.Khi đó ta có

$$\begin{aligned}\|n\|&\le\|a_o\|+\|a_1\|.\|2\|+\cdots+\|a_r\|.\|2^r\|+\cdots+\|a_s\|.\|2^s\|\\&\le 1+2^\alpha+\ldots 2^{s\alpha}\\&\le 2^{s\alpha}\left(1+\frac{1}{2^\alpha}+\ldots+\frac{1}{2^{s\alpha}}\right)\\&\le 2^{s\alpha}.C(\text{vì tổng trong dấu ngoặc hội tụ})\\&\le n^\alpha.C\end{aligned}$$

Suy ra $\|n\|\le n^\alpha.C$ với $n\in\mathbb{N}$ .Nên với mọi $k\in\mathbb{N}$ ta có $\|n^k\|\le n_o^{k\alpha}.C$ suy ra $\|n\|\le n^\alpha.\sqrt[k]{C}$ .Cho $(k\to+\infty)$ ta được $\|n\|\le n^\alpha$. Mặt khác, do $2^s\le n<2^{s+1}$ nên ta có

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

Suy ra

$$\|n\|\ge\|2^{s+1}\|-\|2^{s+1}-n\|\ge 2^{(s+1)\alpha}-(2^{(s+1)}-n)^\alpha$$

Hay

$$\|n\|\ge 2^{(s+1)\alpha}\left[1-\left(1-\frac{1}{2}\right)^\alpha\right]\ge n^\alpha.C'$$

Suy ra

$\|n^k\|\ge n^{\alpha k}.C'$ dẫn đến $\|n\|\ge n^\alpha.\sqrt[k]{C'}$

Cho $(k\to+\infty)$ ta được $\|n\|\ge n^\alpha$. Vậy $\|n\|=n^\alpha$ với mọi n.

Với $x\in\mathbb{Q},\ x>0$ ta viết $x=\frac{m}{n},\ m,n\in\mathbb{N},\ n\ne 0$ thì ta có:

$$\|x\| = \frac{\|m\|}{\|n\|} = \frac{m^\alpha}{n^\alpha} = \left(\frac{m}{n}\right)^\alpha = |x|^\alpha$$

Với $x \in \mathbb{Q}, x < 0$ thì $-x > 0$ nên ta có: $\|x\| = \|-x\| = |-x|^\alpha = |x|^\alpha$

Vậy $\|x\| = |x|^\alpha$ với mọi $x \in \mathbb{Q}$.Theo điều kiện tương tương đương của chuẩn trong trường hợp 1 ta có $\| \ \| \sim |\bullet|$

2.Nếu $\|2\| \le 1$ thì $\| \ \|$ là chuẩn phi *Archimede.*

Từ giả thiết ta có $\|n\| \le 1$ với mọi $n \in \mathbb{N}$. Do $\| \ \|$ là chuẩn không tầm thường nên tồn tại $n \in \mathbb{N}$ sao cho $\|n\| < 1$. Gọi p là số tự nhiên bé nhất thoả $\|p\| < 1$. Khi đó p là số nguyên tố. Thật vậy, giả sử p là hợp số thì $p = p_1.p_2$ với p_1, p_2 là số tự nhiên và $1 < p_1, p_2 < p$. Khi đó $\|p\| = \|p_1\|\|p_2\| < 1$ nên suy ra $\|p_1\| < 1$ hoặc $\|p_2\| < 1$(điều này mâu thuẫn với cách chọn p) Gọi q là số nguyên tố khác p. Ta chứng minh $\|q\| = 1$

Giả sử $\|q\| \le 1$ vì $\left(q^k, p^k\right) = 1$ nên tồn tại $m,n \in \mathbb{Z}$ sao cho $mp^k + nq^k = 1$.

Ta có $1 = \|1\| = \|mp^k + nq^k\| \le \|m\|\|p^k\| + \|n\|\|q^k\| \le \|p^k\| + \|q^k\|$

Cho $k \to +\infty$ ta được $1 \le 0$, điều này vô lý. Vậy $\|q\| = 1$. Lấy $m \in \mathbb{N}$, giả sử $m = p^\alpha.p_1^{\alpha_1}...p_k^{\alpha_k}$

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

Với $x \in \mathbb{Q}$, $x > 0$ ta viết $x = \frac{m}{n}$, $m,n \in \mathbb{N}$, $n \ne 0$ thì ta có:

$$\|x\| = \frac{\|m\|}{\|n\|} = \frac{|m|_p^C}{|n|_p^C} = \left|\frac{m}{n}\right|_p^C = |x|_p^C$$

Với $x \in \mathbb{Q}, x < 0$ thì $-x > 0$ nên ta có: $\|x\| = \|-x\| = |-x|_p^\alpha = |x|_p^\alpha$ .Theo điều kiện tương tương đương của chuẩn trong trường hợp 2 ta có $\| \ \| \sim |\bullet|_p$.■

Chương 2: TRƯỜNG SỐ P-ADIC $\mathbb{Q}_p$ VÀ BỔ ĐỀ HENSEL

Trong chương này chúng tôi sẽ xây dựng trường số *p*-adic $\mathbb{Q}_p$ được xem như là tương tự *p*-adic của trường số thực $\mathbb{R}$. Nghiên cứu khảo sát các tính chất $\mathbb{Q}_p$, so sánh nó với trường số thực $\mathbb{R}$. Đặc biệt là xây dựng Bổ đề Hensel và tìm tòi các ứng dụng của nó.

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

Từ định lý Oxtropxki ta thấy mọi chuẩn không tầm thường trên $\mathbb{Q}$ đều tương đương với giá trị tuyệt đối thông thường $|\bullet|$ hoặc là chuẩn phi *Archimede* $|\bullet|_p$ (*p* là một số nguyên tố). Mặt khác, ta biết rằng làm đầy đủ $\mathbb{Q}$ theo $|\bullet|$ ta được trường số thực $\mathbb{R}$. Làm đầy đủ $\mathbb{Q}$ theo $|\bullet|_p$ ta sẽ được trường mới mà ta gọi là trường các số *p*-adic $\mathbb{Q}_p$ là tương tự *p*-adic của trường số thực $\mathbb{R}$**.** Cụ thể ta xây dựng như sau :

Xét $|\bullet|_p$ là chuẩn *p*-adic trên $\mathbb{Q}$; $|x|_p = \left(\frac{1}{p}\right)^{ord_p(x)}$, $\forall x \in \mathbb{Q}$. Ký hệu *S* là tập tất cả các dãy Cauchy trong $\mathbb{Q}$ theo chuẩn $|\bullet|_p$. Trên *S* xét quan hệ tương đương ~ cho như sau: $\forall \{x_n\}, \{y_n\} \subset \mathbb{Q}, \{x_n\} \sim \{y_n\} \Leftrightarrow \lim_{n\to\infty}(x_n - y_n) = 0$.

Ký hiệu $\mathbb{Q}_p = S/_{\sim} = \left\{\overline{\{x_n\}} : \{x_n\} \text{ Cauchy trong } \mathbb{Q} \text{ theo } |\bullet|_p\right\}$. Ta sẽ trang bị hai phép toán cộng và nhân cho $\mathbb{Q}_p$ để nó trở thành một trường.

Phép cộng: $\forall x = \overline{\{x_n\}}, y = \overline{\{y_n\}} \in \mathbb{Q}_p, x + y = \overline{\{x_n + y_n\}}$

Phép nhân: $\forall x = \overline{\{x_n\}}, y = \overline{\{y_n\}} \in \mathbb{Q}_p, x.y = \overline{\{x_n.y_n\}}$

Dễ dàng chứng minh được với hai phép toán cho như trên, $\mathbb{Q}_p$ là một trường với:

Phần tử không: $\bar{0} = \overline{\{x_n = 0\}}$

Phần tử đơn vị: $\bar{1} = \overline{\{x_n = 1\}}$

Phần tử đối: $x = \overline{\{x_n\}} \Rightarrow -x = \overline{\{-x_n\}}$

Phần tử nghịch đảo: Với $\overline{\{x_n\}} \neq \overline{0}$. Ta có $x_n \not\to 0$ suy ra $\exists N > 0$ sao cho $\forall n > N, |x_n|_p = a \neq 0$.

Khi đó dãy $\{y_n\}$, với $y_n = \begin{cases} 0, n \leq N \\ x_n^{-1}, n > N \end{cases}$, là một dãy Cauchy trong $\mathbb{Q}$ theo $|\ |_p$, và $\overline{\{x_n\}}.\overline{\{y_n\}} = \overline{1}$. Tức phần tử nghịch đảo của $\overline{\{x_n\}}$ là phần tử $\overline{\{y_n\}}$.

Xét $\theta : \mathbb{Q} \to \mathbb{Q}_p, \theta(x) = \overline{\{x_n = x\}}, \forall x \in \mathbb{Q}$, ta chứng minh được θ là đơn cấu trường. Do đó, ta có thể coi $\mathbb{Q} \subset \mathbb{Q}_p$.

Với mỗi $x = \overline{\{x_n\}} \in \mathbb{Q}_p$, ta định nghĩa $|x|_p = \lim_{n\to\infty} |x_n|_p$. Định nghĩa này hợp lý.

Thật vậy, đầu tiên luôn luôn tồn tại $\lim_{n\to\infty} |x_n|_p$. Vì nếu $x_n \to 0$ thì $|x_n|_p \to 0$ suy ra $|x|_p = 0$, còn nếu $x_n \not\to 0$ thì $|x_n|_p = a \neq 0, \forall n > N$ suy ra $|x_n|_p \to a \Rightarrow |x|_p = a$.

Tiếp theo $|x|_p$ không phụ thuộc vào cách chọn phần tử đại diện. Giả sử $x = \overline{\{x_n\}} = \overline{\{y_n\}}$ thế thì $x_n \sim y_n$ nên $\lim_{n\to\infty}(x_n - y_n) = 0$. Mặt khác, ta luôn có $|x_n - y_n|_p \geq \left| |x_n|_p - |y_n|_p \right|_p$ suy ra $\lim_{n\to\infty}(|x_n|_p - |y_n|_p) = 0$ hay $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |y_n|_p$.

Ta dễ dàng kiểm tra $|\bullet|_p$ định nghĩa như trên là một chuẩn trên $\mathbb{Q}_p$. Hơn nữa, mọi dãy Cauchy trong $(\mathbb{Q}, |\bullet|_p)$ đều hội tụ trong $(\mathbb{Q}_p, |\bullet|_p)$, tức $(\mathbb{Q}_p, |\bullet|_p)$ là một mở rộng của $(\mathbb{Q}, |\bullet|_p)$.

■

Nhận xét *Với mọi* $x = \overline{\{x_n\}} \in \mathbb{Q}_p$ *ta luôn có* $\lim_{x\to\infty} x_n = x$.

Chứng minh

$\forall x > 0$ do $\{x_n\}$ là dãy Cauchy nên $\exists N > 0 : \forall n, m > N, |x_m - x_n|_p < \varepsilon$. Khi đó,

$|x - x_n|_p = \lim_{i\to\infty} |x_i - x_n|_p \leq \varepsilon \Leftrightarrow |x - x_n|_p \leq \varepsilon, \forall n > N \Leftrightarrow \lim_{n\to\infty} x_n = x$.■

2.2 Khai triển p-adic của một phần tử trong $\mathbb{Q}_p$

2.2.1 Quan hệ đồng dư trong $\mathbb{Q}_p$

Với $a,b \in \mathbb{Q}_p$ *ta định nghĩa* $a \equiv b(\text{mod } p^n) \Leftrightarrow a-b \vdots p^n$

Nhận xét, với $a,b \in \mathbb{Q}_p$, $a \equiv b(\text{mod } p^n) \Leftrightarrow \left|a-b\right|_p \le p^{-n}$

Chứng minh Giả sử $a \equiv b(\text{mod } p^n) \Leftrightarrow a-b \vdots p^n$ suy ra $a-b = p^m.c \;\; m \ge n, (c,p)=1$, dẫn đến $\left|a-b\right|_p = p^{-m} \le p^{-n}$.

Ngược lại, giả sử $\left|a-b\right|_p \le p^{-n}$ suy ra $a-b = p^m.c \;\; m \ge n, (c,p)=1$, hay

$a-b \vdots p^n \Leftrightarrow a-b \vdots p^n$.■

2.2.2 Bổ đề *Nếu* $x \in \mathbb{Q}_p$ *và* $\left|x\right|_p \le 1$ *thì với mọi* $n \in \mathbb{N}$, *tồn tại* $r \in \mathbb{N}$ *sao cho* $\left|x-r\right| < p^{-n}$.

Hơn nữa, số r có thể chọn trong tập $\left\{0,1,2,...,p^n-1\right\}$.

Chứng minh Giả sử $x = \frac{a}{b} \in \mathbb{Q}, (a,b)=1$. Do $\left|x\right| \le 1$ nên $(b,p)=1$, từ đó ta thấy *b* và p^n là hai số nguyên tố cùng nhau, do đó tốn tại hai số nguyên *u, v* sao cho $bu + p^n v = 1$.

Đặt $r = a.u$, khi đó :

$$\left|x-r\right|_p = \left|\frac{a}{b} - au\right|_p = \left|\frac{a}{b}\right|_p \left|1-bu\right|_p \le \left|1-bu\right|_p \le \left|p^n v\right|_p = p^{-n}$$

Giả sử $r = p^n.q + s,\; 0 \le r \le p^n - 1$, ta có

$$\left|x-s\right|_p = \left|x-r+p^n q\right|_p \le \max\left\{\left|x-r\right|_p, \left|p^n q\right|_p\right\} \le p^{-n}$$

Do đó ta có thể chọn $r = s$ thì khi đó, $r \in \left\{0,1,...,p^n-1\right\}$ và $\left|x-r\right|_p \le p^{-n}$.■

2.2.3 Định lý *Cho* $x \in \mathbb{Q}_p, \left|x\right|_p \le 1$. *Khi đó, x có một đại diện là* $\overline{\{a_n\}}_{n=1,+\infty}$ *thỏa hai điều kiện*

i) $a_n \in \mathbb{Z}, 0 \le a_n < p^n (n = 1,2,...)$

ii) $a_n \equiv a_{n+1}(\text{mod } p^n), (n = 1,2,...)$

Chứng minh Giả sử $x = \overline{\left\{x_n\right\}}$. Vì $\left\{x_n\right\}$ là dãy côsi nên $\forall n \in \mathbb{N}, \exists N_n \in \mathbb{N} : \forall i, j > N_n$ ta có $\left|x_i - x_j\right|_p < p^{-n}$.Ta có thể chọn $\left\{N_n\right\}$ là dãy tăng.

Ta thấy $\left|x_i\right| \le 1, \forall i \ge N_1$. Thật vậy, $\forall j > N_1$ ta có $\left|x_i - x_j\right|_p < p^{-1}$. Khi đó,

$$|x_i|_p = |x_i - x_j + x_j|_p \le \max\left\{|x_i - x_j|_p, |x_j|_p\right\} \le \max\left\{p^{-1}, |x_j|_p\right\}$$

Cho $j \to +\infty$ ta được $|x_i|_p \le \max\left\{p^{-1}, 1\right\} = 1$; do đó $|x_i|_p \le 1$.

Theo bổ đề 2.2.2, $\forall n \in \mathbb{N}, \exists a_n \in \left\{0,1,...p^n - 1\right\} : |x - a_n|_p \le p^{-n}$. Ta sẽ chứng minh dãy $\{a_n\}$ thỏa định lý. Tức còn phải chứng minh $x = \overline{\{a_n\}}$ và $a_n \equiv a_{n+1} \left(\mathrm{mod}\, p^n\right)$.

Thật vậy, $|x_n - a_n|_p = |x_n - x_{N_n} + x_{N_n} - a_n|_p \le \max\left\{|x_n - x_{N_n}|_p, |x_{N_n} - a_n|_p\right\} \xrightarrow{n \to +\infty} 0$

nên $\{x_n\} \sim \{a_n\}$ hay $x = \overline{\{a_n\}}$ .Ta cũng có

$|a_n - a_{n+1}|_p = |a_n - x_{N_n} + x_{N_n} - x_{N_{n+1}} + x_{N_{n+1}} - a_{n+1}|_p \le \max\left\{|a_n - x_{N_n}|_p, |x_{N_n} - x_{N_{n+1}}|_p, |x_{N_{n+1}} - a_{n+1}|_p\right\} \le p^{-n}$

$\Leftrightarrow |a_n - a_{n+1}|_p \le p^{-n} \Leftrightarrow a_n \equiv a_{n+1} \left(\mathrm{mod}\, p^n\right)$.■

2.2.4 Khai triển *p*-adic của *x* trong $\mathbb{Q}_p$.

i) Với $x \in \mathbb{Q}_p, |x|_p \le 1$, theo định lý 2.2.3, tồn tại dãy Cauchy $\{a_n\}$ trong $\mathbb{Q}$ thỏa hai điều kiện $a_n \in \mathbb{Z}, 0 \le a_n < p^n (n = 1,2,...)$ và $a_n \equiv a_{n+1} (\mathrm{mod}\, p^n), n = 1,2,...$ để $x = \overline{\{a_n\}}$. Khi đó, với mỗi $n \in \mathbb{N}$ ta có các khai triển p – phân

$a_n = b_0' + b_1' p + \cdots b_{n-1}' p^{n-1}, \quad b_i' = \overline{0, p-1}$

$a_n = b_0 + b_1 p + \cdots b_{n-1} p^{n-1} + b_n p^n, \quad b_i = \overline{0, p-1}$

Mặt khác, $a_n \equiv a_{n+1} (\mathrm{mod}\, p^n) \Leftrightarrow a_n - a_{n+1} \vdots p^n$ nên suy ra

$b_0' + b_1' p + \cdots b_{n-1}' p^{n-1} = b_0 + b_1 p + \cdots b_{n-1} p^{n-1}$

do đó $a_n = b_0 + b_1 p + \cdots b_{n-1} p^{n-1}$ nên $x = \lim_{n \to \infty} a_n = \lim_{n \to \infty} \sum_{i=0}^{n-1} b_i p^i = \sum_{i=0}^{+\infty} b_i p^i$

Tóm lại với mọi $x \in \mathbb{Q}_p, |x|_p \le 1, \exists b_i \in \{0,1,..,p-1\} : x = \sum_{n=0}^{+\infty} b_n p^n$, gọi là khai triển p-adic của x trong $\mathbb{Z}_p$.

ii) Với x không thỏa điều kiện $|x|_p \le 1$thì ta sẽ nhân x với một số p^m thích hợp sao cho $x' = x.p^m$ thỏa mãn $|x'|_p \le 1$.Khi đó $x' = \sum_{n=0}^{+\infty} b_n p^n$ suy ra

$$x = \sum_{i=-m}^{+\infty} b_i p^i, \quad b_i \in \{0,1,..,p-1\}.$$

Công thức này gọi là khai triển *p*-adic của x trong $\mathbb{Q}_p$.

Nhận xét

i) Nếu $x = \sum_{n=0}^{+\infty} b_n p^n$ mà $b_o = b_1 = \cdots = b_{m-1} = 0, b_m \neq 0$ thì $|x|_p = p^{-m}$

ii) Nếu $x \in \mathbb{Q}_p, |x|_p = p^m (m \in \mathbb{Z})$ thì $x = \sum_{i=-m}^{+\infty} b_i p^i, \quad b_i \in \{0,1,..,p-1\}$

2.3 Vành các số nguyên p-adic $\mathbb{Z}_p$

2.3.1 Định nghĩa

$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}, \quad \mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}, \quad M_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$

2.3.2 Mệnh đề: Ta có

i) $M_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^* = p\mathbb{Z}_p$

ii) M_p *là iđêan tối đại của vành* $\mathbb{Z}_p$ *và* $\mathbb{Z}_p / p\mathbb{Z}_p$ *là trường, gọi là trường thặng dư của* $(\mathbb{Q}_p, |\bullet|_p)$

Chứng minh

i) $\forall x = pa \in p\mathbb{Z}_p, |x|_p = |pa|_p = |p|_p |a|_p \leq p^{-1} < 1 \Rightarrow x \in M_p \Rightarrow p\mathbb{Z}_p \subseteq M_p$.

Ngược lại, $\forall x \in M_p$ giả sử $|x|_p = p^m (m \in \mathbb{Z})$. Do $|x|_p < 1$ nên $m \leq -1$ suy ra $|x|_p \leq p^{-1}$.

Mặt khác, $x = pc$ trong đó, $c = \frac{x}{p}$. Ta có

$$|c|_p = \left|\frac{x}{p}\right|_p = \frac{|x|_p}{|p|_p} \leq \frac{p^{-1}}{p^{-1}} = 1 \Leftrightarrow |c|_p \leq 1 \Leftrightarrow c \in \mathbb{Z}_p$$

Từ đó suy ra $x = pc \in p\mathbb{Z}_p$ nên $M_p \subseteq p\mathbb{Z}_p$.

ii) Suy ra từ Mệnh đề 2.3.4. ■

2.3.3 Mệnh đề: $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = F_p$. *Nghĩa là, trường thặng dư của* $(\mathbb{Q}_p, |\bullet|_p)$ là $F_p = \mathbb{Z}/p\mathbb{Z}$

Chứng minh Xét tương ứng $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_p/p\mathbb{Z}_p, a + p\mathbb{Z} \mapsto a + p\mathbb{Z}_p$. Ta sẽ chứng minh f là đẳng cấu vành. Trước hết ta có f là đơn ánh. Thật vậy,

$$\forall a,b \in \mathbb{Z},\ a - b = pc \in p\mathbb{Z}\ (c \in \mathbb{Z}) \Leftrightarrow a - b = pc \in p\mathbb{Z}\ (c \in \mathbb{Z}_p).$$

Vì $c \in \mathbb{Z}$ nên $c \in \mathbb{Z}_p$. Ngược lại, $c \in \mathbb{Z}_p$. Ta có

$$c = \frac{a-b}{p} \Rightarrow |c|_p = \frac{|a-b|_p}{|p|_p} \le 1 \Rightarrow |a-b|_p \le p^{-1} \Leftrightarrow a - b \vdots p^1 \Rightarrow c \in \mathbb{Z}$$

Tiếp theo ta chứng minh f là toàn ánh:

$$\forall a + p\mathbb{Z}_p \in \mathbb{Z}_p/p\mathbb{Z}_p, \text{ vì } a \in \mathbb{Z}_p \text{ nên } a = \sum_{n=0}^{+\infty} a_n p^n = a_o + p\sum_{n=1}^{+\infty} a_n p^{n-1}$$

Suy ra

$$a - a_o = p\sum_{n=1}^{+\infty} a_n p^{n-1} \in p\mathbb{Z}_p \Rightarrow a - a_o \in p\mathbb{Z}_p \text{ hay } a + p\mathbb{Z}_p = a_o + p\mathbb{Z}_p = f(a_o + p\mathbb{Z})$$

Do đó $f(a_o + p\mathbb{Z}) = a + p\mathbb{Z}_p$

Cuối cùng, kiểm tra trực tiếp ta được f là đồng cấu vành. Do đó, f là đẳng cấu.

Vậy $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = F_p$ ■

2.3.4 Mệnh đề: $\mathbb{Z}_p$ *là vành chính và tập các iđêan của* $\mathbb{Z}_p$ *lập thành một dây chuyền. Cụ thể:* $\mathbb{Z}_p \supset p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset \cdots p^n\mathbb{Z}_p \supset \cdots$.

Chứng minh Giả sử I là một iđêan không tầm thường của $\mathbb{Z}_p$. Với mỗi $x \in I \setminus \{0\}$, do $|x|_p \le 1$ suy ra $|x|_p = p^{-m}, m \in \mathbb{N}$. Gọi a là phần tử của I sao cho $|a|_p = p^{-m}$ lớn nhất. Ta chứng minh $I = p^m\mathbb{Z}_p$.

$\forall x \in I, x = p^m \frac{x}{p^m}$, trong đó, $\left|\frac{x}{p^m}\right|_p = \frac{|x|_p}{|p^m|_p} \le \frac{p^{-m}}{p^{-m}} = 1 \Rightarrow \frac{x}{p^m} \in \mathbb{Z}_p$. Suy ra $x \in p^m\mathbb{Z}_p$, nên $I \subseteq p^m\mathbb{Z}_p$. Để chứng minh chiều ngược lại, ta lấy $x \in p^m\mathbb{Z}_p$ thì $x = p^m c (c \in \mathbb{Z}_p)$, nên $|x|_p = p^{-m}|c|_p \le p^{-m}$. Với $a \in I$ đã chọn ở trên, ta phân tích $x = a.\frac{x}{a}$, ta có $\left|\frac{x}{a}\right|_p = \frac{|x|_p}{|a|_p} = \frac{|x|_p}{p^{-m}}$

. Do vậy, $\left|\frac{x}{a}\right|_p \le \frac{p^{-m}}{p^{-m}} = 1$ hay $\frac{x}{a} \in \mathbb{Z}_p$ và $x = a.\frac{x}{a} \in I$ .Vậy, $p^m\mathbb{Z}_p \subseteq I$.

Từ đó ta có iđêan *I* của $\mathbb{Z}_p$ được sinh bởi phần tử p^m và do đó $\mathbb{Z}_p$ là vành chính và tập các iđêan của $\mathbb{Z}_p$ lập thành một dây chuyền. Cụ thể:

$\mathbb{Z}_p \supset p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset \cdots p^n\mathbb{Z}_p \supset \cdots$ ■

2.3.5 Mệnh đề

$\mathbb{Z}_p$ là tập compact, do đó $\mathbb{Q}_p$ là tập compact địa phương.

Chứng minh Trước hết ta chứng minh $\mathbb{Z}_p$ là tập compact.

Giả sử $\{x_n\}$ là một dãy tùy ý trong $\mathbb{Z}_p$ và

$$x_1 = a_{01} + a_{11}p + a_{21}p^2 + \ldots$$
$$x_2 = a_{02} + a_{12}p + a_{22}p^2 + \ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x_n = a_{0n} + a_{1n}p + a_{2n}p^2 + \ldots$$

Trong đó $0 \le a_{in} \le p-1$ với mọi $i = 0,1,2,\ldots$

Xét các phần tử $a_{0n}\left(n = 1,2,3,\ldots,p-1\right)$ ta thấy các phần tử này nhận các giá trị trong tập hữu hạn $\{0,1,2,\ldots,p-1\}$.

Do đó tồn tại $b_0 \in \{0,1,2,\ldots,p-1\}$ được các phần tử $a_{0n}\left(n = 1,2,3,\ldots,p-1\right)$ nhận giá trị vô hạn lần.

Tồn tại tập K_0 vô hạn các phần tử x_{0n} của dãy $\{x_n\}$ sao cho số hạng đầu tiên trong khai triển *p*-adic của mỗi phần tử đều bằng b_0.

Trong tập K_0 các phần tử x_{0n} có số hạng thứ 2 trong khai triển p-adic là a_{1n} với $n = 0,1,2,...,(p-1)$ nhận các giá trị trong tập hữu hạn $\{0,1,2,...,p-1\}$.

Vậy phải tồn tại $b_1 \in \{0,1,2,...,p-1\}$ được nhận giá trị vô hạn lần.

Do đó tồn tại tập K_1 vô hạn các phần tử x_{1n} của dãy $\{x_{0n}\}$ sao cho số hạng thứ 2 trong khai triển *p*-adic của các phần tử đó bằng nhau và bằng b_1.

Như vậy, với mỗi $m \in \mathbb{N}$ tồn tại tập K_m vô hạn các phần tử x_{mn} của tập K_{m-1} sao cho số hạng thứ m trong khai triển p-adic của các phần tử đó bằng nhau và bằng $b_m \in \{0,1,2,...,p-1\}$. Đặt $b = b_0 + b_1 p + b_2 p^2 + ... + b_m p^m + b_{m+1} p^{m+1} + ...$

Như vậy ta đã xây dựng được $K_0 \supset K_1 \supset ... \supset K_m \supset ...$

Với các phần tử $x_{0n} \in K_0$, $x_{1n} \in K_1, ..., x_{mn} \in K_m, ...$

Từ cách xây dựng trên ta có : $|x_{mn} - b|_p < p^{-m-1} \xrightarrow{m \to \infty} 0$

Do đó $\{x_{mn}\}$ là một dãy con lấy ra từ dãy $\{x_n\}$ mà $\{x_{mn}\}$ hội tụ về b.

Vậy $\mathbb{Z}_p$ là tập compact.

Bây giờ ta lấy phần tử $x_0 \in \mathbb{Q}_p$.

Nếu $x_0 = 0$ thì tồn tại $\mathbb{Z}_p = B[0,1]$ là tập compact chứa x_0.

Nếu $x_0 \neq 0$ ta có ánh xạ $\mathbb{Z}_p \to x_0 + \mathbb{Z}_p$ là phép đồng phôi

$$x \mapsto x_0 + x$$

nên $x_0 + \mathbb{Z}_p$ là tập compact chứa x_0. Do đó với mọi $x_0 \in \mathbb{Q}_p$ đều tồn tại lân cận compact chứa x_0 nên $\mathbb{Q}_p$ compact địa phương. ■

2.3.6 Mệnh đề (*một số tính chất tôpô khác của* $\mathbb{Q}_p$)

i) Mọi hình cầu, mặt cầu trong $\mathbb{Q}_p$ *đều là những tập vừa mở vừa đóng.*

ii) Hai hình cầu bất kỳ trong $\mathbb{Q}_p$ *hoặc lồng nhau hoặc rời nhau.*

iii) Mọi hình cầu, mặt cầu trong $\mathbb{Q}_p$ *đều có vô số tâm. Mọi hình cầu đều có vô số bán kính.*

iv) $\mathbb{Q}_p$ *chỉ có một số đếm được các hình cầu và mặt cầu.*

Chứng minh

i) Giả sử $a \in \mathbb{Q}_p$, $r \in \mathbb{R}^+$, xét hình cầu mở: $B(a,r) = \left\{ x \in \mathbb{Q}_p : |x-a|_p < r \right\}$

Hiển nhiên $B(a,r)$ là tập mở. Ta cần chứng minh $B(a,r)$ là tập đóng, nghĩa là cần chứng minh $B(a,r) \setminus \mathbb{Q}_p$ là tập mở. Thật vậy, nếu lấy bất kỳ $b \in B(a,r) \setminus \mathbb{Q}_p$, suy ra $|b-a|_p \geq r$. Khi đó, luôn tồn tại hình cầu mở $S(b,r)$ nằm hoàn toàn trong $B(a,r) \setminus \mathbb{Q}_p$ vì với mọi $y \in S(b,r)$, suy ra $|y-b|_p < b$.

Mặt khác, ta có $|y-a|_p = |(y-b)+(b-a)|_p$.

Theo nguyên lý tam giác cân, ta phải có:

Do đó, $|y-a|_p \geq r$. Suy ra, $S(b,r) \subset B(a,r) \setminus \mathbb{Q}_p$.

Vậy $B(a,r) \setminus \mathbb{Q}_p$ là tập mở.

Tương tự, ta cũng có $B[a,r] = \left\{ x \in \mathbb{Q}_p : |x-a|_p \leq r \right\}$, $D(a,r) = \left\{ x \in \mathbb{Q}_p : |x-a|_p = r \right\}$ cũng là những tập vừa mở vừa đóng.

ii) Ta xét hai hình cầu mở $B_1(a,r)$ và $B_2(b,s)$. Giả sử $B_1(a,r)\cap B_2(b,s)\neq\varnothing$, ta chứng minh chúng phải lồng nhau.

Thật vậy, không mất tính tổng quát ta có thể giả sử r < s. Sau đây chúng ta sẽ chứng minh $B_1(a,r)\subset B_2(b,s)$. Từ giả thiết $B_1(a,r)\cap B_2(b,s)\neq\varnothing$, suy ra tồn tại $c\in B_1(a,r)\cap B_2(b,s)\neq\varnothing$ hay $|c-a|_p<r$ và $|c-b|_p<s$.

Bây giờ, $\forall y\in B_1(a,r)$ ta có $|y-a|_p<r$

Do đó,

$$|y-b|_p=|(y-a)+(a-c)+(c-b)|_p\le\max\left\{|y-a|_p,|a-c|_p,|c-b|_p\right\}<s$$

Suy ra $y\in B_2(b,s)$ .Vậy $B_1(a,r)\subset B_2(b,s)$.

Ngược lại, nếu $s\le r$ thì bằng cách chứng minh tương tự như trên, ta cũng có $B_1(a,r)\supset B_2(b,s)$

Đối với hình cầu đóng, ta chứng minh hoàn toàn tương tự.

iii) Ta chứng minh mọi hình cầu, mặt cầu trong $\mathbb{Q}_p$ đều có vô số tâm.

Thật vậy, với $a\in\mathbb{Q}_p$, $r\in\mathbb{R}^+$, ta xét một điểm b bất kỳ, $b\neq a$ trong hình cầu mở

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

Ta có, $|b-a|_p<r$ (do cách chọn b).

Hơn thế nữa, ta còn có $B(a,r)=B(b,r)$ vì nếu $x\in B(a,r)$ thì $|x-a|_p<r$.

Khi đó, $|x-b|_p=|(x-a)+(a-b)|_p\le\max\left\{|x-a|_p,|a-b|_p\right\}<r$

Suy ra, $x\in B(b,r)$ hay $B(a,r)\subset B(b,r)$.

Ngược lại, chứng minh tương tự trên ta cũng có $B(b,r)\subset B(a,r)$.

Vậy $B(a,r)=B(b,r)$ với mọi $b\in B(a,r)$. Nói cách khác, $B(b,r)$ có vô số tâm. Chứng minh tương tự ta cũng có $B[a,r]$ và $D(a,r)$ có vô số tâm.

Ta chứng minh mọi hình cầu trong $\mathbb{Q}_p$ đều có vô số bán kính.

Trước tiên ta xét hình cầu mở $B(a,r)$. Ta đã biết hàm chuẩn $|.|_p$ chỉ lấy giá trị trong tập $\{p^n \mid n\in\mathbb{Z}\}\cup\{0\}$ nên tồn tại $n\in\mathbb{Z}$ sao cho $p^n<r\le p^{n+1}$.

Ta chứng minh rằng $B(a,s)=B(a,p^{n+1})$ với mọi s thỏa $p^n<s\le p^{n+1}$.

Thật vậy, $\forall x\in B(a,s)$, ta có $|x-a|_p<s\le p^{n+1}\Rightarrow x\in B(a,p^{n+1})$.

Ngược lại, $\forall y\in B(a,p^{n+1})$ ta có $|y-a|_p<p^{n+1}\Rightarrow |y-a|_p\le p^n<s$ hay $y\in B(a,s)$. Nên $B(a,s)=B(a,p^{n+1})$.

Như vậy, với bất kỳ hình cầu $B(a,r)$ với r thỏa $p^n<r\le p^{n+1}$ ta đều có $B(a,r)=B(a,p^{n+1})$. Do đó, $B(a,r)=B(a,s)$ với mọi s thỏa $p^n<s\le p^{n+1}$. Điều này có nghĩa là mọi hình cầu mở $B(a,r)$ đều có vô số bán kính.

Đối với hình cầu đóng $B[a,r]$ luôn tồn tại n sao cho $p^n\le r<p^{n+1}$. Ta sẽ chứng minh $B[a,s]=B[a,p^n]$ với mọi s thỏa $p^n\le s<p^{n+1}$. Thật vậy, với mọi $x\in B[a,s]$ ta có $|x-a|_p\le s$ mà $p^n\le s<p^{n+1}$ nên $|x-a|_p\le p^n$.

Vậy $x\in B[a,p^n]$.

Ngược lại, với mọi $y\in B[a,p^n]$ ta có $|y-a|_p\le p^n\le s$, suy ra $y\in B[a,s]$. Do đó, $B[a,s]=B[a,p^n]$. Với $p^n\le r<p^{n+1}$, ta có $B[a,r]=B[a,s]$.

Vậy hình cầu đóng $B[a,r]$ có vô số bán kính.

iv) $\mathbb{Q}_p$ chỉ có một số đếm được các hình cầu và mặt cầu.

Theo *iii)* ta có mọi điểm trong hình cầu, mặt cầu đều là tâm của nó. Dùng tính chất này ta sẽ chứng minh $\mathbb{Q}_p$ chỉ có một số đếm được các hình cầu và mặt cầu.

Thật vậy, lấy bất kỳ $a \in \mathbb{Q}_p, r \in \mathbb{R}^+$. Theo *iii)* tồn tại $n \in \mathbb{Z}$ sao cho $B(a,r) = B(a,p^n)$

Vậy $M = \{B(a,r) | r \in \mathbb{R}^+\} = \{B(a,p^n) | n \in \mathbb{Z}\}$ là tập đếm được. Mặt khác mọi hình cầu trong $\mathbb{Q}_p$ đều có thể chọn tâm là một số hữu tỉ. Chẳng hạn, đối với hình cầu mở $B(a,p^n)$. Do $a \in \mathbb{Q}_p$ nên ta giả sử khai triển p-adic của a có dạng

$$a = a_m p^m + a_{m+1} p^{m+1} + ... + a_n p^n + ... \quad (n < m, m \in \mathbb{Z}).$$

Đặt $b = a_m p^m + a_{m+1} p^{m+1} + ... + a_n p^n$. Suy ra $b \in \mathbb{Q}_p$ và $|b-a|_p < \frac{1}{p^n}$

nên $b \in B(a,p^n)$. Do đó $B(a,p^n) = B(b,p^n)$.

Vậy mọi hình cầu trong $\mathbb{Q}_p$ đều có dạng $B(b,p^n)$ trong đó $b \in \mathbb{Q}$ và $n \in \mathbb{Z}$, do đó số hình cầu trong $\mathbb{Q}_p$ là tập đếm được.

Tương tự, ta cũng chứng minh được mọi hình cầu đóng, mặt cầu trong $\mathbb{Q}_p$ cũng là những tập đếm được. ■

2.4 Bổ đề Hensel

Như chúng ta đã biết các phép toán số học như: cộng, trừ, nhân và chia trong $\mathbb{Q}_p$ được thực hiện một cách khá dễ. Tuy nhiên, việc khai căn của một số nguyên và việc tìm nghiệm của một phương trình nào đó trong $\mathbb{Q}_p$ nói chung là vấn đề không phải lúc nào chúng ta cũng thực hiện được. Bổ đề Hensel sẽ giúp chúng ta giải quyết một phần nào của vấn đề trên. Đặc biệt là Bổ đề Hensel giúp chúng ta mô tả các căn của 1 trong $\mathbb{Q}_p$ hay các tự đẳng cấu trong trường $\mathbb{Q}_p$.

2.4.1 Bổ đề Hensel *Cho đa thức* $f(x) = c_0 + c_1 x + ... + c_n x^n \in \mathbb{Z}_p[x],\ c_n \neq 0$ *và* $f'(x) = c_1 + 2c_2 x + ... + nc_n x^{n-1}$ *là đạo hàm của nó. Nếu tồn tại phần tử* $a_0 \in \mathbb{Z}_p$ *thỏa điều kiện:*

$f\left(a_0\right) \equiv 0\left(\mathrm{mod}\, p\right)$ và $f^{'}\left(a_0\right) \not\equiv 0\left(\mathrm{mod}\, p\right)$ thì tồn tại duy nhất $a \in \mathbb{Z}_p$ sao cho $f\left(a\right) = 0$ và $a \equiv a_0\left(\mathrm{mod}\, p\right)$.

Để chứng minh bổ đề Hensel ta cần chứng minh bổ đề sau :

Bổ đề *Cho $a_0 \in \mathbb{Z}_p$, tồn tại duy nhất dãy số tự nhiên $a_1, a_2, \ldots, a_n, \ldots$ thỏa 3 điều kiện*

i) $a_{n+1} \equiv a_n\left(\mathrm{mod}\, p^{n+1}\right), \forall n \in \mathbb{N}^*$;

ii) $0 \le a_n < p^{n+1}, \forall n \in \mathbb{N}$;

iii) $f\left(a_n\right) \equiv 0\left(\mathrm{mod}\, p^{n+1}\right), \ \forall n \in \mathbb{N}^*$.

Chứng minh Ta xây dựng $a_1, a_2, \ldots, a_n, \ldots$ bằng quy nạp.

Gọi $\tilde{a}_0$ là số tự nhiên duy nhất thỏa $0 \le \tilde{a}_0 \le p-1$ mà $a_0 \equiv \tilde{a}_0\left(\mathrm{mod}\, p\right)$ ($\tilde{a}_0$ là chữ số đầu tiên trong khai triển *p*-aidc của a_0.

Giả sử đã có a_1, do a_1 thỏa *i), ii)* nên có thể chọn $a_1 = \tilde{a}_0 + pb$ với $0 \le b \le p-1$ ta chỉ còn phải chọn b phù hợp. Ta có:

$$f\left(a_1\right) = \sum_{i=0}^{n} c_i\left(\tilde{a}_0 + pb\right)^i = \sum_{i=1}^{n}\left(c_i \tilde{a}_0{}^i + ic_i p.b.\tilde{a}_0{}^{i-1} + bội\ của\ p^2\right), \text{suy ra}$$

$$f\left(a_1\right) = f\left(\tilde{a}_0\right) + p.b.f^{'}\left(\tilde{a}_0\right)\left(\mathrm{mod}\, p^2\right)$$

Vì $f\left(\tilde{a}_0\right) \equiv f\left(a_0\right) \equiv 0\left(\mathrm{mod}\, p\right)$ nên $f\left(\tilde{a}_0\right) \equiv 0\left(\mathrm{mod}\, p\right)$, hay $f\left(\tilde{a}_0\right) = p.A; A \in \mathbb{Z}_P$.

Do đó

$$f\left(a_1\right) \equiv p.A + b.p.f'\left(\tilde{a}_0\right)\left(\mathrm{mod}\, p^2\right)$$

Đến đây ta cần tìm *b* sao cho $p.A + b.p.f'\left(\tilde{a}_0\right) \equiv 0\left(\mathrm{mod}\, p^2\right)$.Tức

$$A + b.f'\left(\tilde{a}_0\right) \equiv 0\left(\mathrm{mod}\, p\right)$$

Ta có $f'\left(\tilde{a}_0\right) \not\equiv 0\left(\mathrm{mod}\, p\right)$ nên suy ra $b \equiv \dfrac{-A}{f'\left(\tilde{a}_0\right)}\left(\mathrm{mod}\, p\right)$

Suy ra *b* được chọn duy nhất, là chữ số đầu tiên trong khai triển *p*-adic số $\dfrac{-A}{f'\left(\tilde{a}_0\right)}$. Đến đây ta đã xây dựng được a_1.

Giả sử ta đã có duy nhất dãy số tự nhiên $a_1, a_2, \ldots, a_n$ thỏa *i), ii), iii).* Ta sẽ xây dựng

a_{n+1}

Nếu đã có a_{n+1} thì vì $a_{n+1} \equiv a_n \left(\mathrm{mod}\, p^{n+1}\right)$ nên ta có thể chọn b sao cho

$a_{n+1} = a_n + b.p^{n+1}$ *và* $0 \le a_{n+1} < p^{n+2}$ *nên* $0 \le b \le p-1$

Như vậy với a_{n+1} trên đã thỏa *i), ii).* Ta chỉ cần tìm b thỏa *iii).* Ta có:

$$f\left(a_{n+1}\right) = \sum_{i=0}^{n} c_i \left(a_n + b.p^{n+1}\right)^i = \sum_{i=0}^{n} \left(c_i a_n^i + i.c_i b.p^{n+1}.a_n^{i-1} + bội\ của\ p^{n+2}\right)$$

suy ra

$$f\left(a_{n+1}\right) \equiv f\left(a_n\right) + bp^{n+1}.f'\left(a_n\right)\left(\mathrm{mod}\, p^{n+2}\right).$$

Vì a_n thỏa *iii)* nên $f\left(a_n\right) \equiv 0\left(\mathrm{mod}\, p^{n+1}\right) \Rightarrow f\left(a_n\right) = p^{n+1}.A';\ A' \in \mathbb{Z}_p$

Do đó

$$f\left(a_{n+1}\right) \equiv p^{n+1}.A' + b.p^{n+1}.f'\left(a_n\right)\left(\mathrm{mod}\, p^{n+2}\right)$$

Cần chọn b để $p^{n+1}.A' + bp^{n+1}.f'\left(a_n\right) \equiv 0\left(\mathrm{mod}\, p^{n+2}\right)$ hay $A' + bf'\left(a_n\right) \equiv 0\left(\mathrm{mod}\, p\right)$

Do $a_n \equiv a_0\left(\mathrm{mod}\, p\right)$ nên $f'\left(a_n\right) \equiv f'\left(a_0\right)\left(\mathrm{mod}\, p\right)$ mà $f'\left(a_0\right) \not\equiv 0\left(\mathrm{mod}\, p\right)$. Vì vậy, $f'\left(a_n\right) \not\equiv 0\left(\mathrm{mod}\, p\right)$. Từ đó suy ra $b \equiv \dfrac{-A}{f'\left(a_n\right)}\left(\mathrm{mod}\, p\right)$.

Vậy b là duy nhất và là chữ số đầu tiên trong khai triển *p*-adic của $\dfrac{-A}{f'\left(a_n\right)} \in \mathbb{Z}_p$

Như vậy bằng quy nạp ta đã xây dựng được duy nhất dãy số tự nhiên $a_1, \ldots, a_n$ thỏa bổ đề.
Để chứng minh Bổ đề Hensel ta cần chứng minh các điều sau:

1. Sự tồn tại: Với $a_0 \in \mathbb{Z}_p$, theo bổ đề trên tồn tại duy nhất một dãy số tự nhiên a_1, $a_2,\ldots, a_n$ thỏa điều kiện :

i) $a_{n+1} \equiv a_n \left(\mathrm{mod}\, p^{n+1}\right), \forall n \in \mathbb{N}$

ii) $0 \le a_n < p, \forall n \in \mathbb{N}$

iii) $f\left(a_n\right) \equiv 0\left(\mathrm{mod}\, p^{n+1}\right),\ \forall n \in \mathbb{N}^*$

Do *i),* nên $\left|a_{n+1} - a_n\right|_p \le p^{-n-1}$ suy ra dãy $\left\{a_n\right\}$ là dãy Cauchy trong $\mathbb{Q}$.

Đặt $a = \overline{\left\{a_n\right\}} \in \mathbb{Z}_p$, ta có:

$$\begin{cases} a_1 \equiv a_0 \left(\mathrm{mod}\, p\right) \\ a_2 \equiv a_1 \left(\mathrm{mod}\, p^2\right) \\ \vdots \\ a_n \equiv a_{n-1} \left(\mathrm{mod}\, p^n\right), \forall n \in \mathbb{N} \end{cases}$$

suy ra $a_n \equiv a_{n-1} \equiv ... \equiv a_0 \left(\mathrm{mod}\, p\right),\ \forall n \in \mathbb{N}$. Từ đó, ta được

$$\left|a - a_0\right|_p = \lim_{n\to\infty} \left|a_n - a_0\right|_p \le p^{-1} \Rightarrow \left|a - a_0\right|_p \le p^{-1} \Rightarrow a \equiv a_0 \left(\mathrm{mod}\, p\right) \quad (1)$$

Mặt khác: $a_{n+1} \equiv a_n \left(\mathrm{mod}\, p^{n+1}\right),\ \forall n \in \mathbb{N}$ nên ta có:

$$a_m \equiv a_n \left(\mathrm{mod}\, p^{n+1}\right),\ \forall m,n \in \mathbb{N} : m > n$$

$$\Rightarrow \left|a_m - a_n\right|_p \le p^{-n-1} \Rightarrow \left|a - a_n\right|_p = \lim_{m\to\infty} \left|a_m - a_n\right|_p \le p^{-n-1}$$

$$\Rightarrow \left|a - a_n\right|_p \le p^{-n-1} \Rightarrow a \equiv a_n \left(\mathrm{mod}\, p^{n+1}\right) \Rightarrow f\left(a\right) \equiv f\left(a_n\right) \left(\mathrm{mod}\, p^{n+1}\right)$$

Mà $f\left(a_n\right) \equiv 0 \left(\mathrm{mod}\, p^{n+1}\right)$ nên $f\left(a\right) \equiv 0 \left(\mathrm{mod}\, p^{n+1}\right)$ dẫn đến $\left|f\left(a\right)\right|_p \le p^{-n-1}, \forall n \in \mathbb{N}$ suy ra $\left|f\left(a\right)\right|_p \xrightarrow{n\to\infty} 0$. Do vậy, $f\left(a\right) = 0$ (2)

2. Tính duy nhất: Giả sử có $a' \in \mathbb{Z}_p$ thỏa điều kiện $a' \equiv a_0 \left(\mathrm{mod}\, p\right)$ và $f\left(a'\right) = 0$. Do $a' \in \mathbb{Z}_p$, ta có $a' = b_0 + b_1 p + b_2 p + ... + b_n p^n + ...$

Đặt $a_0{}' = b_0;\ a_1{}' = b_0 + b_1 p;\ ... a_n{}' = b_0 + b_1 p + ... + b_n p^n$. Khi đó $\left\{a_n{}'\right\}$ thỏa *i), ii)* của bổ đề trên . Hơn nữa: $a_n{}' \equiv a' \left(\mathrm{mod}\, p^{n+1}\right)$ suy ra $f\left(a_n{}'\right) \equiv f\left(a'\right) \left(\mathrm{mod}\, p^{n+1}\right)$, ta lại có $f\left(a'\right) \equiv 0 \left(\mathrm{mod}\, p^{n+1}\right)$ nên $f\left(a_n{}'\right) \equiv 0 \left(\mathrm{mod}\, p^{n+1}\right)$. Tức dãy $\left\{a_n{}'\right\}$ thỏa điều kiện *iii)* của bổ đề, nói cách khác dãy $\left\{a_n{}'\right\}$ thỏa bổ đề, do đó $\left\{a'\right\} \equiv \left\{a_n\right\}$ hay $a \equiv a'$.■

2.4.2 Ví dụ *Trong $\mathbb{Q}_7$ luôn tồn tại căn bậc 2 của -3.*

Thật vậy, xét $f\left(x\right) = x^2 + 3$, ta chứng minh *f(x)* có nghiệm trong $\mathbb{Q}_7$

Với $a_0 = 2 \in \mathbb{Z}_7$, ta có $f\left(a_0\right) = 7 \equiv 0 \left(\mathrm{mod}\, 7\right)$ và $f'\left(a_0\right) = 2a_0 = 2.2 = 4 \not\equiv 0 \left(\mathrm{mod}\, 7\right)$

Theo Bổ đề Hensel tồn tại duy nhất $x_0 \in \mathbb{Z}_7$ sao cho $x_0 \equiv 2 \left(\mathrm{mod}\, 7\right)$ và $f\left(x_0\right) = 0$ hay $x_0^2 = -3$.

2.4.3 Ví dụ *Trong* $\mathbb{Q}_2$ *luôn tồn tại căn bậc 2 của 9.*

Thật vậy, dễ dàng nhận thấy tồn tại $3 \in \mathbb{Z}_2 : 3^2 = 9$

Tuy nhiên, ta không thể áp dụng Bổ đề Hensel để chứng minh $\mathbb{Q}_2$ luôn tồn tại căn bậc 2 của 9.

Vì với $f\left(x\right) = x^2 - 9;\ f^{'}\left(x\right) = 2x$. Ta luôn có $f^{'}\left(x_0\right) = 2x_0 \equiv 0\left(\mathrm{mod}\, 2\right), \forall x_0 \in \mathbb{Z}_2$.

Để giải quyết mâu thuẫn của bài toán trên ta cần chứng minh Bổ đề Hensel mở rộng sau.

2.4.4 Bổ đề Hensel mở rộng

Cho $f(x) = c_0 + c_1 x + ... + c_n x^n \in \mathbb{Z}_p\left[x\right]$

Nếu tồn tại phần tử $a_0 \in \mathbb{Z}_p$ *thỏa điều kiện* $\begin{cases} f^{'}\left(a_0\right) \equiv 0\left(mod p^M\right) \\ f^{'}\left(a_0\right) \not\equiv 0\left(\mathrm{mod}\, p^{M+1}\right) \\ f\left(a_0\right) \equiv 0\left(\mathrm{mod}\, p^{2M+1}\right) \end{cases}$

Khi đó, tồn tại duy nhất một số $a \in \mathbb{Z}_p$ *sao cho:* $f\left(a\right) = 0$ *và* $a \equiv a_0\left(\mathrm{mod}\, p^{M+1}\right)$

Để chứng minh bổ để hensel mở rộng ta cần chứng minh bổ đề sau đây :

Bổ đề: *Cho* $a_0 \in \mathbb{Z}_p$ *tồn tại duy nhất dãy số tự nhiên* $a_1, a_2, \ldots, a_{n..}$ *thỏa 3 điều kiện*

i) $a_n = a_{n-1}\left(\mathrm{mod}\, p^{M+n}\right)$;

ii) $0 \le a_n < p^{M+n+1}$;

iii) $f\left(a_n\right) \equiv 0\left(\mathrm{mod}\, p^{2M+n+1}\right)$.

Chứng minh bổ đề

Ta xây dựng dãy số $a_1, a_2, \ldots, a_n$ bằng quy nạp

Gọi $\tilde{a}_0$ là số tự nhiên duy nhất thỏa $0 \le \tilde{a}_0 < p$ mà $a_0 \equiv \tilde{a}_0\left(\mathrm{mod}\, p^{M+1}\right)$(*)

Do $a_0 \in \mathbb{Z}_p$ nên $a_0 = b_0 + b_1 p + b_2 p^2 + ... + b_M p^M + b_{M+1} p^{M+1} + ...$

Chọn $\tilde{a}_0 = b_0 + b_1 p + b_2 p^2 + ... + b_M p^M$

Suy ra $\tilde{a}_0$ duy nhất và thỏa điều kiện (*)

Giả sử đã có a_1, a_1 thỏa *i), ii)* nên có thể chọn: $a_1 = \tilde{a}_0 + b.p^{M+1}$ với $0 \le b < p - 1$

Ta chứng minh có duy nhất *b* thỏa điều kiện $f\left(a_1\right) \equiv 0\left(\mathrm{mod}\, p^{2M+2}\right)$

Thật vậy, ta có $f\left(a_1\right)=\sum_{i=0}^{n} c_i\left(\tilde{a}_0+bp^{M+1}\right)^i=\sum_{i=0}^{n}(c_i\tilde{a}_0{}^i+c_i.i\tilde{a}_0{}^{i-1}.bp^{M+1}+bội\ của\ p^{2M+2})$,

suy ra

$$f\left(a_1\right)\equiv f\left(\tilde{a}_0\right)+b.p^{M+1}.f'\left(\tilde{a}_0\right)\left(\mathrm{mod}\, p^{2M+2}\right).$$

Do $a_0\equiv\tilde{a}_0\left(\mathrm{mod}\, p^{M+1}\right)$ nên $f'\left(a_0\right)\equiv f'\left(\tilde{a}_0\right)\left(\mathrm{mod}\, p^{M+1}\right)$ mà $f'\left(a_0\right)\equiv 0\left(\mathrm{mod}\, p^{M}\right)$ và $f'\left(a_0\right)\not\equiv 0\left(\mathrm{mod}\, p^{M+1}\right)$, vì vậy $f'\left(\tilde{a}_0\right)\equiv 0\left(\mathrm{mod}\, p^{M}\right)$ *và* $f'\left(\tilde{a}_0\right)\not\equiv 0\left(\mathrm{mod}\, p^{M+1}\right)$. Do đó, $f'\left(\tilde{a}_0\right)=p^M.A;\ A\in\mathbb{Z}_p$. Từ đó suy ra:

$$f\left(a_1\right)\equiv f\left(\tilde{a}_0\right)+b.p^{M+1}.p^M.A\left(\mathrm{mod}\, p^{2M+2}\right)$$

hay

$$f\left(a_1\right)\equiv f\left(\tilde{a}_0\right)+b.p^{2M+1}.A.\left(\mathrm{mod}\, p^{2M+2}\right).$$

Đến đây ta cần tìm *b* sao cho $f\left(\tilde{a}_0\right)+b.p^{2M+1}.A\equiv 0\left(\mathrm{mod}\, p^{2M+2}\right)$

Tức

$$\frac{f\left(\tilde{a}_0\right)}{p^{2M+1}}+b.A\equiv 0\left(\mathrm{mod}\, p\right)\text{hay}\ b\equiv\frac{-f\left(\tilde{a}_0\right)}{p^{2M+1}.A}\left(\mathrm{mod}\, p\right)\ \text{với}\ A=\frac{f'(\tilde{a}_0)}{p^M}$$

Suy ra *b* được chọn duy nhất, là chữ số đầu tiên trong khai triển *p*-adic số $\frac{-f(\tilde{a}_0)}{p^{2M-1}.A}$

Đến đây ta xây dựng được a_1.

Giả sử ta đã có duy nhất dãy số tự nhiên $a_1,a_2,...,a_{n-1}$ thỏa *i), ii), iii).* Ta sẽ xây dựng a_n thỏa các điều kiện trên.

Nếu đã có a_{n-1} thì vì $a_n\equiv a_{n-1}(\mathrm{mod}\, p^{M+n})$ nên ta có thể chọn *b* sao cho: $a_n=a_{n-1}+b.p^{M+n}$ và $0\le a_n<p^{M+n+1}$, suy ra $0\le b\le p-1$.

Như vậy với a_n trên đã thỏa *i)* và *ii).* Ta chỉ cần tìm *b* thỏa *iii)*

Ta có: $f(a_n)=\sum_{i=0}^{n} c_i(a_{n-1}+b.p^{M+n})^i=\sum_{i=o}^{n}(c_ia_{n-1}^i+ib.p^{M+n}.a_{n-1}^{i-1}+bội\ của\ p^{2M+2n})$

suy ra

$$f(a_n)\equiv f(a_{n-1})+b.p^{M+n}.f'(a_{n-1})\ (\mathrm{mod}\, p^{2M+2n})$$

hay

$$f(a_n) \equiv f(a_{n-1}) + b.p^{M+n}.f'(a_{n-1}) \pmod{p^{2M+n+1}}$$

Do $a_{n-1} \equiv a_0 \pmod{p^{M+1}}$ nên $f'(a_{n-1}) \equiv f'(a_0) \pmod{p^{M+1}}$.

Mà $f'(a_0) \equiv 0 \pmod{p^M}$ và $f'(a_0) \not\equiv 0 \pmod{p^{M+1}}$,

vì vậy

$$f'(a_{n-1}) \equiv 0 \pmod{p^M} \text{ và } f'(a_{n-1}) \not\equiv 0 \pmod{p^{M+1}}.$$

Do đó, $f'(a_{n-1}) = p^M.A'$; $A' \in \mathbb{Z}_p$. Từ đó suy ra

$$f(a_n) \equiv f(a_{n-1}) + b.p^{M+n}.p^M.A'.(\text{mod } p^{2M+n+1})$$

Đến đây ta tìm *b* sao cho $f(a_{n-1}) + b.p^{2M+n}.A' \equiv 0 \pmod{p^{2M+n+1}}$

Tức $\frac{f(a_{n-1})}{p^{2M+n}} + b.A' \equiv 0 \pmod{p}$ hay $b \equiv \frac{-f\left(a_{n-1}\right)}{p^{2M+n}.A'} \pmod{p}$ với $A' = \frac{f'\left(a_{n-1}\right)}{p^M}$

Vậy, *b* chọn được duy nhất là chữ số đầu tiên của $\frac{-f(a_{n-1})}{p^{2M+n}.A'}$ trong khai triển *p*-adic.

Như vậy bằng qui nạp ta đã xây dựng được dãy $a_1, a_2, ..., a_n$ thỏa bổ đề.

Để chứng minh bổ đề Hensel mở rộng, ta cần chứng minh những điều sau:

1. Sự tồn tại: Với $a_0 \in \mathbb{Z}_p$, theo bổ đề trên tồn tại duy nhất một dãy số tự nhiên $a_1, a_2, ..., a_n$ thỏa điều kiện

i) $a_n \equiv a_{n-1} \pmod{p^{M+n}}$

ii) $0 \le a_n < p^{M+n+1}$

iii) $f(a_n) \equiv 0 \pmod{p^{2M+n+1}}$

Do *i)* nên $\left|a_n - a_{n-1}\right|_p \le p^{-M-n}$, ta có

$$\begin{cases} a_1 \equiv a_0 \pmod{p^{M+1}} \\ a_2 \equiv a_1 \pmod{p^{M+2}} \\ \vdots \\ a_n \equiv a_{n-1} \pmod{p^{M+n}} \end{cases}$$

suy ra $a_n \equiv a_{n-1} \equiv ... \equiv a_0 \pmod{p^{M+1}}, \forall n \in \mathbb{N}$. Từ đó,

$$\left|a - a_0\right|_p = \lim_{n\to\infty} \left|a_n - a_0\right|_p \le p^{-M-1}$$

dẫn đến $\left|a - a_0\right|_p \le p^{-M-1}$. Vì vậy, $a \equiv a_0 \pmod{p^{M+1}}$ (1)

Mặt khác, $a_{n+1} \equiv a_n \pmod{p^{M+n+1}},\ \forall n \in \mathbb{N}$ nên $a_m \equiv a_n \pmod{p^{M+n+1}},\ \forall m > n$ dẫn đến $\left|a_m - a_n\right|_p \le p^{-M-n-1}$, từ đó $\left|a - a_n\right|_p = \lim_{m\to\infty}\left|a_m - a_n\right|_p \le p^{-M-n-1}$.

Do vậy $a \equiv a_n \pmod{p^{M+n+1}}$, ta suy ra $f(a) \equiv f(a_n) \pmod{p^{M+n+1}}$ mà $f(a_n) \equiv 0 \pmod{p^{2M+n+1}}$ nên $f(a) \equiv 0 \pmod{p^{M+n+1}}$, do đó $\left|f(a)\right|_p \le p^{-M-n-1}, \forall n \in \mathbb{N}$ dẫn đến $\left|f(a)\right|_p \xrightarrow{n\to+\infty} 0$. Vì vậy, $f(a) = 0$ (2)

2. Tính duy nhất: Giả sử có $a' \in \mathbb{Z}_p$ thỏa hai điều kiện $a' \equiv a_0 \pmod{p^{M+1}}$ và $f(a') = 0$. Ta có $a' = b_0 + b_1 p + b_2 p^2 + \ldots + b_M p^M + b_M p^{M+1} + \ldots + b_{2M} p^{2M} + \ldots$

Đặt

$$a'_0 = b_0 + b_1 p + \ldots + b_M p^M$$
$$a'_1 = b_0 + b_1 p + \ldots + b_M p^M + b_M p^{M+1}$$
$$\vdots$$
$$a'_n = b_0 + b_1 p + \ldots + b_M p^M + b_M p^{M+1} + \ldots + b_{M+n} p^{M+n}$$
$$\vdots$$
$$a'_m = b_0 + b_1 p + \ldots + b_M p^M + b_M p^{M+1} + \ldots + b_{M+n} p^{M+n} + \ldots + b_{M+m} p^{M+m} \quad \textit{với } m = M + n$$

Khi đó $\left\{a'_m\right\}$ thỏa *i), ii)* thỏa bổ đề. Hơn nữa

$a'_m \equiv a' \pmod{p^{2M+n+1}}$ suy ra $f(a'_m) \equiv f(a') \pmod{p^{2M+n+1}}$ mà $f(a') = 0$, do đó $f(a'_m) = 0 \pmod{p^{2M+n+1}}$.

Dãy $\left\{a'_m\right\}$ thỏa điều kiện *iii)* của bổ đề, nói cách khác dãy $\left\{a'_m\right\}$ thỏa bổ đề, do đó $\left\{a'_m\right\} \equiv \left\{a_n\right\}$ *hay* $a = a'$.■

Áp dụng Bổ đề Hensel mở rộng để chứng minh bài toán trong ví dụ 2.4.3

Trong $\mathbb{Q}_2$ luôn tồn tại căn bậc 2 của 9.

Thật vậy**,** xét $f\left(x\right) = x^2 - 9$, ta chứng minh *f(x)* có nghiệm trong $\mathbb{Q}_2$

Với $a_0 = 1 \in \mathbb{Z}_2$, *M* =1 ta có,

$$\begin{cases} f\left(a_0\right) = -8 \equiv 0\left(\bmod 2^{2.1+1}\right) \\ f'\left(a_0\right) = 2a_0 = 2.1 = 2 \equiv 0\left(\bmod 2^{1}\right) \\ f'\left(a_0\right) = 2a_0 = 2.1 = 2 \not\equiv 0\left(\bmod 2^{1+1}\right) \end{cases}$$

Theo Bổ đề Hensel mở rộng, tồn tại duy nhất $x_0 \in \mathbb{Z}_2$ sao cho $x_0 \equiv 1\left(\mathrm{mod}\, 2^{1+1}\right)$ và $f\left(x_0\right) = 0$ hay $x_0^2 = 9$

2.5 Ứng dụng của Bổ đề Hensel

Ứng dụng 1 (Mô tả căn của 1 trong $\mathbb{Q}_p$)

Cho $\mathbb{F}$ là trường phần tử $x \in \mathbb{F}$ gọi là căn của 1 trong $\mathbb{F}$ nếu tồn tại số tự nhiên n để $x^n = 1$.

Trong trường số thực $\mathbb{R}$, ta biết rằng tập các căn của 1 trong $\mathbb{R}$ chính là $\{-1,1\}$. Vậy tập các căn của 1 trong $\mathbb{Q}_p$ là gì? Để mô tả được các căn của 1 trong $\mathbb{Q}_p$, ta cần phải sử dụng đến Bổ đề Hensel và Bổ đề Hensel mở rộng. Cụ thể ta có các kết quả sau:

2.5.1 Định lý (*Mô tả căn của 1 trong $\mathbb{Q}_p$ với p là số nguyên tố lẻ*)

Cho p là số nguyên tố lẻ. Khi đó:

a) Với mọi $1 \le i \le p-1$ tồn tại duy nhất $\xi_i \in \mathbb{Q}_p$ thỏa $\xi_i^{p-1} = 1$ và $\xi_i = i (\mathrm{mod}\, p)$

Do đó: Tập các căn bậc p-1 của 1 trong $\mathbb{Q}_p$ là: $U_{p-1} = \{\xi_1, \xi_2, ...\xi_{p-1}\}$

b) Tập các căn của 1 trong $\mathbb{Q}_p$ chính là U_{p-1} (hay $x \in \mathbb{Q}_p$, $x^n = 1 \Leftrightarrow x^{p-1} = 1$)

Chứng minh

a) Đặt $f(x) = x^p - x$, ta có $f'(x) = p.x^{p-1} - 1$. Với mỗi $i \in \{1,2,..., p-1\}$ thì $(i, p) = 1$.

Theo định lý Fecma $i^p \equiv i (\mathrm{mod}\, p)$ hay $i^p - i \equiv 0 (\mathrm{mod}\, p)$. Khi đó $f(i) \equiv 0 (\mathrm{mod}\, p)$, mặt khác $f'(i) = pi^{p-1} - 1 \equiv -1 (\mathrm{mod}\, p)$ nên $f'(i) \not\equiv 0 (\mathrm{mod}\, p)$, theo Bổ đề Hensel tồn tại duy nhất $\xi_i \in \mathbb{Q}_p$ sao cho $\xi_i \equiv i (\mathrm{mod}\, p)$ và $f(\xi_i) = 0$. Suy ra $\xi_i^p - \xi_i = 0$ và $\xi_i \neq 0$, do đó $\xi_i^{p-1} = 1$.

Vì vậy, $U_{p-1} = \{\xi_1, \xi_2, ..., \xi_{p-1}\} = \{x \in \mathbb{Q}_p : x^{p-1} = 1\}$.

b) Trước hết ta chứng minh 1 không có căn bậc p nào khác 1 trong $\mathbb{Q}_P$.

Xét đa thức $f(x) = x^p - 1 \in \mathbb{Q}_P[x]$, ta có

$$x^p - 1 = 0 \Leftrightarrow (x-1)(x^{p-1} + x^{p-2} + ... + 1) = 0$$

$$\Leftrightarrow \begin{bmatrix} x = 1 \\ x^{p-1} + x^{p-2} + ... + 1 = 0 \end{bmatrix} \qquad (1)$$

Đặt $f(x)=x^{p-1}+x^{p-2}+...+1=\dfrac{x^{p-1}-1}{x-1}$, lúc đó ta có

$$f(x+1)=\frac{(x+1)^{p-1}-1}{x+1-1}=x^{p-2}+C_{p-1}^{2}.x^{p-3}+...+C_{p-1}^{0}$$

Suy ra *f(x+1)* bất khả qui theo tiêu chuẩn Eisenstein, nên *f(x)* bất khả qui trong $\mathbb{Q}_P\left[x\right]$. Do đó (1) vô nghiệm và ta được $\sqrt[p]{1}=1$

Bây giờ ta chứng minh tập các căn của 1 trong $\mathbb{Q}_P$ chính là U_{P-1}.

Kí hiệu U là tập các căn của 1 trong $\mathbb{Q}_P$, ta có $U=\left\{x\in\mathbb{Q}_p:\exists n\in\mathbb{N}^*:x^n=1\right\}$

Ta sẽ chứng minh $U_{p-1}=\left\{x\in\mathbb{Q}_p:x^{p-1}=1\right\}=U$.Thật vậy, ta luôn có

$$U_{p-1}=\left\{x\in\mathbb{Q}_p:x^{p-1}=1\right\}\subseteq U$$

Ngược lại với $x_0\in U$, ta sẽ chứng minh $x_0\in\left\{x\in\mathbb{Q}_p:x^{p-1}=1\right\}=U_{p-1}$.

Vì $x_0\in U$ nên tồn tại $n\in\mathbb{N}^*$ sao cho ${x_0}^n=1$. Giả sử $n=p^k.m,\ (m,p)=1$, Ta có:

$${x_0}^n=1\Leftrightarrow {x_0}^{p^k.m}=1\Leftrightarrow\left(\left({x_0}^m\right)^{p^{k-1}}\right)^p=1$$

Do 1 không có căn bậc p nào khác 1 trong $\mathbb{Q}_p$ nên biểu thức trên tương đương với $\left({x_0}^m\right)^{p^{k-1}}=1$. Áp dụng liên tiếp tính chất trên ta được ${x_0}^m=1$.

Giả sử $x_0=a_0+a_1p+...+a_mp^m+...$

Vì $\left|x_0\right|_p=1$ nên $0<a_0\le p-1$, suy ra $(a_0,p)=1$, theo định lý Fecma, ta được ${a_0}^{p-1}\equiv 1(\mathrm{mod}\,p)$.

Xét đa thức $f(x)=x^{p-1}-1\in\mathbb{Q}_p\left[x\right]$, ta có $f(a_0)={a_0}^{p-1}-1\equiv 0(\mathrm{mod}\,p)$ và

$f'(a_0)=(p-1).{a_0}^{p-2}\not\equiv 0(\mathrm{mod}\,p)$

Theo Bổ đề Hensel, tồn tại duy nhất $y_0\in\mathbb{Z}_p$ sao cho $y_0\equiv a_0(\mathrm{mod}\,p)$ và ${y_0}^{p-1}=1$, suy ra ${y_0}^{m(p-1)}=1$ và $y_0\equiv a_0(\mathrm{mod}\,p)$. Ta có ${x_0}^{m(p-1)}=1$ và $x_0\equiv a_0(\mathrm{mod}\,p)$.

Xét đa thức $g(x)=x^{m(p-1)}-1\in\mathbb{Q}_p\left[x\right]$, ta có $g(a_0)\equiv {a_0}^{m(p-1)}-1\equiv 0(\mathrm{mod}\,p)$ và

$g'(a_0)\equiv m(p-1).{a_0}^{m(p-1)-1}\not\equiv 0(\mathrm{mod}\,p)$

Theo Bổ đề Hensel, phương trình *g(x)=0* có duy nhất nghiệm $z_0 \in \mathbb{Z}_p$ thỏa $z_0 \equiv a_0 \pmod p$ (*) mà x_0, y_0 cũng là nghiệm của *g(x)=0* thỏa (*). Suy ra

$x_0 = z_0 = y_0$. Vậy $x_0 \in \left\{ x \in \mathbb{Q}_p : x^{p-1} = 1 \right\} = U_{p-1}$.■

2.5.2 Định lý (Mô tả căn của 1 trong $\mathbb{Q}_2$**)** *Tập các căn của 1 trong* $\mathbb{Q}_2$ *là* $\{\pm 1\}$

Nghĩa là nếu $x \in \mathbb{Q}_2$ *và tồn tại* $n \in \mathbb{N}^*$ *để* $x^n = 1$ *thì* $x = \pm 1$

Chứng minh Trước tiên ta có nhận xét phương trình $x^2 + 1 = 0$ vô nghiệm trong $\mathbb{Q}_2$. Thật vậy,giả sử tồn tại $x_0 \in \mathbb{Q}_2$ để ${x_0}^2 = -1$. Do $|x_0|_2^2 = |-1|_2 = 1$ nên $x_0 \in \mathbb{Z}_2$, khi đó x_0 có biểu diễn $x_0 = a_0 + a_1 2 + a_2 .2^2 + ... + a_n .2^n + ...$ $\left(với\ a_i \in \{0,1\} \right)$, suy ra

$(a_0 + a_1 2 + ... + a_n .2^n + ...)^2 = -1$ do đó ${a_0}^2 \equiv -1 (\mathrm{mod}\, 2)$ hay $a_0 = 1$ $(vì\ a_i \in \{0,1\})$.

Với $a_0 = 1$, ta suy ra $(1 + a_1 .2)^2 \equiv -1 (\mathrm{mod}\, 2^2)$ hay $1 \equiv -1 (\mathrm{mod}\, 4)$ (vô lý) .

Vậy $x^2 + 1 = 0$ vô nghiệm trong $\mathbb{Q}_2$.

Tiếp theo, với (n, 2) = 1, giả sử có $x_0 \in \mathbb{Q}_2$, $x_0^n = 1$, ta chứng minh $x_0 = 1$. Thật vậy, $x_0^n = 1$ nên $|x_0|_2 = 1$ và $x_0 \equiv 1 (\mathrm{mod}\, 2)$. Do đó $x_0 \equiv 1 (\mathrm{mod}\, 2)$ và $x_0^n = 1$.

Mặt khác, ta cũng có $1 \equiv 1 (\mathrm{mod}\, 2)$ và $1^n = 1$.

Bây giờ, xét đa thức $f(x) = x^n - 1 \in \mathbb{Q}_2[x]$, ta có $f(1) \equiv 0 (\mathrm{mod}\, 2)$ và $f'(1) \equiv n.1 \not\equiv 0 (\mathrm{mod}\, 2)$. Theo Bổ đề Hensel, tồn tại duy nhất $z_0 \in \mathbb{Z}_2$ sao cho $z_0 \equiv 1 (\mathrm{mod}\, 2)$ và $z_0^n = 1$. Do đó $x_0 = z_0 = 1$.

Cuối cùng với *n* là số tự nhiên chẵn và $x_0 \in \mathbb{Q}_2$, $x_0^n = 1$, ta chứng minh $x_0 = \pm 1$

Ta luôn có $n = 2^k .m$ với *m* lẻ, *k*>1. Khi đó $x^n = 1$ tương đương với $x^{2^k .m} = 1$ hay $\left(x^{2^k} \right)^m = 1$.

Theo chứng minh trên thì $x^{2^k} = 1$. Từ đó ta có :

$$\begin{aligned} x^{2^k} - 1 = 0 &\Leftrightarrow (x^2 - 1)(x^2 + 1)(x^4 + 1)....(x^{2^{k-1}} + 1) = 0 \\ &\Leftrightarrow x^2 - 1 = 0 \\ &\Leftrightarrow x = \pm 1 \end{aligned}$$

Vậy căn của 1 trong $\mathbb{Q}_2$ là $\{\pm 1\}$. ■

Ứng dụng 2 (*Mô tả nhóm thương* $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$)

Cho F là trường, khi đó $(F^*, .)$ nhóm Abel

$\left(F^*\right)^2 = \left\{a^2 / a \in F^*\right\}$; $((F^*)^2, .)$ là nhóm con của nhóm $(F^*, .)$

Xét trường hợp

$F = \mathbb{R}, ta\,có:\ \varphi : \mathbb{R}^* \to \{1,-1\}$

$$a \mapsto \frac{a}{|a|}$$

Dễ dàng nhận thấy φ là toàn cấu nhóm nhân với $Ker\varphi = \left\{a \in \mathbb{R}^* / a > 0\right\} = (\mathbb{R}^*)^2$

Áp dụng định lý Noether ta có : $\mathbb{R}^*/Ker\varphi \cong \{1;-1\}$. Vậy,

$$\mathbb{R}^*/(\mathbb{R}^*)^2 \cong \{1;-1\} = \mathbb{Z}_2 - \text{nhóm xiclic cấp 2}$$

Vấn đề đặt ra là khi ta thay $F = \mathbb{Q}_p$ thì kết quả như thế nào ?.

2.5.3 Định lý (mô tả nhóm $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ khi *p* là số nguyên tố lẻ)

Nếu p là số nguyên tố lẻ thì $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Chứng minh Kí hiệu $F_p = \mathbb{Z}/p\mathbb{Z}$, trong lý thuyết số, ta biết rằng số các lớp là thặng dư bậc 2 trong F_p^* là $\frac{p-1}{2}$, do đó

$$F_p^*/\left(F_p^*\right)^2 \cong \mathbb{Z}/2\mathbb{Z}$$

Xét ánh xạ $\theta : \mathbb{Z}_p^* \longrightarrow F_p^*/\left(F_p^*\right)^2$ với $\theta(\alpha) = \theta(a_0 + a_1 p + a_2 p^2 + ...) = \overline{a_0(\alpha)} = \overline{a_0}$

Với $\alpha = a_0 + a_1 p + a_2 p^2 + ..., \quad \beta = b_0 + b_1 p + ... \in \mathbb{Z}_p^*$, ta có

$$\theta\left(\alpha.\beta\right) = \theta(a_0 b_0 + c_1 p + c_2 p^2 + ...) = \overline{a_0 b_0\left(\alpha.\beta\right)} = \overline{a_0 b_0} = \overline{a_0}.\overline{b_0} = \theta\left(\alpha\right).\theta\left(\beta\right)$$

Suy ra θ là đồng cấu nhóm nhân. Dễ dàng nhận thấy θ là toàn cấu.

Bây giờ ta chứng minh $\mathrm{Ker}\theta = \left(\mathbb{Z}_p^*\right)^2$.Thật vậy, $\alpha \in \mathrm{Ker}\theta, \theta\left(\alpha\right) \in \left(F_p^*\right)^2$.

Suy ra $\alpha = a_0 + a_1 p + a_2 p + ...$ với $\overline{a_0} = \overline{b_0}^2$ hay $a_0 \equiv b_0^2 \pmod{p}$.

Xét phương trình bậc hai $f\left(x\right) = x^2 - \alpha$ .Lúc đó, $f\left(b_0\right) = b_0^2 - \alpha \equiv a_0 - \alpha \equiv 0 \pmod{p}$ và $f'\left(b_0\right) = 2b_0 \not\equiv 0 \pmod{p}$.

Theo Bổ đề Hensel, tồn tại duy nhất $x_0 \in \mathbb{Z}_p$ để $x_0^2 = \alpha$ thỏa $x_0 \equiv b \pmod{p}$, do đó $\alpha \in \left(\mathbb{Z}_p^*\right)^2$. Ngược lại với $\alpha = a_0 + a_1 p + a_2 p + ... \in \left(\mathbb{Z}_p^*\right)^2$.

Suy ra $\alpha = \left(b_0 + b_1 p + b_2 p + ...\right)^2$, do đó $a_0 \equiv b_0^2 \pmod{p}$ dẫn tới $a_0\left(\alpha\right) \in \left(F_p^*\right)^2$.

Vậy $\overline{a_0\left(\alpha\right)} = 0$ hay $\alpha \in \mathrm{Ker}\theta$. Áp dụng định lý Noether ta có :

$$\mathbb{Z}_p^* \Big/ (\mathbb{Z}_p^*)^2 \cong \mathbb{Z}_p^* \Big/ Ker\theta \cong F_p^* \Big/ (F_p^*)^2 \cong \mathbb{Z} \Big/ 2\mathbb{Z} \cong \mathbb{Z}_2 - \text{ nhóm xiclic cấp 2}$$

Tiếp theo, xét ánh xạ

$$\varphi : \mathbb{Q}_p^* \to \mathbb{Z} \Big/ 2\mathbb{Z} \oplus \mathbb{Z}_p^* \Big/ (\mathbb{Z}_p^*)^2$$
$$p^m.u \mapsto (\overline{m}, \overline{u})$$

Với $\alpha = p^m.u;\ \beta = p^n.v\ \in \mathbb{Q}_p^*$, ta có

$$\varphi(\alpha.\beta) = \varphi(p^{m+n}.u.v) = (\overline{m+n}, \overline{uv}) = (\overline{m}, \overline{u}).(\overline{n}, \overline{v}) = \varphi(\alpha).\varphi(\beta)$$

Suy ra φ là đồng cấu nhóm.

Với $(\overline{m}, \overline{u}) \in \mathbb{Z} \Big/ 2\mathbb{Z} \oplus \mathbb{Z}_p^* \Big/ (\mathbb{Z}_p^*)^2$ thì tồn tại $\alpha = p^m.u \in \mathbb{Q}_p^*$ sao cho $\varphi(\alpha) = (\overline{m}, \overline{u})$

Suy ra φ là toàn cấu.

$$Ker\varphi = \left\{\alpha = p^m.u \in \mathbb{Q}_p^* \,/\, \varphi(\alpha) = 1\right\} = \left\{\alpha = p^m.u \in \mathbb{Q}_p^* \,/\, \begin{cases} m \in 2\mathbb{Z} \\ u \in (\mathbb{Z}_p^*)^2 \end{cases}\right\} = (\mathbb{Q}_p^*)^2$$

Theo định lý Noether ta có :

$$\mathbb{Q}_p^* \Big/ (\mathbb{Q}_p^*)^2 \cong \mathbb{Q}_p^* \Big/ Ker\varphi \cong \mathbb{Z} \Big/ 2\mathbb{Z} \oplus \mathbb{Z}_p^* \Big/ (\mathbb{Z}_p^*)^2 \cong \mathbb{Z} \Big/ 2\mathbb{Z} \oplus \mathbb{Z} \Big/ 2\mathbb{Z} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 .\blacksquare$$

2.5.4 Định lý (mô tả $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$)

Với p=2 thì

$$\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Để chứng minh mệnh đề trên ta cần chứng minh các nhận xét sau :

Nhận xét 1 $\mathbb{Z}_2^* = \{1;-1\} \dot{\oplus} \{1+4\mathbb{Z}_2\} \cong \mathbb{Z}/2\mathbb{Z} \dot{\oplus} \{1+4\mathbb{Z}_2\}$

Thật vậy, ta có $-1 \not\equiv 1 \pmod 4 \Rightarrow -1 \notin 1+4\mathbb{Z}_2$

nên $\{1;-1\} \cap \{1+4\mathbb{Z}_2\} = \{1\}$.

Với $\alpha \in \mathbb{Z}_2^*$ α có thể biểu diễn $\alpha = 1 + a_1 2 + a_2 2^2 + a_3 2^3 + ... \ (với\ a_i \in \{0,1\})$

Với $a_1 = 0$ thì $\alpha = 1 + a_2 4 + a_3 2^3 + ...$ Suy ra $\alpha \in 1.(1+4a),\ a \in \mathbb{Z}_2$ hay $\alpha \in 1.\alpha_0,\ \alpha_0 = 1+4a \in 1+4\mathbb{Z}_2$.

Với $a_1 = 1$ thì $\alpha = 1 + 2 + a_2 2^2 + a_3 2^3 + ...$ Suy ra

$\alpha = 3 + 4a = (-1)(-3-4a) = (-1)(1-4(a+1))$ với $a \in \mathbb{Z}_2$

hay $\alpha = (-1).\alpha_0,\ \alpha_0 = 1-4(a+1) \in 1+4\mathbb{Z}_2$.

Vậy $\mathbb{Z}_2^* = \{1;-1\} \dot{\oplus} \{1+4\mathbb{Z}_2\}$

Nhận xét 2 $(1+4\mathbb{Z}_2)/(1+8\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z}$

Thật vậy,

xét : $\theta : 1+4\mathbb{Z}_2 \longrightarrow \mathbb{Z}/2\mathbb{Z}$ với $\theta(\alpha) = \theta(1 + a_2 2^2 + a_3 2^3 + ...) = \overline{a_2}$, $(a_i \in \mathbb{Z}_2)$

Với mọi $\alpha, \beta \in 1+4\mathbb{Z}_2$, $\alpha = \beta \Leftrightarrow 1 + a_2 2^2 + a_3 2^3 + ... = 1 + b_2 2^2 + b_3 2^3 + ...$ Khi đó, $a_2 \equiv b_2 \pmod 4$ nên $a_2 \equiv b_2 \pmod 2$, dẫn đến $\overline{a_2} \equiv \overline{b_2}$ hay $\theta(\alpha) = \theta(\beta)$. Như vậy θ là ánh xạ.

Với mọi $\alpha, \beta \in 1+4\mathbb{Z}_2$, ta có :

$\theta(\alpha\beta) = \theta(1 + (a_2+b_2).2^2 + 8\mathbb{Z}) = \overline{a_2+b_2} = \overline{a_2} + \overline{b_2} = \theta(\alpha) + \theta(\beta)$

Như vậy θ là đồng cấu nhóm.

Với mọi $\overline{a_2} \in \mathbb{Z}/2\mathbb{Z}$, tồn tại $\alpha = 1 + a_2 2^2 + a_3 2^3 + \ldots$ sao cho $\theta(\alpha) = \overline{a_2}$. Suy ra θ là toàn cấu.

Dễ thấy $\mathrm{Ker}\theta = \left\{\alpha \in 1 + 4\mathbb{Z}_2 \,/\, \theta(\alpha) = \overline{a_2} = \overline{0}\right\} = \left\{1 + 8\mathbb{Z}_2\right\}$.

Áp dụng định lý Noether ta có:

$$\left(1 + 4\mathbb{Z}_2\right)/\left(1 + 8\mathbb{Z}_2\right) = \left(1 + 4\mathbb{Z}_2\right)/Ker\theta \cong \mathbb{Z}/2\mathbb{Z}$$

Nhận xét 3 $(\mathbb{Z}_2^*)^2 = 1 + 8\mathbb{Z}_2$

Thật vậy, lấy $\alpha \in (\mathbb{Z}_2^*)^2$ thì α có dạng $(1 + b_1 2 + b_2 2^2 + b_3 2^3 + \ldots)^2$. Khi đó, $\alpha \equiv (1 + b_1 2 + b_2 2^2)^2 \pmod 8$, suy ra $\alpha \equiv (1 + b_1^2 4 + 4b_1) \pmod 8$, hay $\alpha \equiv 1 + 4b_1(b_1 + 1) \pmod 8$. Do đó, $\alpha \in 1 + 8\mathbb{Z}_2$.

Ngược lại, xét $f(x) = x^2 - \alpha$ Ta có:

$$\begin{cases} f(1) = 1 - \alpha \equiv 0 \pmod{2^3 = 2^{2M+1}} \\ f'(1) = 2 \equiv 0 \pmod{2^1 = 2^M} \\ f'(1) = 2 \not\equiv 0 \pmod{4 = 2^{M+1}} \end{cases} \quad \text{với } M=1,\ a_0=1$$

Theo Bổ đề Hensel suy rộng, tồn tại duy nhất $\beta \in \mathbb{Z}_2$ thỏa $f(\beta) = 0$ và $\beta \equiv 1 \pmod{2^2}$.

Khi đó, $\alpha = \beta^2$ hay $\alpha \in (\mathbb{Z}_2^*)^2$.

Vậy, $(\mathbb{Z}_2^*)^2 = 1 + 8\mathbb{Z}_2$.

Cuối cùng, ta chứng minh $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Với $x \in \mathbb{Q}_2^*$, x được biểu diễn dưới dạng $x = 2^m.u,\ u \in \mathbb{Z}_2^*, m \in \mathbb{Z}$. Theo nhận xét 1, ta có u viết được duy nhất dưới dạng $u = \varepsilon.v$ với $\varepsilon \in \left\{+1; -1\right\},\ v \in 1 + 4\mathbb{Z}_2$. Do đó, x có thể viết dưới dạng duy nhất $x = 2^m.\varepsilon.v$ với $\varepsilon \in \left\{+1; -1\right\},\ v \in 1 + 4\mathbb{Z}_2, m \in \mathbb{Z}$. Khi đó, xét ánh xạ

$$\begin{array}{rccc} \theta: & \mathbb{Q}_2^* & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \oplus \left\{+1; -1\right\} \oplus \left(1 + 4\mathbb{Z}_2\right)/\left(1 + 8\mathbb{Z}_2\right) \\ & x = 2^m.\varepsilon.v & \mapsto & \theta(x) = (\overline{m},\ \varepsilon,\ \overline{v}) \end{array}$$

Ta chứng minh θ là toàn cấu nhóm. Thật vậy,

Với mọi $x, y \in \mathbb{Q}_2^*,\ x = 2^m.\varepsilon.v,\ y = 2^n.\varepsilon'.u,\ m, n \in \mathbb{Z},\ \varepsilon, \varepsilon' \in \{1; -1\},\ u, v \in 1 + 4\mathbb{Z}_2$, ta có

$$\theta(x.y) = \theta(2^{m+n}.\varepsilon\varepsilon'.uv) = (\overline{m+n},\ \varepsilon\varepsilon',\ \overline{uv}) = (\overline{m},\ \varepsilon,\ \overline{u}).(\overline{n},\ \varepsilon',\ \overline{v}) = \theta(x).\theta(y)$$

Suy ra θ là đồng cấu nhóm nhân.

Với mọi $t \in \mathbb{Z}/2\mathbb{Z} \oplus \{+1;-1\} \dot{\oplus} 1+4\mathbb{Z}_2$ thì tồn tại $\alpha = 2^m.\varepsilon.v \in \mathbb{Q}_2^*$ sao cho $\theta(\alpha) = t$.

Suy ra θ là toàn cấu.

Tiếp theo ta chứng minh $\mathrm{Ker}\theta = (\mathbb{Q}_2^*)^2$. Thật vậy ta có

$$\mathrm{Ker}\theta = \left\{ x = 2^m.\varepsilon.v \in \mathbb{Q}_2^* \,/\, \theta(x) = (\overline{m}, \varepsilon, \overline{v}) = (\overline{0}, 1, \overline{1}) \right\}$$

Với mọi $x \in (\mathbb{Q}_p^*)^2$ thì có $y \in \mathbb{Q}_2^*$ để $x = 2^m.\varepsilon.v = y^2 = (2^n.\varepsilon'.v')^2 = 2^{2n}.(\varepsilon')^2.(v')^2$. Khi đó $m = 2n,\ \varepsilon = (\varepsilon')^2 = 1$ và $v = (v')^2 = (1+4\mathbb{Z}_2)^2 = 1+8\mathbb{Z}_2 \in 1+8\mathbb{Z}_2$. Suy ra $\overline{m} = \overline{0},\ \varepsilon = 1$ và $\overline{v} = \overline{1}$ tức là $x \in Ker\theta$.

Ngược lại, với $x \in \mathrm{Ker}\theta$ thì $x = 2^m.\varepsilon.v \in \mathbb{Q}_2^*,\ \overline{m} = \overline{0},\ \varepsilon = 1,\ \overline{v} = \overline{1}$. Lúc đó,

$m = 2n,\ \varepsilon = 1,\ v \in 1+8\mathbb{Z}_2$. Theo nhận xét 3, $v \in (\mathbb{Z}_p^*)^2$ nên $v = u^2$, $u \in \mathbb{Z}_p^*$.

Như vậy $x = 2^{2n}.1.u^2 = 2^{2n}.u^2 = y^2 \in (\mathbb{Q}_p^*)^2$ với $y = 2^n.u$

Vậy $(\mathbb{Q}_p^*)^2 = Ker\theta$.

Áp dụng định lý Noether, ta có:

$$\mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2 \cong \mathbb{Q}_2^*/\ker\theta \cong \mathbb{Z}/2\mathbb{Z} \oplus \{-1;1\} \oplus {}^{1+4\mathbb{Z}_2}/_{1+8\mathbb{Z}_2}$$

hay

$$\mathbb{Q}_2{}^*/(\mathbb{Q}_2{}^*)^2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 .\ \blacksquare$$

Ứng dụng 3 *(Nghiên cứu tính đẳng cấu giữa các trường $\mathbb{Q}_p, \mathbb{Q}_q$ và $\mathbb{R}$)*

2.5.5 Định lý (Xét sự đẳng cấu của các trường $\mathbb{Q}_p, \mathbb{Q}_q, \mathbb{R}$)

i) Trường $\mathbb{Q}_p$ và $\mathbb{Q}_q$ không đẳng cấu với $p \neq q$

ii) Trường $\mathbb{Q}_p$ không đẳng cấu với $\mathbb{R}$

Chứng minh

Trước hết ta có nhận xét: Cho F, K là trường

$$\textit{Nếu } F \cong K \textit{ thì } F^*/\left(F^*\right)^2 \cong K^*/\left(K^*\right)^2$$

Thật vậy, giả sử $f : F \longrightarrow K$ là đẳng cấu trường, xét

$$\overline{f}: F^*/\left(F^*\right)^2 \longrightarrow K^*/\left(K^*\right)^2$$
$$\overline{a} \mapsto \overline{f}\left(\overline{a}\right) = \overline{f\left(a\right)}$$

Với $\overline{a}, \overline{b} \in F^*/\left(F^*\right)^2$, ta có

$$\overline{a} = \overline{b} \Leftrightarrow ab^{-1} \in \left(F^*\right)^2$$
$$\Leftrightarrow f\left(ab^{-1}\right) \in f\left(\left(F^*\right)^2\right) = f\left(\left(F^*\right)\right)^2 = \left(K^*\right)^2$$
$$\Leftrightarrow \overline{f\left(a\right)} = \overline{f\left(b\right)}$$

Vậy $\overline{f}$ là ánh xạ và là đơn ánh.

Hiển nhiên $\overline{f}$ là toàn ánh.

Mặt khác, với $\overline{a}, \overline{b} \in F^*/\left(F^*\right)^2$, ta có

$$\overline{f}\left(\overline{a}\overline{b}\right) = \overline{f}\left(\overline{ab}\right) = \overline{f\left(ab\right)} = \overline{f\left(a\right).f\left(b\right)} = \overline{f\left(a\right)}.\overline{f\left(b\right)} = \overline{f}\left(\overline{a}\right).\overline{f}\left(\overline{b}\right)$$

Vậy $\overline{f}$ là đẳng cấu nhóm.

i) Trường $\mathbb{Q}_p$ và $\mathbb{Q}_q$ không đẳng cấu với $p \neq q$

Ta xét 2 trường hợp :

a) Trường $\mathbb{Q}_p$ và $\mathbb{Q}_2$ không đẳng cấu với $p \neq 2$

Thật vậy, theo định lý 2.5.3 và 2.5.4, ta có : $\mathbb{Q}_p^*/\left(\mathbb{Q}_p^*\right)^2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ và

$$\mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Vậy theo nhận xét trên thì $\mathbb{Q}_p$ không đẳng cấu $\mathbb{Q}_2$ với $p \neq 2$.

b) Trường $\mathbb{Q}_p$ và $\mathbb{Q}_q$ không đẳng cấu với p, q ($p \neq q$)là các số nguyên tố lẻ

Ta có nhận xét sau: nếu $f: F \longrightarrow K$ là đẳng cấu trường thì phần tử $u \in F$ là căn của đơn vị 1 khi và chỉ khi $f\left(u\right) \in K$ cũng là căn của đơn vị 1. Do đó nếu f là đẳng cấu trường thì tập các căn của 1 trong F và tập các căn của 1 trong K có số phần tử như nhau. Theo định

lý 2.5.1, tập các căn của 1 trong $\mathbb{Q}_p$ là U_{p-1} (có *p-1* phần tử), tập các căn của 1 trong $\mathbb{Q}_q$ là U_{q-1} (có *q-1* phần tử).

Suy ra $\mathbb{Q}_p$ và $\mathbb{Q}_q$ không đẳng cấu.

Kết luận: $\mathbb{Q}_p$ và $\mathbb{Q}_q$ không đẳng cấu với mọi số nguyên tố $p \neq q$.

ii) Trường $\mathbb{Q}_p$ không đẳng cấu với trường $\mathbb{R}$

Ta cũng xét 2 trường hợp:

a) Nếu $p \neq 2$ thì $\mathbb{Q}_p^* \Big/ \left(\mathbb{Q}_p^*\right)^2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, trong khi đó $\mathbb{R}^* \Big/ \left(\mathbb{R}^*\right)^2 \cong \mathbb{Z}_2$

Suy ra $\mathbb{Q}_p$ không đẳng cấu với $\mathbb{R}$.

b) Nếu $p = 2$ thì $\mathbb{Q}_2^* \Big/ \left(\mathbb{Q}_2^*\right)^2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, trong khi đó $\mathbb{R}^* \Big/ \left(\mathbb{R}^*\right)^2 \cong \mathbb{Z}_2$

Suy ra $\mathbb{Q}_p$ không đẳng cấu với $\mathbb{R}$.

Kết luận: $\mathbb{Q}_p$ không đẳng cấu với $\mathbb{R}$.■

Ứng dụng 4 (Mô tả nhóm các tự đẳng cầu $\mathbb{Q}_p$)

Ta có nhận xét sau : *Trường $\mathbb{R}$ chỉ có 1 tự đẳng cấu duy nhất là ánh xạ đồng nhất*

Thật vậy, giả sử $f : \mathbb{R} \longrightarrow \mathbb{R}$ là 1 đẳng cấu của trường $\mathbb{R}$. Khi đó,

$$f(1) = 1 \Rightarrow f(n) = n, \quad \forall n \in \mathbb{Z}$$

$$\Rightarrow f(-n) = -n, \quad \forall n \in \mathbb{Z}$$

Với mọi $r \in \mathbb{Q}$, $r = \frac{m}{n}, \quad m, n \in \mathbb{Z}, \quad n \neq 0$ nên $f(r) = f\left(\frac{m}{n}\right) = \frac{f(m)}{f(n)} = \frac{m}{n} = r$

Vậy $f(r) = r, \ \forall r \in \mathbb{Q}$.

Tiếp theo ta chứng minh : nếu $\alpha, \beta \in \mathbb{R}, \quad \alpha < \beta$ thì $f(\alpha) < f(\beta)$

Thật vậy, ta có

$$f(\beta) - f(\alpha) = f(\beta - \alpha) = f\left(\left(\sqrt{\beta - \alpha}\right)^2\right) = \left(f\left(\sqrt{\beta - \alpha}\right)\right)^2 > 0$$

Vậy $f(\alpha) < f(\beta)$

Bây giờ ta chứng minh: $f(\alpha)=\alpha;\quad \forall \alpha \in \mathbb{R}$. Thật vậy, giả sử ngược lại ta có $f(\alpha)\neq \alpha$.

Lúc đó xảy ra 2 trường hợp sau :

Trường hợp 1: $f(\alpha)<\alpha$

Vì $f(\alpha)<\alpha$ nên tồn tại $r\in\mathbb{Q}$: $f(\alpha)<r<\alpha$

Do $r<\alpha$, theo chứng minh trên $r=f(r)<f(\alpha)$, điều này mâu thuẫn.

Trường hợp 2: $f(\alpha)>\alpha$

Vì $f(\alpha)>\alpha$ nên tồn tại $r\in\mathbb{Q}$: $f(\alpha)>r>\alpha$.

Do $r>\alpha$, theo chứng minh trên $r=f(r)>f(\alpha)$, điều này mâu thuẫn.

Vậy $f(\alpha)=\alpha,\quad \forall \alpha \in \mathbb{R}$.

Như vậy nếu *f* là 1 tự đẳng cấu của $\mathbb{R}$ thì *f* là ánh xạ đồng nhất. Vấn đề đặt ra đối với trường $\mathbb{Q}_p$ thì kết quả như thế nào? Ta cũng có kết quả tương tự. Cụ thể ta có mệnh đề sau :

2.5.6 Định lý (Mô tả các tự đẳng cấu của $\mathbb{Q}_p$)

Trường $\mathbb{Q}_p$ chỉ có 1 tự đẳng cấu duy nhất là ánh xạ đồng nhất.

Chứng minh Để chứng minh định lý này ta cần chứng minh nhận xét sau

Nhận xét *Cho $u\in\mathbb{Q}_p^*$ khi đó các phát biểu sau là tương đương :*

i) u là phần tử khả nghịch của $\mathbb{Z}_p$ $\left(u\in\mathbb{Z}_p^{\,*}\right)$

ii) $\forall n\in\mathbb{N}$, nếu $(n,p)=1$ thì u^{p-1} có căn bậc n trong $\mathbb{Q}_p$

Chứng minh nhận xét

i) $\Rightarrow$ *ii)*: Giả sử $u\in\mathbb{Z}_p^*$, ta chứng minh: $\forall n\in\mathbb{N}$, $(n,p)=1$ thì u^{p-1} có căn bậc *n* trong $\mathbb{Q}_p$.

Thật vậy,

$u\in\mathbb{Z}_p^*$ thì $u=a_0+a_1p+a_2p^2+\ldots$ với $0\le a_i<p-1$ và $(a_0,p)=1$

Theo định lý Fecma ta có: $a_0^{p-1}\equiv 1 \pmod p$, suy ra $a=u^{p-1}\equiv a_0^{p-1}\equiv 1 \pmod p$

Xét $f(x)=x^n-a$. Ta có : $f(1)=1-a\equiv 0 \pmod p$ và $f'(1)=n\not\equiv 0 \pmod p$.

Theo bổ đề Hensel tồn tại duy nhất $x_0\in\mathbb{Z}_p$ thỏa $x_0\equiv 1 \pmod p$ và

$f(x_0)=x_0^n-a\equiv 0 \pmod p$ tức là $x_0^n=a=u^{p-1}$.

Vậy u^{p-1} có căn bậc n trong $\mathbb{Q}_p$

ii) $\Rightarrow$ ***i):*** Giả sử u^{p-1} luôn có căn bậc n là x_n trong $\mathbb{Q}_p$ với $\forall n \in \mathbb{N}, \quad (n,p)=1$

Ta có : $x_n^n = u^{p-1}$ suy ra $n.ord_p(x_n) = (p-1).ord_p(u)$, dẫn đến *n* là ước của $(p-1).ord_p(u)$ với mọi $n \in \mathbb{N}$, $(n,p)=1$, do đó $(p-1)ord_p(u)=0$ hay $ord_p(u)=0$, vì vậy $|u|_p = 1$, tức là $u \in \mathbb{Z}_p^*$.

Bây giờ ta chứng minh mệnh đề:

Giả sử $f : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ là tự đẳng cấu của trường $\mathbb{Q}_p$. Khi đó, $f(1)=1$ dẫn đến $f(m)=m, \quad \forall m \in \mathbb{Z}$. Do đó, với mọi $r \in \mathbb{Q}$, $r=\frac{m}{n}$, $m,n \in \mathbb{Z}$, $n \neq 0$ thì

$$f(r) = f\left(\frac{m}{n}\right) = \frac{f(m)}{f(n)} = \frac{m}{n} = r,$$

Tiếp theo ta chứng minh nếu $u \in \mathbb{Z}_p^*$ thì $f(u) \in \mathbb{Z}_p^*$. Thật vậy, nếu $u \in \mathbb{Z}_p^*$ thì theo nhận xét trên, với mọi $n \in \mathbb{N}$, $(n,p)=1$ thì u^{p-1} có căn bậc *n* trong $\mathbb{Q}_p$, nghĩa là tồn tại $x_n \in \mathbb{Q}_p$ để $u^{p-1} = x_n^n$, suy ra $f(u^{p-1}) = f(x_n^n) = (f(x_n))^n$ mà

$$f(u^{p-1}) = (f(u))^{p-1}$$

nên $(f(u))^{p-1} = (f(x_n))^n$, có nghĩa là $(f(u))^{p-1}$ có căn bậc *n* trong $\mathbb{Q}_p$. Vậy theo nhận xét trên, ta có $f(u) \in \mathbb{Z}_p^*$.

Bây giờ, ta chứng minh *f* là ánh xạ đẳng cự tức là

Với $\alpha, \beta \in \mathbb{Q}_p$ thì $|f(\alpha)-f(\beta)|_p = |\alpha-\beta|_p$

Thật vậy, giả sử $\alpha-\beta = p^m.u, \quad m \in \mathbb{Z}, \quad u \in \mathbb{Z}_p^*$. Khi đó $|\alpha-\beta|_p = p^{-m}$.

Ta có $f(\alpha)-f(\beta) = f(\alpha-\beta) = f(p^m.u) = f(p^m).f(u) = p^m.f(u)$ dẫn tới

$|f(\alpha)-f(\beta)|_p = p^{-m} = |\alpha-\beta|_p$ vì $f(u) \in \mathbb{Z}_p^*$.

Vậy *f* là ánh xạ đẳng cự, do đó *f* là ánh xạ liên tục.

Cuối cùng ta chứng minh *f* là ánh xạ đồng nhất. Thật vậy, với mọi $x \in \mathbb{Q}_p$, giả sử

$x = a_m p^m + ... + a_k p^k + ...$

Đặt $x_n = a_m p^m + ... + a_{m+n} p^{m+n} \in \mathbb{Q}$ thế thì $x = \lim_{n\to\infty} x_n$. Suy ra $f\left(x\right) = f\left(\lim_{n\to\infty} x_n\right)$, lại vì f liên tục nên $\lim_{n\to\infty} f\left(x_n\right) = \lim_{n\to\infty} x_n = x$. Vậy f là ánh xạ đồng nhất.■

KẾT LUẬN

Trong luận văn này chúng tôi đã trình bày khá đầy đủ về cách xây dựng trường các số *p*-adic $\mathbb{Q}_p$ và khảo sát một cách chi tiết các tính chất của trường các số *p*-adic $\mathbb{Q}_p$. Trong quá trình nghiên cứu chúng tôi luôn cố gắng so sánh sự giống nhau và khác nhau giữa các trường số *p*-adic $\mathbb{Q}_p$ và trường các số thực $\mathbb{R}$. Đặc biệt chúng tôi đã chứng minh Bổ đề Hensel và Bổ đề Hensel mở rộng và tìm tòi được khá nhiều ứng dụng của Bổ đề Hensel để khảo sát, nghiên cứu các tính chất của trường các số *p*-adic $\mathbb{Q}_p$.

TÀI LIỆU THAM KHẢO

[1].Hoàng Xuân Sính, *Đại số đại cương,* NXB Giáo dục, 1970.

[2].Mỵ Vinh Quang, *Đại số đại cương*, NXB Giáo dục, 1998.

[3].Mỵ Vinh Quang, *Bài tập đại số đại cương*, NXB Giáo dục, 1998.

[4].A.J.Baker, *An Introduction to p-adic Nubers and p-adic Analysis*, 2003.

[5].Neal Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-Functions*, Springer, 1996.

[6].Neal Koblitz, *p-adic Analysis: a Short Course an Recent work*, Cambridge University Press, 1980.

[7].P.C.Hu and C.C.Yang, *Meromorphic function over non-Archimedean fiels*, Kluwer Academic Publishers, London, 2000.