

Летняя математическая школа ЛНМО

Поставы, 2022г.

Алгебраическая геометрия и теория чисел

**In nature, poisonous creatures
will develop bright colors to
warn others of their toxicity**



**Graduate Texts
in Mathematics**

Robin Hartshorne

**Algebraic
Geometry**

 Springer

*Конспект по материалам лекций, прочитанных М.И. Магиным
11-му математическому классу*



Лаборатория непрерывного
математического образования

Алгебраическая геометрия и теория чисел

Содержание

1. Нормированные поля	2
1.1 Нормированное поле. Неархимедовы нормы.	2
1.2 Эквивалентные нормы.	3
1.3 Пополнение метрических пространств.	3
1.4 Пополнение нормированного поля.	5
2. p-адические числа	7
2.1 Кольцо целых p -адических чисел.	7

1. Нормированные поля

1.1 Нормированное поле. Неархимедовы нормы.

Здесь и в дальнейшем будем полагать F полем, хотя многие вещи работают и для кольца (а для области целостности существует единственное продолжение на поле частных).

Definition 1. Нормой (нормированием, абсолютным значением) на поле F называют отображение $\|\cdot\|: F \rightarrow \mathbb{R}_{>0}$, удовлетворяющее следующим свойствам:

1. $\|x\| = 0 \Leftrightarrow x = 0$.
2. $\forall x, y \in F \quad \|xy\| = \|x\|\|y\|$.
3. $\exists C > 0: \forall x, y \in F:$

$$\|x + y\| \leq C \cdot \max(x, y)$$

Пара $(F, \|\cdot\|)$ называется нормированным полем.

Remark 1. Тем, кто уже до этого видел определение нормы, это определение может показаться странным, так как обычно вместо третьего свойства требуют неравенство треугольника:

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

Ясно, что третье свойство следует из неравенства треугольника с $C = 2$. Ниже мы покажем и обратную импликацию.

Ясно, что любая норма задаёт метрику $d(x, y) = \|x - y\|$, а любая метрика индуцирует топологию стандартным образом.

Example 1. Если $F \leq \mathbb{C}$, то подходит $|\cdot|$ (модуль комплексного числа). Если $F \leq \mathbb{R}$ или $F \leq \mathbb{Q}$, то подходит $|\cdot|$.

Example 2. На любом поле можно ввести тривиальную норму (иногда соответствующую ей метрику называют метрикой лентяя):

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

Theorem 1. Если в определении 1 постоянная C равна 2, то норма удовлетворяет неравенству треугольника.

Доказательство. Сначала отметим, что если $n, m \in \mathbb{N}$, $n \leq 2^m$, то выполняется оценка:

$$\|x_1 + x_2 + \dots + x_n\| \leq C^m \cdot \max_{1 \leq k \leq n} \|x_k\|$$

Тогда мы можем провести оценки следующим образом:

$$\begin{aligned} \|x+y\|^n &= \|(x+y)^n\| = \left\| \sum_{k=0}^n \binom{n}{k} x^k y^{n-k} \right\| \leq 2(n+1) \max_{0 \leq k \leq n} \left\| \binom{n}{k} x^k y^{n-k} \right\| \leq 2(n+1) \max_{0 \leq k \leq n} \left(2 \binom{n}{k} \|x\|^k \|y\|^{n-k} \right) \leq \\ &\leq 4(n+1)(\|x\| + \|y\|)^n \end{aligned}$$

Преобразуем это неравенство

$$\left(\frac{\|x+y\|}{\|x\| + \|y\|} \right)^n \leq 4(n+1) \Leftrightarrow \frac{\|x+y\|}{\|x\| + \|y\|} \leq 4^{\frac{1}{n}} \cdot (n+1)^{\frac{1}{n}}$$

В пределе при $n \rightarrow \infty$ получаем:

$$\frac{\|x+y\|}{\|x\| + \|y\|} \leq 1 \Leftrightarrow \|x+y\| \leq \|x\| + \|y\|$$

□

Remark 2. Пример $F = \mathbb{C}$ с нормой $\|\cdot\| = |\cdot|^\alpha$, $\alpha > 1$ показывает, что константу $C = 2$ нельзя улучшить.

Remark 3. Тем самым, мы показали, что норму можно понимать, как функтор из категории \mathcal{Field} в категорию \mathcal{Metr} .

Corollary 1. Норма непрерывна.

Definition 2. Нормы, с постоянной $C = 1$ в определении 1 называют неархимедовыми. Нормы, не являющиеся неархимедовыми, называют архимедовыми.

Example 3. Тривиальная норма на любом поле F является неархимедовой.

Definition 3. Ясно, что любое $x \in \mathbb{Q}$ представимо в виде $x = p^n \cdot \frac{a}{b}$, где $a, b \in \mathbb{Z}$, $a \not\equiv 0 \pmod{p}$, $b \not\equiv 0 \pmod{p}$, $a \not\equiv 0 \pmod{p}$, $n \in \mathbb{Z}$. В таком случае число n называют p -адическим показателем числа x и обозначают $v_p(x)$.

Definition 4. (Самое важное)

Пусть p — простое число. Тогда норму

$$\|x\|_p = \begin{cases} 0, & x = 0 \\ p^{-v_p(x)}, & x \neq 0 \end{cases}$$

на поле \mathbb{Q} называют p -адической нормой.

Remark 4. Ясно, что подходит $r^{-v_p(x)}$, где $r > 1$, но p брать удобно, так как для $x \in \mathbb{Q}^*$ справедлива формула произведения

$$1 = \prod_p |x| \cdot \|x\|_p$$

Lemma 1. Если норма неархимедова, то для $x, y: \|x\| \neq \|y\|$ выполняется $\|x + y\| = \max\{\|x\|, \|y\|\}$.

Corollary 2. Рассмотрим $(F, \|\cdot\|)$, где норма $\|\cdot\|$ неархимедова. Тогда, если $b \in B_r(a)$, то $B_r(a) = B_r(b)$.

Corollary 3. (Забавное)

Если на поле F введена неархимедова норма F , то $\forall x, y, z \in F$ по крайней мере два числа из $\|x - y\|$, $\|x - z\|$, $\|y - z\|$ равны.

Иными словами, в метрическом пространстве (F, d) ($d(x, y) = \|x - y\|$) все треугольники равнобедренные.

1.2 Эквивалентные нормы.

Пока не знаю, буду ли рассказывать.

1.3 Пополнение метрических пространств.

Definition 5. Пусть (X, d_X) — метрическое пространство, $\mathcal{F}(X)$ — множество всех ограниченных функций из X в \mathbb{R} . Тогда введём расстояние d_∞ между функциями $f, g \in \mathcal{F}(X)$:

$$d_\infty(f, g) \stackrel{\text{def}}{=} \sup\{|f(x) - g(x)|, x \in X\}$$

Заметим, что определение корректно, так как функции ограничены.

Lemma 2. $(\mathcal{F}(X), d_\infty)$ — метрическое пространство.

Доказательство. Проверим три аксиомы метрики:

1. Пусть $f = g$. Тогда $|f(x) - g(x)| = 0$ для всякого $x \in X$, так что $d_\infty(f, g) = 0$. Если же наоборот $d_\infty(f, g) = 0$, то $0 \leq |f(x) - g(x)| \leq \sup = 0$, а значит $f(x) = g(x)$ для всех $x \in X$, что и означает $f \equiv g$.
2. Так как $|f(x) - g(x)| = |g(x) - f(x)|$, то и $d_\infty(f, g) = d_\infty(g, f)$.
3. Рассмотрим три ограниченные функции $f, g, h \in \mathcal{F}(X)$, и покажем, что

$$d_\infty(f, g) + d_\infty(g, h) \geq d_\infty(f, h)$$

Мы знаем, что:

$$\forall x \in X : |f(x) - g(x)| + |g(x) - h(x)| \geq |f(x) - h(x)|$$

в силу неравенства треугольника для стандартной метрики на \mathbb{R} . Для всякого $\varepsilon > 0$ мы можем взять x_0 такой, что $|f(x_0) - h(x_0)| \geq \sup\{|f(x) - h(x)|, x \in X\} - \varepsilon$. Получаем, что

$$\begin{aligned} d_\infty(f, h) - \varepsilon &= \sup\{|f(x) - h(x)|, x \in X\} - \varepsilon \leq |f(x_0) - h(x_0)| \leq \\ &\leq |f(x_0) - g(x_0)| + |g(x_0) - h(x_0)| \leq d_\infty(f, g) + d_\infty(g, h) \end{aligned}$$

а раз это верно для любого $\varepsilon > 0$, то искомое неравенство доказано.

□

Lemma 3. $\mathcal{F}(X)$ — полно.

Доказательство. Пусть f_n — фундаментальная последовательность функций. Тогда $\forall x_0 \in X : \{f_n(x_0)\}$ — также фундаментальная последовательность, так как $|f_n(x_0) - f_m(x_0)| \leq \sup\{|f_n(x) - f_m(x)|, x \in X\}$. Следовательно,

$$\forall x_0 \in X : \exists \lim_{n \rightarrow \infty} f_n(x_0)$$

и сходимость по всем точкам равномерна, так как не зависит от выбора точки x_0 . Иными словами,

$$\exists f(x) : \forall \varepsilon > 0 : \exists N : \forall n > N : d_\infty(f_n, f) < \varepsilon$$

где $f(x_0)$ определяется как предел $\lim_{n \rightarrow \infty} f_n(x_0)$. Так что $f(x)$ — функция, являющаяся пределом искомой последовательности функций. □

Definition 6. Пусть (X, d_X) — метрическое пространство, $\mathcal{F}(X)$ — множество ограниченных функций из X в \mathbb{R} . Построим изометрическое вложение $k : X \rightarrow \mathcal{F}(X)$ следующим образом:

1. Если X — ограничено, то определим $k(x) = d_x$, где

$$\forall y \in X : d_x(y) \stackrel{\text{def}}{=} d_X(x, y)$$

Функция d_x ограничена, так как X ограничено. Заметим также, что

$$d_\infty(d_x, d_y) = \sup_z |d_x(z) - d_y(z)| = \sup_z (d_X(x, z) - d_X(z, y)) \leq d_X(x, y)$$

однако равенство достигается при $z = y$, так что $d_\infty(d_x, d_y) = d_X(x, y)$, а значит вложение изометрическое.

2. Пусть X , возможно, не ограничено. Тогда определим $k(x) = d_x - d_{x_0}$ для некоторой фиксированной точки $x_0 \in X$, где

$$\forall y \in X : (k(x))(y) \stackrel{\text{def}}{=} d_x(y) - d_{x_0}(y) = d_X(x, y) - d_X(y, x_0)$$

что есть ограниченная функция, так как $\forall y \in X : d_X(x, y) - d_X(y, x_0) \leq d_X(x, x_0)$.
Заметим, что это аналогичным образом будет изометрическим вложением:

$$\begin{aligned} d_\infty(d_x - d_{x_0}, d_y - d_{x_0}) &= \sup_z |d_x(z) - d_{x_0}(z) - d_y(z) + d_{x_0}(z)| = \\ &= \sup_z (d_X(x, z) - d_X(z, y)) \leq d_X(x, y) \end{aligned}$$

где равенство достигается при $z = y$.

Любое метрическое пространство (X, d_X) имеет пополнение $(\bar{X}, d_{\bar{X}})$, то есть такое метрическое пространство \bar{X} , что выполнено:

1. $X \subseteq \bar{X}$
2. X — всюду плотно в \bar{X}
3. $d_{\bar{X}}|_X = d_X$, то есть вложение из X в \bar{X} является изометрическим
4. $(\bar{X}, d_{\bar{X}})$ — полно.

Доказательство. Возьмём изометрическое вложение Куратовского $k : X \rightarrow \mathcal{F}(X)$, и возьмём его замыкание в топологическом пространстве $\mathcal{F}(X)$ с топологией, индуцированной метрикой d_∞ — назовём это замыкание \bar{X} . Заметим, что

1. $X \subseteq \bar{X}$ естественным образом
2. X всюду плотно в \bar{X} , так как любое множество всюду плотно в своём замыкании
3. Вложение X в \bar{X} изометрическое, так как оно изометрическое и во всё пространство $\mathcal{F}(x)$
4. \bar{X} полно как замкнутое подмножество полного пространства.

□

Remark 5. Пополнение метрического пространства **единственно** с точностью до изометрии.

Remark 6. Выражение $X \subseteq \bar{X}$ тоже подразумевается с точностью до изометрии.

1.4 Пополнение нормированного поля.

Теперь мы умеем пополнять метрические пространства, но нам никто не гарантирует, что при пополнении поля по норме получится поле.

Definition 7. Пополнением нормированного поля $(F_0, \|\cdot\|_0)$ называется нормированное поле $(F, \|\cdot\|)$, удовлетворяющее следующим свойствам

1. Существует вложение $i : F_0 \hookrightarrow F$, сохраняющее норму (изометрическое), то есть $\|i(x)\| = \|x\|_0$.
2. $(F, \|\cdot\|)$ полно, как метрическое пространство.
3. $i(F_0)$ всюду плотно в F , то есть, $\forall x, \varepsilon > 0 \exists x_0 \in F_0 : \|x - i(x_0)\| < \varepsilon$.

Example 4. Из курса анализа ясно, что $(\mathbb{R}, |\cdot|)$ — пополнение $(\mathbb{Q}, |\cdot|)$.

Theorem 2. Для любого нормированного поля существует пополнение.

Доказательство. Будем рассматривать случай нормы с неравенством треугольника.

Пусть \mathfrak{A} — множество всех последовательностей Коши $\{x_n\}_{n=1}^\infty$ в пространстве $(F_0, \|\cdot\|_0)$.

На \mathfrak{A} можно естественным образом определить операции сложения и умножения (поточечно), а также ввести норму $\|\cdot\|$, как $\|\{x_n\}\| = \lim_{n \rightarrow \infty} \|x_n\|_0$.

Это определение корректно, так как предел всегда существует в силу неравенства треугольника и того, что $\{x_n\}$ — последовательность Коши

$$|\|x_n\|_0 - \|x_m\|_0| \leq \|x_n - x_m\|_0$$

Ясно, что остальные свойства нормы также выполняются.

Введём на \mathfrak{A} отношение эквивалентности \sim :

$$\{x_n\} \sim \{y_n\} \Leftrightarrow \lim_{n \rightarrow \infty} \|x_n - y_n\|_0 = 0$$

Нетрудно заметить, что это отношение эквивалентности «уважает» арифметические действия и норму, то есть

1. $\{x_n\} \sim \{u_n\}, \{y_n\} \sim \{v_n\} \Rightarrow \{x_n + y_n\} \sim \{u_n + v_n\}, \{x_n y_n\} \sim \{u_n v_n\}$.
2. $\{x_n\} \sim \{y_n\} \Rightarrow \|\{x_n\}\| = \|\{y_n\}\|$.

В качестве поля F возьмем фактормножество \mathfrak{A}/\sim . Приведенные выше свойства естественно индуцируют арифметические операции и норму с A на F :

- $[\{x_n\}] + [\{y_n\}] = [\{x_n + y_n\}]$.
- $[\{x_n\}] \cdot [\{y_n\}] = [\{x_n \cdot y_n\}]$.
- $\|[\{x_n\}]\| = \|\{x_n\}\|$.

Аксиомы кольца вполне очевидны, проверим существование обратного по умножению элемента. Если $[\{x_n\}] \neq 0$, то $\lim \|x_n\|_0 > 0 \Rightarrow \forall n \geq n_0 \ \|x_n\|_0 > \delta > 0$ для некоторого δ .

Тогда в качестве $[\{x_n\}]^{-1}$ возьмем класс $[\{y_n\}]$, где

$$y_n = \begin{cases} 0, & n < n_0 \\ \frac{1}{x_n}, & n \geq n_0 \end{cases}$$

Осталось проверить, что мы получили пополнение.

В качестве вложения возьмем $i(x) = [(x, x, \dots)]$. Ясно, что $i(F_0)$ плотно в F , так как, если $X = [\{x_n\}] \in F$, то $i(x_n) \rightarrow X$ в пространстве $(F, \|\cdot\|)$.

Теперь проверим полноту. Пусть $X^{(n)} = [(x_1^{(n)}, x_2^{(n)}, \dots)] \in F$ — последовательность Коши. Возьмем такую последовательность $k_n \in \mathbb{N}$, что

$$\sup_{k, \ell \geq k_n} \|x_k^{(n)} - x_\ell^{(n)}\|_0 < \frac{1}{n}$$

Покажем, что в качестве предела можно взять $X = [\{x_{k_n}^{(n)}\}]$. Пусть $N \geq k_n$, $M \geq k_m$, $K \geq \max\{k_n, k_m\}$.

$$\|x_N^{(n)} - x_M^{(m)}\|_0 \leq \|x_N^{(n)} - x_K^{(n)}\|_0 + \|x_K^{(n)} - x_K^{(m)}\|_0 \leq \frac{1}{n} + \|x_K^{(n)} - x_K^{(m)}\|_0 + \frac{1}{m}$$

Устремим K к бесконечности и получим

$$\|x_N^{(n)} - x_M^{(m)}\|_0 \leq \|X^{(n)} - X^{(m)}\| + \frac{1}{n} + \frac{1}{m}$$

Положим $N = k_n$, $M = k_m$ и получим, что $x_{k_n}^{(n)}$ — последовательность Коши, а её класс эквивалентности — искомый предел. \square

Далее отождествим $i(F_0)$ с F_0 и будем считать, что $F \subseteq F$.

В неархимедовом случае можно сказать даже несколько больше.

Пусть $(F, \|\cdot\|)$ — неархимедово нормированное поле. Если $\{x_n\} \rightarrow x$, $x \in F^*$, то для достаточно больших n $\|x_n\| = \|x\|$.

Lemma 4. Пусть $(F, \|\cdot\|)$ — пополнение неархимедова поля $(F_0, \|\cdot\|_0)$. Тогда

1. $(F, \|\cdot\|)$ неархимедово.
2. $\text{Im}(\|\cdot\|) = \text{Im}(\|\cdot\|_0)$.

2. p -адические числа

2.1 Кольцо целых p -адических чисел.

Прежде чем давать какие-либо определения, рассмотрим следующий мотивирующий пример.

Рассмотрим сравнение $x^2 \equiv 2 \pmod{7^n}$, $n \in \mathbb{N}$. Если $n = 1$, то ясно, что

$$x_0 \equiv \pm 3 \pmod{7}$$

Теперь рассмотрим $n = 2$. $x^2 \equiv 2 \pmod{7^2} \Rightarrow x^2 \equiv 2 \pmod{7}$, а значит, решения сравнения с $n = 2$ надо искать в виде $x_0 + 7t_1$.

Займемся поиском решений вида $x_1 = 3 + 7t_1$. Подставим:

$$(3 + 7t_1)^2 \equiv 2 \pmod{7^2} \Leftrightarrow 9 + 6 \cdot 7t_1 + 7^2 t_1^2 \equiv 2 \pmod{7^2} \Rightarrow 1 + 6t_1 \equiv 0 \pmod{7} \Rightarrow t_1 \equiv 1 \pmod{7}$$

Отсюда имеем решение $x_1 \equiv 3 + 7 \cdot 1 \pmod{7^2}$.

При $n = 3$ мы получим $x_2 = x_1 + 7^2 t_2$ и подставляя

$$(3 + 7 + 7^2 t_2)^2 \equiv 2 \pmod{7^3}$$

мы найдём $t_2 \equiv 2 \pmod{7}$, а значит,

$$x_2 \equiv 3 + 7 \cdot 1 + 7^2 \cdot 2 \pmod{7^3}$$

Продолжая этот процесс, получим последовательность $x_0, x_1, x_2, \dots, x_n, \dots$ со свойствами

$$x_0 \equiv 3 \pmod{7}, \quad x_n \equiv x_{n-1} \pmod{7^n}, \quad x_n^2 \equiv 2 \pmod{7^{n+1}}$$

Процесс построения этой последовательности может напонмнить внимательному читателю процесс вычисления $\sqrt{2}$ при помощи приближения рациональными числами. Там мы тоже строим последовательность рациональных чисел r_1, r_2, \dots, r_n , квадраты которых становятся сколь угодно близки к 2, например, $|r_n^2 - 2| < 1/10^n$.

Если мы зафиксируем простое число p будем считать два целых числа близкими, если их разность делится на достаточно большую степени p (то есть, близкими в смысле p -адической метрики):

$$d_p(x, y) = \|x - y\|_p = p^{-v_p(x-y)}$$

В конкретном примере выше,

$$\forall \varepsilon > 0 \exists N: \forall n \geq N \ d_7(x_n^2, 2) < \varepsilon$$

Как мы помним, задание последовательности рациональных чисел $\{r_n\}$ определяет вещественное число $\sqrt{2}$. Проводя аналогию, здесь мы также можем предположить, что последовательность $\{x_n\}$ определяет некоторое число α совершенно новой природы.

Заметим также, что если у нас есть такая последовательность рациональных чисел $\{r'_n\}$, что $\forall \varepsilon > 0 \exists N: \forall n > N \ |r_n - r'_n| < \varepsilon$, то её пределом также будет $\sqrt{2}$ (и в этом смысле определение корректно). Соответственно, здесь нам также будет естественно предположить, что последовательность $\{x'_n\}$, для которой $x_n \equiv x'_n \pmod{7^{n+1}}$ определяет то же самое число α .

Remark 7. В общем, во всей этой аналогии мы просто заменили метрику на p -адическую.

Definition 8. Пусть p — некоторое простое число. Последовательность целых чисел $\{x_n\}$, обладающих свойством

$$x_n \equiv x_{n-1} \pmod{p^n} \quad \forall n \geq 1$$

определяет новый объект, называемый p -адическим числом. Две последовательности $\{x_n\}$ и $\{x'_n\}$ определяют одно и то же целое p -адическое число, когда $x_n \equiv x'_n \pmod{p^{n+1}} \quad \forall n \geq 0$.

То есть, целые p -адические числа — предел по p -адической норме целых.

Множество всех целых p -адических чисел мы будем обозначать через \mathbb{Z}_p .

Обычные целые числа (не p -адические) будем с этого момента называть целыми рациональными.

Заметим, что каждому целому рациональному числу x можно сопоставить целое p -адическое число, определяемое последовательностью $\{x, x, x, \dots\}$. Такое целое p -адическое число мы будем обозначать той же буквой x . Таким образом, мы получили естественное вложение $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ (инъективность вполне очевидна).

Remark 8. **Канонический способ задания p -адического числа.**

Пусть целое p -адическое число задается последовательностью $\{x_n\}$. Обозначим наименьшее неотрицательное число, сравнимое с x_n по модулю p^{n+1} за $\overline{x_n}$.

$$x_n \equiv \overline{x_n} \pmod{p^{n+1}}, \quad 0 \leq \overline{x_n} < p^{n+1}$$

Ясно, что

$$\overline{x_n} \equiv x_n \equiv x_{n-1} \equiv \overline{x_{n-1}} \pmod{p^n}$$

То есть, последовательность $\{\overline{x_n}\}$ определяют то же целое p -адическое число, что и $\{x_n\}$. Заметим, что если две последовательности $\{\overline{x_n}\}$ и $\{\overline{y_n}\}$ определяют одно и то же целое p -адическое число, то в силу

$$\overline{x_n} \equiv \overline{y_n} \pmod{p^{n+1}}, \quad 0 \leq \overline{x_n} < p^{n+1}, \quad 0 \leq \overline{y_n} < p^{n+1}$$

мы имеем $\overline{x_n} = \overline{y_n}$, то есть, такое представление единственно. Его мы и будем называть каноническим представлением.

Заметим, что $\overline{x^n} \equiv \overline{x_{n-1}} \pmod{p^n}$, а так как $0 \leq \overline{x_n} < p^{n+1}$, вся каноническая последовательность имеет вид

$$\{a_0, a_0 + a_1p, a_0 + a_1p + a_2p^2, \dots\}, \quad 0 \leq a_i < p$$

С другой стороны, ясно, что каждая последовательность такого вида задаёт некоторое целое p -адическое число.

Ясно, что операции сложения и умножения на p -адических числах определяются поточечными операциями с соответствующими последовательностями.

Все свойства операций очевидны, значит, \mathbb{Z}_p — коммутативное кольцо. Поймём что-нибудь про множество обратимых элементов кольца.

Theorem 3. Целое p -адическое число α , определяемое последовательностью $\{x_0, x_1, \dots, x_n, \dots\}$ я тогда и только тогда, когда $x_0 \not\equiv 0 \pmod{p}$.

Доказательство. Пусть $\alpha \in \mathbb{Z}_p^*$. Тогда существует такое целое p -адическое число β , что $\alpha\beta = 1$.

Пусть β определяется последовательностью $\{y_n\}$. Тогда

$$x_n y_n \equiv 1 \pmod{p^{n+1}}$$

В частности, $x_0 y_0 \equiv 1 \pmod{p} \Rightarrow x_0 \not\equiv 0 \pmod{p}$. И обратно, так как $x_0 \not\equiv 0 \pmod{p}$ и $x_n \equiv x_{n-1} \pmod{p^n}$ мы имеем

$$x_n \equiv x_{n-1} \equiv \dots \equiv x_0 \pmod{p} \Rightarrow x_n \not\equiv 0 \pmod{p}$$

Значит, так как p — простое, $\forall n \exists y_n : x_n y_n \equiv 1 \pmod{p^{n+1}}$.

$$x_n \equiv x_{n-1} \pmod{p^n}, x_n y_n \equiv x_{n-1} y_{n-1} \pmod{p^n} \Rightarrow y_n \equiv y_{n-1} \pmod{p^n}$$

а значит, $\{y_n\}$ определяет некоторое целое p -адическое число β .

Таким образом, $\alpha\beta = 1 \Rightarrow \alpha \in \mathbb{Z}_p^*$. □