1. p-адические числа

Абсолютная величина или нормирование.

K - поле. $|| \, || : K \to \mathbf{R}_{\geq 0}$, при этом:
1) $||x|| = 0 \Leftrightarrow x = 0$.
2) $|| \, || : K^* \to \mathbf{R}^*_{>0}$ - гомоморфизм групп.
3) $\forall \, x, y \; ||x+y|| \leq ||x|| + ||y||$ ("неравенство треугольника").

Нормирование называется неархимедовым, если вместо 3) выполнено
3') $\forall \, x, y \quad ||x+y|| \leq \max(||x||, ||y||)$ ("усиленное неравенство треугольника").

p - показатель $\mathrm{v}_p(x)$.

$\mathcal{O}$ - целостное кольцо главных идеалов (и, значит, факториальное). $p \in \mathcal{O}$ неразложимый элемент. $0 \neq x \in \mathcal{O}$.
$\mathrm{v}_p(x) \overset{\text{def}}{=} \max(n \in \mathbf{Z}_{\geq 0}\text{такое,что}p^n \mid x)$. Продолжается до гомоморфизма мультипликативной группы поля частных $K^* \to \mathbf{Z}$ по формуле $\mathrm{v}_p\left(\frac{x}{y}\right) = \mathrm{v}_p(x) - \mathrm{v}_p(y)$

Кольцо нормирования и идеал нормирования.

K - поле, $|| \, ||$ неархимедово нормирование на K.
$\mathcal{O} = \{x \in K \, , ||x|| \leq 1\}$ - целозамкнутое локальное кольцо, $\mathfrak{p} = \{x \in K \, , ||x|| < 1\}$ - максимальный идеал. $\mathfrak{p} \neq (0) \Leftrightarrow || \, ||$ нетривиально. $\mathfrak{p}$ главный $\Leftrightarrow || \, ||$ дискретно (т.е.$||K^*||$- дискретная подгруппа $\mathbf{R}^*$).

Теорема (1.4).

Пусть K - поле, $||||$ неархимедово нормирование и в K выполнено равенство $x = \sum\limits_{i=0}^{n} x_i$.
Тогда если все $||x_i||$ различны, то $||x|| = \max\limits_i ||x_i||$.

Теорема (1.5).

Пусть K поле, $|| \, ||$ нормирование на K, $I \subset K$ - образ стандартного гомоморфизма колец $i : \; \mathbf{Z} \to K$, $1 \overset{i}{\mapsto} 1$. (I - это $\mathbf{Z}$ или $\mathbf{F}_p$, в зависимости от $\mathrm{char}(K)$). Тогда $|| \, ||$ неархимедово $\Leftrightarrow \forall \, x \in I \; ||x|| \leq 1$.
В частности, если $\mathrm{char}(K) \neq 0$, то любое нормирование неархимедово.

Теорема (1.6).

Пусть k - поле, $K = k(T)$ поле рациональных функций от одной переменной над k. Предположим, что $|| \, || : K \to \mathbf{R}_{\geq 0}$ - нетривиальное нормирование, ограничение которого на k тривиально. Тогда $|| \, ||$ неархимедово, дискретно и задается одной из двух формул:

1) $||x|| = s^{-\mathrm{v}_P(x)}$ (где $s \in \mathbf{R}, s > 1, P \in k[T]$ неприводимый полином, $\deg P \geq 1$)
2) $||x|| = s^{\deg(\mathrm{num}(x)) - \deg(\mathrm{den}(x))}$ (где $s \in \mathbf{R}, s > 1$).

Теорема Островского.

Пусть $|| \, ||$ - нетривиальное нормирование на $\mathbf{Q}$. Тогда оно задается одной из двух формул:
1) $||x|| = s^{-\mathrm{v}_p(x)}$ (где $s \in \mathbf{R}, s > 1, p$ просто)
2) $||x|| = |x|^{\alpha}$ (где $\alpha \in \mathbf{R}, 0 < \alpha \leq 1, | \, |$ - обычный модуль).

Формула произведения.

Рассмотрим специальный набор нормирований поля $\mathbf{Q}$, положив $||x||_{\infty} = |x|$ и $||x||_p = p^{-\mathrm{v}_p(x)}$ для всех простых p. Тогда $||x||_{\infty} \prod\limits_p ||x||_p = 1$.

Пополнение поля, снабженного нормированием.

Алгебраические операции и нормирование могут быть продолжены на $\widehat{K}$ по непрерывности. $||\widehat{K}|| = ||K||$, если $|| \;\; ||$ неархимедово.

Эквивалентные нормирования.

$|| \, ||_1 \sim || \, ||_2$ если $|| \, ||_2 = || \, ||_1^t, t > 0$. Нормирования эквивалентны $\Leftrightarrow$ они определяют одинаковую топологию.

Топологическое определение $\mathbf{Q}_p$.

$\mathbf{Q}_p \stackrel{\mathrm{def}}{=}$ пополнение $\mathbf{Q}$ по $p-$адическому нормированию.

Теорема (1.11).

Пусть K -поле, снабженное неархимедовым нормированием. Бесконечный ряд в K сходится $\Leftrightarrow$ общий член стремится к нулю.

Кольцо целых $p-$адических чисел (алгебраическое определение).

$\mathbf{Z}_p \stackrel{\text{def}}{=} \lim\limits_{\leftarrow}\{\mathbf{Z}/(p^i), \phi_i\}$ ($\phi_i : \mathbf{Z}/(p^i) \to \mathbf{Z}/(p^{i-1})$ - гомоморфизм,отвечающий вложению идеалов $p^i\mathbf{Z} \subset p^{i-1}\mathbf{Z}$). Целое $p-$адическое число x есть набор компонент $\{_i x \in \mathbf{Z}/(p^i), 1 \leq i < \infty\}$ таких, что $\forall i > 1$ $\phi_i(_i x) = {}_{i-1}x$.

Сложение и умножение в $\mathbf{Z}_p$ определяются покомпонентно. Единица представлена набором $\{_i 1 = 1 \in \mathbf{Z}/(p^i)\}$.

Свойства $\mathbf{Z}_p$.

Стандартный гомоморфизм $i : \mathbf{Z} \mapsto \mathbf{Z}_p$ - вложение. Проекция $\epsilon_i : \mathbf{Z}_p \mapsto \mathbf{Z}/(p^i)$ сюръективна и имеет ядро $p^i\mathbf{Z}_p$.
$u \in \mathbf{Z}_p$ обратим $\Leftrightarrow$ $_1 u \neq 0 \Leftrightarrow p \nmid u$ in $\mathbf{Z}_p$. Любой элемент $x \in \mathbf{Z}_p$ представляется в виде $x = p^n u$, где $n \in \mathbf{Z}_{\geq 0}$ и $u \in \mathbf{Z}_p^*$ определены однозначно.

Тем самым, $\mathbf{Z}_p$ - целостное дискретно нормированное кольцо (т.е.область главных идеалов с единственным простым идеалом (p)), при этом $\mathrm{v}_p(x) = n$.

Алгебраическое определение $\mathbf{Q}_p$.

$\mathbf{Q}_p \stackrel{\text{def}}{=} \mathbf{Z}_{p(0)}$ - поле частных кольца $\mathbf{Z}_p$.

Функция $\mathrm{v}_p(x)$ продолжается на $\mathbf{Q}_p$ по формуле $\mathrm{v}_p(\frac{x}{y}) = \mathrm{v}_p(x) - \mathrm{v}_p(y)$. Если выбрать $s \in \mathbf{R}, s > 1$, то формула $||0 \neq z||_p \stackrel{\text{def}}{=} s^{-\mathrm{v}_p(z)}$ задает неархимедово дискретное нормирование на пое $\mathbf{Q}_p$.

Теорема (1.16).

Поле $\mathbf{Q}_p$ (алгебраическое определение) полно относительно нормирования, определяемого функцией v_p, и содержит $\mathbf{Q}$ в качестве плотного подполя. Тем самым алгебраическое определение определяет тот же объект, что и топологическое. $\mathbf{Z}_p$ совпадает с кольцом нормирования в $\mathbf{Q}_p$.

Структура группы $\mathbf{Q}_p^*$.

$\mathbf{Q}_p^* = p^{\mathbf{Z}} \times \mathbf{Z}_p^*$.

Группа $\mathbf{Z}_p^*$ профильтрована подгруппами $U_n = \{1 + p^n \mathbf{Z}_p\}, 1 \leq n < \infty$. Проекция $\epsilon_n : \mathbf{Z}_p^* \mapsto (\mathbf{Z}/(p^n))^*$ сюръективна и имеет ядро U_n .

Разложение Тейхмюллера.

Теорема (лемма Гензеля). Пусть $f \in \mathbf{Z}_p[t], n \in \mathbf{Z}_{>0}, x \in \mathbf{Z}_p$ таково,что $\mathrm{v}_p(f'(x)) = 0$ и $f(x) \equiv 0 \bmod p^n$. Тогда $\exists y \in \mathbf{Z}_p$ такое,что
1) $f(y) \equiv 0 \bmod p^{n+1}$
2) $\mathrm{v}_p(f'(y)) = 0$
3) $y \equiv x \bmod p^n$

Теорема (1.19). $\mathbf{Z}_p^* = T \times U_1$, $T \stackrel{\mathrm{def}}{=} \{x \in U$ такие, что $x^{p-1} = 1\}$ - группа порядка $p-1$, изоморфная $(\mathbf{Z}/(p))^*$ (на самом деле, циклическая).

Экспонента.

Пусть $\alpha \in \mathbf{Z}_p$, $\alpha \equiv 1 \mod p$, $z \in \mathbf{Z}_p$ любое. $\exp_\alpha(z)$ (α^z) $= \lim_{i \to \infty} \{\alpha^{\widetilde{_iz}}\}$, где $\widetilde{_iz} \in \mathbf{Z}_{\geq 0}$ таковы,что $\widetilde{_iz} \equiv \ _iz \bmod p^i$. $\exp_\alpha : \mathbf{Z}_p \to \mathbf{Z}_p$ определена корректно (т.е. предел существует и не зависит от выбора $\widetilde{_iz}$) и является гомоморфизмом групп $\mathbf{Z}_p^+ \to U_1$.

Структура группы U_1.

При $p > 2$ и $\alpha \not\equiv 1 \mod p^2$ $\exp_\alpha$ задает изоморфизм $\mathbf{Z}_p^+ \to U_1$.
При $p = 2$ и $\alpha \equiv 5 \mod 8$ $\exp_\alpha$ задает изоморфизм $\mathbf{Z}_p^+ \to U_2$.

При $p = 2$ группа T тривиальна, а $\mathbf{Z}_p^* = U_1 = \{+1, -1\} \times U_2$.

Натуральный логарифм и натуральная экспонента.

log: $U_1 \to \mathbf{Z}_p$ $\log(1+x) \overset{\text{def}}{=} \sum\limits_{i=1}^{\infty}(-1)^{i-1}\frac{x^i}{i}$.

exp: $(p\mathbf{Z}_p \to U_1$ if $p \neq 2$; $p^2\mathbf{Z}_p \to U_2$ if $p = 2)$ $\exp(z) \overset{\text{def}}{=} \sum\limits_{i=0}^{\infty} \frac{z^i}{i!}$.

При $p \neq 2$ $U_1 \overset{\log}{\cong} p\mathbf{Z}_p$. При $p = 2$ $U_2 \overset{\log}{\cong} p^2\mathbf{Z}_p$.