Лекция 6. p-адические числа

На предыдущей лекции основную роль играли связные пространства. Сейчас мы разберем важные примеры пространств, свойства которых в некотором отношении противоположны свойствам $\mathbb{R}$ и прочих связных пространств.

Определение 6.1. Топологическое пространство называется *вполне несвязным*, если оно не имеет связных подмножеств, за исключением состоящих из одной точки.

Разумеется, вполне несвязным будет всякое дискретное пространство, но существует много менее тривиальных примеров. Например, волне несвязным, но недискретным, будет множество $\mathbb{Q}$ рациональных чисел (с топологией, индуцированной с $\mathbb{R}$): в самом деле,оно не содержит ни одного интервала (см. предложение 5.7).

Сейчас мы приведем пример играющего важную роль во многих вопросах недискретного вполне несвязного компактного хаусдорфова пространства.

Зафиксируем раз и навсегда простое число p.

При записи натуральных чисел в p-ичной системе счисления каждое число представляется в виде конечной последовательности p-ичных цифр (целых чисел от нуля до $p-1$). Давайте разрешим этим последовательностям быть бесконечными.

Определение 6.2. *Целым p-адическим числом* называется бесконечная последовательность $\{a_0, a_1, \ldots\}$, в которой все a_i — p-ичные цифры. Множество целых p-адических чисел обозначается $\mathbb{Z}_p$.

Будем представлять себе последовательности цифр, о которых идет речь в этом определении, записанными в виде «бесконечной влево» последовательности: a_0, слева от него — a_1, еще левее — a_2, и т. д. Тогда каждое натуральное число можно тоже рассматривать как целое p-адическое, если записать его в p-ичной системе счисления, а затем дополнить слева бесконечным «хвостом» из нулей. Тем самым определяется вложение $\mathbb{N}$ в $\mathbb{Z}_p$. Например, число 39 как элемент $\mathbb{Z}_5$ запишется так: $\ldots 000124$.

Над целыми p-адическими числами можно проделывать те же алгебраические операции, что и над целыми числами:

Определение 6.3. *Суммой* (соотв. разностью, произведением) целых p-адических чисел $(a_0, a_1, \ldots)$ и $(b_0, b_1, \ldots)$ называется целое p-адическое число, получаемое из них по правилам сложения (соотв. вычитания, умножения) «в столбик» в p-ичной системе счисления, если записать два числа одно под другим (b_0 под a_0, b_1 под a_1, и т. д.).

Отметим, что вычитание всегда выполнимо, поскольку ввиду «бесконечности влево» наших p-ичных записей всегда можно «занять единицу» в следующем разряде; умножение всегда выполнимо, так как для нахождения каждой цифры необходимо только конечное число сложений.

Покажем, что сложение, вычитание и умножение целых p-адических чисел обладает теми же свойствами (коммутативность, ассоциативность, дистрибутивность...), что и у обычных целых чисел. В самом деле, если m — натуральное число и $a \in \mathbb{Z}_p$, то обозначим через $(a)_m \in \mathbb{Z}$ целое число, записываемое в p-ичной системе в виде $\overline{a_{m-1} \dots a_1 a_0}$ (т. е. образованное m младшими разрядами). Тогда из определения действий над p-адическими числами сразу следует, что m младших разрядов у $(a \pm b)_m$ и $(ab)_m$ такие же, как m младших разрядов у $(a)_m \pm (b)_m$ и $(a)_m(b)_m$ соответственно. Поэтому, например, $(a+b)c = ac+bc$, так как для всякого m у левой и правой частей совпадают m младших разрядов (поскольку умножение обычных целых чисел дистрибутивно). Поскольку это же рассуждение показывает, что вычитание p-адических чисел обратно сложению, получаем, что целые p-адические числа образуют кольцо.

Поскольку натуральные числа вкладываются в $\mathbb{Z}_p$, а целые p-адические числа можно вычитать, целые числа (т. е. разности натуральных) также вкладываются в $\mathbb{Z}_p$ как подкольцо; например, число -1 как элемент $\mathbb{Z}_5$ записывается в виде $\dots 4444$.

Отметим еще, что умножение на p сводится к приписыванию нуля справа, так что целое p-адическое число делится на p тогда и только тогда, когда его «последняя» (т. е. крайняя правая) цифра есть нуль.

Теперь введем на $\mathbb{Z}_p$ структуру метрического пространства.

Определение 6.4. Если $a \in \mathbb{Z}_p$ отлично от нуля, то его *p-адической нормой* называется число p^{-n}, где n — наибольшее натуральное n, для которого a делится на p^n. p-адическая норма числа a обозначается $|a|_p$. Если $a = 0$, полагают $|a|_p = 0$.

Определение 6.5. *p-адическим расстоянием* между числами $a, b \in \mathbb{Z}_p$ называется число $|a-b|_p$.

Множество $\mathbb{Z}_p$, снабженное p-адическим расстоянием, является метрическим пространством. В самом деле, условия (1) и (2) из определения 1.6 выполняются с очевидностью; поскольку $|x-z|_p = |(x-y)+(y-z)|_p$, для проверки неравенства треугольника достаточно убедиться в выполнимости неравенства $|a+b|_p \leqslant |a|_p + |b|_p$. Верно даже более сильное утверждение:

Предложение 6.6. *Для любых $a, b \in \mathbb{Z}_p$ выполнено неравенство*

$$|a+b|_p \leqslant \max(|a|_p, |b|_p). \tag{6.1}$$

Доказательство. Если число a оканчивается на s нулей, а число b — на t нулей, то число $a+b$ оканчивается не менее чем на $\min(s,t)$ нулей, так что $|a+b|_p \leqslant p^{-\min(s,t)}$. □

Неравенство (6.1) называется *ультраметрическим неравенством.*

Неформально говоря, в p-адической метрике число тем «меньше» (ближе к нулю), чем на большую степень p оно делится. В частности, $\lim_{n\to\infty} p^n = 0$.

Заметим, что, поскольку расстояния между точками в $\mathbb{Z}_p$ могут принимать только значения p^{-n}, где n — целое неотрицательное число, все открытые шары в этом метрическом пространстве суть шары радиуса p^{-n}. Далее, открытый шар с центром a и радиусом p^{-n} есть не что иное, как множество чисел, у которых n младших разрядов такие же, как у числа a, т. е «класс вычетов по модулю p^n»: множество чисел $b \in \mathbb{Z}_p$, для которых $b-a$ делится на p^n. В частности, всякий открытый шар имеет мощность континуум, откуда следует, что в $\mathbb{Z}_p$ нет изолированных точек.

Предложение 6.7. *Пространство $\mathbb{Z}_p$ компактно.*

Доказательство. Так как $\mathbb{Z}_p$ — метрическое пространство, достаточно показать, что из всякой последовательности можно выбрать сходящуюся подпоследовательность. Пусть $\{x_n\}$ — последовательность элементов $\mathbb{Z}_p$. Поскольку младший разряд чисел x_n может принимать не более p значений, какая-то из p-ичных цифр (обозначим ее a_0) является младшим разрядом бесконечного количества членов последовательности; обозначим через y_0 первый из членов последовательности, обладающий этим свойством, и удалим из последовательности все члены, младший разряд которых отличен от a_0. Далее, среди оставшихся членов последовательности есть бесконечно много таких, у которых вторая справа цифра одна и та же (обозначим ее a_1); обозначим через y_1 какой-нибудь член последовательности, обладающий этим свойством и идущий позднее, чем y_0, и удалим из последовательности все те члены, у которых вторая справа цифра отлична от a_1. Продолжая по индукции, получим подпоследовательность $y_0, y_1, \ldots$ и p-адическое число $a = \overline{\ldots a_2 a_1 a_0}$. Поскольку по построению $|y_n - a|_p \leqslant p^{-n-1}$, имеем $\lim_{n\to\infty} y_n = a$. $\square$

Поскольку метрическое пространство $\mathbb{Z}_p$ компактно, оно является полным (следствие 5.15). На самом деле в $\mathbb{Z}_p$ верен более сильный критерий сходимости, чем критерий Коши:

Предложение 6.8. *Последовательность $\{x_n\}$ в $\mathbb{Z}_p$ сходится тогда и только тогда, когда $\lim\limits_{n\to\infty}(x_{n+1} - x_n) = 0$.*

Доказательство. Часть «только тогда» очевидна: если $\lim\limits_{n\to\infty} x_n = x$, то и $\lim\limits_{n\to\infty} x_{n+1} = x$, откуда $\lim\limits_{n\to\infty}(x_{n+1} - x_n) = 0$.

Для доказательства части «тогда» заметим, что $\mathbb{Z}_p$ полно ввиду следствия 5.15, так что достаточно показать, что всякая последовательность $\{x_n\}$, удовлетворяющая условиям предложения, является фундаментальной. И действительно, из ультраметрического неравенства (6.1), которое очевидным образом распространяется на любое количество слагаемых, вытекает, что

$$|x_m - x_n|_p = |(x_m - x_{m-1}) + (x_{m-1} - x_{m-2}) + \ldots + (x_{n+1} - x_n)|_p \leqslant \\ \leqslant \max(|x_m - x_{m-1}|_p, \ldots, |x_{n+1} - x_n|_p),$$

причем из условия вытекает, что правая часть стремится к нулю при $m, n \to \infty$. $\square$

Для действительных чисел предложение 6.8, как известно, места не имеет.

Предложение 6.9. *Замыкание подмножества $\mathbb{Z} \subset \mathbb{Z}_p$ совпадает со всем $\mathbb{Z}_p$.*

Доказательство. Пусть $x \in \mathbb{Z}_p$; обозначим через x_n целое число, чья p-ичная запись совпадает с n «последними» (или, если угодно, n первыми, считая справа) цифрами записи числа x. Тогда $x - x_n$ делится на p^n, то есть $|x - x_n|_p \leqslant p^{-n}$, откуда $\lim_{n\to\infty} x_n = x$. $\square$

Из доказанного предложения следует, что $\mathbb{Z}_p$ является пополнением $\mathbb{Z}$ относительно p-адической метрики.

Покажем, наконец, что $\mathbb{Z}_p$ вполне несвязно. Для этого, очевидно, достаточно установить, что если $a \neq b$ — два элемента $\mathbb{Z}_p$, то существуют такие непересекающиеся открытые подмножества $U, V \subset \mathbb{Z}_p$, что $U \ni a$, $V \ni b$ и $U \cap V = \varnothing$. И действительно, если младшие n разрядов у p-адического числа a не такие же, как у b, то в качестве U можно взять класс вычетов числа a по модулю p^n, а в качестве V — объединение классов вычетов по модулю p^n всех p-адических чисел, не входящих в U.

Легко видеть, что в кольце $\mathbb{Z}_p$ нет делителей нуля (рассмотрите первую справа ненулевую цифру в двух сомножителях; это первое место, где используется простота числа p). Поэтому можно перейти от $\mathbb{Z}_p$ к его полю частных (т.е. добавить всевозможные[2] отношения m/n, где $m, n \in \mathbb{Z}_p$ и $n \neq 0$; отношения m/n и m'/n' считаются равными, если $mn' = nm'$); при этом получится *поле p-адических чисел*, обозначаемое $\mathbb{Q}_p$. Сложение, вычитание, умножение и деление p-адических чисел определяется по обычным правилам действий с дробями. Поле $\mathbb{Q}_p$ является пополнением $\mathbb{Q}$ относительно p-адической метрики (определение: для ненулевого $a \in \mathbb{Q}$ полагают $|a|_p = p^{-n}$, если a можно представить в виде $p^n(s/t)$, где числа s и t являются целыми и взаимно простыми с p; расстоянием между рациональными числами a и b называют число $|a-b|_p$).

[2] На самом деле достаточно ограничиться отношениями вида m/p^k, где $k \in \mathbb{N}$: нетрудно показать (см. упражнения), что для всякого $n \in \mathbb{Z}_p$, не делящегося на p, существует такое $n_1 \in \mathbb{Z}_p$, что $nn_1 = 1$.