Лекция 6. Кольца дискретного нормирования.

Определение. Пусть K — поле. Тогда функция $v : K \to \mathbb{Z} \cup \infty$ называется *дискретным нормированием*, если

(i) $v : K^* \to \mathbb{Z}$ сюръективный гомоморфизм групп,

(ii) $v(0) = \infty$,

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$.

Примеры.

(а) K — поле частных кольца $\mathcal{O}_{\mathbb{A}^1,0}$, являющегося локальным кольцом на аффинной прямой $\mathbb{A}^1$ в точке $0 \in \mathbb{A}^1$, то есть поле рациональных функций от одной переменной. $v(P(T))$ равно порядку нуля у многочлена $P(T)$ в $0 \in \mathbb{A}^1$, то есть кратности T в $P(T)$, $v(\frac{P(T)}{Q(T)}) = v(P(T)) - v(Q(T))$.

(б) K — поле частных кольца $\mathbb{Z}_{(p)}$, являющегося локальным кольцом на спектре $\mathrm{Spec}\mathbb{Z}$ в точке (p) (p — простое число), то есть $K = \mathbb{Q}$. $v_p(m)$ равно кратности, с которой p делит целое число m, $v(\frac{m}{n}) = v(m) - v(n)$.

Утверждение 6.1. Подмножество $R = \{x \in K | v(x) \geq 0\}$ в дискретно нормированном поле K является подкольцом. Оно локально с максимальным идеалом $\mathfrak{m} = \{x \in K | v(x) > 0\}$.

Доказательство. То, что R — кольцо проверяется непосредственно, используя свойства дискретного нормирования. Оно локальное из-за того, что $x \in R$ обратим в кольце R тогда и только тогда, когда $v(x) = 0$.

Так получающиеся кольца называются *дискретно нормированными кольцами* (ДНК).

Замечания.

(а) Пусть $x, y \in R$. В таком случае $x|y$ тогда и только тогда, когда $v(x) \leq v(y)$.

(б) Пусть $\pi \in R$ — произвольный элемент, для которого $v(\pi) = 1$ (такие элементы называются *униформизующими*). Тогда для любого $x \in R$ выполняется $x = \pi^{v(x)}u$, где $v(u) = 0$, $u \in R$ — обратимый элемент.

(в) R — факториальное кольцо. Разложение на неприводимые множители описано в (б).

Из всего этого вытекает следующее

Утверждение 6.2. Пусть $I \subset R$ — идеал. Тогда существует такое натуральное n, что $I = (\pi^n) = \mathfrak{m}^n$, где π — некоторый униформизующий.

Доказательство. Для идеала I рассмотрим $x \in I$ такой, что $v(x) = \min_{y \in I} v(y)$. Тогда $I = (x) = (\pi^{v(x)})$.

Обозначим через k поле $R/\mathfrak{m}$.

Утверждение 6.3. Для каждого натурального n существует изоморфизм $k \cong \mathfrak{m}^n/\mathfrak{m}^{n+1}$.

Доказательство. Пусть $\pi \in R$ — униформизующий. Тогда умножение на π^n индуцирует изоморфизм $k \to \mathfrak{m}^n/\mathfrak{m}^{n+1}$.

Следствие. Для кольца R, являющегося ДНК, $\dim R = 1$, $\operatorname{Spec} R$ гладкий (все точки гладкие), причем $\operatorname{Spec} R$ состоит из двух точек: общей, соответствующей нулевому идеалу, и замкнутой, соответствующей идеалу $\mathfrak{m}$. Поэтому $\operatorname{Spec} R$ иногда называют *стрелкой.*

Доказательство следующего утверждения хотя несложное, но довольно длинное и использующее технику из коммутативной алгебры.

Утверждение 6.4. Кольцо R является ДНК тогда и только тогда, когда оно нетерово, целозамкнуто и содержит ровно один ненулевой простой идеал.

Заметим, что в одну сторону утверждение следует из всего вышесказанного про ДНК и из упражнения 6.0.

В отличие от предыдущего, следующее утверждение из коммутативной алгебры является действительно довольно сложным.

Утверждение 6.5. Локальное регулярное кольцо R (то есть такое, для которого $\dim R = \dim_{(R/\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2$, где $\mathfrak{m} \subset R$ максимальный идеал) факториально.

Вот еще один факт из коммутативной алгебры:

Утверждение 6.6. Целостное кольцо R является целозамкнутым тогда и только тогда, когда целозамкнуты все его локализации $R_\mathfrak{p}$ в простых идеалах $\mathfrak{p} \subset R$.

Замечание. Два лучших способа ознакомится с коммутативной алгеброй заключаются либо в прочтении книги Атьи и Макдональда "Введение в коммутативную алгебру", либо посещение периодически повторяющегося на мех-мате одноименного курса Евгения Соломоновича Голода.

Объединяя вместе утверждения 6.4, 6.5 и 6.6, получаем

Следствие. Пусть $\dim R = 1$, кольцо R нетерово. Тогда $\operatorname{Spec} R$ гладкий тогда и только тогда, когда $\operatorname{Spec} R$ нормален.

Определение. Нетерово одномерное целозамкнутое кольцо называется *дедекиндовым.*

Об их важных арифметических свойствах будет рассказано через одну лекцию.

Примеры.

(а) Пусть C — неприводимая алгебраическая кривая (то есть аффинное многообразие размерности 1). Тогда можно рассмотреть кольцо R, являющееся целым замыканием $k[C]$ в $k(C)$. Оно будет обладающим тем же полем частных $k(C)$, что и $k[C]$, а также будет целозамкнутым (композиция целых расширений — целое). Можно показать, что R будет конечно порожденной алгеброй над k. Значит, $R = k[\tilde{C}]$ для некоторой гладкой кривой $\tilde{C}$, конечно бирационально отображающейся на C. Таким образом, мы получили, что у каждой кривой существует *разрешение особенностей.* Заметим, что если C уже была гладкой, то $\tilde{C} = C$. Мы уже строили разрешения особенностей для нода и каспа.

(б) Пусть $\mathcal{O}_K$ — целое замыкание $\mathbb{Z}$ в конечном расширении $K \supset \mathbb{Q}$. Тогда $\varphi : \mathrm{Spec}\mathcal{O}_K \to \mathrm{Spec}\mathbb{Z}$ — конечный морфизм.

Утверждение. При конечных морфизмах размерность сохраняется (сравните с теоремой о размерности слоев).

Значит, $\dim\mathcal{O}_K = 1$ и φ — конечный морфизм гладких спектров.

Выразим теперь алгебраически ту мысль из матанализа, что аналитические функции, у которых совпадает большой начальный кусок их рядов Тейлора, мало отличаются.

Пусть K — дискретно нормированное поле. Расмотрим функцию $|\cdot| : K \to \mathbb{R}$, $|x| = \alpha^{-v(x)}$, где α — произвольное вещественное число, строго большее единицы. Она удовлетворяет следующим свойствам:

(i) $|xy| = |x||y|$,

(ii) $|x| = 0 \Leftrightarrow x = 0$,

(iii) $|x + y| \leq |x| + |y|$ (ибо $|x + y| \leq \max\{|x|, |y|\}$).

Определение. Пусть K поле. Функция $|\cdot| : K \to \mathbb{R}$, удовлетворяющая свойствам (i), (ii) и (iii), назывется *нормированием.* Если вместо (iii) она удовлетворяет более сильному свойству $|x + y| \leq \max\{|x|, |y|\}$, то она называется *неархимедовым нормированием.* Иначе нормирование называется *архимедовым.*

На поле с нормированием можно задать метрику $\rho(x, y) = |x-y|$, определяющую, в свою очередь, топологию (проверьте, что ρ — действительно метрика!).

Примеры.

(а) K — дискретно нормированное поле, $|\cdot| = \alpha^{-v(\cdot)}$ — неархимедово нормирование.

(б) $K = \mathbb{Q}$, $|\cdot|$ — обычное абсолютное значение числа. Это архимедово нормирование. $|\cdot|_p = p^{-v_p(\cdot)}$ — так называемое p-адическое нормирование. Оно неархимедово.

(в) K — поле рациональных функций от одной переменной, $|\cdot| = \alpha^{-v(\cdot)}$, где $v(\cdot)$ — дискретное нормирование, определяемое порядком нуля (полюса) в $0 \in \mathbb{A}^1$. Тогда $\rho(f,g)$ мало тогда, и только тогда, когда $v(f-g)$ велико, то есть когда у разложения f и g в ряд Тейлора (Лорана) в начале совпадает длинный кусок.

Заметим, что если $|\cdot|$ нормирование некоторого поля K, а β положительное вещественное число, то $|\cdot|^\beta$ — тоже нормирование, причем определяющее эквивалентную топологию на K. Такие нормирования, по определению, считаются *эквивалентными*.

Утверждение 6.7.(Теорема Остроградского) С точностью до эквивалентности, на $\mathbb{Q}$ существуют лишь следующие нормирования (попарно неэквивалентные):

(i) абсолютное значение числа,

(ii) p-адические нормирования, определяемые простыми числами p.

Напомним следующие понятия из анализа.

Определение. Метрическое пространство *полное*, если любая последовательность Коши имеет в нем предел.

Определение. *Пополнением* метрического пространства (M,ρ) называется полное метрическое пространство $(\overline{M},\overline{\rho})$, для которого существует изометричное (то есть сохраняющее метрику) вложение $i : M \hookrightarrow \overline{M}$ с плотным в $\overline{M}$ образом.

Теорема. Для любого метрического пространства существует и единственно пополнение.

Например, $\mathbb{R}$ является пополнением $\mathbb{Q}$ в обычной метрике, индуцированной $|\cdot|$. При этом именно из- за полноты $\mathbb{R}$ в нем удается извлекать корень из любого положительного числа, и, как следствие, раскладывать любой многочлен на линейные и квадратичные неприводимые сомножители. Таким образом, такое топологическое свойство, как полнота, существенно упрощает арифметику.

Поэтому разумно рассмотреть пополнения $\mathbb{Q}$ и в других метриках, построенных по p-адическим нормированиям.

Теорема 6.8. Пополнение дискретно нормированного кольца R изоморфно, как кольцо, проективному (обратному) пределу $\hat{R} = \varprojlim R/\mathfrak{m}^i$, где $\mathfrak{m} \subset R$ — единственный максимальный идеал.

Доказательство. Напомним, что по определению обратного предела, каждый элемент $f \in \hat{R}$ является согласованной системой остатков $f_i \in R/\mathfrak{m}^i$, перетекающих друг в друга под действием гомоморфизмов $R/\mathfrak{m}^i \to R/\mathfrak{m}^j$ при $i > j$.

Из упражнения 5.4(б) следует, что естественное отображение $R \to \hat{R}$ является вложением.

Рассмотрим функцию $\hat{v} : \hat{R} \to \mathbb{Z}$, $\hat{v}(f) = \max\{i | f_i = 0\}$ (если все f_i ненулевые, то $\hat{v}(f) = 0$). Легко видеть, что это является дискретным нормированием на $\hat{R}$, продолженным с R.

Докажем теперь, что $\hat{R}$ полно относительно метрики, индуцированной $\hat{v}$. Действительно, пусть $\{x_i\}$ — последовательность Коши в $\hat{R}$. Тогда $\{\forall \varepsilon \exists n | \forall m \geq n \ |x_m - x_n| < \varepsilon\}$. Это значит, что $\{\forall k \exists n | \forall m \geq n \ \hat{v}(x_m - x_n) > k\}$, то есть начиная с некоторого момента n последовательность остатков в $R/\mathfrak{m}^k$, индуцированная $\{x_i\}$, постоянна. Обозначим через f_k остаток $(x_n)_k \in R/\mathfrak{m}^k$. Тогда система остатков f_k согласованна и определяет элемент $f \in \hat{R}$, к которому и сходится последовательность $\{x_i\}$.

Нам осталось доказать, что $R \subset \hat{R}$ плотно. Возьмем произвольный элемент $f \in \hat{R}$. Пусть $y_i \in R$ такой, что $\overline{y_i} = f_i$ в $R/\mathfrak{m}^i$. Тогда нетрудно видеть, что $\lim\limits_{i \to \infty} y_i = f$. Теорема доказана.

Итак, $\hat{R}$ — тоже ДНК, причем его максимальный идеал $\hat{\mathfrak{m}}$ порожден образом $\mathfrak{m}$ при вложении $R \hookrightarrow \hat{R}$, и $\hat{R}/(\hat{\mathfrak{m}})^n \cong R/\mathfrak{m}^n$ (проверьте это!).

Заметим один забавный факт: в полном ДНК ряд $\sum\limits_{i=1}^{\infty} x_i$ сходится тогда и только тогда, когда $|x_i| \to 0$ (это является непосредственным следствием неархимедовости нормирования $|\cdot|$).

Для явного вычисления пополнений нам понадобится следующая

Лемма. Пусть $\mathfrak{m} \subset R$ — максимальный идеал в некотором кольце R. Тогда $R/\mathfrak{m}^n \cong R_\mathfrak{m}/\mathfrak{m}_\mathfrak{m}^n$, где $\mathfrak{m}_\mathfrak{m}$ обозначает максимальный идеал в локальном кольце $R_\mathfrak{m}$ (порожденный образом $\mathfrak{m}$).

Доказательство. Суть утверждения заключается в том, что естественный гомоморфизм $R/\mathfrak{m}^n \to R_\mathfrak{m}/\mathfrak{m}_\mathfrak{m}^n$ является сюръективным. Пусть $\frac{a}{b} \in R_\mathfrak{m}$. Тогда $(b) + \mathfrak{m} = R$ (так как идеал $\mathfrak{m}$ максимальный) и $(b) + \mathfrak{m}^n = R$ (надо возвести предыдущее тождество для идеалов в n-ую степень). Значит, существует $c \in R$, $m \in \mathfrak{m}^n$ такие, что $bc + m = 1$. Тогда $b(ac) + (am) = a$, $ac \in R$ и $\frac{a}{b} \in R_\mathfrak{m}$ имеют одинаковые остатки в $R_\mathfrak{m}/\mathfrak{m}_\mathfrak{m}^n$.

Примеры.

(а) Пусть $R = \mathbb{Z}$, $\mathfrak{m} = (p)$. Тогда $\varprojlim(\mathbb{Z}_{(p)}/(p)_{(p)}^n) \cong \varprojlim \mathbb{Z}/(p^n) = \mathbb{Z}_p$ — целые p-адические числа.

(б) Пусть $R = k[T]$, $\mathfrak{m} = (T)$. Тогда $\varprojlim(\mathcal{O}_{\mathbb{A}^1,0}/(T)^n) \cong \varprojlim k[T]/(T^n) = k[[T]]$ — кольцо формальных степенных рядов.

В обоих случаях R (а не только $R_\mathfrak{m}$) плотно в соответствующих полных ДНК.

Заметим, что $k[[T]] = \{a_0 + a_1T + a_2T^2 + \ldots + a_nT^n + \ldots\}$, где $a_i \in k$. Аналогичное представление возможно и для произвольного полного ДНК R. Для этого надо выбрать униформизующий π, а так же по представителю $u_\alpha \in R$ из каждого класса смежности $\alpha \in R/\mathfrak{m}$. Тогда можно разложить произвольный элемент $f \in R$ в сходящийся к нему ряд $a_0+a_1\pi+a_2\pi^2+\ldots+a_n\pi^n+\ldots$ с коэффициентами из множества представителей $\{u_\alpha\}$. Это делается следующим образом. Пусть $\alpha_0 = f(\mathrm{mod}\mathfrak{m})$, $a_0 = u_{\alpha_0}$, $\alpha_1 = (f - a_0)/\pi(\mathrm{mod}\mathfrak{m})$, $a_1 = u_{\alpha_1}$, $\alpha_2 = (f - a_0 - a_1\pi)/\pi^2(\mathrm{mod}\mathfrak{m})$, $a_2 = u_{\alpha_2}$, и т.д.

Например, в случае $\mathbb{Z}_p$ разумно выбрать в качестве униформизующего само p, а в качестве множества представителей в $\mathbb{Z}_p/(p) = \mathbb{Z}_{(p)}/(p) = \mathbb{Z}/(p) = \mathbb{F}_p$ целые числа $\{0, 1, 2, \ldots, p-1\}$. В таком случае, $\mathbb{Z}_p = \{a_0+a_1p+a_2p^2+\ldots+a_np^n+\ldots\}$, где $a_i \in \mathbb{Z}, 0 \le a_i \le p-1$.

Относительно пополнения полей частных ДНК сформулируем следующее утверждение:

Утверждение 6.9. Поле частных $\hat{K}$ пополнения $\hat{R}$ дискретно нормированного кольца R является пополнением его поля частных K.

Доказательство. Заметим, что $|\cdot|$ является непрерывной функцией на $\hat{K}$ (проверьте это!). Значит, если последовательность $\{x_i\} \subset \hat{K}$ фундаментальна, то последовательность нормирований $\{|x_i|\} \subset \mathbb{R}$ тоже фундаментальна, то есть сходящаяся. В частности, она ограничена сверху, а последовательность дискретных нормирований ограничена снизу. Значит, существует такое $n \in \mathbb{N}$, что последовательность $\{\pi^n x_i\}$ лежит в колце $\hat{R}$, где она сходится (π — униформизующий). Отсюда, деля на π^n, получаем предел исходной последовательности. То, что K плотно в $\hat{K}$ следует непосредственно из равенства $\frac{\lim x_i}{\lim y_i} = \lim \frac{x_i}{y_i}$.

Определение. *Локальным полем* называется поле частных полного ДНК.

Покажем теперь, как полнота влияет на арифметику. Основным утверждением в этом направлении является

Утверждение 6.10.(Лемма Гензеля) Пусть R — полное ДНК, $f \in R[T]$. Пусть существует $\alpha_0 \in R$, для которого $|f(\alpha_0)| < 1$, $\left|\frac{f(\alpha_0)}{(f'(\alpha_0))^2}\right| < 1$. Тогда существует $\alpha \in R$ такой, что $f(\alpha) = 0$ и $|\alpha - \alpha_0| < 1$.

Доказательство. Обозначим $c = \left|\frac{f(\alpha_0)}{(f'(\alpha_0))^2}\right| < 1$. Рассмотрим рекурсивно определяемую последовательность $\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$. Докажем для нее по индукции следующие свойства:

(i) $|\alpha_i| \le 1$

(ii) $|\alpha_i - \alpha_0| \leq c$

(iii) $\left|\frac{f(\alpha_i)}{(f'(\alpha_i))^2}\right| \leq c^{2^i}$

База заложена в условии. Докажем переход от i к $i+1$.

(i) Из (iii) для i и из неравенства $\left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right| \leq \left|\frac{f(\alpha_i)}{(f'(\alpha_i))^2}\right|$ следует, что $|\alpha_i - \alpha_{i+1}| \leq c^{2^i} < 1$. Из этого неравенства и из неархимедовости нормы имеем $|\alpha_{i+1}| \leq 1$.

(ii) Очевидно следует из неархимедовости нормы и из равнства $\alpha_{i+1} - \alpha_0 = (\alpha_{i+1} - \alpha_i) + (\alpha_i - \alpha_0)$.

(iii) Из разложения в ряды Тейлора многочленов f и f' имеем:

$$f(\alpha_{i+1}) = f(\alpha_i) - f'(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)} + \beta\left(\frac{f(\alpha_i)}{f'(\alpha_i)}\right)^2 = \beta\left(\frac{f(\alpha_i)}{f'(\alpha_i)}\right)^2,$$

$$f'(\alpha_{i+1}) = f'(\alpha_i) + \gamma\frac{f(\alpha_i)}{f'(\alpha_i)},$$

где $\beta, \gamma \in R$.

Так как $|f'(\alpha_i)| > \left|\gamma\frac{f(\alpha_i)}{f'(\alpha_i)}\right|$, то $|f'(\alpha_{i+1})| = |f'(\alpha_i)|$.

Значит, $\left|\frac{f(\alpha_{i+1})}{(f'(\alpha_{i+1}))^2}\right| \leq |\beta|\left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|^2\frac{1}{|f'(\alpha_i)|^2} \leq c^{2^{i+1}}$.

Из только что доказанных свойств (i) (ii) и (iii) следует, что последовательность $\{\alpha_i\}$ является фундаментальной, а ее предел удовлетворяет требованиям на α из условия утверждения.

Замечание. Той же самой формулой (и с похожими условиями на значение и производную в начальной точке) задается метод касательных Ньютона, используемый для нахождения вещественных нулей вещественных функций.

Более слабый (и чаще встречаемый) вариант условия леммы Гензеля звучит так:

Утверждение 6.11. Пусть R — полное ДНК, $f \in R[T]$. Пусть $\overline{\alpha} \in k = R/\mathfrak{m}$ является корнем редуцированного многочлена $\overline{f} \in k[T]$, причем $\overline{f}'(\overline{\alpha}) \neq 0$. Тогда существует поднятие данного корня до R, то есть существует $\alpha \in R$, редуцирующийся в $\overline{\alpha}$, и такой, что $f(\alpha) = 0$.

Изучим теперь мультипликативную группу K^* локального поля K. Дискретное нормирование и выбор униформизующего π определяют (неканоническое) разложение $K^* \cong \mathbb{Z} \times R^*$. Пусть поле вычетов конечно: $R/\mathfrak{m} = k = \mathbb{F}_{p^r} = \mathbb{F}_q$. Тогда по лемме Гензеля мы можем поднять корни уравнения $T^q - T = 0$ из поля k до кольца R (производная редуцированного многочлена тождественно равна -1). Так мы канонически получаем систему представителей (для разложения с коэффициентами в ней по степеням униформизующего), а кроме того вкладываем группу k^* в R^*. Значит, $K^* \cong \mathbb{Z} \times R^* \cong \mathbb{Z} \times \mathbb{F}_q^* \times U^1$, где $U^1 = \{x \in R | x \equiv 1(\mathrm{mod}\mathfrak{m})\}$. Из существования в случае $\mathrm{char}k = p \neq 2$ взаимно отбратных отображений $\exp : \pi R \to U^1$ и $\ln : U^1 \to \pi R$, получаем $R^+ \cong \pi R \cong U^1$ и $K^* \cong \mathbb{Z} \times \mathbb{F}_q^* \times R^+$. В случае $\mathrm{char}k = 2$ имеем изоморфизм $R^+ \cong \pi^2 R \cong U^2$, где $U^2 = \{x \in R | x \equiv 1(\mathrm{mod}\mathfrak{m}^2)\}$. Поэтому нам надо поднимать в R^* группу $(R/\mathfrak{m}^2)^*$. В случае 2-адических чисел это сделать просто: $\mathbb{Z}/4\mathbb{Z} \cong \{1, -1\} \subset \mathbb{Z}_2^*$, $\mathbb{Q}_2^* \cong \mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^* \times \mathbb{Z}_2^+$.