4. Лекция 4. Формальные степенные ряды и производящие функции.

4.1. **Формальные степенные ряды.** Пусть R – коммутативное кольцо с единицей.

Определение 4.1. Кольцо формальных степенных рядов с коэффициентами в R это множество

$$R[[x]] := \{\sum_{n\geq 0} a_n x^n \mid a_i \in R\}$$

с операциями

$$\sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} b_n x^n := \sum_{n\geq 0} (a_n + b_n) x^n;$$

$$\left(\sum_{n\geq 0} a_n x^n\right) \cdot \left(\sum_{n\geq 0} b_n x^n\right) := \left(\sum_{n\geq 0} c_n x^n\right), \quad \text{где} \quad c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

Ясно, что $R[[x]]$ – коммутативное кольцо с единицей.

Определение 4.2.

$$R[[x,y]] := (R[[x]])[[y]]$$

Далее будем рассматривать только $\Bbbk[[x]]$, где $\Bbbk$ – поле. Пусть $f(x) = \sum_{n\geq 0} a_n x^n, g(x) = \sum_{n\geq 0} b_n x^n \in \Bbbk[[x]]$ и попробуем определить ряд $f(g(x))$. Уже младший коэффициент ряда (при x^0) имеет вид $\sum_{k=0}^{\infty} b_0 a_k$, то есть не определен. Определим подкольцо

$$N = \{g = \sum_{n\geq 0} b_n x^n \in \Bbbk[[x]] \mid b_0 = 0\}.$$

В этом случае, композиция $f(g(x))$ корректно определена.

4.2. **Обратимые элементы и деление с остатком.** Можно ли в $\Bbbk[[x]]$ делить с остатком?

Лемма 4.3. $f(x) = \sum_{n\geq 0} a_n x^n$ лежит в $\Bbbk[[x]]^\times$ тогда и только тогда когда $a_0 \neq 0$.

Доказательство. Если

$$(\sum_{n\geq 0} a_n x^n)(\sum_{n\geq 0} b_n x^n) = 1,$$

то необходимо

$$a_0 b_0 = 1 \quad (\text{коэффициент при } x^0)$$

$$a_1 b_0 + a_0 b_1 = 0 \quad (\text{коэффициент при } x^1)$$

$$\dots$$

$$\sum a_k b_{n-k} = 0 \quad (\text{коэффициент при } x^n)$$

Если $a_0 \neq 0$, то система имеет решения, а значит элемент обратим. Если $a_0 = 0$, то решений нет уже у первого уравнения. □

Пример 4.4. Пусть $f(x) = 1 - x$. Элемент f – обратим и если $(1-x)^{-1} = \sum_{n\geq 0} b_n x^n$, то решая систему уравнение получаем $b_i = 1\ \forall i$, а значит $\frac{1}{1-x} = \sum_{n\geq 0} x^n$ – сродни формуле суммы геометрической прогрессии.

Для деления с остатком определим $\deg \sum_{n\geq 0} a_n x^n = \min_i a_i \neq 0$. Тогда для любых $f, g \in \Bbbk[[x]]$ существуют $q, r \in \Bbbk[[x]]$ такие, что

$$f = qg + r \qquad \deg f < \deg g$$

Действительно, если $\deg g > \deg f$, то $q = 0, r = f$. Если же $\deg f \geq \deg g$, то пусть $f = x^k f_1, g = x^l g_1$, $\deg f_1 = \deg g_1 = 0$. Тогда $f = g(x^{k-l} f_1 g_1^{-1})$. Таким образом, в

$$\Bbbk[[x]]$$

возможно деление с остатком, а значит в нем есть НОД, алгоритм Евклида, лемма Евклида и, как следствие, факториальность. Разложение $f \in \Bbbk[[x]]$ выглядит как $f = x^k f_1, \deg f_1 = 0$. Единственный простой элемент – это x.

4.3. **Производная и интеграл.**

Определение 4.5. Производной

$$f(x) = \sum_{k\geq 0} a_k x^k$$

называется ряд

$$f'(x) = \sum_{n\geq 1} n a_n x^{n-1}$$

Можно показать, что $f'(x) = \left(\dfrac{f(x+t) - f(x)}{t}\right)_{t=0}$, где $f(x+t) \in \Bbbk[[x,t]]$.

Несложно доказать, что все правила дифференцирования верны в этом случае. Например, проверим, что $(fg)' = f'g + fg'$. Для этого посчитаем коэффициент при x^n в левой и правой части. Слева он равен $(n+1)(\sum_{k=0}^{n+1} a_k b_{n-k})$. Справа

$$\sum_{k=0}^{n}(k+1)a_{k+1}b_{n-k} + \sum_{k=0}^{n} a_k(n-k+1)b_{n-k} = \sum_{k=0}^{n+1} k a_k b_{n-k} + \sum_{k=0}^{n+1} a_k(n-k+1)b_{n-k} = \sum_{k=0}^{n+1}(n+1)a_k b_{n-k}$$

Пример 4.6. Вычислим явно $\frac{1}{(1-x)^k}$.

Заметим, что $\left(\frac{1}{1-x}\right)^{(k-1)} = \frac{(k-1)!}{(1-x)^k}$, значит,

$$\frac{1}{(1-x)^k} = \frac{1}{(k-1)!}\left(\frac{1}{1-x}\right)^{(k-1)} = \frac{1}{(k-1)!}\sum_{n\geq k-1} n(n-1)\ldots(n-k+2)x^{n-k+1} = \sum_{n\geq 0}\binom{n+k-1}{k-1}x^n$$

Определение 4.7. Первообразной

$$f(x) = \sum_{k\geq 0} a_k x^k$$

называется ряд

$$\int f = \sum_{n\geq 1} \frac{a_{n-1}}{n} x^n + , C \in \Bbbk$$

Ясно, что операции дифференцирования и интегрирования взаимнообратны (быть может, с точностью до константы).

Определение 4.8. $\ln(1+x) := \int \frac{1}{1+x} = \sum_{k\geq 1}(-1)^{k+1}\frac{x^k}{k}$

Определим $U = \{\sum_{k\geq 0} a_k x^k \mid a_0 = 1\}$. Ясно, что U – абелева группа относительно умножения рядов.

Более того, если $g(x) \in U$, то корректно определен ряд $\ln g(x) = \ln(1 + (g(x) - 1))$. При этом $\ln g(x) \in N$.

Предложение 4.9. (1) $ln : (U, \cdot) \to (N, +)$ – изоморфизм абелевых групп.
(2) Пусть $\exp(x) = \sum_{n\geq 0} a_n x^n$. Тогда $\ln^{-1} = \exp$.

Доказательство.

Лемма 4.10. Следующие условия на $f, g \in U$ эквивалентны: $f = g$, $f' = g', \ln f = \ln g, (\ln f)' = (\ln g)'$.

Доказательство. 1 и 2 очевидно, эквивалентны, а, значит, (1 -> 2 ->3 ->4). Докажем, (4 ->1). Заметим, что

$$\frac{f'}{f} = \frac{g'}{g}$$

то есть

$$\frac{f'g - g'f}{fg} = \frac{g}{f}\left(\frac{f}{g}\right)'$$

откуда $f = g$.

□

- $\ln e^f = f$ для любого $f \in N$, так как $(\ln e^f)' = \dfrac{e^f f'}{e^f} = f'$.
- $e^{\ln f} = f$ для любого $f \in N$, так как $\dfrac{e^{\ln f}\frac{f'}{f}}{e^{\ln f}} = \frac{f'}{f}$.
- $\ln(fg) = \ln f + \ln g$, так как $\ln(fg)' = (\ln f)' + (\ln g)'$.

□

Определение 4.11. $(1+x)^\alpha := \exp(\ln(1+x)\alpha)$.

Ясно, что для любого $f \in U, \alpha \in \Bbbk$ определён ряд u^α. Несложно проверить, что при этом выполнены все стандартные свойства степени, например, $u^{a+\beta} = u^\alpha + u^\beta$. Для явного вычисления ряда $(1+x)^\alpha = \sum_{n\geq 0} a_n x^n$ заметим, что

$$\frac{((1+x)^\alpha)'}{(1+x)^\alpha} = (\ln(1+x)^\alpha)' = \alpha\ln(1+x)' = \frac{\alpha}{1+x}$$

Отсюда

$$(1+x)((1+x)^\alpha)' = \alpha(1+x)^\alpha,$$

откуда

$$a_k = \frac{\alpha-(k-1)}{k}a_{k-1},$$

то есть

$$a_k = \frac{(\alpha-k+1)\cdot\ldots\cdot(\alpha-1)\alpha}{k!}.$$

и

$$(1+x)^\alpha = \sum_{k\geq 0}\binom{\alpha}{k}x^k$$

Заметим, что при $\alpha = n$ получаем

$$\binom{\alpha}{k} = \binom{n}{k}.$$

4.4. **Линейно-рекуррентные последовательности.** Предположим, что бесконечная последовательность $\{a_n\}_{n=0}^\infty$ задана рекуррентно, то есть

$$a_k + b_1 a_{k-1} + \ldots + b_k a_0 = 0$$

и значения $a_0, \ldots, a_{k-1}$ определены. Как получить явную формулу для этой последовательности?

Определение 4.12. Производящей функцией бесконечной последовательности $\{a_n\}_{n=0}^\infty$ называется формальный степенной ряд $\sum_{n\geq 0} a_n x^n$.

Рассмотрим пример $a_k = a_{k-1} + a_{k-2}, a_0 = a_1 = 1$ – числа Фибоначчи и пусть $F(x)$ – производящая функция нашей последовательности. Тогда несложно видеть, что

$$F(x)(1 - x - x^2) = x,$$

а значит,

$$F(x) = \frac{x}{1 - x - x^2}$$

Корни многочлена $1 - x - x^2$ это $x_{12} = \dfrac{1 \pm \sqrt{5}}{2}$.

Далее, $\dfrac{1}{1 - x - x^2} = \frac{1}{\sqrt{5}} \left(\dfrac{1}{1 - x_1 x} + \dfrac{1}{1 - x_2 x} \right)$ откуда получаем, что

$$a_k = \frac{(1 + \sqrt{5})^k - (1 - \sqrt{5})^k}{2^k \sqrt{5}}$$

В общем случае, если $F(x) = \sum_{n \geq 0} a_n x^n$ производящая функция рекуррентно заданной последовательности, то

$$F(x)(1 + b_1 x + \ldots + b_k x^n) = 1 + c_1 x + \ldots + c_{n-1} x^{n-1}$$

а любую рациональную функцию можно разложить в ряд, используя разложение в простейшие дроби, см. ниже.

4.5. **Китайская теорема об остатках.**

Предложение 4.13. Пусть $f, g \in \Bbbk[x]$ и $g = g_1 \ldots g_n$, где НОД$(g_i, g_j) = 1$ для $i \neq j$. Тогда

$$\Bbbk[x]/(g) \simeq \Bbbk[x]/(g_1) \times \ldots \times \Bbbk[x]/(g_n)$$

Доказательство. Определим $\psi : \Bbbk[x]/(g) \simeq \Bbbk[x]/(g_1) \times \ldots \times \Bbbk[x]/(g_n)$ по правилу $[r] \mapsto ([r_1], \ldots, [r_n])$. Из взаимной простоты g_i следует, что ψ – инъекция. Для сюръективности достаточно показать, что в образе лежат все элементы вида $e_i = ([0], \ldots, [0], [1], [0], \ldots, [0])$,где $i = 1, \ldots, n$: если $\psi(x) = e_i$ и $[r] \in \Bbbk[x]/(g_i)$, то $\psi(xr) = ([0], \ldots, [0], [r], [0], \ldots, [0])$, а значит, так как $\operatorname{Im} \psi$ – подкольцо, то ψ – сюръекция. Покажем, что e_1 лежит в образе. Пусть $G_1 = g_2 \ldots g_n$. НОД (g_1, G_1)=1, значит, существуют $A, B \in \Bbbk[x]$ такие, что

$$A g_1 + B G_1 = 1$$

Тогда $[BG_1]_{g_1} = [1]$, $[BG_1]_{g_i} = [0], i = 2, \ldots, n$. Отсюда, $[BG_1]_g$ отображается в e_1. Для остальных i аналогично. $\square$

Следствие 4.14. Пусть $f, g \in \Bbbk[x]$ и $g = g_1 \ldots g_n$, где НОД$(g_i, g_j) = 1$ для $i \neq j$. существуют единственные $h, r_1, \ldots, r_n, \deg r_i < \deg g_i$ такие, что

$$\frac{f}{g} = h + \frac{r_1}{g_1} + \ldots + \frac{r_n}{g_n}$$

Предложение 4.15. Пусть $f, g \in \Bbbk[x]$ и g – неприводим, $k \in \mathbb{Z}_{>0}$, $\deg f < k \deg g$. Тогда существуют единственные $r_1, \ldots, r_k \in \Bbbk[x], \deg r_i < \deg g$ такие, что

$$\frac{f}{g^k} = \frac{r_1}{g} + \frac{r_2}{g^2} + \ldots + \frac{r_n}{g^k}$$

Вышесказанное позволяет эффективно находить явную формулу для линейной рекуррентно заданной последовательности. В частности, если $\Bbbk = \mathbb{C}$, то, как мы покажем позже, любой неприводимый многочлен имеет степень 1, а значит, для получения явной формулы достаточно разложить в ряд рациональную дробь $\dfrac{1}{(x - c)^n}$, что мы уже сделали.