§3. Дроби и ряды

В этом параграфе мы продолжаем обозначать через K произвольное коммутативное кольцо с единицей, а через $\Bbbk$ — произвольное поле.

3.1. Кольца частных. Способ изготовления поля $\mathbb{Q}$ из кольца $\mathbb{Z}$ как множества дробей с целым числителем и ненулевым целым знаменателем[1] применим в любом коммутативном кольце K с единицей. Подмножество $S \subset K$ называется *мультипликативным*, если $1 \in S$ и $st \in S$ для всех $s, t \in S$. Например, множество всех целых неотрицательных степеней q^k любого элемента $q \in K$ мультипликативно[2]. Множество $K^\circ \subset K$, состоящее из всех не делящих нуль ненулевых элементов, тоже мультипликативно. В частности, множество всех ненулевых элементов любого целостного кольца мультипликативно. Каждое мультипликативное подмножество $S \subset K$ задаёт на множестве упорядоченных пар $K \times S$ отношение эквивалентности $\sim_S$, порождённое[3] отождествлениями $(a, s) \sim_S (at, st)$ для всех $t \in S$. Класс эквивалентности пары (a, s) по модулю этого отношения называется *дробью* со знаменателем в S и обозначается a/s. Множество всех таких дробей обозначается KS^{-1} или $K[S^{-1}]$ и называется *кольцом частных* или *локализацией* кольца K со знаменателями в S.

Пример 3.1

Пусть $K = \mathbb{Z}/(6)$ и $S = \{[1], [2], [-2]\}$. Каждая дробь в KS^{-1} имеет представление со знаменателем $[1]$: $[a]/[\pm 2] = [a][2]/[\pm 2][2] = [\mp a][\mp 2]/[1][\mp 2] = [\mp a]/[1]$. В частности, $[0]/[\pm 2] = [0]/[1]$. Далее, $[3]/[1] = [3][2]/[1][2] = [0]/[2] = [0]/[1]$, а $[\pm 2]/[1] = [\pm 2][2]/[1][2] = [\mp 1][2]/[1][2] = [\mp 1]/[1]$. Мы заключаем, что KS^{-1} исчерпывается дробями $[0]/[1]$, $[1]/[1]$ и $[-1]/[1]$.

Упражнение 3.1. Убедитесь, что эти три дроби различны.

Лемма 3.1

$a/s = b/t$ в KS^{-1} если и только если $atu = bsu$ в K для некоторого $u \in S$.

Доказательство. Положим $(a, s) \approx (b, t)$, если $atu = bsu$ для некоторого $u \in S$. Двухшаговая цепочка отождествлений $(a, s) \sim_S (atu, stu) = (bsu, tsu) \sim_S (b, t)$ показывает, что отношение $\approx$ содержится в отношении $\sim_S$. Остаётся проверить, что отношение $\approx$ является отношением эквивалентности — тогда оно совпадёт с $\sim_S$ в силу минимальности последнего. Рефлексивность и симметричность очевидны. Докажем транзитивность. Пусть $(a, s) \approx (b, t)$ и $(b, t) \approx (c, r)$, т. е. существуют такие $u, w \in S$, что $atu = bsu$ и $brw = ctw$. Тогда

$$ar(tuw) = (atu)rw = (bsu)rw = (brw)su = (ctw)su = cs(tuw),$$

т. е. $(a, s) \approx (c, r)$. □

Лемма 3.2

Операции $\frac{a}{r} + \frac{b}{s} \overset{\text{def}}{=} \frac{as+br}{rs}$ и $\frac{a}{r} \cdot \frac{b}{s} \overset{\text{def}}{=} \frac{ab}{rs}$ корректно задают на KS^{-1} структуру коммутативного кольца с единицей $1/1$ и нулём $0/1$.

[1] См. прим. 0.5 на стр. 12 и прим. 1.2 на стр. 21.

[2] Мы по определению полагаем $q^0 = 1$.

[3] Т. е. наименьшее по включению отношение эквивалентности $R \subset (K \times S) \times (K \times S)$, содержащее все пары вида $\big((a, s), (at, st)\big)$, где $t \in S$, см. n° 0.4.1 на стр. 11.

Доказательство. Так каждое отождествление $\sim_S$ является цепочкой элементарных отождествлений $(a,r) \sim_S (au, ru)$, где $u \in S$, достаточно проверить, что результаты операций не меняются при замене $\frac{a}{r}$ на $\frac{au}{ru}$, а $\frac{b}{s}$ — на $\frac{bw}{sw}$, где $u, w \in S$, что очевидно:

$$\frac{au}{ru} + \frac{bw}{sw} = \frac{ausw + bwru}{rusw} = \frac{(as+br)\cdot wu}{rs \cdot wu} = \frac{as+br}{rs}$$
$$\frac{au}{ru} \cdot \frac{bw}{sw} = \frac{aubw}{rusw} = \frac{(ab)\cdot wu}{rs\cdot wu} = \frac{ab}{rs}\,.$$

Проверку выполнения в KS^{-1} всех аксиом коммутативного кольца с единицей мы оставляем читателю в качестве упражнения. □

Следствие 3.1
Кольцо KS^{-1} нулевое если и только если S содержит нуль.

Доказательство. Если $0 \in S$, то любая дробь $a/s = (a\cdot 0)/(s \cdot 0) = 0/0 = (0\cdot 1)/(1\cdot 0) = 0/1$ эквивалентна нулю. С другой стороны, $1/1 = 0/1$ только если существует такой $s \in S$, что $1\cdot 1\cdot s = 0 \cdot 1 \cdot s = 0$, откуда $s = 0 \in S$. □

Теорема 3.1
Отображение $\iota_S : K \to KS^{-1}$, переводящее $a \in K$ в дробь $a/1$, является гомоморфизмом колец с ядром $\ker \iota_S = \{a \in K \mid \exists\, s \in S : as = 0\}$. Образ $\iota_S(s)$ любого элемента $s \in S$ обратим в KS^{-1}. Для любого гомоморфизма $\varphi : K \to R$ в целостное кольцо R, переводящего каждый элемент из S в обратимый элемент из R, существует единственный такой гомоморфизм колец $\varphi_S : KS^{-1} \to R$, что $\varphi = \varphi_S \circ \iota_S$.

Доказательство. Очевидно, что ι_S является гомоморфизмом. Дробь $\iota_S(a) = a/1$ равна $0/1$ если и только если найдётся такой $s \in S$, что $a \cdot 1 \cdot s = 0 \cdot 1 \cdot s = 0$. Обратным к $\iota_S(s) = s/1$ элементом является дробь $1/s$. Остаётся доказать последнее утверждение. Для продолжения гомоморфизма $\varphi : K \to R$ до гомоморфизма $\varphi_S : KS^{-1} \to R$ нет иного выбора как положить $\varphi_S(1/s) = 1/\varphi(s)$, так как в кольце R должны выполняться равенства $\varphi_S(1/s)\cdot\varphi_S(s) = \varphi_S\big(s\cdot(1/s)\big) = \varphi(1) = 1$. Следовательно, искомое продолжение обязано задаваться формулой $\varphi_S(a/s) \overset{\text{def}}{=} \varphi(a)/\varphi(s)$. Она корректна, поскольку при замене $\frac{a}{s}$ на $\frac{au}{su}$ с $u \in S$ имеем $\varphi_S\left(\frac{au}{su}\right) = \frac{\varphi(au)}{\varphi(su)} = \frac{\varphi(a)\varphi(u)}{\varphi(s)\varphi(u)} = \frac{\varphi(a)}{\varphi(s)}$. Бесхитростную проверку того, что построенное отображение φ_S перестановочно со сложением и умножением, мы оставляем читателю. □

Упражнение 3.2. Пусть $K = \mathbb{Z}/(30)$, а $S = \{[2^k]_{30} \mid k = 0, \dots, 4\}$. Покажите, что $KS^{-1} \simeq \mathbb{Z}/(15)$.

Пример 3.2 (поле частных целостного кольца)
Если кольцо K не имеет делителей нуля, его ненулевые элементы образуют мультипликативную систему. Кольцо частных со знаменателями в этой системе является полем. Оно называется *полем частных* целостного кольца K и обозначается Q_K. Равенство $a/b = c/d$ в Q_K равносильно равенству $ac = bd$ в K, а гомоморфизм $\iota : K \hookrightarrow Q_K$, $a \mapsto a/1$, инъективен, и любой гомоморфизм $\varphi : K \to R$ в целостное кольцо R, переводящий все ненулевые элементы из K в обратимые элементы кольца R, единственным способом продолжается до вложения поля частных $\widetilde{\varphi} : Q_K \hookrightarrow R$.

Пример 3.3 (поле $\mathbb{Q}$)
Полем частных целостного кольца $\mathbb{Z}$ является поле рациональных чисел $\mathbb{Q} = Q_{\mathbb{Z}}$, которое канонически вкладывается в любое поле характеристики нуль в качестве простого подполя[1].

[1] См. n° 1.5.6 на стр. 32.

Пример 3.4 (поле рядов Лорана)

Поле частных кольца формальных степенных рядов $\Bbbk[\![x]\!]$ с коэффициентами в произвольном поле $\Bbbk$ обозначается $\Bbbk(\!(x)\!) \overset{\text{def}}{=} Q_{\Bbbk[\![x]\!]}$. Так как любой ряд с ненулевым свободным членом обратим[1] в $\Bbbk[\![x]\!]$, каждая дробь $p(x)\,/\,q(x) \in \Bbbk(\!(x)\!)$ однозначно представляется в виде $x^m h(x)$, где $h \in \Bbbk[\![x]\!]$ имеет ненулевой свободный член, а показатель $m \in \mathbb{Z}$ равен разности показателей младших членов рядов p и q. Иначе говоря, поле $\Bbbk(\!(x)\!)$ состоит из формальных степенных рядов вида $f(x) = \sum_{k\geqslant m(f)} a_k x^k$, в которых допускается конечное число мономов отрицательной степени. Такие ряды называются *рядами Лорана*, а поле $\Bbbk(\!(x)\!)$ — *полем рядов Лорана*. Номер $m(f) \in \mathbb{Z}$ самого левого ненулевого коэффициента ряда Лорана f называется *порядком* ряда f.

3.2. Рациональные функции. Поле частных кольца $\Bbbk[x]$ обозначается через $\Bbbk(x)$ и называется *полем рациональных функций* от x. Его элементами являются дроби вида $p(x)/q(x)$ с $p, q \in \Bbbk[x]$.

Предложение 3.1

Если $g = g_1 \dots g_m$, где нод$(g_i, g_j) = 1$ при $i \neq j$, то при любом f дробь $f\,/\,g$ единственным образом представляется в виде суммы

$$\frac{f}{g} = h + \frac{f_1}{g_1} + \dots + \frac{f_m}{g_m}\,, \tag{3-1}$$

где $h \in \Bbbk[x]$ и $\deg f_i < \deg g_i$ при всех i.

Доказательство. Деля f на g с остатком[2], заключаем, что $f/g = h + r/g$, где h — неполное частное, а остаток r имеет степень $\deg r < \deg g$. Если $g = g_1 g_2$ и нод$(g_1, g_2) = 1$, то $[g_2]_{g_1}$ обратим в $\Bbbk[x]\,/\,(g_1)$. Представим $[r]_{g_1}\,/\,[g_2]_{g_1} = [f_1]_{g_1}$ многочленом f_1 степени $\deg f_1 < \deg g_1$. Тогда $r = f_1 \cdot g_2 + f_2 \cdot g_1$ для некоторого $f_2 \in \Bbbk[x]$. Сравнивая степени, заключаем, что $\deg f_2 < \deg g_2$. Таким образом, $r/g = f_1/g_1 + f_2/g_2$ и к каждой из этих дробей применимо то же рассуждение, если её знаменатель является произведением взаимно простых многочленов. Это доказывает существование разложения (3-1). Для доказательства его единственности, умножим обе части разложения (3-1) на g. Получим равенство вида $f = hg + f_1 G_1 + \dots + f_m G_m$, где через $G_i = g/g_i$ обозначено произведение всех многочленов g_ν кроме i-го. Так как $\deg(f_1 G_1 + \dots + f_m G_m) < \deg g$, многочлен h является неполным частным, а $r = f_1 G_1 + \dots + f_m G_m$ — остатком от деления f на g. Каждый f_i является тем единственным многочленом степени $< \deg g_i$, класс которого в $\Bbbk[x]/(g_i)$ равен $[f]_{g_i}\,/\,[G_i]_{g_i}$. Таким образом, все ингредиенты формулы (3-1) однозначно определяются многочленами f и $g_1, \dots, g_n$. □

Предложение 3.2

Любую дробь вида $f\,/\,g^m$, в которой $\deg f < \deg g^m = m \deg g$, можно единственным образом представить в виде суммы

$$\frac{f}{g^m} = \frac{f_1}{g} + \frac{f_2}{g^2} + \dots + \frac{f_m}{g^m}\,, \tag{3-2}$$

где $\deg f_i < \deg g$ при всех i.

Доказательство. Представление (3-2) равносильно записи f в виде

$$f = f_1 g^{m-1} + f_2 g^{m-2} + \dots + f_{m-1} g + f_m\,, \tag{3-3}$$

[1] См. прим. 2.2 на стр. 37.

[2] См. n° 2.2 на стр. 39.

аналогичном записи целого числа f в g-ичной позиционной системе исчисления: f_m является остатком от деления f на g, f_{m-1} — остатком от деления частного $(f - f_m)/g$ на g, f_{m-2} — остатком от деления частного $\left(\frac{f-f_m}{g} - f_{m-1}\right)/g$ на g и т. д. □

3.2.1. Разложение на простейшие дроби. Из предыдущих двух предложений вытекает, что каждая дробь $f/g \in \Bbbk(x)$ допускает *единственное* представление в виде суммы неполного частного от деления f на g и дробей вида p/q^m, где q пробегает неприводимые делители знаменателя g, показатель m меняется от 1 до кратности вхождения q в разложение g на неприводимые множители, и в каждой из таких дробей $\deg p < \deg q$. Такое представление называется *разложением f/g на простейшие дроби* и бывает полезно в практических вычислениях с рациональными функциями.

Пример 3.5
Вычислим 2022-ю производную, а также первообразную[1] от $1/(1+x^2)$. Разложим эту дробь в поле $\mathbb{C}(x)$ на простейшие:

$$\frac{1}{1+x^2} = \frac{\alpha}{1+ix} + \frac{\beta}{1-ix}\,, \quad \text{где} \quad \alpha, \beta \in \mathbb{C}\,.$$

Подставляя $x = \pm i$ в равенство $1 = \alpha(1-ix) + \beta(1+ix)$, находим $\alpha = \beta = 1/2$, т. е.

$$\frac{1}{1+x^2} = \frac{1}{2}\left(\frac{1}{1+ix} + \frac{1}{1-ix}\right)\,.$$

Теперь дифференцируем каждое слагаемое:

$$\left(\frac{d}{dx}\right)^{2022} \frac{1}{1+x^2} = \frac{2022!}{2}\left(\frac{(-i)^{2022}}{(1+ix)^{2023}} + \frac{i^{2022}}{(1-ix)^{2023}}\right) =$$
$$= -2022! \cdot \frac{1}{2}\frac{(1-ix)^{2023} + (1+ix)^{2023}}{(1+x^2)^{2023}} = 2022! \cdot \sum_{\nu=0}^{1011} \binom{2023}{2\nu} \cdot \frac{(-1)^{\nu+1}x^{2\nu}}{(1+x^2)^{2023}}\,,$$

и интегрируем каждое слагаемое:

$$\int \frac{dx}{1+x^2} = \frac{1}{2}\int \frac{dx}{1+ix} + \frac{1}{2}\int \frac{dx}{1-ix} = \frac{\ln(1+ix) - \ln(1-ix)}{2i} = \frac{1}{2i}\ln\frac{1+ix}{1-ix} = \operatorname{arctg} x\,.$$

Подчеркнём, что все проделанные вычисления корректно определены в кольце $\mathbb{C}[\![x]\!]$, а все написанные равенства суть равенства между элементами этого кольца[2].

[1]Т. е. такой ряд f без свободного члена, что $f'(x) = 1/(1+x^2)$. Подробнее см. в n° 3.3 на стр. 59.

[2]В частности, последнее равенство вытекает из определения тангенса:

$$\operatorname{tg} t \overset{\text{def}}{=} \frac{\sin t}{\cos t} = \frac{1}{i}\cdot\frac{e^{it} - e^{-it}}{e^{it} + e^{-it}} = \frac{1}{i}\cdot\frac{e^{2it} - 1}{e^{2it} + 1} \in \mathbb{C}[\![t]\!]\,.$$

Полагая $\operatorname{tg} t = x$, получаем $e^{2it} = \frac{1+ix}{1-ix}$. Про экспоненту и логарифм мы ещё подробно поговорим в n° 3.3 на стр. 59 ниже.

3.2.2. Разложение рациональной функции в степенной ряд. По теор. 3.1 на стр. 54 существует единственное вложение $\Bbbk(x) \hookrightarrow \Bbbk(\!(x)\!)$, переводящее каждый многочлен в себя. Иначе говоря, каждую рациональную функцию можно разложить в ряд Лорана. Если основное поле $\Bbbk$ алгебраически замкнуто[1], такое разложение описывается довольно явными формулами. Пусть $\deg f < \deg g$ и знаменатель дроби f/g имеет вид:

$$g(x) = 1 + a_1x + a_2x^2 + \ldots + a_nx^n = \prod (1 - \alpha_i x)^{m_i}\,, \tag{3-4}$$

где все числа $\alpha_i \in \Bbbk$ попарно различны.

Упражнение 3.3. Убедитесь, что при $a_n \neq 0$ числа α_i из разложения (3-4) суть корни многочлена $t^n + a_1t^{n-1} + \ldots + a_{n-1}t + a_n = \prod (t - \alpha_i)^{m_i}$.

По предл. 3.1 и предл. 3.2 функция f/g является суммой простейших дробей

$$\frac{\beta_{ij}}{(1 - \alpha_i x)^{k_{ij}}}\,, \tag{3-5}$$

где при каждом i показатели k_{ij} лежат в пределах $1 \leqslant k_{ij} \leqslant m_i$, а $\beta_{ij} \in \Bbbk$.

Если все кратности $m_i = 1$, то разложение на простейшие дроби имеет вид

$$\frac{f(x)}{(1 - \alpha_1 x) \ldots (1 - \alpha_n x)} = \frac{\beta_1}{1 - \alpha_1 x} + \ldots + \frac{\beta_n}{1 - \alpha_n x}\,.$$

Чтобы найти β_i, умножим обе части на общий знаменатель и подставим $x = \alpha_i^{-1}$. Получим

$$\beta_i = \frac{f\left(\alpha_i^{-1}\right)}{\prod_{\nu \neq i} \left(1 - (\alpha_\nu / \alpha_i)\right)} = \frac{\alpha_i^{n-1} f\left(\alpha_i^{-1}\right)}{\prod_{\nu \neq i} \left(\alpha_i - \alpha_\nu\right)}\,. \tag{3-6}$$

Мы заключаем, что когда все $m_i = 1$, дробь f/g является суммой $n = \deg g$ геометрических прогрессий:

$$\frac{f(x)}{g(x)} = \sum \left(\beta_1\alpha_1^k + \beta_2\alpha_2^k + \ldots + \beta_n\alpha_n^k\right) \cdot x^k\,, \tag{3-7}$$

где β_i находятся по формулам (3-6).

Простейшая дробь (3-5) с показателем $k_{ij} = m > 1$ раскладывается в ряд при помощи формулы Ньютона для бинома с отрицательным показателем

$$\frac{1}{(1 - x)^m} = \sum_{k \geqslant 0} \frac{(k + m - 1)(k + m - 2) \cdots (k + 1)}{(m - 1)!} \cdot x^k = \sum_{k \geqslant 0} \binom{k + m - 1}{m - 1} \cdot x^k\,, \tag{3-8}$$

которая получается $(m - 1)$-кратным дифференцированием обеих частей разложения геометрической прогрессии $(1 - x)^{-1} = 1 + x + x^2 + x^3 + \ldots$.

Упражнение 3.4. Убедитесь, что $\left(\frac{d}{dx}\right)^n (1 - x)^{-1} = n!/(1 - x)^{n+1}$.

Таким образом, разложение простейшей дроби (3-5) имеет вид

$$\frac{\beta}{(1 - \alpha_i x)^m} = \beta \sum_{k \geqslant 0} \alpha_i^k \binom{k + m - 1}{m - 1} \cdot x^k\,. \tag{3-9}$$

[1] Т. е. каждый многочлен из $\Bbbk[x]$ полностью раскладывается в $\Bbbk[x]$ на линейные множители.

3.2.3. Решение линейных рекуррентных уравнений. Предыдущие вычисления можно использовать для отыскания «формулы k-того члена» последовательности z_k, заданной *линейным рекуррентным уравнением n-того порядка*:

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \ldots + a_n z_{k-n} = 0\,, \tag{3-10}$$

где коэффициенты $a_1, \ldots, a_n \in \mathbb{C}$ — заданные числа. При $k \geqslant n$ уравнению (3-10) удовлетворяют коэффициенты z_k любого степенного ряда вида

$$z_0 + z_1 x + z_2 x^2 + \ldots = \frac{b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}}{1 + a_1 x + a_2 x^2 + \ldots + a_n x^k}\,.$$

Если в числителе правой части подобрать коэффициенты $b_0, b_1, \ldots, b_{n-1} \in \mathbb{C}$ так, чтобы первые n коэффициентов $z_0, \ldots, z_{n-1}$ разложения полученной дроби в степенной ряд совпали с первыми n членами последовательности (3-10), то формулы (3-6) и (3-9) дадут явные выражения элементов последовательности z_k через k.

Пример 3.6 (числа Фибоначчи)
Найдём явное выражение через k для элементов последовательности z_k, в которой

$$z_0 = 0\,,\ z_1 = 1 \text{ и } z_k = z_{k-1} + z_{k-2} \text{ при } k \geqslant 2\,.$$

Рекуррентное уравнение $z_k - z_{k-1} - z_{k-2} = 0$ описывает коэффициенты ряда

$$x + z_2 x^2 + z_3 x^3 + \ldots = \frac{b_0 + b_1 x}{1 - x - x^2}\,,$$

у которого $z_0 = 0$ и $z_1 = 1$. Умножая обе части на знаменатель и сравнивая коэффициенты при x^0 и x^1, заключаем, что $b_0 = 0$, а $b_1 = 1$. Таким образом,

$$z(x) = \frac{x}{1 - x - x^2} = \frac{\beta_+}{1 - \alpha_+ x} + \frac{\beta_-}{1 - \alpha_- x}\,,$$

где $\alpha_\pm = (1 \pm \sqrt{5})/2$ суть корни многочлена $t^2 - t - 1$, а $\beta_+ = -\beta_- = 1/(\alpha_+ - \alpha_-) = 1/\sqrt{5}$ по формуле (3-6). Разложение $z(x)$ в ряд имеет вид

$$\frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \alpha_+ x} - \frac{1}{1 - \alpha_- x} \right) = \sum_{k \geqslant 0} \frac{\alpha_+^k - \alpha_-^k}{\sqrt{5}} \cdot x^k\,,$$

т. е.

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

Предложение 3.3
Если последовательность чисел $z_k \in \mathbb{C}$ удовлетворяет при $k \geqslant n$ рекуррентному уравнению

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \ldots + a_n z_{k-n} = 0 \tag{3-11}$$

с постоянными коэффициентами $a_i \in \mathbb{C}$, то $z_k = \alpha_1^k \varphi_1(k) + \ldots + \alpha_r^k \varphi_r(k)$, где $\alpha_1, \ldots, \alpha_r$ — это все различные корни многочлена[1]

$$t^n + a_1 t^{n-1} + \ldots + a_n\,, \tag{3-12}$$

а $\varphi_i(x) \in \mathbb{C}[x]$ имеет степень на единицу меньше кратности соответствующего корня α_i.

[1] Он называется *характеристическим многочленом* рекуррентного уравнения (3-10).

Доказательство. Ряд $\sum z_k x^k \in \mathbb{C}[\![x]\!]$, коэффициенты которого решают уравнение (3-11), является суммой дробей вида $\beta(1-\alpha x)^{-m}$, где α пробегает различные корни многочлена (3-12), показатель m лежит в пределах от 1 до кратности соответствующего корня α, и для каждой пары α, m комплексное число $\beta = \beta(\alpha, m)$ однозначно вычисляется по α, m и первым n коэффициентам последовательности z_k. Согласно формуле (3-9) коэффициент при x^k у разложения дроби $(1-\alpha x)^{-m}$ в степенной ряд имеет вид $\alpha^k \varphi(k)$, где $\varphi(k) = \binom{k+m-1}{m-1}$ является многочленом степени $m-1$ от k. □

3.3. Логарифм и экспонента. Всюду в этом разделе мы рассматриваем ряды с коэффициентами в поле $\Bbbk$ характеристики $\operatorname{char}\Bbbk = 0$. В этом случае для любого ряда $f(x) = a_0 + a_1 x + a_2 x^2 + \dots$ существует единственный ряд без свободного члена, производная от которого равна $f(x)$. Он называется *первообразной* или *интегралом* от f и обозначается

$$\int f(x)\,dx \overset{\text{def}}{=} a_0 x + \frac{a_1}{2}x^2 + \frac{a_2}{3}x^3 + \dots = \sum_{k\geqslant 1} \frac{a_{k-1}}{k}\, x^k\,. \tag{3-13}$$

Первообразный ряд от знакопеременной геометрической прогрессии называется *логарифмом* и обозначается

$$\ln(1+x) \overset{\text{def}}{=} \int \frac{dx}{1+x} = \int \left(1 - x + x^2 - x^3 + \dots\right) dx = \\ = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \dots = \sum_{k\geqslant 1} \frac{(-1)^{k-1}}{k} x^k\,. \tag{3-14}$$

Единственный ряд со свободным членом 1, совпадающий со своей производной, называется *экспонентой* и обозначается

$$e^x \overset{\text{def}}{=} \sum_{k\geqslant 0} x^k/k! = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \frac{x^5}{120} + \dots\,. \tag{3-15}$$

Упражнение 3.5. Убедитесь, что $\frac{d}{dx}\ln u = u'/u$ и $\ln(1/u) = -\ln u$ для всех $u \in U$.

3.3.1. Логарифмирование и экспоненцирование. Обозначим через $N = (x) \subset \Bbbk[\![x]\!]$ аддитивную абелеву группу всех рядов без свободного члена, а через $U = 1 + N \subset \Bbbk[\![x]\!]$ — мультипликативную абелеву группу всех рядов с единичным свободным членом. Подстановка в аргумент логарифма вместо $1+x$ произвольного ряда $u(x) \in U$ означает подстановку в логарифмический ряд (3-14) вместо переменной x ряда $u(x) - 1$ без свободного члена и тем самым является алгебраической операцией[1]. Мы получаем отображение *логарифмирования*

$$\ln : U \to N\,, \quad u \mapsto \ln u\,. \tag{3-16}$$

Подстановка в экспоненту (3-15) вместо x любого ряда $\tau(x) \in N$ даёт ряд $e^{\tau(x)}$ со свободным членом 1. Мы получаем *экспоненциальное отображение*

$$\exp : N \to U\,, \quad \tau \mapsto e^{\tau}\,. \tag{3-17}$$

[1] См. n° 2.1.1 на стр. 36.

Лемма 3.3
Для рядов $u, w \in U$ равенства $u = w$, $u' = w'$, $\ln(u) = \ln(w)$ и $u'/u = w'/w$ попарно эквивалентны друг другу.

Доказательство. Первое равенство влечёт за собой все остальные. Поскольку ряды с равными свободными членами совпадают если и только если совпадают их производные, первые два равенства и последние два равенства равносильны друг другу. Остаётся показать, что из последнего равенства следует первое. Но последнее равенство утверждает, что $u'/u - w'/w = (u'w - w'u)/uw = (w/u) \cdot (u/w)' = 0$ откуда $(u/w)' = 0$, т. е. $u/w = \text{const} = 1$. □

Теорема 3.2
Экспоненциальное и логарифмическое отображения (3-17) и (3-16) являются взаимно обратными изоморфизмами абелевых групп, т. е. для любых рядов u, u_1, u_2 из U и τ, τ_1, τ_2 из N выполняются тождества $\ln e^{\tau} = \tau$, $e^{\ln u} = u$, $\ln(u_1 u_2) = \ln(u_1) + \ln(u_2)$, $e^{\tau_1 + \tau_2} = e^{\tau_1} e^{\tau_2}$.

Доказательство. Равенство $\ln e^{\tau} = \tau$ проверяется сравнением производных от обеих частей:

$$\left(\ln e^{\tau}\right)' = \frac{\left(e^{\tau}\right)'}{e^{\tau}} = \frac{e^{\tau}\tau'}{e^{\tau}} = \tau'\,,$$

а равенство $e^{\ln u} = u$ — сравнением логарифмических производных:

$$\frac{\left(e^{\ln u}\right)'}{e^{\ln u}} = \frac{e^{\ln u}(\ln u)'}{e^{\ln u}} = \frac{u'}{u}\,.$$

Тем самым, экспоненцирование и логарифмирование являются взаимно обратными биекциями. Ряды $\ln(u_1 u_2)$ и $\ln u_1 + \ln u_2$ совпадают, поскольку имеют нулевые свободные члены и равные производные:

$$\left(\ln(u_1 u_2)\right)' = \frac{(u_1 u_2)'}{u_1 u_2} = \frac{u_1' u_2 + u_1 u_2'}{u_1 u_2} = \frac{u_1'}{u_1} + \frac{u_2'}{u_2} = \left(\ln u_1 + \ln u_2\right)'\,.$$

Поэтому логарифмирование — гомоморфизм, а значит, и обратное к нему экспоненцирование — тоже. □

Упражнение 3.6. Докажите в $\Bbbk[\![x, y]\!]$ равенство $e^{x+y} = e^x e^y$ непосредственным сравнением коэффициентов этих двух рядов.

3.3.2. Степенная функция и бином. В этом разделе мы продолжаем считать, что поле $\Bbbk$ имеет характеристику нуль. Для любого числа $\alpha \in \Bbbk$ определим *биномиальный ряд* с показателем α формулой

$$(1 + x)^{\alpha} \overset{\text{def}}{=} e^{\alpha \ln(1+x)}.$$

Подставляя вместо $1 + x$ произвольные ряды $u \in U$, мы для любого числа $\alpha \in \Bbbk$ получаем алгебраическую операцию *возведения в α-тую степень* $U \to U$, $u \mapsto u^{\alpha}$, обладающую всеми интуитивно ожидаемыми от степенной функции свойствами. В частности, для любых рядов $u, v \in U$ и чисел $\alpha, \beta \in \Bbbk$ выполняются равенства

$$u^{\alpha} \cdot u^{\beta} = e^{\alpha \ln u}\, e^{\beta \ln u} = e^{\alpha \ln u + \beta \ln u} = e^{(\alpha+\beta)\ln u} = u^{\alpha+\beta}$$
$$\left(u^{\alpha}\right)^{\beta} = e^{\beta \ln(u^{\alpha})} = e^{\beta \ln\left(e^{\alpha \ln u}\right)} = e^{\alpha\beta \ln u} = u^{\alpha\beta}$$
$$(uv)^{\alpha} = e^{\alpha \ln(uv)} = e^{\alpha(\ln u + \ln v)} = e^{\alpha \ln u + \alpha \ln v} = e^{\alpha \ln u} \cdot e^{\alpha \ln v} = u^{\alpha} v^{\alpha}\,.$$

Например, для любого ряда u с единичным свободным членом ряд $u^{1/n}$ представляет собою $\sqrt[n]{u}$ в том смысле, что $\left(u^{1/n}\right)^n = u$. Чтобы найти коэффициенты a_i биномиального ряда

$$(1+x)^\alpha = a_0 + a_1 x + a_2 x^2 + \dots$$

рассмотрим его логарифмическую производную

$$\frac{\left((1+x)^\alpha\right)'}{(1+x)^\alpha} = \frac{d}{dx}\ln(1+x)^\alpha = \alpha\frac{d}{dx}\ln(1+x) = \frac{\alpha}{1+x}\,.$$

Умножая левую и правую части на $(1+x)^{\alpha+1}$, получаем равенство

$$\left(a_1 + 2a_2 x + 3a_3 x^2 + \dots\right)\cdot(1+x) = \alpha\cdot(1 + a_1 x + a_2 x^2 + a_3 x^3 + \dots)\,.$$

Сравнивая коэффициенты при x^{k-1} в правой и левой части, приходим к рекуррентному соотношению $ka_k + (k-1)a_{k-1} = \alpha a_{k-1}$, из которого

$$a_k = \frac{\alpha-(k-1)}{k}\cdot a_{k-1} = \frac{(\alpha-(k-1))(\alpha-(k-2))}{k(k-1)}\cdot a_{k-2} = \dots$$
$$\dots = \frac{(\alpha-(k-1))(\alpha-(k-2))\cdots(\alpha-1)\alpha}{k!}\,.$$

Стоящая в правой части дробь имеет в числителе и знаменателе по k множителей, представляющих собою последовательно уменьшающиеся на единицу числа: в знаменателе — от k до 1, в числителе — от α до $(\alpha-k+1)$. Эта дробь называется *биномиальным коэффициентом* и обозначается

$$\binom{\alpha}{k} \overset{\text{def}}{=} \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!} \tag{3-18}$$

Таким образом, для любого $\alpha\in\Bbbk$ имеется разложение

$$(1+x)^\alpha = \sum_{k\geqslant 0}\binom{\alpha}{k}x^k = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2}x^2 + \frac{\alpha(\alpha-1)(\alpha-2)}{6}x^3 + \dots\,,$$

известное как *формула Ньютона*.

Пример 3.7 (бином с рациональным показателем)
Если $\alpha = n\in\mathbb{N}$, то при $k>n$ в числителе дроби (3-18) появится нулевой сомножитель. Поэтому разложение бинома в этом случае конечно и имеет вид

$$(1+x)^n = 1 + n\,x + \frac{n(n-1)}{2}\,x^2 + \dots + x^n = \sum_{k=0}^{n}\binom{n}{k}\cdot x^k\,,$$

знакомый нам из форм. (0-9) на стр. 8. При $\alpha = -m$, где $m\in\mathbb{N}$, мы получаем разложение из форм. (3-8) на стр. 57

$$(1+x)^{-m} = 1 - m\,x + \frac{m(m+1)}{2}\,x^2 - \frac{m(m+1)(m+2)}{6}\,x^3 + \dots = \sum_{k\geqslant 0}(-1)^k\binom{k+m-1}{k}\cdot x^k\,.$$

При $\alpha = 1/n$, где $n \in \mathbb{N}$, формула Ньютона разворачивает в степенной ряд радикал

$$\sqrt[n]{1+x} = 1 + \frac{1}{n}x + \frac{\frac{1}{n}\left(\frac{1}{n}-1\right)}{2}x^2 + \frac{\frac{1}{n}\left(\frac{1}{n}-1\right)\left(\frac{1}{n}-2\right)}{6}x^3 + \cdots =$$
$$= 1 + \frac{x}{n} - \frac{n-1}{2}\cdot\frac{x^2}{n^2} + \frac{(n-1)(2n-1)}{2\cdot 3}\cdot\frac{x^3}{n^3} - \frac{(n-1)(2n-1)(3n-1)}{2\cdot 3\cdot 4}\cdot\frac{x^4}{n^4} + \cdots$$

Например, при $n = 2$ и $k \geqslant 1$ в качестве коэффициента при x^k получается дробь

$$(-1)^{k-1}\cdot\frac{1\cdot 3\cdot 5\cdot\ldots\cdot(2k-3)}{2^k k!} = \frac{(-1)^{k-1}}{2k}\cdot\frac{1}{4^{k-1}}\cdot\binom{2k-2}{k-1},$$

т. е.

$$\sqrt{1+x} = 1 + \sum\nolimits_{k\geqslant 1}\frac{(-1)^{k-1}}{k}\cdot\binom{2k-2}{k-1}\cdot\frac{x^k}{4^{k-1}}. \tag{3-19}$$

Пример 3.8 (числа Каталана)
Воспользуемся разложением (3-19) для получения явной формулы для *чисел Каталана*, часто возникающих в комбинаторных задачах. Вычислим произведение $n+1$ чисел

$$a_0 a_1 \ldots a_n, \tag{3-20}$$

делая за один шаг ровно одно из n умножений и заключая перемножаемые числа в скобки. В результате мы расставим n пар скобок в выражении (3-20). Количество различных расстановок скобок, возникающих таким образом, называется n-ым *числом Каталана* c_n. При $n = 1$ есть лишь одна расстановка скобок $(a_0 a_1)$, при $n = 2$ — две $(a_0(a_1 a_2))$ и $((a_0 a_1)a_2)$, при $n = 3$ — пять: $(a_0(a_1(a_2 a_3)))$, $(a_0((a_1 a_2)a_3))$, $((a_0 a_1)(a_2 a_3))$, $((a_0(a_1 a_2))a_3)$, $(((a_0 a_1)a_2)a_3)$. Множество всевозможных расстановок скобок в произведении (3-20) распадается в дизъюнктное объединение n подмножеств, в которых конфигурации наружных скобок имеют вид

$$(a_0(a_1\ldots a_n)),\ ((a_0 a_1)(a_2\ldots a_n)),\ \ldots\ ,\ ((a_0\ldots a_{n-2})(a_{n-1}a_n)),\ ((a_0\ldots a_{n-1})a_n)$$

и которые состоят, соответственно, из c_{n-1}, $c_1 c_{n-2}$, $c_2 c_{n-3}$, …, $c_{n-2}c_1$, c_{n-1} элементов. Если дополнить последовательность чисел Каталана числом $c_0 \overset{\text{def}}{=} 1$, то получится соотношение

$$c_n = c_0 c_{n-1} + c_1 c_{n-2} + \ldots + c_{n-2}c_1 + c_{n-1}c_0,$$

означающее, что *ряд Каталана* $c(x) \overset{\text{def}}{=} \sum_{k\geqslant 0} c_k x^k = 1 + c_1 x + c_2 x^2 + \ldots \in \mathbb{Z}[\![x]\!]$ удовлетворяет уравнению $c(x)^2 = (c(x)-1)/x$, т. е. является лежащим в кольце $\mathbb{Z}[\![x]\!]$ корнем квадратного трёхчлена $xt^2 - t - 1 = 0$ от переменной t. В поле рядов Лорана $\mathbb{Q}(\!(x)\!) \supset \mathbb{Z}[\![x]\!]$ корни находятся по стандартной школьной формуле $t = (1 \pm \sqrt{1-4x})/2x$. Так как $1 + \sqrt{1-4x}$ не делится на $2x$ в $\mathbb{Z}[\![x]\!]$, корень $(1+\sqrt{1-4x})/(2x) \notin \mathbb{Z}[\![x]\!]$. Тем самым, $c(x) = (1-\sqrt{1-4x})/(2x)$, откуда по формуле (3-19)

$$c_k = \frac{1}{k+1}\binom{2k}{k}.$$

Отметим, что даже не сразу понятно, что это число — целое.

3.4. Действие $\mathbb{Q}[[d\,/\,dt]]$ на $\mathbb{Q}[t]$. Рассмотрим кольцо формальных степенных рядов $\mathbb{Q}[\![x]\!]$ от переменной x и кольцо многочленов $\mathbb{Q}[t]$ от переменной t. Обозначим через

$$D = \frac{d}{dt} : \mathbb{Q}[t] \to \mathbb{Q}[t]\,, \quad g \mapsto g'\,,$$

оператор дифференцирования. Оператор D можно подставить вместо переменной x в любой степенной ряд $\Phi(x) = \sum_{k\geqslant 0} \varphi_k x^k \in \mathbb{Q}[\![x]\!]$. Результатом такой подстановки, по определению, является линейное отображение

$$\Phi(D) : \mathbb{Q}[t] \to \mathbb{Q}[t]\,, \quad f \mapsto \sum_{k\geqslant 0} \varphi_k D^k f = \varphi_0 f + \varphi_1 f' + \varphi_2 f'' + \dots\,. \tag{3-21}$$

Поскольку каждое дифференцирование уменьшает степень многочлена на единицу, все слагаемые в правой части (3-21) обратятся в нуль при $k > \deg f$. Таким образом, для каждого многочлена $f \in \mathbb{Q}[t]$, правая часть (3-21) является корректно определённым многочленом, каждый коэффициент которого вычисляется конечным числом действий с коэффициентами исходного многочлена f и первыми $\deg(f)$ коэффициентами ряда Φ. Линейность отображения (3-21) означает, что $\Phi(D)(\alpha f + \beta g) = \alpha\Phi(D)f + \beta\Phi(D)g$ для всех $\alpha, \beta \in \mathbb{Q}$ и $f, g \in \mathbb{Q}[t]$. Результатом подстановки оператора D в произведение рядов $\Phi(x)\Psi(x) \in \mathbb{Q}[\![x]\!]$ является *композиция* $\Phi(D) \circ \Psi(D) = \Psi(D) \circ \Phi(D)$ отображений $\Phi(D)$ и $\Psi(D)$.

Упражнение 3.7. Убедитесь в этом.

Таким образом, все отображения вида $\Phi(D)$ перестановочны друг с другом, и для биективности отображения $\Phi(D)$ необходимо и достаточно, чтобы степенной ряд $\Phi(x)$ был обратим[1] в кольце $\mathbb{Q}[\![x]\!]$. В силу линейности значение отображения $\Phi(D)$ на произвольном многочлене выражается через его значения $\Phi_m(t) \overset{\text{def}}{=} \Phi(D)t^m$ на базисных одночленах t^m:

$$\Phi(D)\left(a_0 + a_1 t + \dots + a_n t^n\right) = a_0 + a_1\Phi_1(t) + \dots + a_n\Phi_n(t)\,.$$

Многочлен $\Phi_m(t) \overset{\text{def}}{=} \Phi(D)t^m$ называется m-тым *многочленом Аппеля* ряда Φ. Его степень не превосходит m, а коэффициенты зависит лишь от первых $m+1$ коэффициентов ряда Φ.

Пример 3.9 (операторы сдвига)
Экспонента $e^D = 1 + D + D^2/2 + D^3/6 + \dots$ имеет многочлены Аппеля

$$e^D t^m = \sum_{k\geqslant 0} \frac{1}{k!} D^k t^m = \sum_{k\geqslant 0} \frac{m(m-1)\dots(m-k+1)}{k!}\, t^{m-k} = \sum_{k=0}^{m} \binom{m}{k} t^{m-k} = (t+1)^m\,.$$

Поэтому $e^D : f(t) \mapsto f(t+1)$ — это *оператор сдвига*. Так как ряды e^x и e^{-x} обратны друг другу в $\mathbb{Q}[\![x]\!]$, операторы e^D и e^{-D} тоже обратны друг другу, т. е. $e^{-D} : f(t) \mapsto f(t-1)$.

Упражнение 3.8. Убедитесь, что $e^{\alpha D} : f(t) \mapsto f(t+\alpha)$ при любом $\alpha \in \mathbb{Q}$.

Пример 3.10 (вычисление суммы степеней)
Для произвольно зафиксированного $m \in \mathbb{Z}_{\geqslant 0}$ рассмотрим сумму

$$S_m(n) \overset{\text{def}}{=} 0^m + 1^m + 2^m + 3^m + \dots + n^m = \sum_{k=0}^{n} k^m \tag{3-22}$$

[1] Т. е. имел ненулевой свободный член, см. прим. 2.2 на стр. 37.

как функцию от n. При $m = 0, 1, 2, 3$ функции $S_m(n)$ достаточно известны:

$$\begin{aligned} S_0(n) &= 1 + \ldots + 1 = n \\ S_1(n) &= 1 + 2 + \ldots + n = n(n+1)/2 \\ S_2(n) &= 1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6 \\ S_3(n) &= 1^3 + 2^3 + \ldots + n^3 = n^2(n+1)^2/4 = S_1(n)^2 . \end{aligned} \tag{3-23}$$

Чтобы получить для $S_m(t)$ явное выражение, применим к этой функции *разностный оператор*

$$\nabla :\ \varphi(t) \mapsto \varphi(t) - \varphi(t-1) .$$

Функция $\nabla S_m(t)$ принимает при всех $t \in \mathbb{Z}_{\geqslant 0}$ те же значения, что и многочлен t^m. Если существует такой многочлен $S_m(t) \in \mathbb{Q}[t]$, что $S_m(0) = 0$ и $\nabla S_m(t) = t^m$, то его значения в точках $t = 0,\ 1,\ 2,\ \ldots$ последовательно вычисляются, начиная с $S_m(0) = 0$, по формуле

$$S_m(n) = S_m(n-1) + \nabla S_m(n) = S_m(n-1) + n^m$$

и совпадают с суммами (3-22). Покажем, что уравнение $\nabla S_m(t) = t^m$ имеет в $\mathbb{Q}[t]$ единственное решение $S_m(t)$ с $S_m(0) = 0$. Согласно прим. 3.9 оператор $\nabla :\ \mathbb{Q}[t] \to \mathbb{Q}[t]$ имеет вид

$$\nabla = 1 - e^{-D} = \frac{1 - e^{-D}}{D} \circ D .$$

Ряд $(1 - e^{-x})/x$ имеет свободный член 1 и обратим в $\mathbb{Q}[\![x]\!]$. Обратный ему ряд

$$\operatorname{td}(x) \overset{\text{def}}{=} \frac{x}{1 - e^{-x}} \in \mathbb{Q}[\![x]\!]$$

называется *рядом Тодда*. Подставляя $x = D$ в равенство $\operatorname{td}(x) \cdot (1 - e^{-x}) = x$, получаем соотношение $\operatorname{td}(D) \circ \nabla = D$. Стало быть, $DS_m(t) = \operatorname{td}(D)\nabla S_m(t) = \operatorname{td}(D) t^m = \operatorname{td}_m(t)$ является многочленом Аппеля ряда Тодда, а искомый нами многочлен $S_m(t) = \int \operatorname{td}_m(t)\, dt$ получается из него интегрированием. Запишем ряд Тодда в «экспоненциальной форме»

$$\operatorname{td}(x) = \sum_{k \geqslant 0} \frac{a_k}{k!}\, x^k. \tag{3-24}$$

Сумма m-тых степеней первых t натуральных чисел равна

$$\begin{aligned} S_m(t) &= \int \Big(\sum_{k=0}^{m} \frac{a_k}{k!} D^k t^m \Big)\, dt = \int \Big(\sum_{k=0}^{m} \binom{m}{k} a_k t^{m-k} \Big)\, dt = \sum_{k=0}^{m} \binom{m}{k} \frac{a_k t^{m-k+1}}{m-k+1} = \\ &= \frac{1}{m+1} \left(\binom{m+1}{1} a_m t + \binom{m+1}{2} a_{m-1} t^2 + \ldots + \binom{m+1}{m} a_1 t^m + \binom{m+1}{m+1} a_0 t^{m+1} \right) . \end{aligned}$$

Эту формулу часто символически пишут в виде

$$(m+1) \cdot S_m(t) = (a^{\downarrow} + t)^{m+1} - a_{m+1} ,$$

где стрелка у $a^{\downarrow}$ предписывает при раскрытии бинома $(a+t)^{m+1}$ заменять a^k на a_k. Коэффициенты a_k рекурсивно вычисляются из равенства $\operatorname{td}(x) \cdot (1 - e^{-x})/x = 1$, которое имеет вид

$$\Big(1 + a_1 x + \frac{a_2}{2} x^2 + \frac{a_3}{6} x^2 + \frac{a_4}{24}\, x^4 + \ldots \Big) \cdot \Big(1 - \frac{1}{2}\, x + \frac{1}{6}\, x^2 - \frac{1}{24}\, x^3 + \frac{1}{120}\, x^4 - \ldots \Big) = 1 .$$

Упражнение 3.9. Найдите первую дюжину чисел a_k, проверьте формулы (3-23), дополните их явными формулами для $S_4(n)$ и $S_5(n)$ и вычислите[1] $S_{10}(1000)$.

Замечание 3.1. (числа Бернулли) Название «ряд Тодда» вошло в обиход во второй половине XX века после работ Хирцебруха и Гротендика, где он использовался для формулировки и доказательства теоремы Римана – Роха. Во времена Бернулли и Эйлера предпочитали пользоваться рядом $\mathrm{td}(-x) = x/(e^x - 1)$, который отличается от $\mathrm{td}(x)$ ровно в одном члене, поскольку

$$\mathrm{td}(x) - \mathrm{td}(-x) = \frac{x}{1 - e^{-x}} + \frac{x}{1 - e^x} = x \cdot \frac{2 - e^x - e^{-x}}{(1 - e^{-x}) \cdot (1 - e^x)} = x\,.$$

Тем самым, коэффициенты при x в $\mathrm{td}(x)$ и в $\mathrm{td}(-x)$ равны соответственно $1/2$ и $-1/2$, а все прочие коэффициенты при нечётных степенях x^{2k+1} с $k \geqslant 1$ в обоих рядах нулевые. Коэффициенты B_k в экспоненциальном представлении

$$\frac{x}{e^x - 1} = \sum_{k \geqslant 0} \frac{B_k}{k!} x^k$$

называются *числами Бернулли*. Таким образом, $B_k = a_k$ при $k \neq 1$ и обращаются в нуль при всех нечётных $k \geqslant 3$, а $B_1 = -a_1 = -1/2$. Со времён своего открытия числа Бернулли вызывают неослабевающий интерес. Им посвящена обширная литература[2] и специальный интернет-ресурс[3], на котором среди прочего есть программа для быстрого вычисления чисел B_k в виде несократимых рациональных дробей. Однако, не смотря на множество красивых теорем о числах Бернулли, про явную зависимость B_n от n известно немного, и любой содержательный новый взгляд в этом направлении был бы интересен.

Упражнение 3.10. Получите для чисел Бернулли рекурсивную формулу

$$(n+1)B_n = -\sum_{k=0}^{n-1} \binom{n+1}{k} \cdot B_k\,.$$

3.5. Ряды Пюизо. Дробно степенной ряд вида $f(t) = \sum_{k \geqslant m} a_k t^{k/q}$, у которого показатели степеней ограничены снизу и имеют конечный общий знаменатель $q \in \mathbb{N}$, называется *рядом Пюизо*. Можно воспринимать ряд Пюизо как ряд Лорана от формальной переменной $\sqrt[q]{t}$, где $q \in \mathbb{N}$ может быть любым. Ряды Пюизо с коэффициентами a_i из поля $\Bbbk$ образуют поле, которое мы будем обозначать через $\Bbbk\{\!\{x\}\!\}$. Основным результатом этого раздела является

Теорема 3.3
Если поле $\Bbbk$ алгебраически замкнуто и $\mathrm{char}\,\Bbbk = 0$, то поле рядов Пюизо $\Bbbk\{\!\{t\}\!\}$ тоже алгебраически замкнуто.

[1] Яков Бернулли (1654 – 1705), пользуясь лишь пером и бумагой, сложил 10-е степени первой тысячи натуральных чисел примерно за 7 минут, о чём не без гордости написал в своём манускрипте «Ars Conjectandi», изданном в 1713 году уже после его кончины.

[2] Начать знакомство с которой я советую с гл. 15 книги *К. Айрлэнд, М. Роузен*. «Классическое введение в современную теорию чисел» и § 8 гл. V книги *З. И. Боревич, И Р. Шафаревич*. «Теория чисел».

[3] http://www.bernoulli.org/

Другими словами, теор. 3.3 утверждает, что корни любого многочлена

$$a_n(t)\,x^n + a_{n-1}(t)\,x^{n-1} + \ldots + a_1(t)\,x + a_0(t)\,,$$

коэффициенты которого являются рядами Пюизо от t, раскладываются в ряды Пюизо по t. Например, любой многочлен $f(x,y) \in \Bbbk[x,y]$ можно рассматривать как многочлен от y с коэффициентами в $\Bbbk[x]$. По теор. 3.3 существует такой ряд Пюизо $\varphi(x) \in \Bbbk\{\!\{x\}\!\}$, что $f(x,\varphi(x)) = 0$ в $\Bbbk\{\!\{x\}\!\}$. Неформально говоря, это означает, что «неявная алгебраическая функция» $y = y(x)$, заданная полиномиальным соотношением $f(x,y) = 0$, всегда может быть *явно выписана* в виде ряда Пюизо от x, если только поле $\Bbbk$, над которым происходит дело, алгебраически замкнуто и имеет характеристику нуль.

Доказательство теор. 3.3 является комбинацией двух соображений, представленных в лем. 3.4 и лем. 3.5 ниже. Собственно доказательство см. в n° 3.5.1 на стр. 68. В n° 3.5.2 приведён пример, показывающий, что при $\operatorname{char}\Bbbk = p > 0$ теор. 3.3 не верна.

Лемма 3.4 (лемма Гензеля)
Пусть $G(t,x) \in \Bbbk[\![t]\!]\,[x]$ — приведённый многочлен от переменной x с коэффициентами в формальных степенных рядах от переменной t над произвольным полем $\Bbbk$. Если при $t = 0$ многочлен $G(0,x) \in \Bbbk[x]$ раскладывается в $\Bbbk[x]$ в произведение взаимно простых приведённых множителей $a(x)$ и $b(x)$ положительных степеней, то существуют единственные такие приведённые многочлены $A(t,x)$, $B(t,x) \in \Bbbk[\![t]\!][x]$, что $\deg A = \deg a$, $\deg B = \deg b$, $A(0,x) = a(x)$, $B(0,x) = b(x)$ и $G(t,x) = A(t,x)\,B(t,x)$ в $\Bbbk[\![t]\!]\,[x]$.

Доказательство. Запишем данный ряд $G(t,x)$ и искомые ряды $A(t,x)$ и $B(t,x)$ в виде рядов от переменной t с коэффициентами в $\Bbbk[x]$:

$$\begin{aligned}G(t,x) &= g_0(x) + g_1(x)\,t + g_2(x)\,t^2 + \ldots\\ A(t,x) &= a_0(x) + a_1(x)\,t + a_2(x)\,t^2 + \ldots\\ B(t,x) &= b_0(x) + b_1(x)\,t + b_2(x)\,t^2 + \ldots\,.\end{aligned}$$

Сравнивая коэффициенты при t^k в равенстве $G(t,x) = A(t,x)\,B(t,x)$, видим, что $a_0b_0 = g_0$ и

$$a_0b_k + b_0a_k = g_k - \sum_{i=1}^{k-1} a_ib_{k-i} \quad \text{при } k \geqslant 1\,. \tag{3-25}$$

Взаимно простые приведённые многочлены $a_0 = a(x)$ и $b_0 = b(x)$, удовлетворяющие равенству $a_0b_0 = g_0$, имеются по условию. Равенство (3-25) однозначно определяет многочлены a_k и b_k степеней $\deg a_k < \deg a$ и $\deg b_k < \deg b$, как только известны все предыдущие многочлены a_i и b_i и $\deg a_i < \deg a$, $\deg b_i < \deg b$ при всех $0 < i < k$. В самом деле, раз G приведён как многочлен от x, то $\deg g_i < \deg g_0$ при всех $i > 0$, и степень многочлена в правой части (3-25) строго меньше $\deg a_0 \cdot \deg b_0$. Тем самым, b_k — это единственный многочлен степени $< \deg b_0$, класс которого по модулю b_0 равен отношению класса правой части формулы (3-25) к классу $a_0 \pmod{b_0}$, а класс a_k играет аналогичную роль по модулю a_0 (ср. с доказательством предл. 3.1 на стр. 55). Таким образом, приведённые многочлены $A(t,x)$ и $B(t,x)$ со свойствами $A(0,x) = a(x)$, $B(0,x) = b(x)$, $\deg A = \deg a$, $\deg B = \deg b$ и $G(t,x) = A(t,x)\,B(t,x)$ существуют и единственны. Проверим, что они взаимно просты. Для этого подберём такие $p_i, q_i \in \Bbbk[x]$, что их степени ограничены по i сверху, а ряды $P(t,x) = \sum_{k\geqslant 0} p_k(x)\,t^k$ и $Q(t,x) = \sum_{k\geqslant 0} q_k(x)\,t^k$

удовлетворяют соотношению $AP + BQ = 1$. Сравнивая в этом соотношении коэффициенты при t^k, заключаем, что $a_0p_0 + b_0q_0 = 1$ и $a_0p_k + b_0q_k = -\sum_{i=1}^{k-1}(a_ip_{k-i} + b_iq_{k-i})$ при $k \geqslant 1$. Так как многочлены $a_0 = a$ и $b_0 = b$ взаимно просты и $\deg a_i < \deg a$, $\deg b_i < \deg b$ при всех $i > 0$, написанные соотношения однозначно задают искомые многочлены p_i и q_i степеней, строго меньших, чем $\deg a$ и $\deg b$ соответственно. □

Лемма 3.5
Над алгебраически замкнутым полем $\Bbbk$ характеристики нуль для любого многочлена

$$F(t,x) = a_n(t)\,x^n + a_{n-1}(t)\,x^{n-1} + \ldots + a_0(x) \in \Bbbk(\!(t)\!)\,[x]$$

от переменной x с коэффициентами в поле рядов Лорана $\Bbbk(\!(t)\!)$ существуют такие число $m \in \mathbb{N}$ и ряд $\vartheta(t) \in \Bbbk(\!(t)\!)$, что $F\left(t^m, \vartheta(t)\right) = 0$ в $\Bbbk(\!(t)\!)$. Иными словами, каждый многочлен с коэффициентами в поле рядов Лорана от t имеет при некотором $m \in \mathbb{N}$ корень в поле $\Bbbk(\!(\sqrt[m]{t})\!)$.

Доказательство. Умножая многочлен F на подходящее t^k, мы можем и будем считать, что все коэффициенты a_i лежат в $\Bbbk[\![t]\!]$. Далее, умножая F на a_n^{n-1} и заменяя x на a_nx, сделаем F приведённым. Наконец, пользуясь тем, что $\operatorname{char}\Bbbk = 0$, заменим x на $x - a_{n-1}/n$, что занулит коэффициент при x^{n-1}.

Упражнение 3.11. Убедитесь, в этом.

Таким образом, достаточно доказать теорему для многочлена вида

$$F(t,x) = x^n + a_{n-2}(t)\,x^{n-2} + \ldots + a_0(t) \in \Bbbk[\![x]\!]\,. \tag{3-26}$$

Если все $a_i = 0$, что так при $n = 1$, можно взять $m = 1$ и $\vartheta = 0$. Поэтому мы можем и будем считать, что $n \geqslant 2$, имеются $a_i \neq 0$, и для всех многочленов степени $< n$ теорема верна.

Если среди коэффициентов a_i имеется ряд с ненулевым свободным членом, то при $t = 0$ многочлен $F(0,x) \neq x^n$ имеет в алгебраически замкнутом поле $\Bbbk$ по крайней мере два разных корня, ибо при $\operatorname{char}\Bbbk = 0$ и $\alpha \neq 0$ чистая степень $(x - \alpha)^n$ имеет ненулевой коэффициент при x^{n-1}. Мы заключаем, что $F(0,x) = a(x)b(x)$, где $\text{нод}(a,b) = 1$ и $\deg a, \deg b < \deg F$. По лем. 3.4 $F(t,x) = A(t,x)B(t,x)$ в $\Bbbk[\![t]\!]\,[x]$, где A, B приведены и $\deg A, \deg B < \deg F$. По индукции теорема верна для многочлена A, а значит, и для F.

Пусть каждый ненулевой ряд a_i делится на t. Обозначим через $\mu_i = \operatorname{ord} a_i$ его порядок[1], приведём все дроби $\mu_i/(n-i)$ к общему знаменателю $q \in \mathbb{N}$ и обозначим через $p \in \mathbb{N}$ наименьший из получившихся после приведения числителей. Таким образом, $q\mu_i \geqslant p(n-i)$ при всех i, и при некотором $i = \ell$ это неравенство обращается в равенство. Теперь заменим в многочлене F параметр t на t^q, а переменную x — на t^px. Получим многочлен

$$\begin{aligned} G(t,x) = F(t^q, t^px) &= t^{pn}\,x^n + \sum_{i=0}^{n-2} a_i(t^q)\,t^{pi}x^i = \\ &= t^{pn}\,x^n + \sum_{i=0}^{n-2} t^{pi}\left(\alpha_{\mu_i}\,t^{q\mu_i} + \text{члены большей степени по } t\right)\cdot x^i = \\ &= t^{pn}\Big(x^n + \sum_{i=0}^{n-2} t^{q\mu_i - p(n-i)}\,(\alpha_{\mu_i} + \text{ члены, делящиеся } t\,)\cdot x^i\,\Big)\,, \end{aligned}$$

[1] Т. е. наименьшую степень t, входящую в ряд с ненулевым коэффициентом, ср. с прим. 3.4 на стр. 55.

который делится в $\Bbbk[\![t]\!][x]$ на t^{pn}, и после сокращения этого множителя коэффициент при x^ℓ у частного будет иметь ненулевой свободный член, так как $q\mu_\ell = p(n-\ell)$. По уже доказанному, приведённый многочлен $G(t,x)/t^{pn}$ приводим в $\Bbbk[\![t]\!][x]$, и тем самым существуют такие $d \in \mathbb{N}$ и $\tau(t) \in \Bbbk(\!(t)\!)$, что $G\left(t^d, \tau(t)\right) = 0$ в $\Bbbk(\!(t)\!)$. Тогда для $m = qd$ и $\vartheta(t) = t^p\,\tau(t)$ имеем $F\left(t^m, \vartheta(t)\right) = F\left(t^{qd}, t^p\,\tau(t)\right) = G\left(t^d, \tau(t)\right) = 0$, что и требовалось. □

3.5.1. Окончание доказательства теор. 3.3. Пусть многочлен

$$f(x) = a_0(t) + a_1(t)\,x + \ldots + a_n(t)\,x^n$$

имеет коэффициенты $a_i(t)$ в поле рядов Пюизо. Обозначим общий знаменатель всех показателей всех рядов a_i через N и положим $t = u^N$. Тогда $a_i(t) = a_i(u^m) \in \Bbbk(\!(u)\!)$ и по лем. 3.5 после ещё одной подстановки $u = s^q$ у многочлена f появится корень в поле $\Bbbk(\!(s)\!)$. Возвращаясь к исходному параметру $t = s^{qm}$ получаем корень многочлена f в виде ряда Лорана от $t^{\frac{1}{qm}}$, что и требуется.

3.5.2. Контрпример к теор. 3.3 в положительной характеристике. Если $\operatorname{char}\Bbbk = p > 0$, лем. 3.5 и теор. 3.3 перестают быть верным. Например, многочлен $x^p - x - t^{-1} \in \mathbb{F}_p(\!(t)\!)[x]$ не имеет корня в поле рядов Пюизо от t. В самом деле, пусть ряд Пюизо $x(t) = c_1 t^{\lambda_1} + c_2 t^{\lambda_2} + \ldots$ с $\lambda_1 < \lambda_2 < \ldots$ и ненулевыми $c_i \in \mathbb{F}_p$ удовлетворяет равенству $x^p - x = t^{-1}$. Так как $c^p = c$ для всех $c \in \mathbb{F}_p$, это равенство переписывается в виде

$$c_1 t^{p\lambda_1} + c_2 t^{p\lambda_2} - c_1 t^{\lambda_1} + c_3 t^{p\lambda_3} - c_2 t^{\lambda_2} + \text{ большие степени } = t^{-1}\,.$$

Мы заключаем, что $\lambda_1 < 0$ и член минимальной степени $c_1 t^{p\lambda}$ ни с чем в левой части не сокращается. Поэтому $c_1 t^{p\lambda} = t^{-1}$, откуда $c_1 = 1$ и $\lambda_1 = -1/p$. Следующие два члена обязаны сокращать друг друга, откуда $c_2 = c_1 = 1$, а $\lambda_2 = \lambda_1/p = -1/p^2$. Следующие два члена также обязаны сокращать друг друга, откуда $c_3 = 1$, а $\lambda_3 = -1/p^3$ и т. д. Таким образом, ряд $x(t) = \sum_{k\geqslant 1} t^{-1/p^k}$ содержит бесконечно много членов отрицательной степени, а у его показателей нет общего знаменателя, т. е. он не является рядом Пюизо вопреки предположению.

Ответы и указания к некоторым упражнениям

Упр. 3.1. Воспользуйтесь лем. 3.1.

Упр. 3.2. По теор. 3.1 на стр. 54 эпиморфизм $\pi : K = \mathbb{Z}/(30) \twoheadrightarrow \mathbb{Z}/(15)$, $[n]_{30} \mapsto [n]_{15}$, раскладывается в композицию гомоморфизма $\iota_S : K \to KS^{-1}$ и гомоморфизма

$$\pi_S : KS^{-1} \twoheadrightarrow \mathbb{Z}/(15)\,, \quad [m]_{30}/[2^k]_{30} \mapsto [m]_{15}[2^k]_{15}^{-1}\,,$$

сюрьективного в силу сюрьективности π. Если $[m]_{30}/[2^k]_{30} \in \ker \pi_S$, то $[m]_{15} = 0$, а значит, $[m]_{30}/[2^k]_{30} = [2m]_{30}/[2^{k+1}]_{30} = 0$ в KS^{-1}. Тем самым, $\ker \pi_S = 0$ и π_S инъективен.

Упр. 3.4. По правилу дифференцирования композиции $\left(f^m\right)' = mf^{m-1}f'$, откуда

$$\frac{d}{dx}(1-x)^{-m} = \frac{d}{dx}\left(\frac{1}{1-x}\right)^m = m(1-x)^{-(m+1)}\,.$$

Нужная формула получается отсюда по индукции.

Упр. 3.5. Первое равенство вытекает и правила дифференцирования сложной функции[1], второе доказывается дифференцированием обеих частей.

Упр. 3.9. Ответы: $a_1 = \frac{1}{2}$, $a_2 = \frac{1}{6}$, $a_3 = 0$, $a_4 = -\frac{1}{30}$, $a_5 = 0$, $a_6 = \frac{1}{42}$, $a_7 = 0$, $a_8 = -\frac{1}{30}$, $a_9 = 0$, $a_{10} = \frac{5}{66}$, $a_{11} = 0$, $a_{12} = -\frac{691}{2730}$,

$$S_4(n) = n(n+1)(2n+1)(3n^2+3n-1)/30$$
$$S_5(n) = n^2(n+1)^2(2n+1)(2n^2+2n-1)/12$$
$$S_{10}(1000) = 91\,409\,924\,241\,424\,243\,424\,241\,924\,242\,500\,.$$

Упр. 3.10. Подставьте $t = 1$ в $(m+1)\,S_m(t) = (a^{\downarrow} + t)^{m+1} - a_{m+1}$.

[1]См. 2-8 на стр. 38.