Записки научных
семинаров ПОМИ
Том 365, 2009 г.

**Е. В. Ференс-Сороцкий**

# ПОДГОТОВИТЕЛЬНАЯ ЛЕММА ВЕЙЕРШТРАССА ДЛЯ НЕКОММУТАТИВНЫХ КОЛЕЦ

## 1. Введение

В теории колец широко известно следующее утверждение, устанавливающее фундаментальное свойство колец степенных рядов над локальными кольцами.

**Подготовительная лемма Вейерштрасса.** *Пусть $R$ – полное локальное кольцо с (единственным) максимальным идеалом $\mathfrak{m}$, $A = R[[x]]$ – кольцо формальных степенных рядов над $R$. Пусть $f(x) = a_0 + a_1x + a_2x^2 + \dots \in A$, причем при некотором натуральном $n$ коэффициент $a_n$ обратим в $R$ ($a_n \in R^*$), а $a_0$, $a_1$, ... , $a_{n-1}$ лежат в $\mathfrak{m}$. Тогда существует $E(x) \in A^*$ (обратимый степенной ряд) и коэффициенты $b_0$, $b_1$ ... $b_{n-1}$ из $\mathfrak{m}$ такие, что $f(x) = E(x)(b_0 + b_1x + \dots + b_{n-1}x^{n-1} + x^n)$.*

В [1, сс. 168, 174] сформулировано аналогичное утверждение для степенных рядов от нескольких переменных над полем.

В данной статье доказывается обобщение подготовительной леммы Вейерштрасса на некоммутативные кольца степенных рядов.

**Теорема 1.** *Пусть $R$ – полное локальное кольцо с (единственным) максимальным идеалом $\mathfrak{m}$, $\sigma$ – $\mathfrak{m}$-инвариантный эндоморфизм $R$, $\sigma(1) = 1$, $A = R_\sigma[[x]]$ – кольцо косых формальных степенных рядов над $R$. Пусть $f(x) = a_0 + a_1x + a_2x^2 + \dots \in A$, причем при некотором натуральном $n$ $a_n \in R^*$, а $a_0, a_1, \dots, a_{n-1}$ лежат в $\mathfrak{m}$. Тогда существует $E(x)$, обратимый в $A$, и коэффициенты $b_0, b_1, \dots, b_{n-1}$ из $\mathfrak{m}$, такие, что*

$$f(x) = E(x)(b_0 + b_1x + \dots + b_{n-1}x^{n-1} + x^n). \tag{1}$$

$\mathfrak{m}$-инвариантностью мы называем свойство: если $a \in \mathfrak{m}$, то $\sigma(a) \in \mathfrak{m}$.

Работа поддержана грантом РФФИ No. 08-01-00777-а.

$R_\sigma[[x]]$ обозначает кольцо косых формальных степенных рядов $R[[x]]$, в котором обычное умножение заменено на умножение по правилу $xa = \sigma(a)x$ ($a \in R$ – коэффициент, $x$ – формальная переменная).

Главный интерес здесь представляет случай, когда $\sigma$ является автоморфизмом Фробениуса кольца $R$. Он обладает свойством $\sigma(a) \equiv a^p \bmod p$ для всех $a \in R$ ($p$ – характеристика поля вычетов $R$), а также $\sigma(1) = 1$.

## 2. Свойства автоморфизма Фробениуса

Докажем, что автоморфизм Фробениуса в полном локальном кольце является $\mathfrak{m}$-инвариантным, так что он может использоваться в качестве $\sigma$ в теореме 1.

Пусть $R$ – полное локальное кольцо, $\mathfrak{m}$ – его единственный максимальный идеал. Сформулируем два очевидных факта.

**Факт 2.1.** *Любой собственный (т.е. отличный от самого кольца) идеал $R$ содержится в $\mathfrak{m}$.*

В [3, глава I] доказывается утверждение, более общее, чем факт 2.1.

**Факт 2.2.** *Если $u \in R^*$, $m \in \mathfrak{m}$, то $v = u + m \in R^*$.*

**Утверждение 2.3.** *Автоморфизм Фробениуса (обозначим его $\sigma$) является $\mathfrak{m}$-инвариантным.*

Нам не нужна явная конструкция автоморфизма Фробениуса, а только его свойство $\sigma(a) \equiv a^p \bmod p$, то есть $\sigma(a) = a^p + pb$, для некоторого $b \in R$. Так как (см. факт 2.1) идеал $(p)$ содержится в $\mathfrak{m}$, то обязательно $pb \in \mathfrak{m}$.

Если $a \in \mathfrak{m}$, то $a^p \in \mathfrak{m}$, и тогда $\sigma(a) \in \mathfrak{m}$, что доказывает $\mathfrak{m}$-инвариантность.

Очевиден также следующий

**Факт 2.4.** *Автоморфизм Фробениуса переводит обратимые элементы в обратимые.*

## 3. Обратимость в кольцах $R_\sigma[[x]]$

В этом параграфе $R$ обозначает коммутативное кольцо, $\sigma$ – его эндоморфизм. Также будем придерживаться обозначений для коэф-

фициентов степенных рядов над $R$:

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + a_3x^3 + \dots \in R_\sigma[[x]], \\ g(x) &= b_0 + b_1x + b_2x^2 + b_3x^3 + \dots \in R_\sigma[[x]], \\ h(x) &= c_0 + c_1x + c_2x^2 + c_3x^3 + \dots \in R_\sigma[[x]]. \end{aligned} \tag{2}$$

$R_\sigma[[x]]$ обозначает здесь и далее кольцо косых формальных степенных рядов. Правило $xa = \sigma(a)x$ означает в точности, что для $h(x) = f(x) \cdot g(x)$ при всех натуральных $n$

$$c_n = a_0b_n + a_1\sigma(b_{n-1}) + \dots + a_{n-1}\sigma^{n-1}(b_1) + a_n\sigma^n(b_0). \tag{3}$$

**Лемма 3.1.** *Степенной ряд в $R_\sigma[[x]]$ обратим справа тогда и только тогда, когда его свободный член обратим в $R$.*

Построим для $f(x) \in R_\sigma[[x]]$ ряд $g(x) \in R_\sigma[[x]]$ такой, что $f(x)g(x) = 1$. Рассматривая свободные члены, получаем $a_0b_0 = 1$, так что необходимость $a_0 \in R^*$ очевидна. Далее, используя формулу (3) и обратимость $a_0$, построим коэффициенты $b_n$ по индукции:

$$b_n = -a_0^{-1}(a_1\sigma(b_{n-1}) + \dots + a_{n-1}\sigma^{n-1}(b_1) + a_n\sigma^n(b_0)). \tag{4}$$

Ясно, что соответствующий ряд $g(x)$ будет искомым.

**Лемма 3.2.** *Степенной ряд в $R_\sigma[[x]]$ обратим слева, если его свободный член и все итерации $\sigma$ от него обратимы в $R$.*

Для $g(x) \in R_\sigma[[x]]$, удовлетворяющего условиям леммы, построим $f(x) \in R_\sigma[[x]]$ такой, что $f(x)g(x) = 1$. Как и в предыдущей лемме, $a_0b_0 = 1$, так что $a_0 = b_0^{-1}$. Далее с помощью формулы (3) строим коэффициенты $a_n$ по индукции:

$$a_n = -\sigma^n(b_0)^{-1}(a_0b_n + a_1\sigma(b_{n-1}) + \dots + a_{n-1}\sigma^{n-1}(b_1)). \tag{5}$$

На каждом шаге построение корректно из-за обратимости $\sigma^n(b_0)$. Из этих коэффициентов составляется искомый ряд $f(x)$. Лемма доказана.

**Следствие 3.3.** *Если $\sigma(1) = 1$, то степенной ряд в $R_\sigma[[x]]$ обратим слева тогда и только тогда, когда его свободный член обратим в $R$.*

Согласно факту 2.4, из обратимости $b_0$ следует обратимость $\sigma(b_0)$, а по индукции – и всех $\sigma^n(b_0)$, так что достаточность следует из леммы 3.2. Необходимость легко получается из равенства $a_0b_0 = 1$.

**Замечание 3.4.** Если элемент некоммутативного кольца обратим слева и справа, то его левый и правый обратный совпадают.

**Следствие 3.5.** *Если $\sigma(1) = 1$, то степенной ряд в $R_\sigma[[x]]$ обратим тогда и только тогда, когда его свободный член обратим в $R$.*

Это непосредственно следует из леммы 3.1, следствия 3.3 и замечания 3.4.

## 4. Основные теоремы

Перейдем к доказательству основного утверждения: теоремы 1, сформулированной во введении.

Заметим, что классическая подготовительная лемма Вейерштрасса – частный случай теоремы 1, когда $\sigma$ – тождественное преобразование кольца $R$. Кольцо $R_\sigma[[x]]$ в таком случае является обычным кольцом степенных рядов $R[[x]]$.

Теорему 1 мы сведем к следствию из другой теоремы.

**Теорема 2.** *В условиях и обозначениях теоремы 1, для любого $g(x) \in A$ существуют и единственны $U(x) \in A$, $b_0$, $b_1$, ... $b_{n-1}$ из $R$, такие, что*

$$g(x) = U(x)f(x) + b_0 + b_1x + \cdots + b_{n-1}x^{n-1}. \tag{6}$$

Теорема 2, на самом деле, аналог так называемой "леммы Вейерштрасса о делении" для некоммутативного кольца степенных рядов.

**Утверждение 4.1.** *Если верна теорема 2, то верна и теорема 1.*

Действительно, применим теорему 2 к $g(x) = -x^n$. Тогда уравнение (6) можно переписать, как

$$U(x)f(x) = -(b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + x^n). \tag{7}$$

Приравняем коэффициенты при $x^i$ $(i < n)$ в последнем равенстве. Пользуясь формулой (3) и вводя обозначение $U(x) = u_0 + u_1x + u_2x^2 + \cdots$, мы получим

$$b_i = -u_0a_i - u_1\sigma(a_{i-1}) - \cdots - u_{i-1}\sigma^{i-1}(a_1) - u_i\sigma^i(a_0). \tag{8}$$

Так как, по условию, $a_0, a_1, \ldots, a_{n-1}$ лежат в $\mathfrak{m}$, а $\sigma$ – $\mathfrak{m}$-инвариантно, то из (8) следует, что $b_i \in \mathfrak{m}$, как и требуется в теореме 1.

Далее приравняем коэффициенты при $x^n$:

$$\begin{aligned} &1 + u_0a_n \\ &\quad = -u_1\sigma(a_{n-1}) - u_2\sigma^2(a_{n-2}) - \cdots - u_{n-1}\sigma^{n-1}(a_1) - u_n\sigma^i(a_0). \end{aligned} \tag{9}$$

Как и прежде, правая часть лежит в $\mathfrak{m}$; обозначим ее $-m$. По условию $a_n \in R^*$, также $1+m \in R^*$ (см. факт 2.2). Тогда из (9) следует $u_0^{-1} = -(1+m)^{-1}a_n^{-1}$, то есть обратимость $u_0$.

Наконец, согласно следствию 3.5, $U(x)$ обратим. Домножив (7) слева на $U(x)^{-1}$, получаем (1) для $E(x) = -U(x)^{-1}$. Очевидно, $E(x)$ обратим.

Теперь, доказав утверждение 4.1, нужно доказать саму теорему 2. Но прежде переформулируем ее, следуя идее Манина, изложенной в [2, с. 21].

Определим на $R_\sigma[[x]]$ следующие линейные операторы $r$ и $h$: для $P(x) = c_0 + c_1x + c_2x^2 + \cdots$ положим ($n$ – из условия теорем 1 и 2)

$$\begin{aligned} r(P) &= c_0 + c_1x + \cdots + c_{n-1}x^{n-1}, \\ h(P) &= c_n + c_{n+1}x + c_{n+2}x^2 + \cdots . \end{aligned} \tag{10}$$

Очевидно, что $P(x) = r(P) + h(P)x^n$ и $h(P(x)x^n) = P(x)$. Также ясно, что утверждение теоремы 2 равносильно существованию и единственности такого $U(x) \in A$, что

$$h(g(x)) = h(U(x)f(x)). \tag{11}$$

Преобразуем правую часть, с учетом вышесказанного:

$$\begin{aligned} h(Uf) &= h(Ur(f) + Uh(f)x^n) = h(Ur(f)) + h(Uh(f)x^n) \\ &= h(Ur(f)) + Uh(f). \end{aligned}$$

Приходим к равенству:

$$h(g) = h(Ur(f)) + Uh(f). \tag{12}$$

Аналогичные преобразования проводятся в [1, сс. 169–170] и в [2, сс. 21–22].

**Замечание 4.2.** Степенной ряд $h(f)$ является обратимым в $A = R_\sigma[[x]]$.

Действительно, $h(f) = a_n + a_{n+1}x + a_{n+2}x^2 + \cdots$, где $a_n \in R^*$ по условию. Дальше всё вытекает из следствия 3.5.

Введем обозначения $H(x) = h(g(x))$, $V(x) = U(x)h(f(x))$ и $M(x) = h(f(x))^{-1}r(f(x))$ ($H$, $V$ и $M$ – ряды из $A$). Заметим, что $H(x)$ и $M(x)$

можно определить из заданных нам $f$ и $g$. Теперь (12) можно записать, как $H = h(VM) + V$. Наконец, введем на $R_\sigma[[x]]$ еще один линейный оператор, $s$: $s(P(x)) = h(P(x)M(x))$. Получаем самую простую запись для (11) и (12):

$$H = s(V) + V. \tag{13}$$

Теперь нужно решить это уравнение, а затем перейти обратно к исходным обозначениям. Этому посвящен следующий, заключительный параграф.

## 5. Доказательство теоремы 2

Здесь и далее мы будем без особых пояснений использовать обозначения параграфа 4.

Формально, в качестве решения уравнения (13) подходит

$$V = H - s(H) + s^2(H) - s^3(H) + \cdots, \tag{14}$$

но нужны дополнительные пояснения по поводу сходимости.

Обозначим $\mathfrak{m}_\sigma^k[[x]]$ подмножество в $R_\sigma[[x]]$, состоящее из рядов, все коэффициенты которых лежат в $\mathfrak{m}^k$ ($k$ натуральное), а также $\mathfrak{m}_\sigma^0[[x]] = R_\sigma[[x]]$. Очевидно, что $\mathfrak{m}_\sigma^k[[x]]$ – подгруппа по сложению в $R_\sigma[[x]]$.

**Лемма 5.1.** *Если*

$$P(x) \in \mathfrak{m}_\sigma^k[[x]] \quad \text{и} \quad Q(x) \in \mathfrak{m}_\sigma[[x]],$$

*то* $P(x)Q(x) \in \mathfrak{m}_\sigma^{k+1}[[x]]$.

Легко видеть, что это действительно так, пользуясь формулой (3) для перемножения рядов и $\mathfrak{m}$-инвариантностью $\sigma$.

**Лемма 5.2.** *Если* $P(x) \in \mathfrak{m}_\sigma^k[[x]]$, *то* $s(P(x)) \in \mathfrak{m}_\sigma^{k+1}[[x]]$.

Из условия следует, что $r(f) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ лежит в $\mathfrak{m}_\sigma[[x]]$. Применив лемму 5.1 для $h(f)^{-1}$ и $r(f)$ ($k = 0$), получим $M(x) = h(f)^{-1}r(f) \in \mathfrak{m}_\sigma[[x]]$. Применим эту лемму еще раз для $P(x)$ и $M(x)$, придем к $P(x)M(x) \in \mathfrak{m}_\sigma^{k+1}[[x]]$. По определению, $s(P(x)) = h(P(x)M(x))$ и следовательно, тоже лежит в $\mathfrak{m}_\sigma^{k+1}[[x]]$, ч.т.д.

**Лемма 5.3.** *Для любого $P(x) \in R_\sigma[[x]]$ и $k \in \mathbb{N}$ имеем $s^k(P) \in \mathfrak{m}_\sigma^k[[x]]$.*

Доказывается индукцией по $k$, с применением леммы 5.2.

**База:** $k = 0$, $P(x) \in \mathfrak{m}_\sigma^0[[x]] = R_\sigma[[x]]$.

**Переход:** пусть, по предположению индукции, $s^k(P) \in \mathfrak{m}_\sigma^k[[x]]$ – применим к нему лемму 5.2. Получится, что

$$s(s^k(P)) = s^{k+1}(P) \in \mathfrak{m}_\sigma^{k+1}[[x]].$$

Таким образом, лемма доказана.

Применим лемму 5.3 к $H(x)$ и рассмотрим равенство (14). У каждого очередного слагаемого $(-1)^k s^k(H)$ все коэффициенты лежат в $\mathfrak{m}^k$. При любом $i \in \mathbb{N}$ сумма коэффициентов при $x^i$ будет сходиться к некоторому предельному значению (используем полноту кольца $R$), которое мы и объявим коэффициентом $V(x)$ при $x^i$.

**Утверждение 5.4.** *Построенный ряд $V(x)$ является решением уравнения $H = s(V) + V$.*

Введем удобные обозначения для частичных сумм в правой части уравнения (14)

$$V_k(x) = H(x) - s(H(x)) + \cdots + (-1)^k s^k(H(x)). \tag{15}$$

Легко видеть, что $V(x) - V_k(x) \in \mathfrak{m}_\sigma^{k+1}[[x]]$, а следовательно (лемма 5.2) $s(V(x) - V_k(x)) \in \mathfrak{m}_\sigma^{k+2}[[x]] \subset \mathfrak{m}_\sigma^{k+1}[[x]]$. Поэтому мы имеем

$$\begin{aligned} s(V) + V &= s(V - V_k + V_k) + V - V_k + V_k \\ &= s(V_k) + V_k + s(V - V_k) + V - V_k \\ &\equiv s(V_k) + V_k = H + (-1)^k s^{k+1}(H) \equiv H \bmod \mathfrak{m}_\sigma^{k+1}[[x]]. \end{aligned}$$

Таким образом, разность $s(V) + V - H$ имеет коэффициенты в $\mathfrak{m}^{k+1}$ при любом натуральном $k$. Но в полном локальном кольце $R$ пересечение этих идеалов по всем $k$ равно нулю, так что и указанная разность равна нулю. Это и означает, что утверждение доказано.

**Утверждение 5.5.** *$V(x)$ является единственным решением уравнения $H = s(V) + V$.*

Пусть имеется два различных решения, $V(x)$ и $W(x)$. Так как их разность ненулевая, то существует *наибольшее* такое $k$, что $V(x) - W(x) \in \mathfrak{m}_\sigma^k[[x]]$. Поскольку $s(V) + V = H = s(W) + W$, то

$$V(x) - W(x) = s(W(x)) - s(V(x)) = -s(V(x) - W(x)). \tag{16}$$

По лемме 5.2, правая часть этого уравнения лежит в $\mathfrak{m}_\sigma^{k+1}[[x]]$. Значит, там же лежит и левая часть – но это противоречит выбору $k$, как наибольшего. Получаем противоречие, так что $V(x)$ – единственное решение.

Теперь завершим доказательство теоремы 2. Возьмем построенное нами $V(x)$ и положим $U(x) = V(x)h(x)^{-1}$. Так как $V(x)$ – решение уравнения (13), то $U(x)$ удовлетворяет уравнениям (11) и (12) (см. преобразования в параграфе 4). Так как $h(g(x) - U(x)f(x)) = 0$, эта разность имеет вид $b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$. Уравнение (6) для них, таким образом, выполняется. Из единственности $V(x)$ (утверждение 5.5) следует единственность $U(x)$, а из нее – единственность $b_0$, $b_1$, ... $b_{n-1}$. Теорема 2 полностью доказана.

## Литература


1. О. Зарисский, П. Самюэль, *Коммутативная алгебра*, т. 2, М., 1963.
2. Ю. И. Манин, *Круговые поля и модулярные кривые.* — Усп. мат. наук **XXVI** (1971), вып. 6, 7–72.
3. М. Атья, И. Макдональд, *Введение в коммутативную алгебру.* Мир, М., 1972.



Ferens-Sorotskiy E. V. Weierstrass preparational theorem for noncommutative rings.

A power series over complete local ring can be canonically decomposed into product of an invertible power series and an unital polynomial, which degree coincides with the number of first invertible coefficient. This statement is known as Weierstrass preparation theorem. It follows from a more general statement, known as Weierstrass division theorem. The given article contains a detailed proof of generalizations of Weierstrass preparation theorem and Weierstrass division theorem for so-called rings of skew power series. Such rings arise in number theory, at first, in studies of formal groups over local fields.



С.-Петербургский
государственный университет
*E-mail*: sorotskiy@rambler.ru


Поступило 12 ноября 2008 г.