Московский Государственный Университет
имени М. В. Ломоносова

Механико-математический факультет

Кафедра высшей геометрии и топологии

Курсовая работа

Об универсальной формальной группе

Черных Георгий
303 группа

Научный руководитель:
Панов Т. Е.

2016 г.

Введение

В данной работе элементарными методами (основанными на теоретико-числовых свойствах биномиальных коэффициентов) доказана важная теорема из теории одномерных коммутативных формальных групп - теорема Лазара о строении универсальной формальной группы.

Основные определения

Все кольца будут предполагаться ассоциативными коммутативными с единицей.

Определение 1. **(Одномерной коммутативной) формальной группой над кольцом R** называется формальный степенной ряд $F(x,y) \in R[[x,y]]$, удовлетворяющий следующим условиям:

1) $F(x,0) = F(0,x) = x$
2) $F(F(x,y),z) = F(x,F(y,z))$
3) $F(x,y) = F(y,x)$

Если $F(x,y) = x+y+\sum\limits_{i,j>0} \alpha_{i,j}x^iy^j$ - формальный ряд над R_1 и $r\colon R_1 \to R_2$ - кольцевой гомоморфизм, то будем обозначать через $r[F]$ формальный ряд $r[F](x,y) = x+y+\sum\limits_{i,j>0} r(\alpha_{i,j})x^iy^j$ над R_2. Ясно, что если $F(x,y)$ является формальной группой, то таковой будет и $r[F](x,y)$.

Определение 2. Формальная группа $F_1(x,y)$ над кольцом R_1 называется **универсальной**, если для любой формальной группы $F_2(x,y)$ над любым кольцом R_2 существует единственный такой кольцевой гомоморфизм $r\colon R_1 \to R_2$, что $r[F_1] = F_2$. Кольцо R_1 в этом случае также называется **универсальным**.

Как обычно, из единственности r следует единственность универсального кольца с точностью до изоморфизма. (Действительно, если есть два универсальных кольца R_1 и R_2 с универсальными формальными группами F_1 и F_2 соответственно, то существуют гомоморфизмы $r_1\colon R_1 \to R_2$ и $r_2\colon R_2 \to R_1$, такие что $r_1[F_1] = F_2$ и $r_2[F_2] = F_1$. Но тогда $r_1r_2[F_2] = F_2 = \mathrm{id}[F_2]$ и $r_2r_1[F_1] = F_1 = \mathrm{id}[F_1]$, и из единственности гомоморфизма в определении универсальной группы получаем, что $r_1r_2 = \mathrm{id}$, $r_2r_1 = \mathrm{id}$, т.е. r_1 и r_2 - взаимообратные изоморфизмы.) С другой стороны, ясно также, что если F - универсальная формальная группа над универсальным кольцом R и $f\colon R \to \hat{R}$ - изоморфизм колец, то $\hat{R}$ - универсальное кольцо с универсальной группой $f[F]$.

Существование универсальной формальной группы и формулировка основной теоремы

Легко видеть, что универсальная формальная группа существует. Действительно, рассмотрим градуированное кольцо $E = \mathbb{Z}[\alpha_{i,j},\, i,j > 0]$, $\deg \alpha_{i,j} =$

$2(i+j-1)$, и формальный ряд $e(x,y) = x + y + \sum \alpha_{i,j} x^i y^j$. Образуем ряды $e(e(x,y),z) = x+y+z+\sum p_{i,j,k} x^i y^j z^k$ и $e(x,e(y,z)) = x+y+z+\sum q_{i,j,k} x^i y^j z^k$. Заметим, что $\deg p_{i,j,k} = \deg q_{i,j,k} = 2(i+j+k-1)$. Обозначим через I - идеал, порождённый $(\alpha_{i,j} - \alpha_{j,i})$ и $(p_{i,j,k} - q_{i,j,k})$. Рассмотрим теперь градуированное факторкольцо $\mathcal{R}_\mathcal{U} = E/I$ и каноническую проекцию $\pi\colon E \to \mathcal{R}_\mathcal{U}$.

Из определения идеала I следует, что $\mathcal{F}_\mathcal{U} = \pi[e]$ - формальная группа.

Пусть теперь $F(x,y) = x + y + \sum a_{i,j} x^i y^j$ - произвольная формальная группа над произвольным кольцом R. Из определения формальной группы следует, что гомоморфизм $r_0\colon E \to R$, $r_0(\alpha_{i,j}) = a_{i,j}$ равен нулю на идеале I. Следовтаельно, он разлагается в композицию гомоморфизмов $E \xrightarrow{\pi} \mathcal{R}_\mathcal{U} \xrightarrow{r} R$, и $r[\mathcal{F}_\mathcal{U}] = r[\pi[e]] = r_0[e] = F$. С другой стороны, единственность гомомморфизма r из определния универсальной формальной группы следует из того, что коэффициенты $\mathcal{F}_\mathcal{U}$ (равные $\pi(\alpha_{i,j}) = \bar{\alpha}_{i,j}$) порождают $\mathcal{R}_\mathcal{U}$.

То есть, мы посторили универсальную группу $\mathcal{F}_\mathcal{U} = x + y + \sum \bar{\alpha}_{i,j} x^i y^j$ над универсальным кольцом $\mathcal{R}_\mathcal{U}$.

Оказывается, универсальное кольцо (структура которого не очень ясна из приведённой только что конструкции) изоморфно кольцу многочленов, т. е. верна следующая

Теорема (Лазар).
Универсальное кольцо $\mathcal{R}_\mathcal{U}$ изоморфно кольцу $\mathbb{Z}[b_1, b_2, \ldots]$, $\deg b_i = 2i$.

Прежде чем приступить непосредственно к доказательству теоремы проведём некоторую подготовительную работу.

Вспомогательные утверждения

Фиксируем произвольное натуральное $n \geqslant 2$.

Пусть $d(n) = \text{НОД}\left(\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}\right)$. Фиксируем целые числа $\lambda_1^{(n)}, \ldots, \lambda_{n-1}^{(n)}$, т. ч. $\dfrac{\lambda_1^{(n)}}{d(n)}\binom{n}{1} + \ldots + \dfrac{\lambda_{n-1}^{(n)}}{d(n)}\binom{n}{n-1} = 1$.

Рассмотрим теперь формальные переменные $x_1, \ldots, x_{n-1}$ т. ч. $x_i = x_{n-i}$ $(1 \leqslant i \leqslant n-1)$. Определим следующие линейные формы: $\lambda^{(n)}(\mathbf{x}) = \lambda_1^{(n)} x_1 + \ldots + \lambda_{n-1}^{(n)} x_{n-1}$ и $P_{i,j}^{(n)}(\mathbf{x}) = \binom{n-i}{j} x_i - \binom{n-j}{i} x_j$ $(i, j \geqslant 1,\ i+j < n)$. (Заметим, что если $i + j = n$, то автоматически получаем $P_{i,n-i}^{(n)}(\mathbf{x}) = \binom{n-i}{n-i} x_i - \binom{i}{i} x_{n-i} = x_i - x_{n-i} = 0$.)

Лемма.

Каждая переменная x_i выражается в виде целочисленной линейной комбинации форм $\lambda^{(n)}(\mathbf{x})$ и $P_{i,j}^{(n)}(\mathbf{x})$.

Следствие.

Линейная комбинация (с целыми коэффициентами) $c_1x_1+\ldots+c_{n-1}x_{n-1}$ такая, что $\frac{c_1}{d(n)}\binom{n}{1}+\ldots+\frac{c_{n-1}}{d(n)}\binom{n}{n-1}=0$, выражается лишь через линейные формы $P_{i,j}^{(n)}(\mathbf{x})$.

(т. к. подстановка $x_i=\binom{n}{i}$ показывает, что $\frac{c_1}{d(n)}\binom{n}{1}+\ldots+\frac{c_{n-1}}{d(n)}\binom{n}{n-1}$ - это в точности коэффициент при $\lambda^{(n)}(\mathbf{x})$.)

Доказательство леммы.

Породим нашими формальными переменными (различными, т. е. $x_1,\ldots,x_{[n/2]}$) свободную абелеву группу M, а формами $\lambda^{(n)}$ и $P_{i,j}^{(n)}$ (как формальными символами) - группу N. Имеем естественное отображение $\psi\colon N\to M$, $\psi(\lambda^{(n)})=\lambda^{(n)}(\mathbf{x})$, $\psi(P_{i,j}^{(n)})=P_{i,j}^{(n)}(\mathbf{x})$, и наша цель - доказать, что оно сюръективно.

Если $\operatorname{rk}\psi(N)<\operatorname{rk}M$, то существует ненулевой набор $\mathbf{c}=(c_1,\ldots,c_{n-1})\in\mathbb{Z}^{n-1}$, $c_i=c_{n-i}$, зануляющий все формы $\lambda^{(n)}(\mathbf{x})$ и $P_{i,j}^{(n)}(\mathbf{x})$ одновременно. (Действительно, выберем в $\psi(N)$ базис $e_1,\ldots,e_m$, $m<\operatorname{rk}M=[n/2]$. Пусть $e_i=\sum a_i^jx_j$ и $\psi(\lambda^{(n)})=\sum\alpha^ie_i$, $\psi(P_{i,j}^{(n)})=\sum\beta_{i,j}^ke_k$. Рассмотрим линейную систему уравнений $\{a_i^1y_1+\ldots+a_i^{[n/2]}y_{[n/2]}=0\}_{i=1}^m$. Уравнений меньше, чем переменных, поэтому система имеет ненулевое решение в $\mathbb{Q}$. Домножив его теперь на общий знаменатель, получим целочисленное решение $(c_1,\ldots,c_{[n/2]})$, а из него симметрией получаем $\mathbf{c}$. Осталось заметить, что $\lambda^{(n)}(\mathbf{c})=\sum\alpha^i(\sum a_i^jc_j)=0$, $P_{i,j}^{(n)}(\mathbf{c})=\sum\beta_{i,j}^k(\sum a_k^sc_s)=0$.)

Если же $\operatorname{rk}\psi(N)=\operatorname{rk}M$, но $\det\psi(N)\neq\pm1$, то $\det\psi(N)$ делится на некоторое простое число p. Тогда после приведения по модулю p определитель станет равным нулю, а значит, существует ненулевой набор $\mathbf{c}=(c_1,\ldots,c_{n-1})\in\mathbb{Z}_p^{n-1}$, $c_i=c_{n-i}$, зануляющий (по модулю p) все формы $\lambda^{(n)}(\mathbf{x})$ и $P_{i,j}^{(n)}(\mathbf{x})$ одновременно (те же рассуждения, что и выше: ранг системы меньше числа переменных, что влечёт существование ненулевого решения в $\mathbb{Z}_p^{[n/2]}$).

А условие $\det\psi(N)=\pm1$ как раз равносильно сюръективности ψ.

То есть, мы видим, что достаточно (и необходимо) показать, что для любого простого p не существует ненулевого набора $(c_1,\ldots,c_{n-1})\in\mathbb{Z}_p^{n-1}$, $c_i=c_{n-i}$, зануляющего (по модулю p) все формы $\lambda^{(n)}(\mathbf{x})$ и $P_{i,j}^{(n)}(\mathbf{x})$ одновременно (если мы нашли целочисленный зануляющий набор $(c_1,\ldots,c_{n-1})$, то, выбрав p, не делящее все c_i одновременно, мы получим ненулевой зануляющий набор из $\mathbb{Z}_p^{n-1}$).

Это мы и докажем.

Фиксируем простое число p. Все сравнения будут по этому модулю.

Пусть $\mathbf{c}=(c_1,\ldots,c_{n-1})\in\mathbb{Z}_p^{n-1}$, $c_i=c_{n-i}$ и $\lambda^{(n)}(\mathbf{c})\equiv0$, $P_{i,j}^{(n)}(\mathbf{c})\equiv0$.

Покажем, что $\mathbf{c}\equiv0$.

Положим $t_k=\frac{1}{d(n)}\binom{n}{k}$. Будем обозначать буквой s такое число, что

$t_s \not\equiv 0$.

Заметим, что для того, чтобы $\mathbf{c}$ был нулевым (в $\mathbb{Z}_p^{n-1}$), достаточно следующего условия:

а) Для всех $k = 1, \ldots, n-1$ выполнено сравнение $c_k \equiv t_k c_s t_s^{-1}$, которое мы будем обозначать $C(k)$

Действительно, из него следует, что $0 \equiv \lambda^{(n)}(\mathbf{c}) \equiv \sum \lambda_k^{(n)} c_k \equiv c_s t_c^{-1} \sum \lambda_k^{(n)} t_k \equiv c_s t_c^{-1}$. Следовтаельно, $c_s \equiv 0$, а значит, $c_k \equiv 0$ для всех k.

Кроме того, заметим, что $\binom{n-k}{s} \not\equiv 0 \Rightarrow C(k)$ и $\binom{k}{s} \not\equiv 0 \Rightarrow C(n-k)$.

В самом деле, если, например, $\binom{n-k}{s} \not\equiv 0$, то $0 \equiv P_{s,k}^{(n)}(\mathbf{c}) \equiv \binom{n-s}{k} c_s - \binom{n-k}{s} c_k = \binom{n-k}{s} (c_s \binom{n-s}{k} \Big/ \binom{n-k}{s} - c_k) \equiv \binom{n-k}{s} (c_s t_k t_s^{-1} - c_k)$, то есть, $c_k \equiv t_k c_s t_s^{-1}$ или $C(k)$. Аналогично, $\binom{k}{s} \not\equiv 0 \Rightarrow C(n-k)$.

Но ясно, что $C(k) \Leftrightarrow C(n-k)$, поэтому имеем $\binom{n-k}{s} \not\equiv 0 \Rightarrow C(k), C(n-k)$ (и аналогично $\binom{k}{s} \not\equiv 0 \Rightarrow C(n-k), C(k)$).

Отсюда, в частности, получаем, что следующее условие

б) Для всех $k = 1, \ldots, n-1$ хотя бы одно из чисел $\binom{n-k}{s}$, $\binom{k}{s}$ не кратно p

влечёт условие а), а значит, и то, что $\mathbf{c} \equiv 0$.

Рассмотрим теперь три случая.

1) n не кратно p. Тогда мы можем выбрать $s = 1$. В этом случае для любого $k = 1, \ldots, n-1$ либо k, либо $n-k$ не кратно p. То есть, выполнено б). Значит, $\mathbf{c} \equiv 0$.

Для оставшихся двух случаев нам понадобится следующее утверждение из теории чисел:

Теорема Куммера

Порядок вхождения простого числа p в разложение на простые множители числа $\binom{n}{m}$ равен количеству переносов в следующий разряд, возникающих при сложении m и $n-m$ в p-ичной системе счисления.

Кроме того, заметим, что $\binom{pm}{pk} = \frac{(pm)!}{(pk)!\,(p(m-k))!} =$

$$= \frac{1 \ldots p\ (p+1) \ldots 2p \ldots (m-1)p+1 \ldots mp}{(1 \ldots p\ (p+1) \ldots 2p \ldots (k-1)p+1 \ldots kp)(1 \ldots p\ (p+1) \ldots 2p \ldots (m-k-1)p+1 \ldots (m-k)p)} =$$

$$= \frac{(m-k)p+1 \ldots (m-k+1)p \ldots (m-1)p+1 \ldots mp}{1 \ldots p \ldots (k-1)p+1 \ldots kp} = \binom{m}{k} \frac{\prod\limits_{i=0}^{k-1} \prod\limits_{j=1}^{p-1} (m-k+i)p+j}{\prod\limits_{i=0}^{k-1} \prod\limits_{j=1}^{p-1} ip+j} =$$

$= \binom{m}{k}\omega,\ \omega \equiv 1 \pmod{p}$.

В частности, $\binom{p^i m}{p^i} = \binom{p^{i-1}m}{p^{i-1}}\omega_1 = \binom{p^{i-2}m}{p^{i-2}}\omega_1\omega_2 = \ldots = \binom{m}{1}\omega_1 \ldots \omega_i = m\omega,\ \omega \equiv 1 \pmod{p}$.

Отсюда следует, например, $d(n) = \begin{cases} p, & \text{если } n = p^k, \text{ где } p \text{ - простое число} \\ 1, & \text{иначе} \end{cases}$.

2) $n = p^m$, $m > 0$. Тогда мы можем положить $s = p^{m-1}$, т. к. $\binom{p^m}{p^{m-1}} = p(1+\alpha p)$ и $t_s = \frac{1}{p}\binom{p^m}{p^{m-1}} \equiv 1$. И в этом случае опять же выполнено условие б). Действительно, для любого $k = 1, \ldots, n-1$ по крайней мере одно из чисел k, $n-k$ не меньше s, и если, например, $k \geqslant s$, то по теореме Куммера получаем, что $\binom{k}{s}$ не делится на p (действительно, $n = p^m > k = x + s = x + p^{m-1}$, т. е. $0 \leqslant x < (p-1)p^{m-1}$ и поэтому ясно, что при сложении x и s переносов не происходит).

3) $n = p^m v$, где $v > 1$ и $p \nmid v$. Мы можем считать, что $s = p^m$, т. к. $t_s = \binom{p^m v}{p^m} = v \not\equiv 0$ (поскольку $d(n) = 1$).

Будем доказывать справедливость условия а).

Если для некоторого k хотя бы один из биномиальных коэффициентов $\binom{k}{s}$, $\binom{n-k}{s}$ не кратен p, то, как мы видели выше, справедливо $C(k)$.

Пусть теперь для некоторого k_0 оба биномиальных коэффициента $\binom{k_0}{s}$, $\binom{n-k_0}{s}$ кратны p.

Заметим, что при $k < s$ из теоремы Куммера получаем, что $\binom{n-k}{s}$ не кратно p (т. к. $0 < k < s = p^m$, $n - k = vp^m - k = (v-1)p^m + (p^m - k)$, $v - 1 > 0$, то $n - k - s = (v-2)p^m + (p^m - k)$, $v - 2 \geqslant 0$ и при сложении $n - k - s$ и s переносов не происходит). Аналогично, при $n - k < s$ имеем, что $\binom{k}{s}$ не кратно p.

Отсюда, во-первых, мы заключаем, что $k_0 \geqslant s$ и $n - k_0 \geqslant s$.

Во-вторых, т. к. $\binom{n-k}{s} \not\equiv 0 \ \Rightarrow\ C(k)$, при $k < s$ получаем, что $c_k \equiv t_k c_s t_s^{-1} \equiv 0$, поскольку $t_k = \binom{n}{k} \equiv 0$ (опять по теореме Куммера).

Но если $k_0 \geqslant s$ и $n - k_0 \geqslant s$, то мы можем применить теорему Куммера к обоим биномиальным коэффициентам $\binom{k_0}{s}$, $\binom{n-k_0}{s}$. Из неё получаем,

что для того, чтобы $\binom{k_0}{s}, \binom{n-k_0}{s}$ делились на p, числа k_0 и $n-k_0$ должны иметь ноль в m-ом разряде в p-ичной системе счисления. То есть, $k_0 = i_1 + p^{m+1}x_1$ и $n-k_0 = i_2 + p^{m+1}x_2$, где $0 \leqslant i_1, i_2 < p^m$, $x_1, x_2 > 0$. Так как $n = k_0 + (n-k_0)$ не делится на p^{m+1}, то одно из чисел i_1, i_2 отлично от нуля.

Пусть, например, $n - k_0 = i + p^{m+1}x$, $0 < i < p^m$, $x > 0$. Тогда $0 \equiv P_{i,k_0}(\mathbf{c}) = \binom{n-i}{k_0}c_i - \binom{n-k_0}{i}c_{k_0}$. Но $c_i \equiv 0$ (т. к. $i < p^m = s$), а $\binom{n-k_0}{i} \not\equiv 0$ (по теореме Куммера: ясно, что при сложении $n-k_0-i = p^{m+1}x$ и $i < p^m$ переносов не происходит). Значит, получаем, что $c_{k_0} \equiv 0$.

Но если $n - k_0 = i + p^{m+1}x$, $0 < i < p^m$, $x > 0$, а $n = p^m v$, $v > 1$, то по теореме Куммера получаем, что $\binom{n}{n-k_0} \equiv 0$, т. е. $t_{n-k_0} = t_{k_0} \equiv 0$. То есть, $c_{k_0} \equiv 0$ равносильно $C(k_0)$.

Таким образом, мы видим, что для любого k выполнено $C(k)$, т. е. выполнено условие а).

Ч.Т.Д.

Доказательство теоремы

Вернёмся к теореме Лазара.

Обозначим градуированное кольцо $\mathbb{Z}[b_1, b_2, \ldots]$, $\deg b_i = 2i$ через B. Рассмотрим ряд $g(x) = x + \sum b_i x^{i+1}$. Положим $F_0(x,y) = g^{-1}(g(x)+g(y)) = x + y + \sum\limits_{i,j>0} a_{i,j}x^i y^j$ (ясно, что F_0 - формальная группа над B) и обозначим через A_0 подкольцо в B, порождённое коэффициентами $a_{i,j}$ (т. к. $\deg a_{i,j} = 2(i+j-1)$, то A_0 - градуированное подкольцо в B). Пусть $r_0 \colon \mathcal{R}_\mathcal{U} \to A_0$ - гомоморфизм, соответствующий формальной группе F_0.

Обозначим через $I_{\mathcal{R}_\mathcal{U}}, I_{A_0}$ и I_B идеалы, порождённые разложимыми элементами в кольцах $\mathcal{R}_\mathcal{U}, A_0$ и B соответственно. $I_{A_0} \subset I_B$.

Легко видеть, что $F_0(F_0(x,y),z) \equiv x+y+z+\sum a_{i,j}(x+y)^i z^j$, $F_0(x,F_0(y,z)) \equiv x+y+z+\sum a_{i,j}x^i(y+z)^j \pmod{I_{A_0}}$.

Отсюда, приравнивая коэффициенты при $x^i y^j z^k$, получаем: $\binom{i+j}{i}a_{i+j,k} \equiv \binom{j+k}{j}a_{i,j+k} \pmod{I_{A_0}}$ или $(i+j+k=n)$ $\binom{i+j}{i}a_{i+j,k} - \binom{j+k}{j}a_{i,j+k} = \binom{i+j}{i}a_{k,i+j} - \binom{j+k}{k}a_{i,j+k} = \binom{n-k}{i}a_{k,n-k} - \binom{n-i}{k}a_{i,n-i} = P^{(n)}_{k,i}(\mathbf{a}) \equiv 0 \pmod{I_{A_0}}$, где $\mathbf{a} = (a_{1,n-1}, a_{2,n-2}, \ldots, a_{n-1,1})$.

Введём теперь элементы $e_{n-1} = \sum\limits_{i=1}^{n-1} \lambda_i^{(n)} a_{i,n-i}$ $(\deg e_i = 2i)$.

Заметим, что форма $a_{i,j} - \binom{n}{i}\frac{e_{n-1}}{d(n)}$ $(i+j=n)$ удовлетворяет условиям следствия из вышедоказанной леммы (как форма от $(a_{1,n-1}, a_{2,n-2}, \ldots, a_{n-1,1})$).

Значит, согласно этому следствию, она выражается через $P_{k,s}(\mathbf{a}) \equiv 0$, т. е. $a_{i,n-i} - \binom{n}{i}\frac{e_{n-1}}{d(n)} \equiv 0 \pmod{I_{A_0}}$.

Совершенно ангалогично, вводя в кольце $\mathcal{R}_{\mathcal{U}}$ элементы $\bar{e}_{n-1} = \sum\limits_{i=1}^{n-1} \lambda_i^{(n)} \bar{\alpha}_{i,n-i}$, мы получаем $\bar{\alpha}_{i,n-i} - \binom{n}{i}\frac{\bar{e}_{n-1}}{d(n)} \equiv 0 \pmod{I_{\mathcal{R}_{\mathcal{U}}}}$

Заметим теперь, что $g^{-1}(x) \equiv x - \sum b_i x^{i+1} \pmod{I_B}$ и $F_0(x,y) \equiv x + \sum b_i x^{i+1} + x + \sum b_i y^{i+1} - \sum b_i (x+y)^{i+1} = x + y - \sum b_i ((x+y)^{i+1} - x^{i+1} - y^{i+1}) \pmod{I_B}$.

Отсюда получаем, приравнивая коэффициенты при $x^i y^j$, что $a_{i,j} \equiv \binom{i+j}{i} b_{i+j-1} \pmod{I_B}$.

То есть, в итоге, имеем: $nb_{n-1} \equiv a_{1,n-1} \equiv \frac{n}{d(n)} e_{n-1} \pmod{I_B}$.

Отсюда уже несложно получить, что e_n алгебраически независимы и порождают A_0.

Действительно, докажем, что через e_n выражаются $a_{i,j}$. Проведём индукцию по $\deg a_{i,j} = 2(i+j-1)$. При $i+j-1 = 1$, имеем, что $e_1 \equiv a_{1,1} \pmod{I_{A_0}}$, но так как e_1 и $a_{1,1}$ имеют минимальную положительную степень, то на самом деле имеем равенство $e_1 = a_{1,1} (= 2b_1)$. Но если мы уже выразили через e_n все $a_{i,j}$ с $\deg a_{i,j} < k$, то: $a_{i,k-i} = \binom{k}{i}\frac{e_{k-1}}{d(k)} +$ (элементы, разложимые в произведение $a_{i,j}$ с $\deg a_{i,j} < k$) $= \binom{k}{i}\frac{e_{k-1}}{d(k)} +$ (элементы, выражаемые через e_n), т. е. $a_{i,k-i}$ тоже выражается через e_n.

Совершенно аналогичные рассуждения доказывают, что $\bar{e}_n$ - порождают $\mathcal{R}_{\mathcal{U}}$.

Проверим, что e_n алгебраически независимы. Проведём индукцию по n. Так как $e_1 = 2b_1$, то e_1 алгебраически независим. Пусть мы доказали, что $e_1, \ldots, e_{n-1}$ - алгебраически независимы. и $P(e_1, \ldots, e_n) = 0$, где $P(x_1, \ldots, x_n) = \sum\limits_{k=0}^{N} x_n^k P_k(x_1, \ldots, x_{n-1})$ - многочлен с целыми коэффициентами. В силу, $(i+1)b_i \equiv \frac{i+1}{d(i+1)} e_i \pmod{I_B}$ имеем: $\frac{i+1}{d(i+1)} e_i = (i+1)b_i + Q_i(b_1, \ldots, b_{i-1})$.

Пусть $A_n = \frac{n+1}{d(n+1)} \ldots \frac{2}{d(2)}$. Тогда, домножив на достаточно большую

степень A_n^M, получим

$$0 = \sum_{k=0}^{N} A_n^M e_n^k P_k(e_1, \ldots, e_{n-1}) =$$

$$= \sum_{k=0}^{N} ((n+1)b_n + Q_n(b_1, \ldots, b_{n-1}))^k A_n^{n_k} P_k(2b_1, \ldots, nb_{n-1} + Q_{n-1}(b_1, \ldots, b_{n-2})) =$$

$$= b_n^N (n+1)^N A_n^{n_N} P_N(2b_1, \ldots, nb_{n-1} + Q_{n-1}(b_1, \ldots, b_{n-2})) + T(b_1, \ldots, b_n),$$

где T - многочлены с целыми коэффициентами, причём степень b_n в нём строго меньше N. Значит, $P_N(2b_1, \ldots, nb_{n-1} + Q_{n-1}(b_1, \ldots, b_{n-2})) = 0$, т.е. $P_N(e_1, \ldots, e_{n-1}) = 0$. Отсюда, в силу индуктивного предположения, следует, что $P_N(x_1, \ldots, x_{n-1}) \equiv 0$. Таким образом, понижая степень и избавляясь от переменных, мы получим, что $P(x_1, \ldots, x_n) \equiv 0$, т. е. $e_1, \ldots, e_n$ - алгебраически независимы.

Но то, что e_n алгебраически независимы и порождают A_0, означает, что отображение $f\colon B \to A_0$, $b_i \mapsto e_i$ является изоморфизмом.

А так как $\bar{e}_n$ - порождают $\mathcal{R}_{\mathcal{U}}$, то отображение $\bar{f}\colon B \to \mathcal{R}_{\mathcal{U}}$, $b_i \mapsto \bar{e}_i$ - сюръективно.

Но оно инъективно, так как инъективно f, совпадающее со сквозным отображением $B \xrightarrow{\bar{f}} \mathcal{R}_{\mathcal{U}} \xrightarrow{r_0} A_0$.

То есть, $\bar{f}\colon B \to \mathcal{R}_{\mathcal{U}}$ - искомый изоморфизм колец.

Таким образом, теорема Лазара полностью доказана.

Список литературы

[1] В. М. Бухштабер, А. В. Устинов. Кольца коэффициентов формальных групп

[2] Р. Стонг. Заметки по теории кобордизмов (Добавление В. М. Бухштабера. Новые методы в теории кобордизмов)

[3] M. Hazewinkel. Formal groups and applications.