МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

*УДК 515.143.533*

Емельянов Данила Юрьевич

# О базисах алгебры Стинрода

Специальность 01.01.04 —
«геометрия и топология»

Диссертация на соискание учёной степени кандидата
физико-математических наук

Научный руководитель:
кандидат физико-математических наук
Фёдор Юрьевич Попеленский

Москва — 2017

# Содержание

# Введение

Алгебра Стинрода $\mathcal{A}_p$ — это алгебра стабильных когомологических операций в когомологиях с коэффициентами в $\mathbb{Z}/p$.

В наиболее общем определении стабильная когомологическая операция — это последовательность $\{\varphi_n\}$ гомоморфизмов $\varphi_n : H^n(X;\Pi) \to H^{n+q}(X;G)$, где $\Pi$ и $G$ — абелевы группы, естественных по $X$ и перестановочных с изоморфизмом надстройки $\Sigma$. Множество всех таких операций образует абелеву группу, обозначим её $\mathcal{O}^S(q,\Pi,G)$.

Тривиальный пример когомологической операции представляет тождественное отображение. Бокштейном в статье [16] был описан связывающий гомоморфизм $\beta$ в длинной точной когомологической последовательности, соответствующей короткой точной последовательности коэффициентов

$$0 \to \mathbb{Z}/p \to \mathbb{Z}/p^2 \to \mathbb{Z}/p \to 0.$$

Таким образом, $\beta \in \mathcal{O}^S(1,\Pi,G)$. Примерно в тоже время Л. С. Понтрягиным в статье [17] рассматривалась операция $\dot{\times}$ позволяющая описать с точностью до гомотопии всевозможные отображения трехмерной сферы в $n$-мерный комплекс с тривиальной фундаментальной группой. Общая конструкция таких операций была предложена Н. Стинродом в работе [18], где были описаны операции $Sq^q \in \mathcal{O}^S(q,\mathbb{Z}/2,\mathbb{Z}/2)$. В последствии в литературе операции $Sq^i$ стали называться квадратами Стинрода, тогда как аналогичные операции $P^i \in \mathcal{O}^S(q,\mathbb{Z}/p,\mathbb{Z}/p)$, где $p > 2$ —простое число, стали называть степенями Понтрягина.

Структура кольца в $\bigoplus\limits_q \mathcal{O}^S(q,G,G)$ задаётся при помощи композиции операций: в качестве произведения операций $\varphi' \in \mathcal{O}^S(q_1,G,G)$ и $\varphi'' \in \mathcal{O}^S(q_2,G,G)$ берётся их композиция $\varphi' \circ \varphi''$, которая также является стабильной операцией $\varphi' \circ \varphi'' \in \mathcal{O}^S(q_1+q_2,\Pi,G)$. Введённое умножение ассоциативно и не коммутативно. Таким образом $\bigoplus\limits_q \mathcal{O}^S(q,G,G)$ является градуированной алгеброй. Среди произведений квадратов Стинрода фиксированной степени имеются соотношения. Они были найдены У [9, 10], и доказаны Адемом [7, 8].

**Теорема** (Адем [7, 8])**.** *Имеют место следующие соотношения*

$$\text{при } a < 2b\text{: } Sq^a Sq^b = \sum_{i=0}^{[a/2]} \binom{b-i-1}{a-2i} Sq^{a+b-i} Sq^i; \tag{1}$$

$$\text{при } a < pb\text{: } P^a P^b = \sum_{i=0}^{[a/p]} \binom{(p-1)(b-i)-1}{a-pi} P^{a+b-i} P^i. \tag{2}$$

*и*

$$\begin{aligned} \text{при } a \leq pb\text{: } P^a \beta P^b = \sum_{i=0}^{[a/p]} (-1)^{a+i} \binom{(p-1)(b-i)}{a-pi} \beta P^{a+b-i} P^i + \\ + \sum_{i=0}^{[(a-1)/p]} (-1)^{a+i+1} \binom{(p-1)(b-i)-1}{a-pi-1} P^{a+b-i} \beta P^i. \end{aligned} \tag{3}$$

Важную роль в описании структуры алгебры $\bigoplus\limits_q \mathcal{O}^S(q,\Pi,G)$ играет следующее утверждение.

**Факт.** *Группа стабильных когомологических операций $\mathcal{O}^S(q,\Pi,G)$ изоморфна обратному пределу последовательности групп $H^{n+q}(K(\Pi,n);G)$ и гомоморфизмов $f_n^*$, индуцированных отображением $f_n : \Sigma K(\Pi,n) \to K(\Pi,n$*

Ж.-П. Серром в работе [11] было проведено вычисление когомологий пространств $K(\Pi, n)$. В частности было показано, что образующие в когомологиях $H^*(K(\mathbb{Z}/p, n); \mathbb{Z}/p)$ при $p = 2$ выражаются про помощи итерированных произведений $Sq^{i_r} Sq^{i_{r-1}} \cdots Sq^{i_0}$ квадратов Стинрода. Прежде чем сформулировать теорему дадим необходимые определения.

**Определение.** Последовательность $I = (i_r, i_{r-1}, \ldots, i_0)$ называется *допустимой*, если $i_l \geq 2i_{l-1}$. Произведение квадратов Стинрода $Sq^{i_r} Sq^{i_{r-1}} \cdots Sq^{i_0}$, соответствующее допустимой последовательности, будем также называть допустимым. *Избыточностью* $e(I)$ допустимой последовательности $I$ будем называть следующую величину $e(I) = \sum_{j=1}^{r} (i_l - 2i_{l-1})$.

> **Теорема** (Серр [11])**.** *Алгебра $H^*(K(\mathbb{Z}/2, n); \mathbb{Z}/2)$ является алгеброй полиномов от образующих $Sq^{i_r} Sq^{i_{r-1}} \cdots Sq^{i_0} \iota_n$, где $\iota_n \in H^n(K(\Pi, n); G)$ — фундаментальный класс и $I = (i_r, i_{r-1}, \ldots, i_0)$ — произвольная допустимая последовательность такая, что $e(I) < n$.*

Отметим, что в левой части соотношений Адема стоят недопустимые произведения, тогда как в правых частях — допустимые. Далее, легко можно показать, что применением соотношений Адема произвольное произведение квадратов Стинрода может быть представлено в виде суммы допустимых произведений. Таким образом, получаем, что алгебра стабильных когомологических операций $\bigoplus_q \mathcal{O}^S(q, \mathbb{Z}/p, \mathbb{Z}/p)$ при $p = 2$ мультипликативно порождается квадратами Стинрода $Sq^i$, соотношения Адема образуют полную систему соотношений, и базисом алгебры как векторного пространства над $\mathbb{Z}/p$

служит множество допустимых мономов.

В случае $p > 2$ аналогичная теорема была доказана А. Картаном [12], однако способ доказательства отличается от предложенного Серром. Доказательство основанное на тех же идеях, что и доказательство Серра, было дано М. М. Постниковым в [13]. Мультипликативными образующими алгебры $\bigoplus\limits_q \mathcal{O}^S(q, \mathbb{Z}/p, \mathbb{Z}/p)$ в этом случае являются степени Понтрягина $P^i$ и $\beta$.

В описанных случаях алгебра стабильных когомологических операций в когомологиях с коэффициентами в группе $\mathbb{Z}/p$, где $p$ — простое число, обозначается $\mathcal{A}_p$ и называется алгеброй Стинрода.

Из сказанного выше получаем, что алгебра Стинрода абстрактно может быть задана с помощью набора мультипликативных образующих $\{P^i\}$ и $\beta$ и соотношений (2), (3), и $\{Sq^i\}$, (1) в случае $p = 2$.

Связь действия алгебры Стинрода $\mathcal{A}_p$ с кольцевой структурой в когомологиях устанавливается следующей формулой:

$$Sq^k(ab) = \sum_{i+j=k} Sq^i(a)Sq^j(b)$$

для $a, b \in H^*(X; \mathbb{Z}/2)$. Она была получена А. Картаном в [14] и носит его имя. Милнором [3] было замечено, что отображение

$$Sq^k = \sum_{i+j=k} Sq^i \otimes Sq^j$$

может быть взято в качестве ко умножения, а отображение

$$c(Sq^i) = \sum_{i+j=k} Sq^i c(Sq^j)$$

как антиподальное отображение, в результате чего в $\mathcal{A}_p$ вводится структура алгебры Хопфа. Результатом указанной работы стало полное описание структуры двойственной алгебры $\mathcal{A}_p^*$. В частности, было показано, что $\mathcal{A}_p^* \cong \mathbb{Z}/p[\xi_i] \otimes \Lambda[\tau_j]$, где $\deg(\xi_i) = 2(p^i - 1)$ и $\deg(\tau_j) = 2(p^j - 1) + 1$. Элемент в $\mathcal{A}_p$, двойственный к $\tau_0^{\varepsilon_0}\tau_1^{\varepsilon_1}\cdots\tau_m^{\varepsilon_m}\otimes\xi_0^{r_0}\xi_1^{r_1}\cdots\xi_n^{r_n}$ в $\mathcal{A}_p^*$ обозначается $Q_0^{\varepsilon_0}Q_1^{\varepsilon_1}\cdots Q_m^{\varepsilon_m}P(r_1$ Данные элементы называются элементами Милнора. Множество элементов Милнора образует базис в $\mathcal{A}_p$. Далее, в статье была предъявлена явная формула для умножения, позволяющая представить явным образом произведение двух элементов базиса Милнора в виде линейной комбинации элементов этого же базиса, см. ниже формулу (4), стр. 15. Подобная формула известна лишь для элементов Милнора. К примеру, произведение двух произвольных допустимых мономов, вообще говоря, уже не является допустимым мономом. Для того, чтобы представить получившийся моном в виде суммы допустимых, к нему необходимо несколько раз применить редукцию с помощью соотношений Адема.

Таким образом, базис допустимых мономов и базис Милнора являются первыми построенными базисами в алгебре Стинрода для всех простых $p$.

Несложное рассуждение [2, Лемма 4.2] показывает, что вместо всех образующих $Sq^i$ достаточно рассматривать только элементы вида $Sq^{2^i}$ (соответственно $P^{p^i}$ в случае $p > 2$). В частности, можно строить новые аддитивные базисы пользуясь этим набором образующих. Так для $p = 2$ в работах Арнона и Уолла [1, 4] были построены так называемые $Z$ и $X$-базисы. Кроме того, Арноном в [1] был построен так называемый $C$-базис, Вудом в работе [15] были построены так называемый $WY$ и $WZ$-базис — элементы этих базисов записываются в образующих $Sq^i$. Ещё одним набором мультипликативных образующих является множество элементов Милнора вида $P(0, 0, \dots, p^s, 0, \dots)$. Примером базиса, строящегося с помощью таких мультипликативных образующих, является $P_t^s$-базис, описанный Марголисом в [19, гл. 15].

В работе Монкса [6] исследовался вопрос, в каких случаях при $p = 2$ матрица перехода от одного аддитивного базиса к другому имеет треугольный вид. Важность этого вопроса основывается, в частности, на том, что в явном виде формула для разложения произведения двух базисных мономов по тому же базису известна лишь для базиса Милнора. Кроме того, в работе [6] исследовался вопрос возможности рекуррентного вычисления столбцов матрицы перехода по предшествующим столбцам.

## Структура работы

Диссертация состоит из введения, и трёх глав списка литературы.

Во введении формулируется цель работы, кратко излагаются её результаты и содержание.

Первая глава содержит необходимые определения и известные результаты.

В главе 2 строится новый $WY$-базис. Назовём $WY$*-мономом* произведение $\bar{Z}_{k_0}^{n_0} \bar{Z}_{k_1}^{n_1} \cdots \bar{Z}_{k_r}^{n_r}$, где последовательность пар $I = ((k_0, n_0), \dots, (k_r, n_r))$ удовлетворяет условиям

1. $(k_r, n_r) \leq_L \cdots \leq_L (k_1, n_1) \leq_L (k_0, n_0)$;

2. если в последовательности $I$ есть подпоследовательность одинаковых пар:

$$(k_t, n_t) <_L (k_{t+1}, n_{t+1}) = \cdots = (k_{t+s}, n_{t+s}) <_L (k_{t+s+1}, n_{t+s+1}),$$

то $s < p$ для любой такой подпоследовательности.

**Теорема 1.** *Множество $WY$-мономов образует базис в $\bar{\mathcal{A}}_p$, $p > 2$.*

В главе 3 доказываются предложения 1 и 2, которые играют важную роль в доказательстве того, что $X$ и $Z$-мономы образуют аддитивные базисы алгебры $\bar{\mathcal{A}}_p$.

**Предложение 1.** *Для любых $n > k$ произведение*

$$Z_k^n P^{p^n} \in \bar{\mathcal{A}}_p$$

*может быть выражено в виде линейной комбинации слагаемых, меньших данного произведения в правом лексикографическом порядке.*

**Предложение 2.** *Для любых $n \geqslant k$ произведение $P^{p^n} Z_k^{n+1}$ может быть представлено в виде линейной комбинации мономов, меньших данного произведения в правом лексикографическом порядке.*

Важно отметить, что эти предложения применяются не так, как это обычно делается в теории базисов Гребнера. А именно, сначала мы доказываем, что любой элемент алгебры $\bar{\mathcal{A}}_p$ при помощи некоторых процедур (среди которых содержатся эти два предложения) сводятся к линейной комбинации $Z$-мономов. Затем доказывается, что в каждой градуировке подпространство, порождённое $Z$-мономами, имеет размерность не большую, чем размерность соответствующей градуировочной компоненты $\bar{\mathcal{A}}_p$ (diamon-лемма при этом получается как следствие).

Глава 4 посвящена исследованию треугольности некоторых базисов друг по отношению к другу в алгебре $\bar{\mathcal{A}}_p$. Будем называть базисы $B_1$ и $B_2$ треугольными друг по отношению к другу, если существуют линейные порядки на них, такие что относительно этих порядков матрица перехода от одного базиса к другому треугольна. Глава содержит следующие результаты.

Построены контрпримеры для пар базисов не являющихся, треугольными друг по отношению к другу, в частности, показано, что $Z$-базис не является треугольным по отношению к базису Милнора,

$Z$ **и** $WZ$ **базисы.** Элементы $Z$-базиса — это мономы вида $Z_{k_0}^{n_0} Z_{k_1}^{n_1} \cdots Z_{k_r}^{n_r}$, где $Z_k^n = P^{p^k} P^{p^{k+1}} \cdots P^{p^n}$. При этом на последовательность пар индексов $((n_0, k_0), \ldots, (n_r, k_r))$ наложены условия: $(n_r, k_r) \leq_L \cdots \leq_L (n_1, k_1) \leq_L (n_0, k_0)$; и, если в последовательности $I$ есть подпоследовательность одинаковых пар

$$(n_t, k_t) <_L (n_{t+1}, k_{t+1}) = \cdots = (n_{t+s}, k_{t+s}) <_L (n_{t+s+1}, k_{t+s+1}),$$

то $s < p$ для любой такой подпоследовательности. Мономы, составленные из элементов $\bar{Z}_k^n = P^{p^k + p^{k+1} + \ldots + p^n}$ с теми же условиями на последовательность пар индексов называются $WZ$ мономами.

**Теорема 4.** *Пусть $Z^I$ — произвольный $Z$-моном, заданный набором индексов $I = ((n_0, k_0), \ldots, (n_r, k_r))$. Тогда для $WZ$-монома*

*$\bar{Z}^I$ выполняется равенство*

$$\bar{Z}_{k_0}^{n_0}\bar{Z}_{k_1}^{n_1}\cdots\bar{Z}_{k_r}^{n_r} = Z_{k_0}^{n_0}Z_{k_1}^{n_1}\cdots Z_{k_r}^{n_r} + L,$$

*где $L$ — линейная комбинация мономов, которые меньше $Z^I$ в смысле правого лексикографического порядка.*

**Следствие 1.** *Множество $WZ$-мономов образует базис в $\bar{\mathcal{A}}_p$. Кроме того, базисы $WZ$ и $Z$ треугольны друг по отношению к другу.*

**Семейство $P_s^t$-базисов.** В алгебре $\bar{\mathcal{A}}_p$ имеются элементы

$$P_s^t = P(0,\ldots,0,p^s,0,\ldots),$$

где $p^s$ стоит на месте с номером $t$, $\deg P_s^t = 2p^s(p^t-1)$. Произведение вида $(P_{s_1}^{t_1})^{m_1}\ldots(P_{s_k}^{t_k})^{m_k}$, где все $P_{s_j}^{t_j}$ попарно различны и $0 < m_j < p$ называется $P_s^t$-мономом. В каждом конечном наборе троек целых чисел $\{(s_j,t_j,m_j) : j = 1,\ldots,k, 0 < m_j < p, s_j \geq 0, t_j > 0\}$ зафиксируем линейный порядок и именно в этом порядке будем перемножать $(P_{s_j}^{t_j})^{m_j}$. Заметим, что таких базисов бесконечно много, поскольку в каждом $P_s^t$-мономе порядок атомарных сомножителей $(P_{s_j}^{t_j})^{m_j}$, хоть и фиксирован, однако может быть выбран произвольным образом. Зафиксируем базис $B_P$ и построим биекцию $\gamma : B_{Mil} \to B_P$. Для милноровского элемента $P(R) = P(r_1,r_2,\ldots)$ рассмотрим $p$-адическое разложение каждого $r_j = \sum\alpha_k(r_j)p^k$ и рассмотрим набор троек целых чисел, построенный по последовательности $R$:

$$M(R) = \{(s,t,\alpha_s(r_t)) : \text{ если } \alpha_s(r_t) > 0\}.$$

Положим $\gamma(P(R))$ равным произведению элементов $(P^t_s)^{\alpha_s(r_t)}$ в том порядке, который зафиксирован для набора $M(R)$. Для элемента $P(R)$ положим $e(P(R)) = \sum r_j$.

**Определение.** Для $P\langle R\rangle, P\langle S\rangle \in B_{Mil}$ будем писать $P\langle R\rangle \prec_E P\langle S\rangle$, если $e(P\langle R\rangle) < e(P\langle S\rangle)$, или $e(P\langle R\rangle) = e(P\langle S\rangle)$ и $P\langle R\rangle \prec_R P\langle S\rangle$.

**Теорема 5.** *Для любого $\theta \in B_P$ имеет место равенство*

$$(\theta)_{Mil} = a(\theta)\gamma^{-1}(\theta) + \sum \mu_i,$$

*где $e(\mu_i) < e(\gamma^{-1}(\theta))$ и коэффициент $a(\theta) \in \mathbb{Z}/p$ отличен от 0.*

**Следствие 3.** *$P^s_t$-базис треугольный по отношению к базису Милнора.*

**$X$-базис.** Определение порядка $<_L$ и биекции $\gamma : B_{Mil} \to B_X$ для случая $X$-базиса достаточно громоздко, подробности см. в разделе 4.

**Теорема 6.** *Пусть* р$\theta$ *— произвольный $X$-моном. Тогда его разложение $(\theta)_{Mil}$ по базису Милнора имеет вид*

$$(\theta)_{Mil} = \gamma^{-1}(\theta) + \sum_i \eta_i,$$

*где $\gamma^{-1}(\theta) <_L \eta_i$ для всех $i$.*

**Следствие 4.** *$X$-базис треугольный по отношению к базису Милнора.*

Известные результаты о треугольности могут быть кратко представлены в виде таблицы:

| | Adm | X | C | WZ | Z |
|---|---|---|---|---|---|
| Mil | + | + | + | − | − |
| Z | − | − | − | + | |

Библиография сдержит 22 наименования. Текст диссертации изложен на 58 страницах.

## Список основных результатов, выносимых на защиту

Результаты диссертации являются новыми. В диссертации получены следующие основные результаты:

1. Построен $WY$-базис для случая алгебры $\bar{\mathcal{A}}_p$ (Теорема 1).

2. Доказан ряд утверждений о редукции элементов алгебры Стинрода к $Z$-мономам (предложения 1 и 2).

3. Результаты о треугольности базисов:

   3.1. Теорема 4 о треугольности $WZ$-базиса по отношению к $Z$-базису.

   Следующие утверждения устанавливают треугольность по отношению к базису Милнора:

   3.2. Теорема 5 — для семейств $P^s_t$-базисов.

   3.3. Теорема 6 — для $X$-базиса.

## Методы исследования

В диссертации применяются методы топологии и алгебры. Использовались системы компьютерной алгебры.

## Апробация работы

Результаты диссертации были представлены на следующих семинарах и конференциях:

- семинар «Некоммутативная геометрия и топология» под руководством профессора А. С. Мищенко, профессора В. М. Мануйлова, профессора И. К. Бабенко, доцента А. А. Ирматова;
- семинар «Дифференциальная геометрия и приложения» под руководством академика А. Т. Фоменко;
- Пятая школа-конференция по алгебраической геометрии и комплексному анализу для молодых математиков России (САФУ, г. Коряжма, 2015);

## Публикации

Основное содержание диссертации опубликовано в работах [3] и [2], все — в журналах из перечня ВАК.

## Благодарности

Автор выражает глубокую благодарность доценту Ф. Ю. Попеленскому за постановку задачи, поддержку и внимание к работе, а также А. Т. Фоменко и А. С. Мищенко за полезные замечания и обсуждения.

# 1 Предварительные сведения

Мы будем рассматривать алгебру $\bar{\mathcal{A}}_p$ для простого $p \geq 3$, порождённую элементами $P^j$, где $j \geq 0$, $\deg(P^j) = 2(p-1)j$, и соотношениями $P^0 = 1$,

$$P^a P^b = \sum_{i=0}^{[a/p]} \binom{(p-1)(b-i)-1}{a-pi} P^{a+b-i} P^i.$$

Алгебра $\bar{\mathcal{A}}_p$ — это подалгебра элементов чётной степени в (полной) алгебре Стинрода $\mod p$. Нас будут интересовать базисы в этой алгебре как в линейном пространстве над $\mathbb{Z}/p$. Случай полной алгебры Стинрода будет рассмотрен в другой работе, он требует дополнительного анализа из-за наличия дополнительной образующей $\beta$ степени 1.

**Определение 1.** *Допустимым мономом* в алгебре $\bar{\mathcal{A}}_p$ называется моном $P^{t_1} P^{t_2} \cdots P^{t_m}$, где $t_{i+1} \geq pt_i$.

Множество всех допустимых мономов образует базис в $\bar{\mathcal{A}}_p$, см. [2].

Теперь обратимся к базису Милнора, подробности см. [3]. Произвольный элемент этого базиса имеет вид $P(t_1, t_2, \ldots)$, где $(t_1, t_2, \ldots)$ — произвольная последовательность неотрицательных целых чисел, в которой лишь конечное число элементов отлично от нуля; степень такого элемента равна

$$\deg(P(t_1, t_2, \ldots)) = \sum_i 2t_i(p^i - 1).$$

Важным свойством базиса Милнора является то, что имеется явная формула для произведения двух милноровских элементов $P(r_1, r_2, \ldots)$ и $P(s_1, s_2, \ldots)$:

$$P(r_1, r_2, \ldots)P(s_1, s_2, \ldots) = \sum_X c(X) P(t_1, t_2, \ldots), \tag{4}$$

где суммирование ведётся по всем матрицам $X = (x_{ij})$, $i, j \geq 0$, удовлетворяющим условиям:

$$\sum_i x_{ij} = s_j, j \neq 0, \tag{5}$$

$$\sum_j p^j x_{ij} = r_i, i \neq 0, \tag{6}$$

$$t_h = \sum_{i+j=h} x_{ij}, \tag{7}$$

а $c(X)$ является произведением мультиномиальных коэффициентов

$$c(X) = \prod_h (x_{h0}, x_{h-1,1}, \ldots, x_{0h}). \tag{8}$$

Будем называть такие матрицы $X$ *допустимыми.*

**Определение 2.** *$C$-мономом* в алгебре $\bar{\mathcal{A}}_p$ называется моном $P^{t_n} P^{t_{n-1}} \cdots P^{t_0}$, где индексы $t_i$ удовлетворяют следующим двум условиям:

1) $t_{i+1} \leq p t_i$,

2) $t_i \mid p^i$.

Множество всех $C$-мономов образует базис в $\bar{\mathcal{A}}_p$.

**Определение 3.** *Левый лексикографический порядок* на множестве конечных последовательностях целых чисел зададим следующим образом: для $I = (i_1, \ldots, i_n)$ и $J = (j_1, \ldots, j_m)$ положим $I <_L J$, если выполнено одно из условий:

1) $I$ — пусто, а $J$ — нет;

2) множества $I$ и $J$ непусты, $i_1 < j_1$;

3) множества $I$ и $J$ непусты, $i_1 = j_1$ и $(i_2, \dots i_n) <_L (j_2, \dots j_m)$.

*Правый лексикографической порядок* $<_R$ определяется аналогично.

Положим $Z_k^n = P^{p^k} P^{p^{k+1}} \cdots P^{p^n}$ и $X_k^n = P^{p^n} P^{p^{n-1}} \cdots P^{p^k}$, где $n \geq k \geq 0$.

**Определение 4.** Определим $Z$*-моном* как произведение

$$Z^I = Z_{k_0}^{n_0} \cdots Z_{k_r}^{n_r},$$

и $X$*-моном* как произведение

$$X^I = X_{k_r}^{n_r} \cdots X_{k_0}^{n_0},$$

где $I$ — произвольная последовательность пар $((n_0, k_0), \dots, (n_r, k_r))$, удовлетворяющая условиям

1) $(n_r, k_r) \leq_L \cdots \leq_L (n_1, k_1) \leq_L (n_0, k_0)$;

2) если в последовательности $I$ есть подпоследовательность одинаковых пар:

$$(n_t, k_t) <_L (n_{t+1}, k_{t+1}) = \cdots = (n_{t+s}, k_{t+s}) <_L (n_{t+s+1}, k_{t+s+1}),$$

то $s < p$ для любой такой подпоследовательности.

В работе [1] показано, что $X$-мономы и $Z$-мономы образуют аддитивный базис $\bar{\mathcal{A}}_p$.

**Определение 5.** Два базиса $M'$ и $M''$ называются *треугольными* друг по отношению к другу, если существуют линейные порядки на $M'$ и $M''$ такие, что матрица перехода от одного базиса к другому треугольна относительно этих порядков.

При доказательстве треугольности некоторого базиса $M$ к базису Милнора мы будем пользоваться следующим рассуждением.

Множество элементов базиса $M$ будем обозначать $B_M$, аналогично, $B_{Mil}$ — множество элементов базиса Милнора. Предположим, что нам удалось найти:

1) линейный порядок $<_{Mil}$ на множестве $B_{Mil}$,

2) биекцию $\gamma : B_{Mil} \to B_M$, сохраняющую степень, с помощью которой индуцируется порядок $<_M$ на $B_M$,

такие что для любого $\theta \in B_M$ выполняются соотношения

$$(\theta)_{Mil} = \gamma^{-1}(\theta) + \sum_i \mu_i,$$

где $(\theta)_{Mil}$ — разложение $\theta$ по базису Милнора, $\mu_i \in B_{Mil}$ и $\mu_i <_{Mil} \gamma^{-1}(\theta)$ для всех $i$.

Тогда матрица перехода от базиса Милнора к базису $M$ имеет треугольный вид по отношению к порядкам $<_M$ и $<_{Mil}$.

Далее символом $L_L(a)$ (соответственно, $L_R(a)$) будем обозначать произвольную линейную комбинацию мономов, строго меньших $a$ в смысле левого (правого) лексикографического порядка, а символом $\overline{L}_L(a)$ (соответственно $\overline{L}_R(a)$) — произвольную линейную комбинацию мономов, которые меньше или равны $a$.

Для вычислений в алгебре $\mathcal{A}_p$ нам понадобится следующее хорошо известное (например, см. [2]) утверждение. Пуст $a$ — целое неотрицательное число. Будем записывать его $p$-адическое представление в виде

$$a = \sum_i \alpha_i(a) p^i.$$

**Лемма 1.** *Пусть $a$ и $b$ — два целых неотрицательных числа, тогда*

$$\binom{a}{b} \equiv \prod_i \binom{\alpha_i(a)}{\alpha_i(b)} \pmod{p}. \tag{9}$$

# 2 $WY$-базис

## Введение и основное утверждение

В работе Вуда [15] для $\mathcal{A}_2$ (алгебры Стинрода $\mod 2$) были построены так называемый $WdY$-базис и $WdZ$-базис. В этой части работы приводится обобщение $WdY$-базиса на случай $\bar{\mathcal{A}}_p$, $p \geq 3$.

Рассмотрим степени Понтрягина вида $\bar{Z}_k^n = P^{p^k + p^{k+1} + \ldots + p^n}$.

**Определение 1.** Назовём $WY$*-мономом* произведение $\bar{Z}_{k_0}^{n_0} \bar{Z}_{k_1}^{n_1} \cdots \bar{Z}_{k_r}^{n_r}$, где последовательность пар $I = ((k_0, n_0), \ldots, (k_r, n_r))$ удовлетворяет условиям

1. $(k_r, n_r) \leq_L \cdots \leq_L (k_1, n_1) \leq_L (k_0, n_0)$;
2. если в последовательности $I$ есть подпоследовательность одинаковых пар:

$$(k_t, n_t) <_L (k_{t+1}, n_{t+1}) = \cdots = (k_{t+s}, n_{t+s}) <_L (k_{t+s+1}, n_{t+s+1}),$$

   то $s < p$ для любой такой подпоследовательности.

Основной результат этого раздела составляет следующее утверждение.

**Теорема 1.** *Множество $WY$-мономов образует базис в $\bar{\mathcal{A}}_p$, $p > 2$.*

## Вспомогательные утверждения

Доказательство теоремы 1 опирается на следующий четыре леммы.

**Лемма 2.** *Пусть $m < n$ и*

$$a = p^m + p^{m-1} + \ldots + 1,$$

$$b = p^n + p^{n-1} + \ldots + 1.$$

*Тогда имеет место соотношение*

$$P^a P^b = \sum (-1)^{a+c+1} P^{a+b-c} P^c,$$

*где суммирование осуществляется по всем $c = p^r + p^{r-1} + \ldots + 1$, при $0 < r < m$.*

*Доказательство.* К произведению $P^a P^b$ применимо соотношение Адема

$$P^a P^b = \sum_{\mathrm{c}=0}^{[a/p]} (-1)^{a+\mathrm{c}} \binom{(p-1)(b-\mathrm{c})-1}{a-p\mathrm{c}} P^{a+b-\mathrm{c}} P^{\mathrm{c}}.$$

Пусть $\alpha_i$ — это разряды $p$-адического представления $c$, то есть

$$c = \sum_l \alpha_l p^l.$$

От противного предположим,что $p$-адическое разложение $c$ имеет вид отличный от указанного в формулировке. Тогда имеются две возможности: (1) $\alpha_j = 0$, $\alpha_{j-1} = \ldots = \alpha_{k+1} = 1$ и $\alpha_k > 1$ для некоторых $j \geq k+1$; (2) каждый разряд $\alpha_i$ равен 0 или 1 и $\alpha_{j+1} = 1$, $\alpha_j = 0$ для некоторого $j \geq 0$.

Рассмотрим первый случай. Прежде всего заметим, что $\alpha_s(a - pc) = \alpha_{s-1}(b - c)$, где $1 \leq s \leq k$ (в действительности это верно при $s \leq m$).

Пусть $j > k+1$. Разряды с $j$ по $k$ числа $(b - c)$ имеют вид:

$$0 \quad (p-1) \quad \cdots \quad (p-1) \quad (p - \alpha_k + \varepsilon),$$

где $\varepsilon$ равно 0 или 1. Пусть $\gamma$ — остаток от деления $(b-c)$ на $p^{j-1}$. Рассмотрим выражение

$$(p-1)((p-1)p^{j-1}+\gamma) = (p-2)p^j + p^{j-1} + (p-1)\gamma.$$

Так как $\gamma < p^{j-1}$, то верна оценка $p^{j-1} + (p-1)\gamma < p^j$. Откуда получим $\alpha_j((p-1)(b-c)) = (p-2)$. Очевидно, вычитание единицы никак не повлияет на значение в разряде $j$. В итоге, $\alpha_j((p-1)(b-c)-1) = (p-2)$ и $\alpha_j(a-pc) = \alpha_{j-1}(b-c) = (p-1)$. По лемме 1 получаем, что соответствующий биномиальный коэффициент в соотношении Адема равен 0.

Пусть $j = k+1$. Теперь $\alpha_{k+1}(b-c) = 0$. Положим $\beta = \alpha_k(b-c)$ и пусть $\gamma$ — остаток от деления $(b-c)$ на $p^k$. Легко видеть, что $\beta \geq 1$. Рассмотрим выражение

$$(p-1)(\beta p^k + \gamma) = \beta p^{k+1} - \beta p^k + (p-1)\gamma.$$

В случае $-\beta p^k + (p-1)\gamma < 0$ получим $\alpha_{k+1}((p-1)(\beta p^k+\gamma)) = \beta - 1$, а остаток от деления $(p-1)(\beta p^k + \gamma)$ на $p^{k+1}$ равен $(p-\beta)p^k + (p-1)\gamma$ — очевидно, он отличен от 0. Поэтому вычитание единицы из $(p-1)(\beta p^k+\gamma)$ никак не повлияет на значение разряда $k+1$ и тогда

$$\alpha_{k+1}((p-1)(\beta p^k+\gamma)-1) = \alpha_{k+1}((p-1)(\beta p^k+\gamma)) = \beta - 1,$$

Получаем, что $\alpha_{k+1}((p-1)(b-c)-1) = \beta - 1$ и $\alpha_{k+1}(a-pc) = \alpha_k(b-c) = \beta$, откуда по лемме 1 биномиальный коэффициент, соответствующий такому $c$, равен 0.

Теперь рассмотрим случай, когда

$$-\beta p^k + (p-1)\gamma = p\gamma - \beta p^k - \gamma \geq 0.$$

Покажем, что на самом деле имеет место строгое неравенство. Так как $\alpha_{k-1}(\gamma) \geq \beta >$ получаем $\gamma > 0$. Из $\gamma < p^k$ следует, что $p^k \nmid \gamma$ и $p^k \nmid (p-1)\gamma$. Но тогда $(p-1)\gamma - \beta p^k$ не делится на $p^k$, откуда

$$\alpha_k((p-1)\gamma - \beta p^k - 1) = \alpha_k((p-1)\gamma - \beta p^k).$$

Из $\gamma < p^k$, следует, что $(p-1)\gamma < p^{k+1}$, тем самым,

$$\alpha_k((p-1)\gamma - \beta p^k) = \alpha_k((p-1)\gamma) - \beta.$$

Заметим, что $\alpha_k((p-1)\gamma) \leq \alpha_{k-1}(\gamma)$, откуда

$$\alpha_k((p-1)\gamma - \beta p^k) \leq \alpha_{k-1}(\gamma) - \beta,$$

и

$$\begin{aligned}
&\alpha_k((p-1)(b-c) - 1) = \\
&\qquad = \alpha_k((p-1)\gamma - \beta p^k - 1) = \\
&\qquad\qquad = \alpha_k((p-1)\gamma - \beta p^k) \leq \alpha_{k-1}(\gamma) - \beta.
\end{aligned}$$

Как и ранее,

$$\alpha_k(a - pc) = \alpha_{k-1}(b - p) = \alpha_{k-1}(\gamma).$$

Так как $\beta \geq 1$, для $k$-х разрядов выражений $((p-1)(b-c)-1)$ и $(a-pc)$ получим

$$\alpha_k((p-1)(b-c) - 1) \leq \alpha_{k-1}(\gamma) - \beta < \alpha_{k-1}(\gamma) = \alpha_k(a - pc),$$

откуда по лемме 1 биномиальный коэффициент, соответствующий такому $c$, равен 0.

Рассмотрим теперь вторую возможность: каждый разряд $\alpha_i$ равен 0 или 1 и $\alpha_{j+1} = 1$, $\alpha_j = 0$ для некоторого $j \geq 0$. Получаем $\alpha_{j+1}(b-c) = 0$. Пусть $\gamma$ — остаток от деления $(b-c)$ на $p^{j+1}$. Так как $\gamma \leq p^j + p^{j-1} + \ldots + p + 1 = \frac{p^{j+1}-1}{p-1}$, то $(p-1)\gamma \leq p^{j+1} - 1$. Получаем, что $\alpha_{j+1}((p-1)(b-c)) = 0$. Из условия $\alpha_j = 0$ следует, что $\gamma > 0$, отсюда $\alpha_{j+1}((p-1)(b-c)-1) = \alpha_{j+1}((p-1)(b-c)) = 0$. По доказанному выше $p$-адическое разложение $c$ состоит из 0 и 1. Из условия $\alpha_j = 0$ получаем $\alpha_j(b-c) = 1$ и $\alpha_{j+1}(a-pc) = \alpha_j(b-c) = 1$. По лемме 1 для таких $c$ биномиальные коэффициенты равны 0.

Пусть теперь $c$ имеет вид $c = p^r + p^{r-1} + \ldots + 1$ при $0 < r < m$. Рассмотрим биномиальный коэффициент

$$\binom{(p-1)(b-c)-1}{a-pc} = \\ = \binom{1}{1} \cdots \binom{1}{1}\binom{0}{0}\underbrace{\binom{p-1}{0}}_{\text{разряд } r}\binom{p-1}{0} \cdots \binom{p-1}{0}\binom{p-1}{1}.$$

Очевидно, он равен $(-1)$. Таким образом, коэффициент при слагаемом $P^{a+b-c}P^c$ в соотношении Адема с учётом знака $(-1)^{a+c}$ имеет вид

$$(-1)^{a+c+1} = (-1)^{m+r+1}.$$

□

Для монома $m = P^{i_1}P^{i_2}\cdots P^{i_n}$ обозначим $|m| = \sum i_k$ очевидно, что $\deg(m) = 2(p-1)|m|$.

**Лемма 3.** *Рассмотрим $P^a \in \bar{\mathcal{A}}_p$, где $p \nmid a$. Тогда*

*1) $P^a$ можно представить в виде*

$$P^a = \sum_i M_i,$$

*где для любого $M_i$ верно следующее: если в $M_i$ входит сомножитель $P^j$ и $j$ не делится на $p$, то $j = p^k + p^{k-1} + \ldots + 1$ для некоторого $k$;*

*2) если $a > 1$, и в обозначениях пункта (1)) $P^j$ — крайний правый сомножитель в $M_i$, для которого $p \nmid j$, то есть $M_i = \tilde{m} P^j m$, где $p \mid l$ для любого сомножителя $P^l$ в $m$, тогда $|\tilde{m}| > 0$.*

*Доказательство.* Будем вести доказательство по индукции. При $a = 1$ искомое представление совпадает с $P^1$.

Пусть $a > 1$. Рассмотрим $p$-адическое представление $a$:

$$a = \sum_{i=0}^{k} \alpha_i(a) p^i,$$

где $\alpha_k(a) \neq 0$. В случае, когда $\alpha_i(a) = 1$ для всех $i$, искомое разложение найдено. Теперь пусть это не так, положим

$$b = \begin{cases} p^k + p^{k-1} + \ldots + 1 & \text{при} \quad a > p^k + p^{k-1} + \ldots + 1, \\ p^{k-1} + p^{k-2} + \ldots + 1 & \text{если верно обратное.} \end{cases}$$

Произведение $P^{a-b} P^b$ не является допустимым: в первом случае $pb > a$, откуда $a - b < pb$; во втором получаем, что $a < p^k + p^{k-1} + \ldots + 1 < pb + 1$ или $a \leq pb$, но $p \nmid a$ и равенства быть не может, откуда $a < pb$ и $a - b < pb$.

Рассмотрим соотношение Адема

$$P^{a-b}P^b = (-1)^{a-b}c_0P^a + \sum_{i=1}^{[\frac{a-b}{p}]}(-1)^{a-b+i}c_iP^{a-i}P^i. \qquad (*)$$

Биномиальный коэффициент $c_0$ имеет вид

$$\binom{(p-1)b-1}{a-b} = \binom{p-1}{*}\cdots\binom{p-1}{*}\binom{p-2}{\alpha_0(a-b)},$$

Так как $\alpha_0(b) = 1$, а $\alpha_0(a) \geq 1$, получаем, что $\alpha_0(a-b) < p-1$, откуда $c_0 \neq 0$. Таким образом, исходный элемент $P^a$ по указанному соотношению может быть представлен в виде суммы мономов. Остаётся применить предположение индукции к каждому $P^l$, где $p \nmid l$, входящему в мономы соотношения $(*)$.

Второе утверждение леммы будем доказывать также по индукции. При $a = 2$ достаточно воспользоваться соотношением $P^2 = \frac{1}{2}P^1P^1$. Пусть $a > 2$. Предположим, что утверждение верно для всех $P^c$, где $p \nmid c$ и $c < a$. Тогда для левой части соотношения $(*)$ утверждение верно, а к степеням, с индексами не делящимися на $p$, входящим в мономы из суммы правой части $(*)$, применимо предположение индукции. □

**Лемма 4.** *Пусть моном $M$ содержит степень $P^a$, где $p \nmid a$. Тогда он может быть представлен в виде:*

$$M = \sum M_\alpha P^{c_\alpha},$$

*для некоторых $c_\alpha = p^{k_\alpha} + p^{k_\alpha - 1} + \ldots + 1$.*

*Доказательство.* По лемме 3(a) без ограничения общности можно считать, что $M$ содержит в качестве множителей $P^a$, где $a = p^k + p^{k-1} + \ldots + 1$ для некоторого $k$. Более того предположим, что $P^a$ — крайняя справа степень указанного вида, то есть моном $M$ может быть представлен в виде $M = \tilde{M}m$ при $m = P^a P^b \tilde{m}$, где $p \nmid a$ и $p \mid b$, и индекс каждой степени из $\tilde{m}$ делится на $p$. Такой подмоном $m$ будем называть *минимальным правым подмономом* монома $M$. Доказательство будем вести индукцией по $|m|$. При $|m| = 1$ получаем $m = P^1$, и утверждение леммы тривиально. Пусть утверждение верно для всех мономов $M'$ таких, что $|m'| < |m|$, где $m'$ — минимальный правый подмоном $M'$. Пусть произведение $P^a P^b$ является допустимым. Легко проверить, что произведение $P^{pb} P^{a-(p-1)b}$ недопустимо. Запишем соотношение

$$P^{pb} P^{a-(p-1)b} = \sum_{i=0}^{b-1} (-1)^{pb+i} c_i P^{a+b-i} P^i + (-1)^{(p+1)b} c_b P^a P^b,$$

где коэффициент $c_b$ равен

$$\binom{(p-1)(a-(p-1)b-b)-1}{pb-pb} = \binom{(p-1)(a-pb)-1}{0} = 1.$$

Заменим произведение $P^a P^b$ с помощью этого соотношения. Произведение $P^{pb} P^{a-(p-1)b}$, стоящее в мономе $M = \tilde{M} P^a P^b \tilde{m}$, даст слагаемое $\tilde{M} P^{pb} P^{a-(p-1)b} \tilde{m}$, где индексы всех степеней из $\tilde{m}$ делятся на $p$, и $p \nmid (a-(p-1)b)$, так как $p \nmid a$ и $p \mid b$, откуда его минимальный правый подмоном $P^{a-(p-1)b}\tilde{m}$. Ясно, что

$$(a-(p-1)b) + |\tilde{m}| < a + b + |\tilde{m}| = |m|,$$

поэтому к $\tilde{M} P^{pb} P^{a-(p-1)b} \tilde{m}$ применимо предположение индукции.

Аналогичное рассуждение верно для всех слагаемых вида $P^{a+b-i} P^i$, где $p \nmid i$, входящих в соотношение, где $p \nmid i$.

Рассмотрим слагаемые $P^{a+b-i} P^i$, где $p \mid i$, им соответствуют мономы

$\tilde{M}P^{a+b-i}P^i\tilde{m}$. Так как $p \nmid a+b-i$ степени $P^{a+b-i}$ применима лемма 3($a$):

$$P^{a+b-i} = \sum_j M_j.$$

Произведение $P^aP^b$ — допустимо, то есть $a \geq pb$, по предположению

$$a+b \neq p^l + p^{l-1} + \ldots + 1$$

ни для какого $l$. То же верно для суммы $a+b-i$, так как $i \leq b-1$. Далее $a+b-i \geq a+1$ и по утверждению ($b$) леммы (3) каждый моном $M_j$ может быть записан в виде $M_j = \tilde{m}_j P^{p^{\alpha_j}+p^{\alpha_j-1}+\ldots+1}\tilde{M}_j$, для некоторого $\alpha_j$ и подмономов $\tilde{M}_j$ такого, что индекс каждой входящей в него степени делится на $p$, и $\tilde{m}_j$ такого, что $|\tilde{m}_j| > 0$. Последнее означает, что для минимального правого подмонома монома $\tilde{M}\tilde{m}_j P^{p^{\alpha_j}+p^{\alpha_j-1}+\ldots+1}\tilde{M}_j\tilde{m}$ верно $|P^{p^{\alpha_j}+p^{\alpha_j-1}+\ldots+1}\tilde{M}_j\tilde{m}| < |m|$, и к указанным мономам также применимо предположение индукции.

В случае, когда произведение $P^aP^b$ не является допустимым, применим к нему соотношение Адема, далее рассуждение аналогично. □

**Лемма 2.1.**

$$P^{p^n+\ldots+p^k}P^{a(p^n+\ldots+p^k)} \equiv (a+1)P^{(a+1)(p^n+\ldots+p^k)} + L_R(P^{p^{n-1}+\ldots+p^{k-1}+1}).$$

*В частности, в случае $a = p-1$ получим*

$$P^{p^n+\ldots+p^k}P^{a(p^n+\ldots+p^k)} \equiv L_R(P^{p^{n-1}+\ldots+p^{k-1}+1}).$$

*Доказательство.* Ключевым моментом доказательства является вычисление биномиального коэффициента $B$ при первом слагаемом в соотношении Адема:

$$P^{p^n+\ldots+p^k}P^{a(p^n+\ldots+p^k)} = (-1)^{p^n+\ldots+p^k}B \cdot P^{(a+1)(p^n+\ldots+p^k)} + L_R(P^{p^{n-1}+\ldots+p^{k-1}+1}).$$

По лемме 1

$$B = \binom{(p-1)a(p^n + \ldots + p^k) - 1}{p^n + \ldots + p^k} \equiv \binom{ap^{n+1} - ap^k - 1}{p^n + \ldots + p^k} \equiv$$

$$\equiv \binom{a-1}{0} \underbrace{\binom{p-1}{1}}_{n\text{-й разряд}} \cdots \binom{p-1}{1} \underbrace{\binom{p-1-a}{1}}_{k\text{-й разряд}} \binom{p-1}{0} \cdots \binom{p-1}{0} \equiv$$

$$\equiv (p-1)^{n-k}(p-1-a) \equiv (-1)^{n-k+1}(a+1) \mod p.$$

$\square$

## Доказательство основного утверждения

По лемме 4.3, размерность данной градуировки $\bar{\mathcal{A}}_p$ совпадает с количеством $Y$-мономов в ней. для данной градуировки её размерность совпадает с количеством $Y$-мономов в ней. Покажем, что произвольный моном $P^I = P^{i_0} P^{i_1} \cdots P^{i_r}$ может быть представлен в виде суммы $Y$-мономов.

Доказательство будем вести индукцией по размерности. Предположим, что теорема верна для градуировок не выше $r-1$. Докажем для $r$.

Пусть $p \mid i_k$ для каждого $k$. Применим к данному моному делящий гомоморфизм, получим моном $P^{\frac{I}{p}} = P^{\frac{i_0}{p}} P^{\frac{i_1}{p}} \cdots P^{\frac{i_r}{p}}$. По предположению индукции разложим получившийся моном по $Y$-базису: $P^{\frac{I}{p}} = \sum\limits_i P^{J_i}$. Поднимем результат обратно: домножим каждый из индексов набора $J_i$, которым задаётся моном $P^{J_i}$, на $p$ для всех $i$. Получившуюся в результате сумму (допустимых) мономов обозначим $P^J$. Далее, найдём разложение $P^I$ и $P^J$ по базису допустимых мономов $(P^I)_{Adm.}$ и $(P^J)_{Adm.}$. Если разность получившихся разложений $(P^I)_{Adm.} - (P^J)_{Adm.}$ равна нулю — разложение найдено. В противном случае данная разность — это совокупность мономов, в каждом из которых есть степень Понтрягина, индекс которой не делится на $p$. Таким образом остаётся рассмотреть случай, когда моном $M$ имеет степень $r$ и содержит $P^j$ для $j$ не делящегося на $p$.

Пусть $M$ моном указанного вида. По лемме (4) $M$ может быть разложен в виде:

$$M = \sum_{\alpha} M_\alpha P^{p^{n_\alpha}+p^{n_\alpha-1}+\ldots+1}.$$

К подмономам $M_\alpha$ применимо предположение индукции. По предположению индукции разложим подмоном $M_\alpha$ по $Y$-базису:

$$M_\alpha = \sum_{\beta} \bar{Z}^{K_{\alpha\beta}},$$

где $K_{\alpha\beta}$ — мультииндекс. Рассмотрим произведение $\bar{Z}^{K_{\alpha\beta}} P^{p^{n_\alpha}+p^{n_\alpha-1}+\ldots+1}$. Пусть последний $Y$-элемент в мономе $\bar{Z}_\alpha^{K_\beta}$ задаётся индексами $(n, k)$, то есть $\bar{Z}^{K_{\alpha\beta}} = \bar{Z}^{\tilde{K}_{\alpha\beta}} \bar{Z}_k^n$. При $k > 0$ или $n > n_\alpha$, указанное произведение является $Y$-мономом. В случае $k = 0$ и $n < n_\alpha$ применим к произведению $\bar{Z}_k^n P^{p^{n_\alpha}+p^{n_\alpha-1}+\ldots+1}$ лемму (2), таким образом представим его в виде суммы мономов вида $mP^{p^l+p^{l-1}+\ldots+1}$, где $l < n_\alpha$. Затем применим индукцию по $l$. Пусть $k = 0$ и $n = n_\alpha$. Предположим, что элемент $\bar{Z}_k^n$ входит в моном $\bar{Z}^{K_{\alpha\beta}}$ в степени $c$. Если $c + 1 < p$, то моном $\bar{Z}_k^n P^{p^{n_\alpha}+p^{n_\alpha-1}+\ldots+1}$ является $Y$-мономом. Если же $c + 1 = p$, то по лемме 2.1 рассуждение может быть сведено к совокупности мономов меньших в смысле правого лексикографического порядка.

## 3 О редукции элементов алгебры $\bar{\mathcal{A}}_p$ относительно порядка $<_R$

Основными результатами данной главы являются предложения 1 и 2, которые используются в доказательстве следующих утверждений.

**Теорема 2.** *Множество всех $Z$-мономов образует аддитивный базис алгебры $\bar{\mathcal{A}}_p$.*

**Теорема 3.** *Множество всех $X$-мономов образует аддитивный базис алгебры $\bar{\mathcal{A}}_p$.*

Полные доказательства приведены в статье [1].

**Предложение 1.** *Для любых $n > k$ произведение*

$$Z_k^n P^{p^n} \in \bar{\mathcal{A}}_p$$

*может быть выражено в виде линейной комбинации слагаемых, меньших данного произведения в правом лексикографическом порядке.*

*Доказательство.* Запишем соотношение (16):

$$Z_k^n P^{p^n} \equiv P^{p^n+\ldots+p^k} P^{p^n} + L_R(P^{p^{n-1}}) P^{p^n}.$$

Произведение $P^{p^n+\ldots+p^k} P^{p^n}$ не является допустимым, поэтому имеет место соотношение

$$P^{p^n+\ldots+p^k} P^{p^n} \equiv (-1)^{p^n+\ldots+p^k} \binom{(p-1)p^n-1}{p^n+\ldots+p^k} P^{2p^n+p^{n-1}+\ldots+p^k} + A,$$

где $A$ — линейная комбинация элементов меньших или равных $P^{2p^n-p^{k-1}}P^{p^{n-1}+\ldots+p^{k-1}}$.
Биномиальный коэффициент $\binom{(p-1)p^n-1}{p^n+\ldots+p^k}$ равен

$$\underbrace{\binom{p-2}{1}}_{n\text{-я цифра}}\binom{p-1}{1}\ldots\underbrace{\binom{p-1}{1}}_{k\text{-я цифра}}\binom{p-1}{0}\ldots\binom{p-1}{0} = (-1)^{n-k}(p-2) = (-1)^{n-k+1}2 \quad \mathrm{m}$$

Применим к недопустимому произведению $P^{p^n}P^{p^n+\ldots+p^k}$ соотношение Адема:

$$P^{p^n}P^{p^n+\ldots+p^k} \equiv (-1)^{p^n}\binom{(p-1)(p^n+\ldots+p^k)-1}{p^n}P^{2p^n+p^{n-1}+\ldots+p^k} + B,$$

здесь $B$ — линейная комбинация элементов, меньших или равных $P^{2p^n+p^{n-1}+\ldots+p^k-p^{n-1}}$

Биномиальный коэффициент $\binom{(p-1)(p^n+\ldots+p^k)-1}{p^n}$ равен

$$\underbrace{\binom{p-1}{1}}_{n\text{-я цифра}}\binom{p-1}{0}\ldots\underbrace{\binom{p-2}{0}}_{k\text{-я цифра}}\binom{p-1}{0}\ldots\binom{p-1}{0} = p-1 = -1 \mod p.$$

Учитывая, что оба элемента $A$ и $B$ имеют вид $L_R(Z_k^n P^{p^n})$, получаем

$$Z_k^n P^{p^n} \equiv P^{p^n+\ldots+p^k}P^{p^n} + L_R(P^{p^{n-1}})P^{p^n} \equiv 2P^{2p^n+p^{n-1}+\ldots+p^k} + A + L_R(P^{p^{n-1}})P^{p^n} \equiv$$
$$\equiv 2P^{p^n}P^{p^n+p^{n-1}+\ldots+p^k} - 2B + A + L_R(P^{p^{n-1}})P^{p^n} \equiv$$
$$\equiv 2P^{p^n}Z_k^n + 2P^{p^n}L_R(P^{p^{n-1}}) - 2B + A + L_R(P^{p^{n-1}})P^{p^n} \equiv L_R(Z_k^n P^{p^n}).$$

□

**Предложение 2.** *Для любых $n \geqslant k$ произведение $P^{p^n}Z_k^{n+1}$ может быть представлено в виде линейной комбинации мономов, меньших данного произведения в правом лексикографическом порядке.*

*Доказательство.* По лемме 4.1 имеет место равенство

$$P^{p^n}Z_k^{n+1} = P^{p^n}Z_k^n P^{p^{n+1}} \equiv P^{p^n}P^{p^n+\ldots p^k}P^{p^{n+1}} + P^{p^n}L_R(P^{p^{n-1}})P^{p^{n+1}}. \qquad (10)$$

Применим соотношение Адема к произведению $P^{p^n}P^{p^n+\ldots p^k}$:

$$P^{p^n}P^{p^n+\ldots+p^k} \equiv (-1)^{p^n}\binom{(p-1)(p^n+\ldots+p^k)-1}{p^n}P^{2p^n+p^{n-1}\ldots+p^k} + A, \qquad (11)$$

где $A$ — сумма мономов, меньших или равных $P^{2p^n+\ldots+p^k-p^{n-1}}P^{p^{n-1}}$ в правом лексикографическом порядке. При $k<n$ коэффициент при первом слагаемом равен

$$(-1)^{p^n}\binom{(p-1)(p^n+\ldots+p^k)-1}{p^n} \equiv -\underbrace{\binom{p-1}{1}}_{n\text{-я цифра}}\binom{*}{0}\cdots\binom{*}{0} \equiv 1 \mod p,$$

и в случае $k=n$:

$$(-1)^{p^n}\binom{(p-1)p^n-1}{p^n} \equiv -\underbrace{\binom{p-2}{1}}_{n\text{-я цифра}}\binom{*}{0}\cdots\binom{*}{0} \equiv 2 \mod p.$$

Откуда получаем соотношение

$$P^{p^n}P^{p^n+\ldots+p^k} \equiv \alpha P^{2p^n+\ldots+p^k} + A, \qquad (12)$$

где $\alpha = 1$, при $k<n$, и $\alpha = 2$, при $k=n$. Подставляя левую часть в соотношение (10), получаем

$$P^{p^n}Z_k^{n+1} \equiv \alpha P^{2p^n+\ldots+p^k}P^{p^{n+1}} + A\cdot P^{p^{n+1}} + P^{p^n}L_R(P^{p^{n-1}})P^{p^{n+1}}. \qquad (13)$$

Произведение $P^{2p^n+\ldots+p^k}P^{p^{n+1}}$ не является допустимым, тем самым:

$$P^{2p^n+\ldots+p^k}P^{p^{n+1}} \equiv (-1)^{2p^n+\ldots+p^k}\binom{(p-1)p^{n+1}-1}{2p^n+\ldots+p^k}P^{p^{n+1}+2p^n+\ldots+p^k} + B,$$

где $B$ — линейная комбинация мономов, меньших или равных $P^{p^{n+1}+2p^n+\ldots+p^k-(2p^{n-1}+\ldots}$ в смысле правого лексикографического порядка. Вычислим биномиальный коэффициент:

$$(-1)^{2p^n+\ldots+p^k}\binom{(p-1)p^{n+1}-1}{2p^n+\ldots+p^k}\equiv$$
$$\equiv(-1)^{n-k}\binom{p-2}{0}\underbrace{\binom{p-1}{2}}_{n\text{-я цифра}}\binom{p-1}{1}\cdots\underbrace{\binom{p-1}{1}}_{k\text{-я цифра}}\binom{p-1}{0}\cdots\binom{p-1}{0}\equiv$$
$$\equiv\frac{(p-1)(p-2)}{2}\equiv\frac{p(p-3)+2}{2}\equiv 1 \mod p.$$

Тем самым,

$$P^{2p^n+\ldots+p^k}P^{p^{n+1}}=P^{p^{n+1}+2p^n+\ldots+p^k}+B. \tag{14}$$

Теперь рассмотрим произведение $P^{p^{n+1}}P^{2p^n+\ldots+p^k}$, которое тоже не является допустимым:

$$P^{p^{n+1}}P^{2p^n+\ldots+p^k}=(-1)^{p^{n+1}}\binom{(p-1)(2p^n+\ldots+p^k)-1}{p^{n+1}}P^{p^{n+1}+2p^n+\ldots+p^k}+C,$$

где $C$ — линейная комбинация мономов, меньших или равных $P^{p^{n+1}+p^n+\ldots+p^k}P^{p^n}$ в смысле правого лексикографического порядка. Вычислим биномиальный коэффициент

$$(-1)^{p^{n+1}}\binom{(p-1)(2p^n+p^{n-1}+\ldots+p^k)-1}{p^{n+1}}\equiv$$
$$\equiv-\binom{p^{n+1}+(p-2)p^n+(p-1)(p^{n-1}+\ldots+p^k)-1}{p^{n+1}}\equiv$$
$$\equiv-\underbrace{\binom{1}{1}}_{(n+1)\text{-я цифра}}\binom{*}{0}\cdots\binom{*}{0}\equiv-1 \mod p.$$

Откуда получим

$$P^{p^{n+1}}P^{2p^n+\ldots+p^k} = -P^{p^{n+1}+2p^n+p^{n-1}\ldots+p^k} + C. \tag{15}$$

Учитывая соотношения (13), (14), (15) можем заключить, что

$$P^{p^n}Z_k^{n+1} \equiv \alpha P^{2p^n+\ldots+p^k}P^{p^{n+1}} + A\cdot P^{p^{n+1}} + P^{p^n}L_R(P^{p^{n-1}})P^{p^{n+1}} \equiv$$
$$\alpha(P^{p^{n+1}+2p^n+\ldots+p^k} + B) + A\cdot P^{p^{n+1}} + P^{p^n}L_R(P^{p^{n-1}})P^{p^{n+1}} \equiv$$
$$\alpha(-P^{p^{n+1}}P^{2p^n+\ldots+p^k} + C + B) + A\cdot P^{p^{n+1}} + P^{p^n}L_R(P^{p^{n-1}})P^{p^{n+1}}$$

Теперь остаётся заметить, что все слагаемые в правой части строго меньше, чем $P^{p^n}Z_k^{n+1}$. □

# 4 Треугольные базисы в алгебре $\bar{\mathcal{A}}_p$

## Контрпримеры

Для произвольного простого $p$ несложно видеть, что подпространство элементов градуировки $2(p-1)(p+2)$ в $\bar{\mathcal{A}}_p$ — двумерно, и в этой размерности $Z$-базис содержит два элемента $Z_1^0 Z_0^0$ и $Z_1^1 Z_0^0 Z_0^0$. Простое вычисление показывает, что

$$Z_1^0 Z_0^0 = P(1,1) + 2P(p+2)$$

$$Z_1^1 Z_0^0 Z_0^0 = 2P(1,1) + 2P(p+2).$$

Отсюда следует, что при любом выборе линейных порядков на $Z$-мономах и на базисе Милнора матрица перехода не будет треугольной.

## $Z$ и $WZ$ базисы

Как видно, из определения, $Z$-мономы строятся из блоков специального вида — элементов $Z_k^n = P^{p^k} P^{p^{k+1}} \cdots P^{p^n}$. Вместо них можно взять элементы $\bar{Z}_k^n = P^{p^k + p^{k+1} + \ldots + p^n}$, где также $n \geq k \geq 0$, и составлять мономы пользуясь теми же правилами, что и в случае $Z$-мономов. В этой части будет показано, что получающиеся в результате мономы образуют базис. Более того, построенный базис даёт пример базиса треугольного по отношению к $Z$-базису.

**Определение 6.** Назовём $WZ$-*мономом* произведение $\bar{Z}_{k_0}^{n_0} \bar{Z}_{k_1}^{n_1} \cdots \bar{Z}_{k_r}^{n_r}$, где последовательность пар $I = ((n_0, k_0), \ldots, (n_r, k_r))$ удовлетворяет тем же условиям, что и для $Z$-мономов, см. определение 4.

Элементы $Z_k^n$ и $\bar{Z}_k^n$ схожи между собой. Следующее утверждение устанавливает связь между ними в алгебре $\bar{\mathcal{A}}_p$.

**Лемма 4.1.** *([1], Lemma 2.8) Для произвольных целых $n \geq k \geq 0$ имеет место равенство*

$$Z_k^n = P^{p^n+\ldots+p^k} + L_R(P^{p^{n-1}}). \tag{16}$$

*Доказательство.* Доказательство будем вести убывающей индукцией по $k$. При $k = n$ утверждение тривиально. В случае $k = n-1$ получим

$$P^{p^{n-1}}P^{p^n} \equiv (-1)^{p^{n-1}}\binom{(p-1)p^n-1}{p^{n-1}}P^{p^n+p^{n-1}} + L_R(P^{p^{n-2}}) +$$
$$(-1)^{p^{n-1}+p^{n-2}}\binom{(p-1)(p^n-p^{n-2})-1}{0}P^{p^n+p^{n-1}-p^{n-2}}P^{p^{n-2}}.$$

По лемме 1 биномиальный коэффициент $\binom{(p-1)p^n-1}{p^{n-1}}$ равен $p-1 \equiv -1(\mod p)$. Откуда получаем

$$P^{p^{n-1}}P^{p^n} \equiv P^{p^n+p^{n-1}} + L_R(P^{p^{n-2}}) + P^{p^n+p^{n-1}-p^{n-2}}P^{p^{n-2}} \equiv P^{p^n+p^{n-1}} + L_R(P^{p^{n-1}}).$$

Теперь предположим, что утверждение леммы верно в случае $Z_{k+1}^n$, докажем для $Z_k^n$:

$$P^{p^k}Z_{k+1}^n \equiv P^{p^k}(P^{p^n+\ldots+p^{k+1}} + L_R(P^{p^{n-1}})) \equiv P^{p^k}P^{p^n+\ldots+p^{k+1}} + L_R(P^{p^{n-1}}) \equiv$$
$$\equiv (-1)^{p^k}\binom{(p-1)(p^n+\ldots+p^{k+1})-1}{p^k}P^{p^n+\ldots+p^k} + L_R(P^{p^{n-1}}).$$

Остаётся заметить, что биномиальный коэффициент $\binom{(p-1)(p^n+\ldots+p^{k+1})-1}{p^k}$ равен $(p-1) \equiv (-1) \mod p$. $\square$

Как видно, $Z$-мономы и $WZ$-мономы сформированы по одним и тем же правилам. Это наблюдение и соотношение (16) позволяют доказать следующее утверждение.

**Теорема 4.** *Пусть* $Z^I$ *— произвольный* $Z$*-моном, заданный набором индексов* $I = ((n_0, k_0), \ldots, (n_r, k_r))$*. Тогда для* $WZ$*-монома* $\bar{Z}^I$ *выполняется равенство*

$$\bar{Z}_{k_0}^{n_0} \bar{Z}_{k_1}^{n_1} \cdots \bar{Z}_{k_r}^{n_r} = Z_{k_0}^{n_0} Z_{k_1}^{n_1} \cdots Z_{k_r}^{n_r} + L,$$

*где* $L = L_R(Z^I)$*.*

*Доказательство.* Проведём индукцию по длине набора $I$. При $r = 0$ утверждение совпадает с леммой 4.1.

Пусть утверждение верно при $r = l$, то есть имеет место разложение

$$\bar{Z}_{k_1}^{n_1} \bar{Z}_{k_1}^{n_1} \cdots \bar{Z}_{k_l}^{n_l} = Z_{k_1}^{n_1} Z_{k_1}^{n_1} \cdots Z_{k_l}^{n_l} + L(Z_{k_1}^{n_1} Z_{k_1}^{n_1} \cdots Z_{k_l}^{n_l}).$$

Тогда при $r = l + 1$ получим

$$\begin{aligned} \bar{Z}_{k_0}^{n_0} \bar{Z}_{k_1}^{n_1} \cdots \bar{Z}_{k_{l+1}}^{n_{l+1}} = (Z_{k_0}^{n_0} Z_{k_1}^{n_1} \cdots Z_{k_l}^{n_l} + L_R(Z_{k_0}^{n_0} Z_{k_1}^{n_1} \cdots Z_{k_l}^{n_l}))(Z_{k_{l+1}}^{n_{l+1}} + L_R(P^{p^{n_{l+1}-1}})) = \\ = Z_{k_0}^{n_0} Z_{k_1}^{n_1} \cdots Z_{k_{l+1}}^{n_{l+1}} + L_R(Z_{k_0}^{n_0} Z_{k_1}^{n_1} \cdots Z_{k_{l+1}}^{n_{l+1}}). \end{aligned}$$

□

**Следствие 1.** *Множество* $WZ$*-мономов образует базис в* $\bar{\mathcal{A}}_p$*. Кроме того, базисы* $WZ$ *и* $Z$ *треугольны друг по отношению к другу.*

*Доказательство.* Упорядочим $WZ$-мономы следующим образом: $\bar{Z}^I \prec \bar{Z}^J$ тогда и только тогда, когда $Z^I <_R Z^J$. По лемме 4 матрица коэффициентов разложения $WZ$-мономов по $Z$-базису имеет треугольный вид с 1 на главной диагонали. □

## Семейство $P_s^t$-базисов

Напомним, что в алгебре $\bar{\mathcal{A}}_p$ имеются элементы $P_s^t = P(0, \ldots, 0, p^s, 0, \ldots)$, где $p^s$ стоит на месте с номером $t$, $\deg P_s^t = 2p^s(p^t - 1)$. Назовём $P_s^t$-мономом произведение вида $(P_{s_1}^{t_1})^{m_1} \ldots (P_{s_k}^{t_k})^{m_k}$, где все $P_{s_j}^{t_j}$ попарно различны и $0 < m_j < p$. В каждом конечном наборе троек целых чисел $\{(s_j, t_j, m_j) : j = 1, \ldots, k, 0 < m_j < p, s_j \geq 0, t_j > 0\}$ зафиксируем линейный порядок и именно в этом порядке будем перемножать $(P_{s_j}^{t_j})^{m_j}$. Ниже мы докажем, что множество $B_P$ полученных произведений образует базис $\bar{\mathcal{A}}_p$, который к тому же является треугольным по отношению базису Милнора. Заметим, что таких базисов бесконечно много, поскольку в каждом $P_s^t$-мономе порядок атомарных сомножителей $(P_{s_j}^{t_j})^{m_j}$, хоть и фиксирован, однако может быть выбран произвольным образом. Зафиксируем базис $B_P$ и построим биекцию $\gamma : B_{Mil} \to B_P$. Для милноровского элемента $P(R) = P(r_1, r_2, \ldots)$ рассмотрим $p$-адическое разложение каждого $r_j = \sum \alpha_k(r_j)p^k$ и рассмотрим набор троек целых чисел, построенный по последовательности $R$:

$$M(R) = \{(s, t, \alpha_s(r_t)) : \text{ если } \alpha_s(r_t) > 0\}.$$

Положим $\gamma(P(R))$ равным произведению элементов $(P_s^t)^{\alpha_s(r_t)}$ в том порядке, который зафиксирован для набора $M(R)$. Легко проверить, что $\gamma$ является биекцией, сохраняющей градуировку. Интересно отметить, что $\gamma^{-1}$ определено корректно одновременно для всех базисов $B_P$. Это наблюдение пригодится нам в доказательстве теоремы 5. Для элемента $P(R)$ положим $e(P(R)) = \sum r_j$. Согласно [5] величина $2e(P(R))$ совпадает с избыточностью элемента $P(R)$. Для простоты величину $e(P(R))$ тоже будем называть избыточностью, это не вызовет путаницы.

**Определение 7.** Для $P\langle R\rangle, P\langle S\rangle \in B_{Mil}$ будем писать $P\langle R\rangle \prec_E P\langle S\rangle$, если $e(P\langle R\rangle) < e(P\langle S\rangle)$, или $e(P\langle R\rangle) = e(P\langle S\rangle)$ и $P\langle R\rangle \prec_R P\langle S\rangle$.

Отметим, что второй случай определения в дальнейшем использоваться не будет и добавлен лишь для того, чтобы порядок был линейным.

**Лемма 4.2.** *Пусть $X$ — допустимая матрица произведения $P\langle R\rangle P\langle S\rangle$, соответствующая элементу $P\langle T\rangle$, где $T \neq R+S$. Тогда $e(P\langle T\rangle) < e(P\langle R+S\rangle)$.*

*Доказательство.* Для $P\langle T\rangle = P(t_1, t_2, \ldots)$ имеем $e(P\langle T\rangle) = \sum t_i$. По (7) каждое $t_i$ равно сумме элементов на $i$-й диагонали матрицы $X = ||x_{ij}||$, откуда $e(P\langle T\rangle) = \sum_{i,j} x_{ij}$. По (5) сумма элементов вне первого столбца

$$\sum_{\substack{i\geq 0\\ j>0}} x_{ij}$$

равна $e(P\langle S\rangle)$. По (6) $x_{i0} \leq x_i$ для каждого $i$. Однако по условию $T \neq R + S$, поэтому в матрице $X$ для некоторых $u > 0$ и $v > 0$ найдётся элемент $x_{uv} \neq 0$. Поэтому имеет место строгое неравенство $x_{u0} < r_u$, и следовательно, сумма элементов первого столбца матрицы $X$ строго меньше $e(P\langle R\rangle)$, то есть

$\sum_i x_{i0} < e(P\langle R\rangle)$. Тогда

$$ex(P\langle T\rangle) = \sum_{i,j} x_{i,j} =$$

$$= \sum_i x_{i0} + \sum_{\substack{i\geq 0\\ j>0}} x_{ij} < e(P\langle R\rangle) + e(P\langle S\rangle) = e(P\langle R+S\rangle).$$

□

**Следствие 2.** *Если $e(P\langle U\rangle) < e(P\langle R\rangle)$, то каждое слагаемое $P\langle T\rangle$ в разложении произведения $P\langle U\rangle P\langle S\rangle$ (или $P\langle S\rangle P\langle U\rangle$) по базису Милнора имеет избыточность строго меньшую, чем $P\langle R+S\rangle$: $e(P\langle T\rangle) < e(P\langle R+S\rangle)$.*

**Теорема 5.** *Для любого $\theta \in B_P$ имеет место равенство*

$$(\theta)_{Mil} = a(\theta)\gamma^{-1}(\theta) + \sum \mu_i,$$

*где $e(\mu_i) < e(\gamma^{-1}(\theta))$ и $a(\theta) \in \mathbb{Z}/p$ отлично от 0.*

*Доказательство.* Пусть $\theta = (P^{t_1}_{s_1})^{m_1} \dots (P^{t_k}_{s_k})^{m_k}$. Проведём индукцию по длине $k$ одновременно для всевозможных базисов $B_P$.

Индукцией по $m$ легко проверить, что

$$(P^t_s)^m = m! P(0, \dots, 0, mp^s, 0, \dots) + \sum \nu_j,$$

где $e(\nu_j) < e(P(0, \dots, 0, mp^s, 0, \dots)))$. А так как $\gamma^{-1}((P^t_s)^m) = P(0, \dots, 0, mp^s, 0, \dots)$, то база индукции верна.

Теперь рассмотрим произведения $\theta' = (P^{t_1}_{s_1})^{m_1} \dots (P^{t_{k-1}}_{s_{k-1}})^{m_{k-1}}$ и $\theta = \theta'(P^{t_k}_{s_k})^{m_k}$. Пусть $P(r_1, \dots, r_m) = \gamma^{-1}(\theta)$. Тогда по определению отображения $\gamma$ имеем равенство $\gamma^{-1}(\theta') = P(r_1, \dots, r_t - mp^s, r_{t+1}, \dots, r_m)$.

По предположению индукции для $\theta'$ утверждение теоремы верно, т.е.

$$(\theta')_{\mathrm{Mil}} = a(\theta')\gamma^{-1}(\theta') + \sum \mu_i,$$

где $e(\mu_i) < e(\gamma^{-1}(\theta'))$ и $a(\theta') \in \mathbb{Z}/p$ отлично от 0.

Тогда

$$\begin{aligned}(\theta)_{\mathrm{Mil}} &= ((\theta')_{\mathrm{Mil}}(P_{s_k}^{t_k})^{m_k})_{\mathrm{Mil}} = \\ &= a(\theta')(\gamma^{-1}(\theta')(P_{s_k}^{t_k})^{m_k})_{\mathrm{Mil}} + \sum(\mu_i(P_{s_k}^{t_k})^{m_k})_{\mathrm{Mil}} = \\ &= a(\theta')\left(\gamma^{-1}(\theta')(m!\gamma^{-1}((P_{s_k}^{t_k})^{m_k}) + \sum \nu_j)\right)_{\mathrm{Mil}} + \sum(\mu_i(P_{s_k}^{t_k})^{m_k})_{\mathrm{Mil}} = \\ &= a(\theta')m!\left(\gamma^{-1}(\theta')\gamma^{-1}((P_{s_k}^{t_k})^{m_k})\right)_{\mathrm{Mil}} + a(\theta')\sum\left(\gamma^{-1}(\theta')\nu_j)\right)_{\mathrm{Mil}} + \sum(\mu_i(P_{s_k}^{t_k})^{m_k})_{\mathrm{Mil}}\end{aligned}$$

По лемме 4.2 наибольшее значение избыточности в первом слагаемом имеет $P(r_1, \ldots, r_m)$, причем, как легко подсчитать, соответствующий коэффициент (8) отличен от 0. По следствию 2 во второй и в третьей сумме избыточности слагаемых строго меньше $e(P(r_1, \ldots, r_m))$. $\square$

Из доказанной теоремы немедленно следует, что любой набор вида $B_P$ является базисом $\bar{\mathcal{A}}_p$, причем треугольным по отношению к базису Милнора. При этом на $B_P$ рассматривается порядок, индуцированный биекцией $\gamma$ и порядком $\prec_E$ на множестве $B_{Mil}$.

**Следствие 3.** *Пусть $P\langle R\rangle \in B_{Mil}$ и $\gamma(P\langle R\rangle)_{Mil} = P\langle R\rangle + \sum_i P\langle R_i\rangle$. Тогда выражение*

$$(P\langle R\rangle)_P = \gamma P\langle R\rangle + \sum_i (P\langle R_i\rangle)_P$$

*задаёт рекуррентную формулу для вычисления $(P\langle R\rangle)_P$ — разложения $P(R)$ по базису $B_P$.*

## $X$-базис

Построим на множестве $B_{Mil}$ некоторый специальный порядок. Затем построим биекцию $\gamma : B_{Mil} \to B_X$.

Рассмотрим милноровский элемент $P(r_0, \ldots, r_m)$. Каждому $r_j$ сопоставим его $p$-адическое разложение

$$r_j = \sum_i \alpha_i(r_j) p^i.$$

Из всевозможных $\alpha_{ij} = \alpha_i(r_j)$ сформируем таблицу так, что первые индексы меняются вдоль столбцов, вторые — вдоль строк; нумерация строк начинается с 0 и идёт снизу вверх; столбцы нумеруются с 0. Например, при $p = 3$ для элемента $P(4, 9, 6)$ получается таблица

$$\begin{array}{c|ccc}
2 & 0 & 1 & 0 \\
1 & 1 & 0 & 2 \\
0 & 1 & 0 & 0 \\
\hline
 & 0 & 1 & 2
\end{array}$$

Таким образом, в $j$-м столбце стоит $p-$адическое разложение $r_j$, и $i$-я строка содержит последовательность $i$-х разрядов $(\alpha_i(r_0), \ldots, \alpha_i(r_m))$ набора $(r_0, \ldots, r_m)$. Такую таблицу будем называть *таблицей разрядов* последовательности $R$.

**Определение 8.** *Развёрткой* таблицы будем называть следующую последовательность её элементов

$$(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{02}, \alpha_{11}, \ldots).$$

Очевидно, сопоставление таблицы и её развёртки фиксированному милноровскому элементу взаимно–однозначно. Приведённой выше таблице соответствует последовательность

$$(1, 0, 1, 0, 0, 0, 0, 2, 1, 0, \ldots).$$

Левый лексикографический порядок $<_L$ на множестве развёрток естественным образом задаёт порядок на множестве элементов базиса Милнора. Будем обозначать этот порядок тем же символом $<_L$.

**Определение 9.** Пусть элементу $P(r_0, \ldots, r_m)$ соответствует развёртка

$$(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{02}, \alpha_{11}, \ldots).$$

Заменим элементы данной последовательности по правилу $\alpha_{ij} \mapsto (X_i^{i+j})^{\alpha_{ij}}$, получим последовательность элементов $X_k^n$:

$$((X_0^0)^{\alpha_{00}}, (X_0^1)^{\alpha_{01}}, (X_1^1)^{\alpha_{10}}, (X_0^2)^{\alpha_{02}}, \ldots).$$

Возьмём их произведение в имеющемся порядке (при $\alpha_{ij} = 0$ соответствующий $X_i^{i+j}$ в произведение не входит, поэтому произведение конечно):

$$(X_0^0)^{\alpha_{00}}(X_0^1)^{\alpha_{01}}(X_1^1)^{\alpha_{10}}(X_0^2)^{\alpha_{02}} \ldots$$

В итоге получим некоторый $X$-моном. Описанное соответствие задаёт отображение множества милноровских элементов в множество $X$-мономов

$$\gamma : P(r_0, \ldots, r_m) \mapsto (X_0^0)^{\alpha_{00}}(X_0^1)^{\alpha_{01}}(X_1^1)^{\alpha_{10}}(X_0^2)^{\alpha_{02}} \ldots$$

**Лемма 4.3.** *Отображение $\gamma$ взаимно однозначно и сохраняет степень.*

*Доказательство.* Напомним, что $\bar{\mathcal{A}}_p^* = \mathbb{Z}/p\,[\xi_1, \xi_2, \ldots]$, где $\deg \xi_k = 2p^k - 2$.

В место элементов базиса Милнора $P(r_0, \ldots, r_m)$, рассмотрим двойственные им базисные элементы $\xi_0^{r_0} \cdots \xi_m^{r_m}$ в алгебре $\bar{\mathcal{A}}_p^*$ и будем рассматривать отображение

$$\bar{\gamma} : \xi_0^{r_0} \cdots \xi_m^{r_m} \mapsto (X_0^0)^{\alpha_{00}}(X_0^1)^{\alpha_{01}}(X_1^1)^{\alpha_{10}}(X_0^2)^{\alpha_{02}} \ldots,$$

задающееся аналогично отображению $\gamma$.

В частности, $\bar{\gamma} : \xi_{n-k+1}^{p^k} \mapsto X_k^n$, причём указанные элементы имеют одну и туже степень $2(p^{n+1} - p^k)$. Тогда обратное отображение $\bar{\gamma}^{-1}$ переводит $X_k^n$ в $\xi_{n-k+1}^{p^k}$. Остаётся заметить, что образующие $\xi_i$ коммутируют между собой, откуда получаем, что по данному $X$-моному элемент двойственной алгебры строится однозначным образом. □

**Теорема 6.** *Пусть $\theta$ — произвольный $X$-моном. Тогда его разложение $(\theta)_{Mil}$ по базису Милнора имеет вид*

$$(\theta)_{Mil} = \gamma^{-1}(\theta) + \sum_i \eta_i,$$

*где $\gamma^{-1}(\theta) <_L \eta_i$ для всех $i$.*

*Доказательство.* Сначала проверим утверждение для $\theta = X_k^k$. В самом деле, $P(p^k) = P^{p^k} = X_k^k$ и $\gamma(P(p^k)) = X_k^k$. Тем самым, $(X_k^k)_{Mil} = \gamma^{-1}(X_k^k)$.

Далее рассмотрим моном $\theta = X_k^n X_{k_1}^{n_1} \cdots X_{k_l}^{n_l}$. Возможны два случая: $k = n$ и $k < n$. Сначала разберем первый случай.

Моном $\theta$ может быть записан в виде $(X_n^n)^w X_{k_1}^{n_1} \cdots X_{k_l}^{n_l}$, где $0 < w < p$. Предположим по индукции, что утверждение теоремы верно для монома

$(X_n^n)^{w-1}X_{k_1}^{n_1}\cdots X_{k_l}^{n_l}$. Тогда

$$\begin{aligned}((X_n^n)^w X_{k_1}^{n_1}\cdots X_{k_l}^{n_l})_{Mil} = (P^{p^n}((X_n^n)^{w-1}X_{k_1}^{n_1}\cdots X_{k_l}^{n_l})_{Mil})_{Mil} = \\ = (P^{p^n}(P(\widetilde{R}) + \sum_l P(Q_l)))_{Mil} = (P^{p^n}P(\widetilde{R}))_{Mil} + (\sum_l P^{p^n}P(Q_l))_{Mil},\end{aligned} \tag{17}$$

где $P(\widetilde{R}) = P(\widetilde{r}_0, \widetilde{r}_1, \ldots, \widetilde{r}_m) = \gamma^{-1}((X_n^n)^{w-1}X_{k_1}^{n_1}\cdots X_{k_l}^{n_l})$ и $P(\widetilde{R}) <_L P(Q_l)$ для любого $l$.

Последовательности $R$ соответствует таблица разрядов, в которой на $n$-й диагонали и ниже стоят нули, исключая элемент $\alpha_{n0} = w$. Кроме того, $\tilde{r}_j = r_j$ при $j > 0$ и $\tilde{r}_0 + p^n = r_0$.

Мы покажем, что в разложении $(P^{p^n}P(\widetilde{R}))_{Mil}$ имеется слагаемое, равное $P(R)$, а все остальные слагаемые больше $P(R)$. Затем мы покажем, что в сумме $(P^{p^n}P(Q_l))_{Mil}$ все слагаемые больше $P(R)$.

Сначала выясним, при каких допустимых матрицах в формуле для произведения произведения $P^{p^n}P(\widetilde{R})$ могут встретиться слагаемые, не превосходящие $P(R)$.

Произведению $P^{p^n}P(\widetilde{R})$ соответствуют допустимые матрицы вида

$$\begin{matrix} * & r_0 - p^n - s_1 & r_1 - s_2 & \ldots & r_{n-1} - s_n & r_n & \ldots \\ s_0 & s_1 & s_2 & \ldots & s_n & 0 & \ldots \end{matrix} \tag{18}$$

Отсюда, в частности, следует, что для такой матрицы коэффициент $c(X)$, определенный соотношением (8), находится из формулы

$$c(X) = \prod_i \binom{t_i}{s_i}, \tag{19}$$

где $t_i$ удовлетворяют равенству (7).

Далее, из $\sum s_i p^i = p^n$ следует, что $s_i \leq p^{n-i}$ для всех $i$. Более того, если при каком-то $i$ достигается равенство $s_i = p^{n-i}$, то $s_j = 0$ при $j \neq i$.

Из условия на нулевые элементы в таблицах разрядов $R$ и $\widetilde{R}$ следует, что $p^{n-j+1}|r_j$ при $j = 1, \ldots, n$. Если допустимая матрица ( 18) соответствует слагаемому, меньшему чем $P(R)$, то для нее с необходимостью выполняются условия

$$
\begin{aligned}
&p \mid r_n + s_n \\
&p^2 \mid r_{n-1} - s_n + s_{n-1} \\
&\ldots \\
&p^n \mid r_1 - s_2 + s_1.
\end{aligned}
$$

Рассматривая их последовательно и учитывая неравенства $s_i \leq p^{n-i}$, получаем, что $s_n = s_{n-1} = \ldots s_1 = 0$. Таким образом, остается единственная возможность $s_0 = p^n$. Такая допустимая матрица соответствуют $P(R)$.

Теперь обратимся ко второму слагаемому в (17) и докажем, что если $\widetilde{R} <_L Q$, то все слагаемые в $((P^{p^n})P(Q))_{Mil}$ больше $P(R)$.

Из равенства $p^n = \sum p^i s_i$ следует, что хотя бы одно $s_j \neq 0$. Предположим сначала, что $s_j \neq 0$ для некоторого $j > 0$ (иначе $s_0 = p^n$, и этот случай мы рассмотрим позже). У этого числа $s_j$ один из разрядов $p$-адического разложения отличен от 0. А именно, пусть в сумме $s_j = \sum p^m \beta_m$ коэффициент $\beta_m \neq 0$. Напомним, что $s_j \leq p^{n-j}$, поэтому $j + m \leq n$. Предположим, что соответствующий этой допустимой матрице милноровский элемент $P(T)$ присутствует в разложении $((P^{p^n})P(S))_{Mil}$. Тогда произведение коэффициентов (19) отлично от 0, в частности, $\binom{t_m}{s_m} \neq 0$. Из леммы 1 следует, что $m$-й разряд $p$-адического разложения числа $t_j$ отличен от 0. Но этот элемент появляется в таблице разрядов последовательности $T$ не выше $n$-й диагонали, следовательно, $P(T) >_L P(R)$.

Рассмотрим теперь допустимую матрицу для $s_0 = p^n$, $s_1 = s_2 = \ldots = 0$. Легко видеть, что тогда для соответствующей последовательности $T = (t_0, t_1, \ldots)$ выполняются равенства $t_0 = q_0 + p^n$ и $t_j = q_j$ при $j > 0$. Аналогичным образом связаны $R$ и $\widetilde{R}$: $r_0 = \tilde{r}_0 + p^n$ и $r_j = \tilde{r}_j$ при $j > 0$. Тогда если $\alpha_n(q_0) < p-1$, то из $Q >_L \widetilde{R}$ следует, что $T >_L R$. Если же $\alpha_n(q_0) = p-1$, то коэффициент (19) равен 0, так он содержит сомножитель $\binom{q_0+p_n}{p_n}$, равный 0 по лемме 1. Поэтому такой соответствующий такой последовательности милноровский элемент $P(T)$ в разложении $(P^{p^n}P(\widetilde{R}))_{Mil}$ не встречается.

Теперь рассмотрим случай $k < n$. Предположим по индукции, что утверждение верно для монома $X_k^{n-1}X_{k_1}^{n_1}\cdots X_{k_l}^{n_l}$. Тогда

$$\begin{aligned}(X_k^n X_{k_1}^{n_1}\cdots X_{k_l}^{n_l})_{Mil} &= (P^{p^n}(X_k^{n-1}X_{k_1}^{n_1}\cdots X_{k_l}^{n_l})_{Mil})_{Mil} = \\ &= (P^{p^n}(P(\widetilde{R}) + \sum_l P(Q_l)))_{Mil} = (P^{p^n}P(\widetilde{R}))_{Mil} + (\sum_l P^{p^n}P(Q_l))_{Mil}, \quad (20)\end{aligned}$$

где $P(\widetilde{R}) = P(\widetilde{r}_0, \widetilde{r}_1, \ldots, \widetilde{r}_m) = \gamma^{-1}(X_k^{n-1}X_{k_1}^{n_1}\cdots X_{k_l}^{n_l})$ и $P(\widetilde{R}) <_L P(Q_l)$ для любого $l$.

Из условия на последовательность $R$ следует, что для чисел $r_{n-k+1}, \ldots, r_n$ имеет место делимость $p^{i+1} \mid r_{n-j}$, а для чисел $r_0, \ldots, r_{n-k}$ — делимость $p^i \mid r_{n-j}$.

Допустимая матрица для произведения $P^{p^n}P(\widetilde{R})$

$$\begin{array}{cccccccc} * & r_0 - s_1 & r_1 - s_2 & \ldots & r_{n-k-1} + p^k - s_{n-k} & r_{n-k} - p^k - s_{n-k+1} & \ldots \\ s_0 & s_1 & s_2 & \ldots & s_{n-k} & s_{s-k+1} & \ldots \end{array} \quad (21)$$

Как отмечалось выше, из равенства $\sum s_i p^i = p^n$ следует, что $s_i \leq p^{n-i}$ для всех $i$; если же при каком-то $i$ достигается равенство $s_i = p^{n-i}$, то $s_j = 0$ при $j \neq i$.

Допустимая матрица, для которой $s_{n-k} = p^{n-k}$, а остальные $s_j$ равны 0, дает слагаемое в разложении $P^{p^n} P(\widetilde{R})$ в точности равное $P(R)$. Теперь мы покажем, что не существует ни одной допустимой матрицы, отличной от только что описанной, которая дает слагаемое $P(T)$, у которого в таблице разрядов на $n-1$-й диагонали и ниже, а также на $n$-й диагонали в строках с 0-й по $k-1$-ю стоят нули стоят нули. Отсюда будет следовать, что в разложении $P^{p^n} P(\widetilde{R})$ все слагаемые, отличные от $P(R)$, больше этого слагаемого.

Из условий на делимость элементов $r_j$ следуют аналогичные условия на делимость элементов $t_j$, откуда

$$
\begin{aligned}
&p \mid r_n + s_n \\
&p^2 \mid r_{n-1} - s_n + s_{n-1} \\
&\dots \\
&p^k \mid r_{n-k+1} - s_{n-k+2} + s_{n-k+1}.
\end{aligned}
$$

Рассматривая утверждения последовательно и учитывая, что для всех $s_i \leq p^{n-i}$ получаем, что $s_{n-k+1} = \ldots = s_n = 0$. Например, из первого условия следует, что $p \mid s_n$, но $s_n \leq p^0$, поэтому $s_n = 0$, и т.п.

Далее, $p^k \mid (r_{n-k} - p^k + s_{n-k})$, откуда $p^k \mid s_{n-k}$. Теперь заметим, что $s_{n-k} \leq p^k$, тем самым у нас две возможности: $s_{n-k} = p^k$, которая обсуждалась выше, и $s_{n-k} = 0$, которую мы сейчас рассмотрим.

Имеем

$$
\begin{aligned}
&p^{k+1} \mid r_{n-k-1} + p^k + s_{n-k-1}\\
&p^{k+2} \mid r_{n-k-2} - s_{n-k-1} + s_{n-k-2}\\
&\ldots\\
&p^{n-1} \mid r_1 - s_2 + s_1\\
&p^n \mid r_0 - s_1 + s_0,
\end{aligned}
$$

откуда

$$
\begin{aligned}
&p^{k+1} \mid p^k + s_{n-k-1}\\
&p^{k+2} \mid -s_{n-k-1} + s_{n-k-2}\\
&\ldots\\
&p^{n-1} \mid -s_2 + s_1\\
&p^n \mid -s_1 + s_0.
\end{aligned}
$$

Теперь домножим первое число на $p^{n-k}$, второе — на $p^{n-k-1}$, ..., последнее — на $p$, и полученные числа сложим. Полученное число $p^n + \sum\limits_{i=0}^{n-k-1} s_i p^{i+1} - \sum\limits_{i=1}^{n-k-1} s_i p^i$ должно делиться на $p^{n+1}$. Пользуясь равенством $\sum s_i p^i = p^n$, нетрудно понять, что это число равно $p^n + p^{n+1} - p^n + s_0$, откуда следует, что $s_0 = 0$, т. к. оно не превосходит $p^n$.

Теперь, рассмотрев условия

$$
\begin{aligned}
&p^n \mid -s_1\\
&p^{n-1} \mid -s_2 + s_1\\
&\ldots\\
&p^{k+2} \mid -s_{n-k-1} + s_{n-k-2}\\
&p^{k+1} \mid p^k + s_{n-k-1}
\end{aligned}
$$

в указанном порядке, последовательно получим $s_1 = s_2 = \ldots = s_{n-k-1} = 0$, и тогда из последнего условия должно следовать, что $p^k$ делится на $p^{k+1}$. Полученное противоречие показывает, что в разложении $(P^{p^n}P(\widetilde{R}))_{Mil}$ все слагаемые, отличные от $P(R)$, больше чем $P(R)$.

Теперь обратимся ко второй сумме в формуле (20) и докажем, что если $\widetilde{R} <_L Q$, то все слагаемые в $((P^{p^n})P(Q))_{Mil}$ больше $P(R)$.

Рассмотрим произвольную допустимую матрицу для произведения $(P^{p^n})P(Q)$

$$\begin{array}{cccccc} * & q_0 - s_1 & q_1 - s_2 & \dots & q_l - s_{l+1} & \dots \\ s_0 & s_1 & s_2 & \dots & s_{l+1} & \dots \end{array} \tag{22}$$

Пусть ей соответствует милноровский элемент $P(T)$.

Из равенства $p^n = \sum p^l s_l$ следует, что $s_j > 0$ для некоторого $j$. Пусть $m$ — отличный от нуля $m$-й разряд $p$–адического разложения $s_j$, т. е. $\alpha_m(s_j) \neq 0$. Предположим, что милноровский элемент $P(T)$ входит в разложение $((P^{p^n})P(Q))_{Mil}$ с ненулевым коэффициентом, см. (8). Тогда по лемме 1 имеем $\alpha_m(t_j) \neq 0$. Таким образом, если $m + j < n$ или $m + j = n$, но при этом $j > n - k$, то $P(T) >_L P(R)$.

Остается рассмотреть случай, когда не найдется $\alpha_m(s_j)$ отличного от 0 для $m+j < n$ или же $m+j = n$ и $j > n-k$. Из равенства $p^n = \sum p^l s_l$ тогда следует, что $s_j = p^{n-j}$ для некоторого $j \leq n - k$, а остальные $s_l = 0$.

Заметим, что если $\alpha_\sigma(q_\tau) \neq 0$ при $\sigma + \tau \leq n - 2$ или при $\sigma + \tau = n - 1$ и $\tau \geq n - k$, то в последовательности $T$, соответствующей рассматриваемой допустимой матрице имеем $\alpha_\sigma(t_\tau) \neq 0$ и тогда $P(T) >_L P(R)$.

Теперь рассмотрим случай, когда $\alpha_\sigma(q_\tau) \neq 0$ при $\sigma + \tau \leq n - 2$ или при $\sigma + \tau = n - 1$ и $\tau \geq n - k$. В этом случае из равенства $\alpha_k(\tilde{r}_{n-k-1}) = 1$ следует, что $\alpha_k(q_{n-k-1}) \geq 1$. Если при этом $j < n - k$, то $\alpha_k(t_{n-k-1}) \geq 1$ и

$P(T) >_L P(R)$.

Случай $j = n-k$ несколько интереснее. А именно, если $1 < \alpha_k(q_{n-k-1})$, то $\alpha_k(t_{n-k-1}) = \alpha_k(q_{n-k})-1 > 0$, и поэтому $P(T) >_L P(R)$. Если же $\alpha_k(q_{n-k-1}) = 1$, то $\alpha_k(t_{n-k-1}) = 0$, и все зависит от $\alpha_k(q_{n-k}) = 0$. А именно, если $\alpha_k(q_{n-k}) < p-1$, то $\alpha_k(t_{n-k}) = \alpha_k(q_{n-k})+1$, остальные элементы разверток $T$ и $Q$ совпадают, за исключением $\alpha_k(t_{n-k-1}) = 0 = \alpha_k(q_{n-k-1})-1$. Поэтому $P(T) >_L P(R)$. Наконец, если $\alpha_k(q_{n-k}) = p-1$, то $\alpha_k(t_{n-k}) = 0$ и возникают переносы в старшие разряды, поэтому, вообще говоря, сравнить $P(T)$ и $P(R)$ становится проблематично. Однако коэффициент (8), соответствующий $T$, в этом случае содержит множитель $\binom{t_{n-k}}{s_{n-k}}$, который равен 0 по лемме 1, т.к. $\alpha_k(t_{n-k}) = 0$ и $\alpha_k(s_{n-k}) = 1$. $\square$

**Следствие 4.** *$X$-базис треугольный по отношению к базису Милнора.*

## Дополнительные сведения

Результаты этого раздела мы приводим для полноты и без доказательств.

### Базис допустимых мономов

**Определение 10.** Для двух последовательностей неотрицательных целых чисел $R = (r_1, r_2, \ldots)$ и $S = (s_1, s_2, \ldots)$, в которых лишь конечное число членов отличны от нуля, будем говорить, что $R$ меньше $S$ в смысле правого лексикографического порядка и писать $R \prec_R S$, если существует такое $i$, что $r_j = s_j$ для всех $j > i$, и $r_i < s_i$.

Обратим внимание, что данный порядок отличается от правого лексикографического порядка из определения 3. Отличие состоит в том, что в определении 3 конечные последовательности выравниваются справа, а в определении 10 сравниваются бесконечные последовательности.

**Определение 11.** Пусть $P\langle R\rangle = P(r_1, \dots, r_m)$ — элемент базиса Милнора. Определим отображение $\gamma : B_{Mil} \to B_{Adm}$ формулой

$$\gamma : P(r_1, \dots, r_m) \mapsto P^{t_1} P^{t_2} \cdots P^{t_m}, \quad \text{где} \quad t_i = \sum_{k=i}^{m} p^{k-i} r_k.$$

Известно, что $\gamma$ является взаимно-однозначным отображением и сохраняет степень, см. [2]. При помощи отображения $\gamma$ перенесём порядок $\prec_R$ на множество допустимых мономов $B_{Adm}$.

Треугольность $B_{Adm}$ по отношению к $B_{Mil}$ вытекает из теоремы 7.

**Теорема 7.** *Пусть $P^T$ — допустимый моном, тогда $\gamma^{-1}(P^T)$ является наибольшим слагаемым разложения $(P^T)_{Mil}$.*

**Следствие 5.** *В разложении $(P\langle R\rangle)_{Adm}$ моном $\gamma P(R)$ является наибольшим слагаемым относительно порядка $\prec_R$.*

**Следствие 6.** *Пусть $P\langle R\rangle \in B_{Mil}$ и $\gamma(P\langle R\rangle)_{Mil} = P\langle R\rangle + \sum_i P\langle R_i\rangle$. Тогда*

$$P\langle R\rangle_{Adm} = \gamma P\langle R\rangle + \sum_i P\langle R_i\rangle_{Adm}$$

*задаёт рекуррентную формулу для вычисления $P\langle R\rangle_{Adm}$.*

### $C$-базис Арнона

**Определение 12.** Пусть $P\langle R\rangle = P(r_1,\ldots,r_m)$ — элемент базиса Милнора. Определим отображение $\gamma : B_{Mil} \to B_C$ формулой

$$\gamma : P(r_1,\ldots,r_m) \mapsto P^{t_m}P^{t_{m-1}}\cdots P^{t_1}, \quad \text{где} \;\; t_i = p^{i-1}\sum_{k=i}^{m} r_k.$$

Как видно из определения, $t_i$ делится на $p^{i-1}$ и $t_{i+1} = pt_i - p^i r_i$, откуда $t_{i+1} \le pt_i$ и поэтому $\gamma P\langle R\rangle \in B_C$. Далее, отображение $\gamma$ является взаимно–однозначным: обратное отображение $\gamma^{-1}(P^{t_m}P^{t_{m-1}}\cdots P^{t_1}) = P(r_1,\ldots,r_m)$ задаётся формулами $r_i = (pt_i - t_{i+1})/p^i$, при $1 \le i < m$, и $r_m = t_m/p^{m-1}$. Наконец, легко видеть, что отображение $\gamma$ сохраняет степень:

$$\begin{aligned}2(p-1)r_1 + 2(p-1)(p+1)r_2 + \ldots + 2(p-1)(p^n + p^{n-1} + \ldots + 1)r_n =\\ = 2(p-1)\sum_{i=1}^{m} r_i + 2(p-1)p\sum_{i=2}^{m} r_i + \ldots + 2(p-1)p^{m-1}r_m =\\ = 2(p-1)t_1 + 2(p-1)t_2 + \ldots + 2(p-1)t_m.\end{aligned}$$

С помощью биекции $\gamma$ перенесём порядок $\prec_R$ на $B_C$.

**Теорема 8.** *Пусть $P^T$ — некоторый $C$-моном. Тогда $\gamma^{-1}(P^T)$ является наибольшим слагаемым в разложении $(P^T)_{Mil}$.*

**Следствие 7.** *Пусть $P\langle R\rangle \in B_{Mil}$ и $\gamma(P\langle R\rangle)_{Mil} = P\langle R\rangle + \sum_i P\langle R_i\rangle$. Тогда выражение*

$$P\langle R\rangle_C = \gamma P\langle R\rangle + \sum_i P\langle R_i\rangle_C$$

*задаёт рекуррентную формулу для вычисления $P\langle R\rangle_C$.*

# Список публикаций по теме диссертации


[1] D. Yu. Emelyanov, Th. Yu. Popelensky, “On monomial bases in the mod $p$ Steenrod algebra”, Journal of Fixed Point Theory and Applications, 17:2 (2015), 341–353.

[2] Д. Ю. Емельянов, “О базисах Вуда алгебры Стинрода $\mod p$”, Фундаментальная и прикладная математика, 20:3 (2015), 83–90.

[3] Д. Ю. Емельянов, Ф. Ю. Попеленский “О заменах базисов в алгебре Стинрода $\mod p$”, Математический сборник, 208:4 (2017)

# Список литературы

[1] D. Arnon, “Monomial bases in the Steenrod algebr”, J. Pure Appl. Algebra, 96 (1994), 215–223.

[2] Н. Стинрод, Д. Эпстейн, “Когомологические операции“, М.: Наука, 1983.

[3] J. Milnor, “The Steenrod algebra and its dual”, Annals of Mathematics, (1958), 150–171.

[4] C. T. C. Wall, “Generators and relations for the Steenrod algebra”, Ann. of Math., 72:2 (1960), 429–444.

[5] D. Kraines, “On excess in the Milnor basis”, Bull. London Math. Soc., 3 (1971), 363–365.

[6] K. G. Monks, "Change of basis, monomial relations, and $P_s^t$ bases for the Steenrod algebra”, Journal of Pure and Applied Algebra, 125:1 (1998), 235–260.

[7] J. Adem, The iteration of Steenrod squares in algebraic topology, Proc. Nat. Acad. Sci. U.S.A. 38 (1952) 720–726.512

[8] J. Adem, The relations in Steenrod powers of cohomology classes, Algebraic geometry and topology, Symposium in honour of S. Lefschetz (Princeton University Press, 1957).

[9] W-T. Wu, Classes caracteristiques et carres de Steenrod, C. R. Acad. Sci. Paris 230 (1950) 508–511.

[10] W-T. Wu, Sur les puissances de Steenrod, Colloq. Toplogie Strasbourg (Publ. Math. Inst. Univ.)

[11] J.-P. Serre, Cohomologie modulo 2 des complexes d'Eilenberg–MacLane, Comment. Math. Helv. 27 (1953) 198–231

[12] H. Cartan, Algebres d'Eilenberg — Maclane et homotopie, Seminaire H. Cartan r . ENS, 7e annee, 1954/55 (русский перевод: А. Картан, Алгебры когомологий пространств Эйленберга — Маклейна; сб. перев. «Математика» 3:5 (1959); 3:6 (1959)).

[13] М. М. Постников, "К теореме Картана", УМН, 21:4(130) (1966), 35–46

[14] H. Cartan, Une theorie axiomatique des carres de Steenrod, C. R. Acad. Sci. Paris 230 (1950) 425–427.

[15] R. M. W. Wood, 'A note on bases and relations in the Steenrod algebra', Bull. London Math. Soc. 27 (1995) 380–386

[16] Bockstein, M. A complete system of fields of coefficients for the $\nabla$-homological dimension. C. R. (Doklady) Acad. Sci. URSS (N.S.) 38, (1943). 187–189.

[17] Понтрягин Л. С, Отображение трехмерной сферы в и-мерный комплекс, Доклады Ак. Наук СССР, XXXIV, No 2 (1942), 39-41.

[18] Steenrod N. E., Products of cocycles and extensions of mappings, Ann. of Math., 48 (1947), 290—320.

[19] H. Margolis, Spectra and the Steenrod algebra, North-Holland Math. Library 29 (Elsevier, Amsterdam, 1983)