О треугольных заменах базисов в алгебре Стинрода $\mathrm{mod}\, p$

Т. В. ОВЧИННИКОВА
Московский государственный университет им. М. В. Ломоносова
e-mail: tasya.ov@gmail.com

Ф. Ю. ПОПЕЛЕНСКИЙ
Московский государственный университет им. М. В. Ломоносова
e-mail: popelens@mech.math.msu.su

УДК 515.143.5

Ключевые слова: алгебра Стинрода, соотношения Адема, элемент Бокштейна, базис допустимых мономов, базис Милнора, базис Арнона, базис Уолла, замена базиса.

Аннотация

Работа посвящена исследованию треугольности замен аддитивных базисов в алгебрах Стинрода $\mathrm{mod}\, p$ (с элементом Бокштейна).

Abstract

T. V. Ovchinnikova, Th. Yu. Popelensky, On triangular changes of bases in the $\mathrm{mod}\, p$ *Steenrod algebra*, Fundamentalnaya i prikladnaya matematika, vol. 22 (2019), no. 6, pp. 183—200.

We discuss which transition matrices between some pairs of additive bases of the $\mathrm{mod}\, p$ Steenrod algebra with the Bockstein element are triangular.

1. Введение

В алгебре Стинрода $\mathrm{mod}\, 2$ известен ряд аддитивных базисов. Наиболее широко в литературе используются базис допустимых мономов и базис Милнора. Кроме этих базисов, в [3, 10] были построены так называемые Z-, X- и C-базисы. В [8] было показано, как из элементов Марголиса P_t^s построить целое семейство базисов алгебры Стинрода $\mathrm{mod}\, 2$. В той же работе исследовался вопрос, в каких случаях при $p = 2$ матрица перехода от одного аддитивного базиса к другому имеет треугольный вид. Важность этого вопроса связана, в частности, с тем, что в явном виде формула для разложения произведения двух базисных мономов по тому же базису известна лишь для базиса Милнора.

В алгебре Стинрода $\mathrm{mod}\, p$ базис допустимых мономов и базис Милнора были известны давно. Семейство P_s^t-базисов было построено в [9]. Для случая

Фундаментальная и прикладная математика, 2019, том 22, № 6, с. 183—200.

$p > 2$ возникают две возможности, а именно вместо изучения полной алгебры Стинрода A_p можно ограничиться лишь подалгеброй $\bar{A}_p$, порождённой элементами P^i, исключив из рассмотрения элемент Бокштейна β (подробности см. в следующем разделе). В [4] были построены X-базис и Z-базис для $p > 2$ (см. также [1]). В [5] были построены аналоги Z-, X- и C-базисов для A_p, мы называем их βZ-, βX- и βC-базисом соответственно. Кроме того, в указанной работе также построены XC- и ZA-базисы. Треугольные замены для базисов подалгебры $\bar{A}_p$ изучались в [2,6].

Данная работа посвящена случаю полной алгебры Стинрода для $p > 2$. Мы докажем, что матрицы перехода от базиса допустимых мономов, любого P^t_s-базиса, βC-базиса, XC-базиса и βX-базиса к базису Милнора являются треугольными. Кроме того, мы покажем, что матрица перехода от базиса Милнора к его модификации — PQ-базису — треугольная. Наконец, мы докажем, что ZA-базис треугольный по отношению к PQ-базису. Отметим, что, вообще говоря, далеко не всегда матрица перехода от мономиального базиса к базису Милнора треугольна. В частности, матрица перехода от Z-базиса к базису Милнора треугольной не является. Мы опустили несколько несложных утверждений о треугольности базисов, которые тривиальным образом выводятся из результатов [4] (например, про треугольность βWZ-базиса по отношению к βZ-базису), а также утверждения о возможности рекуррентного вычисления столбцов треугольных матриц замены через предшествующие столбцы, которые верны для всех рассматриваемых нами случаев.

2. Предварительные сведения

Зафиксируем простое число $p > 2$. Напомним, что алгебра Стинрода A_p, $p > 2$, порождена над $\mathbb{Z}/p$ элементом Бокштейна β и степенями Понтрягина P^i, $i \geqslant 0$, удовлетворяющими соотношениям

$$\text{для } a < pb\colon \quad P^a P^b = \sum_{j=0}^{[a/p]} (-1)^{a+j} \binom{(p-1)(b-j)-1}{a-pj} P^{a+b-j} P^j, \tag{2.1}$$

$$\text{для } a \leqslant pb\colon \quad P^a \beta P^b = \sum_{j=0}^{[a/p]} (-1)^{a+j} \binom{(p-1)(b-j)}{a-pj} \beta P^{a+b-j} P^j + \\ + \sum_{j=0}^{[(a-1)/p]} (-1)^{a+j+1} \binom{(p-1)(b-j)-1}{a-pj-1} P^{a+b-j} \beta P^j. \tag{2.2}$$

Здесь $P^0 = 1$, $\deg \beta = 1$, $\deg P^j = 2(p-1)j$. Обозначим через $\bar{A}_p$ алгебру, порождённую всеми элементами P^i и соотношениями (2.1); её можно рассматривать как подалгебру в A_p.

Напомним, что A_p является алгеброй Хопфа над $\mathbb{Z}/p$, а её двойственная алгебра A_p^* изоморфна (см. [7]) алгебре $\mathbb{Z}/p[\xi_1, \xi_2, \ldots] \otimes \Lambda(\tau_0, \tau_1, \ldots)$, где

$\deg \xi_k = 2p^k - 2$ и $\deg \tau_k = 2p^k - 1$. Элементы базиса Милнора имеют вид $Q_{i_1}Q_{i_2}\dots P(r_1, r_2, \dots)$, где $P(r_1, r_2, \dots)$ является двойственным к $\xi_1^{r_1}\xi_2^{r_2}\dots$, а каждый Q_j — двойственным к τ_j. Последовательность $(r_1, r_2, \dots)$ состоит из неотрицательных целых чисел, число положительных чисел в ней конечно. Произведение $Q_{i_1}Q_{i_2}\dots$ кодируется конечной последовательностью $i_1 < i_2 < \dots$, но часто удобно записать

$$Q_{i_1}Q_{i_2}\dots = Q_1^{\varepsilon_1}Q_2^{\varepsilon_2}\dots = Q(\varepsilon_1, \varepsilon_2, \dots),$$

где каждое из ε_j равно 0 или 1, причём ненулевых лишь конечное число. Если $r_j = 0$ или $\varepsilon_j = 0$ для всех $j > m$, то мы можем использовать конечные последовательности и писать $P(r_1, \dots, r_m)$ или $Q(\varepsilon_0, \dots, \varepsilon_m)$ соответственно. Элементы Q_k удовлетворяют рекуррентному соотношению $Q_0 = \beta$, $Q_{n+1} = P^{p^n}Q_n - Q_nP^{p^n}$ для $n \geqslant 0$. Кроме того, $P^n = P(n)$ для $n \geqslant 1$. Произведение $Q_{i_1}\dots Q_{i_m}$ будем называть Q-частью элемента $Q_{i_1}Q_{i_2}\dots P(r_1, r_2, \dots)$, а элемент $P(r_1, \dots)$ — его P-частью.

В отличие от других известных базисов A_p, для элементов Милнора есть явные формулы для умножения (см. [7]):

$$Q_iQ_j + Q_jQ_i = 0 \quad \text{для} \quad i \neq j, \tag{2.3}$$

$$P(r_1, r_2, \dots)Q_k = Q_kP(r_1, r_2, r_3) + Q_{k+1}P(r_1 - p^k, r_2, \dots) + \\ + Q_{k+2}P(r_1, r_2 - p^k, \dots) + \dots, \tag{2.4}$$

в частности,

$$P^nQ_k = \begin{cases} Q_kP^n & \text{для } p^k > n, \\ Q_kP^n + Q_{k+1}P^{n-p^k} & \text{для } p^k \leqslant n. \end{cases} \tag{2.5}$$

Наиболее важной является формула для произведения элементов $P(r_1, r_2, \dots)$ и $P(s_1, s_2, \dots)$:

$$P(r_1, r_2, \dots)P(s_1, s_2, \dots) = \sum_X c(X)P(t_1, t_2, \dots), \tag{2.6}$$

где $X = (x_{ij} \colon i, j \geqslant 0)$ пробегает множество матриц, таких что

$$\sum_i x_{ij} = s_j, \qquad j \neq 0, \tag{2.7}$$

$$\sum_j p^j x_{ij} = r_i, \quad i \neq 0, \tag{2.8}$$

$$t_h = \sum_{i+j=h} x_{ij}, \tag{2.9}$$

а $c(X)$ является произведением мультиномиальных коэффициентов

$$c(X) = \prod_h (x_{h0}, x_{h-1,1}, \dots, x_{0h}). \tag{2.10}$$

Такие матрицы называются *допустимыми*.

Определение 1. Два базиса M_1 и M_2 называются *треугольными по отношению друг к другу*, если элементы этих базисов могут быть упорядочены так, что матрица перехода будет треугольной по отношению к этим порядкам.

Это отношение рефлексивно, но в общем случае не транзитивно.

Чтобы доказать, что некоторый базис треугольный по отношению к базису Милнора, мы будем придерживаться следующей стратегии.

Обозначим множество элементов базиса M через B_M, а множество элементов базиса Милнора через B_{Mil}. Предположим, что мы нашли

1) полный порядок $<_{\mathrm{Mil}}$ на B_{Mil},
2) сохраняющую градуировку биекцию $\gamma\colon B_{\mathrm{Mil}} \to B_M$, такую что для любого $\theta \in B_M$ его разложение $(\theta)_{\mathrm{Mil}}$ по базису Милнора удовлетворяет соотношению
$$(\theta)_{\mathrm{Mil}} = \gamma^{-1}(\theta) + \sum_i \mu_i,$$
где $\mu \in B_{\mathrm{Mil}}$ and $\mu_i <_{\mathrm{Mil}} \gamma^{-1}(\theta)$.

В этом случае матрица перехода от B_M к B_{Mil} треугольная по отношению к порядку $<_{\mathrm{Mil}}$ на B_{Mil} и индуцированному им с помощью γ порядку на B_M.

Любой милноровский элемент кодируется двумя последовательностями $E = (\varepsilon_0, \varepsilon_1, \ldots)$ и $R = (r_1, r_2, \ldots)$, для которых $\varepsilon_j \in \{0, 1\}$ и $r_k \geqslant 0$ для всех j, k, причём лишь конечное число ε_j и r_k отлично от 0. Определим левый лексикографический порядок на множестве последовательностей $E = (\varepsilon_0, \varepsilon_1, \ldots)$ обычным образом: для двух последовательностей $E' = (\varepsilon'_0, \varepsilon'_1, \ldots)$ и $E'' = (\varepsilon''_0, \varepsilon''_1, \ldots)$ положим $E' <_{\mathrm{L}\varepsilon} E''$ (или $Q(E') <_{\mathrm{L}\varepsilon} Q(E'')$) тогда и только тогда, когда $e'_j < e''_j$ для некоторого j и $\varepsilon'_k = \varepsilon''_k$ для всех $k < j$.

Для последовательности $E = (\varepsilon_0, \varepsilon_1, \ldots)$ рассмотрим последовательность $a_1 < a_2 < \ldots < a_m$, такую что $\varepsilon_j = 1$ в том и только в том случае, когда $j = a_k$ для некоторого k, $1 \leqslant k \leqslant m$. Ясно, что $Q(E) = Q_{a_1} Q_{a_2} \ldots Q_{a_m}$. Пусть $a'_1 < \ldots < a'_m$ и $a''_1 < \ldots < a''_n$ соответствуют E' и E''. Тогда $Q(E') <_{\mathrm{L}\varepsilon} Q(E'')$ тогда и только тогда, когда выполняется одно из следующих условий:

а) $n > m$ и $a'_j = a''_j$ для $j = 1, \ldots, m$;
б) $a''_k < a'_k$ для некоторого $k \leqslant \min(m, n)$ и $a''_j = a'_j$ для всех $j < k$.

3. PQ-базис

Как было сказано в предыдущем разделе, милноровский элемент имеет вид $Q(E)P(R)$, где элементы последовательностей $E = (\varepsilon_0, \varepsilon_1, \ldots)$ и $R = (r_1, r_2, \ldots)$ удовлетворяют $\varepsilon_j \in \{0, 1\}$ и $r_k \geqslant 0$ для всех j, k, причём обе последовательности содержат только конечное число ненулевых элементов. Оказывается, множество всех элементов вида $P(R)Q(E)$ образует базис алгебры A_p, который мы будем называть PQ-базисом.

Определим полный порядок $<_{\mathrm{QP}}$ на множестве рассматриваемых пар (E, R) следующим образом. Положим $(E', R') <_{\mathrm{QP}} (E'', R'')$ (или эквивалентно

$Q(E')P(R') <_{\mathrm{QP}} Q(E'')P(R'')$ и $P(R')Q(E') <_{\mathrm{QP}} P(R'')Q(E'')$) тогда и только тогда, когда

1) $E' <_{L\varepsilon} E''$ или
2) $E' = E''$ и R' меньше R'' относительно левого лексикографического порядка.

Отметим, что второй пункт определения не используется в доказательстве теоремы 1 и добавлен лишь для того, чтобы порядок $<_{\mathrm{QP}}$ был полным.

Теорема 1. *Для любого PQ-элемента $P(R)Q(E)$ его разложение $\big(P(R)Q(E)\big)_{\mathrm{Mil}}$ по базису Милнора имеет вид*

$$\big(P(R)Q(E)\big)_{\mathrm{Mil}} = Q(E)P(R) + \sum_j c_j Q(E_j)P(R_j), \tag{3.1}$$

где $c_j \in \mathbb{Z}/p$ и $E_j <_{L\varepsilon} E$ для всех j. В частности, $(E_j, R_j) <_{\mathrm{QP}} (E, R)$ для всех j.

Доказательство. Если последовательность E состоит только из нулей, то утверждение теоремы очевидно. Пусть $Q(E) = Q_{a_1} \dots Q_{a_m}$, где $a_1 < a_2 < \dots < a_m$. Проведём индукцию по m. Для $m = 1$ утверждение следует из соотношения (2.4).

Для $m > 1$ рассмотрим последовательность $E' = (\varepsilon'_0, \varepsilon'_1, \dots)$, такую что $\varepsilon'_{a_m} = 0$ и $\varepsilon'_j = \varepsilon_j$ для всех $j \neq a_m$. Тогда, в частности, $Q(E')Q_{a_m} = Q(E)$. По предположению индукции имеет место равенство

$$\big(P(R)Q(E')\big)_{\mathrm{Mil}} = Q(E')P(R) + \sum_j c_j Q(E_j)P(R_j),$$

где $c_j \in \mathbb{Z}_p$ и $E_j <_{\mathrm{L}\varepsilon} E'$ для всех j. Тогда

$$\begin{aligned}\big(P(R)Q(E)\big)_{\mathrm{Mil}} &= (P(R)Q(E')Q_{a_m})_{\mathrm{Mil}} = \\ &= (Q(E')P(R)Q_{a_m})_{\mathrm{Mil}} + \sum_j c_j (Q(E_j)P(R_j)Q_{a_m})_{\mathrm{Mil}}.\end{aligned}$$

Мы получим $Q(E)P(R)$ в качестве одного из слагаемых в разложении $(Q(E')P(R)Q_{a_m})_{\mathrm{Mil}}$ с помощью коммутационных соотношений (2.4). Любое другое слагаемое в милноровском разложении $(Q(E')P(R)Q_{a_m})_{\mathrm{Mil}}$ имеет вид $Q(E')Q_{a_m+k}P(R'_k)$ для некоторой последовательности R'_k и подходящего целого $k > 1$. Очевидно,

$$Q_{a_1} \dots Q_{a_{m-1}} Q_{a_m} >_{\mathrm{L}\varepsilon} Q_{a_1} \dots Q_{a_{m-1}} Q_{a_m+k},$$

поскольку $a_1 < \dots < a_{m-1} < a_m < a_m + k$.

Любое слагаемое в милноровском разложении $(Q(E_j)P(R_j)Q_{a_m})_{\mathrm{Mil}}$ имеет вид $Q(E_j)Q_{a_m+k}P(R_{j,k})$ для некоторого целого $k \geqslant 0$ и подходящей последовательности $R_{j,k}$. Пусть $Q(E_j) = Q_{b_1} \dots Q_{b_{m-1}}$, где $b_1 < b_2 < \dots < b_{m-1}$. Так как $E' >_{\mathrm{L}\varepsilon} E_j$, то для некоторого $m - 1 \geqslant l \geqslant 1$

$$a_1 = b_1, \dots,\ a_{l-1} = b_{l-1},\ a_l < b_l.$$

Заметим, что $a_m+k \geqslant a_m > a_l$, следовательно, $Q(E')Q_{a_m} >_{\mathrm{L}\varepsilon} Q(E_j)Q_{a_m+k}$. $\square$

4. Базис допустимых мономов

В этом разделе нам понадобится следующий порядок $<_{\mathrm{A}}$ на множестве B_{Mil} милноровских элементов.

Определение 2. Для двух милноровских элементов $Q(E')P(R')$ и $Q(E'')P(R'')$ положим, что $Q(E')P(R') <_{\mathrm{A}} Q(E'')P(R'')$ тогда и только тогда, когда выполняется одно из двух условий:

1) $E' >_{\mathrm{L}\varepsilon} E''$;
2) $E' = E''$ и $R' <_{\mathrm{MR}} R''$ по отношению к правому лексикографическому порядку, иными словами, существует i, такое что $r'_i < r''_i$ и $r'_j = r''_j$ для всех $j > i$.

Напомним, что *допустимым* называется моном

$$\beta^{\varepsilon_0}P^{t_1}\beta^{\varepsilon_1}P^{t_2}\dots P^{t_m}\beta^{\varepsilon_m},$$

такой что $t_k \geqslant pt_{k+1}+\varepsilon_k$ для всех $1 \leqslant k \leqslant m-1$. Множество B_{Adm} допустимых мономов образует базис A_p.

Определение 3. Определим отображение $\gamma\colon B_{\mathrm{Mil}} \to B_{\mathrm{Adm}}$. Выберем целое число m, такое что $\varepsilon_j = 0$ и $r_j = 0$ для всех $j \geqslant m$. Положим

$$\gamma\colon Q(\varepsilon_0,\varepsilon_1,\dots,\varepsilon_m)P(r_1,r_2,\dots,r_m) \mapsto \beta^{\varepsilon_0}P^{t_1}\beta^{\varepsilon_1}P^{t_2}\dots P^{t_m}\beta^{\varepsilon_m}, \tag{4.1}$$

где

$$t_i = \sum_{k=i}^{m} p^{k-i}(r_k+\varepsilon_k).$$

Отображение γ не зависит от выбора m. Нетрудно проверить, что γ сохраняет степень и является биекцией. Обратное отображение $\gamma^{-1}\colon B_{\mathrm{Adm}} \to B_{\mathrm{Mil}}$ задаётся формулами $r_m = t_m - \varepsilon_m$, $r_k = t_k - pt_{k+1} - \varepsilon_k$ для $1 \leqslant k \leqslant m-1$ и $r_j = 0$, $\varepsilon_j = 0$ для $j > m$.

Отображение γ и порядок $<_{\mathrm{A}}$ на B_{Mil} индуцируют порядок на B_{Adm}.

Лемма 1. *Рассмотрим $E' = (\varepsilon'_0,\varepsilon'_1,\dots)$ и $E'' = (\varepsilon''_0,\varepsilon''_1,\dots)$, для которых $E' <_{\mathrm{L}\varepsilon} E''$. Пусть Q_a — произвольный элемент, такой что $Q(E')Q_a \neq 0$ и $Q(E'')Q_a \neq 0$. Тогда $Q(E')Q_a <_{\mathrm{L}\varepsilon} Q(E'')Q_a$.*

Доказательство состоит в очевидном применении соотношения (2.3).

Лемма 2. *Пусть A и B — два милноровских элемента, причём $A <_{\mathrm{A}} B$. Пусть для некоторого Q_a выполняется $Q_aB \neq 0$. Тогда любое слагаемое в разложении по базису Милнора элемента AQ_a меньше относительно порядка $<_{\mathrm{A}}$, чем Q_aB.*

Доказательство следует из перестановочного соотношения (2.5) и леммы 1.

Лемма 3. *Максимальное слагаемое относительно порядка $<_{\mathrm{A}}$ в разложении по базису Милнора элемента $P(t)Q_{a_1}\dots Q_{a_s}$, где $a_1 < a_2 < \dots < a_s$ и $t \geqslant \sum\limits_i p^{a_i}$, равно*

$$Q_{a_1+1}\dots Q_{a_s+1}P\Big(t-\sum_i p^{a_i}\Big).$$

Доказательство. Применим индукцию по s. Случай $s=1$ следует из формулы (2.5).

Предположим, что $s>1$. Тогда

$$P(t)Q_{a_1}\dots Q_{a_{s+1}} = \Big(Q_{a_1+1}\dots Q_{a_s+1}P\Big(t-\sum_{i=1}^{s}p^{a_i}\Big)+A\Big)Q_{a_{s+1}} =$$

$$= Q_{a_1+1}\dots Q_{a_s+1}Q_{a_{s+1}+1}P\Big(t-\sum_{i=1}^{s+1}p^{a_i}\Big)+$$

$$+ Q_{a_1+1}\dots Q_{a_s+1}Q_{a_{s+1}}P\Big(t-\sum_{i=1}^{s}p^{a_i}\Big)+AQ_{a_{s+1}},$$

где по предположению индукции любое слагаемое в милноровском разложении элемента A относительно порядка $<_{\mathrm{A}}$ меньше, чем

$$Q_{a_1+1}\dots Q_{a_s+1}P\Big(t-\sum_{i=1}^{s}p^{a_i}\Big).$$

Следовательно, в правой части равенства первое слагаемое A-максимально. $\square$

Теорема 2. *Для любого допустимого монома P^T милноровский элемент $P\big(\gamma^{-1}(T)\big)$ является A-максимальным слагаемым в разложении $(P^T)_{\mathrm{Mil}}$.*

Доказательство. Случай $m=0$ совпадает с теоремой 4.1 из [6] (см. также [8, теорема 4.1]).

Для $m>0$ будем рассуждать по индукции. Случай $m=1$ покрывается соотношениями

$$\beta P^n = Q_0P(n),$$
$$P^n\beta = Q_0P(n)+Q_1P(n-1),$$
$$\beta P^n\beta = Q_0Q_1P(n-1).$$

Для $m>1$ рассмотрим последовательность $T=(\varepsilon_0,t_1,\varepsilon_1,\dots,t_m,\varepsilon_m)$, отвечающую допустимому моному P^T. Без ограничения общности можно считать, что $\varepsilon_0=0$. По предположению индукции формула (4.1) верна для $T'=(\varepsilon_1,t_2,\varepsilon_2,\dots,t_m,\varepsilon_m)$. Ясно, что

$$\gamma^{-1}(P^{T'}) = Q(\varepsilon_1,\dots,\varepsilon_m,0,\dots)P(r_2,\dots,r_m,0,\dots).$$

Поэтому

$$P^T = P(t_1)\Big(Q(\varepsilon_1,\varepsilon_2,\dots)P(r_2,r_3,\dots)+\sum_k Q(\Delta_k)P(S_k)\Big), \tag{4.2}$$

где $Q(\Delta_k)P(S_k) <_{\mathrm{A}} \gamma^{-1}(P^{T'})$ для всех k. Из леммы 3 следует, что слагаемым с $L\varepsilon$-минимальной Q-частью в милноровском разложении элемента $P(t_1)Q(\varepsilon_1, \varepsilon_2, \ldots)$ служит

$$Q(0, \varepsilon_1, \varepsilon_2, \ldots)P\biggl(t_1 - \sum_{k=1}^{m} p^{k-1}p^k\biggr).$$

Следовательно, A-максимальное слагаемое в разложении по базису Милнора элемента $P(t_1)Q(\varepsilon_1, \varepsilon_2, \ldots)P(r_2, r_3, \ldots)$ возникает из

$$Q(0, \varepsilon_1, \varepsilon_2, \ldots)P\biggl(t_1 - \sum_{k=1}^{m} p^{k-1}\varepsilon_k\biggr)P(r_2, r_3, \ldots),$$

поскольку у всех остальных слагаемых Q-части больше относительно порядка $<_{\mathrm{L}\varepsilon}$.

Теперь определим A-максимальное слагаемое в милноровском разложении элемента

$$Q(0, \varepsilon_1, \varepsilon_2, \ldots)P\biggl(t_1 - \sum_{k=1}^{m} p^{k-1}\varepsilon_k\biggr)P(r_2, r_3, \ldots).$$

По [6, лемма 4.2] это в точности элемент $P(r_1, r_2, \ldots)$. Отметим, что доказательство этой леммы аналогично доказательству леммы 4.3 работы [8].

Рассмотрим оставшиеся слагаемые в (4.2). Для простоты обозначим произвольный элемент $Q(\Delta_k)R(S_k)$ через

$$Q(\Delta)R(S) = Q_0^{\delta_1}Q_1^{\delta_2}\ldots Q_{l-1}^{\delta_l}P(s_1, s_2, \ldots).$$

Этот элемент A-меньше, чем $Q(\varepsilon_1, \varepsilon_2, \ldots)P(r_2, r_3, \ldots)$, поэтому имеются два случая.

Случай 1: $(\delta_1, \delta_2, \ldots) >_{\mathrm{L}\varepsilon} (\varepsilon_1, \varepsilon_2, \ldots)$. По лемме 3 слагаемые с $L\varepsilon$-минимальной Q-частью в милноровском разложении $P(t_1)Q(\Delta)R(S)$ возникают из

$$Q(0, \delta_1, \delta_2, \ldots)P\biggl(t_1 - \sum_{k} p^{k-1}\delta_k\biggr)P(R),$$

но все они A-меньше, чем $Q(0, \varepsilon_1, \varepsilon_2, \ldots)P(X)$ для всех X.

Случай 2: $(\delta_1, \delta_2, \ldots) = (\varepsilon_1, \varepsilon_2, \ldots)$ и $S <_{\mathrm{MR}} (r_2, r_3, \ldots)$. В милноровском разложении элемента $P(t_1)Q(\Delta)R(S)$ максимальное слагаемое возникает из

$$Q(0, \varepsilon_1, \varepsilon_2, \ldots)P\biggl(t_1 - \sum_{k} p^{k-1}\varepsilon_k\biggr)P(S).$$

Согласно следствию 4.1 из [6], которое является непосредственным обобщением на случай $p > 2$ следствия 4.4 из [8], любое слагаемое в

$$\biggl(P\biggl(t_1 - \sum_{k} p^{k-1}\varepsilon_k\biggr)P(S)\biggr)_{\mathrm{Mil}}$$

MR-меньше, чем $P(r_1, r_2, \ldots)$. □

5. Базис βC-мономов

Определение 4. Определим βC-моном как моном

$$P^J = \beta^{\varepsilon_{r+1}} P^{j_r} \beta^{\varepsilon_r} \dots \beta^{\varepsilon_1} P^{j_0} \beta^{\varepsilon_0},$$

для которого последовательность $J = (\varepsilon_{r+1}, j_r, \varepsilon_r, \dots, \varepsilon_1, j_0, \varepsilon_0)$ удовлетворяет двум условиям:

1) $j_k \leqslant p j_{k-1} + \varepsilon_k$ для всех k,
2) p^k делит $j_k - p j_{k-1} - \varepsilon_k$ для всех k.

Последовательность J, удовлетворяющая условиям 1) и 2), называется βC-последовательностью.

Условие 2) может быть быть заменено на эквивалентное:

2′) p^k делит $j_k - \sum\limits_{l=0}^{k} p^{k-l}\varepsilon_l$ для всех k.

Моном, составленный только из элементов P^j, называется *C-мономом*, если он является βC-мономом, для которого $\varepsilon_k = 0$ для всех k.

Теорема 3 [5]. *Множество $B_{\beta C}$ всех βC-мономов образует базис A_p.*

Рассмотрим на множестве B_{Mil} порядок, использованный в разделе 4 (см. определение 2).

Определение 5. Зададим отображение $\gamma\colon B_{\mathrm{Mil}} \to B_{\beta C}$ следующим образом. Для элемента $Q(E)P(R)$ выберем целое m, для которого $\varepsilon_j = 0$ и $r_j = 0$ для всех $j > m$. Положим

$$\gamma\colon Q(E)P(R) = Q(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_m)P(r_1, r_2, \dots, r_m) \mapsto \\ \mapsto \beta^{\delta_m} P^{t_m} \beta^{\delta_{m-1}} P^{t_{m-1}} \dots P^{t_1} \beta^{\delta_0}, \quad (5.1)$$

где

$$\delta_i = \varepsilon_{m-i}, \quad t_i = p^{i-1} \sum_{k=i}^{m} r_k + \sum_{k=m-1+i}^{m} p^{m-1+i-k}\varepsilon_k.$$

Легко проверить, что $\gamma\big(Q(E)P(R)\big)$ корректно определено, т. е. не зависит от выбора m. Также легко проверить, что γ сохраняет степень и является биекцией. Обратное отображение задаётся формулами

$$r_m = \frac{t_m - (\delta_{m-1} + p\delta_{m-2} + \ldots + p^{m-1}\delta_0)}{p^{m-1}}, \quad (5.2)$$

$$r_k = \frac{pt_k + \delta_k - t_{k+1}}{p^k} \quad \text{для} \quad k = 1, \dots, m-1. \quad (5.3)$$

С помощью отображения γ перенесём A-порядок с B_{Mil} на $B_{\beta C}$.

Теорема 4. *Для произвольного βC-монома P^T милноровский элемент $Q(E)P(R) = \gamma^{-1}(P^T)$ является максимальным в милноровском разложении $(P^T)_{\mathrm{Mil}}$.*

Доказательство. Проведём индукцию по m. Случай $m = 0$ очевиден, а случай $m = 1$ покрывается формулами

$$\beta P^n = Q_0 P(n),$$
$$P^n \beta = Q_0 P(n) + Q_1 P(n-1),$$
$$\beta P^n \beta = Q_0 Q_1 P(n-1).$$

Для $m > 1$ рассмотрим βC-моном $P^T = P^{t_m} \beta^{\delta_{m-1}} P^{t_{m-1}} \beta^{\delta_{m-2}} \dots \beta^{\delta_1} P^{t_1} \beta^{\delta_0}$, где без ограничения общности мы положили $\delta_m = 0$. Пусть $\gamma^{-1}(P^T) = Q(E)P(R)$, где $E = (\varepsilon_0, \dots, \varepsilon_m)$ и $R = (r_1, \dots, r_m)$. По предположению индукции теорема верна для $P^{T'}$, где $T' = (\delta_{m-1}, t_{m-1}, \dots t_1, \delta_0)$. Пусть

$$\gamma^{-1}(P^{T'}) = Q(\varepsilon'_0, \dots, \varepsilon'_{m-1}, 0, \dots) P(r'_1, \dots, r'_{m-1}, 0, \dots),$$

где

$$\varepsilon'_k = \delta_{m-1-k},$$
$$r'_{m-1} = \frac{t_{m-1} - (\delta_{m-2} + p\delta_{m-3} + \dots + p^{m-2}\delta_0)}{p^{m-2}},$$
$$r'_k = \frac{pt_k + \delta_k - t_{k+1}}{p^k} \text{ for } k = 1, \dots, m-2.$$

Нетрудно проверить, что $r'_1 = r_1, \dots, r'_{m-2} = r_{m-2}$, $r'_{m-1} = r_{m-1} + r_m$ и $\varepsilon'_j = \varepsilon_{j+1}$ для всех j. Тогда

$$\gamma^{-1}(P^{T'}) = Q(\varepsilon_1, \varepsilon_2, \dots) P(r_1, \dots, r_{m-2}, r_m + r_{m-1}) + \sum_k c_k Q(\Delta_k) P(S_k),$$

где $c_k \in \mathbb{Z}/p$ и

$$Q(\Delta_k)P(S_k) <_{\mathrm{A}} Q(\varepsilon_1, \varepsilon_2, \dots) P(r_1, \dots, r_{m-2}, r_m + r_{m-1})$$

для всех k. Имеем равенство

$$(P^T)_{\mathrm{Mil}} = \big(P(t_m)P^T\big)_{\mathrm{Mil}} =$$
$$= \Big(P(t_m)\big[Q(\varepsilon_1, \varepsilon_2, \dots) P(r_1, \dots, r_{m-2}, r_m + r_{m-1}) + \sum_k c_k Q(\Delta_k) P(S_k)\big]\Big)_{\mathrm{Mil}}.$$

Максимальное слагаемое в милноровском разложении элемента

$$P(t_m) Q(\varepsilon_1, \varepsilon_2, \dots) P(r_1, \dots, r_{m-2}, r_m + r_{m-1})$$

возникает из милноровского разложения слагаемого

$$Q(0, \varepsilon_1, \varepsilon_2, \dots) P\left(t_m - \sum_k p^{k-1}\varepsilon_k\right) P(r_1, \dots, r_{m-2}, r_m + r_{m-1})$$

по лемме 3. Этот элемент в точности равен

$$Q(0, \varepsilon_1, \varepsilon_2, \dots) P(r_1, \dots, r_{m-2}, r_{m-1}, r_m),$$

детали легко извлечь из доказательства теоремы 6.1 работы [6] (см. также [8, доказательство теоремы 6.1]).

Остаётся показать, что любое слагаемое в $\big(P(t_m)Q(\Delta_k)P(S_k)\big)_{\mathrm{Mil}}$ относительно порядка $<_{\mathrm{A}}$ меньше, чем $Q(E)P(R)$. Если $\Delta_k >_{\mathrm{L}\varepsilon} (\varepsilon_1, \varepsilon_2, \ldots)$, то по лемме 3 Q-часть любого слагаемого в $\big(P(t_m)Q(\Delta_k)P(S_k)\big)_{\mathrm{Mil}}$ $L\varepsilon$-больше, чем $(0, \varepsilon_1, \varepsilon_2, \ldots)$. Если же $\Delta_k = (\varepsilon_1, \varepsilon_2, \ldots)$ и $S_k <_{\mathrm{MR}} (r_1, \ldots, r_{m-2}, r_{m-1} + r_m)$, то максимальное слагаемое в милноровском разложении $\big(P(t_m)Q(\Delta_k)P(S_k)\big)_{\mathrm{Mil}}$ возникает из произведения

$$Q(0, \varepsilon_1, \varepsilon_2, \ldots)P\left(t_m - \sum_l p^{k-1}\varepsilon_k\right)P(S_k).$$

Из доказательства теоремы 6.1 в [6] (см. также [8, доказательство теоремы 6.1]) следует, что любое слагаемое в разложении

$$\left(P\left(t_m - \sum_l p^{k-1}\varepsilon_k\right)P(S_k)\right)_{\mathrm{Mil}}$$

в порядке $<_{\mathrm{MR}}$ меньше, чем $P(r_1, \ldots, r_{m-1}, r_m)$. □

Следствие 1. *Базис допустимых мономов и базис βC-мономов треугольны по отношению друг к другу.*

Это вытекает из теорем 2 и 4, так как в обеих теоремах используется один и тот же полный порядок на базисе Милнора.

6. βX и βZ базисы

Определение 6. Зададим *правый* лексикографический порядок на конечных последовательностях неотрицательных целых чисел следующим образом. Будем считать, что $I <_{\mathrm{R}} J$ для $I = (i_1 \ldots i_n)$ и $J = (j_1 \ldots j_m)$, если выполняется одно из следующих условий:

— I пусто, а J нет,
— $I, J \neq \varnothing$ и $i_n < j_m$,
— $I, J \neq \varnothing$, $i_n = j_m$, and $(i_1, \ldots, i_{n-1}) <_{\mathrm{R}} (j_1, \ldots, j_{m-1})$.

Отметим, что это определение отличается от определения порядка $<_{\mathrm{MR}}$ (см. определение 2).

Определение 7. Аналогичным образом зададим *левый* лексикографический порядок на конечных последовательностях неотрицательных целых чисел. А именно, $I <_{\mathrm{L}} J$ для $I = (i_1, \ldots, i_n)$ и $J = (j_1, \ldots, j_m)$, если выполняется одно из следующих условий:

— I пусто, а J нет,
— $I, J \neq \varnothing$ и $i_1 < j_1$,
— $I, J \neq \varnothing$, $i_1 = j_1$ и $(i_2, \ldots, i_n) <_{\mathrm{L}} (j_2, \ldots, j_m)$.

Определение 8. Положим $Z_k^n = P^{p^k} \cdots P^{p^n}$ и $X_k^n = P^{p^n} \cdots P^{p^k}$ для $0 \leqslant k \leqslant n$. Определим Z-моном как произведение

$$Z^I = Z^I = (Z_{k_1}^{n_1})^{q_1} \ldots (Z_{k_m}^{n_m})^{q_m}, \tag{6.1}$$

а X-моном как произведение

$$X^J = (X_{k_m}^{n_m})^{q_m} \ldots (X_{k_1}^{n_1})^{q_1}, \tag{6.2}$$

где I — последовательность $\big((n_1, k_1, q_1), \ldots, (n_m, k_m, q_m)\big)$, а J — последовательность $\big((n_m, k_m, q_m), \ldots, (n_1, k_1, q_1)\big)$, такие что

$$(n_m, k_m) <_{\mathrm{L}} \ldots <_{\mathrm{L}} (n_2, k_2) <_{\mathrm{L}} (n_1, k_1)$$

и $0 < q_j < p$ для всех j.

Единицу алгебры $1 \in A_p$ можно рассматривать и как Z^I, и как X^I для пустой последовательности I.

Определение 9. Определим βZ-моном как моном, составленный из символов P^{p^j} и β и имеющий вид $Z\beta Z_0^{m_r}\beta Z_0^{m_{r-1}} \cdots \beta Z_0^{m_1}\beta^{\varepsilon}$, где Z — некоторый Z-моном или 1, $m_r > m_{r-1} > \ldots > m_1$ и $\varepsilon \in \{0, 1\}$.

Определение 10. Определим βX-моном как моном, составленный из символов P^{p^j} и β и имеющий вид $\beta^{\varepsilon} X_0^{m_1} \cdots \beta X_0^{m_{r-1}}\beta X_0^{m_r}\beta X$, где X — некоторый X-моном или 1, $m_r > m_{r-1} > \ldots > m_1$ и $\varepsilon = \{0, 1\}$.

Теорема 5 (см. [5]).

1. *Множество всех βZ-мономов образует аддитивный базис A_p.*
2. *Множество всех βX-мономов образует аддитивный базис A_p.*

Теперь зададим специальный порядок на множестве всех элементов вида $P(R)$ и отображение γ множества B_{Mil} в множество всех βX-мономов. Для элемента $P(r_0, \ldots, r_m)$ (заметим, что здесь мы сдвинули нумерацию элементов r_j) рассмотрим p-адические разложения

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

Положим $\alpha_{ij} = \alpha_i(r_j)$, $i, j \geqslant 0$. Расположим числа α_{ij} в последовательность

$$(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{02}, \alpha_{11}, \alpha_{20}, \alpha_{03}, \ldots).$$

Левый лексикографический порядок на множестве всех таких последовательностей задаёт порядок $<_{\mathrm{ML}}$ на множестве милноровских элементов вида $P(R)$.

Пусть $E = (\varepsilon_0, \varepsilon_1, \ldots)$ выполняется $Q(E) = Q_{a_1} \ldots Q_{a_m}$, где $a_1 < \ldots < a_m$. Для милноровского элемента $Q(E)P(R)$ определим

$$\gamma\big(Q(E)P(R)\big) = \\ = X_0^{a_1-1}\beta \ldots X_0^{a_m-1}\beta (X_0^0)^{\alpha_{00}} (X_0^1)^{\alpha_{01}} (X_1^1)^{\alpha_{10}} (X_0^2)^{\alpha_{02}} \ldots (X_i^{i+j})^{\alpha_{ij}} \ldots,$$

где $X_0^{a_1-1} = 1$ для $a_1 = 0$.

Лемма 4. *Отображение γ сохраняет степень и является биекцией из множества B_{Mil} на множество $B_{\beta X}$ всех βX-мономов.*

Определение 11. Для двух милноровских элементов $Q(E')P(R')$ и $Q(E'')P(R'')$ положим $Q(E')P(R') <_{\beta X} Q(E'')P(R'')$ тогда и только тогда, когда выполняется одно из двух условий:

1) $E' >_{\mathrm{L}\varepsilon} E''$;
2) $E' = E''$ и $R' <_{\mathrm{ML}} R''$.

Теорема 6 (см. [2]). *Пусть θ — некоторый X-моном. Тогда его милноровское разложение $(\theta)_{\mathrm{Mil}}$ имеет вид*

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

где $\gamma^{-1}(\theta) <_{\mathrm{ML}} \eta_i$ для всех i.

Лемма 5. *Для любого $m \geqslant 0$ имеет место соотношение*

$$X_0^m\beta = Q_{m+1} + \sum_{j=0}^{m} Q_j P_j, \tag{6.3}$$

где $P_j \in \bar{A}_p$ — элементы подалгебры $\bar{A}_p$.

Доказательство. Для $m = 0$ утверждение следует из равенства

$$X_0^0\beta = P^1\beta = P^1Q_0 = Q_1 + Q_0P^1.$$

Для $m > 0$ будем рассуждать по индукции:

$$X_0^{m+1}\beta = P^{p^{m+1}}X_0^m\beta = P^{p^{m+1}}\left(Q_{m+1} + \sum_{j=0}^{m} Q_jP_j\right) =$$

$$= Q_{m+2} + Q_{m+1}P^{p^{m+1}} + \sum_{j=0}^{m}(Q_jP^{p^{m+1}} + Q_{j+1}P^{p^{m+1}-p^j})P_j. \quad \square$$

Теорема 7. *Для произвольного βX-монома $\theta = \beta^\varepsilon X_0^{a_1}\beta\ldots X_0^{a_m}\beta X$ положим $Q(E)P(R) = \gamma^{-1}(\theta)$. Тогда милноровское разложение θ имеет вид*

$$(\theta)_{\mathrm{Mil}} = Q(E)P(R) + \sum_j c_jQ(E_j)P(S_j), \tag{6.4}$$

где $c_j \in \mathbb{Z}/p$ и $Q(E_j)P(S_j) <_X Q(E)P(R)$ для всех j.

Доказательство. Без ограничения общности можно считать, что $\varepsilon = 0$; в противном случае нужно домножить формулы, которые будут получены ниже, на $\beta = Q_0$ слева. Применим индукцию по m. Для $m = 0$ утверждение совпадает с теоремой 6 (доказательство см. в [2]). Для $m > 0$ рассмотрим βX-моном $\theta' = X_0^{a_2}\beta\ldots X_0^{a_m}\beta X$. По предположению индукции

$$(X_0^{a_2}\beta\ldots X_0^{a_m}\beta X)_{\mathrm{Mil}} = Q_{a_2+1}\ldots Q_{a_m+1}P(R) + \sum_j c'_jQ(E'_j)P(S'_j), \tag{6.5}$$

где $c'_j \in \mathbb{Z}/p$ и $Q(E'_j)P(S'_j) <_X Q(E')P(R)$ для всех j. Таким образом, нам нужно вычислить X-наибольшее слагаемое в милноровском разложении

$$\left(\left(Q_{a_1+1} + \sum_{k=0}^{a_1} Q_k P_k\right)\left(Q_{a_2+1}\dots Q_{a_m+1}P(R) + \sum_j c'_j Q(E'_j)P(S'_j)\right)\right)_{\text{Mil}}. \quad (6.6)$$

Это разложение содержит элемент $Q_{a_1+1}Q_{a_2+1}\dots Q_{a_m+1}P(R) = Q(E)P(R)$. Мы докажем, что все остальные слагаемые X-меньше, чем $Q(E)P(R)$.

Имеем, что $E'_j >_{\text{L}\varepsilon} E'$ для всех j, поэтому произведение $Q_{a_1+1}Q(E'_j)$ либо нулевое, либо $L\varepsilon$-больше, чем $Q_{a_1+1}Q(E') = Q(E)$.

Рассмотрим произвольное произведение $Q_kP_kQ_{a_2+1}\dots Q_{a_m+1}P(R)$. Прокоммутировав P_j с $Q_{a_2+1}\dots Q_{a_m+1}$, получим произведения вида $Q_{b_2}\dots Q_{b_m}$, где $b_l \geqslant a_l + 1$ для всех l, что следует из соотношения (2.4). В свою очередь, произведение $Q_kQ_{b_2}\dots Q_{b_m}$ либо нулевое, либо $L\varepsilon$-больше, чем $Q_{a_1+1}Q(E')$, так как $k \leqslant a_1$. Такое же рассуждение применимо к любому произведению $Q_kP_kQ(E'_j)P(S'_j)$. □

С другой стороны, нетрудно проверить, что βZ-базис не является треугольным по отношению к базису Милнора. В самом деле, βZ-базис A_p в градуировке $2(p-1)(p+2)$ содержит два элемента: $Z_0^1Z_0^0$ и $Z_1^1(Z_0^0)^2$. Непосредственные вычисления с помощью формулы умножения (2.6) показывают, что

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

и

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

Следовательно, при любых упорядочиваниях базиса Милнора и базиса Z-мономов соответствующая матрица перехода не будет треугольной.

7. XC-базис

Определение 12. Определим XC-моном как моном вида

$$\beta^\varepsilon X_0^{m_1}\beta\dots\beta X_0^{m_{r-1}}\beta X_0^{m_r}\beta P^I,$$

где P^I — некоторый C-моном (см. определение 4) или 1, $m_r > m_{r-1} > \dots > m_1 \geqslant 0$ и $\varepsilon \in \{0,1\}$.

Теорема 8 (см. [5]). *Множество B_{XC} всех XC-мономов образует базис A_p.*

Определим отображение $\gamma\colon B_{\text{Mil}} \to B_{XC}$ формулой

$$\gamma\colon Q_{a_1}\dots Q_{a_m}P(r_1,\dots,r_n) \mapsto X_0^{a_1-1}\beta\dots X_0^{a_m-1}\beta P^{t_m}\dots P^{t_0},$$

где $t_i = p^{i-1}\sum\limits_{k=i}^{n} r_k$. Здесь мы считаем, что $a_1 < \dots < a_m$ и что $X_0^{a_1-1} = 1$ для $a_1 = 0$.

Отображение γ сохраняет степень и является биекцией. Рассмотрим полный порядок $<_{\text{A}}$ на B_{Mil} (см. определение 2) и с помощью γ перенесём его на B_{XC}.

Теорема 9. *Для произвольного XC-монома $\theta = \beta^\varepsilon X_0^{a_1}\beta\dots X_0^{a_m}\beta P^I$ положим $Q(E)P(R) = \gamma^{-1}(\theta)$. Тогда милноровское разложение элемента θ имеет вид*

$$(\theta)_{\mathrm{Mil}} = Q(E)P(R) + \sum_j c_j Q(E_j)P(S_j), \tag{7.1}$$

где $c_j \in \mathbb{Z}/p$ и $Q(E_j)P(S_j) <_X Q(E)P(R)$ для всех j.

Доказательство. Без ограничения общности можно считать, что $\varepsilon = 0$; в противном случае домножим итоговую формулу слева на $\beta = Q_0$. Для $m = 0$ доказываемое утверждение совпадает с теоремой 6.1 работы [6] (см. также [8, теорема 6.1]). Для $m > 0$ применим индукцию по аналогии с доказательством теоремы 7. □

Следствие 2. *Базис допустимых мономов, βC-базис и XC-базис треугольны по отношению друг к другу.*

Это следует из теорем 2, 7 и 9, поскольку в них используется одно и то же упорядочение элементов базиса Милнора.

8. ZA-базис

Обозначим $\hat{Z}^m = P^{p^m+p^{m-1}+\dots+p+1}$. Можно показать, что $\hat{Z}^m = Z_0^m$ (см. [5]).

Определение 13. Определим ZA-моном как моном вида

$$P^I\beta\hat{Z}^{m_r}\beta\hat{Z}^{m_{r-1}}\beta\dots\beta\hat{Z}^{m_1}\beta^\varepsilon,$$

где P^I — допустимый моном, составленный только из элементов P^j, или 1, $m_r > m_{r-1} > \dots > m_1 \geqslant 0$ и $\varepsilon \in \{0,1\}$.

Теорема 10 (см. [2]). *Множество B_{ZA} всех ZA-мономов образует базис A_p.*

Определим порядок на множестве B_{PQ} всех PQ-мономов следующим образом. Положим $P(R')Q(E') <_{\mathrm{ZA}} P(R'')Q(E'')$, если выполняется одно из следующих условий:

1) $E' >_{\mathrm{L}\varepsilon} E''$,
2) $E' = E''$ и $R' <_{\mathrm{MR}} R''$.

Определим отображение $\gamma\colon B_{PQ} \to B_{ZA}$ по формуле

$$\gamma\colon P(r_1, r_2, \dots, r_n)Q_{a_1}\dots Q_{a_m} \to P^{t_1}\dots P^{t_n}\beta\hat{Z}^{a_m-1}\dots\beta\hat{Z}^{a_1-1}, \tag{8.1}$$

где $a_1 < \dots < a_m$ и $t_i = \sum\limits_{k=i}^{n} p^{k-i}r_k$ (ср. с формулой (4.1)). Здесь мы считаем, что $\hat{Z}^{a_1-1} = 1$ для $a_1 = 0$. Отображение γ является биекцией, сохраняющей степени. Порядок $<_{\mathrm{ZA}}$ с помощью биекции γ перенесём на B_{ZA}.

Лемма 6.

а) *Для $j > m$ выполняется равенство $Q_jP^{p^m} = P^{p^m}Q_j$.*

б) *Для $j < m$ выполняется равенство*

$$Q_j P^{p^m} = P^{p^m} Q_j - P^{p^m - p^j} Q_{j+1} + \\ + P^{p^m - p^j - p^{j+1}} Q_{j+2} + \ldots \pm P^{p^m - p^j - p^{j+1} - \ldots - p^{m-1}} Q_m. \quad (8.2)$$

в) *Для $m \geqslant 0$ выполняется*

$$\beta \hat{Z}^m = (-1)^{m+1} Q_{m+1} + \sum_{j<m+1} P_j Q_j, \quad (8.3)$$

где для любого j элемент P_j является степенью Понтрягина, такой что $\deg P_j + \deg Q_j = \deg \beta \hat{Z}^m = 2p^{m+1} - 1$.

Доказательство. Утверждение а) следует из соотношения (2.5). Для доказательства б) мы последовательно применяем соотношение (2.5):

$$\begin{aligned} Q_j P^{p^m} &= P^{p^m} Q_j - Q_{j+1} P^{p^m - p^j} = \\ &= P^{p^m} Q_j - P^{p^m - p^j} Q_{j+1} + Q_{j+2} P^{p^m - p^j - p^{j+1}} = \ldots = \\ &= P^{p^m} Q_j - P^{p^m - p^j} Q_{j+1} + P^{p^m - p^j - p^{j+1}} Q_{j+2} + \ldots \pm P^{p^m - p^j - p^{j+1} - \ldots p^{m-1}} Q_m. \end{aligned}$$

Для доказательства утверждения в) мы применим те же рассуждения, что и для б), но заметим при этом, что на последнем шаге самое последнее слагаемое равно $(-1)^{m+1} Q_{m+1}$. □

Теорема 11. *Для произвольного ZA-монома*

$$\theta = P^T \beta \hat{Z}^{a_m - 1} \ldots \beta \hat{Z}^{a_1 - 1}$$

положим

$$P(R)Q(E) = P(R)Q_{a_1} \ldots Q_{a_m} = \gamma^{-1}(\theta).$$

Тогда разложение θ по PQ-базису имеет вид

$$(\theta)_{PQ} = (-1)^{\delta} P(R)Q(E) + \sum_j c_j P(S_j)Q(E_j), \quad (8.4)$$

где $\delta = m(m-1)/2 + \sum\limits_j a_j$, $c_j \in \mathbb{Z}/p$ и $P(S_j)Q(E_j) <_{\mathrm{ZA}} P(R)Q(E)$ для всех j.

Доказательство. Для $m = 0$ утверждение совпадает с теоремой 2. Для $m > 0$ применим индукцию. Рассмотрим ZA-моном

$$\theta' = P^T \beta \hat{Z}^{a_m - 1} \ldots \beta \hat{Z}^{a_2 - 1}$$

(заметим, что $a_2 > 0$). По предположению индукции

$$(\theta')_{PQ} = (-1)^{\delta'} P(R)Q(E') + \sum_{c'_j} P(S'_j)P(E'_j),$$

где $\delta' = (m-2)(m-1)/2 + \sum_{j=2}^{m} c_j \in \mathbb{Z}/p$, $P(S'_j)Q(E'_j) <_{\mathrm{ZA}} P(R)Q(E')$ для всех j и $Q(E') = Q_{a_2} \dots Q_{a_m}$. По лемме 6

$$\beta \hat{Z}^{a_1-1} = (-1)^{a_1} Q_{a_1} + \sum_{i<a_1} P_i Q_i.$$

Следовательно,

$$\begin{aligned}(\theta)_{PQ} &= \left((\theta')_{PQ} \beta \hat{Z}^{a_1-1}\right)_{PQ} = \\ &= \left[\left[(-1)^{\delta'} P(R)Q(E') + \sum_{c'_j} P(S'_j)Q(E'_j)\right]\left[(-1)^{a_1} Q_{a_1} + \sum_{i<a_1} P_i Q_i\right]\right]_{PQ} = \\ &= \Bigg[(-1)^{\delta'+a_1} P(R)Q(E')Q_{a_1} + (-1)^{(m-2)(m-1)/2} P(R)Q(E') \sum_{i<a_1} P_i Q_i + \\ &+ \sum_{c'_j} P(S'_j)Q(E'_j)(-1)^{a_1} Q_{a_1} + \sum_{c'_j, i<a_1} P(S'_j)Q(E'_j)P_i Q_i\Bigg]_{PQ}.\end{aligned}$$

Для первого слагаемого имеем

$$(-1)^{\delta'+a_1} P(R)Q(E')Q_{a_1} = (-1)^{\delta'+a_1+(m-1)} P(R)Q_{a_1}Q(E') = (-1)^{\delta} P(R)Q(E).$$

Это в точности нужное максимальное слагаемое в (8.4). Остальные слагаемые ZA-меньше, чем $P(R)Q(E)$. Это можно установить, рассуждая аналогично доказательству теоремы 1. А именно, достаточно проверить, что коммутирование $Q(E')$ с P_i и $Q(E'_j)$ с P_i не может увеличить соответствующие мономы. □

9. Семейство P_t^s-базисов

Рассмотрим элементы $P_t^s = P(r_1, r_2, \dots) \in \bar{A}_p$, где все r_k равны 0, исключая $r_t = p^s$. Будем называть P_t^s-мономом произведение вида $(P_{t_1}^{s_1})^{m_1} \dots (P_{t_k}^{s_k})^{m_k}$ с попарно различными $P_{t_j}^{s_j}$ и $0 < m_j < p$. Зафиксируем полные порядки на каждом конечном множестве троек целых чисел

$$\{(s_j, t_j, m_j) \colon j = 1, \dots, k,\ 0 < m_j < p,\ s_j \geqslant 0,\ t_j > 0\}.$$

Мономы $(P_{t_j}^{s_j})^{m_j}$ будем перемножать именно в этом порядке. В [9] было показано, что множество $\bar{B}_P$ таких произведений образует базис $\bar{A}_p$. В [2] мы дали другое доказательство этого факта, установив треугольность $\bar{B}_P$ по отношению к базису Милнора подалгебры $\bar{A}_p$. Заметим, что имеется бесконечное число $\bar{B}_P$-базисов, поскольку порядки сомножителей $(P_{t_j}^{s_j})^{m_j}$ в P_t^s-мономе можно выбирать бесконечным числом способов.

Стандартный способ расширить $\bar{B}_P$ до базиса A_p состоит в том, чтобы рассмотреть набор элементов

$$B_P = \{Q_{a_1} \dots Q_{a_m} \theta \mid m \geqslant 0,\ a_1 < \dots < a_m,\ \theta \in \bar{B}_P\}.$$

Тем самым вопрос о треугольности базиса B_P по отношению к базису Милнора B_{Mil} тривиален: соответствующая матрица перехода имеет блочную структуру, причём блоки находятся во взаимно-однозначном соответствии с последовательностями $Q_{a_1} \dots Q_{a_m}$, где $m \geqslant 0$, $a_1 < \dots < a_m$. Каждый такой блок совпадает с матрицей перехода между $\bar{B}_P$ и базисом Милнора подалгебры $\bar{A}_p$.

Закончим этот раздел замечанием, что порядок на множестве милноровских элементов подалгебры $\bar{A}_p$, использованный в [2] для доказательства треугольности матрицы перехода к $\bar{B}_P$, был один и тот же для всех базисов вида $\bar{B}_P$. Из этого наблюдения следует, что любые два P_s^t-базиса алгебры A_p треугольны по отношению друг к другу (равно как и любые два P_s^t-базиса подалгебры $\bar{A}_p$).

Работа выполнена при поддержке программы «Ведущие научные школы» (грант НШ-6399.2018.1, соглашение № 075-02-2018-867) и Российского фонда фундаментальных исследований (грант 18-01-00398-а).

Литература

[1] Емельянов Д. Ю. О базисах Вуда алгебры Стинрода $\mathrm{mod}\, p$ // Фундамент. и прикл. матем. — 2015. — Т. 20, № 3. — P. 83—90.

[2] Емельянов Д. Ю., Попеленский Ф. Ю. О заменах базисов в алгебре Стинрода $\mathrm{mod}\, p$ // Матем. сб. — 2017. — Т. 208, № 4. — P. 3—16.

[3] Arnon D. Monomial bases in the Steenrod algebra // J. Pure Appl. Algebra. — 1994. — Vol. 96. — P. 215—223.

[4] Emelyanov D. Yu., Popelensky Th. Yu. On monomial bases in the $\mathrm{mod}\, p$ Steenrod algebra // J. Fixed Point Theory Appl. — 2015. — Vol. 17, no. 2. — P. 341—353.

[5] Emelyanov D. Yu., Popelensky Th. Yu. On monomial bases in the $\mathrm{mod}\, p$ Steenrod algebra, β included // J. Pure Appl. Algebra. — 2019. — Vol. 223, no. 8. — P. 3386—4301.

[6] Karaça I., Tanai B. The change of bases in the $\mathrm{mod}\, p$ Steenrod algebra: Preprint.

[7] Milnor J. The Steenrod algebra and its dual // Ann. Math. — 1958. — Vol. 67, no. 1 — P. 150—171.

[8] Monks K. G. Change of basis, monomial relations, and P_s^t bases for the Steenrod algebra // J. Pure Appl. Algebra. — 1998 — Vol. 125, no. 1 — P. 235—260.

[9] Palmieri J., Zhang J. J. Commutators in the Steenrod algebra // New York J. Math. — 2013 — Vol. 19 — P. 23—37.

[10] Wall C. T. C. Generators and relations for the Steenrod algebra // Ann. Math. — 1960. — Vol. 72, no. 2. — P. 429—444.