# О базисах Вуда алгебры Стинрода $\mathrm{mod}\, p$

**Д. Ю. ЕМЕЛЬЯНОВ**
*Московский государственный университет им. М. В. Ломоносова*
e-mail: emelyanov.d.yu@gmail.com

УДК 515.14

**Ключевые слова:** алгебра Стинрода, мономиальный базис, базис Вуда.

**Аннотация**

Цель данной работы — предложить обобщение результатов Р. М. В. Вуда о базисах в алгебре Стинрода $\mathrm{mod}\, 2$ для алгебры Стинрода $\mathrm{mod}\, p$.

**Abstract**

*D. Yu. Emelyanov, On Wood basis for the* $\mathrm{mod}\, p$ *Steenrod algebra*, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 3, pp. 83—90.

The purpose of this paper is to generalize results of R. M. W. Wood on monomial bases for the $\mathrm{mod}\, 2$ Steenrod algebra to the $\mathrm{mod}\, p$ Steenrod algebra, $p > 2$.

*Посвящается Анатолию Тимофеевичу Фоменко по случаю его семидесятилетия*

## 1. Введение и основное утверждение

Рассмотрим алгебру $\bar{\mathcal{A}}_p$, $p \geqslant 3$, порождённую степенями Понтрягина $P^j$, где $j \geqslant 0$, $\deg(P^j) = 2(p-1)j$, и соотношениями $P^0 = 1$,

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

Алгебра $\bar{\mathcal{A}}_p$ — это подалгебра элементов чётной степени в алгебре Стинрода $\mathrm{mod}\, p$. В работе Р. М. В. Вуда [3] для $\mathcal{A}_2$ (алгебры Стинрода $\mathrm{mod}\, 2$) были построены так называемые $WdY$-базис и $WdZ$-базис. В данной статье приводится обобщение $W\,dY$-базиса на случай $\bar{\mathcal{A}}_p$, $p \geqslant 3$.

Нам потребуется понятие лексикографического порядка.

**Определение 1.** *Левый лексикографический порядок* на 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 следующих условий:

*Фундаментальная и прикладная математика*, 2015, том 20, № 3, с. 83—90.

1) $I$ пусто, а $J$ непусто;
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.

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

**Определение 2.** 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 $I = \big((k_0,n_0),\dots,(k_r,n_r)\big)$ удовлетворяет следующим условиям:

1) $(k_r,n_r) \leqslant_L \dots \leqslant_L (k_1,n_1) \leqslant_L (k_0,n_0)$;
2) если в последовательности $I$ есть подпоследовательность одинаковых пар,

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

то $s < p$ для любой такой подпоследовательности.

Основной результат данной работы составляет следующее утверждение.

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

Обобщение $WdZ$-базиса на случай алгебры $\bar{\mathcal{A}}_p$, $p > 2$, описывается следующим образом.

**Определение 3.** 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 $I = \big((n_0,k_0),\dots,(n_r,k_r)\big)$ удовлетворяет следующим условиям:

1) $(n_r,k_r) \leqslant_L \dots \leqslant_L (n_1,k_1) \leqslant_L (n_0,k_0)$;
2) если в последовательности $I$ есть подпоследовательность одинаковых пар,

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

то $s < p$ для любой такой подпоследовательности.

**Теорема 2.** *Множество $WZ$-мономов образует базис в $\bar{\mathcal{A}}_p$.*

Это утверждение может быть получено методами настоящей работы, однако имеется более изящное доказательство в рамках другого подхода, оно будет опубликовано в другой работе.

## 2. Вспомогательные утверждения

Пусть $a$ — целое неотрицательное число. Будем записывать его $p$-адическое представление в виде

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

Для дальнейшего нам понадобится следующее хорошо известное (см., например, [2]) утверждение.

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

$$\binom{a}{b} \equiv \prod_i \binom{\alpha_i(a)}{\alpha_i(b)} \pmod{p}. \tag{1}$$

Доказательство теоремы 1 опирается на следующие три леммы.

**Лемма 2.** *Пусть $m < n$ и*

$$a = p^m + p^{m-1} + \ldots + 1, \quad b = p^n + p^{n-1} + \ldots + 1.$$

*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

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

Пусть $\alpha_i$ — это разряды $p$-адического представления $c$, т. е.

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

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 $j \geqslant k+1$;
2) каждый разряд $\alpha_i$ равен 0 или 1 и $\alpha_{j+1} = 1$, $\alpha_j = 0$ для некоторого $j \geqslant 0$.

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

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

$$0 \quad p-1 \quad \ldots \quad p-1 \quad p-\alpha_k+\varepsilon,$$

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

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

Так как $\gamma < p^{j-1}$, то верна оценка $p^{j-1} + (p-1)\gamma < p^j$. Откуда получим, что $\alpha_j\big((p-1)(b-c)\big) = p-2$. Очевидно, вычитание единицы никак не повлияет на значение в разряде $j$. В итоге $\alpha_j\big((p-1)(b-c)-1\big) = p-2$ 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 убедиться, что $\beta \geqslant 1$. 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, что $\alpha_{k+1}\big((p-1)(\beta p^k+\gamma)\big) = \beta - 1$, 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

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

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

Теперь рассмотрим случай, когда

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

Покажем, что на самом деле имеет место строгое неравенство. Так как $\alpha_{k-1}(\gamma) \geqslant \beta > 0$, получаем, что $\gamma > 0$. 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 следует, что

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

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

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

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

$$\alpha_k\big((p-1)\gamma - \beta p^k\big) \leqslant \alpha_{k-1}(\gamma) - \beta$$

и

$$\alpha_k\big((p-1)(b-c)-1\big) = \alpha_k\big((p-1)\gamma - \beta p^k - 1\big) = \alpha_k\big((p-1)\gamma - \beta p^k\big) \leqslant \alpha_{k-1}(\gamma) - \beta.$$

Как и ранее,

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

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

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

откуда по лемме 1 выводим, что 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 $j \geqslant 0$. Получаем, что $\alpha_{j+1}(b-c) = 0$. Пусть $\gamma$ — остаток от деления $b-c$ на $p^{j+1}$. Так как

$$\gamma \leqslant p^j + p^{j-1} + \ldots + p + 1 = \frac{p^{j+1}-1}{p-1},$$

то $(p-1)\gamma \leqslant p^{j+1}-1$. Получаем, что $\alpha_{j+1}\big((p-1)(b-c)\big)=0$. Из условия $\alpha_j=0$ следует, что $\gamma>0$, тогда $\alpha_{j+1}\big((p-1)(b-c)-1\big)=\alpha_{j+1}\big((p-1)(b-c)\big)=0$. По доказанному выше $p$-адическое разложение $c$ состоит из 0 и 1. Из условия $\alpha_j=0$ получаем, что $\alpha_j(b-c)=1$ 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*

а) *$P^a$ можно представить в виде*

$$P^a=\sum_i M_i, \qquad (*)$$

*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 $k$;*

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

**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

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

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

Рассмотрим соотношение Адема

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

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 $\alpha_0(a)\geqslant 1$, получаем, что $\alpha_0(a-b)<p-1$, откуда следует, что $c_0\neq 0$. 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 также будем доказывать 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 утверждению а) леммы 3 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, т. е. моном $M$ может быть представлен в виде $M=\tilde{M}m$ при $m=P^aP^b\tilde{m}$, 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, что $m=P^1$, и утверждение леммы тривиально. Пусть утверждение верно для всех мономов $M'$, таких что $|m'|<|m|$, где $m'$ — минимальный правый подмоном $M'$. Пусть произведение $P^aP^b$ является допустимым. Легко проверить, что произведение $P^{pb}P^{a-(p-1)b}$ недопустимо. Запишем соотношение

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

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 $P^aP^b$ с помощью этого соотношения. Произведение $P^{pb}P^{a-(p-1)b}$, стоящее в мономе $M = \tilde{M}P^aP^b\tilde{m}$, 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 следует, что 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 $p \nmid a+b-i$, к степени $P^{a+b-i}$ применимо утверждение а) леммы 3:

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

Произведение $P^aP^b$ допустимо, т. е. $a \geqslant pb$. По предположению ни для какого $l$ не выполняется

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

То же верно для суммы $a+b-i$, так как $i \leqslant b-1$. Далее, $a+b-i \geqslant a+1$, и по утверждению б) 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. □

## 3. Доказательство основного утверждения

По [1, предложение 2.5] размерность градуировки 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 $P^{I/p} = P^{i_0/p}P^{i_1/p}\cdots P^{i_r/p}$. По предположению индукции разложим получившийся моном по $Y$-базису:

$$P^{I/p} = \sum_i \lambda_i P^{J_i}.$$

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 $P^J$. Найдём разложение $P^I$ и $P^J$ по базису допустимых мономов $(P^I)_{\mathrm{Adm}}$ и $(P^J)_{\mathrm{Adm}}$. Если разность получившихся разложений $(P^I)_{\mathrm{Adm}} - (P^J)_{\mathrm{Adm}}$ 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 следующим образом:

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

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 $(n,k)$, т. е. $\bar{Z}^{K_{\alpha\beta}} = \bar{Z}^{\tilde{K}_{\alpha\beta}}\bar{Z}_k^n$. 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 и 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 аналогично [1, лемма 2.11] рассуждение может быть сведено к совокупности мономов, меньших в смысле левого лексикографического порядка.

# Литература

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

[2] Steenrod N. E., Epstein D. B. A. Cohomology Operations. — Princeton: Princeton Univ. Press, 1962.

[3] Wood R. M. W. A note on bases and relations in the Steenrod algebra // Bull. London Math. Soc. — 1995. — Vol. 27, no. 4. — P. 380—386.