Записки научных
семинаров ПОМИ
Том 349, 2007 г.

А. Л. Смирнов

ОБОБЩЕННЫЕ ПОДКОЛЬЦА АРИФМЕТИЧЕСКИХ КОЛЕЦ

Введение

В работе Н. Дурова [1] построена теория обобщенных колец и модулей над ними. Хотя во многих отношениях эта теория напоминает теорию классических колец и модулей, имеется, однако, много эффектов, неожиданных с классической точки зрения. Например, тензорное произведение конечных обобщенных колец может быть бесконечным, а конечное кольцо может содержать бесконечно много подколец. Для осознания подобных эффектов и выработки интуиции желательно расширить набор конкретных примеров. В этом и состоит основная цель данной заметки.

Если говорить более конкретно, то в работе получена классификация обобщенных подколец $\mathbb{F}_q$, изучены обобщенные подкольца $\mathbb{Z}/p^2$, причем при $p = 2$ получена полная классификация. Кроме того, приведены примеры обобщенных полей типа $\mathbb{F}_\infty$ и вычисления колец $\mathbb{F}_\infty^{\otimes n}$. Помимо этого, описаны коконечные обобщенные подкольца $\mathbb{Z}_p$ и некоторые примеры подколец $\mathbb{Z}_\infty$. Среди прочего, отметим, что в 4.3.2 выдвинуто любопытное предположение (конгруэнц-гипотеза) о коконечных подкольцах $\mathbb{Z}$ и приведены свидетельства в его пользу.

Автор благодарит Н. Дурова за возможность ознакомиться с работой [1] до ее публикации, а также за многочисленные неформальные разъяснения, комментарии и обсуждения.

1. Соглашения и обозначения

В работе, по умолчанию, используются следующие соглашения и обозначения.

1. Обобщенные кольца [1, 5.1.6] называются просто кольцами, а обычные кольца называются классическими. Для кольца

Работа выполнена при поддержке РФФИ (грант 06-01-00471) и INTAS (грант 05-1000008-8118).

R элементы множества $R(n)$ называются n-арными операциями или n-операциями.

2. Если R – подкольцо классического кольца и $(0, \dots, 0) \in R(n)$ для некоторого n, то $0 \in R(1)$. Каждое кольцо с 1-нулем (далее просто кольцо с нулем) имеет две версии, отличающиеся только в $R(0)$ – в одной из них (основной) $R(0) = \{0\}$, а в другой $R(0) = \emptyset$. В классификации для колец с нулем указана только основная версия.
3. Если R – подкольцо классического кольца A, то операция $(a_1, \dots, a_n) \in R(n) \subset A^n$ отождествляется с выражением $a_1x_1 + \dots + a_nx_n$, где x_i – свободные переменные.
4. Для мультипликативного подмоноида $S \subset (A, \times)$ пусть S_A – обобщенное подкольцо A, порожденное $S \subset A(1)$ и дополнительно $0 \in A(0)$ при $0 \in S$. В частности, $\{1\}_A \simeq \mathbb{F}_\emptyset$, а $\{0,1\}_A \simeq \mathbb{F}_1$.
5. Для кольца R операция из $f \in R(n)$ невырождена, если она не может быть индуцирована из $R(m)$ для $m < n$ с помощью какого-либо отображения $\mathbf{m} \to \mathbf{n}$ (здесь и ниже $\mathbf{n} = \{1, \dots, n\}$). Иными словами, f невырождена, если истинная арность $\operatorname{tr.ar} f$ [2, 3.1] равна n. Если R – подкольцо классического кольца A, то операция $(a_1, \dots, a_n) \in R(n) \subset A^n$ невырождена тогда и только тогда, когда $a_i \neq 0$ для каждого i.

2. Подкольца конечных классических колец

В этом разделе обсуждаются понятие конечности, а также классификация подколец $\mathbb{F}_q$ и $\mathbb{Z}/p^2$.

2.1. Конечные расширения

Пусть B – некоторая A-алгебра, то есть задан гомоморфизм обобщенных колец $\rho : A \to B$. Понятие конечности B над A определяется так, чтобы в классическом случае получилось классическое понятие.

2.1.1. Определение. *A-алгебра B называется конечной, если функтор ограничения скаляров $\rho_* : B\text{-Mod} \to A\text{-Mod}$ переводит конечнопорожденные модули в конечнопорожденные.*

В обобщенном случае функтор ограничения скаляров ρ_*, вообще говоря, не точен справа [1, 0.4.27]. Тем не менее, ρ_* переводит сюръекции (строгие эпиморфизмы) в сюръекции, и, таким образом, конечность B над A равносильна тому, что A-модуль $B(n)$ конечнопорожден для всякого $n \geq 0$.

Например, если кольцо R таково, что множество $R(n)$ конечно для каждого n, то R – конечно над $\mathbb{F}_\emptyset$ и $\mathbb{F}_1$. В качестве еще одного примера для $N \in \mathbb{N}_{>0}$ рассмотрим подкольцо $R_N \subset \mathbb{Z}$, где

$$R_N(n) = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n | \exists i \quad a_i = 0, 1 \operatorname{mod} N, \\ a_j = 0 \operatorname{mod} N \quad \text{для} \quad j \neq i\}.$$

Тогда $\mathbb{Z}$ конечно над R_N. Это вытекает из следующего утверждения.

2.1.2. Предложение. *Пусть A – классическое кольцо, I – главный идеал в A, а R – обобщенное подкольцо A, определенное как прообраз $\mathbb{F}_1$ при проекции $A \to A/I$. Тогда конечность A над R равносильна конечности множества A/I.*

Доказательство. Действительно, система образующих $A(1) = A$ над R индуцирует при проекции систему образующих A/I над $\mathbb{F}_1$, то есть конечность A над R влечет конечность множества A/I. Наоборот, пусть A/I – конечное множество. Тогда можно найти набор элементов $x_1, \ldots, x_m$ из A^n, такой, что

1. x_i порождают A^n как A-модуль;
2. $x_i \operatorname{mod} I$ порождают $(A/I)^n$ над $\mathbb{F}_1$.

Для построения достаточно выбрать множество Y, состоящее из $y_i \in A$, таких, что $y_i \operatorname{mod} I$ порождают A/I над $\mathbb{F}_1$. Тогда набор Y^n удовлетворяет второму из вышеуказанных свойств. Чтобы удовлетворить и первому, достаточно добавить к Y^n систему образующих A^n как A-модуля.

Покажем, что всякий такой набор порождает A^n над R. Действительно, пусть $a \in A^n$. Так как x_i порождают $(A/I)^n$ над $\mathbb{F}_1$, то $a = f(x_1, \ldots, x_m) \operatorname{mod} I$, где $f \in R(m)$. Таким образом, $a = f(x_1, \ldots, x_m) + b$, где $b \in I^n$, а так как I – главный идеал, то $a = f(x_1, \ldots, x_m) + \pi c$, где $\pi \in I$, а $c \in A^n$. Так как x_j порождают A^n как A-модуль, то $c = \sum w_i x_i$ и $a = f(x_1, \ldots, x_m) + \pi \sum w_i x_i$. Операция в правой части очевидно лежит в $R(m)$. □

2.1.3. Конечность и замена базы. В классическом случае свойство конечности инвариантно относительно замены базы: если B

– конечная A-алгебра, а C – произвольная A-алгебра, то $C \otimes_A B$ – конечная C-алгебра.

Оказывается, что в обобщенном случае это не так. В качестве примера рассмотрим кольцо $B \subset \mathbb{Z}/4$, порожденное над $\mathbb{F}_1$ операцией $2x+2y \in \mathbb{Z}/4(2)$. При этом $B(n)$ состоит из таких наборов $b = (b_1, \dots, b_n) \in \mathbb{Z}/4(n)$, что либо $b = 0$, либо один из b_i лежит в множестве $\{1 \bmod 4, 2 \bmod 4\}$, а все остальные равны нулю, либо два из b_i равны $2 \bmod 4$, а остальные равны нулю.

Имеется следующее представление B в виде образующих и соотношений:

$$B = \mathbb{F}_1[*, \operatorname{ar} * = 2 | x * x = 0, x * y = y * x, x * (y * z) = x * 0]. \qquad (1)$$

Отметим, что из указанных соотношений вытекает автокоммутативность $*$, так как $(x * y) * (z * t) = (x * y) * 0 = 0 * 0 = 0$.

Чтобы проверить (1), временно обозначим R правую часть этой формулы и рассмотрим гомоморфизм $\rho : R \to \mathbb{Z}/4$, $* \mapsto 2x+2y$. Легко увидеть, что операция $2x+2y$ удовлетворяет всем соотношениям (1) и ρ определен корректно. Несложно проверить, что ρ – строгий эпиморфизм на B. Для проверки инъективности ρ достаточно проверить неравенство $\operatorname{card} R(n) \leq \operatorname{card} B(n) = 1+n+n+\binom{n}{2}$. В свободном R-модуле M, порожденном $x_1, \dots, x_n$, рассмотрим подмножество

$$N = \{0\} \cup \{x_1, \dots, x_n\} \cup \{0 * x_1, \dots, 0 * x_n\} \cup \{x_i * x_j\}_{i<j}.$$

Легко увидеть, что N является R-подмодулем M, проверив замкнутость N относительно $*$. Таким образом, $N = M$ в силу того, что M порожден $\{x_i\}$. Следовательно, $\operatorname{card} M = \operatorname{card} N \leq 1+2n+\binom{n}{2}$, что завершает проверку обратимости ρ на B.

Пусть $C = B \otimes_{\mathbb{F}_1} B$. Рассмотрим в $C(1)$ элементы x, $x \vee 0$, $(x \vee 0) \wedge 0$, $((x \vee 0) \wedge 0) \vee 0, \dots$, где $\vee = * \otimes 1$, $\wedge = 1 \otimes *$, а $x = 1 \otimes 1$ – свободная образующая $C(1)$.

С. Пименов проверил, что все эти элементы различны и, таким образом, $C(1)$ бесконечно. В частности, это означает, что C не является конечной B-алгеброй относительно гомоморфизма $B \otimes_{\mathbb{F}_1} [\mathbb{F}_1 \to B] : B \to C$, то есть относительно замены базы гомоморфизма $\mathbb{F}_1 \to B$. Этот гомоморфизм конечен, так как $B \subset \mathbb{Z}/4$.

Неинвариантность конечности относительно замены базы наводит на мысль рассмотреть свойство универсальной конечности. По определению, A-алгебра B универсально конечна над A, если $\widetilde{A} \otimes_A B$ конечна над $\widetilde{A}$ для всякой A-алгебры $\widetilde{A}$.

Как показывает следующий пример С. Пименова, это понятие также обладает неожиданными свойствами: $\mathbb{F}_2$ не является универсально конечным над $\mathbb{F}_1$. Чтобы увидеть это, достаточно взять $\widetilde{A} = \mathbb{F}_1[t]$, где t – свободная унарная переменная. Тогда $\widetilde{A} \otimes_{\mathbb{F}_1} \mathbb{F}_2 = \mathbb{F}_2[t]$ не конечно над $\widetilde{A} = \mathbb{F}_1[t]$.

Отметим два частных случая, когда конечность все же сохраняется при замене базы.

2.1.4. Теорема. *Пусть имеются гомоморфизмы обобщенных колец $\rho : A \to B$ и $\iota : A \to \widetilde{A}$, причем ρ конечен. Тогда гомоморфизм $\widetilde{\rho} : \widetilde{A} \to \widetilde{B} = \widetilde{A} \otimes_A B$ конечен, если либо $\widetilde{A}$ – плоская A-алгебра, либо B унарно над A.*

Доказательство. Положим $\widetilde{\iota} = B \otimes_A \iota$ и рассмотрим коммутативную диаграмму

$$\begin{array}{ccc} \widetilde{B} & \xleftarrow{\ \widetilde{\iota}\ } & B \\ {\scriptstyle\widetilde{\rho}}\uparrow & & \uparrow{\scriptstyle\rho} \\ \widetilde{A} & \xleftarrow{\ \iota\ } & A \end{array}$$

Тогда $\widetilde{\rho}_* \widetilde{B}(n) \simeq \widetilde{\rho}_* \widetilde{\iota}^* B(n) \simeq \iota^* \rho_* B(n)$, где первое отождествление – следствие того, что функтор расширения скаляров $\widetilde{\iota}^*$, будучи точным справа, переводит прямые суммы в прямые суммы и, таким образом, $B(n)$ в $\widetilde{B}(n)$. Второе отождествление – следствие теоремы о замене базы [1, теорема 5.4.2]. Из этих отождествлений вытекает конечнопорожденность $\widetilde{\rho}_* \widetilde{B}(n)$, поскольку $\rho_* B(n)$ конечнопорожден по условию, а ι^*, будучи точным справа, сохраняет конечнопорожденность. □

2.2. Производящие функции

Пусть обобщенное кольцо R конечно над $\mathbb{F}_\emptyset$. Невырожденная операция $\alpha \in R(d)$ индуцирует с помощью инъекций $n(n-1)\dots(n-d+1)$ вырожденных операций в $R(n)$ при $n \geq d$. Естественно не различать между собой эти операции при подсчетах. Поэтому положим

$$P_R^*(t) = |R^*(0)| + |R^*(1)|\frac{t}{1!} + |R^*(2)|\frac{t^2}{2!} + \dots,$$

где $R^*(d)$ – множество невырожденных операций в $R(d)$.

Несмотря на естественность такого определения, оказывается, что более непосредственное определение

$$P(R,t) = P_R(t) = |R(0)| + |R(1)|\frac{t}{1!} + |R(2)|\frac{t^2}{2!} + \dots$$

приводит практически к "тому же самому" результату.

2.2.1. Теорема. $P_R(t) = P^*_R(t) \cdot e^t$.

Доказательство. Коэффициент при t^n в правой части имеет вид

$$\frac{|R^*(0)|}{0!n!} + \frac{|R^*(1)|}{1!(n-1)!} + \dots + \frac{|R^*(n)|}{n!0!} = \frac{1}{n!}\sum \binom{n}{d}|R(d)^*|.$$

Сумма справа равна $|R(n)|$, поскольку $R(n)$ распадается на классы операций с носителями $S \subset \{1,\dots,n\}$ (носители определены в [2, 3.1]), а операции с носителем S отождествляются с $R^*(|S|)$. $\square$

Например, $P(R,t) = e^{|R|t}$ для классического R, $P(\mathbb{F}_\emptyset, t) = te^t$, $P(\mathbb{F}_1, t) = (1+t)e^t$, $P(\mathbb{F}_{1^n}, t) = (1+nt)e^t$, $P(\mathbb{F}_\infty, t) = e^{3t}$.

2.3. Подкольца $\mathbb{F}_q$

Пусть R – подкольцо классического кольца A.

2.3.1. Определение. *Для операции* $(a_1,\dots,a_n) \in A(n)$ *пусть*

$$\alpha(a_1,\dots,a_n) \text{ – \textit{число таких} } i, \quad \text{\textit{что} } a_i \in A^*.$$

2.3.2. Лемма. *Если* A *конечно и имеется операция* $(a_1,\dots,a_n) \in R(n)$ *с* $\alpha \geq 2$, *то в* $R(3)$ *имеется операция вида* $x+y+cz$, *где* $c \in A$.

Доказательство. Во-первых, в R имеются операции со сколь угодно большим α. Действительно, инвариант α операции

$$a_1(a_1x_1+\dots+a_nx_n)+a_2(a_1y_1+\dots+a_ny_n)+\dots+a_n(a_1w_1+\dots+a_nw_n)$$

равен квадрату α операции $(a_1,\dots,a_n)$. Во-вторых,

$$ax+ay+bz \in R(3), \quad \text{для некоторых} \quad a \in A^*, b \in A. \tag{2}$$

Ввиду вышесказанного, в R имеется операция с $\alpha \geq \operatorname{card} A^*$. Найдется ее обратимая компонента, повторяющаяся дважды, и можно считать, что операция имеет вид $(a,a,b_1,\dots,b_m)$, где $a \in A^*$. Операция $ax+ay+b_1z+\dots+b_mz$ имеет искомый вид.

Покажем теперь, что для всякого $n \geq 1$ в $R(3)$ найдется операция вида

$$a^n x + a^n y + cz \in R(3), \quad \text{для некоторых} \quad a \in A^*, c \in A. \qquad (3)$$

Возьмем a, b из (2). Если $a^n x + a^n y + cz \in R(3)$ для некоторого $n \geq 1$, то и

$$a(a^n x + a^n y + cz) + az + bz = a^{n+1}x + a^{n+1}y + (ac + a + b)z \in R(3).$$

Для завершения доказательства леммы достаточно в (3) взять $n = \operatorname{card} A^*$. □

2.3.3. Лемма. *Пусть A – конечно, а R – такое обобщенное подкольцо Aff_A, что $x+y-z \in R(3)$. Тогда $E = \{a \in A | (a, 1-a) \in R(2)\}$ – подкольцо A, а $R = \mathrm{Aff}_E$.*

Доказательство. Ясно, что $0, 1 \in E$. Пусть $a, b \in E$. Используя операцию $x + y - z$, видим, что

$$(ax + (1-a)y) + (bx + (1-b)y) - y = (a+b)x + (1-a-b)y \in R(2)$$

и

$$a(bx + (1-b)y) + (1-a)y = abx + (1-ab)y \in R(2).$$

Следовательно, $a + b \in E$, $ab \in E$, E – подполукольцо и, следовательно, подкольцо A.

Проверим, что $R(n) \subset \mathrm{Aff}_E(n)$. Пусть $(a_1, \ldots, a_n) \in R(n)$. Тогда $(a_1, a_2 + \cdots + a_n) \in R(2)$ и, по определению, $a_1 \in E$. Аналогично, $a_i \in E$.

Проверим, что $R \supset \mathrm{Aff}_E$. Пусть

$$(a_1, \ldots, a_n, a_{n+1}) \in E(n+1), \quad a_1 + \cdots + a_{n+1} = 1.$$

По индукционному предположению, $(a_1, \ldots, a_{n-1}, a_n + a_{n+1}) \in R(n)$. Используя операцию из $x + y - z$, видим, что

$$(a_1x_1 + \cdots + a_{n-1}x_{n-1} + (a_n + a_{n+1})x_{n+1}) + (a_nx_n + (1-a_n)x_{n+1}) - x_{n+1} =$$

$$= a_1x_1 + \cdots + a_{n+1}x_{n+1} \in R(n+1).$$

□

2.3.4. Теорема. *Всякое обобщенное подкольцо R классического конечного поля F имеет вид:* (1) *обычное подполе;* (2) S_F, *где S – подмоноид $(F, \times)$;* (3) Aff_E, *где E – обычное подполе.*

Доказательство. Если всякая n-операция при $n \geq 2$ вырождена, то $R = S_F$, где $S = R(1)$. Далее считаем, что имеется невырожденная операция арности ≥ 2. В этом случае по лемме 2.3.2 для некоторого $c \in F$

$$x + y + cz \in R(3), \tag{4}$$

и, более того, для всякого $n \geq 1$ в $R(2n+1)$ найдется операция вида

$$x_0 + x_1 + \cdots + x_n + cy_1 + \cdots + cy_n, \tag{5}$$

строящаяся из (4) индуктивно, а именно это: $(x_0 + x_1 + \cdots + x_n + cy_1 + \cdots + cy_n) + x_{n+1} + cy_{n+1}$.

Покажем теперь, что

$$\text{либо} \quad R \subset \mathrm{Aff}_F, \quad \text{либо} \quad R \text{ – кольцо с нулем.} \tag{6}$$

Условие $R \subset \mathrm{Aff}_F$ равносильно тому, что $R(1) = \{1\}$. Действительно, если $R(1) = \{1\}$, то для $(a_1, \ldots, a_n) \in R(n)$ операция $(a_1 + \cdots + a_n) \in R(1)$ совпадает с единственным элементом $1 \in R(1)$ и, следовательно, $R \subset \mathrm{Aff}_F$. Обратное утверждение очевидно.

Итак, предположим, что $R(1) \neq \{1\}$, и проверим в несколько шагов, что $0 \in R(1)$. Во-первых, для некоторого $n \geq 1$, взаимно простого с $\mathrm{char}(F)$,

$$x_0 + x_1 + \cdots + x_n \in R(n+1). \tag{7}$$

Пусть $u \in R(1)$, $u \neq 1$, $p = \mathrm{char}(F)$. Рассмотрим $f \in \mathbb{F}_p[t]$, для которого $f(u) = 0$, а $f(1) \neq 0$. Запишем f в виде $f = t^{d_1} + \cdots + t^{d_n}$. Число слагаемых в таком представлении, то есть n, удовлетворяет (7). Действительно, $n = f(1) \pmod p$ взаимно просто с p. Кроме того, по (5) найдем операцию $x_0 + x_1 + \cdots + x_n + cy_1 + \cdots + cy_n \in R(2n+1)$ и получим из нее операцию $x_0 + x_1 + \cdots + x_n + cu^{d_1}y + \cdots + cu^{d_n}y = x_0 + x_1 + \cdots + x_n$.

Во-вторых, в случае $R(1) \neq \{1\}$ для некоторого $n \geq 1$, взаимно простого с p, в $R(2)$ имеется операция $x + ny$. Действительно, используя операцию $x_0 + x_1 + \cdots + x_n$ получим операцию $x + y + \cdots + y = x + ny \in R(2)$. Более того, в этом случае для всякого натурального m в $R(2)$ имеется операция $x + mny$ (индукция: $(x +$

$mny) + ny = x + (m+1)ny)$. Выберем натуральное m так, что $mn = -1 \bmod p$. Тогда операция $x + mny = x - y$ и $0 = x - x \in R(1)$. Таким образом, утверждение (6) доказано.

Если R – кольцо с нулем, то в R имеется операция $x + y$, так как по (4) в $R(3)$ можно найти операцию $x + y + cz$ и взять $z = 0$. Отсюда вытекает, что $E = R(1)$ – обычное подполе F, и R совпадает с обобщенным подкольцом, порожденным E.

Если же $R \subset \mathrm{Aff}_F$, то $x + y - z \in R(3)$, так как по (4) в $R(3)$ имеется операция $x + y + cz$, неизбежно $c = -1$, и доказательство завершается ссылкой на 2.3.3. $\square$

2.4. Подкольца $\mathbb{Z}/p^2$

Пусть $A = \mathbb{Z}/p^2$, где p – простое, $I = pA$, $F = A/I$, для $a \in A$ пусть $\overline{a} \in F$ – образ a при проекции $A \to F$, для $X \subset F$ пусть $\widetilde{X}$ – прообраз X при проекции $A \to F$. Кроме того, рассмотрим подкольцо $E \subset \mathbb{Z}/p^2$, для которого

$$E(n) = \{(a_1, \ldots, a_n) \in A^n \mid \text{либо все } a_i \in I, \\ \text{либо } \exists i: \quad a_j = 0 \text{ при } j \neq i\}. \quad (8)$$

2.4.1. Теорема. *Всякое обобщенное подкольцо $R \subset A$ имеет вид: (1) прообраз подкольца в поле F; (2) пересечение Aff_A с прообразом подкольца в поле F; (3) подкольцо в E.*

Доказательство. По теореме 2.3.4 имеются следующие возможности:

$$(1)\ \overline{R} = F; \quad (2)\ \overline{R} = \mathrm{Aff}_F; \quad (3)\ \overline{R} = S_F, \text{ где } S \text{ – подмоноид } (F, \times). \quad (9)$$

Проверим, что если $\overline{R} = F$, то $R = A$. Действительно, найдется $a \in R(1)$ с $\overline{a} = 0$. Поэтому $0 = a^2 \in R(1)$. Кроме того, в R найдется операция с $\alpha \geq 2$ и, следовательно (см. 2.3.2), найдется операция $x + y + cz$. Поэтому $x + y + c \cdot 0 = x + y \in R(2)$ и $R = A$.

Проверим, что

$$\text{если } \overline{R} = \mathrm{Aff}_F, \text{ то } R = \mathrm{Aff}_A \quad \text{или } R = \widetilde{\mathrm{Aff}_F}. \quad (10)$$

Во-первых, убедимся, что R заключено в рамки

$$\widetilde{\mathrm{Aff}_F} \supset R \supset \mathrm{Aff}_A\,. \quad (11)$$

Первое включение вытекает из того, что $\overline{R} = \mathrm{Aff}_F$. Для проверки второго включения отметим, что в R найдется операция с $\alpha \geq 2$ и, следовательно (см. 2.3.2), найдется операция $x+y+cz$. Поскольку $\overline{R} = \mathrm{Aff}_F$, то $c = -1 \bmod p$. При этом $(2+c)x = x + x + cx \in R(1)$ и $x+y-z = x+y+c(2+c)z \in R(3)$. Операция $x+y-z$ порождает $\mathrm{Aff}_{\mathbb{Z}}$ и Aff_A для всякого фактора $\mathbb{Z}$. Таким образом, (11) доказано.

Покажем, что

$$\text{строго внутри границ (11) никаких } R \text{ нет.} \tag{12}$$

Пусть в R имеется операция $(a_1, \dots, a_n)$, лежащая в $\widetilde{\mathrm{Aff}_F}$, но не в Aff_A. Тогда операция $a = a_1 + \dots + a_n \in R(1)$ также лежит в $\widetilde{\mathrm{Aff}_F}$, но не в Aff_A. Но группа $\widetilde{\mathrm{Aff}_F}(1) \simeq \mathbb{Z}/p$ порождена любым нетривиальным элементом и, следовательно, $\widetilde{\mathrm{Aff}_F}(1) = R(1)$.

Пусть $(a_1, \dots, a_n) \in \widetilde{\mathrm{Aff}_F}(n)$. С помощью перестановки можно считать, что $\overline{a}_1 \neq 0$. Рассмотрим операцию $(a_1', a_2, \dots, a_n) \in \mathrm{Aff}_A(n)$, где $a_1' = 1 - (a_2 + \dots + a_n)$. При этом $a_1 = a_1' \bmod p$ и, следовательно, $a_1 = \varepsilon a_1'$, где $\varepsilon \in \widetilde{\mathrm{Aff}_F}(1) = R(1)$. Поэтому $(a_1, \dots, a_n) = (\varepsilon a_1', a_2, \dots, a_n) \in R(n)$, и $\widetilde{\mathrm{Aff}_F}(n) = R(n)$, что доказывает (12) и (10).

Разберем теперь последний случай из (9), то есть считаем, что $\overline{R} = S_F$, где S – подмоноид $(F, \times)$. Тогда либо $R \subset E$ (и тогда теорема доказана), либо в R имеется операция $f = ax + v_1 y_1 + \dots + v_n y$, где $a \in A^*$, $v_i \in I$, $v_i \neq 0$, $n \geq 1$. В этом случае

$$R \supset \widetilde{S}_F \cap \mathrm{Aff}_A, \tag{13}$$

ввиду очевидного равенства $\widetilde{S}_F \cap \mathrm{Aff}_A = \widetilde{\mathbb{F}}_1 \cap \mathrm{Aff}_A$ и леммы 2.4.2.

Осталось показать, что $R = \widetilde{S}_F$ в предположении, что R больше $\widetilde{S}_F \cap \mathrm{Aff}_A$. Это предположение равносильно тому, что в $R(2)$ имеется операция вида

$$bx + wy, \text{ где } b \in A^*, w \in I, b + w \neq 1. \tag{14}$$

В самом деле, так как R больше $\widetilde{S}_F \cap \mathrm{Aff}_A$, то в R имеется операция вида $cx + w_1 y_1 + \dots + w_n y_n$, где $c \in A^*$, $n \geq 1$, $w_i \in I$ и $c + w_1 + \dots + w_n \neq 1$. Тем самым, в R имеется операция $cx + w_1 y + w_2 x \dots + w_n x$, имеющая требуемый вид.

Более того, предположение о том, что R больше $\widetilde{S}_F \cap \mathrm{Aff}_A$, равносильно тому, что в $R(1)$ имеется операция

$$ux, \quad \text{где } \overline{u} = 1, \text{ но } u \neq 1. \tag{15}$$

Действительно, операция из (14) индуцирует операцию $bx+wx \in R(1)$, имеющую требуемый вид при $\overline{b}=1$. Иначе по сюръективности $R(1) \to S_F(1)$ найдем $c \in R(1)$, так что $\overline{c}=\overline{b} \neq 1$. Тогда $(1+p)x - cpy \in R(2)$, так как $(1+p)x - py \in R(2)$ по (13), следовательно, $(1+p)x - pcy \in R(2)$ и $(1+p)x - pcx \in R(1)$. Эта операция имеет требуемый вид.

Равенство $R(0) = \widetilde{S}_F(0)$ очевидно, поскольку $R(0) \to S_F(0)$ – эпиморфизм. Проверим, что $R(1+n) = \widetilde{S}_F(1+n)$ при $n \geq 1$. Произвольная $(1+n)$-операция в $\widetilde{S}_F$ после подходящей перестановки имеет вид $ax + w_1y_1 + \cdots + w_ny_n$, где $\overline{a} \in S$, а $w_i \in I$.

Сначала рассмотрим случай, когда $\overline{a}=0$. В этом случае $0 \in R$, так как $0 \in S_F(0)$ (по соглашению в §1) и $0 \in R(0)$ (случай $n=0$ разобран выше). Кроме того, $ax + w_1y_1 + \cdots + w_ny_n + (1-b)z \in R(2+n)$, где $b = a + w_1 + \cdots + w_n$, так как $R \supset \widetilde{S}_F \cap \mathrm{Aff}_A$ (см. (13)). Подставляя $z=0$, получаем исходную операцию.

Если $\overline{a} \neq 0$, то операция $b^{-1}[ax + w_1y_1 + \cdots + w_ny_n]$ лежит в $\mathrm{Aff}_A \cap \widetilde{S}_F$ и значит в R ввиду (13). Осталось убедиться, что $b \in R(1)$. По сюръективности $R(1) \to S_F(1)$ найдется $c \in R(1)$, так что $\overline{c} = \overline{a} = \overline{b}$. Тогда $b = bc^{-1}c$ и достаточно проверить, что $bc^{-1} \in R(1)$. Для этого в свою очередь достаточно проверить, что все операции вида $(1-w)x$ лежат в $R(1)$ при $w \in I$. Это вытекает из наличия в $R(1)$ операции (15). □

2.4.2. Лемма. *Если обобщенное подкольцо $R \subset A$ содержит операцию $f = ax + v_1y_1 + \cdots + v_ny$, где $a \in A^*$, $v_i \in I$, $v_i \neq 0$, $n \geq 1$, то R содержит $\widetilde{\mathbb{F}}_1 \cap \mathrm{Aff}_A$.*

Доказательство. Сначала проверяется, что

$$(1-w)x + wy \in R(2) \text{ для всякого } w \in I. \tag{16}$$

Действительно, в R имеется операция вида $bx+vy$, где $b \in A^*$, $v \in I$, $v \neq 0$, например, операция $f(x, y_1, x, \ldots, x)$ такова. Более того, в R имеется операция $(1-t)x+ty$, где $t \in I$, $t \neq 0$. Действительно, можно взять операцию $bx + vy$ и умножить ее на $\lambda^{(p-1)p}$, где $\lambda = b + v \in R(1)$. Итерируя $(1-t)x + ty$, получим все операции вида $(1-it)x + ity$: $(1-t)((1-it)x + ity) + ty = (1-(i+1)t)x + (i+1)ty$.

Однако операции (16) порождают $\widetilde{\mathbb{F}}_1 \cap \mathrm{Aff}_A$. Действительно, $(n+1)$-операция этого кольца с помощью перестановки приводится к виду $(1 - w_1 - \cdots - w_n - w_{n+1})x + w_1y_1 + \cdots + w_ny_n + w_{n+1}y_{n+1}$, где $w_i \in I$. Такая операция получается итерациями (16): $(1-w_1-\cdots-w_n)((1-w_{n+1})x+w_{n+1}y_{n+1})+w_1y_1+\cdots+w_ny_n$. □

2.4.3. Подкольца E. Полное описание подколец E (см. (8)) выглядит любопытной и, возможно, трудной задачей. Ниже указан набор подколец E, полностью решающий задачу классификации при $p=2$. Для $p \geq 3$ приведены и другие примеры.

Рассмотрим в E подкольцо B, где

$$B(n) = \{a \in A(n) |\ \text{либо}\ a \in \mathbb{F}_\emptyset,\ \text{либо}\ a = 0 \bmod p\}.$$

Например, $x+py \notin B(2)$, а $px+py \in B(2)$. Таким образом, $|B(n)| = n+p^n$, а производящая функция $P_B(t) = te^t + e^{pt}$ представляет собой смесь двух экспонент.

Для $d \geq 1$ рассмотрим в B подкольцо B_d, порожденное всеми операциями вида $p(b_1x_1+b_2x_2+\cdots+b_nx_n)$ с $n \leq d$. Иными словами,

$$B_d(n) = \{a \in A(n) |\ \text{либо}\ a \in \mathbb{F}_\emptyset,\ \text{либо}\ a = 0 \bmod p\ \text{и}\ \operatorname{tr.ar} a \leq d\}.$$

Удобно также считать, что $B_{-1} = \mathbb{F}_\emptyset$, а $B_0 = \mathbb{F}_1$. Кольца B_d различны для различных d, а $P(B_d,t) = te^t + (1+\varphi(p)t+\varphi(p^2)t)^2/2!+\cdots+\varphi(p^d))t^d/d!)e^t$, где φ – функция Эйлера. Таким образом, в B и в $\mathbb{Z}/p^2$ имеется бесконечно много подколец.

Ниже (см. 2.4.5) будет показано, что кольца B_d составляют довольно плотную сеть среди подколец B. А именно, каждое собственное подкольцо $R \subset B$ может быть заключено в рамки $B_d \subset R \subset B_e$ для некоторых d и e. Чтобы указать эффективную границу для d нам потребуется следующее хотя и элементарное, но не вполне тривиальное утверждение.

2.4.4. Предложение. *Пусть $b_1,\ldots,b_{p-1} \in \mathbb{F}_p^*$. Тогда для всякого $c \in \mathbb{F}_p$ существует подмножество $U \subset \{1,\ldots,p-1\}$, такое, что $c = \sum b_i$, где i пробегает U, а пустая сумма считается равной нулю.*

Доказательство. Утверждение равносильно разрешимости уравнения

$$c - b_1x_1^{p-1} - \cdots - b_{p-1}x_{p-1}^{p-1} = 0. \tag{17}$$

Проверим существование решения, используя известный метод Шевалле [3, I,2.2]. А именно, рассмотрим полином $g = 1 - f^{p-1}$, где f – левая часть (17). Тогда $n = \sum g(x)$, где x пробегает $\mathbb{F}_p^{p-1}$, а n – число решений (17), рассмотренное по модулю p. Раскладывая g по мономам и суммируя каждый моном по отдельности, получаем $n = -(p-1)!b_1 \cdots b_{p-1} = b_1 \cdots b_{p-1}$. □

2.4.5. Теорема. *Пусть R – подкольцо B. Если в $R \cap pA$ имеется невырожденная операция арности $n \geq (p-1)d$, где $d \geq 1$, то $R \supset B_d$. В частности, если в R имеются невырожденные операции сколь угодно большой арности, то $R = B$.*

Доказательство. Во-первых, $0 \in R(0)$. По условию, в R найдется невырожденная операция вида $p(b_1x_1 + \cdots + b_nx_n)$, где $n \geq 1$. Тогда в $R(1)$ имеется операция $p(b_1x + \cdots + b_nx)$, а ее квадрат равен нулю.

Покажем, что $B_d \subset R$. По условию, найдется невырожденная операция $p(b_1x_1 + \cdots + b_mx_m)$, где $m = (p-1)d$. Достаточно показать, что все элементы вида $p(c_1z_1 + \cdots + c_dz_d)$ лежат в $R(d)$. Применяя предложение 2.4.4 к наборам $(b_1, \ldots, b_{p-1})$, $\ldots$, $(b_{m-p+1}, \ldots, b_m)$, найдем подмножества $U_1 \subset \{1, \ldots, p-1\}$, $\ldots$, $U_d \subset \{m-p+1, \ldots, m\}$, такие, что $c_i = \sum b_j$, $j \in U_i$. Тогда $p(c_1z_1 + \ldots c_dz_d)$ получается из операции $p(b_1x_1 + \cdots + b_mx_m)$ подстановкой $x_j = z_i$ для $j \in U_i$ и $x_j = 0$ для j, не лежащих ни в одном из U_i. □

Из теоремы 2.4.5 вытекает, в частности, что в B имеется только счетное число подколец.

2.4.6. Следствие. *Для $p = 2$ кольца $\mathbb{F}_\emptyset$, $\mathbb{F}_1$ и B_d исчерпывают список собственных подколец B, а всякое обобщенное подкольцо $R \subset \mathbb{Z}/4$ имеет вид:* (1) *прообраз подкольца $\mathbb{F}_2$;* (2) *пересечение Aff_A с прообразом подкольца $\mathbb{F}_2$;* (3) *B или B_d.*

Доказательство. Действительно, при $p = 2$ кольца E и B совпадают. В частности, если в R имеются невырожденные операции сколь угодно большой арности, то $R = B$ по 2.4.5. Если e – максимальное число, такое, что в R имеется невырожденная операция арности e, то $R \subset B_e$ по определению B_e и $R \supset B_e$ по 2.4.5. Таким образом, в этом случае $R = B_e$. □

В заключение при $p > 2$ приведем пример подкольца B, отличного от B_d. Рассмотрим в $\mathbb{Z}/p^2$ подкольцо R, порожденное $\mathbb{F}_1$ и операцией $p(x_1 + \cdots + x_a)$. Тогда

$$R(n) = \mathbb{F}_\emptyset(n) \cup \{(p\bar{b}_1, \ldots, p\bar{b}_n) | b_1 + \cdots + b_n \leq a\},$$

где b_i – неотрицательные целые числа, а $p\bar{b}_i = pb \bmod p^2$. Для $p \neq 2$ и $a > 1$ кольцо R не совпадает ни с одним из B_d.

3. Кольца, связанные с $\mathbb{F}_\infty$

В этом разделе приведены примеры обобщенных полей типа $\mathbb{F}_\infty$, а также некоторые вычисления для кольца $\mathbb{F}_\infty^{\otimes d}$.

3.1. Кольцо $\mathbb{F}_1[\vee]$

При описании колец, связанных с полями вычетов в архимедовых точках, приходится иметь дело с бинарной операцией $\vee$, удовлетворяющей соотношениям

$$x \vee x = x, x \vee y = y \vee x, (x \vee y) \vee z = x \vee (y \vee z). \tag{18}$$

Кроме того, интересующие нас кольца содержат константу, обозначаемую, как обычно, 0. Таким образом, основой рассмотрения должно быть кольцо $\mathbb{F}_1[\vee]$, полученное добавлением к $\mathbb{F}_1$ указанной выше операции $\vee$.

Для эффективной работы с $\mathbb{F}_1[\vee]$ помимо формального определения желательно иметь явную модель этого кольца. Ближайшая цель – получить такую модель.

3.1.1. Кольцо B. Поскольку свойства (18) операции $\vee$ подобны свойствам операции объединения множеств, то естественно искать подходящую модель в соответствующих терминах. Начнем с кольца B, где $B(X)$ – множество всех конечных подмножеств X, а $B(f)$ переводит подмножество в его образ при f. Структура монады на B задана следующим образом $e : \mathrm{Id}(X) \to B(X)$, $x \mapsto \{x\}$, и $m : B(B(X)) \to B(X)$, $\mathcal{U} \mapsto \bigcup\limits_{U \in \mathcal{U}} U$. Операцию, соответствующую подмножеству $\{x, \dots, z\} \subset X$, обозначаем $x \vee \dots \vee z$.

Таким образом, B – коммутативное кольцо с нулем, однако ноль кольца B обладает следующим свойством: $x \vee 0 = x$. Для описания колец, связанных с полями вычетов в архимедовых точках, такой ноль не подходит. Иными словами, $0 \in B$ – не тот ноль, который нам нужен. Избавимся от него с помощью кольца B^0.

3.1.2. Кольцо B^0 и модули над ним. Пусть $B^0(X)$ – множество всех непустых конечных подмножеств X. Очевидно, что B^0 – подкольцо (без нуля) кольца B и

$$B^0 = \mathbb{F}_\emptyset[\vee], \tag{19}$$

где $\vee$ – бинарная операция, удовлетворяющая соотношениям (18).

Множества с идемпотентной, коммутативной и ассоциативной операцией называются полурешетками [4, I.5]. Структура полурешетки определяет [4, II.2, Лемма] на X частичный порядок: $x \geq y$, если $x \vee y = x$. При этом $x \vee y$ соответствует операции sup. Таким образом, категория B^0-модулей эквивалентна категории частично упорядоченных множеств с точной верхней границей каждых двух элементов, где морфизмы – отображения, коммутирующие с sup (а не просто монотонные отображения).

3.1.3. Описание $\mathbb{F}_1[\vee]$. Интересующее нас кольцо $\mathbb{F}_1[\vee]$ может быть представлено в виде $\mathbb{F}_1 \otimes \mathbb{F}_\emptyset[\vee]$, а с учетом (19) и в виде $\mathbb{F}_1 \otimes B^0$.

Легко увидеть, что $R \otimes \mathbb{F}_1 = R[t]$ для обобщенного кольца R, где t – переменная арности 0. Стрелка справа налево возникает по универсальности из гомоморфизма $R \to R \otimes \mathbb{F}_1$ (структурный гомоморфизм из определения $\otimes$) и элемента $[R \otimes \mathbb{F}_1](0)$, полученного из $0 \in \mathbb{F}_1(0)$ с помощью структурного гомоморфизма $\mathbb{F}_1 \to R \otimes \mathbb{F}_1$. Обратная стрелка возникает по универсальности из гомоморфизма $R \to R[t]$ (структурный гомоморфизм из определения полиномов) и единственного гомоморфизма $\mathbb{F}_1 \to R[t]$ (из $\mathbb{F}_1$ существует единственный гомоморфизм во всякое кольцо с нулем). Проверка взаимообратности этих стрелок опущена.

Более того, для кольца с нулем $R \otimes \mathbb{F}_1 = R$. Действительно, в этом случае $R \to R \otimes \mathbb{F}_1$ – эпиморфизм, так как правая часть порождена новым нулем, совпадающим со старым по коммутативности.

Однако для кольца без нуля не видно простого описания функтора $R[t]$ в общем случае. Для $R = B^0$ эта задача решается непосредственно, благодаря простой структуре B^0. Для этого введем кольцо A, а потом проверим, что $B^0 \otimes \mathbb{F}_1 \simeq A$, то есть

$$\mathbb{F}_1[\vee] \simeq A,$$

что и даст искомое описание $\mathbb{F}_1[\vee]$.

Пусть $A(X) = B^0(X \cup \{0\})$, то есть $A(X)$ – множество всех конечных непустых подмножеств $X \cup \{0_X\}$, где элемент $0 \in X \cup \{0\}$ обозначен 0_X во избежание путаницы. Приведем описание структуры алгебры на A. Единица $e_A(X) : X \to A(X)$ переводит x в $\{x\}$. Для описания умножения $m_A(X) : A(A(X)) \to A(X)$ заметим, что каждый элемент $A(A(X))$ представлен набором одного из двух видов $\{U_i\}$ или $\{V_j, \{0_{A(X)}\}\}$, где U_i, $V_j \subset X \cup \{0_X\}$. Умножение $m_A(X)$ переводит такие наборы в $\bigcup U_i$ или $\{0_X\} \cup \bigcup V_j$, соответственно.

Очевидно, A – коммутативное кольцо с нулем. Покажем, что гомоморфизм $\mathbb{F}_1 \otimes B^0 \to A$, определенный "включением" $\mathbb{F}_1 \to A, 0 \mapsto 0$ и вложением $B^0 \subset A$, является изоморфизмом. Для проверки рассмотрим произвольное коммутативное кольцо R с нулем и операцией $\vee_R \in R(2)$, удовлетворяющей соотношениям (18), и покажем, что имеется единственный гомоморфизм $\mathbb{F}_1$-алгебр $g : A \to R$, такой что $g(\{1,2\}) = \vee_R$. Единственность – следствие того, что A порождено над $\mathbb{F}_1$ операцией объединения, а для построения положим $g(U) = f(x) \vee_R \cdots \vee_R f(z)$, где $U = \{x, \dots, z\} \subset X \cup \{0_X\}$, $f : \mathbb{F}_1 \to R$ структурный гомоморфизм. Проверка того, что f – гомоморфизм, опущена. Таким образом, A универсально и $\mathbb{F}_1 \otimes B^0 \simeq A$.

Категория A-модулей эквивалентна категории пунктированных полурешеток, причем выделенный элемент не обязательно максимален.

3.2. Поле $\mathbb{F}\mathrm{P}$

В [1, 4.8.13] описано обобщенное кольцо $\mathbb{F}_\infty$, представляющее собой поле вычетов в архимедовой точке $\mathbb{Q}$. Изучим обобщенное кольцо $\mathbb{F}\mathrm{P}$, являющееся полем вычетов в архимедовой точке $\mathbb{Q}_{\geq 0}$. Рассмотрим в $\mathbb{R}$ обобщенное подкольцо $\mathbb{P}$, где $\mathbb{P}(n) = \{(\lambda_1, \dots, \lambda_n) | \lambda_i \geq 0\}$ и обобщенное кольцо $\mathcal{O}_\mathbb{P} \subset \mathbb{P}$, где

$$\mathcal{O}_\mathbb{P}(n) = \Big\{(\lambda_1, \dots, \lambda_n) | \lambda_i \geq 0, \sum \lambda_i \leq 1\Big\}.$$

3.2.1. $\mathbb{F}P$ как поле вычетов. Рассмотрим в $\mathcal{O}_\mathbb{P}(1) = [0,1]$ отношение эквивалентности R, отождествляющее точки $[0,1)$. Проверим, что R совместимо с $\mathcal{O}_\mathbb{P}$-действием на $\mathcal{O}_\mathbb{P}(1)$, то есть что $\phi(x_1, \dots, x_n) = \phi(y_1, \dots, y_n) \bmod R$ для всякого $\phi \in \mathcal{O}_\mathbb{P}(n)$ при условии $x_i = y_i \bmod R$ [1, 4.6.11]. Это достаточно проверить для образующих кольца $\mathcal{O}_\mathbb{P}$ над $\mathbb{F}_\emptyset$. Утверждается, что $\mathcal{O}_\mathbb{P}$ порождено 0-арным нулем и всеми бинарными операциями. Поэтому достаточно проверить, что $\lambda x + \mu y = \lambda x' + \mu y' \bmod R$ для $x = x' \bmod R$, $y = y' \bmod R$, где $\lambda + \mu \leq 1$, $\lambda, \mu \geq 0$, $x, y, x', y' \in \mathcal{O}_\mathbb{P}(1)$. Это верно.

Определим $\mathcal{O}_\mathbb{P}$-модуль $Q = \mathcal{O}_\mathbb{P}(1)/R \simeq \{0,1\}$. Хочется, однако, определить Q как $\mathbb{F}\mathrm{P}(1)$ для обобщенного кольца $\mathbb{F}\mathrm{P}$. Как и выше, действуем, следуя [1, 4.8.13]. Структура $\mathcal{O}_\mathbb{P}$-модуля на Q определяет гомоморфизм обобщенных колец [1, 4.3.8] $\rho : \mathcal{O}_\mathbb{P} \to \mathrm{END}(Q)$.

Положим

$$\mathbb{F}\mathrm{P} = \text{ образ } \rho.$$

3.2.2. Конструктивное описание $\mathbb{F}\mathrm{P}$. Приведем элементарное описание $\mathbb{F}\mathrm{P}$. Для этого вспомним [1, 4.7.3], что $\mathrm{END}(Q)(n) = \mathrm{Hom}_{\mathcal{A}}(Q^n, Q)$, где $\mathcal{A}$ – категория эндофункторов категории множеств, а Q рассматривается как постоянный эндофунктор, принимающий на любом множестве значение Q. Отметим, что морфизмы постоянных эндофункторов – то же самое, что и морфизмы определяющих объектов. Таким образом, $\mathrm{END}(Q)(n) = \mathrm{Map}(Q^n, Q)$ и нужно вычислить образ $\mathcal{O}_{\mathbb{P}}(n)$ в этом множестве. Например, $\mathbb{F}\mathrm{P}(0) = \{0\} \subset Q$, $\mathbb{F}\mathrm{P}(1) \subset \mathrm{Map}(Q, Q)$ и состоит из постоянных отображений в 0 и 1, а

$$\mathbb{F}\mathrm{P}(2) = \{0, x, y, x \vee y\} \subset \mathrm{Map}(Q^2, Q).$$

При этом единственная нетривиальная 2-операция $x \vee y$ переводит в ноль все точки Q^2, за исключением точки 1×1, а отображение $\rho : \mathcal{O}_{\mathbb{P}}(2) \to \mathbb{F}\mathrm{P}(2)$ устроено так:

$$(\lambda_1, \lambda_2) \mapsto \begin{cases} 0, & \text{если } \lambda_1 + \lambda_2 < 1; \\ x, & \text{если } \lambda_1 = 1, \lambda_2 = 0; \\ y, & \text{если } \lambda_1 = 0, \lambda_2 = 1; \\ \vee, & \text{если } \lambda_1 + \lambda_2 = 1, \lambda_1 \neq 1, \lambda_2 \neq 1. \end{cases}$$

Поскольку $\mathcal{O}_{\mathbb{P}}$ порождено 2-арными операциями, то же верно и для $\mathbb{F}\mathrm{P}$.

3.2.3. Задание $\mathbb{F}\mathrm{P}$ образующими и соотношениями. $\mathbb{F}\mathrm{P}$ порождено над $\mathbb{F}_1$ одной 2-операцией $\vee$ (следствие представления $\mathbb{F}\mathrm{P}$ как фактора и описания образующих $\mathcal{O}_{\mathbb{P}}$). На $\vee$ достаточно наложить соотношения (18) и добавочное соотношение

$$0 \vee x = 0. \tag{20}$$

3.2.4. Явная модель $\mathbb{F}\mathrm{P}$. Так как $\mathbb{F}\mathrm{P}$ получается из $\mathbb{F}_1[\vee]$ добавлением соотношения $0 \vee x = 0$, то явное описание $\mathbb{F}_1[\vee]$ из 3.1.3 дает явное описание $\mathbb{F}\mathrm{P}$ в виде фактора A. А именно, $\mathbb{F}\mathrm{P}$ получается из A факторизацией по следующему отношению эквивалентности: $U \sim V$, где $U, V \subset X \cup \{0\}$, тогда и только тогда, когда либо $U = V$, либо как U, так и V содержат 0. Иными словами, $\mathbb{F}\mathrm{P}(X)$ состоит из всех конечных непустых подмножеств в $X \cup \{0\}$, причем все подмножества, содержащие 0, отождествляются. При этом $\vee$ совпадает с операцией объединения.

При указанном отождествлении подмножеству $\{x, \ldots, z\} \subset X$ соответствует операция $x \vee \cdots \vee z$, а любому множеству, содержащему 0, соответствует операция 0.

Отметим, что $\mathbb{F}\mathrm{P}(X)$ – отличается от множества всех конечных подмножеств X с операцией объединения, хотя имеет такой же размер и значительную общую часть.

3.2.5. $\mathbb{F}\mathrm{P}$ – поле. Определение обобощенного поля дано в [1, 5.7.5]. Желание считать $\mathbb{F}_\infty$ полем исключает определение свойством свободности модулей. Тривиальное кольцо $\mathbf{1}$ в [1, 4.3.13] определено формулой $\mathbf{1}(X) = 0$ для любого X (финальное кольцо). Кольцо $\mathbf{1}$ содержит единственное подкольцо $\mathbf{1}^+$. Подкольцо $\mathbf{1}^+$ отличается от $\mathbf{1}$ только тем, что $\mathbf{1}^+(\emptyset) = \emptyset$. Имеется критерий: R субтривиально, если бинарные операции $f(x, y) = x$ и $g(x, y) = y$ совпадают [1, 4.3.13].

Для проверки того, что $\mathbb{F}\mathrm{P}$ – поле, надо убедиться, что $\mathbb{F}\mathrm{P}$ не субтривиально (очевидно), но любой его строгий фактор субтривиален (кроме самого $\mathbb{F}\mathrm{P}$). Для проверки второго рассмотрим строгий эпиморфизм $\rho : \mathbb{F}\mathrm{P} \to F$ в некоторое кольцо. Предположим, что ρ склеил различные n-арные операции $f(x_1, \ldots, x_n) = x_{i_1} \vee \cdots \vee x_{i_a}$ и $g(x_1, \ldots, x_n) = x_{j_1} \vee \cdots \vee x_{j_b}$. Так как $f \neq g$, то найдется индекс m, для которого x_m входит только в одну из операций f и g. Считаем, что в f. Приравнивая $x_m = x$, а все остальные аргументы к y, получим соотношение $x \vee y = y$. Меняя их местами, получим $y \vee x = x$. Таким образом, $x = y$ и F субтривиально.

3.2.6. Модули над $\mathbb{F}\mathrm{P}$. Категория $\mathbb{F}\mathrm{P}$-модулей эквивалентна категории частично упорядоченных множеств с точной верхней границей каждых двух элементов и с наибольшим элементом, где морфизмы $\mathbb{F}\mathrm{P}$-Mod – отображения, переводящие 0 в 0 и коммутирующие с sup.

Отметим, что обозначение константы нулем соответствует духу теории обобщенных колец, но противоречит обозначениям теории решеток, где максимальный элемент по отношению к операции $\vee$ следует обозначить 1.

Например, рассмотрим следующие иерархии

$$\begin{tikzcd}
 & 0 \arrow[d] & & 0 \arrow[d] & & 0 \arrow[d] \\
 & x \vee y \arrow[dl] \arrow[dr] & & z & & \bullet \arrow[dl] \\
x & & y & & \bullet & \\
 & M & & N & & P
\end{tikzcd}$$

Модуль M – свободный с образующими x и y, модуль N – свободный с образующей z, модуль P не свободен. Более того, у свободного модуля бывают несвободные подмодули, например, P – подмодуль M. Кроме того, бывают проективные, но не свободные модули. Например, P – проективен, поскольку является ретрактом M.

3.3. Поля $\mathbb{FP}_G$

Далее интересуемся кольцами, аналогичными рассмотренным в 3.1 и 3.2, но расширенными с помощью моноида или группы. Коммутативный моноид M рассматривается как обобщенное кольцо с $M(X) = M \times X$, где операция $\sigma \times x$ обозначается $\sigma \cdot x$ или x^σ.

3.3.1. Явная модель $R \otimes M$**.** Для коммутативного моноида M потребуется явное описание кольца $R \otimes M$, где R – произвольное обобщенное кольцо. Для этого рассмотрим изоморфизм функторов

$$R \circ M \to R \otimes M, \tag{21}$$

устроенный следующим образом. Стрелка слева направо строится для эндофункторов, связанных с призвольными обобщенными кольцами R, S: $R \circ S \to (R \otimes S) \circ (R \otimes S) \to R \otimes S$, где $R \to R \otimes S$ и $S \to R \otimes S$ – структурные гомоморфизмы из определения тензорного произведения.

Для построения стрелки справа налево достаточно указать гомоморфизмы колец $R \to R \circ M$ и $M \to R \circ M$. Первый из них получается применением R к единице $\mathrm{Id} \to M$, а второй вычислением единицы $\mathrm{Id} \to R$ на M.

Утверждается, что стрелка (21) – изоморфизм колец, где структура алгебры на $R \circ M$ описана следующим образом. Единица $R \circ M$ получается композицией M-единицы и R-единицы $e : \mathrm{Id}(X) \to M(X) \to R(M(X))$, а умножение – композицией

$$R \circ M \circ R \circ M \xrightarrow{1 \circ \phi \circ 1} M \circ R \circ M \circ R \xrightarrow{m_R \circ m_M} R \circ M,$$

где $\phi : M \circ R \to R \circ M$ переводит операцию $[f(x_1, \ldots, x_n)]^\sigma$ в операцию $f(x_1^\sigma, \ldots, x_n^\sigma)$.

3.3.2. Кольца R_M и $R_M[\vee]$. Для коммутативного моноида M имеется обобщенное кольцо $R_M = M \otimes \mathbb{F}_1$, причем $R_M(X) = M(X) \cup \{0\}$ (см. 3.3.1). Очевидно, тензорное произведение колец $M \otimes N$ совпадает с кольцом моноида $M \times N$ и

$$R_M \otimes_{\mathbb{F}_1} R_N = R_{M \times N}. \tag{22}$$

Для коммутативного моноида M пусть $R_M[\vee] = \mathbb{F}_1[\vee] \otimes M$. С учетом 3.3.1 и явного описания $\mathbb{F}_1[\vee]$ (см. 3.1.3) получаем следующее явное описание:

$$R_M[\vee](X) = \text{ множество конечных непустых подмножеств } \; M \times X \cup \{0\},$$

причем операция $\vee$ соответствует объединению подмножеств.

3.3.3. Кольцо RP_M. Для коммутативного моноида M положим

$$\mathrm{RP}_M = \mathbb{FP} \otimes_{\mathbb{F}_1} R_M. \tag{23}$$

Поскольку $\mathbb{FP}$ – фактор $\mathbb{F}_1[\vee]$ (см. 3.2.4), то RP_M – фактор $R_M[\vee]$ относительно следующего отношения эквивалентности: $U \sim V$, где $U, V \subset M \times X \cup \{0\}$, тогда и только тогда, когда либо $U = V$, либо как U, так и V содержат 0. Иными словами, $\mathrm{RP}_M(X)$ состоит из всех конечных непустых подмножеств в $M \times X \cup \{0\}$, причем все подмножества, содержащие 0, отождествляются. При этом $\vee$ совпадает с операцией объединения, подмножеству $\{g \times x, \ldots, h \times z\} \subset M \times X$ соответствует операция $x^g \vee \cdots \vee z^h$, а любому множеству, содержащему 0, соответствует операция 0.

Приведенное описание позволяет легко контролировать факторы RP_M.

3.3.4. $\mathrm{RP}_{\pm 1}$ и $\mathbb{F}_\infty$. Кольцо $\mathbb{F}_\infty$ определено в [1, 4.8.13] и представлено [1, 4.8.13] следующим образом $\mathbb{F}_\infty = \mathbb{F}_{\pm 1}[*]$, где 2-операция $*$ удовлетворяет соотношениям (20), а также дополнительному соотношению

$$x * (-x) = 0. \tag{24}$$

Таким образом, $\mathbb{F}_\infty$ – фактор $\mathrm{RP}_{\pm 1}$ по соотношению (24), а явное описание $\mathrm{RP}_{\pm 1}$ (см. 3.3.3) дает явное описание $\mathbb{F}_\infty$. Такое описание приведено ниже в более общем контексте – с заменой $\{\pm 1\}$ на коммутативную группу G. При этом будет полезно следующее определение.

3.3.5. Определение. *Подмножество $U \subset X$ назовем частичным сечением отображения $p : X \to Y$, если сужение $p|_U : U \to Y$ – инъекция.*

3.3.6. Кольцо $\mathbb{F}\mathrm{P}_G$. Для абелевой группы G пусть $\mathbb{F}\mathrm{P}_G = \mathrm{RP}_G/(x \vee gx = 0$ при $g \neq 1)$. В частности, $\mathbb{F}_\infty = \mathbb{F}\mathrm{P}_{\pm 1}$.

С учетом 3.3.3 и того, что $\mathbb{F}\mathrm{P}_G$ – фактор RP_G, получаем следующее явное описание $\mathbb{F}\mathrm{P}_G$. В множестве всех непустых конечных подмножеств $G \times X \cup \{0\}$ рассмотрим отношение эквивалентности, фактор по которому дает $\mathbb{F}\mathrm{P}_G(X)$: $U \sim V$, где $U, V \subset G \times X \cup \{0\}$, тогда и только тогда, когда либо $U = V$, либо ни U, ни V не являются частичными сечениями проекции $G \times X \to X$. Иными словами, $\mathbb{F}\mathrm{P}_G(X)$ состоит из всех конечных непустых подмножеств в $G \times X \cup \{0\}$, причем все подмножества, не являющиеся частичными сечениями, отождествляются. При этом $\vee$ совпадает с операцией объединения, подмножеству $\{g \times x, \ldots, h \times z\} \subset G \times X$ соответствует операция $x^g \vee \cdots \vee z^h$, а любому множеству, не являющемуся частичным сечением, соответствует операция 0.

Из приведенного описания вытекает, что

$$\operatorname{card} \mathbb{F}\mathrm{P}_G(n) = 1 + \sum_{d=1}^{n} \binom{n}{d} |G|^d = (1 + |G|)^n, \tag{25}$$

причем число операций в $\mathbb{F}\mathrm{P}_G(n)$ истинной арности n (см. §1) равно 1.

3.3.7. Теорема. $\mathbb{F}\mathrm{P}_G$ – *поле.*

Доказательство. Утверждение доказывается аналогично 3.2.5. Для проверки того, что $\mathbb{F}\mathrm{P}_G$ – поле, надо убедиться, что $\mathbb{F}\mathrm{P}_G$

не тривиально (вытекает из (25)), но любой его строгий фактор (кроме $\mathbb{FP}_G$) тривиален. Пусть $\rho : \mathbb{FP} \to F$ – эффективный эпиморфизм. Предположим, что $\rho(f) = \rho(g)$, где f, g – различные операции. Можно считать, что $f = x_1^{\sigma_1} \vee \cdots \vee x_a^{\sigma_a} \neq 0$. Подставляя вместо x_i аргумент $y_i^{\sigma_i^{-1}}$ (пользуемся тем, что G – группа, а не просто моноид), можно считать, что

$$f = y_1 \vee \cdots \vee y_m.$$

Если в аналогичное выражение для g входит аргумент, отличный от $y_1, \ldots, y_m$, то, приравнивая его к нулю, а y_i к y, получим в F соотношение $y = 0$, что влечет тривиальность F. Если $g \neq 0$ и в выражение для g не входит хотя бы один из y_i, то применяем предыдущее рассуждение, меняя местами f и g. Таким образом, осталось рассмотреть случай, когда в g входят все y_i, причем хотя бы один из них в виде y_i^σ при $\sigma \neq 1$ (так как $f \neq g$). Подставляя вместо всех y_i аргумент y, получим в F соотношение $y = 0$, то есть тривиальность F. □

3.4. Кольцо $\mathbb{F}_\infty^{\otimes n}$

Начнем с изучения более простого кольца $\mathbb{FP} \otimes_{\mathbb{F}_1} \mathbb{FP}$. Это кольцо порождено над $\mathbb{F}_1$ двумя коммутирующими 2-операциями $\vee$ и $*$, для каждой из которых выполнены соотношения (18) и (20). Коммутирование $*$ и $\vee$ означает, что

$$(x \vee y) * (z \vee w) = (x * z) \vee (y * w). \tag{26}$$

Из (26) вытекают соотношения взаимной дистрибутивности операций $*$ и $\vee$

$$x \vee (y * z) = (x \vee y) * (x \vee z), \quad x * (y \vee z) = (x * y) \vee (x * z). \tag{27}$$

Это проверено в [1, 5.7.2] – надо в (26) взять $w = y$ и $w = z$, соответственно.

3.4.1. Теорема. *Естественный гомоморфизм $\mathbb{FP} \otimes_{\mathbb{F}_1} \mathbb{FP} \to \mathbb{FP}$ – изоморфизм.*

Доказательство. Покажем, что $u * v = u \vee v$. Действительно, $u \vee v = (u \vee v) * (u \vee v) = (u \vee v) * (v \vee u)$. Применяя (26) для $x = u$, $y = v$, $z = v$, $w = u$, получим $u \vee v = (u * v) \vee (v * u) = (u * v) \vee (u * v) = u * v$. □

В доказательстве не использовался 0. Поэтому и $\mathbb{F}_\emptyset[\vee]\otimes\mathbb{F}_\emptyset[\vee] = \mathbb{F}_\emptyset[\vee]$. Кроме того, $\mathbb{F}_\infty \otimes_{\mathbb{F}_{1^2}} \mathbb{F}_\infty = \mathbb{F}_\infty$ и

$$\mathrm{RP}_M \otimes_{\mathbb{F}_1} \mathrm{RP}_N = \mathrm{RP}_{M\times N} \tag{28}$$

для коммутативных моноидов M и N. Это следствие (22), (23) и 3.4.1.

Зафиксируем $n \geq 1$ и вычислим $\mathbb{F}_\infty^{\otimes n} = \mathbb{F}_\infty \otimes_{\mathbb{F}_1} \cdots \otimes_{\mathbb{F}_1} \mathbb{F}_\infty$. Пусть

$$G = \mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2 \qquad (n \text{ раз}),$$

$\sigma_i = (0,\dots,0,1,0,\dots,0) \in G$. Проекция $\phi : \mathrm{RP}_{\pm 1} \to \mathbb{F}_\infty$ (см. 3.3.4) индуцирует проекцию $\phi^{\otimes n} : \mathrm{RP}_{\pm 1} \otimes \cdots \otimes \mathrm{RP}_{\pm 1} \to \mathbb{F}_\infty^{\otimes n}$, а с учетом (28) – эффективный эпиморфизм $\mathrm{RP}_G \to \mathbb{F}_\infty^{\otimes n}$. Его композиция с проекцией $R_G[\vee] \to \mathrm{RP}_G$ (см. 3.3.3) позволяет рассмотреть $\mathbb{F}_\infty^{\otimes n}$ как результат факторизации

$$R_G[\vee] \to \mathbb{F}_\infty^{\otimes n}.$$

Эта факторизация по соотношениям $x \vee x^{\sigma_i} = 0$ индуцирует в $R_G[\vee](X)$, то есть в множестве непустых конечных подмножеств $G\times X \cup \{0\}$, следующее отношение эквивалентности: $U \sim V$, если либо $U = V$, либо ни U, ни V не являются частичными сечениями хотя бы для одной из проекций $p_i : X \times G \to X \times G/\sigma_i$. При этом 0 не считается частичным сечением.

3.4.2. $\mathbb{F}_\infty^{\otimes n}$ и коды. Пусть $A(n)$ – множество двоичных кодов длины n, реализованных как подмножества G. Для кода $U \subset G$ определено кодовое расстояние

$$d(U) = \min\{d(x,y) | x,y \in U, x \neq y\}, \qquad (d - \text{ расстояние Хэмминга}).$$

Для сравнения с $\mathbb{F}_\infty^{\otimes n}$ удобно слегка модифицировать множество $A(n)$. А именно, на множестве $G \cup \{0\}$ введем вырожденное расстояние, совпадающее с расстоянием Хэмминга на G и такое, что $d(0,x) = 0$. Пусть $\widetilde{A}(n)$ – множество подмножеств $G \cup \{0\}$. Будем считать, что $d(\{0\}) = 0$, а $d(\emptyset) = \infty$. Имеется фильтрация

$$\widetilde{A}(n)_0 \subset \widetilde{A}(n)_1 \subset \cdots \subset \widetilde{A}(n)_\infty = \widetilde{A}(n),$$

где $\widetilde{A}(n)_d$ – множество тех “кодов” U, для которых $d(U) \leq d$.

Приведенное выше описание показывает, что $\mathbb{F}_\infty^{\otimes n}(1)$ можно отождествить с множеством $\widetilde{A}(n)_{<\infty}/\widetilde{A}(n)_1$.

3.4.3. Некоторые вычисления. Вычисления показывают, что $\operatorname{card}\mathbb{F}_\infty^{\otimes 2}(1) = 7$, а список нетривиальных элементов $\mathbb{F}_\infty^{\otimes 2}(1)$ таков: $\{(0,0)\}$, $\{(1,0)\}$, $\{(0,1)\}$, $\{(1,1)\}$, $\{(1,0),(0,1)\}$, $\{(0,0),(1,1)\}$.

Вычисления показывают, что $\operatorname{card}\mathbb{F}_\infty^{\otimes 3}(1) = 35$, а список нетривиальных элементов $\mathbb{F}_\infty^{\otimes 3}(1)$ таков: произвольное непустое подмножество U_0 или U_1, где U_0 (соответственно, U_1) – прообраз 0 (соответственно, 1) при гомоморфизме суммы координат $G \to \mathbb{Z}/2$, а также $\{(0,0,0),(1,1,1)\}$, $\{(1,0,0),(0,1,1)\}$, $\{(0,1,0),(1,0,1)\}$, $\{(0,0,1),(1,1,0)\}$.

Кроме того, $\operatorname{card}\mathbb{F}_\infty^{\otimes n}(1) \geq 2 \cdot 2^u - 1$, где $u = 2^{n-1}$. Действительно, помимо нуля к списку элементов $\mathbb{F}_\infty^{\otimes n}(1)$ принадлежит произвольное непустое подмножество U_i, где U_i – прообраз i при гомоморфизме суммы координат $G \to \mathbb{Z}/2$.

Кроме того, $\operatorname{card}\mathbb{F}_\infty^{\otimes n}(m) = q^m$, где $q = \operatorname{card}\mathbb{F}_\infty^{\otimes n}(1)$. Действительно, пусть $U \subset X \times G$ – непусто. Тогда U представляет нетривиальный элемент $\mathbb{F}_\infty^{\otimes n}(X)$ тогда и только тогда, когда $U_x = x \times G \cap U$ либо пусты, либо представляют собой нетривиальный элемент $\mathbb{F}_\infty^{\otimes n}(\{x\})$. Таким образом, число нетривиальных элементов равно

$$\sum_{U \subset X, U \neq \emptyset} (q-1)^{\operatorname{card} U} = \sum_{d=1}^{m} \binom{m}{d} (q-1)^d = q^m - 1, \quad X = \{1, \ldots, m\}.$$

4. Подкольца бесконечных классических колец

В этом разделе рассматриваются подкольца $\mathbb{Z}_p$, $\mathbb{Z}_\infty$ и $\mathbb{Z}$. Приведена любопытная гипотеза о конгруэнц-происхождении подколец $\mathbb{Z}$, содержащих операцию $(a_1, \ldots, a_n)$, где a_i взаимно просты в совокупности.

4.1. Подкольца $\mathbb{Z}_p$

Ниже R – обобщенное подкольцо $\mathbb{Z}_p$, содержащее 0. Естественно рассматривать случай, когда $R(n)$ замкнуто в естественной топологии $\mathbb{Z}_p(n)$ для каждого n. Будем это предполагать.

Выяснение структуры подколец $\mathbb{Z}_p$ начнем со следующего простого утверждения.

4.1.1. Предложение. *Следующие условия равносильны:*

1. $\mathbb{Z}_p = R$;
2. *$R(2)$ содержит хотя бы одну операцию вида $ax + by$, где a и b обратимы в $\mathbb{Z}_p$.*

Доказательство. Достаточно вывести первый пункт из второго. Отметим, что

$$\text{если } a \in R(1) \text{ и } a \text{ обратимо в } \mathbb{Z}_p, \text{ то } a^{-1} \in R(1). \tag{29}$$

Действительно, $a^{-1} = \lim a^{(p-1)p^n-1}$, а $R(1)$ замкнуто в $\mathbb{Z}_p$. Пусть $ax+by \in R(2)$ – операция из условия. Так как $0 \in R$, то $a, b \in R(1)$. Так как a и b обратимы, то $a(a^{-1}x) + b(b^{-1}y) = x + y \in R(2)$. Следовательно, $\mathbb{N} \subset R$ и $R = \mathbb{Z}_p$, поскольку $\mathbb{N}$ плотно в $\mathbb{Z}_p$. $\square$

Следующая цель – описать такие R, что $\mathbb{Z}_p$ конечно над R. Для этого рассмотрим в $\mathbb{Z}_p$ подкольцо $\mathbb{Z}_p^s$, для которого

$$\mathbb{Z}_p^s(n) = \{(a_1, \dots, a_n) \in \mathbb{Z}_p^n | \text{ либо все } a_i \in I, \quad \text{либо } \exists i \quad a_j = 0 \text{ при } xj \neq i\},$$

где $I = p\mathbb{Z}_p$. Отметим, что имеется гомоморфизм

$$\mathbb{Z}_p^s \to \mathbb{F}_1, \tag{30}$$

при котором $(a_1, \dots, a_m) \mapsto (c_1, \dots, c_n)$, где $c_i = 1$ для обратимого a_i, и $c_i = 0$ в ином случае.

4.1.2. Теорема. *Следующие условия равносильны:*

1. $\mathbb{Z}_p$ *конечно над* R*;*
2. $R \supset R_d$ *для некоторого* d*, где* R_d *– прообраз* $\mathbb{F}_1$ *при проекции* $\mathbb{Z}_p \to \mathbb{Z}_p/p^d$*;*
3. $R(2)$ *содержит хотя бы одну операцию вида* $ax+by$*, где* $a \neq 0$*,* $b \neq 0$*, а идеал* (a, b) *совпадает с* $\mathbb{Z}_p$*;*
4. R *не содержится в* $\mathbb{Z}_p^s$*.*

Доказательство. Первый пункт вытекает из второго по 2.1.2. Выведем второй пункт из третьего. Пусть $ax+by \in R(2)$ – операция из третьего пункта. Если и a и b обратимы, то утверждение вытекает из 4.1.1. Осталось разобрать случай, когда a – обратимо, а b – нет. В этом случае последовательно проверим ряд утверждений.

$$x_0 + bx_1 + \dots + bx_n \in R(n+1) \text{ для всякого } n \geq 1. \tag{31}$$

Действительно, операция $x + by = a(a^{-1}x) + by$ лежит в $R(2)$, поскольку a обратимо и в $R(1)$ (см. (29)). По индукции, $(x_0 + bx_1 + \dots + bx_{n-1}) + bx_n \in R(n+1)$.

$$x_0 + bm_1x_1 + \dots + bm_nx_n \in R(n+1) \text{ для всех } n \geq 1, \quad m_i \in \mathbb{N}. \tag{32}$$

Действительно, такая операция получается из операции вида (31) подходящей арности подстановкой, заменяющей подходящие группы переменных одной переменной.

$$x_0+\lambda_1 x_1+\cdots+\lambda_n x_n \in R(n+1) \text{ для всех } n\geq 1, \quad \lambda_i\in b\mathbb{Z}_p. \quad (33)$$

Действительно, операции вида (32) плотны среди операций вида (33).

$$\lambda_1 x_1+\cdots+\lambda_n x_n \in R(n) \text{ для всех } n\geq 1, \quad \lambda_i\in b\mathbb{Z}_p. \quad (34)$$

Действительно, достаточно в операции вида (33) положить $x_0{=}0$.

$$R(1) \text{ содержит подгруппу } U_t=\{u\in\mathbb{Z}_p | u=1 \bmod p^t\} \text{ для некоторого } t. \quad (35)$$

Действительно, $x+b^i y=x+b(b^{i-1}y)\in R(2)$, $1+b^i\in R(1)$, и среди элементов $1+b^i$ только конечное число элементов кручения.

Покажем теперь, что $R_d\subset R$, где $d=\max(t,\operatorname{ord} b)$. Во-первых, $R_d(0)=\{0\}\subset R(0)$. Если все компоненты операции из $R_d(n+1)$ необратимы, то утверждение вытекает из (34). Иначе, операция с точностью до перестановки имеет вид $(1{+}b_0)x_0{+}b_1x_1{+}\cdots{+}b_nx_n$, где $\operatorname{ord} b_i\geq d$. Эта операция лежит в $R_d(n+1)$ ввиду (33) и (35).

Проверим теперь, что третий пункт теоремы вытекает из четвертого. Если R не содержится в $\mathbb{Z}_p^s$, то в R имеется операция вида $a_1x_1+\cdots+a_nx_n$, где по меньшей мере два из a_i отличны от нуля и идеал, порожденный всеми a_i, совпадает с $\mathbb{Z}_p$. С помощью перестановки можно считать, что a_1 обратим в $\mathbb{Z}_p$, а $a_2\neq 0$. Полагая $x_3=\cdots=x_n=0$, находим в R операцию из третьего пункта.

Осталось вывести четвертый пункт теоремы из первого, то есть проверить, что $\mathbb{Z}_p$ не конечно над $\mathbb{Z}_p^s$. Рассмотрим отображение $f:\mathbb{Z}_p(n+1)\to\mathbf{P}^n_\bullet(\mathbb{Z}_p)=\mathbf{P}^n(\mathbb{Z}_p)\cup\{0\}$, при котором $(x_0,\dots,x_n)\mapsto(x_0:\cdots:x_n)$, если $x_0,\dots,x_n$ взаимно просты, и $(x_0,\dots,x_n)\mapsto 0$, иначе. Легко видеть, что отношение эквивалентности на $\mathbb{Z}_p(n+1)$, отождествляющее между собой элементы каждого слоя f, выдерживает действие $\mathbb{Z}_p^s$. Более того, действие $\mathbb{Z}_p^s$ на факторе, то есть на $\mathbf{P}^n_\bullet(\mathbb{Z}_p)$, пропускается через действие $\mathbb{F}_1$ с помощью гомоморфизма (30). Поэтому достаточно проверить, что $\mathbf{P}^n_\bullet(\mathbb{Z}_p)$ – не конечнопорождено над $\mathbb{F}_1$, то есть не конечно. Это так при $n\geq 2$. □

4.2. Подкольца $\mathbb{Z}_\infty$

Ограничимся в этом случае несколькими примерами. Для псевдонормы на $A = \mathbb{R}$, то есть функции $A \to \mathbb{R}_{\geq 0}$, $x \mapsto \|x\|$, такой что $\|x+y\| \leq \|x\| + \|y\|$, $\|xy\| \leq \|x\| \cdot \|y\|$, $\|1\| \leq 1$, положим

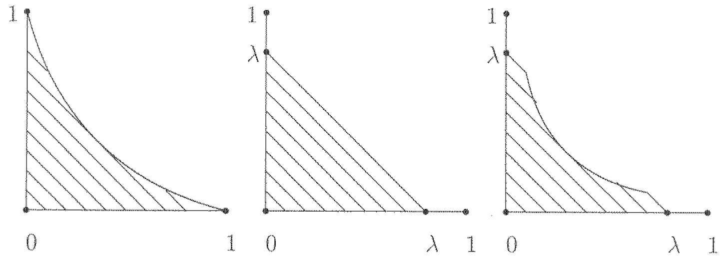
$$R(n) = \{(x_1, \ldots, x_n) \in \mathbb{R}(n) | \quad \|x_1\| + \cdots + \|x_n\| \leq 1\}.$$

Очевидно, что R – подкольцо $\mathbb{R}$ и $R = \mathbb{Z}_\infty$ для $\|x\| = |x|$.

Имеется много других примеров псевдонорм. Например, $\|x\| = |x|^s$ при $0 \leq s \leq 1$ (этот пример принадлежит Н. Дурову). В другом примере для $0 < \lambda \leq 1$ положим

$$\|x\| = \begin{cases} \lambda^{-1}|x|, & 0 \leq |x| \leq \lambda; \\ 1, & \lambda \leq |x| \leq 1; \\ |x|, & \text{если } |x| > 1. \end{cases}$$

Содержащаяся в первом квадранте часть $R(2)$ изображена на рисунке



При этом первая картинка соответствует псевдонорме $|x|^s$, вторая – псевдонорме, связанной с λ, а на третьей картине изображено пересечение колец из первых двух примеров. Таким образом, подкольца $\mathbb{Z}_\infty$ могут иметь довольно замысловатый вид.

4.3. Подкольца $\mathbb{Z}$

Начнем с нескольких примеров. Во-первых, имеются кольца $\mathbb{Z}^u \subset \mathbb{Z}^s$, где

$$\mathbb{Z}^u(n) = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n | \exists j : a_i = 0 \text{ при } i \neq j\},$$

$$\mathbb{Z}^s(n) = \{a = (a_1, \ldots, a_n) \in \mathbb{Z}^n | \text{ либо } a \in \mathbb{Z}^u(n), \text{ либо } \mathrm{GCD}(a_1, \ldots, a_n) \neq 1\}.$$

Кроме того, имеется кольцо $A_N = \mathbb{Z}_{(N)} \cap \mathbb{Z}_{(\infty)}$ [1, 7.1.1] и для $N \in \mathbb{Z}$ кольцо

$$R_N \text{ – прообраз при гомоморфизме } R \subset \mathbb{Z} \to \mathbb{Z}/N \text{ образа } \mathbb{F}_{1^2} \text{ в } \mathbb{Z}/N. \quad (36)$$

При классификации подколец $\mathbb{Z}$ на первом этапе было интересно выделить основные типы таких подколец, соответственно их размеру. Кольца $\mathbb{Z}^u$ и $\mathbb{Z}^s$ представляют собой наибольшие примеры "малых" и "средних" подколец, соответственно.

Возможно, наибольший интерес представляют кольца R, над которыми $\mathbb{Z}$ конечно. Можно показать, что такое кольцо не может содержаться в $\mathbb{Z}^s$. Иными словами, речь идет о кольцах, содержащих хотя бы одну операцию $(a_1, \ldots, a_n)$, где $n \geq 2$, все $a_i \neq 0$ и $\mathrm{GCD}(a_1, \ldots, a_n) = 1$.

4.3.1. Теорема. *Если $(a_1, \ldots, a_n) \in R(n)$, где $n \geq 2$, все $a_i \neq 0$ и $\mathrm{GCD}(a_1, \ldots, a_n) = 1$, то найдется операция $(a, b) \in R(2)$, такая, что $a \neq 0, b \neq 0$, $\mathrm{GCD}(a, b) = 1$.*

Доказательство. Достаточно рассмотреть случай, когда $n \geq 3$ и a_1 – нечетно (используя подходящую перестановку). Пусть $\{p_j\}$ – множество всех простых делителей числа $\mathrm{GCD}(a_1, \ldots, a_{n-2})$ и $N = \prod(p_j - 1)$. Среди p_j нет 2 ввиду нечетности a_1. Рассмотрим операцию $(b_1, \ldots, b_{n-1})$, где $b_1 = a_1, \ldots, b_{n-2} = a_{n-2}$, $b_{n-1} = a_{n-1}^{2N} + a_n^{2N}$. Очевидно, что все $b_i \neq 0$. Покажем, что $\mathrm{GCD}(b_1, \ldots, b_{n-1}) = 1$. Для этого достаточно показать, что

$$a_{n-1}^{2N} + a_n^{2N} \neq 0 \bmod p_j.$$

Это следствие того, что каждое слагаемое в этой сумме равно либо 0, либо 1, по крайней мере одно из них равно 1, а $p_j \neq 2$.

Осталось заметить, что $(b_1, \ldots, b_{n-1}) \in R(n-1)$. Действительно, $a_{n-1}, a_n \in R(1)$, поскольку $0 \in R(0)$. Поэтому

$$f(x_1, \ldots, x_n) = a_1 x_1 + \cdots + a_{n-2} x_{n-2} + a_{n-1}^{2N} x_{n-1} + a_n^{2N} x_n \in R(n)$$

и

$$f(x_1, \ldots, x_{n-2}, x_{n-1}, x_{n-1}) \in R(n-1).$$

Продолжая понижать арность таким образом, можно добраться до подходящей 2-операции. $\square$

Возможно, приведенная теорема является частным случаем непостроенной теории размерности обобщенных колец.

4.3.2. Конгруэнц-гипотеза. Пусть R – обобщенная $\mathbb{F}_{1^2}$-подалгебра $\mathbb{Z}$, $(a,b) \in R(2)$, причем $a \neq 0, b \neq 0$, $\mathrm{GCD}(a,b) = 1$. Конгуэнц-гипотеза состоит в том, что найдется такое $N \geq 1$, что $R \supset R_N$ (см. (36)).

Конгуэнц-гипотеза равносильна тому, что

$$\text{в } R(2) \text{ найдется операция вида } (1,m), \text{ где } m \neq 0. \tag{37}$$

Действительно, если $R \supset R_N$, то $(1,N) \in R(2)$. Наоборот, пусть $(1,m) \in R(2)$. По индукции проверяется, что все операции вида $(1,m,\dots,m)$ лежат в R. Например, $1 \cdot (1,m,0) + m \cdot (0,0,1) = (1,m,m)$. Отсюда легко увидеть, что $R \supset R_m$.

Нижеприведенную гипотезу (38) и редукцию 4.3.2 к (38) автор узнал от Н. Дурова. Пусть S – подкольцо $\mathbb{Z}$, порожденное $\mathbb{F}_{1^2}$ и бинарной операцией (a,b). Тогда гипотеза 4.3.2 вытекает из следующей гипотезы

$$1 \in \langle a,b \rangle, \tag{38}$$

где $\langle a,b \rangle$ – идеал в $S(1)$, порожденный a и b. Иными словами, гипотеза (38) утверждает, что a и b порождают единичный идеал в S, то есть порождают $S(1)$ как S-модуль.

Для проверки того, что (38) влечет гипотезу 4.3.2, рассмотрим множество

$$I = \{n \in \mathbb{Z} | \exists m \in \mathbb{Z}, \text{ так что } (n,m) \in S(2) \text{ и } m \neq 0\}.$$

Покажем прежде всего, что I – идеал. Так как S порождено $\mathbb{F}_{1^2}$ и (a,b), то достаточно проверить следующие утверждения: $0 \in I$; если $u \in I$, то $-u \in I$;

$$u, v \in I \Rightarrow au + bv \in I. \tag{39}$$

Достаточно проверить(39). Пусть $(u,s) \in S(2), s \neq 0$ и $(v,t) \in S(2)$, $t \neq 0$. Тогда $(u, s^\alpha) \in R(2)$ и $(v, t^\beta) \in S(2)$. Поэтому $a(u,s^\alpha) + b(v,t^\beta) = (au+bv, as^\alpha + bt^\beta) \in S(2)$. Так как $as^\alpha + bt^\beta \neq 0$ при подходящих α, β, то $au + bv \in I$ и I – идеал.

Так как $a, b \in I$ по условию, то $I \supset \langle a,b \rangle$. Поэтому, если $1 \in \langle a,b \rangle$, то $1 \in I$ и, таким образом, (38), с учетом (37), влечет гипотезу 4.3.2.

4.3.3. Свидетельства в пользу конгруэнц-гипотезы. Далее считаем, что $0 < a < b$. Для $a = 1$ утверждение из 4.3.2 вытекает из (37). С помощью компьютера проверено, что (38) верно для (a, b), где либо $a = 4$, $b \leq 100$, либо $a = 5$, $b \leq 100$, либо $a \leq 40$, $b \leq 40$.

Ниже, при проверке гипотез, нам потребуется следующее утверждение

$$(a^n, a^{n-1}b, \ldots, ab, b) \in S(n+1). \tag{40}$$

Действительно,

$$a(a^n, a^{n-1}b, \ldots, ab, b, 0) + b(0, \ldots, 0, 1) = (a^{n+1}, a^n b, \ldots, ab, b).$$

Покажем, что гипотеза 4.3.2 верна при $a = 2$. С помощью (40) находим в $S(n+1)$ операцию $(2^n, 2^{n-1}b, \ldots, 2b, b)$. Выберем n так, что $2^n = 1 \bmod b$. Тогда $2^n - 1 = ub$, где $u = (2^n - 1)/b \leq (2^n - 1)/3 < 2^{n-1}$. Рассмотрим 2-адическое разложение $u = \alpha_0 + \alpha_1 \cdot 2 + \cdots + \alpha_{n-2} \cdot 2^{n-2}$, где $\alpha_i \in \{0, 1\}$. Тогда операция

$$(2^n, 2^{n-1}b, -\alpha_{n-2}2^{n-2}b, \ldots, -\alpha_1 2b, -\alpha_0 b) \in S(n+1),$$

поскольку $(2^n, 2^{n-1}b, \ldots, 2b, b) \in S(n+1)$ и $-\alpha_i \in \mathbb{F}_{1^2}(1)$. Отсюда вытекает, что

$$(1, 2^{n-1}b) = (2^n - \alpha_{n-2}2^{n-2}b - \cdots - \alpha_1 2b - \alpha_0 b, 2^{n-1}b) \in S(2),$$

что и доказывает в нашем случае гипотезы (37) и 4.3.2.

Похожим образом можно показать, что гипотеза 4.3.2 верна и при $a = 3$. При этом появляется небольшое осложнение, для преодоления которого потребуется следующее утверждение:

$$\{\alpha_0 + \alpha_1 \cdot 3 + \cdots + \alpha_r \cdot 3^r | \alpha_i \in \{0, \pm 1\}\} = [-d, d] \cap \mathbb{Z}, \text{ где } d = (3^r - 1)/2. \tag{41}$$

В самом деле, при замене комбинации

$$\alpha_0 + \alpha_1 \cdot 3 + \cdots + \alpha_r \cdot 3^r$$

на

$$(\alpha_0 + 1) + (\alpha_1 + 1) \cdot 3 + \cdots + (\alpha_r + 1) \cdot 3^r$$

множество всех комбинаций из (41) превратится, очевидно, в $[0, d] \cap \mathbb{Z}$.

Проверим теперь гипотезу 4.3.2 при $a = 3$. Заменяя операцию $(3, b)$ на операцию $(3, b^r)$, можем считать, что b достаточно велико. В нашем случае достаточно неравенства $b > 6$. С помощью

(40) находим в $S(n+1)$ операцию $(3^n, 3^{n-1}b, \dots, 3b, b)$. Выберем n так, что $3^n = 1 \bmod b$. Тогда $3^n - 1 = ub$, где

$$u = (3^n - 1)/b \leq (3^n - 1)/6 < (3^{n-1} - 1)/2. \tag{42}$$

Рассмотрим "правильное" 3-адическое разложение u, то есть разложение $u = \alpha_0 + \alpha_1 \cdot 3 + \dots + \alpha_{n-2} \cdot 3^{n-2}$, где $\alpha_i \in \{0, 1, -1\}$ (важно, что в это разложение не входят 3^{n-1} и большие степени 3-ки – это вытекает из (41) и (42)). Тогда

$$(3^n, 3^{n-1}b, -\alpha_{n-2}3^{n-2}b, \dots, -\alpha_1 3b, -\alpha_0 b) \in S(n+1),$$

поскольку $(3^n, 3^{n-1}b, \dots, 3b, b) \in S(n+1)$ и $-\alpha_i \in \mathbb{F}_{1^2}(1)$. Отсюда вытекает, что

$$(1, 3^{n-1}b) = (3^n - \alpha_{n-2}3^{n-2}b - \dots - \alpha_1 3b - \alpha_0 b, 3^{n-1}b) \in S(2),$$

что и доказывает в нашем случае гипотезы (37) и 4.3.2.

Другим методом (с помощью интерполяционной техники) можно показать, что гипотеза 4.3.2 верна для всех пар вида $(a, a+1)$.

Литература

1. N. Durov, *New Approach to Arakelov Geometry.* `arXiv: 0704.2030` v1 [math AG] 16 Apr (2007).
2. А. Л. Смирнов, *Градуированные монады и кольца полиномов.* — Зап. научн. семин. ПОМИ **349**, (2007), 174–210.
3. Ж.-П. Серр, *Курс арифметики.* Мир, Москва, 1972.
4. Г. Биркгоф, *Теория решеток.* Наука, Москва, 1984.

Smirnov A. L. Generalized subrings of arithmetic rings.

The generalized subrings of $\mathbb{F}_q$ are classified, generalized subrings of $\mathbb{Z}/p^2$ are investigated and their complete classification is obtained when $p = 2$. Examples of $\mathbb{F}_\infty$-similar generalized fields, a computation of $\mathbb{F}_\infty^{\otimes n}$, a description of cofinite subrings of $\mathbb{Z}_p$ and examples of subrimgs of $\mathbb{Z}_\infty$ are given. A conjecture on cofinite subrings of $\mathbb{Z}$ is proposed and arguments in its favour are considered.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН

E-mail: smirnov@pdmi.ras.ru

Поступило 30 октября 2007 г.