Сибирский математический журнал
Сентябрь—октябрь, 2002. Том 43, № 5

УДК 519.48

ФОРМЫ И ПРЕДСТАВЛЕНИЯ АЛГЕБРЫ ЛИ $sl_2(\mathbb{Z})$

А. В. Ющенко

Аннотация: Выясняется структура целых p-адических форм простой трехмерной расщепляемой алгебры Ли над полем p-адических чисел. Решаются вопросы диагональности таких форм и описания максимальных диагональных идеалов. Рассматриваются конечномерные модули без кручения над простой трехмерной расщепляемой алгеброй Ли с целыми и целыми p-адическими коэффициентами. Дано описание диагональных модулей. Показана конечность числа модулей в каждой размерности и доказан локально-глобальный принцип для неприводимых модулей.

Ключевые слова: алгебра Ли, форма алгебры, неприводимый модуль, диагональная алгебра

Статья посвящена изучению $\mathbb{Z}_p$-форм трехмерной простой расщепляемой алгебры Ли $sl_2(\mathbb{Q}_p)$ и $sl_2(\mathbb{Z})$-модулей. В п. 1 находится базис произвольной $\mathbb{Z}_p$-формы и выясняется ее строение. В п. 2 решаются вопросы диагональности $\mathbb{Z}_p$-форм и описания максимальных диагональных идеалов. В п. 3 рассматриваются конечномерные $sl_2(\mathbb{Z})$-модули без кручения, дано описание диагональных модулей, доказано, что в каждой размерности $sl_2(\mathbb{Z})$-модулей без кручения конечное число, и доказан локально-глобальный принцип для неприводимых модулей.

В дальнейшем используются следующие стандартные обозначения: $\mathbb{Q}_p$ — поле p-адических чисел, $\mathbb{Z}_p$ — кольцо целых p-адических чисел, $\left(\frac{a}{p}\right)$ — символ Лежандра.

1. Строение $\mathbb{Z}_p$-форм алгебры Ли $sl_2(\mathbb{Q}_p)$. В этом и следующем пунктах предполагается, что p — простое число, не равное 2.

Определение. Алгебра Ли $\mathcal{L}$ над $\mathbb{Z}_p$ называется *$\mathbb{Z}_p$-формой алгебры Ли $sl_2(\mathbb{Q}_p)$*, если $\mathcal{L} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong sl_2(\mathbb{Q}_p)$ и $\mathcal{L}$ — конечномерный $\mathbb{Z}_p$-модуль.

Из условия $\mathcal{L} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong sl_2(\mathbb{Q}_p)$ следует, что $\mathcal{L}$ является свободным $\mathbb{Z}_p$-модулем.

Определение. $\mathbb{Z}_p$-форма $\mathcal{L}$ алгебры Ли $sl_2(\mathbb{Q}_p)$ называется *диагональной*, если существуют полупростой $h \in \mathcal{L}$ и его собственные векторы e, f такие, что $\mathcal{L} = \langle e, h, f\rangle$. Множество $\{e, h, f\}$ называется *диагональным базисом* $\mathcal{L}$.

Если $eh = p^n e$, $ef = p^d h$, $fh = -p^n f$, то такую алгебру будем обозначать через $\mathcal{S}(n, d)$.

Теорема 1. *Пусть $\mathcal{L}$ — $\mathbb{Z}_p$-форма алгебры Ли $sl_2(\mathbb{Q}_p)$. Тогда существуют диагональная подалгебра $\mathcal{S}$ и элемент A из $\mathcal{L}$ такие, что $\mathcal{L} = \mathcal{S} + \langle A\rangle$.*

Доказательство. Пусть $\mathcal{S}$ — максимальная диагональная подалгебра в $\mathcal{L}$. Тогда, так как $\mathcal{L}$ — конечномерный $\mathbb{Z}_p$-модуль, то $\mathcal{L} = \mathcal{S} + \langle A_1, \dots, A_k\rangle$ и теорему достаточно доказать в случае $\mathcal{L} = \mathcal{S} + \langle A, B\rangle$. Выберем в $\mathcal{S}$ диагональный базис $\langle e, h, f\rangle$, $eh = p^n e$, $ef = p^d h$, $fh = -p^n f$. Если A или B лежат в $\mathcal{S}$, то утверждение теоремы, очевидно, выполняется. Таким образом, $A, B \notin \mathcal{S}$. В этом случае

$$A = \frac{\alpha e + \beta h + \gamma f}{p^s}, \quad B = \frac{ae + bh + cf}{p^m},$$

причем хотя бы один из коэффициентов A, B не делится на p. Положим $s \geq m$.

Заметим, что два из трех коэффициентов элементов A, B не делятся на p. Действительно, пусть, например, β, γ делятся на p. Тогда, рассматривая элемент $p^{s-1}A = \frac{\alpha e+\beta h+\gamma f}{p}$, получаем, что $\frac{e}{p} \in \mathcal{L}$; противоречие с максимальностью $\mathcal{S}$. В частности, можно считать, что всегда $\alpha \not\equiv 0(p)$. Действительно, в случае $\alpha \equiv 0(p), \gamma \not\equiv 0(p)$ выберем в $\mathcal{S}$ другой базис $\langle e', h', f'\rangle$, $e' = f$, $h' = -h$, $f' = e$, тогда $A = \frac{\gamma e' - \beta h' + \alpha f'}{p^s}$.

Рассмотрим элемент

$$G = \alpha B - ap^{s-m}A = \frac{(\alpha b - a\beta)h + (\alpha c - a\gamma)f}{p^m}.$$

Предположим, что коэффициенты G делятся на p^m. Тогда имеем систему сравнений:

$$a\beta \equiv \alpha b(p^m), \quad \gamma b \equiv c\beta(p^m).$$

Так как $\alpha \not\equiv 0(p)$, то $b = \frac{\beta}{\alpha}a(p^m), c = \frac{\gamma}{\alpha}a(p^m)$, откуда

$$B = \frac{ae + bh + cf}{p^m} \equiv \frac{a}{\alpha}\frac{\alpha e + \beta h + \gamma f}{p^m} \equiv \frac{a}{\alpha}p^{s-m}A \pmod{\mathcal{S}}.$$

Следовательно, $\mathcal{L} = \mathcal{S} + \langle A\rangle$.

Пусть теперь хотя бы один коэффициент G не делится на p^m. Тогда они имеют одинаковый порядок по модулю p. Действительно, умножая G на подходящую степень p, получаем, что либо $\frac{h}{p}$, либо $\frac{f}{p}$ лежит в $\mathcal{L}$; противоречие с максимальностью $\mathcal{S}$.

Положим $\nu_p(\alpha b - a\beta) = \nu_p(\alpha c - \alpha c) = t$. Здесь и далее $\nu_p(x)$ — порядок x по модулю p.

Рассмотрим элемент $H = \frac{p^t}{\alpha b - a\beta}G$. Имеем $H = \frac{h + \tau f}{p^{m-t}}$, где $\tau = \frac{\alpha c - a\gamma}{\alpha b - a\beta}, \tau \not\equiv 0(p)$. Этот элемент полупростой, и его собственными векторами будут $F = f$ и

$$E = \begin{cases} p^{n-d}e + \tau h + \frac{1}{2}\tau^2 f & \text{при } n > d, \\ e + p^{d-n}\tau h + p^{d-n}\frac{1}{2}\tau^2 f & \text{при } n \leq d. \end{cases}$$

Обозначим $\mathcal{J} = \langle E, H, F\rangle$.

Если $n \leq d$, то очевидно, что $\mathcal{S} \subset \mathcal{J}$; противоречие с максимальностью $\mathcal{S}$.

Пусть $n > d$. Выразим элементы e, h, f, A, B через E, H, F. Имеем

$$e = \frac{1}{p^{n-d}}(E - \tau p^{m-t}H + \frac{1}{2}\tau^2 F), \quad h = p^{m-t}H - \tau F, \quad f = F,$$

$$A = \frac{1}{p^{n+d-s}}\left(\alpha E + (p^{n-d+s}\beta - p^s\alpha\tau)H + \left(p^{n-d}(\gamma - \beta\tau) + \frac{1}{2}\alpha\tau^2\right)F\right),$$

$$B = \frac{1}{p^{n+d-m}}\left(aE + (p^{n-d+s}b - p^s a\tau)H + \left(p^{n-d}(c - b\tau) + \frac{1}{2}a\tau^2\right)F\right).$$

Отсюда

$$ap^{s-m}A - \alpha B = p^{s-m}(\beta a - \alpha b)H \equiv 0 \pmod{\mathcal{J}}, \quad p^s A - \alpha e \equiv 0 \pmod{\mathcal{J}}.$$

Так как $\alpha \not\equiv 0(p)$, то

$$B \equiv \frac{a}{\alpha}p^{s-m}A \pmod{\mathcal{J}}, \quad e \equiv \frac{1}{\alpha}p^{s-m}A \pmod{\mathcal{J}}, \quad h, f \in \mathcal{S}$$

Следовательно, $\mathcal{L} = \mathcal{J} + \langle A \rangle$.

Теорема доказана.

Теорема 2. *Пусть $\mathcal{L}$ — $\mathbb{Z}_p$-форма алгебры Ли $sl_2(\mathbb{Q}_p)$, $\mathcal{L} = \mathcal{S} + \langle A \rangle$, где $\mathcal{S} = S(n,d)$ — максимальная диагональная подалгебра, $A = \frac{\alpha e + \beta h + \gamma f}{p^s}$. Тогда $n, d \geq s$ и $\mathcal{S}$ — идеал в $\mathcal{L}$.*

Доказательство. Так же, как и в теореме 1, показывается, что можно считать $\alpha \not\equiv 0(p)$.

Рассмотрим два случая: $n < d$ и $n \geq d$.

Случай 1: $n < d$. Предположим, что $n < s$. Пусть $\beta \not\equiv 0(p)$. Рассмотрим элемент

$$2aeA - \beta(p^n A + Ah) = \frac{2p^d \alpha\gamma - p^n \beta^2)}{p^s}h = \frac{2p^{d-n}\alpha\gamma - \beta^2}{p^{s-n}}h \in \mathcal{L}.$$

Тогда $\frac{h}{p} \in \mathcal{L}$; противоречие с максимальностью $\mathcal{S}$.

Пусть теперь $\beta \equiv 0(p)$. Тогда $p^{s-1}A = \frac{\alpha e + \gamma f}{p} + th$ для некоторого $t \in \mathbb{Z}_p$ и

$$p^{s-n-1}Ah + p^{s-1}A = \frac{\alpha}{p}e + p^{s-1}th.$$

Следовательно, $\frac{e}{p} \in \mathcal{L}$; противоречие с максимальностью $\mathcal{S}$.

Случай 2: $n \geq d$. Предположим, что $d < s$. Рассмотрим элемент

$$B = \frac{1}{\alpha}Af = \frac{p^d h + p^n(\beta/\alpha)f}{p^s} = \frac{h + p^{n-d}(\beta/\alpha)f}{p^{s-d}}.$$

Он полупростой, и его собственными векторами будут $E = e + \frac{\beta}{\alpha}h + \frac{p^{n-d}\beta^2}{2\alpha^2}f$ и $F = f$. Очевидно, что $\mathcal{S} \subset \langle E, B, F \rangle$; противоречие с максимальностью $\mathcal{S}$.

Таким образом, $n, d \geq s$. Непосредственно проверяется, что $Ae, Ah, Af \in \mathcal{S}$, следовательно, $\mathcal{S}$ — идеал в $\mathcal{L}$. Теорема доказана.

Следствие. *Пусть $\mathcal{L}$ — $\mathbb{Z}_p$-форма алгебры Ли $sl_2(\mathbb{Q}_p)$, $\mathcal{L} = \mathcal{S} + \langle A \rangle$, где $\mathcal{S} = S(n,d) = \langle e, h, f \rangle$ — максимальная диагональная подалгебра, $A = \frac{\alpha e + \beta h + \gamma f}{p^s}$, $\alpha \not\equiv 0(p)$. Тогда $\{A, h, f\}$ образуют базис $\mathcal{L}$.*

2. Условия диагональности $\mathbb{Z}_p$-форм и максимальные диагональные идеалы. Согласно теоремам 1 и 2 в дальнейшем можно рассматривать только $\mathbb{Z}_p$-формы алгебры Ли $sl_2(\mathbb{Q}_p)$, определенные следующим образом:

$$\begin{gathered}\mathcal{L} = \mathcal{S} + \langle A \rangle, \text{ где } \mathcal{S} = \mathcal{S}(n,d) = \langle e, h, f \rangle, \ eh = p^n e, \ ef = p^d h, \ fh = -p^n f, \\ A = \frac{\alpha e + \beta h + \gamma f}{p^s}, \quad n, d \geq s.\end{gathered} \tag{1}$$

В этом случае $\mathcal{S}$ будет диагональным идеалом в $\mathcal{L}$.

Лемма 1. *Пусть $\mathfrak{L}$ — $\mathbb{Z}_p$-форма алгебры Ли $sl_2(\mathbb{Q}_p)$, определенная соотношениями (1), $H = \frac{ae+bh+cf}{p^m} \in \mathfrak{L}$, $0 < m \le s$.*

1. *Если $n \ge d$, $n - d \equiv 0(2)$ и $p^{n-d}\beta^2 - 2\alpha\gamma \not\equiv 0(p)$, то H полупростой тогда и только тогда, когда $\frac{p^{n-d}\beta^2-2\alpha\gamma}{p} = 1$.*

2. *Если $n \ge d$, $n - d \equiv 1(2)$ и $p^{n-d}\beta^2 - 2\alpha\gamma \not\equiv 0(p)$, то H не является полупростым.*

3. *Если $n < d$ и $\beta \not\equiv 0(p)$, то H полупростой.*

Доказательство. Вначале заметим, что $a \equiv \mu\alpha(p)$, $b \equiv \mu\beta(p)$, $c \equiv \mu\gamma(p)$ и $\mu \not\equiv 0(p)$.

1. Пусть $H = \frac{ae+bh+cf}{p^m} \in \mathfrak{L}$ — полупростой элемент, E — собственный вектор, $E = xe + yh + zf$, $EH = \frac{1}{p^m}(p^n(xb - ya)e + p^d(xc - za)h + p^n(yc - zb)f) = k_h(xe + yh + zf)$. Получаем систему линейных уравнений

$$\begin{cases} (p^{n-m}b - k_h)x - p^{n-m}ay = 0, \\ p^{d-m}cx - k_hy - p^{d-m}az = 0, \\ p^{n-m}cy - (p^{n-m}b + k_h)z = 0. \end{cases} \tag{2}$$

Она имеет ненулевое решение, следовательно, ее определитель равен нулю. Вычисляем его: $(p^{2(n-m)}b^2 - k_h^2)k_h - 2p^{n+d-2m}ack_h = 0$. Так как $k_h \ne 0$, то $p^{2(n-m)}b^2 - k_h^2 - 2p^{n+d-2m}ac = 0$. Разделив последнее равенство на p^{n+d-2m}, получим $p^{n-d}b^2 - 2ac = k^2$, где $k_h = p^{(n+d)/2-m}k$, т. е. $p^{n-d}b^2 - 2ac$ — квадрат в $\mathbb{Z}_p$ и из условия $p^{n-d}b^2 - 2ac \equiv \mu^2(p^{n-d}\beta^2 - 2\alpha\gamma) \not\equiv 0(p)$ получаем $\left(\frac{p^{n-d}\beta^2-2\alpha\gamma}{p}\right) = 1$.

Обратно, положим

$$H = \frac{ae + bh + cf}{p^s}, \quad p^{2t}b^2 - 2ac \not\equiv 0(p), \quad t = \frac{n-d}{2}.$$

Из условий

$$\frac{p^{n-d}\beta^2 - 2\alpha\gamma}{p} = 1, \quad \mu^2(p^{n-d}\beta^2 - 2\alpha\gamma) \equiv p^{n-d}b^2 - 2ac(p)$$

находим, что $p^{n-d}b^2 - 2ac$ — квадрат в $\mathbb{Z}_p$, т. е. $p^{n-d}b^2 - 2ac = k^2$. Тогда

$$E = p^{l_1}\left(\frac{p^t a}{p^t b - k}e + h + \frac{p^t c}{p^t b + k}f\right), \quad F = p^{l_2}\left(\frac{p^t a}{p^t b + k}e + h + \frac{p^t c}{p^t b - k}f\right) \tag{3}$$

— собственные векторы H, где $l_1, l_2 \in \mathbb{N}$, такие, что $E, F \in \mathfrak{L}$, $EH = k_hE$, $FH = -k_hF$, $k_h = p^{\frac{n+d}{2}-s}k$.

2. Пусть $H = \frac{ae+bh+cf}{p^m} \in \mathfrak{L}$ — полупростой элемент. Аналогично п. 1 вычислив определитель системы (2), получим, что $(p^{n-d}b^2 - 2ac)p = k^2$, где $k_h = p^{\frac{n+d-1}{2}-m}k$. Следовательно,

$$p^{n-d}b^2 - 2ac \equiv \mu^2(p^{n-d}\beta^2 - 2\alpha\gamma)(p) \equiv 0(p),$$

откуда $p^{n-d}\beta^2 - 2\alpha\gamma \equiv 0(p)$; противоречие.

3. Пусть $n < d$, $H = \frac{ae+bh+cf}{p^m} \in \mathfrak{L}$. Так как $n < d$ и $b \not\equiv 0(p)$, то $b^2 - 2p^{n-d}ac$ — ненулевой квадрат в $\mathbb{Z}_p$. Положим $b^2 - 2p^{n-d}ac = k^2$. Легко проверить, что

$$E = a(b + k)e + (b^2 - k^2)h + c(b - k)f, \quad F = a(b - k)e + (b^2 - k^2)h + c(b + k)f$$

будут собственными векторами H, $EH = p^{n-m}kE$, $FH = -p^{n-m}kF$. Лемма доказана.

Пусть $\mathfrak{J}$ — подалгебра в $\mathfrak{L}$, $\langle A, B, C\rangle$ — ее базис. Обозначим через $\Delta(A, B, C)$ определитель матрицы перехода от $\langle e, h, f\rangle$ к $\langle A, B, C\rangle$. Тогда легко проверяется, что $[\mathfrak{L} : \mathfrak{J}] = s + \nu_p(\Delta(A, B, C))$.

Лемма 2. *Пусть $\mathcal{L}$ — $\mathbb{Z}_p$-форма алгебры Ли $sl_2(\mathbb{Q}_p)$, определенная соотношениями (1), $n \geq d$, $H = ae + bh + cf \in \mathcal{S}$ — полупростой элемент, E, F — собственные векторы для H. Тогда $\langle E, H, F\rangle \subset \mathcal{S}$.*

Доказательство. Если $n - d \equiv 0(2)$, то возьмем $t = (n-d)/2$ в случае $n - d \equiv 1(2)$, $t = (n-d+1)/2$. Тогда

$$E = p^{l_1}\left(\frac{p^t a}{p^t b - k}e + h + \frac{p^t c}{p^t b + k}f\right), \quad F = p^{l_2}\left(\frac{p^t a}{p^t b + k}e + h + \frac{p^t c}{p^t b - k}f\right)$$

— собственные векторы для H, l_1, l_2 — минимальные числа со свойством $E, F \in \mathcal{L}$. Тогда

$$\Delta(E, H, F) = p^{l_1+l_2}\frac{4p^t k^3}{p^{2t}b^2 - k^2}.$$

Положим

$$\frac{p^t a}{p^t b - k} = p^{m_1}a', \quad \frac{p^t c}{p^t b + k} = p^{m_2}c', \quad a', c' \not\equiv 0(p).$$

Теперь

$$\nu_p(p^{m_1}a'p^{m_2}c') = m_1 + m_2 = \nu_p\left(\frac{p^{2t}ac}{p^{2t}b^2 - k^2}\right) = 2t.$$

Так как $2t \geq 0$, то либо $m_1 \geq 0$, либо $m_2 \geq 0$.

Рассмотрим случай $m_1 \geq 0$, $m_2 < 0$. Пусть $m_2' = -m_2$, тогда

$$E = \frac{p^{m_1+m_2'}a'e + p^{m_2'}h + c'f}{p^{m_2'-l_1}}.$$

Если $m_2' - l_1 > 0$, то из условия $E \in \mathcal{L}$ и $E \notin \mathcal{S}$ получим систему сравнений

$$p^{m_1+m_2'}a' \equiv \lambda\alpha(p^{m_2'-l_1}), \quad p^{m_2'} \equiv \lambda\beta(p^{m_2'-l_1}), \quad c' \equiv \lambda\gamma(p^{m_2'-l_1}).$$

Из последнего сравнения и из $c' \not\equiv 0(p)$ имеем $\lambda \not\equiv 0(p)$. Так как $m_1 + m_2' > 0$ и $m_2' > 0$, то $\alpha, \beta \equiv 0(p)$. Получаем противоречие с условием $p^{n-d}\beta^2 - 2\alpha\gamma \not\equiv 0(p)$. Следовательно, $m_2' - l_1 \leq 0$ и $E \in \mathcal{S}$. Аналогично доказывается, что $F \in \mathcal{S}$.

Случай $m_1 < 0$, $m_2 \geq 0$ рассматривается так же. Лемма доказана.

Теорема 3. *Пусть $\mathcal{L}$ — $\mathbb{Z}_p$-форма алгебры Ли $sl_2(\mathbb{Q}_p)$, определенная соотношениями (1).*

1. *Если $n \geq d$, $n \equiv d(2)$ и $p^{n-d}\beta^2 - 2\alpha\gamma \not\equiv 0(p)$, то $\mathcal{L}$ диагональная тогда и только тогда, когда $n = d$ и $\left(\frac{\beta^2 - 2\alpha\gamma}{p}\right) = 1$.*

2. *Если $n < d$ и $\beta \not\equiv 0(p)$, то $\mathcal{L}$ диагональная.*

Доказательство. 1. Ввиду леммы 2 достаточно рассмотреть случай, когда полупростой элемент вида $H = \frac{ae+bh+cf}{p^s}$ входит в диагональный базис. Из условия $H \in \mathcal{L}$ получаем

$$a \equiv \mu\alpha(p^s), \quad b \equiv \mu\beta(p^s), \quad c \equiv \mu\gamma(p^s), \quad \mu \not\equiv 0(p).$$

По лемме 1 имеем $\left(\frac{b^2-2ac}{p}\right) = 1$, следовательно,

$$\left(\frac{\mu^2(\beta^2 - 2\alpha\gamma)}{p}\right) = \left(\frac{\beta^2 - 2\alpha\gamma}{p}\right) = 1.$$

Пусть $\alpha\gamma \not\equiv 0(p)$, тогда $ac \not\equiv 0(p)$ и

$$E = \frac{1}{p^{l_1}}\left(\frac{p^t a}{p^t b - k}e + h + \frac{p^t c}{p^t b + k}f\right), \quad F = \frac{1}{p^{l_2}}\left(\frac{p^t a}{p^t b + k}e + h + \frac{p^t c}{p^t b - k}f\right)$$

— собственные векторы H. Пусть $l_1 > 0$. Тогда из условия $E \in \mathcal{L}$ и $E \notin \mathcal{S}$ получим систему сравнений

$$\frac{p^t a}{p^t b - k} \equiv \lambda\alpha(p^{l_1}), \quad 1 \equiv \lambda\beta(p^{l_1}), \quad \frac{p^t c}{p^t b + k} \equiv \lambda\gamma(p^{l_1}).$$

Из второго сравнения $\lambda \not\equiv 0(p)$, $\beta \not\equiv 0$, $\lambda \equiv 1/\beta(p)$, и если $t > 0$, то $\alpha/\beta \equiv \gamma/\beta \equiv 0(p)$; противоречие. Следовательно, либо $t = 0$ либо $t \neq 0$ и $l_1 = l_2 = 0$.

Пусть $t = 0$, тогда система сравнений примет вид

$$\frac{a}{b-k} \equiv \frac{\alpha}{\beta}, \quad \frac{c}{b+k} \equiv \frac{c}{\beta}.$$

Перемножая эти сравнения и пользуясь условием $2ac = b^2 - k^2$, получим $\frac{2\alpha\gamma}{\beta^2} \equiv 1(p)$, или $\beta^2 - 2ac \equiv 0(p)$; противоречие. Таким образом, если $\alpha\gamma \not\equiv 0(p)$, то $l_1 = l_2 = 0$.

Из замечания перед леммой 2 $\mathcal{L} = \langle E, H, F\rangle$ в том и только том случае, если $\nu_p(\Delta(E,H,F)) = -s$. Вычисляя $\Delta(E,H,F)$, получим $\Delta(E,H,F) = -\frac{p^t k^3}{p^s ac}$. Так как $ac \not\equiv 0(p)$, $k \not\equiv 0(p)$, то $\nu_p(\Delta(E,H,F)) = t - s$, следовательно, $t = 0$ и $n = d$.

Положим теперь $\alpha\gamma \equiv 0(p)$. Тогда из условия $p^{n-d}\beta^2 - 2\alpha\gamma \not\equiv 0(p)$ следует, что $n = d$, т. е. $t = 0$. Пусть $H = \frac{ae+bh+cf}{p^s}$ — полупростой элемент, $2ac = b^2 - k^2$. Поскольку $p \neq 2$, то либо $b-k \equiv 0(p)$, $b+k \not\equiv 0(p)$, либо $b-k \not\equiv 0(p)$, $b+k \equiv 0(p)$.

Рассмотрим случай $b - k \equiv 0(p)$, $b + k \not\equiv 0(p)$. Тогда

$$E = \frac{1}{p^{l_1}}\left(\frac{a^2}{ac - k(b-k)}e + \frac{a(b-k)}{ac-k(b-k)}h + f\right),$$
$$F = \frac{1}{p^{l_2}}\left(e + \frac{c(b-k)}{ac-k(b-k)}h + \frac{c^2}{ac-k(b-k)}f\right)$$

— собственные векторы H. Заметим, что $ac - k(b-k) \not\equiv 0(p)$.

Пусть $l_1 \neq 0$, тогда из условия $E \in \mathcal{L}$ получим систему сравнений:

$$\frac{a^2}{ac-k(b-k)} \equiv \lambda\alpha(p) \equiv \lambda a(p), \quad \frac{a(b-k)}{ac-k(b-k)} \equiv \lambda\beta(p) \equiv \lambda b(p), \quad 1 \equiv \lambda\gamma(p).$$

Из третьего сравнения вытекает, что $c \not\equiv 0(p)$, значит, $a \equiv 0(p)$, из второго — $a \equiv \frac{b(ac-k(b-k))}{c(b-k)}(p)$, следовательно, $b \equiv 0(p)$ и $b^2 - ac \equiv \beta^2 - \alpha\gamma \equiv 0(p)$; противоречие. Таким образом, $l_1 = 0$; аналогично доказывается, что $l_2 = 0$.

Вычисляя $\Delta(E,H,F)$, получим

$$\Delta(E,H,F) = \frac{k^3(b-k)^3}{p^s(ac-k(b-k))^2}.$$

Так как $k, b-k$ и $ac - k(b-k)$ не делятся на p, то $\nu_p(\Delta(E,H,F)) = -s$ и, следовательно, $\mathcal{L}$ диагональная. Случай $b - k \not\equiv 0(p)$, $b + k \equiv 0(p)$ разбирается полностью аналогично.

2. Пусть $H = \frac{ae+bh+cf}{p^s}$. По лемме 1 H — полупростой элемент. Предположим, что $b - k \not\equiv 0(p)$, $b + k \equiv 0(p)$ и собственные векторы H определены следующими формулами:

$$E = \left(\frac{p^{d-n}a^2}{p^{d-n}ac - k(b-k)}e + \frac{p^{d-n}a(b-k)}{p^{d-n}ac-k(b-k)}h + f\right),$$
$$F = \left(e + \frac{p^{d-n}c(b-k)}{p^{d-n}ac-k(b-k)}h + \frac{p^{d-n}c^2}{p^{d-n}ac-k(b-k)}f\right).$$

Проверим, что E, H, F — базис $\mathfrak{L}$.

Действительно,

$$\Delta(E,H,F) = \frac{k^3(b-k)^3}{p^s(p^{d-n}ac - k(b-k)^2)}.$$

Так как $k \not\equiv 0(p)$ и $b-k \not\equiv 0(p)$, то $\nu_p(\Delta(E,H,F)) = -s$, следовательно, E, H, F образуют базис $\mathfrak{L}$.

В случае $b-k \not\equiv 0(p), b+k \equiv 0(p)$ собственными векторами H будут

$$E = \left(\frac{p^{d-n}a^2}{p^{d-n}ac - k(b+k)}e + \frac{p^{d-n}a(b+k)}{p^{d-n}ac - k(b+k)}h + f\right),$$
$$F = \left(e + \frac{p^{d-n}c(b+k)}{p^{d-n}ac - k(b+k)}h + \frac{p^{d-n}c^2}{p^{d-n}ac - k(b+k)}f\right).$$

Аналогично предыдущему случаю показывается, что $\nu_p(\Delta(E,H,F)) = -s$. Теорема доказана.

Пусть $n \geq d$ и $p^{n-d}\beta^2 - 2\alpha\gamma \not\equiv 0(p)$. Выясним, когда элемент $u_1e+u_2h+u_3f$ принадлежит идеалу $\langle E,H,F\rangle$, где $H = \frac{ae+bh+cf}{p^s}$ — полупростой элемент с соответствующими собственными векторами E, F, заданными формулами (3). Кроме того, при доказательстве теоремы 3 было показано, что $l_1 = l_2 = 0$. Поскольку $xE + yH + zF = u_1e + u_2h + u_3f$, то

$$\frac{p^ta}{p^tb-k}x + \frac{a}{p^s}y + \frac{p^ta}{p^tb+k}z = u_1, \quad x + \frac{b}{p^s}y + z = u_2, \quad \frac{p^tc}{p^tb+k}x + \frac{c}{p^s}y + \frac{p^tc}{p^tb-k}z = u_3.$$

При решении системы получим

$$\begin{aligned} x &= \frac{1}{2k^2p^t}((p^tb+k)cu_1 + (p^tb-k)au_3 - 2acp^tu_2), \\ y &= -\frac{p^s}{k^2}(cu_1 + au_3 - p^{2t}bu_2), \\ z &= \frac{1}{2k^2p^t}((p^tb-k)cu_1 + (p^tb+k)au_3 - 2acp^tu_2). \end{aligned} \tag{4}$$

Предложение 1. *Пусть $\mathfrak{L}$ — недиагональная $\mathbb{Z}_p$-форма алгебры Ли $sl_2(\mathbb{Q}_p)$, определенная соотношениями* (1), *$n \geq d$, $n-d \equiv 0(2)$, $p^{n-d}\beta^2 - 2\alpha\gamma \not\equiv 0(p)$, $t = (n-d)/2$, $H = \frac{ae+bh+cf}{p^s}$, $\langle E,H,F\rangle$ — максимальный диагональный идеал. Тогда $\langle p^te, h, p^tf\rangle \subset \langle\ E,H,F\rangle$ и для любого $l < t$ элементы p^le, p^lf не принадлежат идеалу $\langle E,H,F\rangle$.*

Доказательство. Пусть $t = 0$. Тогда из предыдущей теоремы и леммы 1 получаем, что в $\mathfrak{L}$ нет диагональных идеалов вида $\langle E,H,F\rangle$, где $H = \frac{ae+bh+cf}{p^s}$. Пусть теперь $t \neq 0$, тогда $ac \not\equiv 0(p)$. Из формул (4), где $e = xE + yH + zF$, имеем

$$x = \frac{1}{2k^2p^t}(p^tb+k)c, \quad y = -\frac{p^s}{k^2}c, \quad z = \frac{1}{2k^2p^t}(p^tb-k)c,$$

$$\nu_p(x) = -t, \quad \nu_p(y) = s, \quad \nu_p(z) = -t.$$

Следовательно, $p^te \in \langle E,H,F\rangle$ и $p^le \notin \langle E,H,F\rangle$ для любого $l < t$. То, что $h, p^tf \in \langle E,H,F\rangle$, проверяется аналогично. Предложение доказано.

Теорема 4. *Пусть $\mathcal{L}$ — недиагональная $\mathbb{Z}_p$-форма алгебры Ли $sl_2(\mathbb{Q}_p)$, определенная соотношениями* (1), $p^{n-d}\beta^2 - 2\alpha\gamma \not\equiv 0(p)$.

1. *Пусть* $n > d$, $n - d \equiv 1(2)$. *Тогда* $\mathcal{S}$ *— единственный максимальный диагональный идеал в* $\mathcal{L}$.

2. *Пусть* $n \geq d$, $\left(\frac{p^{n-d}b^2-2ac}{p}\right) = -1$. *Тогда* $\mathcal{S}$ *— единственный максимальный диагональный идеал в* $\mathcal{L}$.

3. *Пусть* $n > d$, $n - d \equiv 0(2)$, $\left(\frac{-2ac}{p}\right) = 1$. *Тогда все максимальные диагональные идеалы в* $\mathcal{L}$ *имеют вид либо* $\mathcal{S}$, *либо* $\langle E, H, F\rangle$, *где* $H = \frac{ae+bh+cf}{p^s}$ *полупростой,* E, F *собственные для* H.

При этом если $H' = \frac{a'e+b'h+c'f}{p^s}$ *— другой полупростой элемент, то* $\langle E, H, F\rangle = \langle E', H', F'\rangle$ *тогда и только тогда, когда* $ac' \equiv a'c(p^{s+(n-d)/2})$.

Доказательство. Случаи 1 и 2 непосредственно следуют из лемм 1 и 2.

Рассмотрим случай 3. Возьмем полупростой элемент $H = \frac{ae+bh+cf}{p^s}$ и соответствующий идеал $\langle E, H, F\rangle$. Из предложения 1 получаем $\langle e, h, f\rangle \not\subset \langle E, H, F\rangle$. Следовательно, $\langle e, h, f\rangle$ — максимальный диагональный идеал в $\mathcal{L}$.

Далее, пусть $H' = \frac{a'e+b'h+c'f}{p^s}$ — другой полупростой элемент, $\langle E', H', F'\rangle$ — соответствующий ему идеал. Выясним, когда $E', H', F' \in \langle E, H, F\rangle$.

Пусть $E' = xE + yH + zF$. Из (4) получаем

$$x = \frac{1}{2k^2p^t}\left((p^tb + k)c\frac{p^ta'}{p^tb' - k'} + (p^tb - k)a\frac{p^tc'}{p^tb' + k'} - 2acp^t\right) \in \mathbb{Z}_p,$$

аналогично выводим, что $z, y \in \mathbb{Z}_p$, т. е. $E' \in \langle E, H, F\rangle$. Те же рассуждения проводим для $H' = \frac{a'e+b'h+c'f}{p^s}$. Предварительно заметим, что $a' \equiv \mu a(p^s)$, $b' \equiv \mu b(p^s)$, $c' \equiv \mu c(p^s)$, $\mu \not\equiv 0(p)$.

Пусть $H' = xE + yH + zF$. Из формул (4) получим

$$x = \frac{1}{2k^2}\left(\mu(bca_2 + bac_2 - 2acb_2) - \frac{k}{p^{s+t}}(ca' - c'a)\right),$$

аналогично вычисляем z. Таким образом, $x, z \in \mathbb{Z}_p$ тогда и только тогда, когда $ca' - c'a \equiv 0(p^{s+t})$. Коэффициент

$$y = \frac{p^s}{2k^2}\left(c\frac{a'}{p^s} + a\frac{c'}{p^s} - p^{2t}b\frac{b'}{p^s}\right)$$

всегда принадлежит $\mathbb{Z}_p$.

Следовательно, $H' \in \langle E, H, F\rangle$ тогда и только тогда, когда $ca' - c'a \equiv 0(p^{s+t})$; симметрично получаем $H \in \langle E', H', F'\rangle$ тогда и только тогда, когда $ca' - c'a \equiv 0(p^{s+t})$. Теорема доказана.

3. Представления кольца Ли $sl_2(\mathbb{Z})$**.** Положим $R = sl_2\mathbb{Z}$, p — произвольное простое число. Обозначим через $\mathcal{O}$ категорию $sl_2\mathbb{Z}$-модулей конечного типа без кручения. Пусть $M \in \mathcal{O}$, тогда $M_\mathbb{Q} = M \otimes_\mathbb{Z} \mathbb{Q}$ будет конечномерным $sl_2\mathbb{Q}$-модулем, причем $\dim M = \dim_\mathbb{Q}(M_\mathbb{Q})$. Определим также $sl_2(\mathbb{Z}_p)$-модуль $M_p = M \otimes_\mathbb{Z} \mathbb{Z}_p$.

Зафиксируем в R стандартный базис $\{e, h, f\}$, где $eh = 2e$, $ef = h$, $fh = -f$. Введем обозначение: $M = \langle w_0, \dots, w_k\rangle$, если элементы $w_0, \dots, w_k$ образуют базис модуля M.

Пусть V — $sl_2\mathbb{Q}$-модуль; выберем в нем некоторый базис $\langle w_0, \dots, w_k\rangle$ так, чтобы действие e, h, f определялось с целыми коэффициентами. Тогда мы можем рассмотреть R-модуль $V_\mathbb{Z} = \langle w_0, \dots, w_k\rangle$, который будем называть *редукцией модуля V по базису $w_0, \dots, w_k$*.

R-модуль M будем называть *неприводимым*, если соответствующий $sl_2\mathbb{Q}$-модуль $M_\mathbb{Q} = M \otimes_\mathbb{Z} \mathbb{Q}$ неприводим.

Хорошо известно, что существует единственный неприводимый $(m+1)$-мерный $sl_2\mathbb{Q}$-модуль $V_\mathbb{Q}$, который можно задать, например, следующим образом: $V_\mathbb{Q} = \langle v_0, \dots, v_m\rangle$, где

$$v_ie = v_{i+1}, \quad v_me = 0, \quad v_ih = (m-2i)v_i, \quad v_if = -i(m-i+1)v_{i-1}.$$

Редукцию модуля $V_\mathbb{Q}$ по этому базису назовем *стандартным R-модулем размерности $m+1$*. Пусть $M \in \mathcal{O}$ — произвольный неприводимый $(m+1)$-мерный модуль; тогда $M_\mathbb{Q} \cong V_\mathbb{Q}$.

Модуль D назовем *диагональным*, если он имеет базис из собственных векторов h, т. е. $D = \langle d_0, \dots, d_s \mid \exists k_i \in \mathbb{Z}\ d_ih = k_id_i\rangle$. Обозначим через M_d максимальный диагональный подмодуль в M. Очевидно, что M_d порождается множеством всех собственных векторов $\{v \in M \mid \exists k \in \mathbb{Z}\ vh = kv\}$. Заметим, что если M неприводимый, то M_d также неприводим.

Следующее предложение полностью описывает неприводимые диагональные R-модули.

Предложение 2. *Пусть $\alpha = (\alpha_0, \dots, \alpha_{m-1}) \in \mathbb{Z}^n_+$ таков, что $(i+1)(m-i)/\alpha_i = \beta_{i+1} \in \mathbb{Z}$. Определим модуль $D(\alpha) = \langle d_0, \dots, d_m\rangle$ следующим образом:*

$$d_ie = \alpha_id_i, \quad d_me = 0, \quad d_if = \beta_id_{i-1}, \quad d_ih = (m-2i)d_i, \quad i = 0, \dots, m.$$

Тогда $D(a)$ — неприводимый диагональный R-модуль и все неприводимые диагональные модули из $\mathcal{O}$ могут быть получены таким образом для некоторого α. При этом $D(\alpha) \cong D(\gamma)$ тогда и только тогда, когда $\alpha = \gamma$.

Доказательство. То, что $D(\alpha)$ будет R-модулем, проверяется прямым вычислением. Неприводимость следует по определению, так как $D(\alpha)_\mathbb{Q} \cong V_\mathbb{Q}$.

Пусть $W \in \mathcal{O}$ — неприводимый диагональный модуль. Тогда $W_\mathbb{Q} \cong V_\mathbb{Q}$; будем считать, что $W_\mathbb{Q} = V_\mathbb{Q}$. Положим $W = \langle w_0, \dots, w_m\rangle$ и $w_i = x_iv_i$, где $x_i \in \mathbb{Q}$. Здесь $w_ie = (x_iv_i)e = x_iv_{i+1} = (x_i/x_{i+1})w_{i+1}$, откуда $\alpha_i = (x_i/x_{i+1}) \in \mathbb{Z}$. Кроме того,

$$w_if = (x_iv_i)f = -x_ii(m-i+1)v_{i-1} = -(x_ii(m-i+1)/x_{i-1})w_{i+1}$$

и $\beta_i = -(x_ii(m-i+1)/x_{i-1}) \in \mathbb{Z}$. Далее,

$$\alpha_i\beta_{i+1} = -(x_i/x_{i+1})(x_{i+1}(i+1)(m-i)/x_i) = -(i+1)(m-i).$$

Следовательно, $W = D(\alpha)$.

Пусть $M_1 = D(\alpha)$, $M_2 = D(\gamma)$, $M_1 \cong M_2$ и $\varphi : M_1 \to M_2$ — изоморфизм. Рассмотрим $M_1 = \langle w_0, \dots, w_m\rangle$, $M_2 = \langle u_0, \dots, u_m\rangle$ — соответствующие диагональные базисы. Тогда очевидным образом $\varphi(w_i) = x_iu_i$, причем $x_i = p^m1$. Рассмотрим элемент $\varphi(w_ie) = \varphi(\alpha_iw_{i+1}) = \alpha_ix_{i+1}u_{i+1}$. С другой стороны, $\varphi(w_ie) = \varphi(w_i)e = x_iu_ie = x_i\gamma_iu_{i+1}$; получим $\alpha_i = p^m\gamma_i$, и так как $\alpha_i, \gamma_i > 0$, то $\alpha_i = \gamma_i$. Значит, $\alpha = \gamma$. Предложение доказано.

Лемма 3. *Пусть $M \in \mathcal{O}$ — неприводимый R-модуль. Тогда существует константа $c \in \mathbb{Z}$, зависящая только от $\dim M$, такая, что $cV \subset M \subset V$, где V — стандартный R-модуль.*

Доказательство. Положим $M = \langle w_0, \dots, w_m \rangle$. Так как $M_{\mathbb{Q}} \cong V_{\mathbb{Q}}$, мы можем отождествить модуль M с подмодулем V. Действительно, $w_i = \sum a_{ij} v_j$, где $a_{ij} \in \mathbb{Q}$. Обозначим общий знаменатель элементов a_{ij} через a, вместо модуля V возьмем $\frac{1}{a}V$. Тогда $w_i = \sum a a_{ij} v_j$, но уже $a a_{ij} \in \mathbb{Z}$. Аналогичным образом показывается, что можно выбрать V так, что a_{ij} будут взаимно просты, т. е. $(a_{ij}) = 1$.

Рассмотрим равенства

$$w_i f^k e^m f^s = \left(\sum a_{ij} v_j\right) f^k e^m f^s = a_{ik} \beta_k \dots \beta_1 \beta_m \dots \beta_{m-s} v_{m-s} \in M,$$

где $\beta_i = -i(m - i + 1)$.

Положим

$$c = (\beta_1 \dots \beta_m)^2 = \left(\prod_{i=0}^{m-1} (i+1)(m-i)\right)^2,$$

тогда $a_{ik} c v_j \in M$ для любых $i, j, k \in 0, \dots, m$, и так как мы выбрали $(a_{ij}) = 1$, получаем $c v_j \in M$ для любого $i \in 0, \dots, m$. Следовательно, $cV \subset M \subset V$. Лемма доказана.

Предложение 3. *Пусть $M \in \mathcal{O}$ — конечномерный R-модуль без кручения. Тогда существуют диагональный модуль D и константа c, зависящая только от* $\dim M$, *такие, что $cD \subset M \subset D$.*

Доказательство. Рассмотрим модуль $M = \langle w_0, \dots, w_m \rangle$. Модуль $M_{\mathbb{Q}}$ вполне приводим, следовательно, $M_{\mathbb{Q}} = V_0 \oplus \dots \oplus V_k$, где V_i — неприводимый $sl_2\mathbb{Q}$-модуль. Выберем в V_i диагональные базисы так, чтобы w_j выражались с целыми коэффициентами. Обозначим через N_i редукции модулей V_i по этим базисам. Тогда N_i будет неприводимым диагональным R-модулем и модуль M вкладывается в прямую сумму N_i; $M \subset N_1 \oplus \dots \oplus N_k$.

Модуль $M \cap N_i$ неприводим, следовательно, по предыдущей лемме существует такая константа c_i, что $c_i V_i \subset M \cap N_i \subset V_i$, здесь V_i — стандартный R-модуль некоторой размерности. Положим $D = V_0 \oplus \dots \oplus V_k$ и $c = \prod c_i$. Тогда $cD \subset M \subset D$. Предложение доказано.

Следствие. *Конечномерных без кручения $sl_2\mathbb{Z}$-модулей конечное число в каждой размерности.*

В следующей теореме показывается локально-глобальный принцип для $sl_2\mathbb{Z}$-модулей.

Теорема 5. *Пусть $M, N \in \mathcal{O}$ — неприводимые конечномерные $sl_2\mathbb{Z}$-модули без кручения. Тогда $M \cong N$ в том и только том случае, если $M_p \cong N_p$ для каждого простого числа p.*

Доказательство. Вначале докажем теорему в случае диагональных модулей

Пусть $M = D(\alpha)$, $N = D(\gamma)$, $M = \langle d_0, \dots, d_m \rangle$, $M = \langle c_0, \dots, c_m \rangle$. Предположим, что для каждого простого p $M_p \cong N_p$ и $\varphi_p : M_p \to N_p$ — соответствующие изоморфизмы. Легко проверяется, что $\varphi_p(d_i) = x_{p,i} c_i$, причем $x_{p,i}$ обратим в $\mathbb{Z}_p$, т. е. $p \nmid x_{p,i}$. Тогда $\varphi_p(d_i e) = \varphi_p(\alpha_i d_{i+1}) = \alpha_i x_{p,i+1} c_{i+1}$. С другой стороны, $\varphi_p(d_i e) = \varphi_p(d_i) e = \gamma_i x_{p,i} c_{i+1}$, значит, $\alpha_i = y_{p,i} \gamma_i$ в $\mathbb{Z}_p$, где $y_{p,i} = x_{p,i} / x_{p,i+1}$,

$p \nmid y_i$. Отсюда следует, что $\alpha_i = y_i\gamma_i$ в $\mathbb{Z}$, а из условия для любого p, $p \nmid y_{p,i}$, получаем, что $p \nmid y_i$ в $\mathbb{Z}$ для любого p. Следовательно, $y_i = p^m 1$ и $\alpha_i = p^m\gamma_i$. Так как $\alpha_i, \gamma_i > 0$, то $\alpha_i = \gamma_i$ и по предложению 2 $M = N$.

В случае диагональных модулей теорема доказана.

Пусть $M, N \in \mathcal{O}$ — произвольные неприводимые модули. Пусть $C = M_d$, $D = N_d$ — максимальные диагональные подмодули в M, N. Тогда C_p, D_p будут максимальными диагональными подмодулями соответственно в M_p и N_p. Из условия $M_p \cong N_p$ для любого p получаем, что $C_p \cong D_p$ для любого p, и по только что доказанному это эквивалентно $C \cong D$.

В дальнейшем мы можем отождествить максимальные диагональные подмодули в M и N; $M_d = N_d = D = \langle d_0, \dots, d_m \rangle$.

Обозначим через $\varphi_p : M_p \to N_p$ соответствующие изоморфизмы над $\mathbb{Z}_p$. Тогда $\varphi_p(D) = D$.

Пусть $m \in M$; так как $M_{\mathbb{Q}} = D_{\mathbb{Q}}$, то m можно выразить через d_i, $m = \sum a_i d_i$, $a_i \in \mathbb{Q}$. Обозначим через a общий знаменатель a_i, тогда $am \in D$ и отсюда вытекает, что $\varphi_p(am) = am$, следовательно, $\varphi_p(m) = m \in N_p$.

Осталось доказать, что если $m \in N_p$ при любом простом p, то $m \in N$.

Положим $N = \langle n_0, \dots, n_m \rangle$. Так как $M_{\mathbb{Q}} = N_{\mathbb{Q}}$, то $m = \sum x_i n_i$, где $x_i \in \mathbb{Q}$. С другой стороны, из условия $m \in N_p$ получаем

$$m = \sum b_{p,i} n_i, \quad b_{p,i} \in \mathbb{Z}_p.$$

Таким образом, $x_i \in \mathbb{Z}_p$ для любого простого p, откуда $x_i \in \mathbb{Z}$. Таким образом, $m \in N$. Теорема доказана.

ТЕРАТУРА

1. *Джекобсон Н.* Алгебры Ли. М.: Мир, 1964.
2. *Боревич З. И. Шафаревич И. Р.* Теория чисел. М.: Наука, 1985.
3. *Ющенко А. В.* $\mathbb{Z}_p$-формы алгебры Ли $sl_2(\mathbb{Q}_p)$ // Вестн. Омского ун-та. 1999. Т. 1. С. 19–21.

Статья поступила 1 декабря 1999 г.

Ющенко Александр Викторович
Омский гос. университет, кафедра алгебры, пр. Мира, 55-А, Омск 644077
yuschenk@univer.omsk.su