Наш семинар: математические сюжеты

Заметки об исключительных изоморфизмах

В. В. Доценко

Эрнесту Борисовичу Винбергу к юбилею,
с уважением и восхищением

Введение

Предметом предлагаемого читателю текста является некоторая разновидность «математической зоологии». А именно, я приведу довольно простые и элегантные конструкции некоторых «исключительных изоморфизмов» (так традиционно называются изоморфизмы между двумя группами из известных серий групп, сами по себе не образующие серию), и опишу ситуации, в которых простой конструкции не известно, в надежде, что кому-то из читателей удастся заполнить имеющиеся тут пробелы.

Я признателен всем моим друзьям и коллегам, с кем я обсуждал в разные моменты вопросы, затрагиваемые здесь. Особо я хочу поблагодарить М. Финкельберга, который сообщил эффектное (и, возможно, совершенно новое) доказательство изоморфизма $PSL_2(\mathbb{F}_9) \simeq A_6$, и М. Вялого, который предложил красивый путь доказательства изоморфизма $Sp_4(\mathbb{F}_2) \simeq \simeq S_6$, вдохновивший меня на доказательство изоморфизма $GL_4(\mathbb{F}_2) \simeq A_8$. Столь изящное рассуждение не имело шанса быть совершенно новым: как выяснилось в ходе написания этого текста, мы переоткрыли результаты статьи [4], и опубликованное здесь доказательство по существу не отличается от приведённого в той статье. После того, как первая версия текста

была представлена в редакцию, Э. Б. Винберг сообщил мне ряд комментариев и уточнений, которые сделали некоторые доказательства и структуру текста в целом значительно более прозрачными, за что я ему чрезвычайно признателен.

Серии конечных групп, которым мы уделяем тут наибольшее внимание, суть симметрические группы S_n, знакопеременные группы A_n и проективные группы симметрий $PGL_n(\Bbbk)$ и $PSL_n(\Bbbk)$, в случае, когда $\Bbbk = \mathbb{F}_q$ — конечное поле из q элементов. Группы S_n и A_n хорошо известны всем, кто имел дело с понятием группы. Что касается проективных групп, они могут быть известны не всем читателям, и мы напомним их определение.

Определение 1. Общая (соответственно, специальная) линейная группа $GL_n(\Bbbk)$ (соответственно, $SL_n(\Bbbk)$) — это группа всех обратимых матриц с элементами из поля $\Bbbk$ (соответственно, всех матриц с коэффициентами из поля $\Bbbk$ и с определителем 1).

Будучи интересными сами по себе, такие группы не имеют шанса быть изоморфными симметрическим и знакопеременным группам, потому что обычно имеют нетривиальный центр (элементы, которые перестановочны со всеми элементами группы).

Упражнение. Проверьте, что центр каждой из этих групп состоит из скалярных матриц (т. е. матриц, кратных единичной).

Определение 2. Проективная общая линейная группа $PGL_n(\Bbbk)$ — это факторгруппа группы $GL_n(\Bbbk)$ по ее центру. Проективная специальная линейная группа $PSL_n(\Bbbk)$ — это образ группы $SL_n(\Bbbk)$ в $PGL_n(\Bbbk)$ при гомоморфизме факторизации.

Геометрический смысл этих групп такой. Каждая из них действует на n-мерном векторном пространстве над полем $\Bbbk$. Если рассматривать точки этого пространства с точностью до одновременного умножения всех их координат на ненулевое число, т. е. перейти к множеству прямых, проходящих через начало координат, мы получим $(n-1)$-мерное проективное пространство над полем $\Bbbk$. Наши группы, будучи факторгруппами по подгруппе, которая сохраняет все прямые, которые проходят через начало координат, действуют на этом проективном пространстве автоморфизмами. Это будет очень существенно для нас.

Приведем для использования в дальнейшем несколько стандартных фактов. Все они не очень сложно доказываются, и мы предлагаем читателю доказать их самостоятельно или обратиться к стандартным учебникам ([2], [3], [5]) за доказательствами.

Порядки линейных и проективных групп читатель легко вычислит в качестве упражнения, доказав тем самым следующее предложение.

Предложение 1.

$$\#GL_n(\mathbb{F}_q) = (q^n - 1)(q^n - q) \cdot \ldots \cdot (q^n - q^{n-1}),$$
$$\#SL_n(\mathbb{F}_q) = \frac{1}{q-1}(q^n - 1)(q^n - q) \cdot \ldots \cdot (q^n - q^{n-1}),$$
$$\#PGL_n(\mathbb{F}_q) = \frac{1}{q-1}(q^n - 1)(q^n - q) \cdot \ldots \cdot (q^n - q^{n-1}),$$
$$\#PSL_n(\mathbb{F}_q) = \frac{1}{(q-1)\,(n, q-1)}(q^n - 1)(q^n - q) \cdot \ldots \cdot (q^n - q^{n-1})$$

Следующее предложение (тоже предлагаемое в качестве упражнения) тоже не очень сложно и довольно стандартно.

Предложение 2.

1. *Группы A_n просты*[1)] *при $n \geqslant 5$.*
2. *Нормальные подгруппы группы S_n при $n \geqslant 5$ суть $\{e\}$, A_n и S_n.*
3. *Группы $PSL_n(\mathbb{F}_q)$ просты при $n \geqslant 3$ и при $n = 2$, $q > 3$.*
4. *Нормальная подгруппа группы $PGL_n(\mathbb{F}_q)$ либо равна $\{e\}$, либо содержит $PSL_n(\mathbb{F}_q)$ во всех случаях кроме $n = 2$, $q = 2, 3$.*

Это предложение демонстрирует дополнительную причину интересоваться изоморфизмами между данными группами. Классификация конечных простых групп является одним из центральных вопросов теории групп, и для двух бесконечных списков простых групп хотелось бы знать, насколько эти списки пересекаются.

Схема доказательств в большинстве обсуждаемых нами случаев одна и та же. Чтобы доказать, что две группы G и H изоморфны, мы сначала строим гомоморфизм $\varphi\colon G \to H$. Далее мы проверяем инъективность или сюръективность этого гомоморфизма и привлекаем знания о порядках наших групп, чтобы установить, что построенный гомоморфизм в действительности является изоморфизмом.

От геометрии к алгебре

В этом разделе мы для построения гомоморфизмов используем естественное действие проективных групп на соответствующих пространствах, находя подходящие геометрические объекты, на которых эти группы действуют.

В простейших примерах естественное действие проективных преобразований приводит к успеху. Напомним, что преобразование из $PGL_2(\Bbbk)$,

---

[1)] Т. е. не имеют нетривиальных нормальных подгрупп.

которое сохраняет все точки проективной прямой (их в случае конечного поля $1 + \#\Bbbk$), тождественно, и потому естественный гомоморфизм из $PGL_2(\mathbb{F}_q)$ в S_{q+1} инъективен.

Предложение 3.

$$\begin{gathered} PGL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) = GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) \simeq S_3, \\ PGL_2(\mathbb{F}_3) \simeq S_4, \\ PSL_2(\mathbb{F}_3) \simeq A_4, \\ PSL_2(\mathbb{F}_4) = PGL_2(\mathbb{F}_4) \simeq A_5. \end{gathered}$$

Доказательство. Центр группы матриц над полем $\mathbb{F}_2$ тривиален, а определитель обратимой матрицы может быть равен только единице, так что

$$PGL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) = GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2).$$

Порядок группы $GL_2(\mathbb{F}_2)$ равен 6, так что естественный гомоморфизм в S_3 является изоморфизмом.

Порядок группы $PGL_2(\mathbb{F}_3)$ равен 24, и потому гомоморфизм в S_4 является изоморфизмом. В случае группы $PSL_2(\mathbb{F}_3)$ можно использовать то, что у S_4 только одна подгруппа индекса 2, или найти в $PSL_2(\mathbb{F}_3)$ цикл длины 3, или рассуждать каким-либо иным способом.

Порядок группы $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4)$ равен 60. Поэтому образ этой группы при естественном гомоморфизме в S_5 — подгруппа индекса 2 (которая обязательно нормальна). Чтобы доказать, что эта подгруппа есть A_5, можно рассуждать разными способами. Теоретико-групповой подход говорит, что пересечение этой подгруппы с A_5 — нормальная подгруппа, и предложение 2 позволяет этим завершить доказательство. Геометрический подход подсказывает более простое рассуждение. Проективное преобразование может перевести любые три точки в любые три. Возьмем три точки A, B и C и циклически переставим их проективным преобразованием. Это даст нам в образе гомоморфизма либо тройной цикл (ABC) (а потому все тройные циклы в силу нормальности подгруппы и все четные подстановки, поскольку A_n порождается тройными циклами), либо перестановку с цикловым типом $(ABC)(DE)$, квадрат которой — тройной цикл.

Следующее рассуждение является несколько более тонким.

Предложение 4.

$$\begin{gathered} PGL_2(\mathbb{F}_5) \simeq S_5, \\ PSL_2(\mathbb{F}_5) \simeq A_5. \end{gathered}$$

Доказательство. Порядок группы $PGL_2(\mathbb{F}_5)$ равен 120. Действие на точках проективной прямой дает гомоморфизм из $PGL_2(\mathbb{F}_5)$ в S_6. Дальнейшее наше рассуждение не использует геометрию и является чисто теоретико-групповым. Мы докажем, что вообще любая подгруппа $H \subset \subset S_6$ порядка 120 изоморфна S_5. А именно, рассмотрим множество смежных классов S_6/H. Действие S_6 сдвигами на множестве смежных классов приводит к гомоморфизму $\alpha\colon S_6 \to S_6$ (поскольку смежных классов ровно 6). Попробуем выяснить, каково ядро этого гомоморфизма. Это нормальная подгруппа. Нормальные подгруппы в S_6 суть $\{e\}$, A_6 и S_6. Действие группы на смежных классах по подгруппе транзитивно, поэтому два последних варианта отпадают. Значит, α является изоморфизмом. Осталось заметить, что при действии на смежных классах по подгруппе стабилизатор точки изоморфен этой подгруппе. Стабилизатор же точки для обычного действия S_6 на 6-элементном множестве есть S_5. Значит, исходная подгруппа H изоморфна S_5. Отметим, что эта подгруппа S_5 не сопряжена стандартному вложению S_5, поскольку ее действие транзитивно (и потому не имеет неподвижных точек).

Утверждение о группе $PSL_2(\mathbb{F}_5)$ проще всего доказать с помощью предложения 2: в S_5 ровно одна подгруппа индекса 2.

Предложение 5. *$PSL_2(\mathbb{F}_9) \simeq A_6$.*

Доказательство. Порядок группы $PSL_2(\mathbb{F}_9)$ равен 360. Поэтому достаточно построить нетривиальный гомоморфизм этой группы в S_6 (он будет инъективен в силу простоты групп PSL, а единственной подгруппой индекса 2 в S_6 является A_6). Мы сделаем это, предъявив подгруппу $H \subset PSL_2(\mathbb{F}_9)$ индекса 6 (тогда гомоморфизм возникнет из действия на смежных классах по этой подгруппе). Подгруппа индекса 6 в A_6 изоморфна A_5 (это доказывается аналогично тому, что подгруппа индекса 6 в S_6 изоморфна S_5; см. доказательство предложения 4), так что мы и будем искать подгруппу A_5. Хорошо известно, что A_5 изоморфна группе вращений додекаэдра, поэтому она действует на двумерной сфере в $\mathbb{R}^3$. Теперь главное — правильно эту сферу интерпретировать. Легко понять, что группа вращений додекаэдра вкладывается в группу симметрий сферы, понимаемой как сфера Римана (комплексная проективная прямая), то есть в $PSL_2(\mathbb{C})$. Можно проверить, что это вложение определено над $\mathbb{Q}(\sqrt[5]{1}) = \mathbb{Q}(\sqrt{5}, i)$, и потому можно рассмотреть его по модулю 3, что приведет к вложению $A_5 = PSL_2(\mathbb{F}_5)$ в $PSL_2(\mathbb{F}_9)$, поскольку $\mathbb{F}_9 = \mathbb{F}_3(i)$, а $\sqrt{5} \equiv \sqrt{-1} = i \pmod 3$.

Задача*. Можно ли придумать аналогичное рассуждение, которое использует изоморфизм A_5 и $PSL_2(\mathbb{F}_4)$?

Задача*. Можно ли, используя двумерные комплексные представления групп $SL_2(\mathbb{F}_q)$, доказать изоморфизм $PSL_2(\mathbb{F}_4) \simeq PSL_2(\mathbb{F}_5)$ напрямую?

Замечание 1. Доказанные ранее утверждения могут навести читателя на мысль, что имеет место и изоморфизм $PGL_2(\mathbb{F}_9) \simeq S_6$. Это неверно (попробуйте понять, почему).

Интермедия: внешний автоморфизм S_6, простые группы небольших порядков и всё такое

В этом разделе мы извлечем из обсуждавшихся доказательств (да-да, именно из доказательств, а не из доказанного) следствия, которые могут быть интересны любителям теории групп. Во втором из них полезны знания из университетского курса алгебры (теоремы Силова).

Следствие 1. *У группы S_6 существует внешний (не внутренний, то есть не задаваемый сопряжением никаким элементом) автоморфизм.*

Доказательство. Таким автоморфизмом является отображение α из доказательства предложения 4. В самом деле, прообраз стандартного вложения S_5 является подгруппой без общей неподвижной точки, и потому этот автоморфизм не может быть внутренним.

Построенный нами внешний автоморфизм сам по себе является исключительным. Чтобы продемонстрировать это, мы докажем следующее утверждение.

Предложение 6. *При $n \neq 6$ любой автоморфизм группы S_n является внутренним.*

Доказательство. Ясно, что автоморфизм переводит сопряженные элементы в сопряженные элементы. Наше доказательство будет состоять из двух частей. Чтобы доказать, что автоморфизм является внутренним, мы проверим, что транспозиции переходят в транспозиции, после чего убедимся, что автоморфизм, переводящий транспозиции в транспозиции, обязательно внутренний.

Всякая транспозиция является инволюцией (в квадрате равна единице), поэтому класс сопряженности транспозиции переходит в класс сопряженности произведения нескольких непересекающихся транспозиций. Пусть этих транспозиций $k \leqslant n/2$. Вычислим число элементов в соответствующем классе (здесь и далее можно считать, что $n \geqslant 4$, чтобы в S_n были нетривиальные инволюции). Это число равно индексу централизатора такого элемента, т. е. $\dfrac{n!}{k!2^k(n-2k)!}$, что, очевидно, не меньше (а при $k > 1$ — больше), чем $\dfrac{n!}{(2k)!(n-2k)!} = C_n^{2k}$. Число транспозиций равно C_n^2. Поскольку числа сочетаний при фиксированном n возрастают до середины строки, C_n^2 не меньше, чем C_n^{2k}, только если $2k$ равно одному из чисел

$2, n-2, n-1, n$. Если $2k = 2$, то всё доказано. В остальных случаях $n > 4$, а количества элементов в соответствующем классе сопряженности равны, соответственно,

$$\frac{n!}{2 \cdot 4 \cdot \ldots \cdot (n-2) \cdot 2}, \ \frac{n!}{2 \cdot 4 \cdot \ldots \cdot (n-1)} \text{ и } \frac{n!}{2 \cdot 4 \cdot \ldots \cdot n}.$$

Первое число больше $\frac{n(n-1)}{2}$ при $n > 4$, второе число не меньше $n(n-2)$, что больше $\frac{n(n-1)}{2}$ при $n > 3$, и, наконец, третье число не меньше $(n-1)\times$ $\times(n-3)$, что больше $\frac{n(n-1)}{2}$ при $n > 6$ и не равно $\frac{n(n-1)}{2}$ при $n = 5$. Поэтому при $n \neq 6$ любой автоморфизм переводит транспозиции в транспозиции.

Пусть теперь известно, что транспозиции переходят в транспозиции. Докажем, что в этом случае автоморфизм обязательно является внутренним. Будем последовательно подправлять его, умножая на внутренние автоморфизмы, так, что в результате получится тождественный автоморфизм. Можно с самого начала считать, что транспозиция (12) остается на месте. Далее, транспозиция (23) переходит в транспозицию, которая не коммутирует с (12), и потому есть либо $(1k)$, либо $(2k)$, где $k \geqslant 3$. Такую транспозицию сопряжением с помощью элемента, который коммутирует с (12), можно перевести в (23) — так что можно домножить наш автоморфизм на подходящий внутренний, так что в итоге и (12), и (23) остаются на месте. Далее, если мы уже добились того, что транспозиции (12), (23), $\ldots$, $(k{-}1\ k)$ остаются на месте, то транспозиция $(k\ k{+}1)$ должна переходить в транспозицию (kl) или $(k{+}1\ l)$ (поскольку она коммутирует со всеми из них, кроме последней), и сопряжением перестановкой, которая коммутирует со всеми перечисленными транспозициями, такую транспозицию можно перевести в $(k\ k{+}1)$, так что в итоге и эта транспозиция будет оставаться на месте. Всевозможные транспозиции $(k\ k{+}1)$ порождают S_n, так что если все они неподвижны при автоморфизме, то этот автоморфизм тождественный.

Замечание 2. Из структуры доказательства немедленно следует, что любой внешний автоморфизм S_6 переводит каждую транспозицию в произведение трех непересекающихся транспозиций (это единственный класс сопряженности нужной мощности, который состоит из инволюций). Мы используем это ниже. Немедленное же следствие этого факта состоит в том, что группа внешних автоморфизмов S_6 состоит из двух элементов. В самом деле, любые два внешних автоморфизма S_6 переводят класс сопряженности транспозиций в один и тот же класс сопряженности, и потому отличаются на автоморфизм, который переводит транспозиции в транспозиции, а значит, является внутренним.

Задача*. Постройте три существенно различных (не отличающихся на внутренний автоморфизм) внешних автоморфизма A_6, и три неизоморфных группы, которые содержат A_6 в качестве подгруппы индекса 2.

Следствие 2. *Простая группа порядка* 60 *единственна с точностью до изоморфизма.*

Доказательство. Рассмотрим действие нашей группы на множестве ее силовских 5-подгрупп с помощью сопряжения. Теоремы Силова гласят, что число этих подгрупп сравнимо с единицей по модулю 5 и является делителем порядка группы. Значит, это число делит 12. Если силовская подгруппа единственна, то она нормальна, что противоречит простоте нашей группы. Значит, в нашей группе шесть силовских 5-подгрупп (других делителей 12, сравнимых с единицей по модулю 5, нет). Отсюда следует, что наша группа гомоморфно отображается в S_6. Более того, в силу простоты нашей группы этот гомоморфизм инъективен, а его образ лежит в A_6 (инъективность следует из того, что ядро было бы нормальной подгруппой, а если образ не лежит в A_6, то ядро гомоморфизма вычисления четности образа было бы нормальной подгруппой). Дальнейшее доказательство аналогично приведенному выше (подгруппа в A_6 индекса 6 изоморфна A_5).

Неабелевых простых групп порядка меньше 60 не существует. Следующий возможный порядок неабелевой простой группы равен 168. Среди проективных групп есть сразу две группы такого порядка: $PSL_2(\mathbb{F}_7)$ и $PSL_3(\mathbb{F}_2)$. Оказывается, что эти группы изоморфны. Мы приводим набросок доказательства, опуская технические проверки. Подробное доказательство см., например, в [1].

Предложение 7. $PSL_2(\mathbb{F}_7) \simeq PSL_3(\mathbb{F}_2)$.

Эскиз доказательства. Как известно, двумерная проективная геометрия над полем из двух элементов с точностью до проективной двойственности задается отношением инцидентности. Именно, если мы знаем для множества из 14 элементов (точек и прямых в двумерном проективном пространстве), какие пары элементов этого множества *инцидентны*[2)], то мы восстановим геометрию с точностью до, возможно, проективной двойственности (т. е. прямые окажутся точками, и наоборот). В частности, группа проективных преобразований $PGL_3(\mathbb{F}_2) = PSL_3(\mathbb{F}_2)$ является подгруппой индекса 2 в группе всех перестановок подмножеств проективной плоскости, которые сохраняют инцидентность.

Предъявим совершенно аналогичную картину «с точки зрения группы $PSL_2(\mathbb{F}_7)$». В качестве 14-элементного множества точек и прямых мы

[2)] Т. е. один из которых содержится в другом.

рассмотрим множество всех максимальных по включению подгрупп в $PSL_2(\mathbb{F}_7)$, которые состоят из инволюций (элементов, которые в квадрате равны e). Мы предоставляем читателю убедиться в том, что таких подгрупп ровно 14. Среди них есть две, которые содержат инволюцию $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, а именно

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix}, \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix} \right\}$$

и

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \right\},$$

остальные получаются из этих с помощью сопряжениями матрицами $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$. Две подгруппы называются инцидентными, если их пересечение отлично от $\{e\}$. Можно проверить[3)], что отношение инцидентности на этих подгруппах изоморфно отношению инцидентности на точках и прямых проективной плоскости над $\mathbb{F}_2$. Поэтому группа $PSL_2(\mathbb{F}_7)$ (которая действует на нашем множестве подгрупп сопряжениями) изоморфна подгруппе индекса 2 в группе всех перестановок подмножеств проективной плоскости, которые сохраняют инцидентность. Поскольку группы $PSL_2(\mathbb{F}_7)$ и $PSL_3(\mathbb{F}_2)$ просты, две построенные подгруппы обязательно должны совпадать.

Замечание 3. Приведем набросок другого варианта доказательства[4)]. Рассмотрим множество всех четверок точек проективной прямой над $\mathbb{F}_7$, двойное отношение которых равно 3 (или 5, если перечислять их в другом порядке). Таких четверок точек ровно 28 (проверьте!). Если не отличать четверку точек от «дополнительной» четверки (вспомните, что проективная прямая над $\mathbb{F}_7$ состоит из 8 точек), то такие классы четверок образуют 14-элементное множество. На этом множестве отношение инцидентности вводится аналогично приведённому выше отношению инцидентности на подгруппах, и далее доказательство аналогично.

Задача*. Двумерная проективная геометрия над полем из двух элементов возникает также при изучении умножения в алгебре октав (чисел Грейвса – Кэли). Есть ли какая-то разумная связь группы $PSL_2(\mathbb{F}_7)$ с октавами?

Задача*. Докажите, что любая группа порядка 168 изоморфна $PSL_2(\mathbb{F}_7)$.

Замечание 4. Подсчет порядков показывает, что количества элементов в группах $PSL_4(\mathbb{F}_2)$ и $PSL_3(\mathbb{F}_4)$ одинаковы. Можно предположить,

---

3) Говорить «легко проверить» тут было бы чрезмерным издевательством над читателем.

4) Это доказательство автор узнал от Э. Б. Винберга.

что, как и выше, удастся связать теоретико-групповые конструкции для $PSL_3(\mathbb{F}_4)$ с проективной геометрией над $\mathbb{F}_2$, и использовать это для доказательства изоморфизма. Оказывается, что эти две группы неизоморфны. Попробуйте это доказать. Один из путей состоит в том, чтобы изучить классы сопряженности инволюций в этих группах. Может быть, Вы придумаете другой путь?

От алгебры к геометрии

В этом разделе наша стратегия радикально изменится. Если до этого мы изучали геометрию действий проективных групп и обнаруживали объекты, на которых эти группы действуют, то теперь мы стартуем с действий симметрических и знакопеременных групп, и обнаружим действие этих групп на геометрических объектах. Следующее предложение является первым нетривиальным примером такой ситуации.

Предложение 8. $S_6 \simeq Sp_4(\mathbb{F}_2)$. *Здесь $Sp_4(\Bbbk)$ обозначает группу линейных преобразований четырехмерного пространства над полем $\Bbbk$, которые сохраняют кососимметричную билинейную форму*

$$\langle (x_0, x_1, x_2, x_3), (y_0, y_1, y_2, y_3) \rangle = x_0 y_1 - x_1 y_0 + x_2 y_3 - x_3 y_2.$$

Доказательство. Рассмотрим 16-элементное множество, элементами которого являются все двухэлементные подмножества шестиэлементного множества и его пустое подмножество. Определим на этом множестве «сложение»: сумма пустого множества с любым элементом A снова равна A, сумма $A + A$ всегда равна пустому множеству, если два непустых подмножества не пересекаются, то их сумма равна дополнению к их объединению, если же они пересекаются по одному элементу, то их сумма равна их симметрической разности (разности их объединения и пересечения). Можно проверить, что это «сложение» ассоциативно, и тем самым на нашем множестве задается структура четырехмерного векторного пространства над полем из двух элементов.

Определим билинейную форму на нашем векторном пространстве формулой $(A, B) = \#A \cap B$ (это число надо понимать как элемент $\mathbb{F}_2$, т. е. нас интересует лишь его четность; проверку того, что это действительно билинейная форма, мы оставляем читателю). Легко видеть, что в базисе $\{1, 2\}$, $\{2, 3\}$, $\{4, 5\}$, $\{5, 6\}$ эта форма имеет вид, указанный в формулировке предложения. Кроме того, действие симметрической группы, очевидно, сохраняет эту форму, и потому мы имеет гомоморфизм $S_6 \to Sp_4(\mathbb{F}_2)$. Нетрудно проверить, что порядок группы $Sp_4(\mathbb{F}_2)$ равен 6!, так что надо лишь проверить, что этот гомоморфизм не имеет ядра. Но нетрудно видеть, что его образ состоит из более чем двух элементов, а нетривиальные нормальные подгруппы S_6 суть A_6 и S_6.

Замечание 5. Нетривиальный способ интерпретировать использованную в доказательстве конструкцию, который помимо прочего приводит к ясному доказательству ассоциативности суммы подмножеств, состоит в том, чтобы понимать эту конструкцию как частный случай следующей общей конструкции. Пусть M — конечное множество. На множестве $\mathcal{P}(M)$ всех его подмножеств имеется естественная структура абелевой группы, задаваемая вычислением симметрической разности. Ясно, что каждый элемент этой группы имеет порядок 2, так что $\mathcal{P}(M)$ — не только абелева группа, но и векторное пространство над $\mathbb{F}_2$. Подмножество $\{\varnothing, M\}$ является подпространством, и мы можем образовать соответствующее факторпространство. Оно состоит из смежных классов $\{A, M \setminus A\}$. Если в множестве M четное число элементов, то подпространство $\mathcal{P}^+(M) \subset \mathcal{P}(M)$, состоящее из всех подмножеств, в которых четное число элементов, содержит подпространство, по которому мы факторизуем. Обозначим через V образ $\mathcal{P}^+(M)$ в факторпространстве.

В случае, если множество M шестиэлементно, пространство V четырехмерно, и естественно отождествляется с построенным выше четырехмерным пространством. В самом деле, выбирая в каждом смежном классе то из множеств, в котором меньше элементов, мы можем сопоставить каждому элементу $v \in V$ подмножество множества M, которое либо пусто, либо двухэлементно. Симплектическая форма, как нетрудно видеть, определена на всём $\mathcal{P}(M)$, и ее ограничение на $\mathcal{P}^+(M)$ опускается на V после факторизации.

Теорема 1. $GL_4(\mathbb{F}_2) \simeq A_8$.

Эскиз доказательства. Здесь мы тоже ограничимся наброском доказательства, оставляя некоторые детали в качестве (весьма полезного) упражнения.

Из замечания 2 мы знаем, что внешний автоморфизм S_6 переводит класс сопряженности транспозиции в класс сопряженности произведения трех непересекающихся транспозиций (далее мы называем перестановку, которая является произведением r непересекающихся транспозиций, r-инволюцией). Выше мы научились сопоставлять транспозициям в S_6 (то есть двухэлементным подмножествам шестиэлементного множества) ненулевые элементы 4-мерного векторного пространства над $\mathbb{F}_2$. Перенесем с помощью внешнего автоморфизма это сопоставление на 3-инволюции. Мы построим действие A_8 на этих объектах, которое и задаст гомоморфизм $A_8 \to GL_4(\mathbb{F}_2)$. Для начала заменим 3-инволюции в S_6 на 4-инволюции в S_8 с помощью гомоморфизма $\imath\colon S_6 \to A_8$, заданного правилом

$$\imath(\sigma) = \begin{cases} \sigma, & \text{если } \sigma \in A_6, \\ \sigma \cdot (7\ 8) & \text{иначе.} \end{cases}$$

Теперь группа A_8 могла бы действовать на этих перестановках сопряжением, завершая доказательство. Увы, это действие не подходит: оно не согласовано со структурой векторного пространства (и потому не задает гомоморфизм в $GL_4(\mathbb{F}_2)$). В действительности всё устроено чуть сложнее (но весьма изящно).

Вспомним доказательство теоремы Кэли (которая гласит, что каждая конечная группа изоморфна подгруппе симметрической группы). Именно, это доказательство нумерует элементы данной группы, и каждому элементу сопоставляет перестановку элементов группы, задаваемую правым сдвигом на этот элемент. Простое наблюдение, которое будет для нас очень важным, заключается в том, что 4-инволюции можно понимать как образы элементов векторного пространства $\mathbb{F}_2^3$ при вложении Кэли этого векторного пространства в S_8. (В самом деле, эти образы имеют порядок 2 и не имеют неподвижных точек, и потому обязаны быть 4-инволюциями.) Всевозможные образы вложений Кэли этого векторного пространства (отвечающие разным нумерациям элементов) образуют множество, на котором A_8 (и даже S_8) естественно действует. Сформулируем в виде упражнений несколько свойств этого действия.

Упражнение. 1. Для любого вложения Кэли $\mathbb{F}_2^3 \hookrightarrow S_8$ каждая транспозиция $(i\ j) \subset S_8$ входит сомножителем ровно в один элемент образа.

2. Нормализатор такой подгруппы изоморфен полупрямому произведению $GL_3(\mathbb{F}_2) \ltimes \mathbb{F}_2^3$ и целиком содержится в A_8.

3. Действие S_8 на разных вложениях Кэли с помощью сопряжений имеет одну орбиту, действие A_8 — две орбиты.

4. Любые две подгруппы из одной A_8-орбиты пересекаются лишь по единичному элементу.

Выберем представителей двух A_8-орбит на множестве вложений Кэли. Обозначим эти подгруппы через G_+ и G_-. Будем называть подгруппы, сопряженные с G_+, четными, а подгруппы, сопряженные с G_-, нечетными.

Ровно один элемент $g \subset G_+$ содержит транспозицию $(7\ 8)$ в качестве сомножителя. Сопоставляя подгруппе элемент g, мы получаем биекцию между множеством четных подгрупп и множеством 4-транспозиций, которые получаются из 3-транспозиций S_6 с помощью гомоморфизма $\imath$. Аналогичное верно для нечетных подгрупп.

С помощью этой биекции мы получаем на множестве четных подгрупп структуру векторного пространства над $\mathbb{F}_2$. Ключевое (и наиболее нетривиальное) утверждение, которое осталось доказать, таково.

Предложение 9. *Действие A_8 с помощью сопряжений на этом векторном пространстве линейно.*

Доказательство. Скажем, что четная подгруппа H инцидентна нечетной подгруппе K, если пересечение H и K содержит более одного элемента. Отношение инцидентности важно по той причине, что подгруппа, являющаяся суммой H и K относительно нашей структуры векторного пространства, является единственной подгруппой, которая инцидентна всем подгруппам, инцидентным и H, и K. Из этого немедленно следует наше предложение, поскольку мы определили сумму векторов нашего пространства в чисто теоретико-групповых терминах — а значит, это определение стабильно относительно действия сопряжениями.

Желательное нам утверждение составляет содержание следующего упражнения.

Упражнение. 1. Подгруппа H инцидентна подгруппе K если и только если отвечающие им 4-инволюции коммутируют.

2. Пусть s и t — две различных 3-инволюции в S_6. Существует единственная 3-инволюция, отличная от s и t, которая коммутирует со всеми 3-инволюциями, которые коммутируют и с s, и с t. Это в точности инволюция, являющаяся суммой s и t относительно существующей на 3-инволюциях структуры векторного пространства над $\mathbb{F}_2$.

Замечание 6. Выше мы построили отображение S_6 в группу линейных преобразований четырехмерного пространства над полем из двух элементов. Построенный сейчас гомоморфизм A_8 в $GL_4(\mathbb{F}_2)$ расширяет этот гомоморфизм с подгруппы $\imath(S_6)$ на всю группу.

Список литературы

[1] О'Мира О. *Лекции о линейных группах* // Автоморфизмы классических групп. М.: Мир, 1976.

[2] Винберг Э. Б. *Курс алгебры*. М.: Факториал, 2002.

[3] Lang S. *Algebra*. Rev. 3rd ed. Springer, 2002.

[4] Murray J., *The alternating group A_8 and the general linear group $GL_4(2)$* // Math. Proc. of the Royal Irish Academy, 1999. Vol. 99A, no. 2. P. 123–132.

[5] Каргаполов М. И., Мерзляков К. И. *Основы теории групп*. М.: Наука, 1977.

В. В. Доценко: Trinity College, Dublin

Издательство МЦНМО

Дж. Кингман. **Пуассоновские процессы.** Под ред. А.М. Вершика. 2007. 136 с.

Книга признанного мирового специалиста в области теории вероятностей, математической статистики и их приложений Дж. Кингмана представляет собой систематическое изложение классической теории пуассоновских процессов в произвольных пространствах. Книга предназначена как для начинающих изучение теории случайных процессов, так и для специалистов, поскольку сочетает ясное и красивое изложение основ теории с представлением новых идей, связанных прежде всего с разнообразными приложениями пуассоновских процессов к геометрии, теории массового обслуживания, экологии, генетике, астрономии и др.

М. Я. Кельберт, Ю. М. Сухов. **Вероятность и статистика в примерах и задачах.** Том I. Основные понятия теории вероятностей и математической статистики. 2007. 456 с.

Для освоения теории вероятностей и математической статистики тренировка в решении задач и выработка интуиции важны не меньше, чем изучение доказательств теорем; большое разнообразие задач по этому предмету затрудняет студентам переход от лекций к экзаменационным задачам, а от них — к практике.

Ввиду того, что предмет этой книги критически важен и для современных приложений (финансовая математика, менеджмент, телекоммуникации, обработка сигналов, биоинформатика), так и для приложений классических (актуарная математика, социология, инженерия), авторы собрали большое количество упражнений, снабженных полными решениями. Эти решения адаптированы к нуждам и умениям учащихся. Для удобства усвоения текста авторы приводят в книге целый ряд основных математических фактов; кроме того, текст снабжен историческими отступлениями.

В. И. Арнольд. **Экспериментальное наблюдение математических фактов**. 2006. 120 с.

Книга содержит записи курсов лекций, прочитаных академиком В. И. Арнольдом в 2005 г., в Дубне, на летней школе «Современная математика». В книге рассказывается о нескольких новых направлениях математических исследований, основанных на численных экспериментах.

Игорь Фёдорович Шарыгин. К 70-летию со дня рождения. Сост. А. А. Заславский, В. Ю. Протасов, Д. И. Шарыгин. 2007. 304 с.

В книге собраны различные материалы, связанные с жизнью и деятельностью выдающегося педагога и учёного, популяризатора науки Игоря Фёдоровича Шарыгина (1937–2004), его статьи и воспоминания о нём.

Отдельная часть книги содержит задачи и подробные решения геометрических олимпиад им. И. Ф. Шарыгина, проводимых с 2005 года.

Книга предназначена для всех интересующихся вопросами математического образования, школьных учителей и руководителей кружков.

Ж.-П. Серр. **Собрание сочинений. Том III.** (Совместно с НМУ) 2007. 540 с.

Жан-Пьер Серр — один из величайших математиков нашего времени, чьи работы на протяжении последнего полувека преобразили современную математику, в особенности алгебраическую топологию, алгебраическую геометрию, теорию алгебр и групп Ли, теорию чисел.

Собрание сочинений выпускается к 75-летию ученого. В 3-й том настоящего издания включены работы 1961–68 гг.