ПРОСТЫЕ ГРУППЫ

Член-корреспондент АН СССР
А. И. КОСТРИКИН

В конце 1980 г. математический и околоматематический мир облетела новость первостепенной важности: конечные простые группы классифицированы! На обложку одного математического журнала был вынесен список 26 известных «спорадических» групп. Этот список, воспроизводимый ниже в чуть измененном виде (см. таблицу), кочевал на протяжении пяти лет по алгебраическим конференциям и сам по себе не был новостью. Но — и это самое существенное — под списком помещено яркое примечание: ...«классификация конечных простых групп завершена; других спорадических групп нет». На обложке слово «известных» перед списком было красноречиво зачеркнуто.

Непосвященному читателю значение таинственной таблицы чисел, сопровождаемой не менее таинственными терминами, вряд ли о чем говорит. Более того, специализация наук такова, что для большинства математиков кое-какие разъяснения тоже необходимы.

Время от времени в каждой области человеческого знания происходят кардинальные изменения. В нашем случае специалисты склонны говорить о сенсации века. О полной драматизме истории ... ся не только в неожиданном и исчерпывающем решении древней проблемы: он переносит центр тяжести исходной задачи на методы ее решения. А этим методам, связанным с понятием *группы* данного уравнения, суждено проникнуть во все без исключения разделы математики, в физику, химию, кристаллографию...

Но злой рок преследует работы Галуа. В Парижской академии наук дважды теряют его рукописи. В очередном варианте работы не могут разобраться рецензенты-академики. А сразу после смерти двадцатилетнего юноши на дуэли (обстоятельства дуэли сродни политическому убийству) чудом уцелевший окончательный вариант его работы ... не принимает к публикации ни один научный журнал.

Клейн и Ли: группы в геометрии и в анализе

Лишь 35 лет спустя, когда яркий образ студента-республиканца и математика стал постепенно исчезать из человеческой памяти, идеи Галуа получили признание. Сначала, в 1846 году, Ж. Лиувилль опубликовал его работу в своем научном журнале. Работа, однако, была оценена по достоинству не сенсации века. С полной драматических поворотов истории этого события — наш рассказ.

Галуа и группа уравнения

Все началось более 150 лет тому назад. Студент-первокурсник парижской высшей Нормальной школы Эварист Галуа решает едва ли не важнейшую математическую задачу своего времени: он дает полный ответ на вопрос о разрешимости в радикалах алгебраических уравнений любых степеней*). Гениальность Галуа проявляется, однако, была оценена по достоинству не сразу. Первым, видимо, ее значение понял французский алгебраист Камиль Жордан. Но широкому проникновению идей теории групп в математическую науку мы в первую очередь обязаны двум начинающим математикам, его ученикам: Феликсу Клейну и Софусу Ли.

*) Именно, с каждым алгебраическим уравнением Галуа связывает некоторый объект — «группу уравнения»; уравнение оказывается разрешимым в радикалах (т. е. его корни выражаются через коэффициенты уравнения с помощью арифметических операций и извлечения корней) в том и только в том случае, когда группа уравнения обладает некоторым просто проверяемым свойством. Подробнее об этом см. «Квант», 1986, № 12, с. 2.

И здесь не обошлось без политики. Начавшаяся в 1870 году франко-прусская война привела к гибели почти всего тиража книги Жордана о теории Галуа и на долгие годы разъединила француза Жордана и немца Клейна. А ни в чем не повинный норвежец Ли и вовсе оказался за решеткой: подталкиваемые волной шовинистического угара, набравшей силу с первых дней войны 1870 г., не в меру бдительные французские граждане определили, что светловолосый голу-

боглазый красавец, сосредоточенно заносивший таинственные знаки в небольшой блокнот и говорящий с акцентом, конечно же — немецкий шпион.

В тюрьме недалеко от Парижа созревают глубокие идеи Софуса Ли о применении теории групп в анализе, в частности — в дифференциальных уравнениях. Зарождаются основы теории, плодотворно развивающейся и по сей день,— *теории групп Ли*. А у себя на родине Клейн обдумывает роль групп в геометрии. Роль эта оказывается определяющей для самих оснований геометрической науки, и Клейн разъясняет это с блеском в своей знаменитой *эрлангенской программе*.*)

Задача классификации конечных групп

Группы выступают не только в качестве метода в различных областях математики, но постепенно становятся самостоятельным предметом изучения. Особенно это касается конечных групп, изучение которых идет еще от самого Галуа. Математиками XIX столетия ставилась задача их **классификации**: предъявить полный список, без повторений, всех конечных групп.*) Насколько это трудно, свидетельствует тот факт, что настойчивые усилия по составлению каталогов конечных групп заводят в тупик даже при сравнительно небольших порядках групп (порядок $|G|$ — число элементов в группе G). Например, списка групп порядка $1024=2^{10}$ до сих пор нет.

Поэтому задачу классификации стоит ослабить. Подобно тому, как белки составлены из аминокислот, химические соединения состоят из атомов или натуральные числа являются произведением простых, конечные группы тоже строятся (хотя и весьма сложным образом) из элементарных составляющих: именно, из так назы-

*) Для понимания математической части дальнейшего текста достаточно знать, что такое конечная группа (в частности, циклическая группа и

*) См. «Квант», 1975, № 12, с. 6.

группа перестановок) и гомоморфизм. Об этом написано на с. 9, 11.

Спорадические конечные простые группы

Группа	Год открытия	Порядок группы	Авторы
M_{11}	1861	$2^4 3^2 5\cdot 11=7920$	Матье
M_{12}	1861	$2^6 3^3 5\cdot 11=95040$	Матье
M_{22}	1873	$2^7 3^2 5\cdot 11=443\,520$	Матье
M_{23}	1873	$2^7 3^2 5\cdot 7\cdot 11\cdot 23=10\,200\,960$	Матье
M_{24}	1873	$2^{10} 3^3 5\cdot 7\cdot 11\cdot 23=244\,823\,040$	Матье
J_1	1965	$2^3 3\cdot 5\cdot 7\cdot 11\cdot 19=175\,560$	Янко
HS	1967	$2^9 3^2 5^3 7\cdot 11=44\,353\,000$	Хигман, Симс
$J_2=HJ$	1967	$2^7 3^3 5^2 7=604\,800$	Холл, Уелс
Mc	1968	$2^7 3^6 5^3 7\cdot 11=898\,128\,000$	Маклафлин
Sz	1968	$2^{13} 3^7 5^2 7\cdot 11\cdot 13$	Судзуки
$J_3=HJM$	1968	$2^7 3^5 5\cdot 17\cdot 19=50\,232\,960$	Хигман, Мак-Кей
Co_1	1968	$2^{21} 3^9 5^4 7^2 11\cdot 13\cdot 23$	Конвей
Co_2	1968	$2^{18} 3^6 5^3 7\cdot 11\cdot 23$	Конвей
Co_3	1968	$2^{10} 3^7 5^3 7\cdot 11\cdot 23$	Конвей
$He=HHM$	1968	$2^{10} 3^3 5^2 7^3\cdot 17$	Хелд, Хигман и др.
F_{22}	1969	$2^{17} 3^9 5^2 7\cdot 11\cdot 13$	Фишер
F_{23}	1969	$2^{18} 3^{13} 5^2\cdot 7\cdot 11\cdot 13\cdot 17\cdot 23$	Фишер
F_{24}	1969	$2^{21} 3^{16} 5^2 7^3\cdot 11\cdot 13\cdot 17\cdot 23\cdot 29$	Фишер
$Ly=LyS$	1970	$2^8 3^7 5^6\cdot 7\cdot 11\cdot 31\cdot 37\cdot 67$	Лионс, Симс
Ru	1972	$2^{14} 3^3 5^3\cdot 7\cdot 13\cdot 29$	Рудвалис, Конвей и др.
$O=O'NS$	1973	$2^9 3^4 5\cdot 7^3\cdot 11\cdot 19\cdot 31$	О'Нэн, Симс
$F_2=B$	1973	$2^{41} 3^{13} 5^6 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\times$ $\times 31\cdot 47$	Фишер, Симс и др.
$F_3=E$	1974	$2^{15} 3^{10} 5^3 7^2\cdot 13\cdot 19\cdot 31$	Смит, Томпсон
$F_5=O$	1974	$2^{14} 3^6 5^6\cdot 7\cdot 11\cdot 19$	Конвей, Фишер и др.
$M=F_1$	1974	$2^{46} 3^{20} 5^9 7^6 11^2 13^3\cdot 17\cdot 19\cdot 23\times$ $\times 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$	Фишер, Грисс
J_4	1975	$2^{21} 3^3\cdot 5\cdot 7\cdot 11^3\cdot 23\cdot 29\cdot 31\times$ $\times 37\cdot 43$	Конвей, Янко и др.

1*

ваемых *простых групп*. И поэтому первоочередной становится *задача классификации конечных простых групп*.

Известно, что любая конечная группа является подгруппой одной из групп перестановок S_n, $n=1, 2, \ldots$ (см. с. 9 этого номера). Поэтому поиск простых конечных групп можно начать с исследования подгрупп группы S_n.

Но что же такое простая группа? Назовем гомоморфизм $\alpha: G\to H$ *упрощающим*, если в его образе $\alpha(G)\subset H$ более одного элемента, но меньше, чем в G. Конечная группа G называет-

алгебраического происхождения. Опишем эти группы.

Рассмотрим группу S_n. Ее элемент $t\in S_n$ называется *транспозицией*, если он оставляет на месте все элементы 1, 2, ..., n кроме двух, которые он переставляет местами. Примеры:

$$S_5\ni\begin{pmatrix}1&2&3&4&5\\1&2&5&4&3\end{pmatrix},\quad S_4\ni\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}.$$

Очевидно, что любая перестановка может быть представлена в виде композиции транспозиций; перестановка $\sigma\in S_n$, которую можно представить в виде композиции четного числа транспозиций, называется *четной*;

ся *простой*, если у нее нет упрощающих гомоморфизмов.

Самый очевидный пример простой группы — это *циклическая группа* $\mathbf{Z}_p$ любого простого порядка p:

$$\mathbf{Z}_p = \left\{z, z^2, \ldots, z^p = e \mid z = \begin{pmatrix} 1 & 2 & \ldots & (p-1) & p \\ 2 & 3 & \ldots & p & 1 \end{pmatrix}\right\} \subset S_n.$$

Действительно, если бы существовал упрощающий гомоморфизм $\alpha\colon \mathbf{Z}_p \to H$, то один из не равных e элементов $w \in \mathbf{Z}_p$ перешел бы в единицу, но тогда и любой элемент из $\mathbf{Z}_p$ перешел бы в единицу (подумайте, почему) и $\alpha(\mathbf{Z}_p) = \{e\}$ — противоречие! Простота p здесь существенна, ибо группу $\mathbf{Z}_m$ при составном m можно гомоморфно отобразить на $\mathbf{Z}_k$, где k — делитель m.

Простейшие простые группы: две алгебраические серии

Простых конечных групп $\mathbf{Z}_p$ бесконечно много (так как простых чисел бесконечно много), так что группы $\mathbf{Z}_p$ образуют (бесконечную) *серию* конечных простых групп. Имеется еще одна легко описываемая серия простых групп, так называемые *знакопеременные группы* A_n, $n = 1, 2, \ldots$, тоже множество всех четных перестановок очевидно образует подгруппу группы S_n, которая и называется *знакопере-*

менной группой n-й степени и обозначается через A_n. Можно доказать, что в группе A_n имеется $n!/2$ элементов и что при $n > 4$ группа A_n — простая.

Матье послужили основой для конструирования высокоэффективных корректирующих кодов.

В целом же пять простых групп

Таким образом, *знакопеременные группы*

$$A_n,\ n=5,\ 6,\ 7,\ \ldots,$$

составляют вторую серию конечных простых групп.

Шестнадцать геометрических серий

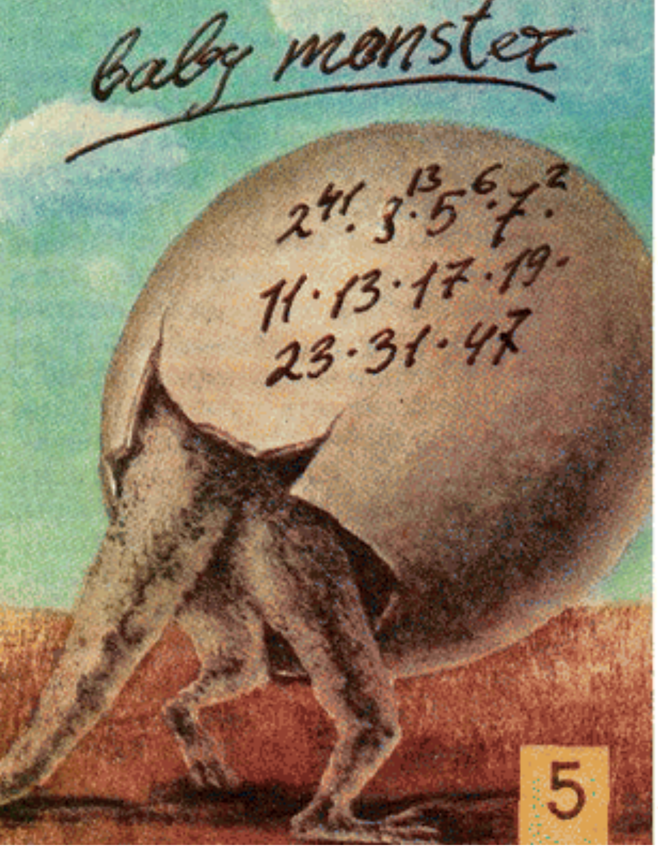
Конечные простые группы не исчерпываются сериями Z_p и A_n. Имеется еще 16 других серий конечных простых групп. Они устроены уже более сложно. Группы этих серий, как правило, — конечные подгруппы «групп Ли». Можно сказать, что они скорей геометрической, чем алгебраической природы. В их открытии участвовало много математиков. Основополагающую роль сыграли работы француза К. Шевалле, выполненные вскоре после войны и завершенные в пятидесятые годы. Бесконечные геометрические серии охватывают основную массу типичных простых групп и допускают много разных описаний, приспособленных для тех или иных целей.

Спорадические простые группы

Задолго до того как задача выявления всех 18 бесконечных серий конечных простых групп уступила перед натиском исследователей, было известно о существовании изолированных простых групп, названных *спорадическими*. До 1965 г. их было всего пять, и все они были связаны с именем французского математика-аналитика Э. Матье. Слово «группа» не фигурировало в названиях его работ периода 1861—1873 гг., где были описаны функции и комбинаторные структуры в пространствах размерностей 12 и 24 с очень специальной и красивой симметрией. Управляют этой симметрией пять групп, носящих теперь название *групп Матье* (см. таблицу на с. 3). Интересно, что в наше время группы Матье простояли особняком, полузабытые, около столетия, пока в 1965 г. З. Янко из Гейдельберга не нашел еще одну простую группу, тоже не укладывающуюся ни в какую бесконечную серию. Но найдена она была не случайным образом, а в ходе решения одной специальной классификационной задачи. Подобными задачами занимались десятки других математиков. Успех З. Янко, открывшего впоследствии еще три спорадические группы, послужил своего рода катализатором. Как грибы после дождя, для постороннего наблюдателя — без всякой причины, непонятно откуда, с помощью ЭВМ и без, стали появляться все новые спорадические простые группы. Имена удачливых «грибников», в сокращенном виде повторяемые названиями самих «грибов» — спорадических групп, приведены в уже упомянутой таблице, второй столбец которой указывает на год находки. Этот год не всегда совпадает с годом фактического построения группы.

«Большой монстр» и «бэби монстр»

Наибольшая из спорадических групп F_1, или M, заслуживает отдельного рассказа. Ее существование впервые



было предсказано независимо Б. Фишером, Дж. Томпсоном и Р. Гриссом еще в 1974 г. Строгую конструкцию этой группы лишь в 1981 г. предложил Грисс, основываясь на некотором семействе поворотов в пространстве размерности 196883 (!) Число элементов этой — с позволения сказать — простой группы равно 808 017 424 794 512 875 886 459 904 961 710 757 005 754 $368 \cdot 10^9$ (примерно 10^{54}). Не удивительно, что математики окрестили ее «big monster» («большой монстр») и долго подбирались к доказательству ее существования. Примечательно, что Грисс обошелся без помощи ЭВМ и тем самым избавил от первоначальных компьютерных родов многие другие спорадические группы, оказавшиеся «детенышами» (т. е. подгруппами) монстра F_1. К ним относится, в частности, группа F_2, известная под названием «baby monster» и ранее реализованная перестановками в S_n при n, близком к $14 \cdot 10^9$ (!). С течением времени были обнаружены поразительные связи монстра с классическими разделами математики (такими, как теория чисел) и получили широкое распространение «фантазии на тему монстра», не исключающие далеких параллелей между симметрией типа F_1 и новейшими физическими теориями.

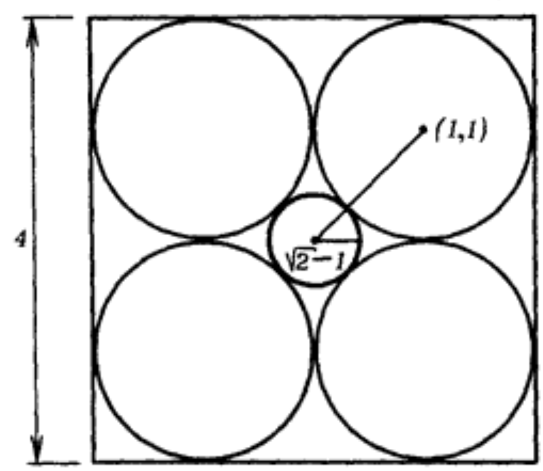
Теория и интуиция

Хотя ажиотаж вокруг упомянутых выше конструкций возник немалый, не нужно думать, что поиск рекордных спорадических групп превратился в бессмысленное спортивное соревнование, сродни популярным в США конкурсам по количеству студентов, поместившихся в телефонную будку. Построение спорадических групп проходило на пути глубочайшей интуиции и разумных догадок, предписываемых классификационной теорией, которая была развита на протяжении ста (!), но зато оно содержало в зародыше всю последующую теорию.

Помимо общих теоретико-групповых соображений, конструирование каждой отдельной спорадической группы основывалось на глубоких идеях из других разделов математики. Так, в работах Дж. Конвея, открывшего три спорадические группы, используются одновременно и теория кодирования, и замечательные результаты о плотной упаковке сфер в многомерной геометрии. А тут обычная трехмерная интуиция часто отказывает.

Поучительный пример *)

Рассмотрим квадрат со стороной длиной 4 с центром в начале координат плоскости $\mathbf{R}^2$. В его четыре угла впишем четыре окружности радиуса 1, так как показано на рисунке. Каж-



дая окружность касается двух других, и вся конфигурация симметрична относительно начала координат. Добавим теперь окружность с центром в начале координат, касающуюся четырех вписанных внешним образом. Точка (1; 1) — центр окружности в правом верхнем углу. Расстояние между центром внутренней окружности и центром единичной окружности в правом верхнем углу равно $\sqrt{2}$. Следовательно, радиус центральной окружности должен быть $\sqrt{2}-1$.

Перейдем теперь в трехмерное пространство $\mathbf{R}^3$ и повторим процесс, начав с куба ребром 4 с центром в начале координат и поместив в его 8 углов сферы радиуса 1. Каждая из сфер касается трех других, а все 8 симметричны относительно начала. Добавим теперь сферу с центром в начале координат, касающуюся

25 лет целым рядом крупных математиков. В самом начале этого удивительного периода в истории алгебры стоят Дж. Томпсон и У. Фейт, доказавшие, что *всякая простая группа нечетного порядка* (т. е. с нечетным числом элементов) *должна быть циклической группой* $\mathbf{Z}_p$ *для некоторого простого* p. Это доказательство заняло 250 страниц сухого журнального тек-

восьми вписанных внешним образом. Ее радиус легко вычислить, снова обратив внимание на центр (1; 1; 1) сферы в правом верхнем углу куба, который находится на расстоянии $\sqrt{3}$ от начала. Поскольку внутренняя сфера касается этой единичной сферы, ее радиус должен быть $\sqrt{3}-1$.

Продолжим в том же духе! В пространстве $\mathbf{R}^n$ рассмотрим n-мерный куб с ребром 4 с центром в начале координат и поместим в его

*) По Дж. Ивингу (*The Mathematical Intelligencer*, 1980, 3, № 1, с. 45—46).

2^n углах единичные сферы*). Каждая касается n других, и все они симметричны относительно начала. Поместим сферу с центром в начале координат, касающуюся внешним образом n вписанных. Чему равен ее радиус? То же рассуждение показывает, что он должен быть $\sqrt{n}-1$.

Например, в $\mathbf{R}^{10}$ радиус внутренней сферы равен $\sqrt{10}-1\approx 2{,}16$. Но ... минуточку! Что случилось? «Внутренняя» сфера выглядывает из куба!

Этот поразительный факт противоречит нашей интуиции. Но он верен. И дает некоторое представление о неожиданностях, поджидающих исследователей теории простых групп.

Вместо заключения: решена ли проблема классификации конечных простых групп?

Так или иначе, было найдено всего 26 спорадических групп. Но все ли? Какова их роль в системе всех конечных простых групп? Стоят ли они особняком или образуют начало новой серии? Или начало нескольких серий? На все эти вопросы могла дать ответ только глубоко развитая теория. Такая теория была создана международным коллективом математиков. После многолетних настойчивых усилий специалисты постепенно пришли в выводу, что *весь список конечных простых групп должен состоять из 18 известных серий и еще 26 отдельно стоящих, и тоже известных, спорадических групп.*

Вводные слова нашего рассказа, основанные на сообщениях (и даже рекламных интервью в газетах) двух ведущих специалистов М. Ашбахера

неточностей. Ими было недосуг заняться, а между тем из каждой дырки, по мнению пессимистов, готова выскочить спорадическая группа. Как пишет Дж. Конвей, начинается длительный период «ревизионизма», идейного пересмотра и упрощения доказательств, после завершения которого потомкам останутся ... несколько толстых, тщательно подготовленных томов.

В последние годы начато издание трехтомного сочинения Д. Горенстейна, содержащего детальный набросок (всего-то!) в принципе осуществленной программы, которая привела к впечатляющим результатам и коренным образом перестроила теорию конечных групп. Наиболее интересный вводный том издан в переводе на русский язык.*)

Итак, драматическая история простых групп еще не окончена. Скорее всего, таинственные тысячи страниц сплошного, тщательно подготовленного текста никто не напишет, да и достоверность их в любом случае вышла бы за рамки обычных математических стандартов. Сила математики — в ее единстве, и кто знает, на каком пути и какими средствами будут даны убедительные, легко проверяемые аргументы в пользу с таким трудом полученных выводов. Проблема заключается не только в перечислении всех конечных простых групп, но и в том, чтобы развить удобный сопутствующий аппарат, который и Д. Горенстейна, категоричны и оптимистичны. Но тот же Ашбахер несколько раньше писал: «Я верю, что существует не слишком много групп, которые ожидают своего открытия. Однако если бы я держал пари, у меня не нашлось бы дополнительных аргументов». Все дело в том, что текста доказательства как такового нет, а многие его куски попросту аккуратно не записаны. Рассчитывать на появление связного текста в ближайшие годы не приходится. Арифметической суммой из 5 или 15 тысяч журнальных страниц, написанных почти за три десятилетия сотнями специалистов во многих странах мира, можно пользоваться лишь как черновым материалом, содержащим множество имел бы общематематическое значение. Первые обнадеживающие связи с конечной геометрией и с теорией комплексных групп Ли уже обнаружены. Во всяком случае, конечные простые группы, о которых мы так много узнали в XX веке, продолжают оставаться чрезвычайно интересной и интригующей областью современной алгебры, ждущей молодых исследователей и свежих идей.

*) О том, что такое n-мерный куб, можно прочитать в «Кванте» 1986, № 6, с. 7.

*) Горенстейн Д., *Конечные простые группы. Введение в их классификацию*, М.: Мир, 1985 г.