ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 4
2012

В. Г. Алябьева (Пермь, ПГПУ). **Исследования конечных алгебраических структур в XIX веке.**

Группа является одной их общематематических и основной алгебраической структурой. Основной проблемой, решение которой привело к появлению понятия группы, была проблема разрешимости алгебраических уравнений в радикалах. Процесс формирования теоретико-группового мышления происходил также в геометрии и теории чисел. К 70-м годам XIX в. теоретико-групповое мышление в этих науках достигло достаточной зрелости.

В геометрии теоретико-групповое мышление прошло путь от «различных классов геометрических задач» Мебиуса до Эрлангенской программы Клейна, в которой разные геометрии характеризовались соответствующей группой преобразований, в теории чисел – от «равнозначных» остатков $r + np$ Эйлера, циклических групп первообразных корней сравнения $x^k \equiv a \pmod m$ $((a, m) = 1)$ Гаусса к определению Кронекера, данному им в процессе исследования композиционных форм, и эквивалентному определению конечной абелевой группы. В алгебре теоретико-групповое мышление развивалось от идеи Лагранжа, предложившего исследовать связь между разрешимостью уравнения и свойствами подстановок его корней, до «Трактата о подстановках» Жордана, в котором подведены итоги развития групп подстановок, обозначены проблемы, сформулированы решения некоторых их них.

Первые группы были группами подстановок. Теория групп подстановок выделилась в самостоятельную область исследований в 60-х гг. XIX в. Ж. Л. Лагранж первым (1771) установил связь между разрешимостью алгебраических уравнений и свойствами подстановок корней. Он показал, что каждый полином P от корней x_i алгебраического уравнения при всех возможных подстановках принимает $n(P) = n!/m$ значений, где m — число подстановок, оставляющих инвариантным полином P. Эта теорема соответствует в теории групп теореме о разложении симметрической группы на смежные классы по некоторой подгруппе или теореме о существовании подгруппы индекса $n(P)$ в S_n. Через 30 лет Руффини воспользовался результатами Лагранжа для доказательства неразрешимости в радикалах уравнения пятой степени. Доказывая, что не существует функции пяти переменных, которая при всех перестановках переменных принимает 8, 4 или 3 значения, Руффини, по существу, определил все подгруппы симметрической группы S_5. Он владел (правда, недостаточно отчетливо) представлениями о транзитивной и примитивной группе подстановок и, работая с конкретными подгруппами, пришел к выводу, что нормальный делитель (если пользоваться современной терминологией) должен быть транзитивным. Гаусс в 1799–1801 гг. приходит к мысли о неразрешимости уравнений общего вида в радикалах. Учение о корнях из единицы явилось для Гаусса примером, который позволил ему выделить главные свойства абелевых групп.

Большой вклад в развитие групп подстановок внес О. Коши. Группам подстановок он посвятил статьи 10-х, затем 40-х гг. XIX в. В статье 1815 года Коши доказал,

что число различных значений несимметрических функций n букв всегда отлично от 2 и не может быть меньше самого большого простого p, содержащегося в n. Статья была опубликована в известном и распространенном научном журнале «Journal de l'École polytechnique». На публикацию Коши первоначально никто не откликнулся. Коши сам вернулся к этой проблематике в 40-е гг. Он задался целью ответить на вопросы: «Каково число значений, которые может принять функция n букв? Как можно эффективно строить функции, принимающие заданное число значений?» Для функций из 6 букв Коши построил функции, принимающие 6, 15. 20, 10 значений. Коши ввел понятия композиции (умножения) подстановок, порядка подстановок (Коши называл его «указательный делитель»), циклическую запись подстановок. Он использовал выражение «система сопряженных элементов» для обозначения группы подстановок. Коши оказал большое влияние на развитие групп подстановок своим резюмирующим изложением теории подстановок в третьем томе «Этюдов по анализу» (1844) [1]. У него, однако, еще нет понятия группы подстановок как множества подстановок, замкнутого относительно умножения.

Термин «группа» впервые употребил Галуа (именно его называют творцом теории групп). Хотя он применял этот термин непоследовательно, все, что он называл группой, группой является. Галуа использовал мультипликативную замкнутость, хотя нигде это не доказал. Галуа понял решающую роль нормальных делителей: два совпавших разложения группы по подгруппе он назвал «собственным разложением» и первым четко обозначил предмет математики будущего — изучение математических структур, назвав это «анализом анализа». «Структурное» мышление Галуа, сжатость изложения затрудняли понимание его сочинений. Галуа погиб в 1832 г. в возрасте 21 года. Он написал небольшое количество работ [3]. При жизни его работы не были опубликованы. Лишь спустя десятилетие после смерти Галуа его другу А. Шевалле удалось обратить внимание на научный архив Галуа ведущего математика Франции Ж. Лиувилля. С 1846 г. Лиувилль издает труды Галуа в своем журнале, но лишь в 50-е гг. начинается возрождение и признание его идей [2].

В 1854 г. определение группы дал А. Кэли. Он ввел таблицу умножения конечной группы, называемую ныне таблицей умножения Кэли, доказал теорему о представлении любой конечной группы группой подстановок. В 1878 г. Кэли ввел для задания группы определяющие соотношения.

Знаменательной вехой в истории развития групп подстановок было издание в 1870 г. обширного труда К. Жордана «Трактат о подстановках» [3]. В связи с франко-прусской войной 1870–1871 гг. почти весь тираж «Трактата» погиб. Это в значительной степени ограничило влияние трактата на теорию групп (в 1957 г. он был переиздан). Жордан фиксирует состояние теории групп к 1870 г., подводит итоги своим исследованиям в этой области. В «Трактате» содержится определение группы подстановок: «Мы будем говорить, что система подстановок образует группу, если произведение двух произвольных подстановок само принадлежит системе ... ».

Систематическое изучение конечных полей началось с начала XIX века. Современная теория конечных полей — раздел алгебры, актуальность которого чрезвычайно возросла в связи с разнообразными приложениями в комбинаторике, теории кодирования, в математической теории переключательных схем. Конечные поля функционально полны. Это значит, что любое отображение конечного поля в себя можно представить в виде некоторого многочлена.

Простые поля F_p были исследованы Ферма, Эйлером, Лагранжем, Лежандром и Гауссом. Поля F_{p^n} впервые появились в статье Э. Галуа 1830 года «Из теории чисел» в связи с решением сравнений по модулю p в расширениях поля F_p (в честь Галуа конечные поля F_q стали называть полями Галуа и обозначать GF_q).

Э. Галуа, продолжая исследования Гаусса, рассматривает процедуру расширения поля F_p при помощи корня многочлена $f(x)$ степени n, неприводимого над F_p. После работ Галуа изучение «высших сравнений», как тогда называли уравнения над

конечными полями, было продолжено в работах Шенемана (Schönemann T., 1846), Серре (Serre J. A., 1854), Дедекинда (Dedekind R., 1857).

В докладе, прочитанном в 1893 году на Международном математическом конгрессе в Чикаго, американский математик Э. Г. Мур (E. H. Moore) сообщил о доказательстве теоремы: «*Любое конечное поле есть поле Галуа*»[4].

Ученик Мура Л. Диксон (L. E. Dickson) дал первое систематическое изложение теории конечных полей. Совместно с М. Уэддерберном (J. H. M. Wedderburn) Диксон доказал в 1905 году, что, говоря современным языком, любое конечное тело есть поле. В большой статье 1905 года «О конечных алгебрах» [5] Диксон исследовал независимость постулатов конечного поля и построил два типа конечных алгебр, для которых не выполняются некоторые постулаты поля. Одна алгебра — с делением, в ней умножение некоммутативно и выполняется правый дистрибутивный закон умножения относительно сложения. Диксон доказал, что коммутативность сложения и коммутативность умножения элементов конечной алгебры с делением являются следствиями остальных аксиом поля, но ни один из дистрибутивных законов исключить нельзя, если мы хотим, чтобы алгебра относительно сложения и умножения элементов оставалась полем.

Исследования Диксона некоммутативных алгебр с делением продолжил в 1935 году Ганс Цассенхаус (Hans Zassenhaus). Цассенхаус перечислил все возможные конечные алгебры с делением, в которых выполняется лишь один из дистрибутивных законов, например, левый. Цассенхаус назвал такие алгебры почти-полями и в статье «О конечных почти-полях» [6] дал общий метод их построения.

СПИСОК ЛИТЕРАТУРЫ

1. *Cauchy A.-L.* Mémoire sur les arrangements que l'on peut former avec des lettres données, et sur les permutations ou substitutions à l'aide desquelles on passé d'un arrangement à un autre. — In: Exercises d'analyse et de physique mathématique, 3. Paris: 1844, p. 151–252.
2. Галуа Э. Сочинения. М.-Л.: ОМТИ, 1936, с. 35-47.
3. *Jordan C.* Traité des substitutions et des équations algébriques. Paris: 1870.
4. *Moore E. H.* A doubleinfinite systems of simple groups. — In: Mathematical Papers Read at the International Mathematical Congress in Chicago 1893, published by MacMillan, 1896, p. 208–242.
5. *Dickson L. E.* Of finite algebras. — In: Nachrichten von der Königlichen Gesellschaft der Wissenschaften und der GeorgAugustUniversität zu Göttingen, 1905, p. 358-393.
6. *Zassenhaus H.* Über endliche Fastkörper. — In: Abhandlungen aus dem mathematischer Seminar der Universität Hamburg, 1935, v. 11, p. 187-220.