**Теория групп — наука о совершенстве**

Евгений Вдовин

**Введение**

Настоящий текст появился по нескольким причинам. Во-первых, подавляющее большинство не представляет, чем занимается современная математика. Теория групп — это, конечно, далеко не вся современная математика, а лишь малая ее часть, но она находится на одном из самых высоких уровней абстракции, что делает ее неплохим примером раздела современной математики.

Во-вторых, такой естественный и простой (для объяснения) объект, как группы, практически незнаком большинству ученых. Действительно, что может быть естественнее и привычнее для человека, чем понятие симметрии. Мы с самого рождения вольно или невольно ищем в окружающих предметах симметрию, и чем симметричнее предмет, тем совершеннее он нам кажется. Древние греки считали шар идеальной фигурой, именно из-за того, что у шара очень много симметрий. Взгляните на любую известную картину, и вы увидите там явную ось (а иногда и не одну симметрии). Любое музыкальное произведение развивается по циклу, постоянно возвращаясь к исходной теме, т. е. и там тоже есть симметрия. Даже такой, всем известный символ, как крест, почитаемый во многих религиях, кажется нам красивым из-за большого количества симметрий: его можно и крутить, и отражать относительно любой из его частей. Но превратите крест в свастику, и у вас сразу возникнет неуютное ощущение, ведь большую часть симметрий креста вы уничтожили. Таким образом, именно симметрия определяет, насколько совершенным кажется нам тот или иной объект, и теория групп, как наука, изучающая симметрии, может без преувеличения называться наукой о совершенстве.

И в-третьих, я вдохновлен примером таких замечательных ученых и популяризаторов науки, как Сергей Попов и Игорь Иванов, научно-популярные статьи которых я с интересом читаю.

Поскольку текст изначально задумывался доступным для читателя, знающего математику в объеме школьной программы, некоторые специальные части текста (на самом деле, подавляющая его часть), содержащие более трудный для понимания материал, чем обычно дается в школьном курсе алгебры, будут начинаться знаком и заканчиваться знаком (это не означает, что для понимания такого текста требуется что-то большее, чем школьная математика, трудности будут возникать логического характера). Дело в том, что теория групп находится на одном из самых высоких уровней абстракции в современной математике и потому группы иногда состоят из элементов, которые весьма сложно представить неискушенному читателю.



**Некоторые исходные определения и обозначения**



Мы постараемся использовать как можно меньше формул и специальных математических знаков, но совсем без них обойтись не получится. Множества, как правило, будут обозначаться заглавными латинскими буквами, а их элементы — строчными. Если A — множество, а a — некоторый элемент, то запись a A следует читать «элемент a принадлежит множеству A»; соответственно, запись a A означает, что «элемент a не принадлежит множеству A».



Напомним, что понятия множества, элемента и принадлежности являются базисными неопределяемыми понятиями современной математики. Любое множество определяется элементами, входящими в него (которые, в свою очередь, тоже могут быть множествами). Таким образом, мы говорим, что множество определено или задано, если для любого элемента мы можем сказать, принадлежит ли он этому множеству или нет. Для двух множеств A, B записи B A, B A, B ∩ A, B A, B \ A, A × B означают соответственно, что B является подмножеством множества A (т. е. любой элемент из B содержится также и в A, например множество натуральных чисел содержится в множестве действительных чисел; кроме того, всегда A A), B является собственным подмножеством множества A (т. е. B A и B ≠ A), пересечение множеств B и A (т. е. все такие элементы, которые лежат одновременно и в A, и в B, например пересечение целых чисел и положительных действительных чисел есть множество натуральных чисел), объединение множеств B и A (т. е. множество, состоящее из элементов, которые лежат либо в A, либо в B), разность множеств B и A (т. е. множество элементов, которые лежат в B, но не лежат в A), декартово произведение множеств A и B (т. е. множество пар вида (a, b), где a A, b B). Через |A| всегда обозначается мощность множества A, т. е. количество элементов в множестве A. Определяемые понятия всегда выделяются курсивом.



Нам не обойтись без понятий отображения, отношения и эквивалентности. Мы не будем давать строгих логических определений этих понятий, лишь поясним их. Отображение можно рассматривать как некоторую функцию, сопоставляющую одному элементу (называемому прообразом) некоторый другой элемент (называемый образом). В жизни мы постоянно сталкиваемся с понятием отображения, например, покупая билет в театр мы тем самым устанавливаем отображение между билетом и некоторым местом в зале театра. Получая зарплату, мы устанавливаем отображение между работой, проделанной за месяц и деньгами, которые за нее будут заплачены. Изучая списки игроков футбольных команд, мы устанавливаем отображение между игроками и командами, за которые они играют. Таким образом, отображений существует великое множество, почти всё в нашей жизни так или иначе является отображениями. Выделяют различные типы специальных отображений, далее в тексте будут использоваться следующие 3 типа: инъективное отображение (инъекция), сюръективное отображение (сюръекция) и биективное отображение (биекция). Инъективное отображение — это такое отображение, которое разным исходным элементам сопоставляет разные образы. Сюръективное отображение — это такое отображение, при котором у каждого образа есть прообраз. Наконец, биективное отображение — это отображение, которое одновременно является и инъективным, и сюръективным.

Поясним эти понятия на примере отображения между множеством билетов и множеством мест в театре. Представим себе некий кинотеатр в уездном городе N, в котором в тысячу какой-то раз идет «Щит и меч». Естественно, желающих посмотреть его немного, и находится лишь одна парочка, которая берет два билета в «ряду для поцелуев». Придя в кинотеатр, парочка, к своей радости, понимает, что они здесь одни, но как люди воспитанные, занимает свои места, указанные в билетах. В данном случае отображение, конечно, является инъективным, так как разные билеты соответствуют разным местам. Но оно не является сюръективным, так как у нас еще осталась куча пустых мест, на которые не продано ни одного билета. Таким образом, несюръективное отображение явно невыгодно администрации кинотеатра.

Представим теперь, что на следующий день в том же кинотеатре того же города пообещали запустить новый блокбастер от Тарантино и намекнули при этом, что сам Тарантино будет отвечать на вопросы зрителей после фильма. Естественно, кассы ломятся от народа, и дирекция, «по ошибке», продает два комплекта билетов на одни и те же места. Мы не будем здесь описывать разборки из-за одного места, произошедшие на сеансе, отметим лишь, что теперь отображение является сюръективным, так как на каждое место продан билет, но не является инъективным, так как билетов на каждое место приходится два. Таким образом, неинъективное отображение входит в прямое противоречие с правами потребителей и, наверное, попадает под какую-то статью закона «О защите прав потребителей».

Ну и последний случай, посмотрим на тот же кинотеатр в городе N накануне 1 января 2006 года. Широко разрекламированный первый фильм года вновь вызывает ажиотаж публики, но теперь дирекция, наученная предыдущим горьким опытом, тщательно следит за тем, чтобы на каждый сеанс продавался ровно один комплект билетов. В итоге, каждый зритель спокойно занимает свое место, и каждый сеанс начинается при полном аншлаге. Таким образом, этот последний пример является и инъективным, и сюръективным отражением, т. е. биекцией. Следовательно, биекция — это та золотая середина, которая максимально выгодна дирекции и при этом максимально удобна зрителям. Только что данное понятие биекции является математической формализацией интуитивного понятия симметрии, о котором шла речь во введении. Поэтому неудивительно, что именно биекция является наиболее совершенным отображением в данном случае.



Отображением из множества A в множество B называют некоторое правило, используя которое, каждому элементу из A можно сопоставить единственный элемент из B. Отображения мы обычно будем обозначать греческими буквами и записывать φ : A → B, а образ любого элемента a A относительно отображения φ записывается aφ. Такая запись кажется сначала непривычной и неудобной тем, кто привык записывать функции (частный случай отображений) как φ(a), но для нашего изложения именно она будет более удобной. Если есть 3 множества A, B, C и даны отображения φ : A → B и ψ : B → C, то можно построить отображение φψ : A → C как композицию (последовательное выполнение) отображений φ и ψ. Заметим, что если бы мы записывали отображение слева, то композицию φψ нам бы пришлось читать справа налево, по-арабски. В дальнейшем нам потребуются следующие специальные типы отображений: инъекция (отображение φ : A → B называется инъективным, если для любых различных x, y A элементы xφ, yφ также различны), сюръекция (отображение φ : A → B называется сюръективным, если для любого y B существует такой x A, что xφ = y), биекция (инъекция и сюръекция одновременно). Примерами отображений из рациональных чисел в рациональные могут служить отображения: x → x3, x → x2, x → x/2. Первое является инъективным, но не сюръективным, второе не является ни сюръективным, ни инъективным, третье является биекцией.



Другим важным понятием математики является понятие отношения. Отношение можно представлять себе как некоторое правило, которое по любым двум элементам (предметам, вещам, живым существам и т. д.) находятся ли они в этом отношении или нет. В нашей жизни мы постоянно вступаем и находимся волей или неволей в множестве различных отношений. Например, в отношении родства (с той или иной степенью близости), отношении работник-работодатель, отношении водитель-пассажир, продавец-покупатель и т. д. Все эти отношения имеют разную природу, разные свойства, и математика изучает именно свойства отношений, не заботясь об их природе.



Мы говорим, что на некотором множестве A задано отношение R, если для любых двух элементов a, b из A мы можем сказать, находятся ли они в отношении R или нет. Иными словами, отношение R есть отображение R : A × B → {1, 0}, где значение 1 соответствует «истине», а значение 0 — «лжи» (заметим, что здесь важен порядок, в котором берутся элементы a и b). Обычно, для обозначения отношений мы будем использовать специальные символы ≡, ~, и т. д. Отношение удобно записывать как a ~ b, если a и b находятся в отношении R и a b, если a и b не находятся в отношении R. Отношение ~ на множестве A называется эквивалентностью, если выполнены следующие аксиомы:



(ЭКВ1)

для любого a A выполнено a ~ a (аксиома рефлексивности);



(ЭКВ2)

для любых a, b из A из a ~ b следует b ~ a (аксиома симметричности);

(ЭКВ3)

для любых a, b, c из A из a ~ b и b ~ c следует a ~ c (аксиома транзитивности).

Примерами отношений может служить отношение порядка ≥ на множестве действительных чисел, отношение делимости на множестве целых чисел, отношение равенства на множестве действительных чисел, отношение равенства остатков от деления на фиксированное натуральное число на множестве натуральных чисел. Заметим, что первые два отношения не являются эквивалентностями, а последние два являются. Для последнего отношения есть специальное название: целые числа m, n называются сравнимыми по модулю k (записывается как m ≡ n (mod k)), если n – m делится на k.

Если на множестве A задано отношение эквивалентности ~, то всё множество распадается на классы эквивалентности — подмножества попарно эквивалентных элементов, причем любые два класса либо не пересекаются, либо совпадают. Действительно, предположим, что C1, C2 — два класса эквивалентности и их пересечение C1 ∩ C2 непусто и содержит некоторый элемент x. Тогда для любого элемента y C1, по определению класса эквивалентности, выполнено x ~ y. Кроме того, для любого z C2, вновь по определению класса эквивалентности, выполнено z ~ x. В силу аксиомы транзитивности (условие (ЭКВ3)), мы получаем, что y ~ z, значит C1 = C2. Множество классов множества A по эквивалентности ~ обозначается через A / ~.



**Аксиомы группы**

В этом разделе заканчивается текст, который не начинается знаком . Следующие два абзаца — последние абзацы, для чтения которых не требуется прилагать особых усилий.



Рассмотрим всё тот же кинотеатр уездного города N и предположим, что на одном из сеансов зрителям пришло в голову устроить обмен билетами по какому-нибудь правилу. Например, первое место каждого ряда меняется со вторым, третье с четвертым и т. д. В результате все остаются с одной стороны «при своих» — у каждого есть билет, а с другой стороны — каждому удалось сменить место. Если теперь провести обмен по какому-нибудь другому правилу, потом по третьему, то результат — у каждого есть ровно один билет — не изменится. При этом порядок посадки может измениться весьма сильно, по сравнению с начальным. Таким образом, подобные преобразования являются симметриями множества мест (или, точнее, множества зрителей), причем сколько бы раз мы их не проводили, основное свойство, что у каждого зрителя есть ровно один билет, не изменится. Если последовательное выполнение обмена билетами назвать «умножением» (хоть оно и очень далеко от реального умножения, к которому мы все привыкли), то множество всех обменов с таким «умножением» образует очень важную алгебраическую структуру — группу. Вообще, любая группа — это множество симметрий какого-либо объекта (множества), на котором задано умножение также, как это только что было проделано с обменами билетов — последовательным выполнением.

Таким образом, группа симметрий объекта тем больше, чем больше у него симметрий. Вспоминая о том, что чем больше симметрий, тем совершеннее объект, мы получаем, что размер группы симметрий играет роль измерителя совершенства того или иного объекта. Рассмотрим правильные фигуры на плоскости: треугольник, квадрат, шестиугольник и круг. Все они симметричные фигуры, но симметричны они по-разному. Так у треугольника есть лишь шесть симметрий: поворот вокруг центра масс (точки пересечения медиан) на угол, кратный 120 градусам (таких поворотов 3), и отражение относительно любой из его медиан (таких отражений тоже 3). У квадрата уже есть восемь симметрий: поворот вокруг центра (точки пересечения диагоналей) на угол, кратный 90 градусам (таких поворотов уже 4), а также симметрия относительно любой диагонали (их две) и любой прямой, соединяющей середины противоположных сторон квадрата (их тоже две). Шестиугольник уже имеет 12 симметрий (предлагаем читателю перечислить их все), а у круга симметрий бесконечно много — это и поворот на любой угол, и симметрия относительно любой прямой, проходящей через центр круга. Таким образом, самой совершенной фигурой является круг, потом — шестиугольник, за ним квадрат и наименее совершенная фигура — треугольник.

и до конца



Пусть G — произвольное множество и предположим, что на нем задана некоторая бинарная (двухместная, от двух аргументов) операция «·», обычно называемая умножением, которая для любых двух элементов a, b из данного множества сопоставляет им единственным образом элемент, обозначаемый a · b или просто ab. При этом элемент ab называется произведением элементов a и b. Если при этом выполнены дополнительно следующие три условия (называемые аксиомами группы):

(ГР1)

для любых трех a, b, c из G верно равенство (ab)c = a(bc) (закон ассоциативности);

(ГР2)

существует такой элемент e, что для любого элемента a из G верно равенство ae = ea = a (существование единицы); такой элемент e называется единицей группы;

(ГР3)

для любого элемента a из G существует такой элемент b, что верно равенство ab = ba = e (существование обратного); такой элемент b называется обратным для элемента a и обозначается a–1;

то множество G относительно операции умножения образует группу. Если при этом выполнена еще одна аксиома:

(ГР4)

для любых элементов a, b из G верно равенство ab = ba (закон коммутативности),

то группа называется коммутативной или абелевой. Примеры различных групп, а также естественные ситуации, в которых появляются группы мы приведем чуть ниже. Очевидными примерами являются множество целых чисел по сложению, множество ненулевых рациональных чисел по умножению и т. д. Отметим несколько простых следствий из аксиом группы: единичный элемент и обратный элемент определяются единственным образом. Действительно, предположим, что существует два единичных элемента e1, e2, тогда применение аксиомы (ГР2) дает нам следующую цепочку равенств e1 = e1e2 = e2. Аналогично, если для некоторого элемента a существует два обратных b1, b2, то, используя аксиомы (ГР1)–(ГР3), мы получаем следующую цепочку равенств b1 = b1e = b1(ab2) = (b1a)b2 = eb2 = b2.

Если M — произвольное подмножество группы G, то мы можем рассмотреть операцию умножения на множестве M, которая является отображением · : M × M → G. Операцию · на множестве M мы будем называть индуцированной операцией. Подмножество H группы G называется подгруппой, если оно само является группой относительно индуцированной операции. Легко проверить, что подмножество является подгруппой, если оно замкнуто относительно произведения (т. е. для любых двух h1, h2 H элемент h1 · h2 вновь лежит в H) и замкнуто относительно взятия обратного (т. е. для любого h H элемент h–1 вновь лежит в H). Коротко это записывают как HH H и H–1 H. Далее утверждение «H является подгруппой группы G» коротко мы будем записывать следующим образом H ≤ G.



Пусть G — произвольная группа, H — ее подгруппа и g — произвольный элемент группы G. Множество Hg = {hg | h H} называется смежным классом (правым смежным классом) элемента g. Введем отношение g1 ≡ g2 (mod H) на множестве элементов группы G по правилу: g1 ≡ g2 (mod H) в том и только в том случае, если Hg1 = Hg2. Использование обозначения, сходного с отношением делимости для целых чисел (см. выше) неслучайно, поскольку отношение делимости является частным случаем равенства смежных классов. Действительно, в качестве группы G берется множество целых чисел по сложению, а в качестве подгруппы H берется подмножество k чисел, которые делятся на k. Очевидно, что определенное нами отношение является эквивалентностью, множество классов эквивалентности обозначается через G / H, мощность |G / H| множества классов эквивалентности обозначается еще как |G : H| и называется индексом подгруппы H в группе G. Очевидно, что для любого g G справедливо |Hg| = |H|, откуда мы сразу получаем важную теорему Лагранжа: |G| = |G : H| · |H|, в частности порядок подгруппы всегда делит порядок группы.



На множестве G / H можно естественным образом определить операцию умножения: Hg1 · Hg2 : = Hg1 · g2. Для того чтобы определение было корректным, т. е. чтобы выполнялось равенство множеств Hg1 · Hg2 = {h1g1 · h2g2 | h1, h2 H} и Hg1 · g2 = {hg1 · g2 | h H}, необходимо и достаточно, чтобы для любого g G выполнялось равенство g–1Hg = {g–1hg = h | h H} = H (это условие мы будем коротко записывать HG H). Выражение g–1Hg называется сопряжением с помощью элемента g и часто обозначается Hg. Выражение gHg–1 = Hg–1 мы будем записывать gH. Подгруппа H, удовлетворяющая условию HG H, называется нормальной подгруппой группы G (обозначается H G), а получившаяся группа G / H называется факторгруппой группы G по подгруппе H. Понятия нормальной подгруппы и факторгруппы являются одними из важнейших в теории групп, поскольку позволяют частично сводить изучение групп к меньшим группам (частично, так как по данным H и G / H группа G определяется неоднозначно). Группа, не содержащая нормальных подгрупп, называется простой.



Очевидно, что пересечение любого количества подгрупп вновь является подгруппой. Это позволяет нам определить подгруппу, порожденную множеством M, как наименьшую подгруппу, содержащую подмножество M, т. е. пересечение всех подгрупп группы G, содержащих множество M. Подгруппа, порожденная множеством M, будет обозначаться M. Легко проверить, что M является множеством всевозможных произведений элементов из M и обратных к ним. Группа, порожденная одним элементом a называется циклической, а ее порядок |a| : = |a| называется порядком элемента a. Легко проверить, что порядок элемента — это такое наименьшее число n, для которого равно e. Из теоремы Лагранжа следует, что порядок элемента всегда делит порядок группы.



В конце данного раздела мы приведем понятие изоморфизма групп. Если G, H — группы, то отображение φ : G → H, сохраняющее операцию (т. е. для всех g1, g2 G выполнено (g1 · g2)φ = g1φ · g2φ), называется гомоморфизмом, множество Ker(φ) = {g G | gφ = e} называется ядром гомоморфизма, а множество Gφ = {gφ | g G} называется образом гомоморфизма. Если Ker(φ) = {e}, а Gφ = H, т. е. если φ является биекцией, то отображение φ называется изоморфизмом, а группы G и H изоморфными (обозначается G H). Теорема о гомоморфизмах утверждает, что H = Ker(φ) — нормальная подгруппа группы G и Gφ G / H. Изоморфизм можно мыслить для себя, как такую «похожесть» двух групп, что мы их не различаем (хотя реально они могут быть разными множествами). Таким образом, теория, строго говоря, изучает классы изоморфизма групп. Заметим, что и в обыденной жизни мы тоже нередко устанавливаем изоморфизмы более или менее высокого уровня абстракции. Так, например, есть класс изоморфизма мебели, называемый понятием «шкаф» и мы по некоторым признакам безошибочно определяем, относится ли данный объект к «шкафам» или нет. Когда нам не хватает столь высокого уровня абстракции, мы спускаемся к более низкому уровню и начинаем делить шкафы на «кухонные», «книжные», «платяные» и т. д. Понятие изоморфизма для групп — это как раз тот инструмент, с помощью которого мы на нашем уровне абстракции различаем или отождествляем объекты.



**Примеры групп**

Примерами групп, известных нам с начальной школы, являются целые, рациональные, действительные, комплексные числа по сложению, ненулевые рациональные, действительные, комплексные числа по умножению. Все эти группы являются абелевыми. Другой важный пример групп дает нам следующая конструкция. Пусть X — произвольное множество и SymX — множество всевозможных биекцией множества X на себя. Зададим умножение на SymX как композицию. Тогда SymX относительно операции композиции является группой и называется симметрической группой на множестве X или группой подстановок (иногда используется также термин группа перестановок, но нам он кажется неудачным, об этом чуть ниже). Если множество X конечно и |X| = n, то можно считать, что X = {1, ..., n} и SymX обозначается за Symn. Если Ψ — некоторое свойство отображений, которое сохраняется при композиции, то подмножество отображений, удовлетворяющих свойству Ψ, группы SymX образует подгруппу группы SymX. Покажем, что композиция отображений удовлетворяет аксиоме ассоциативности (ГР1) (проверка остальных аксиом существенно проще, они вытекают из определения биекции). Для того, чтобы доказать, что композиция отображений ассоциативна, необходимо сначала понять, когда же отображения равны. Несмотря на очевидность определения, оно нередко вызывает сложности. Отображения φ : A → B и ψ : A → B (где A, B — произвольные множества) равны, если для любого x A его образы xφ и xψ равны. Пусть теперь φ, ψ, χ SymX и x X. Тогда x((φψ)χ) = (x(φψ))χ = ((xφ)ψ)χ, с другой стороны, x(φ(ψχ)) = (xφ)(ψχ) = ((xφ)ψ)χ, что доказывает ассоциативность композиции.



Этот пример не только позволяет строить большое количество различных групп (чуть ниже мы убедимся, что все группы), но и показывает широкую область применения теории групп. Везде, где есть хоть какая-то симметрия (т. е. биекция), немедленно возникают и группы. Задачи о построении с помощью циркуля и линейки, о разрешимости алгебраических уравнений в радикалах, дифференциальных уравнений в первообразных и т. д. естественным образом сводятся к задачам в теории групп. Различные комбинаторные задачи сводятся к подсчету объектов, удовлетворяющих некоторым свойствам и вновь к теории групп.

Если G — группа, X — множество и задан гомоморфизм φ : G → SymX, то говорят, что группа G действует на множестве X. Если Ker(φ) = {e}, то действие называется точным. Для «облегчения» обозначений мы будем отождествлять g с его образом gφ и для произвольного x X его образ относительно gφ будем записывать xg. Введем отношение эквивалентности ~ на X по правилу: элементы x, y X являются эквивалентными, если существует такой g G, что xg = y. Классы эквивалентности называются орбитами группы G. Говорят, что группа G действует транзитивно (а представление является транзитивным), если существует лишь одна орбита. Гомоморфизм φ : G → SymX называется подстановочным представлением группы G (именно из-за термина «подстановочное представление» термин «группа перестановок» считается неудачным, так как термин «перестановочное представление» имеет другое значение). Если Ker(φ) = {e}, то представление называется точным.



Рассмотрим теперь произвольную группу G и ее подгруппу H. Группа G действует на множестве смежных классов по подгруппе H умножением справа: (Hg1)g2 = H(g1g2). Таким образом, существует транзитивное представление φ : G → SymG/H. Если H не содержит отличных от единичной нормальных подгрупп группы G, то это представление является точным. В частности, если H = {e} то представление G → SymG/{e} = SymG всегда является точным и называется регулярным представлением группы G. Таким образом, любую группу можно рассматривать как группу подстановок. Оказывается, любое транзитивное представление группы G можно получить таким образом.

для понимания дальнейшего текста необходимо знание университетского курса алгебры



Следующий пример групп возникает из векторных пространств. Пусть V — векторное пространство над полем F (я не буду давать определение векторного пространства и поля, примером векторного пространства является плоскость, а примером поля — множество рациональных чисел относительно сложения и умножения). Множество невырожденных линейных преобразований векторного пространства V образует группу и называется общей линейной группой (обозначается GL(V)). Легко проверить, что векторные пространства одинаковой размерности n над одним и тем же полем изоморфны пространству строк длины n, а множество невырожденных линейных преобразований совпадает с множеством невырожденных матриц. При этом общая линейная группа записывается в виде GLn(F). На самом деле, данный пример не является, строго говоря, новым, поскольку GL(V) ≤ SymV. Однако важностью данного класса групп обусловлено его выделение в отдельный пример. Гомоморфизм φ : G → GLn(F) называется линейным представлением группы G над полем F степени n, а пространство V называется G-модулем. Группа симметрий шара, о которой упоминалось во введении, совпадает с группой всех линейных преобразований трехмерного пространства, сохраняющих длину векторов, называемую общей ортогональной группой.



Третий пример групп возникает следующим образом. Пусть X = {x1, x2, ...} — некоторый алфавит (конечный или бесконечный). Пополним его формальными символами X–1 = {x1–1, x2–1, ...} и рассмотрим множество слов в алфавите X X–1. Введем преобразования:



(1)

вычеркивание стоящих рядом символов xixi–1 или xi–1xi;

(2)

добавление в любое место слова подслов xixi–1 или xi–1xi.

Два слова u, v назовем эквивалентными, если существует цепочка преобразований типа (1) или (2), переводящих одно слово в другое. На множестве классов эквивалентности зададим операцию умножения приписыванием одного слова в конец другому. Тогда мы получим группу, называемую свободной группой и обозначаемую через F[X], а элементы этой группы принято называть словами. Универсальность данной конструкции делает свободные группы незаменимыми при изучении формальных языков (например, языков программирования), а также различных других задач из теории кодирования, распознавания и т. д. Термин «свободная» обусловлен тем, что если у нас есть произвольная группа G и существует такое ее подмножество M, что M = G, то мы можем рассмотреть множество слов X с условием |X| = |M| и тогда существует гомоморфизм φ : F[X] → G. Ядро гомоморфизма Ker(φ) порождается некоторым множеством слов R и запись группы G в виде G = < X|R > называется заданием группы определяющими и порождающими соотношениями. Пожалуй, это самый абстрактный способ задания группы и потому самый сложный. Мы не будем приводить здесь примеров групп, заданных таким образом.



**Заключение**

На этом нам бы хотелось закончить первую часть знакомства с теорией групп. Все замечания, пожелания, отзывы будут с благодарностью прочтены автором этой заметки. Если данная тема вызовет интерес, то, возможно, появится продолжение, с обзором наиболее значимых (по мнению автора) результатов, с формулировкой наиболее известных задач и изложением некоторых методов и приемов, используемых при изучении групп.