# Аксиоматический метод (лекции, ОТиПЛ)

к.ф.-м.н., с.н.с. Е. Е. Золин*

## Содержание



*Будет справедливым отметить, что настоящим автором части курса, касающейся собственно аксиоматического метода, является проф. В.А. Успенский, и основной материал взят из его книги «Что такое аксиоматический метод?» (2001), с некоторыми изменениями, в том числе терминологического характера, и упрощениями.

# 1 Что такое аксиоматический метод

> ***Аксиоматический метод*** — это способ построения и систематизации научного знания в форме так называемых *аксиоматических теорий*, при котором некоторые утверждения выбираются в качестве исходных положений (*аксиом*), а все остальные утверждения (*теоремы*) этой теории доказывают (или выводят), исходя лишь из аксиом с помощью *чисто логических рассуждений*.

И аксиомы, и теоремы — это высказывания (утверждения) на некотором языке о некоторых *понятиях* (или *терминах*). Поэтому, прежде чем формулировать аксиомы и доказывать теоремы, мы должны договориться, о каких именно понятиях пойдет речь в излагаемой теории. Понятия делятся на два вида: одни обозначают *объекты*, которыми занимается теория, другие обозначают *отношения* между ними.

Одни понятия можно определять через другие. В какой-то момент необходимо остановиться и объявить некоторые понятия *неопределяемыми* (или *исходными*),[1] и через них определять все остальные понятия (*определяемые* или *производные*), о которых говорится в данной теории.

Итак, чтобы пользоваться аксиоматическим методом построения теории, нужно:

(1) выбрать исходные понятия;

(2) сформулировать аксиомы («исходные» утверждения) об этих понятиях;

(3) выводить новые утверждения (теоремы) о них, пользуясь логикой и аксиомами.[2]

В пунктах (2) и (3) можно вводить новые понятия (*определяемые*) через исходные и определенные ранее. Ввод новых понятий не добавляет новой информации, так как всегда можно заменить употребление этих понятий на их определение через исходные. Однако их использование позволяет сделать формулировки утверждений и доказательств короче и понятней. При этом надо следить, чтобы понятия вводились «последовательно» — каждое «следующее» новое понятие определялось через «ранее» определенные, то есть чтобы не возникал «порочный круг» (одно понятие определяется через второе, второе — через третье, и т.д., последнее — через первое).

Аналогично, в пункте (3) можно опираться не только на выбранные аксиомы, но и на доказанные «ранее» теоремы. Это позволяет делать доказательства более краткими, не доказывая одни и те же утверждения повторно. Однако, опять же надо следить за тем, чтобы теоремы доказывались «последовательно», то есть каждая «следующая» теорема опиралась на аксиомы и «предыдущие» теоремы, то есть чтобы не возникал «порочный круг».

## 1.1 Формальный аксиоматический метод

И утверждения, и доказательства можно записывать в естественном языке (скажем, русском), пользуясь «психологическим» понятием *доказательства*,[3] и тогда с помощью этого метода будет строиться (*неформальная*) *аксиоматическая теория*. Но недостатком естественного языка является то, что слова не всегда имеют ясный смысл.[4]

Можно же строить теорию иначе (повысив уровень строгости «на две ступеньки»):

---

[1] Аналогия с толковым словарем, где одни слова объясняются через другие, но некоторые слова не объяснены.

[2] А не, скажем, интуицией, наглядными представлениями, или какими-то свойствами выбранных понятий, которые имеются в нашем сознании, но не были сформулированы в виде аксиом или доказаны в качестве теорем.

[3] Согласно определению В.А. Успенского, *доказательство* — это рассуждение, которое убеждает нас настолько, что с его помощью мы готовы убеждать других.

[4] Например, высказывание «Диагонали параллелограмма, пересекаясь, делятся пополам» утверждает ли, что диагонали параллелограмма обязательно пересекаются? Или оно лишь утверждает, что «если они пересекаются, то непременно делятся пополам»? Аналогичный вопрос про высказывание «Медианы треугольника своей

**формализация языка:** фиксировать точный (*формальный*) язык, на котором будут записываться все утверждения излагаемой теории;

**формализация логики:** точно задать, что называется доказательством (одного утверждения из других), то есть строго задать, что такое упоминавшееся выше «чисто логическое рассуждение». В результате мы сможем абсолютно точно сказать, является ли некоторый данный нам текст доказательством или не является. Заметим, что при этом абсолютно точный смысл автоматически приобретет и понятие «теорема» данной теории — это такое утверждение, которое получается из данных аксиом путем доказательства.

Теория, построенная таким образом, будет называться *формальной аксиоматической теорией*, а сам описанный способ построения теории — *формальным аксиоматическим методом*.

Формализация нужна, чтобы достичь высокой (абсолютной) достоверности выводов. С позиции сегодняшнего дня мы можем сказать, что это формализовать можно всю математику, и тем самым развивать различные ее разделы (геометрию, математический анализ, алгебру, топологию, теорию вероятностей, теорию дифференциальных уравнений и т.д.) в рамках формальной аксиоматической теории; более того, в большой степени это было проделано в трудах Н. Бурбаки. Помимо цели достичь высокой достоверности и точности, в наш век развития вычислительных средств формализация позволяет поручить компьютеру многие этапы деятельности математика; например, позволяет проверить правильность доказательства, облегчить поиск самого доказательства желаемого результата, особенно, если доказательство длинное и, например, вовлекает трудоемкий перебор.

## 1.2 Возникновение аксиоматического метода

Зародился аксиоматический метод еще в Древней Греции. В знаменитом сочинении Евклида «Начала» (3 век до н.э.) были систематизированы основные известные в то время геометрические сведения. Главная же заслуга Евклида в том, что в «Началах» был развит аксиоматический подход к построению геометрии, который состоит в том, что сначала формулируются исходные положения — аксиомы («очевидные истины, не требующие доказательства»), а затем на их основе посредством рассуждений доказываются другие утверждения — теоремы.

Среди аксиом Евклида была так называемая «аксиома о параллельных прямых» (она же — «пятый постулат Евклида»). Сегодня она формулируется так:[5] «Через точку, не лежащую на данной прямой, можно провести ровно одну прямую, параллельную данной» (у Евклида была несколько иная формулировка, но эквивалентная этой, как показали более поздние ученые). По своему характеру эта аксиома сильно отличалась от остальных его аксиом, была сложнее их. Многие математики в течение почти двух тысяч лет предпринимали попытки доказать этот постулат, исходя из остальных аксиом. И лишь в 19 веке было окончательно выяснено (и в чем состоял выдающийся вклад русского математика Николая Лобачевского), что данную аксиому нельзя вывести из остальных аксиом геометрии.

---

точкой пересечения делятся в отношении 1:2». Высказывание «Существует точка пересечения у любых двух непараллельных прямых» говорит ли «существует точка $A$, такая что для любых двух непараллельных прямых $p$ и $q$ ...» или же «для любых двух непараллельных прямых $p$ и $q$ существует точка $A$, такая что ...», то есть имеет ли оно вид $\exists\forall$ или $\forall\exists$? Даже слово «два» может иметь разный смысл в разных контекстах, например, сравните «любые два числа можно сложить» (имеется в виду, два числа, не обязательно различных) и «любые два материальных тела притягиваются друг к другу» (здесь — два различных тела).

[5]Некоторые полагают, что аксиома о параллельных утверждает, что *параллельные прямые не пересекаются*. Некоторых даже не смущает, что, как они сами же знают, параллельными называются прямые, которые не пересекаются, и таким образом, аксиома становится тавтологией «Непересекающиеся прямые не пересекаются». Наконец, некоторые полагают, что вклад Н.Лобачевского состоит в том, что он доказал, что *параллельные прямые пересекаются*. Более подробно об этих «мифах» в массовом сознании, связанных с данной аксиомой, читайте в книге В.А. Успенского «Апология математики», 2009 г.

Наконец, на рубеже 19–20 веков немецкий математик Давид Гильберт, во-первых, записал евклидову геометрию в виде формальной аксиоматической теории (дописав, в том числе, некоторые недостающие аксиомы), а во-вторых, показал, что эта теория *полна*, то есть всякое утверждение можно в данной теории либо доказать, либо опровергнуть (то есть доказать его отрицание). Это было одним из величайших вкладов в развитие аксиоматического метода и подтолкнуло к последовавшей формализации всей математики.

## 1.3 Игрушечный пример аксиоматической теории

Что же представляют из себя идеальные геометрические объекты: точки, прямые, углы, плоскости и тому подобные, — отражающие наши представления о физической реальности? И в каком смысле они подчиняются аксиомам? Проще всего объяснить это с помощью хотя и искусственной, но поучительной аналогии. Выпишем следующие четыре утверждения:[6]

**Исходные понятия:** *бокр*, *куздра*, *будлать* (отношение между куздрами и бокрами).
**Аксиомы:**
(K1) *Для каждых двух бокров существует куздра, которая их будлает.*
(K2) *Два различные бокра могут будлаться не более одной куздрой.*
(K3) *Каждая куздра будлает по меньшей мере двух бокров.*
(K4) *Существуют три бокра, для которых нет такой куздры, которая их будлает.*

Ни что такое бокры, ни что такое куздры, ни что такое будлать — всё это оставляется неразъяснённым. Оказывается, однако, что разъяснения и не требуются для получения из этих утверждений определённых заключений — то есть таких утверждений, которые непременно являются истинными при условии истинности всех утверждений нашего исходного квартета. Убедимся, например, что

(K5) *Две различных куздры не могут одновременно будлать более одного бокра.*

В самом деле, если бы таких бокров было два, то они будлались бы обеими нашими куздрами, что запрещено утверждением (2). Для собственного развлечения читатель может доказать, например, такой факт:

(K6) *Для каждых двух различных бокров найдётся такой третий*[7] *бокр, что не существует куздры, будлающей всех этих трёх бокров.*

Итак, что мы имеем. Мы имеем какие-то объекты (в данном случае — бокры и куздры) и отношения между ними (в данном случае — отношение будлания). Относительно этих объектов и отношений нам не известно ничего, кроме некоторых их свойств, сформулированных в заявленных утверждениях, в данном случае — в утверждениях (K1)–(K4). Эти заявленные утверждения суть не что иное, как *аксиомы* (в данном случае — аксиомы куздрологии). Они используются для того, чтобы, принимая их в качестве истин, выводить из них *теоремы*, то есть дальнейшие утверждения о наших объектах и отношениях (одну теорему куздрологии мы доказали, другую предложили доказать читателю). Так строится любая аксиоматическая теория, в частности — геометрия.

На примере бокр, куздров и будлания мы попытались вкратце изложить суть аксиоматического метода. Несколько заключительных замечаний относительно этого примера. Заменим в

[6]Употребляемые в них странные слова заимствованы у выдающегося отечественного языковеда Льва Владимировича Щербы, который в двадцатых годах XX века учил студентов извлекать максимум лингвистической информации из фразы: *Глокая куздра штеко будланула бокра и курдячит бокрёнка.*

[7]В формулировке утверждения слово «третий» не подразумевает, что он обязательно отличен от двух предыдущих. Однако, в данном конкретном случае легко понять, что он непременно будет отличным от них.

вышеприведённых аксиомах (K1)–(K4) слово «бокр» на слово «точка», слово «куздра» на слово «прямая», слово «будлать» на выражение «проходить через». Если какая-то прямая проходит через какую-то точку, то будем говорить — с тем же смыслом — также, что эта точка «лежит» на этой прямой. Аксиома (K3) превратится тогда в такое утверждение:

(A3) *На каждой прямой лежат по меньшей мере две точки.*

Аналогично, аксиомы (K1), (K2) и (K4) превратятся в утверждения (A1), (A2) и (A4), которые мы просим любезного читателя образовать самостоятельно. Утверждения (K1)–(K4) составляют в своей совокупности группу так называемых «аксиом принадлежности» планиметрии, регулирующих то, как точки связаны с прямыми.

Читатель может теперь перевести аксиому о параллельных на язык бокр: *Для бокра, не будлаемого заданной куздрой, существует не более одной куздры...* (благоволите продолжить).

**Упражнение 1.** Выводится ли в куздрологии, что существует бокр? Существуют два бокра? Три бокра? Четыре бокра? А сколько (как минимум) существует куздр?

**Упражнение 2.** Выводится ли аксиома (K1) из остальных трех аксиом? А аксиома (K2)?

Система аксиом называется *непротиворечивой*, если из нее нельзя вывести противоречие — то есть некоторое утверждение и его отрицание.

**Упражнение 3.** Является ли система аксиом «Куздрология» непротиворечивой?

Чтобы решить эти задачи, нужно понятие *модели*.

Предъявим набор объектов и отношений между ними, удовлетворяющий системе аксиом Куздрологии. Возьмем три бокра b1, b2, b3 и три куздры z1, z2, z3, и пусть каждая куздра будлает ровно двух бокров с отличными от нее индексами. Проверьте, что все аксиомы выполены. Однако утверждение «Существует по меньшей мере четыре бокра» не выполняется. Поэтому оно и не выводится. Ведь если бы это утверждение можно было доказать чисто логическими рассуждениями из данных аксиом, то оно было бы верно (истинно) и для предъявленных выше объектов.

Если бы система аксиом Куздрологии была бы противоречива, то в ней бы можно было доказать два противоречащих друг другу утверждения, а значит, и любое вообще утверждение о бокрах, куздрах и отношении «будлать». Но, как мы увидели выше, некоторые утверждения в ней доказать нельзя. Итак, система аксиом Куздрологии непротиворечива.

Про невыводимость аксиом (K1) и (K2) мы поговорим позже, в терминах точек и прямых. Впрочем, можно и здесь предъявить контрпримеры.

# 2 Аксиомы геометрии (планиметрии) Гильберта

## 2.1 Аксиомы принадлежности

**Исходные понятия:** *точка*, *прямая*, *лежать на*. Наряду с фразой «точка лежит на прямой» будем пользоваться (исключительно с целью внести разнообразие в нашу речь) синонимами: «точка принадлежит прямой», «прямая проходит через точку».

**Примечание.** Там, где слово «два» означает «два различных», слово «различные» пишется явно; если же оно не написано, то в таком контексте слово «два» означает «два, включая случай, когда они совпадают друг с другом», как во фразе «Любые два числа можно сложить».

**Исходные понятия:** *точка*, *прямая*, *лежать на* («точка лежит на прямой»).
**Аксиомы:**

(A1) *Через любые две точки проходит прямая.*
(A2) *Любые две различные точки могут лежать не более чем одной прямой.*
(A3) *На каждой прямой лежат по меньшей мере две точки.*
(A4) *Существуют три точки, не лежающие на одной и той же прямой.*

## 2.2 Формальная запись аксиом принадлежности

Помимо формулировки аксиом и теорем на естественном языке будем их записывать и на ***формальном языке***. Это позволит, в частности, не утруждать себя соглашениями о том, как мы понимаем одно и то же слово (например, «два») в разных контекстах — формально записанные утверждения имеют единственный точно определенный смысл.

Соглашения: точки обозначаем буквами $A, B, C, D$; прямые $p, q, r, s$; отношение «точка точка $A$ лежит на прямой $p$» будем записывать как $A \in p$. Имеется также отношение *равенства* ($=$), которым можно связывать как точки, так и прямые; например, можно писать $A = B$, $p = q$ и т.д. Для составления сложных утверждений из более простых в языке имеются

- связки *и* ($\&$), *или* ($\vee$), *не* ($\neg$), *если ... то ...* ($\Rightarrow$), *равносильно* ($\Leftrightarrow$);
- кванторы *существует* ($\exists$) и *для любого* ($\forall$).

Вспомогательные сокращения:

- запись $x \neq y$ служит обозначением для $\neg(x = y)$;
- запись $A, B \in p$ обозначает $A \in p \ \& \ B \in p$; аналогично для трех и более точек;
- запись $\exists^{\leqslant 1} x\, \Phi(x)$ обозначает $\neg\exists x \exists y\, (x \neq y \ \& \ \Phi(x) \ \& \ \Phi(y))$;
- запись «$\exists$ различные $A, B$, такие что $\Phi$» обозначает: $\exists A\ \exists B\ (A \neq B \ \ \& \ \ \Phi)$;
- запись «$\forall$ различных $A, B$ верно $\Phi$» обозначает: $\forall A\ \forall B\ (A \neq B \ \ \Rightarrow \ \ \Phi)$.

Описав формальный язык, мы можем записать в нем наши аксиомы принадлежности:

(A1) $\forall A\ \forall B\ \exists p \ \ (A, B \in p)$.
(A2) $\forall$ различных $A, B \ \ \exists^{\leqslant 1} p \ \ (A, B \in p)$.
(A3) $\forall p \ \ \exists$ различные $A, B \ \ (A, B \in p)$.
(A4) $\exists A, B, C \ \ \neg\exists p \ \ (A, B, C \in p)$.

## 2.3 Некоторые теоремы, выводимые из аксиом принадлежности

Итак, мы построили *систему аксиом* (A1)–(A4). Напомним, что

- *доказательство* (из данной системы аксиом) — это текст, оперирующий понятиями нашей теории, который обосновывает некоторое утверждение, опираясь лишь на выбранные аксиомы и используя лишь логические рассуждения;
- *теорема* (данной теории) — это утверждение, для которого имеется доказательство.

Бывают еще *леммы* — но это всего лишь теоремы, которые по каким-то причинам не слишком важны для нас (то есть отличие от теорем скорее психологическое). Докажем в нашей системе аксиом некоторые простейшие теоремы.

**Теорема 1.** *Двум различным прямым не может принадлежать более одной общей точки.*

*Доказательство.* От противного: если бы две различные прямые $p \neq q$ имели по меньшей мере две (различные!) общие точки $A \neq B$, то это противоречило бы аксиоме (A2). □

**Теорема 2.** *Для любой прямой существует точка, не лежащая на ней.*

*Доказательство.* Берем любую прямую $p$. По аксиоме (A4) существуют три точки $A, B, C$, не лежащие вместе ни на какой прямой. В частности, они не лежат вместе на прямой $p$, то есть $A \notin p$ или $B \notin p$ или $C \notin p$, что и требовалось. □

**Теорема 3.** *Для любых двух различных точек найдется точка, не лежащая с ними на общей прямой.*

Заметим, что это отличается от аксиомы (A4): в той аксиоме утверждалось существование трех точек $A, B, C$ с указанным свойством; здесь же мы утверждаем, что первые две точки — $A$ и $B$ — можно выбрать произвольно и к ним подобрать подходящую точку $C$.

*Доказательство.* Берем любые две различные точки $A$ и $B$. По аксиоме (A1) через них проходит некоторая прямая; обозначим ее $p$. По **теореме 3** есть точка, обозначим ее $C$, не лежащая на прямой $p$. Итак, точки $A, B, C$ не лежат вместе на прямой $p$. Но может они лежат вместе на какой-то другой прямой $q$? Если бы это было так, то (различные!) точки $A$ и $B$ оказались бы лежащими и на прямой $p$, и на прямой $q$ (отличной от $p$). Это противоречит аксиоме (A2). □

Мы сознательно не рисовали чертежи, чтобы не было «соблазна» воспользоваться геометрической наглядностью и использовать в рассуждениях пассажи вроде «из чертежа видно, что...». Мы же в доказательствах опирались лишь на четыре аксиомы (и логику).

**Упражнение 4.** Запишите утверждения этих теорем на формальном языке. Можно записать формально и все промежуточные утверждения, имеющиеся в доказательствах теорем.

**Упражнение 5.** Запишите формально и выведите утверждения:
(а) Существует не менее трех прямых.
(б*) Если точек не менее четырех, то и прямых не менее четырех.

**Вопрос.** Разрешима ли система аксиом (A1)–(A4)? То есть можно ли построить алгоритм, который по произвольному утверждению отвечал бы на вопрос, выводимо ли оно из данных аксиом или не выводимо? Верно ли, что если утверждение не выводимо из этих аксиом, то для него есть конечная контрмодель? (Автору ответ неизвестен, хотя, возможно, он не сложный.)

# 3 Понятия, относящиеся к системам аксиом

## 3.1 Модель системы аксиом

*Модель* системы аксиом — это (конечный или бесконечный) набор объектов и заданные на них отношения, такие что для них выполняются все аксиомы. Просто набор объектов с отношениями на них будем называть *структурой*.

Сформулируем одно утверждение, касающееся любых систем аксиом. Поскольку это утверждение не о точках, прямых или других объектах, о которых говорят изучаемые нами аксиоматические теории, а о самих теориях (об их аксиомах, теоремах, доказательствах, моделях и т.д.), то мы будем такие утверждения называть МЕТАТЕОРЕМАМИ.[8]

МЕТАТЕОРЕМА **1.** *Во всякой модели системы аксиом $\mathcal{A}$ выполняются (не только каждая аксиома из $\mathcal{A}$, но и) каждая теорема, выводимая из $\mathcal{A}$.*

*Доказательство.* Причина в том, что «чисто логические рассуждения» — это такие рассуждения, которые гарантируют истинность заключений (в любой структуре) при условии истинности посылок (в той же структуре). □

Строго доказывать эту (и другие) метатеоремы мы в этом курсе не в состоянии, поскольку для этого нужно задать строго (формально) не только язык, что мы сделали выше для нашей системы аксиом, но и понятие доказательства («чисто логического вывода»). Это технически сложнее, и будет сделано в другом курсе («Математическая логика») в виде *исчисления предикатов* (или «*логики первого порядка*»).

### 3.1.1 Совместность системы аксиом

**Определение 1.** Система аксиом называется ***совместной***, если она имеет модель.

Построим модель системы аксиом принадлежности (A1)–(A4). Возьмем три точки $A, B, C$ и три прямые $p, q, r$ и скажем, что $A, B \in r$, $A, C \in q$, $B, C \in p$. Легко проверить, что все аксиомы выполнены. Таким образом, эта система аксиом совместна.

**Задача 1.** Является моделью системы аксиом (A1)–(A4) следующая структура?
(а) ⊠ без центра, (б) ⊠ с центром, (в) полный граф на четырех точках.

**Задача 2.** В модели системы аксиом (A1)–(A4), нельзя добавить или удалить прямые (в любом количестве) так, чтобы она по-прежнему осталась моделью этой системы аксиом.

**Задача 3.** Для каждого $n \geqslant 3$ постройте модель системы аксиом (A1)–(A4), имеющую ровно $n$ точек и $n$ прямых.

**Задача 4.** В модели системы аксиом (A1)–(A4) имеется $n$ точек. Каково максимальное количество прямых в ней может быть? Приведите пример такой модели. Почему в такой модели непременно каждая прямая проходит лишь через две точки?

**Задача 5.** Можно ли построить модель системы аксиом (A1)–(A4) из 4 точек и 3 прямых?

[8] Греч. «*мета*» ($\mu\varepsilon\tau\alpha$) — после, через, за.

### 3.1.2 Изоморфные модели

Напомним, что структура состоит из объектов и отношений между ними.

**Определение 2.** Две структуры $\mathcal{M}$ и $\mathcal{N}$ называются ***изоморфными***, если между объектами из $\mathcal{M}$ и из $\mathcal{N}$ можно установить взаимно-однозначное соответствие (то есть биекцию), при которой объекты из $\mathcal{M}$, находившиеся в некотором отношении, переходят в объекты из $\mathcal{N}$, находящиеся в том же отношении, и наоборот.

**Задача 6.** Постройте все неизоморфные друг другу модели системы аксиом (A1)–(A4), имеющие 3, 4, 5 точек.

**Задача 7.** При каком минимальном числе точек $n$ можно построить две неизоморфные друг другу модели с одинаковым числом точек ($n$) и одинаковым числом прямых?

## 3.2 Непротиворечивость системы аксиом

Мы уже упоминали ранее понятие непротиворечивой системы аксиом (см. упражнение 3). Сейчас мы дадим сразу четыре определения этого понятия,[9] и покажем, что все они эквивалентны друг другу. Удобнее будет вводить понятие *противоречивой* системы, а затем просто сказать: ***непротиворечивой*** называется система, которая не является противоречивой.

**Определение 3.** Система аксиом $\mathcal{A}$ называется ***противоречивой***, если выполнено какое-то из следующих условий:

(C1) из $\mathcal{A}$ выводится Ф и ¬Ф для *некоторого* утверждения Ф;
(C2) из $\mathcal{A}$ выводится Ф и ¬Ф для *всех* утверждений Ф;
(C3) из $\mathcal{A}$ выводятся все утверждения;
(C4) из $\mathcal{A}$ выводится отрицание некоторой ее аксиомы.

**Упражнение 6.** Убедитесь, что условия (C1)–(C4) эквивалентны друг другу.

Следующее утверждение интуитивно довольно очевидно: для данных нам объектов и отношений некий факт может либо выполняться, либо не выполняться (причем обязательно либо первое, либо второе, но не одновременно оба). Например, в структуре из трех точек и трех прямых, приведенной выше, из двух утверждений «Существуют не менее двух точек» и «Существует менее двух точек» верно лишь первое; из двух утверждений «Точка $A$ лежит на прямой $p$» и «Точка $A$ не лежит на прямой $p$» верно лишь второе.

Сформулируем это наблюдение точно.

Метатеорема **2.** *В любой структуре $\mathcal{M}$ для каждого утверждения* Ф *имеет место ровно одно из двух: в $\mathcal{M}$ верно либо само утверждение* Ф*, либо его отрицание* ¬Ф*.*

*Доказательство.* Для строгого обоснования нужно строгое определение того, что значит, что утверждение верно в структуре. Это будет дано в курсе «Математической логики». □

### 3.2.1 Совместность влечет непротиворечивость

Метатеорема **3.** *Всякая совместная система аксиом непротиворечива.*

*Доказательство.* Это простое утверждение. Пусть система аксиом $\mathcal{A}$ совместна, то есть имеет некоторую модель $\mathcal{M}$. Допустим, что $\mathcal{A}$ противоречива. Тогда из нее выводится некоторое утверждение Ф и его отрицание ¬Ф. Но всё, что выводится из $\mathcal{A}$, тоже верно в $\mathcal{M}$, согласно Метатеореме 1. Но это противоречит Метатеореме 2. □

[9] Точнее, *метапонятия*, коль скоро мы различаем предметный язык и метаязык (теоремы и метатеоремы).

Теперь мы видим, что поскольку у системы аксиом (A1)–(A4) имеется модель, эта система совместна, а значит, непротиворечива. Как мы видим, предъявление некоторой структуры позволяет доказать довольно удивительную вещь — отсутствие некоторого текста! А именно, отсутствие доказательства противоречия из данной системы аксиом.

### 3.2.2 Непротиворечивость влечет совместность

Зададимся вопросом: а верно ли обратное утверждение к **Метатеореме 3**? У всякой ли непротиворечивой системы аксиом есть модель? Оказывается, да, верно. Но это уже довольно сложный результат, называемый *Теоремой о полноте логики первого порядка.*[10] Он был получен австрийским логиком Куртом Гёделем в 1930 году.

Метатеорема **4** (Гёдель, 1930)**.** *Всякая непротиворечивая система аксиом совместна.*

Поразмышляйте над тем, как в принципе можно было бы из факта отсутствия текста (!), то есть доказательства противоречия из данной системы аксиом, извлечь структуру — объекты и отношения, — в которой выполнялись бы все аксиомы данной системы.

### 3.2.3 Выводимость и следование

Как мы помним, утверждение $\Phi$ ***выводится*** из системы аксиом $\mathcal{A}$, если существует доказательство этого утверждения из данных аксиом.

**Определение 4.** Утверждение $\Phi$ ***следует*** из системы аксиом $\mathcal{A}$, если во всякой модели $M$ системы аксиом $\mathcal{A}$ утверждение $\Phi$ истинно.

Согласно Метатеореме 1, из того, что $\Phi$ выводится из $\mathcal{A}$, вытекает, что $\Phi$ следует из $\mathcal{A}$. Верно ли обратное? Оказывается, да, верно.

Метатеорема **5** (Гёдель, 1930)**.** *Утверждение выводится из системы аксиом тогда и только тогда, когда оно следует из этой системы аксиом.*

*Доказательство.* Это простое следствие того факта, что непротиворечивость и совместность равносильны (см. Метатеоремы 3 и 4). Действительно, имеем два простых факта:

- *Утверждение* $\Phi$ *выводимо из* $\mathcal{A} \iff$ *система аксиом* $\mathcal{A} \cup \{\neg\Phi\}$ *противоречива.*
  ▷ Если $\Phi$ выводится из $\mathcal{A}$, то из $\mathcal{A} \cup \{\neg\Phi\}$ выводится как $\Phi$, так и $\neg\Phi$. Обратно, пусть система $\mathcal{A} \cup \{\neg\Phi\}$ противоречива, то есть из нее выводится $P$ и $\neg P$, для некоторого утверждения $P$. Выведем $\Phi$ из $\mathcal{A}$: «Предположим противное, то есть $\neg\Phi$. Из этого предположения и аксиом $\mathcal{A}$ выводим $P$ и $\neg P$. Получили противоречие. Значит, наше предположение было неверно. Итак, мы доказали $\Phi$.» ◁

- *Утверждение* $\Phi$ *следует из* $\mathcal{A} \iff$ *система аксиом* $\mathcal{A} \cup \{\neg\Phi\}$ *несовместна.*
  ▷ Утверждение $\Phi$ следует из $\mathcal{A} \iff$ в любой модели системы $\mathcal{A}$ верно $\Phi \iff$ нет модели, в которой бы было верно $\mathcal{A}$ и $\neg\Phi \iff$ система аксиом $\mathcal{A} \cup \{\neg\Phi\}$ несовместна. ◁

Из них легко следует теорема, ибо противоречивость и несовместность равносильны. □

[10] Здесь принципиально важно, что наш формальный язык позволяет писать лишь кванторы по объектам («для любой точки», «существует прямая»), но не по более сложным вещам (по множествам, функциям, отношениям и т.п.). Именно поэтому эта логика называется логикой *первого порядка.*

**Упражнение 7.** Можно ли из системы аксиом (A1)–(A4) вывести следующие утверждения?
(а) Для любой прямой найдутся по крайней мере две точки, на ней не лежащие.
(б) Существуют параллельные прямые (сначала сформулируйте требуемое определение).
(в) Существуют пересекающиеся (но не равные) прямые.
(г) Для любой прямой найдется отличная от нее прямая, ее пересекающая.
(д) Для любой прямой найдется параллельная ей прямая.
(е) Для любой точки найдется не менее двух проходящих через нее прямых.
(ж) Для любой точки найдется не менее трех проходящих через нее прямых.

## 3.3 Независимость аксиом

Все ли выписанные аксиомы (A1)–(A4) необходимы? Нельзя ли вывести какую-нибудь из них из других аксиом? И если нет, то как это можно проверить?

**Определение 5.** *Аксиома* $\Phi$ *системы аксиом* $\mathcal{A}$ *называется* ***независимой****, если она не выводится из остальных аксиом. Иначе говоря, если* $\Phi$ *не выводится из системы аксиом* $\mathcal{A} \setminus \{\Phi\}$.

Таким образом, установить независимость какой-либо аксиомы означает доказать отсутствие текста — доказательства этой аксиомы из оставшихся аксиом. В этом (синтаксическом!) вопросе нам поможет семантика. Выше мы уже видели один прием, который позволяет доказать отсутствие текста (тогда текстом было доказательство противоречия) — для этого надо было предъявить некоторую структуру (модель).

Здесь мы будем действовать аналогично — чтобы доказать, что некоторая аксиома $\Phi$ системы аксиом $\mathcal{A}$ независима, мы будем находить структурую $\mathcal{M}$, в которой верны все аксиомы из $\mathcal{A}$, кроме $\Phi$. Такую структуру можно назвать *контрмоделью* для $\Phi$. Если бы $\Phi$ была выводима из остальных аксиом, то она должна была быть истинной в этой модели, согласно Метатеореме 1, что не так.

**Определение 6.** Система аксиом $\mathcal{A}$ называется ***независимой***, если все ее аксиомы таковы.

**Упражнение 8.** Докажите, что система аксиом (A1)–(A4) независима.

**Решение.** Предъявим контрмодель к каждой из аксиом.
(A1) независима: три точки без прямых (либо одна прямая, соединяющая две точки).
(A2) независима: модель «треугольник» плюс одна прямая, соединяющая $A$ и $B$.
(A3) независима: модель «треугольник» плюс одна прямая, не имеющая точек.
(A4) независима: $A, B \in p$ и всё. ◁

Подведем итог приему, которым мы пользовались, чтобы доказывать независимость.

Метатеорема **6.** *Аксиома* $\Phi$ *независима в системе аксиом* $\mathcal{A}$ *тогда и только тогда, когда совместна система аксиом* $\mathcal{A}'$*, полученная из* $\mathcal{A}$ *заменой аксиомы* $\Phi$ *на* $\neg\Phi$.

*Доказательство.* Это фактически переформулировка Метатеоремы 5, в которой в качестве системы аксиом надо взять нашу систему $\mathcal{A}$, из которой выкинули аксиому $\Phi$. □

## 3.4 О синтаксисе и семантике

Выписывание аксиом (на формальном или неформальном языке, доказательство теорем на их основе (чисто логическими рассуждениями), непротиворечивость системы аксиом (то есть невыводимость противоречия) — это всё «игра в слова», то есть запись одних фраз (цепочек букв) и получение новых фраз из старых по некоторым (вполне известным науке) правилам игры (правилам логического вывода). При этом непротиворечивость — это как бы гарантия, что эта игра не приведет к нежелаемым нами фразам. Всё это — *синтаксис*.

Напротив, рассмотрение структур — то есть объектов (реально существующих или умозрительных) и отношений между ними, — проверка того, что для структуры выполняются те или иные фразы (утверждения, аксиомы, теоремы), и тем самым построение модели и обнаружение совместности системы аксиом — это *семантика*. Семантика занимается приписыванием смысла понятиям и утверждениям, фигурирующим в языке теории.

| **Синтаксические понятия** | **Семантические понятия** |
|---|---|
| Понятия (исходные и определяемые), утверждения, аксиомы, теоремы, доказательства | Структуры (объекты и отношения между ними), истинность утверждения в структуре, модель |
| ***Непротиворечивость*** системы аксиом (не существует доказательства двух противоречащих друг другу утверждений) | ***Совместность*** системы аксиом (существует модель у данной системы аксиом) |
| Они равносильны согласно Метатеоремам 3 и 4. | |
| Утверждение $\Phi$ ***выводится*** из системы аксиом $\mathcal{A}$ | Утверждение $\Phi$ ***следует*** из системы аксиом $\mathcal{A}$ |
| Они равносильны согласно Метатеореме 5. | |
| Аксиома $\Phi$ ***независима*** в системе аксиом $\mathcal{A}$ (и независимость системы аксиом) | Это можно проверять семантически, предъявляя модель для $\mathcal{A} \cup \{\neg\Phi\}$, согласно Метатеореме 6. |

# 4 Аксиома о параллельных

**Определение 7.** Две прямые назовем ***параллельными***, если они не имеют общих точек.

Формально: запись $p \parallel q$ является сокращением для записи $\neg\exists A\ (A \in p\ \&\ A \in q)$.

**Упражнение 9.** Назовите пары параллельных прямых в следующих моделях:

а) полный граф на 4 точках; б) полный граф на 5 точках.

Если прямые $p$ и $q$ не параллельны, то либо они совпадают ($p = q$), либо различны, но пересекаются (обозначаем $p \cap q$), причем в единственной точке по аксиоме (A2).

Как мы видели, у системы аксиом (A1)–(A4) бывают модели, в которых нет пар параллельных прямых, и есть модели, в которых они имеются. Сформулируем аксиому, утверждающую наличие параллельных прямых (и даже нечто большее).

(A5∃) *Через всякую точку, не лежащую на данной прямой,*
***можно*** *провести прямую, параллельную данной.*

Если бы мы изучали не только аксиомы принадлежности (A1)–(A4), а все аксиомы геометрии, то утверждение (A5∃) из них бы выводилось. Но вся аксиоматика геометрии довольно сложна. Поэтому мы сосредоточились на изучении простой системы аксиом и нам приходится рассматривать утверждение (A5∃) как отдельную аксиому.

## 4.1 Аксиома Евклида

Однако интересная многовековая история с «аксиомой о параллельных» — вовсе не об утверждении о существовании параллельной прямой, а об утверждении о *единственности* параллельной прямой — вот эта *аксиома Евклида*:

(A5E) *Через всякую точку, не лежащую на данной прямой,*
*проходит* ***не более одной*** *прямой, параллельной данной.*

Вместе аксиомы (A5∃) и (A5E) утверждают, что *через всякую точку, не лежащую на данной прямой, проходит* ***единственная*** *прямая, параллельная данной.*

Будем под «Евклидовой геометрией» понимать систему аксиом (A1)–(A4), (A5∃), (A5E).

**Упражнение 10.** Докажите в Евклидовой геометрии:

(а) Будем говорить, что прямые «квазипараллельны», если они либо совпадают, либо параллельны. Докажите, что «квазипараллельность» — отношение эквивалентности.

(б) Если $p \cap q$, то найдется прямая $r$, отличная от $p$ и $q$, которая пересекает и $p$, и $q$. Более того, если $p$ и $q$ пересекались в точке $A$, то всегда найдется такая прямая $r$, что она пересекает $p$ и $q$ в точках, отличных от $A$.

(в) Если $p \parallel q$ и $p \cap r$, то $q \cap r$;

(г) Если $p \parallel q$ и $r \parallel s$, а также $p \cap r$, то $q \cap s$.

**Упражнение 11.** Убедитесь, что Евклидова геометрия — это независимая система аксиом.

**Задача 8.** Есть ли конечная модель аксиом (A1)–(A4),(A5∃), в которой для некоторых $A \notin p$ есть единственная прямая, проходящая через $A$ и параллельная $p$, а для некоторой другой $B \notin q$ есть как минимум две прямые, проходящие через $B$ и параллельные $q$?

## 4.2 Аксиома Лобачевского

Вследствие последнего упражнения (и МЕТАТЕОРЕМЫ 6) мы можем к указанной системе аксиом добавить *отрицание* аксиомы Евклида, и полученная система аксиом окажется непротиворечивой. Следующее утверждение называется *аксиомой Лобачевского*:[11]

(A5L) *Через всякую точку, не лежащую на данной прямой,*
*проходит* ***более одной*** *прямой, параллельной данной.*

Будем под «геометрией Лобачевского» понимать систему аксиом (A1)–(A4), (A5∃), (A5L).

**Упражнение 12.** Убедитесь, что геометрия Лобачевского — это независимая система аксиом.

В полной геометрии Лобачевского (включающей не только аксиомы принадлежности) выводятся странные для нас утверждения, например:

– сумма углов треугольника всегда меньше двух прямых углов (и у разных треугольников она может быть разной);

– если два треугольника подобны, то они равны.

Под «абсолютной геометрией» понимается геометрия, не использующая ни аксиомы Евклида, ни аксиомы Лобачевского. Вот пример утверждения абсолютной геометрии:

– сумма углов треугольника не превосходит суммы двух прямых углов.

[11] Оно более сильное, чем просто отрицание аксиомы Евклида, но обычно рассматривают именно его, ибо можно доказать (исходя из остальных аксиом, не только аксиом принадлежности), что если для некоторой точки $A$ и некоторой прямой $p$, таких что $A$ не лежит на $p$, можно через $A$ провести более одной прямой, параллельной $p$, то это же можно сделать и для любых других точек $B$ и прямых $q$, таких что $B$ не лежит на $q$.

# 5 Теория множеств Кантора

(Формальная) теория множеств — аксиоматическая теория, лежащая в основе всей (или почти всей) математики. Мы не будем изучать ее аксиомы, так как они довольно сложны для начинающих. Здесь мы рассмотрим некоторую упрощенную систему аксиом, которую будем называть *канторовской* (или наивной) теорией множеств, и попытаемся понять, что именно она «знает» про множества и вообще какие понятия в ней можно выразить.

**Исходные понятия:** *множество*; отношение *принадлежать* $\in$ (и, как всегда, равенство $=$).

Таким образом, наша теория будет говорить исключительно о множествах. Для обозначения множеств будем использовать любые буквы в любом регистре ($x, y, A, B, a, b, M, N, f, R, S, \ldots$). Запись $x \in y$ читаем как «$x$ принадлежит $y$» или «$x$ является *элементом* множества $y$».

### Аксиомы

(M1) *Множества равны тогда и только тогда, когда они у них одни и те же элементы:*

$$\forall x, y \ \big( x = y \quad \leftrightarrow \quad \forall a \, (a \in x \leftrightarrow a \in y) \big).$$

Фактически, эта аксиома позволяет считать, что равенство можно считать производным понятием, определяемым через отношение принадлежности.

(M2) *Каждое свойство* $\Phi$ *задает множество* $M$ *всех объектов, удовлетворяющих свойству* $\Phi$.

Это целая серия аксиом — по одной для каждого выражения $\Phi$ языка теории множеств:

- для каждого выражения $\Phi(x)$ с одним параметром[12] $x$ получается аксиома:

$$\exists M \ \forall x \ \big( x \in M \quad \leftrightarrow \quad \Phi(x) \big);$$

- для каждого выражения $\Phi(x, A)$ с параметрами $x$ и $A$ получается аксиома:

$$\forall A \ \exists M \ \forall x \ \big( x \in M \quad \leftrightarrow \quad \Phi(x, A) \big);$$

- для каждого выражения $\Phi(x, A, B)$ с параметрами $x, A, B$ получается аксиома:

$$\forall A, B \ \exists M \ \forall x \ \big( x \in M \quad \leftrightarrow \quad \Phi(x, A, B) \big);$$

- аналогично для выражения $\Phi(x, A_1, \ldots, A_n)$ с параметрами $x, A_1, \ldots, A_n$.

Посмотрим, существование каких множеств можно установить в этой системе аксиом.

- В качестве $\Phi(x)$ возьмем $x \neq x$. Получится утверждение: $\exists M \ \forall x \ \big( x \in M \quad \leftrightarrow \quad x \neq x \big)$. Но выражение $x \neq x$ всегда ложно. Значит, $M$ — такое множество, не имеющее элементов, то есть пустое множество. Введем для него обозначение: $M = \varnothing$. Таким образом, этот частный случай аксиомы (M2) утверждает существование пустого множества.

- В качестве $\Phi(x)$ возьмем $x = x$. Как выше, получим, что элементом множества $M$ является любое множество $x$. Итак, утверждается, что существует множество всех множеств.[13]

- В качестве $\Phi(x, A, B)$ возьмем $(x \in A) \,\&\, (x \in B)$. Получим: $x \in M \leftrightarrow (x \in A) \,\&\, (x \in B)$. Значит, что для любых множеств $A$ и $B$ существует их пересечение $M = A \cap B$.

- Аналогично для объединения $M = A \cup B$ надо взять $(x \in A) \vee (x \in B)$.

[12] Под *параметром* надо понимать переменную, не «связанную» никаким квантором. См. примеры ниже.

[13] В «настоящей» математике его не существует. Наша система аксиом далека от настоящей математики!

- Введем обозначение $A \subseteq B$ для $\forall z\,(z \in A \to z \in B)$. Смысл: $A$ — подмножество $B$.
- В качестве $\Phi(x, A)$ возьмем $x \subseteq A$. Получим: $\forall A\ \exists M\ \forall x\ \big(x \in M \quad \leftrightarrow \quad x \subseteq A\big)$. Значит, существует множество всех подмножеств множества $A$. Введем обозначение: $M = \mathcal{P}(A)$.

  **Упражнение 13.** Сколько элементов в множестве $\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing)))$? Выпишите их.

- В качестве $\Phi(x, a)$ возьмем $x = a$. Получим: $\forall a\ \exists M\ \forall x\ \big(x \in M \quad \leftrightarrow \quad x = a\big)$. Значит, множество $M$ имеет единственный элемент — $a$. Тем самым утверждается, что для любого множества $a$ существует одноэлементное множество, которое мы обозначим $M = \{a\}$.
- В качестве $\Phi(x, a, b)$ возьмем $(x = a) \vee (x = b)$. Получим: $x \in M \leftrightarrow (x = a) \vee (x = b)$. Элементами множества $M$ являются лишь $a$ и $b$. Это — *неупорядоченная пара* $M = \{a, b\}$.
- Введем *упорядоченную пару* как $\langle a, b\rangle := \{a, \{a, b\}\}$. В нашей системе можно доказать:

  **Лемма 4** (Основное свойство упорядоченных пар)**.** $\langle a, b\rangle = \langle c, d\rangle \implies a = c\ и\ b = d$.

  **Упражнение 14.** а) Докажите лемму. б) Какое выражение $\Phi(x, a, b)$ даст $M = \langle a, b\rangle$?

- Существование *декартова произведения* $M = A \times B$ утверждается в следующем частном случае аксиомы (M2): $\forall A, B\ \exists M\ \forall x\ \big(x \in M \ \leftrightarrow\ \exists a, b\ (a \in A \,\&\, b \in B \,\&\, x = \langle a, b\rangle)\big)$.
- Далее можно определять все известные понятия: разность множеств, бинарное отношение, функция, биекция, равномощность; доказывать теорему Кантора ($|A| < |\mathcal{P}(A)|$); теорему Кантора–Бернштейна (любые два множества сравнимы по мощности).

  **Упражнение 15.** Выразите: «$R$ — отношение эквивалентности на множестве $A$».

- Можно ввести («закодировать») натуральные числа: $0 := \varnothing$, $n{+}1 := n \cup \{n\}$.

  **Упражнение 16.** Выпишите явно числа $0, 1, 2, 3, 4$. Какова мощность множества $n$?

- Далее можно ввести множества $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, развивать в рамках этой теории множеств алгебру, анализ, геометрию, даже математическую логику и теорию алгоритмов и т.п.
- Однако возникает проблема. В качестве $\Phi(x)$ возьмем $x \notin x$. Тогда аксиома (M2) даст: $\exists M$ $\forall x\ \big(x \in M \ \leftrightarrow\ x \notin x\big)$. Поскольку это верно $\forall x$, то верно и для $x = M$, и мы получаем: $M \in M \leftrightarrow M \notin M$, то есть противоречие (***парадокс Рассела***).[14] Таким образом, данная система аксиом противоречива и в ней выводится любое утверждение!

Как же исправить ситуацию? Один из способов — ослабить аксиому (M2). Так была построена теория множеств Цермело–Френкеля ZF. В ней (и в некоторых ее расширениях, например, аксиомой выбора) можно развивать значительную часть математики, как мы делали выше. Но можно ли теперь быть уверенными, что система ZF, на которой основана математика, непротиворечива? К. Гёдель показал, что такие выразительные системы, способные говорить о натуральных числах, способны (посредством кодирования) говорить и о своих выражениях, о доказательствах, о непротиворечивости, и верна следующая теорема:[15]

**Теорема Гёделя о неполноте (для ZF):** *Если ZF непротиворечива, то утверждение «ZF непротиворечива» недоказуемо* ***в самой системе ZF****.*

[14] Первоначально данную систему аксиом, на неформальном уровне, изучал Г. Кантор, позже Г. Фреге записал ее формально. Лишь спустя некоторое время Б. Рассел обнаружил в ней указанное противоречие.

[15] В оригинале она была получена не для ZF, а системы, формализующей арифметику натуральных чисел.

# 6 Теория групп

Рассмотрим два примера структур и выделим в них общие свойства.

**Пример 1.** $(\mathbb{Z}, +)$ — множество целых чисел с операцией сложения. Известны свойства:
**а)** $x + (y + z) = (x + y) + z$ — ассоциативность сложения;
**б)** Есть число, которое при сложении с любым числом $x$ дает его же. А именно, это число 0, ибо $x + 0 = x$ и $0 + x = x$;
**в)** У каждого числа $x$ есть обратное, то есть такое $y$, что $x + y = 0$ и $y + x = 0$. Именно, $y = -x$.

Кроме того, выполняется еще и свойство:
**г)** Сумма не зависит от порядка слагаемых: $x + y = y + x$.

**Пример 2.** $(M, \circ)$, где $M$ — множество поворотов треугольника на плоскости.[16] Операция — композиция (последовательное выполнение) поворотов. Легко понять, что $M = \{\varphi_0, \varphi_1, \varphi_2\}$, где $\varphi_\kappa$ — поворот на $\kappa \cdot 120^\circ$ (для определенности, против часовой стрелки).

Вспомним, что повороты — это движения плоскости, а движения — это отображения плоскости в себя (то есть функции), сохраняющие расстояния между точками. Композиция функций, как всегда, понимается «справа налево»: чтобы получить результат применения функции $f \circ g$ к точке $x$, нужно сначала применить $g$ к $x$, а затем к результату применить $f$, то есть $(f \circ g)(x) := f(g(x))$. Композиция функций ассоциативна.[17]

В множестве $M$ есть элемент $\varphi_0$, такой что $\varphi_0 \circ \varphi = \varphi$ и $\varphi \circ \varphi_0 = \varphi$ для любого $\varphi \in M$.

Для любого элемента $\varphi \in M$ имеется элемент $\psi \in M$, такой что $\varphi \circ \psi = \varphi_0$ и $\psi \circ \varphi = \varphi_0$. Для $\varphi_0$ — это $\varphi_0$, для $\varphi_1$ — это $\varphi_2$, для $\varphi_2$ — это $\varphi_1$.

Таким образом, структура $(M, \circ)$ тоже обладает свойствами а) б) в). Кроме того, она обладает также и свойством г), что можно проверить перебором.

Структуры, обладающие свойствами а), б), в), называются *группами*. Структуры, дополнительно обладающие свойством г), называются *коммутативными группами*.

## 6.1 Определениие группы

**Определение 8.** *Двуместной* (или *бинарной*) *операцией* на множестве $M$ называется отображение, которое ставит каждой упорядоченной паре элементов из $M$ некоторый (единственный) элемент из $M$. Другими словами, это функция $M \times M \to M$.

Например, сложение является бинарной операцией на множестве натуральных чисел, тогда как вычитание — не является. Заметим, что порядок элементов в паре важен — паре $(a, b)$ и паре $(b, a)$ операция вполне может сопоставлять разные элементы.

**Определение 9.** *Группа* — это пара $(G, \circ)$, состоящая из непустого множества $G$ и двуместной операции $\circ$ на нем (называемой *групповым умножением*), удовлетворяющая *аксиомам группы*:

(Г1) $\forall x\ \forall y\ \forall z \quad (x \circ y) \circ z = x \circ (y \circ z)$ (*аксиома ассоциативности*)

(Г2) $\exists e\ \forall x \quad x \circ e = x$ и $e \circ x = x$ (*существует нейтральный элемент*)

(Г3) $\forall x\ \exists y \quad x \circ y = e$ и $y \circ x = e$ (*у каждого элемента существует обратный*)

Группа называется *коммутативной* (или *абелевой*), если выполняется также и аксиома:

(Г4) $\forall x\ \forall y \quad x \circ y = y \circ x$ (*аксиома коммутативности*)

*Порядком* (или размером) группы называется число элементов во множестве $G$ (более точно — мощность этого множества). Обозначение: $|G|$.

[16] Мы будем отождествлять повороты, отличающиеся друг от друга на полный оборот.

[17] Напомним доказательство. Пусть даны три функции: $X \xrightarrow{h} Y \xrightarrow{g} Z \xrightarrow{f} V$. Докажем: $(f \circ g) \circ h = f \circ (g \circ h)$. Чтобы доказать, что две функции равны, надо применить их к любому элементу из $X$ и убедиться, что результаты равны. Это легко: $[(f \circ g) \circ h](x) = [f \circ g](h(x)) = f(g(h(x)))$ и $[f \circ (g \circ h)](x) = f([g \circ h](x)) = f(g(h(x)))$.

Примеры групп и не групп: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ относительно сложения; они же относительно умножения; они же без нуля; они же положительные. В будущем, для множества чисел $M \subseteq \mathbb{R}$ будем обозначать $M^* = \{x \in M \mid x \neq 0\}$, $M^+ = \{x \in M \mid x > 0\}$. Четные целые числа по сложению. Нечетные числа (сложение на них — не операция). Какие из них — абелевы?

Примеры: $(\{\pm 1\}, \cdot)$, $(\{1\}, \cdot)$, $(\{0\}, +)$, $(\{0\}, \cdot)$. Последние две — это одна и та же структура!

**Теорема 5.** *В группе нейтральный элемент единственен.*

*Доказательство.* Допустим, элементы $e$ и $e'$ — нейтральные. Тогда $e = e \circ e' = e'$. □

Только теперь аксиома (Г3) приобрела корректный смысл, иначе же можно было задаться вопросом — какой именно нейтральный элемент $e$ фигурирует в этой аксиоме?

**Теорема 6.** *В группе у любого элемента обратный элемент единственен.*

*Доказательство.* Если $y$ и $y'$ — обратные к $x$, то $y = y \circ e = y \circ (x \circ y') = (y \circ x) \circ y' = e \circ y' = y'$. □

Теперь мы вправе ввести обозначение для обратного элемента: $y := x^{-1}$.

**Пример 3.** Еще примеры групп:

– (векторы на плоскости, выходящие из начала координат; сложение) — абелева группа.

– (движения[18] плоскости; композиция). Это неабелева группа: поворот на 90° вокруг начала координат и отражение относительно оси Ox не коммутируют.

– Отдельно сдвиги, отдельно повороты вокруг начала координат — абелевы группы.

– Отдельно отражения относительно всевозможных прямых — не группа.

– (преобразования подобия[19] плоскости; композиция) — неабелева группа.

**Задача 9.** Пусть $M = \mathbb{Q} + \sqrt{2}\mathbb{Q} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Группы ли $(M, +)$, $(M^*, \cdot)$, $(M^+, \cdot)$?

Еще примеры групп: (все движения правильного $n$-угольника, оставляющие его на месте, композиция) — называется *группой симметрий правильного $n$-угольника.* В ней $2n$ элементов. Из них вращения вокруг центра составляют тоже группу размера $n$.

**Задача 10.** Пусть $a \circ a = e$ для всех элементов $a$ группы $(G, \circ)$. Тогда эта группа абелева.

*Таблица умножения* (или *таблица Кэли*) конечной группы — это квадратная таблица, где над столбцами выписаны элементы группы, перед строками — тоже, в том же порядке, и на пересечении строки $a_i$ и столбца $a_j$ стоит результат умножения $a_i \circ a_j$.

**Пример 4.** Приведем пример группы из 4 элементов $\{e, a, b, c\}$, в которой порядок каждого неединичного элемента равен двум. Такая группа даже единственная, так как таблица умножения восстанавливается из указанных условий однозначным образом. Получающаяся группа называется *четвертной группой Клейна* и обозначается $V_4$. Ее таблица умножения:

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $\boldsymbol{e}$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $\boldsymbol{e}$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $\boldsymbol{e}$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $\boldsymbol{e}$ |

Докажите, что группа $V_4$ изоморфна группе симметрий ромба, не являющегося квадратом.

**Задача 11.** Рассмотрим 4 функции из $\mathbb{R}^*$ в $\mathbb{R}^*$: $f_0(x) = x$, $f_1(x) = -x$, $f_2(x) = 1/x$, $f_3(x) = -1/x$. Доказать, что относительно композиции они образуют группу, составить таблицу умножения, выяснить, коммутативна ли эта группа. (На будущее: изоморфна ли она $\mathbb{Z}_4$ или $V_4$?)

[18] *Движение* — это биекция плоскости, сохраняющая расстояние между точками. **Теорема.** *Любое движение плоскости есть композиция поворота, параллельного переноса (сдвига) и отражения относительно прямой.*

[19] *Преобразование подобия* — биекция, изменяющая расстояния между точками в одинаковое число раз.

## 6.2 Свойства групп

Пусть $(G, \circ)$ — произвольная группа. Тогда в ней выполняются следующие свойства:

1. В произведениях трех и более сомножителей скобки можно расставлять любым способом — результат от этого не зависит. Например: $a \circ (b \circ (c \circ d)) = (a \circ b) \circ (c \circ d) = ((a \circ b) \circ c) \circ d$. Поэтому в дальнейшем вы вообще будем опускать скобки в произведениях.

2. $e^{-1} = e$.

3. $(a^{-1})^{-1} = a$.

4. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ (пиджак одевают после рубашки, а снимают до нее).

5. $(a_1 \circ \ldots \circ a_n)^{-1} = {a_n}^{-1} \circ \ldots \circ {a_1}^{-1}$, для любого числа множителей $n \geqslant 2$.

   Введем целочисленные *степени* элемента $a \in G$:

   $a^n := \underbrace{a \circ \ldots \circ a}_{n \text{ множителей}}$ для $n \geqslant 1$; $\quad a^0 := e$; $\quad a^{-n} = (a^n)^{-1}$ для $n \geqslant 1$.

6. Свойства степеней: $a^{m+n} = a^m \circ a^n$, $(a^m)^n = a^{mn} = (a^n)^m$, $a^{-n} = (a^n)^{-1} = (a^{-1})^n$, $e^n = e$.

   **Определение 10.** ***Порядок*** элемента $a \in G$ — это наименьшая *положительная* степень, в которую надо возвести данный элемент, чтобы получить нейтральный элемент; то есть это наименьшее целое число $n \geqslant 1$, такое что $a^n = e$. Если такого числа $n$ не существует, то говорят, что $a$ — элемент *бесконечного порядка*. Порядок элемента обозначается $|a|$; если же это можно спутать с модулем числа, то используют обозначение $\mathsf{ord}(a)$.

7. Разрешимость уравнений (или «возможность деления слева и справа»):
   $\forall a, b \; \exists! x \quad a \circ x = b$. А именно, $x = a^{-1} \circ b$.
   $\forall a, b \; \exists! y \quad y \circ a = b$. А именно, $y = b \circ a^{-1}$.

8. Законы сокращения слева и справа:
   слева: $a \circ x = a \circ y \implies x = y$;
   справа: $x \circ a = y \circ a \implies x = y$.

**Теорема 7.** *Ассоциативность и разрешимость уравнений (даже без требования единственности решения) — достаточные условия для того, чтобы получилась группа.*

*Доказательство.* Возьмем любой элемент $a \in G$. Решим уравнение $ax = a$. Получим некоторый элемент $c \in G$, такой что $ac = a$. Докажем, что он является и левым, и правым нейтральным элементом.

Для любого $b \in G$ проверим, что $bc = b$. Для этого возьмем решение уравнения $ya = b$. Тогда имеем: $bc = yac = ya = b$. Итак, $c$ — правый нейтральный элемент (мы воспользуемся этим ниже).

Для любого $b \in G$ проверим, что $cb = b$. Для этого возьмем $c'$ — решение уравнения $zb = b$. Значит, $c'b = b$, то есть именно для этого элемента $b$ элемент $c'$ является левым нейтральным. Докажем, что $c = c'$. Для этого еще возьмем такой $d$, что $bd = c$. Теперь имеем: $c' = c'c = c'bd = bd = c$.

Более того, как и раньше, мы можем доказать, что (левый и правый) нейтральный элемент — единственен. Теперь мы можем обозначить его через $e$.

Существование обратных у каждого элемента доказывается просто: у уравнений $ax = e$ и $ya = e$ имеются решения — они и будут обратными (слева и справа). Можно даже убедиться, что они совпадают: $x = ex = yax = ye = y$ (как и прежде). □

**Замечание 1.** $(\mathbb{N}, +)$ — ассоциативность и законы сокращения верны, но это не группа.

**Задача 12.** Пусть $(G, \circ)$ — группа, $a, b, c \in G$. Докажите:
а) $|a \circ b| = |b \circ a|$.
б) $|a \circ b \circ c| = |b \circ c \circ a| = |c \circ a \circ b|$.
в) Если $a$ и $b$ коммутируют, то $a^{-1}$ и $b^{-1}$ — тоже.
г) Если $a$ и $b$ коммутируют, то $a$ и $b^{-1}$ — тоже, а также $a^{-1}$ и $b$.

## 6.3 Циклические группы

Пусть $(G, \circ)$ — группа, $a \in G$. Будем возводить элемент $a$ во всевозможные степени (как положительные, так и отрицательные). Если при этом мы исчерпаем всё множество $G$, то говорят, что данная группа является *циклической* группой, *порожденной* элементом $a$. Сам элемент $a$ при этом называется *порождающим*. Обозначение: $G = \langle a \rangle$.

Если при этом среди степеней элемента $a$ лишь конечное число различных элементов, то группа $(G, \circ)$ будет *конечной циклической группой*: $G = \{e = a^0, a = a^1, a^2, \ldots, a^{n-1}\}$. В противном случае это *бесконечная циклическая группа.*

**Пример 5.** Группа $(\mathbb{Z}, +)$ — порождена элементом 1; она же порождена элементом $-1$. Значит, это — бесконечная циклическая группа, а именно, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

**Пример 6.** *Группа вычетов по модулю $n$* — это группа $(\mathbb{Z}_n, \oplus)$, где $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, а операция $\oplus$ задана так: $a \oplus b = (a+b) \bmod n$ — сумма по модулю $n$, то есть отстаток от деления суммы $a + b$ на $n$. Нейтральный элемент 0. Группа коммутативна. Она порождена элементом 1, а также элементом $n-1$. Бывают и другие порождающие (см. задачу 13 ниже).

**Лемма 8.** *Всякая циклическая группа абелева.*

*Доказательство.* Следует из тождества $a^m \circ a^n = a^{m+n} = a^n \circ a^m$. □

**Лемма 9.** *Если $|a| = n$, то элементы $\{a^0 = e,\ a^1 = a,\ a^2,\ \ldots,\ a^{n-1}\}$ попарно различны.*

*Доказательство.* Допустим, некоторые из них совпадают: $a^k = a^\ell$ для некоторых $0 \leqslant k < \ell < n$. Это равенство можно переписать как $a^k \circ e = a^k \circ a^{\ell-k}$. Сокращая на $a^k$, получаем $e = a^{\ell-k}$. Но $0 < \ell - k < n$. Получилось, что мы нашли положительную степень, меньшую чем $n$, в которой $a$ дает нейтральный элемент. Это противоречит минимальности $n$. □

Из этой леммы вытекает следующий факт.

**Лемма 10.** *Пусть $(G, \circ)$ — группа порядка $|G| = n$, $a \in G$. Тогда:*

$$(G, \circ) \text{ — циклическая группа, порожденная элементом } a \quad \Longleftrightarrow \quad |a| = n.$$

*Доказательство.* $G$ порождена элементом $a \Longleftrightarrow G = \{e, a, a^2, \ldots, a^{n-1}\}$. Значит, перечисленные элементы попарно различны. Это возможно тогда и только тогда, когда $|a| = n$. □

**Задача 13.** Элемент $k \in \mathbb{Z}_n$ — порождающий в $\mathbb{Z}_n \Leftrightarrow$ числа $k$ и $n$ взаимно просты, то есть НОД($k$,$n$)=1 $\Leftrightarrow$ элемент $k$ имеет порядок $n$.

**Задача 14.** Порядок любого элемента $k \in \mathbb{Z}_n$ равен: $\mathsf{ord}(k) = \dfrac{n}{\text{НОД}(k, n)}$.

## 6.4 Группа подстановок

*Подстановкой* (или *перестановкой*) $n$ элементов называется всякая биекция из множества $M = \{1, \ldots, n\}$ в $M$. Каждая подстановка записывается в виде таблицы из двух строк, где во второй строке стоят числа $1, \ldots, n$ в каком-то порядке: $P = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$. *Тождественная подстановка* обозначается $I = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$. Множество всех подстановок $n$ элементов обозначается $S_n$.

**Вопрос.** Чему равно количество всех перестановок $n$ элементов, то есть $|S_n|$?

Подстановки можно перемножать, то есть выполнять одну за другой. Запись $P \circ Q$ означает, как и в случае композиции функций, что сначала выполняется $Q$, а затем $P$. Композиция является ассоциативной. Нейтральным элементом является $I$. Подстановкой, обратной к $P = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$, является $P^{-1} = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ 1 & 2 & \ldots & n \end{pmatrix}$, лишь нужно переставить столбцы в «стандартном» порядке. Итак, $(S_n, \circ)$ — группа.

**Пример 7.** Пусть $P = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ и $Q = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Тогда $P \circ Q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ и $Q \circ P = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

В этом примере $P \circ Q \neq Q \circ P$. Значит, группа $(S_3, \circ)$ не абелева. Передейлайте этот пример в пример, показывающий, что при любом $n \geqslant 3$ группа $(S_n, \circ)$ не абелева.

Как и в любой группе, у каждой подстановки $P$ есть *порядок* — наименьшее целое число $n \geqslant 1$, такое что $P^n = I$. В примере выше имеем $|P| = 3$ и $|Q| = 2$.

### 6.4.1 Циклические подстановки

*Циклической подстановкой* (или просто *циклом*) называется подстановка $P$, которая на некоторых элементах $1 \leqslant k_1, \ldots, k_s \leqslant n$ действует «циклическим сдвигом»: $k_1 \mapsto k_2 \mapsto \ldots \mapsto k_s \mapsto k_1$, а остальные числа из множества $\{1, \ldots, n\}$ оставляет на месте. Такую подстановку записывают проще: $P = (k_1\, k_2\, \ldots\, k_s)$. Число $s$ называется *длиной* цикла $P$.

Например, $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 7 & 4 & 3 & 6 & 2 \end{pmatrix} = (2\,5\,3\,7)$ — циклическая подстановка длины 4.

Очевидно, порядок циклической подстановки равен ее длине: $|P| = s$.

Две циклические подстановки $P = (k_1\, k_2\, \ldots\, k_s)$ и $Q = (\ell_1\, \ell_2\, \ldots\, \ell_r)$ называются *независимыми*, если множества «сдвигаемых» ими чисел, то есть $\{k_1, \ldots, k_s\}$ и $\{\ell_1, \ldots, \ell_r\}$, не пересекаются.

**Задача 15.** Пусть $P$ и $Q$ — независимые циклы. Докажите: а) $P \circ Q = Q \circ P$;
б) $|P \circ Q| = \text{НОК}(|P|, |Q|)$. Аналогично для произведения нескольких независимых циклов.

**Теорема 11.** *Всякую подстановку можно представить в виде произведения независимых циклов. Такое представление единственно с точностью до порядка сомножителей.*

*Доказательство.* Предъявим алгоритм разложения подстановки на независимые циклы. Берем подстановку $P$, ищем наименьший элемент, не оставляемый ею на месте, и выписываем цикл, содержащий этот элемент. Как только цикл выписан, ищем наименьший элемент, не вошедший в уже выписанный цикл и не оставляемый подстановкой $P$ на месте, и выписываем цикл, содержащий этот элемент. Так продолжаем до тех пор, пока все не оставляемые подстановкой элементы будут выписаны.

Например, $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 2 & 4 & 7 & 6 & 1 & 9 & 3 \end{pmatrix} = (1\,5\,7)(2\,8\,9\,3)(4)(6)$.

Единственность следует из того, что каждое чичло принадлежит лишь одному циклу.[20] $\square$

[20] Если каждый цикл записывать, начиная с наименьшего входящего в него числа, а разные циклы выписывать в порядке возрастания первого выписанного в них элемента, то разложение будет единственным.

### 6.4.2 Транспозиции

*Транспозиция* — это цикл длины 2. Например, $P = \binom{1\,2\,3\,4\,5}{1\,2\,5\,4\,3} = (3\,5)$ — это транспозиция.

**Лемма 12.** *Всякую подстановку можно разложить в произведение транспозиций.*

*Доказательство.* С учетом теоремы 11 достаточно показать, как разложить цикл на транспозиции. Мы приведем пример, на его основе общую «формулу» выпишите самостоятельно: $(1\,2\,3\,4\,5) = (1\,2)(2\,3)(3\,4)(4\,5) = (1\,5)(1\,4)(1\,3)(1\,2)$. Видно, что разложение не единственно. □

**Задача.** Придумайте третий способ разложить цикл $(1\,2\,3\,4\,5)$ на 4 транспозиции.
Количество транспозиций в разложении тоже может быть разным: $(1\,3) = (1\,2)(2\,3)(1\,2)$.
Как мы увидим ниже, неизменна четность числа транспозиций в разложении.
**Задача.** Какие подстановки разлагаются в произведение *независимых* транспозиций?

### 6.4.3 Четность подстановки

*Инверсией* (или *беспорядком*) в подстановке $P = \binom{1\ 2\ \dots\ n}{i_1\ i_2\ \dots\ i_n}$ называется упорядоченная пара чисел $\langle k, \ell\rangle$, такая что $k > \ell$, но в нижней строке число $k$ стоит левее числа $\ell$. Подстановка $P$ называется *четной*, если в ней четное число инверсий; в противном случае — *нечетной*. Множество всех четных подстановок $n$ элементов обозначим $A_n$.

Например, подстановка $P = \binom{1\,2\,3\,4\,5}{1\,5\,2\,4\,3}$ четная, ибо в ней 4 инверсии: $\langle 5,2\rangle$, $\langle 5,4\rangle$, $\langle 5,3\rangle$, $\langle 4,3\rangle$.

**Лемма 13.** *Четность подстановки меняется при умножении на транспозицию слева.*[21]

*Доказательство.* При умножении на транспозицию $(i\,j)$ у подстановки в нижней строке меняются местами числа $i$ и $j$: $(i\,j) \circ \binom{\dots\ k\ \dots\ \ell\ \dots}{\dots\ i\ \dots\ j\ \dots} = \binom{\dots\ k\ \dots\ \ell\ \dots}{\dots\ j\ \dots\ i\ \dots}$.

Свойство «быть инверсией» поменялось, во-первых, у пары $\langle i, j\rangle$, а во-вторых, у всех пар вида $\langle i, s\rangle$ и $\langle s, j\rangle$, где число $s$ стояло в нижней строке между числами $i$ и $j$. То есть, оно поменялось у нечетного числа пар. Значит, четность подстановки изменилась. □

Эта лемма имеет много полезных следствий.

1. *Любая транспозиция нечетна.*
   Пусть $T$ — транспозиция. Подстановка $I$ четна, ибо в ней нет инверсий. Имеем: $T = T \circ I$.

2. *Четных подстановок в $S_n$ — ровно половина: $|A_n| = |S_n|/2 = n!/2$.*
   Действительно, умножение на любую фиксированную транспозицию, например, на $(1\,2)$, является биекцией между четными и нечетным подстановками. Биективность следует из закона сокращения: если $(1\,2) \circ P = (1\,2) \circ Q$, то $P = Q$.

3. *Подстановка четна $\Longleftrightarrow$ она является произведением четного числа транспозиций.*
   Пусть $P = T_s \circ \dots \circ T_1$. Имеем: $T_1$ нечётна, $T_2 \circ T_1$ чётна, и т.д. Итак, $P$ чётна $\Longleftrightarrow$ $s$ чётно.

4. *Цикл чётной длины нечётен, цикл нечётной длины чётен.*

5. *Четность подстановок при умножении меняется по закону:*

| | ч | н |
|---|---|---|
| ч | ч | н |
| н | н | ч |

6. *Множество четных подстановок образует группу $(A_n, \circ)$.*
   Действительно, $A_n$ содержит $I$, замкнуто относительно умножения и взятия $P^{-1}$.

**Задача 16.** Выпишите все подстановки, входящие в группы $A_3$ и $A_4$. Абелевы ли эти группы?

[21] Конечно же, она меняется и при умножении на транспозицию справа, но доказательство чуть сложнее.

## 6.5 Изоморфизм групп

**Определение 11.** Группы $(G, \circ)$ и $(H, *)$ называют *изоморфными* и пишут так: $(G, \circ) \cong (H, *)$, если существует *изоморфизм* из $(G, \circ)$ в $(H, *)$, то есть такая функция $f\colon G \to H$, что

а) $f$ — биекция (то есть взаимно-однозначное отображение);

б) $f$ сохраняет умножение: $f(a \circ b) = f(a) * f(b)$, для всех элементов $a, b \in G$.

Отношение «быть изоморфными группами» — отношение эквивалентности. Действительно:
– рефлексивность: $(G, \circ) \cong (G, \circ)$, поскольку изоморфизмом будет функция $f(a) = a$;
– симметричность: $(G, \circ) \cong (H, *) \Longrightarrow (H, *) \cong (G, \circ)$, ибо изоморфизм $f^{-1}$;
– транзитивность: $(G, \circ) \cong (H, *) \cong (K, \cdot) \Longrightarrow (G, \circ) \cong (K, \cdot)$, ибо изоморфизм $g \circ f$.

**Свойства изоморфизмов.** Пусть $f\colon G \to H$ — изоморфизм из $(G, \circ)$ в $(H, *)$. Тогда:

– Сохранение единицы: $f(e) = e'$, где $e'$ — нейтральный элемент группы $H$;
▷ $f(e) * f(e) = f(e \circ e) = f(e) = f(e) * e'$; сокращаем на $f(e)$. ◁
– Сохранение обратных: $f(a^{-1}) = (f(a))^{-1}$.
▷ $f(a) * f(a^{-1}) = f(a \circ a^{-1}) = f(e) = e'$. ◁
– Сохранение степеней: $f(a^n) = (f(a))^n$, для любых $n \in \mathbb{Z}$.
– Сохранение порядка: $|f(a)| = |a|$.
– группа $(G, \circ)$ конечная / абелева / циклическая $\Longleftrightarrow$ группа $(H, *)$ такова же.

**Пример 8.** Группа $(\mathbb{Z}_3, \oplus)$ изоморфна группе вращений правильного треугольника $(\{\varphi_0, \varphi_1, \varphi_2\}, \circ)$, ибо изоморфизм такой: $f(n) = \varphi_n$ для $n = 0, 1, 2$.
– Аналогично, $\mathbb{Z}_n$ изоморфна группе вращений правильного $n$-угольника.
– Группа симметрий ромба (не явл. квадратом) изоморфна $V_4$ (четвертной группе Клейна).
– $\mathbb{Z}_4 \ncong V_4$, ибо порядки элементов различны (слева есть 4, а справа только 2).

**Задача 17.** Группа симметрий правильного треугольника изоморфна группе $(S_3, \circ)$.

**Задача 18.** Изоморфны ли группы:
– счётные $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{Q}^+, \cdot)$? Ещё $(M^*, \cdot)$, $(M^+, \cdot)$, где $M = \mathbb{Q} + \mathbb{Q}\sqrt{2}$.
– континуальные: $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{R}^+, \cdot)$? Аналогично с $\mathbb{C}$ и между ними.

**Теорема 14** (Классификация циклических групп)**.** *Любая циклическая группа изоморфна либо группе целых чисел $(\mathbb{Z}, +)$, либо группе вычетов $(\mathbb{Z}_n, \oplus)$ по модулю $n \geqslant 1$.*

*Доказательство.* Пусть $(G, \circ)$ — циклическая группа, порожденная элементом $a$: $G = \langle a \rangle$.

**Случай 1.** Если $G$ бесконечна, то $G = \{a^n \mid n \in \mathbb{Z}\}$. Тогда $(\mathbb{Z}, +) \cong (G, \circ)$, поскольку изоморфизмом является функция $f(k) = a^k$, для всех $k \in \mathbb{Z}$. Сохранение операции проверяется легко: $f(k + \ell) = a^k \circ a^\ell = f(k) \circ f(\ell)$. Биективность $f$: если бы $f(k) = f(\ell)$ для некоторых $k \neq \ell$, то $a^k = a^\ell$; пусть для определенности $k < \ell$; тогда $e = a^{\ell - k}$ (мы сократили на $a^k$); получилось, что $a$ — элемент конечного порядка, но тогда он не мог породить бесконечную группу.

**Случай 2.** Если $|G| = n$, то $G = \{a^0, a^1, \ldots, a^{n-1}\}$. Вспомним, что $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Тогда $(\mathbb{Z}_n, \oplus) \cong (G, \circ)$, поскольку изоморфизмом является функция $f(k) = a^k$. Сохранение операции вытекает из цепочки равенств, где $s \in \{0, 1\}$ и $k \oplus \ell = k + \ell - s \cdot n$:

$$f(k \oplus \ell) = a^{k \oplus \ell} = a^{k + \ell - s \cdot n} = a^k \circ a^\ell \circ (a^n)^{-s} = f(k) \circ f(\ell), \quad \text{так как } a^n = e.$$

Поскольку элементы $a^0, a^1, \ldots, a^{n-1}$ попарно различны, то $f$ — биекция из $\mathbb{Z}_n$ в $G$. □

Как видим, бесконечная циклическая группа всего одна (с точностью до изоморфизма).

## 6.6 Подгруппа

**Определение 12.** Пусть $(G, \circ)$ — группа, $H \subseteq G$ — подмножество. Если $(H, \circ)$ является группой, то она называется *подгруппой* группы $(G, \circ)$. При этом пишут: $(H, \circ) \subseteq (G, \circ)$.

**Пример 9.** Всегда $(\{e\}, \circ)$ и $(G, \circ)$ — подгруппы $(G, \circ)$. Еще: $(2\mathbb{Z}, +) \subseteq (\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +)$.
Еще: группа вращений $n$-угольника $\subseteq$ группа симметрий $n$-угольника (правильного).

Чтобы выяснить, что $(H, \circ) \subseteq (G, \circ)$, достаточно проверить:
– $e \in H$;
– если $a, b \in H$, то $a \circ b \in H$ (замкнутость $H$ относительно операции $\circ$);
– если $a \in H$, то $a^{-1} \in H$ (замкнутость $H$ относительно обратных элементов);
Ассоциативность проверять не требуется, ведь она верна для всех элементов группы $G$!

**Задача 19.** Докажите, что в подгруппе $H$ не может быть «своей» единицы, отличной от единицы группы $G$; а также, не может быть в подгруппе $H$ у некоторого элемента $a$ «своего» обратного, отличного от обратного элемента в группе $G$. Формально, это означает: если $(H, \circ) \subseteq (G, \circ)$, $e$ — единица в $G$, $e'$ — единица в $H$, то $e = e'$. Аналогично, если $a \in H$, $b \in G$ — обратный к элементу $a$ в группе $G$, $c \in H$ — обратный к тому же элементу $a$ в подгруппе $H$, то $b = c$.

**Пример 10.** $(\mathbb{Z}_2, \oplus_2)$ — не подгруппа группы $(\mathbb{Z}_4, \oplus_4)$, ибо разная операция: $1 \oplus_2 1 \neq 1 \oplus_4 1$.

**Теорема 15** (Лагранж)**.** *Порядок конечной группы делится на порядок любой ее подгруппы.*

*Доказательство.* Пусть $(H, \circ) \subseteq (G, \circ)$. Докажем: $|G| \vdots |H|$. Для этого построим, для каждого элемента $a \in G$, так называемые *левые смежные классы группы $G$ по подгруппе $H$*:

$$a \circ H \;:=\; \{\, a \circ h \;\mid\; h \in H \,\}.$$

Достаточно легко доказать следующие три факта:
1) одним из классов является сама подгруппа $H$, а именно $H = e \circ H$;
2) в этих классах одинаковое число элементов: $|a \circ H| = |H|$, для всех $a \in H$;
▷ Отображение $f(h) = a \circ h$ является биекцией из $H$ в $a \circ H$. ◁
3) разные классы не пересекаются: если $a \circ H$ пересекается с $b \circ H$, то $a \circ H = b \circ H$.
▷ Пусть $ah = bh'$, где $h, h' \in H$. Отсюда $a = bh'h^{-1}$. Тогда каждый элемент $ag$ из $aH$ равен $ag = b(h'h^{-1}g)$, то есть — в $bH$. Итак, $aH \subseteq bH$. Аналогично, $bH \subseteq aH$. Значит, $aH = bH$. ◁

Отсюда следует, что конечное множество $G$ разбилось на некоторое семейство подмножеств, имеющих одинаковое количество элементов, равное $|H|$. Значит, $|G|$ делится на $|H|$. □

**Следствие 16.** *Порядок конечной группы делится на порядок любого его элемента.*

*Доказательство.* Рассмотреть $H = \langle a \rangle$ — подгруппу, порожденную элементом $a \in G$. Тогда по теореме Лагранжа $|G|$ делится на число $|H| = |a|$. □

**Следствие 17.** *Всякая группа простого порядка — циклическая.*

*Доказательство.* Пусть $(G, \circ)$ — группа, причем $|G| = p$ — простое число, пусть $p \geqslant 2$. Возьмем любой ее элемент, отличный от нейтрального: $a \neq e$, а значит, $|a| \neq 1$. По Следствию 16 число $p$ делится на $|a|$. Поэтому $|a| = p$. По лемме 10 заключаем, что $G = \langle a \rangle$. □

**Следствие 18.** *Любая подгруппа циклической группы — циклическая.*

*Доказательство.* Пусть $G = \langle a \rangle$, $H \subseteq G$ — подгруппа. Ее элементы — тоже степени элемента $a$. Рассмотрим наименьшую степень $r \geqslant 1$, такую что $a^r \in H$. Если таковой нет, то $H = \{e\}$ — циклическая группа. Если же таковая есть, то докажем, что $H = \langle a^r \rangle$. Допустим противное — пусть в $H$ имеется элемент $b = a^k$, не являющийся степенью элемента $a^r$, то есть $k$ не делится на $r$. Разделим $k$ на $r$ с остатком: $k = tr + s$, где $0 < s < r$. Поскольку в $H$ лежат элементы $b = a^k$ и $a^r$, а значит и $a^{-tr}$, то лежит и их произведение $a^{k-tr} = a^s$. Но это противоречит тому, что $r$ является наименьшей положительной степенью элемента $a$, попадающей в $H$. □

**Теорема 19** (Кэли)**.** *Всякая конечная группа изоморфна некоторой подгруппе группы подстановок $S_n$ (для некоторого $n$).*

*Доказательство.* Пусть $(G, *)$ — группа порядка $|G| = n$, $G = \{g_1, \ldots, g_n\}$. Мы докажем, что эта группа изоморфна некоторой подгруппе группы $S_n(G)$ перестановок множества $G$.[22] Для этого сопоставим каждому элементу $a \in G$ следующую перестановку элементов множества $G$:

$$P_a = \begin{pmatrix} g_1 & \cdots & g_n \\ a * g_1 & \ldots & a * g_n \end{pmatrix}.$$

Все эти $n$ перестановок соберем в множество $H = \{P_a \mid a \in G\}$. Мы получили функцию $f\colon G \to H$, где $f(a) = P_a$. Осталось проверить следующие факты:

- $f$ — биекция между $G$ и $H$: если $P_a = P_b$, то $a * g_i = b * g_i$, откуда $a = b$.
- $P_a$ — это действительно перестановка, то есть в нижней строке все элементы различны: если бы $a * g_i = a * g_j$, то по закону сокращения $g_i = g_j$. Таким образом, $H \subseteq S_n(G)$.
- $f$ сохраняет операцию: $f(a * b) = f(a) \circ f(b)$, то есть $P_{a*b} = P_a \circ P_b$. Чтобы проверить, что эти две подстановки равны, применим их к произвольному элементу $g_i \in G$:

  Слева: $P_{a*b}(g_i) = (a * b) * g_i$. Справа: $[P_a \circ P_b](g_i) = P_a(P_b(g_i)) = a * (b * g_i)$. Равны!
- $(H, \circ)$ образует подгруппу в $(S_n, \circ)$. Действительно, в $H$ имеется нейтральный элемент: $P_e \in H$; $H$ замкнуто относительно произведения подстановок, как было показано выше: $P_a \circ P_b = P_{a*b}$; $H$ замкнуто относительно взятия обратной подстановки: $(P_a)^{-1} = P_{a^{-1}}$. □

## 6.7 Классификация групп малых порядков

Пусть $(G, \circ)$ — группа порядка $|G| = n$. Изучим, сколько имеется групп порядка $n$, с точностью до изоморфизма, и какие они.

$n = 1$**.** Единственная группа: $\mathbb{Z}_1$.
$n = 2$**.** Единственная группа: $\mathbb{Z}_2$, ибо 2 — простое число.
$n = 3$**.** Единственная группа: $\mathbb{Z}_3$, ибо 3 — простое число.
$n = 4$**.** Есть две группы $\mathbb{Z}_4$ и $V_4$. Обе абелевы. Любые другие им изоморфны (задача).
$n = 5$**.** Единственная группа: $\mathbb{Z}_5$, ибо 5 — простое число.
$n = 6$**.** Есть две группы $\mathbb{Z}_6$ (абелева) и $S_3$ (неабелева). Других нет (док-во сложнее).
$n = 7$**.** Единственная группа: $\mathbb{Z}_7$, ибо 7 — простое число.

Как мы видим, наименьший порядок неабелевой группы — 6.

**Задача 20.** Найти, с точностью до изоморфизма, все подгруппы группы $\mathbb{Z}$, $\mathbb{Z}_{15}$, $S_3$.

**Задача 21.** Докажите, что группа порядка 4 изоморфна либо $\mathbb{Z}_4$, либо $V_4$. (См. Пример 4).

[22] Теорема тогда будет следовать из очевидного факта, что $S_n(G) \cong S_n$. Ведь не важно, какие $n$ элементов переставляются — $\{1, \ldots, n\}$ или $\{g_1, \ldots, g_n\}$.