

# ВВЕДЕНИЕ В МАТЕМАТИКУ

конспект лекций для школьников и студентов  
по мотивам «100 уроков математики»

**А. В. Савватеев**

**Москва, 2020**



## ОГЛАВЛЕНИЕ

---

Глава 0. Логика и множества (факультативно)	7
Глава 1. Визуальная арифметика	18
Глава 2. Движения прямой	26
Глава 3. Вокруг окружности	38
Глава 4. Целые числа и ОТА	47
Глава 5. Симметрии фигур	54
Глава 6. Исчисление остатков	61
Глава 7. Движения плоскости и пространства	74
Глава 8. Перестановки	83
Глава 9. Линейные уравнения	98
Глава 10. Числовые поля	108
Глава 11. Начала комплексного анализа	122
Глава 12. Некоторые иррациональности	139
Глава 13. Континуум	160
Глава 14. Расширение алгебраических конструкций	189
Приложение А. Схемы и таблицы	191

<b>Глава 0. Логика и множества (факультативно)</b>	<b>7</b>
0.1 Суждения и силлогизмы	7
0.2 Высказывания и предикаты	9
0.3 Связь предикатов и множеств	12
0.4 Построение множеств	15
<b>Глава 1. Визуальная арифметика</b>	<b>18</b>
1.1 Сложение и вычитание	18
1.2 Сравнение	20
1.3 Умножение	20
1.4 Натуральные числа	22
1.5 Теорема Пифагора графически	23
1.6 Бином Ньютона и другие формулы визуально	24
1.7 Соизмеримость отрезков, алгоритм Евклида	24
<b>Глава 2. Движения прямой</b>	<b>26</b>
2.1 Сдвиг, композиция сдвигов, группа	26
2.2 Отражение	30
2.3 Таблица Кэли движений прямой	33
2.4 Теорема о гвоздях, аналог теоремы Шаля	34
2.5 Все конечные подгруппы движений прямой	36
<b>Глава 3. Вокруг окружности</b>	<b>38</b>
3.1 Движения окружности	38
3.2 Группа движений окружности, теорема Шаля	40
3.3 Наматывание прямой на окружность	44
<b>Глава 4. Целые числа и ОТА</b>	<b>47</b>
4.1 Целые числа. Кольцо	47
4.2 Кузнечик НОД и алгоритм Евклида	49
4.3 Простые числа и ОТА	50
4.4 Некоторые следствия ОТА	53
<b>Глава 5. Симметрии фигур</b>	<b>54</b>
5.1 Симметрии правильного треугольника	54
5.2 Симметрии правильного многоугольника	55
5.3 Подгруппы движений окружности	56

5.4	Симметрии ромба, группа Клейна	59
<b>Глава 6.</b>	<b>Исчисление остатков</b>	<b>61</b>
6.1	Арифметика остатков	61
6.2	Свойства арифметики остатков	66
6.3	*Вычеты и операции Минковского	68
6.4	*Теория множеств: отношения	70
<b>Глава 7.</b>	<b>Движения плоскости и пространства</b>	<b>74</b>
7.1	Виды движений плоскости. Теорема Шаля	74
7.2	Сравнение движений прямой, окружности и плоскости	76
7.3	Векторно-числовое представление движений плоскости	77
7.4	Пара слов о движениях сферы	78
7.5	Пара слов о движениях пространства	79
<b>Глава 8.</b>	<b>Перестановки</b>	<b>83</b>
8.1	*Теория множеств: функции	83
8.2	Конечные группы	84
8.3	Арифметика перестановок	90
8.4	Четверная группа Клейна	97
<b>Глава 9.</b>	<b>Линейные уравнения</b>	<b>98</b>
9.1	Уравнение прямой на плоскости	98
9.2	Линейные уравнения в целых числах	102
<b>Глава 10.</b>	<b>Числовые поля</b>	<b>108</b>
10.1	Рациональные числа	108
10.2	Соизмеримость. Иррациональности	115
10.3	Поле вычетов по простому модулю	120
<b>Глава 11.</b>	<b>Начала комплексного анализа</b>	<b>122</b>
11.1	Алгебра комплексных чисел	122
11.2	Гауссовы целые числа	128
<b>Глава 12.</b>	<b>Некоторые иррациональности</b>	<b>139</b>
12.1	*Упорядоченные множества	139
12.2	Плотные множества	144
12.3	Зазоры между рациональными числами	145
12.4	Многочлены и алгебраические числа	147
<b>Глава 13.</b>	<b>Континуум</b>	<b>160</b>
13.1	Мощности множеств	160
13.2	Изоморфизмы	167

13.3 Действительные числа	169
13.4 Модели действительных чисел	180
13.5 Комплексные числа	188
13.6 Гомотетии прямой и плоскости	188
<b>Глава 14. Расширение алгебраических конструкций</b>	<b>189</b>
14.1 Матрицы	189
14.1.1 Конспект	189
14.1.2 Задачи	189
<b>Приложение А. Схемы и таблицы</b>	<b>191</b>

# Логика и множества (факультативно)

## Аннотация.

В этой главе обсуждаются основы математической логики и теории множеств, построение высказываний и множеств на бытовых примерах. Вводится понятие суммы и произведения числовых множеств по Минковскому.

Данная глава носит справочный характер и может быть пропущена при первом чтении конспекта. Тем не менее, настоятельно рекомендуется регулярно возвращаться к ней по мере освоения материала.

## 0.1 Суждения и силлогизмы

### Конспект

1

1. Типовая конструкция суждения: *Посылки*  $\vdash$  *Вывод*.

2. Пример:

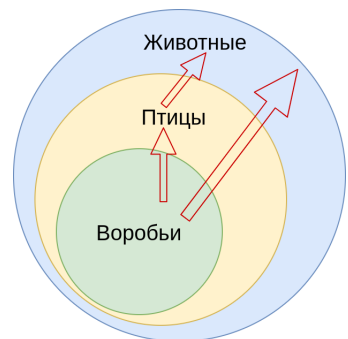
(Все птицы — животные) и (все воробьи — птицы),

вывод: (все воробьи — животные).

Такой вывод является правильным независимо от того, правильные ли посылки.

(Все птицы — животные) и (все цветы — птицы), вывод: (все цветы — животные).

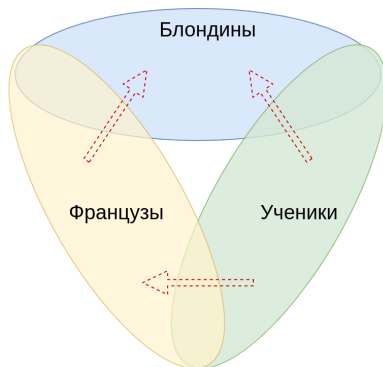
Это суждение истинно независимо от ложности посылок. Суждение показывает *только взаимосвязь* посылок и вывода. Принцип «чушь на входе — чушь на выходе».



3. При построении суждения посылки могут быть ложными. Более того, в математической логике из ложной посылки следует все, что угодно. Например, *если снег черный, то лес зеленый*. Лес при этом может быть зеленым (летом) и не быть таковым (зимой), но суждение остается истинным, т.к. посылка про снег является ложной.

4. Сравните: если запись числа  $a$  оканчивается на 0, то оно кратно 5. Здесь мы ничего не знаем про число  $a$ , но если для него выполняется посылка, то выполняется и вывод. А если не выполняется, то истинность самого суждения при этом никак не страдает. Более того, мы знаем, что на 5 также делятся и другие числа, и это значит, что путать местами посылки и вывод ни в коем случае нельзя! Ведь **не всегда верно**, что если число делится на 5, то его запись заканчивается на 0.
5. Другой пример:

(Некоторые французы — блондины)  
и (некоторые ученики — французы),  
следовательно, (некоторые ученики — блондины). **Такое суждение неверно.** Поскольку слово «некоторые» не гарантирует, что таковым признаком обладают все французы. А значит, из свойства «быть французом» не всегда следует «быть блондином».



6. Здесь обе посылки истинные, но вывод ложный. Хотя легко представить ситуацию, когда некоторые ученики действительно будут блондинами. Но это — лишь предположение, а не строгое рассуждение.
7. В этом примере нарушается именно связка между посылками и выводом, т.к. две посылки не склеиваются по общему признаку. В первой посылке стоит «некоторые французы», а во второй просто «французы», это разные **множества**, а потому связать две посылки вместе мы не можем!
8. Для построения **силлогизма** принципиально, чтобы связующее звено было одинаковым:

**если** ( $A$  есть  $B$ ) и ( $B$  есть  $C$ ), **то** ( $A$  есть  $C$ )

здесь связывание посылок происходит по свойству  $B$ , и если в нем допустить какое-то искажение, то можно прийти к неверным выводам!

## Задачи

1. Постройте вывод из посылок: (Сократ человек) И (все люди смертны).



## 0.2 Высказывания и предикаты

### Конспект

1. **Высказывание** — это любое утверждение на любом языке, которое может быть либо только истинным, либо только ложным.
2. Примеры высказываний: «Шесть больше трех», «Дважды два — пять», « $\sqrt{2}$  — число иррациональное», «среди натуральных чисел существует наибольшее», «всякое четное число является суммой двух простых чисел».
3. Все эти высказывания имеют либо истинное, либо ложное значение, хотя про последнее мы не знаем точный ответ. Но мы точно знаем, что их значения не могут быть переменными, т.е. зависеть от каких-то внешних факторов или других высказываний.
4. Из выше приведенных примеров: «все птицы — животные» и «все воробьи — птицы» есть истинные высказывания.
5. Но эти высказывания можно разобрать на составляющие. Для чего нам понадобятся предикаты.
6. **Предикат** — это суждение, зависящее от переменных, обозначающих объекты данного суждения.
7. Например, « $x$  есть воробей», « $x$  есть птица», « $x$  есть животное». Каждое из них может быть истинным или ложным, смотря что подставить вместо  $x$ . При  $x$  = «рыба» первые два будут ложными, а при  $x$  = «ромашка» ложными будут все три предиката.
8. Аналогично, « $x$  есть ученик», « $x$  есть француз», « $x$  есть блондин». Заметим, что если ранее мы оперировали **свойствами** (быть учеником, французом, блондином), то теперь перешли к оперированию **объектом**  $x$ , который может обладать тем или иным свойством.
9. Из предикатов можно построить новые предикаты, используя логические связки: И( $\wedge$ ), ИЛИ( $\vee$ ), НЕ( $\neg$ ), СЛЕДУЕТ( $\rightarrow$ ).
10. Например, «( $x$  есть воробей) $\rightarrow$ ( $x$  есть птица)», «( $x$  есть птица) $\rightarrow$ ( $x$  есть животное)». Эти предикаты содержат переменную  $x$ , но они всегда истинны. Такие тождественно истинные предикаты называются **тавтологиями**. Тавтологии отличаются от истинных высказываний тем, что содержат переменные, которые можно считать фиктивными. Чтобы тавтологию сделать высказыванием, достаточно перед ним сказать «для любого  $x$ », тогда  $x$  перестанет быть параметром, а выражение превратится в истинное высказывание:

$$\langle \text{для любого } x \rangle (x \text{ есть воробей}) \rightarrow (x \text{ есть птица})$$

11. Это называется правилом введения **квантора всеобщности**.
12. Далее, рассмотрим высказывание «*некоторые французы блондины*». Поступить аналогично предыдущему и заменить его на предикат « $(x \text{ есть француз}) \rightarrow (x \text{ есть блондин})$ » нельзя! Дело в том, что высказывание «*все воробьи — птицы*» говорит о вложении одного свойства в другое: быть воробьем означает также быть птицей. Но при слове «*некоторые*» мы понимаем, что речь идет не о свойстве «*быть французом*», а о том, что некоторые из французов обладают свойством «*быть блондином*». То есть, мы утверждаем, что существует хотя бы один такой объект  $x$ , который есть и француз и блондин одновременно!
13. Иначе говоря, мы имеем дело со связкой И:

$$(x \text{ есть француз}) \wedge (x \text{ есть блондин}),$$

- данный предикат не всегда является истиной, его истинность зависит от конкретного  $x$ .
14. Тем не менее, и такой предикат можно превратить в высказывание, причем истинное. Для этого нужно слово «*некоторые*» превратить в «*существует  $x$* », так что получится истинное высказывание

$$«(существует\ x)\ (x \text{ есть француз}) \wedge (x \text{ есть блондин})»$$

15. Это называется правилом введения **квантора существования**.
16. Примеры перевода высказываний с языка свойств на язык объектов:

Все птицы — животные	(для любого $x$ ) $(x \text{ есть птица}) \rightarrow (x \text{ есть животное})$
Все воробьи — птицы	(для любого $x$ ) $(x \text{ есть воробей}) \rightarrow (x \text{ есть птица})$
Все воробьи — животные	(для любого $x$ ) $(x \text{ есть воробей}) \rightarrow (x \text{ есть животное})$
Если число заканчивается на 0, то оно кратно 5	(для любого $a$ ) $(a \text{ заканчивается на } 0) \rightarrow (a \text{ кратно } 5)$
Некоторые французы — блондины	$(существует\ x)\ (x \text{ есть француз}) \wedge (x \text{ есть блондин})$
Некоторые ученики — французы	$(существует\ x)\ (x \text{ есть ученик}) \wedge (x \text{ есть француз})$
Некоторые ученики — блондины	$(существует\ x)\ (x \text{ есть ученик}) \wedge (x \text{ есть блондин})$

17. Видим, что построить вывод можно только в том случае, когда две посылки склеиваются по общему предикату « $x \text{ есть птица}$ », при этом сами посылки являются импликациями (следование).

18. Можно комбинировать общие и частные суждения:

$$\langle (x \text{ есть птица}) \wedge (\text{все птицы} - \text{животные}) \rangle,$$

откуда следует вывод  $\langle (x \text{ есть животное}) \rangle$ .

Здесь мы объединили в посылке предикат, что-то говорящий о свойстве объекта  $x$ , с высказыванием, которое что-то говорит о связи двух свойств, и нашли новое свойство объекта  $x$ . Это типичное рассуждение от общего к частному.

19. Построение выводов из заданных или полученных ранее истинных высказываний и предикатов называется **дедукцией** и является основным методом рассуждений при получении математических теорем.

20. Иногда для построения нужного вывода требуется перебрать сотни комбинаций ранее доказанных посылок. Но часто для нащупывания правильной цепочки доказательства хватает вспомогательных иллюстраций или опыта исследователя, погруженного в данную тему.

21. Ранее мы отмечали, что рассуждения в обратную сторону — от вывода к посылкам — неверны. Однако очень часто это верно отчасти. Например, мы знаем дедуктивный вывод: если число оканчивается на 0, то оно делится на 5. На основе этого мы не можем доказать точно, но **можем предположить**, что если число делится на 5, то оно, вероятно, может оканчиваться на 0. Как мы знаем, это верно примерно в половине случаев. Если бы такое *разворачивание импликации* было бы всегда абсолютно невозможным, то дедукция представляла бы собой простейший случай вывода, когда ложь влечет любое суждение. Для построения теорий это абсолютно бесполезно.

22. Метод *рассуждения назад*, к уже известной посылке, называется **абдукцией**. Именно таким методом, как правило, пользовался Шерлок Холмс в своих умозаключениях. Именно поэтому его выводы всегда носят вероятностный характер и сопровождаются словами «вероятно», «скорее всего» и т.п. Искусство Шерлока Холмса заключается в том, чтобы из всех возможных посылок в данной конкретной ситуации выбрать наиболее вероятную.

23. Например, цитируем из рассказа «Этюд в багровых тонах» (Конан Дойль),

*«Этот человек по типу — врач, но выправка у него военная. Значит, военный врач. Он только что приехал из тропиков — лицо у него смуглое, но это не природный оттенок его кожи, так как запястья у него гораздо блее. Лицо изможденное, — очевидно, немало натерпелся и перенес болезнь. Был ранен в левую руку — держит ее неподвижно и немножко неестественно. Где же под тропиками военный врач-англичанин мог натерпеться лишений и получить рану? Конечно же, в Афганистане». Весь ход мыслей не занял и секунды. И вот я сказал, что вы приехали из Афганистана.*

24. Рассмотрим только часть умозаклучений Холмса и сравним их с арифметическим примером

Ватсон — военный врач с изможденным лицом и загорелый	Число 30 — делится на 5
Воевавшие в Афганистане — военные с изможденным лицом и загорелые	Оканчивающее на 0 число — делится на 5
Вывод: Ватсон прибыл из Афганистана	Вывод: 30 оканчивается на 0

25. Как видим, нам дано две посылки, в одной из которых дается некая связь между свойствами (воевавшие есть военные и т.д., а также оканчивающиеся на 0 делятся на 5), а в другой дается свойство конкретного объекта (Ватсон и число 30). Это свойство общее в обеих посылках, но по нему нельзя склеить их в силлогизм, т.к. свойство всегда стоит в конце посылки. Но Холмс знает, что практически все военные с изможденным лицом и загорелые — это воевавшие в Афганистане (хотя это и неверно на 100%), и на основании этого он предполагает(!), что и Ватсон такой же, раз он обладает таким же свойством.
26. На примере числа 30 это тоже сработало, однако стоит нам подставить 25 вместо 30, как вся цепочка рассуждений порушится! Поэтому абдуктивные умозаклучения нельзя считать математическими, однако они могут привести на правильное дедуктивное умозаклучение, в результате чего либо появляется теорема (*Все военные с изможденным лицом воевали в Афганистане*), либо обнаруживается контрпример (в нашем случае это число 25, которое опровергает предположение о том, что все делящиеся на 5 числа оканчаиваются на 0).

### Задачи

1. Какое абдуктивное предположение можно сделать из следующих посылок: (Зимой выпадает снег) И (Сейчас есть снег) ?

## 0.3 Связь предикатов и множеств

### Конспект

1. Выше мы оперировали такими понятиями как свойство и объект, обладающий свойством, на основе чего вводили различные высказывания и предикаты. Посмотрим, как они связаны с понятием **множество**.
2. Пусть  $M$  — множество всех людей, живущих на планете. Тогда предикат  $h(x)$  « $x$  есть человек» можно переписать следующим способом:  $h(x) = (x \in M)$ . Это одновременно означает и то, что  $x$  находится в множестве  $M$ , и то, что  $x$  обладает свойством «быть человеком». Говорят также, что  $M$  есть область

истинности предиката  $h(x)$ . Таким образом, множество олицетворяет собой свойство, а элементы множества — объекты, обладающие данным свойством.

3. Если множество  $X$  является частью множества  $Y$ , (например, множество всех женщин есть часть множества  $M$ ), то мы пишем  $X \subseteq Y$  ( $X$  содержится в  $Y$ ,  $Y$  включает  $X$ ). Важно не путать значки  $\in$  и  $\subseteq$ , т.к. первый говорит о принадлежности объекта к свойству, а второй — о вложении свойств (о том, что одно свойство меньше или равно другому). Используется также символ строгого вложения  $\subset$ , означающий, что вложение имеется, но при этом множества не равны.
4. Вложение множеств выражается с помощью принадлежности:

$$X \subseteq Y \text{ эквивалентно } (\forall x)(x \in X) \rightarrow (x \in Y)$$

По сути, это ровно то же самое, что мы ранее делали при переводе языка свойств на язык объектов: *все  $X$  есть  $Y$*  равносильно высказыванию (для любого  $x$ )  $(x \text{ обладает свойством } X) \rightarrow (x \text{ обладает свойством } Y)$ .

5. Обозначим далее:  $p(x)$  предикат « $x$  есть воробей»,  $o(x)$  предикат « $x$  есть птица»,  $a(x)$  предикат « $x$  есть животное». Ранее мы получали следующий вывод:

$$(\forall x)(p(x) \rightarrow o(x)) \wedge (\forall x)(o(x) \rightarrow a(x)) \vdash (\forall x)(p(x) \rightarrow a(x))$$

6. Попробуем то же самое выразить множествами. Обозначим через  $P$  область истинности предиката  $p(x)$ , т.е. множество всех воробьев,  $O$  — множество всех птиц,  $A$  — множество всех животных. Тогда написанный выше с помощью предикатов вывод можно записать на языке множеств так:

$$(P \subseteq O \subseteq A) \vdash (P \subseteq A),$$

поскольку все воробьи есть птицы, все птицы есть животные, а в итоге все воробьи есть животные.

7. На самом деле, существует намного более тесная связь между логическими связками и операциями над множествами. Вернемся снова к картинке про французов, блондинов и учеников. На ней есть три множества, обозначенные соответствующими овалами. Обозначим их следующим способом:

$$F = \{x \mid x \text{ — француз}\}, \quad B = \{x \mid x \text{ — блондин}\}, \quad E = \{x \mid x \text{ — ученик}\}$$

8. Здесь можно увидеть примеры **пересечений** множеств:

$$F \cap B = \{x \mid (x \text{ — француз}) \wedge (x \text{ — блондин})\},$$

$$F \cap E = \{x \mid (x \text{ — француз}) \wedge (x \text{ — ученик})\},$$

$$E \cap B = \{x \mid (x \text{ — ученик}) \wedge (x \text{ — блондин})\}.$$

Видим, что они соответствуют логической связке И соответствующих предикатов, выражающих свойства.

9. На той же схеме мы можем усмотреть и такие теоретико-множественные конструкции, как:

$$F \setminus B = \{x \mid (x - \text{француз}) \wedge \neg(x - \text{блондин})\},$$

т.е. множество французов, не являющихся блондинами.  $F \setminus B$  есть операция **ВЫЧИТАНИЯ** множеств.

10. Наконец, множество

$$F \cup E = \{x \mid (x - \text{француз}) \vee (x - \text{ученик})\}$$

представляет собой свойство быть французом ИЛИ учеником. Оно содержит в себе как всех французов, так и всех учеников, причем среди них есть как французы, не являющиеся учениками, так и французы, являющиеся учениками, а также ученики, не являющиеся французами. **Объединение** множеств соответствует логической связке ИЛИ.

11. Итак, мы можем легко оперировать предикатами, представляя, что они выражают свойство объекта принадлежать некоторому множеству, и наоборот, оперировать множествами, представляя, что оперируем предикатами, для которых эти множества суть область истинности. При этом И соответствует пересечению, ИЛИ — объединению множеств. Отрицание соответствует вычитанию множеств, причем разность  $X \setminus Y$  можно рассматривать как пересечение  $X \cap (\neg Y)$ . Наконец, вложение множеств соответствует импликации предикатов.

## Задачи

1. Выразить свойство «*быть учеником и блондином одновременно*» через множества  $E$  и  $B$ .
2. Написать множество, соответствующее всем «*птицам, не являющимся воробьями*» через множества  $O$  и  $P$ .
3. Какие элементы содержит множество  $P \setminus A$ , множество  $M \cap F$ , множество  $(F \cup B) \setminus (F \cap B)$ ?
4. Что выражает высказывание  $(M \setminus F) \subseteq (M \setminus B)$ ?
5. Докажите:  $(E \subseteq F) \vdash (M \setminus F) \subseteq (M \setminus E)$  (от противного).

## 0.4 Построение множеств

### Конспект

1. Построение множеств прямо наследует из их связи с предикатами. Тем не менее, важно знать язык, позволяющий компактно и наглядно записывать конструктивные примеры построения множеств.
2. Конечное множество, элементами которого являются объекты  $a, b, \dots, z$  (их не обязательно 26, просто какой-то набор), обозначается

$$\{a, b, \dots, z\},$$

при этом неважно, в каком порядке записаны элементы внутри скобок, и есть ли там дубликаты. Если в списке один и тот же элемент повторяется несколько раз, то его дубли можно спокойно выбрасывать.<sup>1</sup>

3. Примеры:  $\{0\}$ ,  $\{0, 1\}$ ,  $\{0, 1, 2, 3\}$ ,  $\{0, 0, 1, 1, 1\}$ . Последнее множество равно множеству  $\{0, 1\}$  (убрали кратные вхождения). Еще пример:  $\{\}$  — **пустое множество**, обозначаемое также символом  $\emptyset$ .
4. Как мы уже видели ранее, множество можно задать в **предикативной форме**, общий вид которой такой:

$$\{x \mid \varphi(x)\}, \quad \{f(x) \mid \varphi(x)\},$$

где  $\varphi(x)$  — это предикат, выражающий свойство объекта  $x$ , а  $f(x)$  — некоторое преобразование объекта  $x$  (функция).

В первом случае данное множество является областью истинности предиката  $\varphi(x)$  и содержит в себе все элементы, и только их, для которых  $\varphi(x)$  истинно. Во втором случае множество содержит все значения функции  $f(x)$ , примененные к объектам из области истинности  $\varphi(x)$ . Очевидно, что

$$\{f(x) \mid \varphi(x)\} = \{y \mid (y = f(x)) \wedge \varphi(x)\}$$

5. Конечное множество в предикативной форме записывается так:

$$\{a, b, \dots, z\} = \{x \mid (x = a) \vee (x = b) \vee \dots \vee (x = z)\},$$

где предикат  $\varphi(x) = (x = a) \vee (x = b) \vee \dots \vee (x = z)$  выражает свойство  $x$  входить в список объектов  $a, b, \dots, z$ .

---

<sup>1</sup>В математике существует понятие **мультимножество**, в котором как раз количество дубликатов имеет значение и называется кратностью элемента. Мультимножество удобно, например, для записи разложения числа по степеням простых.

6. Объединение (или сумма) множеств:

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\},$$

например,  $\{a, b\} \cup \{b, c\} = \{a, b, c\}$ .

7. Пересечение множеств:

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\},$$

например,  $\{a, b\} \cap \{b, c\} = \{b\}$ .

8. Разность множеств:

$$A \setminus B = \{x \mid (x \in A) \wedge (x \notin B)\},$$

например,  $\{a, b\} \setminus \{b, c\} = \{a\}$ . Заметим, что  $A \setminus B$  не всегда равно  $B \setminus A$ .

9. Если элементы множеств — это числа, то с ними можно производить арифметические операции:

$$A + B = \{x + y \mid (x \in A) \wedge (y \in B)\}, \quad kA = \{kx \mid x \in A\},$$

здесь первое множество — это сумма по Минковскому двух множеств, оно содержит все возможные суммы  $x + y$ , где первое слагаемое берется из первого множества, второе — из второго.

Легко видеть также, что  $A + \emptyset = \emptyset$ , т.к. предикат  $y \in B$  в случае  $B = \emptyset$  тождественно ложный.

**Важно:** не следует путать  $A + A$  и  $2A$ ! Например,

$$\{0, 1\} + \{0, 1\} = \{0, 1, 2\}, \text{ но } 2\{0, 1\} = \{0, 2\}.$$

10. Аналогично можно определить произведение множеств по Минковскому:

$$AB = \{xy \mid (x \in A) \wedge (y \in B)\},$$

откуда легко определяется степень множества  $A^k$ , а также его экспонента  $\exp(A) = \sum_k (1/k!) A^k$ .

Аналогично сумме видим, что  $A\emptyset = \emptyset$ .

## Задачи

1. Найти объединение, пересечение и разность множеств  $\{0, 1, 2, 3\}$  и  $\{1, 2, 5\}$  (разность как в прямом, так и в обратном порядке).
2. Записать множество  $\{0, 1, 2\}$  в предикативной форме.



3. Записать множество всех простых чисел в предикативной форме.
4. Доказать, что  $A + \{0\} = A$ ,  $A \cdot \{1\} = A$ .
5. \*\*Когда  $A \setminus B = B \setminus A$ ?
6. \*\*\*Доказать, что  $\max \exp(\{0, x\}) = e^x$ .

# Визуальная арифметика

### Аннотация.

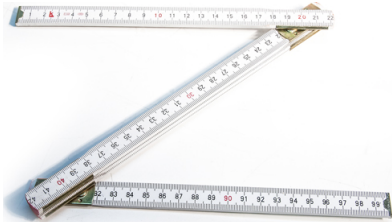
В данной главе закладывается фундамент арифметики с помощью визуальных образов. Действия с отрезками и прямоугольниками являются иллюстрацией действий с числами. Цель — дать наглядное обоснование законам арифметики и получить некоторые навыки арифметических операций и сравнений чисел.

Попутно вводится понятие натурального числа как количества применяемых операций композиции, а также как меры длины, площади, объема относительно заданной мерной единицы.

## 1.1 Сложение и вычитание

### Конспект

1. Берем произвольную прямую, и на ней будем откладывать отрезки — вправо и влево.
2. Откладывание вправо есть прибавление длины, а откладывание влево — вычитание (уменьшение) длины.
3. Можно откладывать ноль, т.е. ничего не делать. В этом случае все равно — прибавляем или вычитаем ноль.
4. Мы можем комбинировать откладывание отрезков вправо и влево, т.е. производить серию последовательных откладываний отрезков (они могут быть разными по длине), на каждом шаге — от текущей точки положения.
5. Результат *серии откладываний* равносителен одному откладыванию отрезка, соединяющего стартовую и финишную точки, причем финишная точка:
  - может быть справа от стартовой (результатом является одно откладывание вправо, т.е. прибавление длины),
  - может совпадать с ней (результатом оказалось нулевое откладывание)
  - или быть слева от стартовой точки (результатом является одно откладывание влево, т.е. вычитание).

6. Откладывание *изотропно*, т.е. одинаковые серии откладываний, приложенные к разным стартовым точкам, приводят к одинаковым результирующим отрезкам, отложенным от этих стартовых точек. Иначе говоря, величина и направление откладывания не зависит от начального местоположения!
7. Серии откладываний можно проиллюстрировать складным метром. Раскладывание колена на  $180^\circ$  означает прибавление его длины к общей серии откладываний, а складывание — вычитание его длины из общей серии откладываний. При этом от стартовой точки можно уйти как вправо, так и влево, или остаться на месте.
- 
8. С помощью этой же линейки нетрудно продемонстрировать, что композиция откладываний **ассоциативна** и **коммутативна**: можно сначала сложить-/разложить одну линейку, затем вторую, затем приложить вторую к первой или первую ко второй — результат будет один и тот же!
9. Кроме того, очевидно, что у каждого откладывания существует обратное, приводящее в результате к нулевому откладыванию. Для этого нужно произвести ровно ту же самую серию откладываний, только поменять ось направления. Или, что то же самое, пройти по линейке в обратную сторону.
10. Далее любое откладывание будем записывать буквами  $a, b, c, \dots$ , имея ввиду под ними как прибавления, так и вычитания.
11. Откладывание, противоположное  $a$ , будем обозначать  $-a$ . При этом комбинация откладываний соединяется знаком '+', а если встречается комбинация  $a + (-b)$ , то пишем проще:  $a - b$ .
12. Обратные откладывания — это просто перевернутые в обратную сторону «линейки»!
13. Результат откладывания (конфигурацию линейки с учетом ее направления) будем называть **вектором**. Если вектор смотрит влево (финишная точка левее стартовой), то вектор называется *отрицательным*, а если вправо — *положительным*. Нулевой вектор — когда финиш и старт совпадают.
14. Композицию откладываний будем называть **суммой векторов** или просто суммой, а процедуру откладывания — **сложением**.

### **Свойства сложения:**

S1  $(a + b) + c = a + (b + c)$  (ассоциативность);

S2  $a + b = b + a$  (коммутативность);

- S3  $a + 0 = 0 + a = a$  (аддитивное свойство нуля);
- S4  $a + (-a) = 0$  (обратный элемент);
- S5 если  $a + x = b + x$ , то  $a = b$  (правило сокращения);
- S6 верно одно и только одно: либо  $a = b$ , либо  $a = b + x$ , либо  $a = b - x$ , где  $x$  — откладывание вправо (трихотомия)

## Задачи

1. Вывести свойства сложения.

## 1.2 Сравнение

### Конспект

1. Понятие отрицательного и положительного векторов позволяют ввести сравнение на векторах.
2. Для начала скажем, что положительный вектор больше нуля:  $x > 0$ .
3. Далее, если  $b = a + x$ , где  $x > 0$ , то пишем  $a < b$ .

**Свойства сравнения** (можно вывести из определения):

- O1 не верно, что  $x < x$  (антирефлексивность);
- O2 если  $a < b$  и  $b < c$ , то  $a < c$  (транзитивность);
- O3 верно одно и только одно: либо  $a = b$ , либо  $a < b$ , либо  $b < a$  (трихотомия);
- O4  $a < b \Leftrightarrow a + x < b + x$ , где  $x > 0$  (изотропность сравнения)

## Задачи

1. Вывести свойства сравнения.

## 1.3 Умножение

### Конспект

1. Строим две перпендикулярно направленные оси  $Ox$  и  $Oy$ . На каждой оси — свой собственный мир векторов и линеек.
2. Умножение — это площадь, построенная на перпендикулярных векторах. Картинка  $2 \times 2 = 4$ .

3. Поскольку векторы у нас двух знаков, умножение также бывает двух знаков. Знак умножения определяется знаком (направлением) векторов и таблицей перемножения знаков:

	+	−
+	+	−
−	−	+

4. Понятие группы на данном примере. Элемент '+' является нейтральным элементом группы знаков. Многократные умножения знаков не выводят за пределы группы.
5. Умножение коммутативно и ассоциативно — можно продемонстрировать на картинках с квадратами и кубами.
6. Умножение на нулевой отрезок (мультипликативное свойство нуля) — очевидно из равенства и свойств сложения:

$$0 + a \times 0 = a \times 0 = a \times (0 + 0) = (a \times 0) + (a \times 0) \Rightarrow 0 = (a \times 0)$$

7. Дистрибутивный закон, в том числе при разнонаправленных векторах проверяется непосредственно на картинке:  $a \times (b + c) = a \times b + a \times c$ .
8. **Единичный отрезок** — способ свести многократное сложение одного вектора к умножению на сумму единичных отрезков! Прямоугольник единичной высоты и длины  $an$  перекладывается в прямоугольник  $a \times n$ , тем самым сложение превращается в умножение.
9. Умножение на единичный отрезок:  $a \times 1 = a$ .
10. Сложение отрезков — это также сложение прямоугольников единичной высоты.
11. Умножение отрезков — это не только площадь, но также и объем, который замечает вертикальный единичный отрезок на площади  $a \times b$ , поэтому  $ab = a \times b \times 1$ .
12. *Степень*: многократное умножение отрезка самого на себя. Иллюстрация — отрезок, квадрат, куб.
13. В дальнейшем умножение векторов в смысле нахождения площади/объема, т.е.  $a \times b$ , и умножение чисел как таковых, т.е.  $ab$ , будем считать одним и тем же понятием, так что  $a \times b = ab$ .

### Свойства умножения:

- P1  $(a \times b) \times c = a \times (b \times c)$  (ассоциативность);

- P2  $a \times b = b \times a$  (коммутативность);
- P3  $a \times 0 = 0 \times a = 0$  (мультипликативное свойство нуля);
- P4  $a \times 1 = 1 \times a = a$  (нейтральный элемент по умножению);
- P5  $a \times (b + c) = a \times b + a \times c$  (дистрибутивный закон);
- P6 если  $a \times b = 0$ , то  $a = 0$  или  $b = 0$  (отсутствие делителей нуля);
- P7 если  $a \times c = b \times c$  и  $c \neq 0$ , то  $a = b$  (правило сокращения);
- P8 если  $a \times c < b \times c$ , то  $a < b$  (монотонность);
- P9 если  $a < b$  и  $c > 0$ , то  $a \times c < b \times c$ .

## Задачи

1. Вывести свойства умножения.

## 1.4 Натуральные числа

### Конспект

1. Кратность операций сложения и умножения:  $a + a + a + a + a + \dots, aaa \dots$ . Натуральное число вводится для обозначения кратности одинаковых операций!
2. Нулевая кратность: в случае сложения ничего не складываем, остаемся на месте в начальной точке, поэтому

$$\underbrace{a + \dots + a}_{0 \text{ раз}} = 0.$$

3. Нулевая степень: в случае умножения ничего не умножаем, от умножения остается только кратность 1, наследуемая от сложения, т.е. в произведении  $1 \times a \times a \times \dots$  выбрасываем все, остается только 1. Поэтому

$$\underbrace{a \times \dots \times a}_{0 \text{ раз}} = 1,$$

кроме того, это согласуется с законом ассоциативности умножения. Многие правила в математике для крайних значений определяются с целью сохранить общий вид формул, если это не приводит к противоречию!

4. **Натуральные числа** — это показатели кратности операций (сложения и умножения).

5. С другой стороны, натуральные числа можно рассматривать как суммы единичных отрезков.

$$n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ раз}}$$

6. Чудо, но это вполне согласуется с операциями сложения и умножения, сохраняя все законы арифметики: ассоциативность, коммутативность, дистрибутивность.
7. Поэтому натуральные числа, привязанные к единичным отрезкам, можно также считать мерой длины, площади, объема и т.д.
8. Ноль — натуральное число, поскольку мы рассматриваем нулевую кратность для однородности законов арифметики.

otaBene Натуральные числа — это и кратности операций, и единицы измерения, т.е. числа.

9. Натуральные числа отвечают за соизмеримость и арифметическую кратность:  $a$  **кратно**  $b$  ( $a \dot{:} b$ ), если  $a = bn$  или  $a = (-b)n$  при некотором натуральном  $n$ . Ноль кратен любому числу! Нулю кратен только ноль!
10. Если  $a$  кратно  $b$ , то говорят также, что  $b$  делит  $a$ , или что  $b$  является делителем  $a$  ( $b|a$ ).
11. Если  $a > 0$  кратно  $b > 0$ , то  $a = kb = b + (k-1)b$ , где  $k > 0$ . Здесь  $x = (k-1)b$ . Поэтому  $a \geq b$ . Так что для положительных векторов кратность означает превосходство в смысле сравнения. И наоборот, если  $b$  делит  $a$ , то  $b \leq a$ . Аналогичные неравенства можно получить и для отрицательных векторов.

## Задачи

- Доказать, что если  $a|b$  и  $b|c$ , то  $a|c$ .
- Доказать, что если  $a|b$  и  $b|a$ , то  $a = \pm b$  ( $a, b$  — натуральные).

## 1.5 Теорема Пифагора графически

### Конспект

- Строим квадрат  $a + b \times a + b$  и внутри квадраты  $a \times a$  и  $b \times b$
- Строим квадрат  $a + b \times a + b$  и внутри квадрат  $c \times c$
- Делаем вывод, перекладывая треугольники

4. \*Построение  $\sqrt{2}$ ,  $\sqrt{7}$  (используются признаки подобия треугольников, отношения сторон)
5. Примеры пифагоровых троек (анонс теоремы!)

## 1.6 Бином Ньютона и другие формулы визуально

### Конспект

1. Визуализация  $(a - b)(a + b) = a^2 - b^2$ .
2. Сумма подряд идущих чисел  $1, 2, \dots, n$  с помощью сложения прямоугольников.
3. Сумма подряд идущих нечетных чисел.
4. Вывод формулы  $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$ .
5. Разрезание сырного кубика на 8 частей тремя плоскостями.

### Задачи

1. Вывести формулу квадрата суммы визуально.

## 1.7 Соизмеримость отрезков, алгоритм Евклида

### Конспект

1. Два отрезка  $a$  и  $b$ , кузнечики прыгают, один на  $a$  и  $-a$  сколько угодно раз, второй на  $b$  и  $-b$  сколько угодно раз
2. Кузнечики стартуют в одной и той же точке (назовем ее  $O$ ). Могут ли они попасть в одну точку, отличную от  $O$ , когда-нибудь?
3. Ответ — да, если есть такая точка  $A$ , что отрезок  $OA$  кратен и  $a$ , и  $b$  одновременно, т.е. при некоторых натуральных  $n, m$ , не равных нулю, будет верно равенство  $an = bm$ :

$$\underbrace{a + a + \dots + a}_{n \text{ раз}} = \underbrace{b + b + \dots + b}_{m \text{ раз}}$$

4. Отрезки, которые имеют общий кратный отрезок, называются **соизмеримыми**
5. Иллюстрация: строим прямоугольник  $a \times b$  ( $a < b$ ), начинаем отсекасть в нем квадраты: сначала отсекаем квадраты  $a \times a$ , пока можем, останется кусок  $a \times b_1$  ( $b_1 < a$ ), затем отсекаем квадраты  $b_1 \times b_1$ , пока можем, останется кусок  $a_1 \times b_1$  ( $a_1 < b_1$ ), и т.д.



6. Если исходные отрезки соизмеримы, то процесс остановится: исходный прямоугольник будет разбит на конечное число квадратов.
7. Финальный квадратик будет иллюстрировать НОД отрезков  $a$  и  $b$ , т.к. это максимальный квадрат, которым можно замостить прямоугольник  $a \times b$ .
8. Такой процесс называется **алгоритмом Евклида**, к нему мы еще вернемся с более формальной точки зрения.
9. Заметим, что числа  $a$  и  $b$  при этом вовсе не обязан быть натуральными.
10. Несоизмеримость стороны квадрата и его диагонали: 1 и  $\sqrt{2}$ .
11. Алгоритм Евклида никогда не остановится. НОДом будет бесконечно малое число.

### Задачи

1. Найти НОД(10,6) методом прямоугольников.
2. Сколько и каких шагов должен сделать кузнечик НОД(10,6), чтобы попасть в точку НОД(10,6)?

# Движения прямой

## Аннотация.

В этой главе мы переходим к более формальной работе с точками и векторами на прямой. Целью является знакомство с понятиями «движение», «композиция движений». Проводится полный анализ видов движений и свойств их композиций.

Попутно вводится понятие группы и подгруппы в приложении к группе движений на прямой. Изучаются все конечные подгруппы движений прямой.

## 2.1 Сдвиг, композиция сдвигов, группа

### Конспект

1. **Иллюстративная сказка.** Представим себе очень длинную однорядную автомобильную парковку на территории какого-нибудь бизнес-центра. На этой парковке размечены места номерами 0, 1, 2 и т.д. (слева направо). В какой-то момент парковку достроили влево и решили, не мудрствуя лукаво, продолжить нумерацию отрицательными числами  $-1$ ,  $-2$ ,  $-3$  и т.д. Получилась шкала примерно как на градуснике для измерения уличной температуры. Водителям, работающим в этом бизнес-центре, выдали парковочные талоны с номерами парковочных мест, т.е. такие же числа 0,  $\pm 1$ ,  $\pm 2$  и т.д. В соответствии с талонами они занимают свои места, так что получается, что водитель с талоном номер 0 встает на место номер 0, водитель с талоном номер 1 — на место номер 1 и т.д.
2. Но потом появляется необходимость поменять бордюр и плитку там, где находятся два крайних левых парковочных места, пусть это будут номера  $-3$  и  $-2$ . Возникает потребность куда-то девать те а/м, для которых зарезервированы номера  $-3$  и  $-2$ . Вместо того, чтобы предложить обменять талоны  $-3$  и  $-2$  на резервные номера парковки, начальнику охраны приходит в голову гениальная идея: повесить на въезде плакат с надписью (красным фломастером на А4): «Внимание! Занимайте номер парковки на 2 больше, чем указан в вашем талоне!!»

3. Так что водитель, имеющий парковочный талон номер -3, занимает место -1, номер -2 — место 0, номер -1 — место 1, и т.д.



4. Иначе говоря, все автомобили должны теперь вставать на 2 места правее, т.е. произвести сдвиг относительно своего обычного места, указанного в парковочных талонах.
5. Отметим еще одну особенность истории с парковкой: несмотря на произведенное перемещение автомобилей, они по-прежнему остаются на парковке, не занимая места где-либо еще, например, на проезжей части или тротуаре. Просто потому, что запас мест справа оказался достаточным для данной манипуляции.
6. А что, если бы парковка была неограниченно расширяемой в обе стороны автоматически всякий раз, когда не хватает места? Как говорят математики, она была бы потенциально бесконечной.
7. Геометрически мы можем представить это так: у нас имеется прямая, на которой нанесена разметка числами  $0, \pm 1, \pm 2$  и т.д. через равные расстояния между соседними точками. Прямая — бесконечная в обе стороны. Но вдруг возникает необходимость сдвинуть эту прямую вправо на 2 единицы. Для этого всем точкам прямой дается команда сдвинуться на вектор длины 2 вправо.
8. Однако, чтобы сохранить историю этого сдвига и проверить его правильность, следует сдвигать не саму прямую, а ее копию. В итоге мы получаем прямую-оригинал и прямую-образ. Если уж быть совсем точными, то у нас возникает то, что в математике называется функцией, т.е. соответствие между оригинальными точками и их точками-образами на копии прямой.
9. Так мы видим не только новое положение точек, после сдвига, но и как оно соотносится с прежним их положением!
10. Понятно, что сдвигать геометрическую прямую, не выходя за ее пределы, можно только вправо или влево, причем на вектор произвольной длины, не

обязательно на число 2 или 3, или им подобное. Тем более что цифровую разметку на прямую можно и вовсе не наносить.

11. Преобразование, состоящее в том, что все точки прямой сдвигаются на вектор  $a$ , называется **сдвигом** на вектор  $a$ . При этом, чтобы узнать, в какую точку (относительно исходной разметки) перейдет точка  $A$ , нужно от точки  $A$  отложить вектор  $a$ , т.е. найти сумму  $A + a$ . Это будет некоторая точка  $A'$  на этой же прямой.
12. Преобразование сдвига на вектор  $a$  обозначим  $T_a$ , а его действие на точку  $A$  обозначим  $T_a(A)$ . Так что

$$T_a(A) = A', \quad a = \vec{AA'}.$$

13. Сдвиг является движением (не случайно это однокоренные слова!).
14. Вообще, **движение** — это преобразование, сохраняющее расстояния (размеры и форму): если между точками  $A$  и  $B$  было расстояние  $x$ , то после преобразования движения расстояние между точками  $A'$  и  $B'$ , в которые перешли исходные точки, тоже будет  $x$ , и так для любой пары точек! Для сдвига это очевидно, поскольку ко всем точкам прибавляется один и тот же вектор.
15. Математическое движение — это результат физического движения (есть только начальное и конечное состояние системы).
16. Сдвиг характерен тем, что он в качестве параметра имеет только вектор, т.е. величину и направление сдвига, но он никак не связан с исходной разметкой прямой!
17. Композиция сдвигов — это их последовательное применение:

$$(T_b \circ T_a)(A) = T_b(T_a(A)).$$

18. Композиция сдвигов соответствует сумме векторов:  $T_b \circ T_a = T_{a+b}$ .
19. Композиция сдвигов перестановочна в силу коммутативности сложения:

$$T_b \circ T_a = T_a \circ T_b.$$

20. Композиция сдвигов ассоциативна, т.е. если мы имеем последовательность из трех и более сдвигов, мы можем начать вычислять ее с любого места цепочки, постепенно сворачивая выражение, как с обычными числами:

$$T_a \circ T_b \circ T_c = (T_a \circ T_b) \circ T_c = T_a \circ (T_b \circ T_c),$$

т.е. сначала вычислить композицию последних и результат подставить в первую, либо же наоборот — сначала вычислить первую, и ее применить к

последней. Это правило можно тиражировать на цепочку композиций любой длины. Результат при этом будет один и тот же, совершенно так же, как если бы мы складывали подряд несколько чисел.

21. Кратность сдвига обозначается как степень

$$\underbrace{T_a \circ \dots \circ T_a}_{n \text{ раз}} = T_a^n$$

и соответствует кратности сложения или умножению на степень кратности:  
 $T_a^n = T_{an}$ .

22. Нулевой сдвиг  $T_0 = \text{id}$  — это **тождественное преобразование**, которое ничего не меняет.

23. Обратный сдвиг  $T_a^{-1}$  — это сдвиг на вектор  $-a$ , т.е. сдвиг в обратном направлении на ту же величину.

24. Вообще, если есть какие-то два преобразования  $u$  и  $v$  и операция композиции  $\circ$ , то эти преобразования **взаимно обратны**, если  $u \circ v = \text{id}$  и  $v \circ u = \text{id}$ , т.е. последовательное применение этих преобразований в любом порядке является тождественным преобразованием.

25. Очевидно, что всякий сдвиг имеет обратный, причем  $T_a \circ T_a^{-1} = T_a^{-1} \circ T_a = \text{id}$ .

26. Нулевой сдвиг сам себе обратен.

27. Обобщая свойства сдвигов, фиксируем понятие **группы**. Это — такое множество  $G$  с заданной на нем одной бинарной операцией  $\circ$ , для которой выполняются аксиомы:

**G1)** Результат групповой операции снова лежит в этом же множестве (например, композиция сдвигов есть сдвиг):

$$u, v \in G \Rightarrow u \circ v \in G.$$

**G2)** Групповая операция **ассоциативна** (сочетательный закон): для любых элементов  $u, v, w$  группы  $G$

$$(u \circ v) \circ w = u \circ (v \circ w)$$

(например,  $(T_a \circ T_b) \circ T_c = T_a \circ (T_b \circ T_c)$ ).

**G3)** Существует **нейтральный элемент**  $\text{id}$  такой, что для любого элемента  $u$  имеет место равенство

$$u \circ \text{id} = u = \text{id} \circ u.$$

**G4)** Групповая операция **обратима**: для всякого элемента  $u$  существует обратный ему элемент  $v$  такой, что

$$u \circ v = \text{id} = v \circ u$$

(например, обратный сдвиг — это сдвиг в противоположную сторону:  $T_a^{-1} = T_{-a}$ ). Элемент  $v$  в таком случае обозначается как  $u^{-1}$  и называется **обратным** к элементу  $u$ .

28. Множество всех сдвигов образует группу относительно операции композиции!

29. Мало того, группа сдвигов **коммутативна** (абелева), т.е. для ее групповой операции выполняется переместительный закон:

**G5)**  $u \circ v = v \circ u$  для всех  $u, v$  из группы  $G$ .

30. Кратность обратного сдвига:  $T_a^{-n} = (T_a^{-1})^n = T_{-a}^n = T_{-an}$ .

31. Обратный сдвиг к композиции сдвигов:  $(T_a \circ T_b)^{-1} = T_b \circ T_a$ . Это легко следует из общего свойства группы:

$$(u \circ v)^{-1} = v^{-1} \circ u^{-1}, \text{ поскольку } (u \circ v) \circ (v^{-1} \circ u^{-1}) = u \circ (v \circ v^{-1}) \circ u = \text{id}.$$

32. На основе только одного сдвига  $T_a$  можно построить подгруппу сдвигов

$$\langle T_a \rangle = \{T_a^n, T_a^{-n} \mid n = 0, 1, 2, \dots\}$$

33. Эта подгруппа — реализация целых чисел  $\mathbb{Z}$ , к которым мы еще вернемся позже.

34. Фиксируем понятие **подгруппы**. Это — подмножество группы, на котором групповая операция удовлетворяет групповым аксиомам, т.е. подгруппа сама является группой с той же операцией, которая задана в группе.

35. Каждый сдвиг  $T_a$  порождает (с помощью его многократного тиражирования) свою подгруппу в группе всех сдвигов.

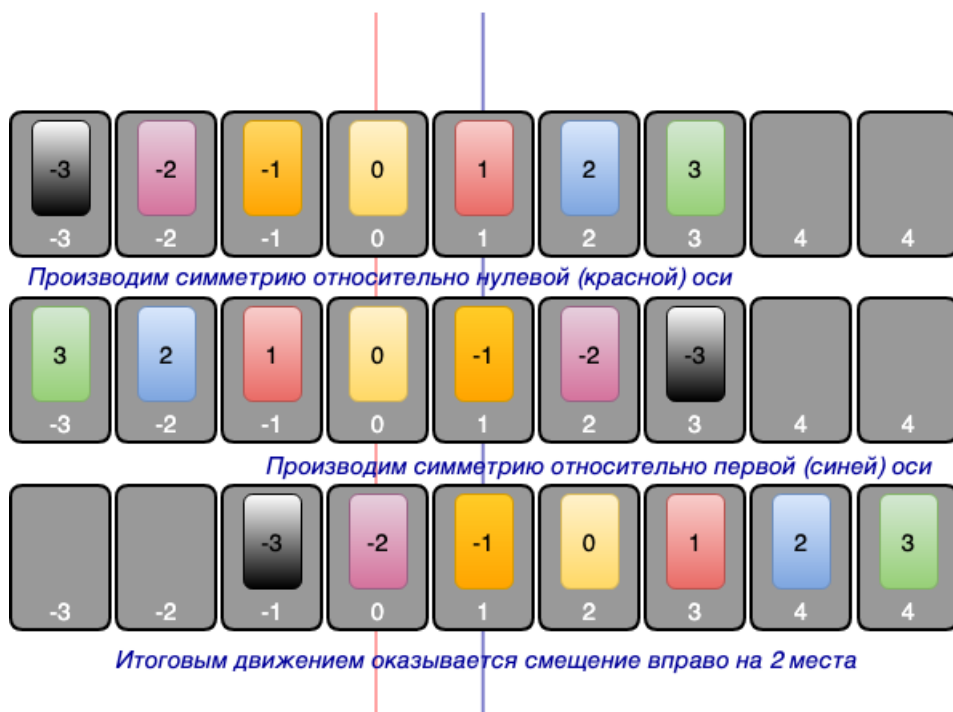
## 2.2 Отражение

### Конспект

1. Продолжим нашу историю с движением автомобилей. Пусть на сей раз вместо парковки они готовятся к параду и должны занять свои места в ряду с номерами  $0, \pm 1, \pm 2$  и т.д. Номера мест нанесены, как и ранее, на асфальт и представляют собой один ряд. У водителей а/м есть предписания, в которых

указано, какие места нужно занять. Следующим шагом предписания является команда обменяться местами так, чтобы порядок а/м сменился на противоположный. Иначе говоря, каждому нужно проехать полукруг и занять место, симметричное относительно заданного. Например, центром симметрии и соответствующих полукругов является место 0. Тогда а/м, стоящий на 1-м месте, должен переехать на место  $-1$ , стоящий на 2-м месте — на место  $-2$ , и т.д.

- В результате мы получим перестроение на параде, при котором а/м опишут полукруги и встанут в обратном порядке, причем нулевой а/м сохранит свое место.



- Заметим, что и в этом случае расстояние между а/м сохранится: как было ранее 2 а/м между 0-м и 3-м, так и останется. И так для всех пар автомобилей.
- Такой вид движений называется **отражением**. Вся наша линейная парковка отразилась относительно нулевого места.
- Особо отметим, что физически отражение всегда требует выхода за пределы исходной фигуры. Если сдвиг мы могли осуществить, находясь внутри парковочной сетки (ну, да, предположим, что мы имеем дело с танками, которые могут на месте повернуться на 90 градусов, произвести перемещение, а затем развернуться снова, либо что имеем дело с параллельной парковкой, где

а/м стоят вдоль направления нумерации), то отражение никак невозможно выполнить, оставаясь в пределах исходной парковки — потребуется выезд на проезжую часть.

6. Отражение на геометрической прямой — то же самое. Сначала мы должны выбрать центр отражения, который останется на месте, затем перевернуть прямую в обратном направлении (снова имеем выход во внешнее пространство, если представить отражение как физический процесс!).
7. Отражение с центром в точке  $O$  будем обозначать  $S_O$ . Отражение можно представить как огромное количество сдвигов, выполняемых одновременно. Для каждой точки — свой сдвиг. Так, в результате действия отражения  $S_O$  на точку  $A$  мы получим точку  $A' = T_a(A)$ , где вектор  $a = \vec{AO}$ . То есть, мы производим сдвиг на расстояние  $OA$ , только в противоположную от  $A$  сторону.
8. Как и в случае со сдвигом, отражение — это функция, т.е. оно «помнит» исходную разметку прямой, а значит, мы всегда можем сказать, какая точка откуда пришла в свое новое состояние.
9. Отражение, в отличие от сдвига, намертво привязано к одной выделенной точке на прямой *в исходной разметке*, и полностью ею определяется! Мы можем рассмотреть два и более отражений, но все они должны быть заданы в одной исходной разметке прямой, чтобы не возникла путаница.
10. Отражение обратно самому себе:  $S_O \circ S_O = \text{id}$ , т.е.  $S_O^{-1} = S_O$ .
11. В терминах парада, показанного на рисунке, все отражения задаются относительно разметки мест на асфальте! В этом случае водителям для выполнения операции отражения не нужно знать, где какие номера а/м находятся, им достаточно видеть номер своего парковочного места, знать номер места—центра симметрии, и выполнить перемещение на удвоенное расстояние, чтобы занять противоположное место (см. рис. выше).
12. Поэтому композиция отражений, т.е. их последовательное применение, легко вычисляется:

$$S_O \circ S_C = T_{CO}, \quad S_C \circ S_O = T_{OC}. \quad (2.1)$$

Если вспомнить общее групповое правило  $(u \circ v)^{-1} = v^{-1} \circ u^{-1}$ , то второе равенство легко получить из первого:

$$T_{OC} = T_{CO}^{-1} = (S_O \circ S_C)^{-1} = S_C^{-1} \circ S_O^{-1} = S_C \circ S_O.$$

13. Заметим, что композиция отражений является сдвигом и при этом не коммутативна! То есть, отражения, производимые в разной последовательности, приводят, вообще говоря, к разным результирующим сдвигам, а именно — к противоположным.



14. Композиция отражения и сдвига:

$$S_O \circ T_a = S_{O-a/2}, \quad T_a \circ S_O = S_{O+a/2}. \tag{2.2}$$

Это легко проверить, если вместо  $a$  подставить  $2CO$ , и в предыдущих равенствах произвести необходимые домножения. предлагаем это проделать самостоятельно.

15. Итак, композиция сдвига и отражения является отражением и при этом также не коммутативна!

16. Таблица композиций отражений и сдвигов:

	$T_a$	$S_O$
$T_b$	$T_{a+b}$	$S_{O+b/2}$
$S_C$	$S_{C-a/2}$	$T_{2OC}$

17. Кратность отражения  $S_O^n$  определяется четностью числа  $n$ . В случае четного  $n$  это  $\text{id}$ , в случае нечетного — исходное  $S_O$ .

18. Пара  $\{\text{id}, S_O\}$  образует самую маленькую нетривиальную группу движений, которая, к тому же, является абелевой и циклической (т.е. все ее элементы есть степени какого-то одного, а именно  $S_O = S_O^1, \text{id} = S_O^2$ ).

	$\text{id}$	$S_O$
$\text{id}$	$\text{id}$	$S_O$
$S_O$	$S_O$	$\text{id}$

19. Видим, что таблица полностью повторяет таблицу умножения знаков, причем  $\text{id}$  является нейтральным элементом.

20. Суммируя, находим, что вообще все сдвиги и отражения вместе образуют группу (относительно операции композиции), т.е. для них выполняются аксиомы группы G1–G4. При этом данная группа не является абелевой (не выполняется G5), поскольку, как мы видели, далеко не все композиции движений перестановочны.

### Задачи

1. Вывести равенства (2.2) из равенств (2.1).

## 2.3 Таблица Кэли движений прямой

### Конспект

1. Еще пример группы: рассмотрим класс всех сдвигов  $\mathbb{T}$  и класс всех отражений  $\mathbb{S}$

2. Мы можем определить композицию классов  $T \circ T$ ,  $T \circ S$ ,  $S \circ T$  и  $S \circ S$  как все возможные композиции движений из этих классов в указанном порядке. Иначе говоря, композиции классов — это их умножение по Минковскому:

$$T \circ T = \{t \circ t' \mid (t \in T) \wedge (t' \in T)\}, \quad T \circ S = \{t \circ s \mid (t \in T) \wedge (s \in S)\}$$

$$S \circ T = \{s \circ t \mid (s \in S) \wedge (t \in T)\}, \quad S \circ S = \{s \circ s' \mid (s \in S) \wedge (s' \in S)\}$$

3. Из произведенных выше вычислений легко видеть таблицу композиций этих классов:

	T	S
T	T	S
S	S	T

4. Видим полную аналогию с таблицей знаков и таблицей для  $\text{id}, S_O$ . Здесь класс  $T$  является нейтральным элементом
5. Если теперь собрать в одну кучу все сдвиги и отражения, то получим группу движений прямой
6. Наша цель — доказать, что других движений нет, т.е. что множество  $\{T_a, S_O\}_{a,O}$  полностью исчерпывает все возможные движения прямой

## Задачи

Пусть на прямой даны 4 точки  $A, B, C, D$ , поставленные друг за другом с одинаковым шагом (см.рис).



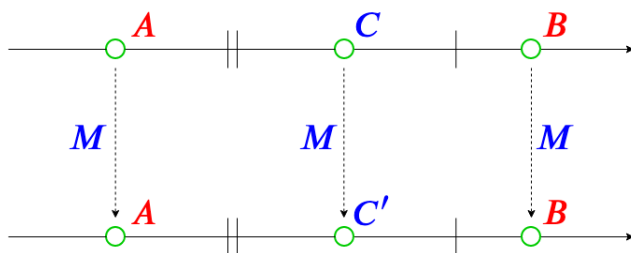
1. Куда перейдет точка  $A$  при преобразовании  $S_B$ ?
2. Куда перейдут точки  $B, C, D$  при преобразовании  $T_{AB} \circ T_{CA}$ ?
3. Куда перейдут точки  $A, B, C$  при преобразовании  $S_C \circ T_{AB}$ ?

## 2.4 Теорема о гвоздях, аналог теоремы Шаля

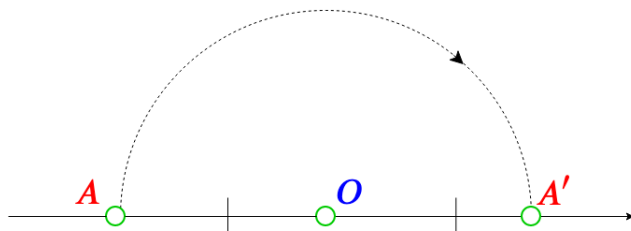
### Конспект

1. Анализ движений проводится на основе наблюдений за количеством стационарных точек
2. Пусть движение  $M$  таково, что оно оставляет на месте две точки  $A \neq B$ .

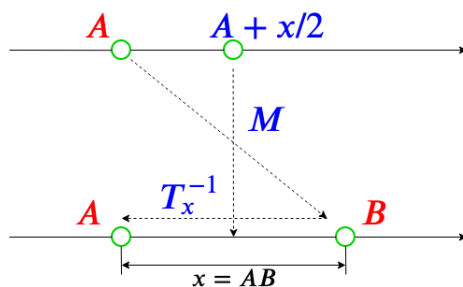
3.  $M(A) = A$  и  $M(B) = B$ . Пусть  $C' = M(C)$ .  $M$  сохраняет расстояния  $AC$  и  $BC$ , откуда  $AC = AC'$  и  $BC = BC'$ , откуда  $C = C'$ . Т.е.  $M(C) = C$  для любых точек  $C$ , т.е.  $M = \text{id}$



4. Пусть движение  $M$  оставляет на месте ровно одну точку  $O$ . В этом случае  $A' = M(A)$  и  $A \neq A'$  и  $OA = OA'$ , тогда  $A'$  — отражение  $A$  относительно  $O$ . Следовательно,  $M = S_O$



5. Пусть движение  $M$  не оставляет на месте ни одной точки и пусть  $B = M(A)$  ( $B \neq A$ ). Обозначим  $x = AB$ . Тогда  $T_x^{-1} \circ M(A) = A$ , т.е.  $T_x^{-1} \circ M$  оставляет на месте хотя бы одну точку  $A$ .



Если оно оставляет на месте ровно одну точку  $A$ , то это некоторая симметрия  $S_A$ , но тогда  $M = T_x \circ S_A = S_{A+x/2}$ . Получается, что  $M$  сохраняет точку  $A + x/2$  на месте. Противоречие. Остается вариант, что  $T_x^{-1} \circ M$  оставляет на месте как минимум две точки, но тогда  $T_x^{-1} \circ M = \text{id}$ , откуда  $M = T_x \circ \text{id} = T_x$  — сдвиг.

6. Таким образом, все движения прямой — это либо сдвиги (в частности,  $\text{id}$ ), либо отражения (теорема Шаля).
7. При этом, любое движение — это либо одна симметрия, либо композиция двух симметрий.

## Задачи

1. Построить сдвиг на 7 единиц вправо с помощью композиции двух симметрий.
2. Каким движением является следующая композиция?

$$S_{O+n} \circ S_{O+n-1} \circ \cdots \circ S_{O+1} \circ S_O.$$

Ответ получить в зависимости от четности  $n$ .

## 2.5 Все конечные подгруппы движений прямой

### Конспект

1. Ранее мы нашли некоторые подгруппы группы движений прямой, а именно:
  - группа всех сдвигов — бесконечная коммутативная группа;
  - группа, порожденная одним сдвигом  $\langle T_a \rangle$  — тоже бесконечная коммутативная группа;
  - группа одного отражения  $\{\text{id}, S_O\}$  — конечная группа, состоящая из двух элементов.
2. Возникает вопрос: а существуют ли промежуточные по размеру конечные подгруппы группы движений? Попробуем описать все конечные подгруппы движений прямой.
3. Пусть  $G$  — конечная подгруппа группы движений прямой.
4. Во-первых, ясно, что  $\text{id} \in G$  в силу определения группы.
5. Во-вторых, никакой сдвиг  $T_a$  при ненулевом  $a$  не может быть элементом  $G$ , иначе в  $H$  окажутся все степени  $T_a$ , т.е.  $\langle T_a \rangle \subseteq G$ , и  $G$  будет бесконечной.

6. В-третьих, если в  $G$  есть хотя бы два различных отражения  $S_A$  и  $S_B$  ( $A \neq B$ ), то и их композиция также находится в  $G$ , но это ненулевой сдвиг  $T_{2AB}$ , а все такие сдвиги мы исключили чуть выше. Следовательно, если в группе  $G$  и есть отражение, то только одно.
7. Таким образом, либо  $G = \{\text{id}\}$  (тривиальная группа), либо  $G = \{\text{id}, S_O\}$  при некотором отражении  $S_O$ .

# Вокруг окружности

## Аннотация.

В этой главе мы расширяем сферу деятельности и переходим к движениям окружности. Снова изучаем виды движений, строим таблицу композиций, доказываем теорему Шаля.

Попутно сопоставляем движения окружности с движениями прямой, выходим на отрицательные степени композиций и их арифметические свойства, как следствие, получаем целые числа.

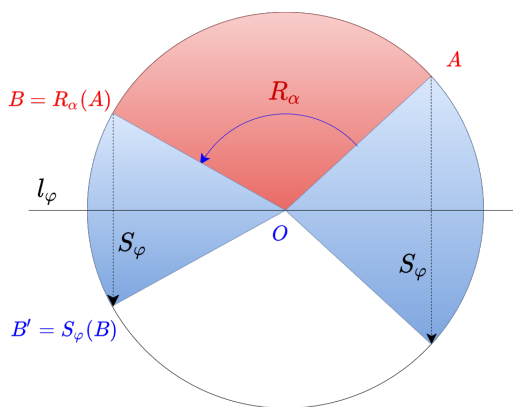
По аналогии с натуральными числами говорим о том, что целые числа — это и степени композиций движений, и мера длины, только оснащенная знаком, т.е. направлением измерения длины.

## 3.1 Движения окружности

### Конспект

1. Берем окружность (обруч). Какие у нее есть движения, переводящие его в самого себя?
2. Прежде всего, повторим, что движение — это преобразование, сохраняющее расстояния (изометрия). Поэтому, если мы говорим о движении, переводящем фигуру (прямую, круг, квадрат, многоугольник, плоскость и т.д.) в саму себя, то это значит, что мы берем копию этой фигуры и накладываем ее на оригинал до полного совмещения контуров. При этом допускается вертеть ее как угодно, лишь бы наложение фигур оказалось идеальным — без выступов и впадин, без какой-либо деформации.
3. Для того, чтобы уточнить смысл определения движения, нужно зафиксировать способ измерения расстояний на окружности. Расстоянием между точками окружности  $A$  и  $B$  будем называть длину меньшей из дуг, соединяющих эти точки.
4. Очевидно, что движениями окружности являются как минимум: вращение вокруг ее центра, а также симметрии относительно прямых, проходящих через ее центр.

5. В некотором смысле окружность — аналог прямой. Только эту прямую взяли за 2 конца и замкнули где-то на бесконечности.
6. Поэтому вращение окружности соответствует сдвигу прямой, а симметрия окружности относительно прямой — отражению на прямой относительно точки (можно считать ее симметрией относительно перпендикулярной прямой).
7. Если представить, что на окружности большого радиуса живут маленькие одномерные математики, то для них окружность будет практически не отличима от прямой, и движения окружности они будут воспринимать именно как движения прямой.
8. Поворот на угол  $\alpha$  обозначим  $R_\alpha$  (положительный — против часовой стрелки), симметрию относительно прямой, имеющей угол наклона  $\varphi$ , обозначим  $S_\varphi$  ( $0 \leq \varphi < 180^\circ$ ). Угол наклона прямой измеряется от некоторого заданного раз и навсегда радиуса окружности, который можно считать точкой отсчета (аналог нуля на прямой).
9. Ось симметрии  $S_\varphi$  мы будем обозначать  $l_\varphi$  (см. рис.)



10. Вновь замечаем, что композиция поворотов есть поворот на суммарный угол:  
 $R_\alpha \circ R_\beta = R_{\alpha+\beta}$
11. У каждого поворота есть обратный:  $R_\alpha^{-1} = R_{-\alpha}$ , т.н. поворот в противоположном направлении.
12. Повороты коммутируют:  $R_\alpha \circ R_\beta = R_\beta \circ R_\alpha$ .
13. Есть нейтральный поворот  $\text{id} = R_0$ .
14. Так что все повороты образуют группу относительно операции композиции.
15. Тем не менее, есть одна особенность: поворот на угол  $360^\circ k$  — это тоже  $\text{id}$ .
16. Вообще, повороты, заданные углами с шагом  $360^\circ$ , равны:  $R_\alpha = R_{\alpha \pm 360^\circ k}$ , где  $k$  — натуральное число.

17. Некоторые повороты дают  $\text{id}$  в некоторой степени, например,  $R_{90^\circ}^4 = \text{id}$ ,  $R_{60^\circ}^6 = \text{id}$  и т.д.
18. Если угол, выраженный в градусах, соизмерим с величиной  $360^\circ$ , то поворот на данный угол имеет положительную степень, в которой он обращается в  $\text{id}$ .
19. Но есть угол, не обладающий таким свойством, это угол в 1 радиан. Если бы он был соизмерим с полным оборотом, то число  $\pi$  оказалось бы соизмеримым с 1, а это не так! Доказательство этого факта является сложной математической теоремой!
20. В зависимости от соизмеримости угла поворота с полным оборотом некоторые повороты порождают конечные циклические подгруппы в группе движений, а некоторые — нет.

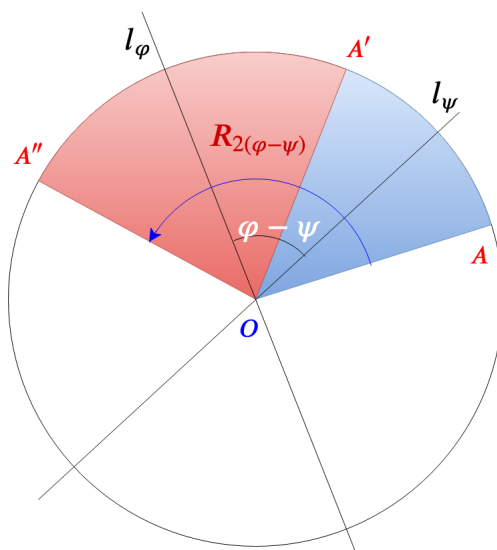
## 3.2 Группа движений окружности, теорема Шаля

### Конспект

1. Композиция симметрий:

$$S_\psi \circ S_\varphi = R_{2(\psi-\varphi)}, \quad S_\varphi \circ S_\psi = R_{2(\varphi-\psi)}$$

Этот факт легко увидеть из картинки, где точка  $A$  переходит в  $A'$  под действием симметрии  $S_\psi$  относительно оси  $l_\psi$ , а затем  $A'$  переходит в  $A''$  под действием симметрии  $S_\varphi$  относительно оси  $l_\varphi$ :





Суммарный угол поворота точки  $A$  при переходе в точку  $A''$  можно разбить на 2 пары углов так, что в каждой паре углы равны в силу свойств симметрии (разные пары отмечены разным цветом), и в то же время угол между осями состоит как раз из суммы углов, принадлежащих разным парам. Нетрудно убедиться в аналогичном результате и в том случае, если точка лежит между осями симметрии.

2. Итак, композиция симметрий является поворотом на двойной угол между их осями. Отсюда видно также, что композиция симметрий не коммутативна! Перестановка симметрий приводит к смене направления вращения.
3. Композиция симметрии и поворота:

$$S_\varphi \circ R_\alpha = S_{\varphi-\alpha/2}, \quad R_\alpha \circ S_\varphi = S_{\varphi+\alpha/2}$$

Это легко доказать из предыдущего равенства для композиции симметрий. Рассмотрим композицию  $S_\varphi \circ R_\alpha$ . Пусть также  $\psi = \varphi - \alpha/2$ . Домножая слева равенство  $S_\varphi \circ S_\psi = R_{2(\varphi-\psi)}$  на симметрию  $S_\varphi$ , получим

$$S_\varphi \circ R_{2(\varphi-\psi)} = S_\varphi \circ (S_\varphi \circ S_\psi) = (S_\varphi \circ S_\varphi) \circ S_\psi = S_\psi,$$

откуда

$$S_\varphi \circ R_\alpha = S_\varphi \circ R_{2(\varphi-\psi)} = S_\psi = S_{\varphi-\alpha/2}.$$

Аналогично доказывается второе равенство.

4. Итак, композиция симметрии и поворота является симметрией и при этом тоже не коммутативна!
5. Запишем полную таблицу композиций симметрий и вращений окружности:

	$R_\alpha$	$S_\psi$
$R_\beta$	$R_{\alpha+\beta}$	$S_{\psi+\beta/2}$
$S_\varphi$	$S_{\varphi-\alpha/2}$	$R_{2(\varphi-\psi)}$

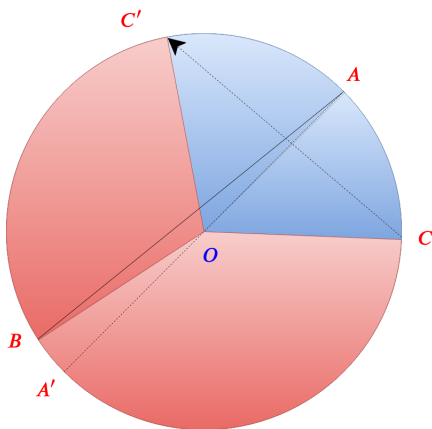
6. По аналогии с прямой обозначим  $\mathbb{T}$  класс всех вращений окружности,  $\mathbb{S}$  — класс всех симметрий окружности
7. Получаем аналогичную таблицу композиций классов:

	$\mathbb{T}$	$\mathbb{S}$
$\mathbb{T}$	$\mathbb{T}$	$\mathbb{S}$
$\mathbb{S}$	$\mathbb{S}$	$\mathbb{T}$

8. Снова наблюдаем все ту же группу умножения знаков!
9. Существуют ли другие движения окружности? Ответ — нет!

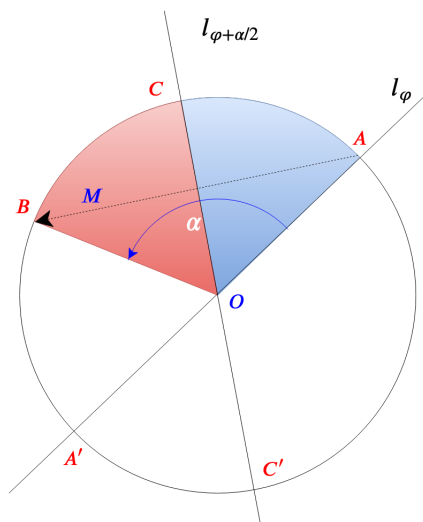
10. Анализ движений проводится, как и в случае прямой, на основе наблюдений за количеством стационарных точек.
11. Для начала заметим, что если при движении окружности одна точка остается на месте, то неподвижной будет и диаметрально противоположная ей точка. Если бы это было не так, то, очевидно, расстояние между этими точками (равное половине дуги окружности) не сохранялось бы — оно стало бы меньше. А это невозможно при движении.
12. Поэтому при анализе движений окружности всегда нужно иметь ввиду, что пары противоположных точек ведут себя одинаково — либо они обе стационарны, либо обе движутся.
13. Пусть движение  $M$  таково, что оно оставляет на месте две точки  $A \neq B$ , не являющиеся диаметрально противоположными.
14.  $M(A) = A$  и  $M(B) = B$ . Пусть  $C' = M(C)$ . Здесь могут быть два варианта: либо  $C$  лежит на малой дуге  $AB$ , либо на большой. Эти дуги не могут быть равны по длине, т.к.  $A$  и  $B$  не являются противоположными (см.рис.). Точка  $C'$  может лежать строго на одной из этих дуг.

Поскольку  $M$  сохраняет расстояния, дуги  $AC$  и  $AC'$  равны, дуги  $BC$  и  $BC'$  равны. А значит, равны и суммы длин дуг  $AC + CB$  и  $AC' + C'B$ . Отсюда следует, что  $C$  и  $C'$  могут лежать только на одной и той же дуге. Но тогда, в силу равенства дуг  $AC$  и  $AC'$  точки  $C$  и  $C'$  также должны совпадать (они лежат на одной дуге и на равных расстояниях от концов). Таким образом,  $M(C) = C$  для любых точек  $C$ , т.е.  $M = \text{id}$ .



15. Пусть движение  $M$  оставляет на месте ровно одну пару противоположных точек  $A$  и  $A'$ . В этом случае  $C' = M(C)$ ,  $C \neq C'$  и  $AC = AC'$ , тогда  $C'$  — отражение  $C$  относительно оси симметрии  $AA'$ . Следовательно,  $M = S_\varphi$ , где  $\varphi$  — угол наклона прямой  $AB$ .

16. Пусть движение  $M$  не оставляет на месте ни одной точки и пусть  $B = M(A)$  ( $B \neq A$ ). Обозначим за  $\alpha$  угол дуги  $AB$ .



Тогда  $R_\alpha^{-1} \circ M(A) = A$ , т.е.  $R_\alpha^{-1} \circ M$  оставляет на месте хотя бы одну точку  $A$  (а точнее, пару противоположных точек  $A$  и  $A'$ ). Если оно оставляет на месте ровно одну пару точек  $A$  и  $A'$ , то это некоторая симметрия  $S_\varphi$  (на рис. ось симметрии  $l_\varphi$ ), но тогда  $M = R_\alpha \circ S_\varphi = S_{\varphi+\alpha/2}$ . Получается, что  $M$  сохраняет точку  $C$  на месте ( $C$  есть середина дуги  $AB$ ). Противоречие с тем, что  $M$  не оставляет на месте ни одной точки. Остается вариант, что  $R_\alpha^{-1} \circ M$  оставляет на месте как минимум две точки, не являющихся противоположными, но тогда  $R_\alpha^{-1} \circ M = \text{id}$ , откуда  $M = R_\alpha \circ \text{id} = R_\alpha$  — поворот.

17. Таким образом, всякое движение окружности — это либо поворот (в частности,  $\text{id}$ ), либо симметрия относительно оси, проходящей через центр окружности (теорема Шаля).
18. При этом, любое движение — это либо одна симметрия, либо композиция двух симметрий.

## Задачи

1. Центральная симметрия — это какое движение?
2. Композицией каких симметрий можно выразить центральную симметрию?
3. С помощью симметрии относительно оси  $Ox$  и вращений выразить симметрию относительно оси  $Oy$ .

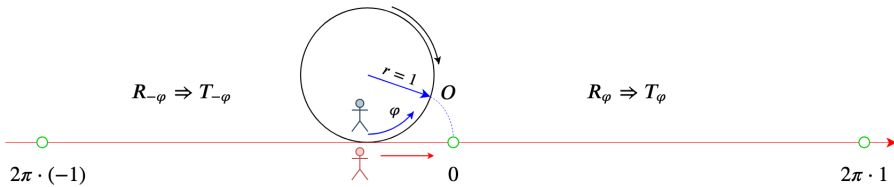
### 3.3 Наматывание прямой на окружность

#### Конспект

1. Совместим теперь окружность с прямой иным способом. Выделим на окружности точку  $O$  и начнем ее обход (вращение) в положительном направлении.
2. Выше мы видели, что углы поворота, кратные  $360^\circ$ , т.е. полному обороту, соответствуют тождественному движению, т.е. приведут нас в точку отправления  $O$ .
3. Однако, если с точки зрения математического движения ничего не изменилось, физически мы проделали путь, равный длине окружности. Для удобства будем считать, что радиус окружности есть единичный вектор, так что ее длина равна  $2\pi$ , и с каждым полным оборотом мы будем «наматывать» расстояние  $2\pi$ .
4. Вообще, расстояние, пройденное по окружности единичного радиуса, когда этот радиус заметает угол  $\alpha$ , равно  $\alpha(2\pi/360^\circ)$ . Чтобы каждый раз не переводить единицы измерения радиуса в градусы и наоборот, углы также примут измерять в единицах длины — радианах. А именно, *угол в 1 радиан соответствует повороту, при котором точка проделает по окружности путь, равный по длине радиусу данной окружности*. Нетрудно видеть, что в градусах 1 радиан будет иметь выражение  $360^\circ/(2\pi)$  или  $180^\circ/\pi \approx 57^\circ$ .
5. В дальнейшем условимся все углы измерять в радианах, если не потребуется иное.
6. Известно, что число  $\pi$  не соизмеримо с целыми числами, так что поворот  $R_1$  на 1 радиан ни в какой положительной степени не приведет нас снова в точку исхода  $O$ .
7. Зато поворот  $R_{2\pi}$  в точности возвращает нас в точку отправления  $O$ .
8. При каждом таком повороте мы проделываем путь, равный углу поворота, т.е.  $2\pi$  (радиус равен 1).
9. Следовательно степени такого поворота  $R_{2\pi}^n$  дадут прохождение пути длиной  $2\pi n$ .
10. Представим эту картину не с точки зрения жителей окружности, бегающих по замкнутой траектории, а с точки зрения жителей прямой, которая наматывается на окружность. С их точки зрения все выглядит несколько иначе и больше напоминает движение оклеса по дорожному полотну: окружность катится по прямой и через равные промежутки касается точкой  $O$  данной прямой.
11. Если при этом два друга — один из мира окружности, второй из мира прямой, — двигаются с одинаковой скоростью в одном направлении, то они могут

синхронизироваться в точке касания окружности и прямой и разговаривать друг с другом.

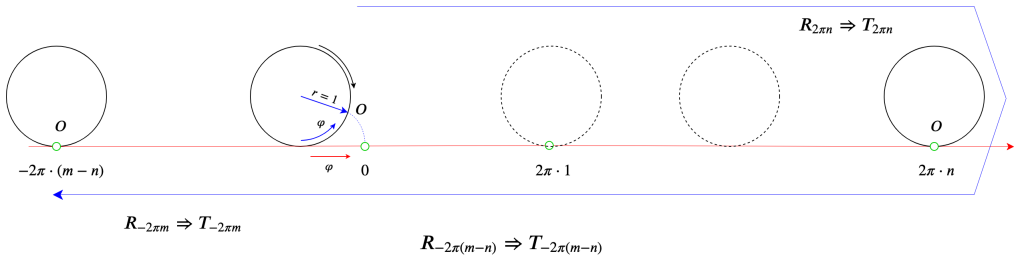
12. Нужно заметить при этом, что если колесо вращается по часовой стрелке, т.е. в отрицательном направлении, то вдоль прямой оно движется направо, т.е. в положительном направлении. Но фокус в том, что житель окружности для синхронизации с жителем прямой должен идти навстречу вращению колеса, т.е. тоже в положительном направлении! Таким образом, движения обоих друзей имеют одинаковый знак! На рис. ниже мы отметили синей стрелкой направление движения жителя окружности, а черной — встречное вращение самой окружности.
13. Итак, колесо катится, два друга беседуют, точка  $O$  то и дело, а именно через каждые  $2\pi$  метров соприкасается с прямой. Каждый раз, когда точка  $O$  касается прямой, наш ученый друг из мира прямой ставит на ней отметины и считает их по порядку, т.е. приравнивает к степени совершенного поворота колеса: в начальный момент времени это был 0, затем 1 оборот, затем 2 оборота, и т.д.



14. Что же мы видим на прямой? Мы видим не что иное как шкалу натуральных чисел, в точности соответствующую степеням вращений окружности. Число  $2\pi$ , фигурирующее как коэффициент, является не более чем единицей измерения. Кто-то измеряет в метрах, кто-то — в ярдах, а мы измеряем в длинах единичной окружности.
15. Представим теперь, что в какой-то момент касания точки  $O$  с прямой физика мира изменилась, и вращение начало осуществляться в обратную сторону!
16. Наши друзья-ученые при этом продолжают совместное путешествие, но только назад. Они пойдут отсчитывать уже проставленные отметки на прямой в убывающем порядке, пока не вернутся в точку 0. Но здесь состоится чудо, и движение продолжится дальше.
17. Как все это записать на языке вращений и сдвигов?
18. Предположим, что сначала окружность повернулась на  $n$  полных оборотов вперед, а затем на  $m$  полных оборотов назад.
19. Мы получаем итоговое вращение, записываемое как  $R_{2\pi n} \circ R_{2\pi m}^{-1}$ .

20. А что мы имеем с точки зрения движения на прямой?
21. Сначала был произведен сдвиг  $T_{2\pi n}$ , затем сдвиг  $T_{-2\pi m}$ .
22. И мы видим, что индекс, определяющий итоговое вращение и итоговый сдвиг, — один и тот же!
23. Причем, если  $n > m$ , то сдвиг будет вправо на расстояние  $2\pi(n-m)$ , а поворот будет положительным на угол  $2\pi(n-m)$ .
24. Если же  $n < m$ , то сдвиг будет влево на расстояние  $2\pi(m-n)$ , а поворот будет отрицательным (по часовой стрелке) на угол  $2\pi(m-n)$ .
25. Ранее мы уже договаривались, что перед векторами, направленными влево, будем ставить знак '-'. Так же будем поступать и с углами вращений в отрицательную сторону.
26. Соответственно, при  $n < m$  мы будем иметь итоговый сдвиг  $T_{-2\pi(m-n)}$  и итоговый поворот  $R_{-2\pi(m-n)}$ , которые также можно записать в виде степеней:

$$T_{-2\pi(m-n)} = T_{2\pi}^{-(m-n)} \text{ и } R_{-2\pi(m-n)} = R_{2\pi}^{-(m-n)}.$$



27. Осталось добавить маленький штрих к портрету, а именно: в случае  $n < m$  под разностью  $n - m$  будем понимать запись  $-(m - n)$ .
28. Тогда уже независимо от того,  $n < m$ , или  $m < n$ , или  $n = m$ , композиция поворотов и сдвигов сначала на  $n$  вправо и затем на  $m$  влево будет записываться одинаково:

$$T_{2\pi(n-m)} = T_{2\pi}^{n-m} \text{ и } R_{2\pi(n-m)} = R_{2\pi}^{n-m}.$$

29. В итоге мы приходим к тому, что называется **целыми числами**, включающими натуральные числа и отрицательные натуральные числа (при этом  $-0 = 0$ ).
30. Сколько бы мы ни вращали окружность на  $2\pi$  в ту или иную сторону с помощью поворота  $R_{2\pi}$ , мы совершаем поворот на целую степень полного оборота. При этом как бы мы ни катали окружность по прямой, точка  $O$  будет ставить отметки в точках  $2\pi k$ , где  $k$  — целое число.

# Целые числа и ОТА

## Аннотация.

Это — первая глава, где мы по-настоящему погружаемся в арифметику, используя тот понятийный аппарат, который был наработан в предыдущих главах. Здесь вводится обозначение множества целых чисел, дается строгое определение алгебраического понятия «кольцо», обосновывается алгоритм Евклида.

Ключевым моментом является получение теоремы о том, что НОД двух чисел можно записать в виде их линейной комбинации с целыми коэффициентами. Этот факт выводится как непосредственно из алгоритма Евклида, так и с помощью сумм Минковского (что отсылает нас к главе 0).

Далее отсюда выводится основная теорема арифметики и некоторые ее следствия.

## 4.1 Целые числа. Кольцо

### Конспект

1. Итак, совмещение вращений со сдвигами дает нам полную свободу перемещений в положительном и отрицательном направлении. При этом, с точки зрения окружности ничего не меняется — происходит итоговое движение  $\text{id}$ , а с точки зрения прямой — происходит разметка точек с равным шагом. Ясно, что сам шаг при этом не имеет значения. Мы могли бы взять окружность радиуса  $R$ , и тогда шаг был бы равен  $2\pi R$ . В частности, можно взять радиус  $R = 1/2\pi$ , и тогда точки на прямой расположатся с шагом 1.
2. Такую же картину можно получить, если взять все точки, получаемые из выделенной точки 0 степенями сдвига на единичный вектор, используя положительные и отрицательные, т.е. целые, степени.
3. Как видим, целые числа, как и натуральные, можно интерпретировать и как степени движений (и вообще любых преобразований, имеющих обратные), и как векторы сдвигов на прямой, а значит, к ним применимы определенные ранее операции сложения, вычитания и умножения. При этом результат умножения получает такой знак, который определяется из таблицы умножения знаков.

4. Множество всех целых чисел принято обозначать  $\mathbb{Z}$ . Вместе с операциями сложения (вычитания) и умножения структура  $(\mathbb{Z}, +, \cdot)$  называется **кольцом целых чисел**. Кольцо — это структура, где можно складывать, вычитать и умножать.
5. Понятие кольцо является расширением понятия группы, т.к. добавляется операция умножения.
6. Ранее мы уже видели такие группы, как группа движений прямой, группа умножения знаков, группа композиций классов сдвигов и симметрий, группа вращений окружности. Все они обладали одной операцией — композицией, которая соответствовала сложению параметров сдвигов и вращений.
7. Кроме того, мы ввели такое понятие как кратность, заменяя тем самым многократное сложение умножением на целое число.
8. Кратность операций нельзя рассматривать как умножение сдвигов или вращений, поскольку это сущности разного рода. Поэтому движения в общем случае образуют только лишь группу.
9. Однако, уже сами кратности, как самостоятельные сущности, можно и складывать, и умножать. Например, если мы рассмотрим сдвиг  $T_1$  и композицию его кратностей  $T_1^n \circ T_1^m$ , то получим тот же сдвиг но в суммарной кратности  $T_1^{n+m}$ , где  $n, m \in \mathbb{Z}$ . Но ничто не мешает нам рассмотреть кратность  $m$  сдвига  $T_1^n$ , т.е. сдвиг  $(T_1^n)^m$ , а это уже будет не что иное, как сдвиг кратности  $nm$ , т.е.  $T_1^{nm}$ .
10. Иначе говоря, умножение на целых числах можно представить как кратности кратностей сдвигов!
11. Целые числа, если их рассматривать как счетчик витков по окружности, образуют так называемую **фундаментальную группу** окружности, которая является важным топологическим свойством окружности и ей подобным (в топологии) фигурам. Зная фундаментальную группу, можно определить, насколько схожи фигуры в топологическом смысле — можно ли из одной получить другую путем деформации без разрывов и склеиваний.
12. Фиксируем понятие **кольцо**. Это — множество  $K$  с двумя бинарными операциями  $+$  (плюс) и  $\cdot$  (точка), которые подчинены следующим законам:
  - Ring1**  $a, b \in K \Rightarrow a + b \in K, a \cdot b \in K$  (замкнутость операций);
  - Ring2**  $a, b, c \in K \Rightarrow (a + b) + c = a + (b + c), (a \cdot b) \cdot c = a \cdot (b \cdot c)$  (ассоциативность операций);
  - Ring3** существует элемент  $0 \in K$  такой, что  $a + 0 = 0 + a = a$  для всех  $a \in K$  (аксиома нуля);
  - Ring4** для всякого элемента  $a \in K$  существует противоположный  $-a$  такой, что  $a + (-a) = 0$  (аксиома противоположного элемента);



**Ring5** для всех  $a, b, c \in K$  имеем  $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$ ,  $c \cdot (a+b) = (c \cdot a) + (c \cdot b)$  (правая и левая дистрибутивность);

**Ring6** для всех  $a, b \in K$  имеем  $a + b = b + a$  (коммутативность сложения).

Обычно изучаются **кольца с единицей**, т.е. такие кольца, для которых

**Ring7** существует элемент  $1 \in K$  такой, что  $a \cdot 1 = 1 \cdot a = a$  для всех  $a \in K$  (аксиома единицы),

а также **коммутативные кольца**, т.е. такие кольца, для которых

**Ring8** для всех  $a, b \in K$  имеем  $a \cdot b = b \cdot a$  (коммутативность умножения).

Иначе говоря, в коммутативном кольце с единицей можно складывать, вычитать и умножать по обычным правилам.

## Задачи

1. Докажите, что  $m\mathbb{Z}$  — подкольцо кольца  $\mathbb{Z}$ , т.е. в нем также можно складывать, вычитать и умножать.  $m$  — положительное целое число.

## 4.2 Кузнечик НОД и алгоритм Евклида

### Конспект

1. Поработаем теперь непосредственно с целыми числами. Пусть у нас есть кузнечик, стоящий в точке 0, который умеет прыгать с шагом  $a$  и с шагом  $b$  в любую сторону. Числа  $a, b$  — натуральные.
2. Ясно, что он может попасть в любую точку вида  $ka + mb$ , где кратности  $k, m$  — целые. Как понять, в какие точки он может попасть, а в какие — нет?
3. Пусть  $d$  — наименьшее положительное число, в которое кузнечик может попасть, т.е. оно имеет вид  $d = ka + mb$  при некоторых  $k, m$ . Тогда он может попасть и в любое число вида  $nd$ , поскольку  $nd = (nk)a + (nm)b$ , где  $n \in \mathbb{Z}$ . Следовательно, кузнечик может попасть во все целые числа, кратные  $d$  (множество  $d\mathbb{Z}$ ).
4. Но в любые другие целые числа он не сможет попасть. Действительно, если он попадает в какое-то число  $x$ , лежащее между двумя соседними кратностями  $d$ , т.е. в число  $x = nd + y$ , где  $0 < y < d$ , то тогда он может попасть в число  $y$ , т.е. остаток от деления  $x$  на  $d$ . Но  $y < d$  и притом положительное, а это противоречит выбору числа  $d$ . Таким образом, кузнечик попадает во все точки  $d\mathbb{Z}$ , и только в эти точки!
5. Что такое  $d$  на самом деле?

6. Для ответа на этот вопрос вспомним про алгоритм Евклида (с отсечениями квадратов). Пусть  $a < b$ . Вычтем из  $b$  столько  $a$ , сколько сможем:  $b = k_0a + r_1$ , где  $0 \leq r_1 < a$ . Далее, из  $a$  вычитаем столько  $r_1$ , сколько сможем, если  $r_1 > 0$ . Получим  $a = k_1r_1 + r_2$ , где  $0 \leq r_2 < r_1$ . Снова, если  $r_2 > 0$ , вычитаем из  $r_1$  столько  $r_2$ , сколько можем:  $r_1 = k_2r_2 + r_3$ , где  $0 \leq r_3 < r_2$ . И так далее.
7. Видим, что всякий раз, если  $r_i > 0$ , то мы приходим к  $r_{i+1} < r_i$ . Проблема в том, что это не может продолжаться бесконечно долго, т.к. от всякого натурального числа в сторону нуля можно спуститься за конечное число шагов (а ведь остатки у нас все положительные!). Так что рано или поздно случится  $r_{n+1} = 0$ , и на этом алгоритм Евклида остановится! Это значит, что прямоугольник  $a \times b$  можно сложить квадратами  $r_n \times r_n$ .
8. Если теперь раскрутить равенства  $r_{i-1} = k_i r_i + r_{i+1}$  в обратную сторону, то мы получим, во-первых, что  $a$  и  $b$  кратны  $r_n$ , и во-вторых, что  $r_n = Ka + Mb$  при некоторых целых  $K, M$ . То есть,  $r_n$  есть общий делитель исходных чисел  $a$  и  $b$ , и наш кузнечик способен попасть в точку  $r_n$  (а значит, и во все точки, ему кратные, т.е. в  $r_n \mathbb{Z}$ ).
9. С другой стороны, если какое-то  $q$  является общим делителем  $a$  и  $b$ , то  $q$  делит  $r_1 = b - k_0a$ , делит  $r_2 = a - k_1r_1$ , делит  $r_3 = r_1 - k_2r_2$ , и т.д., и, наконец, делит  $r_n$ . Стало быть,  $q \leq r_n$ , и  $r_n$  — наибольший общий делитель  $a$  и  $b$ .
10. Итак, кузнечик способен попасть в  $\text{НОД}(a, b)$ , следовательно,  $d \leq \text{НОД}(a, b)$ . С другой стороны, выбор  $d$  таков, что  $d = ka + mb$  при некоторых целых  $k, m$ , но тогда всякий делитель  $a$  и  $b$  является и делителем  $d$ , в частности  $\text{НОД}(a, b)$  делит  $d$ , откуда  $\text{НОД}(a, b) \leq d$ . Таким образом, минимальный шаг, на который способен сдвинуться кузнечик, — это наибольший общий делитель чисел  $a$  и  $b$ . Поэтому кузнечика с ногами  $a$  и  $b$  можно назвать  $\text{НОД}(a, b)$ . Он способен прыгнуть (в несколько прыжков) во ВСЕ точки, кратные  $\text{НОД}(a, b)$ , и ТОЛЬКО в эти точки!

## Задачи

1. С помощью алгоритма Евклида найти  $\text{НОД}(2020, 555)$ .

## 4.3 Простые числа и ОТА

### Конспект

1. У кузнечика  $\text{НОД}$  может получиться уникальная ситуация, когда при достаточно больших числах  $a$  и  $b$  он способен прыгнуть в любое целое число! Это верно в том и только том случае, когда  $\text{НОД}(a, b) = 1$ . При этом говорят, что  $a$  и  $b$  взаимно просты. Например, 125 и 63 взаимно просты.

2. Взаимная простота также обеспечивается, если одно из чисел само по себе **простое**, т.е. не делится ни на что, кроме 1 и самого себя. Например, 101 — простое, так что в паре с любым другим числом (кроме кратного 101) оно будет взаимно просто, и наш кузнечик сможет прыгнуть в любую целую точку! Например, он умеет прыгать на 101 и 62, значит, он умеет прыгать в любое целое число!
3. Любое число можно представить как произведение степеней простых. Действительно, 1 есть произведение нулевых степеней простых чисел, например,  $2^0$ . Предположим, что для всех чисел от 1 до  $n$  утверждение о разложимости справедливо (внимание! индукция!) и рассмотрим число  $n + 1$ . Оно либо уже простое, либо делится на число меньше  $n$ , отличное от 1. Тогда  $n + 1 = mk$ , причем  $m, k \leq n$ , а они есть произведение степеней простых по предположению индукции, но тогда и  $n + 1$  есть произведение степеней простых!
4. Простых чисел бесконечно много. Предположим, что это не так, и пронумеруем все простые числа:

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \dots, p_n$$

Далее рассмотрим число  $m = p_1 p_2 \dots p_n + 1$ . Оно не кратно никакому простому числу из ряда  $p_1, \dots, p_n$ , иначе бы 1 также было бы кратно этому простому. Следовательно, оно простое, но не входит в данный ряд. Противоречие.

5. Если простое число  $p$  делит произведение чисел  $ab$ , то оно по крайней мере делит одно из них. Доказательство: допустим, что  $p$  не делит  $a$ , тогда  $\text{НОД}(p, a) = 1$ , но тогда, как мы уже видели выше,  $1 = kp + ta$  при некоторых целых  $k, t$ . Умножим это равенство на  $b$ :  $b = kpb + tab$ . Справа оба слагаемых делятся на  $p$ , значит, и  $b$  делится на  $p$ .
6. Из этого свойства легко получить **основную теорему арифметики**: каждое натуральное число единственным образом представляется в виде произведения степеней простых чисел:

$$n = p_1^{k_1} p_2^{k_2} \dots$$

Набор степеней  $k_1, k_2, \dots$  уникален для каждого числа  $n$ . Действительно, если бы было два разложения, то после сокращения на одинаковые сомножители мы бы получили равенство

$$p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} = q_1^{s_1} q_2^{s_2} \dots q_t^{s_t}$$

Но каждое простое слева делит все число справа, значит, делит один из его множителей, а значит, совпадает с одним из  $q_i$ , что по предположению невозможно. Противоречие! Следовательно, разложение по степеням простых единственно.

7. Здесь еще нужно сделать оговорку про  $\mathbb{Z}$ . Любое целое число также единственным образом раскладывается по степеням простых, но с точностью до знака  $\pm$  перед этим разложением.

Основную теорему арифметики можно доказать разными способами. Покажем еще один способ, который использует множества и операции Минковского с этими множествами.

T1 Пусть  $P, Q \subseteq \mathbb{Z}$ . Суммой и разностью по Минковскому называются, соответственно, множества:

$$P \oplus Q = \{x + y \mid x \in P, y \in Q\}, \quad P \ominus Q = \{x - y \mid x \in P, y \in Q\}.$$

T2 Множества вида  $a\mathbb{Z}$  замкнуты относительно операций сложения и умножения (являются подкольцами кольца  $\mathbb{Z}$ ), поэтому для любых  $P, Q \subseteq a\mathbb{Z}$  и любых  $k, n \in \mathbb{Z}$  имеет место вложение:

$$kP \oplus nQ \subseteq a\mathbb{Z}.$$

T3  $a|b$  тогда и только тогда, когда  $b\mathbb{Z} \subseteq a\mathbb{Z}$ .

Действительно, если  $a|b$ , то  $b = ka$ . Если  $x \in b\mathbb{Z}$ , то  $x = by = ak y \in a\mathbb{Z}$ .

Пусть  $b\mathbb{Z} \subseteq a\mathbb{Z}$ , тогда  $b \in b\mathbb{Z}$  и, следовательно,  $b \in a\mathbb{Z}$ , т.е.  $b = ka$  при некотором целом  $k$ , тогда  $a|b$ .

T4 Решим неравенство  $P \ominus P \subseteq P$ , где  $P \subseteq \mathbb{Z}$ .

1) Пустое множество удовлетворяет этому неравенству.

2) Множество  $P = \{0\}$  также удовлетворяет данному неравенству.

3) Пусть  $c \in P$  и  $c \neq 0$ . В этом случае ясно, что в  $P$  есть положительные числа ( $0 = c - c$ , а значит, есть  $c$  и  $-c$ ). Пусть  $a = \min\{x \mid (x \in P) \wedge (x > 0)\}$ . Легко видеть, что  $a\mathbb{Z} \subseteq P \ominus P \subseteq P$ . Но если  $P \setminus a\mathbb{Z}$  не пусто, то существует  $x \in P \setminus a\mathbb{Z}$ , причем  $x = ka + d$ , где  $0 < d < a$ . Но  $d = x - ka \in P \ominus P$ , т.е.  $d \in P$ , что противоречит выбору  $a$ . Следовательно,  $P = a\mathbb{Z}$ .

Таким образом, если  $P \ominus P \subseteq P$ , то либо  $P = \emptyset$ , либо  $P = a\mathbb{Z}$  при некотором целом  $a$ .

T5  $a\mathbb{Z} \oplus b\mathbb{Z} = \text{НОД}(a, b)\mathbb{Z}$ .

Действительно,  $P = a\mathbb{Z} \oplus b\mathbb{Z}$  удовлетворяет неравенству  $P \ominus P \subseteq P$ , и значит, по свойству T4  $a\mathbb{Z} \oplus b\mathbb{Z}$  совпадает с множеством  $c\mathbb{Z}$  при некотором  $c$  (причем, если  $a, b > 0$ , то и  $c > 0$ ), т.е.

$$a\mathbb{Z} \oplus b\mathbb{Z} = c\mathbb{Z}.$$

Отсюда, с одной стороны, следует, что  $a\mathbb{Z}, b\mathbb{Z} \subseteq c\mathbb{Z}$ , откуда (свойство Т3)  $c|a$  и  $c|b$ . С другой стороны, если  $d|a$  и  $d|b$ , то  $a\mathbb{Z}, b\mathbb{Z} \subseteq d\mathbb{Z}$ , откуда (свойство Т2)  $c\mathbb{Z} \subseteq d\mathbb{Z}$ , откуда (свойство Т3)  $d|c$ . То есть, любой делитель  $a$  и  $b$  не превосходит  $c$ , а  $c$  также является делителем  $a$  и  $b$ . Следовательно,  $c = \text{НОД}(a, b)$ .

Т6 Если простое  $p$  делит произведение  $ab$ , то или  $p|a$ , или  $p|b$ .

Предположим, что  $p \nmid a$ , тогда  $\text{НОД}(p, a) = 1$  и (по свойству Т5)  $p\mathbb{Z} \oplus a\mathbb{Z} = \mathbb{Z}$ . Откуда  $1 = kp + ma$  при некоторых целых  $k, m$ . Тогда  $b = kbp + mab$ , откуда следует, что  $p|b$ .

Если предположить, что  $p \nmid b$ , то аналогично выводим соотношение  $p|a$ .

Т7 Отсюда, как уже отмечалось выше, легко выводится Основная теорема арифметики.

## Задачи

1. Докажите, что если  $P \ominus P \subseteq P$ , то выполняется равенство  $P \ominus P = P$ .
2. Докажите, что неравенство  $P \ominus P \subseteq P$  определяет все подгруппы  $\mathbb{Z}$  по сложению.
3. Натуральное число называется **совершенным**, если сумма всех его делителей, меньших его, равно ему самому. Например, 6 и 28 — совершенные числа. Докажите, что число  $2^{n-1}(2^n - 1)$  будет совершенным, если  $2^n - 1$  — простое число.

## 4.4 Некоторые следствия ОТА

# Симметрии фигур

## Аннотация.

В этой главе мы снова возвращаемся к геометрии и занимаемся полным описанием групп движений правильных многоугольников, а заодно и всех конечных подгрупп движений окружности. В конце главы рассматривается нестандартный пример группы движений ромба и вводится определение четверной группы Клейна.

## 5.1 Симметрии правильного треугольника

### Конспект

1. Возвращаемся на окружность и рассмотрим на ней вращение  $R_{2\pi/3}$ , т.е. на  $120^\circ$ .
2. Множество вращений  $R^3 = \{R_{2\pi/3}, R_{2\pi/3}^2, R_{2\pi/3}^3\}$  образует циклическую группу. Видим, что

$$R^3 = \{\text{id}, R_{2\pi/3}, R_{4\pi/3}\}.$$

3. Зафиксируем точку  $A$  на окружности и найдем ее образы при действии этой группы:  $B = R_{2\pi/3}(A)$ ,  $C = R_{4\pi/3}(A)$ . Набор точек  $\{A, B, C\}$  образует орбиту точки  $A$  при действии группы  $R^3$ .
4. Посмотрим теперь на треугольник  $ABC$ . Какие движения переводят его в себя? Очевидно, вращения из группы  $R^3$ , но также есть и симметрии  $S^3 = \{S_A, S_B, S_C\}$  относительно осей, проходящих через центр окружности и вершины треугольника.
5. Можем проверить, что объединение  $R^3 \cup S^3$ , состоящее из трех вращений и трех симметрий, образует группу относительно операции композиции движений.
6. Выпишем полную таблицу Кэли для этой группы:
7. На примере этой группы мы можем заметить, во-первых, что в группе можно выделить подгруппу вращений (верхний левый квадрат  $3 \times 3$ ), во-вторых, что группа движений треугольника конечна и некоммутативна, поскольку

id	$R_{2\pi/3}$	$R_{4\pi/3}$	$S_A$	$S_B$	$S_C$
$R_{2\pi/3}$	$R_{4\pi/3}$	id	$S_B$	$S_C$	$S_A$
$R_{4\pi/3}$	id	$R_{2\pi/3}$	$S_C$	$S_A$	$S_B$
$S_A$	$S_C$	$S_B$	id	$R_{4\pi/3}$	$R_{2\pi/3}$
$S_B$	$S_A$	$S_C$	$R_{2\pi/3}$	id	$R_{4\pi/3}$
$S_C$	$S_B$	$S_A$	$R_{4\pi/3}$	$R_{2\pi/3}$	id

ее таблица умножения несимметрична. Кроме того, в полном соответствии с таблицей умножения классов  $\mathbb{R}$  и  $\mathbb{S}$  видим, что композиция вращений есть вращение, композиция вращения и симметрии есть симметрия, композиций двух симметрий есть вращение.

8. В группе симметрий треугольника можно выделить базовые элементы: либо пара  $(R_{2\pi/3}, S_A)$ , либо пара  $(S_A, S_C)$ . Понятно, что здесь можно заменить поворот и симметрии на другие.
9. Вопрос: есть ли еще какие-то движения окружности, переводящие правильный треугольник в себя?
10. Заметим, что при движении, переводящем треугольник в себя, вершины обязательно переходят в вершины. Если бы это было не так, то какая-то вершина перешла бы в точку на стороне треугольника, но тогда преобразование не сохранило бы угол при этой вершине. Таким образом, преобразований треугольника не может быть больше, чем всех возможных перестановок трех вершин:

$$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}, \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}, \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix},$$

$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}, \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}, \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Нетрудно видеть, что эти перестановки в точности соответствуют преобразованиям  $\text{id}$ ,  $R_{2\pi/3}$ ,  $R_{4\pi/3}$ ,  $S_A$ ,  $S_B$ ,  $S_C$ . Так что данными преобразованиями исчерпываются все возможные движения, переводящие правильный треугольник в себя.

## Задачи

1. Выписать все перестановки на 4 символах  $A, B, C, D$ .

## 5.2 Симметрии правильного многоугольника

## Конспект

1. Рассмотрим еще один случай преобразований фигуры в себя. Пусть имеется правильный  $n$ -угольник. Тогда очевидными преобразованиями, сохраняющими форму и размеры фигуры, будут:

$$R_{2\pi k/n}, \quad S_k, \quad k = \overline{1, n}$$

2. В случае четного  $n$  в многоугольнике все вершины разбиваются на пары противоположных, лежащих на общей оси симметрии, поэтому имеется  $n/2$  осей симметрии, проходящих через вершины, и  $n/2$  осей, проходящих через середины сторон. В случае нечетного  $n$  на каждую вершину приходится своя ось симметрии.
3. Как и в случае треугольника, несложно показать, что этими  $2n$  преобразованиями исчерпываются все преобразования правильного многоугольника в себя, что, как видим, сильно меньше общего числа перестановок вершин, которое равно  $n!$  (совпадение получается только при  $n = 3$ ).
4. Однако и в этом случае в качестве базисных можно выбрать всего два преобразования:  $R_{2\pi/n}$  и  $S_1$ , либо две симметрии, оси которых являются соседними.

## Задачи

1. Составить полную таблицу Кэли для группы движений правильного 4-угольника.
2. Выразить поворот на 90 градусов с помощью двух симметрий.

## 5.3 Подгруппы движений окружности

### Конспект

1. Правильные  $n$ -угольники дают приблизительное представление о подгруппах движений окружности. Приблизительное — именно в том смысле, что движения  $n$ -угольников с любой наперед заданной точностью (при достаточно большом  $n$ ) будут представлять движения окружности.
2. Вопрос: все ли конечные подгруппы движений окружности задаются движениями правильных  $n$ -угольников?
3. Ответ: да, но с оговоркой. Некоторые конечные подгруппы совпадают с группами движений  $n$ -угольников, другие же являются их собственными подгруппами.



4. Действительно, пусть  $G$  — некоторая подгруппа движений окружности, причем конечная, т.е.

$$G = \{g_1, g_2, \dots, g_m\}.$$

5. Возьмем произвольный элемент  $g_k$  и рассмотрим множество всех его целых степеней:

$$\langle g_k \rangle = \{\dots, g_k^{-1}, g_k^0, g_k, g_k^2, \dots\}$$

6. Данное множество, очевидно, является подгруппой группы  $G$ , а значит, конечно. Но тогда среди степеней  $g_k$  точно есть два совпадающих значения:  $g_k^s = g_k^t$  при  $t \neq s$ . Пусть для определенности  $t > s$ . Тогда, умножая равенство на  $g_k^{-s}$ , получаем  $g_k^{t-s} = g_k^0 = \text{id}$ . Иначе говоря,  $g_k$  в некоторой положительной степени превращается в  $\text{id}$ .
7. **Порядком элемента**  $g \in G$  называется минимальное натуральное число  $s$  такое, что  $g^s = \text{id}$ . Как видим, для всякого  $g_k \in G$  такой порядок существует.
8. При этом, как мы установили ранее,  $g_k$  — это либо поворот окружности, либо отражение относительно оси, проходящей через ее центр. В первом случае порядок может быть любым начиная с 1. В случае, когда порядок элемента  $g_k$  равен 1, получаем, что  $g_k = \text{id}$ , т.е. поворот на нулевой угол (или угол  $2\pi$ ). Во втором случае, очевидно, что порядок  $g_k$  строго равен 2, т.к. отражение само себе обратно.
9. Если  $g_k$  — поворот, то это поворот на угол  $2\pi/s$ , где  $s$  — порядок  $g_k$ .
10. Порядок элемента является одновременно и порядком подгруппы  $\langle g_k \rangle$ . Действительно, если  $s$  — порядок элемента  $g_k$ , то все  $g_k$  в степенях меньше  $s$  различны (иначе порядок оказался бы меньше  $s$ ), а все большие степени сводятся к меньшим сокращением на  $g_k^s$ . Так что в подгруппе  $\langle g_k \rangle$  ровно  $s$  элементов!
11. Конечная группа  $\langle g_k \rangle$ , порожденная степенями одного своего элемента, называется **циклической**. Это название вполне соответствует тому, что все элементы группы в нашем случае есть повороты окружности на определенный угол, нацело делящий  $2\pi$ .
12. Итак, мы видим, что в  $G$  есть подгруппы вида  $\langle g_k \rangle$ , которые либо тривиальны (состоят из одного элемента  $\text{id}$ ), либо соответствуют группам вращения многоугольников (если  $g_k$  — поворот, причем здесь стоит оговориться, что при  $g_k = R_\pi$  многоугольника как такового нет, это вырожденный двуугольник), либо соответствуют группам отражений вида  $\{\text{id}, S_\varphi\}$  при некотором угле наклона  $\varphi$  оси отражения. Наша задача состоит в том, чтобы показать, что все эти подгруппы, а равно и сама группа  $G$ , есть подгруппы движений какого-то одного  $n$ -угольника.

13. Пусть  $G' = \{g \in G \mid g \text{ — поворот или id}\}$ . Ясно, что  $G'$  — подгруппа группы  $G$ . Предположим далее, что  $G' \neq G$ , т.е. в группе  $G$  существует хотя бы одно отражение  $h$ . В этом случае, как мы видели ранее, все элементы произведения Минковского  $hG'$  также являются отражениями. Предположим, что существует отражение  $h' \in G \setminus (hG' \cup G')$ . Но ранее мы установили, что  $hh'$  есть поворот, причем  $hh' = g \in G'$ , т.к.  $hh' \in G$ . Но тогда  $h' = h^{-1}g = hg \in hG'$  (отражение обладает свойством  $h = h^{-1}$ ), а это противоречит выбору  $h'$ .
14. Итак, если в группе  $G$  есть отражения, то все они находятся в одном классе  $hG'$ , причем этот класс не зависит от выбора отражения  $h$ . Иначе говоря, все отражения порождены каким-то одним отражением и всеми поворотами. При этом может оказаться, что в группе  $G$  есть только один поворот —  $\text{id}$ , а значит, там есть и только одно отражение.
15. Осталось разобраться с подгруппой  $G'$  всех поворотов.
16. Возьмем из  $G'$  самый маленький поворот  $g_0$ , т.е. такой, у которого порядок наибольший. Угол поворота  $g_0$  обозначим через  $x_0$ , а порядок  $g_0$  — через  $s_0$ . Так что  $x_0 s_0 = 2\pi$ .
17. Пусть  $g$  — произвольный поворот из  $G'$  и его угол поворота равен  $x > 0$  (если угол поворота отрицательный, то можно рассмотреть  $g^{-1}$ , который также принадлежит  $G'$ ). Если  $x$  не делится нацело на  $x_0$ , то имеет место представление

$$x = kx_0 + y,$$

где  $0 < y < x_0$ . Кроме того, углу  $y$  соответствует поворот  $g' = g(g_0)^{-k}$ , который, очевидно, принадлежит группе  $G'$ , а значит, имеет конечный порядок.

18. Каков порядок этого поворота? Ясно, что  $s_0 y < s_0 x_0 = 2\pi$ , следовательно, порядок поворота  $g'$  должен быть больше  $s_0$ . Но  $s_0$  — наибольший порядок среди всех поворотов группы  $G'$ . Противоречие! Значит,  $y = 0$ , т.е.  $x$  нацело делится на  $x_0$ :  $x = kx_0$  при некотором целом положительном  $k$ .
19. Таким образом, подгруппа  $G'$  группы  $G$  состоит из поворотов, являющихся степенями поворота  $g_0$  — самого маленького поворота! В частности, отсюда следует и то, что порядок самой группы  $G'$  равен порядку этого наименьшего поворота  $g_0$  (т.е. поворота с наибольшим порядком).
20. Итак, произвольная конечная группа движений окружности:
- а) либо тривиальна, т.е. совпадает с  $\{\text{id}\}$ ,
  - б) либо является циклической группой поворотов  $\langle g_0 \rangle$ , совпадающей с группой поворотов правильного  $n$ -угольника, где  $n$  — порядок этой группы (включая вырожденный случай 2-угольника),
  - с) либо является группой одного отражения  $\{\text{id}, S_\varphi\}$ ,

- д) либо есть объединение  $\langle g_0 \rangle \cup h\langle g_0 \rangle$ , где  $h$  — некоторое отражение того же самого правильного  $n$ -угольника.

21. Наконец, заметим, что и тривиальная группа, и циклическая конечная группа поворотов порядка  $n$ , и группа одного отражения  $\{\text{id}, S_\varphi\}$  (здесь важно отметить, что для согласования  $S_\varphi$  с многоугольником нужно, чтобы ось отражения проходила через вершину или середину стороны многоугольника), и наиболее полная группа  $\langle g_0 \rangle \cup h\langle g_0 \rangle$  — все они являются подгруппами группы движений правильного  $m$ -угольника, где  $m \vdots n$ . Отсюда следует, что все конечные группы движений окружности являются подгруппами движений правильных многоугольников, лежащих на данной окружности.

## Задачи

1. Доказать, что  $\langle g_0 \rangle \cap h\langle g_0 \rangle = \emptyset$ , т.е. группа движений распадается на два равномошных класса. один из которых получается применением отражения ко второму.
2. Пусть  $G$  — коммутативная группа,  $g \in G$  и  $H$  — подгруппа группы  $G$ . Доказать, что множество  $gH$  равномошно множеству  $H$ .
3. Вывести из предыдущего **теорему Лагранжа**: порядок подгруппы делит порядок группы.
4. Обобщить результат на некоммутативные группы.

## 5.4 Симметрии ромба, группа Клейна

### Конспект

1. Рассматриваем ромб, не являющийся квадратом.
2. Движения ромба состоят из:
  - а) двух симметрий: относительно его диагоналей, обозначим эти симметрии  $S_1$  и  $S_2$ ;
  - б) одного вращения: на угол  $\pi$ , обозначим это вращение  $R$ ;
  - с) тождественного преобразования  $\text{id}$ .
3. Других движений ромба не существует. Докажем это.

Пронумеруем вершины ромба цифрами 1,2,3,4 (1 и 3 противоположны). Предположим, что при некотором преобразовании 1 переходит в 1. В этом случае 3 не может перейти ни в 1, ни в 2 или 4, иначе произойдет потеря инцидентности — вершина 3 либо совпадет с 1, либо будет соседней. Стало быть,

3 также останется на месте. Но тогда остается ровно два преобразования:  $\text{id}$  и симметрия относительно оси 13 (обозначим ее  $S_1$ ).

Очевидно также, что 1 не может перейти в 2 или 4, т.к. в противном случае расстояние 1–3 перейдет в расстояние 2–4, а это невозможно для ромба с различными диагоналями. Остается вариант перехода 1 в 3, который дает два оставшихся преобразования: поворот на  $180^\circ$  и симметрию относительно диагонали 24 (обозначим ее  $S_2$ ).

Если провести аналогичный анализ для остальных вершин, то мы получим те же самые преобразования.

#### 4. Таблица Кэли группы движений ромба:

	id	$R$	$S_1$	$S_2$
id	id	$R$	$S_1$	$S_2$
$R$	$R$	id	$S_2$	$S_1$
$S_1$	$S_1$	$S_2$	id	$R$
$S_2$	$S_2$	$S_1$	$R$	id

- Отличие данной группы от группы движений правильного  $n$ -угольника состоит в том, что группа ромба является коммутативной (абелевой). Тем не менее, это не единственное отличие от групп движений правильного многоугольника.
- Ведь в группе движений правильного многоугольника есть абелева подгруппа вращений. Например, группа вращений квадрата тоже имеет порядок 4. Но и тут мы находим отличие от группы движений ромба. Дело в том, что вращения квадрата есть степени одного поворота на прямой угол. То есть группа вращений квадрата — циклическая. А если мы посмотрим на таблицу умножения группы движений ромба, то заметим, что степени вращения  $R$  не дают ни одну из симметрий, так же как и степени симметрий не дают вращения. Это значит, что группа движений ромба не является циклической.
- Тем не менее, такая группа не уникальна по своей природе. Ее ипостаси мы еще встретим при изучении вычетов и перестановок. С точностью до переобозначений элементов это будет все та же группа движений ромба. Вообще, если у двух групп получается одна и та же таблица умножения при некотором соответствии элементов одной группы элементам другой, то такие группы называются **изоморфными**. Общее название класса групп, изоморфных группе движений ромба, — «четверная группа Клейна», и общее обозначение —  $V_4$ .

# Исчисление остатков

## Аннотация.

Арифметика остатков дает богатый фактологический материал для изучения свойств простых чисел, а также позволяет по-новому взглянуть на операции Минковского с числовыми множествами и выйти на такие важные вехи теории множеств, как виды отношений и фактормножества.

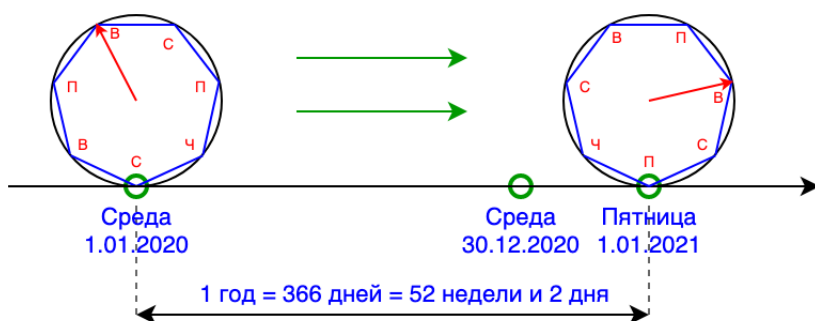
## 6.1 Арифметика остатков

### Конспект

1. Рассмотрим бытовую задачу. Вам нужно выключить печку через 40 минут, но у вас нет таймера, зато есть будильник, на котором можно выставить время звонка. Сейчас 12:30, на какое время требуется поставить будильник? Ответ: 13:10. Почему так? Дело в том, что в часе 60 минут, и если к 30 минутам прибавить 40, получается 70 минут, что больше часа. Поэтому добавляем 1 час и остаток — 10 минут.
2. Еще пример: сколько часов будет через 20 часов, если сейчас 8 утра? Можно решать аналогично:  $8 + 20 = 28$ , затем убираем полные сутки, т.е. 24 часа, остается 4 часа утра.
3. Можно решать иначе. 20 часов — это  $-4$  часа от суток. Следовательно, нужно протот вычесть из 8 утра 4 часа и получим те же 4 часа утра.
4. Во всех случаях мы решаем задачу нахождения остатка от деления на некоторое число. В случае минут это 60, в случае часов это 24.
5. Когда вас просят отметить в анкете количество полных лет, то вам по сути нужно найти неполное частное от деления вашего возраста на 1 год. Конечно, в данном случае нам это просто сделать, т.к. каждый год мы запоминаем именно количество прожитых лет, а не дней или недель.
6. Но, например, во многих сферах деятельности планирование календаря происходит неделями (и даже у себя в компьютере в настройках календаря вы можете вывести номер текущей недели в году). А сколько недель в году?

Для этого нужно найти неполное частное от деления 365 (или 366) на 7, оно составляет 52.

7. Остаток от деления на неделю есть число от 0 до 6, которое определяет сдвиг вперед относительно текущего дня недели. Например, если сегодня четверг, то какой день недели будет через 30 дней? Мы выбрасываем из 30 4 полных недели, что составляет 28 дней, и находим остаток, который равен 2. Это значит, что через 30 дней будет четверг плюс 2 дня, т.е. суббота.
8. Точно так же можно легко заметить, что каждый год происходит смещение дат на 1 или два дня вперед относительно дней недели. Так, если в этом году 1 января было средой, то в следующем оно будет или четвергом (если мы не переходим через 29 февраля), или пятницей (если текущий год — високосный, т.е. содержит 366 дней), как на картинке ниже.



9. Каждые 28 лет (а 28 — это наименьшее общее кратное 7 и 4) соответствие дат и дней недели повторяется.
10. При расчетах на более длительные периоды, а именно, при переходе через 1900 год или 2100 год, нужно учитывать также, что 3 раза за 400 лет не происходит добавление лишнего дня (29 февраля) для более точного соответствия календаря астрономическому году, т.е. 1900, 1800, 1700 годы не являются високосными, как и 2100, 2200 и 2300.
11. Тем не менее, часто в жизни встречается задача вычисления дня недели, и здесь нам на помощь приходит исчисление остатков по модулю 7. Например, сегодня 21 марта 2020 суббота, а нам нужно знать, какой день недели будет 31 августа 2020. Сначала мы находим день недели 21 августа, т.к. до этой даты целое число месяцев. При этом мы 3 раза переходим через 31 число (март, май, июль) и 2 раза — не переходим (апрель, июнь). Следовательно, 3 раза прибавляется остаток 3, и 2 раза — остаток 2, итого сумма остатков составляет 13. Но это больше 7, причем очень близко к 14, поэтому сумму остатков мы запишем как -1. Наконец, остается добавить 10 дней (от 21 августа до 31 августа). Итого получается 9, а по модулю 7 — всего 2. Таким образом, 31 августа 2020 года есть понедельник!

12. Из приведенной выше картинке с семиугольником на окружности, совмещенной с прямой линией, мы можем ясно представить себе, как работает исчисление остатков по модулю 7, т.е. исчисление дней недели. Мы катим окружность по прямой времени, пока не достигнем нужной нам даты. При этом неважно, сколько целых оборотов совершит семиугольник, т.е. сколько недель мы проедем, а вот последний полувиток как раз и дает нам ответ на вопрос о дне недели. Так что, если мы пронумеруем дни недели цифрами от 0 до 6, то любое расстояние между датами можно представить как какое-то целое количество недель плюс остаток, лежащие в диапазоне от 0 до 6 (включительно).
13. Эта картинка легко обобщается на случай произвольного основания. Представим, что в неделе у нас не 7 дней, а, например, 28 (лунный месяц), и тогда любое расстояние между датами выражается как целое число 28-дневных циклов плюс некоторый остаток от 0 до 27. И так далее.
14. Таким образом, мы приходим к тому, что всякое натуральное число (количество) можно представить в виде  $a = km + b$ , где  $k$  — неполное частное от деления  $a$  на  $m$ ,  $b$  — остаток от деления, который находится в промежутке от 0 (включая) до  $m$  (не включая).
15. Равенство  $a = km + b$  при исчислении остатков принято записывать так:

$$a \equiv b \pmod{m},$$

Читается:  $a$  сравнимо с  $b$  по модулю  $m$ .

Причем, если модуль  $m$  известен из контекста и не меняется при вычислениях, то его можно опускать, записывая просто  $a \equiv b$ . Читается:  $a$  **сравнимо с  $b$**  (по модулю  $m$ ).

16. На картинке, приведенной выше, даты 1 января 2020 и 30 декабря 2020 сравнимы по модулю 7, т.е. по дням недели. А про интервал в 366 дней мы запишем  $366 \equiv 2 \pmod{7}$ . Такая запись никак не информирует нас о коэффициенте  $k$  (количестве целых недель), но показывает самое главное — сколько дней надо прибавить к среде.
17. Остатками можно оперировать так же, как обычными числами, сбрасывая всякий раз накопленные при сложении целые «обороты» модулей. Иначе говоря, если мы хотим, например, к текущей среде прибавить 6 дней, то мы совмещаем наш семиугольник вершиной «среда» с прямой времени, а затем прокатываем его вперед на 6 делений (что чуть меньше полного оборота), и в точке касания с прямой получаем вторник. Заметим, что ровно тот же результат мы получим, если прокатим семиугольник назад на 1 деление. Это значит, что числа 6 и -1 сравнимы по модулю 7. И на практике можно также пользоваться отрицательными числами для исчисления остатков.

18. Ранее мы много времени уделяли таблицам композиций движений многоугольников. И, как мы помним, композиция вращений многоугольника соответствовала сложению углов этих вращений. При этом мы также отбрасывали 360 градусов (или  $2\pi$ ), если сумма углов переваливала за полный оборот. При описании конечных подгрупп движений правильных многоугольников мы выяснили, что каждый поворот является степенью некоторого минимального поворота на угол  $2\pi/n$  (для  $n$ -угольника), т.е. все повороты выражаются углами  $k(2\pi/n)$ , где  $k = 0, \dots, n - 1$  (ничего не напоминает?).
19. Забудем теперь про вращения и углы, а просто понаблюдаем за степенями этих поворотов при композициях, т.е. при сложении углов. Для примера рассмотрим случаи  $n = 7$  и  $n = 8$ , и выпишем таблицу композиций, которая представляет собой таблицу сложения остатков по модулям 7 и 8, соответственно.
20. Таблицы сложения остатков по модулям 7 и 8:

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

- Таблица сложения получается последовательными циклическими сдвигами верхней строки влево.
21. Помимо сложени остатков мы можем их умножать (в терминологии вращений многоугольника умножение соответствует многократной композиции одинаковых поворотов, так что первое число произведения отвечает за величину поворота, а второе — за его кратность, либо наоборот). Таблица умножения остатков по модулям 7 и 8 (отметим важную особенность этих таблиц: они имеют центральную симметрию, если вычеркнуть нулевые строку и столбец):



	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

22. Отметим еще одно свойство таблицы умножения: строка или столбец, номер которого НЕ взаимно прост с модулем, содержит нули. Это легко доказать. Пусть номер строки равен  $k$ , и  $s = \text{НОД}(k, m) > 1$ . При этом ясно, что  $s < m$ , т.к.  $s$  является делителем  $m$ . Пусть также  $t = m/s$ . Рассмотрим тогда строку  $k$  и столбец  $t$ . Произведение их номеров равно  $kt = km/s$ . Поскольку  $k/s$  также целое, получаем, что  $kt$  кратно  $m$ , а значит,  $kt \equiv 0 \pmod{m}$ . Отметим, что  $s = 1$  здесь не проходит ровно потому, что в этом случае  $t$  не будет номером столбца таблицы умножения.
23. На самом деле, верно и обратное: если строка таблицы умножения содержит нули, то номер строки не взаимно прост с модулем. Для этого мы докажем эквивалентное утверждение

**Теорема 6.1.** Пусть  $k > 0$  и  $k \perp m$ , тогда все остатки

$$k, \quad 2k, \quad 3k, \quad \dots, \quad (m-1)k \pmod{m}$$

попарно различны и отличны от нуля.

*Доказательство.* Предположим, что один из остатков равен нулю:  $kl \equiv 0 \pmod{m}$ , где  $l \in \{1, 2, \dots, m-1\}$ . Тогда  $kl = mt$  при некотором  $t$ . Но поскольку  $k \perp m$ , в силу ОТА число  $k$  делит  $t$ , а значит,  $k \leq t$ . Однако  $l < m$ , следовательно,  $kl < mt$ . Противоречие.

Далее, если среди остатков есть равные, например,  $kl \equiv kt$ , то здесь же найдется и остаток  $k(l-t)$  (или  $k(t-l)$ , если  $t > l$ ), который равен 0. А это невозможно по доказанному.

Таким образом, эти остатки все различны и положительны, а значит, являются перестановкой множества  $\{1, 2, \dots, m-1\}$ . □

24. Множество  $\{0, 1, 2, \dots, m-1\}$  с операциями сложения и умножения по модулю  $m$  называется **кольцом вычетов** по модулю  $m$  и обозначается  $\mathbb{Z}_m$ .

25. Множество  $\mathbb{Z}_m^*$ , состоящее только из взаимно простых с модулем  $m$  элементов  $\mathbb{Z}_m$ , образует группу по умножению остатков. Это легко увидеть из таблиц умножения, если исключить в них строки и столбцы, содержащие нули. Например, таблицами умножения для групп  $\mathbb{Z}_5^*$  и  $\mathbb{Z}_8^*$  будут

$\mathbb{Z}_5^*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_8^*$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

26. И тут мы снова видим знакомую ситуацию: если группа  $\mathbb{Z}_5^*$  циклическая (все ее элементы могут быть получены как степени двойки), и ее можно изоморфно сопоставить с группой  $\mathbb{Z}_4$  с операцией сложения, а также с группой вращений квадрата, то группа  $\mathbb{Z}_8^*$  уже не является циклической, хотя остается абелевой. И это — еще одно проявление группы Клейна. Чуть позже мы дадим сравнение нескольких ипостасей групп 4-го порядка.

### Задачи

- Если сегодня понедельник, от какой день недели будет через 10 дней, через 90 дней, через 2 года (невисокосных)?
- Найти день недели через месяц, квартал, полгода и год, отправляясь от текущей даты.
- Построить таблицы сложения и умножения для остатков: 2,3,4,5,6.
- Сравнить таблицу сложения остатков по модулю 2 с таблицами умножения классов сдвигов  $\mathbb{T}$  и симметрий  $\mathbb{S}$  для прямой и окружности.
- Сравнить таблицу симметрий ромба с таблицей умножения группы  $\mathbb{Z}_8^*$ .
- В группе  $\mathbb{Z}_8^*$  найти обратные элементы:  $3^{-1}, 5^{-1}, 7^{-1}$ .
- Проверить, что  $\mathbb{Z}_m$  удовлетворяет аксиомам кольца.

## 6.2 Свойства арифметики остатков

### Конспект

- Свойства сравнений таковы:

- M1.  $a \equiv b \pmod{m}$  тогда и только тогда, когда  $a - b$  кратно  $m$ ;
- M2. если  $a \equiv b, c \equiv d$ , то  $a + c \equiv b + d, a - c \equiv b - d$  и  $ac \equiv bd$ ;

М3. для  $n \geq 0$  если  $a \equiv b$ , то  $a^n \equiv b^n$ ;

М4. признаки делимости на 3 и на 9:  $a_0 + a_1 10 + a_2 10^2 + \dots + a_n 10^n \equiv a_0 + \dots + a_n$   
по модулю 3 и по модулю 9;

М5. если  $m > 0$  и  $d \perp m$ , то

$$ad \equiv bd \pmod{m} \iff a \equiv b \pmod{m}$$

М6. если  $m, d > 0$ , то

$$ad \equiv bd \pmod{md} \iff a \equiv b \pmod{m}$$

М7. если  $m > 0$ , то для любого  $d$

$$ad \equiv bd \pmod{m} \iff a \equiv b \pmod{m/\text{НОД}(m, d)}$$

М8. если  $m, d > 0$ ,  $a \equiv b \pmod{md}$ , то  $a \equiv b \pmod{m}$

М9. если  $m, n > 0$ , то

$$a \equiv b \pmod{m}, \quad a \equiv b \pmod{n} \iff a \equiv b \pmod{\text{НОК}(m, n)}$$

М10. если  $m, n > 0$  и  $m \perp n$ , то

$$a \equiv b \pmod{m}, \quad a \equiv b \pmod{n} \iff a \equiv b \pmod{mn}$$

М11. пусть  $n_p$  — степень простого числа  $p$  в разложении  $n$  по степеням простых (ОТА), тогда

$$a \equiv b \pmod{n} \iff \forall p \quad a \equiv b \pmod{p^{n_p}} \quad (p \text{ — простое})$$

2. **Китайская теорема об остатках.** Пусть числа  $m_1, \dots, m_k > 0$  попарно взаимно просты,  $m = m_1 \dots m_k$ . Тогда

$$a \equiv b \pmod{m} \iff a \equiv b \pmod{m_j}, \quad j = 1, \dots, k$$

3. **Малая теорема Ферма:**  $n^{p-1} \equiv 1 \pmod{p}$ , где  $p$  — простое и  $p \nmid n$ .

4. Малая теорема Ферма обеспечивает существование обратных элементов в группе по умножению остатков  $\mathbb{Z}_p^*$ . Достаточно  $n$  умножить на  $n^{p-2}$ , и мы получим 1.

5. Отсюда следует, что  $\mathbb{Z}_p$  при простом  $p$  является **полем**.

6. Поле — это кольцо, в котором все ненулевые элементы обратимы. Кольцо целых чисел не является полем. Рассмотренные нами ранее группы движений также нельзя назвать полем, т.к. в них всего одна операция. Первое поле, которое мы встречаем в курсе — это  $\mathbb{Z}_p$ , поле вычетов по простому модулю.

## Задачи

1. Доказать, что  $2^n - 1$  кратно трем тогда и только тогда, когда  $n$  — четное, и  $2^n + 1$  кратно трем тогда и только тогда, когда  $n$  — нечетное.
2. Что означает запись  $a \equiv b \pmod{0}$ ?
3. В силу ОТА будем записывать положительное натуральное число  $m$  как последовательность  $\overline{m}$  степеней простых:

$$m = p_0^{\alpha_0} p_1^{\alpha_1} \dots p_k^{\alpha_k} \dots \iff \overline{m} = (\alpha_0, \alpha_1, \dots, \alpha_k, \dots),$$

где  $p_0 < p_1 < p_2 < \dots$  — все простые числа, начиная с 2.

Докажите, что если  $\overline{m} = (\alpha_0, \alpha_1, \dots, \alpha_k, \dots)$  и  $\overline{n} = (\beta_0, \beta_1, \dots, \beta_k, \dots)$ , то

$$\begin{aligned}\overline{nm} &= (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \dots, \alpha_k + \beta_k, \dots) \\ \overline{\text{НОД}(n, m)} &= (\min(\alpha_0, \beta_0), \min(\alpha_1, \beta_1), \dots, \min(\alpha_k, \beta_k), \dots), \\ \overline{\text{НОК}(n, m)} &= (\max(\alpha_0, \beta_0), \max(\alpha_1, \beta_1), \dots, \max(\alpha_k, \beta_k), \dots).\end{aligned}$$

4. Докажите, что  $\text{НОД}(n, m)\text{НОК}(n, m) = nm$ .
5. Докажите, что

$$\text{НОД}(kn, km) = k\text{НОД}(n, m), \quad \text{НОК}(kn, km) = k\text{НОК}(n, m).$$

## 6.3 \*Вычеты и операции Минковского

### Аннотация.

---

Данный раздел нужно изучать вместе с главой 0. При первом чтении можно пропустить.

---

### Конспект

1. Вернемся к арифметическим операциям над множествами. Пусть задано целое число  $m > 1$ , тогда

$$m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}.$$

2. Как мы помним, это — кольцо, т.е. в  $m\mathbb{Z}$  можно складывать, вычитать и умножать, но нельзя делить любое число на любое ненулевое. Что будет если сдвинуть его на некоторое целое число? Т.е. взять множество

$$m\mathbb{Z} + n = \{mk + n \mid k \in \mathbb{Z}\}$$

3. При каких  $n$  множество  $m\mathbb{Z} + n$  останется кольцом? В кольце должен быть ноль, следовательно, если  $m\mathbb{Z} + n$  — кольцо, то при некотором  $k$  имеем  $mk + n = 0$ , откуда следует, что  $n$  кратно  $m$ . Обратно, если  $n$  кратно  $m$ , то  $m\mathbb{Z} + n = m\mathbb{Z}$ . Действительно,  $n = km$ , и тогда  $ml + n = m(l + k) \in m\mathbb{Z}$ , т.е.  $m\mathbb{Z} + n \subseteq m\mathbb{Z}$ . Кроме того,  $ml = m(l - k) + mk = m(l - k) + n$ , откуда  $m\mathbb{Z} \subseteq m\mathbb{Z} + n$ . Таким образом,  $m\mathbb{Z} + n = m\mathbb{Z}$ .
4. Итак,  $m\mathbb{Z} + n$  остается кольцом тогда и только тогда, когда  $n$  кратно  $m$ , причем это все то же кольцо  $m\mathbb{Z}$ .
5. Пусть теперь  $n = mk + d$ , где  $d$  — остаток от деления  $n$  на  $m$ .
6. В этом случае  $m\mathbb{Z} + n = m\mathbb{Z} + mk + d = m\mathbb{Z} + d$ . Отсюда легко получить следующее свойство

$$m\mathbb{Z} + n = m\mathbb{Z} + n' \iff n \equiv n' \pmod{m},$$

т.е. сложение с  $m\mathbb{Z}$  в каком-то смысле напоминает операцию сложения по модулю  $m$  — оно «забывает» все, что кратно  $m$ , оставляя только остаток.

7. Это значит, что существует ровно  $m$  различных множеств вида  $m\mathbb{Z} + n$ , а именно:

$$m\mathbb{Z}, \quad m\mathbb{Z} + 1, \quad \dots, \quad m\mathbb{Z} + m - 1.$$

8. Далее, эти множества попарно не пересекаются и в сумме дают все  $\mathbb{Z}$ . Это утверждение предлагается доказать самостоятельно.
9. **Важный логический шаг!** Рассмотрим теперь множества  $m\mathbb{Z} + n$  как новые элементы (т.е. мы забываем их природу и считаем их отдельными точками, такими же, как до этого считали целые числа) и соберем из них новое множество

$$\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, \quad m\mathbb{Z} + 1, \quad \dots, \quad m\mathbb{Z} + m - 1\},$$

которое в алгебре называется **фактормножеством**.

10. Наконец, вспомним о том, что мы можем умножать и складывать множества, т.е. определены операции Минковского

$$(m\mathbb{Z} + n) + (m\mathbb{Z} + n'), \quad (m\mathbb{Z} + n)(m\mathbb{Z} + n').$$

11. Нетрудно показать следующие свойства этих операций:

$$Z1 \quad (m\mathbb{Z} + n) + (m\mathbb{Z} + n') = m\mathbb{Z} + (n + n' \pmod{m})$$

$$Z2 \quad (m\mathbb{Z} + n)(m\mathbb{Z} + n') = m\mathbb{Z} + (nn' \pmod{m})$$

Действительно,  $mk + n + mk' + n' \equiv n + n' \pmod{m}$  и  $(mk + n)(mk' + n') \equiv nn' \pmod{m}$ .

12. Это значит, что операции Минковского над элементами  $\mathbb{Z}/m\mathbb{Z}$  в точности дают алгебру остатков, которую мы рассматривали выше.
13. То есть  $\mathbb{Z}/m\mathbb{Z}$  — кольцо, построенное на фактормножестве, причем его операциями являются операции Минковского, определенные через операции исходного кольца. Такое кольцо называется **факторкольцом** кольца  $\mathbb{Z}$ .
14. **Зафиксируем:** в исходном кольце (например,  $\mathbb{Z}$ ) рассматривается подкольцо (например,  $m\mathbb{Z}$ ) и все его сдвиги, полученные смещением на элементы этого же кольца, получается набор множеств, попарно не пересекающихся и дающих в сумме исходное кольцо, далее на этих множествах вводятся операции сложения и умножения, полученные как операции Минковского. Итоговая структура называется факторкольцом.
15. Аналогично можно построить такое понятие как факторгруппа, воспользовавшись лишь одной операцией — сложением.
16. Факторкольца и факторгруппы являются мощным инструментом абстракции и получения общих результатов в алгебре и теории множеств.

## Задачи

1. Доказать, что  $m\mathbb{Z} + n \cap m\mathbb{Z} + n' = \emptyset$ , если  $0 \leq n < n' \leq m - 1$ .
2. Доказать, что

$$m\mathbb{Z} \cup (m\mathbb{Z} + 1) \cup \dots \cup (m\mathbb{Z} + m - 1) = \mathbb{Z}.$$

3. Построить факторкольцо  $(\mathbb{Z}/6\mathbb{Z})/2(\mathbb{Z}/6\mathbb{Z})$ . Алгебру остатков по какому модулю мы получим?
4. Построить факторкольцо  $(\mathbb{Z}/6\mathbb{Z})/5(\mathbb{Z}/6\mathbb{Z})$ . Почему получается одноэлементное фактормножество, т.е. тривиальное кольцо, состоящее из одного нуля.

## 6.4 \*Теория множеств: отношения

### Аннотация.

---

Данный раздел нужно изучать вместе с главой 0. При первом чтении можно пропустить.

---

## Конспект

1. Пусть заданы два множества  $A$  и  $B$ . Под их **прямым произведением** мы понимаем множество всех пар точек  $(a, b)$ , где  $a \in A$ ,  $b \in B$ . Пары при этом обладают свойством позиционного равенства, т.е.

$$(a, b) = (c, d) \iff (a = c) \wedge (b = d)$$

2. Обозначение для прямого произведения:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

3. В качестве примера можно рассмотреть множество пар целых чисел на плоскости или, например, таблицу умножения остатков, где помимо пары чисел еще задано значение их произведения по модулю.
4. **Отношением между множествами**  $A$  и  $B$  называется всякое подмножество  $R \subseteq A \times B$ . Обычно вместо  $(a, b) \in R$  принято записывать  $aRb$ . В случае, когда  $A = B$ , говорят, что  $R$  есть отношение **на множестве**  $A$
5. Примеры отношений:

R1 Отношение отец–сын ( $a$  есть отец  $b$ ). Оно *несимметричное*!

R2 Отношение предок–потомок. Оно также несимметричное, но *транзитивное*! Если  $a$  есть предок  $b$  и  $b$  есть предок  $c$ , то  $a$  есть предок  $c$ .

R3 Отношение братства:  $a$  есть брат  $b$ . Оно и симметричное, и транзитивное (имеются ввиду родные братья, т.е. у них общий отец).

R4 Отношение  $a < b$  на целых числах: транзитивное и *антисимметричное*: невозможно одновременно  $a < b$  и  $b < a$

R5 Отношение сравнения по модулю:  $a \equiv b \pmod{m}$ . Это отношение симметрично, транзитивно и *рефлексивно*, т.е. всякое число само с собой сравнимо.

6. Если отношение симметрично, рефлексивно и транзитивно, то оно называется **отношением эквивалентности**.
7. Отношение сравнения по модулю — отношение эквивалентности.
8. Обычное равенство — отношение эквивалентности.
9. Если каждого человека считать братом самому себе, то отношение братства становится отношением эквивалентности.
10. Отношение эквивалентности разбивает множество, на котором оно задано, на непересекающиеся классы эквивалентности:

$$A = A_1 \sqcup A_2 \sqcup \dots$$

При этом внутри каждого класса сидят эквивалентные друг другу элементы. Например, всех мужчин можно разделить на классы эквивалентности, в каждом из которых находятся родные братья.

11. А еще можно рассмотреть классы эквивалентности по отношению сравнимости целых чисел по заданному модулю. И этими классами будут:

$$m\mathbb{Z}, \quad m\mathbb{Z} + 1, \quad m\mathbb{Z} + 2, \quad \dots, \quad m\mathbb{Z} + m - 1$$

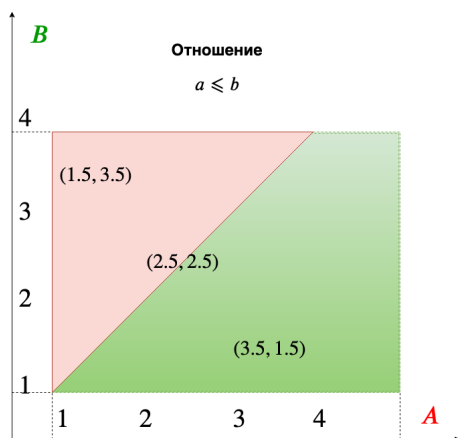
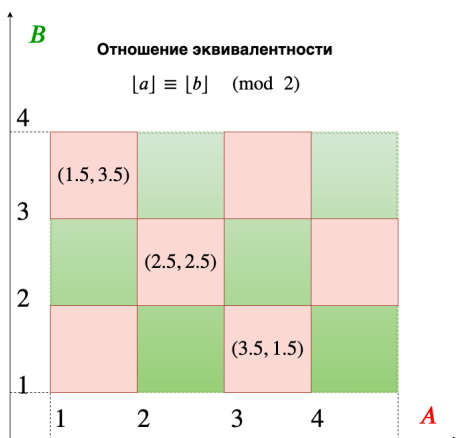
Именно эти классы у нас формировали фактормножество  $\mathbb{Z}/m\mathbb{Z}$ !

12. Вообще, если  $R$  есть отношение эквивалентности на множестве  $A$ , то множество классов эквивалентности обозначается  $A/R$  и называется фактормножеством множества  $A$  по отношению эквивалентности  $R$ .

## Задачи

1. Чему равно  $\emptyset \times \emptyset$ ,  $A \times \emptyset$ ,  $\emptyset \times B$ ?
2. Найти  $\{1, 2, 3\} \times \{\emptyset\}$ .
3. В чем отличие  $\{a, b\} \times \{1, 2\}$  от  $\{1, 2\} \times \{a, b\}$ ?
4. Постройте фактормножество множества  $\mathbb{Z}_9$  по отношению сравнимости по модулю 3.
5. Рассмотрим группу движений правильного  $n$ -угольника. Пусть два движения эквивалентны, если их композиция является поворотом (или  $\text{id}$ ). Докажите, что это и в самом деле отношение эквивалентности, постройте классы эквивалентности, постройте факторгруппу на этих классах. Какова ее таблица умножения?
6. \*\*Изучить картинки с примерами отношений, почему они так выглядят? Функция  $\lfloor x \rfloor$  обозначает целую часть числа. Здесь мы неявно предполагаем знакомство продвинутого читателя с нецелыми числами.





# Движения плоскости и пространства

## Аннотация.

Данная глава продолжает тему групп движений. Здесь мы получаем теорему Шаля (для движений плоскости), а затем широкими мазками освещаем тему движений сферы и пространства.

Разделы о сфере и пространстве могут быть пропущены при первом ознакомлении с конспектом.

## 7.1 Виды движений плоскости. Теорема Шаля

### Конспект

1. Разбираем движения, попутно доказывая лемму «о гвоздях».
2. Пусть на плоскости три точки, не лежащие на одной прямой, остаются неподвижными при движении. Вывод: это  $\text{id}$ .
3. Пусть на плоскости неподвижны 2 точки и вся прямая, проходящая через них, остальные точки подвижны. Тогда это симметрия относительно данной прямой.
4. Пусть неподвижна лишь одна точка. Такое возможно лишь при вращении вокруг этой точки на угол, не кратный полному обороту.
5. Пусть вообще нет неподвижных точек. Берем любую точку, смотрим, куда она переходит, применяем сдвиг (параллельный перенос). Оставшееся преобразование имеет как минимум 1 неподвижную точку, а значит, является либо  $\text{id}$ , либо симметрией, либо поворотом. Интересно, что поворот в данном случае можно исключить, т.к. композиция сдвига и поворота есть просто поворот, а значит, в исходном преобразовании была как минимум одна неподвижная точка. Следовательно, исходное движение есть либо сдвиг, либо смещенная симметрия (композиция сдвига и симметрии).
6. Таким образом, движение плоскости можно рассматривать как комбинацию

параллельного переноса (в частности, на нулевой вектор), поворота (в частности, на нулевой угол) и симметрии относительно произвольной прямой.

7. **Теорема Шаля.** Произвольное движение (без разложения его на компоненты) есть движение одного из следующих классов:

- класс параллельных переносов (на произвольный вектор), который мы обозначим  $\Rightarrow$ ;
- класс поворотов относительно произвольного центра, который мы обозначим  $\bigcirc$ ;
- класс **скользящих симметрий** (сдвиг на произвольный вектор с последующей симметрией относительно оси данного вектора), который мы обозначим  $\Leftarrow\Leftarrow$ .

8. Таблица композиций для таких классов выглядит следующим образом:

	$\Rightarrow$	$\bigcirc$	$\Leftarrow\Leftarrow$
$\Rightarrow$	$\Rightarrow$	$\bigcirc$	$\Leftarrow\Leftarrow$
$\bigcirc$	$\bigcirc$	$\Rightarrow$ или $\bigcirc$	$\Leftarrow\Leftarrow$
$\Leftarrow\Leftarrow$	$\Leftarrow\Leftarrow$	$\Leftarrow\Leftarrow$	$\Rightarrow$ или $\bigcirc$

- Аналогично одномерным случаям (прямая и окружность) можно выбирать различные базовые преобразования для построения с их помощью всех движений.
- Всякое движение есть композиция не более трех симметрий (относительно разных и, вообще говоря, не обязательно параллельных осей).
- Сдвиг можно представить как композицию двух симметрий (относительно параллельных осей).
- Поворот можно представить как композицию двух симметрий (относительно пересекающихся осей).
- Скользкую симметрию можно представить как композицию трех симметрий (две на сдвиг и одна собственно симметрия).

## Задачи

- Показать, что композиция поворотов (относительно разных центров) есть либо сдвиг, либо поворот (вычислить его центр).
- Показать, что композиция сдвига и поворота есть поворот.

## 7.2 Сравнение движений прямой, окружности и плоскости

### Конспект

1. Отметим несколько общих свойств рассмотренных нами движений прямой, окружности и плоскости.
2. Во-первых, их всех можно свести к композиции симметрий. Для одномерных объектов (прямая и окружность) — не более двух, для двумерных — не более трех.
3. Во-вторых, все движения можно разделить на два класса: сохраняющие и меняющие **ориентацию**. Те движения, которые сводятся к композиции четного числа симметрий, сохраняют ориентацию фигур, а те, которые сводятся к композиции нечетного числа симметрий, — меняют ориентацию фигур. Изменение ориентации означает, что право и лево меняются местами, т.е. мы как бы переходим в зазеркалье.
4. При этом нужно отметить, что преобразования, меняющие ориентацию, обязательно требуют выхода в пространство, если мы хотим осуществить их непрерывным движением.
5. В-третьих, есть и более глубинная связь движений прямой, окружности и плоскости. Мы уже отмечали, что окружность можно рассматривать как прямую, у которой склеили противоположные концы (где-то на бесконечности). И с этой точки зрения сдвиг на прямой является прямой аналогией вращения окружности. Особенно, если величина сдвига сильно меньше радиуса.
6. А симметрия прямой при этом естественным образом превращается в симметрию окружности. Только ось симметрии должна проходить через место склейки двух бесконечностей. Остальные же симметрии можно получить дополнительным сдвигом, т.е. вращением.
7. Далее, окружность находится на плоскости. И поэтому вращение окружности полностью аналогично вращению плоскости, если при этом совместить их центры.
8. Еще проще увидеть совпадения понятий сдвига на прямой и плоскости. В обоих случаях мы просто смещаем все точки на какой-то вектор.
9. Тем не менее, на плоскости появляется новый вид движения, который комбинирует в себе сдвиг и отражение относительно оси сдвига. Это — скользящая симметрия, т.е. симметрия с последующим применением сдвига вдоль оси симметрии. На одномерных объектах такое движение в принципе невозможно. На прямой симметрия относительно этой же прямой ничего не дает,

т.е. является  $\text{id}$ , а на окружности симметрия относительно самой окружности вообще требует специального построения в геометрии плоскости.

## 7.3 Векторно-числовое представление движений плоскости

### Конспект

1. **Аффинное пространство** — множество точек и векторов. В аффинном пространстве мы работаем сразу с двумя сортами объектов — точками и векторами, на которых заданы операции сложения и вычитания. При этом в сумме  $a + b$  и разности  $a - b$  могут быть такие комбинации:
  - 1)  $a$  — точка,  $b$  — вектор, результатом  $a + b$  будет точка, соответствующая концу вектора  $b$ , когда он отложен от точки  $a$ , результатом  $a - b$  будет точка  $c$  такая, что  $c + b = a$ ;
  - 2)  $a$  и  $b$  — векторы, результатом  $a + b$  будет вектор, построенный по правилу параллелограмма, результатом  $a - b$  будет вектор  $c$  такой, что  $c + b = a$ ;
  - 3)  $a$  и  $b$  — точки, результатом  $a - b$  будет вектор с началом в точке  $b$  и концом в точке  $a$ .
2. Движения — это преобразования точек. Параметром движения может быть вектор и/или угол (число).
3. Сдвиг на плоскости на вектор  $a$  обозначим  $T_a$ . Операция  $T_a$  осуществляет прибавление вектора  $a$  к точкам плоскости. Композиция сдвигов соответствует сумме векторов сдвига:  $T_a \circ T_b = T_{b+a}$ .
4. Поворот вокруг нуля мы ранее обозначали  $R_\alpha$ , где  $\alpha$  — угол в радианах.
5. Поворот на угол  $\alpha$  относительно произвольной точки  $M$  можно выразить так:

$$R_{M,\alpha} = T_{O+M} \circ R_\alpha \circ T_{O-M},$$

т.е. сначала сдвигаем точку  $M$  в центр вращения, отмеченный точкой  $O$ , затем производим вращение, затем возвращаем точку  $M$  на место обратным сдвигом.

6. Наконец, у нас остается такой вид движения, который осуществляет отражение относительно произвольной прямой на плоскости. Обозначим его  $S_l$ .
7. Предположим, что на плоскости помимо точки  $O$  мы также зафиксировали некоторую прямую, проходящую через  $O$  с выделенным направлением  $OA$  ( $A$  лежит на этой прямой и не совпадает с  $O$ ). Зафиксируем отражение  $S_{OA}$  относительно данной выбранной оси  $OA$ . Отметим, что  $S_{OA} = S_{AO}$ , т.е. отражение не зависит от направления оси отражения.

8. Выразим произвольное отражение через базовое отражение  $S_{OA}$  и другие движения. Для этого обозначим через  $M$  произвольную точку прямой  $l$ , через  $\alpha$  — угол наклона прямой  $l$  относительно направления  $OA$ . Тогда

$$S_l = T_{O+M} \circ R_\alpha \circ S_{OA} \circ R_{-\alpha} \circ T_{O-M},$$

т.е. сначала мы сдвигаем плоскость так, чтобы точка  $M$  оказалась в точке  $O$ , затем выполняем поворот на угол  $-\alpha$ , далее выполняем стандартное отражение, а затем производим обратные операции, которые возвращают прямую  $l$  на место.

9. Соответственно, скользящая симметрия, при которой выполняется отражение относительно оси  $l$  и сдвиг на вектор  $MM'$  ( $M, M' \in l$ ), записывается так:

$$S_l = T_{O+M} \circ R_\alpha \circ S_{OA} \circ R_{-\alpha} \circ T_{O-M} \circ T_{M'-M},$$

10. В терминах движений  $T, R, S$  можно записать все возможные виды движений плоскости, т.е. сдвиг на произвольный вектор, поворот на произвольный угол относительно произвольной точки, скользящую симметрию относительно произвольной прямой  $l$  со сдвигом на произвольный вектор, лежащий на этой прямой.
11. Если мы вернемся на окружность, то нам потребуется исключить сдвиги, оставив только вращения и симметрии.

## 7.4 Пара слов о движениях сферы

### Конспект

1. Имея опыт перехода от прямой к окружности, мы можем легко найти движения сферы, отправляясь от движений плоскости.
2. Представим себе сферу как плоскость, у которой бесконечно удаленный край был стянут в точку (метод «хинкали»).
3. Во что превращаются при этом движения плоскости?
4. Сдвиг, он же параллельный перенос, превращается в такое движение, при котором все точки движутся по параллельным траекториям. С точки зрения географии это есть движение вдоль широтных линий. Да, проходят они при этом разное расстояние! Из-за чего, кстати, и появляются силы Кориолиса, создающие океанические течения вроде Гольфстрима. Но собственные расстояния между точками сохраняются, и это, несомненно, движение.

5. Вращение, которое, как мы помним, на окружности соответствует сдвигу на прямой, в случае сферы в прямом смысле слова совпадает со сдвигом! Дело в том, что вращение сферы вокруг оси, — это вращение вокруг полюса, при котором угол поворота измеряется меридианом. Но ведь то же самое движение около экватора есть то, что мы только что отнесли к сдвигам вдоль широтных линий.
6. Таким образом, сдвиг прямой и вращение окружности в случае сферы чудесным образом объединяются в один вид движений — осевое вращение. И это делает движения сферы чуть проще, чем движения плоскости, где сдвиг можно представить лишь как композицию двух вращений.
7. Далее, симметрия плоскости относительно прямой естественным образом переходит в отражение сферы относительно центральной секущей плоскости или, иначе говоря, относительно окружности большого круга. При такой симметрии полюса сферы меняются местами (полюса определяются пересечением со сферой прямой, пересекающей плоскость отражения в центре сферы и перпендикулярной ей), а плоскость отражения остается на месте.
8. Наконец, скользящая симметрия плоскости есть композиция сдвига и осевой симметрии, и ей на сфере соответствует **зеркальное вращение**, т.е. композиция отражения и вращения параллельно плоскости отражения.
9. Таким образом, все движения сферы распадаются на два класса: вращения и зеркальные вращения. При этом, все движения есть композиция не более чем трех отражений.
10. Этот аналог теоремы Шалля для сферы можно доказать, используя очередную лемму о гвоздях, предполагая неподвижность пары противоположных точек (случай одной точки на плоскости), неподвижность целой окружности большого круга (случай двух точек на плоскости), отсутствие неподвижных точек.

## Задачи

1. Построить таблицу движений сферы аналогично таблице движений плоскости (символику придумайте сами).
2. \*\*Доказать, что других движений на сфере не существует (лемма о гвоздях).

## 7.5 Пара слов о движениях пространства

## Конспект

1. Наконец, мы можем от сферы перейти к пространству. На самом деле, переход в пространство сопровождается лишь добавлением сдвига в пространстве. Т.е. любое движение сферы можно рассматривать как движение пространства с одной неподвижной точкой — центром сферы. После чего можно применить сдвиг этого центра, и получить новые движения. Понятно, что никаких других движений тут быть не может.
2. Тем не менее, классификация движений пространства становится сложнее примерно так же, как классификация движений плоскости превосходит классификацию движений окружности. А именно, в пространстве появляется **винтовое движение** как композиция осевого вращения и сдвига вдоль оси вращения. Это — обобщение скользящей симметрии на плоскости (если винт осуществляет поворот на  $180^0$ , мы как раз получаем скользящую симметрию).
3. Есть также и собственно **скользящая симметрия пространства**. Это — отражение относительно плоскости с последующим сдвигом вдоль направления, параллельного данной плоскости. Такое движение также является обобщением скользящей симметрии на плоскости.
4. Заметим, что более сложное движение винт включает в себя более простые. Так, если винт имеет нулевой сдвиг, то он доставляет осевое вращение, а если винт имеет нулевой поворот, то он доставляет сдвиг. Понятно, что в случае полного зануления параметров винта мы получим  $\text{id}$ .
5. Точно так же, **зеркальное вращение**, как и в случае сферы, при нулевом повороте доставляет просто симметрию.
6. Наконец, скользящая симметрия своим частным случаем имеет просто симметрию относительно плоскости.
7. Таким образом, классификация движений пространства включает следующие виды движений:
  - а) винт (в частности, сдвиг, осевое вращение,  $\text{id}$ );
  - б) зеркальное вращение (в частности, отражение);
  - в) скользящая симметрия (в частности, отражение).

## Задачи

1. Построить таблицу движений пространства аналогично таблице движений плоскости (символику придумайте сами).
2. \*Показать, что центральная симметрия пространства — это зеркальное вращение.



3. \*\*Доказать, что других движений в пространстве не существует (лемма о гвоздях).

Таблица 7.1: Сравнение движений.

		Собственные движения (не меняют ориентацию)		Несобственные движения (меняют ориентацию)	
	Перенос	Поворот	Смещение по- ворота	Симметрия	Смещенная симметрия
Прямая	сдвиг на число			относительно точки	
Окружность		вращение		осевая симметрия	
Плоскость	параллельный перенос	относительно точки		осевая симметрия	скользящая симметрия (перенос + симметрия)
Сфера	вращение вблизи экватора	вращение вблизи полюса		отражение относительно плоскости	зеркальное вращение (вращение + симметрия)
Пространство	параллельный перенос	осевое вращение	винт (перенос + вращение)	отражение относительно плоскости	зеркальное вращение (вращение + симметрия)

# Перестановки

## Аннотация.

В этой главе мы в основном изучаем конечные группы а примере перестановок. Кроме того, дается промежуточная сводка по свойствам групп.

## 8.1 \*Теория множеств: функции

### Конспект

1. Введем понятие функции. Пусть у нас имеется отношение  $F$  между множествами  $X$  и  $Y$ . Отношение  $F$  называется

**Func1** *всюду значимым*, если для каждого  $y \in Y$  найдется  $x \in X$  такое, что  $xFu$ ;

**Func2** *всюду определенным*, если для каждого  $x \in X$  найдется  $y \in Y$  такое, что  $xFu$ ;

**Func3** *однозначным*, если всякий раз из одновременного выполнения  $xFu$  и  $xFu'$  следует, что  $y = y'$ , т.е. каждому  $x$  соответствует не более одного  $y$ ;

**Func4** *обратно однозначным*, если всякий раз из одновременного выполнения  $xFu$  и  $x'Fu$  следует, что  $x = x'$ , т.е. каждому  $y$  соответствует не более одного  $x$ ;

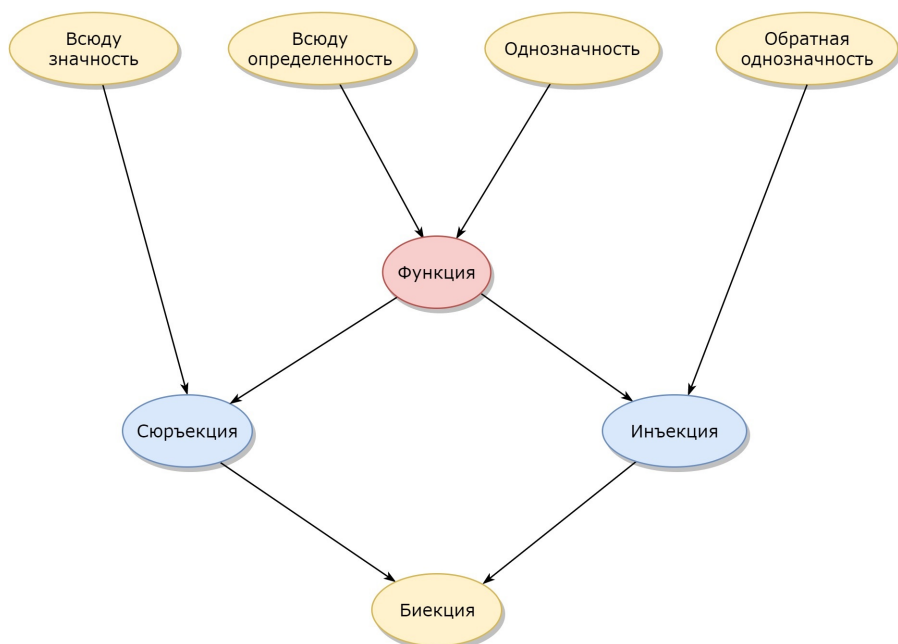
**Func5** *функцией из  $X$  в  $Y$* , если оно всюду определенное и однозначное;

**Func6** *частичной функцией из  $X$  в  $Y$* , если оно однозначное;

**Func7** (частичной) *сюръекцией из  $X$  на  $Y$* , если это всюду значимая (частичная) функция;

**Func8** (частичной) *инъекцией из  $X$  в  $Y$* , если это обратно однозначная (частичная) функция;

**Func9** *биекцией множеств  $X$  и  $Y$* , если это инъекция и сюръекция одновременно, т.е. отношение  $F$  в данном случае взаимно однозначно связывает пары  $(x, y)$ .



Обычно функция из  $X$  в  $Y$  обозначается  $F : X \rightarrow Y$ , а если  $xFy$ , то пишут  $y = F(x)$ . Для обозначения биекции часто используется символ  $F : X \leftrightarrow Y$ .

2. Обратным к  $F$  отношением называется отношение  $F^{-1} = \{(y, x) \mid xFy\}$ . Если обратное отношение есть (частичная) функция, то она называется **обратной функцией**. Легко видеть, что  $F(F^{-1}(y)) = y$  и  $F^{-1}(F(x)) = x$ , если только  $F(x)$  и  $F^{-1}(y)$  определены.
3. **Областью определения** функции  $F$  называется множество  $X$ , а областью **определения частичной функции**  $F$  — подмножество  $X$ , для элементов которого  $F$  определена, **областью значений** (частичной) функции  $F$  называется подмножество  $Y$ , для элементов которого  $F$  определена.
4. Итак, функция — это есть однозначное соответствие элементов одного множества элементам другого (или того же самого). Функции обычно задаются формулами, предписывающими некоторой алгоритм вычисления  $y$  через  $x$ . Но иногда такие формулы не указаны явно или же их указать вовсе невозможно, хотя существование функции строго доказывается (такие теоремы называют теоремами существования).

## 8.2 Конечные группы

## Конспект

1. Рассмотрим группу  $G$ , состоящую из  $n$  элементов, с операцией  $\cdot$  (которую часто будем пропускать для удобства). В терминах функций операция  $\cdot$  есть функция из  $G \times G$  в  $G$ :

$$\cdot : G \times G \rightarrow G.$$

Напомним аксиомы группы:

- G1  $ab \in G$  для всех  $a, b \in G$  (группоид);
- G2 для любых  $a, b, c \in G$  имеем тождество  $(ab)c = a(bc)$  (ассоциативность);
- G3 существует элемент  $e \in G$  такой, что  $ae = ea = a$  для всех  $a \in G$  (единица);
- G4 для всякого  $a \in G$  существует обратный элемент  $a^{-1} \in G$  такой, что  $aa^{-1} = a^{-1}a = e$  (обратный элемент).

Кроме того, группа называется абелевой (или коммутативной), если  $ab = ba$  для всех  $a, b \in G$ . Количество элементов в группе называется ее порядком.

2. В группе существует только одна единица. Действительно, если их две  $e$  и  $e'$ , то в силу их же свойств получим

$$e' = ee' = e$$

(при первом равенстве мы рассматривали  $e$  как единицу, а при втором  $e'$ ).

3. Обратный элемент для каждого  $a \in G$  определен однозначно. Предположим, что для элемента  $a$  нашлось два обратных элемента  $b, c$ , т.е.  $ab = ba = e$  и  $ac = ca = e$ . Тогда

$$b = be = b(ac) = (ba)c = ec = c.$$

4. Степень элемента  $\underbrace{a \cdots a}_{k \text{ раз}}$  обозначается  $a^k$ , где  $k \in \mathbb{N}$ . Кроме того, по определению,  $a^0 = e$ .

5. Отрицательная степень элемента по определению:  $a^{-k} = (a^{-1})^k$ ,  $k \in \mathbb{N}$ .

6. Операции над степенями:

$$(a^k)(a^m) = a^{k+m},$$

где  $k, m \in \mathbb{Z}$ . Если  $k$  и  $m$  одного знака, то это очевидно, а если разного, то пусть  $k > 0$ ,  $m < 0$ , тогда

$$(a^k)(a^m) = \underbrace{a \cdots a}_{k \text{ раз}} \underbrace{a^{-1} \cdots a^{-1}}_{|m| \text{ раз}}.$$

Пользуясь ассоциативностью, начинаем сворачивать пары  $aa^{-1}$ , стоящие в середине, заменяя их на  $e$ , а затем выбрасывая  $e$ . В итоге либо ничего не останется (когда  $k = -m$ ), либо останутся только  $a$  в количестве  $k + m$  (если  $k > -m$ ), либо останутся только  $a^{-1}$  в количестве  $-m - k$  (когда  $k < -m$ ). В любом случае это записывается как  $a^{k+m}$  ( $(a^{-1})^{-m-k} = a^{m+k}$  по определению).

7. В конечной группе каждый элемент в некоторой конечной степени обращается в  $e$ . Действительно, все степени  $a^k$  лежат в конечном множестве  $G$ , а число  $k$  пробегает бесконечный натуральный ряд. Следовательно, хотя бы два разных  $k$  дадут один и тот же элемент (принцип Дирихле):  $a^k = a^{k'}$ , где  $k < k'$ . Домножим это равенство на  $a^{-k}$  и получим  $a^{k'-k} = e$ . Наименьший положительный показатель степени  $m$  для элемента  $a$ , дающий равенство  $a^m = e$ , называется порядком элемента  $a$  в группе  $G$ .

Таким образом, в конечной группе у всякого элемента конечный порядок.

8. Отсюда следует, что всякую отрицательную степень элемента в конечной группе можно записать как положительную, поскольку

$$a^k = a^{k \pmod{p}},$$

где  $p$  — порядок элемента  $a$ .

9. Подмножество  $T \subseteq G$ , все возможные произведения степеней элементов которого, т.е. выражения вида  $t_1^{k_1} \cdots t_m^{k_m}$ , где  $t_j \in T$ ,  $k_j \in \mathbb{N}$ , образуют всю группу  $G$ , называется **системой образующих** группы  $G$ . При этом пишут  $G = \langle T \rangle$  или  $G = \langle t_1, \dots, t_m \rangle$ .
10. Наименьшая по вложению система образующих группы называется **базисом**. Если базис состоит из одного элемента, то группа называется циклической. При этом ее можно записать так:  $G = \langle g \rangle$ , где  $T = \{g\}$ . Иначе говоря, циклическая группа состоит из степеней одного своего элемента.
11. Например, группа  $\mathbb{Z}_n$  вычетов по модулю  $n$  с операцией сложения является циклической:  $\mathbb{Z}_n = \langle 1 \rangle$ , поскольку все ее элементы — это конечные суммы единиц (от одной до  $n$  штук). Группа вращений правильного  $n$ -угольника является циклической, где образующим элементом является поворот на угол  $2\pi/n$ . Группа  $\mathbb{Z}_5^*$  с операцией умножения по модулю 5 является циклической вида  $\langle 2 \rangle$  и  $\langle 3 \rangle$ .
12. Циклические группы являются абелевыми. Действительно, любые два элемента такой группы — это некоторые степени образующего элемента, поэтому  $(a^k)(a^m) = a^{k+m} = a^{m+k} = (a^m)(a^k)$ . Коммутативность наследуется от группы  $\mathbb{Z}$ .

13. Подмножество  $H \subseteq G$  называется подгруппой группы  $G$ , если  $H$  само является группой с той же операцией, которая определена в  $G$ . Например,  $\{0, 2\}$  образует подгруппу группы  $\mathbb{Z}_4$ . Тривиальная подгруппа  $\{e\}$  является подгруппой любой группы.

14. Операции Минковского для подгруппы:

$$gH = \{gh \mid h \in H\}, \quad Hg = \{hg \mid h \in H\},$$

где  $gH$  называется левым, а  $Hg$  — правым классом смежности, порожденным элементом  $g \in G$ .

15. Классы смежности содержат одинаковое количество элементов.

Действительно, пусть  $h_1 \neq h_2$ , где  $h_1, h_2 \in H$ . Предположим, что  $gh_1 = gh_2$ . Домножая слева на  $g^{-1}$ , находим, что  $h_1 = h_2$ . Противоречие. Следовательно, умножение на  $g$  слева различные элементы переводит в различные. Аналогично — для умножения справа.

16. Классы смежности подгруппы  $H$  либо совпадают, либо не пересекаются, а их объединение равно  $G$ . То есть, классы смежности образуют разбиение множества  $G$ . Такую ситуацию мы уже наблюдали в связи с подгруппами  $m\mathbb{Z}$  и их сдвигами внутри  $\mathbb{Z}$  и получали там  $m$  классов смежности.

Пусть классы  $g_1H$  и  $g_2H$  имеют общий элемент  $g$ . Этот элемент будет иметь два представления:  $g = g_1h_1 = g_2h_2$ , где  $h_1, h_2 \in H$ , откуда  $g_1 = g_2h_2(h_1)^{-1}$ . Возьмем любой элемент  $g_1h$  из первого класса, тогда

$$g_1h = g_2h_2(h_1)^{-1}h,$$

где  $h_2(h_1)^{-1}h \in H$ , т.к.  $H$  — подгруппа. Следовательно,  $g_1h \in g_2H$ , и  $g_1H \subseteq g_2H$ . Аналогично рассуждая, находим, что  $g_2H \subseteq g_1H$ , т.е.  $g_1H = g_2H$ .

Тот факт, что любой элемент  $G$  находится в каком-то классе смежности, следует из того, что  $e \in H$ , так что для любого  $g \in G$  имеем  $g \in gH$ . И аналогично для правых классов.

17. Итак, множество  $G$  есть сумма непересекающихся классов одного размера, причем размер классов равен порядку подгруппы  $H$ . Следовательно, порядок подгруппы делит порядок группы. Это утверждение называется **теоремой Лагранжа**.

18.  $g_1H = g_2H$  тогда и только тогда, когда  $(g_1)^{-1}g_2 \in H$ .

Пусть  $g_1H = g_2H$ , тогда любой элемент из этого множества имеет представление  $g_1h_1 = g_2h_2$ , откуда  $h_1(h_2)^{-1} = (g_1)^{-1}g_2$ . Элемент слева — это элемент подгруппы  $H$ .

Обратно, пусть  $(g_1)^{-1}g_2 = h \in H$ , тогда  $g_1h = g_2e$ . Элемент слева принадлежит  $g_1H$ , элемент справа —  $g_2H$ , т.е. эти классы имеют общий элемент, а значит, совпадают.

19. Если группа имеет порядок  $p$ , где  $p$  простое число, то такая группа является циклической.

Действительно, возьмем элемент  $g \neq e$  (поскольку  $p > 1$ , то такое всегда возможно). Пусть  $H = \langle g \rangle$  — циклическая подгруппа  $G$ . Ее порядок делит порядок группы  $G$ , т.е. простое число  $p$ . В то же время, порядок  $H$  отличен от 1, т.к.  $H$  содержит как минимум два элемента  $e, g$ . Но так как  $p$  делится только на 1 и на  $p$ , то порядок группы  $H$  равен  $p$ . Следовательно,  $G = \langle g \rangle$ .

20. Подгруппа  $H$  группы  $G$  называется **нормальной**, если для любого  $g \in G$  верно равенство  $gH = Hg$ , т.е. левые и правые классы не различаются. Обозначение:  $H \triangleleft G$ .

В абелевых группах любая подгруппа будет нормальной. В частности,  $m\mathbb{Z}$  — нормальная в  $\mathbb{Z}$ .

21. Классы смежности нормальной подгруппы можно умножать так же, как сами элементы группы  $G$ :

$$(g_1H)(g_2H) = (g_1g_2)H.$$

Это следует из того, что  $(g_1h_1)(g_2h_2) = g_1(h_1g_2)h_2$ , и при этом  $h_1g_2 = g_2h_3$  при некотором  $h_3$  в силу нормальности  $H$ . Следовательно,

$$(g_1h_1)(g_2h_2) = g_1(h_1g_2)h_2 = g_1(g_2h_3)h_2 = (g_1g_2)(h_3h_2) \in (g_1g_2)H.$$

Обратно,  $(g_1g_2)h = (g_1e)(g_2h)$ . Здесь первый множитель принадлежит  $g_1H$ , второй  $g_2H$ . Так что мы имеем взаимное вложение множеств  $(g_1H)(g_2H)$ ,  $(g_1g_2)H$ , т.е. их равенство.

22. Такое свойство умножения классов смежности по нормальной подгруппе позволяет задать групповую операцию на множестве всех классов смежности, которое обозначается

$$G/H = \{gH \mid g \in G\}$$

и называется **фактор-группой** группы  $G$  по нормальной подгруппе  $H$ . Опять же, мы уже встлкивались с примером фактор-группы  $\mathbb{Z}/m\mathbb{Z}$  при изучении группы вычетов (см. раздел 6.3)

23. Факторизацию группы можно воспринимать как делимость групп, и в этом смысле группы становятся подобны числам. Есть простые группы — они ни на что не делятся, а есть составные — они делятся на нормальные подгруппы.



24. Естественно ввести и умножение групп. Пусть даны две группы  $G_1$  и  $G_2$  с операциями  $\circ$  и  $\star$ , соответственно. Тогда на прямом произведении  $G_1 \times G_2$  определим операцию умножения по правилу

$$(g_1, g_2)(g'_1, g'_2) = (g_1 \circ g'_1, g_2 \star g'_2),$$

т.е. будем покомпонентно перемножать все пары элементов прямого произведения. Легко проверить, что это — групповая операция, т.е. она ассоциативна, имеет единицу, а для каждой пары есть обратная. Все эти свойства наследуются от исходных групп напрямую. Кроме того, если исходные группы абелевы, то и произведение групп будет абелевой группой. Такая конструкция называется внешним **прямым произведением групп**  $G_1$  и  $G_2$ .

Если в исходных группах операция интерпретируется как сложение, то прямое произведение называют прямой суммой групп. Но, учитывая, что это может привести к путанице понятий, мы в любом случае будем пользоваться мультипликативной терминологией и символикой. Тем более, что она согласуется с теоретико-множественным прямым произведением.

25. Рассмотрим простой пример произведения групп:  $\mathbb{Z}_2 \times \mathbb{Z}_2$ . Вот ее таблица умножения:

$\mathbb{Z}_2 \times \mathbb{Z}_2$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

где вместо пары  $(i, j)$  мы про пишем  $ij$  для краткости.

Видим, что эта группа абелева, но не циклическая. В этой группе есть три подгруппы  $\{00, 01\}$ ,  $\{00, 10\}$  и  $\{00, 11\}$ .

Если сравнить ее с группой  $\mathbb{Z}_4$  по сложению, то мы увидим существенную разницу. Во-первых, в  $\mathbb{Z}_4$  только одна подгруппа  $\{0, 2\}$ , а во-вторых,  $\mathbb{Z}_4$  является циклической группой.

Этот пример показывает нам, что порядок группы не определяют однозначно ее структуру (как нам того бы хотелось, памятуя об основной теореме арифметики).

Однако, нам уже хорошо знакома группа, которая имеет такую же таблицу умножения, как и  $\mathbb{Z}_2 \times \mathbb{Z}_2$ . Это все та же группа симметрий ромба, т.е. четверная группа Клейна. Чуть позже мы к ней вернемся.

26. Говорят, что функция  $f : G_1 \rightarrow G_2$  является **изоморфизмом** групп  $(G_1, \circ)$  и  $(G_2, \star)$ , если  $f$  осуществляет взаимно однозначное соответствие обеих групп

$g_2 = f(g_1)$  так, что и результат операций в первой группе переходит в результат операций во второй:

$$f(g_1 \circ g'_1) = f(g_1) \star f(g'_1).$$

Например, если мы рассмотрим группы  $G_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$  и  $G_2 = \mathbb{Z}_8^*$ , то следующее соответствие

$$01 \mapsto 1, \quad 01 \mapsto 3, \quad 10 \mapsto 5, \quad 11 \mapsto 7$$

будет изоморфизмом этих групп. Это видно из следующих таблиц:

$\mathbb{Z}_8^*$	1	3	5	7	$\mathbb{Z}_2 \times \mathbb{Z}_2$	00	01	10	11
1	1	3	5	7	00	00	01	10	11
3	3	1	7	5	01	01	00	11	10
5	5	7	1	3	10	10	11	00	01
7	7	5	3	1	11	11	10	01	00

### 8.3 Арифметика перестановок

#### Конспект

1. Рассмотрим множество  $X_n = \{x_1, \dots, x_n\}$ , состоящее из  $n$  элементов. На этом множестве рассмотрим все возможные биекции множества  $X_n$  в себя. Обозначим

$$S(X_n) = \{f \mid f : X_n \leftrightarrow X_n\},$$

проще говоря, это множество всех возможных **перестановок** элементов множества  $X_n$ .

2. Для функций, заданных на множестве, естественной операцией является операция композиции, т.е. последовательное применение функций друг к другу. Обычно композиция функций записывается символом  $\circ$  или пропускается как умножение. Мы будем пользоваться первым вариантом, так что:

$$(f \circ g)(x) = f(g(x))$$

по определению.

3. Итак, мы имеем множество биекций (перестановок) с операцией композиции. Свойства композиции биекций таковы:

1. композиция биекций есть снова биекция;
2.  $f \circ (g \circ h) = (f \circ g) \circ h$ , поскольку это последовательное вычисление  $f(g(h(x)))$ ;

3. существует функция, которая ничего не меняет:  $\text{id}(x) = x$ , она также является биекцией;
4. для всякой биекции существует обратная функция, которая также является биекцией:  $f \circ f^{-1} = f^{-1} \circ f = \text{id}$ ;

Таким образом, множество  $S(X_n)$  (и вообще, для любого множества  $X$ ) с операцией композиции является группой. И называется группой перестановок множества  $X_n$ .

4. Один простой пример такой группы перестановок мы уже встречали, когда рассматривали все возможные симметрии правильного треугольника. Именно в этом случае все перестановки вершин треугольника оказались движениями, и только они.
5. Сколько всего перестановок в группе  $S(X_n)$ ?

Для ответа на этот вопрос посмотрим, сколько существует вариантов перехода одних элементов в другие. Очевидно, что первый элемент может перейти в любой, в том числе в самого себя, так что для него существует  $n$  вариантов. Второй элемент может перейти куда угодно, кроме того места, которое занял первый, так что для него существует  $n - 1$  вариант. Третьему остается  $n - 2$  варианта. И т.д. Последнему элементу остается выбор из одного оставшегося места. Таким образом, всего вариантов перестановок на  $n$  элементах существует ровно

$$n(n - 1)(n - 2) \dots 2 \cdot 1 = n!$$

Иначе говоря, группа  $S(X_n)$  имеет порядок  $n!$ .

6. Группа перестановок на 3х элементах имеет порядок  $3! = 6$ , что соответствует количеству симметрий правильного треугольника. Однако уже для квадрата число перестановок равно 24, в то время как число всех движений составляет всего лишь 8, а для ромба так и вовсе 4. Вообще, как мы помним, количество движений правильного  $n$ -угольника равно  $2n$ . С ростом  $n$  это число становится во много раз меньше, чем  $n!$  (а точнее, в  $3 \cdot 4 \dots (n - 1) = (n - 1)!/2$  раз).
7. Чтобы не заострять внимание на происхождении элементов множества  $X_n$ , обычно они обозначаются числами от 1 до  $n$ , так что  $X_n = \{1, 2, \dots, n\}$ , а соответствующая группа биекций —  $S_n$ . Легко видеть, что группы  $S_n$  и  $S(X_n)$  изоморфны, т.е. между ними существует биекция, сохраняющая операцию композиции. Поэтому в дальнейшем, говоря о группе перестановок, мы будем иметь ввиду  $S_n$ , заданную на множестве чисел  $1, \dots, n$ .
8. Теория групп в XIX в. начиналась именно с изучения групп подстановок, и лишь позже понятие группы было обобщено Артуром Кэли. Он же сделал первый важный шаг на пути классификации групп.

**Теорема 8.1** (Кэли). *Любая конечная группа порядка  $n$  изоморфна некоторой подгруппе  $S_n$ .*

Для доказательства достаточно заметить, что каждый элемент  $g$  исходной группы  $G$  порождает биекцию на  $G$  по правилу  $h \mapsto gh$  («правые» биекции), а эти биекции образуют изоморфную  $G$  подгруппу внутри группы биекций на  $G$ .

9. В группе  $S_n$ , как и в любой другой, можно построить циклическую подгруппу, отправляясь от произвольно взятого элемента, т.е. биекции на  $X_n$ . Например, пусть  $s \in S_n$ , тогда можно рассмотреть циклическую подгруппу  $G(s) = \{s, s^2, s^3, \dots\}$ , где под степенью понимается многократная композиция биекции  $s$  с самой собой. Ясно, что эта подгруппа не может быть бесконечной, т.к. она входит в конечную группу, поэтому при некотором  $k$  имеем  $s^k = \text{id}$ .
10. Рассмотрим некоторую перестановку  $s \in S_n$ . Ее можно записать в виде таблицы аргумент–значение:

$$s = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ s_1 & s_2 & \dots & s_{n-1} & s_n \end{pmatrix}$$

т.е.  $s(i) = s_i$ . При этом  $\{1, 2, \dots, n\} = \{s_1, s_2, \dots, s_n\}$  в полном соответствии с определением равенства множеств.

11. Возьмем теперь элемент 1 и начнем «раскручивать» его так же, как мы «раскручивали» степени элемента в циклической группе:

$$1 \mapsto s(1) \mapsto s(s(1)) \mapsto \dots \mapsto s^k(1)$$

Мы получим то, что называется **орбитой** элемента 1 при действии группы  $G(s)$  на множестве  $X_n$ . Действительно, все элементы данной цепочки составляют множество  $G(s)1 = \{g(1) \mid g \in G(s)\}$ . Кроме того, если  $s^k = e$ , то  $s^k(1) = 1$ , и мы получаем **цикл**:

$$(1 \ s(1) \ s(s(1)) \ \dots \ s^{k-1}(1))$$

(единицу в конце мы не пишем, подразумевая, что последний элемент цикла переходит в первый).

12. Действие группы  $G(s)$  на множестве  $X_n$  позволяет разбить это множество на несколько попарно непересекающихся орбит или циклов. Отсюда мы получаем представление самой перестановки  $s$  как набора независимых циклов. Поэтому перестановки принято записывать в виде последовательности циклов. Например, пусть

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$$

В этой перестановке мы наблюдаем два цикла:  $(1243)$  и тривиальный  $(5)$ . Тогда

$$s = (1243)(5),$$

причем, тривиальные циклы принято пропускать в такой «циклической» записи, т. к. они однозначно восстанавливаются по всем остальным циклам и по параметру  $n$  (в нашем случае  $n = 5$ ).

13. Рассмотрим более сложный пример:

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 1 & 7 & 5 & 6 \end{pmatrix} = (124)(3)(576) = (124)(576)$$

14. Предположим теперь, что у нас имеется три перестановки:

$$s_1 = \begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 1 \end{pmatrix} \quad s_2 = \begin{pmatrix} 5 & 6 & 7 \\ 7 & 5 & 6 \end{pmatrix} \quad s_3 = \text{id}$$

Тогда исходная перестановка  $s$  получается как последовательное применение этих новых перестановок:

$$s = s_1 s_2 s_3,$$

причем порядок перестановок в композиции неважен, т. к. две из них «работают» на разных орбитах, а третья тождественна и коммутирует с любой перестановкой.

15. Таким образом, каждую перестановку из  $S_n$  можно единственным образом (с точностью до порядка) представить как композицию циклов, и, таким образом, запись перестановки в виде набора ее циклов является не только удобным соглашением, но еще и функционально верной.

16. Наконец, введем такое понятие как **транспозиция**. Это — микроцикл, состоящий из двух элементов, например,  $(12)$  или  $(59)$  и т. п. Транспозиция меняет местами два элемента  $X_n$ , а остальные оставляет на месте. Любой цикл длины  $k$  можно представить как композицию  $k - 1$  транспозиций. Например,

$$(1234) = (14)(13)(12),$$

причем, это представление неоднозначное, поскольку:

$$(2341) = (21)(24)(23),$$

тем не менее, любая перестановка (не только цикл) имеет *инвариант* по разложению в транспозиции.

**Теорема 8.2.** Если перестановка  $g \in S_n$  имеет два представления транспозициями

$$t_1 \dots t_k = g = \tau_1 \dots \tau_m,$$

то  $k \equiv m \pmod{2}$ .

Иначе говоря, четность перестановки, определяемая количеством входящих в ее разложение транспозиций, не зависит от способа этого разложения. Величина  $\text{sgn}(g) = (-1)^k = (-1)^m$  называется **знаком перестановки**  $g$ .

17. Функция  $\text{sgn}$ , определенная на элементах группы  $S_n$  и принимающая значения из множества  $B = \{-1, 1\}$ , является гомоморфизмом групп  $S_n$  и  $B$  (проверьте, что  $(B, \cdot)$  есть группа по умножению, изоморфная  $\mathbb{Z}_2$ ).
18. В связи с этим дадим общее определение: **гомоморфизмом групп**  $(G, \cdot)$  и  $(G', \circ)$  называется всякая функция  $h : G \rightarrow G'$ , сохраняющая групповую операцию, т.е.

$$h(g_1 \cdot g_2) = h(g_1) \circ h(g_2).$$

Изоморфизм — частный случай гомоморфизма. Ядром гомоморфизма  $h$  называется прообраз единицы:

$$\text{Ker}(h) = h^{-1}\{e'\} = \{g \in G \mid h(g) = e'\},$$

где  $e'$  — единица группы  $G'$ .

Гомоморфизм обладает следующими свойствами

- 1° Ядро гомоморфизма есть нормальная подгруппа:  $\text{Ker}(h) \triangleleft G$ .
  - 2° Если  $H \triangleleft G$ , то существует гомоморфизм  $h : G \rightarrow G/H$  такой, что  $H = \text{Ker}(h)$ .
  - 3° Фактор-группа  $G/\text{Ker}(h)$  изоморфна образу  $hG$  в группе  $G'$ .
19. Нетрудно видеть, что функция  $\text{sgn}$  на группе  $S_n$  действует как гомоморфизм в группу  $B$ , поэтому прообраз 1 в группе  $S_n$  относительно данного гомоморфизма, а именно, *все четные перестановки* образуют нормальную подгруппу в группе подстановок  $S_n$ . Эта нормальная подгруппа обозначается  $A_n$  и называется **знакопеременной группой** порядка  $n$ . Следует не путать употребленное здесь слово «порядок» с порядком группы, означающем количество ее элементов, поскольку в  $A_n$  находится ровно половина элементов группы  $S_n$ , т.е.  $n!/2$ , что значительно больше  $n$ .
  20. Четность перестановки является инвариантом на подгруппе  $A_n$  (т.е. принимает одно и то же значение на всех ее элементах), а также на ее смежном классе в  $S_n$  (принимает другое постоянное значение). Поиск инвариантов является одним из мощных математических инструментов при поиске закономерностей и доказательстве невозможности некоторых объектов или действий.

21. С конца XIX века известна игра «пятнашки», суть которой в следующем. Имеем поле  $4 \times 4$ , в котором расставлены одинаковые по размеру фишки размером  $1 \times 1$ . Всего фишек 15, и они пронумерованы числами от 1 до 15. Одно место на поле пустое, что позволяет производить следующие простые манипуляции: занимать данное место фишкой с любого смежного места, т. е. передвигать ее на это место, освобождая соседнее. При этом нельзя совершать никакие другие действия, например, вынимать фишки с поля и расставлять их произвольным образом.

В результате таких действий порядок номеров у фишек меняется, т. е. мы осуществляем перестановку из группы  $S_{15}$ .

«Фишка» этой игры в том, что все разрешенные манипуляции не меняют четности исходной перестановки номеров. А это значит, что никакую нечетную изначальную расстановку невозможно привести (разрешенными действиями) к четной перестановке, и наоборот. Например, две расстановки фишек, отличающиеся лишь одной транспозицией (обменом двух соседних фишек местами), не могут быть переведены одна в другую.

Создатель игры (никто еще не знал тогда алгебраического решения задачи) даже обещал приз 100 долларов тому, кто приведет расстановку

1	2	3	4	к виду	1	2	3	4
5	6	7	8		5	6	7	8
5	6	7	8		5	6	7	8
9	10	11	12		9	10	11	12
13	15	14			13	14	15	

(они отличаются транспозицией (15 14)).

С тех пор прошло больше 100 лет, и до сих пор многие пытаются это сделать, но алгебра дает нам беспощадный ответ: это сделать невозможно! Потому что четность перестановки инвариантна относительно действий с фишками!

22. Другой замечательный пример инварианта — теорема Эйлера о числе выпуклого многогранника: величина  $V-P+G=2$  для всех выпуклых многогранников ( $V$  — число вершин,  $P$  — ребер,  $G$  — граней). Отсюда, в частности, следует, что на футбольном мяче, сшитом только из правильных 5- и 6-угольников, может быть только 12 пятиугольников, никакое другое число не удовлетворяет этому инварианту.

23. Как уже отмечалось выше, все конечные группы изоморфны некоторым подгруппам в группах перестановок. Ранее изученная нами группа  $\mathbb{Z}_2 \times \mathbb{Z}_2$  имеет изоморфный клон среди подгрупп группы перестановок  $S_4$ . В таблице A.1 (в

конце книги) помещена полная таблица умножения группы  $S_4$  с использованием кратких обозначений перестановок как произведений циклов. Там же выделены две подтаблицы, отвечающие группам  $A_4$  и  $V_4$ , а также отмечены (жёлтым) элементы (и их произведения) подгруппы 8-го порядка, которая не является ни нормальной, ни абелевой.

Выделенная подгруппа 8-го порядка:

$$\{e, (12)(34), (13)(24), (14)(23), (12), (34), (1324), (1423)\}.$$

Все подгруппы 8-го порядка изоморфны. Аналогичная ситуация с подгруппами 6-го порядка, вот одна из них:  $\{e, (123), (132), (12), (13), (23)\}$ , которая совпадает с  $S_3$ .

24. В группе  $S_4$  существует только 2 нетривиальные нормальные подгруппы:  $A_4$  и  $V_4$ . Все подгруппы порядков 2,3,6,8 не являются нормальными.
25. Говорят, что группа  $G$  имеет **субнормальный ряд** (называемый также **субнормальной башней**, **субинвариантным рядом**, **субнормальной матрёшкой** или просто **рядом**) длины  $n$ , если имеют место вложения:

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{n-1} \triangleleft G_n = G,$$

где  $G_i$  — собственная нормальная подгруппа в  $G_{i+1}$ . Ряд называется **нормальным**, если все  $G_i$  нормальны также в исходной группе  $G$ . Факторгруппы  $G_{i+1}/G_i$  называются **факторами** (факторгруппами) **ряда**.

Для простых групп (например,  $\mathbb{Z}_p$ ) тривиальный субнормальный ряд длины 1 является единственно возможным:  $\{e\} \triangleleft G$ .

Для группы  $S_4$  имеем:

$$\{e\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4, \quad \{e\} \triangleleft V_4 \triangleleft S_4$$

Эти утверждения можно извлечь непосредственно из таблицы А.1. Например, нормальность  $V_4$  в  $A_4$  следует из того, что симметричные столбец и строка в зеленой области напротив и под группой  $V_4$  совпадают с точностью до перестановки элементов (т. е. выполняется условие  $gH = Hg$ ).

26. Если для группы  $G$  существует такой субнормальный ряд, что все его факторы — абелевы группы, то группа  $G$  называется **разрешимой**.

Так как

- а)  $S_4/A_4 \cong \mathbb{Z}_2$ , т. е. является циклической и, тем более, абелевой группой,
- б)  $A_4/V_4 \cong \mathbb{Z}_3$ , т. е. является циклической и, тем более, абелевой,
- с)  $V_4/\{e\}$  — абелева группа (см. таблицу А.1),



то  $S_4$  разрешима. Заметим, что ряд  $\{e\} \triangleleft V_4 \triangleleft S_4$  не годится для установления разрешимости, поскольку фактор  $S_4/V_4 \cong S_3$  не является абелевой группой.

Для  $n = 3$  имеем  $\{e\} \triangleleft A_3 \cong \mathbb{Z}_3 \triangleleft S_3$  и, таким образом,  $S_3$  также разрешима. Тем более разрешима и  $S_2 \cong \mathbb{Z}_2$ .

Известно, что все  $S_n$  порядка  $n \geq 5$  неразрешимы. Именно на этом замечательном факте построено доказательство знаменитой теоремы Галуа о неразрешимости в радикалах уравнений степени 5 и выше.

## 8.4 Четверная группа Клейна

Четверная группа Клейна					Циклическая 4-го порядка				
$\diamond$	id	$R$	$S_1$	$S_2$	$\square$	id	$R_{\pi/2}$	$R_\pi$	$R_{3\pi/2}$
id	id	$R$	$S_1$	$S_2$	id	id	$R_{\pi/2}$	$R_\pi$	$R_{3\pi/2}$
$R$	$R$	id	$S_2$	$S_1$	$R_{\pi/2}$	$R_{\pi/2}$	$R_\pi$	$R_{3\pi/2}$	id
$S_1$	$S_1$	$S_2$	id	$R$	$R_\pi$	$R_\pi$	$R_{3\pi/2}$	id	$R_{\pi/2}$
$S_2$	$S_2$	$S_1$	$R$	id	$R_{3\pi/2}$	$R_{3\pi/2}$	id	$R_{\pi/2}$	$R_\pi$
$\mathbb{Z}_8^*$	1	3	5	7	$\mathbb{Z}_4$	0	1	2	3
1	1	3	5	7	0	0	1	2	3
3	3	1	7	5	1	1	2	3	0
5	5	7	1	3	2	2	3	0	1
7	7	5	3	1	3	0	1	2	3
$\mathbb{Z}_2 \times \mathbb{Z}_2$	00	01	10	11	$\mathbb{Z}_5^*$	1	2	4	3
00	00	01	10	11	1	1	2	4	3
01	01	00	11	10	2	2	4	3	1
10	10	11	00	01	4	4	3	1	2
11	11	10	01	00	3	3	1	2	4
id	(12)(34)	(13)(24)	(14)(23)		$\sqrt[4]{1}$	1	$i$	-1	$-i$
(12)(34)	id	(14)(23)	(13)(24)		1	1	$i$	-1	$-i$
(13)(24)	(14)(23)	id	(12)(34)		$i$	$i$	-1	$-i$	1
(14)(23)	(13)(24)	(12)(34)	id		-1	-1	$-i$	1	$i$
					$-i$	$-i$	1	$i$	-1

## 8.5 Перестановки: деликатесы

# Линейные уравнения

## Аннотация.

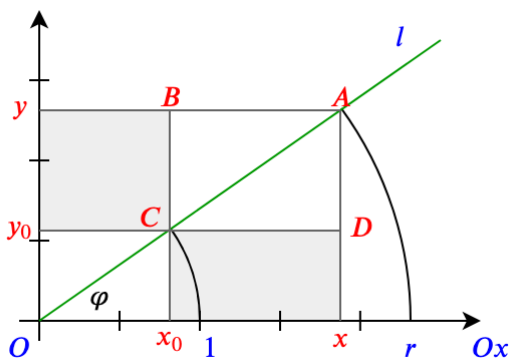
Основная задача данной главы — дать полное описание решений линейных уравнений в целых числах. Попутно вводится уравнение прямой на координатной плоскости, хотя мы все еще подразумеваем, что работаем только с целыми числами.

## 9.1 Уравнение прямой на плоскости

### Конспект

1. Рассмотрим плоскость с координатными осями  $Ox$  и  $Oy$ . Что будет, если ее начать поворачивать? Во что переходит при этом ось  $Ox$ ?
2. Поскольку вращение — это движение, расстояние между точками сохраняется, и значит, никакие три точки, лежащие на прямой  $Ox$ , при повороте не могут перейти в точки, образующие невырожденный треугольник — они снова лягут на прямую, причем в том же самом порядке. Стало быть,  $Ox$  при вращении плоскости переходит в некоторую прямую.
3. Пусть центром вращения является точка  $O = (0, 1)$ , и ось  $Ox$  при вращении  $R_\varphi$  переходит в прямую  $l$ . Ясно, что  $l$  также проходит через начало координат  $O$ , т.к. это — стационарная точка вращения.
4. Фиксируем на  $Ox$  точку  $(1, 0)$  и посмотрим, куда она переходит под действием всех возможных вращений. Поскольку расстояние от центра вращения сохраняется, ясно, что эта точка остается на окружности радиуса 1. В то же время, выбирая произвольную точку на этой окружности, мы легко укажем угол  $\varphi$ , на который нужно осуществить поворот плоскости относительно центра  $O$ , чтобы точка  $(1, 0)$  перешла в выбранную нами точку.
5. Итак, под действием группы вращений точка  $(1, 0)$  переходит во все точки единичной окружности. Аналогично, если мы выберем произвольную точку  $(r, 0)$  ( $r > 0$ ), она будет переходить во все точки окружности радиуса  $r$  под действием группы вращений с центром в точке  $O$ .

6. В этом случае принято говорить, что группа вращений *действует* на плоскости, а множество всех значений, в которые она переводит выбранную точку, называют *орбитой* этой точки. В нашем примере орбитами являются концентрические окружности с центром  $O$ .
7. Можно доказать, что орбиты образуют классы эквивалентности, т.е. они попарно не пересекаются и в сумме дают всю область действия группы.
8. Фиксируем некоторое вращение  $R_\varphi$ , и пусть точка  $(0, 1)$  при таком вращении перешла в точку  $C = (x_0, y_0)$ , лежащую на единичной окружности.
9. Возьмем произвольную точку  $(r, 0)$ , где  $r > 0$ , и проследим ее судьбу под действием того же вращения  $R_\varphi$ . Пусть  $A = (x, y) = R_\varphi(r, 0)$ . Ясно, что точки  $O, C, A$  лежат на одной прямой  $l$ .
10. Проведем вертикальные линии через абсциссы  $x_0$  и  $x$ , а также горизонтальные линии через ординаты  $y_0$  и  $y$ . Добавим новые точки пересечения  $B$  и  $D$  (см. рисунок).



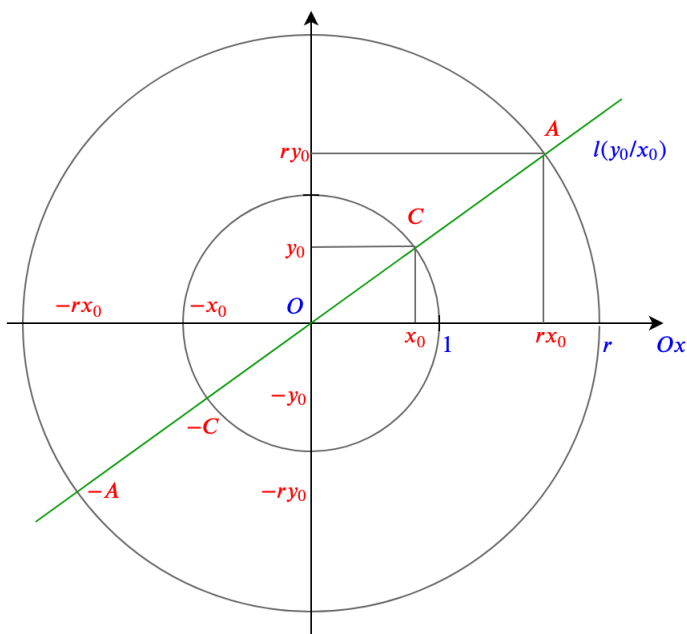
11. Видим, что треугольники  $ABC$  и  $ADC$  равны по трем сторонам, также равны треугольники  $Oy_0C$  и  $Ox_0C$ , и треугольники  $OyA$  и  $OxA$ . Отсюда легко установить равенство площадей  $x_0(y - y_0) = y_0(x - x_0)$ , откуда получаем

$$xy_0 - yx_0 = 0.$$

12. Поскольку  $(x, y)$  — это произвольная точка прямой  $OC$  (для отрицательного  $r$  все доказывается аналогично), данное уравнение есть уравнение прямой, проходящей через начало координат с углом наклона  $\varphi$ .
13. Отметим, что точка  $(x_0, y_0)$  полностью определяется углом поворота  $\varphi$ , т.к. является образом точки  $(0, 1)$  при повороте на угол  $\varphi$ . В то же время, произвольная точка на единичной окружности однозначно задает угол поворота в

интервале от 0 до  $2\pi$ . Таким образом, задать поворот с центром  $O$  и задать точку на единичной окружности — суть одно и то же.

14. Зная тригонометрию, можно также заметить, что  $x_0 = \cos \varphi$  и  $y_0 = \sin \varphi$ , а отношение  $y_0/x_0 = \tan \varphi$ .
15. Кроме того, отношение  $y_0/x_0$  также однозначно определяет угол поворота, но только в интервале от 0 до  $\pi$ .
16. Наконец, поворот прямой(!) на угол  $\pi + \alpha$  — это поворот на угол  $\alpha$  с последующим отражением прямой  $l$  относительно точки  $O$ . Но отражение прямой относительно своей же точки дает нам ту же самую прямую с тем же самым уравнением для ее точек! Таким образом, прямая, проходящая через начало координат полностью определяется тангенсом угла наклона, т.е. отношением  $y_0/x_0$ .
17. Но раз все дело в отношении, стало быть, прямая задается любой точкой, координаты которой находятся в таком же соотношении, что и координаты точки  $(x_0, y_0)$ , лежащие на единичной окружности. Иначе говоря, одну и ту же прямую задают также точки вида  $(-x_0, -y_0)$ ,  $(rx_0, ry_0)$ ,  $(-rx_0, -ry_0)$ , если коэффициент  $r > 0$ . На рис. мы обозначили эти точки, соответственно,  $C$ ,  $A$  и  $-C$ ,  $-A$ .



18. Этот вывод можно получить и более формально, просто глядя на уравнение

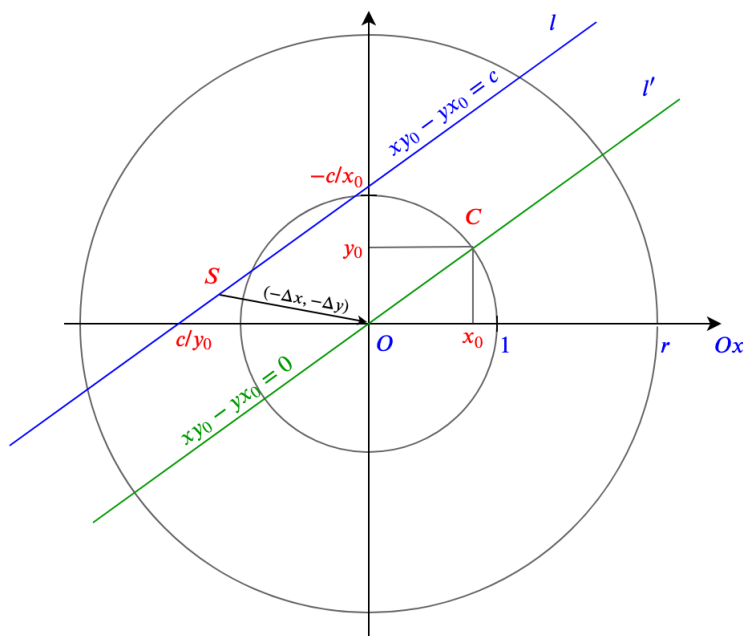
прямой

$$xy_0 - yx_0 = 0.$$

Ведь если мы домножим обе части уравнения на  $r$ , ничего не изменится!

$$x(ry_0) - y(rx_0) = 0.$$

19. Что если прямая  $l$  не проходит через центр координат  $O$ ? В этом случае мы можем сдвинуть ее на некоторый вектор так, чтобы произвольно выбранная точка этой прямой перешла в точку  $O$ . Обозначим эту точку на прямой  $l$  за  $S = (\Delta x, \Delta y)$ , а сдвиг, соответственно, осуществим на вектор  $(-\Delta x, -\Delta y)$ .



20. Тогда смещенные координаты  $(x - \Delta x, y - \Delta y)$  уже будут пробегать прямую  $l'$ , проходящую через центр  $O$ , а ее уравнение нам известно:

$$(x - \Delta x)y_0 - (y - \Delta y)x_0 = 0,$$

или

$$xy_0 - yx_0 = c, \quad \text{где } c = y_0\Delta x - x_0\Delta y.$$

При этом коэффициенты  $(x_0, y_0)$  все так же отвечают за наклон прямой  $l$  и полностью определяются тангенсом угла наклона прямой  $l$  относительно положительного направления  $Ox$ , т.е. отношением  $y_0/x_0$ .

21. Может показаться, что уравнение сильно зависит от выбора точки  $S$ , поскольку слагаемое  $c$  зависит от координат точки  $S$ . Покажем, что это не так. Пусть  $S' = (\Delta x', \Delta y')$  — какая-то другая точка прямой  $l$ . Но в этом случае она удовлетворяет найденному уравнению, т.е.

$$\Delta x' y_0 - \Delta y' x_0 = c,$$

но уравнение, найденное с помощью точки  $S'$  будет иметь вид

$$x y_0 - y x_0 = y_0 \Delta x' - x_0 \Delta y',$$

откуда из предыдущего получаем, что вновь

$$x y_0 - y x_0 = c.$$

22. Таким образом, для нахождения  $c$  мы можем выбрать любую понравившуюся нам точку прямой  $l'$ , например, отчку пересечения с одной из координатных осей.
23. В случае, когда  $x_0 \neq 0$ , уравнение прямой можно переписать в виде

$$y = ax + b, \quad \text{где } a = \frac{y_0}{x_0}, \quad b = -\frac{c}{x_0}.$$

В случае  $x_0 = 0$  мы имеем вертикальную прямую  $x = c$  (при угле  $\varphi = \pi/2$  мы получим  $y_0 = 1$ ).

## Задачи

- В какие точки переходят точки  $(0, 3)$  и  $(4, 0)$  при повороте на  $90$  градусов? На  $-90$  градусов?
- Каков угол поворота, если точка  $(a, b)$  перешла в точку  $(-a, -b)$ ? В точку  $(-b, a)$ ? В точку  $(b, -a)$ ?
- Чему равен тангенс угла наклона прямой  $3x - 5y = 7$ ?
- Какой угол наклона у прямой  $y = -x + 3$ ?

## 9.2 Линейные уравнения в целых числах

### Конспект

- Поскольку мы пока владеем аппаратом только целых чисел (множество  $\mathbb{Z}$ ), рассмотрим задачу о нахождении всех целых точек плоскости, через которые проходит заданная прямая. Под целыми точками плоскости мы будем понимать такие точки, координаты которых принадлежат  $\mathbb{Z}$ .

2. В общем виде **линейное уравнение в целых числах** выглядит следующим образом:

$$ax - by = c, \quad \text{где коэффициенты } a, b, c \in \mathbb{Z}.$$

Задача: найти все такие  $x, y$ , тоже целые, которые удовлетворяют данному уравнению.

3. Сначала рассмотрим случай т.н. **однородного уравнения**:

$$ax - by = 0,$$

т.е. мы отбрасываем ту часть уравнения, которая не зависит от переменных  $x, y$ .

4. Как мы уже знаем, данное уравнение задает прямую, проходящую через начало координат, а ее наклон определяется отношением  $a/b$ .
5. Для начала проверим, нельзя ли данное отношение упростить. Если числа  $a, b$  имеют какой-то общий делитель, то разумно было бы на него сократить. И чтобы не проверять это много раз, сократим их сразу на  $\text{НОД}(a, b)$ . Множество решений от этого не изменится, а само уравнение по-прежнему останется однородным и целочисленным:

$$\tilde{a}x - \tilde{b}y = 0, \quad \text{где } \tilde{a} = \frac{a}{\text{НОД}(a, b)}, \quad \tilde{b} = \frac{b}{\text{НОД}(a, b)}.$$

6. Таким образом, мы приходим к уравнению со взаимно простыми коэффициентами  $\tilde{a}$  и  $\tilde{b}$ .
7. Перепишем уравнение иначе:  $\tilde{a}x = \tilde{b}y$ . Заметим, что все числа здесь — целые. Причем  $\tilde{b}y$  делится на  $\tilde{a}$ . Но так как  $\tilde{a}$  и  $\tilde{b}$  взаимно просты, то  $y$  делится на  $\tilde{a}$ . Это есть следствие того факта, который мы доказывали ранее в разделе 4.3: если простое число  $p$  делит произведение  $ab$ , то оно делит  $a$  или  $b$  (или их обоих). Поэтому если простое  $p$  делит  $\tilde{a}$ , то оно делит  $\tilde{b}y$ , но оно не может делить  $\tilde{b}$ , т.к.  $\text{НОД}(p, \tilde{b}) = 1$ , значит, оно делит  $y$ . Это значит, что все простые, составляющие число  $\tilde{a}$ , являются делителями  $y$ . В то же время, эти простые не входят в  $\tilde{b}$ , поскольку  $\text{НОД}(\tilde{a}, \tilde{b}) = 1$ . Поэтому, если  $p^\alpha$  входит в разложение  $\tilde{a}$ , то  $p^\alpha$  также делит  $y$ . Следовательно,  $y$  делится на  $\tilde{a}$ , т.е.

$$y = k\tilde{a}$$

при некотором целом  $k$ .

8. Симметрично рассуждая, получаем, что  $x$  делится на  $\tilde{b}$ , т.е.

$$x = t\tilde{b}$$

при некотором целом  $t$ .

9. Подставим эти выражения в наше однородное уравнение:

$$\tilde{a}(t\tilde{b}) = \tilde{b}(k\tilde{a}),$$

откуда

$$t = k,$$

и больше никаких ограничений на выбор коэффициента  $k$  мы не имеем.

10. Таким образом, решениями уравнения  $\tilde{a}x - \tilde{b}y = 0$  являются

$$\begin{cases} x = k\tilde{b} = kb/\text{НОД}(a, b), \\ y = k\tilde{a} = ka/\text{НОД}(a, b), \end{cases}$$

где  $k \in \mathbb{Z}$ . Эти же  $x$  и  $y$  являются решениями исходного однородного уравнения  $ax - by = 0$ .

11. Вернемся к неоднородному уравнению  $ax - by = c$ .

12. Для начала заметим, что если данное уравнение имеет решение в целых числах, то  $ax - by$  делится на  $\text{НОД}(a, b)$ , а значит,  $c$  делится на  $\text{НОД}(a, b)$ . Поэтому, если  $c$  не делится на  $\text{НОД}(a, b)$ , то решений точно нет, т.е. в таком случае прямая  $ax - by = c$  проходит мимо всех целых точек плоскости!

13. Покажем, что в случае делимости  $c$  на  $\text{НОД}(a, b)$  решения обязательно есть, и опишем все такие решения.

14. Пусть  $c = d\text{НОД}(a, b)$ .

15. В разделе 4.3 мы установили, что  $\text{НОД}(a, b)$  является линейной комбинацией чисел  $a$  и  $b$ , т.е.

$$\text{НОД}(a, b) = an - bm$$

при некоторых целых  $n$  и  $m$  (понятно, что знак перед  $m$  можно выбирать любой, поэтому выберем так, как нам удобнее).

16. Отсюда следует, что пара чисел  $(dn, dm)$  удовлетворяет уравнению  $ax - by = c$ , поскольку  $adn - bdm = d\text{НОД}(a, b) = c$ .

17. Итак, представив  $\text{НОД}(a, b)$  в виде линейной комбинации  $a$  и  $b$ , мы можем найти одно решение исходного уравнения.

18. Далее применим тот же прием, что и при изучении уравнений прямых — сдвинем прямую  $ax - by = c$  так, чтобы точка  $(dn, dm)$  оказалась в начале координат. Для этого введем новые переменные

$$\hat{x} = x - dn, \quad \hat{y} = y - dm.$$



19. Тогда получаем, что  $a\hat{x} - b\hat{y} = 0$ . А такое уравнение мы уже решили выше, и его решением будет пара чисел  $\hat{x} = kb/\text{НОД}(a, b)$  и  $\hat{y} = ka/\text{НОД}(a, b)$ , где  $k$  — любое целое число.

20. Собирая все вместе, находим общее решение исходного уравнения:

$$\begin{cases} x = kb/\text{НОД}(a, b) + dn, \\ y = ka/\text{НОД}(a, b) + dm, \end{cases}$$

21. Таким образом, решением линейного уравнения  $ax - by = c$  в целых числах является сумма общего решения однородного уравнения  $ax - by = 0$  и какого-нибудь частного решения исходного уравнения.

22. Основной трудностью при поиске частного решения является нахождение коэффициентов  $n$  и  $m$  представления  $\text{НОД}(a, b)$ .

23. Это представление можно найти с помощью алгоритма Евклида. Рассмотрим для примера уравнение

$$18x - 11y = 2$$

24. Следуя алгоритму Евклида, получаем выкладки:

$$\begin{aligned} 18 &= 11 \cdot 1 + 7, \\ 11 &= 7 \cdot 1 + 4, \\ 7 &= 4 \cdot 1 + 3, \\ 4 &= 3 \cdot 1 + 1 \end{aligned}$$

Последняя 1 — это и есть  $\text{НОД}(18, 11)$ . Раскрутим алгоритм в обратную сторону:

$$\begin{aligned} 1 &= 4 - 3 = 4 - (7 - 4) = 4 \cdot 2 - 7 = (11 - 7) \cdot 2 - 7 = \\ &= 11 \cdot 2 - 7 \cdot 3 = 11 \cdot 2 - (18 - 11) \cdot 3 = \\ &= 11 \cdot 5 - 18 \cdot 3. \end{aligned}$$

Таким образом, наши искомые числа  $n = -3$ ,  $m = -5$ . Напомним, что мы ищем представление  $\text{НОД}(18, 11)$  в виде  $18n - 11m$ , исходя из чего нужно правильно выбирать знаки перед коэффициентами.

Кроме того,  $d = 2$ , т.к.  $c = 2$  и  $\text{НОД}(a, b) = 1$ . Откуда общее решение уравнения  $18x - 11y = 2$  получаем в виде:

$$\begin{cases} x = 11k - 6, \\ y = 18k - 10, \end{cases}$$

где  $k$  — любое целое число. Проверим:

$$18(11k - 6) - 11(18k - 10) = 198k - 108 - 198k + 110 = 2.$$

25. Наконец, приведем еще один замечательный способ найти разложение НОД. Этот метод основан на представлении дробей в виде т.н. *цепных дробей*. Пусть дано уравнение

$$112x - 34y = 16.$$

26. Ищем приближение дроби  $112/34$  следующим способом:

$$\frac{112}{34} = 3 + \frac{5}{17} = 3 + \frac{1}{3 + \frac{2}{5}} = 3 + \frac{1}{3 + \frac{1}{2 + \frac{1}{2}}}$$

По сути дела, это — другая запись выкладок алгоритма Евклида, поскольку мы каждый раз последовательно выделяем неполное частное предыдущих остатков.

Как только мы дошли до хвоста вида  $1/k$ , мы останавливаемся, отбрасываем этот хвост и сворачиваем дробь обратно, получая приближение исходной дроби:

$$\frac{112}{34} \approx 3 + \frac{5}{17} = 3 + \frac{1}{3 + \frac{2}{5}} = 3 + \frac{1}{3 + \frac{1}{2}} = \frac{23}{7}$$

Далее, перемножая накрест эти дроби, получаем представление для НОД:

$$\text{НОД}(112, 34) = 112 \cdot 7 - 34 \cdot 23.$$

Искомые коэффициенты:  $n = 7$ ,  $m = 23$ . Общее решение уравнения, таким образом, получаем в виде

$$\begin{cases} x = 34k + 8 \cdot 7, \\ y = 112k + 8 \cdot 23, \end{cases}$$

где  $k$  — любое целое число, а  $8 = 16/\text{НОД}(112, 34)$ . Проверяем:

$$112(34k + 8 \cdot 7) - 34(112k + 8 \cdot 23) = 8(112 \cdot 7 - 34 \cdot 23) = 16.$$

27. Выше мы всюду рассматривали уравнения, в которых  $x$  идет с положительным коэффициентом, а  $y$  — с отрицательным. Иначе говоря, прямая, заданная таким уравнением, имеет наклон «вправо». Но уравнение может быть, например, таким

$$5x + 9y = 1.$$

Если мы хотим решать его по тем же формулам, то лучше перейти к новым переменным  $\hat{x} = x$ ,  $\hat{y} = -y$ , и тогда мы получим уравнение

$$5\hat{x} - 9\hat{y} = 1.$$

Найдя его решения, мы просто меняем знак у  $\hat{y}$ , и получаем исходное уравнение.

## Задачи

1. Найти представление  $\text{НОД}(5, 9)$  с помощью алгоритма Евклида и методом цепных дробей.
2. Найти представление  $\text{НОД}(18, 15)$  с помощью алгоритма Евклида и методом цепных дробей.
3. Найти представление  $\text{НОД}(225, 81)$  с помощью алгоритма Евклида и методом цепных дробей.
4. Решить уравнение  $5x - 9y = 2$  в целых числах.
5. Найти все решения уравнения  $225x + 81y = 18$  в целых числах.
6. Найти все решения уравнения  $10x - 18y = 3$  в целых числах или доказать, что их нет.

# Числовые поля

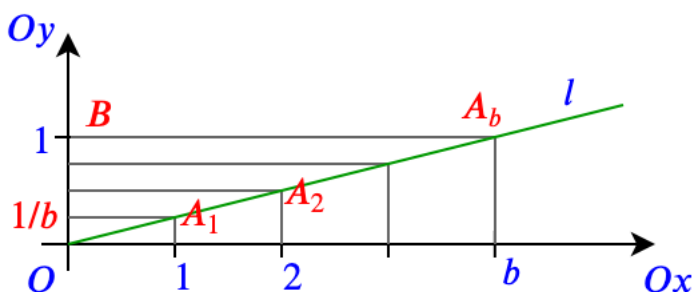
## Аннотация.

В этой главе мы ачинаем выход за пределы целых чисел, и прежде всего займемся построением чисел рациональных. Кроме того, здесь будет введено определение поля и приведены примеры конечных полей.

## 10.1 Рациональные числа

### Конспект

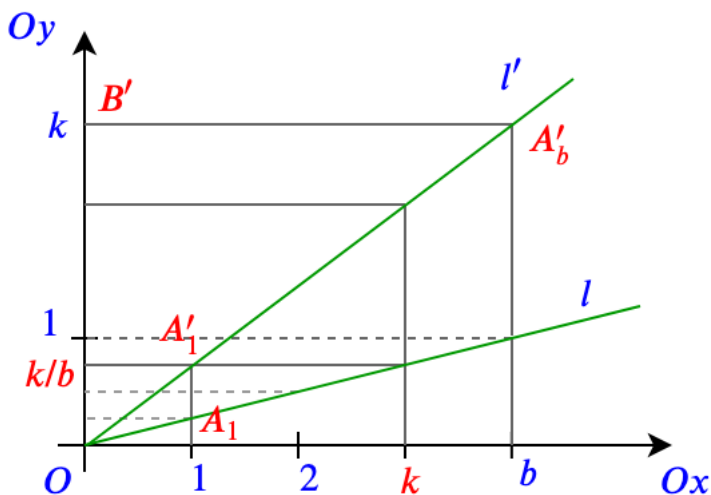
1. Предыдущую главу мы закончили действиями с дробями, хотя нигде до сих пор о них не говорили. Разве что, упоминали отношение  $y_0/x_0$  как некоторый параметр, определяющий угол наклона прямой на координатной плоскости.
2. Итак, рассмотрим прямую  $l$ , заданную уравнением  $ax - by = 0$ , где  $a, b$  — целые числа.
3. Для начала пусть  $a = 1$  и  $b > 1$ . Легко видеть, что такая прямая проходит через точки  $(0, 0)$  и  $(b, 1)$  (см. рис.).



4. На прямой  $l$  мы можем поставить точки  $A_1, A_2, \dots, A_b$  в местах пересечения этой прямой с вертикальными прямыми, имеющими уравнения  $x = 1, x = 2, \dots, x = b$ , соответственно.
5. Теперь рассмотрим треугольник  $OBA_b$ , где точка  $B = (0, 1)$ . В этом треугольнике мы можем провести линии, параллельные его горизонтальной стороне

$BA_b$ , которые отсекут на вертикальной стороне  $OB$  нашего треугольника отрезки.

6. Эти отрезки будут иметь одинаковую длину по теореме Фалеса, т.к. точки на прямой  $l$  также расставлены с одинаковым шагом, что следует уже из выбора вертикальных секущих (они идут с шагом 1).
7. Итак, на вертикальной оси мы получили  $b$  одинаковых отрезков, сумма длин которых равна 1.
8. Какова же длина каждого из таких отрезков? Ответ: она равна одной  $b$ -ой части единицы. И эта часть записывается как дробь  $1/b$ . Собственно, отношение  $1/b$ , как мы видели ранее, является определяющим для прямой  $l$ .
9. Мы можем брать сумму нескольких таких частей, например,  $k$  частей размера  $1/b$  дают в сумме отрезок длины в  $k$  раз больше, чем отрезок  $1/b$ . Такая часть записывается в виде дроби  $k/b$ .
10. Величину  $k/b$  можно получить иным способом. Возьмем теперь прямую  $l'$ , заданную уравнением  $kx + by = 0$  (см. рис.).



11. Эта прямая проходит через начало координат и точку  $(b, k)$ .
12. Прделаем аналогичные предыдущему построения: проведем вертикальные линии с шагом 1, а затем горизонтальные линии от точек пересечения вертикальных с прямой  $l'$ , и посмотрим, какие отрезки у нас получатся на оси  $Oy$ .
13. Нетрудно видеть, что линия, соответствующая  $x = k$ , для прямой  $l$  отсекает на оси  $Oy$  метку, которую мы обозначили как  $k/b$ . Но ровно ту же самую

метку покажет построение с помощью вертикальной линии  $x = 1$  и прямой  $l'$ . Почему? А очень просто: достаточно сравнить уравнения этих прямых

$$l : x - by = 0, \quad l' : kx - by = 0.$$

Если в первом вместо  $x$  подставить  $k$ , а во втором вместо  $x$  подставить  $1$ , то получим одно и то же значение  $y$ . Отсюда и совпадение меток.

14. Таким образом, прямая  $l'$  дает на оси  $Oy$  шаг в  $k$  раз больше, чем прямая  $l$ , если мы строим сечения при одном и том же  $x$  (не обязательно  $x = 1$ ).
15. Получается, что прямая, заданная уравнением  $kx - by = 0$ , задает умножение на число  $k$  всех чисел, получаемых прямой, заданной уравнением  $x - by = 0$ .
16. Рассматривая эти прямые как некие *новые объекты*, мы можем ввести понятие умножения прямой на целое число. Если у нас есть прямая  $\{ax - by = 0\}$ , то результатом ее умножения на число  $k$  является прямая  $\{kax - by = 0\}$ . Запишем это так:

$$k\{ax - by = 0\} = \{(ka)x - by = 0\}.$$

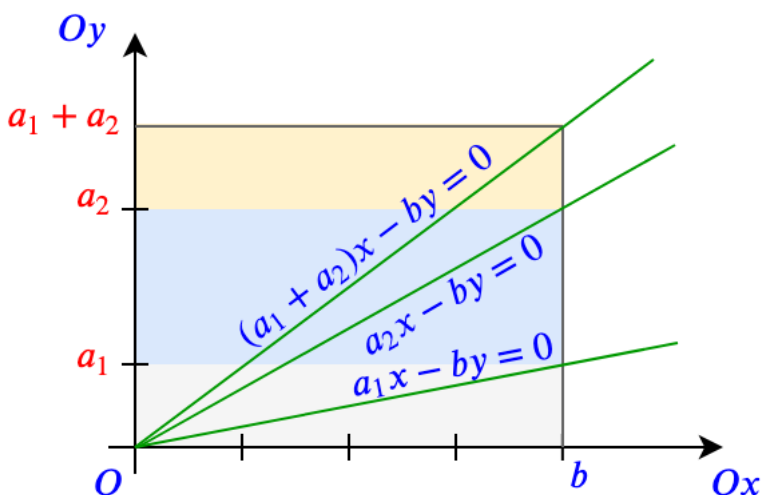
17. Заметим, что сложение (и вычитание) таких прямых определить еще проще:

$$\{a_1x - by = 0\} \pm \{a_2x - by = 0\} = \{(a_1 \pm a_2)x - by = 0\}.$$

**Важно:** при сложении прямых коэффициент перед  $y$  должен быть одинаковым у обеих прямых! Только в этом случае мы получаем согласование операций сложения и умножения, а именно:

$$\underbrace{\{ax - by = 0\} + \dots + \{ax - by = 0\}}_{k \text{ раз}} = \{kax - by = 0\} = k\{ax - by = 0\},$$

18. Сложение прямых можно интерпретировать графически как сложение площадей прямоугольников с основанием  $b$  и высотой  $a_1$  и  $a_2$ . В результате получается прямоугольник с тем же основанием  $b$  и высотой  $a_1 + a_2$ . При этом прямые всегда проходят через точку  $(0, 0)$  и правый верхний угол прямоугольников.



С помощью этой же картинки можно представить себе и умножение прямой на целое число  $k$ . Для этого нужно растиражировать соответствующий этой прямой прямоугольник вверх  $k$  раз.

19. На самом же деле операции сложения, вычитания и умножения на целое число, производимые с коэффициентом перед  $x$ , в точности повторяют таковые операции над целыми числами (поскольку это и есть целые числа!) и, соответственно, подчиняются всем аксиомам кольца целых чисел. [А вот и более умный термин для тех, кто собирается идти в математику глубоко: *прямые с общим основанием  $b$  образуют векторное пространство над кольцом  $\mathbb{Z}$ .*]
20. Поэтому все прямые вида  $ax - by = 0$  при фиксированном  $b \neq 0$  с определенными выше операциями сложения и умножения образуют кольцо (изоморфное кольцу целых чисел).
21. Если вместо сложной записи  $ax - by = 0$ , описывающей прямую, записать просто отношение  $a/b$ , то мы увидим, что операции с прямыми образуют в точности операции с дробями:

$$k \frac{a}{b} = \frac{ka}{b} \quad \text{и} \quad \frac{a_1}{b} + \frac{a_2}{b} = \frac{a_1 + a_2}{b}.$$

22. Заметим теперь, что уравнение  $x - by = 0$  прямой  $l$  можно переписать иначе:  $kx - (bk)y = 0$ . Чем оно отличается от уравнения  $kx - by = 0$  прямой  $l'$ ? Очевидно, тем, что перед  $y$  появился коэффициент  $k$ . А теперь вспомним, что прямая  $l$  задает отношение в  $k$  раз меньше, чем прямая  $l'$ ! И это значит, что если мы хотим разделить прямую  $l'$  на  $k$ , то мы должны умножить на  $k$  ее коэффициент перед  $y$ .

23. Итак, если мы хотим умножить прямую на число, то мы умножаем на это число коэффициент перед  $x$  (прямая становится более крутой), а если мы хотим разделить прямую на число, то мы умножаем на это число коэффициент перед  $y$  (прямая становится более пологой).

24. Делаем следующий шаг: умножение двух прямых. На самом деле, любую прямую  $ax - by = 0$  мы можем переписать как серию ранее определенных операций:

$$\{ax - by = 0\} = a\{x - y = 0\}/b,$$

при этом прямая  $x - y = 0$  имеет наклон 45 градусов и соответствует отношению 1/1, т.е. по-просту 1, и в операциях умножения может опускаться. Таким образом, умножение прямых выглядит следующим образом

$$\begin{aligned} & \{a_1x - b_1y = 0\} \cdot \{a_2x - b_2y = 0\} = \\ & = a_1\{x - y = 0\}/b_1 \cdot a_2\{x - y = 0\}/b_2 = \{a_1a_2x - b_1b_2y = 0\}, \end{aligned}$$

а это в точности умножение дробей:  $(a_1/b_1)(a_2/b_2) = (a_1a_2)/(b_1b_2)$ .

25. Отсюда нетрудно получить и процедуру деления прямых друг на друга:

$$\{a_1x - b_1y = 0\}/\{a_2x - b_2y = 0\} = \{(a_1b_2)x - (a_2b_1)y = 0\},$$

что соответствует операции с дробями:

$$\frac{a_1}{b_1} / \frac{a_2}{b_2} = \frac{a_1b_2}{a_2b_1}.$$

26. Наконец, чтобы научиться складывать произвольные прямые, мы должны уметь сводить сложение произвольных прямых к сложению прямых с одинаковым коэффициентом перед  $y$ , т.к. сложение мы определили выше только для данного случая.

27. Но и это не проблема:

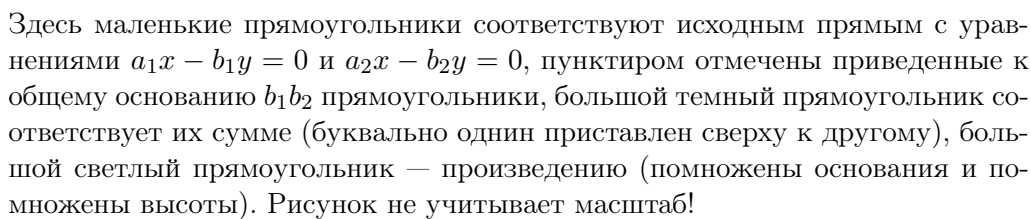
$$\begin{aligned} (a_1x - b_1y = 0) + (a_2x - b_2y = 0) &= (a_1b_2x - b_1b_2y = 0) + (a_2b_1x - b_1b_2y = 0) = \\ &= ((a_1b_2 + a_2b_1)x - (b_1b_2)y = 0), \end{aligned}$$

что соответствует операциям с дробями

$$\frac{a_1}{b_2} + \frac{a_2}{b_2} = \frac{a_1b_2 + a_2b_1}{b_1b_2}.$$

28. Следующая картинка показывает «арифметику прямых» с произвольными параметрами.





30. Итак, имея только множество целых чисел  $\mathbb{Z}$ , мы построили на плоскости всевозможные прямые, заданные линейными уравнениями с целыми коэффициентами, научились их складывать, вычитать, умножать и делить. Тем самым, мы построили новую алгебраическую структуру, которая называется **полем**. Поле — это кольцо, в котором можно делить на любое число, кроме нуля.
31. Записывая эти прямые не уравнениями, а отношением коэффициентов (вместо  $ax - by = 0$  пишем  $a/b$ ), мы получаем **поле рациональных чисел**, которое принято обозначать  $\mathbb{Q}$ .
32. На самом деле, в нашем построении есть еще и такая прямая, которая соответствует бесконечности. Это прямая, заданная уравнением  $x = 0$ . А нулевая прямая определяется уравнением  $y = 0$ . В полном соответствии с установленными правилами, мы можем заметить, что если  $a \neq 0 \neq b$ , то

$$\{ax - by = 0\}\{y = 0\} = \{y = 0\}, \quad \{ax - by = 0\}\{x = 0\} = \{x = 0\}, \\ \{ax - by = 0\}/\{y = 0\} = \{x = 0\}, \quad \{ax - by = 0\}/\{x = 0\} = \{y = 0\},$$

или, иначе:

$$\frac{a}{b} \cdot 0 = 0, \quad \frac{a}{b} \cdot \infty = \infty, \quad \frac{a}{b}/0 = \infty, \quad \frac{a}{b}/\infty = 0$$

при  $a \neq 0 \neq b$ , т.е. деление на ноль дает бесконечность, а деление на бесконечность дает ноль.

33. Но тут кроется проблема:  $\{x = 0\} \cdot \{y = 0\} = \{0x - 0y = 0\}$  — такое уравнение на задает прямую, его решением является вся плоскость! Проще говоря, при умножении  $0 \cdot \infty$  может получиться любое число!
34. Поэтому при определении поля бесконечный элемент не постулируется и, соответственно, деление на ноль не разрешено.
35. Приведем полный формальный список аксиом поля. Множество  $F$  с операциями  $+$  и  $\cdot$  называется **полем**, если:
- Field1**  $a, b \in F \Rightarrow a + b \in F, a \cdot b \in F$  (замкнутость операций);
- Field2**  $a, b, c \in F \Rightarrow (a + b) + c = a + (b + c), (a \cdot b) \cdot c = a \cdot (b \cdot c)$  (ассоциативность операций);
- Field3** для всех  $a, b \in F$  имеем  $a + b = b + a$  и  $a \cdot b = b \cdot a$  (коммутативность операций);
- Field4** существует элемент  $0 \in F$  такой, что  $a + 0 = 0 + a = a$  для всех  $a \in F$  (аксиома нуля);
- Field5** для всякого элемента  $a \in F$  существует противоположный  $-a$  такой, что  $a + (-a) = 0$  (аксиома противоположного элемента);

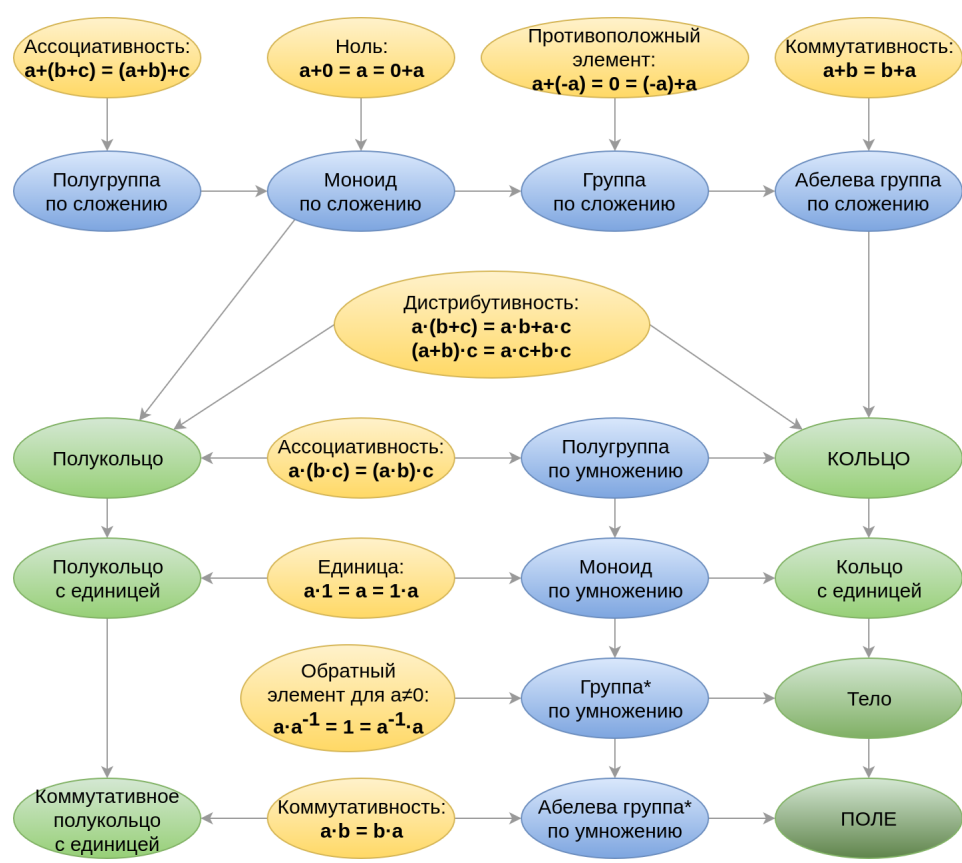
- Field6

существует элемент  $1 \in F$  такой, что  $a \cdot 1 = 1 \cdot a = a$  для всех  $a \in F$  (аксиома единицы),
- Field7

для всякого элемента  $a \in F$ , если  $a \neq 0$ , то существует обратный  $a^{-1}$  такой, что  $a \cdot a^{-1} = 1$  (аксиома обратного элемента).
- Field8

для всех  $a, b, c \in F$  имеем  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ ,  $c \cdot (a + b) = (c \cdot a) + (c \cdot b)$  (правая и левая дистрибутивность);

36. Иначе говоря, поле — это коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим. На следующей схеме представлено формирование таких понятий как поле и кольцо из более простых свойств (или аксиом):



### Задачи

## 10.2 Соизмеримость. Иррациональности

## Конспект

1. Рациональные числа мы построили с помощью прямых, заданных уравнением  $ax - by = 0$ , где  $a$  и  $b$  — произвольные целые числа, одновременно не равные нулю. Оказалось, что такая прямая отсекает отрезки длины  $a/b$  на вертикальной оси, когда  $x$  меняется с шагом 1, т.е. пробегает все целые числа. В частности, при  $x = 1$  мы получаем уравнение  $by = a$ , решением которого является единственное число  $y = a/b$ .
2. Говоря алгебраическим языком, рациональные числа — это корни линейных уравнений, т.е. уравнений вида  $a - by = 0$ , с целыми коэффициентами  $a, b$ .
3. Таким образом, выход в поле рациональных чисел происходит при попытке разрешить линейное уравнение, заданное над кольцом целых чисел.
4. Что если мы рассмотрим линейное уравнение, но над полем рациональных чисел? Будет ли оно разрешимо?
5. Пусть  $rx - q = 0$  и  $r, q \in \mathbb{Q}$ . Тогда представим эти рациональные числа в виде дробей  $r = a/b$ ,  $q = c/d$ , откуда

$$0 = rx - q = \frac{a}{b}x - \frac{c}{d} = \frac{adx - cb}{bd},$$

откуда ясно, что данное уравнение эквивалентно линейному уравнению  $(ad)x - (cb) = 0$  с целыми коэффициентами, а значит, разрешимо в поле рациональных чисел.

6. Таким образом, поле  $\mathbb{Q}$  замкнуто относительно линейных уравнений. Посмотрим, как оно справится с уравнениями более высокой степени! Рассмотрим уравнение  $x^2 - 2 = 0$ . Это уравнение с целыми коэффициентами (1 и 2). Разрешимо ли оно в  $\mathbb{Z}$  или хотя бы в  $\mathbb{Q}$ ?
7. Ответ: нет! Предположим, что  $x = n/m$  разрешает такое уравнение, т.е.  $(n/m)^2 = 2$ . Предположим сразу же, что  $n \perp m$ , т.е. дробь  $n/m$  несократимая. Далее имеем

$$n^2 = 2m^2.$$

Отсюда видно, что  $n^2$  делится на 2, а значит, 2 входит в разложение числа  $n^2$  по степеням простых. Проблема в том, что если бы 2 не входила в разложение числа  $n$ , то ее не было бы и в разложении числа  $n^2$ , т.к.  $n^2$  есть поризведение степеней тех же самых простых, что и  $n$ , только в удвоенной степени. А значит,  $n$  делится на 2, откуда следует, что  $n^2$  делится на 4. Но тогда  $m^2$  делится на 2 и, аналогично рассуждая, получаем, что и  $m$  делится на 2. А это уже противоречит тому, что дробь  $n/m$  несократимая — ее как минимум можно сократить на 2.

Следовательно, корень уравнения  $x^2 - 2 = 0$  не может быть рациональным числом.

8. Тем не менее, положительный корень такого уравнения можно оценивать сверху и снизу сколь угодно точно. Например, корень извлекается из числа 2.25 и равен 1.5, при этом  $x^2 = 2 < 2.25$ , так что  $x < 1.5$ . В то же время,  $2 > 1.96 = 1.4^2$ , так что  $x > 1.4$ . Можно еще усилить оценку:  $1.41 < x < 1.42$ . И так далее. Это позволяет нам думать, что на самом деле число такое есть, просто оно сидит где-то между рациональными числами. Обоснование его существования мы отложим на потом, а пока просто обозначим его  $\sqrt{2}$ .
9. Есть ее один способ удостовериться в том, что  $\sqrt{2}$  не является рациональным числом. И тут снова нам на выручку приходят цепные дроби. Теперь-то мы вправе ими оперировать!
10. Воспроизведем алгоритм Евклида для дроби  $\alpha = r_0/r_1$ , считая, что  $r_0 > r_1$  (если это не так, то приведем дробь к виду  $1/(r_1/r_0)$  и будем работать дальше только со знаменателем). Как и раньше, будем выделять остаток  $r_{k+1}$  от деления  $r_k - 1$  на  $r_k$  и сохранять неполное частное  $m_k$ . Только запишем весь алгоритм не в несколько строк, а в виде многоэтажной дроби. Поехали!

$$\begin{aligned} \frac{r_0}{r_1} &= \frac{k_1 r_1 + r_2}{r_1} = \boxed{k_1} + \frac{1}{\frac{r_1}{r_2}} = \boxed{k_1} + \frac{1}{\frac{k_2 r_2 + r_3}{r_2}} = \\ &= \boxed{k_1} + \frac{1}{\boxed{k_2} + \frac{1}{\frac{r_2}{r_3}}} = \boxed{k_1} + \frac{1}{\boxed{k_2} + \frac{1}{\boxed{k_3} + \dots + \frac{1}{\boxed{k_n} + \frac{1}{r_{n+1}/r_n}}}}, \end{aligned}$$

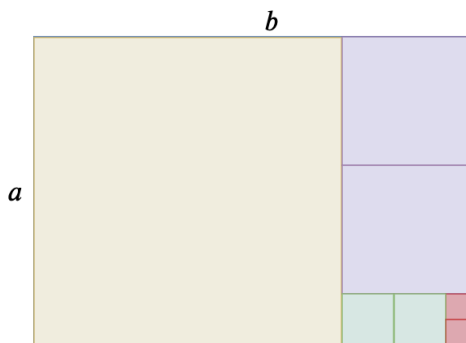
где  $r_0 > r_1 > r_2 > \dots > r_n > r_{n-1}$ .

11. Поскольку остатки всегда являются натуральными числами, рано или поздно этот алгоритм прервется. Пусть это случится на шаге с номером  $n$ , так что мы полагаем  $r_{n+1} = 0$ , и цепная дробь закончится на числе  $k_n$ .
12. В таком случае цепную дробь принято записывать последовательностью выделенных на каждом шаге целых частей:

$$\frac{r_0}{r_1} = [k_1, k_2, \dots, k_n].$$

13. Отсюда следует, что всякая рациональная дробь представима в виде конечной цепной дроби. Обратное, очевидно, также верно, ибо каждую конечную цепную дробь можно свернуть по правилам арифметики в обычную рациональную дробь.
14. Заметим также, что любое целое число представляется в виде тривиальной цепной дроби, в которой есть только  $k_1$ .

15. Алгоритм Евклида можно применять к любым числам, лишь бы можно было выделять остаток от деления. Например, его можно применить к паре чисел  $\pi/2$  и  $\pi/3$  и получить конечную цепную дробь. А все потому, что отношение этих чисел является рациональным числом  $3/2$ . Поэтому, если отношение двух чисел  $a/b$  рационально, их принято называть **соизмеримыми**.
16. Соизмеримые числа хорошо иллюстрируются следующей картинкой:



Видим, что прямоугольник  $a \times b$  мы делим на квадраты, каждый раз выбирая максимальный квадрат, который вписывается в оставшуюся область. Если  $a$  и  $b$  соизмеримы, то процесс разрезания прямоугольника на квадраты закончится за конечное число шагов, причем количество одинаковых квадратов, посчитанное в порядке их убывания, есть как раз те самые числа  $k_1, k_2, \dots, k_n$ , появляющиеся в записи цепной дроби. Поскольку вырезание максимального квадрата — это не что иное как процесс выделения целой части из остатка, т.е. алгоритм Евклида.

17. То, что сами числа  $a$  и  $b$  при этом могут не быть целыми или рациональными — не важно. Важно, что их отношение рационально. Также легко видеть, что всякое рациональное число соизмеримо с 1 и, наоборот, всякое число, соизмеримое с 1, рационально.
18. Посмотрим теперь, что происходит при попытке записать цепную дробь для  $\sqrt{2}$ .
19. Мы уже знаем, что  $1 < \sqrt{2} < 2$ , кроме того,  $(\sqrt{2} + 1) = 1/(\sqrt{2} - 1)$  так что

$$\begin{aligned} \sqrt{2} &= \boxed{1} + (\sqrt{2} - 1) = \boxed{1} + \frac{1}{1/(\sqrt{2} - 1)} = \boxed{1} + \frac{1}{\sqrt{2} + 1} = \\ &= \boxed{1} + \frac{1}{\boxed{2} + (\sqrt{2} - 1)} = \boxed{1} + \frac{1}{\boxed{2} + \frac{1}{\sqrt{2} + 1}} = \boxed{1} + \frac{1}{\boxed{2} + \frac{1}{\boxed{2} + \frac{1}{\sqrt{2} + 1}}} = \dots \end{aligned}$$

20. Как видим, остатком после выделения целой части всегда является одно и то же число  $\sqrt{2} - 1$ , и процесс алгоритма Евклида никогда не остановится. При этом цепная дробь характеризуется последовательностью одинаковых целых частей, равных 2. То есть представление для корня из 2 в виде цепной дроби будет бесконечным:

$$\sqrt{2} = [1, 2, 2, 2, 2, \dots],$$

и, следовательно,  $\sqrt{2}$  не является рациональным числом.

21. Числа, не являющиеся рациональными, называются **иррациональными**.
22. Наличие иррационального числа  $\sqrt{2}$  позволяет нам рассмотреть числа вида  $r + q\sqrt{2}$ , где  $r, q \in \mathbb{Q}$ .
23. Множество таких чисел, полученных присоединением к полю  $\mathbb{Q}$  положительного корня уравнения  $x^2 = 2$ , принято обозначать  $\mathbb{Q}[\sqrt{2}]$  и называть расширением поля  $\mathbb{Q}$ .

24. Очевидно, что множество  $\mathbb{Q}[\sqrt{2}]$  замкнуто относительно сложения и вычитания, т.к.

$$(r_1 + q_1\sqrt{2}) + (r_2 + q_2\sqrt{2}) = (r_1 + r_2) + (q_1 + q_2)\sqrt{2},$$

т.е. числом такого же вида.

25. Чуть сложнее увидеть, что и умножение и деление таких чисел имеют тоже вид  $r + q\sqrt{2}$ :

$$(r_1 + q_1\sqrt{2})(r_2 + q_2\sqrt{2}) = (r_1r_2 + 2q_1q_2) + (r_1q_2 + r_2q_1)\sqrt{2},$$

$$\begin{aligned} \frac{r_1 + q_1\sqrt{2}}{r_2 + q_2\sqrt{2}} &= \frac{(r_1 + q_1\sqrt{2})(r_2 - q_2\sqrt{2})}{(r_2 + q_2\sqrt{2})(r_2 - q_2\sqrt{2})} = \frac{(r_1r_2 - 2q_1q_2) + (r_2q_1 - r_1q_2)\sqrt{2}}{r_2^2 - 2q_2^2} = \\ &= \frac{r_1r_2 - 2q_1q_2}{r_2^2 - 2q_2^2} + \frac{r_2q_1 - r_1q_2}{r_2^2 - 2q_2^2}\sqrt{2}, \end{aligned}$$

т.е. в обоих случаях результат снова находится в  $\mathbb{Q}[\sqrt{2}]$ .

26. Это значит, что множество  $\mathbb{Q}[\sqrt{2}]$  с обычными операциями сложения и умножения является полем.
27. В поле  $\mathbb{Q}[\sqrt{2}]$  уравнение  $x^2 - 2 = 0$  разрешимо. Причем, в нем лежат оба корня данного уравнения:  $\sqrt{2}$  и  $-\sqrt{2}$ .
28. Отметим еще один важный факт. В поле  $\mathbb{Q}[\sqrt{2}]$  выражение  $x^2 - 2$  можно записать в виде произведения линейных членов  $(x - \sqrt{2})(x + \sqrt{2})$ , поскольку  $\sqrt{2}$  здесь стал разрешенным числом. Точно так же мы ранее сначала не могли записывать уравнения  $0.5x - 1 = 0$ , т.к. работали только с целыми числами (но могли заменить его эквивалентным уравнением  $x - 2 = 0$ ), а после выхода в поле  $\mathbb{Q}$  у нас появилась возможность использовать дробные коэффициенты.

29. Возникает резонный вопрос: а если уравнение какое-то более сложное? Например,  $x^5 + 3x^3 - 5 = 0$ . Всегда ли его можно разложить на линейные множители в поле  $\mathbb{Q}[\sqrt{2}]$ ? Или понадобится какое-то новое расширение  $\mathbb{Q}$ ? Иначе говоря, всегда ли будут корни такого уравнения лежать в построенных нами полях?
30. Ответ: нет. Но существует такое всеобъемлющее поле, в котором это действительно возможно. И постепенно мы дойдем до него...

Задачи

1. Разложите в цепную дробь числа  $9/5, 22/7, 3/13, 55/27$ .
2. Какое число и цепная дробь зашифрованы на картинке в пункте 16?
3. Найти цепную дробь для  $\sqrt{3}$ .
4. Найти цепную дробь для отношения

$$\frac{\sqrt{2} + 1}{\sqrt{2} - 1}.$$

Соизмеримы ли эти числа?

10.3 Поле вычетов по простому модулю

Конспект

1. Изучая числовые поля, невозможно обойти пример поля, который неявно уже появлялся у нас в главе 6.
2. При построении таблиц сложения и умножения по модулю  $m$ , мы заметили, что в таблице умножения появляются нули в тех и только тех строках, номера которых не взаимно просты с модулем  $m$ . Например, таблицы умножения остатков по модулям 7 и 8:

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1



3. Мы также выяснили, что если из кольца вычетов  $\mathbb{Z}_m$  выбросить все элементы, не взаимно простые с  $m$ , то полученное множество  $\mathbb{Z}_m^*$  станет группой по умножению. Правда, в этом случае нельзя гарантировать, что оно останется замкнутым относительно операции сложения. Например, в том же  $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$  сумма  $1 + 3 = 4 \notin \mathbb{Z}_8^*$ .
4. Тем не менее, есть случай, когда  $\mathbb{Z}_m^*$  включает все элементы  $\mathbb{Z}_m$ , кроме нуля. Очевидно, это должен быть тот случай, когда все числа  $1, 2, \dots, m-1$  взаимно просты с  $m$ . Но ведь это определение простого числа!
5. Таким образом, множество  $\mathbb{Z}_p$  при простом числе  $p$  удовлетворяет всем аксиомам поля, т.е. является полем.
6. Интересной особенностью поля  $\mathbb{Z}_p$  является то, что оно конечно.
7. Существуют и другие конечные поля, но их структура сложнее, чем у  $\mathbb{Z}_p$ . Эти поля можно получить присоединением корней специальных многочленов, примерно так же, как мы строили поле  $\mathbb{Q}[\sqrt{2}]$ . Известно, что любое конечное поле содержит  $p^k$  элементов, где  $p$  — простое число,  $k$  — натуральное.
8. Примеры конечных полей:

$$\mathbb{Z}_2, \quad \mathbb{Z}_3, \quad \mathbb{Z}_5, \quad \mathbb{Z}_{101}, \quad \mathbb{Z}_{2027}$$

# Начала комплексного анализа

## Аннотация.

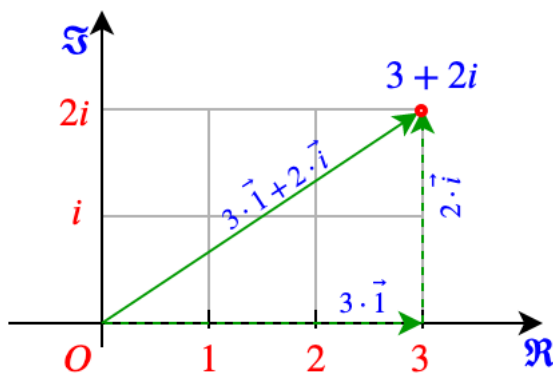
В этой главы мы начинаем строить поле комплексных чисел, пока еще без участия вещественных. По сути мы здесь работаем только с комплексными рациональностями, что, однако, не мешает показать тесную геометрическую связь комплексных чисел и движений плоскости, а также изучить числа Гаусса.

## 11.1 Алгебра комплексных чисел

### Конспект

1. Когда мы строили поле  $\mathbb{Q}[\sqrt{2}]$ , мы ввели в обращение новое число, которое позволяло решать уравнение  $x^2 = 2$ . Это число не является рациональным, но лежит где-то между рациональными числами. Тогда же мы задались вопросом, как быть с поиском корней других уравнений с целыми коэффициентами, неразрешимых в  $\mathbb{Q}$ .
2. Рассмотрим еще один пример уравнения:  $x^2 = -1$ .
3. Ворде бы, все коэффициенты — целые числа, и степень всего лишь вторая. Однако же, при детальном рассмотрении становится ясно, что у него нет решений не только в рациональных числах, но и где-то между ними, поскольку никакое известное нам число, возведенное в квадрат, и близко не подходит к  $-1$ .
4. Стало быть, если мы хотим ввести в обращение корень такого уравнения, то его необходимо поместить где-то вне числовой оси, «подвесить в воздухе».
5. Сделаем это из чисто эстетико-геометрических соображений. Как геометрически проявляют себя числа на прямой? Они обеспечивают сдвиг вдоль прямой: положительные — вправо, отрицательные — влево. Причем у всех этих сдвигов есть единица измерения — число 1, которая заодно выступает и в роли мультипликативной единицы, когда мы определяем умножение чисел. Кроме того, сдвиг на 1 вправо и затем влево (или в обратном порядке) приводит нас обратно, т.е. является сдвигом на 0, или  $\text{id}$ .

6. Новое же число мы хотим поместить так, чтобы оно обеспечивало сдвиг на плоскости, аналогичный сдвигу вдоль прямой.
7. Поскольку мы привыкли считать направление «вверх» положительным, поместим это число над числовой осью.
8. Заложим в этом числе сразу и единицу измерения: пусть оно отстоит от нуля на расстояние 1, тем самым мы согласуем масштаб сдвигов на плоскости со сдвигами на прямой. Наконец, сдвиг в направлении и на величину этой новой единицы не должен содержать в себе горизонтальных сдвигов, их проще добавить потом, взяв от сдвигов прямой, которые нам уже известны. Иначе говоря, числовая прямая при сдвиге на эту новую единицу должна сдвинуться вверх на расстояние 1 и таким образом, чтобы ее числовая разметка никуда не сдвинулась вправо или влево.
9. Так мы приходим к тому, что новую единицу сдвига следует отложить от нуля строго вверх на расстояние 1.
10. На координатной сетке она окажется в точке  $(0, 1)$ .
11. Назовем это новое число-вектор буквой  $i$ , которую принято называть **мнимой единицей** (от фр. *imaginaire*).
12. Теперь всякий сдвиг плоскости мы можем записать как композицию сдвига, выраженного в единицах (горизонтальный сдвиг), и сдвига, выраженного в мнимых единицах (вертикальный сдвиг). Просто по свойствам суммы векторов.
13. Иначе говоря, сдвиг на произвольный вектор  $\vec{z}$  мы распишем как сдвиг на сумму векторов  $x\vec{1} + y\vec{i}$ . См. рис.



14. Как и прежде, мы умеем отличать на плоскости векторы и точки. Векторы — это направленные отрезки, которые можно откладывать от точек. Сложе-

ние вектор означает их последовательное откладывание. В результате таких откладываний мы уходим от некоторой стартовой точки и приходим в какую-то финишную точку. Результирующий вектор соединяет стартовую и финишную точки. Договоримся для удобства считать стартовой точкой начало координат  $O$ , а финишную точку обозначать почти так же, как вектор, который в нее входит, только без векторной символики.

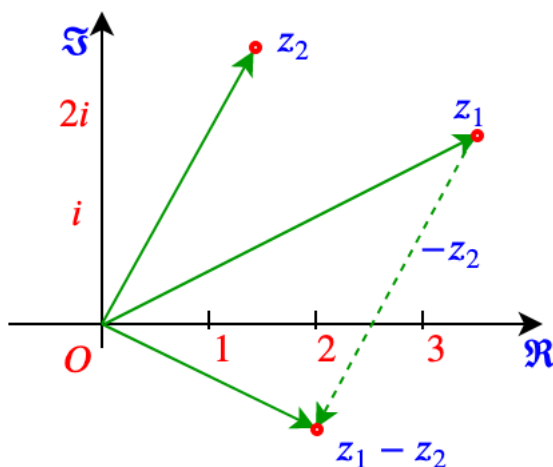
15. Итак, если вектор равен  $x\vec{1} + y\vec{i}$ , то его финишная точка обозначается  $x + yi$ .
16. Пока все, что мы сделали — это построили обычную арифметику векторов на плоскости. При чем же тут алгебраическая ипостась мнимой единицы, вытекающая из уравнения  $x^2 = -1$ ?
17. Алгебраическая ипостась  $i$  нам нужна как раз для того, чтобы построить алгебру точек плоскости, т.е. научиться их не только складывать и умножать на число, но еще и умножать и делить друг на друга.
18. Примем за аксиому, что с числами вида  $x + iy$  мы будем обращаться как с обычными числами, пользуясь аксиомами поля, и при этом пользоваться тем самым свойством мнимой единицы, которое ее определяет, т.е. равенством  $i^2 = -1$ .
19. Например,

$$(a + bi)(x + yi) = ax + ayi + bxi + byi^2 = (ax - by) + (ay + bx)i.$$

20. Числа вида  $z = x + iy$  с заданными операциями сложения и умножения (сложение — покоординатное, а умножение определено выше) называются **комплексными числами**. При этом  $x$  называется **действительной** (или вещественной) частью комплексного числа  $z$  и имеет также обозначение  $\Re z$ , а  $y$  называется **мнимой** частью числа  $z$  и имеет также обозначение  $\Im z$ .
21. Координатная ось  $Ox$  на комплексной плоскости называется действительной осью, а координатная ось  $Oy$  — мнимой.
22. Дадим следующие определения. Число  $\bar{z} = x - yi$  называется **комплексно сопряженным** к числу  $z = x + iy$ . Комплексное сопряжение — это отражение относительно действительной оси.
23. Модулем комплексного числа  $z = x + yi$  называется число

$$|z| = \sqrt{x^2 + y^2}.$$

Нетрудно видеть, что модуль комплексного числа — это длина соответствующего ему вектора (по теореме Пифагора). Кроме того, из геометрических соображений понятно, что  $|z_1 - z_2|$  — это расстояние между точками  $z_1$  и  $z_2$  на плоскости.



24. Посмотрим, какие арифметические свойства комплексных чисел можно извлечь.

**C1)**  $z\bar{z} = |z|^2$ . Действительно,  $(x + yi)(x - yi) = x^2 + y^2$ .

**C2)**  $z = 0$  (т.е.  $z = 0 + 0i$ ) тогда и только тогда, когда  $|z| = 0$ .

**C3)** Обратное по умножению число для  $z \neq 0$  существует и равно

$$z^{-1} = \frac{1}{x + yi} = \frac{x - yi}{(x + yi)(x - yi)} = \frac{\bar{z}}{|z|^2}$$

Это можно получить и напрямую из свойства C1.

**C4)** Мультипликативное свойство сопряжения:  $\overline{zw} = \bar{z}\bar{w}$ . Действительно,

$$\overline{(x + yi)(a + bi)} = \overline{(ax - by) + (ay + bx)i} = (ax - by) - (ay + bx)i$$

и

$$\overline{(x + yi)(a + bi)} = (x - yi)(a - bi) = (ax - by) - (ay + bx)i.$$

**C5)** Мультипликативное свойство модуля:  $|zw| = |z||w|$ . Действительно,

$$|zw|^2 = zw\bar{zw} = zw\bar{z}\bar{w} = z\bar{z}w\bar{w} = |z||w|.$$

25. Сложение с числом  $z = x + iy$  — это параллельный перенос  $T_{\vec{z}}$  на вектор  $\vec{z} = x\vec{1} + y\vec{i}$ . Это следует из геометрических свойств комплексных чисел, о которых мы говорили выше.

Кроме того, это легко проверить арифметически. Пусть даны две точки  $z_1$  и  $z_2$ . Добавим к ним вектор  $z$ , получим новые точки  $z'_1 = z_1 + z$  и  $z'_2 = z_2 + z$ . Во-первых, заметим, что расстояние сохранилось:

$$|z'_1 - z'_2| = |(z_1 + z) - (z_2 + z)| = |z_1 - z_2|,$$

т.е прибавление  $z$  — это движение. Во-вторых, если  $z \neq 0$ , то у этого движения нет неподвижных точек, иначе мы бы получили равенство  $z_1 + z = z_1$ , откуда  $z = 0$ . Следовательно, в силу теоремы Шаля прибавление  $z$  есть параллельный перенос. Прибавление  $z = 0$  есть  $\text{id}$ .

26. Умножение на комплексное число, по модулю равное 1, есть поворот с центром в нуле.

Пусть  $|z| = 1$ . Возьмем точки  $w_1 = a_1 + b_1i$  и  $w_2 = a_2 + b_2i$ , умножим их на  $z$ , получим точки  $w'_1 = w_1z$  и  $w'_2 = w_2z$ .

Найдем расстояние между  $w'_1$  и  $w'_2$ :

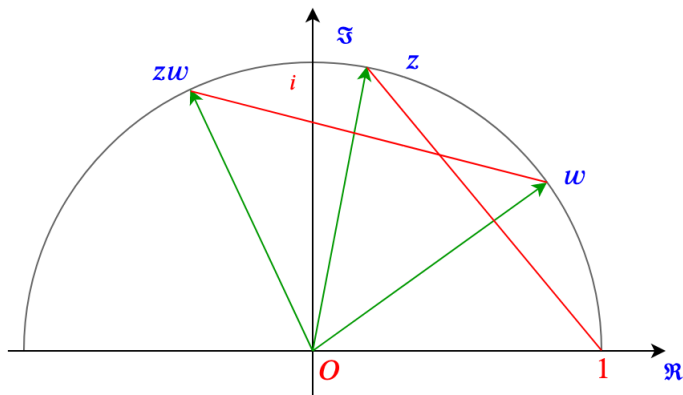
$$|w'_1 - w'_2| = |(w_1 - w_2)z| = |w_1 - w_2| \cdot |z| = |w_1 - w_2|,$$

т.е. умножение на  $z$  сохраняет расстояние. В то же время, очевидно, что при  $z \neq 1$  единственной неподвижной точкой при умножении будет  $w = 0$ , иначе мы бы получили  $wz = w$ , т.е.  $z = w/w = 1$ . Умножение на  $z = 1$  есть  $\text{id}$ .

Итак, умножение на число  $z$ , по модулю равное 1, является поворотом с центром в нуле. *Каков при этом угол поворота?*

Чтобы ответить на данный вопрос, рассмотрим для начала случай  $|w| = 1$ , т.е. точку с единичной окружности будем умножать на другую точку с единичной окружности. По свойствам модуля имеем  $|zw| = |z||w| = 1$ , т.е. в результате умножения мы вновь получим точку на единичной окружности! Иначе говоря, единичная окружность с операцией умножения комплексных чисел образует группу.

Теперь, заметим, что на окружности радиуса 1 хорда однозначно определяет опирающийся на нее угол. Рассмотрим углы, которые опираются на хорду  $[z; 1]$  и на хорду  $[zw; w]$ . На рисунке они выделены красным цветом.



Легко видеть, что длины хорд равны:  $|zw - w| = |z - 1||w| = |z - 1|$ , так что и углы равны. Следовательно, точка  $zw$  получается из точки  $w$  поворотом на угол, соответствующий углу наклона вектора  $z$  относительно положительного направления действительной оси.

Что происходит в случае, когда  $w$  не лежит на единичной окружности и отлична от нуля? Для этого представим произведение  $zw$  следующим образом:

$$zw = z \frac{w}{|w|} |w|,$$

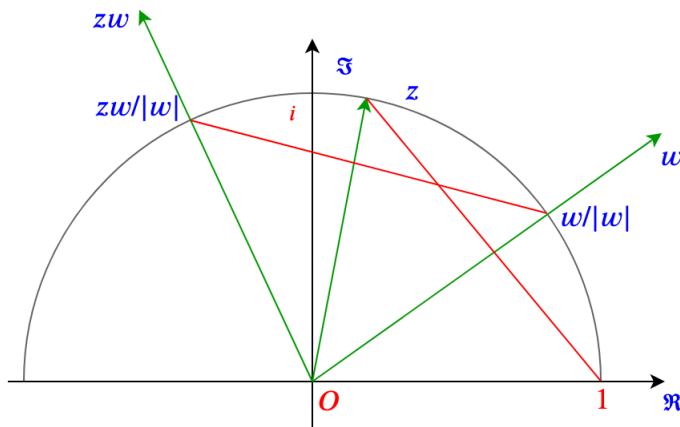
где отношение  $w/|w|$  уже является комплексным числом единичной длины. Следовательно, число  $zw/|w|$  получается из числа  $w/|w|$  его поворотом на угол, заданный числом  $z$ . Осталось выяснить, как связаны  $w$  с  $w/|w|$  и  $zw$  с  $zw/|w|$ .

В общем случае это означает, что мы имеем два комплексных числа, одно  $v$ , второе  $\lambda v$ , где действительное число  $\lambda > 0$ . Пусть  $v = a + bi$ . Вспомним уравнение прямой, проходящей через начало координат и точку  $(a, b)$ . Это уравнение имеет вид  $ay - bx = 0$ . А теперь умножим в этом уравнении обе части на  $\lambda$ , и получим  $(\lambda a)y - (\lambda b)x = 0$ . То есть точка  $\lambda v$  лежит на той же прямой, что и  $v$ .

Остался вопрос — с одной ли стороны относительно нуля они лежат? Чтобы это проверить, нужно сравнить длину их разности с суммой длин:

$$|\lambda v - v| = |v||\lambda - 1| < (1 + \lambda)|v| = |v| + |\lambda v|,$$

т.е. да, они лежат на одной прямой по одну сторону от нуля.



Итак, число  $zw$  получается следующим способом: сначала  $w$  переводится на единичную окружность нормировкой, т.е. делением на модуль, получается  $w/|w|$ . Затем оно поворачивается на угол, заданный числом  $z$ , затем оно

возвращается на свою орбиту, т.е. домножается на  $|w|$ . В итоге это есть не что иное, как поворот точки  $w$  на угол, заданный числом  $z$ .

27. Кстати, угол, заданный числом  $z$ , а в общем случае, числом  $z/|z|$  (если  $z$  — произвольное ненулевое комплексное число), называется **аргументом числа**  $z$  и обозначается  $\arg z$ .

28. Основные тригонометрические функции определяются с помощью комплексного числа с единичной окружности так: пусть задан угол  $\varphi$ . Повернем вектор  $(1, 0)$  на этот угол и найдем число  $z$  на единичной окружности такое, что  $\arg z = \varphi$ , тогда

$$\cos \varphi = \Re z, \quad \sin \varphi = \Im z.$$

29. Как уже отмечалось выше, операция комплексного сопряжения есть не что иное как отражение относительно действительной оси. Так что все базовые виды движений плоскости у нас представлены. Учитывая также, что поворот с произвольным центром можно представить как композицию сдвига, поворота с центром в нуле и обратного сдвига, а отражение относительно произвольной оси — как композицию поворота или сдвига, отражения относительно действительной оси и обратного поворота или сдвига, приходим к тому, что все движения плоскости можно выразить через три изученных нами действия с комплексными числами: сложение (произвольный сдвиг), умножение на число с единичной окружности (поворот с центром в нуле) и сопряжение (отражение относительно действительной оси).

30. На будущее у нас остается вопрос: *какое преобразование плоскости осуществляет умножение на произвольное ненулевое комплексное число?*

31. Поскольку мы пока знакомы только с рациональными дробями, комплексные числа у нас также являются рациональными, т.е. имеют вид  $\frac{a}{b} + \frac{c}{d}i$ , где  $a, b, c, d \in \mathbb{Z}$  и  $b, d \neq 0$ . Но даже при таком существенном ограничении мы уже имеем дело с еще одним полем — **полем комплексных рациональностей**, поскольку сложение, вычитание, умножение и деление не выводит нас за пределы этого множества (единственное исключение — модуль числа может выпасть из  $\mathbb{Q}$ ). Такое поле обозначается  $\mathbb{Q}[i]$  и является расширением поля  $\mathbb{Q}$ , аналогично полю  $\mathbb{Q}[\sqrt{2}]$ , рассмотренному ранее.

## Задачи

1. Докажите, что если  $\lambda > 0$ , то  $|\lambda - 1| < \lambda + 1$ .

## 11.2 Гауссовы целые числа



## Конспект

1. В этом разделе мы ограничимся рассмотрением комплексных чисел с целыми координатами, т.е. чисел вида

$$a + bi, \quad a, b \in \mathbb{Z}$$

Легко видеть, что такие числа образуют коммутативное кольцо с единицей. Данное кольцо обозначается  $\mathbb{Z}[i]$  и называется кольцом **гауссовых целых чисел**. На координатной плоскости точки  $\mathbb{Z}[i]$  сосредоточены в узлах целочисленной решетки.

2. Число  $a + bi$  **делится на**  $c + di$ , если существует число  $a' + b'i$  такое, что  $a + bi = (c + di)(a' + b'i)$ . Обозначение аналогично обычному в натуральных числах:  $(c + di)|(a + bi)$ . Например, число 2 делится на  $(1 + i)$ , т.к.  $2 = (1 + i)(1 - i)$ .
3. Нормой гауссова числа  $a + bi$  называется величина

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2,$$

т.е. норма числа  $z$  равна  $z\bar{z}$

Несколько свойств нормы:

**Norm1**  $N(a + bi) = 0$  тогда и только тогда, когда  $a = b = 0$ .

**Norm2** Нормы комплексно сопряженных чисел совпадают.

**Norm3** Если норма нечётна, то она имеет вид  $4k + 1$ , никакая норма не может быть равна  $4n + 3$ .

Поскольку  $N(a + bi) = a^2 + b^2$ , легко видеть, что она является нечетным числом только в том случае, когда  $a$  четное,  $b$  нечетное, либо наоборот.

Пусть  $a = 2k$ ,  $b = 2j + 1$ , тогда  $a^2 + b^2 = 4k^2 + 4j^2 + 4j + 1 = 1 \pmod{4}$ .

**Norm4**  $N(zw) = N(z)N(w)$ , где  $z, w$  — гауссовы числа.

Пусть  $z = a + bi$ ,  $w = c + di$ , тогда

$$N(zw) = N(ac - bd + i(ad + bc)) = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$$

$$N(z)N(w) = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2.$$

Последнее свойство означает, что делителями единицы (обратимыми элементами) могут быть только числа с нормой 1, т.е.  $\pm 1$  и  $\pm i$ . Других обратимых нет. Геометрически делителями единицы, являются те и только те гауссовы числа, которые лежат на единичной окружности. Отметим также, что все делители единицы образуют множество всех корней 4 степени из 1, т.е. корней уравнения  $x^4 = 1$ .

Наконец, множество  $\{1, -1, i, -i\}$  является группой по умножению, причем уже хорошо знакомой нам группой, если не обращать внимание на символ операции и символы элементов группы. Сравните таблицы «умножения двух групп»: этой и группы сложения вычетов по модулю 4  $\mathbb{Z}_4$ :

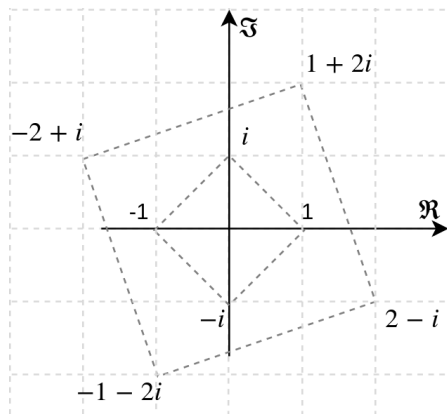
*	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Если произвести соответствие  $1 \mapsto 0$ ,  $i \mapsto 1$ ,  $-1 \mapsto 2$ ,  $-i \mapsto 3$ , а операции умножения поставить в соответствие операции сложения по модулю 4, то мы получим и полное соответствие между результатами умножения в первой группе и сложения во второй:  $i(-1) \mapsto 1 + 2$  и т.д.

В том случае, когда можно предъявить взаимно однозначное соответствие элементов двух групп так, чтобы операция в первой группе соответствовала операции во второй, говорят о том, что эти две группы **изоморфны**. Очень часто такие группы даже считают равными, хотя природа у них разная. Итак, группа по умножению обратимых гауссовых чисел изоморфна группе  $\mathbb{Z}_4$ .

- Все гауссовы числа делятся на делители единицы. Это легко понять из групповых свойств делителей единицы. Действительно, разделить на 1 означает умножить на нее, т.к. 1 сама себе обратна по умножению. Разделить на  $i$  означает умножить на  $-i$ , т.к. эти числа взаимно обратны по умножению. Аналогично, разделить на  $-1$  означает умножить на  $-1$ , и разделить на  $-i$  означает умножить на  $i$ .
- Делители единицы обладают еще одним замечательным свойством: умножение на них — это поворот относительно начала координат, причем умножение на  $i$  есть поворот на угол  $\pi/2$ , умножение на  $-1$  — поворот на угол  $\pi$  (т.е. центральная симметрия), умножение на  $-i$  — поворот на угол  $3\pi/2$  или  $-\pi/2$ . То есть делители единицы соответствуют еще и группе вращений квадрата.
- Два гауссовых числа называют **ассоциированными**, если одно получается из другого умножением на делитель единицы. Ассоциированность является отношением эквивалентности, причем каждый класс эквивалентности включает ровно 4 числа, расположенных в углах квадрата с центром в 0. Например,  $1 + 2i$ ,  $-2 + i$ ,  $-1 - 2i$  и  $2 - i$  ассоциированы.



7. Свойства делимости гауссовых чисел очень похожи на таковые свойства в арифметике натуральных чисел, но есть и отличия. Приведем несколько свойств:

**Div1** Если гауссово число  $a + bi$  делится на обычное целое число  $c + i0$ , то  $c|a$  и  $c|b$  в целых числах.

Это легко видеть из равенства  $a + bi = (x + yi)(c + i0) = xc + yci$ , откуда  $a = xc$  и  $b = yc$ .

**Div2** Если  $z|w$  и  $w|z$ , то  $z$  и  $w$  ассоциированы.

Пусть  $w = z'z$  и  $z = w'w$ , откуда  $N(w) = N(z')N(z)$  и  $N(z) = N(w')N(w)$ , откуда  $N(z')N(w') = 1$  и, следовательно,  $N(z') = N(w') = 1$ , поскольку в натуральных числах это единственное решение. Стало быть,  $z'$  и  $w'$  — делители единицы.

**Div3** Ассоциированность сохраняет делимость: если  $z$  и  $w$  ассоциированы,  $u$  и  $v$  ассоциированы, то  $(z|u) \rightarrow (w|v)$ .

Действительно, пусть  $z = z'w$  и  $u = u'v$ , где  $z', u'$  — делители единицы. Тогда

$$\frac{u}{z} = \frac{u'}{z'} \frac{w}{v},$$

так что если отношение  $u/z$  является гауссовым числом, то отношение  $v/w$  является ассоциированным с ним числом.

**Div4**  $z$  ( $N(z) > 1$ ) имеет как минимум 8 делителей: своих ассоциированных и ассоциированных с 1.

**Div5** Делители  $z$  являются делителями  $N(z)$ , если  $N(z)$  рассматривать как гауссово число.

Пусть  $w|z$ , т.е.  $z = uw$ . Поскольку  $N(z) = z\bar{z} = w(u\bar{z})$ , очевидно, что  $N(z)$  делится на  $w$ .

**Div6** Норма  $z = a + bi$  четна тогда и только тогда, когда  $(1 + i)|z$ , в частности, если  $a$  и  $b$  имеют разную четность, то  $z$  не делится на  $1 + i$ .

Для начала заметим, что норма  $z = a + bi$  четна тогда и только тогда, когда  $a$  и  $b$  имеют одинаковую четность, т.е. сравнимы по модулю 2. Далее, поскольку  $(1 + i)|z$ , существует  $c + di$  такое, что

$$a + bi = (1 + i)(c + di) = c - d + i(c + d),$$

т.е.  $a = c - d$ ,  $b = c + d$ , что равносильно  $a - b = -2d$ ,  $a + b = 2c$  при некоторых  $d \in \mathbb{Z}$ , а это равносильно тому, что  $a \equiv b \pmod{2}$ .

8. В кольце  $\mathbb{Z}[i]$  можно любое число  $u$  разделить на любое число  $v \neq 0$  с остатком, так что получится

$$u = qv + r, \quad N(r) < N(v). \quad (11.1)$$

При этом выбор чисел  $q$  и  $r$  можно строго ограничить, выбирая  $q$  как ближайшее гауссово число к комплексному  $u/v \in \mathbb{Q}[i]$ , а  $r$  как разность между  $u$  и  $qv$ . В случае, когда выбор  $q$  неоднозначен (может быть максимум 4 числа), можно договориться выбирать то, которое на координатной сетке находится левее и/или ниже.

Приведем один из вариантов вычисления  $r$ . Пусть  $u = a + bi$  и  $v = c + di$ . Далее оперируем в поле  $\mathbb{Q}[i]$ :

$$\frac{a + bi}{c + di} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} = q_1 + \frac{r_1}{c^2 + d^2} + q_2i + \frac{r_2}{c^2 + d^2}i,$$

где  $ac + bd = q_1(c^2 + d^2) + r_1$  и  $bc - ad = q_2(c^2 + d^2) + r_2$ . Здесь мы воспользовались делением с остатком в кольце  $\mathbb{Z}$ . При этом мы выбираем знаки  $r_1$  и  $r_2$  так, чтобы выполнялись неравенства:

$$|r_1|, |r_2| \leq (c^2 + d^2)/2.$$

Это всегда возможно, поскольку остатки от деления можно выбирать не только из ряда  $0, 1, 2, \dots, c^2 + d^2 - 1$ , но также из ряда  $0, \pm 1, \pm 2, \dots, \pm k$ , где  $k$  — целая часть от деления  $c^2 + d^2$  на 2, так что всегда  $k \leq (c^2 + d^2)/2$ . Здесь как раз и может оказаться вплоть до 4-х вариантов выбора.

Тогда

$$u = (q_1 + q_2i)v + \frac{(r_1 + r_2i)(c + di)}{c^2 + d^2} = (q_1 + q_2i)v + \frac{r_1 + r_2i}{N(v)},$$

эту последнюю дробь мы и выберем в качестве остатка  $r$ .

При этом заметим, что поскольку разность  $u - (q_1 + q_2i)v$  является гауссовым числом, то таковым же будет и число  $(r_1/N(v) + r_2i/N(v))v$ , хоть оно и выглядит нецелым.

Далее,

$$N\left(\frac{r_1}{N(v)} + \frac{r_2}{N(v)}i\right) = \frac{r_1^2 + r_2^2}{(c^2 + d^2)^2} \leq \frac{1}{2},$$

откуда  $N(r) \leq (1/2)N(v) < N(v)$ .

9. На основе деления с остатком нетрудно получить выполнимость алгоритма Евклида (см. раздел 4.2) для гауссовых чисел:

$$\begin{aligned} u &= q_1v + r_1, & N(r_1) &< N(v), \\ v &= q_2r_1 + r_2, & N(r_2) &< N(r_1), \\ r_1 &= q_3r_2 + r_3, & N(r_3) &< N(r_2), \\ &\dots\dots\dots \\ r_{n-1} &= q_{n+1}r_n + r_{n+1}, & N(r_{n+1}) &< N(r_n), \\ r_n &= q_{n+2}r_{n+1}, & N(r_{n+1}) &< N(r_n), \end{aligned}$$

поскольку норма является натуральным числом и не может убывать бесконечно.

Отсюда так же, как для целых чисел, выводится и представление  $\text{НОД}(u, v)$  в виде линейной комбинации исходных чисел  $u, v$ . Но мы докажем этот факт иным способом.

**Лемма 11.1.** *Для любых гауссовых чисел  $u, v \neq 0$  существует гауссово число  $r$  такое, что:*

- 1)  $r|u$  и  $r|v$  (общий делитель);
- 2) если  $(q|u) \wedge (q|v)$ , то  $q|r$  (наибольший общий делитель);
- 3) существуют гауссовы  $x, y$  такие, что  $r = xu + yv$ .

Кроме того,

- 4) число  $r$ , удовлетворяющее 1)–3), единственное с точностью до ассоциированности.

*Доказательство.* Рассмотрим множество  $R(u, v) = \{xu + yv \mid x, y \in \mathbb{Z}[i]\} \setminus \{0\}$ . В множестве норм  $\{N(z) \mid z \in R(u, v)\}$  существует наименьшее положительное число (т.к. нуля там быть не может). Пусть  $r \in R(u, v)$  такое число, у которого норма минимальная (оно может быть не единственным, выберем одно). Остается показать, что  $r$  — искомое.

Во-первых,  $r$  имеет вид  $xu + yv$  по построению, т.е. выполняется пункт 3). Во-вторых, если  $(q|u)$  и  $(q|v)$ , то очевидно, что  $q|r$  также по построению  $r$ , т.е. выполняется пункт 2).

Докажем пункт 1). Из (11.1) имеем:  $u = rt + s$ , где  $N(s) < N(r)$ . Подставляя представление  $r$ , имеем:  $u = xut + yvt + s$ , откуда  $s = (1 - xt)u + (-yt)v$ . Если  $s \neq 0$ , то  $s \in R$  как линейная комбинация  $u$  и  $v$ , но тогда  $N(s) \geq N(r)$  в силу выбора  $r$ , а это не так в силу (11.1). Следовательно,  $s = 0$ , откуда  $r|u$ . Аналогично,  $r|v$ .

Докажем пункт 4). Пусть  $r' = x'u + y'v$  также удовлетворяет свойствам 1)–3). Тогда  $r|r'$  и  $r'|r$ . Из первого следует, что  $r' = rt$  и  $N(r') = N(r)N(t)$ , из второго следует, что  $r = r't'$  и  $N(r) = N(r')N(t')$ . Таким образом, нормы  $N(t)$  и  $N(t')$  взаимно обратны в натуральных числах, откуда следует  $N(t) = N(t') = 1$ , т. е.  $t$  — делитель 1 и, следовательно,  $r$  и  $r'$  ассоциированы.  $\square$

10. Доказанная лемма позволяет определить понятие НОД для гауссовых чисел с точностью до ассоциированности. В качестве НОД мы будем выбирать какое-то одно из четырех (наиболее удобного вида).
11. Гауссово число называется **простым**, если оно не имеет никаких делителей, кроме тривиальных (ассоциированных с 1 и самим собой), и не является делителем 1, т. е. простое гауссово число имеет ровно 8 делителей. Два гауссовых числа называются **взаимно простыми** (обозначается  $u \perp v$ ), если их НОД — обратимое число, т. е. 1 и ассоциированные с ней.
12. Верны следующие свойства простых гауссовых чисел:

**Prim1** Если  $a + bi$  простое, то  $a - bi$  также простое.

Действительно, если  $a - bi = uv$ , где  $u, v$  не ассоциированы с 1, то  $a + bi = \bar{u}\bar{v}$ , где  $\bar{u}$  и  $\bar{v}$  не ассоциированы с 1 (т.к. для делителей нуля сопряжение не нарушает ассоциированности), нотогда  $a + bi$  не является простым.

**Prim2** Если  $z$  простое, то его ассоциированные также простые.

**Prim3** Если  $z$  простое и  $z|uv$ , то  $(z|u) \vee (z|v)$ ;

Действительно. Пусть простое  $z|uv$ . Предположим, что  $\neg(z|u)$ , тогда  $z \perp u$ , откуда по лемме 11.1 получаем, что  $1 = xz + yu$ . Умножаем на  $v$ :  $v = xzv + yuv$ . Справа оба слагаемых делятся на  $z$ , следовательно,  $z|v$ . Аналогично, если  $\neg(z|v)$ , то  $z|u$ .

**Prim4** Норма простого, неассоциированного с  $1 + i$ , всегда нечетна, т. е. имеет вид  $4k + 1$ .

Это следует из свойства Div6. Если простое число не ассоциировано с  $1 + i$ , то оно и не делится на него, а значит, по свойству Div6 его норма нечетная. То, что она имеет вид  $4k + 1$ , следует из  $(2k)^2 + (2n + 1)^2 = 4m + 1$ .

**Prim5** Натуральное простое не всегда есть гауссово простое:  $5 = (2 + i)(2 - i)$ .

**Prim6** **Критерий Гаусса:**

**Теорема 11.1.**  $a + bi$  простое тогда и только тогда, когда

1) либо одно из чисел  $a, b$  нулевое, а второе — простое целое числа вида

$$\pm(4k+3) \ (k > 0),$$

2) либо  $a, b$  ненулевые и норма  $N(a+bi) = a^2+b^2$  — простое натуральное число.

**Prim7 Следствие:** простое натуральное вида  $4k+1$  не может быть простым гауссовым, простые натуральные вида  $4k+3$  являются простыми гауссовыми.

**Prim8** Простое натуральное  $4k+1$  можно представить как сумму квадратов  $a^2+b^2$  (**рождественская теорема Ферма**).

**Prim9** Если  $N(z) \perp N(w)$  в натуральных числах, то  $z \perp w$  в гауссовых числах. Пусть  $u = \text{НОД}(z, w)$  в гауссовых числах. Тогда  $z = ut$ ,  $w = ut'$  и  $N(z) = N(u)N(t)$ ,  $N(w) = N(u)N(t')$ . Откуда  $N(u)|N(z)$  и  $N(u)|N(w)$ . Тогда из условия  $N(z) \perp N(w)$  следует, что  $N(u) = 1$ , т. е.  $u$  — ассоциированное с 1 гауссово число. Откуда  $z \perp w$ .

Примеры простых гауссовых чисел:  $\pm 3, \pm 7, \pm 3i; 1 \pm i, 1 \pm 2i, 1 \pm 4i$ .

13. Для гауссовых чисел существует аналог основной теоремы арифметики (см. раздел 4.3):

**Теорема 11.2** (Основная теорема арифметики гауссовых чисел).

*Каждое ненулевое неассоциированное с 1 гауссово число раскладывается на гауссовы простые множители, причем это разложение единственно с точностью до ассоциированных с этими множителями простых и порядка множителей, т. е. разложение имеет вид*

$$\alpha_1^{s_1} \dots \alpha_n^{s_n} = \beta_1^{s_1} \dots \beta_n^{s_n},$$

где пары  $\alpha_i, \beta_i$  являются ассоциированными простыми числами, а степени  $s_i$  — натуральными числами.

Доказательство теоремы прямо следует из свойства Prim3.

Пример:  $5 = (2+i)(2-i) = (1+2i)(1-2i)$  (множители переводятся друг в друга умножением на  $i$  и на  $-i$ ).

14. Из ОТА легко выводится следующее утверждение

**Лемма 11.2.** *Если  $(u \perp v) \wedge (uv = c^n)$ , то существуют  $a \perp b$  такие, что  $u = a^n$  и  $v = b^n$  и  $c = ab$ .*

Заметим, что и в обычной арифметике целых чисел верна такая же лемма. Более того, как основная теорема арифметики 11.2, так и лемма 11.2 верны в любом **евклидовом кольце** (т. е. в таком кольце, где возможно деление с остатком в виде (11.1) при некоторой натурально-значной норме и, как следствие, алгоритм Евклида). Этим свойством евклидовых колец мы еще воспользуемся в дальнейшем.

15. Рассмотрим парочку примеров, где числа Гаусса дают заметный выигрыш по скорости и простоте решения задач, связанных с уравнениями в целых числах, т.е. **диофантовыми уравнениями**.

16. Рассмотрим уравнение

$$x^2 + 1 = y^3, \quad x, y \in \mathbb{Z}.$$

В гауссовых числах оно эквивалентно уравнению

$$(x + i)(x - i) = y^3.$$

17. Покажем, что  $x + i \perp x - i$ . Действительно, если это не так, т.е.  $z|x + i$  и  $z|x - i$ , то  $z|(x + i) - (x - i) = 2i$ , откуда  $z = 1 + i$  или ему ассоциированное. Кроме того,  $z|y^3$ , причем, поскольку  $1 + i$  — простое, оно должно входить в разложение  $y^3$  трижды, т.е.  $z^3|y^3$ , но тогда в разложение  $x + i$  или  $x - i$  входит  $z^2 = 2i$ , чего быть не может, т.к.  $x \pm i$  не делится на 2 (см. свойство Div1). Следовательно,  $x + i \perp x - i$ .

18. Из предыдущего и леммы 11.2 следует, что существует число  $a + bi$  такое, что  $x + i = (a + bi)^3$ . Возводя в куб и сравнивая коэффициенты при  $i$ , находим, что  $1 = b(a^2 - b^2)$ . Это — уравнение в целых числах, поэтому  $b = \pm 1$ , откуда  $a^2 = 0$  или 2. Но  $a^2 = 2$  неразрешимо в целых числах, поэтому  $a = 0$ , откуда  $x = 0$ . Таким образом, единственно возможное решение в целых числах у исходного уравнения  $x^2 + 1 = y^3$  — это  $x = 0, y = 1$ .

19. Рассмотрим **Теорему Ферма** при  $n = 2$ :  $a^2 + b^2 = c^2$  (в натуральных числах). Ясно, что можно сразу считать, что все числа  $a, b, c$  попарно взаимно простые натуральные числа (иначе можно было бы сократить уравнение на общий множитель). Отсюда также следует, что  $a$  и  $b$  имеют разную четность. Действительно, если  $a$  и  $b$  четные, то таково же и  $c$ , а значит, они не взаимно простые. Если  $a$  и  $b$  нечетные, то  $a^2 + b^2$  имеет остаток 2 при делении на 4, но  $c^2$  может иметь остаток либо 0 (четное), либо 1 (нечетное). Таким образом, допускается только случай, когда  $a$  и  $b$  имеют различную четность. Тогда по свойству Div6 число  $a + bi$  не делится на  $1 + i$ .

20. Заметим, что  $(a + bi)(a - bi) = a^2 + b^2 = c^2$ . Предположим, что НОД чисел  $a + bi$  и  $a - bi$  равен  $r$  и отличен от делителя 1. Тогда  $r|2a$  и  $r|2bi$ . Но  $a \perp b$  в натуральных числах, тогда  $N(a) \perp N(b)$ , откуда по свойству Prim9  $a \perp b$  в гауссовых числах. Это значит, что  $r$  есть НОД 2 и  $2i$ , т.е.  $r = 1 + i$  или его ассоциированным. Но такое число не может быть делителем  $a + bi$  и  $a - bi$  по доказанному выше. Следовательно,  $(a + bi) \perp (a - bi)$ .

21. Тогда по лемме 11.2 существуют такие  $z, w$ , что  $a + bi = z^2$ ,  $a - bi = w^2$  и  $c = zw$ . Пусть  $z = n + mi$ , тогда  $a + bi = n^2 - m^2 + 2nmi$ , откуда  $a - bi = n^2 - m^2 - 2nmi$ , откуда  $w = n - mi$  и  $c = n^2 + m^2$ .



22. Таким образом, мы получаем формулу **пифагоровых троек**:

$$a = n^2 - m^2, \quad b = 2nm, \quad c = n^2 + m^2,$$

где натуральные  $n, m > 0$ .

23. Рассмотрим теперь уравнение  $x^4 + y^4 = z^4$ , неразрешимость которого доказал еще сам Ферма методом, который мы покажем ниже.

24. Докажем более сильное утверждение:  $x^4 + y^4 = z^2$  неразрешимо в целых положительных числах.

25. Как и прежде, считаем сразу же, что  $x \perp y$ . Посмотрим на это уравнение как на уравнение второй степени:  $(x^2)^2 + (y^2)^2 = z^2$ . Если оно разрешимо, то существуют ненулевые взаимно простые  $n, m$  такие, что

$$x^2 = n^2 - m^2, \quad y^2 = 2nm, \quad z = n^2 + m^2,$$

откуда вновь получаем уравнение второй степени  $x^2 + m^2 = n^2$ , а значит, его решение имеет вид:

$$x = a^2 + b^2, \quad m = 2ab, \quad n = a^2 + b^2,$$

где ненулевые  $a \perp b$ . Тогда для  $y$  имеет место равенство:  $y^2 = 4nab$  и, поскольку число 2 простое (в обычных целых числах),  $y = 2y'$ .

Тогда  $(y')^2 = nab$ . Так как  $n, a, b$  попарно взаимно просты (это следует из того, что  $a \perp b$  и  $n = a^2 + b^2$ ), в силу леммы 11.2 (для обычных целых чисел) существуют такие  $s, t, k$ , что  $n = s^2$ ,  $a = t^2$ ,  $b = k^2$ . Подставляем это в равенство  $n = a^2 + b^2$ , получаем:

$$t^4 + k^4 = s^2,$$

где  $t \perp k$  и  $z > s > 0$  (это следует из того, что  $s = \sqrt{n}$ ,  $n^2 < z$ ).

Таким образом, имея одно решение  $(x, y, z)$  исходного уравнения, мы построили еще одно  $(t, k, s)$ , где  $s < z$ . Продолжая применять эти построения далее, мы получим бесконечную последовательность решений  $(t_j, k_j, s_j)$  такую, что  $z > s > s_1 > s_2 > \dots$ . Но это невозможно, т. к. в натуральном ряде не существует бесконечная строго убывающая последовательность.

26. Полученное противоречие доказывает неразрешимость уравнения  $x^4 + y^4 = z^2$  в целых положительных числах, а значит, и неразрешимость уравнения  $x^4 + y^4 = z^4$ . Заметим, что отсюда сразу же следует справедливость теоремы Ферма для всех степеней  $n$ , кратных 4.

27. Предъявленный здесь метод доказательства называется **методом бесконечного спуска**. Он напоминает индукцию, только не доказующую, а опровергающую, поскольку приводит к противоречию.

## Задачи

# Некоторые иррациональности

## Аннотация.

В этой главе мы заглянем за пределы поля рациональных чисел при помощи многочленов с рациональными коэффициентами, построим поле алгебраических чисел, разберем некоторые теоремы о многочленах над кольцами и полями.

## 12.1 \*Упорядоченные множества

### Конспект

1. Ранее мы определяли **отношение на множестве**  $A$  как произвольное подмножество  $R \subseteq A \times A$ .
2. Рассмотрим здесь частный случай отношений: **отношения порядка**.
3. Вспоминая изучение движений прямой, скажем, что точка  $X$  на прямой **больше**, чем точка  $Y$ , если  $X$  находится правее, чем  $Y$ . Иначе это можно сформулировать так: если  $X = T_a(Y)$ , где  $a$  — вектор движения вправо, т.е. положительный вектор. То есть,  $X > Y$  (или  $Y < X$ ), если  $X$  получается смещением  $Y$  в положительном направлении.
4. Симметрично рассуждая, получаем, что  $X < Y$ , если  $X$  находится левее  $Y$ , либо если из точки  $Y$  можно попасть в  $X$  сдвигом влево.
5. Пользуясь этим наглядным представлением, легко получить следующие свойства сравнения:

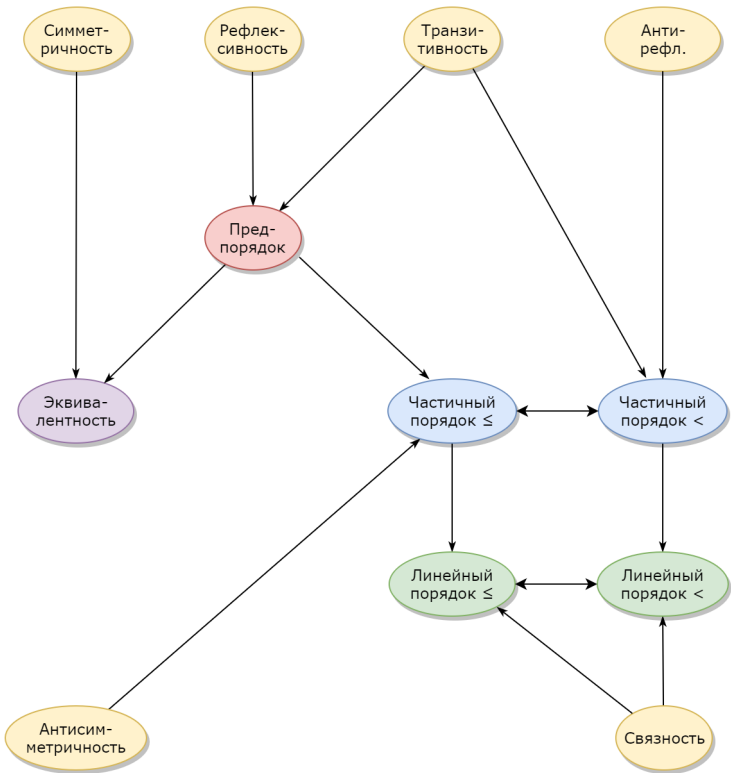
**Rel1** если  $X < Y$  и  $Y < Z$ , то  $X < Z$  (транзитивность отношения  $<$ );  
Это достаточно очевидно, поскольку сдвиг  $T_{XZ}$  есть композиция положительных сдвигов  $T_{XY}$  и  $T_{YZ}$ .

**Rel2** для любой точки  $X$  не верно, что  $X < X$  (антирефлексивность);  
Это также довольно-таки очевидно, т.к. сдвиг, сотавляющий на месте  $X$ , является  $\text{id}$ , а не положительным сдвигом.

**Rel3** для любых точек  $X, Y$  имеет место одно из трех отношений:  $X < Y$  или  $X = Y$  или  $X > Y$  (связность).

Это следует из того, что если  $X \neq Y$ , то можно построить вектор  $\vec{XY}$ , а он может смотреть либо влево, либо в право, что и будет соответствовать оставшимся двум сравнениям. Заметим сразу, что для любой пары точек всегда выполняется только одно из трех отношений, поскольку равенство  $X = Y$  исключает неравенства  $X < Y$  и  $Y < X$  в силу свойства антирефлексивности, а неравенство  $X < Y$  исключает неравенство  $Y < X$ , т.к. иначе по свойству транзитивности мы бы получили  $X < X$ , что противоречит антирефлексивности.

- Транзитивное антирефлексивное связанное отношение на множестве называется **линейным порядком**, а само множество, на котором задан линейный порядок, называется **линейно упорядоченным**.
- Ранее мы уже определяли отношение эквивалентности как рефлексивное транзитивное симметричное отношение (см. раздел6.4). Ниже представлена графическая схема того, из каких понятий формируются отношение эквивалентности и линейного порядка.



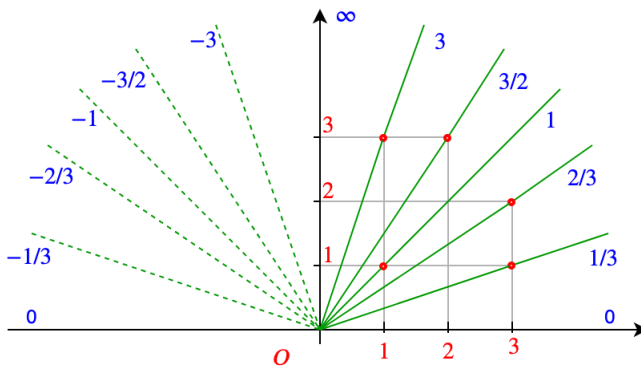
Обратим внимание на то, что отношение линейного порядка здесь представлено в двух ипостасях: как антирефлексивное транзитивное и связное отношение, а также как рефлексивное антисимметричное транзитивное и связное отношение. Первый случай соответствует отношению строгого порядка ( $<$ ), второй — нестрогого ( $\leq$ ). Можно доказать, что это на самом деле одно и то же с точностью до исключения равенства.

**Лемма 12.1.** *Отношение  $<$  является отношением строгого линейного порядка тогда и только тогда, когда отношение  $\leq ((x \leq y) \Leftrightarrow (x < y) \vee (x = y))$  является отношением нестрогого линейного порядка.*

В дальнейшем под термином «линейный порядок» мы будем понимать именно строгий линейный порядок, а нестрогим будем делать его, используя знак  $\leq$  и ему подобные.

8. Множества  $\mathbb{N}$  и  $\mathbb{Z}$  упорядочены естественным образом: числа, стоящие правее, больше, чем их левые собратья.
9. Множество  $\mathbb{Q}$  мы, на самом деле, упорядочили еще во время его построения, когда говорили о наклоне прямой, задающей рациональное число: чем круче наклон, тем больше число. Но это верно только для положительных дробей. С отрицательными числами все наоборот (в полной аналогии с целыми числами!) — чем круче наклон, тем меньше число.
10. Это же можно записать и более формально: если  $b > 0$  и  $d > 0$ , то

$$\frac{a}{b} < \frac{c}{d} \Leftrightarrow ad < bc$$



11. Если на множестве  $L$  задан линейный порядок  $<$ , то **интервалом**  $(x; y)$  называется множество всех точек множества  $L$ , лежащих между  $x$  и  $y$ :

$$(x; y) = \{z \in A \mid x < z < y\}$$

В частности, если  $x > y$ , то интервал  $(x; y)$  пуст. На множестве  $\mathbb{Z}$  имеем следующие примеры:

$$(0; 1) = \emptyset, \quad (0; 2) = \{1\}, \quad (0; n+1) = \{1, 2, \dots, n\}.$$

12. Линейный порядок  $<$  называется **плотным**, если между любыми двумя элементами всегда есть третий:

$$\forall x, y \in L (x < y) \rightarrow \exists z (x < z < y),$$

т.е. когда любой интервал  $(x; y)$  непуст при условии, что  $x < y$ .

13. Линейно упорядоченное множество с плотным линейным порядком называется **плотным линейно упорядоченным множеством**.

14. Подмножества линейно упорядоченного множества можно сравнивать. Пусть множество  $L$  линейно упорядочено отношением  $<$ , тогда для его подмножеств  $X, Y \subseteq L$  положим

$$X < Y \Leftrightarrow \forall x \forall y (x \in X) \wedge (y \in Y) \rightarrow (x < y),$$

т.е. когда все точки множества  $X$  меньше всех точек множества  $Y$ .

15. Нетрудно проверить, что отношение  $<$  на подмножествах  $L$  транзитивно и антирефлексивно. Однако же легко привести пример, когда множества могут быть несравнимы между собой, например, в качестве  $X$  взять все четные числа, а в качестве  $Y$  — все нечетные числа. Несмотря на то, что эти множества не пересекаются, невозможно сказать, что  $X < Y$  или что  $Y < X$ , и уж тем более неверно  $X = Y$ . Таким образом, отношение  $<$ , определенное на подмножествах  $L$  не является линейным порядком.

16. Про отношение, которое является транзитивным и антирефлексивным, говорят, что оно является **частичным порядком**.

17. Если множество снабжено частичным порядком, то оно называется **частично упорядоченным множеством**.

18. Сравнения множеств, как и операции Минковского над ними, удобны тем, что сокращают длинные формальные выкладки, а кроме того, образно очень хорошо воспринимаются: одно множество меньше другого, если оно целиком лежит левее другого.

19. Пусть  $(L, <)$  — линейно упорядоченное множество и  $A, B \subset L$ , причем  $A \neq \emptyset$ ,  $B \neq \emptyset$ ,  $A \cap B = \emptyset$ ,  $A \cup B = L$ ,  $A \leq B^1$ . Тогда пара  $(A, B)$  называется **сечением** множества  $L$ ,  $A$  — нижним классом сечения,  $B$  — верхним классом сечения.

---

<sup>1</sup>Здесь и далее сравнение множеств означает сравнение их элементов с квантором всеобщности:  $X \leq Y$  ( $X < Y$ ) означает, что  $\forall x \in X \forall y \in Y : x \leq y$  ( $x < y$ ). То же относится к сравнению множества и элемента:  $c \leq Y$ .

20. Линейный порядок  $<$  на множестве  $L$  называется **непрерывным** (множество  $L$  с таким порядком непрерывно), если каково бы ни было его сечение, либо в нижнем классе сечения существует наибольший элемент, а в верхнем нет наименьшего, либо в верхнем классе существует наименьший элемент, а в нижнем нет наибольшего (такие сечения называются **дедекиндовыми**). Такое свойство линейного порядка еще называется **аксиомой непрерывности** или аксиомой полноты.
21. Отметим, что плотное линейно упорядоченное множество не всегда непрерывно. Например,  $\mathbb{Q}$  плотно, но не непрерывно (сечение для  $\sqrt{2}$  не является дедекиндовым).<sup>2</sup>
22. Завершим этот раздел соединением двух разнородных понятий: алгебраической структуры и отношения.
23. Пусть имеется числовая структура с операциями  $+$  (сложение) и  $\cdot$  (умножение), причем символ  $0$  обозначает в ней нейтральный элемент по сложению. Пусть также на этой структуре задано отношение  $<$  линейного порядка. Говорят, что **отношение  $<$  согласовано с операцией  $+$** , если выполнено условие:

**Rel4** Если  $a \leq b$ , то  $a + c \leq b + c$  (и  $c + a \leq c + b$ ) для любых чисел  $a, b, c$  из данной структуры.

Говорят, что **отношение  $<$  согласовано с операцией  $\cdot$** , если выполнено условие:

**Rel5** Если  $a \geq 0$  и  $b \geq 0$ , то  $ab \geq 0$ .

Соответственно, если на элементах группы  $(G, +)$  задан линейный порядок  $<$ , согласованный с групповой операцией, то структура  $(G, +, <)$  называется **линейно упорядоченной группой**. Пример такой группы — группа целых чисел по сложению с обычным порядком.

Если на элементах кольца  $(K, +, \cdot)$  задан линейный порядок, согласованный с операциями кольца, то структура  $(K, +, \cdot, <)$  называется **упорядоченным кольцом**. Пример такого кольца — кольцо целых чисел с обычным порядком.

Наконец, если на элементах поля задан линейный порядок, согласованный с его операциями, то такая структура называется **упорядоченным полем**. Пример такого поля — поле рациональных чисел с обычным порядком.

---

<sup>2</sup>ВНИМАНИЕ! Термин «дедекиндово сечение» в разных источниках определяется по-разному, хотя все эти определения эквивалентны. Часто в качестве сечения берется не пара множеств, а только нижний класс сечения.

Безусловно, самым «продвинутым» для нас на текущий момент понятием является *непрерывное упорядоченное поле*, т.е. поле с непрерывным линейным порядком, согласованным с операциями сложения и умножения. Именно построение такого уникального поля является основной целью нашего курса.

## Задачи

1. Пусть множество  $X$  не пусто. Верно ли, что  $\emptyset < X$ ? Верно ли, что  $X < \emptyset$ ? Верно ли, что  $\emptyset < \emptyset$ ?
2. Каким отношением (антирефлексивным, транзитивным, связным) является отношение несобственного вложения множеств?  $X$  есть несобственное подмножество  $Y$  (обозначение:  $X \subset Y$ ), если  $X \subseteq Y$  и  $X \neq Y$ .
3. Каким отношением является отношение делимости  $x|y$  на положительных целых числах?
4. Является ли всюду плотным множество всех десятично рациональных чисел, т.е. чисел вида  $k/10^n$ , где  $k \in \mathbb{Z}$  и  $n \in \mathbb{N}$ ?
5. Выпишите полный список аксиом упорядоченного поля.

## 12.2 Плотные множества

### Конспект

1. Вернемся к анализу поля рациональных чисел  $\mathbb{Q}$ . Данное поле интересно тем, что какие бы два различных числа мы ни взяли, между ними всегда найдется третье рациональное число. Действительно, пусть есть две дроби  $r = n/m$  и  $q = t/s$ , тогда их среднее арифметическое  $(r + q)/2$  является рациональным числом и лежит строго между ними.
2. Таким образом, множество рациональных чисел с обычным отношением сравнения является плотным линейно упорядоченным множеством.
3. К определению понятия плотного множества существует и другой, топологический подход. Пусть  $A \subseteq B$ , где  $B$  — линейно упорядоченное множество. Говорят, что множество  $A$  **плотно в  $B$** , если любой непустой интервал множества  $B$  содержит точки  $A$ . Иначе говоря, как бы мы ни старались выбрать как можно более маленький (но непустой) интервал множества  $B$ , в нем всегда будут сидеть и точки множества  $A$ .
4. Можно взять, например, множество  $\mathbb{B} \subseteq \mathbb{Q}$  всех двоичных рациональностей, т.е. дробей вида  $k/2^n$ , где  $k \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ . Такое множество, во-первых, является



плотным, поскольку среднее арифметическое любых двух его представителей

$$\left(\frac{k}{2^n} + \frac{l}{2^m}\right) / 2 = \frac{k \cdot 2^{\max(n,m)-n} + l \cdot 2^{\max(n,m)-m}}{2^{\max(n,m)+1}}$$

является двоично-рациональным числом.

5. А во-вторых, множество  $\mathbb{B}$  плотно в  $\mathbb{Q}$ , поскольку каковы бы ни были два рациональных числа  $r \neq q$ , между ними найдется двоично-рациональное. Предлагаем доказать это самостоятельно в качестве упражнения.
6. На самом деле, это легко понять, если представить себе, как нужно наносить на числовую ось двоично-рациональные дроби. Сначала мы берем все целые числа, затем ровно между ними ставим все полуцелые (с шагом  $1/2$ ), затем в оставшихся полуцелых интервалах отмечаем середины (получаем числа с шагом  $1/4$ ), затем снова делим эти интервалы пополам (получаем шаг  $1/8$ ), и т.д. Ясно, что чем больше шагов мы пройдем, тем мельче будет сетка двоичных рациональностей, тем точнее с их помощью можно приблизить произвольное рациональное число. А это и есть свойство быть плотным в  $\mathbb{Q}$ .
7. Более того, какую бы точку на прямой мы ни выбрали, ее можно сколь угодно точно приблизить с помощью точек множества  $\mathbb{B}$ . Действительно, пусть имеется точка  $A$  на прямой. Снова начнем наносить сетку двоично-рациональных чисел. Сначала на расстоянии 1, и выберем тот отрезок, в котором эта точка сидит. Если она совпадает с одной из его границ, то мы уже нашли ее приближение (абсолютно точное) точками множества  $\mathbb{B}$ . Если нет, разделим отрезок пополам и снова выберем ту его часть, в которой находится точка  $A$ . Снова, если она совпадает с границей отрезка, то мы нашли точное приближение, иначе продолжим процесс деления отрезков. С каждым шагом точность приближения точки  $A$  будет удваиваться. Сначала она будет лучше чем 1, затем лучше, чем  $1/2$ , и т.д., на  $n$ -м шаге мы найдем точки множества  $\mathbb{B}$  на расстоянии менее  $1/2^n$  от точки  $A$ . Так что, рано или поздно мы достигнем заданной нам точности.
8. Множество  $\mathbb{B}$ , обладающее способностью подбираться сколь угодно близко к произвольным точкам прямой, называется **всюду плотным множеством**. Ясно, что и множество  $\mathbb{Q}$  всюду плотно, поскольку оно содержит в себе  $\mathbb{B}$ .
9. Более того, всякое множество, плотное в  $\mathbb{Q}$ , всюду плотно на прямой.

## 12.3 Зазоры между рациональными числами

### Конспект

1. Ранее мы уже приводили пример числа, которое определяется уравнением в целых числах, но притом не является рациональным. Это число  $\sqrt{2}$ , которое

разрешает уравнение  $x^2 - 2 = 0$ .

2. Такое число как бы вставляет клин между рациональными числами, рассекая их на две части. Действительно, если мы посмотрим на два множества

$$X = \{r \in \mathbb{Q} \mid r^2 < 2 \text{ или } r < 0\}, \quad Y = \{r \in \mathbb{Q} \mid r^2 > 2 \text{ и } r > 0\},$$

то можно заметить, что, во-первых, их объединение  $X \cup Y$  равно  $\mathbb{Q}$ , т.к. они включают в себя все рациональные числа, во-вторых, что они не пересекаются:  $X \cap Y = \emptyset$ . Наконец, в-третьих,  $X < Y$  в смысле сравнения множеств. Такие пары множеств называются дедекиндовыми сечениями, и к ним мы еще вернемся чуть позже.

3. Заметим еще одну особенность такого разбиения  $\mathbb{Q}$ : какой бы интервал  $(x; y)$  с концами  $x \in X$ ,  $y \in Y$  мы ни взяли, он всегда не пуст, что является следствием плотности  $\mathbb{Q}$ . То есть мы можем сколь угодно близко подбираться к условной границе двух множеств  $X$  и  $Y$ , но никогда не найдем крайние, т.е. соседствующие точки! В множестве  $X$  нет максимума, а в множестве  $Y$  нет минимума. А в интервале  $(x; y)$  всегда найдется бесконечно много точек как из множества  $X$ , так и из множества  $Y$ .
4. Получается, что множество  $\mathbb{Q}$  удастся распилить на два луча, причем таким способом, что у них нет граничных точек!
5. И единственно возможным кандидатом на роль границы будет именно число  $\sqrt{2}$ , которое, как мы уже выяснили, не является рациональным, т.е. не принадлежит  $\mathbb{Q}$ .
6. Стало быть между точками множества рациональных чисел есть дырки. Причем, их довольно много.
7. Возьмем, например, произвольное простое число  $p$  и два целых положительных числа  $k, l$ , взаимно простых ( $k \perp l$ ). И запишем уравнение

$$x^k - p^l = 0. \tag{12.1}$$

Это — уравнение в целых числах. Но может ли оно иметь рациональный корень?

8. Предположим, что существует рациональное число  $x = n/m$  ( $n \perp m$ ), которое разрешает данное уравнение. Тогда

$$n^k = p^l m^k,$$

откуда в силу основной теоремы арифметики следует, что простое число  $p$  присутствует в разложении  $n$  по степеням простых. Пусть оно входит в разложение  $n$  со степенью  $t \geq 1$ , т.е.  $n = p^t s$ , где  $s$  не делится на  $p$ .

Отсюда следует, что  $n^k = p^{kt} s^k = p^l m^k$ . но при этом, поскольку  $n \perp m$ ,  $m$  не делится на  $p$ , значит, вся степень  $p^{kt}$  совпадает со степенью  $p^l$ , т.е.  $kt = l$ , т.е.  $l$  делится на  $k$ .

По условию  $\text{НОД}(k, l) = 1$ , значит,  $k = 1$ . Отсюда следует, что при указанных условиях корень уравнения (12.1) будет рациональным числом тогда и только тогда, когда  $k = 1$ , т.е. уравнение имеет вид  $x - p^l = 0$ .

9. Как только мы берем  $k = 2, 3, \dots$ , уравнение (12.1) становится неразрешимым в рациональных числах.
10. Между тем, как и в случае  $\sqrt{2}$ , мы можем сколь угодно близко подбираться к положительному решению  $x$ , которое мы обозначим  $\sqrt[k]{p^l}$ , при помощи рациональных чисел. Это прямо следует из наших рассуждений о всюду плотности множества  $\mathbb{W}$  и, как следствие, множества  $\mathbb{Q}$ .
11. Итак, мы видим, что «дырки» между рациональными числами — явление нередкое. И точно так же, как мы расширяли  $\mathbb{Q}$  до поля  $\mathbb{Q}[\sqrt{2}]$ , мы можем строить любые расширения  $\mathbb{Q}[\sqrt[k]{p^l}]$ , почти всегда получая новые поля.

## 12.4 Многочлены и алгебраические числа

### Конспект

1. Заметим, что уравнение (12.1) — это алгебраическое уравнение, т.е. уравнение, записанное с помощью суммы степеней переменной  $x$  с некоторыми коэффициентами из данной нам алгебраической структуры, в нашем случае — кольца целых чисел.
2. Пусть дано какое-то коммутативное кольцо  $K$  с единицей. Тогда **многочленом степени  $n \geq 0$  над  $K$**  называется всякое выражение вида

$$\sum_{s=0}^n k_s x^s = k_n x^n + k_{n-1} x^{n-1} + \dots + k_1 x + k_0,$$

где  $k_0 \neq 0$ . Заметим, что многочлен степени  $n = 0$  — это константа  $k_0$ , отличная от нуля. Тождественный ноль принято называть многочленом степени  $-\infty$ . Степень многочлена  $P$  принято обозначать  $\deg P$ . Например,  $\deg(x^2 - 1) = 2$ .

3. Множество всех многочленов с коэффициентами из  $K$  обозначается  $K[x]$ . Например,  $\mathbb{Z}[x]$  — многочлены с целыми коэффициентами, к которым, в частности, относится многочлен  $x^k - p^l$ , рассмотренный нами выше.  $\mathbb{Q}[x]$  — многочлены с рациональными коэффициентами.

4. Многочлены **равны**, если равны коэффициенты при соответствующих степенях, т.е. если  $P(x) = \sum p_k x^k$  и  $Q(x) = \sum q_k x^k$ , то

$$P = Q \Leftrightarrow \forall k \ p_k = q_k.$$

5. Многочлены можно складывать, вычитать и умножать. Операции сложения и умножения вводятся следующим образом:

$$(P + Q)(x) = \sum_k (p_k + q_k)x^k, \quad (PQ)(x) = \sum_k \sum_{i+j=k} (p_i q_j)x^k.$$

Множество  $K[x]$  с такими операциями называется **кольцом многочленов** и является кольцом.

**Теорема 12.1** (Безу́). Пусть  $P$  — многочлен над коммутативным кольцом  $K$  с единицей. Тогда для любого  $c \in K$  существует многочлен  $Q \in K[x]$  такой, что

$$P(x) = (x - c)Q(x) + P(c).$$

*Доказательство.* Пусть  $P(x) = p_0 + p_1x + \dots + p_nx^n$ ,  $Q(x) = q_0 + q_1x + \dots + q_nx^n$ . Тогда решим уравнение

$$P(x) = (x - c)Q(x) + h$$

относительно коэффициентов  $q_k$ . Раскрывая скобки и приравнявая коэффициенты при одинаковых степенях, получаем систему уравнений

$$\begin{aligned} k_0 &= h - cq_0 \\ k_1 &= q_0 - cq_1 \\ &\dots\dots\dots \\ k_{n-1} &= q_{n-2} - cq_{n-1} \\ k_n &= q_{n-1} - cq_n \\ q_n &= 0 \end{aligned}$$

Решая эту систему снизу вверх, находим, что

$$\begin{aligned} q_{n-1} &= k_n \\ q_{n-2} &= k_{n-1} + ck_n \\ &\dots\dots\dots \\ q_0 &= k_1 + ck_2 + \dots + c^{n-1}k_n \\ h &= k_0 + k_1c + \dots + k_nc^n = P(c) \end{aligned}$$

Как видим, система однозначно разрешается в кольце  $K$ , и остаток  $h$  действительно равен  $P(c)$ . □

Теорема Безу хороша тем, что работает в кольце многочленов над любым коммутативным кольцом с единицей.

6. **Корнями многочлена** называются числа, зануляющие его, т.е. это такие числа, которые, будучи подставленными вместо переменной  $x$  обращают значение многочлена в ноль. Например, числа  $\sqrt{2}$  и  $-\sqrt{2}$  являются корнями многочлена  $x^2 - 2$ , а числа  $\pm i$  являются корнями многочлена  $x^2 + 1$ . Корни многочлена не всегда лежат в том же кольце, где и его коэффициенты. Это делает возможным расширять кольца и поля с помощью присоединения корней многочленов, заданных над этими кольцами и полями.
7. Из теоремы Безу следует, что  $\alpha$  — корень  $P(x)$  тогда и только тогда, когда  $P$  есть произведение двучлена  $(x - \alpha)$  и другого многочлена меньшей степени, т.е. когда  $P$  делится на  $(x - \alpha)$ . Например, многочлен  $x^k - 1$  делится на  $x - 1$ .
8. Заметим, что в привычной нам арифметике степень произведения многочленов равна сумме степеней сомножителей:

$$\deg(PQ) = \deg(P) + \deg(Q).$$

Однако, это не всегда верно. Рассмотрим, к примеру кольцо вычетов по модулю 8, т.е. множество  $\mathbb{Z}_8$  с операциями сложения и умножения по модулю 8. В таком кольце:

$$(2x^2 + 3x + 7)(4x + 4) = (8x^3 + 20x^2 + 40x + 28) \equiv 4x^2 + 4 \pmod{8},$$

т.е. правило сложения степеней нарушилось, т.к. коэффициент перед старшей степенью оказался сравним с нулем по модулю 8.

9. Это — не единственная проблема многочленов над кольцами. Рассмотрим многочлен  $x^2 - 1$  над тем же самым кольцом  $\mathbb{Z}_8[x]$ . Попробуем его разложить на множители. Школьная формула разности квадратов сразу дает ответ:

$$x^2 - 1 = (x - 1)(x + 1),$$

но поскольку  $1 \equiv -7 \pmod{8}$ , правильно будет записать так:

$$x^2 - 1 = (x - 1)(x - 7).$$

Однако, легко проверить, что числа 3 и 5 также являются корнями многочлена  $x^2 - 1$  в кольце  $\mathbb{Z}_8$ . Стало быть, он делится также на  $(x - 3)$  и  $(x - 5)$ .

Если бы для многочленов над произвольным кольцом выполнялась ОТА, мы должны были бы предположить, что

$$x^2 - 1 = (x - 1)(x - 3)(x - 5)(x - 7),$$

что невозможно из-за различия степеней многочленов слева и справа (и в данном случае различие степеней уже не спишешь на сравнение по модулю, т.к. коэффициенты при старших степенях равны 1).

На самом деле, ОТА не работает для кольца многочленов над произвольным кольцом из-за наличия делителей нуля в этом кольце (вспомним, что в кольце вычетов таблица умножения ненулевых элементов содержит нули тогда и только тогда, когда модуль вычетов не является простым числом).

Если же  $K$  является кольцом без делителей нуля (в Алгебре коммутативное кольцо без делителей нуля еще называется областью целостности, к таковому, например, относится кольцо целых чисел), а еще лучше — полем, то такой проблемы нет, и кольцо многочленов  $K[x]$  становится намного более привлекательным, а его арифметика — похожей на арифметику целых чисел.

10. Многочлены, заданные над полем, можно делить друг на друга с остатком так же, как это делается с обычными целыми числами. Например,

$$2x^3 - 2 = (3x^2 - 1) \left( \frac{2}{3}x \right) + \left( \frac{2}{3}x - 2 \right),$$

т.е. при делении  $(2x^3 - 2)/(3x^2 - 1)$  мы получаем неполное частное  $\frac{2}{3}x$  и остаток  $\frac{2}{3}x - 2$ . А, например,  $x^3 - 1$  делится на  $x - 1$  без остатка, т.к.

$$(x^3 - 1) = (x - 1)(x^2 + x + 1).$$

11. Теория делимости многочленов над полем во многом повторяет теорию делимости целых чисел. Здесь также есть простые, или **неприводимые**, многочлены, которые невозможно разложить в произведение многочленов меньшей степени над тем же полем, а также есть алгоритм Евклида и аналог основной теоремы арифметики о единственности разложения многочлена в произведение неприводимых.

Так, при делении многочленов в остатке всегда получается многочлен степени, меньшей, чем делитель. Точнее, пусть  $P_n$  — многочлен степени  $n$ , а  $Q_m$  — многочлен степени  $m < n$ , тогда справедливо представление

$$P_n = Q_m G + H,$$

где степень многочлена  $H$  меньше  $m$ . При этом степень неполного частного  $G$  будет равна  $n - m$ . Степень многочлена в данном случае следует рассматривать как его евклидову норму (вспомним числа Гаусса — там тоже была норма!).

В процессе выполнения алгоритма Евклида норма (т.е. степень) остатка все время падает. Такое снижение степени в остатке и позволяет провести алгоритм Евклида за конечное число шагов, т.к. в конце концов остаток будет

иметь степень 0, т.е. будет каким-то числом, не зависящим от переменной  $x$ . Заметим, что на делимость многочленов делимость их коэффициентов никак не влияет, поэтому многочлен нулевой степени рассматривается как условная единица делимости. Если же остаток окажется чистым нулем, т.е. многочленом степени  $-\infty$ , то мы нашли НОД многочленов, отличный от константы.

Например, пусть даны два многочлена  $x^2 - 3x + 2$  и  $x^2 - 2x - 3$ , тогда

$$x^2 - 3x + 2 = 1 \cdot (x^2 - 2x - 3) - (x - 5)$$

$$x^2 - 2x - 3 = (x + 3)(x - 5) + 12$$

В данном случае алгоритм Евклида в конце дает остаток 12, т.е. многочлен нулевой степени, и это есть НОД многочленов  $x^2 - 3x + 2$  и  $x^2 - 2x - 3$ . Такие многочлены являются взаимно простыми. Сравните этот факт с разложением исходных многочленов:  $x^2 - 3x + 2 = (x - 1)(x - 2)$ ,  $x^2 - 2x - 3 = (x - 3)(x + 1)$ .

Теперь в качестве второго многочлена возьмем  $x^2 - 1$ :

$$x^2 - 3x + 2 = 1 \cdot (x^2 - 1) - (3x - 3)$$

$$x^2 - 1 = ((1/3)x + 1/3)(3x - 3) + 0$$

Выходим на остаток 0, стало быть, предпоследний остаток и есть НОД. Причем, как мы уже говорили, умножение и деление многочлена на константу можно отбрасывать, так что

$$\text{НОД}(x^2 - 3x + 2, x^2 - 1) = x - 1.$$

Сравните этот факт с разложением исходных многочленов:  $x^2 - 3x + 2 = (x - 1)(x - 2)$ ,  $x^2 - 1 = (x - 1)(x + 1)$ .

12. Разложение многочлена на линейные множители сразу же дает нам список корней этого многочлена. Но, как мы видели выше, этот список не всегда полный. Покажем, что для многочленов над полем (а если точнее — над целостным кольцом) такой проблемы не существует.

**Теорема 12.2** (о корнях многочлена над полем). *Если  $K$  — поле, то количество различных корней многочлена из  $K[x]$  не превышает его степени.*

*Доказательство.* Воспользуемся индукцией. Очевидно, что для линейного многочлена  $k_0 + k_1x$  корень определяется однозначно: он равен числу  $-k_0/k_1$ .

Предположим, что для всех степеней ниже  $n$  теорема верна, и рассмотрим многочлен  $P(x)$  степени  $n$  (т.е.  $k_n \neq 0$ ).

Предположим, что  $P(x)$  имеет более чем  $n$  различных корней. Пусть  $\alpha$  — один из его корней. Тогда по теореме Безу

$$P(x) = (x - \alpha)Q(x), \tag{12.2}$$

где  $Q(x)$  — многочлен степени  $n - 1$ . Но у  $P(x)$  есть еще как минимум  $n$  различных корней, кроме  $\alpha$ . Пусть  $\beta$  — один из таких корней  $P(x)$ , тогда  $\beta \neq \alpha$  и

$$0 = P(\beta) = (\beta - \alpha)Q(\beta),$$

откуда  $Q(\beta) = 0$  (поскольку в поле нет делителей нуля), т.е.  $\beta$  оказался корнем многочлена  $Q(x)$ . И так — для всех корней  $P(x)$ , отличных от  $\alpha$ . Следовательно, если таковых будет не меньше  $n$ , то многочлен  $Q(x)$  имеет как минимум  $n$  различных корней, в то время как его степень равна  $n - 1$ . А это противоречит предположению индукции.

Следовательно  $P(x)$  не может иметь более, чем  $n$ , различных корней.  $\square$

13. Эту теорему можно уточнить, учитывая кратности корней. Корень  $\alpha$  многочлена  $P(x)$  имеет кратность  $k$ , если  $P$  делится на  $(x - \alpha)^k$  и не делится на  $(x - \alpha)^{k+1}$ . Пусть многочлен  $P$  имеет степень  $n$  и корни  $\alpha_1$  кратности  $k_1$ , и т.д.  $\alpha_m$  кратности  $k_m$ . Тогда  $k_1 + \dots + k_m \leq n$ . Для доказательства этого факта нужно в разложении (12.2) делить сразу на максимальную степень двучлена  $(x - \alpha)$ .
14. Неравенство  $k_1 + \dots + k_m \leq n$  превращается в равенство, если мы имеем дело с многочленами над полем комплексных чисел, поскольку над этим полем любой многочлен раскладывается в произведение линейных многочленов! И этот замечательный факт называется **Основной теоремой алгебры**.
15. Перейдем теперь к изучению многочленов над полем  $\mathbb{Q}$ .
16. Корни многочленов над  $\mathbb{Q}$  называются **алгебраическими числами**. Множество всех алгебраических чисел обозначается  $\mathbb{A}$ . Заметим, что алгебраические числа, вообще говоря, лежат в комплексной плоскости, т.е. могут иметь мнимую часть.
17. Все корни многочленов из  $\mathbb{Q}[x]$  и все корни многочленов из  $\mathbb{Z}[x]$  — это одно и то же множество  $\mathbb{A}$ . Действительно,  $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ , поскольку  $\mathbb{Z} \subseteq \mathbb{Q}$ , так что корни многочленов с целыми коэффициентами принадлежат  $\mathbb{A}$ . С другой стороны, если какое-то  $x$  зануляет многочлен с рациональными коэффициентами, то он же зануляет и многочлен с целыми коэффициентами. Этот многочлен получается из исходного домножением на все знаменатели всех его коэффициентов, так что вместо дробей мы получаем целые числа, а равенство нулю при этом сохраняется.
18. Поэтому часто при анализе корней многочленов используется один из следующих подходов: либо рассматриваются многочлены с произвольными целыми коэффициентами, либо рассматриваются многочлены с рациональными коэффициентами, у которых старший коэффициент  $k_n = 1$ :

$$k_n x^n + k_{n-1} x^{n-1} + \dots + k_1 x + k_0, \quad k_s \in \mathbb{Z}, \quad \text{либо} \quad x^n + q_{n-1} x^{n-1} + \dots + q_1 x + q_0, \quad q_s \in \mathbb{Q}.$$



19. Есть, правда, один объединяющий эти два кейса вариант многочленов — многочлены с целыми коэффициентами и старшим коэффициентом  $k_n = 1$ . Корни таких многочленов называются **целыми алгебраическими числами**. Таких числа образуют собственное подмножество в  $\mathbb{A}$ .
20. Введем следующее понятие. Пусть  $f \in \mathbb{Z}[x]$ . **Содержанием многочлена**  $f$  называется наибольший общий делитель всех его коэффициентов:

$$\text{count}(k_0 + k_1x + \dots + k_nx^n) = \text{НОД}(k_0, k_1, \dots, k_n)$$

**Лемма 12.2** (Гаусса). Пусть  $f, g \in \mathbb{Z}[x]$ , тогда

$$\text{count}(fg) = \text{count}(f) \text{count}(g)$$

*Доказательство.* Ясно, что достаточно рассмотреть случай  $\text{count}(f) = \text{count}(g) = 1$ . Остальные случаи приводятся к этому делением коэффициентов многочленов на их содержание. При этом, очевидно, они не перестают быть многочленами над  $\mathbb{Z}$ .

Итак, предполагая  $\text{count}(f) = \text{count}(g) = 1$ , покажем, что  $\text{count}(fg) = 1$ . Пусть, кроме того,

$$f(x) = f_0 + f_1x + \dots + f_nx^n, \quad g(x) = g_0 + g_1x + \dots + g_mx^m$$

Предположим, что  $\text{count}(fg) = d > 1$ . Пусть  $p$  — простое число, делящее  $d$ . Так как  $\text{count}(f) = 1$ , существует хотя бы один коэффициент многочлена  $f$ , который не делится на  $p$ . Пусть  $f_k$  — коэффициент с минимальным номером, не делящийся на  $p$ . Аналогично обозначим за  $g_s$  коэффициент многочлена  $g$  с минимальным номером, не делящийся на  $p$ .

Найдем коэффициент многочлена  $fg$  при степени  $x^{k+s}$ . Она равен

$$[x^{k+s}]f(x) = f_0g_{k+s} + f_1g_{k+s-1} + \dots + f_kg_s + f_{k+1}g_{s-1} + \dots + f_{k+s}g_0 \equiv f_kg_s \pmod{p},$$

поскольку  $f_0, \dots, f_{k-1} \equiv 0 \pmod{p}$  и  $g_{s-1}, \dots, g_0 \equiv 0 \pmod{p}$ .

Но  $f_kg_s \not\equiv 0 \pmod{p}$  в силу их выбора, а значит,  $[x^{k+s}]f(x) \not\equiv 0 \pmod{p}$ , т.е. среди коэффициентов многочлена  $fg$  есть такой, который не делится на  $p$ , откуда следует, что  $p$  не может быть общим делителем коэффициентов  $fg$ , а значит, не делит и наибольший общий делитель  $\text{count}(fg) = d$ . Противоречие.  $\square$

**Следствие 12.1.** Многочлен с целыми коэффициентами неприводим над  $\mathbb{Z}$  тогда и только тогда, когда он не приводим над  $\mathbb{Q}$ .

*Доказательство.* Ясно, что если многочлен неприводим над  $\mathbb{Q}$ , то он неприводим и над  $\mathbb{Z}$ , поэтому докажем обратное. А точнее, покажем, что если многочлен раскладывается в произведение над  $\mathbb{Q}$ , то его можно разложить и над  $\mathbb{Z}$ .

Пусть  $f \in \mathbb{Z}[x]$  и  $f = gh$ , где  $g, h \in \mathbb{Q}[x]$ . Можно считать, что  $\text{count}(f) = 1$  (если это не так, то разделим равенство  $f = gh$  на  $\text{count}(f)$  и получим то, что требуется,  $f$  при этом не выпадет из  $\mathbb{Z}[x]$ ).

Найдем такое натуральное число  $n > 0$ , что  $ng \in \mathbb{Z}[x]$  (например, произведение всех знаменателей коэффициентов  $g$ ). И пусть  $m = \text{count}(ng)$ . Тогда рациональное число  $r = n/m$  таково, что  $rg \in \mathbb{Z}[x]$  и  $\text{count}(rg) = 1$ . Аналогично найдем рациональное  $s$  такое, что  $sh \in \mathbb{Z}[x]$  и  $\text{count}(sh) = 1$ .

По лемме Гаусса получаем

$$1 = \text{count}(rg) \text{count}(sh) = \text{count}(rsg h) = \text{count}(rsf) = rs \text{count}(f) = rs,$$

Но тогда имеем следующее разложение

$$f = gh = rsg h = (rg)(sh),$$

где  $rg, sh \in \mathbb{Z}[x]$ , т.е.  $f$  разложим над  $\mathbb{Z}$ . □

21. Если  $\alpha$  — алгебраическое число, то минимальная степень многочлена, корнем которого является  $\alpha$ , называется **степенью алгебраического числа**  $\alpha$ .
22. Например, мы ранее показали, что  $\sqrt{2}$  не является рациональным числом, значит, никакой многочлен первой степени, т.е.  $x + q$ , не обращается в ноль при  $x = \sqrt{2}$ , значит,  $\sqrt{2}$  не является алгебраическим числом первой степени.
23. На самом деле, все рациональные числа, и только они, являются алгебраическими числами первой степени. То есть,  $\mathbb{Q} \subset \mathbb{A}$  (вложение собственное!)
24. С другой стороны,  $x^2 - 2$  зануляется числом  $\sqrt{2}$ , так что это число является алгебраическим числом степени 2. То же самое можно сказать про любой квадратный корень из любого простого числа или его нечетной степени (ибо нечетные числа взаимно просты с двойкой, см. выше про корни  $\sqrt[k]{p^l}$ ).
25. Далее мы установим, что число  $\sqrt[3]{2}$  является алгебраическим числом степени 3. Для этого нам нужно показать, что никакой многочлен степени 2 не может его занулить.
- 26.

**Лемма 12.3.** Пусть  $f(x)$  — многочлен минимальной степени, зануляющий число  $\alpha \in \mathbb{A}$ , и пусть многочлен  $g(\alpha) = 0$ , тогда существует многочлен  $h(x)$  такой, что

$$g = fh.$$

*Доказательство.* Пусть степень  $f$  равна  $m$ , а степень  $g$  равна  $n$ . Ясно, что  $n \geq m$  в силу минимальности  $f$ . Разделим  $g$  на  $f$  с остатком:  $g = fh + r$ . Здесь степень  $h$  равна  $n - m$ , а степень  $r$  строго меньше  $m$ .

Но поскольку  $g(\alpha) = 0$  и  $f(\alpha) = 0$ , получаем, что и  $r(\alpha) = 0$ . Таким образом,  $r$  является многочленом, зануляющим  $\alpha$ , и притом его степень меньше  $m$  в противоречии с определением числа  $m$ . Следовательно,  $r$  есть тождественный ноль, а значит,  $g$  делится на  $f$  без остатка.  $\square$

27. Перейдем к  $\sqrt[3]{2}$ , точнее, к определяющему его многочлену.

**Лемма 12.4.** *Многочлен  $x^3 - 2$  неразложим на множители с целыми коэффициентами степени  $\geq 1$ .*

*Доказательство.* Предположим, что это не так, тогда  $x^3 - 2$  делится на линейный многочлен вида  $(ax + b)$  (если он делится на многочлен второй степени, то делится и на многочлен первой степени):

$$x^3 - 2 = (ax + b)(kx^2 + tx + n),$$

где  $a, b, k, t, n \in \mathbb{Z}$  и  $a, k \neq 0$ . Сравним коэффициенты при одинаковых степенях:

$$\begin{aligned} 1 &= ak \\ 0 &= at + bk \\ 0 &= an + bt \\ -2 &= bn \end{aligned}$$

Из первого равенства следует, что либо  $a = k = 1$ , либо  $a = k = -1$ . Учитывая это, из второго равенства получаем, что  $t = -b$ , откуда с помощью третьего равенства получаем, что  $an = b^2$ . Наконец, четвертое равенство предлагает варианты:

$$b = 2, n = -1 \text{ или } b = -2, n = 1 \text{ или } b = 1, n = -2 \text{ или } b = -1, n = 2.$$

В первом и втором случае получаем, что  $an = 4$ , но это невозможно, поскольку  $a, n \in \{1, -1\}$ .

В третьем и четвертом случае  $an = 1$ , но и это невозможно при  $a \in \{1, -1\}$ ,  $b \in \{2, -2\}$ .  $\square$

28. В силу следствия из леммы Гаусса и леммы о неразложимости  $x^3 - 2$  получаем, что  $x^3 - 2$  неразложим на множители с рациональными коэффициентами. Во-вторых, если бы минимальный многочлен для  $\sqrt[3]{2}$  имел степень 1 или 2, то в силу леммы 12.3  $x^3 - 2$  делился бы на него. А это невозможно в силу неразложимости  $x^3 - 2$ . Следовательно, минимальным многочленом для  $\sqrt[3]{2}$  является многочлен третьей степени, значит,  $\sqrt[3]{2}$  — алгебраическое число степени 3.
29. Существует подробно разработанная теория алгебраических чисел, из которой, в частности, следует, что число  $\sqrt[k]{p}$  является алгебраическим числом степени  $k$ . То есть, по крайней мере, для каждого натурального  $k$  и каждого простого  $p$  можно найти свое алгебраическое число.
30. Про множество алгебраических чисел известна следующая теорема, доказательство которой опирается на теорию расширения полей.

**Теорема 12.3.** (1)  $\mathbb{A}$  является полем, (2)  $\mathbb{A}$  алгебраически замкнуто.

Первое утверждение говорит нам о том, что алгебраические числа можно складывать, вычитать, умножать и делить, а результат все равно останется алгебраическим числом, т.е. корнем некоторого многочлена с целыми коэффициентами. Второе — о том, что если даже мы рассмотрим кольцо многочленов  $\mathbb{A}[x]$ , т.е. всех многочленов с коэффициентами из поля  $\mathbb{A}$ , то корни таких многочленов все равно будут алгебраическими числами. Иначе говоря, замкнутость  $\mathbb{A}$  означает, что его невозможно расширить алгебраическими методами, как это мы проделывали с полем  $\mathbb{Q}$ . Для дальнейшего расширения  $\mathbb{A}$  понадобятся многочлены бесконечной степени, т.е. ряды.

31. Отметим, что если число  $\alpha$  — алгебраическое степени  $n > 1$ , то числа  $\alpha, \alpha^2, \dots, \alpha^{n-1}$  также являются алгебраическими степени не выше  $n$  и притом иррациональными (если бы какое-то из них было рациональным, то степень  $\alpha$  оказался бы ниже  $n$ ). Например,  $(\sqrt[3]{2})^2 = \sqrt[3]{4}$  — алгебраическое число степени 3.
32. Более того, если  $\alpha$  — алгебраическое число степени выше 1, то любая комбинация  $k + \alpha t$  с целыми коэффициентами  $k, t$  ( $t \neq 0$ ) также будет алгебраическим числом той же степени. И еще более того, любая комбинация вида

$$k_0 + k_1\alpha + k_2\alpha^2 + \dots + k_m\alpha^m,$$

где  $\alpha$  — алгебраическое степени  $n$ ,  $k_m$  — целое ненулевое число,  $m < n$ , также будет алгебраическим числом степени выше 1 (иначе перед нами был бы многочлен степени  $< n$ , аннулирующий  $\alpha$ ), причем все такие комбинации различны (если бы нашлось две равные комбинации с разными наборами коэффициентов, то их разность была бы многочленом степени  $< n$ , аннулирующим  $\alpha$ ).

33. Таким образом, мы уже существенно пополнили множество иррациональных чисел всего лишь с помощью алгебраических корней и целочисленных линейных комбинаций их степеней. Точнее, мы надстроили над множеством  $\mathbb{Q}$  бескончный слоеный пирог, в каждом слое которого сидят алгебраические числа какой-то одной степени (а первый слой пирога — это само  $\mathbb{Q}$ ), причем каждый слой содержит бесконечно много чисел. И все эти слои каким-то образом умещаются в «дырках» между рациональными числами, не смотря на то, что  $\mathbb{Q}$  всюду плотно на прямой.

34. *Насколько же плотны алгебраические числа заданной степени на числовой прямой?*

35. Возьмем произвольное алгебраическое число  $\alpha$  (например,  $\sqrt{2}$ ) какой-то алгебраической степени  $> 1$ . Это число иррациональное, т.е. не соизмеримо с целыми числами. И пусть у нас кузнечик одной ногой прыгает на 1, а второй — на  $\alpha$ . *Вопрос:* какими свойствами обладает множество всех тех точек, куда может допрыгнуть кузнечик?

36. Ясно, что все точки, в которые попадает кузнечик, описываются в общем виде формулой

$$k + \alpha t, \quad k, t \in \mathbb{Z},$$

т.е. это числа-собратья исходного числа  $\alpha$  по степени своей алгебраичности. Выбрав число определенной алгебраической степени, кузнечик прыгает только по числам такой же степени.

37. Вспомним наш пример с наматыванием прямой на окружность (колесо на дороге), и выберем радиус окружности так, чтобы один полный виток по ней составлял как раз 1 единицу длины ( $R = 1/2\pi$ ). Тогда однократное наматывание прямой на окружность будет соответствовать прыжку кузнечика на 1, а значит, с точки зрения жителя окружности кузнечик будет топтаться на месте всякий раз, когда он прыгает на любое целое число.

38. В то же время, если кузнечик начинает прыгать с шагом  $\alpha$ , он, очевидно, начинает встречаться с жителем окружности в каких-то других точках, отличных от нуля. Посмотрим, как расположены эти точки на окружности.

39. Для начала заметим, что кузнечик при этом никогда не повторяется, т.к. точки  $k\alpha$  и  $l\alpha$  при  $k \neq l$ , намотанные на окружность, соответствуют длинам дуг за вычетом каких-то целых оборотов:

$$k\alpha = n + \beta, \quad l\alpha = m + \gamma,$$

и если бы мы получили совпадение дуг  $\beta$  и  $\gamma$ , то получилось бы уравнение

$$k\alpha - n = l\alpha - m,$$

откуда видно, что  $\alpha = (n - m)/(k - l)$  — рациональное число, а это противоречит иррациональности  $\alpha$ .

40. Итак, все шаги кузнечика вида  $0, \pm\alpha, \pm2\alpha, \dots$  дают попарно различные точки на окружности.
41. Далее. Покажем, что какое бы маленькое  $\varepsilon$  мы ни выбрали, найдется такое целое  $t$ , что число  $\alpha t$  будет отстоять от некоторого целого числа на расстояние меньше этого  $\varepsilon$ .
42. Действительно, выберем целое число  $N$  заведомо большее, чем  $1/\varepsilon$ , и поделим окружность на  $N$  равных секторов. В каждом секторе длина дуги будет равна  $1/N$ , что меньше  $\varepsilon$ . Но всех различных точек, кратных  $\alpha$ , как мы доказали чуть выше, бесконечно много, а значит, хотя бы на одной дуге из этих  $N$  штук окажется хотя бы 2 точки, и мы получим, что

$$k\alpha = n + \beta, \quad l\alpha = m + \gamma, \quad |\beta - \gamma| < \varepsilon.$$

Для удобства можем считать, что  $\beta > \gamma$  и, следовательно,  $\gamma < \beta < \gamma + \varepsilon$ . Тогда

$$l\alpha - m < k\alpha - n < l\alpha - m + \varepsilon,$$

откуда

$$n - m < (k - l)\alpha < n - m + \varepsilon,$$

т.е. при  $t = k - l$  число  $\alpha t$  отстоит от целого  $n - m$  на расстояние меньше  $\varepsilon$ .

43. А это значит, что кузнечик попадает в точки, сколь угодно близкие к нулю (ведь до нуля он может допрыгать своей целочисленной ногой, сделав  $m - n$  шагов).
44. Но, умея сдвигаться на какое-то число  $\delta$  от нуля хоть в какую-то сторону, кузнечек может повторять этот алгоритм раз за разом, и уходить от 0 на расстояние  $\pm\delta, \pm2\delta, \pm3\delta$  и т.д. То есть, числа вида  $k + \alpha t$ , достигаемые кузнечиком, находятся сколь угодно близко к любой точке на прямой!
45. Но в таком случае множество  $\{k + \alpha t \mid k, t \in \mathbb{Z}\}$  всюду плотно на прямой, как и множество  $\mathbb{Q}$ . Хотя, строго говоря, оно не содержит в себе  $\mathbb{Q}$  (ведь коэффициенты  $k$  — целые, а при  $t \neq 0$  комбинация  $k + \alpha t$  и вовсе иррациональна). Получается, что множество алгебраических чисел одной выбранной степени всюду плотно, причем не за счет  $\mathbb{Q}$ , а за счет точек, лежащих вне  $\mathbb{Q}$ !
46. По сути, мы получаем, что между рациональными числами столь много «дырок», что там уместается бесконечно много всюду плотных попарно различных множеств.

47. Вопрос: а все ли «дырки» могут быть ими заполнены? Сколько вообще существует алгебраических чисел и сколько существует «дыр» на рациональной прямой?
48. Для ответа на этот вопрос нам снова следует обратиться к теории множеств.

# Континуум

## Аннотация.

В этой главе мы полностью завершим наполнение геометрической прямой числами, обсудим разные версии понятия полноты вещественной прямой, построим до конца комплексную плоскость.

## 13.1 Мощности множеств

### Конспект

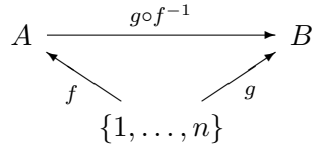
1. Если в множестве  $n \in \mathbb{N}$  элементов, то число  $n$  называется мощностью этого множества. Множества, имеющие мощность, равную натуральному числу, называются **конечными**.
2. Очевидно, что само множество натуральных чисел не является конечным. Вопрос: как сравнивать мощности любых множеств?
3. Если мы возьмем конечное множество  $A = \{a_1, \dots, a_n\}$ , то мы сразу же подразумеваем наличие нумерации его элементов: номеру  $k$  ставится в соответствие элемент  $a_k$ . И если все  $a_k$  попарно различны, то в этом множестве столько же элементов, сколько чисел  $1, \dots, n$ , т.е.  $n$  штук.
4. В этом рассуждении мы неявно указали на то, что существует взаимно однозначное соответствие между элементами множества  $A$  и множеством-эталон  $\{1, \dots, n\}$ .
5. Теперь, если задано некоторое множество  $B = \{b_1, \dots, b_n\}$ , у которого также все  $b_k$  попарно различны, то мы вновь имеем дело со взаимно однозначным соответствием между  $B$  и множеством-эталон  $\{1, \dots, n\}$ . Иначе говоря, мы имеем биекции

$$f : \{1, \dots, n\} \leftrightarrow A \text{ и } g : \{1, \dots, n\} \leftrightarrow B.$$

6. Но тогда сложная функция  $h(a) = g(f^{-1}(a))$  устанавливает взаимно однозначное соответствие между  $A$  и  $B$ . Это можно проиллюстрировать на диа-



грамме:



7. Таким образом, мы находим, что конечные множества  $A$  и  $B$  обладают одинаковой мощностью (количеством элементов), если между ними существует биекция.
8. Именно такой подход и выбирается при определении равномощности произвольных множеств!
9. Множества  $X$  и  $Y$  **равномощны** (будем это записывать так:  $X \leftrightarrow Y$ ), если существует биекция  $f : X \leftrightarrow Y$ .
10. Заметим, что при этом мы не требуем наличия какого-то эталонного множества, хотя для конечных множеств, как мы уже видели, таковыми могут считаться множества  $\{1, \dots, n\}$  или, как принято в теории множеств, множества  $\{0, \dots, n - 1\}$ .
11. Отношение  $\leftrightarrow$  рефлексивно (всякое множество само себе равномощно), симметрично (если  $X \leftrightarrow Y$ , то  $Y \leftrightarrow X$ ) и транзитивно (если  $X \leftrightarrow Y$  и  $Y \leftrightarrow Z$ , то  $X \leftrightarrow Z$ ), т.е. является отношением эквивалентности. Это значит, что, вообще говоря, все множества можно разделить на непересекающиеся классы, так что внутри каждого класса будут находиться только равномощные множества. Такой класс и принято называть **мощностью множества**.
12. Другой подход к определению самого понятия мощности заключается в том, чтобы в каждом таком классе найти некоторого типичного представителя и его объявить мерой мощности всех множеств данного класса. В случае конечных множеств такими представителями как раз и являются отрезки натурального ряда  $\{0, \dots, n - 1\}$ .
13. Множество, не содержащее элементов, т.е. пустое множество  $\emptyset$ , имеет мощность 0, оно биективно не сопоставляется ни с каким другим множеством, т.е. является уникальным представителем своего класса, и само себе является мерой мощности.
14. Еще одна разновидность множеств, имеющих эталон мощности — **счетные множества**. К ним относятся все множества, равномощные  $\mathbb{N}$ .
15. Например, счетными являются такие множества:

$$2\mathbb{N}, \mathbb{Z}, 2\mathbb{Z}, \{p \in \mathbb{N} \mid p \text{ — простое}\}, \mathbb{Z}[i], \mathbb{Q}, \mathbb{A}.$$

Все множества, которые не конечны, и элементы которых можно перенумеровать (пересчитать) натуральными числами, являются счетными.

16. Нумерацию  $2\mathbb{N}$  представить очень просто: каждому номеру  $k$  поставим в соответствие элемент  $2k$ , тем самым мы перенумеруем все четные числа, а значит, множество четных чисел счетное. Здесь мы впервые сталкиваемся с тем, что бесконечное множество равномощно какой-то своей части (которая может казаться очень маленькой, ведь точно так же устанавливается биекция между  $\mathbb{N}$  и  $10^9\mathbb{N}$  и т.п.). Иногда такое свойство бесконечных множеств берется за их определение: *множество бесконечное, если оно равномощно некоторому своему собственному подмножеству*.
17. Биекцию  $\mathbb{N} \leftrightarrow \mathbb{Z}$  установить также относительно просто: будем нумеровать целые числа по мере их удаления от нуля:  $0, 1, -1, 2, -2, 3, -3$ , и т.д. Ясно, что каждое целое число будет пронумеровано, и притом только один раз. Следовательно,  $\mathbb{Z}$  — счетное.
18. Для нумерации  $\mathbb{Z}[i]$  нужно воспользоваться нумерацией змейкой: обходить все точки  $\mathbb{Z}[i]$  по спирали, постепенно удаляясь от 0. Построим биекцию в обратную сторону, т.е. из  $\mathbb{Z}[i]$  в  $\mathbb{N}$ , следующим способом:

$$f(n + mi) = n + (n + m + 1)(n + m)/2.$$

Вспоминая теперь, что  $\mathbb{Z}[i] = \mathbb{Z} \times \mathbb{Z}$  (если забыть об арифметике на этом множестве), то мы получаем замечательный факт, который называется **теоремой о квадрате**:  $\mathbb{Z} \leftrightarrow \mathbb{Z} \times \mathbb{Z}$ . То есть, счетное множество равномощно своему квадрату. Конечным множествам такое и не снилось!

19. Можно развить это достижение и дальше. Имея нумерацию  $\mathbb{Z} \times \mathbb{Z}$  и  $\mathbb{Z}$ , мы можем пронумеровать  $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ , т.е. куб множества  $\mathbb{Z}$ , и так далее. Любая конечная степень  $\mathbb{Z}$  равномощна  $\mathbb{Z}$ .
20. Рациональные числа — это пары целых чисел, но не всех, а только взаимно простых. Это значит, что они тоже получают номера в процессе нумерования  $\mathbb{Z} \times \mathbb{Z}$ , только с пропусками. Если затем эти номера перенумеровать заново, уже без пропусков, то мы получим взаимно однозначное соответствие  $\mathbb{Q}$  и  $\mathbb{N}$ . То есть множество  $\mathbb{Q}$  также счетно.
21. Для нумерации  $\mathbb{A}$  воспользуемся следующим приемом. Вспомним, что  $\mathbb{A}$  — это все корни всех многочленов с целыми коэффициентами. Возьмем тогда некоторое целое положительное число  $L$  и соберем в множество  $\mathbb{A}_L$  те и только те алгебраические числа, которые определяются многочленами вида  $P(x) = k_0 + k_1x + \dots + k_nx^n$  ( $k_n \neq 0$ ), удовлетворяющими условию

$$|k_0| + |k_1| + \dots + |k_n| + n = L.$$

Ясно, что таких многочленов существует лишь конечный набор, т.к. выбор коэффициентов  $k_s$  и степени  $n$  ограничен числом  $L$ . Но и корней у многочлена — тоже конечное количество, не превышающее его степень (см. выше теорему о корнях над полем). Таким образом, множество  $\mathbb{A}_L$  конечно.

С другой стороны, множество  $\mathbb{A}$  есть объединение всех множеств  $\mathbb{A}_L$  при  $L = 1, 2, \dots$ . Поэтому, нумеруя последовательно, сначала числа из  $\mathbb{A}_1$ , затем числа из  $\mathbb{A}_2$ , и т.д. мы пронумеруем все множество  $\mathbb{A}$ , а значит, это множество счетное!

22. Что же получается в итоге? Множество алгебраических чисел, которыми мы старались заткнуть все дыры между рациональными числами, и которое состоит из бесконечного числа бесконечных слоев, равномощно множеству  $\mathbb{Q}$ ! С точки зрения мощности множества мы так ничего и не добавили к рациональным числам, хотя и позатыкали много дыр.
23. Возникает вопрос: *а бывают ли вообще какие-то другие мощности, кроме счетной?* Ответ на этот вопрос дает

**Теорема 13.1** (Кантора). *Никакое множество не равномощно множеству всех своих подмножеств.*

*Доказательство.* Пусть имеется множество  $X$ . Можем сразу считать, что оно непустое, т.к. для пустого множества теорема, очевидно, верна (в пустом множестве 0 элементов, а в множестве  $\{\emptyset\}$  — один элемент). Через  $\mathcal{P}(X)$  обозначим множество всех подмножеств множества  $X$ .

Предположим, что существует биекция  $f : X \leftrightarrow \mathcal{P}(X)$ . Ясно, что поскольку для всякого  $x \in X$  значение  $f(x)$  есть какое-то подмножество  $X$ , то возможны две ситуации: либо  $x \in f(x)$ , либо  $x \notin f(x)$ . Соберем тогда в множество  $Y$  все такие элементы  $x$ , которые удовлетворяют второму соотношению:

$$Y = \{x \in X \mid x \notin f(x)\}.$$

Понятно, что  $Y \subseteq X$ , а значит,  $Y \in \mathcal{P}(X)$ , а значит, существует единственный элемент  $y \in X$  такой, что  $f(y) = Y$  (поскольку  $f$  — биекция по предположению).

Вопрос:  $y \in Y$  или нет?

Если  $y \in Y$ , то по определению множества  $Y$  получаем, что  $y \notin f(y)$ , но тогда  $y \notin Y$ . Противоречие.

Если  $y \notin Y$ , то по определению множества  $Y$  получаем, что **неверно**  $y \notin f(y)$ , т.е.  $y \in Y$ . Противоречие.

Любой вариант приводит к противоречию, следовательно, предположение о существовании биекции  $f : X \leftrightarrow \mathcal{P}(X)$  неверно, т.е. множество  $X$  и множество всех его подмножеств неравномощны.  $\square$

Теорему Кантора можно дополнить тем, что множество всех подмножеств множества  $X$  мощнее исходного множества  $X$ , т.к.  $X$  в него инъективно вкладывается, т.е. равномощно некоторой части  $\mathcal{P}(X)$ . Действительно, в  $\mathcal{P}(X)$  существует подмножество следующего вида:

$$\{\{x\} \mid x \in X\},$$

это — множество всех синглетов (т.е. одноточечных подмножеств), образованных точками множества  $X$ . Таким образом,  $\mathcal{P}(X)$  получается более мощным множеством, чем  $X$ .

24. Приведем пример. Пусть  $X = \{1, 2, 3\}$ . Тогда

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Подмножество синглетов здесь — это множество  $\{\{1\}, \{2\}, \{3\}\}$ .

25. Для конечного множества  $X$  мощности  $n$  мощность множества его подмножеств  $\mathcal{P}(X)$  равна  $2^n$ . Это легко проверить, поскольку каждое подмножество  $X$  задается состояниями его элементов: каждый из них может входить в данное подмножество или не входить. Поскольку у каждого элемента ровно 2 состояния, а всего элементов  $n$ , то общее количество состояний всех элементов равно  $2 \cdot 2 \cdot \dots \cdot 2$  ( $n$  раз), т.е.  $2^n$ .

26. Отсюда берет начало второе обозначение для множества всех подмножеств множества  $X$  —  $2^X$ .

27. Но если с конечными множествами все укладывается в рамки обычно арифметики, то с множеством  $2^{\mathbb{N}}$  возникают проблемы. Его мощность не только не выражается натуральным числом, но она также не равна и мощности  $\mathbb{N}$ , как мы только что доказали. Эта мощность называется **мощностью континуума** и обозначается  $\mathfrak{c}$ .

28. Итак, мы теперь знаем, что бесконечные множества отличаются по мощности. Как же можно устанавливать их равномощность, если сложно или невозможно в явном виде указать биекцию между множествами? ответ на этот вопрос дает

**Теорема 13.2** (Кантора–Бернштейна). *Если существуют инъекции  $f : A \rightarrow B$  и  $g : B \rightarrow A$ , то множества  $A$  и  $B$  равномощны.*

*Доказательство.* Рассмотрим функцию  $H : 2^A \rightarrow 2^B$ , определяемую следующей формулой:

$$H(X) = A \setminus g[B \setminus fX] \text{ для всех } X \subseteq A.$$

*Примечание:* здесь под записью  $fX$  и  $f[X]$  понимается **образ множества**  $X$ , т.е.

$$f[X] = \{f(x) \mid x \in X\}.$$

Предположим, что существует корень уравнения  $H(X) = X$  — некоторое множество  $X_0$ . Посмотрим, какими свойствами оно обладает. Обозначим через  $Y_0$  множество  $B \setminus fX_0$ . Поскольку  $H(X_0) = X_0$ , то  $gY_0 = A \setminus X_0$ . Таким образом, сужения функций  $f|_{X_0}$  и  $g|_{Y_0}$  действуют на непересекающихся подмножествах множеств  $A$  и  $B$  и «покрывают» эти множества целиком.

Точнее, рассмотрим обратную к  $g|_{Y_0}$  функцию, определенную на множестве  $A \setminus X_0$ , обозначив ее  $h$ . Имеем:  $h : A \setminus X_0 \rightarrow Y_0$  — биекция,  $f|_{X_0} : X_0 \rightarrow B \setminus Y_0$  — тоже биекция. Тогда объединение этих функций  $h \cup f|_{X_0}$  есть биекция между  $A$  и  $B$ .

Итак, доказательство теоремы свелось к поиску корня уравнения  $H(X) = X$ . Назовем множество  $X$  *хорошим*, если  $X \subseteq H(X)$  (почти как в теореме Кантора!), и через  $Z$  обозначим объединение всех хороших множеств.

Нетрудно проверить, что функция  $H$  монотонна по вложению множеств, т.е. если  $X \subseteq Y$ , то  $H(X) \subseteq H(Y)$ . Пусть  $z \in Z$ . Тогда существует хорошее множество  $X$  такое, что  $z \in X$ . Кроме того, имеем  $H(X) \subseteq H(Z)$  и  $X \subseteq H(X)$ . Отсюда заключаем, что  $z \in H(Z)$ , и это верно для любого  $z \in Z$ . Таким образом,  $Z$  — хорошее множество.

Чтобы показать, что  $Z$  и есть корень нашего уравнения, надо проверить обратное вложение, т.е. что  $H(Z) \subseteq Z$ . Допустим, что это не так. Тогда существует  $x \in H(Z) \setminus Z$ . Рассмотрим множество  $Z' = Z \cup \{x\}$ . Это множество не может быть хорошим, т.к. иначе оно бы содержалось в  $Z$ . Поэтому  $Z' \not\subseteq H(Z')$ . Ясно, что  $H(Z) \subseteq H(Z')$ , поэтому  $Z' \not\subseteq H(Z)$ . С другой стороны,  $Z \subseteq H(Z)$ . Следовательно, точка  $x$  — единственная точка множества  $Z'$ , не попадающая в  $H(Z)$ . Получено противоречие с тем, что  $x \in H(Z)$ .

Итак,  $H(Z) \subseteq Z$ , откуда  $H(Z) = Z$ , т.е.  $Z$  — искомое множество.  $\square$

29. Теорема Кантора–Бернштейна дает достаточно простой инструмент сравнения мощностей. Достаточно показать, что первое множество равномощно какой-то части второго, а второе — какой-то части первого, т.е. что они взаимно друг в друга вкладываются. Это будет означать, что между ними существует биекция, т.е. что они равномощны. При этом данная теорема не предъявляет нам какого-то простого алгоритма построения этой биекции, т.к. явно найти и описать все хорошие множества — далеко не всегда разрешимая задача.
30. С помощью этой теоремы легко показать равномощность  $\mathbb{Q}$  и натурального ряда. Действительно,  $\mathbb{Q}$  легко вкладывается в часть множества  $\mathbb{Z} \times \mathbb{Z}$  (пары

взаимно простых составляют его часть). Но  $\mathbb{Z} \times \mathbb{Z}$  мы умеем явно нумеровать целыми числами, т.е. умеем строить инъекцию из  $\mathbb{Z} \times \mathbb{Z}$  в  $\mathbb{Z}$ , а значит, мы имеем вложение  $\mathbb{Q}$  в  $\mathbb{Z}$ . Ну, а вложение в обратную сторону тривиально. Таким способом получается много результатов о равномощности.

31. Назовем множество **не более чем счетным**, если оно счетно или конечно (или пустое).

**Теорема 13.3.** *Объединение не более чем счетного множества не более чем счетных множеств не более чем счетно.*

*Доказательство.* Мы можем считать, что нам дан счетный набор не более счетных множеств. При необходимости мы просто дополним этот набор до счетного пустыми множествами (ведь формулировка не требует, что они были разные). Раз их счетный набор, значит, они как-то уже пронумерованы. Пусть они обозначаются символами  $A_n$ . Тогда требуемое объединение равно

$$A = \bigcup_{n=1}^{\infty} A_n,$$

где все  $A_n$  — не более чем счетные множества.

Поскольку нам известно, что  $A_n$  — не более чем счетное, значит, существуют биекции  $f_n$  между  $A_n$  и либо  $\mathbb{N}$ , либо каким-то-конечным отрезком  $\mathbb{N}$ . В любом случае  $f_n$  — это инъекция из  $A_n$  в  $\mathbb{N}$ .

Теперь построим инъекцию из  $A$  в  $\mathbb{Z} \times \mathbb{Z}$ .

Пусть  $a \in A$ . Тогда существует  $n$  такой, что  $a \in A_n$ . Может оказаться так, что  $a$  лежит сразу во многих множествах  $A_n$ , в таком случае выберем наименьший из их номеров и обозначим его за  $n_a$ . Поскольку  $a \in A_{n_a}$ , мы можем применить к нему функцию  $f_{n_a}$ . Положим далее

$$g(a) = (n_a, f_{n_a}(a)).$$

Ясно, что  $g$  — инъекция, т.к. для разных точек  $a$  и  $a'$  либо отличаются номера  $n_a$  и  $n_{a'}$ , и следовательно  $g(a) \neq g(a')$  по свойствам упорядоченной пары, либо у них общий номер  $n_a$ , но тогда отличаются значения  $f_{n_a}(a)$  и  $f_{n_a}(a')$ , поскольку  $f_{n_a}$  является инъекцией, и, стало быть,  $g(a) \neq g(a')$ .

Итак, у нас есть инъекция  $g : A \rightarrow \mathbb{Z} \times \mathbb{Z}$ . К ней можно применить биекцию  $f : \mathbb{Z} \times \mathbb{Z} \leftrightarrow \mathbb{Z}$ , которую мы ранее выписывали в явном виде, а затем применить биекцию  $h : \mathbb{Z} \leftrightarrow \mathbb{N}$ , полагая  $h(m) = 2m$ , если  $m \geq 0$ , и  $h(m) = -2m - 1$ , если  $m < 0$ . Тогда композиция  $P = h(f(g(a)))$  будет инъекцией из  $A$  в  $\mathbb{N}$ .

Область значений  $P$  есть подмножество в  $\mathbb{N}$ . Она либо имеет максимум, и тогда это конечное множество, либо не имеет максимума, и тогда это бесконечное множество. В любом случае, область значений  $P$  можно перенумеровать так, чтобы номера шли подряд от нуля без пропусков. И тогда с помощью  $P^{-1}$  мы построим биекцию между  $A$  и либо конечным отрезком натурального ряда, либо самим  $\mathbb{N}$ .  $\square$

## 13.2 Изоморфизмы

### Конспект

1. Установление биекции между множествами позволяет нам судить об их количественном сходстве, но ничего не говорит о том, насколько похожи могут быть структуры, заданные на них. Поэтому на базе понятия биекции строятся более сильные критерии «похожести» двух множеств.
2. Центральным термином здесь является **«изоморфизм»**. Это — биекция, сохраняющая операции (например, сложение или умножение) и/или отношения (например, линейный порядок или отношение эквивалентности) и/или функционалы (например, норма или длина), заданные на этих двух множествах.
3. Поясним. Пусть у нас задана группа  $\mathbb{Z}_4$  со сложением по модулю 4, и группа корней 4 степени из 1 с операцией умножения (делители 1 в кольце гауссовых чисел). В обоих множествах 4 элемента, следовательно, существует биекция между ними. Причем, таких биекций ровно столько, сколько перестановок в группе  $S_4$ , т.е. 24 штуки. Однако, если дополнительно потребовать, чтобы результат сложения двух элементов в первой группе переходил в результат умножения образов этих элементов во второй группе, то таких биекций окажется всего две. Они-то и будут изоморфизмами этих групп.
4. Рассмотрим таблицы умножения группы  $\mathbb{Z}_9^*$  и сложения группы  $\mathbb{Z}_6$ :

$\mathbb{Z}_9^*$	1	2	4	5	7	8		$\mathbb{Z}_6$	0	1	2	5	4	3
1	1	2	4	5	7	8		0	0	1	2	5	4	3
2	2	4	8	1	5	7		1	1	2	3	0	5	4
4	4	8	7	2	1	5		2	2	3	4	1	0	5
5	5	1	2	7	8	4		5	5	0	1	4	3	2
7	7	5	1	8	4	2		4	4	5	0	3	2	1
8	8	7	5	4	2	1		3	3	4	5	2	1	0

Во второй таблице мы специально перемешали порядок элементов таким образом, чтобы показать изоморфизм групп, при котором умножение в  $\mathbb{Z}_9^*$  соответствует сложению в  $\mathbb{Z}_6$ , а соответствие элементов можно установить по

правилу:  $2^a \equiv b \pmod{9}$ , где  $a \in \mathbb{Z}_6$ ,  $b \in \mathbb{Z}_9^*$ , поскольку  $\mathbb{Z}_9^* = \langle 2 \rangle$ . Аналогичное соответствие можно посторить, опираясь на степени элементов 5 и 7 группы  $\mathbb{Z}_9^*$ .

5. Заметим, что не любая группа  $\mathbb{Z}_m^*$  изоморфна некоторой группе  $\mathbb{Z}_n$ . Например, в группе  $\mathbb{Z}_8^*$  содержится 4 элемента, но ни один из них не является образующим, группа  $\mathbb{Z}_8^*$  не является циклической, а значит, она не может быть изоморфна  $\mathbb{Z}_4$ .
6. Еще пример. Рассмотрим множества  $\mathbb{Z}$  и  $2\mathbb{Z}$  с обычными операциями сложения и умножения, и обычным линейным порядком на них. Мы уже знаем, что эти множества равномощны. Но посмотрим повнимательнее на биекцию  $f(n) = 2n$ , действующую из  $\mathbb{Z}$  в  $2\mathbb{Z}$ . Оказывается, что:

$$f(n + m) = f(n) + f(m), \quad n < m \Leftrightarrow f(n) < f(m),$$

т.е.  $f$  сохраняет сложение и порядок. А это значит, что  $f$  является изоморфизмом упорядоченных групп  $(\mathbb{Z}, <)$  и  $(2\mathbb{Z}, <)$ .

Однако,  $f$  не сохраняет умножение, поскольку  $f(nm) = 2nm \neq f(n)f(m)$ . Следовательно,  $f$  не является изоморфизмом колец  $(\mathbb{Z}, +, \cdot)$  и  $(2\mathbb{Z}, +, \cdot)$ . Более того, эти два кольца вовсе не изоморфны. Дело в том, что изоморфизм должен сохранять единицу, т.е. если какое-то число  $e$  является единицей по умножению в первом кольце, то  $f(e)$  будет единицей во втором кольце. Просто потому, что  $ne = n$  соответствует  $f(n) = f(n)f(e)$ . Но чему бы ни было равно  $f(1)$  в кольце  $2\mathbb{Z}$ , оно не обладает свойствами единицы, а значит, эти кольца не изоморфны.

7. Бывает и еще хуже. Изоморфизм работает только по отношению порядка, но не работает по алгебраическим операциям. Для этого достаточно вспомнить два изученных нами поля:  $\mathbb{Q}$  и  $\mathbb{A}$ .
8. Ясно, что эти поля не могут быть изоморфны по операциям, т.к. иначе в обоих полях одинаково бы разрешалось или не разрешалось уравнение  $x^2 = 2$ . Но мы знаем, что оно разрешается в  $\mathbb{A}$  и не разрешается в  $\mathbb{Q}$ . Тем не менее, с порядковым изоморфизмом у них все в порядке.

**Теорема 13.4.** *Все счетные неограниченные сверху и снизу плотные линейно упорядоченные множества порядково изоморфны друг другу.*

Иначе говоря, пусть у нас имеется два множества  $A$  и  $B$ , которые счетны (т.е. все их элементы можно перенумеровать натуральными числами), на них заданы линейные порядки  $<_A$  и  $<_B$  такие, что в обоих множествах нет ни наибольшего, ни наименьшего элемента, и эти множества плотны в своем порядке, тогда существует изоморфизм  $f : A \leftrightarrow B$ , сохраняющий порядок, т.е.  $f(x) <_B f(y) \Leftrightarrow x <_A y$ .



*Доказательство.* Будем строить соответствие пошагово. Пусть мы сделали некоторое соответствие для подмножеств  $A_n \subset A$  и  $B_n \subset B$  из  $n$  элементов. Возьмем любой элемент одного из множеств (для определенности  $A$ ), который не вошел в  $A_n$ . Посмотрим, в каком отношении он находится со всеми элементами из  $A_n$ . Он оказался либо наибольшим элементом, либо наименьшим элементом, либо стоящим между некоторыми элементами  $a_i$  и  $a_{i+1}$ . Найдем элемент в  $B$ , находящийся в таком же отношении со всеми элементами  $B_n$ . Мы можем это сделать, так как  $B$  — плотное множество без наибольшего и наименьшего элементов. Будем считать эти два элемента сопоставленными. Таким образом, мы научились получать из соответствия для  $n$  элементов соответствие для  $n + 1$  элемента. Чтобы в пределе получить соответствие для всех элементов, воспользуемся счетностью множеств  $A$  и  $B$ . Пронумеруем все элементы и на каждом четном шаге будем выбирать еще не взятый элемент из множества  $A$  с наименьшим номером, а на нечетном — из  $B$ .  $\square$

Из этой теоремы следует, например, что множество  $\mathbb{Q}$  с обычным линейным порядком и множество  $\mathbb{A}$  всех алгебраических чисел с обычным линейным порядком порядково изоморфны! Больше того, рациональный интервал  $(a; b)$  порядково изоморфен всему множеству  $\mathbb{Q}$ .

## 13.3 Действительные числа

### Конспект

1. Вспомним снова про множество  $\mathbb{B}$ , которое состоит из рациональных чисел вида  $k/2^n$ , где  $k \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ .
2. Это множество есть собственное подмножество  $\mathbb{Q}$ . Оно счетно и всюду плотно. Но главное — оно очень удобно устроено. При  $n = 0$  мы имеем целочисленную решетку на числовой прямой, при  $n = 1$  мы получаем все целые и полуцелые числа, при  $n = 2$  — все числа с шагом  $1/4$ . Обозначим

$$\mathbb{B}_n = \{k/2^n \mid k \in \mathbb{Z}\}.$$

Тем самым мы определяем некоторый слой в множестве  $\mathbb{B}$  с фиксированным шагом, равным  $1/2^n$ .

3. Множества  $\mathbb{B}_n$  хороши тем, что образуют возрастающую последовательность по вложению, которая стартует с  $\mathbb{Z}$  и заканчивается  $\mathbb{B}$ :

$$\mathbb{Z} = \mathbb{B}_0 \subset \mathbb{B}_1 \subset \mathbb{B}_2 \subset \dots \subset \mathbb{B}$$

В таком случае принято называть множество  $\mathbb{B}$  **пределом возрастающей цепи множеств**.

4. Поскольку расстояние между соседними точками  $\mathbb{B}_n$  очень быстро сокращается с ростом  $n$ , то любая точка на прямой может быть сколь угодно точно приближена точками множества  $\mathbb{B}$ .
5. Процесс последовательного приближения произвольной точки  $A$  на числовой прямой можно осуществить следующим образом.

**Step1** Находим целое число  $k$  такое, что точка  $A$  лежит в полуинтервале  $[k; k + 1)$ , т.е. либо между соседними целыми числами, либо совпадает с целым числом. Очевидно, что такое  $k$  определяется однозначно и всегда существует. Обозначим отрезок  $[k; k + 1]$  за  $\Delta_0$ . Ясно, что его границы  $k$  и  $k + 1$  есть элементы множества  $\mathbb{B}_0$ .

**Step2** Пусть далее  $n$  — это номер текущего интервала (начиная с нуля).

**Step3** Находясь в отрезке  $\Delta_n$ , делим его на 2 части посередине так, чтобы получилось два одинаковых полуинтервала: если  $\Delta_n = [a; b]$ , то новые полуинтервалы будут  $[a; (a+b)/2]$  и  $[(a+b)/2; b]$ . Точка  $A$  лежит в одном из этих полуинтервалов: либо в левом, либо в правом, третьего не дано. Заметим, что и границы  $\Delta_n$ , и его середина — это точки множества  $\mathbb{B}$ , причем границы  $\Delta_n$  находятся в множестве  $\mathbb{B}_n$ , а его середина — в множестве  $\mathbb{B}_{n+1}$ . Таким образом, это подразбиение является переходом к следующему уровню разбиения в множестве  $\mathbb{B}$ .

**Step4** Тогда через  $\Delta_{n+1}$  обозначим отрезок  $[a; (a+b)/2]$ , если  $A \in [a; (a+b)/2]$ , и отрезок  $[(a+b)/2; b]$ , если  $A \in [(a+b)/2; b]$ . После чего перейдем на предыдущий шаг, увеличивая номер  $n$  на 1.

В результате мы получим последовательность вложенных отрезков

$$[k; k + 1] = \Delta_0 \supset \Delta_1 \supset \Delta_2 \supset \dots$$

Эта последовательность монотонно убывает, причем на каждом шаге отрезок становится вдвое короче, а концы отрезков прыгают по точкам множества  $\mathbb{B}$ , постепенно переходя ко все более мелкой сетке — от  $\mathbb{B}_n$  к  $\mathbb{B}_{n+1}$ .

6. Где же в итоге окажется точка  $A$ ?
7. Поскольку  $A \in \Delta_n$  для всех  $n$ , то она также лежит в пересечении всех этих отрезков:

$$A \in \bigcap_n \Delta_n.$$

Такое пересечение называется пределом убывающей цепи множеств.

8. Может ли в этом пересечении лежать еще какая-то точка? Ответ: нет. Если мы возьмем любую другую точку  $B \neq A$ , то, очевидно, что между ними есть какое-то расстояние  $\varepsilon > 0$ . Возьмем тогда такое  $n$ , что  $\varepsilon > 1/2^n$ , и посмотрим на отрезок  $\Delta_n$ . Его длина равна  $1/2^n$  и он содержит точку  $A$ . Но тогда он

не содержит точку  $B$ , а значит, и пересечение всех отрезков  $\Delta_n$  не содержит точку  $B$ .

9. Итак, точка  $A$  — единственный представитель пересечения отрезков  $\Delta_n$ :

$$\bigcap_n \Delta_n = \{A\}.$$

10. По сути, мы уже сформулировали главный принцип непрерывности (полноты) числовой прямой — принцип вложенных отрезков. Однако, здесь нужно проявить осмотрительность. Дело в том, что мы не доказали существование точки  $A$ , а сразу же выбрали ее из существующих точек прямой. Но в настоящий момент нам известны только рациональные числа и алгебраические, поэтому разумно ожидать, что точка  $A$  есть одно из таких чисел. Но рассмотренный принцип «ловли» произвольной точки на прямой с помощью стягивающейся сетки двоично-рациональных чисел сам по себе является мощным инструментом для определения новых чисел и, что самое главное, для ликвидации всех возможных дыр на числовой оси, состоящей из алгебраических чисел.
11. На самом деле, вовсе не очевидно, что если мы выберем произвольную последовательность вложенных отрезков, длина которых стремится к нулю с ростом номера, то в пределе получим множество, состоящее из одной точки. Быть может, никакой точки там вовсе не окажется. Поэтому приходится вводить принцип непрерывности при помощи **аксиомы непрерывности** (она же — аксиома полноты).
12. У этой аксиомы существует много равносильных формулировок, и мы начнем с той, к которой нас подготовил сюжет по поимке точки  $A$  в сеть множества  $\mathbb{B}$ .

## A1. Принцип вложенных отрезков

*Пусть дана последовательность вложенных отрезков на прямой:*

$$[a_0; b_0] \supseteq [a_1; b_1] \supseteq [a_2; b_2] \supseteq \dots [a_n; b_n] \supseteq \dots,$$

*где  $a_n < b_n$  для всех  $n$ . Тогда множество точек, принадлежащих всем отрезкам одновременно, не пусто.*

13. В терминах, которые мы упоминали выше, принцип A1 можно переформулировать так: любая убывающая по вложению бесконечная цепь отрезков имеет непустой предел.

14. Отметим, что в формулировке мы не требовали, чтобы концы отрезков были двоично-рациональными числами, а также не требовали, чтобы их длина стремилась к нулю. Очевидно, что случай с двоично-рациональными отрезками является частным случаем последовательности вложенных отрезков, а значит, в силу принципа **A1** имеет непустой предел.

На самом деле, если сформулировать принцип вложенных отрезков, используя только двоично-рациональные концы отрезков и деление отрезка пополам на каждом шаге, мы получим эквивалентную формулировку принципа вложенных отрезков. Но доказательство этого факта мы оставим за рамками курса.

15. Принцип вложенных отрезков уже позволяет нам доказать, что на числовой прямой существуют не только алгебраические числа, более того, что точек на прямой существует несчетное множество.

Предположим, что это не так, и пусть на прямой есть только счетный набор точек. В соответствии с определением счетности мы можем перенумеровать все эти точки натуральными числами  $x_0, x_1, x_2, \dots$ .

Построим цепь вложенных отрезков следующим способом. Выберем любой отрезок  $\Delta_0$  (можно считать, что он имеет концы в множестве  $\mathbb{W}$ , но это не обязательно) так, чтобы  $x_0 \notin \Delta_0$ . Точка  $x_1$  может лежать или не лежать в отрезке  $\Delta_0$ , но в любом случае мы можем выбрать отрезок  $\Delta_1$  так, чтобы выполнялись условия:  $\Delta_1 \subseteq \Delta_0$  и  $x_1 \notin \Delta_1$ . Заметим, что при этом также  $x_0 \notin \Delta_1$ . Далее, точка  $x_2$  может лежать или не лежать в отрезке  $\Delta_1$ , но мы всегда можем выбрать отрезок  $\Delta_2 \subseteq \Delta_1$  так, чтобы  $x_2 \notin \Delta_2$ . Продолжаем эту процедуру до бесконечности, поддерживая следующую ситуацию:

$$\Delta_{n+1} \subseteq \Delta_n, \quad x_0, \dots, x_{n+1} \notin \Delta_{n+1}.$$

Но тогда в пересечении  $\cap \Delta_n$  нет ни одной точки  $x_n$ , т.е. нет вообще ни одной точки числовой прямой. Но в силу принципа **A1** там должна быть хотя бы одна точка. Противоречие.

Таким образом, принцип вложенных отрезков гарантирует нам несчетность множества чисел на прямой. Насколько велико это множество, мы сможем оценить чуть позже.

16. Следующее, что можно отметить, опираясь на наш пример с поимкой точки  $A$  в сеть множества  $\mathbb{W}$ , это что последовательность левых границ вложенных отрезков не убывает. На каждом шаге левая граница  $\Delta_n$  либо остается такой же, как у предыдущего отрезка, либо перескакивает в его середину. Но при этом все левые границы отрезков  $\Delta_n$  остаются ограниченными сверху правой границей начального отрезка  $\Delta_0$ . То же самое мы видим и в ситуации с произвольной последовательностью вложенных отрезков, которую мы описывали при формулировке принципа **A1**.

17. Аналогичное наблюдение можно вывести и для правых концов вложенных отрезков. Мы имеем некую бесконечную монотонную последовательность точек, и притом ограниченную, т.е. находящуюся в некотором заранее известном отрезке.

18. Введем определения. Последовательность  $\{x_n\}_{n=0}^{\infty}$  называется **убывающей** (или **возрастающей**), если для всех  $n$  выполняется неравенство  $x_n \geq x_{n+1}$  ( $x_n \leq x_{n+1}$ ). Убывающие и возрастающие последовательности называются **монотонными**. Последовательность **строго** монотонна (строго убывающая или строго возрастающая), если указанное неравенство всегда строгое.

Множество  $X$  на прямой называется **ограниченным сверху**, если существует точка  $a$  такая, что  $X \leq a$ .<sup>1</sup> Если ситуация противоположная, т.е.  $X \geq a$ , то множество  $X$  называется **ограниченным снизу**. Если множество ограничено сверху и снизу, то оно называется **ограниченным**.

Последовательность ограничена (сверху и/или снизу), если ограничено ее множество значений (сверху и/или снизу). Отметим, что последовательность мы рассматриваем не просто как множество точек на прямой, а как функцию из  $\mathbb{N}$  в множество точек прямой или любое другое множество. Это позволяет рассматривать, например, стационарные последовательности, когда  $x_n = \text{const}$ , или циклические последовательности, когда  $x_n$  принимает конечный набор значений, последовательно повторяя их. Например,  $x_n = n \pmod{m}$  повторяет значения  $0, 1, \dots, m-1$ .

19. Имея любую монотонную ограниченную последовательность, мы легко можем выстроить цепь вложенных отрезков. Если эта последовательность неубывающая, то в качестве левых границ отрезков берем ее элементы, а правую границу зафиксируем в какой-то одной точке, которая точно больше всех членов последовательности (ее существование следует из ограниченности последовательности).

20. Можем усилить эффект, если в качестве правых границ вложенных отрезков на  $n$ -ом шаге выбирать наименьшее из чисел множества  $\mathbb{B}_n$ , превосходящих все оставшиеся члены последовательности.

$$a_n = x_n, \quad b_n = \min\{q \in \mathbb{B}_n \mid \forall j \geq n \ x_j \leq q\}$$

В этом случае последовательность  $b_n$  будет убывающей, причем она будет очень быстро сближаться с «хвостом» последовательности  $\{x_n\}$ , т.к. шаг между соседними числами в множестве  $\mathbb{B}_n$  равен  $1/2^n$ . И тогда длина отрезка  $[a_n; b_n]$  с каждым шагом будет становиться все меньше, так что в предельном множестве, существование которого нам гарантирует принцип **A1**, не сможет

<sup>1</sup>Мы ранее уже вводили сравнение множеств и множеств с точкой.  $X \leq Y$ , если для всех  $x \in X, y \in Y$  имеем  $x \leq y$ .  $X \leq a$ , если  $X \leq \{a\}$ .

находиться две и более точек. А та единственная, которая останется внутри пересечения всех  $[a_n; b_n]$ , будет пределом последовательности  $\{x_n\}$ , т.е. такой точкой, к которой данная последовательность приближается вплотную, не оставляя никакого зазора.

21. Введем одно из основных понятий математического анализа. Число  $a$  называется **пределом последовательности**  $\{x_n\}$  и обозначается

$$a = \lim_{n \rightarrow \infty} x_n,$$

если для любого  $\varepsilon > 0$  существует такой номер  $N$ , что для всех  $n > N$  имеет место неравенство  $|x_n - a| < \varepsilon$ . Если последовательность  $\{x_n\}$  имеет предел, то она называется **сходящейся** (к данному пределу), в противном случае — **расходящейся**.

Назовем интервал  $(a - \varepsilon; a + \varepsilon)$   $\varepsilon$ -окрестностью точки  $a$ . Ясно, что утверждение  $|x_n - a| < \varepsilon$  означает, что  $x_n$  лежит в  $\varepsilon$ -окрестности точки  $a$ . Кроме того, очень часто говорят «почти все члены последовательности», когда имеют ввиду некоторый ее хвост, т.е. ту же последовательность, но за исключением, быть может, какого-то ее конечного начального отрезка. Поэтому тот факт, что  $a$  является пределом последовательности  $\{x_n\}$ , можно записать следующими словами: *в любой сколь угодно малой окрестности точки  $a$  лежат почти все члены последовательности  $\{x_n\}$ .*

Стоит отметить, что символика пределов в обязательном порядке предписывает указывать, при каком именно изменении параметра совершается предельный переход. В нашем случае параметром последовательности является индекс (или номер) ее членов, т.е. число  $n$ . И если еще раз внимательно прочитать определение предела, а также смысл фразы «почти все члены последовательности», то мы увидим, что требование малого отклонения от предела выполняется при больших  $n$ , т.е. при  $n > N$  при некотором номере  $N$ , который, вообще говоря, зависит от выбранного  $\varepsilon$ . И весь смысл данного предела в том, что при забегании индекса  $n$  в сторону бесконечности величина  $x_n$  становится близкой к  $a$ .

Кроме того, параметров может быть несколько, и поэтому всегда следует указывать, относительно какого из них осуществляется предельный переход.

Приведем пример. Пусть  $x_{n,m} = m/(1 + (n - m)^2)$ . Найдём её предел при  $n \rightarrow \infty$ . Мы можем построить экспериментальный график и убедиться в том, что предел равен нулю.

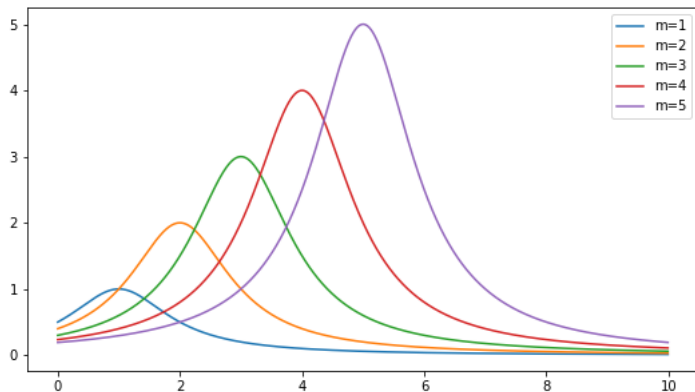


График  $x_{n,m} = \frac{m}{(1 + (n - m)^2)}$ .

Докажем, что так оно и есть на самом деле. Выберем произвольный достаточно малый  $\varepsilon > 0$ . Поскольку  $x_{n,m} > 0$ , нам достаточно установить, при каких  $n$  выполняется неравенство  $x_{n,m} < \varepsilon$ , что и будет означать близость к нулю. Решая это неравенство, находим, что

$$n > m + \sqrt{\frac{m}{\varepsilon} - 1},$$

откуда видно, что начиная с некоторого  $N$  (например, можно округлить вверх корень и добавить  $m$ ) для всех последующих  $n$  требуемое неравенство выполняется. Стало быть, по определению получаем, что

$$\lim_{n \rightarrow \infty} \frac{m}{(1 + (n - m)^2)} = 0.$$

Однако, даже по графику видно, что если мы будем менять параметр  $m$  вместо  $n$ , то мы увидим неограниченный рост величины  $x_{n,m}$ , так что ее предел при  $m \rightarrow \infty$  и любом фиксированном  $n$  будет равен  $+\infty$ .

Но и это еще не все. Можно так подобрать зависимость параметров  $n$  и  $m$  (например, положить  $m = t^2$  и  $n = t^2 + t$ , тогда получим  $x_{n,m} = t^2/(1 + t^2) \rightarrow 1$  при  $t \rightarrow \infty$ ), что  $x_{n,m}$  будет сходиться к любому наперед заданному положительному числу.

Поэтому всегда очень важно указывать, при каком изменении какого параметра ищется предел.

22. Из рассуждений, проведенных выше относительно монотонной ограниченной последовательности, ясно, что она должна иметь предел в силу принципа **A1**.

На самом деле, верно как это, так и обратное: если монотонные ограниченные последовательности имеют предел, то выполняется принцип вложенных отрезков. Это совсем легко установить, поскольку границы вложенных отрезков образуют две монотонные ограниченные последовательности, а значит, имеют пределы. Причем как эти пределы, так и точки, лежащие между ними, будут принадлежать пределу цепи вложенных отрезков.

## A2. Предел монотонной последовательности

*Всякая монотонная ограниченная последовательность имеет предел.*<sup>2</sup>

23. Принцип **A2** равносильен принципу **A1**.
24. Следующее, что мы можем заметить из сюжета с поимкой точки  $A$  сетью точек множества  $\mathbb{B}$ , это то, что границы отрезков не просто стремятся к точке  $A$ , но и как бы стремятся друг к другу, т.е. расстояния между всеми членами последовательности, начиная с некоторого номера, становятся сколь угодно малыми. Поэтому, даже ничего не зная о существовании предела, мы можем сделать некоторые выводы о последовательности.
25. Последовательность  $\{x_n\}$  называется **фундаментальной**, если для любого  $\varepsilon > 0$  существует такой номер  $N$ , что для всех номеров  $n, m > N$  выполняется  $|x_n - x_m| < \varepsilon$ . Иными словами, *почти все члены фундаментальной последовательности находятся сколь угодно близко друг к другу*.

## A3. Предел фундаментальной последовательности

*Всякая фундаментальная последовательность имеет предел.*

26. Принцип **A3** равносильен двум предыдущим принципам.
27. Мы уже говорили о том, что множество может быть ограничено сверху или снизу. Пусть  $X$  ограничено сверху числом  $a$ . Тогда число  $a$  называется его **верхней гранью**. Ясно, что если  $a$  — верхняя грань  $X$ , то верхними гранями будут также  $a + 1, a + 10000, a + 0.0001$  и т.д. Все числа, большие  $a$ , будут верхними гранями  $X$ .
28. Вспомним уравнение  $x^2 = 2$ . Пусть  $X = \{x \mid x^2 < 2 \wedge x > 0\}$ . Это есть интервал  $(0; \sqrt{2})$ . Мы помним, что в  $\mathbb{Q}$  нет числа  $\sqrt{2}$ , поэтому в рамках множества  $\mathbb{Q}$  верхними гранями  $X$  будут положительные рациональные числа  $r$  такие, что  $r^2 > 2$ . И среди этих чисел нет наименьшего, т.к. он недостижимо в  $\mathbb{Q}$ .

---

<sup>2</sup>Если быть точным, то еще требуется архимедовость системы чисел, в которой этот принцип постулируется, но для числовой прямой, в которой множество  $\mathbb{Z}$  не ограничено ни сверху, ни снизу, это выполняется автоматически.



Однако, стоит нам выйти в поле алгебраических чисел, как мы уже можем использовать  $\sqrt{2}$ , и он будет не просто верхней гранью  $X$ , а наименьшей из всех верхних граней.

29. Наименьшая из верхних граней  $X$  называется **супремумом**  $X$  или **точной верхней гранью**  $X$ .
30. Предлагаем читателю самостоятельно определить понятие точной нижней грани.
31. К точной верхней грани  $X$  мы можем подбираться, находясь внутри  $X$ , выбирая каждый раз все новое число из  $X$ , находящееся как можно ближе к его верхней грани. Например, у цепи вложенных отрезков есть множество левых границ, образующее возрастающую последовательность. При этом все правые границы отрезков будут верхними гранями для этой последовательности. И если в пределе получится множество, состоящее из одной точки (как в сюжете с ловлей точки  $A$  точками множества  $\mathbb{B}$ ), то эта точка и будет точной верхней гранью для последовательности левых границ вложенных отрезков.
32. Мы снова видим некоторую связь между существованием супремума и аксиомой непрерывности в ее трех предыдущих формулировках. На самом деле, эта связь абсолютная.

#### A4. Существование точных граней

**A4** Всякое ограниченное сверху множество имеет точную верхнюю грань.

**A4'** Всякое ограниченное снизу множество имеет точную нижнюю грань.

33. Эти два принципа непрерывности эквивалентны друг другу и трем предыдущим принципам.
34. Наконец, заметим, что существует некоторая двойственность между верхними и нижними гранями и точными гранями. Так, если взять некоторое множество  $X$ , ограниченное сверху, то оно само будет множеством нижних граней (не обязательно всех) для множества  $Y$  своих верхних граней. При этом окажется, что  $\sup X = \inf Y$ . Аналогичная ситуация и с ограниченным снизу множеством. Возникает желание разбить всю числовую прямую на два луча — левый и правый, — так, чтобы левый был множеством нижних граней для верхнего и наоборот. Такое разбиение называется сечением.
35. В соответствии с определением, данным в разделе 12.1, пара  $(X, Y)$  непустых подмножеств, таких, что их объединение  $X \cup Y = \mathbb{Q}$ ,  $X \cap Y = \emptyset$  и  $X < Y$ , называется **сечением**.<sup>3</sup>

---

<sup>3</sup>Иногда определяется только нижний класс, и он называется сечением. Оба определения эквивалентны.

36. Ранее мы уже видели такое разбиение. Оно представляло собой два интервала рациональных чисел:  $(-\infty; \sqrt{2})$  и  $(\sqrt{2}; +\infty)$ . Действительно, их объединение равно  $\mathbb{Q}$ , пересечение пусто, и левый интервал меньше правого.
37. В случае  $\mathbb{Q}$  сечение может состоять из двух интервалов, т.е. таких множеств, что верхнее не имеет минимума, а нижнее не имеет максимума, и при этом между ними ничего нет. И это говорит нам о том, что в  $\mathbb{Q}$  имеются дырки. В случае  $\mathbb{A}$  дырки найти сложнее, но, например, разбиение на интервалы  $(-\infty; \pi)$  и  $(\pi; +\infty)$  доставляет такой пример, поскольку число  $\pi$  не является алгебраическим.<sup>4</sup>
38. Так вот, еще один подход к определению непрерывности числовой прямой заключается в том, чтобы исключить такие дырки.

## А5. Дедекиндовы сечения

*Если  $(X, Y)$  — сечение числовой прямой, то существует точка  $z$  такая, что  $X \leq z \leq Y$ .*

39. При этом точка  $z$  обязана попасть либо в верхний, либо в нижний класс разбиения (ей просто деваться некуда), т.е. всякое сечение числовой прямой должно быть дедекиндовым (в соответствии с данным нами определением в разделе 12.1). Иначе говоря, принцип **A5** утверждает, что линейный порядок на числовой прямой должен быть непрерывным.
40. Формулировка аксиомы непрерывности в виде принципа **A5** эквивалентна всем предыдущим формулировкам **A1–A4**.
41. Наконец, самое главное определение данной главы. Числовая прямая, удовлетворяющая аксиоме непрерывности, называется **вещественной (действительной) прямой** и обозначается  $\mathbb{R}$ .
42. Если мы соберем вместе все накопленные свойства  $\mathbb{R}$ , то мы увидим, что  $\mathbb{R}$  — это *непрерывное линейно упорядоченное поле*. Известно, что такое поле единственное с точностью до изоморфизма, сохраняющего операции поля и линейный порядок.

## Задачи

- Доказать, что между любыми двумя рациональными числами  $r \neq q$  лежит какое-то двоично-рациональное.
- 

---

<sup>4</sup>Этот факт был доказан только в XX веке!

#### § 4. Созидание иррациональных чисел

Последними словами уже достаточно ясно указывается, каким образом разрывная область  $R$  рациональных чисел должна быть дополнена до превращения ее в непрерывную. Как это поставлено было на вид в § 1 (III), каждое рациональное число  $a$  производит разложение системы  $R$  на два класса  $A_1$  и  $A_2$  такого рода, что каждое число  $a_1$  первого класса меньше каждого числа  $a_2$  второго класса. Число  $a$  представляет либо наибольшее число класса  $A_1$ , либо наименьшее число класса  $A_2$ . Если теперь дано какое-либо подразделение системы  $R$  на два класса  $A_1, A_2$ , обладающее только тем характерным свойством, что каждое число  $a_1$  из  $A_1$  меньше каждого числа  $a_2$  из  $A_2$ , то для краткости мы будем называть такое подразделение *сечением* и будем его обозначать через  $(A_1, A_2)$ . Мы можем тогда сказать, что каждое число  $a$  производит одно или, собственно, два сечения, на которые мы, однако, не будем смотреть, как на существенно различные \*); это сечение имеет *кроме того* то свойство, что либо между числами первого класса есть наибольшее, либо между числами второго класса существует наименьшее. И наоборот, если сечение обладает и этим свойством, то оно производится *этим* наибольшим или наименьшим числом.

Рис. 13.1: Цитата из работы О.Дедекинда «Непрерывность и иррациональные числа» в пер. Шатуновского, 1923.

- 3.
- 4.
- 5.
- 6.

## 13.4 Модели действительных чисел

### Конспект

1. В предыдущем разделе было сформулировано пять вариантов аксиомы непрерывности, которая необходима для того, чтобы узаконить действительные числа как непрерывную числовую структуру. Аксиома непрерывности не оставляет дыр на числовой прямой, поскольку вводит в обращение все числа, к которым можно обратиться с помощью счетной последовательности рациональных чисел.
2. Тем не менее, одной лишь аксиомы недостаточно, чтобы действительные числа имели право на существование. Необходимо убедиться в том, что их можно непротиворечиво сконструировать. Поэтому здесь мы рассмотрим несколько подходов к построению действительных чисел.

### Дедекиндовы сечения

3. Первый подход связан непосредственно с тем, чем мы закончили предыдущий раздел — с дедекиндовыми сечениями. А именно, рассмотрим все сечения множества рациональных чисел, причем только такие, у которых нижний класс не содержит наибольшего элемента (т.е. если есть между классами граница, то она отнесена к верхнему классу). И соберем в множество  $R$  нижние классы всех таких сечений. Таким образом,  $R$  состоит из подмножеств  $X \subset \mathbb{Q}$  таких, что

$$X \neq \emptyset, \quad X \neq \mathbb{Q}, \quad \forall r, q \in \mathbb{Q} (q \in X \wedge (r < q) \rightarrow (r \in X)), \quad \nexists \max X.$$

Таким образом,  $R$  — это множество лучей из рациональных чисел, направленных в  $-\infty$ .

4. На множестве  $R$  введем операцию сложения: пусть  $\alpha, \beta \in R$ , тогда положим

$$\alpha + \beta = \{x + y \mid x \in \alpha, y \in \beta\},$$

т.е. просто сложим их по Минковскому.

5. Можно проверить, что  $R$  с такой операцией сложения является абелевой группой, т.е. сложение ассоциативно, коммутативно, имеется нейтральный элемент  $0 = \{x \in \mathbb{Q} \mid x < 0_{\mathbb{Q}}\}$ , где  $0_{\mathbb{Q}}$  — ноль в системе рациональных чисел, и для каждого  $\alpha$  имеется противоположный элемент  $-\alpha = \{x \in \mathbb{Q} \mid (-x > \alpha) \wedge (-x \neq \min \mathbb{Q} \setminus \alpha)\}$ .

Здесь появляется первая тонкость определения. По сути, в качестве  $\alpha$  мы берем соответствующий ему верхний класс сечения и умножаем на -1 (в поле рациональных чисел). Однако верхний класс может иметь минимум, а элемент  $R$  не должен иметь максимума, поэтому мы подстраховываемся и выбрасываем из верхнего класса  $\mathbb{Q} \setminus \alpha$  его минимум (если такой существует).

6. Достаточно легко определяется и порядок на  $R$ . Скажем, что  $\alpha < \beta$ , если  $\alpha \subset \beta$  (как собственное подмножество).
7. Отсюда же следует согласованность сложения и порядка, поскольку сдвиг вверх или вниз интервалов  $\alpha < \beta$  не меняет их вложенности.
8. Сложнее дело обстоит с умножением. Если мы попытаемся умножить  $\alpha \cdot \beta$  по Минковскому, то произведение будет содержать сколь угодно большие числа (при перемножении двух чисел, сильно меньших 0 в поле  $\mathbb{Q}$ ). Поэтому сначала определяется произведение положительных чисел: пусть  $\alpha > 0$  и  $\beta > 0$ , тогда

$$\alpha \cdot \beta = \{xy \mid (x \in \alpha) \wedge (x \geq 0) \wedge (y \in \beta) \wedge (y \geq 0)\} \cup \mathbb{Q}^-,$$

где  $\mathbb{Q}^-$  — все отрицательные рациональные числа.

Далее, просто полагаем, что

$$\alpha \cdot \beta = \begin{cases} 0, & \text{если } (\alpha = 0) \vee (\beta = 0) \\ (-\alpha) \cdot \beta, & \text{если } (\alpha < 0) \wedge (\beta > 0) \\ \alpha \cdot (-\beta), & \text{если } (\alpha > 0) \wedge (\beta < 0) \\ (-\alpha) \cdot (-\beta), & \text{если } (\alpha < 0) \wedge (\beta < 0) \end{cases}$$

9. Можно проверить, что такая операция умножения на  $R$  ассоциативна, коммутативна, имеет единицу  $1 = \{x \in \mathbb{Q} \mid x < 1_{\mathbb{Q}}\}$ , где  $1_{\mathbb{Q}}$  — единица в системе рациональных чисел, и для каждого положительного  $\alpha \in R$  имеется обратный по умножению

$$1/\alpha = \{x \in \mathbb{Q} \mid \exists y > \alpha (x < 1/y)\},$$

а обратный к отрицательному числу определяется сменой знака:  $1/\alpha = -(1/(-\alpha))$ , если  $\alpha < 0$ .

10. Кроме того, можно доказать, что операции сложения и умножения удовлетворяют дистрибутивному закону, а также что умножение согласовано с порядком.

11. Таким образом,  $R$  с указанными операциями и порядком есть упорядоченное поле. Остается показать его непрерывность.
12. Для этого воспользуемся формулировкой аксиомы непрерывности в виде **A4**. Пусть  $X \subset R$  непусто и ограничено сверху. Положим  $\alpha = \cup X$ . Т.е. мы включаем в множество  $\alpha$  все рациональные числа входящие во все элементы множества  $X$ . Легко видеть, что  $X \leq \alpha$  (в смысле сравнения множества и числа в линейном порядке на  $R$ ). В то же время любая верхняя грань  $X$  окажется не меньше  $\alpha$ , иначе она бы отсекала какое-то рациональное число одного из элементов  $X$ . Таким образом,

$$\sup X = \cup X.$$

13. Итак, множество  $R$ , построенное из подмножеств  $\mathbb{Q}$  специального вида, с заданными на нем операциями и порядком, является непрерывным упорядоченным полем, т.е. полем действительных чисел  $\mathbb{R}$ .

## Двочинные дроби

14. Следующий подход к моделированию  $\mathbb{R}$  прямо связан с нашим множеством  $\mathbb{B}$ . Вспомним сюжет о поимке точки  $A$  в сеть точек множества  $\mathbb{B}$ , т.е. рациональных точек со знаменателями вида  $2^n$ . Мы выстраивали убывающую цепь отрезков, концы которых находятся в множестве  $\mathbb{B}_n$ , т.е. имеют вид  $[k/2^n; (k+1)/2^n]$ . Длина этих отрезков быстро стремится к нулю, а по аксиоме непрерывности в форме **A1** существует непустой предел этой цепи отрезков, который состоит из единственной точки  $A$ .
15. Почему бы тогда не обращаться к точке  $A$  с помощью этой последовательности? Точнее, мы определим некоторый условный код, который позволит нам однозначно поймать точку  $A$  и никакую другую.
16. Вспомним алгоритм построения этих отрезков. Сначала мы выбираем целочисленный полуинтервал  $[k; k+1)$ , в котором лежит  $A$ . Ок — запишем число  $k$  как стартовое число кода.
17. Затем мы делим этот интервал ровно пополам:  $[k; k+1) = [k+1/2; k+1) \cup [k+1/2; k+1)$ . Точка  $A$  лежит либо в левом полуинтервале, либо в правом. Ок, следующим числом кода запишем 0, если  $A$  лежит в левом интервале, и 1 — если в правом. Перйдем к соответствующему интервалу.
18. Снова поделим его пополам и произведем аналогичную процедуру записи следующей цифры кода. И так будем продолжать до бесконечности.

19. В итоге у нас получится код, стартующий с некоторого целого числа, после которого идет бесконечная (счетная) цепочка нулей и единиц. Этот код однозначно формируется по заданной точке  $A$  (поскольку мы всегда работаем с полуинтервалами, а они всякий раз выбираются единственным способом).
20. Особенностью данного кода является то, что в нем нет хвоста единиц, т.е. когда начиная с некоторой позиции все цифры равны 1. Это объясняется очень просто: если есть хвост единиц, то начиная с какого-то шага алгоритм всегда выбирал правый интервал, в результате чего хвост последовательности вложенных отрезков имел бы вид

$$[r/2^m - 1/2; r/2^m] \supset [r/2^m - 1/4; r/2^m] \supset [r/2^m - 1/8; r/2^m] \supset \dots,$$

где  $r$  и  $m$  не зависят от  $n$ . Но пределом такой цепи будет, очевидно, множество  $\{r/2^m\}$ , т.е. такая цепь вложенных отрезков должна сходиться к числу  $r/2^m$ . Проблема в том, что алгоритм еще на предыдущем  $m - 1$  шаге выберет полуинтервал, лежащий справа от этой точки, в результате чего отрезками, сходящимися к точке  $r/2^m$ , будут такие

$$[r/2^m; r/2^m + 1/2] \supset [r/2^m; r/2^m + 1/4] \supset [r/2^m; r/2^m + 1/8] \supset \dots,$$

и мы увидим не хвост единиц, а хвост нулей! Правда, перед ним будет стоять единица.

То есть, кодовая последовательность вида  $k, [01]*\dots 0111111\dots$  невозможна, а вместо нее будет последовательность  $k, [01]*\dots 1000000\dots$ . Здесь символ  $[01]*$  представляет собой *регулярное выражение*, означающее цепочку произвольной конечной длины (в том числе нулевой длины), состоящую только из символов 0 и 1.

21. Верно и обратное. По такому коду (без хвоста единиц) можно однозначно восстановить закодированную им точку  $A$ .
22. Поэтому между точками вещественной прямой  $\mathbb{R}$  и кодами указанного вида существует взаимно однозначное соответствие (биекция), и это значит, что моделью  $\mathbb{R}$  может быть множество всех таких цепочек.
23. Точнее, положим

$$R = \{(k, f) \mid k \in \mathbb{Z}, f : \mathbb{N} \rightarrow \{0, 1\}, \forall n \exists m > n (f(m) = 0)\}.$$

Здесь условие  $\forall n \exists m > n (f(m) = 0)$  как раз и означает, что в последовательности  $f$  нет хвоста единиц (ноль встречается бесконечно часто).

24. Сложности в такой модели  $\mathbb{R}$  начинаются, когда мы хотим определить операции сложения и умножения. Порядок же определяется предельно просто.

Пусть даны две последовательности  $(k, f)$  и  $(k', f')$ . Отношение порядка между ними основано на сравнении первого расхождения кодов. Если  $k < k'$ , то  $(k, f) < (k', f')$ . Если  $k = k'$ , смотрим  $f(0)$  и  $f'(0)$ . Если  $f(0) < f'(0)$ , то  $(k, f) < (k', f')$ . Если они равны, то переходим к следующей цифре кода, и т.д. Если не нашлось ни одного расхождения в коде, то числа  $(k, f)$  и  $(k', f')$  равны.

25. Мы не будем здесь заниматься рекурсивным определением операций сложения и умножения. Скажем только, что его можно задать, используя арифметику двоично-рациональных чисел множества  $\mathbb{B}$ , и во многом он напоминает определение операций в следующей модели  $\mathbb{R}$ , основанная на классах эквивалентных последовательностей. Действительно, ведь двоичный код задает не только алгоритм вычисления вложенных отрезков, он задает последовательность их левых границ, которая сходится к адресуемому числу  $A$ . А это — последовательность двоично-рациональных чисел, которые мы умеем складывать и умножать, не выходя за рамки множества  $\mathbb{B}$ .

26. Больше того, число, которое закодировано парой  $(k, f)$ , можно записать в виде бесконечной суммы

$$A = k + \sum_{n=0}^{\infty} \frac{f(n)}{2^n},$$

поскольку переход к правому отрезку на  $n$ -ом шаге в описанном алгоритме означает добавление  $1/2^n$  к левой границе предыдущего отрезка, а переход к левому отрезку означает добавление  $0/2^n$ . Так что любое действительное число можно записать в виде разложения по степеням 2, а это и есть не что иное как записать произвольного числа в двоичной системе счисления. Число  $k$  при этом можно тоже записать в двоичном коде, и тогда код произвольного числа будет иметь вид: конечный набор нулей и единиц, затем стоит точка, затем идет бесконечный набор нулей и единиц (без хвоста единиц).

27. Завершая описание двоичной модели, скажем, что в качестве основания можно выбрать любое натуральное число  $d > 1$ . Например, если мы хотим получить троичные последовательности, нам следует модифицировать алгоритм разбиения на отрезки следующим образом: интервал  $[k; k + 1)$  делить на три части  $[k; k + 1/3)$ ,  $[k + 1/3; k + 2/3)$  и  $[k + 2/3; k + 1)$ , и далее к каждому следующему интервалу применять аналогичное деление на 3 части. В результате для записи кода будем выбирать 0, если  $A$  оказалась в левом интервале, 1 — если в среднем, 2 — если в правом. И получим код из цифр 0,1,2, причем без хвоста двоек. Все рассуждения здесь полностью аналогичны предыдущему.

28. Мы можем использовать число  $d = 10$  в качестве основания, и каждое действительное число записывать кодом из цифр  $0 \dots 9$  без хвоста девяток (хвост



девяток всегда можно заменить хвостом нулей, увеличив стоящую перед девятками цифру на 1).

29. Двичное представление вещественных чисел открывает нам возможность оценить мощность множества  $\mathbb{R}$ , а точнее, полуинтервала  $[0; 1)$ . Всякое число  $\alpha \in [0; 1)$  имеет код, заданный функцией  $f : \mathbb{N} \rightarrow \{0, 1\}$ , т.е. мощность множества вещественных чисел в полуинтервале  $[0; 1)$  равна мощности множества таких функций без хвоста единиц.

С другой стороны, всякая функция вида  $f : \mathbb{N} \rightarrow \{0, 1\}$  взаимно однозначно задает некоторое подмножество в  $\mathbb{N}$ . Нужно в этом подмножестве собрать только те элементы, на которых  $f = 1$ .

Это значит, что мы можем построить инъекцию  $F : [0; 1) \rightarrow \mathcal{P}(\mathbb{N})$ .

Теперь по произвольному подмножеству  $\mathbb{N}$  построим функцию  $f : \mathbb{N} \rightarrow \{0, 1\}$ . Такая функция может содержать хвост единиц. Но теперь мы этот код будем рассматривать не как двоичный, а как троичный! У нас гарантированно не будет хвоста двоек, а значит, мы инъективно построим какие-то числа в  $[0; 1)$  (точнее, даже в  $[0; 2/3)$ , причем с очень многими дырами). Тем самым, мы имеем инъекцию  $G : \mathcal{P}(\mathbb{N}) \rightarrow [0; 1)$ .

Окончательно, по теореме Кантора–Берштейна мы получаем равномощность множеств  $[0; 1)$  и  $\mathcal{P}(\mathbb{N})$ . То есть, интервал  $[0; 1)$  имеет мощность континуума!

30. Чтобы перейти к  $\mathbb{R}$ , нужно сначала научиться строить биекцию между интервалом и полуинтервалом.

Легко видеть, что функция

$$f(x) = \begin{cases} 1/2, & x = 0 \\ x/2, & x = 1/2^n, n = 1, 2, \dots \\ x, & \text{иначе} \end{cases}$$

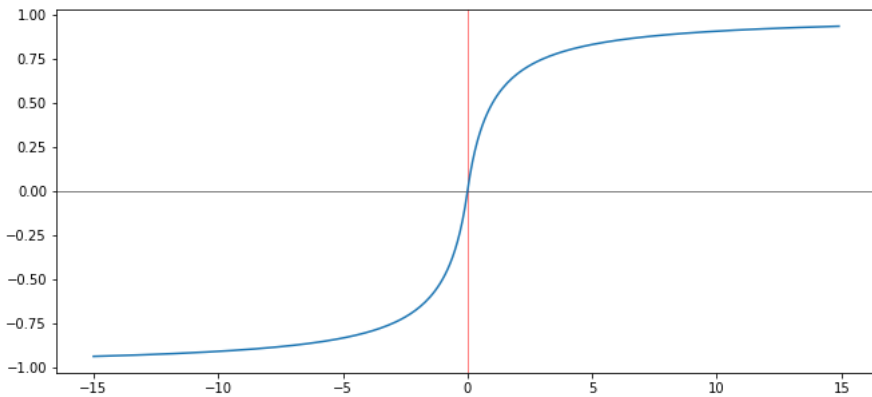
биективно переводит  $[0; 1)$  в  $(0; 1)$ . Все точки вида  $1/2^n$  сдвигаются вниз на 1 шаг, а на место  $1/2$  встает ноль.

Далее, функция  $g(x) = 2x - 1$ , очевидно, биективно переводит  $(0; 1)$  в  $(-1; 1)$ .

Наконец, функция

$$h(x) = \begin{cases} \frac{x}{1-x}, & 0 \leq x < 1 \\ \frac{x}{1+x}, & -1 < x < 0 \end{cases}$$

биективно переводит интервал  $(-1; 1)$  в  $\mathbb{R}$ . График функции, обратной к  $h(x)$ , представлен на рисунке ниже:



Таким образом, композиция  $h(g(f(x)))$  биективно переводит  $[0; 1)$  в  $\mathbb{R}$ . Следовательно, множество вещественных чисел имеет мощность континуума.

## Эквивалентные последовательности

31. Наконец, рассмотрим еще один способ конструирования множества  $\mathbb{R}$ .
32. Обозначим за  $Q$  множество всех фундаментальных последовательностей рациональных чисел. Напомним, что последовательность фундаментальная, если почти все ее члены лежат в сколь угодно малой окрестности. На множестве  $Q$  введем отношение следующим образом:

$$q \sim r \Leftrightarrow \lim_{n \rightarrow \infty} (q_n - r_n) = 0.$$

Вспоминая аксиому непрерывности в форме **A3**, мы понимаем, что если  $q \sim r$ , то эти последовательности имеют одинаковый предел. Отсюда легко видеть, что отношение  $\sim$  является отношением эквивалентности, а значит, мы можем разбить  $Q$  на классы эквивалентных последовательностей, т.е. построить фактормножество  $R = Q / \sim$ .

Вот это множество мы и объявляем множеством действительных чисел.

33. После чего мы должны ввести соответствующие операции и отношение сравнения.
34. Сложение классов эквивалентности вводится с помощью их представителей:

$$[q] + [r] = [q + r].$$

Необходимо лишь доказать, что если  $q \sim q'$  и  $r \sim r'$ , то  $q + r \sim q' + r'$ . Это легко заметить из следующего неравенства

$$|(q + r)_n - (q' + r')_n| \leq |q_n - q'_n| + |r_n - r'_n|,$$

поскольку два модуля справа стремятся к нулю.

35. Аналогично вводится умножение:

$$[q] \cdot [r] = [qr]$$

Для доказательства корректности определения заметим, что если  $q \sim q'$  и  $r \sim r'$ , то

$$|q_n r_n - q'_n r'_n| \leq |q_n| |r_n - r'_n| + |r'_n| |q_n - q'_n|.$$

Здесь справа стоят слагаемые, в каждом из которых ограниченная величина (в силу фундаментальности) умножается на величину, стремящуюся к нулю. Так что и все вместе стремится к нулю.

36. Наконец, о сравнении:

$$[q] < [r], \text{ если } \exists \varepsilon > 0 \exists N (\forall n > N)(q_n < r_n - \varepsilon),$$

т.е. для почти всех индексов разность  $r_n - q_n$  отделена от нуля положительным числом  $\varepsilon$  (оно может быть очень маленьким, но не нулевым).

37. Итак, мы видим, что при определении  $\mathbb{R}$  через эквивалентные классы фундаментальных последовательностей и операции, и отношение чисел просто переносятся один-в-один с рациональных чисел. Главная задача тут — показать корректность такого определения. Кроме того, здесь мы активно пользуемся понятием предела.

38. Выше мы рассмотрели три модели  $\mathbb{R}$ :

М1 Модель дедеиндовых сечений.

М2 Модель двоичных (в общем случае  $d$ -ичных) дробей.

М3 Модель классов фундаментальных последовательностей.

39. Попутно мы установили раномощность  $\mathbb{R}$  и множества всех подмножеств  $\mathbb{N}$ .

40. Возникает вопрос: если  $\mathbb{R}$  такое большое множество, а  $\mathbb{Q}$  такое маленькое (по мощности), есть ли какие-то множества, имеющие промежуточные мощности между счетной и континуумом? Ответ на этот вопрос дали два человека: К.Гёдель и П.Коэн. Первый доказал, что отсутствие промежуточных мощностей не противоречит аксиоматике теории множеств, второй — что существование таких мощностей также не противоречит аксиоматике теории множеств. Таким образом, мы оказываемся в ситуации пятого постулата Евклида, когда можем принимать или отвергать континуум-гипотезу (именно так называется утверждение о том, что между счетной мощностью и континуумом нет промежуточных мощностей), не опасаясь получить противоречие.

## 13.5 Комплексные числа

### Конспект

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

### Задачи

## 13.6 Гомотетии прямой и плоскости

### Конспект

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

### Задачи

# Расширение алгебраических конструкций

## 14.1 Матрицы

### 14.1.1 Конспект

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

### 14.1.2 Задачи

- Аксиома
  - непрерывности (полноты), 124
- Группа, 26
- Кольцо, 45
  - коммутативное, 46
  - с единицей, 46
- Континуум-гипотеза, 169
- Порядок
  - линейный
  - непрерывный, 124
- Сечение л.у.м., 123
  - дедекиндово, 124

# Схемы и таблицы

Таблица А.1: Таблица умножения симметрической группы  $S_4$

Знакопеременная группа $A_4$											
Четверная группа Клейна											
e	(12)(34)	(13)(24)	(14)(23)	(123)	(132)	(124)	(142)	(134)	(143)	(234)	(243)
(12)(34)	e	(14)(23)	(13)(24)	(243)	(143)	(234)	(134)	(142)	(132)	(124)	(123)
(13)(24)	(14)(23)	e	(12)(34)	(142)	(234)	(143)	(123)	(243)	(124)	(132)	(134)
(14)(23)	(13)(24)	(12)(34)	e	(134)	(124)	(132)	(243)	(123)	(234)	(143)	(142)
(123)	(134)	(243)	(142)	(132)	e	(13)(24)	(143)	(234)	(14)(23)	(12)(34)	(124)
(132)	(234)	(124)	(143)	e	(123)	(243)	(14)(23)	(12)(34)	(142)	(134)	(13)(24)
(124)	(143)	(132)	(234)	(14)(23)	(134)	(142)	e	(13)(24)	(243)	(123)	(12)(34)
(142)	(243)	(134)	(123)	(234)	(13)(24)	e	(124)	(132)	(12)(34)	(14)(23)	(143)
(134)	(123)	(142)	(243)	(124)	(14)(23)	(12)(34)	(234)	(143)	e	(13)(24)	(132)
(143)	(124)	(234)	(132)	(12)(34)	(243)	(123)	(13)(24)	e	(134)	(142)	(14)(23)
(234)	(132)	(143)	(124)	(13)(24)	(142)	(134)	(12)(34)	(14)(23)	(123)	(243)	e
(243)	(142)	(123)	(134)	(143)	(12)(34)	(14)(23)	(132)	(124)	(13)(24)	e	(234)
(12)	(34)	(1324)	(1423)	(23)	(13)	(24)	(14)	(1342)	(1432)	(1234)	(1243)
(13)	(1234)	(24)	(1432)	(12)	(23)	(1243)	(1423)	(34)	(14)	(1342)	(1324)
(14)	(1243)	(1342)	(23)	(1234)	(1324)	(12)	(24)	(13)	(34)	(1423)	(1432)
(23)	(1342)	(1243)	(14)	(13)	(12)	(1324)	(1432)	(1234)	(1423)	(34)	(24)
(24)	(1432)	(13)	(1234)	(1423)	(1342)	(14)	(12)	(1324)	(1243)	(23)	(34)
(34)	(12)	(1423)	(1324)	(1243)	(1432)	(1234)	(1342)	(14)	(13)	(24)	(23)
(1234)	(13)	(1432)	(24)	(1324)	(14)	(1342)	(34)	(1423)	(23)	(1243)	(12)
(1243)	(14)	(23)	(1342)	(1432)	(34)	(1423)	(13)	(24)	(1324)	(12)	(1234)
(1324)	(1423)	(12)	(34)	(14)	(1234)	(1432)	(23)	(1243)	(24)	(13)	(1342)
(1342)	(23)	(14)	(1243)	(24)	(1423)	(34)	(1234)	(1432)	(12)	(1324)	(13)
(1423)	(1324)	(34)	(12)	(1342)	(24)	(13)	(1243)	(23)	(1234)	(1432)	(14)
(1432)	(24)	(1234)	(13)	(34)	(1243)	(23)	(1324)	(12)	(1342)	(14)	(1423)

\*Здесь особым фоном выделены элементы, образующие группу, изоморфную  $\mathbb{Z}_3$ , поскольку их 3-я степень равна e.



Таблица А.2: Продолжение таблицы А.1

(12)	(13)	(14)	(23)	(24)	(34)	(1234)	(1243)	(1324)	(1342)	(1423)	(1432)
(34)	(1432)	(1342)	(1243)	(1234)	(12)	(24)	(23)	(1423)	(14)	(1324)	(13)
(1423)	(24)	(1243)	(1342)	(13)	(1324)	(1432)	(14)	(34)	(23)	(12)	(1234)
(1324)	(1234)	(23)	(14)	(1432)	(1423)	(13)	(1342)	(12)	(1243)	(34)	(24)
(13)	(23)	(1423)	(12)	(1243)	(1234)	(1342)	(1324)	(24)	(34)	(1432)	(14)
(23)	(12)	(1432)	(13)	(1324)	(1342)	(34)	(24)	(1243)	(1234)	(14)	(1423)
(14)	(1324)	(24)	(1234)	(12)	(1243)	(1423)	(1432)	(1342)	(13)	(23)	(34)
(24)	(1342)	(12)	(1423)	(14)	(1432)	(23)	(34)	(13)	(1324)	(1234)	(1243)
(1234)	(14)	(34)	(1324)	(1342)	(13)	(1243)	(12)	(1432)	(1423)	(24)	(23)
(1243)	(34)	(13)	(1432)	(1423)	(14)	(12)	(1234)	(23)	(24)	(1342)	(1324)
(1342)	(1423)	(1234)	(24)	(34)	(23)	(1324)	(13)	(14)	(1432)	(1243)	(12)
(1432)	(1243)	(1324)	(34)	(23)	(24)	(14)	(1423)	(1234)	(12)	(13)	(1342)
e	(132)	(142)	(123)	(124)	(12)(34)	(234)	(243)	(13)(24)	(134)	(14)(23)	(143)
(123)	e	(143)	(132)	(13)(24)	(134)	(12)(34)	(124)	(243)	(234)	(142)	(14)(23)
(124)	(134)	e	(14)(23)	(142)	(143)	(123)	(12)(34)	(132)	(13)(24)	(234)	(243)
(132)	(123)	(14)(23)	e	(243)	(234)	(134)	(13)(24)	(124)	(12)(34)	(143)	(142)
(142)	(13)(24)	(124)	(234)	e	(243)	(14)(23)	(143)	(134)	(132)	(123)	(12)(34)
(12)(34)	(143)	(134)	(243)	(234)	e	(124)	(123)	(14)(23)	(142)	(13)(24)	(132)
(134)	(14)(23)	(234)	(124)	(12)(34)	(123)	(13)(24)	(132)	(142)	(143)	(243)	e
(143)	(243)	(13)(24)	(12)(34)	(123)	(124)	(142)	(14)(23)	(234)	e	(132)	(134)
(14)(23)	(124)	(243)	(134)	(132)	(13)(24)	(143)	(142)	(12)(34)	(123)	e	(234)
(234)	(142)	(12)(34)	(13)(24)	(134)	(132)	(243)	e	(143)	(14)(23)	(124)	(123)
(13)(24)	(234)	(123)	(142)	(143)	(14)(23)	(132)	(134)	e	(243)	(12)(34)	(124)
(243)	(12)(34)	(132)	(143)	(14)(23)	(142)	e	(234)	(123)	(124)	(134)	(13)(24)

Желтым фоном выделена таблица подгруппы 8 порядка. Данная подгруппа некоммукативна.



Лямбда-Исчисление, его синтаксис  
и семантика

Барендрегт Х.

В.Ф. КОЛЧИН • СЛУЧАЙНЫЕ ГРАФЫ

III MC III

А. И. Кострикин ВВЕДЕНИЕ В АЛГЕБРУ

Н. Г. ЧЕБОТАРЕВ • ТЕОРИЯ ГАЛУА

В. В. ПРАСОЛОВ

Многочлены

Вычислимые функции

В. В. ЦЕЛИЩЕВ

ТЕЗИС ЧЕРЧА

А. Б. СОСИНСКИЙ

КАК НАПИСАТЬ МАТЕМАТИЧЕСКУЮ СТАТЬЮ ПО-АНГЛИЙСКИ

Э. Б. Винберг

Курс алгебры

Алексей  
САВВАТЕЕВ

МАТЕМАТИКА ДЛЯ ГУМАНИТАРИЕВ

Живые лекции

КЛАССИЧЕСКИЙ  
УЧЕБНИК

Л. Э. Эльсгольц

ВАРИАЦИОННОЕ ИСЧИСЛЕНИЕ

КЛАССИЧЕСКИЕ ГРУППЫ  
ИХ ИНВАРИАНТЫ И ПРЕДСТАВЛЕНИЯ

Г. Вейль

Р. Курант Г. Роббинс

Что такое  
математика?



Сборник научных трудов РНОЦ "Логос" (вып. 9)

Языки и исчисления

В. В. ПРАСОЛОВ

В. М. ТИХОМИРОВ

ГЕОМЕТРИЯ

Г. Г. Харди

АПОЛОГИЯ МАТЕМАТИКА

Л. С. Понтрягин \* ОБОБЩЕНИЯ ЧИСЕЛ

ТЕОРИЯ ФУНКЦИЙ КОМПЛЕКСНОЙ ПЕРЕМЕННОЙ



АВТОМАТИЗАЦИЯ РУТИННЫХ  
ЗАДАЧ С ПОМОЩЬЮ RUTRON

ЗА СВЕЙГАРТ



Р. Грэхем  
Д. Кнут  
О. Паташник

КОНКРЕТНАЯ МАТЕМАТИКА