

СОДЕРЖАНИЕ

Глава 0. Логика и множества (факультативно)	3
0.1 Суждения и силлогизмы	3
0.2 Высказывания и предикаты	5
0.3 Связь предикатов и множеств	8
0.4 Построение множеств	11
Глава 1. Визуальная арифметика	14
1.1 Сложение и вычитание	14
1.2 Сравнение	16
1.3 Умножение	16
1.4 Натуральные числа	18
1.5 Теорема Пифагора графически	19
1.6 Бином Ньютона и другие формулы визуально	20
1.7 Соизмеримость отрезков, алгоритм Евклида	20
Глава 2. Движения прямой	22
2.1 Сдвиг, композиция сдвигов, группа	22
2.2 Отражение	24
2.3 Таблица Кэли движений прямой	25
2.4 Теорема о гвоздях, аналог теоремы Шаля	26
2.5 Все конечные подгруппы движения прямой	28
Глава 3. Вокруг окружности	29
3.1 Движения окружности	29
3.2 Группа движений окружности, теорема Шаля	31
3.3 Наматывание прямой на окружность	35
Глава 4. Целые числа и ОТА	38
4.1 Целые числа. Кольцо	38
4.2 Кузнечик НОД и алгоритм Евклида	40
4.3 Простые числа и ОТА	41
4.4 Некоторые следствия ОТА	44
Глава 5. Симметрии фигур	45
5.1 Симметрии правильного треугольника	45
5.2 Симметрии правильного многоугольника	46
5.3 Подгруппы движений окружности	47

5.4	Симметрии ромба, группа Клейна	50
Глава 6.	Движения плоскости и пространства	52
6.1	Виды движений плоскости. Теорема Шаля	52
6.2	Сравнение движений прямой, окружности и плоскости	54
6.3	Векторно-числовое представление движений плоскости	55
6.4	Пара слов о движениях сферы	56
6.5	Пара слов о движениях пространства	57
Глава 7.	Исчисление остатков	61
7.1	Арифметика остатков	61
7.2	Свойства арифметики остатков	66
7.3	*Вычеты и операции Минковского	68
7.4	*Теория множеств: отношения	70
Глава 8.	Линейные уравнения	73
8.1	Уравнение прямой на плоскости	73
8.2	Линейные уравнения в целых числах	77
Глава 9.	Числовые поля	83
9.1	Рациональные числа	83
9.2	Соизмеримость. Иррациональности	89
9.3	Поле вычетов по простому модулю	94
Глава 10.	Начала комплексного анализа	96
10.1	Алгебра комплексных чисел	96
10.2	Гауссовы целые числа	103
Глава 11.	Континуум	104
11.1	Действительные числа	104
11.2	Комплексные числа	104
11.3	Гомотетии прямой и плоскости	105
Глава 12.	Многочлены	106
Глава 13.	Расширение алгебраических конструкций	107
13.1	Матрицы	107
13.1.1	Конспект	107
13.1.2	Задачи	107

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

2. Пример:

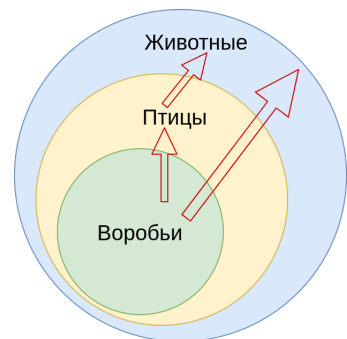
(Все птицы — животные) и (все воробьи — птицы),

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).

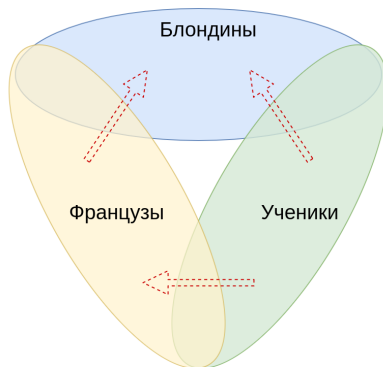
Это суждение истинно независимо от ложности посылок. Суждение показывает *только взаимосвязь* посылок и вывода. Принцип «чушь на входе — чушь на выходе».



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:

<i>Все птицы — животные</i>	$(\text{для любого } x) (x \text{ есть птица}) \rightarrow (x \text{ есть животное})$
<i>Все воробьи — птицы</i>	$(\text{для любого } x) (x \text{ есть воробей}) \rightarrow (x \text{ есть птица})$
<i>Все воробьи — животные</i>	$(\text{для любого } x) (x \text{ есть воробей}) \rightarrow (x \text{ есть животное})$
Если число заканчивается на 0, то оно кратно 5	$(\text{для любого } a) (a \text{ заканчивается на } 0) \rightarrow (a \text{ кратно } 5)$
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 навести 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.¹

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 .

¹В 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° 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.

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

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 отсекаать 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. Рассмотрим аффинную прямую, т.е. набор точек и векторов на прямой.
2. Сумма точки и вектора есть точка, сумма векторов есть вектор, разность точек есть вектор.
3. Команда «прибавить ко всем точкам вектор a » называется **сдвигом** прямой на вектор a .
4. Сдвиг на a — это операция сложения с вектором без указания конкретной точки приложения, она применяется сразу ко всем точкам! В итоге вся прямая смещается как единое целое.
5. Сдвиг является движением (не случайно это однокоренные слова!)
6. 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!
7. Математическое движение — это результат физического движения (есть только начальное и конечное состояние системы).
8. Сдвиг на вектор a будем обозначать T_a : $T_a(A)$ — это точка B такая, что AB есть вектор a (совпадает по направлению и длине).

9. Композиция сдвигов — это их последовательное применение:

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

.

10. Композиция сдвигов соответствует сумме векторов: $T_b \circ T_a = T_{a+b}$.

11. Композиция сдвигов перестановочна в силу коммутативности сложения:

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

.

12. Кратность сдвига обозначается как степень

$$\underbrace{T_a \circ \dots \circ T_a}_n = T_a^n$$

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

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

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

15. 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 является тождественным преобразованием.

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

17. Нулевой сдвиг сам себе обратен.

18. Обобщая свойства сдвигов, фиксируем понятие **группы**. Это — множество G с одной бинарной операцией \circ , для которой выполняются законы:

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** 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 .

19. Множество всех сдвигов образует группу относительно операции композиции!

20. 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 .

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

22. На основе только одного сдвига T_a можно построить подгруппу сдвигов

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

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

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

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

2.2 Отражение

Конспект

1. Еще один вид движений прямой — **отражение**
2. Отражение связано с выделенной точкой — центром отражения, и все точки переводит в симметричные относительно данного центра. Взяли прямую и перевернули ее на 180° , оставляя центр отражения на месте
3. Отражение с центром O будем обозначать S_O

4. Композиция отражений:

$$S_O \circ S_C = T_{2CO}, \quad S_C \circ S_O = T_{2OC}$$

5. Видим, что композиция отражений является сдвигом и при этом не коммутативна!

6. Композиция отражения и сдвига:

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

7. Такая композиция является отражением и при этом не коммутативна!

8. 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}

9. Кратность отражения S_O^n определяется четностью числа n . В случае четного n это id , в случае нечетного — исходное S_O

10. Отражение обратно самому себе: $S_O \circ S_O = \text{id}$

11. 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 $S_O = S_O^1, \text{id} = S_O^2$)

	id	S_O
id	id	S_O
S_O	S_O	id

12. Видим, что таблица полностью повторяет таблицу умножения знаков, причем id является нейтральным элементом.

13. 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.

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 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).



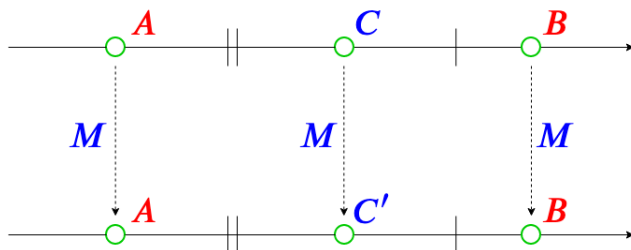
1. Куда перейдет точка A при преобразовании S_B ?
2. Куда перейдут точки B, C, D при преобразовании $T_{AB} \circ T_{CA}$?
3. Куда перейдут точки A, B, C при преобразовании $S_C \circ T_{AB}$?

2.4 Теорема о гвоздях, аналог теоремы Шаля

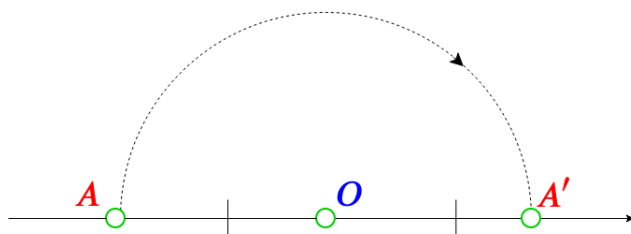
Конспект

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

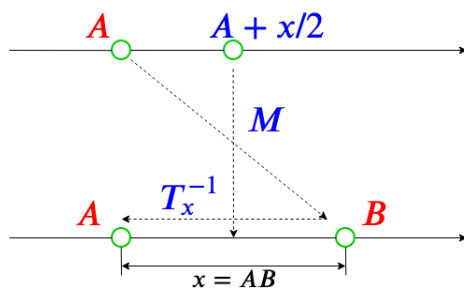
3. $M(A) = A$ и $M(B) = B$. Пусть $C' = M(C)$. M сохраняет расстояния AC и BC , откуда $AC = AC'$ и $BC = BC'$, откуда $C = C'$. Т.е. $M(C) = C$ для любых точек C , т.е. $M = \text{id}$



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, 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 движения прямой

Конспект

- 1.

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.

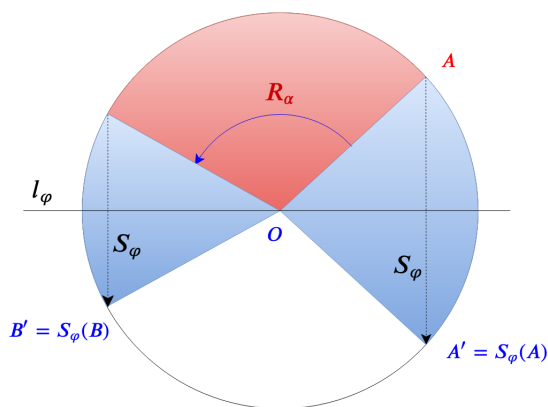
По аналогии с натуральными числами говорим о том, что целые числа — это и степени композиций движений, и мера длины, только оснащенная знаком, т.е. направлением измерения длины.

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 α обозначим R_α (положительный — против часовой стрелки), симметрию относительно прямой, имеющей угол наклона φ , обозначим S_φ ($0 \leq \varphi < 180^\circ$). 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_φ мы будем обозначать l_φ (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 id .
16. Вообще, повороты, заданные углами с шагом 360° , равны: $R_\alpha = R_{\alpha \pm 360^\circ k}$, где k — натуральное число.

17. Некоторые повороты дают 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° , то поворот на данный угол имеет положительную степень, в которой он обращается в id .
19. Но есть угол, не обладающий таким свойством, это угол в 1 радиан. Если бы он был соизмерим с полным оборотом, то число π 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.

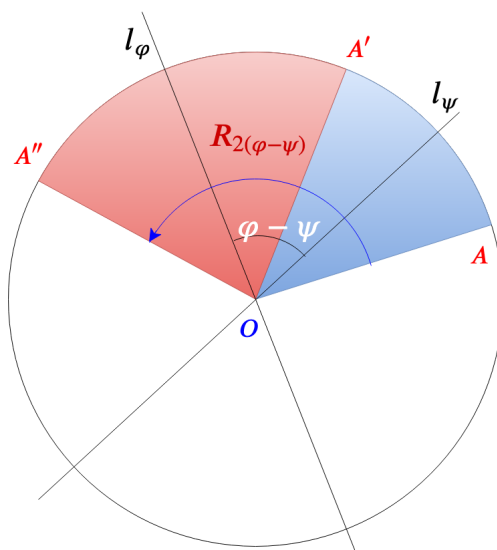
3.2 Группа движений окружности, теорема Шаля

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 картинке, где точка A переходит в A' под действием симметрии S_ψ относительно оси l_ψ , а затем A' переходит в A'' под действием симметрии S_φ относительно оси l_φ :



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_φ , 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_α	S_ψ
R_β	$R_{\alpha+\beta}$	$S_{\psi+\beta/2}$
S_φ	$S_{\varphi-\alpha/2}$	$R_{2(\varphi-\psi)}$

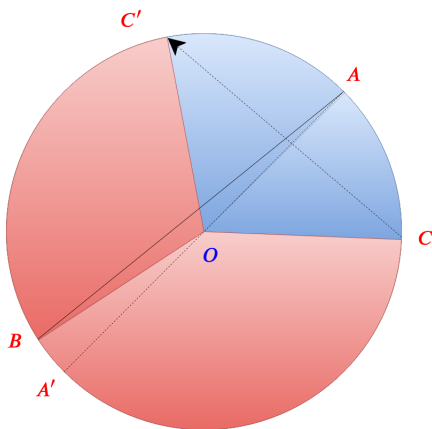
6. По аналогии с прямой обозначим \mathbb{T} класс всех вращений окружности, \mathbb{S} — класс всех симметрий окружности
7. Получаем аналогичную таблицу композиций классов:

	\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!

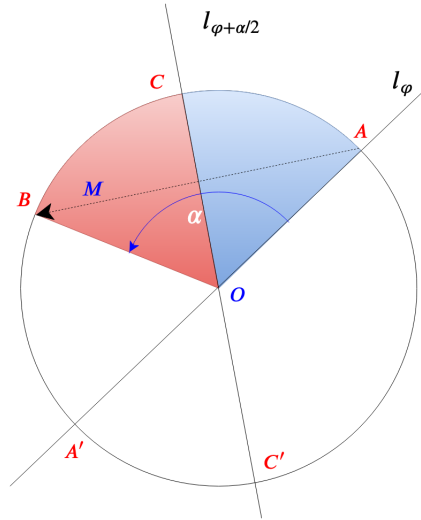
10. Анализ движений проводится, как и в случае прямой, на основе наблюдений за количеством стационарных точек.
11. Для начала заметим, что если при движении окружности одна точка остается на месте, то неподвижной будет и диаметрально противоположная ей точка. Если бы это было не так, то, очевидно, расстояние 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 φ — 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 α 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_φ (на рис. ось симметрии l_φ), 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, 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 .

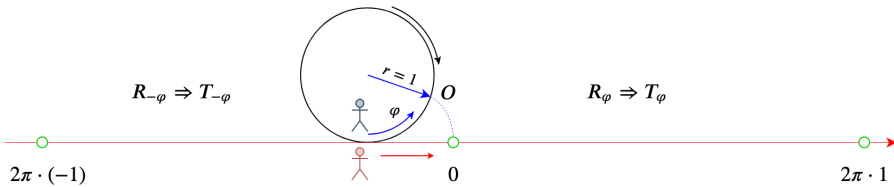
3.3 Наматывание прямой на окружность

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° , 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 2π , и с каждым полным оборотом мы будем «наматывать» расстояние 2π .
4. Вообще, расстояние, пройденное по окружности единичного радиуса, когда этот радиус заметает угол α , равно $\alpha(2\pi/360^\circ)$. Чтобы каждый раз не переводить единицы измерения радиуса в градусы и наоборот, углы также примем 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 π 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. 2π (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.

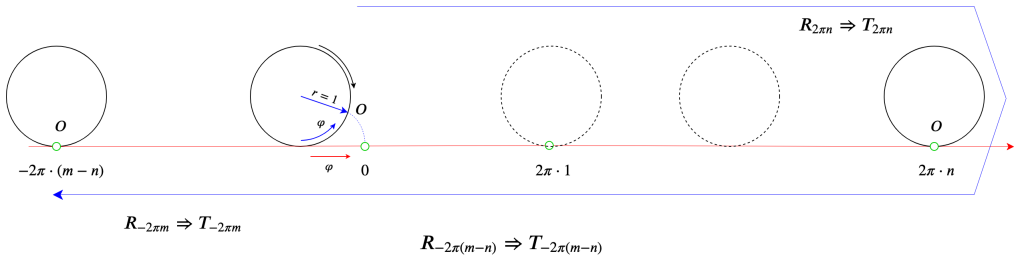
12. Нужно заметить при этом, что если колесо вращается по часовой стрелке, т.е. в отрицательном направлении, то вдоль прямой оно движется направо, т.е. в положительном направлении. Но фокус в том, что житель окружности для синхронизации с жителем прямой должен идти навстречу вращению колеса, т.е. тоже 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 2π 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 2π , 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 2π 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 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:
 - K1)** $a, b \in K \Rightarrow a + b \in K, a \cdot b \in K$ (замкнутость операций);
 - K2)** $a, b, c \in K \Rightarrow (a + b) + c = a + (b + c), (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (ассоциативность операций);
 - K3)** существует элемент $0 \in K$ такой, что $a + 0 = 0 + a = a$ для всех $a \in K$ (аксиома нуля);
 - K4)** для всякого элемента $a \in K$ существует противоположный $-a$ такой, что $a + (-a) = 0$ (аксиома противоположного элемента);

К5) 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);

К6) для всех $a, b \in K$ имеем $a + b = b + a$ (коммутативность сложения).

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

К7) 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

К8) 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 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 $a \mid b$ тогда и только тогда, когда $b\mathbb{Z} \subseteq a\mathbb{Z}$.

Действительно, если $a \mid b$, 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 $a \mid b$.

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 T3) $c|a$ 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 T2) $c\mathbb{Z} \subseteq d\mathbb{Z}$, откуда (свойство T3) $d|c$. То есть, любой делитель a и b не превосходит c , а c также является делителем a и b . Следовательно, $c = \text{НОД}(a, b)$.

T6 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 T5) $p\mathbb{Z} \oplus a\mathbb{Z} = \mathbb{Z}$. Откуда $1 = kp + ta$ при некоторых целых k, t . Тогда $b = kbp + tab$, откуда следует, что $p|b$.

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

T7 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° .
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 3×3), 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 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 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 2π). 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 2π .
12. Итак, мы видим, что в G есть подгруппы вида $\langle g_k \rangle$, которые либо тривиальны (состоят из одного элемента 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 φ 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 — 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_φ 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 π , обозначим это вращение R ;
 - с) тождественного преобразования 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: 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° 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
R	id	S_2	S_1
S_1	S_2	id	R
S_2	S_1	R	id

5. Отличие данной группы от группы движений правильного n -угольника состоит в том, что группа ромба является коммутативной (абелевой).
6. Эта группа нам еще встретится позднее под именем «четверная группа Клейна», когда мы будем говорить об арифметике остатков.

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.

6.1 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 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 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:

- а) класс параллельных переносов (на произвольный вектор), который мы обозначим \Rightarrow ;
- б) класс поворотов относительно произвольного центра, который мы обозначим \bigcirc ;
- с) 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

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

Задачи

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

6.2 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 id , а на окружности симметрия относительно самой окружности вообще требует специального построения в геометрии плоскости.

6.3 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_α , где α — угол в радианах.
5. Поворот на угол α 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 α — 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.

6.4 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).

6.5 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 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, 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 6.1: 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)

Исчисление остатков

Аннотация.

Покончив с движениями, мы снова погружаемся в алгебру целых чисел и приступаем к изучению остатков (вычетов).

Арифметика вычетов 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.

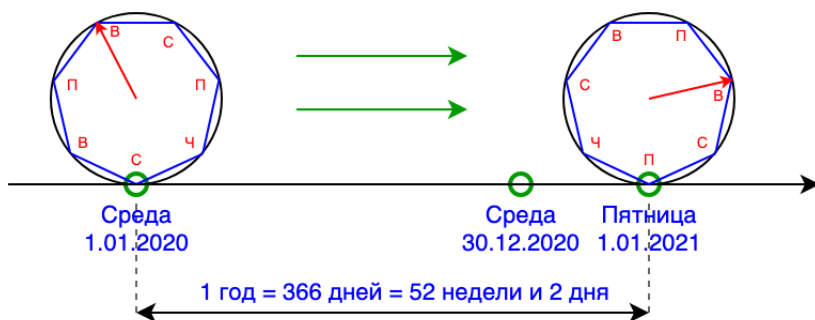
7.1 Арифметика остатков

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 просот 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 2π), 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 сложения 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 . 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 $\{1, 2, \dots, m-1\}$. \square

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, таблицей умножения для группы \mathbb{Z}_8^* будет

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Задачи

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

7.2 Свойства арифметики остатков

Конспект

1. Свойства сравнений таковы:
 - М1. $a \equiv b \pmod{m}$ тогда и только тогда, когда $a - b$ кратно m ;
 - М2. 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 m_p — степень простого числа p в разложении m по степеням простых (ОТА), тогда

$$a \equiv b \pmod{m} \iff \forall p \quad a \equiv b \pmod{p^{m_p}} \quad (p — простое)$$

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

- 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.
- 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

$$\overline{nm} = (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \dots, \alpha_k + \beta_k, \dots)$$

$$\overline{\text{НОД}(n, m)} = (\min(\alpha_0, \beta_0), \min(\alpha_1, \beta_1), \dots, \min(\alpha_k, \beta_k), \dots),$$

$$\overline{\text{НОК}(n, m)} = (\max(\alpha_0, \beta_0), \max(\alpha_1, \beta_1), \dots, \max(\alpha_k, \beta_k), \dots).$$

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

5. Докажите, что

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

7.3 *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:

$$\text{Z1 } (m\mathbb{Z} + n) + (m\mathbb{Z} + n') = m\mathbb{Z} + (n + n' \bmod m)$$

$$\text{Z2 } (m\mathbb{Z} + n)(m\mathbb{Z} + n') = m\mathbb{Z} + (nn' \bmod m)$$

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 факормножество, т.е. тривиальное кольцо, состоящее из одного нуля.

отношение эквивалентности
отношения вообще

7.4 *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:

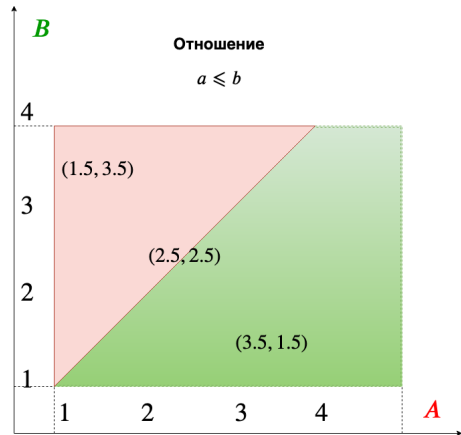
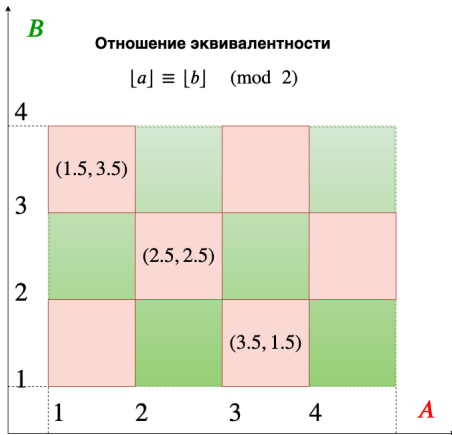
$$m\mathbb{Z}, \quad m\mathbb{Z} + 1, \quad m\mathbb{Z} + 2, \quad \dots, \quad m\mathbb{Z} + m - 1$$

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 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 $[x]$ обозначает целую часть числа. Здесь мы неявно предполагаем знакомство продвинутого читателя с нецелыми числами.



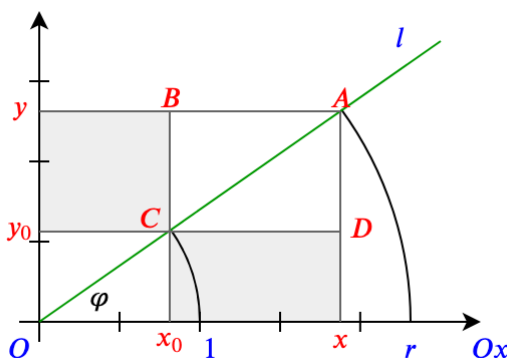
Линейные уравнения

8.1 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_φ 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 φ , 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_φ , 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_φ . 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).

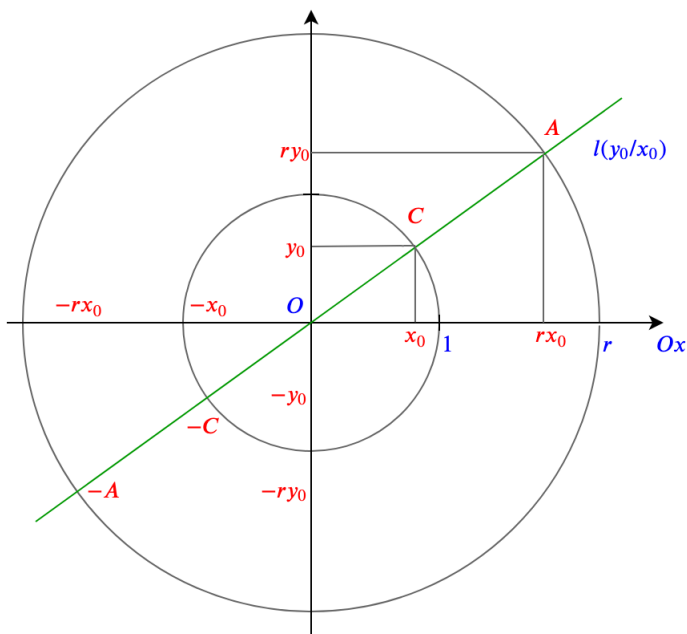


11. Видим, что треугольники ABC и ADC равны по трем сторонам, также равны треугольники Oy_0C и Ox_0C , и треугольники OyA и OxA . Отсюда легко установить равенство площадей $x_0(y - y_0) = y_0(x - x_0)$, откуда получаем

$$xy_0 - yx_0 = 0.$$

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 φ .
13. Отметим, что точка (x_0, y_0) полностью определяется углом поворота φ , т.к. является образом точки $(0, 1)$ при повороте на угол φ . В то же время, произвольная точка на единичной окружности однозначно задает угол поворота в интервале от 0 до 2π . 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 π .

16. Наконец, поворот прямой(!) на угол $\pi + \alpha$ — это поворот на угол α 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

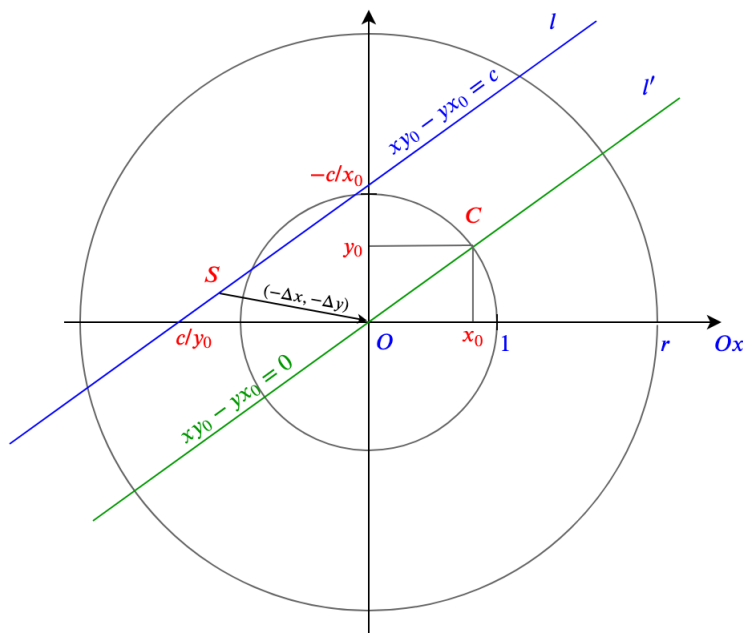
$$xy_0 - yx_0 = 0.$$

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

$$xy_0 - yx_0 = y_0\Delta x' - x_0\Delta y',$$

откуда из предыдущего получаем, что вновь

$$xy_0 - yx_0 = c.$$

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

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

8.2 Линейные уравнения в целых числах

Конспект

1. 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^α входит в разложение \tilde{a} , то p^α 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 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 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 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 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:

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

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

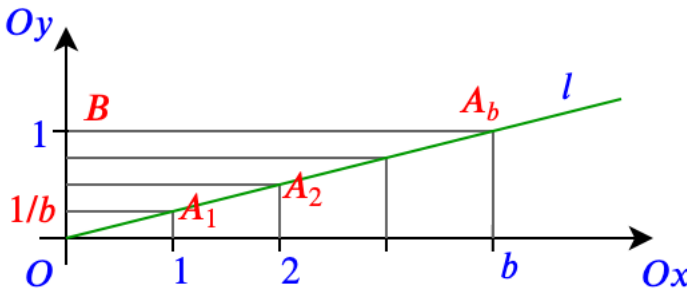
1. Найти представление $\text{НОД}(5, 9)$ с помощью алгоритма Евклида и методом цепных дробей.
2. Найти представление $\text{НОД}(18, 15)$ с помощью алгоритма Евклида и методом цепных дробей.
3. Найти представление $\text{НОД}(225, 81)$ с помощью алгоритма Евклида и методом цепных дробей.
4. Решить уравнение $5x - 9y = 2$ 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

9.1 Рациональные числа

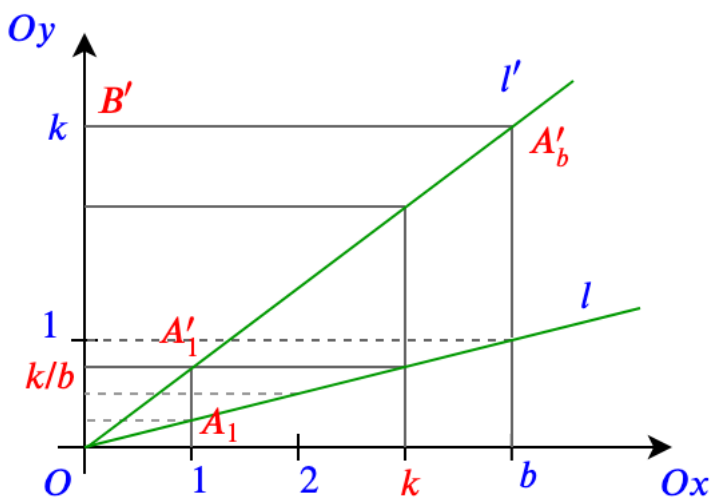
Конспект

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:

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

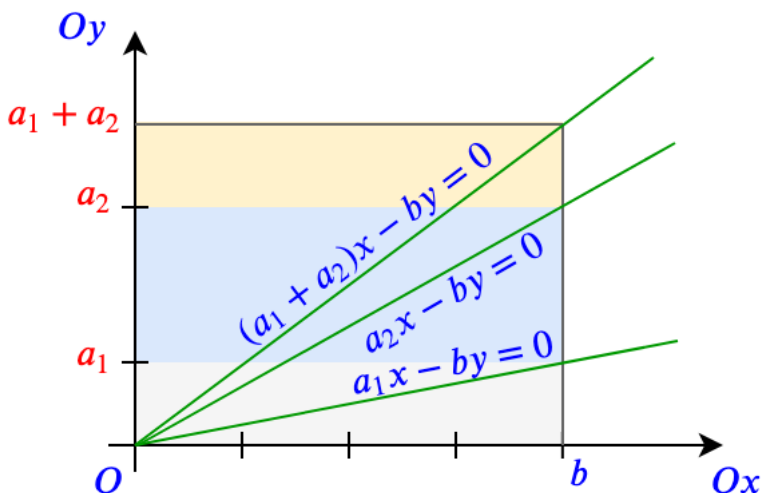
17. Заметим, что сложение (и вычитание) таких прямых определить еще проще:

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

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 полой).
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.

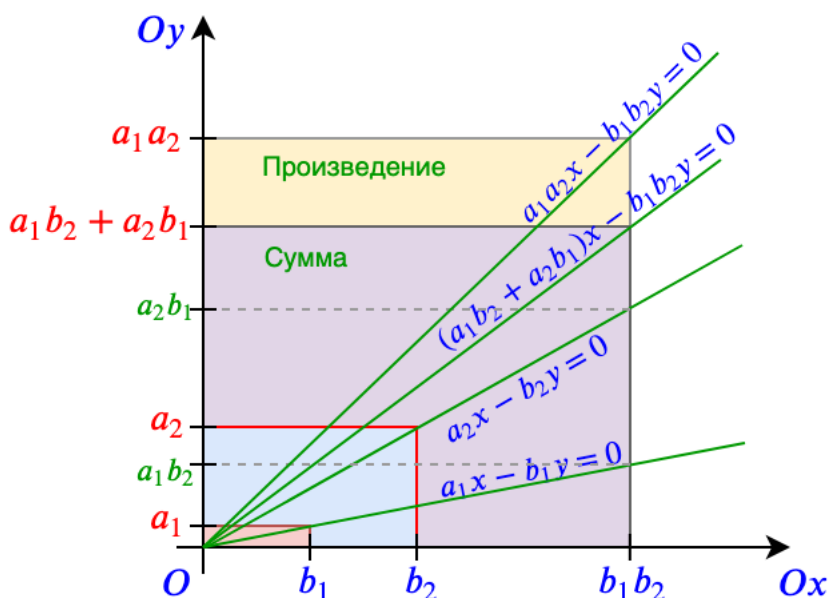
27. Но и это не проблема:

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

что соответствует операциям с дробями

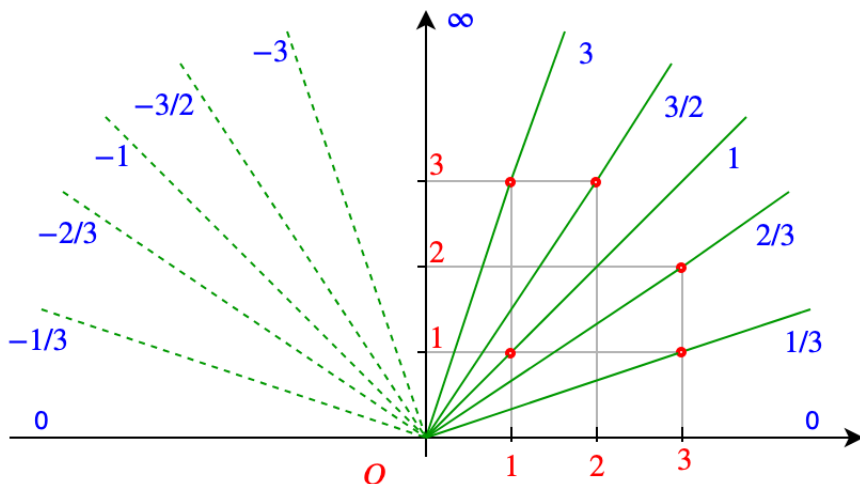
$$\frac{a_1}{b_2} + \frac{a_2}{b_2} = \frac{a_1b_2 + a_2b_1}{b_1b_2}.$$

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



Здесь маленькие прямоугольники соответствуют исходным прямым с уравнениями $a_1x - b_1y = 0$ и $a_2x - b_2y = 0$, пунктиром отмечены приведенные к общему основанию b_1b_2 прямоугольники, большой темный прямоугольник соответствует их сумме (буквально один приставлен сверху к другому), большой светлый прямоугольник — произведению (помножены основания и помножены высоты). Рисунок не учитывает масштаб!

29. В целом картина представления рациональных чисел с помощью прямых с целочисленными коэффициентами выглядит следующим образом:



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

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

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:
- F1)** $a, b \in F \Rightarrow a + b \in F, a \cdot b \in F$ (замкнутость операций);
 - F2)** $a, b, c \in F \Rightarrow (a + b) + c = a + (b + c), (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (ассоциативность операций);
 - F3)** для всех $a, b \in F$ имеем $a + b = b + a$ и $a \cdot b = b \cdot a$ (коммутативность операций);
 - F4)** существует элемент $0 \in F$ такой, что $a + 0 = 0 + a = a$ для всех $a \in F$ (аксиома нуля);
 - F5)** для всякого элемента $a \in F$ существует противоположный $-a$ такой, что $a + (-a) = 0$ (аксиома противоположного элемента);
 - F6)** существует элемент $1 \in F$ такой, что $a \cdot 1 = 1 \cdot a = a$ для всех $a \in F$ (аксиома единицы),
 - F7)** 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).
 - F8)** 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.

Задачи

9.2 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!

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

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

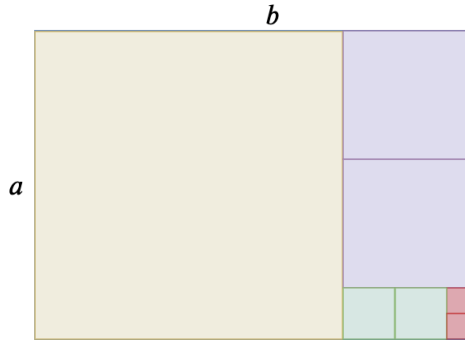
11. Поскольку остатки всегда являются натуральными числами, рано или поздно этот алгоритм прервется. Пусть это случится на шаге с номером n , так что мы полагаем $r_{n+1} = 0$, и цепная дробь закончится на числе k_n .
12. В таком случае цепную дробь принято записывать последовательностью выделенных на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

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

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?

9.3 Поле вычетов по простому модулю

Конспект

1. Изучая числовые поля, невозможно обойти пример поля, который неявно уже появлялся у нас в главе 7.
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.

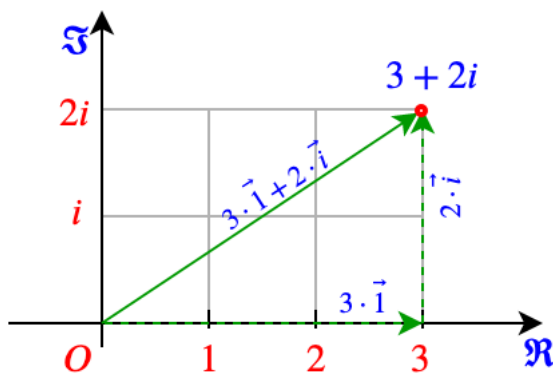
В этой главы мы начинаем строить поле комплексных чисел, пока еще без участия вещественных. По сути мы здесь работаем только с комплексными рациональностями, что, однако, не мешает показать тесную геометрическую связь комплексных чисел и движений плоскости, а также изучить числа Гаусса.

10.1 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 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.

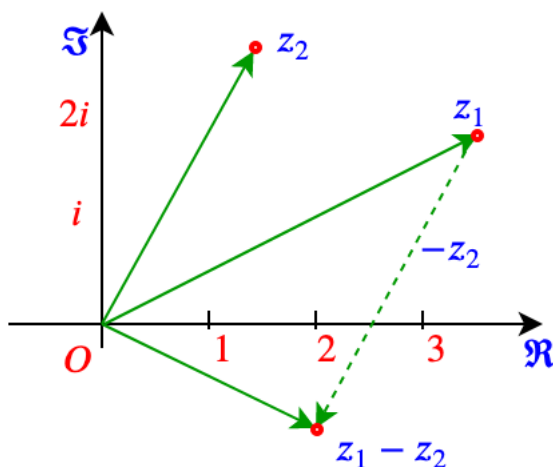
15. Итак, если вектор равен $x\vec{1} + y\vec{i}$, то его финишная точка обозначается $x + yi$.
16. Пока все, что мы сделали — это построили обычную арифметику векторов на плоскости. При чем же тут алгебраическая ипостась мнимой единицы, вытекающая из уравнения $x^2 = -1$?
17. Алгебраическая ипостась 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: $\overline{z\bar{w}} = \bar{z}\bar{w}$. 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,

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

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 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 :

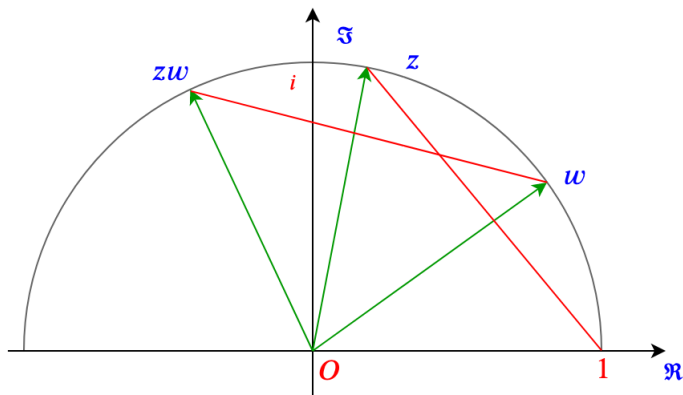
$$|w'_1 - w'_2| = |(w_1 - w_2)z| = |w_1 - w_2| \cdot |z| = |w_1 - w_2|,$$

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 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 $zw/|w|$.

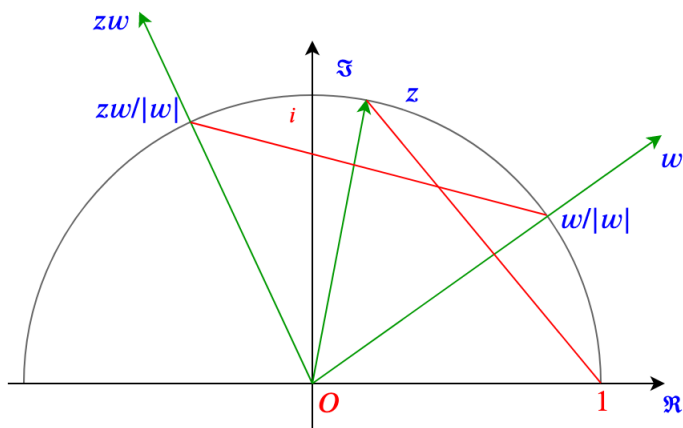
В общем случае это означает, что мы имеем два комплексных числа, одно v , второе λv , где действительное число $\lambda > 0$. Пусть $v = a + bi$. Вспомним уравнение прямой, проходящей через начало координат и точку (a, b) . Это уравнение имеет вид $ay - bx = 0$. А теперь умножим в этом уравнении обе части на λ , и получим $(\lambda a)y - (\lambda b)x = 0$. То есть точка λv 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 φ . 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 $|\lambda - 1| < \lambda + 1$.

10.2 Гауссовы целые числа

Конспект

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

Задачи

Континуум

11.1 Действительные числа

Конспект

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

Задачи

11.2 Комплексные числа

Конспект

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

- 8.
- 9.
- 10.

Задачи

11.3 Гомотетии прямой и плоскости

Конспект

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

Задачи

Многочлены

Расширение алгебраических конструкций

13.1 Матрицы

13.1.1 Конспект

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

13.1.2 Задачи