Элементы математики в задачах:

через олимпиады и кружки — к профессии

Алгебра

А. Б. Скопенков

Геометрия и комбинаторика

Под редакцией А. А. Заславского и М. Б. Скопенкова

В книги вошли материалы занятий, проведенных в разное время в ряде российских университетов, школ и кружков. Большинство задач подобраны так, что в процессе их решения читатель (точнее, решатель) познакомится с глубокими идеями и освоит основы важных теорий. Книга может использоваться как школьниками и студентами для самостоятельных занятий, так и преподавателями. К ключевым задачам приведены указания или решения.

Это обновляемая электронная версия. Ее пересечение с изданной книгой выложено в интернет с разрешения издательства.

Часть опубликованной версии книги:
`https://mccme.ru/~mskopenkov/skopenkov-pdf/sturm-2018.pdf`.

Оглавление

Оглавление

1 Введение

1.1 Зачем и для кого эта книга

Глубокое понимание математики полезно и математику, и профессионалу в наукоёмкой отрасли. В частности, «профессия» в названии этой книги не обязательно означает профессию математика.

Эта книга предназначена для старшеклассников и младшекурсников (в частности, ориентированных на олимпиады). См. подробнее п. 11.1 «Олимпиады и математика». Книгу можно использовать как для самостоятельных занятий, так и для преподавания.

В этой книге мы пытаемся построить мост (путем указания на отсутствие пропасти) между обычными школьными задачами и более сложными абстрактными математическими понятиями. Наша основная цель — помочь широкой аудитории читателей научиться применять математические методы для решения проблем, мотивированных «реальным миром или реальной работой» [Mey], и овладеть инструментами и способами мышления, которые будут полезны за пределами школы в самых разных дисциплинах.

Книга содержит наиболее стандартный «базовый» материал (впрочем, частично, скорее, для повторения, чем для первоначального изучения). Основное содержание книги составляет более сложный материал. Некоторые темы малоизвестны в традиции математических кружков, но полезны как для математического образования, так и для подготовки к олимпиадам.

Книга основана на занятиях, проведённых авторами и редакторами в разное время на математическом факультете Высшей школы экономики, в Независимом московском университете, в школах им. А. Н. Колмогорова (СУНЦ МГУ), «Интеллектуал» и № 1543 г. Москвы, летней школе «Современная математика», в Кировской и Костромской летних математических школах, в Московской выездной олимпиадной школе, в кружках «Математический семинар» и «Олимпиады и математика», на летней конференции Турнира городов, при подготовке команды России к международной математической олимпиаде, в системе дистанционного обучения математике МИОО.

Книга доступна уже старшеклассникам, интересующимся мате-

матикой[1]. Приводятся почти все определения, не входящие в школьную программу. Если где-то нужны дополнительные сведения, то приводятся ссылки.

При этом многие темы трудны, если изучать их «с нуля». Однако *последовательность изложения* помогает преодолевать трудности. В то же время многие темы *независимы* друг от друга. См. подробнее п. 1.4 «Как устроена книга».

1.2 Изучение путём решения и обсуждения задач

Мы следуем традиции изучения материала в виде решения и обсуждения задач. Эти задачи подобраны так, что в процессе их решения читатель (точнее, решатель) освоит основы важных теорий — как классических, так и современных. Основные идеи демонстрируются по одной и на «олимпиадных» примерах, т. е. на простейших частных случаях, свободных от технических деталей. Этим мы показываем, *как можно придумать* эти теории. См. подробнее п. 11.1 «Олимпиады и математика».

Обучение путём решения задач не только характерно для серьёзного изучения математики, но и продолжает древнюю культурную традицию. Например, послушники дзенских монастырей обучаются, размышляя над загадками, данными им наставниками. Впрочем, эти загадки являются скорее парадоксами, а не задачами. См. подробнее [Su]; ср. [Pl, с. 26–33]. А вот некоторые «математические» примеры: [Ar01, BS, GDI, GIF, KK08, Pr07-1, PoSe, SCY, Sk09, Sk19, SZ, Vag, Zv]; кое-где не только приведены задачи, но и изложены *принципы отбора* удачных задач. Об американской традиции см. [IBL, Mey, RMP].

Учиться, решая задачи, трудно. В частности, потому, что такое обучение обычно не создаёт *иллюзию* понимания. Однако усилия сполна вознаграждаются глубоким пониманием материала — в первую очередь, умением проводить аналогичные (и даже не очень

[1] Часть материала в некоторых кружках и летних школах изучается теми, кто только знакомится с математикой (например, 6-классниками). Однако приводимое изложение рассчитано на читателя, уже имеющего хотя бы минимальную математическую культуру. Заниматься с 6-классниками нужно по-другому, см., например, [GIF].

аналогичные) рассуждения. Кое-где вслед за великими математиками в процессе изучения интересных задач читатель увидит, как естественно возникают важные понятия и теории. Надеемся, это поможет ему совершить собственные настолько же полезные открытия (не обязательно в математике)!

Для решения задач достаточно понимания их условий. Другие знания и теории не нужны. (Впрочем, такие знания и теории как раз появляются при решении подобранных задач.) Но может потребоваться владение другими частями книги, что отражено в подсказках и указаниях.

К важнейшим задачам приводятся подсказки, указания, решения и ответы. Они расположены в конце каждого пункта. Однако к ним стоит обращаться после прорешивания каждой задачи.

Если задача выделена словом «теорема» («лемма», «следствие» и т. д.) и жирным шрифтом, то её утверждение важное.

Как правило, мы приводим *формулировку* красивого или важного утверждения (в виде задачи) перед его *доказательством*. В таких случаях для доказательства утверждения могут потребоваться следующие задачи. Это всегда явно оговаривается в подсказках, а иногда и прямо в тексте. Поэтому если некоторая задача не получается, то читайте дальше. (На занятии задача-подсказка выдаётся только тогда, когда ученик немного подумал над самой задачей.) Такой процесс обучения полезен, поскольку моделирует реальную исследовательскую ситуацию. См. подробнее п. 11.3 «О необходимости мотивировок».

Всё это — попытка продемонстрировать занятие в виде *диалога*, основанного на решении и обсуждении задач. Подробнее см. [KK15].

Напутствие. *А. Я. Канель-Белов*

Для успешного решения задач математических олимпиад высшего уровня необходимы в первую очередь общеукрепляющие средства: хорошая проработка алгебры (культура алгебраических преобразований), проработка школьной геометрии. Задачи этих олимпиад (кроме первых задач) практически всегда предполагают смешанный сценарий решения; редки задачи на применение некоторого метода или идеи в чистом виде. Решению таких «смешанных» задач

должна предшествовать работа с ключевыми задачами, в которых идеи работают в чистом виде.

Умение преобразовывать алгебраические выражения — одно из базовых. Его недостает «олимпиадникам», из-за его отсутствия часто возникают нелепые и обидные ошибки. Поэтому для успешного решения задач алгебраического, теоретико-числового и комбинаторного типа рекомендуем нарабатывать культуру арифметических выкладок.

1.3 Исследовательские задачи для школьников

Многим талантливым школьникам и студентам интересно решать исследовательские задачи. Они часто предлагаются в форме сложных задач, разбитых на шаги, см. [LKTG]. Возможно, конечный результат даже неизвестен заранее, а естественно появляется в процессе работы. Это одна из форм развития творческих способностей, близкая к научной деятельности, которая для многих учеников может оказаться наиболее удачной. Кроме того, обычно ученику интереснее изучать теорию в том случае, когда он сразу же применяет ее к конкретным задачам. Поэтому интерес к исследовательским задачам полезно поддерживать и развивать. Надеемся, настоящая книга поможет это делать.

Многие из приведённых задач — хорошие темы для исследовательских работ старшеклассников и младшекурсников, связанных с алгеброй, комбинаторикой и информатикой. С их решениями можно выступать на конференциях. Описание удачных примеров этой деятельности читатель может найти в материалах Московской математической конференции школьников [M]. Хотя большинство этих задач не претендуют на научную новизну, возможно их развитие в сторону новых результатов.

1.4 Как устроена книга

Книгу не обязательно изучать подряд. Читатель может выбрать удобную ему последовательность изучения (или вовсе опустить некоторые пункты) на основании приводимого плана. Для занятия кружка можно использовать любой пункт (или подпункт) книги.

Книга разбита на главы, параграфы и пункты (некоторые пункты разбиты на подпункты). Структура параграфов приблизительно описана в их начале. Если в задаче используется материал другого пункта, то можно либо игнорировать эту задачу, либо посмотреть то место, на которое приводится ссылка. Это даёт большую свободу читателю при изучении книги, но одновременно может требовать его внимательности.

Пункты внутри каждого параграфа расположены примерно в порядке возрастания сложности материала. Цифры в скобках после названия пункта означают его «относительный уровень»: 1 — самый простой, 4 — самый сложный. Первые пункты (не отмеченные звёздочкой) являются базовыми; если не указано противное, с них можно начать изучение параграфа. А к остальным пунктам (отмеченным звёздочкой) можно возвращаться потом; если не указано противное, то они независимы друг от друга. При изучении полезно *возвращаться* к пройденному материалу, но на новом уровне. Поэтому разные пункты одного параграфа можно изучать *не подряд*, а с перерывами на другие темы.

Обозначения, используемые во всей книге, приведены в конце введения. Понятия и обозначения, используемые в некоторой главе, вводятся в начале главы. В конце книги есть предметный указатель. Жирным шрифтом выделены номера страниц, на которых приводятся *формальные определения* понятий.

Параграф 11 составлен из заметок об общих принципах преподавания, адресованных прежде всего учителям. Возможно, заметки окажутся полезными и ученикам.

Обновляемая электронная версия части книги, пересечение которой с изданной книгой выложено в интернет с разрешения издательства: `http://www.mccme.ru/circles/oim/materials/sturm.pdf`.

О литературе и источниках

В конце каждого параграфа приводится литература, относящаяся ко всему параграфу, и отдельно литература по каждому пункту. Ссылки на книги [GDI, GKP, ZSS, Sk19, SZ], относящиеся ко многим параграфам, приведены в этом параграфе. Мы старались указать не только литературу, использованную при подготовке кон-

кретного материала, но также и жемчужины научно-популярного жанра на изучаемые темы. Мы надеемся, что наш список литературы, хотя бы в первом приближении, сможет стать путеводителем в море научно-популярной литературы по математике. Однако в него наверняка не вошли многие замечательные материалы, ввиду необъятности их количества. Важно, что обращение к литературе не нужно для решения задач, если явно не указано обратное.

Многие задачи не оригинальны, но первоисточник (даже если его можно установить) обычно не указывается. Ссылка после условия задачи указывает источник, из которого взята задача. Эти ссылки приведены для того, чтобы читатель смог сравнить своё решение с приведённым там. Если мы знали, что пересечение какого-то пункта с каким-то источником велико, то упоминали об этом.

Мы не даём ссылок на интернет-версии статей в журналах «Квант» и «Математическое Просвещение», их можно найти на сайтах

`http://kvant.ras.ru`, `http://kvant.mccme.ru`,

`http://www.mccme.ru/free-books/matpros.html`.

Благодарности и сведения о редакторах

Мы благодарим за серьёзную работу авторов материалов. Благодарим за полезные замечания рецензентов книги Е. А. Авксентьева, А. В. Антропова, Е. В. Бакаева, В. Н. Дубровского, К. А. Кнопа, Д. В. Мусатова, Л. Э. Медникова, А. А. Полянского, А. И. Сгибнева, С. Л. Табачникова, А. И. Храброва, Г. И. Шарыгина, и Д. Э. Шноля, а также анонимных рецензентов отдельных материалов. Благодарим А. Я. Канеля-Белова и А. В. Шаповалова (http://www.ashap.info), авторов большого количества материалов, высказавших также ряд полезных идей и замечаний. Благодарим Д. А. Пермякова, редактора книги [ZPS]. Благодарим учеников за каверзные вопросы и указания на неточности. Благодарим Е. С. Горскую и П. В. Широкова за подготовку многих рисунков. Благодарности по отдельным материалам приводятся прямо в них.

Мы приносим извинения за допущенные неточности и будем благодарны читателям за указания на них.

Главы 1 «Геометрия» и 2 «Комбигаторика» редактировали А. А. Заславский и М. Б. Скопенков соответственно. Мы организовали ре-

цензирование материалов параграфа 11, но редактировали их сами авторы.

А. Б. Скопенков и М. Б. Скопенков частично поддержаны грантами фонда Саймонса и фонда «Династия».

Места работы и интернет-страницы.

А. А. Заславский: ЦЭМИ РАН, школа 1543.

А. Б. Скопенков: Московский физико-технический институт (ГУ) и Независимый московский университет, `www.mccme.ru/~skopenko`.

М. Б. Скопенков: Национальный исследовательский университет Высшая школа экономики (факультет математики) и Институт проблем передачи информации РАН, `www.mccme.ru/~mskopenkov`.

1.5 Важные соглашения

Пункты внутри каждого параграфа расположены примерно в порядке возрастания сложности материала. Цифры в скобках после названия пункта означают его «относительный уровень»: 1 — самый простой, 4 — самый сложный. Первые пункты (не отмеченные звёздочкой) являются базовыми; если не указано противное, с них можно начать изучение главы. А к остальным пунктам (отмеченным звёздочкой) можно возвращаться потом; если не указано противное, то они независимы друг от друга.

Номера задач обозначаются жирным шрифтом. Если условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. *Загадкой* называется не сформулированный чётко вопрос; здесь нужно придумать и чёткую формулировку, и доказательство, ср. [VIN]. В задачах, отмеченных кружочком °, требуется привести только ответ без доказательства. Наиболее трудные задачи отмечены звёздочкой *. Если в условии задачи написано «найдите», то нужно дать ответ без знака суммы и многоточия. *Указание и решение* к задаче может опираться на *подсказку* к ней. Если некоторая задача не получается, то читайте дальше — следующие задачи могут оказаться подсказками.

1.6 Основные обозначения

• $\lfloor x \rfloor = [x]$ — (нижняя) целая часть числа x («пол»), т. е. наибольшее целое число, не превосходящее x.

• $\lceil x \rceil$ — верхняя целая часть числа x («потолок»), т. е. наименьшее целое число, не меньшее x.

• $\{x\}$ — дробная часть числа x.

• $d \mid n$, или $n \vdots d$ — число n *делится* на число d, т. е. $d \neq 0$ и существует такое целое k, что $n = kd$ (число d называется *делителем* числа n).

• $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ — множества всех действительных, рациональных и целых чисел соответственно.

• $\mathbb{Z}_2$ — множество $\{0, 1\}$ остатков от деления на 2 с операциями сложения и умножения по модулю 2.

• $\mathbb{Z}_m$ — множество $\{0, 1, \ldots, m-1\}$ остатков от деления на m с операциями сложения и умножения по модулю m. (Специалисты по алгебре чаще обозначают это множество $\mathbb{Z}/m\mathbb{Z}$, а через $\mathbb{Z}_m$ обозначают множество *целых m-адических чисел* для простого m.)

• $\binom{n}{k}$ — количество k-элементных подмножеств n-элементного множества (другое обозначение: C_n^k).

• $|X|$ — число элементов во множестве X.

• $A - B = \{x \mid x \in A \text{ и } x \notin B\}$ — разность множеств A и B.

• $A \sqcup B$ — дизъюнктное объединение множеств A и B, т. е. объединение $A \cup B$ непересекающихся множеств A и B.

• $A \subset B$ — «множество A содержится в множестве B». (В некоторых других книгах это обозначают $A \subseteq B$, а $A \subset B$ означает «множество A содержится в множестве B и не равно B».)

• Фраза «обозначим $x = a$» сокращается до $x := a$.

• id — отображение множества в себя, переводящее каждый элемент в себя (тождественное).

Литература

[GDI] *Глибичук А. А.*, *Дайняк А. Б.*, *Ильинский Д. Г.*, *Купавский А. Б.*, *Райгородский А. М.*, *Скопенков А. Б.*, *Чернов А. А.* Элементы дискретной математики в задачах. М.: МЦНМО, 2016. Abridged version: `http://www.mccme.ru/circles/oim/discrbook.pdf`.

[GIF] *Генкин С. А.*, *Итенберг И. В.*, *Фомин Д. В.* Ленинградские математические кружки. Киров, 1994.

[GKP] *Грэхем Р.*, *Кнут Д.*, *Паташник А.* Конкретная математика. М.: Мир, 1998.

[LKTG] Summer Conferences of Town Tournament. http://www.turgor.ru/en/lktg/index.php

[M] Московская математическая конференция школьников. `http://www.mccme.ru/mmks/index.htm`.

[Mey] *D. Meyer.* `http://blog.mrmeyer.com/starter-pack` .

[Pl] *Платон.* Федон, в кн.: Федон, Пир, Федр, Парменид. М.: Мысль, 1999.

[Ro04] *Рохлин В. А.* Лекция о преподавании математики нематематикам // Математическое просвещение. Сер. 3. 2004. Вып. 8. С. 21–36.

[RMP] Ross Mathematics Program, `http://u.osu.edu/rossmath` .

[VIN] *Виро О. Я.*, *Иванов О. А.*, *Нецветаев Н. Ю.*, *Харламов В. М.* Элементарная топология. М.: МЦНМО, 2010.

[Ar04] *Арнольд В. И.* Задачи для детей от 5 до 15 лет. М.: МЦНМО, 2004.

[BSh] *Блинков А. Д.*, *Шаповалов А. В.* (ред.). Серия «Школьные математические кружки».

[IBL] `http://en.wikipedia.org/wiki/Inquiry-based_learning`

[KK08] *Канель-Белов А. Я.*, *Ковальджи А. К.* Как решают нестандартные задачи. М.: МЦНМО, 2008.

[KK15] *Ковальджи А. К.*, *Канель-Белов А. Я.* Занятия по математике — листки и диалог // Математическое просвещение. Сер. 3. 2015. Вып. 19. С. 206–233.

[PoSe] *Пойа Д*, *Сегё Г.* Задачи и теоремы из анализа. М.: Наука, 1978.

[Pr07-1] *Прасолов В. В.* Задачи по планиметрии. М.: МЦНМО, 2007.

[Sk09] *Скопенков А. Б.* Основы дифференциальной геометрии в интересных задачах. М.: МЦНМО, 2009;
`http://arxiv.org/abs/0801.1568`.

[Sk19] *A. Skopenkov,* Mathematics via problems: from olympiades and math circles to a profession. Algebra. AMS, Providence, to appear.

[SCY] *Шклярский Д. О.*, *Ченцов Н. Н.*, *Яглом И. М.* Избранные задачи и теоремы элементарной математики. М.: Физматлит, 2001.

[Su] *Судзуки Д.* Основы дзэн-буддизма. Наука дзэн — ум дзэн. Киев: Преса України. 1992.

[SZ] *Mathematics via problems: from olympiades and math circles to a profession. Geometry and Combinatorics*, editors: M. Skopenkov and A. Zaslavsky. AMS, Providence, to appear.

[ZSS] Элементы математики в задачах: через олимпиады и кружки к профессии. Сборник под редакцией А. Заславского, А. Скопенкова и М. Скопенкова. Изд-во МЦНМО, 2018. Abridged version: `http://www.mccme.ru/circles/oim/materials/sturm.pdf`.

[ZPS] Математика в задачах. Сборник материалов московских выездных математических школ. Под редакцией А. Заславского, Д. Пермякова, А. Скопенкова, М. Скопенкова и А. Шаповалова. М.: МЦНМО, 2009; `http://www.mccme.ru/free-books/olymp/matprob.pdf`.

[Va87-1] *Васильев Н. Б.* и др. Заочные математические олимпиады. М.: Наука, 1987.

[Zv] *Звонкин А. К.* Малыши и математика. М.: МЦНМО, 2006.

2.1 Делимость (1)

2.1.1. (a) Сформулируйте и докажите признаки делимости на 2, 4, 5, 10, 3, 9, 11.

(b) Делится ли число $11\ldots1$ из 1993 единиц на 111111?

(c) Число $1\ldots1$ из 2001 единиц делится на 37.

2.1.2. Если a делится на 2 и не делится на 4, то количество чётных делителей числа a равно количеству его нечётных делителей.

2.1.3. Какие из следующих утверждений верны для любых a, b:

(a) $2|(a^2-a)$; (b) $4|(a^4-a)$; (c) $6|(a^3-a)$; (d) $30|(a^5-a)$;

(e) если $c|a$ и $c|b$, то $c|(a+b)$;

(f) если $b|a$, то $bc|ac$ для любого $c \neq 0$;

(g) если $bc|ac$ для некоторого c, то $b|a$?

При решении задачи 2.1.3 (c) вы использовали следующий факт 2.1.4 (a). Докажите его по определению делимости, не используя единственности разложения на простые множители (задача 2.2.8 (c))! Использование единственности может привести к порочному кругу, ведь обычно при доказательстве единственности используется факт, близкий к утверждению 2.1.4 (a).

2.1.4. (a) Если число a делится на 2 и на 3, то a делится на 6.

(b) Если число a делится на 2, на 3 и на 5, то a делится на 30.

(c) Если число a делится на 17 и на 19, то a делится на 323.

2.1.5. (a) Если k не кратно ни 2, ни 3, ни 5, то k^4-1 кратно 240.

(b) Если $a+b+c$ делится на 6, то и $a^3+b^3+c^3$ делится на 6.

(c) Если $a+b+c$ делится на 30, то и $a^5+b^5+c^5$ делится на 30.

(d) Если $n \geqslant 0$, то $20^{2n}+16^{2n}-3^{2n}-1$ делится на 323.

Подсказки

2.1.4. (a) Имеем $3a-2a=a$, поэтому a делится на 6.

3 Умножение по простому модулю

Из этого параграфа далее используются в основном теорема Ферма—Эйлера (задачи 3.1.1 и 3.1.5) и теорема о первообразном корне (задача 3.5.6 (b)). Впрочем, при применении теорем понимать их доказательство не обязательно.

В этом параграфе латинскими буквами обозначаются *целые числа* или *вычеты* по простому модулю p (что именно — видно из контекста).

3.1 Малая теорема Ферма (2)

3.1.1. (a) Обозначим $\mathbb{Z}_{97} = \{0, 1, \ldots, 96\}$. Определим отображение $f\colon \mathbb{Z}_{97} \to \mathbb{Z}_{97}$ так: $f(a)$ равно остатку от деления числа $14a$ на 97. Тогда f — взаимно однозначное соответствие.

Обсуждение. Достаточно доказать либо сюръективность, либо инъективность. Обычно доказывают *инъективность*. Но необходимая для этого основная лемма арифметики 2.5.7.b обычно доказывается через разрешимость уравнения $97x + 14y = 1$, из которой сразу вытекает *сюръективность*.

(b) Справедливо соотношение $(14 \cdot 1) \cdot (14 \cdot 2) \cdot \ldots \cdot (14 \cdot 96) \equiv 96! \pmod{97}$.

(c) Справедливо соотношение $14^{96} \equiv 1 \pmod{97}$.

(d) **Малая теорема Ферма.** Если p простое, то $n^p - n$ делится на p для любого целого n.

(e) *Alio modo.* Если p простое и n не делится на p, то $n^{p-1} - 1$ делится на p.

(f) Для простого p число $\binom{p}{k}$ делится на p для любого $k = 1, 2, \ldots, p-1$. (Из этого получается иное — по индукции — доказательство малой теоремы Ферма.)

3.1.2. Найдите остаток от деления

(a) 2^{100} на 101; (b) 3^{102} на 101; (c) 8^{900} на 29;

(d) 3^{2000} на 43; (e) 7^{60} на 143; (f) $2^{60} + 6^{50}$ на 143.

3.1.3. (a) Если p простое и $p > 2$, то $7^p - 5^p - 2$ делится на $6p$.

(b) Число $111\ldots11$ из 2002 единиц делится на 2003.

(c) Если p и q — различные простые числа, то $p^q + q^p - p - q$ делится на pq.

(d) Число $30^{239} + 239^{30}$ составное.

(e) Если p простое, то длина периода десятичной дроби $1/p$ делит $p - 1$.

3.1.4. Для простого p и a, не делящегося на p, назовём *порядком* $\operatorname{ord}\, a = \operatorname{ord}_p a$ числа (или вычета) a по модулю p наименьшее $k > 0$, для которого $a^k \equiv 1 \pmod p$:

$$\operatorname{ord}\, a = \operatorname{ord}_p a := \min\{k \geqslant 1 \mid a^k \equiv 1 \pmod p\}.$$

(a) Множество $\{m \geqslant 0\colon a^m \equiv 1 \pmod p\}$ состоит из целых неотрицательных чисел, кратных $\operatorname{ord} a$.

(b) Если $a^m \equiv a^n \pmod p$, то $m - n$ делится на $\operatorname{ord} a$.

(c) **Лемма.** Число $p - 1$ делится на $\operatorname{ord} a$.

(d) Если $\operatorname{ord} x$ и $\operatorname{ord} y$ взаимно просты, то $\operatorname{ord}(xy) = \operatorname{ord} x \cdot \operatorname{ord} y$.

(e) Для любых ли a, x, p верно, что $a \operatorname{ord}_p x^a = \operatorname{ord}_p x$?

Заметим, что по простому модулю можно определить деление и отрицательные степени. Аналоги утверждений 3.1.4 (a, b) справедливы для отрицательных степеней.

3.1.5. В этой задаче буквами $p, q, p_1, \ldots, p_k$ обозначаются различные простые числа.

(a) Если $p \neq q$ и n не делится ни на p, ни на q, то $n^{(p-1)(q-1)} - 1$ делится на pq.

(b) Если n не делится на p, то $n^{p^\alpha(p-1)} - 1$ делится на $p^{\alpha+1}$.

(c) **Теорема Эйлера.** Пусть n взаимно просто с $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Обозначим $\varphi(m) := (p_1 - 1)p_1^{\alpha_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{\alpha_k - 1}$. Тогда $n^{\varphi(m)} - 1$ делится на m.

(d) Число $\varphi(m)$ равно количеству чисел от 1 до m, взаимно простых с m.

3.1.6. (Загадка.) Известно, что n — нечётное число от 3 до 47, не делящееся на 5. Как быстро вычислять неизвестное n по известному $n^7 \bmod 50$?

3.3 Квадратичные вычеты (2*)

Цель этого цикла задач — мотивировать и обсудить проблему разрешимости сравнения $x^2 \equiv a \pmod p$ для простого p. В этом пункте через p обозначается нечётное простое число.

3.3.1. (a) Какие остатки могут давать квадраты целых чисел при делении на 3, 4, 5, 6, 7, 8, 9, 10?

(b) Если a^2+b^2 делится на 3 (на 7), то a и b делятся на 3 (на 7).

(c) Число вида $4k+3$ не представимо в виде суммы двух квадратов.

(d) Существует бесконечно много целых положительных чисел, не представимых в виде суммы трёх квадратов.

3.3.2. Решите уравнения в целых числах:

(a) $x_1^2+x_2^2+x_3^2+x_4^2+x_5^2=y^2$ (в нечётных числах);

(b) $3x=5y^2+4y-1$; (c) $x^2+y^2=3z^2$; (d) $2^x+1=3y^2$;

(e) $x^2=2003y-1$; (f) $x^2+1=py$, где $p=4k+3$;

3.3.3. (a) Если $p=4k+3$ делит a^2+b^2, то $p|a$ и $p|b$.

(b) Число, в каноническое разложение которого некоторый простой делитель вида $4k+3$ входит в нечётной степени, не представимо в виде суммы двух квадратов (целых чисел).

(c)* Уравнение $x^2+1=py$ разрешимо в целых числах при $p=4k+1$ (и неразрешимо при $p=4k+3$).

(d)* Любое простое число вида $4k+1$ представимо в виде суммы двух квадратов.

(e)* Число, в каноническое разложение которого любой простой делитель вида $4k+3$ входит в чётной степени, представимо в виде суммы двух квадратов.

(f) Простых чисел вида $4k+1$ бесконечно много.

Доказательство Дон Загира утверждения (d) можно найти в книге [Pr07-1].

3.3.4. (Загадка.) «Сведите» уравнение $py=at^2+bt+c$, $a\neq 0$, к сравнению $x^2\equiv k \pmod p$.

Остаток $a\neq 0$ называется *квадратичным вычетом* (*квадратичным невычетом*) *по модулю* p, если сравнение $x^2\equiv a(p)$ разрешимо (неразрешимо). Слова «по модулю p» далее опускаются.

3.4 Квадратичный закон взаимности (3*)

Здесь строится алгоритм выяснения разрешимости сравнения $x^2 \equiv a \pmod p$ для простого p. Используется п. 3.3 «Квадратичные вычеты».

3.4.1. Если число $p = 8k + 5$ простое, то
(a) $2^{4k+2} \equiv -1 \pmod p$;
(b) уравнение $x^2 - 2 = py$ неразрешимо в целых числах.

3.4.2. Если число $p = 8k + 1$ простое, то
(a) $2^{4k} \equiv 1 \pmod p$;
(b) уравнение $x^2 - 2 = py$ разрешимо в целых числах.

3.4.3. (a) Если число $p = 8k \pm 1$ простое, то $2^{(p-1)/2} \equiv 1 \pmod p$.
(b) Если число $p = 8k \pm 3$ простое, то $2^{(p-1)/2} \equiv -1 \pmod p$.
(c) Для каких простых p разрешимо в целых числах уравнение $x^2 - 2 = py$?

3.4.4. (a) Если число $p = 12k \pm 1$ простое, то $3^{(p-1)/2} \equiv 1 \pmod p$.
(b) Если число $p = 12k \pm 5$ простое, то $3^{(p-1)/2} \equiv -1 \pmod p$.
(c) Для каких простых p разрешимо в целых числах уравнение $x^2 - 3 = py$?

3.4.5. Для нечётного простого числа p рассмотрим *символ Лежандра*

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & a \text{ — квадратичный вычет по модулю } p; \\ -1, & a \text{ — квадратичный невычет по модулю } p. \end{cases}$$

Например, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ по задаче 3.4.3 и $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ по задаче 3.3.8.

(a) **Критерий Эйлера.** Справедливо соотношение

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

(b) **Лемма Гаусса.** Справедливо соотношение

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{(p-1)/2} \left[\frac{2ax}{p}\right]}.$$

3.5 Первообразные корни (3*)

3.5.1. (2–7) Сформулируйте и обоснуйте алгоритм решения сравнения $a^x \equiv b \ (m)$ для заданных a, b, взаимно простых с заданным $m \in \{2, 3, 4, 5, 6, 7\}$.

(Решение такого сравнения — одна из основных мотивировок этого занятия.)

3.5.2. (a) Если $(a, 35) = 1$, то $a^{12} \equiv 1 \pmod{35}$.

(b) Если m делится на два различных простых нечётных числа и $(a, m) = 1$, то $a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$.

Пусть $(g, m) = 1$. Вычет g называется *первообразным корнем* по модулю m, если остатки от деления на m чисел $g^1, g^2, \ldots, g^{\varphi(m)} \equiv 1$ различны. Например,

• число 2 является первообразным корнем по модулю 5, а число 4 — нет;

• по задаче 3.5.2 (b) если m делится на два различных простых нечётных числа, то не существует первообразного корня по модулю m.

3.5.3. Докажите существование первообразного корня по простому модулю следующего вида:

(a) 257; (b) $2^l + 1$; (c) $2^k \cdot 3^l + 1$; (d) 151; (e) $2^k \cdot 3^l \cdot 5^m + 1$.

Простой метод решения пунктов (a), (b), (c), не проходит для (d), (e). Продемонстрируем метод решения пунктов (d), (e) на примерах.

3.5.4. (a) Вычет g — первообразный корень по модулю 97 тогда и только тогда, когда ни g^{48}, ни g^{32} не сравнимы с 1 по модулю 97.

(b) Сравнение $x^{48} \equiv 1 \pmod{97}$ имеет ровно 48 решений.

(c) Сравнение $x^{32} \equiv 1 \pmod{97}$ имеет ровно 32 решения.

(d) Существует первообразный корень по модулю 97.

(e) Количество первообразных корней по модулю 97 равно 32.

3.5.5. (a) Вычет g — первообразный корень по модулю 151 тогда и только тогда, когда ни g^{30}, ни g^{50}, ни g^{75} не сравнимы с 1 по модулю 151.

3.6 Высокие степени (3*). *А. Я. Канель-Белов, А. Б. Скопенков*

3.6.1. (a) Для любых n и нечетного k число $k^{2^n}-1$ делится на 2^{n+2}.

(b) Для любого n число $2^{3\cdot 7^n}-1$ делится на 7^{n+1}.

3.6.2. При каких a

(a) 2^a-1 делится на 3^{100}; (b) 2^a+1 делится на 3^{100};

(c) 5^a-1 делится на 2^{100}; (d) 2^a-1 делится на 5^{100}?

Утверждение 3.6.1 (a) означает, что ни при каком $n \geqslant 3$ не существует первообразного корня по модулю 2^n (см. определение в п. 3.5). Ответы к задачам 3.6.2.(a),(d),(c) и утверждение 3.6.1.(b) означают, что для любого n число 2 является первообразным корнем по модулю 3^n и по модулю 5^n, а числа 5 и 2 не являются первообразными корнями по модулю 2^n и по модулю 7^n.

3.6.3. (a) Найдите первообразный корень по модулю 7^{100}.

(b) **Теорема.** Первообразные корни существуют только по модулям $2, 4, p^n, 2p^n$.

3.6.4. Пусть $p>2$ простое, g — первообразный корень по модулю p и $g^{p-1}-1$ не делится на p^2. Тогда g — первообразный корень по модулю

(a) p^2; (b) p^3; (c) p^n для любого n.

3.6.5. Пусть $p>2$ простое.

(a) Если g — первообразный корень по модулю p, то одно из чисел $g^{p-1}-1$ и $(g+p)^{p-1}-1$ не делится на p^2.

(b) Если g — первообразный корень по модулю p^2, то g — первообразный корень по модулю p^n для любого n.

(c) Для любого целого положительного n существует первообразный корень по модулю p^n.

(d) То же по модулю $2p^n$.

3.6.6. Лемма об уточнении показателя. Пусть p — простое число, $p>2$ или $n>1$, q не делится на p и $x-1$ делится на p^n, но не на p^{n+1}.

(a) Число x^q-1 делится на p^n, но не на p^{n+1}.

4.2 Решение уравнений 3-й и 4-й степени (2)

Благодарю О. Е. Орёл за полезные обсуждения.

Приведённый здесь материал важен и широко известен, но не входит в школьную или университетскую программу. Отличие приводимого рассуждения от встречающихся в других источниках в том, что (вместо немотивированных замен) уравнения естественно сводятся к таким, которые ясно, как решать.

Например, уравнение $x^2 + 4x - 1 = 0$ сводится к уравнению $y^2 - 5 = 0$ заменой переменной $y = x + 2$.

4.2.1. (a) Уравнение $x^3 + 3x^2 + 5x + 7 = 0$ «сводится» заменой переменной к уравнению $y^3 + py + q = 0$ с некоторыми числами p, q.

(b) Уравнение $ax^3 + bx^2 + cx + d = 0$ при $a \neq 0$ «сводится» заменой переменной к уравнению $y^3 + py + q = 0$ с некоторыми числами p, q.

(c) Уравнение $ax^4 + bx^3 + cx^2 + dx + e = 0$ при $a \neq 0$ «сводится» заменой переменной к уравнению $y^4 + py^2 + qy + r = 0$ с некоторыми числами p, q, r.

4.2.2. (a) Докажите, что $\sqrt[3]{2 + \sqrt{5}} - \sqrt[3]{\sqrt{5} - 2} = 1$.

(b) Найдите хотя бы одно решение уравнения $x^3 - 3\sqrt[3]{2}x + 3 = 0$.

Указание. **Метод дель Ферро.** Так как

$$(u + v)^3 = u^3 + v^3 + 3uv(u + v),$$

то число $u + v$ является корнем уравнения $x^3 - 3uvx - (u^3 + v^3) = 0$.

(c) Решите уравнение $x^3 - 3\sqrt[3]{2}x + 3 = 0$.

4.2.3. (a) Разложите на множители выражение $a^3 + b^3 + c^3 - 3abc$.

(b) Справедливо неравенство $a^2 + b^2 + c^2 \geqslant ab + bc + ca$. Когда достигается равенство?

(c) Справедливо неравенство $a^3 + b^3 + c^3 \geqslant 3abc$ при $a, b, c > 0$.

(d) Разложите выражение $a^3 + b^3 + c^3 - 3abc$ на линейные множители с комплексными коэффициентами.

Задачи этого пункта о комплексных числах можно пропустить. Но для их решения необходимы лишь минимальные сведения о комплексных числах: достаточно уметь решать задачи 4.5.1 и 4.5.2.

4.2.4. (a) Сформулируйте и докажите теоремы, описывающие все вещественные (все комплексные) решения уравнения $x^2+px+q=0$.

(b) Сформулируйте и докажите теоремы, описывающие все вещественные (все комплексные) решения уравнения $x^3+px+q=0$ в том случае, когда работает метод дель Ферро (см. задачу 4.2.2). А при каком условии на p, q применим этот метод для вещественных решений, если квадратные корни разрешается извлекать только из положительных чисел?

(c) Составьте алгоритм (точного, или символьного) нахождения всех вещественных корней уравнения $ax^3+bx^2+cx+d=0$, где $a\neq 0$.

При решении некоторых кубических уравнений методом дель Ферро в формулах неожиданным образом возникают комплексные числа — как раз тогда, когда все корни исходного уравнения вещественны. Такие уравнения можно также решать следующим «чисто вещественным» методом. Он также интересен тем, что подводит к *трансцендентным методам* решения уравнений [PSo].

4.2.5. (a) Решите уравнение $4x^3-3x=\frac{1}{2}$.

(b) Решите уравнение $x^3-3x-1=0$.

(c) Используя функции cos и arccos, напишите общую формулу для решения уравнения $x^3+px+q=0$ методом, намеченным в этой задаче. При каком условии уравнение $x^3+px+q=0$ решается этим методом?

4.2.6. Решите уравнение

(a) $(x^2+2)^2=9(x-1)^2$; (b) $x^4+4x-1=0$;

(c) $x^4+2x^2-8x-4=0$; (d) $x^4-12x^2-24x-14=0$.

Указание к задаче 4.2.6 (b). **Метод Феррари.** Подберите такие α, b, c, что

$$x^4+4x-1=(x^2+\alpha)^2-(bx+c)^2.$$

Для этого найдите хотя бы одно α, для которого квадратный трёхчлен $(x^2+\alpha)^2-(x^4+4x-1)$ от x является полным квадратом. Для этого найдите дискриминант этого квадратного трёхчлена. Он является кубическим многочленом от α и называется *кубической резольвентой* многочлена x^4+4x-1.

4.7 Диофантовы уравнения и гауссовы числа (4*). *А. Я. Канель-Белов*

Всем хорошо знаком алгоритм Евклида. Даны два числа a, b. Из них выбирается большее, из большего вычитается меньшее, большее заменяется на разность, и с новой парой чисел производится та же процедура. См. задачу 2.5.9 (b). С помощью алгоритма Евклида доказываются арифметические свойства чисел и это Вы изучали раньше (см. п. 2.5 «Линейные диофантовы уравнения» и п. 4.4 «Делимость для многочленов»). Приведём принципиально новые (для большинства школьников) его применения.

4.7.1. Решите уравнения в целых числах:
(a) $x^2 + 4 = y^3$; (b) $x^2 + 2 = y^n$; (c)* $x^3 + y^3 = z^3$.

Попробуйте порешать их, не читая дальнейшего! Впрочем, у Вас вряд ли получится. Возвращайтесь к этой задаче по мере чтения дальнейшего материала.

При решении уравнения $x^2 + 4 = y^3$ в целых числах хочется действовать так: $x^2 + 4 = (x + 2i)(x - 2i)$. При нечётном x оба эти множители взаимно просты, и потому оба являются кубами. Из этого получается решение. (Случай чётного x хитрее: обе скобки могут делиться на $(1 + i)^3$.) Попробуйте довести решение до конца, а затем сравнить с приведённым в конце темы.

Одним словом, хочется наслаждаться дополнительными возможностями при разложении на множители за счёт использования *гауссовых чисел*, т. е. чисел вида $a + bi$ с целыми a и b. Однако не всё коту масленица — так получается не всегда (см. задачи 2.2.8 (b) и 4.7.3 (b)), но иногда получается. Чтобы применять разложение на множители для решения уравнений, нужна *однозначность разложения на простые множители*. Если она имеет место, то мы имеем всё те же арифметические удовольствия, что и для целых чисел. Следующая задача показывает удивительный факт: для *арифметических* удовольствий достаточно доказать *геометрический* факт о возможности деления с остатком.

4.7.2. Гауссово число называется *(гауссово) простым*, если оно не разлагается на два гауссовых множителя, каждый из которых отли-

чен от ± 1 и $\pm i$. В этой задаче латинские буквы обозначают гауссовы числа.

(a) Однозначность разложения на простые множители вытекает из следующего свойства (аналога леммы Евклида 2.5.7 (c)).

Факториальность. Для любых a, b если простое число p делит ab, то p делит a или p делит b.

(b) Факториальность вытекает из следующего свойства (аналога леммы о представлении НОД 2.5.7 (a)).

Главноидеальность. Для любых a, b существуют такие x, y, что $xa + yb = \gcd(a, b)$. (Дайте определение наибольшего общего делителя $\gcd(a, b)$ чисел a, b самостоятельно!)

(c) Главноидеальность обеспечивается следующим свойством (аналогом теоремы о делении с остатком 2.4.1 (b)).

Евклидовость. Для любых $b \neq 0$ и a существует такое k, что $|a - kb| < |b|$.

4.7.3. Верна ли евклидовость (и, значит, факториальность!) для множества $\mathbb{Z}[\xi]$ чисел вида $a + b\xi$ с целыми a, b, если ξ есть

(a) $\sqrt{-2}$; (b) $\sqrt{-3}$; (c) $(1 - \sqrt{-3})/2$; (d) $(1 - \sqrt{-5})/2$;

(e) $(1 - \sqrt{-7})/2$?

4.7.4. (a) Никакое простое число вида $4k-1$ не разлагается в сумму двух квадратов.

(b) Любое простое число вида $4k + 1$ разлагается в сумму двух квадратов, причём ровно одним способом.

(b) Существует целое число, ровно 1024 способами разлагающееся в сумму двух квадратов.

Эту задачу проще решать без гауссовых чисел (см. п. 3.3), однако полезно потренироваться в их применении!

Подробнее см. [Pos, § 4]. См. также задачу 4.4.7.

Указания, ответы и решения

4.7.1. (a) (Р. И. Девятов) *Ответ*: $x = \pm 2$, $y = 2$ и $x = \pm 11$, $y = 5$.

Перейдём к целым гауссовым числам и получим $(x+2i)(x-2i) = y^3$.

5.3 Комбинаторика классов эквивалентности (2)

Этот пункт посвящён подсчёту числа классов эквивалентости (т. е. раскрасок и т. д.). Такой подсчёт подводит читателя к важному понятию *группы преобразований* и к элементарной формулировке *леммы Бёрнсайда.* Формулировка и доказательство этого и других результатов на языке абстрактной теории групп делает их менее доступными. Ср. [ZSS, § 28 «О необходимости мотивировок»].

Не требуется, чтобы в раскраске присутствовали все данные цвета. Раскраски, совмещающиеся вращением пространства (т. е. движением пространства, сохраняющим ориентацию и имеющим неподвижную точку), считаются одинаковыми.

Следующие определения используются только в задачах 5.3.1.(b), 5.3.5.(e), 5.3.10 (и потому могут быть пропущены при решения остальных задач).

Изоморфизм между графами— такая биекция между множествами их вершин, что для любых двух вершин эти вершины соединены ребром тогда и только тогда, когда их образы при биекции соединены ребром. *Автоморфизм* графа— его изоморфизм на себя.

5.3.1. Найдите количество

(a) раскрасок граней куба в красный и серый цвета;

(b) замкнутых ориентированных связных p-звенных ломаных (возможно, самопересекающихся), проходящих через все вершины данного правильного p-угольника.

Здесь p простое и ломаные, совмещающиеся поворотом, неотличимы.

Задачи 5.3.1 простые, их можно решить без идей, приводящих к лемме Бёрнсайда.

5.3.2. Найдите количество раскрасок карусели из n незанумерованных вагончиков в r цветов (т. е. количество раскрасок вершин правильного n-угольника в r цветов, если раскраски, совмещающиеся поворотом, неотличимы) для

(a) $n = 5$; (b) $n = 4$; (c) $n = 6$.

Задачу 5.3.2 для произвольного n можно решить способом, аналогичным придуманному вами для малых n. Однако решение будет

громоздким. Приведём более простой (для «очень непростых» n) способ на примере решения задачи 5.3.2 (c).

Назовём (*раскрашенным*) *поездом* раскраску карусели из *занумерованных* вагончиков в r цветов. Тогда всего имеется r^6 поездов из 6 вагончиков.

Распределим поезда по вокзалам так, чтобы на каждом вокзале находились все поезда, полученные из некоторой одной раскраски карусели всевозможными разрубаниями. Тогда искомое количество Z раскрасок равно количеству вокзалов.

Назовем *периодом* $T(\alpha)$ поезда α наименьшую положительную величину циклического сдвига, переводящего поезд α в себя.

5.3.3. Количество поездов на вокзале равно периоду каждого из поездов, стоящих на этом вокзале. В частности, периоды поездов, стоящих на одном вокзале, равны.

На каждом вокзале выберем один поезд. Посадим в него 6 пассажиров и выдадим им билеты с числами 0, 1, 2, 3, 4, 5. Тогда нужно найти общее число $6Z$ пассажиров.

По команде каждый пассажир переходит в (раскрашенный) поезд, полученный из выбранного поезда циклическим сдвигом на число, указанное в билете пассажира. Ясно, что каждый пассажир остается на прежнем вокзале.

5.3.4. (a) В выбранном поезде α останется $6/T(\alpha)$ пассажиров. Более формально, количество тех $s \in \{0,1,2,3,4,5\}$, для которых циклический сдвиг на s переводит поезд α в себя, равно $6/T(\alpha)$.

(b) В каждом поезде α окажется $6/T(\alpha)$ пассажиров.

Значит, общее число $6Z$ пассажиров равно количеству всех пар (α, s), в которых $s \in \{0,1,2,3,4,5\}$ и α — поезд, переходящий в себя при циклическом сдвиге на s вагончиков. Циклический сдвиг на s переводит в себя ровно $r^{\gcd(s,6)}$ поездов. Поэтому

$$6Z = r^6 + r + r^2 + r^3 + r^2 + r.$$

Приведенный план решения можно представить в виде формулы

$$6Z = \sum_x T(x) \cdot \frac{6}{T(x)} = \sum_\alpha \frac{6}{T(\alpha)} = r^6 + r + r^2 + r^3 + r^2 + r.$$

Здесь первое суммирование происходит по всем по всем раскраскам x каруселей, а второе — по всем поездам α.

5.3.5. Найдите количество раскрасок

(a) карусели из n вагончиков в r цветов;

(b) раскрасок ожерелий из $n = 2k+1$ бусин в r цветов (ожерелья считаются одинаковыми, если они совмещаются либо поворотом вокруг центра ожерелья, либо осевой симметрией ожерелья);

(c) незанумерованных граней куба в r цветов;

(d) незанумерованных вершин куба в r цветов;

(c) в r цветов вершин правильного тетраэдра?

(e) раскрасок незанумерованных вершин графа $K_{3,3}$ (рис. 2) в r цветов (раскраски считаются одинаковыми, если они совмещаются автоморфизмом этого графа).

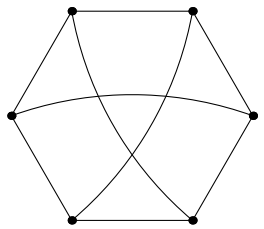

Рис. 2: Граф $K_{3,3}$

5.3.6. Перечислите все вращения куба (т. е. вращения пространства, переводящие куб в себя). (Эта задача разбита на шаги в [SZ, п. «Самосовмещения»].)

Приведем план решения задачи 5.3.5 (c). (Пункты (b)–(e) решаются аналогично. Пункт (b) решается и без этого указания.)

Назовём *(раскрашенной) коробкой* (или *замороженной раскраской*) раскраску занумерованых граней куба в r цветов. Тогда всего имеется r^6 коробок.

Распределим коробки по комнатам так, чтобы в каждой комнате находились все коробки, полученные из некоторой одной коробки всевозможными вращениями. Тогда искомое количество Z раскрасок равно количеству комнат.

В каждой комнате выберем одну коробку. Посадим в нее 24 таракана, соответствующих вращениям куба. Тогда нужно найти общее число тараканов $24Z$.

По команде каждый таракан переползает в коробку, полученную из выбранной тем вращением, которое соответствует этому таракану. Ясно, что каждый таракан остается в прежней комнате. Число тараканов, оставшихся в выбранной коробке, равно количеству вращений куба, переводящих эту коробку в себя. Обозначим через $\mathrm{st}\alpha$ количество вращений куба, переводящих (раскрашенную) коробку (т. е. замороженную раскраску) α в себя.

5.3.7. (a) Число тараканов, оказавшихся в коробке α, равно $\mathrm{st}\alpha$. Более формально, если существует вращение, переводящее замороженную раскраску α в замороженную раскраску α', то количество таких вращений равно $\mathrm{st}\alpha$.

(b) В любой другой коробке из некоторой комнаты окажется столько же тараканов, сколько в выбранной коробке из этой комнаты. Более формально, для любых двух замороженных раскрасок α и α', переходящих друг в друга при некотором вращении, выполняется равенство $\mathrm{st}\alpha = \mathrm{st}\alpha'$. (Эти равные числа обозначаются $\mathrm{st}x$, где x — соответствующая раскраска незанумерованных граней куба.)

Поэтому общее число тараканов равно количеству всех пар (α, s), в которых s — вращение куба и α — коробка, переходящая в себя при вращении s. Поэтому осталось решить следующую задачу.

5.3.8. Для каждого вращения куба s найдите количество $\mathrm{fix}s$ коробок (т. е. замороженных раскрасок), переходящих в себя при вращении s.

Обозначим через N_x количество замороженных раскрасок, отвечающих раскраске x. Тогда для любой раскраски x число $\mathrm{st}x \cdot N_x$ равно количеству вращений куба, т. е. 24. Поэтому приведенный план решения можно представить в виде формулы

$$24Z = \sum_x \mathrm{st}x \cdot N_x = \sum_\alpha \mathrm{st}\alpha = \sum_s \mathrm{fix}s.$$

Здесь первое суммирование происходит по всем раскраскам x незанумерованных граней, второе — по всем замороженным раскраскам α, а третье — по всем вращениям куба s.

Как сформулировать общий результат, который можно было применять вместо повторения намеченных решений задач 5.3.5 (a), (c)?

5.3.9. Лемма Бёрнсайда. Пусть заданы конечное множество M и семейство $\{g_1, g_2, \ldots, g_n\}$ преобразований этого множества, замкнутое относительно взятия композиции и взятия обратного элемента. Назовём элементы множества M *эквивалентными*, если один из них можно перевести в другой одним из данных преобразований. Тогда количество классов эквивалентности равно $\frac{1}{n}\sum\limits_{k=1}^{n} \mathrm{fix}(g_k)$, где $\mathrm{fix}(g_k)$ — количество элементов множества M, которые преобразование g_k переводит в себя.

5.3.10. Найдите количество графов с n вершинами с точностью до изоморфизма. (Ответ можно оставить в виде суммы.)

5.3.11. Найдите количество b_n отображений $\{0,1\}^n \to \{0,1\}$ с точностью до перестановки переменных.

Подсказки

5.3.1. *Ответы*: (a) 10; (b) $p-2+((p-1)!+1)/p$.

5.3.2. *Ответы*: (a) $(r^5+4r)/5$; (b) $(r^4+r^2+2r)/4$;

5.3.5. (a) *Ответ*: $\frac{1}{n}\sum\limits_{d|n}\varphi\left(\frac{n}{d}\right)r^d$. Функция Эйлера $\varphi(n)$ определена в задаче 3.1.5.

7 Последовательности и пределы

Этот параграф почти независим от остальной части книги. В других местах из него используются лишь простые факты.

7.1 Конечные суммы и разности (3)

Последовательностью сумм последовательности $\{a_n\}_{n=1}^{\infty}$ называется последовательность $b_n = \Sigma a_n := a_1 + \ldots + a_n$, а *последовательностью разностей* — последовательность $c_n = \Delta a_n := a_{n+1} - a_n$.

Например, $\Delta 2^n = 2^n$ и $\Sigma 2^n = 2^{n+1} - 2$.

(Сумма и разность — аналоги *интеграла* и *производной*.)

В этом пункте n обозначает номер члена последовательности, «по которому» берётся сумма и разность. Так, например, $\Delta 2^k = 0$.

7.1.1. Найдите

(a) Δn^k для каждого целого $k \geqslant -1$; (b) $\Delta \cos n$; (c) $\Delta(n \cdot 2^n)$.

7.1.2. Найдите

(a) $\Sigma \sin n$; (b) $\Sigma \frac{1}{n(n+1)\ldots(n+k)}$ для каждого целого $k > 0$.

7.1.3. Какие из следующих равенств выполняются для некоторой непостоянной последовательности a_n:

(a) $\Delta a_n = 0$; (b) $\Delta a_n = 1$; (c) $\Delta a_n = a_n$;

(d) $\Sigma a_n = a_n$; (e) $\Sigma \Delta a_n = a_n$; (f) $\Delta \Sigma a_n = a_n$?

7.1.4. (a) Найдите $\sum\limits_{k=0}^{n} (-1)^k k^2 \binom{n}{k}$.

(b) **Лемма.** k-я разность многочлена k-й степени есть постоянная, а $(k+1)$-я равна 0.

(c) (Загадка.) Выразите $\Delta^k a_n$ через $a_n, a_{n+1}, \ldots, a_{n+k}$.

(d) **Лемма.** Равенство $\Delta^k a_n = 0$ имеет место тогда и только тогда, когда a_n — многочлен от n степени не выше $k-1$.

(e) Для некоторого многочлена $P_\lambda(n)$, имеющего степень l при $\lambda \neq 1$ и степень $l-1$ при $\lambda = 1$, выполняется равенство $\Delta(n^l \lambda^n) = P_\lambda(n)\lambda^n$.

(f) **Формула Лейбница.** Справедливо равенство

$$\Delta(a_n b_n) = a_{n+1}\Delta b_n + b_n \Delta a_n.$$

7.3 Конкретная теория пределов (4*)

Задачи этого пункта интересны не только как простейший способ разобраться в теории пределов. Похожие задачи о конкретных, хотя и грубых оценках часто возникают и на олимпиадах, и в прикладной математике, и в теоретической математике.

В решении этих задач нельзя пользоваться функциями $\sqrt[n]{x}$, a^x, $\log_a x$, $\arcsin x$ и т. п. без определения этих функций (поскольку для их определения — например, для доказательства существования такого x, что $x^2 = 2$, — фактически нужно эти задачи решить). Исключение: если некоторая функция используется в условии, то её можно использовать и в решении. Можно пользоваться без доказательства свойствами неравенств.

7.3.1. Найдите хотя бы одно такое N, чтобы для любого $n > N$ выполнялось неравенство $a_n > 10^9$, если

(a) $a_n = \sqrt{n}$; (b) $a_n = n^2 - 3n + 5$; (c) $a_n = 1{,}02^n$;

(d) $a_n = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots + \frac{1}{n}$.

7.3.2. Неравенство Бернулли. Докажите, что $(1 + x)^a \geqslant 1 + ax$ для любых $x \geqslant -1$ и

(a) целого $a \geqslant 1$; (b) рационального $a \geqslant 1$;

(c) действительного $a \geqslant 1$.

7.3.3. Найдите хотя бы одну пару таких a и N, чтобы для любого $n > N$ выполнялось неравенство $|a_n - a| < 10^{-8}$, если

(a) $a_n = \frac{n^2-n+28}{n-2n^2}$; (b) $\sqrt{5 + \frac{2}{n}}$; (c) $a_n = n\left(\sqrt{1 + \frac{1}{n}} - 1\right)$;

(d) $a_n = n\left(\sqrt[3]{1 + \frac{1}{n}} - 1\right)$; (e) $a_n = 0{,}99^n$; (f) $a_n = \sqrt[n]{2}$;

(g) $a_n = n^9/2^n$; (h)* $a_n = (1 + 1/n)^n$; (i) * $a_n = n(\sqrt[n]{2} - 1)$;

(j) $a_n = \frac{1}{1^2} + \frac{1}{2^2} + \ldots + \frac{1}{n^2}$; (k)* $a_n = \frac{1}{1\sqrt{1}} + \frac{1}{2\sqrt{2}} + \frac{1}{3\sqrt{3}} + \ldots + \frac{1}{n\sqrt{n}}$;

(l)* $a_n = \frac{1}{0!} + \frac{1}{1!} + \ldots + \frac{1}{n!}$; (m)* $a_n = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots + \frac{(-1)^n}{2n+1}$.

7.3.4. Найдите хотя бы одну пару таких a и $\delta > 0$, чтобы для любого $x \in (-\delta, \delta)$ было выполнено неравенство $|f(x) - a| < 3 \cdot 10^{-9}$ для функции $f(x)$, равной

(a) x^3; (b) 3^x; (c) $\sin x$; (d) $\frac{\sin x}{x}$;

(e) $\frac{\sqrt{1+x^5}}{\cos x - 2}$; (f) $\frac{1+\sin x}{x^3-1}$; (g) $(1 + 1/x)^x$.

7.6 Примеры трансцендентных чисел

7.6.1 Введение (1)

Число x называется *трансцендентным*, если оно не является корнем уравнения $a_t x^t + a_{t-1}x^{t-1} + \ldots + a_1 x + a_0 = 0$ с целыми коэффициентами $a_t \neq 0$, $a_{t-1}, \ldots, a_0$. Первый явный пример трансцендентного числа был приведен Жозефом Лиувиллем в 1835 (см. теорему 7.6.4.a и [CR, Гл. 2, §6]). В 1929 Курт Малер [Ma29] доказал трансцендентность *числа Малера* (см. теорему 7.6.7; эта трансцендентность не следует ни из общей теоремы Лиувилля 7.6.4.b, ни из теорем Туэ, Зигеля и Рота [CR, Гл. 2, §6], [Fe83]). В работе [Ma29] был получен более общий результат, ср. [Ga80, Ni96]. Но доказательство в [Ma29] (так же как и в [Ni96]) не элементарно и длинно.

В этом пункте мы приведем простые доказательства трансцендентности чисел Лиувилля и Малера. Первое из них основано на элементарной версии теоремы Лагранжа о среднем значении 8.2.7 (c). Хотя оно известно специалистам, к сожалению, обычно изучаются более сложные доказательства. Второе из них основано на двоичной записи. Видимо, оно не было известно до [Sk02] и [AS03, §13.3, pp. 399-401]. Доказательства доступны старшеклассникам.

Заметим, что имеется простое теоретико-множественное доказательство *существования* трансцендентных чисел [CR, Гл. 2, §6]. Оно не дает явного примера трансцендентного числа, хотя дает алгоритм построения его десятичной записи.

Предварительная версия части этого пункта представлялась в 2002 г. А. Каибхановым на международной конференции Intel ISEF (США, Луисвилль), а также И. Никокошевым и А. Скопенковым на Летней Конференции Турнира Городов (Россия, Белорецк). Благодарим В. Волкова, А. Галочкина, Д. Лешко, А. Пахарева, А. Руховича и Л. Шабанова за полезные обсуждения.

Перед изучением этого пункта полезно прорешать п. 4.1.

8.2 Элементы анализа для многочленов (2)

Переменой знака в конечной последовательности $b_0, \ldots, b_k$ ненулевых чисел называется такой индекс $i \in \{1, \ldots, k\}$, что числа b_{i-1} и b_i имеют разные знаки. *Переменой знака* в конечной последовательности называется перемена знака в последовательности, полученной из данной вычёркиванием нулей.

8.2.1. (a) Число *положительных* решений уравнения $ax^2+bx+c = 0$ не превосходит числа перемен знака в последовательности a, b, c.

(b) Число положительных решений уравнения $ax^3+bx^2+cx+d = 0$ не превосходит числа перемен знака в последовательности a, b, c, d.

8.2.2. (a) **Правило знаков Декарта.** Число положительных решений уравнения $p_n x^n + \ldots + p_1 x + p_0 = 0$ не превосходит числа перемен знака в последовательности $p_0, \ldots, p_n$.

(b) Как аналогично правилу знаков Декарта оценить количество *отрицательных* корней данного многочлена?

(c)* Как аналогично правилу знаков Декарта оценить количество корней данного многочлена на данном промежутке $[a, b]$?

(d) **Неравенства Маклорена.** Для $x_1, \ldots, x_n > 0$ обозначим

$$M_k = \sqrt[k]{\frac{\sum\limits_{i_1<\ldots<i_k} x_{i_1} \cdot \ldots \cdot x_{i_k}}{\binom{n}{k}}}.$$

(Заметьте, что M_1 — это среднее арифметическое и M_n — среднее геометрическое.) Тогда $M_1 \geqslant \ldots \geqslant M_n$.

8.2.3. (a) При чётном n многочлен $\sum\limits_{k=0}^{n} \frac{x^k}{k!}$ не имеет вещественных корней, а при нечётном n имеет ровно один вещественный корень.

(b) Единственный вещественный корень при нечётном n (или минимальный модуль комплексного корня при любом n) многочлена $\sum\limits_{k=0}^{n} \frac{x^k}{k!}$ стремится к бесконечности при $n \to \infty$.

Для решения этих и многих других задач полезно следующее понятие. *Предпроизводной* f' многочлена f называется многочлен $D_f(x, y) := \frac{f(y)-f(x)}{y-x}$ от двух переменных x, y. (Сообразите, почему

8.5 Применения компактности (4*). *А. Я. Канель-Белов*

В этом пункте задачи посложнее и подсказок поменьше. Однако он будет интересен читателю, так как, насколько нам известно, такая подборка интересных задач по этой важной теме впервые публикуется в неспециальной литературе.

8.5.1. Близкая идея в конечном случае. Запись числа состоит из нулей и единиц. Любой фрагмент «10» числа заменяют на «0001». Докажите, что рано или поздно заменять будет нечего.

8.5.2. Идея компактности. (a) Известно, что человечество живёт вечно, а число людей в каждом поколении конечно. Докажите, что найдётся бесконечная цепочка наследников.

(b) В бесконечном парламенте у каждого парламентария не более трёх врагов. Докажите, что парламент можно разбить на две палаты так, что у каждого парламентария будет не более одного врага в своей палате. (Для конечного парламента эта задача разбирается в [SZ, задача 7 в п. «Полуинварианты»].)

(c) Известно, что любую *конечную* карту на плоскости можно правильно раскрасить в 4 цвета. Докажите, что тогда *произвольную* карту на плоскости также можно правильно раскрасить в 4 цвета. (Страны можно считать многоугольниками. Раскраска называется *правильной*, если любые две страны с общим участком границы раскрашены в разные цвета.)

(d) (Загадка.) Прочитайте [SZ, п. «Полуинварианты»]. Какие утверждения верны для бесконечных множеств, а какие нет?

8.5.3. Для любых M и k найдётся достаточно большое v с таким свойством: если все рёбра полного графа с v вершинами покрашены в M цветов, то найдётся полный подграф с k вершинами, все рёбра которого покрашены в один цвет.

8.5.4. Из любой бесконечной последовательности целых чисел можно выбрать подпоследовательность либо так, чтобы каждый её член делился на предыдущий, либо так, чтобы ни один член не делился на другой.

9 К алгоритмам решения алгебраических уравнений

Listeners are prepared to accept unstated (but hinted) generalizations much more than they are able ... to decode a precisely stated abstraction and to re-invent the special cases that motivated it in the first place.
P. Halmos, How to talk mathematics.

9.1 Введение и формулировки результатов

9.1.1 О чём этот параграф

Знаменитые теоремы Гаусса 9.1.5, Руффини 9.2.5, Абеля, Галуа 9.1.13, 9.1.14 и Кронекера о построимости правильных многоугольников и о неразрешимости алгебраических уравнений в радикалах — классический результат алгебры, интересный для информатики (теории символьных вычислений).

Определения построимости и разрешимости в радикалах, а также формулировки указанных теорем, приведены в п. 9.1.2–9.1.4. Я не привожу историю этих теорем, направляя заинтересованного читателя к текстам [Gi, Gi1, Ma].

Основное содержание данного текста— изложение глубоких идей алгебры (точнее, теории Галуа) на красивых простых доказательствах этих теорем, см. п. 9.1.5 и [ZSS, § 27]. Этот текст адресован всем любителям такого изложения: старшеклассникам, студентам, учителям и профессиональным математикам. Приводимые доказательства (п. 9.2.5 и 9.4) интересны тем, что для их понимания достаточно уметь доказывать иррациональность (п. 4.1), делить многочлены с остатком (п. 4.3 и задачи 4.4.3, 4.4.4), извлекать корни из комплексных чисел (задача 4.5.4), умножать перестановки (п. 5.1) и решать системы линейных уравнений. (Для каждого одного доказательства необходима только часть этих умений.) Напомним, что несмотря на простоту этих доказательств, они иллюстрируют глубокие идеи алгебры. Разбор доказательств (или их начала) полезен для закрепления тем «иррациональность», «многочлены», «комплексные числа», «перестановки» и «основы линейной алгебры».

И тот, кто не дойдёт до полного доказательства основных результатов, получит хороший опыт по этим темам и даже сможет порешать задачи для исследования, см. п. 9.1.5 и [E2, Es, AB, Ko17, Saf] и ссылки в этих работах.

Перед доказательствами неразрешимости алгебраических уравнений мы разберем общий способ их решения — метод резольвент Лагранжа (п. 9.2). Идея Абеля и Галуа фактически заключается в том, что если уравнение разрешимо в радикалах, то его можно решить этим методом. Эта идея формализуется критерием 9.2.12.а Галуа разрешимости уравнения. Этим же методом строятся и алгоритмы — распознаваемости разрешимости уравнений в радикалах и решения в радикалах разрешимого уравнения.

Для практики приближённые методы вычисления тригонометрических функций и решения уравнений полезнее радикальных формул. Кроме того, уравнения можно решать при помощи трансцедентных функций (см. метод Виета в п. 4.2 и [PSo]; о развитии этих идей рассказывается, например, в [Sk10]). Однако проблема разрешимости в радикалах интересна как пробная задача современных теорий символьных вычислений и сложности вычислений.

О новизне. Приводимые доказательства не претендуют на новизну, хотя в этом тексте имеется много методических находок, см. п. 9.1.5 и 9.1.6. Однако, к сожалению, они малоизвестны. Как следствие, малоизвестно, что не только решать квадратные и кубические уравнения, но и доказывать указанные теоремы экономнее не строя и затем применяя теорию Галуа (как, например, в стандартных учебниках по алгебре, [Kh13, Kir]), а напрямую (см. ссылки в п. 9.1.6)— но при этом, конечно, открывая и используя базовые идеи этой теории.

План параграфа. Этот параграф не обязательно изучать подряд. Например, начать его изучение можно не с п. 9.1, а с решения задач в п. 9.2, 9.3, поскольку большинство из них использует предыдущий материал только в качестве мотивировки. Читатель может выбрать удобную ему последовательность изучения (или вовсе опустить некоторые пункты) на основании приводимого плана.

В п. 9.1.2–9.1.4 приведены формулировки основных результатов. Следующие три пункта введения независимы от остального текста

(т. е. они не используются в остальном тексте и для его изучения достаточно прочитать п. 9.1.2–9.1.4). В п. 9.1.7 приводится переформулировка теоремы Гаусса (упомянутая в п. 9.1.2).

План п. 9.2–9.4 приводится в их начале. Доказательства основных результатов приводятся в п. 9.2.3, 9.2.5 и 9.4. Формально они независимы от задач, подводящих к ним (п. 9.2–9.3).

Благодарности. Благодарю А. Я. Белова-Канеля, И. И. Богданова, Э. Б. Винберга, В. В. Волкова, М. Н. Вялого, А. С. Голованова, П. А. Дергача, Д. Зунга, А. Л. Канунникова, В. А. Клепцына, П.А. Козлова, Г. А. Мерзона, А. А. Пахарева, В. В. Прасолова, А. Д. Руховича, Л. М. Самойлова, М. Б. Скопенкова, Г. Р. Челнокова, Л. Э. Шабанова и В. В. Шувалова за полезные обсуждения. Этот текст основан на занятиях в Московской выездной школе по математике, на Летней Конференции Турнира Городов [ABG, ECG], в кружках «Математический семинар» и «Олимпиады и математика».

9.1.2 Построимость (1)

Замечание 9.1.1. Известно, что

$$\cos\frac{2\pi}{3}=-\frac{1}{2},\quad \cos\frac{2\pi}{4}=0,\quad \cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4},\quad \cos\frac{2\pi}{6}=\frac{1}{2},$$
$$\cos\frac{2\pi}{8}=\frac{1}{\sqrt{2}},\quad \cos\frac{2\pi}{10}=\frac{\sqrt{5}+1}{4},\quad \cos\frac{2\pi}{12}=\frac{\sqrt{3}}{2}.$$

А для каких еще n число $\cos\frac{2\pi}{n}$ выражается аналогичной формулой? Т.е. для каких n его можно получить на калькуляторе, выполняющем только четыре арифметических действия и извлечения квадратных корней?

Вещественное число называется **вещественно построимым**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений квадратных корней из положительных чисел. Т.е. если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя операции добавления к уже имеющемуся множеству M, содержащему числа x, y,

чисел $x+y, x-y, xy$, числа x/y при $y\neq 0$ и числа $\sqrt{x}$ при $x>0$.

Или если это число можно получить на калькуляторе из замечания 9.1.1.

Например, вещественно построимы числа

$$\sqrt[4]{2}=\sqrt{\sqrt{2}},\quad \sqrt{2\sqrt{3}},\quad \sqrt{2}+\sqrt{3},\quad \sqrt{1+\sqrt{2}},\quad 1+\sqrt{3-2\sqrt{2}},\quad \frac{1}{1+\sqrt{2}},$$

числа из замечания 9.1.1 и утверждения 9.1.3.

Вещественная построимость числа равносильна его *построимости циркулем и линейкой*. Поэтому приводимые ниже результаты решают знаменитые проблемы древности о построимости циркулем и линейкой. Мы обсудим эту равносильность в п. 9.1.7; впрочем, она не используется в остальном тексте. Изучение вещественной постоимости важно также как пробная задача современных теорий символьных вычислений и сложности вычислений [Ko17].

Теорема 9.1.2. Число $\sqrt[3]{2}$ не является вещественно построимым.

См. доказательство в п. 9.4.4.

Вопрос об обобщении формул из замечания 9.1.1 формализуется так: для каких n число $\cos(2\pi/n)$ вещественно построимо?

9.1.3. Число $\cos(2\pi/n)$ вещественно построимо для $n = 15$, 16, 20, 24, 60.

Лемма 9.1.4 (об умножении; вещественная версия)**.** (a) Если число $\cos(2\pi/n)$ вещественно построимо, то число $\cos(\pi/n)$ вещественно построимо.

(b) Если числа $\cos(2\pi/n)$ и $\cos(2\pi/m)$ вещественно построимы и m, n взаимно просты, то число $\cos(2\pi/mn)$ вещественно построимо.

Теорема 9.1.5 (Гаусс)**.** Число $\cos(2\pi/n)$ вещественно построимо тогда и только тогда, когда $n = 2^\alpha p_1 \cdot \ldots \cdot p_l$, где $p_1, \ldots, p_l$ — различные простые числа вида $2^{2^s} + 1$.

Построимость в теореме Гаусса доказана в п. 9.2.3 и 9.2.5 (или п. 9.2.6), а непостроимость — в п. 9.4.4.

Строго говоря, теорема Гаусса не даёт настоящего решения проблемы вещественной построимости числа $\cos(2\pi/n)$, поскольку неизвестно, какие числа вида $2^{2^s} + 1$ являются простыми. Однако теорема Гаусса даёт, например, быстрый алгоритм распознавания построимости.

Из теоремы Гаусса вытекает вещественная непостроимость числа $\cos(2\pi/9)$ (впрочем, ее проще доказать напрямую, см. задачу 9.3.12.a). Отсюда вытекает следующий результат, показывающий *невозможность трисекции угла циркулем и линейкой.*

Теорема 9.1.6. Существует такое α (например, $\alpha = 2\pi/3$), что число $\cos\alpha$ вещественно построимо, а число $\cos(\alpha/3)$ — нет.

9.1.3 Неразрешимость в вещественных радикалах (2)

Вещественное число называется **вещественно радикальным**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений корней целых положительных степеней из положительных чисел. Т.е. если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя операции добавления к уже имеющемуся множеству $M \subset \mathbb{R}$, содержащему числа x, y,

$$\text{чисел} \quad x+y, x-y, xy, \quad \text{числа } x/y \text{ при } y \neq 0$$

$$\text{и числа } \sqrt[n]{x} \text{ при } x > 0 \text{ и целом } n > 0.$$

Это определение можно сформулировать и на языке калькулятора аналогично замечанию 9.1.1. Стандартный термин: число лежит в некотором вещественном радикальном расширении поля $\mathbb{Q}$. Вещественная радикальность числа α равносильна существованию таких

- целых положительных чисел $s, k_1, \ldots, k_s$,
- вещественных чисел $f_1, \ldots, f_s$ и многочленов $p_0, p_1, \ldots, p_s$ от $0, 1, \ldots, s$ переменных, соответственно, с рациональными коэффициентами, что

$$\begin{cases} f_1^{k_1} = p_0 \\ f_2^{k_2} = p_1(f_1) \\ \ldots \\ f_s^{k_s} = p_{s-1}(f_1, \ldots, f_{s-1}) \\ \alpha = p_s(f_1, \ldots, f_s) \end{cases}.$$

Замечание 9.1.7. (a) Любой вещественный корень квадратного уравнения с рациональными коэффициентами вещественно радикален.

(b) Уравнение $x^3 + x + 1 = 0$ имеет ровно один вещественный корень, который вещественно радикален (п. 4.2), см. также задачу 9.2.6 (c).

(c) Уравнение $x^4 + 4x - 1 = 0$ имеет два вещественных корня, каждый из которых вещественно радикален (задача 4.2.6.b) , см. также задачу 9.2.9 (d).

(d) Любое вещественно построимое число (п. 9.1.2) вещественно радикально.

Теорема 9.1.8. (a) Число $\cos(2\pi/9)$ не является вещественно радикальным.

(b) Существует многочлен 3-й степени с рациональными коэффициентами (например, x^3-3x+1), ни один из корней которого не является вещественно радикальным.

Deduction of (a) from (b). По формуле 4.1.5 (e) косинуса тройного угла каждое из чисел $\cos(2\pi/9)$, $\cos(8\pi/9)$, $\cos(14\pi/9)$ удовлетворяет уравнению $8y^3-6y+1=0$. Замена $x=2y$ превращает его в уравнение $x^3-3x+1=0$. Тогда по п. (b) ни одно из этих чисел не является вещественно радикальным. □

Замечание 9.1.9. (a) *Для любого $n\geqslant 3$ существует многочлен n-й степени, один из корней которого не является вещественно радикальным.* (Это следует из теоремы 9.1.10.b.)

(b) Справедлив аналог утверждения (a) с заменой слов «один из корней» на «ни один из корней». (Он доказывается более сложно, см. теорему 9.1.11 ниже.) При этом корни *некоторых* уравнений высоких степеней (например, $x^5=2$) вполне могут быть вещественно радикальны, см. также п. 9.2.5.

(c) Трисекция угла невозможна при помощи вещественных радикалов, т.е. существует такое α (например, $\alpha=2\pi/3$), что число $\cos\alpha$ вещественно радикально, а число $\cos(\alpha/3)$ — нет. (Это следует из теоремы 9.1.10.a.)

Теорема 9.1.10 (о разрешимости в вещественных радикалах)**.** Следующие условия на многочлен f третьей степени с рациональными коэффициентами равносильны:

(i) многочлен f имеет либо хотя бы один рациональный корень, либо ровно один вещественный корень;

(ii) многочлен f имеет вещественно радикальный корень;

(iii) все вещественные корни многочлена f вещественно радикальны.

Единственность вещественного корня «укороченного» уравнения $x^3+px+q=0$ равносильна условию «$p=q=0$ или $(p/3)^3+(q/2)^2>0$», см. задачу 8.1.4 (d).

Равносильность $(ii)\Leftrightarrow(iii)$ очевидна, ср. с замечанием 9.1.7.a. Разрешимость в теореме 9.1.10 (т.е. $(i)\Rightarrow(ii)$) доказывается *методом дель Ферро* , см. теоремы, приведённые в указаниях к задачам 4.2.4 и 8.1.4 (d) ; см. другое доказательство в п. 9.2.2. Неразрешимость в теореме 9.1.10 (т.е. $(ii)\Rightarrow(i)$) доказывается сложнее, см п. 9.4.5. Более просто доказывается аналогичный результат о *неразрешимости в многочленах*, см. п. 9.3.5 и п. 9.4.2.

Многочлен с коэффициентами в F называется *неприводимым* над множеством F, если он не раскладывается в произведение многочленов меньшей степени с коэффициентами в F.

Теорема 9.1.11. Если многочлен простой нечётной степени с рациональными коэффициентами неприводим над $\mathbb{Q}$ и имеет более одного вещественного корня, то ни один из его корней не является вещественно радикальным.

Это вещественный аналог теоремы Кронекера 9.1.15. Доказательство приведено в п. 9.4.8.

Гипотеза 9.1.12.* (a) Каждый вещественный корень неприводимого над $\mathbb{Q}$ многочлена четвёртой степени с рациональными коэффициентами вещественно радикален тогда и только тогда, когда хотя бы один корень его кубической резольвенты (определенной после задачи 4.2.6.b) вещественно радикален. (Ср. с задачей 9.3.13.d.)

(b) Если число $\cos(2\pi/n)$ вещественно радикально, то оно вещественно построимо. (Ср. с теоремой Гаусса 9.1.5 о построимости правильных многоугольников.)

Возможно, справедливость этих гипотез известна специалистам. Гипотезу 9.1.12.b (и ответ к задаче 9.3.2 с набросками доказательств) мне сообщил А. А. Канунников. Читатель может пробовать доказать эти гипотезы после изучения §9.3 и §9.4.

9.1.4 Неразрешимость в комплексных радикалах (2)

Перейдём к формулам, которые могут содержать комплексные числа. Оказывается, кубическое уравнение (например, x^3-3x+1),

неразрешимое в вещественных радикалах, разрешимо в комплексных.

Комплексное число называется (комплексно) **радикальным**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений корней целых положительных степеней. Т.е. если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя операции добавления к уже имеющемуся множеству M, содержащему числа x, y,

$$\text{чисел } x+y, x-y, xy, \quad \text{числа } x/y \text{ при } y \neq 0$$

и любого такого числа $r \in \mathbb{C}$, что $r^n = x$ для некоторого целого $n > 0$.

Это определение можно сформулировать и на языке калькулятора аналогично замечанию 9.1.1. (Правда, калькулятор будет необычный: он оперирует с комплексными числами и при нажатии кнопки $\sqrt[n]{\ }$ выдаёт все значения корня.) Стандартный термин: число лежит в некотором радикальном расширении поля $\mathbb{Q}$.

Например, любой (комплексный) корень квадратного уравнения с рациональными коэффициентами является радикальным. Аналогичные утверждения справедливы для уравнений 3-й и 4-й степени. Они доказываются *методами дель Ферро и Феррари*, см. теоремы, приведённые в указаниях к задачам 4.2.4 и 4.2.7; см. другое доказательство в п. 9.2.2.[3] Однако аналог этих утверждений для более высоких степеней неверен.

Теорема 9.1.13 (Галуа)**.** Существует уравнение 5-й степени с рациональными коэффициентами (например, $x^5 - 4x + 2 = 0$), ни один из корней которого не является радикальным.

Знаменитую проблему о разрешимости уравнений в радикалах решили доказанные немного ранее более слабые теоремы Руффини–Абеля. Теорема Руффини 9.2.5 сложнее формулируется, но подводит нас к доказательству теоремы Галуа. Четкая формулировка теоремы Абеля еще более сложна и здесь не приводится, см. [Sk15, Замечание 7]. Экономнее решить проблему разрешимости, доказав

[3] Об оценках на количество необходимых корней см. п. 9.3.9 и [ABG].

(в п. 9.4.6) следующую теорему Галуа (более слабую и более просто доказываемую, чем теорема Галуа 9.1.13). Для $X \subset \mathbb{C}$ комплексное число называется *X-радикальным*, если его можно получить из множества $X \cup \{1\}$ при помощи операций из определения радикальности.

Теорема 9.1.14. Существуют такие $a_0, a_1, a_2, a_3, a_4 \in \mathbb{C}$, что ни один корень уравнения $x^5 + a_4x^4 + \ldots + a_1x + a_0 = 0$ не является $\{1, a_0, a_1, a_2, a_3, a_4\}$-радикальным.

Analogous result (with analogous proof) holds for equations of any degree $n \geqslant 5$.

А более сильная теорема Галуа 9.1.13 вытекает из следующего результата.

Теорема 9.1.15 (Кронекер)**.** Если многочлен простой степени с рациональными коэффициентами неприводим над $\mathbb{Q}$, имеет более одного вещественного корня и хотя бы один невещественный, то ни один из его корней не является радикальным.

Эта теорема интересна и нетривиальна даже для многочлена пятой степени. Она доказана в п. 9.4.7. Для её доказательства необходимо следующее обобщение теоремы Гаусса 9.1.5. Обозначим

$$\varepsilon_q := \cos(2\pi/q) + i\sin(2\pi/q).$$

Теорема 9.1.16 (Гаусса о понижении)**.** (a) Если q простое, то можно получить ε_q при помощи операций из определения радикальности так, чтобы корни извлекались только $(q-1)$-й степени.

(b) Для любого q можно получить ε_q при помощи операций из определения радикальности так , чтобы корни извлекались только степеней, строго меньших q.

Часть (a) доказывается аналогично доказательству построимости в теореме Гаусса (п. 9.2.5, 9.2.6). Часть (b) выводится из (a) при помощи индукции по q. (Если $q = ab$ для некоторых целых a, b, $0 < a, b < q$, то шаг индукции следует из равенства $\varepsilon_q = \sqrt[a]{\varepsilon_b}$. Если же q простое, то шаг индукции следует из части (a).)

Справедлив комплексный аналог замечания 9.1.9 для $n \geqslant 5$ и теоремы Кронекера 9.1.15 вместо теоремы 9.1.11. При этом доказательство теоремы 9.1.14 легко переносится на уравнения любой степени $n \geqslant 5$.

Теорема 9.1.17. There is an algorithm deciding, for $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$, whether all the roots of the equation $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ are expressible by radicals.

Theorem 9.1.17 can be proved using Galois Solvability Criterion 9.2.12.a and an estimation 9.3.42.b of the number of operations.

9.1.5 Чем интересны приводимые доказательства

Приводимые доказательства намного проще и короче тех, которые излагаются в стандартных учебниках по алгебре. (Здесь я имею в виду доказательства «с нуля», а не вывод нужной теоремы из построенной перед этим теории, в которой фактически заключается всё доказательство.) Сравнение с доказательствами из менее стандартной более популярной литературы приведено в п. 9.1.6.

Эта простота достигается благодаря тому, что, в отличие от большинства учебников, приводимые доказательства не используют термина «группа Галуа» (даже термина «группа»). Несмотря на отсутствие этих *терминов*, *идеи* приводимых доказательств являются *отправными* для теории Галуа и *конструктивной теории Галуа* [E2]. Более подробно это обсуждается в [ZSS, §27 и §28].

Доказательство разрешимости основано на методе *резольвент Лагранжа*. Доказательства неразрешимости основаны на идеях *симметрии* и *сопряжения*. (Вторая идея более учёно называется идеей *автоморфизма поля*; замечательное изложение см. в [Vag].)

Основные идеи представлены на «олимпиадных» примерах: на простейших частных случаях, свободных от технических деталей, и со сведением научного языка к необходимому минимуму. Хотя основные результаты касаются уравнений высших степеней, идеи демонстрируются на квадратных и кубических уравнениях. Неразрешимость доказывается сначала при условии, что *корень извлекался только один раз* (в задачах в п. 9.3.1, 9.3.3, 9.3.4). Благодаря

этому основные идеи преподносятся на примере рациональных чисел (а не произвольных полей и даже не полей из башни расширений). Эти основные идеи (сопряжения, поля и другие) заключены в леммах о калькуляторе, о линейной независимости и о сопряжении (§9.3 и 9.4). При доказательстве неразрешимости в теореме Гаусса 9.1.5 используется степень *многочлена* (вместо степени *расширения поля*) Перед доказательствами неразрешимости (в теоремах 9.1.13, 9.1.14, 9.1.15 Галуа и Кронекера) доказывается неразрешимость *в многочленах* (теоремы Руффини 9.2.5, 9.4.3), а также неразрешимость в *вещественных* радикалах уравнений третьей степени (теорема 9.1.10). Важные идеи доказательств явно выделены в виде четко сформулированных на простом языке лемм (о сохранении четносимметричности 9.3.35, 9.4.4, о степенях двойки 9.4.6, о рационализации 9.4.11). Все это делает доказательства неразрешимости более доступными (за счёт введения интересных чётко выделенных промежуточных «ступенек»). Кроме того, это подводит читателя к предположению о том, что приведённые доказательства можно развить до теории (Галуа), полезной для доказательства других интересных результатов (подробнее см. [ZSS, п. 28.2]).

Мы показываем, *как можно придумать* приводимые доказательства. Пути к ним намечены в виде задач в п. 9.2.4 и 9.3. О традиции изучения материала в виде решения и обсуждения задач см. п. 1.2 и [ZSS, §26]. Хотя *придумать* доказательства непросто, *изложить* их можно коротко (см. п. 9.2.5 и 9.4). Освобождение доказательства от деталей, возникших при его придумывании, но не нужных для него самого, — важная часть его проверки.

Многие из приведённых задач — хорошие темы исследовательских работ старшеклассников и младшекурсников, связанные с алгеброй, комбинаторикой и информатикой, см. п. 1.3. Вот работы, уже подготовленные с использованием предыдущих версий этого текста: [Saf, AB, Ko17]. А вот примеры задач для исследования: 9.1.12, 9.2.11, 9.2.12, 9.3.2, 9.1.10, 9.1.11, 9.2.11, 9.2.16, 9.3.4, 9.3.8 (h), 9.3.16 (e), 9.3.18 (b), 9.3.20 (d), 9.3.24, 9.3.38, 9.3.40, 9.3.41, 9.2.2, 9.2.4, 9.2.5, 9.3.32, 9.3.37.

9.1.6 Исторические комментарии

Доказательство построимости в теореме Гаусса получено из [E1, § 24] некоторым упрощением (мы обходим использование леммы 2, см. подробнее абзац перед задачей 9.2.18). Оно также более простое по сравнению с доказательством из [KS]. Элементарное доказательство построимости для $n = 17$ приводится, например, в [BK, Ch, Gi, Pr07-2, Pos, PSo, Kol], [Dor, § 37] (при этом иногда приводятся явные формулы, как с доказательствами утверждений о знаках перед радикалами [Dor, § 37], [Saf], так и без [BK]). Для общего случая оно намечено в [Ga, Gi] (где ясности доказательства немного мешает построение общей теории вместо доказательства конкретного результата). Подход из [Ki] даёт ответ на вопрос «почему», и было бы интересно довести его до полного доказательства.

Доказательство непостроимости в теореме Гаусса основано на [Dor, Supplement to § 35–37]. Оно более простое по сравнению с доказательствами из [KS].

Мне неизвестно, опубликовано ли короткое прямое доказательство теорем 9.1.10, 9.1.11 о неразрешимости в вещественных радикалах. Доказательство теоремы Руффини 9.2.5, 9.4.3 следует приведенному в замечательной книге [Kol] (я не смог разобрать приведенного там доказательства, пока не переоткрыл его, явно выделив лемму о сохранении четносимметричности 9.3.35, 9.4.4). Доказательство теоремы 9.1.14 следует приведенному в замечательной книге [PSo] (я смог убедиться в правильности предложенных там идей только переписав доказательство, явно выделив лемму о рационализации 9.4.11). Другое доказательство теоремы Абеля приведено в [Al], [FT, Lecture 5], [Sk11][4]. Доказательство теоремы Кронекера 9.1.15 основано на замечательных статье [T] и книгах [Dor, § 25], [Pr07-2, дополнение 8] (здесь исправлены неточности, см. сноски 11 и 13).

Другие элементарные изложения приводятся, например, в [Ber, Br, Had, Vi, Ka, Ler, Pe, Ro, St94]. Note that proofs in some of these

[4] Доказательство из [Al] более коротко и понятно изложено в [FT, Lecture 5] и, возможно, в [Sk11]. Большая часть [Al] посвящена изложению теории, не нужной для доказательства теоремы Абеля. Однако автору книги [Al] удалось избежать немотивированного изложения части этой теории.

sources are incomplete, see [Sk15, Discussion].

Вышеупомянутые элементарные изложения были для меня полезнее (несмотря на указанные недостатки), чем формальные изложения (в стандартных учебниках, излагающих теории), которые начинаются с нескольких сотен страниц определений и следствий, роль которых в доказательстве теоремы о неразрешимости неясна на момент их формулировки.

9.1.7 Связь с построениями циркулем и линейкой (1)

9.1.18. (a) Используя отрезки длины x и y, можно построить с помощью циркуля и линейки отрезок длины $\sqrt{3xy + y\sqrt[4]{xy^3}}$.

(b) Используя отрезки длины a, b и c, можно построить с помощью циркуля и линейки отрезки длины $a+b$, $a-b$, ab/c, $\sqrt{ab}$.

Ввиду утверждения 9.1.18.b если на плоскости задан отрезок длины 1, то отрезок вещественно построимой длины можно построить циркулем и линейкой. Этот простой результат был известен ещё древним грекам. Оказывается, верно и обратное.

Теорема 9.1.19 (Основная теорема о построениях циркулем и линейкой)**.** Если отрезок длины a можно построить циркулем и линейкой, имея отрезок длины 1, то число a вещественно построимо.

Этот несложный результат (доказанный лишь в XIX веке) показывает, что из непостроимости числа $\cos(2\pi/n)$ вытекает непостроимость правильного n-угольника циркулем и линейкой. Для доказательства этого результата можно рассмотреть все возможные случаи появления новых объектов (точек, прямых, окружностей) и показать, что координаты всех построенных точек и коэффициенты уравнений всех проведённых прямых и окружностей являются построимыми. Детали читатель сможет восполнить самостоятельно или найти в [Kol, CR, Ma, Pr07-2]. О построениях с другим набором инструментов см. [SZ].

Подсказки

9.1.18. (a) Достаточно, применяя (b), последовательно построить отрезки с длинами $z_1 = \sqrt{xy}$, $z_2 = \sqrt{yz_1}$, $z_3 = 3x + z_2$, $z = \sqrt{yz_3}$.

9.2 Решаем уравнения: метод резольвент Лагранжа

Метод резольвент Лагранжа на простейших примерах иллюстрируется в п. 9.2.2. Его применение к доказательству построимости в теореме Гаусса иллюстрируется на примерах и задачах в п. 9.2.4. Построимость в теореме Гаусса доказана в п. 9.2.3 и п. 9.2.5. При этом в п. 9.2.3 приводится более простая часть доказательства, не использующая резольвент Лагранжа; этот пункт не зависит от предыдущих. Материал п. 9.2.6 не используется далее.

Определения вещественной построимости и радикальности чисел см. в п. 9.1.2, 9.1.4. In this section equality signs involving polynomial f (or f_j) mean equality of polynomials (покоэффициентное). Напомним, что

$$\varepsilon_q := \cos(2\pi/q) + i\sin(2\pi/q).$$

9.2.1 Определение радикальности многочлена (2)

Решение квадратного уравнения $t^2+bt+c=0$ можно выразить формулами

$$(x-y)^2=(x+y)^2-4xy=b^2-4c \text{ и } x=\frac{x+y+(x-y)}{2}=\frac{-b+(x-y)}{2}.$$

Всегда ли можно, зная $x+y$ и xy, однозначно найти x? Вот простейшая формализация этого вопроса: *существует ли функция* $q\colon \mathbb{R}^2\to\mathbb{R}$, *для которой* $q(x+y,xy)=x$ *при любых* $x,y\in\mathbb{R}$? (Т.е. разрешимо ли функциональное уравнение $q(x+y,xy)=x$?) Ответ: не существует (действительно, рассмотрите пары $x=1,y=0$ и $x=0,y=1$).

Аналогично, зная

$$\sigma_1:=x+y+z,\quad \sigma_2:=xy+yz+zx \quad\text{и}\quad \sigma_3:=xyz,$$

невозможно однозначно найти $(x-y)(y-z)(z-x)$ (действительно, рассмотрите тройки $x=0,y=1,z=-1$ и $x=1,y=0,z=-1$).

9.2.1. Для каких k следующая система уравнений разрешима в многочленах с вещественными коэффициентами

$$\begin{cases} f^k(x,y)=p(x+y,xy) \\ x=q\left(x+y,xy,f(x,y)\right) \end{cases} ?$$

9.2.2. Для каких k разрешима следующая система уравнений разрешима в многочленах с вещественными коэффициентами

$$\begin{cases} f^k(x,y,z)=p\big(\sigma_1,\sigma_2,\sigma_3\big) \\ x=q\big(\sigma_1,\sigma_2,\sigma_3,f(x,y,z)\big) \end{cases} ?$$

Обобщение этой задачи на любое количество шагов формализуется следующим определением радикальности.

Обозначим элементарные симметрические многочлены

$$\sigma_1(x_1,\dots,x_n):=x_1+\dots+x_n,\quad \dots,\quad \sigma_n(x_1,\dots,x_n)=x_1\cdot\ldots\cdot x_n.$$

Если число n и аргументы $x_1,\dots,x_n$ ясны из контекста, то они пропускаются из обозначений.

Многочлен $p \in \mathbb{R}[x_1, \ldots, x_n]$ называется **вещественно радикальным** (или выразимым в вещественных радикалах), если p можно добавить в набор $\{\sigma_1, \ldots, \sigma_n\} \cup \mathbb{R}$ многочленов цепочкой операций следующего вида:

• добавить в набор сумму или произведение уже имеющихся многочленов;

• если многочлен из набора равен f^k для некоторых $f \in \mathbb{R}[x_1, \ldots, x_n]$ и целого $k > 1$, то добавить в набор многочлен f.

Замечание 9.2.3. (a) Например, к многочленам $x^2 + 2y$ и $x - y^3$ операциями первого типа можно добавить многочлен $-5(x^2+2y)^2 + 3(x^2+2y)(x-y^3)^6$. А к многочлену $x^2 - 2xy + y^2$ операцией второго типа можно добавить многочлен $x - y$ (или $y - x$).

(b) Операции первого типа добавляют многочлен с вещественными коэффициентами от уже имеющихся.

(c) Радикальность многочлена x_1 равносильна существованию таких

• целых положительных чисел $s, k_1, \ldots, k_s$,

• многочленов $f_1, \ldots, f_s$ от n переменных и $p_0, p_1, \ldots, p_s$ от $n, n+1, \ldots, n+s$ переменных, соответственно, с вещественными коэффициентами, что

$$\begin{cases} f_1^{k_1} = p_0(\sigma_1, \ldots, \sigma_n) \\ f_2^{k_2} = p_1(\sigma_1, \ldots, \sigma_n, f_1) \\ \ldots \\ f_s^{k_s} = p_{s-1}(\sigma_1, \ldots, \sigma_n, f_1, \ldots, f_{s-1}) \\ x_1 = p_s(\sigma_1, \ldots, \sigma_n, f_1, \ldots, f_s) \end{cases}.$$

В этих равенствах мы опускаем переменные $(x_1, \ldots, x_n)$ многочленов $\sigma_1, \ldots, \sigma_n, f_1, \ldots, f_s$.

(d) По теореме Виета $\sigma_1, \ldots, \sigma_n$ есть коэффициенты многочлена

$$t^n - \sigma_1 t^{n-1} + \ldots + (-1)^{n-1}\sigma_{n-1}t + (-1)^n\sigma_n \in \mathbb{C}[x_1, \ldots, x_n][t]$$

с корнями $x_1, \ldots, x_n$. Поэтому радикальность многочлена x_1 означает выразимость в радикалах (в указанном в определении радикальности смысле) корня многочлена через его коэффициенты.

Решение задачи 9.2.1 для $k = 2$ показывает, что многочлен x вещественно радикален для $n = 2$.

Теорема 9.2.4. Многочлен x не является вещественно радикальным для $n = 3$.

Теорема 9.2.4 есть еще одна формализация того, что *корень кубического уравнения не выразим в вещественных радикалах через его коэффициенты*, ср. с замечанием 9.1.7.e.

Определение (комплексной) **радикальности** получается из его вещественного аналога заменой вещественных коэффициентов на комплексные. Решения задач 9.2.1.(2), 9.2.6.c и 9.2.9.d показывают, что многочлен x_1 радикален для $n \leqslant 4$.

Теорема 9.2.5 (Руффини)**.** Ни для какого целого $n \geqslant 5$ многочлен x_1 не радикален.

Из доказательства будет вытекать, что даже многочлен $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$ не радикален для $n = 5$.

Указания, ответы и решения

9.2.1. (2) Системе уравнений удовлетворяют, например, многочлены

$$f(x, y) = x - y, \quad p(u, v) = u^2 - 4v \quad \text{и} \quad q(u, v, w) = \frac{u + w}{2}.$$

(3) Подставьте $(x, y) = (0, 1)$ и $(x, y) = (1, 0)$.

9.2.4. При $n = 3$ множество вещественно радикальных многочленов содержится в множестве циклически симметрических многочленов. Это утверждение доказывается при помощи индукции по количеству операций из определения радикальности. Шаг индукции вытекает из леммы 9.3.30 о сохранении циклической симметричности.

Поскольку многочлен x не является циклически симметрическим, то он не является вещественно радикальным.

9.2.2 Решение уравнений малых степеней (2)

В задачах этого пункта далее используйте представимость любого симметрического многочлена в виде многочлена от элементарных симметрических многочленов (основная теорема о симметрических многочленах 4.6.3).

9.2.6. Следующие многочлены радикальны для $n = 3$:
(a) $(x-y)(y-z)(z-x)$; (b) $x^9y + y^9z + z^9x$; (c) x.

Подсказкой к (c) являются следующие задачи 9.2.7.a и 9.2.8.c.

9.2.7. Многочлен $f \in \mathbb{R}[u_1, u_2, \ldots, u_n]$ называется **циклически симметрическим**, если $f(u_1, u_2, \ldots, u_n) = f(u_2, u_3, \ldots, u_{n-1}, u_n, u_1)$.

(a) Найдите хотя бы одну пару $\alpha, \beta \in \mathbb{C}$, для которой многочлен $(u+v\alpha+w\beta)^3$ циклически симметрический, а многочлен $u+v\alpha+w\beta$ — нет.

(b) Получите многочлен $x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1$ операциями из определения радикальности из некоторых *циклически* симметрических многочленов от $x_1, x_2, \ldots, x_{10}$.

9.2.8. Решите системы уравнений (x, y, z, t — неизвестные, a, b, c, d известны):

$$\text{(a)}\quad \begin{cases} x+y+z+t=a,\\ x+y-z-t=b,\\ x-y+z-t=c,\\ x-y-z+t=d; \end{cases} \qquad \text{(b)}\quad \begin{cases} x+y+z+t=a,\\ x+iy-z-it=b,\\ x-y+z-t=c,\\ x-iy-z+it=d; \end{cases}$$

$$\text{(c)}\quad \begin{cases} x+y+z=a,\\ x+\varepsilon_3 y+\varepsilon_3^2 z=b,\\ x+\varepsilon_3^2 y+\varepsilon_3 z=c. \end{cases}$$

9.2.9. Следующие многочлены радикальны для $n = 4$:
(a) $(x-y)(x-z)(x-t)(y-z)(y-t)(z-t)$;
(b) $xy + zt$; (c) $x + y - z - t$; (d) x.

Выражения из задачи 9.2.8 называются *резольвентами Лагранжа*. Они «лучше» корней, поскольку «симметричнее» в следующем смысле.

Решение кубического уравнения при помощи резольвент Лагранжа (решение задачи 9.2.6.c). Для нахождения корней x, y, z кубического уравнения достаточно найти выражения a, b, c из задачи 9.2.8 (c). (Заметим, что метод дель Ферро из задачи 4.2.2 фактически приводит к тому же.) По теореме Виета $a = a(x, y, z)$ — коэффициент уравнения. При замене $x \leftrightarrow y$ многочлен $b = b(x, y, z)$ переходит в $\varepsilon_3 c$, а $c = c(x, y, z)$ в $\varepsilon_3^2 b$ (проверьте!). Значит, многочлены bc и $b^3 + c^3$ не меняются при этой замене. Аналогично они не меняются при замене $z \leftrightarrow y$. Поэтому многочлены bc и $b^3 + c^3$ *симметрические*, т. е. не меняются при любой перестановке переменных. Тогда из теоремы Виета и основной теоремы о симметрических многочленах 4.6.3 (c) следует, что эти многочлены от x, y, z представляются в виде многочленов от коэффициентов уравнения. Теперь, решая квадратное уравнение, можно получить b^3 и c^3. Далее легко получить сами b и c.

Замечание 9.2.10. In solution of Problem 9.2.6.c we constructed polynomials

$$f_1(x, y, z), \quad f_2(x, y, z), \quad f_3(x, y, z),$$

$$p_0(u, v, w), \quad p_1(u, v, w, t_1), \quad p_2(u, v, w, t_1, t_2), \quad p_3(u, v, w, t_1, t_2, t_3)$$

with complex coefficients such that

$$\begin{cases} f_1^2 = p_0(\sigma_1, \sigma_2, \sigma_3) \\ f_2^3 = p_1(\sigma_1, \sigma_2, \sigma_3, f_1) \\ f_3^3 = p_2(\sigma_1, \sigma_2, \sigma_3, f_1) \\ x = p_3(\sigma_1, \sigma_2, \sigma_3, f_1, f_2, f_3) \end{cases}.$$

(If we allow p_3 to be a rational function, then we can omit the third equation and f_3 in the fourth equation.) There are no polynomials with real coefficients such that the above system holds. A generalization of this fact to more general systems is Theorem 9.2.4.

Решение уравнения 4-й степени при помощи резольвент Лагранжа (решение задачи 9.2.9.d). Для нахождения корней x, y, z, t уравнения 4-й степени достаточно найти выражения a, b, c, d от корней из задачи 9.2.8.a. По теореме Виета a — коэффициент уравнения.

При замене $x \leftrightarrow y$ многочлены c^2 и d^2 меняются местами, а многочлен b^2 переходит в себя. При циклической замене $x \to y \to z \to t \to x$ многочлены b^2 и d^2 меняются местами, а многочлен c^2 переходит в себя. Значит, многочлены b^2, c^2, d^2 переставляются при любой перестановке переменных. Поэтому виетовские многочлены от них, т. е.

$$b^2 + c^2 + d^2, \quad b^2c^2 + b^2d^2 + c^2d^2, \quad b^2c^2d^2,$$

симметрические. Тогда эти многочлены от x, y, z представляются в виде многочленов от коэффициентов уравнения. Теперь, решая кубическое уравнение, можно получить сами b^2, c^2, d^2. Далее легко получить b, c, d.

Ввиду теоремы Руффини 9.2.5 метод резольвент Лагранжа, продемонстрированный на примере решения уравнений 3-й и 4-й степени, не работает для уравнения 5-й степени. Сообразите, почему!

Обозначим через Σ_q множество перестановок q-элементного множества. For a permutation $\alpha \in \Sigma_q$ denote

$$\vec{u}_\alpha := (u_{\alpha(1)}, \ldots, u_{\alpha(q)}).$$

Определим *резольвенту Лагранжа* как

$$t(u_1, \ldots, u_q) := \varepsilon_q u_1 + \varepsilon_q^2 u_2 + \ldots + \varepsilon_q^q u_q.$$

Определим *резольвенту Галуа* как

$$Q(u_1, \ldots, u_q, y) := \prod_{\alpha \in \Sigma_q} (y - t(\vec{u}_\alpha)) \in \mathbb{Q}[\varepsilon_q][u_1, \ldots, u_q, y].$$

9.2.11. (a) Имеем $Q(\varepsilon_q u_1, \ldots, \varepsilon_q u_q, y) = Q(u_1, \ldots, u_q, y)$.

(b) Для некоторого $R_Q \in \mathbb{Q}[\varepsilon_q][z]$ имеем $Q(u_1, \ldots, u_q, y) = = R_Q(u_1, \ldots, u_q, y^q)$.

(c) Если $x_1, \ldots, x_5$ — корни многочлена $f \in \mathbb{Q}[x]$ 5-й степени, то $Q(x_1, \ldots, x_5, y) \in \mathbb{Q}[\varepsilon_5][y]$ и даже $Q(x_1, \ldots, x_5, y) \in \mathbb{Q}[y]$.

Многочлен $R_Q(x_1, \ldots, x_5, z) \in \mathbb{Q}[z]$ называется *разрешающим многочленом* для f.

(d)* Все корни разрешающего многочлена для $f(x) = x^5 + 15x + 44$ (а значит, и самого многочлена f) радикальны.

Using (a version of) критерия Галуа разрешимости 9.2.12.a below one can prove that *при* $a, b \in \mathbb{Q}$ *все корни многочлена* $x^5 + ax + b$ *радикальны тогда и только тогда, когда либо многочлен приводим над* $\mathbb{Q}$, *либо* $a = \dfrac{5\lambda^4(3 \pm 4c)}{c^2+1}$ *и* $b = \dfrac{4\lambda^5(11 \mp 2c)}{c^2+1}$ *для некоторых* $\lambda, c \in \mathbb{Q}$, $c \geqslant 0$, $\lambda \neq 0$ [PSo, Chapter 6, §7, Theorem 1].

9.2.12. (a) **Критерий Галуа разрешимости (гипотеза).** Для любых $a_{n-1}, \dots, a_0 \in \mathbb{Q}$ все корни уравнения $A(x) := x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$ радикальны тогда и только тогда, когда некоторый набор многочленов степени 1 с коэффициентами в $\mathbb{Q}$ может быть получен из $\{A\}$ при помощи следующих операций:

• (факторизация) если один из многочленов равен $P_1 P_2$ для некоторых $P_1, P_2 \in \mathbb{Q}[x]$, не являющихся константами, то заменим $P_1 P_2$ на P_1 и P_2;

• (извлечение корня) если один из наших многочленов равен $P(x^q)$ для некоторого $P \in \mathbb{Q}[x]$, то заменим $P(x^q)$ на $P(x)$;

• (взятие резольвенты Галуа) заменим один из наших многочленов P на многочлен $Q(y_1, \dots, y_q, y)$, где $y_1, \dots, y_q$ – все корни многочлена P. (По утверждению 9.2.11.c $Q(y_1, \dots, y_q, y) \in \mathbb{Q}[y]$.)

(b) Докажите часть «тогда» критерия (a).

(c) Сформулируйте и докажите вещественный аналог критерия (a).

(d) Сформулируйте и докажите аналог критерия (a) for equations solvable using one radical, cf. [AB, ABG].

(e)* Does the analogue of (a) hold for every $a_{n-1}, \dots, a_0 \in \mathbb{C}$ with 'expressible by radicals' replaced by 'expressible by radicals from $\{1, a_{n-1}, \dots, a_0\}$'?

Доказательство части «только тогда» в критерии (a) аналогично теореме 9.1.14, см. также теорему Галуа 9.1.13 и §9.3.9. I would be grateful if a specialist in algebra could confirm that criterion (a) is correct (and is equivalent to the Galois Solvability Criterion in its usual textbook formulation, please give a reference), or describe required changes. (I asked some specialists since July 2017, but so far obtained no answer.)

9.2.3 Переформулировка теоремы Гаусса (2)

Комплексное число называется (комплексно) **построимым**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений квадратных корней. Т.е. если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя операции добавления к уже имеющемуся множеству $M \subset \mathbb{C}$, содержащему числа x, y,

$$\text{чисел } x+y, x-y, xy, \quad \text{числа } x/y \text{ при } y \neq 0$$

$$\text{и любого такого числа } r \in \mathbb{C}, \text{ что } r^2 = x.$$

9.2.14. Число $\cos(2\pi/n)$ построимо тогда и только тогда, когда число ε_n построимо.

Лемма 9.2.15 (о комплексификации)**.** Комплексное число построимо тогда и только тогда, когда его вещественная и мнимая части вещественно построимы.

Из этой леммы вытекает, что вещественное число построимо тогда и только тогда, когда оно вещественно построимо[5]. Значит, теорему Гаусса 9.1.5 достаточно доказать с заменой «вещественной построимости» на «построимость».

9.2.16. * Является ли $\{e+\pi i\}$-радикальным число e? (См. определение перед теоремой 9.1.14. Используйте без доказательства то, что числа e и π не радикальны.)

[5]Заметим, что в определении построимости нет операций Re и Im. Однако их можно «реализовать», доказав, что если можно получить число z, то можно получить и $\overline{z}$. Но так будет доказана *построимость* вещественной и мнимой частей, а не их *вещественная построимость*. Для доказательства вещественной построимости нужно извлекать комплексный корень при помощи вещественных корней. Это возможно только для корней второй степени. Если в определениях построимости и вещественной построимости допускать извлечения корней третьей степени, то аналог леммы о комплексификации будет неверен. Действительно, $\varepsilon_9 \in \sqrt[3]{\sqrt[3]{1}}$ радикально с извлечением корней только третьей степени, а $\cos(2\pi/9)$ не является вещественном радикальным, см. замечание 9.1.7f.

9.2.4 Идея доказательства построимости в теореме Гаусса

Обозначим $\varepsilon_q := \cos(2\pi/q) + i\sin(2\pi/q)$.

Комплексное число называется (комплексно) **построимым**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений квадратных корней. Т.е. если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя операции добавления к уже имеющемуся множеству $M \subset \mathbb{C}$, содержащему числа x, y,

$$\text{чисел } x+y, x-y, xy, \quad \text{числа } x/y \text{ при } y \neq 0$$

$$\text{и любого такого числа } r \in \mathbb{C}, \text{ что } r^2 = x.$$

9.2.17. (α) Число ε_q построимо для $q = 2, 3, 6, 8, 12, 16$.

(a) Число ε_5 построимо.

(β) Число ε_q построимо для $q = 10, 15, 20$.

(b) Число ε_7 можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений комплексных корней второй и третьей степени.

(c) То же для числа ε_{11} и корней только второй и пятой степени.

(d) Число ε_{17} построимо.

(e) (Теорема Гаусса) Если $q = 2^\alpha p_1 \cdot \ldots \cdot p_l$, где $p_1, \ldots, p_l$ — различные простые числа вида $2^{2^s} + 1$, то число ε_q построимо.

Пункты (a) и (b) можно решить непосредственно. Далее уже нужна новая идея. Оказывается, вместо работы с набором корней часто удобнее работать с некоторыми выражениями от корней — *резольвентами Лагранжа*, которые определены в задаче 0.

0. Решите системы уравнений (x, y, z, t — неизвестные, a, b, c, d известны):

$$\text{(a)} \quad \begin{cases} x+y+z+t=a, \\ x+y-z-t=b, \\ x-y+z-t=c, \\ x-y-z+t=d; \end{cases} \qquad \text{(b)} \quad \begin{cases} x+y+z+t=a, \\ x+iy-z-it=b, \\ x-y+z-t=c, \\ x-iy-z+it=d; \end{cases}$$

$$\text{(c)} \quad \begin{cases} x+y+z=a, \\ x+\varepsilon_3 y+\varepsilon_3^2 z=b, \\ x+\varepsilon_3^2 y+\varepsilon_3 z=c. \end{cases}$$

Идея доказательства построимости числа $\varepsilon := \varepsilon_5$. Во-первых,

$$T_0 := \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1.$$

Сначала докажем построимость числа

$$T_2 := \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8.$$

При замене ε на ε^2 число T_2 переходит в $-T_2$. Значит, T_2^2 не меняется при этой замене. Поэтому T_2^2 не меняется при двукратной и трехкратной таких заменах, т. е. при заменах ε на ε^4 и ε на $\varepsilon^8 = \varepsilon^3$. Итак, для любого k число T_2^2 не меняется при замене ε на ε^k.

Раскроем скобки в произведении T_2^2 и заменим ε^5 на 1. Получим равенство

$$T_2^2 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{для некоторых} \quad a_k \in \mathbb{Z}.$$

Так как для любого k число T_2^2 не меняется при замене ε на ε^k, то $a_1 = a_2 = a_3 = a_4$. Поэтому $T_2^2 = a_0 - a_1 \in \mathbb{Z}$. Значит, T_2 построимо.

Обозначим

$$T_1 := \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8 \qquad \text{и} \qquad T_3 := \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8.$$

Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать построимость чисел T_1 и T_3. Сделаем это для T_1; доказательство для T_3 аналогично.

При замене ε на ε^2 число T_1 переходит в $-iT_1$. Значит, T_1^4 при этой замене не меняется. Поэтому T_1^4 не меняется при двукратной и трёхкратной замене такого вида, т. е. при замене ε на ε^4 и ε на $\varepsilon^8 = \varepsilon^3$. Итак, для любого k число T_1^4 не меняется при замене ε на ε^k.

Раскроем скобки в произведении T_1^4 и заменим ε^5 на 1. Получим равенство

$$T_1^4 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{для некоторых} \quad a_k \in \mathbb{Z} + i\mathbb{Z}.$$

Так как для любого k число T_1^4 не меняется при замене ε на ε^k, то $a_1 = a_2 = a_3 = a_4$. Поэтому $T_1^4 = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$. Значит, T_1 построимо.

In the above arguments we need to prove that the 'replacing ε by ε^k' is well-defined. Обоснование для общего случая трудное; читатель может найти пример такого рассуждения в [E1, § 24]. Поэтому вместо того, чтобы его приводить, мы немного изменим доказательство; именно этим приводимое доказательство проще данного в [E1], [PSo, § 6.4]. Вместо работы с *числами* мы будем работать с *многочленами* и подставлять в них ε в качестве аргумента. Два многочлена с комплексными коэффициентами называются *сравнимыми по модулю многочлена* p, если их разность делится (в $\mathbb{C}[x]$) на p.

9.2.18. Обозначим $T_1(x) := x + ix^2 - x^4 - ix^8$. Тогда
(a) $iT_1(x^2) \equiv T_1(x) \bmod (x^5 - 1)$;
(b) $T_1^4(x^2) \equiv T_1^4(x) \bmod (x^5 - 1)$;
(c) $T_1^4(x^k) \equiv T_1^4(x) \bmod (x^5 - 1)$ для любого $k = 1, 2, 3, 4$.

Доказательство построимости числа $\varepsilon := \varepsilon_5$. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$. Поэтому достаточно доказать построимость каждого из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$. Имеем

$$iT_1(x^2) \underset{x^5-1}{\equiv} T_1(x) \quad \Longrightarrow \quad T_1^4(x^2) \underset{x^5-1}{\equiv} T_1^4(x) \quad \Longrightarrow$$
$$\Longrightarrow \quad T_1^4(x^k) \underset{x^5-1}{\equiv} T_1^4(x) \quad \text{для любого } k.$$

Возьмём многочлен $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ с коэффициентами в $\mathbb{Z} + i\mathbb{Z}$, сравнимый с $T_1^4(x)$ по модулю $x^5 - 1$.

Тогда $a_1 = a_2 = a_3 = a_4$. Поэтому[6] $T_1^4(\varepsilon) = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$.

Значит, $T_1(\varepsilon)$ построимо. Аналогично $T_2(\varepsilon)$ и $T_3(\varepsilon)$ построимы. □

[6] Другой способ, предложенный М. Ягудиным:

$$T_1^4(\varepsilon) = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 = a_0 + a_1\varepsilon^2 + a_2\varepsilon^4 + a_3\varepsilon + a_4\varepsilon^3 =$$
$$= a_0 + a_1\varepsilon^3 + a_2\varepsilon + a_3\varepsilon^4 + a_4\varepsilon^2 = a_0 + a_1\varepsilon^4 + a_2\varepsilon^3 + a_3\varepsilon^2 + a_4\varepsilon.$$

Суммируя эти выражения, получим $4T_1^4(\varepsilon) = a_0 - a_1 - a_2 - a_3 - a_4 \in \mathbb{Z} + i\mathbb{Z}$.

9.2.19. (a) Обозначим

$$\beta := \varepsilon_6 = \frac{1+i\sqrt{3}}{2} \quad \text{и} \quad T(x) := x+\beta x^3+\beta^2 x^9+\beta^3 x^{27}+\beta^4 x^{81}+\beta^5 x^{243}.$$

Докажите, что $T(x) \equiv \beta T(x^3) \bmod (x^7-1)$.

(b) Обозначим

$$\beta := \varepsilon_{10} \quad \text{и} \quad T(x) := x+\beta x^2+\beta^2 x^4+\beta^3 x^8+\beta^4 x^{16}+\ldots+\beta^9 x^{512}.$$

Докажите, что $T(x) \equiv \beta T(x^2) \bmod (x^{11}-1)$.

Решения задач 9.2.17 (c,d) и 9.2.19 аналогичны приведённому доказательству построимости числа ε_5.

9.2.5 Доказательство построимости в теореме Гаусса (3)

Лемма 9.2.20 (об умножении)**.** (a) Если ε_n построимо, то ε_{2n} построимо.

(b) Если ε_n и ε_m построимы и m, n взаимно просты, то ε_{mn} построимо.

Доказательство получается из формул $\varepsilon_{2n} \in \sqrt{\varepsilon_n}$ и $\varepsilon_{mn} = \varepsilon_m^x \varepsilon_n^y$, где x и y — целые числа, для которых $nx+my=1$. □

При решении задачи 9.2.17 (a) мы использовали различность остатков от деления чисел $2, 2^2, 2^3, 2^4$ на 5. Для решения задач 9.2.17 (b,c,d) и 9.2.19 (a,b) полезно аналогичное свойство чисел 3 и 7, 2 и 11, 6 и 17. Для общего случая необходимо следующее.

Теорема 9.2.21 (о первообразном корне)**.** Для любого простого p существует число g, для которого остатки от деления на p чисел $g^1, g^2, g^3, \ldots, g^{p-1}$ различны.

Указание к доказательству для $p = 2^m+1$ (только этот случай нужен для теоремы Гаусса). Если первообразного корня нет, то сравнение $x^{2^{m-1}} \equiv 1 \bmod p$ имеет $p-1 = 2^m > 2^{m-1}$ решений. Это противоречит теореме Безу.

Заинтересованный читатель может получить и полное доказательство, см. п. 3.5.

Доказательство построимости в теореме Гаусса 9.1.5. По лемме 9.2.15 о комплексификации и по лемме 9.2.20 об умножении достаточно доказать, что ε_n построимо для любого простого $n = 2^{2^s} + 1$. Так как $n - 1 = 2^m$, то по лемме 9.2.20 об умножении $\beta := \varepsilon_{n-1}$ построимо. Обозначим

$$\mathbb{Z}[\beta] := \{b_0 + b_1\beta + b_2\beta^2 + \ldots + b_{n-2}\beta^{n-2} \mid b_0, b_1, \ldots, b_{n-2} \in \mathbb{Z}\}.$$

Обозначим через g первообразный корень по модулю n. Для $r = 0, 1, 2, \ldots, n-2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \ldots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

Тогда $(T_0 + T_1 + \ldots + T_{n-2})(\varepsilon) = (n-1)\varepsilon$. Кроме того, $T_0(\varepsilon) = -1$. Поэтому достаточно доказать построимость каждого из чисел $T_r(\varepsilon)$, $r = 1, 2, \ldots, n-2$. Имеем

$$\beta^r T_r(x^g) \underset{x^n-1}{\equiv} T_r(x) \quad \Longrightarrow \quad T_r^{n-1}(x^g) \underset{x^n-1}{\equiv} T_r^{n-1}(x) \quad \Longrightarrow$$
$$\Longrightarrow \quad T_r^{n-1}(x^k) \underset{x^n-1}{\equiv} T_r^{n-1}(x) \quad \text{для любого } k.$$

Возьмём многочлен $a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1}x^{n-1}$ с коэффициентами в $\mathbb{Z}[\beta]$, сравнимый с $T_r^{n-1}(x)$ по модулю $x^n - 1$. Тогда $a_1 = a_2 = \ldots = a_{n-1}$. Поэтому $T_r^{n-1}(\varepsilon) = a_0 - a_1 \in \mathbb{Z}[\beta]$. Значит, $T_r(\varepsilon)$ построимо. $\square$

9.3 Задачи о неразрешимости в радикалах

В этом пункте мы на простых примерах демонстрируем идеи доказательств теорем о неразрешимости из п. 9.1. Этот пункт независим от предыдущего. Более того, он почти независим от п. 9.1, поскольку большинство приводимых здесь задач касается непредставимости чисел в некотором специальном виде и не использует определений и формулировок из п. 9.1. Непредставимость, хоть она и кажется очень естественной, может доказываться нетривиально!

К теореме 9.1.2 и непостроимости в теореме Гаусса 9.1.5 (п. 9.4.4) подводят задачи из п. 9.3.1–9.3.2. К неразрешимости в вещественных радикалах из теоремы 9.1.10 (п. 9.4.5), к теореме 9.1.11 (п. 9.4.8), и к теореме Кронекера 9.1.15 (п. 9.4.7) подводят задачи из п. 9.3.1–9.3.4. К теореме 9.1.14 и неразрешимости в критерии 9.2.12.а (п. 9.4.3 и 9.4.6) подводят задачи из п. 9.3.1–9.3.6. К теореме 9.1.17 подводят задачи всего этого пункта, включая п. 9.3.9.

Таким образом, п. 9.3.1–9.3.4 развивают идею сопряжения, а п. 9.3.5–9.3.9 — идею симметрии. Заметим, что в п. 9.3 эти идеи раскрываются в обратном порядке (поскольку, в противоположность первым шагам, окончательная реализация идеи сопряжения более сложна, чем идеи смммметрии).

В этом пункте «многочлен с рациональными коэффициентами» коротко называется многочленом. Числа $v_1, \dots, v_n \in \mathbb{C}$ называются *линейно зависимыми над* $\mathbb{Q}$, если найдутся $\lambda_1, \dots, \lambda_n \in \mathbb{Q}$, не все равные нулю, для которых $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$. Напомним, что

$$\varepsilon_q := \cos(2\pi/q) + i \sin(2\pi/q).$$

9.3.1 Одно извлечение квадратного корня (1-2)

9.3.1. Представимо ли следующее число в виде $a+\sqrt{b}$, где $a, b \in \mathbb{Q}$:
(a) $\sqrt{3+2\sqrt{2}}$; (b) $\frac{1}{7+5\sqrt{2}}$; (c) $\sqrt[3]{7+5\sqrt{2}}$; (d) $\sqrt[3]{2}$;
(e) $\sqrt{2}+\sqrt[3]{2}$; (f) $\sqrt{2+\sqrt{2}}$; (g) $\sqrt{2}+\sqrt{3}+\sqrt{5}$.

9.3.2.* Для каких n число $\cos(2\pi/n)$ представимо в виде $a+\sqrt{b}$, где $a, b \in \mathbb{Q}$? В качестве отдельных пунктов засчитываются случаи $n =$ 16, 24, 20, 15, 9, 7, 17, 25. (Ответ на этот вопрос нужен, например, для изучения *внешних бильярдов*.)

«Многочлен с рациональными коэффициентами» коротко называется многочленом.

Лемма 9.3.3. Пусть $r \in \mathbb{R} - \mathbb{Q}$ и $r^2 \in \mathbb{Q}$.
(a) **О неприводимости.** Многочлен $x^2 - r^2$ неприводим над $\mathbb{Q}$.
(b) **О линейной независимости.** Если $a, b \in \mathbb{Q}$ и $a + br = 0$, то $a = b = 0$.
(c) Если многочлен P имеет корень r, то P делится на $x^2 - r^2$.
(d) **О сопряжении.** Если многочлен имеет корень r, то корнем этого многочлена является также число $-r$.
(e) **О сопряжении.** Если $a, b \in \mathbb{Q}$ и многочлен имеет корень $a + br$, то корнем этого многочлена является также число $a - br$.
(f) Если $a, b \in \mathbb{Q}$ и кубический многочлен имеет корень $a + br$, то он имеет рациональный корень.

Теорема 9.3.4. Если многочлен степени выше 2 неприводим над $\mathbb{Q}$, то ни один из его корней не представим в виде $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$.

9.3.5. (a) Решите уравнение $x^6 - 2x^4 - 12x^3 - 2x^2 + 1 = 0$.
(b) Число $\cos(2\pi/7)$ является корнем многочлена, полученного из функции $x^3 + x^2 + x + 1 + x^{-1} + x^{-2} + x^{-3}$ заменой Жуковского $z = \frac{1}{2}(x + \frac{1}{x})$.

9.3.6. (a) Приводим ли многочлен $x^5 - 4x^3 + 6x^2 + 4x + 2$ над $\mathbb{Z}$? $\mathbb{Q}$?
(b) Для каждого $q = 5, 7, 11, 9, 25, 15, 16, 20$ найдите неприводимый над $\mathbb{Q}$ многочлен, корнем которого является число $\varepsilon_q := \cos(2\pi/q) + i\sin(2\pi/q)$.
(c) То же с заменой ε_q на $\cos(2\pi/q)$.

Лемма 9.3.7 (о расширении)**.** Пусть число можно получить из числа 1 при помощи нескольких операций сложений, вычитаний, умножений, делений на ненулевые числа, и одной операции извлечения квадратного корня из положительного числа (т.е. число вещественно построимо с извлечением корня только один раз). Тогда оно имеет вид $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$ и $b > 0$.

Из теоремы 9.3.4 и леммы 9.3.7 о расширении вытекает, что *если многочлен степени выше второй неприводим над* $\mathbb{Q}$*, то ни один из его корней не является вещественно радикальным с извлечением корня только один раз, причём второй степени.* Справедлив и комплексный аналог этого утверждения. Это наше первое продвижение к теоремам о неразрешимости из §9.1. Аналогичные продвижения в следующих подпунктах (сформулируйте их самостоятельно) вытекают из аналогичных теорем и лемм.

Подсказки

9.3.7. Было бы достаточно доказать, что множество чисел такого вида замкнуто относительно сложения, вычитания, умножения и деления. Это, естественно, не так: $(1+\sqrt{2})+(1+\sqrt{3})$ не представимо в виде $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$ (докажите!).

9.3.3. (a) Если многочлен $x^2 - r^2$ приводим над $\mathbb{Q}$, то он имеет рациональный корень. Противоречие.

(b) Если $b \neq 0$, то $r = -a/b \in \mathbb{Q}$, что невозможно. Поэтому $b = 0$, а значит, $a = 0$.

(c) Поделим многочлен с остатком[8] на $x^2 - r^2$:

$$P(x) = (x^2 - r^2)Q(x) + mx + n.$$

Подставляя $x = r$, по лемме о линейной независимости (см. п. (b)) получаем, что остаток нулевой.

(d) Из п. (c) следует, что если $R^2 = r^2$, то R есть корень многочлена.

Указание к другому решению. Отображение $u \mapsto \overline{u}$ множества $\mathbb{Q}[r] := \{a + br \colon a, b \in \mathbb{Q}\}$ в себя корректно определено формулой

[8] Это деление с остатком — то же самое, что «замена» x^2 на r^2.

$\overline{a+br} := a-br$. Кроме того, $\overline{u+v} = \overline{u}+\overline{v}$ и $\overline{u\cdot v} = \overline{u}\cdot\overline{v}$ для любых $u, v \in \mathbb{Q}[\sqrt{2}]$.

(e) Обозначим через P многочлен из условия, и пусть $G(t) := P(a+bt)$. Тогда $G(r) = 0$. Значит, по пункту (d) имеем $G(-r) = 0$.

(f) Если $b = 0$, то утверждение доказано. В противном случае по п. (e) многочлен имеет (различные) корни $a \pm br$, значит третий корень рационален по теореме Виета.

Указания, ответы и решения

9.3.1. *Ответы*: (a), (b), (c) — да, (d), (e), (f), (g) — нет.

(a), (c) Имеем $\sqrt{3+2\sqrt{2}} = \sqrt[3]{7+5\sqrt{2}} = 1+\sqrt{2}$.

(b) Имеем $\frac{1}{7+5\sqrt{2}} = \frac{7-5\sqrt{2}}{7^2-2\cdot 5^2} = -7+5\sqrt{2}$.

(d) Пусть число $\sqrt[3]{2}$ представимо. Тогда

$$2 = (\sqrt[3]{2})^3 = (a^3+3ab) + (3a^2+b)\sqrt{b}.$$

Так как $3a^2+b \neq 0$, то $\sqrt{b} \in \mathbb{Q}$. Значит, $\sqrt[3]{2} \in \mathbb{Q}$ — противоречие.

Ср. с задачей 4.1.1 (h).

Другой способ — аналогично теореме 9.3.4.

Ещё один способ. Пусть число $\sqrt[3]{2}$ представимо. Тогда

$$1 = 1,$$
$$\sqrt[3]{2} = a + b\sqrt{2},$$
$$\sqrt[3]{4} = a' + b'\sqrt{2}$$

для некоторых рациональных чисел a, b, a', b'. Векторы $(1,0)$, (a,b), (a',b') на плоскости линейно зависимы с рациональными коэффициентами, т. е. существуют λ_0, λ_1, λ_2, не все равные нулю, для которых $\lambda_0(1,0)+\lambda_1(a,b)+\lambda_2(a',b') = 0$. Тогда $\lambda_0+\lambda_1\sqrt[3]{2}+\lambda_2\sqrt[3]{4} = 0$. Противоречие с леммой о линейной независимости 9.3.17 (b).

(e) *Набросок первого решения.* Предположим противное и возведем в куб равенство $\sqrt[3]{2} = a+\sqrt{b}-\sqrt{2}$.

Набросок второго решения. Докажем, что

$$\sqrt[3]{2} \neq a+p\sqrt{b}+q\sqrt{c}+r\sqrt{bc} \quad \text{ни для каких} \quad a,b,c,p,q,r \in \mathbb{Q}.$$

9.3.5 Неразрешимость «в вещественных многочленах» (2)

In this and the following subsubsection equality signs involving polynomial f (or f_j) mean equality of polynomials (покоэффициентное). В этом пункте аргументы (x, y, z) многочленов в формулах часто пропускаются.

9.3.27. Существуют ли многочлены с вещественными коэффициентами, удовлетворяющие системе из замечания 9.2.10 с заменой f_2^3, f_3^3 на f_2^2, f_3^2?

Для решения полезны следующее понятие и утверждение. Многочлен $g \in \mathbb{R}[x, y, z]$ называется **циклически симметрическим**, если $g(x, y, z) = g(y, z, x)$.

9.3.28. Если $f \in \mathbb{R}[x, y, z]$ и многочлен

(a) f^3; (b) f^2

циклически симметрический, то f циклически симметрический.

9.3.29. Пусть $f, g \in \mathbb{R}[x, y, z]$.

(a) **Лемма.** Если $fg = 0$, то $f = 0$ или $g = 0$.

Предостережения: существуют функции $F, G : \mathbb{R} \to \mathbb{R}$, для которых $FG = 0$, $F \neq 0$, $G \neq 0$; существуют два разных многочлена от двух переменных, равные в бесконечном множестве точек; не пользуйтесь без доказательства равенством многочленов от двух переменных, значения которых совпадают в любой точке.

(b) Если $f^2 = g^2$, то $f = g$ или $f = -g$.

(c) Если $f^2 + fg + g^2 = 0$, то $f = 0$ и $g = 0$.

(d) Если $f^3 = g^3$, то $f = g$.

(e) Если $f^5 = g^5$, то $f = g$.

(f) $f^5 - g^5 = (f - g)(f - \varepsilon_5 g)(f - \varepsilon_5^2 g)(f - \varepsilon_5^3 g)(f - \varepsilon_5^4 g)$.

Теорема 9.2.4 вытекает из следующей леммы.

Лемма 9.3.30 (о сохранении циклической симметричности)**.** Если $q > 0$ целое, $f \in \mathbb{R}[x, y, z]$ и многочлен f^q циклически симметрический, то f циклически симметрический.

9.3.31. Аналоги каких утверждений этого пункта справедливы для

(a) многочленов с комплексными коэффициентами?

(b) с заменой многочлена f на функцию $f : \mathbb{R}^3 \to \mathbb{R}$ (не предполагаемую непрерывной).

9.3.6 Неразрешимость «в многочленах» (3)

Теорема Руффини 9.2.5 вытекает из леммы 9.3.35. Самое трудное и интересное — придумать формулировку этой леммы. Для этого докажем следующие более простые факты.

9.3.32. Многочлен x_1 не радикален для $n = 3$ так, что вторая операция из определения радикальности применяется только для

(a) $k = 2$ (*подсказка:* см. задачу 9.3.31); (b) $k = 3$.

9.3.33. Какие из следующих утверждений верны для любого $f \in \mathbb{C}[x_1, \ldots, x_5]$?

(a) Если f^5 циклически симметрический, то f циклически симметрический.

(b) Если f^3 циклически симметрический, то f циклически симметрический.

(c) Если f^2 симметрический, то f симметрический.

(d) Если f^3 симметрический, то f симметрический.

Циклом длины 3 называется перестановка n-элементного множества, переставляющая некоторые 3 элемента по циклу и оставляющая на месте каждый из оставшихся элементов. Многочлен $f \in \mathbb{C}[x_1, \ldots, x_n]$ называется **четносимметрическим**, если $f(x_1, x_2, \ldots, x_n) = f(x_{\alpha(1)}, x_{\alpha(2)}, \ldots, x_{\alpha(n)})$ для любого цикла α длины 3.

9.3.34. Придумайте циклически симметрический многочлен, не являющийся четносимметрическим.

Лемма 9.3.35 (о сохранении четносимметричности)**.** Если $q > 0$ целое, $f \in \mathbb{C}[x_1, \ldots, x_5]$ и многочлен f^q четносимметрический, то f четносимметрический.

9.3.36. Пусть $f \in \mathbb{C}[x_1, \ldots, x_n]$ — многочлен.

(a) Если многочлен f^7 четносимметрический, то f четносимметрический.

(b) Если $n \geqslant 5$ и многочлен f^3 четносимметрический, то f четносимметрический.

(c) Если $n \geqslant 5$, то любой цикл длины 3 на n-элементном множестве разлагается в произведение перестановок вида $(ab)(cd)$ с различными a, b, c, d (т.е. в произведение композиций транспозиций с непересекающимися носителями).

9.4 Доказательства неразрешимости в радикалах

Формально, для понимания этого пункта достаточно прочитать формулировки в п. 9.1.2–9.1.4 (хотя мы иногда ссылаемся на п. 9.3 по поводу простых деталей доказательств и в п. 9.4.7 на теорему 9.1.16 Гаусса о понижении). Познакомиться с идеями по п. 9.3 полезно, но не обязательно. Какие подпункты из п. 9.3 полезны для каких подпунктов этого пункта, написано в начале п. 9.3.

П. 9.4.1 используется во всех пунктах этого параграфа. Лемма 9.4.12.b используется в п. 9.4.6, 9.4.7. Теорема 9.4.3 используется в п. 9.4.6. П. 9.4.7 используется в п. 9.4.8. В остальном пункты этого параграфа формально независимы друг от друга. Кроме указанных формальных зависимостей для каждого пункта, в который ведет стрелка, полезно прочитать пункт, из которого она исходит:

$$9.4.2 \to 9.4.3, \quad 9.4.4 \to 9.4.5 \to 9.4.6, 9.4.7.$$

План доказательства в каждом пункте получается из текста пункта пропуском доказательств лемм.

9.4.1 Поля и их расширения (2)

Если $F \subset \mathbb{C}$, $r \in \mathbb{C}$ и $r^q \in F$ для некоторого целого положительного q, то обозначим

$$F[r] := \{a_0 + a_1 r + a_2 r^2 + \ldots + a_{q-1} r^{q-1} \mid a_0, \ldots, a_{q-1} \in F\}.$$

Definitions of constructibility, real constructibility, expressibility by radicals and real expressibility by radicals are given in §§9.2.3, 9.1.2, 9.1.4, 9.1.3, respectively.

Лемма 9.4.1 (о башне расширений)**.** (a) Число $x \in \mathbb{C}$ построимо тогда и только тогда, когда существуют такие $r_1, \ldots r_{s-1} \in \mathbb{C}$, что

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset \ldots \subset F_{s-1} \subset F_s \ni x,$$

где $r_k^2 \in F_k$, $r_k \notin F_k$ и $F_{k+1} = F_k[r_k]$ для любого $k = 1, \ldots, s-1$.

(b) Число $x \in \mathbb{C}$ радикально тогда и только тогда, когда существуют такие $r_1, \ldots r_{s-1} \in \mathbb{C}$ и такие простые $q_1, \ldots, q_{s-1}$, что

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset \ldots \subset F_{s-1} \subset F_s \ni x,$$

где $r_k^{q_k} \in F_k$, $r_k \notin F_k$ и $F_{k+1} = F_k[r_k]$ для любого $k = 1, \dots, s-1$.

Такая последовательность называется *башней* (квадратичных или радикальных) *расширений*. Доказательство невозможности, основанное на рассмотрении аналогичных цепочек-башен, называется в математической логике и программировании *индукцией по глубине формулы*.

Эта лемма доказывается индукцией по количеству операций, необходимых для получения числа, аналогично леммам о расширении из §9.3. Аналог этой леммы для вещественных построимости и радикальности справедлив и доказывается аналогично.

Чтобы поменьше упоминать эту естественную, но несколько громоздкую лемму, введем следующее понятие. В этом параграфе **полем** называется подмножество множества $\mathbb{C}$, замкнутое относительно операций сложения, умножения, вычитания и деления на ненулевое число. Общепринятое название: числовое поле (а *полем* в математике называется немного другой объект). Это понятие полезно для нас тем, что теорема делении с остатком верна для многочленов с коэффициентами в поле. We use the standard notation $F[u_1, \dots, u_n]$ and $F(u_1, \dots, u_n)$ for the sets of polynomials and rational fractions (i.e., formal ratios of polynomials) with coefficients in F. Equality signs involving polynomial or rational fraction P, f or f_j mean equality of polynomials or rational fractions (покоэффициентное).

Напомним, что

$$\varepsilon_q := \cos(2\pi/q) + i\sin(2\pi/q) \quad \text{и} \quad \vec{y} := (y_1, \dots, y_n).$$

9.4.2 Неразрешимость «в вещественных многочленах» (3)

Лемма 9.4.2 (keeping cyclic symmetry)**.** If P is a rational fraction of 3 variables with coefficients in $\mathbb{R}$, and P^q is cyclic-symmetric for some integer q, then P is cyclic-symmetric.

Доказательство. Обозначим $R(x_1, x_2, x_3) := P(x_2, x_3, x_1)$. Так как P^q циклически симметрическая, то $P^q = R^q$.

Если q нечетно, то $P = R$ (аналогично задаче 9.3.29). Значит, P циклически симметрическая.

А если q четно, то $P = R$ или $P = -R$. При $P = R$ получаем, что P циклически симметрическая. А при $P = -R$ имеем

$$P(x_1, x_2, x_3) = -P(x_2, x_3, x_1) = P(x_3, x_1, x_2) = -P(x_1, x_2, x_3).$$

Поэтому $P = 0$, значит, P циклически симметрическая. □

9.4.3 Неразрешимость «в многочленах» (3)

См. [Sk15].

Here we prove the Ruffini Theorem in the following form required for Theorem 9.1.14, cf. Ruffini Theorem 9.2.5. An extension and a radical extension is defined at the beginning of §9.4.2. Denote

$$\mathbb{Q}_\varepsilon := \bigcup_{q=3}^{\infty} \mathbb{Q}(\varepsilon_3, \varepsilon_4, \ldots, \varepsilon_q).$$

Теорема 9.4.3 (Ruffini)**.** There are $a_0, a_1, a_2, a_3, a_4 \in \mathbb{C}$ such that no root of the equation $x^5 + a_4x^4 + \ldots + a_1x + a_0 = 0$ is contained in any radical extension of

$$\mathbb{Q}_\varepsilon(\vec{a}) := \mathbb{Q}_\varepsilon(a_0, a_1, a_2, a_3, a_4)$$

contained in $\mathbb{Q}_\varepsilon(\vec{x})$, where $x_1, \ldots, x_5$ are the roots of the equation.

Лемма 9.4.4 (Keeping symmetry through extraction of a radical)**.** If P is a rational fraction of 5 variables with coefficients in $\mathbb{C}$, and P^q is even-symmetric for some integer q, then P is even-symmetric.

9.4.4 Непостроимость в теореме Гаусса (3*)

Теорема 9.1.2 (вещественная непостроимость числа $\sqrt[3]{2}$) вытекает из вещественного аналога леммы 9.4.1.a о башне расширений и следующей леммы.

Лемма 9.4.5. Пусть $F \subset \mathbb{R}$ — поле, $r \in \mathbb{R} - F$ и $r^2 \in F$.

(a) Тогда $F[r]$ — поле.

(b) Если $\sqrt[3]{2} \notin F$, то $\sqrt[3]{2} \notin F[r]$.

Доказательство части (a). Нужно доказать, что $F[r]$ замкнуто относительно сложения, вычитания, умножения и деления на ненулевое число. Это не очевидно только в случае деления, который следует из равенства $\frac{1}{a+br} = \frac{a}{a^2-b^2r^2} - \frac{b}{a^2-b^2r^2}r$. □

Доказательство части (b). Предположим, напротив, что $\sqrt[3]{2} \in F[r]$. Тогда $\sqrt[3]{2} = a + br$ для некоторых $a, b \in F$. Получаем

$$2 = (\sqrt[3]{2})^3 = (a^3 + 3ab^2r^2) + (3a^2b + b^3r^2)r.$$

Так как $\sqrt[3]{2} \notin F$, то $b \neq 0$ и $r \notin F$. В частности, $r \neq 0$. Поэтому $3a^2 + b^2r^2 > 0$. Так как $2 \in \mathbb{Q} \subset F$, то $r \in F$. Противоречие. □

Перейдем к доказательству непостроимости в теореме Гаусса 9.1.5.

Лемма 9.4.6 (о степенях двойки)**.** Если неприводимый над $\mathbb{Q}$ многочлен P с рациональными коэффициентами имеет построимый корень, то $\deg P$ есть степень двойки.

Эта лемма вытекает из леммы 9.4.1.a о башне расширений и части (b) следующей леммы. Доказательство ее части (a) оставляем читателю в качестве упражнения.

Лемма 9.4.7 (о сопряжении)**.** Пусть $F \subset \mathbb{C}$ — поле, $r \in \mathbb{C} - F$ и $r^2 \in F$.

(a) Определим отображение сопряжения $\bar{\cdot}: F[r] \to F[r]$ формулой $\overline{x + yr} := x - yr$. Это отображение корректно определено, $\overline{z + w} = \overline{z} + \overline{w}$ и $\overline{zw} = \overline{z} \cdot \overline{w}$.

(b) Если многочлены $P \in F[x]$ и $Q \in F[r][x]$ имеют общий корень и неприводимы над F и над $F[r]$, соответственно, то $\deg P \in \{\deg Q, 2\deg Q\}$.

Доказательство части (b). По комплексному аналогу леммы 9.4.5.a $F[r]$ поле. Будем рассматривать делимость, неприводимость и НОД в $F[r]$, если не указано другое. Так как P и Q имеют общий корень и Q неприводим, то P делится на Q. Тогда по п. (a) $P = \overline{P}$ делится на $\overline{Q}$. Так как Q неприводим и делится на $D := \gcd(Q, \overline{Q})$, то либо $D = Q$, либо $D = 1$.

Если $D = Q$, то из $\overline{D} = D$ получаем $Q = D \in F[x]$. Отсюда, так как P неприводим над F, получаем $P = Q$.

Если $D = 1$, то P делится на $M := Q\overline{Q}$. Так как $\overline{M} = M$, получаем $M \in F[x]$. Так как P неприводим над F, получаем $P = M$. Значит, $\deg P = 2 \deg Q$. □

Лемма 9.4.8 (признак Эйзенштейна)**.** Пусть p простое. Если для многочлена с целыми коэффициентами старший коэффициент не делится на p, остальные делятся на p, а свободный член не делится на p^2, то этот многочлен неприводим над $\mathbb{Z}$.

Лемма 9.4.9 (Гаусс)**.** Если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$.

И признак Эйзенштейна, и лемма Гаусса легко доказываются переходом к многочленам с коэффициентами $\mathbb{Z}_p$. (Для леммы Гаусса рассмотрим разложение $P = P_1P_2$ данного многочлена P над $\mathbb{Q}$, возьмём такие целые n_1 и n_2, что и n_1P_1, и n_2P_2 имеют целые коэффициенты, и возьмём простой делитель p числа n_1n_2. For the Eisenstein criterion see solution of Problem 9.3.1.f.)

Доказательство непостроимости в теореме Гаусса 9.1.5. Так как $\varepsilon_n = \varepsilon_{nk}^k$, то из построимости числа ε_{nk} вытекает построимость числа ε_n. Поэтому достаточно показать, что ε_n непостроимо для

(A) простого числа n, не представимого в виде $2^m + 1$;

(B) квадрата простого числа, т. е. $n = p^2$.

Непостроимость числа ε_n следует из леммы 9.4.6 о степенях двойки для корня ε_n многочлена

- $P(x) := x^{n-1} + x^{n-2} + \ldots + x + 1$ в случае (A) и
- $P(x) := x^{p(p-1)} + x^{p(p-2)} + \ldots + x^p + 1$ в случае (B).

Неприводимость этих многочленов над $\mathbb{Q}$ вытекает из их неприводимости над $\mathbb{Z}$ и леммы 9.4.9 Гаусса. Неприводимость этих многочленов $P(x)$ над $\mathbb{Z}$ вытекает из неприводимости многочленов $P(x+1)$ над $\mathbb{Z}$. Последняя неприводимость доказывается применением признака 9.4.8 Эйзенштейна. Выполнение предположений признака Эйзенштейна для многочленов $P(x+1)$ легко проверяется с помощью сравнения $(a+b)^p \equiv a^p + b^p \bmod p$. □

9.4.5 Неразрешимость «в вещественных числах» (3*)

Импликация $(ii) \Rightarrow (i)$ в теореме 9.1.10 вытекает из вещественного аналога леммы 9.4.1.b о башне расширений и части (a) следующей леммы.

Лемма 9.4.10. Пусть q простое, $F \subset \mathbb{R}$ — поле, $r \in \mathbb{R} - F$ и $r^q \in F$.

(a) If a polynomial with coefficients in F has degree 3, has three real roots none of which lies in F, then none of the roots lies in $F[r]$.

(b) **О неприводимости.** Многочлен $t^q - r^q$ неприводим над $F[\varepsilon_q]$.

(c) **О линейной независимости.** Если $P(r) = 0$ для некоторого многочлена $P \in F[\varepsilon_q][t]$ степени меньше q, то $P = 0$.

(d) **О сопряжении.** Если $P \in F[\varepsilon_q][t]$ и $P(r) = 0$, то $P(r\varepsilon_q^k) = 0$ для любого $k = 0, 1, \ldots, q-1$.

Доказательство части (b). Пусть, напротив, многочлен $t^q - r^q$ приводим над $F[\varepsilon_q]$, т.е. имеет собственный делитель $P \in F[\varepsilon_q][t]$. Все корни многочлена $t^q - r^q$ есть $r, r\varepsilon_q, r\varepsilon_q^2, \ldots, r\varepsilon_q^{q-1}$. Свободный член многочлена P равен произведению некоторых k из этих корней. Тогда $r^k \in F[\varepsilon_q]$. Так как q простое, то $kx + qy = 1$ для некоторых целых x, y. Тогда $r = (r^k)^x (r^q)^y \in F[\varepsilon_q]$.

Поэтому[10] $r^2, r^3, \ldots, r^{q-1} \in F[\varepsilon_q]$. Составим таблицу $a_{kl} \in F$ размера $q \times (q-1)$ из разложений чисел r^k по степеням числа ε_q:

$$r^k = \sum_{l=0}^{q-2} a_{kl} \varepsilon_q^l, \quad 0 \leqslant k \leqslant q-1.$$

[10] Другая запись этого абзаца с использованием понятия размерности: тогда $\dim_F F[r] \leqslant \dim_F F[\varepsilon_q] \leqslant q-1$.

При помощи нескольких операций прибавления к одной строке другой, умноженной на число из F, можно получить таблицу с нулевой строкой.

Значит, имеется ненулевой многочлен $Q \in F[t]$ степени меньше q с корнем r. Тогда $\gcd(t^q - r^q, Q)$ имеет корень r и степень k, $0 < k \leqslant \deg Q < q$. Поэтому многочлен $t^q - r^q$ приводим над F.

Тогда аналогично первому абзацу этого доказательства получаем, что $r \in F$, используя $F \subset \mathbb{R}$. Противоречие. □

Part (c) follows by part (b) analogously to the last but one paragraph of the proof of (b).

Доказательство части (d). Так как $P(r) = 0$, то остаток от деления многочлена $P(t)$ на $t^q - r^q$ принимает значение 0 в точке r. Since the degree of this remainder is less than q, по части (c) этот остаток равен нулю. Thus P is divisible by $t^q - r^q$. For every $j = 0, 1, \ldots, q-1$ since $(r\varepsilon_q^j)^k = r^k$, we obtain $P(r\varepsilon_q^j) = 0$. □

Доказательство части (a). Пусть, напротив, некоторый корень x_0 многочлена A лежит в $F[r]$. Тогда $x_0 = H(r)$ для некоторого многочлена H с коэффициентами в F степени больше 0 и меньше q. Применим п. (d) к многочлену $P(t) := A(H(t))$. Так как $A(H(r)) = 0$, то $H(r\varepsilon_q^k)$ является корнем многочлена A для любого $k = 0, 1, \ldots, q-1$. Если $H(r\varepsilon_q^k) = H(r\varepsilon_q^l)$ для некоторых k, l, $0 \leqslant k < l \leqslant q-1$, то по п. (c) получим, что $\deg H = 0$ — противоречие. Итак, числа $H(r\varepsilon_q^k)$, $0 \leqslant k \leqslant q-1$, — попарно различные корни многочлена A. Значит, $q \leqslant 3$.

Если $q = 2$, то по теореме Виета третий корень многочлена A лежит в F — противоречие. Поэтому $q = 3$. Так как $\overline{\varepsilon_3} = \varepsilon_3^2$, то $\overline{H(r\varepsilon_3)} = H(r\varepsilon_3^2)$. Так как последние два числа различны, то ни одно них не вещественно. □

9.4.6 Неразрешимость «в числах» (4*)

См. [Sk15] или англ. версию.

Лемма 9.4.11 (Rationalization)**.** Let $x_1, \ldots, x_5, r \in \mathbb{C}$ be numbers, q a prime and $F \subset \mathbb{C}$ a field containing elementary symmetric polynomials

of $x_1, \dots, x_5$ and also ε_q, r^q but not r. If $F[r] \cap \mathbb{Q}_\varepsilon(\vec{x}) \not\subset F$, then there is $\rho \in \mathbb{Q}_\varepsilon(\vec{x})$ such that $\rho^q \in F$ and $F[\rho] = F[r]$.

Лемма 9.4.12. Let q be a prime, $r \in \mathbb{C}$ a number and $F \subset \mathbb{C}$ a field containing ε_q, r^q but not r.

(a) **Irreducibility.** Then the polynomial $t^q - r^q \in F[t]$ is irreducible over F.[11]

(b) **Linear independence.** Если $P(r) = 0$ для некоторого многочлена $P \in F[t]$ степени меньше q, то $P = 0$.

(c) **Conjugation.** If $Q \in F[t]$ a polynomial and $Q(r) = 0$, then $Q(r\varepsilon_q^j) = 0$ for every $j = 1, \dots, q-1$.

9.4.7 Теорема Кронекера о неразрешимости (4*)

Теорема Кронекера 9.1.15 (и, тем самым, теорему Галуа 9.1.13) follows by the Plugging Lemma 9.4.13 and Lemma 9.4.14.a below.

For a prime q, a field $F \subset \mathbb{C}$ and a number $r \in \mathbb{C} - F$ such that $r^q \in F$ назовём расширение $F[r]$ поля F *нормальным*, если $\varepsilon_q \in F$.

Лемма 9.4.13 (об уплотнении)**.** Если число x радикально, то существует башня нормальных расширений из леммы 9.4.1.b, для которой при любом $k = 1, 2, \dots, s-1$ либо $r_k \in \mathbb{R}$, либо $|r_k|^2 \in F_k$.

Лемма 9.4.14. Пусть q простое, $F \subset \mathbb{C}$ — поле, $r \in \mathbb{C} - F$ и $r^q, \varepsilon_q \in F$.

(a) Suppose that $F = \overline{F}$, either $r \in \mathbb{R}$ or $|r|^2 \in F$, a polynomial $G \in F[t]$ has prime degree, has more than one real roots and at least one non-real root. If G is irreducible over F, then G is irreducible over $F[r]$.

---

[11] Аналог леммы о неприводимости без условия «$\varepsilon_q \in F$» неверен для $q > 2$, $F = \mathbb{R}$ и $r = \varepsilon_q$. Например, условие «$\varepsilon_q \in F$» пропущено в замечательной книге [Pr07-2, с. 580–581]. Поясним это тонкое место более детально. В [Pr07-2] утверждение «$q = p$» на с. 581 (для $p = 2$) означает следующее: если квадратный трёхчлен f неприводим над полем F, содержащим i, и приводим над $F[\sqrt[q]{a}]$ для некоторого $a \in F$ и простого q, то $q = 2$. Это неверно для $f(x) = x^2 + x + 1$, $q = 3$, $a = 1$ и $F = \mathbb{Q}[i]$. Ошибка в доказательстве в [P] — в предыдущем предложении: (верную) теорему 1 на с. 572 применить нельзя, так как возможно, $a = b^q$ для некоторого $b \in F$ (хотя $\sqrt[q]{a} \notin F$).

(b) **Параметрическая лемма о сопряжении.** Если $P \in F[x,t]$ и $P(x,r) = 0$ как многочлен от x, то $P(x, r\varepsilon_q^k) = 0$ как многочлен от x для любого $k = 0, 1, \ldots, q-1$.

Доказательство части (b). Утверждение инвариантно относительно замены многочлена P на остаток от его деления на $t^q - r^q$. Поэтому можно считать, что $\deg_t P < q$. В этом случае лемма получается покоэффициентным применением леммы о линейной независимости 9.4.12.b. □

Лемма 9.4.15 (о рациональности)**.** Пусть $F \subset \mathbb{C}$ — поле, q целое, $r \in \mathbb{C}$, $r^q \in F$ и $H \in F[x,t]$. Тогда $H(x,r)H(x,\varepsilon_q r)\ldots H(x,\varepsilon_q^{q-1} r) \in F[x]$.

Доказательство. (Предложено И. И. Богдановым.) Произведение $H(x,x_0)H(x,x_1)\ldots H(x,x_{q-1})$ является симметрическим многочленом от $x_0, x_1, \ldots, x_{q-1}$. Значит, оно является многочленом от x и от элементарных симметрических многочленов от $x_0, x_1, \ldots, x_{q-1}$. Значения этих элементарных симметрических многочленов при $x_k = r\varepsilon_q^k$, $k = 0, 1, \ldots, q-1$, равны коэффициентам многочлена $x^q - r^q$, лежащим в F.[12] □

Доказательство леммы 9.4.14.a. Consider divisibility and irreducibility in $F[r]$, unless otherwise stated. Suppose to the contrary that G is reducible. Тогда в $F[r][x]$ существует неприводимый делитель многочлена G. Этот делитель получается подстановкой $t = r$ в некоторый многочлен $H \in F[x,t]$ степени по t больше 0 и меньше q, а по x меньше $\deg G$. Итак, $H(x,r)$ неприводим и $G(x) = H(x,r)H_1(x,r)$ для некоторого многочлена $H_1 \in F[x,t]$. Обозначим $\varepsilon := \varepsilon_q$. Применим п. (b) к $P(x,t) := G(x) - H(x,t)H_1(x,t)$. Получим, что $G(x)$ делится на многочлен $H(x, r\varepsilon^k)$ для любого $k = 0, 1, \ldots, q-1$.

[12] *Другое доказательство.* By the Linear Independence Lemma 9.4.12.b this product can be uniquely represented in the form

$$a_0(x) + a_1(x)r + \ldots + a_{q-1}(x)r^{q-1} \quad \text{for some} \quad a_k \in F[x].$$

The product goes to itself under the change $r \to r\varepsilon$ which is well defined by the Linear Independence Lemma 9.4.12.b. So again by the same lemma $a_k(x) = a_k(x)\varepsilon^k \in F[x]$ for each $k = 1, 2, \ldots, q-1$. Hence $a_k(x) = 0$ for each $k = 1, 2, \ldots, q-1$. Thus the product is $a_0(x) \in F[x]$.

Если многочлен $H(x, r\varepsilon^k)$ приводим для некоторого $k = 0, 1, \ldots, q-1$, то $H(x, r\varepsilon^k) = H_2(x, r)H_3(x, r)$ для некоторых многочленов $H_2, H_3 \in F[x, t]$. Применим (b) к $P(x, t) := H(x, t\varepsilon^k) - H_2(x, t)H_3(x, t)$. Получим, что многочлен $H(x, r)$ приводим. Противоречие. Значит, многочлен $H(x, r\varepsilon^k)$ неприводим для любого $k = 0, 1, \ldots, q-1$.

По лемме о линейной независимости 9.4.12.b многочлены $H(x, r\varepsilon^k)$ различны для различных $k = 0,\ 1, \ldots, q-1$. Значит, G делится на их произведение. Лемма 9.4.15 о рациональности утверждает, что коэффициенты этого произведения лежат в F. Из этого и неприводимости G над F следует, что G равно этому произведению с точностью до множителя $a \in F$. Тогда $\deg G = q \deg_x H$. Так как $\deg G$ простое и $\deg_x H < \deg G$, то $\deg_x H = 1$ (и $\deg G = q$). So there are $h_0, \ldots, h_{q-1} \in F$ such that корни многочлена G суть

$$x_k := h_0 + h_1 r\varepsilon^k + \ldots + h_{q-1} r\varepsilon^{k(q-1)}, \quad k = 0, 1, \ldots, q-1.$$

Вещественность числа x_k равносильна тому, что $x_k = \overline{x}_k$. Заметим, что $\overline{\varepsilon_q^k} = \varepsilon_q^{-k}$.

Если $r \in \mathbb{R}$, то по лемме о линейной независимости 9.4.12.b и ввиду $F = \overline{F}$, для любого $k = 0, 1, \ldots, q-1$ условие $x_k = \overline{x_k}$ равносильно тому, что

$h_s\varepsilon^{2sk} = \overline{h_s}$ для любого $s = 0, 1, \ldots, q-1$.

Следовательно, $x_k \in \mathbb{R}$ не более чем для одного k.

Если $r \notin \mathbb{R}$, то $|r|^2 \in F$. Тогда $\overline{r}^s = \frac{|r|^{2s}}{r^q} r^{q-s}$, где $\frac{|r|^{2s}}{r^q} \in F$. Значит, по лемме о линейной независимости 9.4.12.b и ввиду $F = \overline{F}$, для любого $k = 0, 1, \ldots, q-1$ условие $x_k = \overline{x_k}$ равносильно тому, что

$h_0 = \overline{h_0}$ и $h_s = \overline{h_{q-s}} \frac{|r|^{2q-2s}}{r^q}$ для любого $s = 1, 2, \ldots, q-1$.

Эти равенства не зависят от k. Поэтому если среди чисел $x_0, \ldots, x_{q-1}$ есть вещественное, то все они вещественны.

Противоречие.[13] □

Доказательство леммы 9.4.13 об уплотнении. При помощи индукции «вниз» по q покажем, что *из произвольной башни расширений*

[13] Два разбираемых случая в конце доказательства теоремы Кронекера 9.1.15 немного отличаются от случаев, разобранных в конце доказательства из статьи [T]. В начале 2-й колонки на с. 14 в [T] фактически используется, что $\rho \in R$, а это неверно без дополнительных стараний типа леммы 9.4.13 об уплотнении.

можно получить башню расширений, для которой $\varepsilon_{q_k} \in F_k$ *при любом* $k = 1, 2, \ldots, s-1$, *для которого* $q_k > q$. Тогда при $q = 1$ получим башню нормальных расширений. База: $q = \max_k q_k$; в этом случае доказывать нечего. Для доказательства шага индукции возьмём наименьшее k, что $q_k = q$. Если такого k нет, то шаг индукции очевиден. Вставим «между» F_{k-1} и F_k «получение ε_q при помощи корней степени меньше q» из теоремы 9.1.16.а Гаусса о понижении, увеличив «при необходимости» поля $F_k, \ldots, F_s$. Более формально, возьмем башню

$$F_{k-1} \subset G_1 \subset G_2 \subset \ldots \subset G_m \subset F_{k-1}[\varepsilon_q]$$

из теоремы 9.1.16.а Гаусса о понижении. Заменим подбашню $F_{k-1} \subset F_k \ldots \subset F_s$ на подбашню

$$F_{k-1} \subset G_1 \subset G_2 \subset \ldots \subset G_m \subset F_{k-1}[\varepsilon_q] \subset F_k[\varepsilon_q] \subset \ldots \subset F_s[\varepsilon_q].$$

Then, whenever possible, replace each extraction of a root of a composite degree ab by extraction of roots of a-th and b-th degrees. The condition '$\varepsilon_{q_k} \in F_k$ при любом $k = 1, 2, \ldots, s-1$, для которого $q_k \geqslant q$' is preserved, because if $\varepsilon_{ab} \in F_k$, then $\varepsilon_a \in F_k$ and $\varepsilon_b \in F_k$. Далее в новой башне из каждого набора совпадающих соседних полей оставляем только одно. Шаг индукции доказан.

При помощи индукции «вниз» по l покажем, что *из произвольной башни нормальных расширений можно получить башню нормальных расширений, для которой при любом* $k \leqslant s - l$ *выполняются условия*

$$\overline{F}_k = F_k \quad \text{и} \quad \text{либо} \quad r_k \in \mathbb{R}, \quad \text{либо} \quad |r_k|^2 \in F_k.$$

Тогда при $l = 0$ получим утверждение леммы. База: $l = s-1$; в этом случае доказывать нечего. Докажем шаг индукции. (Если $r_k \in \mathbb{R}$, то шаг индукции очевиден, но следующее рассуждение тоже проходит.) Так как $F_k = \overline{F_k}$ и $r_k^{q_k} \in F_k$, то $|r_k|^{2q_k} = r_k^{q_k}\overline{r_k^{q_k}} \in F_k$. Поэтому $F_k[|r_k|^2] = F_k[\sqrt[q_k]{|r_k|^{2q_k}}]$, где берётся вещественное значение корня. Заменим подбашню $F_k \subset F_{k+1} \subset \ldots \subset F_s$ на подбашню

$$F_k \subset F_k[|r_k|^2] \subset F_k[r_k, \overline{r_k}] = F_{k+1}[\overline{r_k}] \subset \ldots \subset F_s[\overline{r_k}].$$

Литература

[Al] *Алексеев В. Б.* Теорема Абеля. М.: Наука, 1976.

[AB] *Akhtyamov D., Bogdanov I.* Solvability of cubic and quartic equations using one radical. `http://arxiv.org/abs/1411.4990`.

[ABG] Solving equations using one radical, presented by D. Akhtyamov, I. Bogdanov, A. Glebov, A. Skopenkov, E. Streltsova and A. Zykin. `http://www.turgor.ru/lktg/2015/4/index.htm`.

[Ar84] *Арнольд В.И.* Обыкновенные дифференциальные уравнения, М. Наука, 1984.

[Ber] *Bergen J.* A Concrete Approach to Abstract Algebra: From the Integers to the Insolvability of the Quintic, 2010.

[BK] *Бурда Ю., Кадец Л.* Семнадцатиугольник и закон взаимности Гаусса // Мат. Просвещение. 2013, № 17.

[Br] J. Brown, Abel and the insolvability of the quintic, `http://www.math.caltech.edu/~jimlb/abel.pdf`.

[Ch] *Чеботарёв Н. Н.* Основы теории Галуа. Часть 1. Л., М.: Гостехиздат, 1934.

[CR] *Курант Р., Роббинс Дж.* Что такое математика. М.: МЦНМО, 2004.

[Dor] *Dörrie H.* 100 Great Problems of Elementary Mathematics: Their History and Solution. New York: Dover Publ, 1965.

[E1] *Edwards H. M.* Galois Theory. Springer Verlag, 1984.

[E2] *Edwards H. M.* The construction of solvable polynomials // Bull. Amer. Math. Soc. 2009. V. 46. P 397–411. Errata: Bull. Amer. Math. Soc. 46 (2009), 703-704.

[ECG] Toward algorithms of solving algebraic equations, presented by A. Enne, A. Chilikov, A. Glebov, A. Skopenkov, B. Vukorepa, `https://www.turgor.ru/lktg/2018/5/index.html`.

[Es] *Esterov A.* Galois theory for general systems of polynomial equations, `https://arxiv.org/abs/1801.08260`

[FT] *Табачников С. Л., Фукс Д. Б.* Математический дивертисмент, М.: МЦНМО, 2011.

[Ga] *Гаусс К. Ф.* Арифметические исследования. Труды по теории чисел. М.: Изд-во АН СССР, 1959. С. 9–580.

[Gi] *Гиндикин С.* Дебют Гаусса // Квант. 1972. № 1. С. 2–11.

[Gi1] *Гиндикин С.* Великое искусство // Квант. 1976. № 9. С. 2–10.

[Had] *Hadlock Ch. R.* Field Theory and its Classical Problems. The Mathematical Association of America, 1978. (Carus Mathematical Monographs, № 19.)

[Ka] *Канунников А. Л.* Начала теории Галуа: разрешимость алгебраических уравнений в радикалах.
`http://www.mathnet.ru/conf1015`.

[Ki] *Кириллов А. А.* О правильных многоугольниках, функции Эйлера и числах Ферма // Квант. 1977. № 7. С. 2–9; 1994. № 6. С. 15–18.

[Kir] *Кириченко В. А.* Построения циркулем и линейкой и теория Галуа.
`http://www.mccme.ru//dubna/2005/courses/kirichenko.html`.

[Ko17] *Коган Е.* Множественная сложность построения правильного многоугольника, `https://arxiv.org/abs/1711.05807`.

[Kol] *Колосов В. А.* Теоремы и задачи алгебры, теории чисел и комбинаторики. М.: Гелиос, 2001.

[KS] *Козлов П.*, *Скопенков А.* В поисках утраченной алгебры: в направлении Гаусса (подборка задач) // Мат. Просвещение. 2008. № 12. С. 127–144;
`http://arxiv.org/abs/0804.4357(v1)`.

[Kh13] *Хованский А. Г.* Построения циркулем и линейкой // Мат. Просвещение. 2013. № 17.

[Ler] *Lerner L.* Galois Theory without abstract algebra.
`http://arxiv.org/abs/1108.4593`.

[Ma] *Манин Ю. И.* О разрешимости задач на построение с помощью циркуля и линейки // В кн.: Энциклопедия элементарной математики. Книга четвёртая (геометрия) / Под редакцией П. С. Александрова, А. И. Маркушевича и А. Я. Хинчина. М.: Физматгиз, 1963.

[Pe] P. Pesic, Abel's Proof, The MIT Press, 2004, Cambridge, Massachusetts, London, England.

[Pos] *Постников М. М.* Теория Галуа. М.: Физматлит, 1963.

[Pr07-2] *Прасолов В. В.* Задачи по алгебре, арифметике и анализу. М.: МЦНМО, 2007.

[PSo] *Прасолов В. В.*, *Соловьев Ю. П.* Эллиптические функции и алгебраические уравнения. М.: Факториал, 1997.

[Ro] M. I. Rosen, Niels Hendrik Abel and Equations of the Fifth Degree, Amer. Math. Monthly, 102:6 (1995) 495-505.

[Saf] *Сафин А.* Программа для построения правильных многоугольников циркулем и линейкой (доклад на ММКШ-2008). `http://www.mccme.ru/mmks/dec08/Safin.pdf`.

[Sk08] *Скопенков А.* Ещё несколько доказательств из Книги: разрешимость и неразрешимость уравнений в радикалах. http://arxiv.org/abs/0804.4357.

[Sk10] *Скопенков А.* Базисные вложения и 13-я проблема Гильберта // Мат. Просвещение. 2010. № 14. С. 143–174; http://arxiv.org/abs/1001.4011.

[Sk11] *Скопенков А.* Простое доказательство теоремы Абеля о неразрешимости уравнений в радикалах // Мат. Просвещение. 2011. № 15. С. 113–126; http://arxiv.org/abs/1102.2100.

[Sk15] *Skopenkov A.* A short elementary proof of the insolvability of the equation of degree 5. http://arxiv.org/abs/1508.03317.

[St94] *Stillwell J.* Galois theory for beginners, Amer. Math. Monthly, 101 (1994), 22-27.

[T] *Тихомиров В. М.* Абель и его великая теорема // Квант. 2003. № 1. С. 11–15.

[Vag] *Вагутен Н.* Сопряжённые числа // Квант. 1980. № 2. С. 26–32.

[Vi] *Винберг Э. Б.* Алгебра многочленов. М.: Просвещение, 1980.

[W] *Ван дер Варден Б. Л.* Алгебра. М.: Наука, 1976.

11 О преподавании

11.1 Олимпиады и математика

To him a thinking man's job was not to deny one reality at the expense of the other, but to include and to connect
U. K. Le Guin. The Dispossessed[22]

Перед школьниками, их учителями и руководителями кружков встаёт вопрос: готовиться к олимпиадам или к «серьёзной» математике? Некоторые думают, что для первого надо прорешивать задачи последних олимпиад, для второго надо читать вузовские учебники, и что ввиду принципиальной разницы первого и второго бессмысленно пытаться достичь и того, и другого. Я придерживаюсь распространённого мнения о том, что эти подходы недостаточно эффективны и приводят к вредным «побочным эффектам»: школьники либо чрезмерно увлекаются *спортивным* элементом в решении задач, либо изучают *язык* математики вместо её содержания[23].

По моему мнению, основу математического образования должно составлять *решение и обсуждение интересных ученику задач, в процессе которых он знакомится с важными математическими идеями и теориями.* Это одновременно подготовит школьника и к математической науке, и к олимпиадам и не нанесёт вред его развитию в целом. Это будет более эффективно и для достижения успеха только в олимпиадах или только в науке (если не учитывать большого количества других факторов, кроме разумной организации занятий).

Как и при естественном развитии самой математики, каждая следующая задача должна быть мотивирована либо практикой, ли-

[22] Для него работой мыслителя было не отрицание одной реальности за счёт другой, а взаимовключение и взаимосвязь. *У. К. Ле Гуин*, «Обделённые» (пер. автора).

[23] Имеется обширная литература, в которой в первую очередь излагается содержание, а язык появляется по ходу дела. Однако часто такая *популярная* литература недооценивается ввиду её «недостаточной серьёзности» по сравнению с учебниками *для университета*. Подробнее см. § 11.2 «Начинать с языка или содержания?».

Кроме того, даже чтение хороших книг без решения задач, как правило, неэффективно.

бо уже решёнными задачами (см. подробнее § 11.2 «Начинать с языка или содержания?» и 11.3 «О необходимости мотивировок»). Ученик, занимающийся «мотивированной для него» математикой (обычно более элементарной, но содержательной и потому сложной) вместо «немотивированной для него» математики (обычно менее элементарной, но языковой и потому тривиальной), имеет преимущество в дальнейшей учёбе и научной работе. А. Н. Колмогоров говорил, что до тридцати лет математику разумнее всего заниматься решением конкретно поставленных задач. А значит, умение решать сложные задачи является одним из важнейших для молодого математика.

Олимпиадных задач очень много; большинство из них интересны школьнику, и среди них много математически содержательных. Такие задачи могут составить основу изучаемого материала. Однако решение олимпиадных задач без изучения математических идей и теорий недостаточно эффективно для подготовки к олимпиадам (на долгих — год и более — промежутках времени, как и вообще решение сиюминутных задач без фундаментального развития). А решение олимпиадных задач *вместе* с изучением стоящих за ними математических идей и теорий более эффективно. Это также позволит по-настоящему разобраться в идеях и теориях.

Кроме того, большинству людей легче достичь успеха на олимпиадах в том случае, когда они не считают успех главной целью. Задачу легче решить, если спокойно думать о самой задаче, а не о награде, которая последует за её решением. Поэтому школьник, мотивированный более высокой целью, чем успех на олимпиаде, имеет на этой олимпиаде психологическое преимущество.

См. также п. 1.2 «Изучение путём решения и обсуждения задач».

11.2 Начинать с языка или содержания?

По моему мнению, именно с *новых идей*, изложенных на уже имеющемся языке, а не с *введения нового языка*, полезно *начинать* изучение любой теории. Удачно представлять основные идеи на «олимпиадных» примерах: на простейших частных случаях, свободных от технических деталей. Как правило, такие идеи наибо-

лее ярко выражаются доказательствами, подобными приведённым в § 9, 10 и других частях этой книги. Имеется много других ярких примеров, упомянем только фейнмановские лекции по физике (там приводятся физические рассуждения, а не доказательства).

«*Мы стараемся свести к минимуму число понятий, откладывая определения до момента, когда они напрашиваются сами собой, и избегая задач на понимание и применение формальных определений (типа „является ли множество целых чисел группой по сложению?“)*»[Shen].

«*При изложении материала нужно ориентироваться на объекты, которые основательнее всего укореняются в человеческой памяти. Это — отнюдь не системы аксиом и не логические приёмы в доказательстве теорем. Изящное решение красивой задачи, формулировка которой ясна и доступна, имеет больше шансов удержаться в памяти студента, нежели абстрактная теория. Скажем больше, именно по такому решению, при наличии некоторой математической культуры, студент впоследствии сможет восстановить теоретический материал. Обратное же, как показывает опыт, практически невозможно*» [Kol, предисловие].

Такой стиль изложения не только делает материал более доступным, но позволяет сильным ученикам (для которых доступно даже абстрактное изложение) приобрести математический вкус и стиль. Это означает разумный выбор проблем для исследования и их мотивировки. Например, математик, понимающий, что теория Галуа мотивируется более важными и более сложными проблемами, чем построимость правильных многоугольников и разрешимость алгебраических уравнений в радикалах, вряд ли станет мотивировать созданную им теорию приложениями, которые можно получить и без его теории. Вкус и стиль означают также ясное изложение собственных открытий, не скрывающее ошибку или известность полученного результата за чрезмерным формализмом. К сожалению, такое — обычно непреднамеренное — сокрытие ошибки часто происходит с математиками, воспитанными на чрезмерно формальных курсах. Происходило это и с автором этих строк; к счастью, все мои серьёзные ошибки исправлялись *перед* публикациями.

Мода на искусственно формализованное изложение привела к сле-

дующему парадоксу. По данному *известному понятию* высшей математики зачастую непросто восстановить *конкретный красивый результат*, для которого это понятие действительно необходимо (и при получении которого это понятие возникло).

Доказательство с использованием некоторого нового термина имеют свои преимущества: оно подготавливает читателя к доказательству тех теорем, которые уже трудно или невозможно доказать без этого термина. Однако такие доказательства, как правило, не должны быть *первыми* доказательствами данного результата (легко себе представить результат *первого* знакомства с теоремой Пифагора на основе понятий векторного пространства и скалярного умножения). Кроме того, при приведении «терминологического» доказательства полезно оговорить его мотивированность не доказываемым результатом, а обучением полезному новому методу. Ну и, конечно, важно соблюсти баланс между доказываемым результатом и уровнем предлагаемой абстракции. Вот пример.

«*Векторное доказательство теоремы Пифагора уже является достаточным основанием для введения понятий векторного пространства и скалярного умножения, хотя эти понятия и не являются необходимыми для доказательства упомянутой теоремы*» (Э. Б. Винберг, из запланированных для публикации дополнений к «Философско-методическому отсуплению» в статье [KS]).

По моему мнению, новое доказательство теоремы Пифагора уместно для мотивировки понятий векторов *на плоскости* и их скалярного произведения. Но для введения понятий векторного пространства и скалярного умножения абстрактных векторов нужны более продвинутые мотивировки.

Приведённая в этом параграфе точка зрения разделяется многими математиками (а некоторыми — нет); я унаследовал её от Ю. П. Соловьёва. Она отражает принцип «путь познания должен повторять путь развития». Конечно, этот принцип не всегда разумно применять буквально. Например, по-видимому, теорема о неразрешимости в вещественных радикалах (п. 9.1.4) была доказана *позже* теоремы Галуа (п. 9.1.4). Однако изучать первую полезно раньше, в качестве ступеньки к более трудной второй. Вот другой пример.

«*Изучение геометрии Лобачевского вовсе не обязательно на-*

чинать с попыток доказать Пятый Постулат. Геометрия Лобачевского для нас сейчас важна, в первую очередь, её приложениями в ТФКП, теории чисел, топологии, теории групп, алгебраической геометрии, космологии и т. д., а вовсе не тем, что она демонстрирует независимость Пятого Постулата от остальных аксиом Евклида. С этой точки зрения более плодотворно её построение не на основе аксиом Евклида—Гильберта, а на основе понятия группы преобразований (Клейн) или римановой метрики (Риман). Аналогично изучение теории Галуа вовсе не обязательно начинать с задачи о решении алгебраического уравнения в радикалах или квадратных радикалах. С современной точки зрения теория Галуа есть теория алгебраических расширений полей, составляющая неотъемлемую часть алгебры и имеющая приложения и аналоги в других разделах математики (алгебраическая геометрия, теория накрытий, теория инвариантов), а решение алгебраических уравнений в радикалах — это маргинальная задача.» (Э. Б. Винберг).

При этом проблема Пятого Постулата доступна и интересна широкому кругу людей (хотя и выглядит далёкой от приложений). А вот формулировки большей части упомянутых приложений, к сожалению, мне не удалось найти в доступной мне начальной учебной литературе по геометрии Лобачевского. См., впрочем статью [PS15] и ссылки в ней. Популяризации геометрии Лобачевского послужила бы дальнейшая публикация чётких формулировок интересных теорем, формулируемых без её понятий, но при попытках доказать которые она естественно возникает. То же справедливо и для теории Галуа, см. последний абзац п. 11.3.2.

См. также [Ro04] и § 11.3 «О необходимости мотивировок».

11.3 О необходимости мотивировок

It startled the well informed by being a new and fantastic idea they had never encountered. It startled the ignorant by being an old and familiar idea they never thought to have seen revived.

G. K. Chesterton. The Man Who Knew Too Much

Благодарю О. Иванова за предоставление некоторых ссылок.

11.3.1 «За» и «против» мотивировок

Решение задачи (неважно, учебной или научной) может прийти не сразу. При размышлении над ним выдвигаются естественные гипотезы, для доказательства которых нужны новые гипотезы, и т. д. В результате может быть построена целая теория. А решение исходной задачи может получиться при доказательстве утверждений, связь которых с исходной задачей неочевидна. В таких случаях разбиение материала на утверждения, каждое из которых легко доказать, доказав только *предыдущие*, нарушает естественную мотивированность изложения (хотя оно необходимо при написании формального доказательства). Однако многие учебники и курсы по «высшей» математике устроены именно так. Формулировки красивых результатов и важных проблем, ради которых была придумана теория, приводятся только *после* продолжительного изучения этой теории (или не приводятся совсем). Это способствует появлению представления о математике как науке, изучающей немотивированные понятия и теории. Такое представление принижает ценность математики.

О необходимости мотивировок говорили классики математики [Kl], [Poi1, гл. 2], [Poi2, с. 455–475].

«*...Обычно определяют группу как множество с двумя операциями, удовлетворяющими набору аксиом вроде* $f(gh) = (fg)h$. *Эти аксиомы автоматически выполняются для групп преобразований. В действительности эти аксиомы означают просто, что группа образована из некоторой группы преобразований забыванием преобразуемого множества. Такие аксиомы, наряду с другими немотивированными определениями, служат математикам главным образом для того, чтобы затруднить непосвящённым овладение своей наукой и тем самым повысить её авторитет*»[24] (В. И. Арнольд) [Ar84, с. 49, комментарий к задаче 5].

[24] Думаю, в последнем предложении несколько сгущены краски. Имеется традиция мотивированного изложения математики. Например, мои собственные попытки вернуть мотивировки в изложение были поддержаны математическим сообществом (по крайней мере, пока я не говорил о необходимости мотивировок явно и не приводил этой цитаты В. И. Арнольда). См. список литературы; для меня было также важно устное поощрение математиков.

Необходимость мотивировок выглядит банальностью. Однако на практике в большинстве курсов и учебников по математике «университетского» уровня либо мотивировок нет, либо приводятся общие слова без ссылок на чёткие формулировки результатов, доступные ученику или неспециалисту, а не скрытые под толщей обозначений и терминов. В тех ситуациях, когда эти общие слова удаётся проверить, они иногда оказываются неадекватными, см. п. 11.3.2. Для разных людей мотивировки разные: для одних новое определение само по себе интересно, а для других необходима его полезность для уже имеющейся математики и её приложений. Подробнее о «естественно-научном» и «философском» аспектах математики см. в [PS15, конец § 2].

О необходимости мотивировок высказываются открыто, а желание их пропустить не осознают или не афишируют. Судить о том, почему мотивированное изложение не принимается, приходится его сторонникам.

«*Часто имеются непреодолимые трудности к мотивированности определений в курсе. Такое изложение требует высокого уровня общематематической подготовки и мотивированности его слушателей (а обычно большая часть слушателей хочет выучить и сдать). Преподавателю часто жалко времени на мотивировку определений...*» (И. С. Рубанов, из письма).

Думаю, большинство математиков согласны с необходимостью мотивировок. Однако трудно понимать, какие утверждения ученику неизвестны, когда преподавателю известно больше. Ещё труднее понимать, какие вещи для ученика не мотивированы его знаниями, когда знаниями преподавателя мотивировано гораздо больше. Тем более что ученик мотивирован не только знаниями, но доверием преподавателю, оценкой, etc. Может быть не только трудно, но даже неприятно посмотреть на материал с точки зрения неспециалиста и осознать немотивированность изложения, особенно привычного, своего или уважаемого автора. Знаю это по собственному опыту. Поэтому часто необходимость мотивировок *вообще* признаётся, но *в данном конкретном случае* находятся причины неприятия мотивированного изложения. Эти причины не продумываются, поскольку продумывание может привести к неприятному осозна-

нию немотивированности. В итоге эти причины легко опровержимы. Возможно, примеры такого рода приведены в п. 11.3.3 и [Or].

Для пользователя (т. е. ученика или коллеги из другой области) важен результат: потратил ли математик время и силы на то, чтобы продумать мотивировки в курсе/учебнике/лекции, поддержать мотивированное изложение и т. д.

См. также § 11.1 «Олимпиады и математика», § 11.2 «Начинать с языка или содержания?» и [PS15].

11.3.2 О мотивировках теории Галуа

Приводимые порой в качестве *основных* приложений теории Галуа теорема Гаусса о правильных многоугольниках [Kir] и теоремы о неразрешимости уравнений в радикалах неубедительны для мотивировки этой теории (так же как приложение к решению квадратных уравнений неубедительно для мотивировки общей теории разрешимости уравнений произвольной степени в радикалах). Действительно, эти теоремы имеют элементарное доказательство, не использующее «группы Галуа». В терминах теории Галуа формулируется общий критерий разрешимости алгебраического уравнения в радикалах. Но этот критерий не даёт настоящего решения проблемы разрешимости, а лишь сводит её к трудной задаче вычисления группы Галуа уравнения. (То, что никакая *другая теория* не даёт лёгкого для применений ответа, не позволяет утверждать, что *теория Галуа* даёт такой ответ.) Но, конечно, формулировка общего критерия в адекватных проблеме терминах может иметь важное философское значение.

При этом проблемы разрешимости уравнений в радикалах доступны и интересны широкому кругу людей. Они связаны с приложениями к символьным вычислениям. Попытка популяризации базовых идей теории Галуа на примере проблем разрешимости уравнений в радикалах предпринята в § 9. Её популяризации послужила бы дальнейшая публикация интересных теорем, формулируемых без её понятий, но при попытках доказать которые она естественно возникает. Примеры таких теорем мне сообщили А. Я. Канель-Белов, С. М. Львовский и Г. Р. Челноков (к сожалению, в доступной мне начальной учебной литературе по теории Галуа мне не удалось

найти такие теоремы, формулировка которых не была бы скрыта под толщей обозначений и терминов).

11.3.3 Почему не принимается мотивированное изложение?

Приведу высказывания о § 10 «Группы», иллюстрирующие написанное в п. 11.3.1.

Данный пункт сложнее остальных. Однако разобраться в парадоксе «против мотивированного изложения никто не выступает, но в основном используется немотивированное» (см. п. 11.3.1) невозможно без детального разбора критики мотивированного изложения на конкретном примере.

Приведённый ниже отзыв на статью [BKS] представлен редколлегией журнала «Математическое Просвещение». Текст этой статьи почти совпадает с § 10 «Группы». Приводятся ссылки на [BKS] и в скобках соответствующие ссылки на § 10. Нумерация моя — для удобства приведенных далее комментариев. Правильность этих комментариев косвенно подтверждается тем, что ответа редколлегии на комментарии не поступило (май 2019). Впрочем, отзыв и комментарии достаточно широко доступны. Поэтому я надеюсь, что многие читатели смогут составить свое собственное мнение о правильности комментариев. Продолжение обсуждения и детали, важные для понимания общей картины, но менее интересные широкому кругу читателей, приведены еще ниже.

Отзыв

13.01.2016

Уважаемые авторы!

Редколлегия сборника «Математическое просвещение» рассмотрела вашу статью «Когда любая группа из N элементов циклическая?» На наш взгляд, тема статьи представляет интерес, но

(1) *избранный вами способ изложения — отказ от использования понятия абстрактной группы и некоторых элементов теории групп — не облегчает, а, наоборот, искусственным образом усложняет понимание доказательства для аудитории сборника.*

(2а) *Опыт общения со школьниками и студентами говорит*

о том, что понятие группы преобразований (и даже композиции преобразований) вовсе не является для них простым.

(2b) *С другой стороны, понятие операции на множестве принципиально не более сложно, чем понятие преобразования.*

(2c) *Рассмотрение лишь групп перестановок усложняет формулировки стандартных теорем теории групп.*

(3) *Вы придумали изощрённое доказательство основной теоремы, не использующее понятий нормальной подгруппы и факторгруппы, теории конечных абелевых групп и теорем Силова, но при этом вы всё же вынуждены ввести понятия порядка элемента, сопряжённых элементов, центра группы, доказать теорему Лагранжа и использовать без доказательства теорему о цикличности мультипликативной группы поля вычетов*

(4) *(которую вы не называете группой из-за обязательства рассматривать только группы преобразований).*

(5) *Изложение материала в виде серии задач, часть из которых может быть решена читателем лишь после знакомства с последующим текстом, также не представляется удачным.*

В связи со сказанным выше редколлегия считает нецелесообразной публикацию вашей статьи в сборнике «Математическое просвещение».

С уважением,

Редакция сборника «Математическое просвещение».

PS. Высказанные в отзыве оценки, касающиеся изложения материала в виде задач и т. д., относятся не к методике как таковой, а к её конкретной реализации в данной статье.

Комментарии к отзыву

10.02.2016

Уважаемая редакция,

Спасибо за труд по написанию отзыва на статью [BKS], который можно опубликовать. Привожу комментарии. Ссылки в скобках — это ссылки на настоящую книгу; ссылки вне скобок — на параграфы и пункты из [BKS].

Резюме

Статья отклонена на основании *неудачности* способа изложения в ней. В замечаниях (3, 4, 7) неясно, что именно неудачно.

В замечаниях (1, 2, 5) эта неудачность не обоснована и не приведены замечания к обоснованию *удачности* приведённого способа изложения в §1 (соответственно в п. 10.1). Подробнее см. ниже. По моему опыту рецензента, в процессе попыток обоснования своего мнения мнение рецензента может меняться, даже на противоположное (поэтому в таких попытках заключается профессионализм рецензента).

Приведённые ниже комментарии к замечаниям приводят к предположению о том, что статья отклонена из-за *мотивированности* изложения (хотя это и отрицается в постскриптуме — возможно, по причинам, приведённым в п. 11.3.1). Ответ редакции, содержащий попытки обоснования замечаний, позволит прояснить ситуацию. Буду рад опубликовать такой ответ — в форме новой версии отзыва или ответа на мои комментарии. Думаю, это обсуждение полезно ввиду важности и сложности реализации мотивированного изложения.

(1,2) Читатель, которому определение абстрактной группы нравится больше группы преобразований, может с этим абстрактным определением и работать. Об этом написано в сноске 6 на с. 3 (соответственно, в п. 10.2.1). Для абстрактных групп ничего в доказательстве основного результата менять не нужно (и ничего упростить не получается). В частности, замечание (2c) неверно.

(2a) В статье не утверждается, что понятие группы преобразований (=перестановок) и композиции преобразований (= перестановок) является простым для школьников и студентов. Напротив, в первом параграфе статьи (соответственно в п. 10.1) написано:

«Заметка может быть интересна читателю... изучавшему перестановки...» «Для понимания доказательства необходим опыт работы с перестановками...»

Обычно в материалах сборника «Математическое просвещение», `http://www.mccme.ru/free-books/matpros.html`, используются не менее продвинутые знания, чем начальные сведения о перестановках, изучаемые на кружках в 7–10 классах (см., например §5 «Перестановки»).

(2b) Что проще — понятие композиции перестановок или операции на произвольном множестве — вопрос спорный. Но основная

сложность понятие группы всё равно не в понятии операции, а в выборе набора её свойств (аксиом). Для того, кто не изучал преобразования, наиболее естественные операции — сложение и умножение натуральных чисел. Для них не выполнено свойство обратного элемента. Выбор набора аксиом группы ясен *начинающему* только после изучения преобразований. Тот же, кто *привык* к понятию группы, может просто не заметить этой главной сложности. Ср. с цитатой из В. И. Арнольда в сноске 5 на с. 2 (в п. 11.3.1). Как, например, в замечании (2b), где более сложное понятие группы подменено более простым понятием операции на множестве.

(3) Замечание является похвалой (вопреки эмоциональному и потому ничего не проясняющему слову «изощрённое»). Действительно, понятия порядка элемента, сопряжённых элементов, центра группы, а также теорема Лагранжа существенно более просты, чем понятие факторгруппы, теория конечных абелевых групп и теорема Силова. (Существование первообразного корня по простому модулю используется во всех доказательствах основной теоремы.)

(4) Мы не называем группой множество вычетов по простому модулю с операцией умножения, поскольку это не нужно для доказательства основного результата. Указанная теорема (о первообразном корне) приведена в статье в элементарной формулировке, не использующей языка абстрактной теории групп. Известно и доказательство этой теоремы, также не использующее языка абстрактной теории групп (см., например, п. 3.5 «Первообразные корни»). В сноске 7 на с. 3 (соответственно в сноске в конце п. 10.2.1) написано:

«Операция умножения на множестве ненулевых вычетов по простому модулю имеет общее обобщение с операцией композиции перестановок. Но для исследовании основного вопроса не нужно понимать этого.»

Многие просто формулируемые факты имеют обобщения (в том числе полезные; в том числе ещё не открытые!). Обобщения порождают наукообразные переформулировки этих фактов или их доказательств. Но это не значит, что тексты, которые не используют и не приводят этих переформулировок, не нужно читать/публиковать (например, что текст о применении теоремы Пифагора плох, если

в нем не сформулировано равенство Парсеваля).

(5) В замечании имеется фактическая ошибка. В § 3 (соответственно в п. 10.3) приведено полное доказательство *не в виде задач*. В п. 1.1 написано

«Заметка... может быть интересна и читателю, знакомому с этими основами [абстрактной теории групп]... Такому читателю может оказаться достаточным прочитать § 3».

«Параграфы 2 и 3 формально независимы друг от друга.»

(Соответственные вещи написаны в п. 10.1.)

Изложение в виде подборки задач, приведённое в § 2 (соответственно в п. 10.2), действительно уменьшает количество читателей, поскольку не создаёт иллюзию понимания. Но книги Пойа, Сегё и Прасолова — общепризнанные хорошие учебники, несмотря на этот «недостаток». Публикации [IKR, IRSe, KS, RS00, RS02, Sk09], [Sk10, § 3], [Sk11, Sk99] гораздо хуже и указанных учебников, и рассматриваемой статьи, поскольку там меньше решений. Но раз они приняты в сборник «Математическое просвещение», а брошюру [Sk09] пришлось дважды переиздать, то, видимо, их достоинство (мотивированное изложение) перевесило недостатки.

Возможно, в замечании (5) имеется в виду, что недостаток — не изложение в виде подборки задач, а то, что часть из них может быть решена читателем лишь после знакомства с последующим текстом. Об этом написано в начале п. 2.1 (соответственно в п. 1.2):

«Если некоторая задача не получается, то читайте дальше» — соседние задачи могут оказаться подсказками.

Эта фраза позволяет читателю преодолевать указанное неудобство. Почему это неудобство необходимо, написано в начале п. 11.3.1. Впрочем, тот, кто не хочет решать задачи, да ещё сформулированные в том порядке, в котором они естественно появляются при решении основной задачи, может читать сразу § 3 (соответственно п. 10.3).

Замечу, что указанный в замечании (5) «недостаток» имеют, например, статьи [IKR, IRSe] из «Математического просвещения» и брошюра [Sk09] (о ней см. выше).

В любом случае это замечание неуместно в списке замечаний, на основании которых статья отклонена, вместо списка предло-

жений по мелкой правке. Поскольку задач, для решения которых нужно знакомство с последующим текстом, немного, и — при наличии аргументированного предложения редколлегии — изменить порядок легко.

(6) Это замечание неуместно в списке замечаний, на основании которых статья отклонена, вместо списка предложений по мелкой правке. В первой фразе статьи явно указывается, что она адресована учащимся и руководителям занятий. По моему мнению, вся она может быть интересна и тем, и другим. Если редколлегия считает, что какая-то часть статьи скорее интересна одним и не интересна другим, то авторы с удовольствием процитировали бы предложенную редколлегией фразу об этом.

(7) Это замечание неуместно в списке замечаний, на основании которых статья отклонена. Статьи в сборнике «Математическое просвещение» не претендуют на научную, а часто и на методическую, новизну. В п. 3.1 (соответственно, в начале п. 10.1) написано «доказательство этой теоремы... не претендует на новизну». (Тем не менее, судя по замечаниям (1, 3, 4, 5), определенная методическая новизна, степень которой неясно зачем устанавливать, в статье есть.)

(PS) Увы, это неверно. Замечания, аналогичные приведённым в отзыве, справедливы по отношению к любому другому мотивированному изложению, в котором общие понятия не вводятся раньше тех проблем, для которых они нужны. В частности, ко многим текстам, уже опубликованным в сборнике «Математическое просвещение». Нужно только сделать очевидные замены терминов, ссылок и т. д. Например, заменить «группы перестановок» и «абстрактные группы» на «эйлерову характеристику двумерной поверхности» и «целочисленный характеристический класс абстрактного двумерного многообразия». Кроме того (PS) противоречит (1), ибо способ изложения и есть методика.

Ваш Аркадий Скопенков.

Другие высказывания

Обсуждение приведено в классической форме диалога: высказывания (о §10 «Группы») выделены италиком, а после них приводятся мои комментарии. Я старался сохранить живость обсужде-

ний; увы, это невозможно сочетать с их академичностью[25].

• *В этом кратком пересказе теории групп на языке групп перестановок предпочтение отдаётся краткости, а не понятности.*

АС: Это не так. Просто для нас *понимание — в первую очередь умение проводить аналогичные (и даже не очень аналогичные) рассуждения, а не умение говорить на языке данной теории.* Соответственно, наша цель другая — в первую очередь понятность идей доказательства и их исполнения, а не философское обсуждение обобщений. Когда уже есть первое, второе также становится важным. Но второго и так в литературе достаточно.

• *Использование «негруппового» языка приводит к тому, что для понимания утверждений и доказательств приходится мысленно делать их «обратный перевод» на язык теории групп. Утверждение «если* $k^q \equiv 1 \bmod m$*, то* k *и* m *взаимно просты» (см. п. 10.3.3, доказательство того, что* $hf = fh$*) требует объяснений. Оно получается применением теоремы Лагранжа к мультипликативной группе кольца вычетов, но сама эта группа (преобразований?) не определяется и не обсуждается.*

АС: Думаю, первое предложение неверно. В §10 все термины используются в общепринятом смысле (кроме термина «группа», но если всюду понимать его в общепринятом смысле, то всё остаётся верным). При наличии конкретных примеров использования «негруппового» языка можно было бы уточнить это замечание и обсуждать уточнённое.

---

[25] Похожие высказывания возникли в ходе обсуждения версии `http://arxiv.org/pdf/1108.5406v2.pdf` статьи [BKS], представленной в 2010 г. в журнал «Математическое просвещение» (высказывались в основном не члены редколлегии). Многие замечания оказались полезны и были учтены. Однако статья была отклонена, поскольку авторы не согласились с предложением редколлегии резко сократить её, рассчитывая изложение только на читателя, уже изучавшего абстрактную теорию групп (мотивировка редколлегии — всё равно статья не будет интересна и доступна для других читателей). Окончательный отзыв, на основании которого статья отклонена, утерян редколлегией.

Я просил, но не получил разрешения опубликовать эти высказывания. Поэтому, вопреки опасению неточно переформулировать чужие мысли, я привожу *свои* представления о высказываниях. Они основаны на многих устных обсуждениях и указанном предварительном обсуждении, но ни одно из них не совпадает с высказыванием из того предварительного обсуждения.

Указанное в замечании утверждение следует из того, что 1 делится на $\gcd(k, m)$. Значит, ни теорема Лагранжа, ни понятия мультипликативной группы кольца вычетов, ни понятие группы для доказательства не нужны. См. последний абзац комментария к замечанию (4) в предыдущем подпункте.

Возможно, дело в следующем. При решении более сложных задач вместо «$a^{-1}xa$» иногда полезно думать «образ элемента x при автоморфизме сопряжения элементом a». Человеку, специализирующемуся на таких задачах, элементарный язык действительно может мешать. А начинающему, напротив, мешает «теорема Лагранжа для мультипликативной группы кольца вычетов» вместо «очевидное свойство делимости целых чисел».

• *Профессиональный математик разберётся в математическом содержании и подберёт методику, нужную для обсуждения этого материала в своём кружке.*

АС: Это означает, что никакая методическая литература вообще не нужна. Думаю, это не так. Профессионализм в математике и в преподавании — разные (хотя и коррелирующие) вещи. Многим профессиональным математикам будет полезен пример методики, нужной для обсуждения материала в кружке. А если они ещё и в преподавании разбираются, то смогут оценить, какой огромный труд нужен для подбора методики, т. е. для написания доступного ученикам изложения классического результата.

• *У* §10 *две цели*:

1) *изложить красивый факт из теории групп для возможно более широкого круга читателей и* 2) *показать подход к изложению теории групп, идущему от конкретного к абстрактному, а не наоборот.*

АС: Не совсем так. Мотивировка решением интересной проблемы более существенна, чем мотивировка обобщением имеющихся примеров (не дающим решения интересной проблемы). Так считали математики до XX века, так же считают многие современные математики и студенты.

Солидаризуясь с обеими целями, с сожалением должен констатировать, что обе цели не достигнуты. Я полностью согласен с тем, что непродуктивно начинать изучение теории групп

с определения абстрактной группы. Но так начинают только дуболомы. Умные преподаватели сначала рассматривают конкретные примеры интересных множеств преобразований, а также группы остатков, обнаруживают между ними связь, создают мотивацию к поиску общего и только тогда вводят понятие группы, закрепляя *его определением. То же самое касается и понятия циклической группы. Простой же заменой абстрактной группы на подгруппу группы перестановок проблема* восхождения *учащегося к понятию группы не решается.*

АС: Этого и не написано в § 10. Проблема *восхождения* не может решаться никаким одним приёмом. Параграф предназначен быть лишь ступенькой в восхождении.

• *Мне кажется, что* § 10 *практически недоступен учителям, школьникам и т. д.* (*не имеющим алгебраической культуры на уровне* 1 *курса мехмата МГУ*). *Формально текст, может, и проходим, но у читателя, который неуверенно владеет достаточно большим набором средств теории групп, трудности будут на каждом шагу. Текст изобилует пробелами* (*например, не объясняется, почему построенные примеры групп не циклические*), *и восполнить их можно только* понимая *теорию групп.*

АС: Да, пробелы есть. Но как раз при решении задач (в частности, восполнении пробелов) рождается понимание теории и уверенное владение её средствами. Подробнее см. п. 10.1. Конечно, простота заполнения пробелов определяет широту круга читателей.

• *Читателю предлагается читать решения? Тогда непонятно, зачем нужно дробить текст на неестественные порции «условия» и «решения», а не написать всё вместе.*

АС: Это дробление естественное, поскольку читателю предлагается читать решения *после* того, как он подумал над задачей и, возможно, решил её. См. комментарий к замечанию (5) в предыдущем подпункте и п. 1.2 «Изучение путем решения и обсуждения задач».

• *Разве есть учителя и старшеклассники, не знакомые с абстрактной теорией групп, но изучавшие перестановки и теорию чисел?*

АС: Конечно, есть! Ибо разумная последовательность изучения,

которой многие придерживаются, — абстрактная теория групп *после* перестановок и теории чисел (причём не сразу, а с перерывом на многочлены и комплекные числа, геометрические преобразования и разрешимость в радикалах). См. начало § 5 «Перестановки».

• *Если уж школьнику рассказали про перестановки и теоретико- числовые теоремы с групповой подоплёкой, как после этого удержаться и не изложить основные понятия теории групп?*

АС: Конечно, нужно изложить! Но важно именно *после* и *для решения интересных задач.* Такому изложению и посвящён § 10, см. п. 10.1.

• *Я возражаю против цитаты из В. И. Арнольда, дискредитирующей абстрактную теорию групп. Сама постановка основного вопроса, а также приводимое доказательство, где авторы вынуждены вводить некоторые понятия этой теории, опровергают тезис, что только группы преобразований имеют право на существование.*

АС: По-моему, указанного тезиса в цитате нет. Цитата дискредитирует не абстрактную теорию групп, а немотивированное изложение.

• *Для читателей, не знакомых с теорией групп, постановка вопроса не мотивирована.*

АС: Не согласен, см. конец п. 10.2.1.

• *§ 10 по своему содержанию рассчитан на профессионального математика.*

АС: Не согласен. Поскольку в высказывании не приводится обоснование, я констатирую различие мнений и также не привожу обоснования.

11.4 Кружки и олимпиады как путь в математику и как спорт. *А. Я. Канель-Белов, А. И. Буфетов*

11.4.1 Введение

Внешкольные занятия математикой, которым посвящена находящаяся в руках у читателя книга, играют в математическом образовании в нашей стране важнейшую роль, которую трудно переоценить. При этом значительное число занятий так или иначе оказываются связанными с олимпиадами. Школьников и их учителей часто сводят вместе математические олимпиады (например, в 1993 году А. Я. был членом жюри московской олимпиады, а девятиклассник А. И. участником — так мы и познакомились).

Многие школьники, особенно на периферии, получают математическое образование, нацеленное в первую очередь на подготовку к олимпиадам. С этим необходимо считаться научным руководителям и организаторам учебного процесса. Даже те, кто не занимается подготовкой к олимпиадам в тренерском смысле этого слова, активно используют идеи и задачный материал олимпиад.

У истоков олимпиадного движения стояли великие ученые, однако позже олимпиадный мир стал жить собственной жизнью. По всему миру проводятся математические конкурсы и олимпиады. Появились специалисты по их проведению, возникла олимпиадная математика со своей методикой работы и своей литературой. С некоторой долей условности можно сказать, что в олимпиадном мире сложились две ценностные ориентации: «научная» и «спортивная». Эти различные взгляды на олимпиады проявляются в подборе задач, выработке критериев оценок, в кадровых вопросах, в организации математических лагерей.

В нашей заметке мы кратко противопоставляем эти подходы.

11.4.2 Спортивный подход

Несколько сгущая краски, попробуем передать спортивный подход фразой: «олимпиада — это спорт по решению головоломок». Такая ориентация влечет за собой многое: усиливается тренерство, ужесточаются формальные требования и, соответственно, критерии оценок. Так, если спортсмен переступит черту на 10 см, а прыгнет

на 10 метров, ему не зачтут прыжок 9,9 м, его прыжок не зачтут вовсе. Аналогично на описку учащегося, исходя из ориентации на спорт, можно реагировать так: «А если бы в ведомости на зарплату описка была?»

При таком подходе математическая значимость задачи отходит на второй план. Комбинируется всё со всем. Важны внешний блеск, необычность условия. Вот примеры такого рода задач.

1. *Можно ли расставить числа от* 1 *до* 100 *в ряд так, чтобы сумма любых трех чисел, идущих подряд, была простым числом?*

2. *Стороны треугольника — простые числа. Может ли его площадь быть целым числом?*

В этих двух задачах простота числа не возникает, на наш взгляд, естественно.

Вот ещё один пример.

3. *Найдите все целые числа, равные сумме факториалов своих цифр.*

Мы не видим в этой задаче математического содержания.

Большой спорт тяготеет к ограничению поля деятельности и четкой формализации правил. Отсюда вытекает, на наш взгляд, сужение тематики задач. На одном математическом фестивале С. С. Анисовым была предложена задача на нахождение угла между диагоналями правильного додекаэдра. Идея решения состояла в рассмотрении вписанного куба. Задача была отвергнута жюри фестиваля как «неолимпиадная». Между тем сообразительный школьник, даже не имеющий специальной подготовки, может, нам представляется, увидеть куб, вписанный в додекаэдр. Тренированный на «стандартные» олимпиадные сюжеты «спортсмен» не имеет тут преимущества.

С другой стороны, многие задачи, например, на построение инвариантов, могут быть решены только учащимися, хорошо владеющими этой техникой, которая, к сожалению, даже намеками не входит в школьный курс.

Взгляд на математику как на науку о решении занимательных задач и головоломок — самый доступный. Совершенно естественно, что он получает распространение. Он может быть очень полезен

при первоначальном знакомстве с математикой, а следовательно, и в преподавании. Олимпиадный тренер спортивного толка может много сделать для развития образования в своем регионе.

Глубина понимания без узости объекта изучения сразу не достигается. С этим связан подростковый экстремизм в духе «ничего мне не нужно, кроме геометрии». Лучше вначале достичь глубины и потом искать широты.

11.4.3 Олимпиада как путь в математику

Девиз другой олимпиадной идеологии: *преподавание и олимпиады должны отражать науку*. Этой идеологии следовали всесоюзные олимпиады и старые олимпиады во многих странах.

Олимпиада – это, в частности, полигон для отработки новых тем и сюжетов (см. задачник «Кванта», особенно в 1970-е–80-е годы). В современных олимпиадах эта идеология в наиболее чистом виде присутствует в Турнире городов, особенно на его летних конференциях [KoFr, LK], и на Московской олимпиаде.

При таком подходе естественность постановки задачи — ключевое соображение, в соответствии с представлением, что неестественная трудная задача на олимпиаде портит вкус и наносит вред участникам. Жюри опирается на своё чувство естественного.

Чаще всего хорошая олимпиадная задача получается путем оформления идей и сюжетов из науки. Реже возникает новый сюжет в элементарной математике.

Для такого подхода характерно отношение к спорту – как к средству побудить подростка выложиться, достичь глубины, изучить технику. Соображения, уважающие содержание, имеют приоритет над спортивными.

Математик, занимающийся большой проблемой, ищет связанные с ней задачи, где предполагаемые идеи решения работают в более простой ситуации. Трудно придумать несколько идей сразу – нужны промежуточные этапы, поэтому ценятся *продвижения* школьников в задаче.

История нашей науки больше интересуется блестящими идеями, чем второстепенными неточностями первопроходцев. Именно

поэтому мы считаем, например, что теория Галуа принадлежит Галуа.[26]

Такой подход можно переносить и на олимпиадное творчество. Академические ценности имеют фундаментальное значение для воспитания будущих ученых. Практически, это означает, среди прочего, что олимпиадная работа проверяется существенно мягче, чем принято, скажем, на вступительном экзамене, а наличие у школьника идеи играет более важную роль, чем строгость и точность её оформления.

В заключение приведём примеры олимпиадных задач, которые могут, на наш взгляд, открыть новые двери молодому математику.

1. *Поезд ехал один час от пункта A в пункт B, проехав* 60 *км. Докажите, что в какой-то момент его ускорение было не менее* 240 *км/ч*^{2} (В. М. Тихомиров).

Эта красивая и нетривиальная задача с простой и естественной формулировкой даёт, на наш взгляд, блестящую иллюстрацию основ исчисления бесконечно малых.

2. *Плоскость покрыта единичными кругами. Докажите, что некоторая точка покрыта не менее трех раз* (А. Я. Канель-Белов).

Вторая задача отражает в простейшей форме фундаментальное понятие *топологической размерности*. Напомним, что топологическое пространство имеет *размерность* n, когда (неформально говоря) существуют сколь угодно мелкие покрытия его окрестностями без перекрытий по $n+2$, но нельзя избавиться от перекрытий по $n+1$.

3. *Ломаная делит круг на две равные части. Докажите, что она проходит через его центр* (А. К. Ковальджи).

Стиль решения этой задачи непривычен для олимпиадника. Тут дело вовсе не в трюке. Надо осознать, что значит *две равные части.*

[26] *Замечание А. Скопенкова.* Вопрос о том, что относить к идеям, а что — к второстепенным неточностям, сложный. Например, одна из важнейших идей доказательства неразрешимости в радикалах и теории Галуа (посмотреть, как меняется степень симметричности многочлена при извлечении радикала) присутствовала уже у Руффини. Однако мы не считаем, что Галуа и Абель исправили второстепенные неточности блестящих идей Руффини и не называем теорему о неразрешимости в радикалах теоремой Руффини, а теорию Галуа теорией Руффини.

Это значит, что *есть движение, переводящее одну часть в другую*. А все типы движений плоскости описаны в теореме Шаля. Далее следует небольшой перебор. (Подробнее см. «Математическое просвещение», сер. 3, вып. 6, 2002. С. 139–140.)

Современные исследования отражаются и в вариантах международных олимпиад последних лет. (Далее цифры означают год олимпиады и номер задачи в варианте.) Приведём два примера, связанных с современной комбинаторикой.

2014.6, Герхард Вегингер, Австрия. Говорят, что прямые на плоскости находятся в общем положении, если никакие две из них не параллельны и никакие три из них не проходят через одну точку. Любые несколько прямых общего положения разбивают плоскость на части; ограниченными частями разбиения будем называть те из частей, которые имеют конечную площадь. Докажите, что для всех достаточно больших n в каждом множестве из n прямых общего положения можно покрасить не менее $\sqrt{n}$ прямых в синий цвет так, чтобы граница никакой из ограниченных частей разбиения не была полностью синей.

Замечание: за доказательство утверждения задачи, в котором $\sqrt{n}$ заменено на $c\sqrt{n}$, будут начисляться баллы, в зависимости от константы c.

Эта задача возникла из исследования [BCC], связанного с проблемами Эрдёша—Секереша и Сильвестра—Каллаи.

2012.3, Дэвид Артур, Канада. Два игрока A и B играют в игру Угадай-ка. Правила этой игры зависят от двух положительных целых чисел k и n, и эти числа известны обоим игрокам. В начале игры игрок A выбирает такие целые числа x и N, что $1 \leqslant x \leqslant N$. Он держит число x в секрете, а число N честно сообщает игроку B. После этого игрок B пытается получить информацию о числе x, задавая игроку A вопросы следующего типа: за один вопрос игрок B указывает по своему усмотрению множество S, состоящее из целых положительных чисел (возможно, это множество уже было указано в одном из предыдущих вопросов), и спрашивает игрока A, принадлежит ли число x множеству S. Игрок B может задавать столько вопросов, сколько он хочет. На каждый вопрос игрока B игрок A должен сразу ответить «да» или «нет», при этом ему разрешается

Глава 1

Геометрия

В этой главе, если задачу можно решать разными методами, она приводится в пункте, посвящённом одному из них, а о возможности других решений говорится в комментарии. Помимо обозначений, принятых во всей книге, в данной главе везде, где не оговорено обратное, используются принятые в геометрии обозначения элементов треугольника, описанные в начале параграфа «Треугольник».

12 Треугольник

Всюду в данной главе, кроме специально оговорённых случаев, используются следующие обозначения: ABC — данный треугольник, A_i, B_i, C_i, $i = 1, 2, \ldots,$ — точки на сторонах BC,CA и AB соответственно (или на продолжениях этих сторон, если это оговорено в условии задачи); ω — вписанная окружность, I — её центр, r — её радиус; Ω — описанная окружность, O — её центр, R — её радиус; G — точка пересечения медиан (центр тяжести, центроид), H — точка пересечения высот (ортоцентр). Проведём биссектрисы AI, BI, CI до пересечения с Ω в точках A', B', C' соответственно. Таким образом, A', B', C' — середины дуг AB, BC, CA. *Ортотреугольник* — треугольник с вершинами в основаниях высот, *серединный треугольник* — треугольник с вершинами в серединах сторон данного треугольника. Перпендикуляр, опущенный из точки A на BC, обозначается $h(A, BC)$.

Окружностью ABC называется окружность, описанная вокруг треугольника ABC.

12.1 Принцип Карно (1). *В. Ю. Протасов, А. А. Гаврилюк*

12.1.1. Теорема Карно. В точках A_1, B_1, C_1, лежащих на сторонах треугольника ABC или на их продолжениях, восставлены перпендикуляры к этим сторонам. Докажите, что они пересекаются в одной точке тогда и только тогда, когда

$$C_1A^2 - C_1B^2 + A_1B^2 - A_1C^2 + B_1C^2 - B_1A^2 = 0.$$

12.1.2. Сформулируйте и докажите обобщённую теорему Карно для произвольных точек плоскости A_1, B_1, C_1, не обязательно лежащих на прямых, содержащих стороны треугольника ABC.

12.1.3.° В каком из следующих случаев перпендикуляры, восставленные к сторонам треугольника в указанных точках, могут не пересекаться в одной точке:

1) A_1, B_1, C_1 — точки касания сторон с вписанной окружностью;

2) A_2, B_2, C_2 — точки касания сторон с соответствующими вневписанными окружностями;

3) A_3, B_3, C_3 — основания биссектрис треугольника?

12.1.4. На плоскости даны три пересекающиеся окружности. Докажите, что три их общие хорды пересекаются в одной точке.

Примечание. Это утверждение обычно доказывают, используя понятие степени точки (см. п. 13.4). Однако его легко вывести и из обобщённой теоремы Карно.

12.1.5. Пользуясь принципом Карно, получите ещё одно доказательство теоремы о пересечении трёх высот треугольника.

12.1.6. Охарактеризуйте все треугольники, у которых перпендикуляры к сторонам, восставленные в точках пересечения сторон с биссектрисами противоположных углов, пересекаются в одной точке.

12.3.8. В вершинах остроугольного треугольника проведены касательные к его описанной окружности. Докажите, что центр описанной окружности треугольника, образованного этими тремя касательными, лежит на прямой Эйлера исходного треугольника.

Указания, ответы и решения

12.3.3. Угол C должен быть острым, так как в противном случае точки O и H лежат по разные стороны от AB. Так как расстояние от O до AB равно $R\cos C$, а высота, проведённая из вершины C, равна $AC\sin A = 2R\sin A\sin B$, параллельность прямой Эйлера и прямой AB равносильна равенству $3\cos C = 2\sin A\sin B$. Учитывая, что $\cos C = -\cos(A+B) = \sin A\sin B - \cos A\cos B$, получаем утверждение задачи.

12.3.6. Из условия следует, что степени точки O относительно этих окружностей равны R^2. Кроме того, если AA' и BB' — высоты треугольника, то четырёхугольник $ABA'B'$ вписанный, и, значит, $HA\cdot HA' = HB\cdot HB'$. Поэтому степени точки H относительно всех трёх окружностей также равны, т. е. прямая OH является их общей радикальной осью.

12.4 Формула Карно (2*). *А. Д. Блинков*

Формула Карно (по имени французского математика, физика и политического деятеля Лазаря Карно, 1753–1823) утверждает, что в остроугольном треугольнике сумма расстояний от центра описанной окружности до сторон треугольника равняется сумме радиусов описанной и вписанной окружностей, т. е. $OM_1+OM_2+OM_3 = R+r$, где M_1, M_2, M_3 — середины BC, CA, AB соответственно. Её доказательство с помощью теоремы Птолемея приводится в п. 13.6 «Теоремы Птолемея и Кези». Здесь мы рассмотрим её применения и ещё один способ её доказательства, в процессе которого будут получены другие важные факты.

12.4.1. Пусть биссектриса угла A пересекает окружность, описанную около треугольника ABC, в точке W, а точка D диаметрально противоположна точке W. Докажите, что

(a) $M_1W = (r_a - r)/2$;

(b) $M_1D = (r_b + r_c)/2$, где r, r_a, r_b, r_c — радиусы вписанной и вневписанных окружностей.

12.4.2. Докажите формулу Карно.

Рассмотрим теперь несколько задач на применение формулы Карно. Если явно не оговорено обратное, то треугольник, заданный в условии, остроугольный.

12.4.3. Докажите, что сумма расстояний от вершин треугольника до ортоцентра равна сумме диаметров его вписанной и описанной окружностей.

12.4.4. Докажите, что в треугольнике ABC выполняются неравенства

(a) $AH + BH + CH \leqslant 3R$;

(b) $3OH \geqslant R - 2r$.

12.4.5. (a) Докажите, что $m_a + m_b + m_c \leqslant \frac{9}{2}R$, где m_a, m_b и m_c — длины медиан треугольника.

(b) Пусть в треугольнике ABC биссектрисы углов A, B и C пересекают описанную окружность в точках W_1, W_2 и W_3 соответственно. Докажите, что $AW_1 + BW_2 + CW_3 \leqslant 6{,}5R - r$.

12.4.6. (a) Докажите, что для углов треугольника выполняется неравенство

$$\frac{3r}{R} \leqslant \cos A + \cos B + \cos C \leqslant \frac{3}{2}.$$

(b) Пусть AH_1, BH_2 и CH_3 — высоты треугольника ABC. Выразите сумму диаметров окружностей, описанных около треугольников AH_2H_3, BH_1H_3 и CH_1H_2, через R и r.

12.4.7. В окружность радиуса R вписан треугольник, а в каждый сегмент, ограниченный стороной треугольника и меньшей из дуг окружности, вписана окружность наибольшего возможного радиуса. Найдите сумму диаметров трёх получившихся окружностей и радиуса окружности, вписанной в треугольник.

12.4.8. (a) Докажите, что в треугольнике ABC выполняется равенство

$$a(OM_2 + OM_3) + b(OM_1 + OM_3) + c(OM_1 + OM_2) = 2pR.$$

(b) **Неравенство Эрдёша.** Пусть h_a — наибольшая высота треугольника ABC. Докажите, что $h_a \geqslant R + r$.

12.4.9. (a) Выведите аналоги формулы Карно для прямоугольного и тупоугольного треугольников.

(b) Четырёхугольник $ABCD$ вписанный. Пусть r_1 и r_2 — радиусы окружностей, вписанных в треугольники ABC и ADC, а r_3 и r_4 — радиусы окружностей, вписанных в треугольники ABD и CBD. Докажите, что $r_1 + r_2 = r_3 + r_4$.

12.4.10. Пусть d, d_1, d_2 и d_3 — расстояния от центра O окружности, описанной около треугольника, до центров его вписанной и вневписанных окружностей. Докажите, что

$$R^2 = \frac{d^2 + d_1^2 + d_2^2 + d_3^2}{12}.$$

12.4.11. (a) Докажите, что если точка принадлежит отрезку, соединяющему основания двух биссектрис треугольника, то сумма расстояний от этой точки до двух сторон треугольника равна расстоянию от неё до третьей стороны.

(b) Пусть центр окружности, описанной около треугольника, лежит на отрезке, соединяющем основания двух биссектрис. Докажите, что расстояние от ортоцентра треугольника до одной из его вершин равно $R + r$.

Указания, ответы и решения

12.4.1. (a) Пусть точки I и I_a соответственно — центры вписанной окружности и вневписанной окружности, касающейся стороны BC, K и P — точки касания этих окружностей с BC, L — точка пересечения I_aP с прямой, проходящей через I и параллельной BC, Q — середина IL. Так как W — середина отрезка II_a (следствие из теоремы о трезубце, см. задачу 12.7.3 п. 12.7 «Биссектрисы, высоты

12.8 «Полувписанная» окружность (3*). *П. А. Кожевников*

Пусть A' и A'' — середины дуг BC описанной окружности Ω, соответственно не содержащей и содержащей точку A; B' и B'', C' и C'' определяются аналогично.

Рассмотрим окружность S_A (назовём её *полувписанной*), касающуюся сторон AB, AC и окружности Ω (внутренним образом). Основными в этой серии являются следующие факты:

— прямая, проходящая через точки касания полувписанной окружности со сторонами, содержит точку I;

— точка касания полувписанной окружности с окружностью Ω лежит на прямой $A''I$.

Основная серия-1

Докажите следующие утверждения.

12.8.1. Пусть перпендикуляр к биссектрисе AI, проведённый через точку I, пересекает AB и AC в точках K и L соответственно. Тогда окружности BKI, CLI и Ω пересекаются в одной точке T.

12.8.2. Точки T, I, A'' лежат на одной прямой.

12.8.3. Точки T, K, C' лежат на одной прямой.

12.8.4. Точки K, L и T являются точками касания окружности S_A с прямыми AB, AC и окружностью Ω.

12.8.5. (a) Прямая CC' касается окружности $TBKI$.

(b) Точка T — центр поворотной гомотетии, переводящей треугольник BKI в треугольник ILC.

Основная серия-2

12.8.6. Прямая AT проходит через центр гомотетии с положительным коэффициентом, переводящей окружность ω в Ω.

12.8.7. Пусть A_1 и A_2 — точки касания вписанной и вневписанной окружностей со стороной BC соответственно. Тогда

(a) AA' — биссектриса угла TAA_2;
(b) $\angle BTA_1 = \angle ABC$. (*Задача* 4.7.7 *из* [GZ].)

12.8.8. Пусть AT пересекает KL в точке Z. Тогда $\angle BZK = \angle CZL$. (*Задача* 4.7.5 *из* [GZ].)

12.8.9. Прямые KL, TA' и BC пересекаются в одной точке или параллельны. (*И. Шарыгин.*)

12.8.10. Точка пересечения Y_A из предыдущей задачи и точки Y_B, Y_C, определённые аналогичным образом, лежат на одной прямой.

Дополнительные задачи-1

12.8.11. Пусть P — произвольная точка на дуге $BA'C$.

(a) Пусть $P_b = BB' \cap PC'$, $P_c = CC' \cap PB'$. Тогда окружность PP_bP_c проходит через T. ([Za14], *задача* 8.8, 2013 *г.*)

(b) Пусть J_b и J_c — центры вписанных окружностей треугольников PAB и PAC. Тогда окружность PJ_bJ_c проходит через T. (*Задача* 4.7.9 *из* [GZ].)

(c) Пусть касательные к ω из точки P пересекают BC в точках U_1 и U_2. Тогда окружность PU_1U_2 проходит через T. (*Задача* 4.7.10 *из* [GZ].)

(d) Пусть прямые, проходящие через I параллельно биссектрисам углов между прямыми AP и BC пересекают прямую BC в точках V_1 и V_2 Тогда окружность PV_1V_2 проходит через T. (*См. частный случай задачи* 4.7.18 *из* [GZ].)

Дополнительные задачи-2

Следующие задачи — про «обобщённые полувписанные» окружности, т. е. окружности, касающиеся двух прямых и окружности.

12.8.12. Пусть D — точка на стороне AC треугольника ABC, и пусть S_1 — окружность, касающаяся окружности Ω внутренним образом в точке R, а также отрезков BD и AD в точках M и N соответственно.

(a) Докажите, что точки B, M, I, R лежат на одной окружности.

(b) **Лемма Саваямы.** Прямая MN проходит через центр I вписанной окружности ω треугольника ABC.

12.8.13. Пусть D — точка на отрезке AC треугольника ABC; S_1 — окружность, касающаяся отрезков BD и AD, а также окружности Ω внутренним образом; S_2 — окружность, касающаяся отрезков BD и CD, а также окружности Ω внутренним образом.

(a) **Теорема Тебо.** Линия центров окружностей S_1 и S_2 проходит через I.

(b) Докажите, что окружности S_1 и S_2 равны тогда и только тогда, когда $D = B_2$.

12.8.14. Найдите аналоги предложенных задач для «полувписанных» и «обобщённых полувписанных» окружностей, касающихся Ω внешним образом.

Указания, ответы и решения

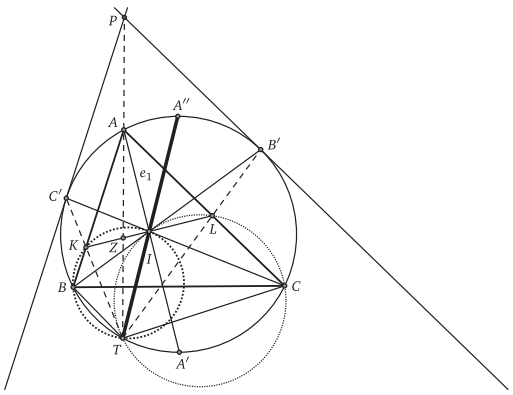

Рис. 1.5:

12.8.1. Это частный случай следующего известного факта: если точки X', Y', Z' лежат на прямых YZ, ZX, XY соответственно, то окружности $XY'Z'$, $YZ'X'$, $ZX'Y'$ проходят через одну точку. В данном случае точки B, C, I лежат на прямых, содержащих стороны треугольника AKL, следовательно, окружности BKI, CLI и ABC пересекаются в одной точке.

12.8.2. Из окружностей $TBKI, TCLI$ получаем (см. рис. 1.5), что $\angle BTI = \angle AKI = \angle ALI = \angle CTI$. Это означает, что TI — биссектриса угла BTC, поэтому TI проходит через середину дуги A''.

12.8.14. *Комментарий.* Есть «алгебраические» причины, по которым, например, вписанная и вневписанная окружности обладают похожими свойствами. Уравнение окружности, касающейся трёх данных прямых, — это уравнение либо вписанной, либо одной из вневписанных окружностей, разница лишь в геометрическом расположении. Поэтому факты для вписанной окружности зачастую имеют своего «близнеца» для вневписанной окружности.

12.9 Обобщённая теорема Наполеона (2*). *П. А. Кожевников*

Классическая теорема Наполеона гласит, что центры правильных треугольников, построенных на сторонах произвольного треугольника вне его, являются вершинами равностороннего треугольника.

Теорема Наполеона является частным случаем утверждения задачи 16.1.7, п. «Комплексные числа и геометрия». В этом пункте мы докажем другое обобщение теоремы Наполеона.

Предлагаем для решения серию задач, внешне не имеющих никакой связи с теоремой Наполеона. Можно решать задачи любыми методами, а затем познакомиться с обобщением теоремы Наполеона и получить решения задач как следствия этого сильного факта.

Вводные задачи

12.9.1. Докажите, что центры квадратов, построенных на сторонах параллелограмма вне его, являются вершинами квадрата.

12.9.2. На боковых сторонах трапеции $ABCD$ построены треугольники ABE и CDF так, что $AE \parallel CF$ и $BE \parallel DF$. Докажите, что если E лежит на стороне CD, то F лежит на стороне AB.

12.9.3. (а) Две окружности пересекаются в точках A и B. Через точку A проведена прямая, вторично пересекающая первую окружность в точке C, а вторую — в точке D (можно считать, что точки C и D лежат по разные стороны от точки A). Пусть M и N — середины дуг BC и BD, не содержащих точку A, а K — середина отрезка

Формулировка и доказательство обобщённой теоремы Наполеона

Через $\angle(\vec{a},\vec{b})$ будем обозначать угол поворота от вектора $\vec{a}\neq\overrightarrow{0}$ до вектора $\vec{b}\neq\overrightarrow{0}$, отсчитываемый против часовой стрелки. Этот угол определён с точностью до прибавления $2\pi k$, $k\in\mathbb{Z}$. Например, равенство $\angle(\vec{a},\vec{b})\equiv 0 \pmod{2\pi}$ означает, что $\angle(\vec{a},\vec{b})=2k\pi$ для некоторого $k\in\mathbb{Z}$.

12.9.9.* Обобщённая теорема Наполеона. Пусть на сторонах треугольника ABC построены такие треугольники (возможно, вырожденные) BCA_1, CAB_1, ABC_1, что выполнены следующие условия:

1) $\angle(\overrightarrow{A_1B},\overrightarrow{A_1C})+\angle(\overrightarrow{B_1C},\overrightarrow{B_1A})+\angle(\overrightarrow{C_1A},\overrightarrow{C_1B})\equiv 0 \pmod{2\pi}$;

2) $AB_1\cdot BC_1\cdot CA_1=BA_1\cdot CB_1\cdot AC_1$.

Тогда углы треугольника $A_1B_1C_1$ находятся из равенств

$$\angle(\overrightarrow{A_1C_1},\overrightarrow{A_1B_1})\equiv\angle(\overrightarrow{BC_1},\overrightarrow{BA})+\angle(\overrightarrow{CA},\overrightarrow{CB_1}) \pmod{2\pi};$$
$$\angle(\overrightarrow{B_1A_1},\overrightarrow{B_1C_1})\equiv\angle(\overrightarrow{CA_1},\overrightarrow{CB})+\angle(\overrightarrow{AB},\overrightarrow{AC_1}) \pmod{2\pi};$$
$$\angle(\overrightarrow{C_1B_1},\overrightarrow{C_1A_1})\equiv\angle(\overrightarrow{AB_1},\overrightarrow{AC})+\angle(\overrightarrow{BC},\overrightarrow{BA_1}) \pmod{2\pi}.$$

Примечание. В теореме предполагается, что точка A_1 отлична от B, C, B_1, C_1 и т. д. Однако допускается, что вершины каких-то из треугольников BCA_1, CAB_1, ABC_1 и $A_1B_1C_1$ лежат на одной прямой. В этом случае говорят, что соответствующий треугольник является вырожденным, а его углы считают равными (с точностью до 2π) 0, 0 и π.

Таким образом, в теореме утверждается, что при выполнении условий 1 и 2 углы треугольника $A_1B_1C_1$ зависят лишь от углов треугольников, построенных на сторонах треугольника ABC, и не зависят от углов самого треугольника ABC. Условие теоремы может быть описано также таким изящным образом (см. [Bel]): пусть даны точки M,N,P,T и на сторонах треугольника ABC строятся треугольники ABC_1, BCA_1, CAB_1, подобные с сохранением ориентации соответственно треугольникам MNT, NPT, PMT. Действительно, выполнение условий 1 и 2 в этом случае проверяется непосредственно. С другой стороны, если треугольники ABC_1,

13.6 Теоремы Птолемея и Кези (3*). *А. Д. Блинков, А. А. Заславский*

13.6.1 Теорема Птолемея

13.6.1. (a) Докажите, что для любых четырёх различных точек A, B, C, D выполнено *неравенство Птолемея*

$$AB \cdot CD + AD \cdot BC \geqslant AC \cdot BD.$$

(b) **Теорема Птолемея.** Это неравенство обращается в равенство тогда и только тогда, когда $ABCD$ — вписанный четырёхугольник.

13.6.2. В остроугольном треугольнике ABC обозначим $|BC| = a$, $|AC| = b$. Найдите $|AB|$, если радиус окружности, описанной около $\triangle ABC$, равен R.

13.6.3. Биссектриса угла A треугольника ABC пересекает описанную около него окружность в точке W.

(a) Выразите отношение AW/IW, где I — центр окружности, вписанной в треугольник ABC, через длины сторон треугольника.

(b) Докажите, что $AW > \frac{AB+AC}{2}$.

13.6.4. На гипотенузе AB прямоугольного треугольника ABC во внешнюю сторону построен квадрат, O — его центр. Найдите $|OC|$, если a и b — катеты треугольника.

13.6.5. Дан правильный треугольник ABC и точка P.

(a) Докажите, что если точка P лежит на описанной около треугольника окружности, то расстояние от неё до одной из вершин треугольника равно сумме расстояний до двух других вершин.

(b) **Теорема Помпейю**. Для любой точки P, не лежащей на описанной окружности, из отрезков PA, PB, PC можно составить треугольник.

13.6.6. Сумма расстояний от точки X, выбранной вне квадрата, до двух его ближайших соседних вершин равна m. Найдите наибольшее значение суммы расстояний от X до двух других вершин квадрата.

13.6.7. Точки M и N — середины диагоналей AC и BD вписанного четырёхугольника $ABCD$. Известно, что $\angle ABD = \angle MBC$. Докажите, что $\angle BCA = \angle NCD$. (*Кубок Колмогорова*, 1999 *г.*)

13.6.8. (a) Точки A, B, C и D — четыре последовательные вершины правильного семиугольника. Докажите, что $\frac{1}{AB} = \frac{1}{AC} + \frac{1}{AD}$.

(b) Докажите, что $\frac{1}{\sin(\pi/7)} = \frac{1}{\sin(2\pi/7)} + \frac{1}{\sin(3\pi/7)}$.

13.6.9. В выпуклом шестиугольнике $ABCDEF$ известно, что $AB = BC = a$, $CD = DE = b$, $EF = FA = c$. Докажите, что $\frac{a}{BE} + \frac{b}{AD} + \frac{c}{CF} \geqslant \frac{3}{2}$.

13.6.10. Стороны вписанного четырёхугольника равны a, b, c, d. Найдите его диагонали.

13.6.11. Выведите из теоремы Птолемея формулу Карно (см. п. 12.4 «Формула Карно»).

13.6.2 Теорема Кези

13.6.12. Обобщённая теорема Птолемея, или теорема Кези. (a) Даны четыре непересекающихся круга, ограниченных окружностями α, β, γ, δ. Докажите, что окружность, касающаяся их внешним образом, или прямая, касающаяся их всех так, что круги лежат относительно неё в одной полуплоскости, существует тогда и только тогда, когда

$$l_{\alpha\beta}l_{\gamma\delta} + l_{\alpha\delta}l_{\beta\gamma} = l_{\alpha\gamma}l_{\beta\delta},$$

где $l_{\alpha\beta}$ — длина общей внешней касательной к окружностям α, β и т. д.

(b) Сформулируйте теорему Кези для случая, когда искомая окружность касается некоторых из данных окружностей внутренним образом.

13.6.13. Сформулируйте утверждение, аналогичное теореме Кези, для случая, когда

(a) одна;

(b) две из данных окружностей вырождаются в прямые;

(c) какие-то из данных окружностей вырождаются в точки.

13.6.14. Пусть на сторонах AC и BC треугольника ABC взяты такие точки X, Y, что $XY \parallel AB$. Докажите, что существует окружность, проходящая через X, Y и касающаяся одинаковым образом вневписанных окружностей треугольника, вписанных в углы A и B.

13.6.15. Докажите **теорему Фейербаха**: окружность, проходящая через середины сторон треугольника, касается его вписанной и вневписанных окружностей.

13.6.16. Докажите, что три окружности, каждая из которых касается внутренним образом одной из вневписанных окружностей треугольника и внешним образом двух других, пересекаются в одной точке.

13.6.17. Даны две окружности, лежащие одна вне другой. Произвольная окружность, касающаяся их одинаковым образом, пересекает одну из их общих внутренних касательных в точках A и A', а другую — в точках B и B'. Докажите, что среди прямых AB, AB', $A'B$, $A'B'$ найдутся две, параллельные общим внешним касательным к данным окружностям.

13.6.18. Даны две концентрические окружности a_1 и a_2. Каждая из окружностей b_1 и b_2 касается внешним образом окружности a_1 и внутренним — a_2, а каждая из окружностей c_1 и c_2 касается внутренним образом обеих окружностей a_1 и a_2. Оказалось, что окружности b_1, b_2 пересекают c_1, c_2 в восьми точках. Докажите, что эти точки лежат на двух окружностях или прямых, отличных от b_1, b_2, c_1, c_2. (*В. Протасов*, III *Олимпиада им. И. Ф. Шарыгина.*)

Указания, ответы и решения

13.6.1. Сделайте инверсию с центром A и воспользуйтесь утверждениями задач 14.10.2, 14.10.5. Заметим, что неравенство Птолемея верно даже для точек, не лежащих в одной плоскости.

13.6.2. *Ответ*: $\frac{a\sqrt{4R^2-b^2}+b\sqrt{4R^2-a^2}}{2R}$.

Проведите диаметр CD и примените к полученному четырёхугольнику теорему Птолемея.

14 Геометрические преобразования

В данном параграфе задачи расположены так, чтобы сначала новые понятия (геометрических преобразований) использовались для решения интересных задач, формулируемых без этих понятий, и только потом эти новые (но уже мотивированные) понятия изучались сами по себе.

Подробнее о геометрических преобразованиях см., например, [Za03] (теорема Шаля — § 1.2, подобие и гомотетия — § 1.3, аффинные преобразования — гл. 2, проективные преобразования — гл. 3, инверсия — гл. 4, комплексная интерпретация движений и подобий — § 6.1, комплексная интерпретация инверсии — § 6.2), [Pr95] и [Ya75].

14.1 Применения движений. (1) *А. Д. Блинков*

Поворотом вокруг точки O на угол φ называется преобразование плоскости, оставляющее точку O на месте и переводящее любую отличную от O точку X в такую точку X', что $|OX| = OX'$ и ориентированный угол между векторами $\overrightarrow{OX}$ и $\overrightarrow{OX'}$ равен φ. Поворот на 180° называется *центральной симметрией*.

Параллельным переносом на вектор $\overrightarrow{m}$ называется преобразование плоскости, переводящее любую точку X в такую точку X', что $\overrightarrow{XX'} = \overrightarrow{m}$.

Осевой симметрией относительно прямой l называется преобразование плоскости, переводящее любую точку X в такую точку X', что $XX' \perp l$ и точки X, X' лежат по разные стороны от прямой l и равноудалены от неё.

14.1.1.° Параллелограмм имеет ровно четыре оси симметрии. Какое из следующих утверждений верно?

1) это прямоугольник, отличный от квадрата;
2) это ромб, отличный от квадрата;
3) это квадрат;
4) такого параллелограмма не существует.

14.1.2.° Треугольник имеет центр симметрии. Какое из следующих утверждений верно?

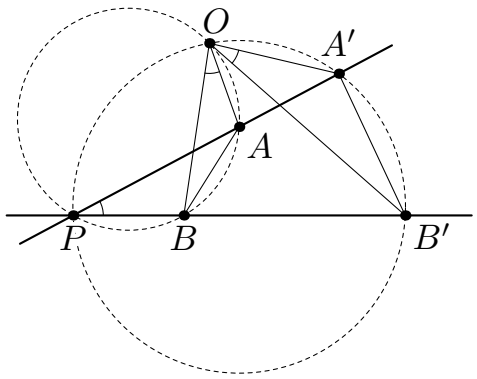

Рис. 1.41:

Это означает, что существует поворотная гомотетия, переводящая отрезок AA' в $[BB']$, причём O — её центр.

Пусть P — точка пересечения данных прямых, а α — угол между ними. Так как при поворотной гомотетии с центром O образом точки A является точка B, отрезок AB должен быть «виден» из точки O под углом α. Следовательно, O лежит на дуге окружности, описанной около треугольника APB. Аналогично отрезок $A'B'$ должен быть «виден» из точки O под углом α, значит, точка O лежит на дуге окружности, описанной около треугольника $A'PB'$. Таким образом, O — вторая точка пересечения этих окружностей.

Если построенные окружности касаются, значит, обе точки проходят через P одновременно. В этом случае точка P сама будет искомой.

14.5 Поворотная гомотетия (2). *П. А. Кожевников*

14.5.1 Вводные задачи: немного о велосипедистах

14.5.1. По двум окружностям, пересекающимся в точках P и Q, одновременно начали движение из точки P по часовой стрелке с равными угловыми скоростями два велосипедиста A и B.

(a) Докажите, что прямая AB всё время проходит через Q.

(b) Докажите, что треугольники PAB всё время подобны друг другу и треугольнику PO_1O_2, где O_1 и O_2 — центры окружностей.

(c) Найдите ГМТ (траекторию движения) середин отрезков AB; центров вписанных окружностей треугольников PAB; любых соот-

ветственных точек подобных треугольников PAB.

(d) **Задача о велосипедистах.** Докажите, что A и B всё время равноудалены от фиксированной точки. (См. [VSh].)

14.5.2. По трём окружностям, имеющим общую точку O и попарно различные точки пересечения P, Q и R, одновременно начали движение из точки O по часовой стрелке с равными угловыми скоростями три велосипедиста A, B и C.

(a) Докажите, что все треугольники ABC подобны между собой и треугольнику $O_1O_2O_3$, где O_1, O_2 и O_3 — центры окружностей.

(b) Какова траектория движения центра масс треугольника ABC?

14.5.3. Два велосипедиста P и Q едут равномерно по двум прямым, пересекающимся в точке O.

(a) Найдите траекторию середины отрезка PQ.

(b) Докажите, что если скорости велосипедистов равны, то середина дуги (одной из дуг) PQ окружности OPQ неподвижна.

(c) Докажите, что если велосипедисты проходят O не одновременно, то окружности OPQ имеют вторую общую точку, отличную от O.

14.5.4. Дан фиксированный треугольник ABC. По прямым BC, CA, AB едут соответственно велосипедисты P, Q, R так, что углы между RP и PQ, PQ и QR, QR и RP фиксированные.

(a) Докажите, что точка пересечения окружностей RAQ, RBP, PCQ неподвижна.

(b) Найдите ГМТ центров вписанных окружностей треугольников PQR.

14.5.2 Основные задачи

14.5.5. Три велосипедиста P, Q и R едут равномерно по трём прямым. Известно, что в некоторые два момента времени треугольник PQR был подобен с сохранением ориентации фиксированному треугольнику XYZ. Докажите, что это условие будет выполняться в любой момент времени.

14.5.6. В треугольник ABC вписан подобный ему треугольник PQR ($P \in BC$, $Q \in CA$, $R \in AB$, $\angle P = \angle A$, $\angle Q = \angle B$, $\angle R = \angle C$).

(a) Докажите, что центр описанной окружности треугольника ABC совпадает с ортоцентром треугольника PQR.

(b) Найдите максимальное значение выражения $\frac{S_{ABC}}{S_{PQR}}$.

(c) Докажите, что центр описанной окружности треугольника PQR равноудалён от центра описанной окружности и ортоцентра треугольника ABC.

14.5.7. Через вершины треугольника ABC проводятся три произвольные параллельные прямые d_a, d_b, d_c. Прямые d'_a, d'_b, d'_c, симметричные d_a, d_b, d_c относительно BC, CA, AB соответственно, образуют треугольник XYZ. Найдите геометрическое место центров вписанных окружностей таких треугольников.

14.5.8. Дан выпуклый четырёхугольник $ABCD$, стороны BC и AD которого равны, но не параллельны. Пусть E и F — внутренние точки отрезков BC и AD соответственно, удовлетворяющие условию $BE = DF$. Прямые AC и BD пересекаются в точке P, прямые BD и EF пересекаются в точке Q, прямые EF и AC пересекаются в точке R. Докажите, что для всевозможных способов выбора точек E, F окружности PQR имеют общую точку, отличную от P. (См. [IMO], 2005 г.)

14.5.9. Пусть O и I — центры описанной и вписанной окружностей треугольника ABC соответственно. Точки D, E и F выбраны на сторонах BC, CA и AB соответственно так, что $BD + BF = CA$ и $CD + CE = AB$. Описанные окружности треугольников BDF и CDE пересекаются в точках D и P. Докажите, что $OP = OI$. (См. [IMO], 2012 г.)

14.5.3 Дополнительные задачи

14.5.10. Впишите в данный остроугольный треугольник равносторонний треугольник с минимальной стороной.

14.5.11. На пол положили правильный треугольник ABC, выпиленный из фанеры. В пол вбили три гвоздя (по одному вплотную к каждой стороне треугольника) так, что треугольник невозможно повернуть, не отрывая от пола. Первый гвоздь делит сторону AB

в отношении $1:3$, считая от вершины A, а второй делит сторону BC в отношении $2:1$, считая от вершины B. В каком отношении делит сторону AC третий гвоздь? (*Московская математическая олимпиада* 1998 *г.*)

14.5.12. Выпуклый многоугольник M можно поместить в треугольник T. Докажите, что это можно сделать так, чтобы одна из сторон многоугольника M лежала на стороне треугольника T.

Поворотной гомотетией называют преобразование $H_O^{k,\varphi} := H_O^k \circ R_O^\varphi$.

14.5.13. (a) Окружности α и β пересекаются в точках A и B. Пусть H — поворотная гомотетия с центром в точке A, переводящая α в β. Докажите, что для любой точки $X \in \alpha$ точка $H(X)$ получена пересечением прямой BX с окружностью β. (См. [Pr95, 19.27].)

(b) Окружности $S_1, \ldots, S_n$ проходят через точку O. Кузнечик из точки $X_i \in S_i$ прыгает в точку $X_{i+1} \in S_{i+1}$ так, что прямая X_iX_{i+1} проходит через вторую точку пересечения окружностей S_i и S_{i+1}. Докажите, что после n прыжков (с S_1 на $S_2, \ldots,$ с S_n на S_1) кузнечик вернётся в исходную точку. (См. [Pr95, 19.28].)

(c) Пусть концы отрезков AB и CD попарно различны, а P — точка пересечения прямых AB и CD. Центром поворотной гомотетии, переводящей AB в CD, является (отличная от P) точка пересечения описанных окружностей треугольников ACP и BDP. (См. [Pr95, 19.41 (б)].)

Указания, ответы и решения

14.5.1. (a) Из равенства угловых скоростей следует, что $\angle(PQ, QA) = \angle(PQ, QB)$.

(b) Угол $\angle(BA, AP) = \angle(QA, AP)$ постоянный и равен $\angle(O_2O_1, O_1P)$.

(c) Если M — середина AB, то $\angle(QM, MP)$ постоянный, поэтому M движется по окружности Γ, проходящей через P и Q.

Пусть N — любая точка треугольника PAB (в некоторый фиксированный момент). Рассмотрим поворотную гомотетию (см. определение перед задачей 14.5.13) с центром P, переводящую A в N.

15.3 Полярное соответствие (2). *А. А. Гаврилюк, П. А. Кожевников*

Традиционно при изучении полярного соответствия существенно используются свойства проективных преобразований. Мы же делаем попытку познакомиться с полярным соответствием и применением его свойств без привлечения проективной геометрии.

Введём нужные нам определения и обозначения. Пусть на плоскости фиксированы точка O и окружность ω радиуса R с центром в O.

Для каждой точки $X \neq O$ на луче OX строим такую точку X', что $OX \cdot OX' = R^2$. (Говорят, что X' и X *инверсны* относительно окружности ω.) Через точку X' проведём прямую x, перпендикулярную OX'. Прямая x называется *полярой* точки X, а точка X называется *полюсом* прямой x. Соответствие $X \leftrightarrow x$ является взаимно однозначным соответствием между точками, отличными от O, и прямыми, не проходящими через O. Это соответствие и называется *полярным соответствием*.

Ниже мы обозначаем точки, отличные от O (полюсы), большими латинскими буквами, а их поляры — соответствующими маленькими буквами: $A \leftrightarrow a$, $B \leftrightarrow b$, $C \leftrightarrow c$, ...

Основные свойства и вводные задачи

Установите два основных *свойства полярного соответствия.*

П1. Двойственность. Включение $A \in b$ выполняется тогда и только тогда $B \in a$, т. е. поляра любой точки является геометрическим местом полюсов проходящих через неё прямых.

П2.* Пусть две прямые m и l, проходящие через произвольную точку $A \notin \omega$, пересекают ω в точках M_1, M_2 и L_1, L_2. Тогда $M_1L_1 \cap M_2L_2 \in a$ или $M_1L_1 \parallel M_2L_2 \parallel a$.

Докажите следующие факты.

В1. Если $A \in \omega$, то a — это касательная к ω, проведённая через A.

В2. Если точка A расположена вне окружности ω, то a проходит через точки касания с ω касательных, проведённых через A.

B3. Если O, A, B не лежат на одной прямой, то $a \cap b \leftrightarrow AB$.

B4. Точки A, B, C лежат на одной прямой тогда и только тогда, когда a, b, c проходят через одну точку или параллельны.

Основные задачи

15.3.1.° Даны окружность и её хорда AB. Где лежит точка пересечения поляр точек A и B?

1) внутри окружности; 2) вне окружности; 3) на окружности.

15.3.2.° Пусть C — середина хорды AB. Тогда поляра точки C

1) параллельна AB;
2) перпендикулярна AB;
3) касается окружности.

15.3.3.° При полярном соответствии относительно вписанной окружности треугольник переходит

1) в серединный треугольник;
2) в ортотреугольник;
3) в треугольник, образованный точками касания сторон с вписанной окружностью.

15.3.4. Даны окружность ω и прямая l, не имеющие общих точек. Из точки X, которая движется по прямой l, проводятся касательные XA, XB к ω. Докажите, что все хорды AB имеют общую точку.

15.3.5. Симметричная бабочка. (a) Дана точка A на диаметре BC полуокружности ω. Точки X, Y на ω таковы, что $\angle XAB = \angle YAC$. Докажите, что прямые XY проходят через одну точку или параллельны.

(b) Точки A и A' инверсны относительно окружности ω, причём точка A' расположена внутри ω. Через A' проводятся хорды XY. Докажите, что центры вписанной и одной из вневписанных окружностей треугольника AXY фиксированны. (*С. Маркелов, см.* [Sh97].)

15.3.6. Основное свойство симедианы. Касательные к описанной окружности треугольника ABC, проведённые через точки B

и C, пересекаются в точке P. Докажите, что AP — симедиана (т. е. прямая, симметричная медиане AM относительно биссектрисы угла A).

15.3.7. Гармонический четырёхугольник. Пусть четырёхугольник $ABCD$ вписан в окружность ω. Известно, что касательные к ω, проведённые в точках A и C, пересекаются на прямой BD или параллельны BD. Докажите, что касательные к ω, проведённые в точках B и D, пересекаются на прямой AC или параллельны AC.

В следующих трёх задачах дан четырёхугольник $ABCD$, у которого диагонали пересекаются в точке P, продолжения сторон AB и CD — в точке R, продолжения сторон BC и DA — в точке Q.

15.3.8. Вписанный четырёхугольник. Пусть четырёхугольник $ABCD$ вписан в окружность с центром O. Докажите, что четвёрка точек O, P, Q, R ортоцентрическая (т. е. каждая точка является ортоцентром треугольника с вершинами в оставшихся трёх точках).

15.3.9. Описанный четырёхугольник. Пусть четырёхугольник $ABCD$ описан около окружности; K, L, M, N — точки касания с окружностью сторон AB, BC, CD, DA соответственно; прямые KL и MN пересекаются в точке S, а прямые LM и NK — в точке T.

(a) Докажите, что точки Q, R, S, T лежат на одной прямой.

(b) Докажите, что KM и LN пересекаются в точке P.

15.3.10. Вписанно-описанный четырёхугольник. Четырёхугольник $ABCD$ описан около окружности ω с центром I и вписан в окружность Ω с центром O.

(a) Докажите, что O, I, P лежат на одной прямой.

(b) Зафиксируем ω и Ω и рассмотрим всевозможные четырёхугольники $ABCD$, описанные около окружности ω и вписанные в окружность Ω. Докажите, что для всех таких четырёхугольников точки P совпадают, а также что прямые QR совпадают.

Комментарий. Согласно теореме Понселе если существует хотя бы один четырёхугольник, описанный около окружности ω и вписанный в окружность Ω, то существует бесконечно много таких четырёхугольников.

16.1 Комплексные числа и элементарная геометрия.

Пусть на плоскости задана система координат. Тогда комплексному числу $z = x + yi$ соответствует точка плоскости Z с координатами (x, y). При этом модуль числа z равен расстоянию от Z до начала координат O, а аргумент равен ориентированному углу между положительным направлением оси Ox и вектором $\overrightarrow{OZ}$, т. е. углу, на который надо повернуть против часовой стрелки ось Ox, чтобы совместить её положительное направление с направлением вектора $\overrightarrow{OZ}$. Оси Ox и Oy называют *действительной* и *мнимой* осями.

16.1.1. (Загадка.) Выясните геометрический смысл сложения комплексных чисел.

16.1.2. (a) Каким геометрическим преобразованием комплексной плоскости получается число iz из числа z?

(b) (Загадка.) Обозначим $e^{i\varphi} := \cos\varphi + i\sin\varphi$. Каков геометрический смысл умножения на $e^{i\varphi}$? А на $re^{i\varphi}$, где r — вещественное число (см. определение тригонометрической формы комплексного числа в п.4.5

(c) Выразите число w, полученное из числа z поворотом на угол φ против часовой стрелки относительно центра z_0, через z, z_0 и φ.

(d) Докажите, что композиция поворотов плоскости (с различными центрами) — поворот или параллельный перенос.

(e) Докажите, что точки z_1, z_2, z_3 лежат на одной прямой тогда и только тогда, когда отношение $(z_3 - z_1)/(z_2 - z_1)$ вещественно.

Комментарий. Задача 16.1.2 (b) легко решается с помощью тригонометрических формул сложения. Однако можно поступить наоборот: решить эту задачу геометрически, доказать, что при умножении комплексных чисел их модули перемножаются, а аргументы складываются, а затем, используя этот результат, получить доказательство формул сложения, не требующее перебора различных случаев.

16.1.3.° Какое преобразование плоскости задаётся формулой $z \mapsto 2z + 2$?

Теперь воспользуемся тем, что аффинное преобразование однозначно определяется образами трёх точек, не лежащих на одной прямой. Пусть точки 0, 1 и i переходят в z_0, z_1, z_2 соответственно. Тогда данное преобразование задаётся формулой требуемого вида, в которой $c = z_0$, $a = (z_1 + z_2 - 2z_0)/2$, $b = (z_1 - z_2)/2$. Из того, что z_0, z_1, z_2 не лежат на одной прямой, следует, что $|a| \neq |b|$.

16.1.7. Пусть $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Тогда точки $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ являются вершинами правильного n-угольника. Согласно предыдущей задаче можно считать, что вершинами данного многоугольника являются точки $a\varepsilon^k + b\varepsilon^{-k}, k = 0, 1, \ldots, n-1$. Значит, центр k-го правильного n-угольника z_k удовлетворяет равенству $a\varepsilon^{k+1} + b\varepsilon^{-k-1} - z_k = \varepsilon(a\varepsilon^k + b\varepsilon^{-k} - z_k)$. Отсюда легко получить, что z_k образуют геометрическую прогрессию с знаменателем ε, т. е. являются вершинами правильного n-угольника.

16.2 Комплексные числа и круговые преобразования.

Преобразование круговой плоскости, сохраняющее обобщённые окружности, называется *круговым*. Произвольное отличное от подобия круговое преобразование может быть представлено как композиция инверсии и движения.

16.2.1.° Четвёрка комплексных чисел z_1, z_2, z_3, z_4 удовлетворяет равенству $\frac{(z_1-z_3)(z_2-z_4)}{(z_1-z_4)(z_2-z_3)} = 2$. Что можно сказать о четвёрке точек плоскости, соответствующих числам z_1, z_2, z_3, z_4?

1) Они являются вершинами параллелограмма.

2) Они лежат на одной прямой или на одной окружности.

3) Площадь треугольника $0z_1z_2$ равна площади треугольника $0z_3z_4$ (точка 0 — начало координат).

16.2.2. Докажите, что преобразование комплексной плоскости является круговым тогда и только тогда, когда оно задаётся дробно-линейной функцией вида $f(z) = (az + b)/(cz + d)$ или $f(z) = (a\bar{z} + b)/(c\bar{z} + d)$, где $ad - bc \neq 0$.

16.2.3. Докажите, что для любых шести различных точек A, B, C, A', B', C' существует ровно два круговых преобразования, переводящих A в A', B в B', C в C'.

Двойным отношением четырёх комплексных чисел a, b, c, d, где $a \neq d$, $b \neq c$, называется комплексное число $(a, b, c, d) = \frac{(a-c)(b-d)}{(a-d)(b-c)}$.

16.2.4. Докажите, что для данных восьми различных точек A, B, C, D; A', B', C', D' круговое преобразование, переводящее A в A', B в B', C в C', D в D', существует тогда и только тогда, когда для соответствующих комплексных чисел выполняется равенство $(a, b, c, d) = (a', b', c', d')$ или $\overline{(a, b, c, d)} = (a', b', c', d')$.

16.2.5. Даны два треугольника ABC и $A'B'C'$. Докажите, что существует инверсия, переводящая треугольник ABC в треугольник, равный $A'B'C'$.

16.2.6. Дан четырёхугольник $ABCD$. Докажите, что существует инверсия, переводящая его вершины в вершины параллелограмма, причём все параллелограммы, полученные в результате таких инверсий, подобны.

См. также задачу 14.10.4 (c) п. «Инверсия».

Дополнительные задачи

16.2.7. (a) Пусть a, b, c — комплексные числа, соответствующие не лежащим на одной прямой точкам A, B, C; $f(z) = (z-a)(z-b)(z-c)$. Докажите, что две точки, соответствующие корням производной $f'(z)$, изогонально сопряжены относительно треугольника ABC.

(b)* *Эллипсом Штейнера* треугольника ABC называется эллипс наибольшей площади, лежащий внутри треугольника. Докажите, что фокусы эллипса Штейнера соответствуют корням производной $f'(z)$.

16.2.8. Пусть a, b, c — комплексные числа, соответствующие точкам A, B, C, причём $|a| = |b| = |c| = 1$. Докажите, что точки Z_1, Z_2 изогонально сопряжены относительно треугольника ABC тогда и только тогда, когда соответствующие комплексные числа удовлетворяют соотношению

$$z_1 + z_2 + abc\bar{z_1}\bar{z_2} = a + b + c.$$

сторонах четырёхугольника, проходящий через середины его диагоналей, за исключением концов.

Для параллелограмма ответ очевиден.

Пусть P и Q — середины диагоналей AC и BD данного четырёхугольника, отличного от параллелограмма (см. рис. 1.54 *б*). Тогда $S_{ABP} + S_{CDP} = S_{ABQ} + S_{CDQ} = S_{ABCD}/2$.

Если точка M лежит внутри $ABCD$ на PQ, то $S_{APM} = S_{CPM}$ (так как точки A и C равноудалены от PM) и $S_{BPM} = S_{DPM}$ (так как точки B и D равноудалены от PM). Таким образом, $S_{ABM} + S_{CDM} = S_{ABP} + S_{CDP} + S_{APM} + S_{BPM} - S_{CPM} - S_{DPM} = S_{ABP} + S_{CDP} = S_{ABCD}/2 = S_{ADM} + S_{BCM}$.

Если точка M не лежит на указанном отрезке, то, действуя аналогично, проверяем, что указанное в условии равенство не выполняется.

17.3 Построения. Ящик инструментов (2). *А. А. Гаврилюк*

При изучении материала этого раздела желательно знакомство с § 13 «Окружность» и рекомендованной в нем литературой.

17.3.1. (a) Даны две параллельные прямые, на одной из которых дан отрезок. С помощью одной линейки разделите его пополам.

(b) Даны две параллельные прямые, на одной из которых дан отрезок. С помощью одной линейки удвойте его.

(c) Даны две параллельные прямые, на одной из которых дан отрезок. С помощью одной линейки разделите его на n равных частей.

Ср. с задачей 14.9.5 п. «Центральная проекция и проективные преобразования".

17.3.2. Даны окружность ω, её диаметр AB и точка X. С помощью одной линейки постройте перпендикуляр из точки X на AB, если точка X лежит

(a) не на окружности; (b) на окружности.

17.3.3. Даны окружность ω и точка X. С помощью одной линейки постройте (все возможные) касательные, проведённые из точки X к окружности, если точка X лежит

(a) вне окружности; (b) на окружности.

17.3.4. При помощи только циркуля постройте образ данной точки X при инверсии относительно данной окружности ω.

17.3.5. Дана окружность на плоскости. С помощью двусторонней линейки постройте её центр. (С помощью двусторонней линейки можно проводить прямую через две точки, проводить прямую, параллельную проведённой ранее прямой и отстоящую от неё на расстояние, равное ширине линейки, а также проводить через две точки, расстояние между которыми не меньше ширины линейки, две параллельные прямые, расстояние между которыми равно ширине линейки.)

17.3.6. Даны прямая l и отрезок OA, ей параллельный. С помощью двусторонней линейки постройте точки пересечения прямой l с окружностью радиуса OA и с центром в точке O.

17.3.7. При помощи только циркуля постройте окружность, проходящую через три данные точки.

17.3.8. Задача Аполлония. Постройте окружность, касающуюся трёх данных, при помощи циркуля и линейки.

В последующих задачах этого пункта *построением* будем называть некоторую последовательность следующих элементарных операций:

— с помощью линейки провести прямую через две данные или ранее построенные точки;

— с помощью циркуля построить окружность с центром A и радиусом BC, где A, B, C — данные или ранее построенные точки;

— найти точки пересечения двух данных или ранее построенных линий (прямых или окружностей).

В последующих теоремах никакие другие операции не разрешаются (в отличие от предыдущих задач, где разрешена, например, операция «взять произвольную точку уже построенного множества»). В частности, если изначально не даны хотя бы две точки, ничего построить нельзя.

17.3.9.* **Теорема.** Отрезок длины a можно построить циркулем и линейкой, имея отрезок длины 1, тогда и только тогда, когда число a можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений квадратных корней из положительных чисел.

17.3.10.* **Теорема** (Мор—Маскерони). Любое построение, осуществимое циркулем и линейкой, можно осуществить одним циркулем (прямая считается построенной, если построены две различные лежащие на ней точки, см. [Fu87]).

17.3.11.* **Теорема** (Штейнер). Любое построение, осуществимое циркулем и линейкой, можно осуществить одной линейкой, если начерчена одна окружность и отмечен её центр (окружность считается построенной, если построены её центр и лежащая на ней точка, см. [Smo]).

Следующая задача предназначена для закрепления материала.

17.3.12.° Пользуясь теоремами Мора—Маскерони и Штейнера, определите, какие инструменты необходимы для построения центра данной окружности.

1) циркуль и линейка; 2) только линейка; 3) только циркуль.

Указания, ответы и решения

17.3.1. (a) Пусть AB — данный отрезок. Возьмём точку X вне полосы, ограниченной данными прямыми, и найдём точки C и D пересечения прямых XA и XB с прямой, отличной от AB. Пусть Y — точка пересечения диагоналей трапеции $ABCD$. Тогда прямая XY делит основания трапеции пополам.

(b) Возьмите на другой прямой произвольный отрезок и разделите его пополам.

(c) Возьмите на другой прямой произвольный отрезок и, повторив несколько раз предыдущее построение, увеличьте его в n раз.

17.3.2. Если прямые XA, XB вторично пересекают окружность в точках B', A', то точка пересечения прямых AA' и BB' — ортоцентр треугольника XAB.

[fest] Шесть фестивалей (материалы Российских фестивалей юных математиков). Краснодар: ГИНМЦ, 1996.

[Fu87] *Фукс Д.* Построения одним циркулем // Квант. 1987. №7. С. 34–37.

[Smo] *Смогоржевский А. С.* Линейка в геометрических построениях. М.: Гостехиздат, 1956.

18 Стереометрия

Чужбина так же сродственна отчизне,
Как тупику соседствует пространство.

И. Бродский.

18.1 Задачи на пространственное воображение *М. А. Корчемкина, И. А. Пушкарев*

Задачи о траекториях придуманы по мотивам [Do, SE], а многие задачи о фигурах из кубиков — по мотивам [Ag], см. также [R].

18.1.1 Фигуры из кубиков

Будем рассматривать три (ортогональные) проекции пространственной фигуры — вид спереди, сверху и справа (см. пример на рис. 1.56).

18.1.1. Существует ли фигура, не являющаяся кубом, проекция которой на каждую грань некоторого куба совпадает с проекцией всего этого куба?

Игрушкой будем называть фигуру, склеенную из одинаковых кубиков (грани склеиваются целиком), если из каждого кубика можно добраться до любого другого, переходя из кубика в кубик только через соприкасающиеся грани. Если у Вас есть кубики, то перед рисованием игрушки можете сделать ее модель.

18.1.2. (a,b) Нарисуйте игрушку по трём её проекциям на рис. 1.56.

(c) (Загадка) Однозначно ли игрушка восстанавливается по трём её проекциям?

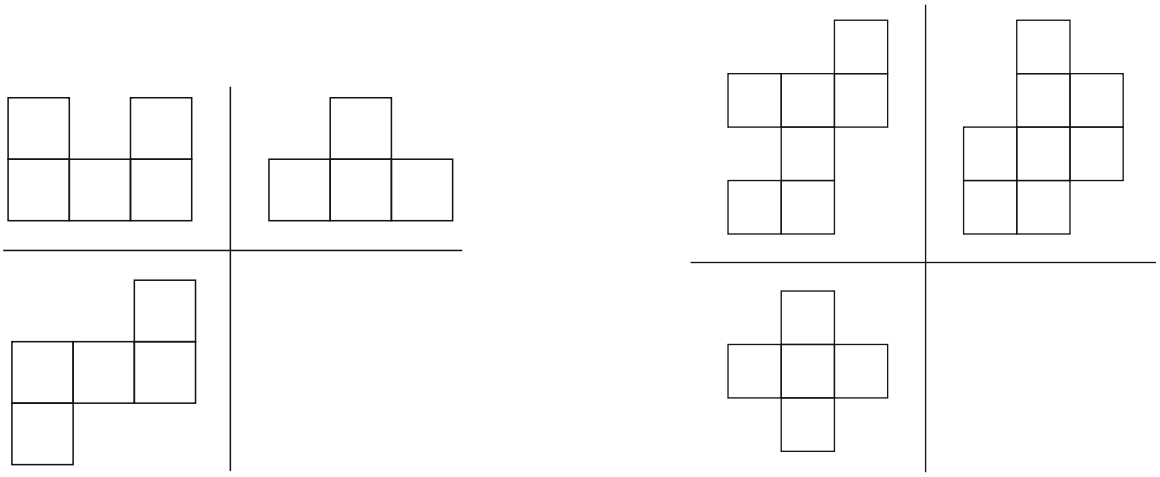

Рис. 1.56: Три проекции

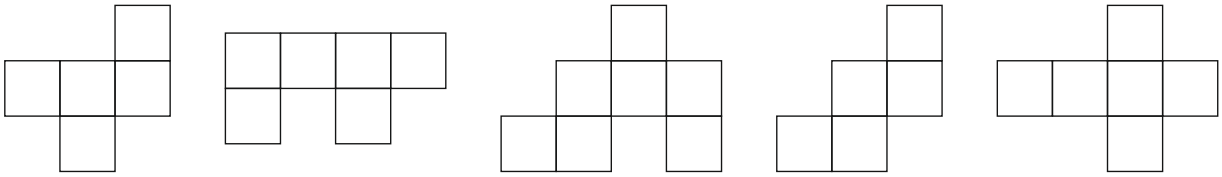

Рис. 1.57: Клетчатые фигуры

18.1.3. (a) Из клетчатых фигур на рис. 1.57 выберите три, которые могут быть тремя проекциями одной и той же игрушки (вращать клетчатые фигурки нельзя). Нарисуйте эту игрушку.

(b) Для какой-нибудь другой тройки клетчатых фигур из приведенных (на Ваш выбор) объясните, почему она не может образовывать набор трех проекций одной и той же игрушки.

18.1.2 Траектории

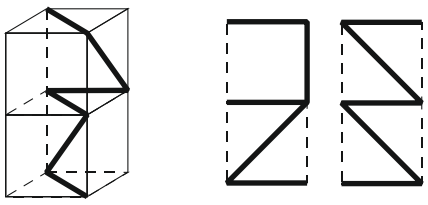

Рис. 1.58: Линия в параллелепипеде

Рис. 1.59: Восстановите линию в параллелепипеде по ее проекциям

18.1.4. (a) В параллелепипеде размера $1 \times 1 \times 2$ нарисовали линию, см. рис. 1.58 слева. Изобразите её вид спереди и справа.

(b,c) Восстановите линию в параллелепипеде размера $1 \times 1 \times 2$ по её видам спереди и справа, см. рис. 1.59.

(d) (Загадка) Однозначно ли восстанавливается линия по двум её проекциям?

18.1.3 Рисование

18.1.5. (a,b) На поверхности стеклянного куба нарисовали линию, см. рис. 1.60 (представьте себе, что по поверхности куба проползла улитка, оставляя за собой заметный след). Изобразите её вид спереди, сверху и справа.

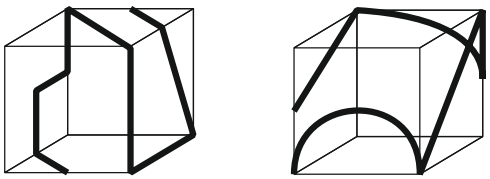

Рис. 1.60: Линии на поверхности стеклянного куба

18.1.6. (a,b) По видам спереди, сверху и справа на рис. 1.61 восстановите линию в кубе (т.е. проходящую по поверхности или внутри куба; представьте себе, что куб заполнен водой и внутри получившегося аквариума или вдоль его стенок может плавать рыбка).

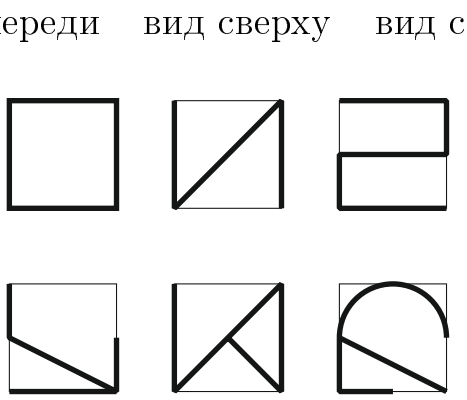

Рис. 1.61: Проекции линии в кубе

18.2 Рисование. А. Б. Скопенков (1-2)

Предмет математики настолько серьезен, что полезно не упускать случаев делать его немного занимательным.
Б. Паскаль.

Пространственное воображение необходимо в разных областях знания и техники, прежде всего в математике, программировании и физике. Более того, эти науки часто работают с многомерным пространством! Поэтому полезно и рано начинать развитие пространственного воображения, и не пропускать это развитие, даже если не получилось начать рано. Пространственное воображение является важным предварительным умением, а его развитие — одной из сверхзадач школьного курса стереометрии и даже базовых университетских курсов геометрии и топологии.[3]

При этом многие задачи в этом тексте являются скорее занимательными, чем математическими. Для их решения не требуется предварительных знаний по стереометрии. Они использовались для 6-11 классников на кружках «Олимпиады и математика» в школе «Интеллектуал» и МЦНМО, а также в Московской летней математической школе. Благодарю А.И. Сгибнева за обсуждения.

18.2.1. Нарисуйте сечение куба плоскостью, которое является

[3]Например, несколько первых занятий курсов топологии на ФИВТ и ФОПФ МФТИ отведены на такие задачи [Ku]. Из приведенных ниже задач используются лишь немногие, в основном разбираются «топологические» наглядные задачи [Sk, §2], см. также [Fr].

(a) правильным треугольником; (b) квадратом;
(c) правильным шестиугольником.

Сообразите, почему сечение куба плоскостью не может быть правильным n-угольником при $n \geqslant 7$. Оно не может быть и правильным пятиугольником. Но чтобы доказать это, нужны минимальные знания по стереометрии.

18.2.2. Из 27 одинаковых кубиков составлен куб $3\times3\times3$. Нарисуйте
(a) ежа (т.е. объединение центрального кубика и кубиков, имеющих с ним общую грань);
(b) то, что получается при выкидывании угловых кубиков из куба;
(c) то, что получается при выкидывании ежа из куба.

18.2.3. Можно ли пространство заполнить попарно непересекающимися ежами?

18.2.4. Нарисуйте пространственную фигуру, три проекции которой являются («заполненными», т.е. двумерными) треугольником, квадратом и кругом, соответственно.

18.2.5. (a) Нарисуйте пересечение правильного тетраэдра с тетраэдром, полученным из него поворотом на 90° относительно прямой, соединяющей середины противоположных рёбер.
(b) То же для объединения.
(c)* Нарисуйте объединение куба с кубом, полученным из него поворотом на 60° относительно большой диагонали.
(d)* Для каждой грани тетраэдра проведем две параллельные ей плоскости, делящие каждое ребро, не лежащее в этой грани, на три равных отрезка. На сколько частей разбивают тетраэдр проведенные плоскости?

18.2.6. (a) Как на двух гвоздях, вбитых в плоскую стену, подвесить замкнутую веревку (с тяжелой медалью), чтобы веревка не падала, но после вынимания любого гвоздя падала?
(b) Нарисуйте в пространстве три резиновые кольца, которые нельзя расцепить, но после разрезания любого из них они расцеплялись бы.

18.3.21. (a) Укажите два вращения правильного додекаэдра, композициями которых можно получить любое другое.

(b) Постройте биекцию, сохраняющую композицию, между множеством вращений додекаэдра и множеством чётных перестановок пяти элементов.

18.4 Многомерье (4^*). *А. Я. Канель-Белов*

18.4.1 Простейшие многогранники в многомерном пространстве. *Ю. М. Бурман, А. Я. Канель-Белов*

Хорошо известно, что точке плоскости можно сопоставить пару чисел — её декартовых координат (для этого нужно предварительно выбрать систему координат, то есть начало координат и оси). Тем самым плоскость можно понимать просто как множество всевозможных пар (x_1, x_2) действительных чисел. Аналогично трёхмерное пространство можно считать просто множеством всевозможных троек (x_1, x_2, x_3). Накладывая на числа различные ограничения, мы получим описание разнообразных подмножеств плоскости и пространства (плоских фигур и трёхмерных тел).

18.4.1.$^\circ$ Даны три набора условий на числа x_1, x_2, x_3:

1) $x_1 = x_2 = 2x_3$;

2) $x_1 + 2x_2 + 3x_3 = 0$, $3x_1 + 2x_2 + x_1 = 1$;

3) $x_1^2 + x_3^2 - 2x_3 = -1$.

Какие из них задают прямую в трёхмерном пространстве?

Когда измерений больше, чем три, координатный подход становится ведущим: удобно *определить*, скажем, четырёхмерное пространство как множество всевозможных наборов (x_1, x_2, x_3, x_4) из четырёх действительных чисел.

В этом пункте *отрезком* мы будем называть множество $[-1, 1] = \{x\colon |x| \leqslant 1\}$ чисел, по модулю не превосходящих 1; *квадратом* — множество $[-1, 1]^2 = \{(x_1, x_2)\colon |x_1|, |x_2| \leqslant 1\}$ пар чисел, каждое из которых по модулю не превосходит 1; *кубом* — множество $[-1, 1]^3 = \{(x_1, x_2, x_3)\colon |x_1|, |x_2|, |x_3| \leqslant 1\}$ троек таких чисел; *четырёхмерным кубом* — четвёрок и т. д. См. рисунок 1.65.

18.4.18. Докажите, что любое n-мерное сечение $(n+1)$-мерного куба, перпендикулярное диагонали и проходящее через вершину, комбинаторно эквивалентно «зоне» в n-мерном кубе между двумя аналогичными сечениями. Точнее, пусть $L_n(a,b) = \{(x_1,\ldots,x_n) \mid x_i \in [0,1], a \leqslant x_1 + \ldots x_n \leqslant b\}$. Докажите, что $L_{n+1}(k,k)$ комбинаторно эквивалентно $L_n(k-1,k)$. Начните со случая $n=3$, $k=2$.

18.4.19. Пусть (гипер)плоскость $\sum_1^n a_i x_i = c$, где $n > 2$, $a_i > 0$, числа a_i взаимно простые в совокупности, пересекает единичную решётку, состоящую из кубов. Докажите, что количество возникающих частей с точностью до параллельных переносов равно $\sum_{i=1}^n a_i$.

18.4.20. Дан n-мерный куб с центром в начале координат, координаты вершин которого равны ± 1. Число n мы будем называть *адамаровым*, если можно указать набор из n попарно ортогональных векторов с координатами ± 1. Докажите, что числа 1, 2, 4, 8 хорошие, а числа 3, 5, 6 — нет.

18.4.21. Докажите, что адамарово число, большее 2, имеет вид $4k$.

18.4.22. Докажите что все степени двойки — адамаровы числа.

18.4.23. Докажите, что число 12 адамарово.

18.4.24. Докажите, что число 20 адамарово.

Очень важная открытая проблема: верно ли, что все числа вида $4k$ адамаровы? См. подробнее [GDI, п. 7.2] и приведенные там ссылки.

18.4.2 Многомерные объёмы

Объём n-мерного многогранника определяется аналогично площади фигуры на плоскости (см. п. 26.5 «Принцип Дирихле и его применения в геометрии»).

Объёмом n-мерных многогранников называется заданная на множестве многогранников неотрицательная функция V, удовлетворяющая следующим условиям:

— если многогранник M_1 можно движением перевести в многогранник M_2, то $V(M_1) = V(M_2)$;

— $V(M_1 \cup M_2) = V(M_1) + V(M_2) - V(M_1 \cap M_2)$;

— объём любого подмножества $(n-1)$-мерной гиперплоскости равен нулю;

— объём куба с ребром a равен a^n.

Используя эти свойства и при необходимости верхние и нижние оценки, можно найти объём любого многогранника. Например, объём n-мерной пирамиды задаётся формулой $V = \frac{1}{n}Sh$, где S — $(n-1)$-мерный объём основания пирамиды, а h — её высота. Можно также находить объёмы некоторых n-мерных тел (т. е. ограниченных подмножеств n-мерного пространства), не являющихся многогранниками.

18.4.25. У 100-мерного арбуза (шара) радиус равен 1 метру, а толщина корки — 1 см. Какой процент его объёма занимает мякоть?

18.4.26. Докажите, что в единичный куб достаточно большой размерности можно поместить здание МГУ, т. е. существует трёхмерная плоскость, в пересечение которой с кубом можно поместить это здание.

18.4.27. Укажите какое-нибудь такое n, что в n-мерный единичный куб можно поместить круг радиуса R.

18.4.28. Укажите какое-нибудь такое n, что в n-мерный единичный куб можно поместить шар радиуса R.

18.4.29. Укажите какое-нибудь такое n, что в n-мерный единичный куб можно поместить n-мерный шар радиуса R.

18.4.30. К чему стремится объём n-мерного шара радиуса 2015 при $n \to \infty$?

Известно, что объём n-мерного шара радиуса R равен

$$B_n = \frac{\pi^{n/2}}{\Gamma(n/2+1)},$$

где $\Gamma(z) = \int\limits_0^\infty y^z e^{-y} dy$, $z > 0$ — знаменитая *гамма-функция* Эйлера. Она доопределяет факториал на комплексную плоскость: $\Gamma(k) =$

$(k+1)!$ при целом k и $\Gamma(z) = \Gamma(z-1)z$. Последнее равенство позволяет доопределить $\Gamma(z)$ также и при $\mathrm{Re}(z) < 0$. Известно, что $\Gamma(x)\Gamma(1-x) = \pi/\sin(\pi z)$, в частности $\Gamma(1/2) = \sqrt{\pi}/2$.

18.4.31. Найдите площадь поверхности n-мерного шара единичного объёма.

18.4.32. Найдите объём n-мерного симплекса с единичным ребром. Найдите ребро n-мерного симплекса с единичным объёмом. (Определения n-мерных симплекса и октаэдра приведены в п. 18.4.1 «Комбинаторная геометрия в многомерном пространстве».)

Диаметром ограниченного подмножества M n-мерного пространства называется $\sup\{|XY|, X, Y \in M\}$, где $\mathrm{dist}(X, Y)$ — расстояние между точками X и Y.

18.4.33. Найдите объём n-мерного октаэдра с единичным ребром. Найдите диаметр n-мерного симплекса с единичным объёмом.

18.4.3 Объёмы и сечения

Обозначим $x_+ = \max(x, 0) = \begin{cases} x & \text{при } x \geqslant 0, \\ 0 & \text{при } x \geqslant 0. \end{cases}$

Открытой полуплоскостью называется множество точек плоскости, лежащих строго по одну сторону от некоторой прямой. *Замкнутой полуплоскостью* называется объединение открытой полуплоскости и ее граничной прямой. Прямая, заданная уравнением $ax + by + c = 0$, разбивает плоскость на две полуплоскости (замкнутую и открытую), координаты точек которых удовлетворяют неравенствам $ax + by + c \geqslant 0$ и $ax + by + c < 0$. Аналогично определяются открытое и замкнутое *полупространство* в n-мерном пространстве.

В задачах этого пункта слова «открытое» и «замкнутое» будут опускаться, поскольку несущественно, какое именно подпространство рассматривается.

18.4.34. Обозначим через $S(a, b, d)$ площадь пересечения единичного квадрата $K = \{(x, y)\colon 0 \leqslant x, y \leqslant 1\}$ с полуплоскостью $ax + by \leqslant d$,

Задачи на пространственное воображение

[Ag] *Агаханов С.* Проекции фигур // Квантик. 2015. № 2. С. 11-13.

[Dor] *Дориченко С.* Стереометрия для всех // Квантик. 2012. № 1. С. 28.

[R] *В. Красноухов*, Недетские кубики-2, // Квантик. 2018. № 10. С. 15

[ShEr] *Шарыгин И. Ф., Ерганжиева Л. Н.* Математика. Наглядная геометрия. (второе издание). М.: 2015. 192 с.

[Nik] *Никитин Б. П.* Интеллектуальные игры. (шестое издание). Обнинск.: "Световид". 2009. 216 с. http://nikitiny.ru/Kirpichiki

Рисование

[BKK+] И. Богданов, А. Каибханов, Ю. Кудряшов, А. Скопенков, А. Сосинский и Г. Челноков. Новые способы плетения корзинок http://www.turgor.ru/lktg/2004/lines.ru/index.htm.

[Fr] Дж. Франсис, Книжка с картинками по топологии (как рисовать математические картинки). Москва, Мир, 1991.

[GSS+] А. А. Гайфуллин, А. Б. Скопенков, М. Б. Скопенков и А. В. Шаповалов. Проекции скрещивающихся прямых. http://www.turgor.ru/lktg/2001/index.php.

[Ku] Курсы топологии в исполнении А.Б. Скопенкова, http://www.mccme.ru/circles/oim/home/combtop13.htm

[PS] В.В. Прасолов и И.Ф. Шарыгин. Задачи по стереометрии. Москва, Наука, 1989.

[Sk] А.Б. Скопенков, Алгебраическая топология с геометрической точки зрения. Москва, МЦНМО, 2015. Часть книги: http://www.mccme.ru/circles/oim/home/combtop13.htm#photo

Глава 2

Комбинаторика

20 Подсчеты в комбинаторике

Этот параграф посвящен в основном вопросу «Сколько существует объектов с данными свойствами?». В нем собраны материалы для самого первого знакомства с подсчетами в комбинаторике. Продолжить их изучение мы рекомендуем по главе 1 книги [GDI].

20.1 Подсчеты числа способов (1). *А. А. Гаврилюк, Д. А. Пермяков*

Этот пункт не требует никаких знаний и подходит для первого знакомства с комбинаторикой.

20.1.1. (a) Назовем натуральное число *симпатичным*, если в его записи встречаются только четные цифры. Выпишите все двузначные симпатичные числа и подсчитайте их количество.

(b) Сколько существует пятизначных симпатичных чисел?

(c) Сколько существует шестизначных чисел, в записи которых есть хотя бы одна четная цифра?

(d) Каких семизначных чисел больше: тех, в записи которых есть единица, или остальных?

20.1.2. Из двух математиков и десяти экономистов надо составить комиссию из восьми человек. Сколькими способами можно составить комиссию, если в нее должен входить хотя бы один математик?

20.1.3. (a) Найдите сумму всех семизначных чисел, которые можно получить всевозможными перестановками цифр $1, \ldots, 7$.

(b) Из цифр $1, 2, 3, \ldots, 9$ составлены все четырехзначные числа, не содержащие повторяющихся цифр. Найдите сумму этих чисел.

(c) Найдите сумму всех четырехзначных чисел, не содержащих повторяющихся цифр.

20.1.4. (a) На двух клетках шахматной доски стоят черный и белый короли. За один ход можно пойти любым королем (короли дружат, так что могут стоять в соседних клетках, но не в одной и той же). Могут ли в результате их передвижений встретиться все возможные варианты расположения этих королей, причем ровно по одному разу?

(b) Тот же вопрос, если короли разучились ходить по диагонали.

20.1.5. (a) Найдите сумму всех 6-значных чисел, получаемых при всех перестановках цифр $4, 5, 5, 6, 6, 6$.

(b) Найдите сумму всех 10-значных чисел, получаемых при всех перестановках цифр $4, 5, 5, 6, 6, 6, 7, 7, 7, 7$.

20.1.6. (a) Тому Сойеру поручили покрасить забор из 8 досок в белый цвет. В силу своей лени он покрасит не более 3 досок. Сколько у него способов это сделать?

(b) А сколько способов покрасить не более 5 досок?

(c) А сколько способов покрасить любое количество досок?

Указания, ответы и решения

20.1.1. *Ответы*: (b) 2500; (c) 884 375; (d) в которых есть единица.

(b) *Решение* (написано А. Колоченковым). Первой цифрой симпатичного числа может быть 2, 4, 6, или 8 — всего 4 варианта. Для каждой цифры со второй по пятую есть 5 вариантов: 0, 2, 4, 6, 8. Значит, всего симпатичных чисел $4 \cdot 5 \cdot 5 \cdot 5 \cdot 5 = 2500$.

Это рассуждение в комбинаторике называется *правилом произведения* и подробно обсуждается в статье [Vi71].

(c) *Решение* (написано А. Колоченковым). Вычтем из общего количества шестизначных чисел количество шестизначных чисел,

нет). Если нет, то предположим, без ограничения общности, что $2007 \notin X_1$ и что $2, \ldots, 52 \in X_1$. Тогда для всех $j = 2, \ldots, 52$ пересечение $X_j \cap X_{2007}$ должно состоять ровно из одного элемента, причём разного для разных j (так как любые два множества по условию имеют ровно один общий элемент). Но это невозможно, поскольку X_{2007} состоит всего из 40 элементов, что меньше 51.

20.2.5. *Ответ*: да.

20.2.6. *Ответ*: да.

20.2.7. *Ответ*: $(N+1)! - 1$.

20.3 Формула включений и исключений (2). *Д. А. Пермяков*

Этот пункт посвящен доказательству и использованию формулы включений и исключений. Она позволяет отвечать на вопрос «Сколько существует объектов с данными свойствами?» во многих непростых случаях. Потребуются базовые навыки решения задач по комбинаторике. В частности, нужно уметь приводить строгие доказательства с использованием взаимно однозначных соответствий, правил суммы и произведения. Например, полезно прорешать п. 20.1 «Подсчеты числа способов» или задачи из статьи [Vi71].

20.3.1. Сколькими способами можно переставить числа от 1 до n, чтобы

(a) и 1, и 2 не оказались на своем месте;

(b) ровно одно из чисел 1, 2 и 3 оказалось на своем месте;

(c) каждое из чисел 1, 2 и 3 оказалось не на своем месте;

(d) каждое из чисел 1, 2, 3 и 4 оказалось не на своем месте?

Обозначим через $\varphi(n)$ функцию Эйлера, т. е. количество чисел от 1 до n, взаимно простых с числом n.

20.3.2. (a) Найдите количество целых чисел от 1 до 1001, не делящихся ни на одно из чисел 7, 11, 13.

(b) Найдите $\varphi(1)$, $\varphi(p)$, $\varphi(p^2)$, $\varphi(p^\alpha)$, где p — простое число, $\alpha > 2$.

(c) Докажите, что $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_s}\right)$, где $n = p_1^{\alpha_1} \cdot \dots \cdot p_s^{\alpha_s}$ — каноническое разложение числа n.

20.3.3. (a) На полу комнаты площадью 24 м^2 расположены три ковра (произвольной формы) площадью 12 м^2 каждый. Тогда площадь пересечения некоторых двух ковров не меньше 4 м^2.

(b) На кафтане расположено пять заплат (произвольной формы). Площадь каждой из них больше трех пятых площади кафтана. Тогда площадь общей части некоторых двух заплат больше одной пятой площади кафтана.

(c)* То же, что в п. (b), если площадь каждой заплаты больше *половины* площади кафтана.

В этом пункте предлагаются задачи следующего типа: даны конечное множество U и набор свойств (подмножеств) $A_k \subset U$, $k = 1, \dots, n$. Требуется найти количество элементов, для которых выполнено хотя бы одно из свойств A_k (т. е. $|A_1 \cup \dots \cup A_n|$), либо количество элементов, для которых не выполнено ни одно из свойств A_k (т. е. $|U - (A_1 \cup \dots \cup A_n)|$). Для этого используются два варианта формулы включений и исключений (см. задачу 20.3.5 (b)). При этом если во всех пересечениях множеств набора число элементов зависит только от количества пересекаемых множеств, то формулу можно упростить (см. задачу 20.3.5 (a)).

20.3.4. Рассмотрим подмножества A_1, A_2, A_3, A_4 конечного множества U. Докажите равенства

(a) $A_1 \cup A_2 = (A_1 \backslash A_2) \sqcup (A_1 \cap A_2) \sqcup (A_2 \backslash A_1)$;

(b) $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$;

(c) $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|$.

(d) Количество элементов в U, не принадлежащих ни одному из подмножеств A_1, A_2, A_3, равно

$$|U| - |A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_2 \cap A_3| + |A_1 \cap A_3| - |A_1 \cap A_2 \cap A_3|.$$

(e) Для $k = 1, 2, 3, 4$ обозначим

$$M_k := \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant 4} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}|.$$

Докажите, что количество элементов в A, не принадлежащих ни одному из A_i, равно $|U| - M_1 + M_2 - M_3 + M_4$.

(f) В условиях п. (e) количество элементов, принадлежащих ровно одному из множеств A_i, равно $M_1 - 2M_2 + 3M_3 - 4M_4$.

20.3.5. Формула включений и исключений. Рассмотрим подмножества $A_1, \ldots, A_n$ конечного множества U. Положим по определению $\Big|\bigcap\limits_{j \in \emptyset} A_j\Big| := U$.

(a) Пусть число $\alpha_{|S|} := \Big|\bigcap\limits_{j \in S} A_j\Big|$ зависит только от размера $|S|$ набора $S \subset \{1, \ldots, n\}$ индексов, а не от самого набора. Тогда

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} \alpha_k,$$

$$|U - (A_1 \cup \ldots \cup A_n)| = \sum_{k=0}^{n} (-1)^{k} \binom{n}{k} \alpha_k.$$

(b) Обозначим $M_k := \sum\limits_{S \in \binom{n}{k}} \Big|\bigcap\limits_{j \in S} A_j\Big|$, где суммирование производится по всем k-элементным подмножествам множества $\{1, \ldots, n\}$. В частности, $M_0 := |U|$. Тогда

$$|A_1 \cup \ldots \cup A_n| = M_1 - M_2 + M_3 - \ldots + (-1)^{n+1} M_n,$$
$$|U - (A_1 \cup \ldots \cup A_n)| = M_0 - M_1 + M_2 + \ldots + (-1)^{n} M_n.$$

(c) **Неравенства Бонферрони.** Для любого $0 \leqslant s < n/2$ справедливы неравенства

$$M_1 - M_2 + M_3 - \ldots - M_{2s} \leqslant |A_1 \cup \ldots \cup A_n| \leqslant M_1 - M_2 + M_3 - \ldots + M_{2s+1},$$
$$M_0 - M_1 + M_2 - \ldots + M_{2s} \geqslant |U - (A_1 \cup \ldots \cup A_n)| \geqslant$$
$$\geqslant M_0 - M_1 + M_2 - \ldots - M_{2s+1}.$$

(d) Число элементов, принадлежащих ровно r из подмножеств $A_1, \ldots, A_n$, равно $\sum\limits_{k=r}^{n} (-1)^{k-r} \binom{k}{r} M_k$.

20.3.6. На полке стоят 10 различных книг.

(a) Сколькими способами их можно переставить так, чтобы ни одна книга не осталась на своем месте?

(b) Количество таких перестановок книг, при которых на месте остаётся ровно 4 книги, больше 50 000.

В следующей задаче в ответе можно использовать суммы (аналогично формуле включений и исключений).

20.3.7. (a) Сколькими способами можно расселить 20 туристов по 5 различным домикам, чтобы ни один домик не оказался пустым?

(b) Сколько существует различных сюръекций $f\colon \mathbb{Z}_k \to \mathbb{Z}_n$?

20.3.8. По кругу стоят числа $1, 2, \ldots, n$. Найдите число способов выбрать k из них, чтобы никакие два выбранных числа не стояли рядом.

(b) Найдите число способов рассадить n пар враждующих рыцарей за круглый стол с нумерованными местами, чтобы никакие два враждующих рыцаря не сидели рядом.

20.3.9. Куб с ребром длины 20 разбит на 8000 единичных кубиков, и в каждом кубике записано число. Известно, что в каждом столбике из 20 кубиков, параллельном ребру куба, сумма чисел равна 1 (рассматриваются столбики всех трех направлений). В некотором кубике записано число 10. Через этот кубик проходят три слоя $1 \times 20 \times 20$, параллельные граням куба. Найдите сумму всех чисел вне этих слоев.

20.3.10.* Сколько существует шестизначных трамвайных билетов, в которых нет двух семерок рядом и всего

(a) не более трех семерок;

(b) не более четырех семерок;

(c) сколько угодно семерок?

20.3.11.* Докажите следующую формулу:

$$n! \cdot x_1 x_2 \ldots x_n = (x_1 + x_2 + \ldots + x_n)^n - \\ - \sum_{1 \leqslant i_1 < i_2 < \ldots < i_{n-1} \leqslant n} (x_{i_1} + x_{i_2} + \ldots + x_{i_{n-1}})^n + \\ + \sum_{1 \leqslant i_1 < i_2 < \ldots < i_{n-2} \leqslant n} (x_{i_1} + x_{i_2} + \ldots + x_{i_{n-2}})^n - \ldots + (-1)^{n-1} \sum_{i=1}^{n} x_i^n.$$

Указания, ответы и решения

20.3.1. (a) *Ответ*: $n! - 2(n-1)! + (n-2)!$.

Указание. Всего имеется $n!$ способов переставить наши числа. Вычтем из них $(n-1)!$ способов перестановки, при которых число 1 остается на месте. Вычтем также $(n-1)!$ способов перестановки, при которых число 2 остается на месте. При этом $(n-2)!$ способов перестановки, при которых оба числа 1 и 2 остаются на месте, мы «вычли дважды». Значит, число $(n-2)!$ нужно добавить, чтобы в итоге мы эти способы «посчитали один раз». Получаем ответ: $n! - 2(n-1)! + (n-2)!$.

Комментарий. Это решение формализуется формулой включений и исключений 20.3.5, которую предлагается доказать и использовать в последующих задачах.

20.3.2. (a) *Ответ*: 720.

Первое указание. Для каждого j, делящего 1001, обозначим через A_j множество чисел от 1 до 1001, делящихся на j. Тогда

$$|A_j| = \frac{1001}{j} \quad \text{и} \quad A_{p_1} \cap \ldots \cap A_{p_k} = A_{p_1 \cdot \ldots \cdot p_k}$$

для различных простых чисел $p_1, \ldots, p_k$. Следовательно, искомое

23.1 Конструкции[3] (1). *А. В. Шаповалов*

Если на вопрос «Может ли?» вы подозреваете ответ «Может», то стоит спросить себя: «Как такое может быть?». Уточните вопрос: «Какими свойствами эта конструкция должна обладать?». Дополнительное знание поможет сильно сузить круг поисков. Задавайте себе вопросы на протяжении всего построения. Вы с удивлением увидите, как много конструкций окажутся логичными и единственно возможными.

Часто примеров много, а нужен только один. Избыток свободы может сбивать с толку: неясно, с чего начинать. Примените *здравый смысл*, *естественные соображения*. Они ограничивают поле для поиска примера, но зато поиск убыстряется и облегчается. Вообще, ваш опыт гораздо больше, чем вы думаете. Ответом может оказаться *хорошо знакомый объект*, просто надо посмотреть на него под нужным углом.

23.1.1. У двух треугольников равны по две стороны, а также равны высоты, проведённые к третьей стороне. Обязательно ли эти треугольники равны?

23.1.2. Верно ли, что в вершинах любого треугольника можно поставить по положительному числу так, чтобы длина каждой стороны была равна сумме чисел в её концах?

23.1.3. В кружке у каждого участника ровно по 6 друзей. Может ли у каждой пары участников быть ровно по два общих друга?

Конструкцию с большим числом деталей проще строить из одинаковых «кирпичей». Даже если все они одинаковыми быть не могут, попробуйте взять одинаковых побольше. Можно ещё выбрать два вида деталей и посчитать, сколько нужно тех и других.

Ну, а если детали «для сборки» заданы и они разные? Тогда стоит попытаться объединить эти части в *одинаковые блоки*, и строить из блоков.

23.1.4. Назовём неотрицательное целое число *зеброй*, если в его записи строго чередуются чётные и нечётные цифры и среди цифр

[2]Эта подборка задач составлена по книгам [Shap14] и [Shap15].

есть не менее трёх различных. Может ли разность двух 100-значных зебр быть 100-значной зеброй?

23.1.5. Грани параллелепипеда со сторонами 3, 4 и 5 разбиты на единичные клетки. В каждую клетку вписали по натуральному числу. Рассмотрим всевозможные кольца шириной в одну клетку, параллельные какой-нибудь грани. Может ли сумма чисел в каждом таком кольце быть одной и той же?

В задачах, где требуются равные части, приходится выбирать форму частей. Тут может помочь такое соображение: части заведомо равны, если они получаются друг из друга симметрией, сдвигом или поворотами. Так, для квадрата популярны разрезания, переходящие в себя при повороте на 90°, а для правильного треугольника — при повороте на 120°. Для симметричных объектов поиск примера начинают с симметричных или «почти симметричных» конструкций. Симметрия и идея «расположить объекты по кругу» применима и в негеометрических задачах.

23.1.6. Можно ли рёбра куба занумеровать числами -6, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, 6 так, чтобы для каждой тройки рёбер, выходящих из одной вершины, сумма была одинакова?

23.1.7. Круг разрезали на несколько равных частей. Обязательно ли граница каждой части проходит через центр круга?

Если к конструкции предъявляются противоречивые требования, присмотритесь внимательнее. Часто эти противоречия мнимые. Так, *большой* периметр не противоречит *малой* площади. Вообще, словам «много», «мало», «сильно» нужно уметь придать в решении точный математический смысл с помощью уравнений и неравенств.

23.1.8.* В море плавает айсберг в форме выпуклого многогранника. Может ли случиться, что 90 % его объёма находится ниже уровня воды и при этом больше половины его поверхности находится выше уровня воды?

23.1.9. Есть три игральных кубика с нестандартными наборами чисел на гранях. Скажем, что кубик A *выигрывает* у кубика B, если

при их одновременном бросании число на A будет больше числа на B с вероятностью *больше* 0,5. Может ли первый кубик выигрывать у второго, второй — у третьего, а третий — у первого?

(Приведём равносильную формулировку этой же задачи, не использующую понятие вероятности: для пары кубиков A и B составим 36 упорядоченных пар вида (грань A, грань B). Заменим в каждой паре грань на число, стоящее на грани. Кубик A *выигрывает* у B, если более чем в половине пар первое число больше второго.)

Помешать решить задачу могут невидимые барьеры в голове решателя. Если очевидного решения не видно, надо расширять список вариантов, по возможности до полного. *Инерция мышления* проявляется в том, что ключевой вариант пропускают либо не подозревают, что вариантов более одного. Примените «метод Шерлока Холмса»: отбросьте все невозможные случаи, тогда *последний вариант* окажется возможным, каким бы невероятным он ни казался.

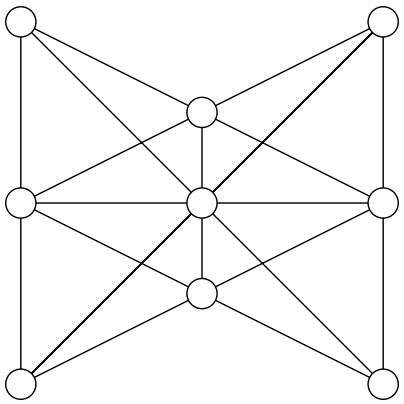

Рис. 2.3:

23.1.10. На столе лежат 9 яблок, образуя 10 рядов по 3 яблока в каждом (см. рис. 2.3). Известно, что у девяти рядов веса одинаковы, а вес десятого ряда отличается. Есть электронные весы, на которых за рубль можно узнать вес любой группы яблок. Какое наименьшее число рублей надо заплатить, чтобы узнать, вес какого именно ряда отличается?

23.1.11. Может ли прямая разбить какой-нибудь шестиугольник на 4 равных треугольника?

Редукция — это сведе́ние сложной задачи к более простой. Так, если сложную конструкцию не удаётся сразу построить целиком, постройте её *необходимую часть*. Даже если эту часть не удастся потом достроить до целого, решение упрощённой задачи может послужить разминкой, после чего вы вернётесь к сложной задаче уже с накопленным опытом.

23.1.12. Барон Мюнхгаузен говорит, что у него есть многозначное число-*палиндром* (т. е. оно читается одинаково слева направо и справа налево). Написав его на бумажной ленте, барон сделал несколько разрезов между цифрами. Лента распалась на N кусков. Переложив куски в другом порядке, барон увидел, что на кусках по разу записаны числа 1, 2, ..., N. Могут ли слова барона быть правдой?

При построении конструкции может мешать неоднозначность выбора. В *узком месте* всё однозначно или неопределённость минимальна, что сокращает перебор. Начав с узкого места, мы либо быстро придём к противоречию, либо построим большой кусок конструкции. Как искать узкие места? Присмотритесь: они служат препятствиями к построению конструкции или кажутся таковыми.

23.1.13. Записав числа 1, $\frac{1}{2}$, $\frac{1}{3}$, ..., $\frac{1}{10}$ в некотором порядке, соедините их знаками четырёх арифметических действий так, чтобы полученное выражение равнялось 0. (Скобки использовать нельзя.)

23.1.14. Существуют ли три равных семиугольника, все вершины которых совпадают, но никакие стороны не совпадают?

23.1.15. Можно ли разрезать какой-нибудь треугольник на четыре выпуклые фигуры: треугольник, четырёхугольник, пятиугольник и шестиугольник?

При *постепенном конструировании* к примеру идут через цепочку вспомогательных конструкций-*заготовок*. На каждом шаге очередная конструкция *улучшается* до следующей. В заготовке требования к окончательной конструкции выполнены лишь частично. Оставляем *принципиальные* условия, временно забываем или ослабляем *технические*.

23.1.16. Могут ли в остроугольном треугольнике все стороны и высоты измеряться целым числом сантиметров?

23.1.17. Докажите, что существует палиндром, делящийся на 6^{100}. (Напомним, что *палиндром* — это число, которое не меняется при записи его цифр в обратном порядке.)

Наконец, при *конструкции по индукции* результат получается постепенно, но уже за бесконечное число шагов. Таким конструкциям посвящён п. 21.5 «Конечное и счётное».

Продолжить знакомство с конструкциями можно по статье [GK] и книгам [Shap14, Shap15, Shap08].

Указания, ответы и решения

Решения задач и *пути к решению* тщательно разделены. Решение — это то, что решающий задачу в идеале должен написать. Путь к решению должен остаться в голове, здесь он поясняет, как это решение можно было придумать. В задачах на конструкцию решение и путь к решению обычно имеют мало общего.

Решение в задаче на конструкцию состоит из двух частей: *примера*, то есть описания конструкции, и *доказательства* того, что она удовлетворяет условию задачи. Для наших задач вторая часть не представляет труда и обычно опускается. Но иногда из многих возможных примеров нужно ещё выбрать тот, для которого доказательство проще.

23.1.1. *Ответ*: не обязательно.

Решение. Рассмотрим равнобедренный треугольник ACD и точку B на продолжении основания DC. У треугольников ABC и ABD сторона AB и высота AH общие, стороны AC и AD равны. Однако эти треугольники не равны: один — часть другого.

Путь к решению. Попробуем *построить* треугольник по двум сторонам b, c и высоте h, проведённой к третьей стороне. Для этого проведём прямую l (на ней будет лежать третья сторона) и построим вершину A на расстоянии h от l. Две другие вершины треугольника должны лежать на этой прямой на расстояниях b и c от точки A. Проведя окружности указанных радиусов с центром

23.4.12. Какое наименьшее число уголков из трёх клеток нужно разместить в квадрате 8×8 клеток, чтобы в него нельзя было поместить без наложения ни одной такой фигуры?

23.4.13. В квадрате 7×7 клеток нужно отметить центры n клеток так, чтобы никакие 4 отмеченные точки не являлись вершинами прямоугольника со сторонами, параллельными сторонам квадрата. При каком наибольшем n это возможно?

Указания, ответы и решения

23.4.1. Каждая фигура «домино» содержит одну белую и одну чёрную клетку. Но в нашей фигуре 32 чёрных и 30 белых клеток (или наоборот). Подробный разбор см. в статье [Soi].

23.5 Полуинварианты[7](1). *А. В. Шаповалов*

Если слово «инвариант» означает «неизменный», то «полуинвариант» — неизменный наполовину.

Бывает так, что мы меняем конструкцию, а какая-то связанная с этой конструкцией величина может меняться только в одну сторону, то есть либо только увеличиваться, либо только уменьшаться. Ещё возможно, что мы делаем ходы и в одну сторону меняется величина, связанная с позицией. Например, при игре в крестики-нолики число заполненных клеток с каждым ходом увеличивается. На ограниченной доске из этого следует, что рано или поздно игра закончится. При игре на бесконечной доске игра может не закончиться никогда, но зато мы можем гарантировать, что позиция не повторится, — ведь число заполненных клеток каждый раз новое!

Чуть более формально: пусть мы меняем конструкции (или позиции) с помощью *разрешённых операций* (или *ходов*) и нам удалось связать с каждой конструкцией/позицией *величину*, значение которой при любом разрешённом преобразовании либо не меняется, либо меняется всегда в одну и ту же сторону. Тогда эта величина

[7]Идейными предшественниками подборок «Инварианты» и «Полуинварианты» были, среди прочего, соответствующие параграфы книги [KK08].

называется *полуинвариантом*[8]. Если полуинвариант меняется при каждой операции/ходе, он называет *строгим*, иначе — *нестрогим*.

В типовых задачах «на полуинвариант» доказывают невозможность а) повторения позиций; б) бесконечного числа ходов; в) построения конструкций. Для последнего находят полуинвариант и проверяют, что для получения искомой конструкции из исходной полуинвариант должен был бы *меняться не в ту сторону*.

Но как найти полуинвариант? Начните с проверки типовых величин: сумм, произведений, площадей, периметров и их комбинаций. Если конструкция зависит от целых чисел, то полуинвариантом может быть НОД или НОК.

В следующих двух задачах важно, что полуинвариант целочисленный и не может быть больше определённого числа.

23.5.1. На шахматной доске 100×100 королю разрешено ходить вправо, вверх или вправо-вверх по диагонали. Какое наибольшее число ходов он может сделать?

23.5.2. В клетках таблицы 99×99 расставлены целые числа. Если в каком-то ряду (строке или столбце) сумма отрицательна, разрешается в этом ряду поменять знаки всех чисел на противоположные. Докажите, что в итоге можно сделать лишь конечное число таких операций.

Если полуинвариант не целочисленный, то его ограниченность ещё не гарантирует окончания процесса (например, убывающий положительный полуинвариант мог бы бесконечно долго принимать значения $1, 1/2, 1/3, 1/4, \ldots, 1/n, \ldots$). В этих случаях прекращение ходов гарантируется конечным числом позиций.

23.5.3. Дано 10 чисел. За одну операцию можно два неравных числа заменить на два равных с той же суммой. Может ли этот процесс для какого-то исходного набора чисел

(a) продолжаться бесконечно долго;

(b) зациклиться (то есть может ли один и тот же набор чисел возникнуть дважды)?

[8] Эта фраза не является формальным определеним полуинварианта. Но для решения задач формальное определение этого понятия не нужно.

23.5.4. По кругу выписано несколько чисел. Если для некоторых четырёх идущих подряд чисел a, b, c, d оказывается, что $(a-d)(b-c) < 0$, то числа b и c можно поменять местами. Докажите, что такую операцию можно проделать лишь конечное число раз.

Очень часто положение, в котором нет разрешённых операций, и является искомым.

23.5.5. В клетки прямоугольной таблицы вписаны числа. Разрешается одновременно менять знак у всех чисел некоторого столбца или некоторой строки. Докажите, что многократным повторением этой операции можно превратить данную таблицу в такую, у которой суммы чисел в любой строке или любом столбце неотрицательны.

В комбинаторных задачах полуинвариантом часто служит число комбинаций, например пар, троек, подмножеств или перестановок какого-то вида.

23.5.6. В тридевятом царстве все города подняли над ратушами флаги — голубые либо оранжевые. Каждый день жители узнают цвета флагов у соседей в радиусе 100 км. Один из городов, где у большинства соседей флаги другого цвета, меняет свой флаг на этот другой цвет. Докажите, что со временем смены цвета флагов прекратятся.

Некоторые конструкции создаются «методом последовательного улучшения». Мы берём несовершенную конструкцию и начинаем её преобразовывать. Полуинвариант гарантирует завершение процесса и достижение нужного эффекта в конце.

23.5.7. В парламенте каждый депутат имеет не более трёх врагов. Докажите, что парламент можно так разбить на две палаты, что у каждого депутата в его палате будет не более одного врага.

23.5.8. На плоскости дано 100 красных и 100 синих точек, никакие три из которых не лежат на одной прямой. Докажите, что можно провести 100 непересекающихся отрезков с концами разных цветов.

Полуинвариант может быть и *нестрогим*, т. е. не меняться при некоторых ходах. Тогда полезно найти ещё один полуинвариант, который строго меняется как раз тогда, когда первый остаётся неизменным.

23.5.9. На шахматной доске 100×100 королю разрешено ходить вправо, вверх, вправо-вверх или вправо-вниз по диагонали. Докажите, что он может сделать лишь конечное число ходов.

Если и второй полуинвариант оказывается нестрогим, то приходится рассматривать и третий, и четвёртый и т. д. В этом случае естественно рассматривать наборы значений полуинвариантов как строки, упорядоченные *лексикографически* (как слова в словаре: сравниваются первые элементы, при равенстве — вторые и т. д. и так до первого несовпадения).

23.5.10. В колоде часть карт лежит рубашкой вниз. Время от времени Петя вынимает из колоды пачку из нескольких подряд идущих карт, в которой верхняя и нижняя карты лежат рубашкой вниз (в частности, может вынуть просто одну карту рубашкой вниз), переворачивает эту пачку как одно целое и вставляет в то же место колоды. Докажите, что независимо от того, как Петя выбирает пачки, в конце концов все карты лягут рубашкой вверх.

В заключение — ещё несколько задач на полуинварианты и их комбинации.

23.5.11. В строке записано несколько чисел. Каждую секунду робот выбирает какую-либо пару рядом стоящих чисел, в которой левое число больше правого, меняет их местами и при этом умножает оба числа на 2. Докажите, что через некоторое время сделать очередную такую операцию будет невозможно.

23.5.12. У Карлсона есть 1000 банок с вареньем. Банки не обязательно одинаковые, но в каждой — не больше чем сотая часть всего варенья. На завтрак Карлсон может съесть поровну варенья из любых 100 банок. Докажите, что Карлсон может действовать так, чтобы за некоторое количество завтраков съесть всё варенье.

23.5.13. На окружности расставлено несколько положительных чисел, каждое из которых не больше 1. Докажите, что можно разделить окружность на три дуги так, что суммы чисел на соседних дугах будут отличаться не больше чем на 1. (Если на дуге нет чисел, то сумма на ней считается равной нулю.)

24 Алгоритмы

24.1 Игры (1)[9]. *Д. А. Пермяков, М. Б. Скопенков, А. В. Шаповалов*

На конкретных примерах мы познакомимся с некоторыми красивыми идеями теории игр. Общие методические указания по теме «Игры» можно найти в соответствующем разделе книги [GIF].

Симметричная стратегия

Самая распространённая стратегия в играх — *симметричная* (а также её обобщение — *дополняющая*). Для решения последующих задач полезно знакомство с п. 23.2 «Инварианты I», поскольку многие стратегии в играх основаны на инвариантах (пример инварианта — симметричность позиции).

24.1.1. (a) Двое по очереди выкладывают доминошки на шахматную доску. Каждая доминошка покрывает ровно две клетки доски, каждая клетка может быть покрыта не более чем одной доминошкой. Проигрывает тот игрок, который не может положить очередную доминошку. Кто выигрывает при правильной игре? Как он должен для этого играть?

(b) То же для доски 8×9.

Вот что означают вопросы этой задачи. В ответе на первый вопрос нужно назвать игрока, который выигрывает при *любой* игре своего противника. В ответе на второй вопрос нужно привести *алгоритм* действий этого игрока, который гарантирует выигрыш (*выигрышную стратегию*). Важно чётко отделять *сам* алгоритм от *доказательства* того, что алгоритм приводит к желаемому результату.

Второй пункт этой задачи показывает, что не всегда симметричность позиции гарантирует, что симметричная стратегия работает.

[9]Подпункты «Симметричная стратегия», «Выращивание дерева позиций», «Передача хода» написаны Д. А. Пермяковым и М. Б. Скопенковым, «Игры-шутки», «Игра на опережение», «Накопление преимущества» — А. В. Шаповаловым, «Смесь» — всеми тремя авторами.

24.1.2.° (Загадка.) К какому результату приведёт попытка чёрных зеркально-симметрично копировать ходы противника в обычных шахматах при правильной игре белых? Выберите верный вариант ответа:

1) к ничьей; 2) к выигрышу белых; 3) к выигрышу чёрных.

Ключевой идеей является не столько симметрия, сколько разбиение всех возможных позиций на пары. *Дополняющая стратегия* состоит в том, чтобы на ход противника отвечать ходом во вторую позицию соответствующей пары.

24.1.3. На шахматной доске стоит король. Двое по очереди ходят им. Проигрывает игрок, после хода которого король оказывается в клетке, в которой побывал ранее. Кто выигрывает при правильной игре и как он должен для этого играть?

Игра на опережение

Игра на опережение — распространённый приём в нематематических играх. Но и в математических играх бывает, что выигрыш достаётся тому, кто первый сумеет занять ключевое положение. После этого, как правило, работает дополняющая стратегия.

24.1.4. Есть 9 запечатанных прозрачных коробок соответственно с $1, 2, 3, \ldots, 9$ фишками. Двое играющих по очереди берут по одной фишке из любой коробки, распечатывая, если необходимо, коробку. Проигрывает тот, кто последним распечатает коробку. Кто из них может всегда выиграть независимо от игры противника?

24.1.5. В одном из углов шахматной доски лежит плоский картонный квадрат 2×2, а в противоположном — квадрат 1×1. Двое играющих по очереди перекатывают каждый свой квадрат через сторону: Боря — большой квадрат, а Миша — маленький. Боря выигрывает, если не позднее 100-го хода Мишин квадрат окажется на клетке, накрытой Бориным квадратом. Может ли Боря выиграть независимо от игры Миши, если

(a) первым ходит Боря;

(b) первым ходит Миша?

Накопление преимущества

Накопление преимущества — тоже весьма распространённый приём в нематематических играх. В математических играх накопление обычно связано с каким-нибудь полуинвариантом. Поэтому для изучения таких игр полезно знакомство с п. 23.5 «Полуинварианты». При этом надо придумать алгоритм, ведущий к накоплению независимо от сопротивления соперника.

24.1.6. Миша стоит в центре круглой лужайки радиуса 100 метров. Каждую минуту он делает шаг длиной 1 метр. Перед каждым шагом он объявляет направление, в котором хочет шагнуть. Катя имеет право заставить его сменить направление на противоположное. Может ли Миша действовать так, чтобы в какой-то момент обязательно выйти с лужайки, или Катя всегда сможет ему помешать?

24.1.7. На клетчатой доске $1 \times 100\,000$ (вначале пустой) двое ходят по очереди. Первый может за ход выставить два крестика в любые два свободных поля доски. Второй может стереть любое количество крестиков, идущих подряд — без пустых клеток между ними. Если после хода первого образуется 13 или более крестиков подряд, он выиграл. Может ли первый игрок выиграть при правильной игре обеих сторон?

24.1.8. Двое играющих по очереди ломают палку: первый на две части, затем второй ломает любой из кусков на две части, затем первый — любой из кусков на две части и т. д. Один из игроков выигрывает, если сможет после какого-то из своих ходов сложить из 6 кусков два равных треугольника. Может ли другой ему помешать?

Игры-шутки

В *играх-шутках* побеждает всегда одна из сторон независимо от её желания.

24.1.9. (а) На столе лежат 2015 кучек по одному ореху. За один ход разрешается объединить две кучки в одну. Двое играющих делают

ходы по очереди, кто не сможет сделать ход, тот проигрывает. Кто выиграет?

(b) То же, но разрешается объединять кучки только с одинаковым числом орехов.

24.1.10. Дана клетчатая полоса $1 \times N$. Двое играют в следующую игру. На очередном ходу первый игрок ставит в одну из свободных клеток крестик, а второй — нолик. Не разрешается ставить в соседние клетки два крестика или два нолика. Проигрывает тот, кто не может сделать ход. Кто из игроков выигрывает при правильной игре? Как он должен для этого играть?

Кроме игр-шуток бывают и *почти шутки*, где выигрышная стратегия такова: если есть выигрыш в один ход, его надо сделать, иначе можно делать любой ход. Или, наоборот: делать любой ход, кроме тех, которые проигрывают в один ход. В таких играх важно догадаться, кому обязательно представится возможность сделать выигрышный ход или кто будет вынужден сделать проигрывающий ход, — и доказать это. Кроме того, выигрышная стратегия может состоять в достижении позиции, после которой игра превращается в игру-шутку с нужным исходом.

24.1.11. В десяти корзинах лежат яблоки: 1, 3, 5, ..., 19 яблок. Сначала берёт одно яблоко из любой корзины Вася, потом — Гена, потом Лёва, потом опять Вася и т. д. по кругу. Проигрывает тот, после чьего хода в каких-то корзинах станет яблок поровну. Кто из них не может избежать проигрыша?

24.1.12. Из спичек сложен клетчатый квадрат 9×9, сторона каждой клетки — одна спичка. Петя и Вася по очереди убирают по спичке, начинает Петя. Выиграет тот, после чьего хода не останется целых квадратиков 1×1. Кто может действовать так, чтобы обеспечить себе победу, как бы ни играл его соперник?

Выращивание дерева позиций

Один из универсальных способов анализа игры — *выращивание дерева позиций*.

24.1.13. *Ферзя — в угол, или «цзяньшицзы».* Ферзь стоит на d1. Двое по очереди ходят им по направлению вверх, вправо или вправо-вверх. Выигрывает тот, кто поставит его на h8. Кто выигрывает при правильной игре и как он должен для этого играть?

Если не получается, подумайте сначала над следующим вопросом.

24.1.14.° Кто выигрывает в игре из предыдущей задачи, если в начальный момент ферзь стоит на клетке f4? Выберите верный вариант ответа:

1) первый игрок; 2) второй игрок.

Выращивание дерева позиций означает полный анализ игры. Перейдём теперь к более сложной идее *передачи хода*, которая помогает даже тогда, когда для полного анализа нет никакой возможности.

Передача хода

24.1.15. В *двухходовых* шахматах фигуры ходят по обычным правилам, только за каждый ход разрешается сделать ровно два хода одной фигурой. Цель игры — съесть короля соперника. Правила троекратного повторения позиции и 50 ходов не действуют[10]. Докажите, что белые в двухходовых шахматах могут играть так, что заведомо не проиграют (т. е. либо выиграют, либо сыграют вничью).

24.1.16.° Правила *шахмат без цугцванга*[11] отличаются от правил обычных шахмат только добавлением возможности пропустить свой ход для каждого из игроков. Могут ли чёрные выиграть при правильной игре белых? Выберите верный вариант ответа:

1) могут; 2) не могут.

[10] Если не знаете, что это за правила, игнорируйте это предложение.

[11] *Цугцвангом* в шахматах называется такая позиция для игрока, в которой любой его ход эту позицию ухудшает.

Данный параграф посвящён простейшим понятиям и применениям теории вероятности. Для его изучения необходимо знакомство с основами комбинаторики, например с п. 20.1 «Подсчёт числа способов» и 20.3 «Формула включений и исключений» данной книги. Кроме того, знакомство с теорией вероятностей полезно начинать на «физическом» уровне строгости, как в книге [Shen],[Kolm]. Здесь же мы сразу даём «математические» определения. Однако мы приводим многие задачи на «практическом» языке и показываем на примерах, как их формализовать. Формализацию остальных задач оставляем читателю. Такая формализация является первым шагом решения, от которого может зависеть ответ. См., например, задачи 25.2.7 (c),(d), 25.4.14, 25.3.5, [GDI, задачи 6.3.1.b и 6.3.3.c].

25.1 Классическое определение вероятности (1). *А. А. Заславский, А. Б. Скопенков*

Рассмотрим эксперимент, имеющий m равновозможных исходов, например бросание игральной кости, вытаскивание карты из колоды и т. д. Если интересующее нас событие (например, выпадение шестёрки, вытаскивание туза и т. д.) происходит в a из этих исходов, то *вероятность* события считают равной $p = a/m$.

Это пояснение полезно для начинающего, но не является математическим определением. Вот математическое определение.

Вероятностью подмножества A конечного множества M называется число

$$P(A) = P_M(A) := |A|/|M|.$$

Далее, если не оговорено противное, множество M фиксировано и пропускается из обозначений. Тогда вероятность определена для всех его подмножеств. Их часто называют *событиями*.

25.1.1. Из колоды в 52 карты вытаскивается одна карта. Найдите вероятность того, что она окажется

(a) чёрной масти; (b) тузом; (c) картинкой;

(d) дамой пик; (e) королём или бубной.

Например, в задаче 25.1.1 (c) множество M («всех возможных исходов») совпадает с множеством карт в колоде, а множество A

(«исходов, в которых происходит рассматриваемое событие») — с множеством картинок. Так эта и многие другие вероятностные задачи могут быть строго сформулированы на комбинаторном языке.

25.1.2. Монета бросается 3 раза. Найдите вероятность выпадения
(a) трёх орлов; (b) двух орлов и решки.

25.1.3. Пассажиру купейного вагона удобно, если все его попутчики одного с ним пола. Какая часть пассажиров испытывает удобства?

25.1.4. Найдите вероятность того, что при бросании двух игральных костей
(a) на первой выпадет больше очков, чем на второй;
(b) сумма выпавших очков составит $2, 3, \ldots, 12$.

25.1.5. Найдите вероятность того, что случайное целое число от 1 до 105
(a) делится на 5; (b) делится на 7; (c) делится на 35.
(a′, b′, c′) То же для случайного целого числа от 1 до 100.

Для решения некоторых из вышеприведённых задач полезны следующие.

25.1.6. (a) **Правило сложения.** Пусть $A \cap B = \emptyset$. Выразите $P(A \cup B)$ через $P(A)$ и $P(B)$.
(b) Выразите вероятность $P(A \cup B)$ через $P(A)$, $P(B)$ и $P(A \cap B)$.
(c) **Правило умножения.** Выразите вероятность $P_{M\times N}(A \times B)$ через $P_M(A)$ и $P_N(B)$.
Комментарий: $P_M(A) = P_{M\times N}(A \times N)$ и $P_N(B) = P_{M\times N}(M \times B)$.

Следующее определение обобщает ситуацию правила умножения 25.1.6 (c). Подмножества (т. е. события) A и $B \neq \emptyset$ конечного множества M *независимы*, если доля (т. е. вероятность) множества $A \cap B$ в B равна доле (т. е. вероятности) множества A в M. Приведём симметричную переформулировку, которая работает и для $B = \emptyset$. Подмножества A и B конечного множества M называются *независимыми*, если

$$|A \cap B| \cdot |M| = |A| \cdot |B|.$$

Основной пример независимых подмножеств — в множестве всех клеток шахматной доски подмножество клеток в первых трёх её строках и подмножество клеток в последних четырёх её столбцах, или, более строго, $A \times N$ и $M \times B$ в $M \times N$.

25.1.7. Зависимы ли следующие подмножества? (Мы называем *зависимыми* подмножества, не являющиеся независимыми.)

(a) Подмножества $\{1,2\} \subset \{1,2,3,4\}$ и $\{1,3\} \subset \{1,2,3,4\}$.

(b) Подмножества $\{1,2\} \subset \{1,2,3,4,5,6\}$ и $\{1,3\} \subset \{1,2,3,4,5,6\}$.

25.1.8. Зависимы ли следующие подмножества множества целых чисел от 1 до 105?

(a) Подмножество чисел, делящихся на 5, и подмножество чисел, делящихся на 7.

(b) Подмножество чисел, делящихся на 15, и подмножество чисел, делящихся на 21.

(c) Подмножество чисел, делящихся на 15, и подмножество чисел, делящихся на 5.

(d) Подмножество чисел, делящихся на 10, и подмножество чисел, делящихся на 7.

См. комбинаторные применения, например, в [GDI, п. 6.2].

Указания, ответы и решения

25.1.3. *Ответ*: 1/8.

25.1.5. *Ответы*: (a) 0,2; (b) $\frac{1}{7}$; (c) $\frac{1}{35}$; (a′) 0,2; (b′) 0,14; (c′) 0,02.

(a) *Решение* (написано Е. Павловым). Пусть $M = \{1,2,\ldots,105\}$ — множество всех возможных исходов, $A = \{5,10,\ldots,105\} = \{x \in M : 5 \mid x\}$ — множество благоприятных исходов. Тогда по определению вероятность множества A равна $P(A) = \frac{|A|}{|M|} = \frac{\lfloor \frac{105}{5} \rfloor}{105} = 0{,}2$.

25.1.6. *Ответы*: (a) $P(A \cup B) = P(A) + P(B)$;

(b) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$;

(c) $P_{M\times N}(A \times B) = P_M(A)P_N(B)$.

25.2 Более общее определение вероятности (1). *А. А. Заславский, А. Б. Скопенков*

Вероятность того, что целое число от 1 до 100 делится на 7, равна 0.14 (задача 25.1.5.b′). Вероятности того, что при одновременном бросании двух монет будет 0, 1 или 2 орла, равны 0.25, 0.5 и 0.25, соответственно. Часто удобно считать «элементарными» исходами именно «делимость на 7» или «выпадение 0, 1 или 2 орлов». Иногда такие исходы возникают и без «разложения в более элементарные».

Для формализации следующее более общее определение. Пусть задано конечное множество M и каждому $m \in M$ поставлено в соответствие неотрицательное число $P(m)$, причём сумма всех этих чисел равна 1. Тогда *вероятностью* события A называется сумма чисел $P(m)$ по всем $m \in A$. Такая пара (M, P) называется *(конечным) вероятностным пространством*, ср. [CLRS].

25.2.1. (Загадки) Сформулируйте и докажите аналог правила
(a) сложения; (b) умножения
для вышеприведённого обобщения.

Подмножества A и B множества M с указанным отображением $P : M \to [0, 1]$ называются *независимыми*, если $P(A \cap B) = P(A) \cdot P(B)$.

25.2.2. (a) Один стрелок попадает в цель с вероятностью 0,8, другой — 0,7. Найдите вероятность поражения цели, если оба стреляют одновременно.

(b) Рабочий обслуживает три станка. Вероятности их остановки равны соответственно 0,1; 0,2; 0,15. Найдите вероятность безотказной работы всех станков.

(c)* Отец, мать и сын увлекаются шахматами. Отец обещает сыну приз, если он выиграет две партии подряд из трёх, сыгранных поочерёдно с отцом и матерью. Сын знает, что отец играет лучше матери. С кем ему выгоднее играть первую партию?

25.2.3. (a) Вероятность рождения мальчика равна 0,515. Найдите вероятность того, что среди 6 детей не более 2 девочек.

(b)* (Загадка) Старик ловил неводом рыбу ровно тридцать лет и три года. Каждый день он ловил ровно 7 рыб, которых как раз

хватало на ужин. Живущий у старухи кот-долгожитель ест только макрель, которая ловится вдвое реже остальных рыб. В результате он 700 раз оставался голодным. Плавает ли макрель в море косяками или поодиночке?

Комментарий. Конечно, точно ответить на поставленный вопрос невозможно. Однако можно оценить, какая из двух гипотез лучше согласуется с данными. Ср. с законом больших чисел 25.5.3.b.

Схемой Бернулли из n испытаний с вероятностью успеха p (каждого испытания) называется множество $\mathbb{Z}_2^n$ упорядоченных наборов длины n из 0 и 1, вместе с функцией $P : \mathbb{Z}_2^n \to [0,1]$, определенной формулой $P(x) = p^{|x|}(1-p)^{n-|x|}$, где $|x|$ — количество единиц в наборе x, т.е. *число успехов* для набора x. Схема Бернулли являются одной из фундаментальных теоретико-вероятностных моделей, возникающей во многих задачах.

25.2.4. В схеме Бернулли из n испытаний с вероятностью успеха p найдите

(a) вероятность ровно k успехов;

(b) наиболее вероятное значение числа успехов.

Приведённое определение вероятности можно обобщить на случай бесконечного множества M. (В этом случае для всех $m \in M$, кроме счётного числа, $P(m) = 0$.) Ещё более интересно следующее обобщение.

25.2.5. Найдите вероятность того, что случайная точка правильного треугольника лежит

(a) в треугольнике, образованном средними линиями;

(b) во вписанном круге.

(Формализация приводится после условий.)

Пусть $A \subset M$ — подмножества прямой (или плоскости, или пространства), имеющие длину (или площадь, или объем). Не все подмножества имеют длину (или площадь или объём), см. замечание в п. 26.5 «принцип Дирихле и его применения в геометрии». Тогда *вероятностью* подмножества A в M называется число

$$P(A) = P_M(A) := L(A)/L(M),$$

где $L(A), L(M)$ — длины (или площади, или объемы) подмножеств.

Как и в дискретном случае, когда множество M фиксировано, его подмножества, имеющие длину (или площади, или объемы), часто называются *событиями*.

25.2.6.* Сформулируйте и докажите аналоги правил суммы и произведения для вышеопределенных «геометрических» вероятностей.

25.2.7.* (a) Дуэли в городе Осторожности редко кончаются печальным исходом. Дело в том, что каждый дуэлянт прибывает на место встречи в случайный момент времени между 5 и 6 часами утра и, прождав соперника 5 минут, удаляется. В случае же прибытия последнего в эти 5 минут дуэль состоится. Какая часть дуэлей действительно заканчивается поединком?

(b) Стержень случайным образом ломают на три части. С какой вероятностью из этих частей можно составить треугольник?

(c) Найдите вероятность того, что случайный треугольник является остроугольным.

(d) С какой вероятностью случайная хорда в круге длиннее стороны вписанного в этот круг правильного треугольника?

Парадоксально, что у каждого из пунктов (c) и (d) имеются разные естественные формализации, дающие разный ответ!

Указания, ответы и решения

25.2.2. (a) *Ответ*: $1 - (1 - 0{,}7)(1 - 0{,}8) = 0{,}94$.

(c) *Ответ*: с отцом.

Решение. Обозначим через p_1 и p_2 вероятность выигрыша одной партии у отца и у матери соответственно: $0 < p_1 < p_2$. Обозначим через M множество строк длины 3 из символов 0 и 1 (для каждого $k = 1, 2, 3$ символ на k-м месте "кодирует" результат k-й партии). Обозначим через $P_1(m)$ и $P_2(m)$ вероятности элемента $m \in M$ в случае, когда первая партия играется с отцом и с матерью соответственно. Эти вероятности определяются правилом произведения 25.2.1. В частности, $P_1(111) = p_1p_2p_1$, $P_1(110) = P_1(011) = (1 - p_1)p_2p_1$, $P_2(111) = p_2p_1p_2$, $P_2(110) = P_2(011) = (1 - p_2)p_1p_2$.

Чтобы каждая из этих частей была меньше суммы двух других, изображающая разлом точка в правильном треугольнике должна лежать в правильном треугольнике, образованном средними линиями. Поэтому искомая вероятность равна 1/4.

(c) *Первая интерпретация условия. Ответ*: $12\ln 2 - 8$. Каждому разлому стержня из п. (b) можно сопоставить треугольник, составленный из получившихся кусков. При этом полученный треугольник остроугольный, если и только если сумма квадратов длин любых двух кусков больше квадрата длины третьего.

Вторая интерпретация условия. Ответ: 1/4. Каждому разлому стержня из п. (b) можно сопоставить вспомогательный треугольник, величины *углов* которого относятся как длины получившихся кусков. При этом составить из кусков треугольник можно тогда и только тогда, когда вспомогательный треугольник остроугольный. Поэтому естественно считать, что искомая вероятность равна полученной в п. (b) величине.

(d) Если считать равномерно распределенными на окружности концы хорды, получаем 1/3. Если середина хорды равномерно распределена в круге, то 1/4. А, если зафиксировать перпендикулярный хорде диаметр и равномерно выбирать точку на нем, то 1/2.

25.3 Условная вероятность (1). *А. А. Заславский, А. Б. Скопенков*

25.3.1. Федя знает ответы на 10 вопросов из 30. Билет состоит из двух вопросов. С какой вероятностью Федя ответит на оба вопроса?

25.3.2. (a) В ящике лежат красные и чёрные носки. Какое минимальное количество носков может быть в ящике, если вероятность того, что два случайно вытянутых носка красные, равна 1/2?

(b) То же, если дополнительно известно, что число чёрных носков чётно.

25.3.3.* (a) С какой вероятностью треугольник, образованный тремя случайными вершинами правильного $2n$-угольника, будет прямоугольным; остроугольным; тупоугольным?

(b) Найдите пределы полученных вероятностей при $n \to \infty$. (Подумайте о смысле полученных результатов. Ср. с задачей 25.2.7 (c).)

25.3.4. Два дворянина из свиты короля в ожидании выхода его Величества решили сыграть в кости. Они сделали одинаковые ставки и договорились, что тот, кто первым выиграет 10 партий, получает все деньги. При счёте 9:8 появился король и игру пришлось закончить. Как следует поделить деньги?

Это одна из задач, положивших начало теории вероятностей. (Решить её вам будет проще после задачи 25.3.11.) В XVII в. её предложил великому французскому математику Блезу Паскалю его знакомый — один из тех дворян, о которых говорится в задаче. Паскаль понял, что следует поделить деньги пропорционально шансам, которые имели игроки на окончательную победу в момент остановки игры. Он нашёл способ вычисления этих шансов (для любого счёта). Другой метод решения задачи, приводящий к тому же результату, нашёл другой великий математик XVII в. Пьер Ферма. Их методы основаны на следующем понятии.

Условной вероятностью подмножества A при условии подмножества B, для которого $P(B) \neq 0$, называется отношение

$$P(A|B) = P(A \cap B)/P(B).$$

Ясно, что независимость подмножеств A и B равносильна тому, что $P(A|B) = P(A)$.

25.3.5. (a) Известно, что при броске игральной кости выпало чётное число. Найдите вероятность того, что оно меньше 5.

(b) **Парадокс мальчика и девочки.** В семье два ребёнка. Известно, что один из них мальчик. Найдите вероятность того, что второй ребёнок тоже мальчик. (Мы предполагаем, что вероятности рождения мальчика и девочки равны половине и что пол второго ребёнка не зависит от пола первого.)

Для определения вероятности из предыдущего пункта независимость и условная вероятность определяются аналогично.

25.3.6. Лампочки выпускаются двумя заводами, причём первый из них производит 70 % всей продукции. Лампочки, произведённые первым заводом, горят с вероятностью 0,98, вторым — 0,95. Найдите вероятность того, что купленная лампочка горит.

Решение этой задачи обобщает следующий факт.

25.3.7. Формула полной вероятности. Если $P : M \to [0,1]$ — вероятностная функция, $M = B_1 \sqcup \ldots \sqcup B_n$ и $P(B_j) \neq 0$ (говорят, что $B_1, \ldots, B_n$ — *полная система событий*), то

$$P(A) = P(A|B_1)P(B_1) + \ldots + P(A|B_n)P(B_n).$$

25.3.8. Победитель в поединке двух боксёров определяется большинством голосов трёх судей. Двое судей выносят верное решение с вероятностью p, а третий голосует, бросая монету. Найдите вероятность принятия судьями верного решения.

25.3.9.* Правила распространённой в ряде стран игры следующие: игрок бросает две кости. Он выигрывает, если сумма выпавших очков равна 7 или 11, и проигрывает, если она равна 2, 3 или 12. Во всех остальных случаях он бросает кости до тех пор, пока не выиграет, выбросив первоначальную сумму, или не проиграет, выбросив 7. Найти вероятность выигрыша.

25.3.10. Лампочки выпускаются двумя заводами, причём первый из них производит 70 % всей продукции. Лампочки, произведённые первым заводом, горят с вероятностью 0,98, вторым — 0,95. Купленная лампочка оказалась бракованной. Найдите вероятность того, что она выпущена первым заводом.

Решение этой задачи обобщает следующий факт.

25.3.11. Формула Байеса. Для любых вероятностной функции $P : M \to [0,1]$ и подмножеств $A, B \subset M$ выполнено $P(B|A) = P(A|B)P(B)/P(A)$.

Часто применяется следствие формул 25.3.7 и 25.3.11:

$$P(X|A) = \frac{P(A|X)P(X)}{P(A|B_1)P(B_1) + \ldots + P(A|B_n)P(B_n)}.$$

25.3.12. Вероятность того, что изделие бракованное, равна 0,04. Если изделие бракованное, то оно пройдёт тест с вероятностью 0,05, а иначе — с вероятностью 0,98. Найдите (с точностью до 0,0001) вероятность того, что изделие, дважды выдержавшее тест, бракованное.

25.3.13. Король Артур проводит рыцарский турнир по системе с выбыванием. Среди 2^n одинаково искусных рыцарей два близнеца. Найдите вероятность их встречи.

25.3.14.* **Разборчивая невеста.** (Загадка.) Девушка выбирает себе жениха из n претендентов, поочерёдно делающих ей предложение. Каждое предложение она может принять (тогда всё заканчивается) или отвергнуть (отвергнутый претендент с повторным предложением не обращается). Она хочет действовать так, чтобы вероятность выбрать наиболее достойного жениха была наибольшей.

(a) Докажите, что оптимальная стратегия имеет следующий вид: отвергнуть первые $s(n)$ предложений, а затем принять первое предложение от претендента, превосходящего всех предыдущих.

(b) Определите оптимальное значение $s(n)$.

Указания, ответы и решения

25.3.1. *Ответ*: $\frac{3}{29}$.

Решение (написано П. Белопашенцевой). Обозначим через M множество всех неупорядоченных пар различных чисел от 1 до 30. Это множество соответствует множеству всех возможных билетов. Количество элементов в M равно $|M| = \binom{30}{2}$.

Обозначим через A множество всех неупорядоченных пар различных чисел от 1 до 10. Множество A соответствует множеству выученных Федей билетов. Количество элементов в A есть $|A| = \binom{10}{2}$. Вероятность подмножества A в множестве M есть по определению отношение $P_M(A) = |A|/|M| = \binom{10}{2}/\binom{30}{2} = \frac{10\cdot 9/2}{30\cdot 29/2} = \frac{3}{29}$.

25.3.2. *Ответы*: (a) 4; (b) 21.

Указание. Обозначим через r и b количество красных и чёрных носков соответственно. Тогда вероятность вытащить два красных носка равна $\frac{r(r-1)}{(r+b)(r+b-1)}$. Это выражение равно $1/2$ для бесконечного множества пар (r, b), наименьшими из которых будут $(3, 1)$ и $(15, 6)$. Подробнее см. задачу 1 из книги [Mo].

25.3.3*. (a) *Ответ*: $\frac{3}{2n-1}$, $\frac{n-2}{2(2n-1)}$, $\frac{3(n-2)}{2(2n-1)}$.

Указание. Первую вершину можно считать фиксированной. Если вторая попадает в противоположную точку, то треугольник точ-

что вероятность выбрать наилучшего жениха, отвергнув k-го, является убывающей функцией от k. Поэтому пока первая вероятность меньше второй, женихов надо отвергать, а когда первая вероятность станет больше, надо принять предложение первого жениха, превосходящего всех предыдущих.

(b) Если невеста действует по описанной стратегии, то она получает лучшего жениха при выполнении следующих двух условий: номер k этого жениха больше $s = s(n)$ и лучший из первых $k-1$ женихов попадает в число первых s. Вероятность этого равна $\frac{1}{n}\left(1 + \frac{s}{s+1} + \ldots + \frac{s}{n-1}\right)$, что примерно равно $\frac{s}{n}\ln(n/s)$. Потому оптимальное значение s примерно равно $\frac{n}{e}$. При этом вероятность выбрать лучшего жениха при больших n примерно равна $\frac{1}{e}$ (см. [Mo, задача 47], [GZ]).

25.4 Математическое ожидание (3). *А. А. Заславский, А. Б. Скопенков*

25.4.1. (a) Монета подбрасывается 5 раз. Для каждого $k = 0, 1, 2, 3, 4, 5$ найдите вероятность того, что выпало k орлов.

(b) Федя знает ответы на 20 из 30 вопросов. В билет входят 3 вопроса. Для каждого $k = 0, 1, 2, 3$ найдите вероятность того, что Федя сможет ответить на k вопросов.

Пусть дано конечное или счётное множество M и для каждого элемента $m \in M$ задано число (вероятность) $P(m) \geqslant 0$, причем $\sum\limits_{m\in M} P(m) = 1$. *Случайной величиной* называется функция $\xi : M \to Y$ (обычно $Y = \mathbb{Z}_2, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$ — числовое множество). *Распределением* случайной величины ξ называется функция $p_\xi : Y \to [0, 1]$, заданная формулой

$$p_\xi(y) := \sum_{\xi(m)=y} P(m).$$

Комментарии. Как правило, при изучении случайной величины не требуется знать, на каком множестве она определена. Достаточно знать только её распределение.

Если $Y = \mathbb{R}$, то *функцией распределения* называется функция $F_\xi : Y \to [0,1]$, заданная формулой $F_\xi(y) := \sum\limits_{\xi(m)<y} P(m)$.

25.4.2. (a) Вам предлагается такая игра. Вы платите 2 конфеты, затем бросается игральная кость, и вы получаете столько конфет, сколько очков выпадает. Выгодна ли вам эта игра?

(b) Правила те же, только в случае выпадения 1 очка вы платите 100 конфет. (У вас достаточно конфет, чтобы заплатить.) Выгодна ли вам эта игра?

(c) Вы кладете в банк 8 конфет, после чего бросается игральная кость. Если выпадает 2, 3 или 4 очка, то вы получаете назад свой вклад плюс еще 1 конфету вдобавок. Если выпадает 5 или 6 очков («рост рынка»), то вы получите даже плюс 2 конфеты вдобавок. А если выпадет 1 очко, то это «кризис», и вы теряете весь свой вклад. Выгодна ли вам эта игра?

(d) В распространённой азартной игре игрок может делать ставку на один из номеров от 1 до 6. Бросаются 3 кости, и если выбранный номер выпал хотя бы на одной, то игрок получает свою ставку плюс столько же за каждое появление выбранного номера. Выгодна ли игра для игрока?

25.4.3. (a) *Cherchez la femme.* На русско-французской встрече не было представителей других стран. Суммарное количество денег у французов оказалось больше суммарного количества денег у русских, и суммарное количество денег у женщин оказалось больше суммарного количества денег у мужчин. Обязательно ли на встрече была француженка?

(b) Денежные купюры разного достоинства и разных стран упакованы в два чемодана. Средняя стоимость купюры равна 100 рублям. Общее число купюр в левом чемодане больше, чем в правом. Обязательно ли в левом чемодане найдется купюра стоимостью не более 200 рублей? (Ср. с неравенством Маркова 25.4.4.c.)

(c)* Для любых целых $l, q > 0$ существует граф, не содержащий несамопересекающихся циклов длины менее l и который невозможно правильно раскрасить в q цветов.

Утверждение 25.4.3.c доказывается при помощи излагаемой ниже теории, см. [GDI, §6.3].

Математическим ожиданием или *средним значением* случайной величины $\xi : M \to Y$ называется сумма

$$\mathbb{E}\xi := \sum_{m \in M} \xi(m) P(m).$$

Комментарий. Если множество M бесконечно, то это определение нуждается в уточнении. Сумма ряда в правой части называется *математическим ожиданием*, только когда этот ряд сходится абсолютно. В противном случае говорят, что у случайной величины *не существует математического ожидания*. В дальнейшем мы предполагаем, что для всех рассматриваемых случайных величин математические ожидания существуют.

25.4.4. Пусть $\xi : M \to \mathbb{R}$ — случайная величина и $a \in \mathbb{R}$.

(a) Пусть $\xi(m) = a$ для любого $m \in M$. Найдите $\mathbb{E}\xi$.

(b) Если $\mathbb{E}\xi \leqslant a$, то существует $m \in M$, для которого $\xi(m) \leqslant a$.

(c) *Неравенство Маркова.* $P(|\xi| > a) \leqslant \mathbb{E}|\xi|/a$ для любого $a > 0$.

(Здесь через $|\xi| > a$ сокращённо обозначено событие $\xi^{-1}(a, +\infty)$. Ср. с задачей 25.4.3.b.)

25.4.5. (a,b) В задачах 25.4.1.ab найдите средние значения количества орлов и правильных ответов, соответственно.

(c) В схеме Бернулли из n испытаний с вероятностью успеха p найдите среднее значение числа успехов.

25.4.6. Пусть $\xi, \eta : M \to \mathbb{R}$ — случайные величины.

(a) $\mathbb{E}(a\xi) = a\mathbb{E}\xi$ для любого $a \in \mathbb{R}$.

(b) $\mathbb{E}(\xi + \eta) = \mathbb{E}\xi + \mathbb{E}\eta$.

(c) $\mathbb{E}\xi = \sum\limits_{y \in Y} y p_\xi(y)$.

25.4.7. Найдите

(a) наиболее вероятное; (b) среднее

число бросков кубика до появления первой шестерки.

25.4.8. Кубик бросается до первого появления числа, меньшего 6, но не более четырёх раз. Найдите среднее число бросков.

25.4.9. Каждая из двух одинаковых колод карт перетасовывается, и карты последовательно парами выкладываются на стол. Найдите среднее значение числа пар, карты в которых совпадают.

25.4.10. Предприниматели предоставляют всем рабочим выходной, если хотя бы у одного из них день рождения. Остальные дни являются рабочими. Сколько человек нужно принять на работу, чтобы среднее значение числа рабочих человекодней было максимальным?

25.4.11. В ряд в случайном порядке выписаны m единиц и n нулей. Найдите среднее число серий из k одинаковых цифр подряд.

25.4.12. Из колоды в 52 карты вынимаются карты до первого туза. Сколько карт в среднем будет вынуто?

25.4.13. По узкой дороге в одном направлении едут n машин. Вначале скорости всех машин различны. Каждая машина едет с постоянной скоростью, пока не догонит едущую впереди, после чего едет со скоростью передней машины. В результате через достаточно большое время машины разбиваются на несколько групп. Найдите среднее значение числа групп.

25.4.14. (Загадка.) Площадка имеет форму квадрата со стороной 350 м. При измерении стороны вероятность ошибки ± 10 м равна 0,16, ± 20 м — 0,08, ± 30 м — 0,05. Найдите среднее значение измеренной площади.

Комментарий. На самом деле ответ на этот вопрос зависит от того, как формализовано понятие измерения площади. Если независимо измерить каждую из сторон квадрата и перемножить полученные значения, то по задаче 25.4.15.c среднее значение будет равно 350^2 м^2. Если же измерить только одну сторону и возвести результат в квадрат, то ответ будет другим.

25.4.15. (a) (Загадка) Можно ли выразить $\mathbb{E}\xi\eta$ через $\mathbb{E}\xi$ и $\mathbb{E}\eta$?

(b) *Неравенство Коши-Буняковского.* Если $\xi(m), \eta(m) \geqslant 0$ для любого $m \in M$, то $(\mathbb{E}\xi\eta)^2 \leqslant \mathbb{E}\xi^2\mathbb{E}\eta^2$.

(c) Событие $\xi^{-1}(y) = \{m \in M\colon \xi(m) = y\}$ в дальнейшем сокращённо обозначается $\xi = y$. Случайные величины ξ и η называются

независимыми, если события $\xi = x$ и $\eta = y$ независимы при любых $x, y \in Y$, т. е.

$$P(m \in M\colon \xi(m) = x \text{ и } \eta(m) = y) = p_\xi(x)p_\eta(y).$$

Неформально независимость означает, что значения одной из случайных величин не влияют на распределение другой. Например, для схемы Бернулли любые две из определённых на множестве $\mathbb{Z}_2^n$ случайных величин $\xi_i(x_1, \ldots, x_n) := x_i$, $i = 1, \ldots, n$, независимы.

Докажите, что если случайные величины ξ и η независимы, то математическое ожидание их произведения равно произведению их математических ожиданий: $\mathbb{E}\xi\eta = \mathbb{E}\xi\mathbb{E}\eta$.

Указания, ответы и решения

Большинство решений получены редактированием текстов, написанных Т. Чергановым.

25.4.1. (a) *Ответ:* $p(0) = p(5) = \frac{1}{32}$, $p(1) = p(4) = \frac{5}{32}$, $p(2) = p(3) = \frac{10}{32}$.

(b) *Ответ:* $p(0) = \frac{6}{203}$, $p(1) = \frac{45}{203}$, $p(2) = \frac{95}{203}$, $p(3) = \frac{57}{203}$.

Решение. Множество билетов M — это множество неупорядоченных троек различных чисел от 1 до 30. Тогда $|M| = \binom{30}{3}$.

Обозначим через A_0 множество неупорядоченных троек различных чисел от 21 до 30. Тогда $P(A_0) = \binom{10}{3}/\binom{30}{3} = \frac{6}{203}$.

Обозначим через A_1 множество неупорядоченных троек различных чисел, в которых два числа принадлежат $\{21, \ldots, 30\}$ и одно число принадлежит $\{1, \ldots, 20\}$. Тогда $P(A_1) = 20\binom{10}{2}/\binom{30}{3} = \frac{45}{203}$.

Аналогично $P(A_2) = 10\binom{20}{2}/\binom{30}{3} = \frac{95}{203}$ и $P(A_3) = \binom{20}{3}/\binom{30}{3} = \frac{57}{203}$.

25.4.2. (d) *Ответ:* нет.

Решение. Обозначим через ξ число выпадений выбранного номера. Тогда

$$p_\xi(0) = \frac{5^3}{6^3}, \quad p_\xi(1) = \frac{3 \cdot 5^2}{6^3}, \quad p_\xi(2) = \frac{3 \cdot 5}{6^3}, \quad p_\xi(3) = \frac{1}{6^3}.$$

Значит, математическое ожидание выигрыша при единичной ставке равно

$$\frac{2 \cdot 3 \cdot 5^2 + 3 \cdot 3 \cdot 5 + 4}{6^3} \approx 0.92 < 1.$$

25.4.15. (c) *Решение.*

$$\mathbb{E}\xi\eta = \sum_{m\in M} \xi(m)\eta(m)P(m) = \sum_{x\in X,\ y\in Y} xyP\left(\xi(m)=x, \eta(m)=y\right) =$$
$$= \sum_{x\in X,\ y\in Y} xyp_\xi(x)p_\eta(y) = \sum_{x\in X} xp_\xi(x) \sum_{y\in Y} yp_\eta(y) = \mathbb{E}\xi\mathbb{E}\eta.$$

25.5 Дисперсия и ее применения (3). *А. А. Заславский, А. Б. Скопенков*

Дисперсией случайной величины ξ называется число

$$\mathbb{D}\xi = \mathbb{E}\big((\xi - \mathbb{E}\xi)^2\big).$$

Комментарий. Если множество значений случайной величины бесконечно, то дисперсия может не существовать. В дальнейшем предполагается, что для всех рассматриваемых случайных величин дисперсия существует.

25.5.1. (a) Найдите дисперсию числа успехов для схемы Бернулли из n испытаний с вероятностью успеха p.

(b) Для любой случайной величины ξ выполнено $\mathbb{D}\xi = \mathbb{E}\xi^2 - (\mathbb{E}\xi)^2$.

(c) Для любых ли случайных величины ξ, η выполнено $\mathbb{D}(\xi+\eta) = \mathbb{D}\xi + \mathbb{D}\eta$?

(d) Для любых независимых случайных величины ξ, η выполнено $\mathbb{D}(\xi+\eta) = \mathbb{D}\xi + \mathbb{D}\eta$.

25.5.2. Кооператив отгружает железные балки. Средняя длина балки 3 м, дисперсия 0,09 м^2. Сколько балок надо заказать, чтобы с вероятностью, не меньшей чем 0,999, хотя бы 1000 из них имели длину не менее 2 м?

25.5.3. (a) **Неравенство Чебышёва.** Для любой случайной величины ξ и любого $t > 0$ выполнено

$$P\big(|\xi - \mathbb{E}\xi| \geqslant t\big) \leqslant \mathbb{D}\xi/t^2.$$

(b) **Закон больших чисел.** Обозначим через ξ число успехов в схеме Бернулли из n испытаний с вероятностью успеха p. Для любого $t > 0$ выполнено

$$P\big(|\xi - np| \geqslant t\big) \leqslant np(1-p)/t^2$$

Закон больших чисел означает, что при большом числе испытаний вероятность того, что число успехов сильно отличается от его среднего значения, мала. Аналогичный закон справедлив не только для схемы Бернулли: если наблюдать много независимых реализаций произвольной случайной величины, то их среднее арифметическое с большой вероятностью будет мало отличаться от её среднего значения. Этот закон позволяет, например, проводить социологические исследования, в которых на основе опроса некоторого количества случайно выбранных людей (достаточно большого, но составляющего малую часть всего населения) делаются выводы о распространённости в обществе тех или иных мнений и предпочтений.

25.5.4. В условиях задачи 25.2.3.b предположим, что макрель плавает

(a) поодиночке; (b) косяками.

Тогда вероятность того, что число голодных дней кота меньше 1000,

(a) больше 0.99; (b) меньше 0.0001.

Указания, ответы и решения

Большинство решений получены редактированием текстов, написанных Т. Чергановым.

25.5.1. (a) *Ответ*: $np(1-p)$.

(b) *Решение*

$$\mathbb{D}\xi = \mathbb{E}(\xi - \mathbb{E}\xi)^2 = E(\xi^2 - 2\xi\mathbb{E}\xi + (\mathbb{E}\xi)^2) = \\ = \mathbb{E}\xi^2 - 2(\mathbb{E}\xi)(\mathbb{E}\xi) + (\mathbb{E}\xi)^2 = \mathbb{E}\xi^2 - (\mathbb{E}\xi)^2.$$

26.8 Собери квадрат (3*). *М. Б. Скопенков, О. А. Малиновская, С. А. Дориченко, Ф. А. Шаров*

Этот пункт посвящён решению такой задачи (для некоторых частных случаев).

Задача. Когда из прямоугольников, подобных данному, можно составить квадрат?

В процессе решения мы познакомимся с красивыми применениями алгебры в комбинаторной геометрии, а именно — систем линейных уравнений и многочленов с целыми коэффициентами. Для решения задач необходимо первоначальное знакомство с этими темами, см., например, [Gu]. Желательно также первоначальное знакомство с задачами на разрезание, см., например, [Sa97].

Наш подход к решению развивает идеи книги [Ya68].

Другой подход к решению — это физическая интерпретация, использующая электрические цепи (хотя без неё решать проще). Познакомиться с этой физической интерпретацией и её применением к решению поставленной задачи можно в статьях [SPD, SMD]. Увлекательный рассказ об истории её возникновения можно прочитать в книге [Ga99].

Наводящие вопросы

> — У меня есть мысль! — сказал удав, открывая глаза. — Мысль. И я её думаю.
> — Какая мысль? — спросила мартышка.
> — Так сразу не скажешь...
> — Ух ты! — подпрыгнула мартышка. — Ох, какая хорошая мысль. А можно я её тоже немножко подумаю?
>
> *Г. Остёр.* Бабушка удава

26.8.1.° Верно ли, что при любых натуральных m и n из нескольких прямоугольников $m \times n$ можно сложить квадрат? Выберите верный вариант ответа:

1) верно; 2) неверно.

26.8.2. Дизайнеру заказали рамы для квадратного окна. На проектах (рис. 2.37 A, B) показано, как должны примыкать стёкла друг к другу и как они должны быть ориентированы (короткой или длинной стороной вверх). Можно ли сделать все стёкла в каждой раме подобными прямоугольниками?

A B

Рис. 2.37: Проекты оконных рам; см. задачу 26.8.2

26.8.3. Можно ли разрезать квадрат на три подобных, но неравных прямоугольника?

26.8.4. Можно ли разрезать квадрат на 5 квадратов?

26.8.5. Все полки у шкафа на рис. 2.38 C, как и все лоскутки, из которых сшито одеяло на рис. 2.38 D — квадратные. Являются ли квадратными сами шкаф и одеяло?

26.8.6. Можно ли замостить всю плоскость попарно различными квадратами, длины сторон которых — целые числа?

26.8.7. Можно ли разрезать квадрат на прямоугольники с отношением сторон $2+\sqrt{2}$? То же для $2-\sqrt{2}$, для $3+2\sqrt{2}$ и для $3-2\sqrt{2}$.

26.8.8. Является ли $1+\sqrt{2}$ суммой квадратов чисел вида $a+b\sqrt{2}$, где a и b рациональны?

C

D

Рис. 2.38: Шкаф и одеяло; см. задачу 26.8.5

Определение. Пусть на прямоугольном листе бумаги нарисовано разбиение на прямоугольники. Разрешается разрезать лист вдоль любого отрезка на два прямоугольника, потом произвести такие операции по отдельности с каждой из получившихся частей и так далее. Если таким образом можно реализовать исходное разбиение, то назовём его *тривиальным*. Например, разбиения на рис. 2.37 тривиальные, а на рис. 2.38 нетривиальные.

Следующие 4 задачи предлагается сначала решить для тривиальных разбиений, а уже потом подумать над произвольными разбиениями. В последующих подпунктах будут даны подсказки к решению этих трудных задач.

26.8.9. Какие прямоугольники можно (тривиально) разрезать на прямоугольники со стороной 1?

26.8.10. Какие прямоугольники можно (тривиально) разрезать на квадраты?

26.8.11. Можно ли квадрат (тривиально) разрезать на прямоугольники с отношением сторон $\sqrt{2}$? То же для $1+\sqrt{2}$.

Все числа, которые можно представить в виде $x = a + b\sqrt{2}$ с рациональными a и b, назовём *хорошими*.

26.8.12. (Основная задача.) При каких хороших x квадрат можно (тривиально) разрезать на прямоугольники с отношением сторон x?

Прямоугольник из квадратов.

Ты, дорога, иду по тебе и гляжу, но мне думается,
Мне думается, в тебе много такого, чего не увидишь глазами.
Уолт Уитмен. Песня большой дороги

В этом подпункте мы наметим новый вариант элементарного решения задач 26.8.10 и 26.8.12. В этом подпункте латинские буквы a, b, c, d и эти же буквы с индексами обозначают *рациональные* числа.

26.8.13. Можно ли прямоугольник $1 \times \sqrt{2}$ разрезать на квадраты с рациональными сторонами? А со сторонами, которые либо рациональны, либо имеют вид $b\sqrt{2}$? А со сторонами, которые являются произвольными хорошими числами? Те же вопросы для прямоугольников $1 \times (1 + \sqrt{2}\,)$ и $1 \times (2 + \sqrt{2}\,)$.

Для доказательства невозможности разрезаний естественно использовать площадь и её *аддитивность*: площадь целого равна сумме площадей частей. Вряд ли получится ответить на вопросы задачи 26.8.13 для прямоугольника $1 \times (2 + \sqrt{2}\,)$ без следующего обобщения понятия площади (мы обобщаем понятие площади так, чтобы площадь этого прямоугольника стала отрицательной, а площади квадратов оставались неотрицательными).

Определение. Пусть x — действительное число. Назовём *x-площадью* (или *площадью Гамеля*) прямоугольника $(a + b\sqrt{2}\,) \times (c + d\sqrt{2}\,)$ число $(a + bx)(c + dx)$. Число $\bar{s} := a - b\sqrt{2}$ назовём *сопряжённым* к числу $s = a + b\sqrt{2}$.

26.8.14. Обычная площадь прямоугольника $(a + b\sqrt{2}\,) \times (c + d\sqrt{2}\,)$ и сопряжённое к ней число — это одни из его x-площадей. Чему равно x в каждом из случаев?

26.8.15. Найдите все прямоугольники вида $(a+b\sqrt{2})\times(c+d\sqrt{2})$, x-площади которых неотрицательны при всех x.

26.8.16. Аддитивность x-площади. Если прямоугольник разрезан на конечное число прямоугольников, стороны которых — хорошие числа, то для любого $x\in\mathbb{R}$ x-площадь разрезаемого прямоугольника равна сумме x-площадей прямоугольников, на которые он разрезан.

Указание. Начните со случая разрезания на 2 прямоугольника.

26.8.17. Решите задачи 26.8.10 и 26.8.12 для частного случая, когда стороны всех квадратов и всех прямоугольников, участвующих в разрезании, — хорошие числа (разрезание не обязательно тривиально).

Для доказательства теоремы Дена в общем случае определение x-площади нам уже не годится: ведь она определена только для хороших чисел, а теперь у нас в разрезании могут присутствовать квадраты с какими угодно сторонами.

В следующих трёх задачах мы считаем, что прямоугольник $s_0\times t_0$ разрезан на прямоугольники $s_1\times t_1$, $s_2\times t_2$, …, $s_N\times t_N$, причем s_0 и t_0 несоизмеримы.

26.8.18. Обозначим

$$P=\{s_0,t_0,s_1,t_1,\ldots,s_N,t_N\}.$$

Тогда можно выбрать такие числа $e_1,e_2,\ldots,e_n\in P$, чтобы любое число $p\in P$ единственным образом представлялось в виде

$$p=as_0+bt_0+a_1e_1+a_2e_2+\ldots+a_ne_n.$$

Указание. Начните с примера, изображённого на рис. 2.39.

Зафиксируем набор чисел s_0, t_0, e_1, e_2, …, e_n из задачи 26.8.18. Он называется *базисом*.

Определение. Пусть y — действительное число. Назовём *y-площадью* прямоугольника со сторонами

$as_0+bt_0+a_1e_1+a_2e_2+\ldots+a_ne_n$ и $cs_0+dt_0+c_1e_1+c_2e_2+\ldots+c_ne_n$

число $(a+by)(c+dy)$.

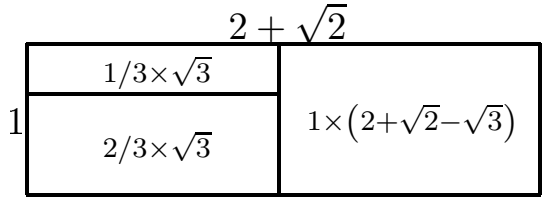

Рис. 2.39: К построению базиса

Обратите внимание на то, что при $y = x$ и хороших несоизмеримых s_0, t_0 это определение не всегда эквивалентно определению x-площади выше!

26.8.19. Вычислите y-площадь разрезаемого прямоугольника $s_0 \times t_0$. Является ли она неотрицательной при всех y?

26.8.20. Докажите, что для любого y y-площадь разрезаемого прямоугольника $s_0 \times t_0$ равна сумме y-площадей прямоугольников, на которые он разрезан.

26.8.21. Теорема Дена. Если прямоугольник разрезан на квадраты (не обязательно равные), то отношение его сторон рационально.

26.8.22. Если квадрат 1×1 разрезан на прямоугольники, отношение сторон каждого из которых — хорошее число, то и сами стороны всех прямоугольников — хорошие числа.

От разрезаний к корням многочленов

Вот испытанье для мудрых,
Для мудрости, не пройденной в школе...
Уолт Уитмен. Песня большой дороги

26.8.23. Из нескольких прямоугольников с отношением сторон r составили прямоугольник. Докажите, что стороны полученного прямоугольника относятся как $P(r) : Q(r)$, где $P(x)$ и $Q(x)$ — некоторые многочлены с целыми коэффициентами.

26.8.24. Эти многочлены можно выбрать так, что $P(-x)/Q(-x) = -P(x)/Q(x)$ при всех x и $P(x)/Q(x) > 0$ при всех $x > 0$.