КВАДРАТИЧНЫЕ ИРРАЦИОНАЛЬНОСТИ

А. Белов-Канель, П. Козлов и А. Скопенков

Понял ты или нет,
Отчего мы жили так странно две тысячи лет?
Б. Гребенщиков, Вавилон.

Введение.

Теорема Гаусса. *Калькулятор (вычисляющий числа с абсолютной точностью) имеет кнопки*

$$1, \quad +, \quad -, \quad \times, \quad : \quad \text{и} \quad \sqrt{}$$

(и неограниченную память). На этом калькуляторе можно вычислить число $\cos\dfrac{2\pi}{n}$ *тогда и только тогда, когда* $n = 2^\alpha p_1 \dots p_l$*, где* $p_1, \dots, p_l$ *— различные простые числа вида* $2^{2^s}+1$.

(Переформулировка теоремы Гаусса в терминах построений циркулем и линейкой правильных многоугольников приводится в отступлении и не используется в остальном тексте. История этой знаменитой теоремы приводится в [Gi]. *Невозможность* в этой теореме не была явно доказана Гауссом [Ga], однако второе доказательство невозможности в настоящей заметке можно принять за рассуждение Гаусса.)

В этой заметке предлагается набросок *элементарного доказательства приведенной теоремы.* Оно не использует терминов 'группа Галуа' (даже термина 'группа') и 'поле' (доказательство невозможности использует квадратичные расширения только *множества рациональных чисел*). Несмотря на отсутствие *терминов*, *идеи* приводимых доказательств — *группируй и властвуй* или *объединяй и властвуй* — являются отправной точкой для теории Галуа (см. философское отступление).

Приводимое доказательство известно в математическом фольклоре, однако авторам не удалось найти его в явном виде в литературе.

(Элементарное доказательство *возможности* для $n = 17$ приводится в [Ch, Gi, Po, PS, Ko]. Для общего случая оно намечено в [Ga, Gi], где ясности мешает построение общей теории вместо доказательства конкретного результата.) Относительно простое доказательство *невозможности* в [Vi, гл. 5] использует понятие 'расширения поля'. Это доказательство, наряду с элементарным, изложено в настоящей заметке, при этом необходимые термины не вводятся немотивированно впрок, а естественно появляются в процессе размышления над проблемой. Элементарное изложение идеи другого неэлементарного доказательства невозможности см. в [Ki]. Первое приводимое доказательство невозможности в теореме Гаусса является алгебраическим выражением этой идеи.)

Приводимые доказательства возможности и невозможности независимы друг от друга, что отражено и в нумерации задач. В этих доказательствах используется определение построимости из второго отступления и эквивалентность теоремы Гаусса аналогичной теореме для *комплексного* калькулятора (задача D).

Доказательства представлены в виде циклов задач. Решение задач потребует от многих читателей усилий (впрочем, опытный математик, не знакомый с теорией Галуа, с легкостью восстановит решения по приведенным указаниями или даже без них). Однако эти усилия будут сполна оправданы тем, что вслед за великими математиками в процессе изучения интересной проблемы читатель познакомится с некоторыми основными идеями алгебры. Надеюсь, это поможет читателю совершить собственные настолько же полезные открытия (не обязательно в математике)!

Если условие задачи является утверждением, то в задаче требуется это утверждение доказать.

Эта заметка представлялась П. Дергачом и авторами в виде цикла задач на Летней Конференции Турнира Городов в августе 2007 (до промежуточного финиша предлагалось первое отступление и доказательство построимости, а после — доказательство непостроимости). Сокращенный английский перевод (выполненный П. Дергачом и А. Скопенковым) доступен на www.mccme.ru/circles/oim/materials/constreng.pdf.

Благодарим Э. Б. Винберга, М. Н. Вялого, А. С. Голованова, П. А. Дергача, А. И. Ефимова, А. А. Казначеева, В. В. Прасолова и Г. Челнокова за полезные обсуждения.

Философское отступление.

Изложение доказательства теоремы Гаусса на языке 'групп Галуа' делает его менее доступным. Более того, мне кажется, что именно с доказательств, подобных приведенным здесь (а не с терминов), полезно начинать изучение теории Галуа.

'При изложении материала нужно ориентироваться на объекты, которые основательнее всего укореняются в человеческой памяти. Это — отнюдь не системы аксиом и не логические приемы в доказательстве теорем. Изящное решение красивой задачи, формулировки 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' [Ко, предисловие].

Мне кажется, такой стиль изложения не только сделает материал более доступным, но позволит сильным студентам (для которых доступно даже абстрактное изложение) приобрести математический вкус и стиль с тем, чтобы разумно выбирать проблемы для исследования, а также ясно излагать собственные открытия, не скрывая ошибки (или известности полученного результата) за чрезмерным формализмом. К сожалению, такое (бессознательное) сокрытие ошибки часто происходит с молодыми математиками, воспитанные на чрезмерно формальных курсах (происходило и с автором этих строк; к счастью, почти все мои ошибки исправлялись *перед* публикациями).

Приводимые порой в качестве приложений теории Галуа доказательство теоремы Гаусса и другие результаты о разрешимости уравнений в радикалах неубедительны для мотивировки этой теории (как и приложение к решению уравнений степени не выше четырех неубелительно для мотивировки общей теории разрешимости уравнений произвольной степени в радикалах). Действительно, теорема Гаусса имеет элементарное доказательство, не использующее 'групп Галуа'. Теорема Руффини-Абеля о неразрешимости в радикалах *общего* алгебраического уравнения степени 5 и выше (как и достаточность условия Кронекера неразрешимости в радикалах *конкретного* уравнения простой степени) также имеет алгебраическое доказательство, не использующее 'групп Галуа' [Ко, Pr] (и *топологическое* доказательство [Al]). В терминах теории Галуа формулируется общий критерий разрешимости *конкретного* алгебраического уравнения в радикалах, но этот критерий не дает настоящего решения проблемы разрешимости, а лишь сводит ее к трудной задаче вычисления группы Галуа уравнения.

(Возможно, именно поэтому работы Галуа были забыты на 20 лет после их выхода — пока не появилось важных задач, при решении которых уже трудно обойтись без теории Галуа. Конечно, приведенная гипотеза нуждается в серьезной проверке.)

Однако теория Галуа выходит далеко за рамки проблемы разрешимости уравнений в радикалах. Ее популяризации послужит дальнейшая публикация интересных теорем, формулируемых без понятий теории Галуа, но при попытках доказать которые она естественно возникает. Примеры таких теорем мне сообщили А. Я. 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).

Отступление: связь с построениями циркулем и линейкой.

A. Используя отрезки длины a, b и c, можно построить циркулем и линейкой отрезки длины $a+b$, $a-b$, ab/c, $\sqrt{ab}$.

Вещественное число называется *квадратичной иррациональностью*, или *построимым*, если его можно получить на нашем калькуляторе (т.е. получить из 1 при помощи сложения, вычитания, умножения, деления и извлечения квадратного корня из положительного числа). Например, числа

$$1+\sqrt{2},\quad \sqrt[4]{2}=\sqrt{\sqrt{2}},\quad \sqrt{2\sqrt{3}},\quad \sqrt{2}+\sqrt{3},\quad \sqrt{1+\sqrt{2}},\quad \frac{1}{1+\sqrt{2}}\quad \text{и}\quad \cos 3^\circ$$

построимы. Про последние два числа это не совсем очевидно.

B. Любое построимое число построимо циркулем и линейкой (далее слова 'циркулем и линейкой' опускаютя).

Этот простой (вытекающий из A) результат был известен еще древним грекам. Он показывает, что из *выразимости* в теореме Гаусса вытекает *построимость* соответствующих n-угольников.

C*. *Основная теорема теории геометрических построений.* Обратное тоже верно.

Этот несложный результат [Pr, Ko] (доказанный лишь в 19-м веке) показывает, что из *невыразимости* в теореме Гаусса вытекает *непостроимость* соответствующих n-угольников.

Для его доказательства рассмотрите все возможные случаи появления новых объектов (точек, прямых, окружностей). Покажите, что координаты всех построенных точек и коэффициенты уравнений всех проведённых прямых и окружностей являются квадратичными иррациональностями. См. детали в [Ko, Pr].

D. Если комплексное число комплексно построимо (определение аналогично, только квадратные корни извлекаются из произвольных уже выраженных чисел и можно брать любое значение квадратного корня), то его вещественная и мнимая части (вещественно) построимы.

Указание. Если $\sqrt{a+bi}=u+vi$, то u, v выражаются через квадратные радикалы через a и b.

E. Если правильный mn-угольник построим, то и правильный m-угольник построим.

F. Правильные 3-угольник и 5-угольник построимы.

G. Правильный 120-угольник построим. Или, эквивалентно, угол 3° построим.

Указание. Если не получается, то см. далее.

H. Если правильный n-угольник построим, то и правильный $2n$-угольник построим.

Указание. Получается делением угла пополам или применением формулы половинного угла.

I. Пусть правильные m- и n-угольники построимы, причем $GCD(m,n)=1$. Тогда правильный mn-угольник построим.

Указание. Так как $GCD(m,n)=1$, то существуют целые a, b такие, что $am+bn=1$.

Доказательство возможности в теореме Гаусса.

Нетрудно доказать возможность в теореме Гаусса для $n \le 16$.

Доказательство возможности в теореме Гаусса для $n=5$. Видимо, приводимый способ сложнее придуманного Вами. Зато из него будет видно, что делать в общем случае.

Достаточно выразить число $e = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$. Сразу это сделать трудно, поэтому сначала построим некоторые многочлены от e. Мы знаем, что $e+e^2+e^3+e^4 = -1$. Легко проверить, что $(e+e^4)(e^2+e^3) = e+e^2+e^3+e^4 = -1$. Обозначим $A_0 := e+e^4$ и $A_1 := e^2+e^3$. Тогда по теореме Виета числа A_0 и A_1 являются корнями уравнения $t^2+t-1=0$. Поэтому можно выразить A_0 (и A_1). Поскольку $e\cdot e^4 = 1$, то по теореме Виета числа e и e^4 являются корнями уравнения $t^2 - A_0 t + 1 = 0$. Поэтому можно выразить e (и e^4).

1. Если число 2^m+1 простое, то m — степень двойки.

Идея доказательства построимости в теореме Гаусса. Достаточно выразить число $e = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ для простого $n = 2^m+1$ (тогда m обязано быть степенью двойки).

Сначала хорошо бы разбить сумму

$$e + e^2 + \cdots + e^{n-1} = -1$$

на два слагаемых A_0 и A_1, *произведение* которых построимо (иными словами, *сгруппировать* хитрым образом корни уравнения $1+e+e^2+\cdots+e^{n-1}=0$). Тогда A_0 и A_1 построимы по теореме Виета. Затем хорошо бы разбить сумму A_0 на два слагаемых $A_0 = A_{00} + A_{01}$, произведение которых построимо, и аналогично разбить $A_1 = A_{10} + A_{11}$. И так далее, пока не построим $A_{0\ldots0} = e$.

Однако придумать нужные группировки корней уравнения $1 + e + e^2 + \cdots + e^{n-1} = 0$ совершенно нетривиально и возможно не для всех n. Как это можно придумать, описано в [Ка]. Здесь я приведу лишь ответ, который очень прост.

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

Как строить нужные группировки, видно из задач 3a, 4a и 5a ниже.

2. *Доказательство теоремы о первообразном корне.* Пусть p простое и a не делится на p.

(a) $p-1$ делится на наименьшее $k>0$, для которого $a^k \equiv 1\ (p)$.

Указание: используйте малую теорему Ферма.

(b) Для любых целых n и a сравнение $x^n \equiv a\ (p)$ имеет не более n решений.

(c) Если $p-1$ делится на d, то сравнение $x^d \equiv 1\ (p)$ имеет ровно d решений.

(d) Докажите теорему о первообразном корне для $p = 2^m+1$. (Только этот частный случай нужен для теоремы Гаусса.)

(e)* Докажите теорему о первообразном корне для $p = 2^m\cdot 3^n + 1$.

(f)* Докажите теорему о первообразном корне для *произвольного* простого p.

(g)* Верно ли, что число 3 является первообразным корнем по модулю любого простого числа вида $p = 2^m+1$?

Начиная с этого момента $p = 2^m+1 \geq 5$ — простое число и g — (любой) первообразный корень по модулю p.

3. (a) Положим

$$A_0 := e^{g^2} + e^{g^4} + e^{g^6} + \cdots + e^{g^{2^m}} \quad \text{и} \quad A_1 := e^{g^1} + e^{g^3} + e^{g^5} + \cdots + e^{g^{2^m-1}}.$$

Докажите, что $A_0 A_1 = -\frac{p-1}{4}$. (Следующие задачи являются подсказками.)

(b) $g^k + g^l \equiv 0\ (p)$ тогда и только тогда, когда $k - l \equiv \frac{p-1}{2}\ (p-1)$.

(c) $A_0 A_1 = \sum\limits_{s=1}^{2^m} e^s \alpha(s)$, где $\alpha(s)$ равно числу решений (k,l) (в вычетах по модулю $p-1$) сравнения $g^{2k} + g^{2l+1} \equiv s\ (p)$.

(d) $\alpha(s) = \alpha(gs)$.

(e) $\alpha(s)$ не зависит от $s = 1, \dots, 2^m$.

4. (a) Положим

$$A_{00} := e^{g^4} + e^{g^8} + e^{g^{12}} + \cdots + e^{g^{2^m}} \quad \text{и} \quad A_{01} := e^{g^2} + e^{g^6} + e^{g^{10}} + \cdots + e^{g^{2^m-2}}.$$

Докажите, что $A_{00}A_{01} = sA_0 + tA_1$ для некоторых целых чисел s и t ($s + t = \frac{p-1}{8}$). (Следующая задача является подсказкой.)

(b) Сравнение $g^{4k} + g^{4l+2} \equiv 1\ (p)$ имеет столько же решений (k, l) (в вычетах по модулю $p-1$), сколько сравнение $g^{4k} + g^{4l+2} \equiv g^2\ (p)$.

(c) Положим

$$A_{10} := e^{g^1} + e^{g^5} + e^{g^9} + \cdots + e^{g^{2^m-3}} \quad \text{и} \quad A_{11} := e^{g^3} + e^{g^7} + e^{g^{11}} + \cdots + e^{g^{2^m-1}}.$$

Докажите, что $A_{10}A_{11} = uA_0 + vA_1$ для некоторых целых чисел u и v ($u + v = \frac{p-1}{8}$).

(d) Закончите доказательство возможности в теореме Гаусса.

5. Найдите явно выражение через квадратные радикалы числа

(a) A_0 из задачи 3a. (b) $\cos\dfrac{2\pi}{17}$. (c)* $\cos\dfrac{2\pi}{257}$. (d)* $\cos\dfrac{2\pi}{65537}$.

При помощи приведенного метода и компьютера эту задачу можно решить быстро, несмотря на следующую историю [Li]. "Один слишком навязчивый аспирант довел своего руководителя до того, что тот сказал ему: "Идите и разработайте построение правильного многоугольника с 65 537 сторонами". Аспирант удалился, чтобы вернуться через 20 лет с соответствующим построением (которое хранится в архивах в Геттингене)."

Замечание. Построимость можно доказывать по тому же плану без использования комплексных чисел. Указание к случаю правильного 17-угольника. Положим $a_k = \cos(2\pi k/17)$. Тогда $a_k = a_{17-k}$, $2a_ka_l = a_{k+l} + a_{k-l}$ и $a_1 + a_2 + a_3 + \cdots + a_8 = -1/2$. Сначала выразите $a_1 + a_2 + a_4 + a_8$ и $a_3 + a_5 + a_6 + a_7$. Затем выразите $a_1 + a_4$, $a_2 + a_8$, $a_3 + a_5$ и $a_6 + a_7$. Наконец, выразите a_1.

Указания и решения к некоторым задачам о построимости.

Указание к 1. Если n нечётно, то $2^{kn} + 1$ делится на $2^k + 1$.

Указание к 2b. Докажем более общее утверждение: *многочлен степени n над $\mathbb{Z}_p$ не может иметь более n корней в $\mathbb{Z}_p$.* Здесь многочленом называется набор его коэффициентов, а не функция.

Пусть многочлен $P(x)$ степени n имеет в $\mathbb{Z}_p$ различные корни $x_1, \dots, x_n, x_{n+1}$. Представьте его в виде

$$P(x) = b_n(x - x_1)\dots(x - x_n) + b_{n-1}(x - x_1)\dots(x - x_{n-1}) + \cdots + b_1(x - x_1) + b_0$$

('*интерполяция Ньютона*'). Последовательно подставляя в сравнение $P(x) \equiv 0\ (p)$ вычеты $x_1, \dots, x_n, x_{n+1}$, получим $b_0 \equiv b_1 \equiv \cdots \equiv b_{n-1} \equiv b_n \equiv 0\ (p)$.

То же самое решение можно записать и так. Пусть P — многочлен. Тогда многочлен $P - P(a)$ делится на $x - a$, т.е. $P - P(a) = (x - a)Q$ для некоторого многочлена Q с $\deg Q < \deg P$. Поэтому если $P(a) = 0$, то $P = (x - a)Q$ для некоторого многочлена Q степени меньше $\deg P$. Теперь требуемое в задаче утверждение доказывается индукцией по степени многочлена P.

Первое указание к 2c. Заметьте, что многочлен $x^{p-1} - 1$ над $\mathbb{Z}_p$ имеет ровно $p-1$ корень и делится на $x^d - 1$. Докажите, что если многочлен степени a имеет ровно a корней и делится на многочлен степени b, то этот многочлен степени b имеет ровно b корней.

Второе указание к 2c. Если $p = kd$, то для любого a сравнение $y^k \equiv a\ (p)$ имеет не более k решений.

Указание к 2d. Если первообразного корня нет, то по 2a сравнение $x^{2^{m-1}} \equiv 1\ (p)$ имеет $p - 1 = 2^m > 2^{m-1}$ решений.

Указание к 2ef. Аналогично 2d.

Замечание к 2f. Из существования первообразного корня легко вывести, что для $p-1 = p_1^{a_1} \dots p_k^{a_k}$ первообразных корней ровно $(p-1)(1-\frac{1}{p_1})\dots(1-\frac{1}{p_k}) = \varphi(p-1)$.

Указание к 3c. Раскройте скобки и сгруппируйте равные слагаемые.

Указание к 3d. Если (a, b) — решение сравнения $g^{2k}+g^{2l+1} \equiv s\ (p)$, то $(b+1, a)$ — решение сравнения $g^{2k} + g^{2l+1} \equiv gs\ (p)$. Если (a, b) — решение сравнения $g^{2k} + g^{2l+1} \equiv gs\ (p)$, то $(b, a-1)$ — решение сравнения $g^{2k} + g^{2l+1} \equiv s\ (p)$.

Указание к 5c. (Написано с использованием текста И. Лукьянеца и В. Соколова.) Положим

$$\overline{i_0 \dots i_x} := i_0 2^0 + \dots + i_x 2^x \quad \text{и} \quad A_{i_0 \dots i_x} := \sum_{s=0}^{2^{m-s}} e^{g^{\overline{i_0 \dots i_x} + s 2^{x+1}}}.$$

Тогда $A_{i_0 \dots i_x 0} + A_{i_0 \dots i_x 1} = A_{i_0 \dots i_x}$. При $x < m$ имеем

$$A_{i_0 \dots i_x 0} A_{i_0 \dots i_x 1} = \sum_{s=0}^{2^m} \alpha(s) e^s = \sum_{(j_0 \dots j_x)} b_{j_0 \dots j_x} A_{j_0 \dots j_x} \quad \text{для некоторых} \quad b_{j_0 \dots j_x} \in \mathbb{Z}.$$

Здесь в первом равенстве $\alpha(s)$ равно числу решений (k, l) (в вычетах по модулю $p-1$) сравнения

$$g^{\overline{i_0 \dots i_x} + k 2^{x+1}} + g^{\overline{i_0 \dots i_x} + l 2^{x+1} + 2^x} \equiv s\ (p).$$

По 3b $\alpha(0) = 0$ при $x < m$. Аналогично 3c $\alpha(s) = \alpha(sg^{2^x})$. Отсюда вытекает второе равенство.

Доказательство невозможности в теореме Гаусса.

Перед доказательствами теоремы Гаусса некоторые их идеи демонстрируются по одной и на простейших примерах (задачи 1, 2c и 3). Эти примеры, впрочем, дают решение классических задач древности об удвоении куба и трисекции угла, ждавших своего решения 2000 лет. Первое доказательство невозможности в теореме Гаусса намечено в задачах 2ab и 4–7. Внешне другие (но по сути такие же) доказательства намечены в задачах 8-11 (используя 4, но не используя 6) и 13–16. Второе доказательство наиболее близко к идеям самого Гаусса. Задачи 17, 18 и 19 приводятся для общего развития. По поводу невыразимости через *вещественные* корни произвольной целой степени см. [Va].

1. Не существует рациональных чисел a, b, c, d, для которых $\sqrt[3]{2} =$

(a) $a + \sqrt{b}$; (b) $a - \sqrt{b}$; (c) $\dfrac{1}{a + \sqrt{b}}$; (d) $a + \sqrt{b} + \sqrt{c}$; (e) $a + \sqrt{b} + \sqrt{c} + \sqrt{bc}$;

(f) $a + \sqrt{b + \sqrt{c}}$; (g) $a + \sqrt{b} + \sqrt{c} + \sqrt{d}$.

2. (a) Оторвем у (комплексного аналога) калькулятора из теоремы Гаусса кнопку ':', но разрешим использовать все рациональные числа. Тогда множество чисел, которые можно реализовать на калькуляторе, не изменится.

(b) Число A построимо тогда и только тогда, когда существуют такие положительные $r \in \mathbb{Z}$ и $a_1, \dots a_r \in \mathbb{R}$, что

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \dots \subset Q_{r-1} \subset Q_r \supset A, \quad \text{где} \quad a_k \in Q_k, \quad \sqrt{a_k} \notin Q_k,$$

$$Q_{k+1} = Q_k[\sqrt{a}_k] := \{\alpha + \beta\sqrt{a}_k \mid \alpha, \beta \in Q_k\} \quad \text{для любого} \quad k = 1, \ldots, r-1.$$

Такая последовательность называется *цепочкой квадратичных расширений* (это единый термин, термин 'квадратичное расширение' мы не используем).

(c) $\sqrt[3]{2}$ непостроимо. (Значит, удвоение куба циркулем и линейкой невозможно.)

3. (a) Число $\cos(2\pi/9)$ является корнем уравнения $8x^3 - 6x + 1 = 0$.

(b) Не существует рациональных чисел a и b, для которых $\cos(2\pi/9) = a + \sqrt{b}$.

(c) Число $\cos(2\pi/9)$ не построимо (значит, трисекция угла $\pi/3$ циркулем и линейкой невозможна и правильный 9-угольник не построим).

(d) Корни кубического уравнения с рациональными коэффициентами построимы тогда и только тогда, когда один из них рационален.

4. *Лемма о сопряжении.* В обозначениях задачи 2b положим $a = a_k$ и определим отображение сопряжения $\bar{\cdot} : Q_k[\sqrt{a}] \to Q_k[\sqrt{a}]$ формулой $\overline{x + y\sqrt{a}} = x - y\sqrt{a}$. Тогда

(a) Это определение корректно.

(b) $\overline{z + w} = \overline{z} + \overline{w}$, $\quad \overline{zw} = \overline{z}\,\overline{w}$ $\quad$ и $\quad \overline{z} = z \Leftrightarrow z = x + 0\sqrt{a} \in Q_{k-1}$.

(c) Если $z \in Q_k[\sqrt{a}]$ — корень многочлена P с рациональными коэффициентами, то $P(\overline{z}) = 0$.

(Сравните с леммой о комплексных корнях многочлена с вещественными коэффициентами.)

5. (a) Многочлен $\Phi(x) := x^{12} + x^{11} + \cdots + x + 1$ неприводим над $\mathbb{Q}$.

Указание: если не получается, то используйте лемму Гаусса и признак Эйзенштейна (см. ниже).

(b) Если $e = \cos(2\pi/13) + i\sin(2\pi/13)$ построимо, то существует такая цепочка $\mathbb{Q} = Q_1 \subset Q_2 \subset \ldots \subset Q_k \subset Q_{k+1}$ квадратичных рассширений, что Φ приводим над Q_{k+1} и неприводим над Q_k.

(c) Если Φ делится на многочлен P с коэффициентами в Q_{k+1}, то Φ делится на сопряженный (относительно Q_k) многочлен $\overline{P}$.

(d) Если многочлен R с коэффициентами из Q_{k+1} неприводим, то сопряженный (относительно Q_k) многочлен $\overline{R}$ неприводим.

(e) Разложение многочлена $\Phi(x)$ над Q_{k+1} на неприводимые над Q_{k+1} множители ссостоит из двух сопряженных (относительно Q_k) множителей.

(f) Для каждого из этих множителей существует цепочка, аналогичная (b), но, возможно, с другим k.

(g) Число $\cos(2\pi/13)$ не построимо.

6. (a) *Лемма Гаусса.* Если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$ [Pr].

(b) *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 $\mathbb{Z}$ [Pr].

7. (a) Минимальная степень многочлена, корнем которого является данное построимое число, является степенью двойки.

(b) Число $\cos(2\pi/n)$ не построимо для n простого, $n \neq 2^m + 1$.

(c) Многочлен $\Phi(x) = 1 + x^{17} + x^{34} + x^{51} + \cdots + x^{272}$ неприводим над $\mathbb{Q}$.

Указание: используйте лемму Гаусса и признак Эйзенштейна.

(d) Число $\cos(2\pi/289)$ не построимо.

(e) Докажите невозможность в теореме Гаусса.

Другие доказательства невозможности в теореме Гаусса.

8. Число $\cos(2\pi/7)$ не построимо (значит, правильный 7-угольник не построим).

9. Пусть $n = 4k + 3$ простое. Обозначим $f_s = e^s + e^{-s}$. Назовем *рангом* квадратичной иррациональности наименьшую длину минимальной цепочки из 2b.

(a) Для любого k число $f_1^k + f_2^k + \cdots + f_{(p-1)/2}^k$ рационально.

(b) После раскрытия скобок и приведения подобных в выражении $(x - f_1)(x - f_2)\dots(x - f_{(p-1)/2})$ получается многочлен с рациональными коэффициентами.

(c) Ранги чисел $e, e^2, \dots, e^{p-1}$ одинаковы.

(d) Ранги чисел $f_1, \dots, f_{(p-1)/2}$ одинаковы.

(e) Число $\cos(2\pi/n)$ не построимо

10. Обозначим $e = \cos(2\pi/13) + i\sin(2\pi/13)$, $g = 2$ — первообразный корень по модулю 13,

$$A_0 = e^{g^0} + e^{g^3} + e^{g^6} + e^{g^9}, \quad A_1 = e^{g^1} + e^{g^4} + e^{g^7} + e^{g^{10}} \quad \text{и} \quad A_2 = e^{g^2} + e^{g^5} + e^{g^8} + e^{g^{11}}.$$

$$(a) \quad A_0^2 = 4 + A_1 + 2A_2, \quad A_1^2 = 4 + A_2 + 2A_0 \quad \text{и} \quad A_2^2 = 4 + A_0 + 2A_1.$$

(b) Числа A_0, A_1, A_2 являются корнями неприводимого кубического уравнения с рациональными коэффициентами.

(c) Числа A_0, A_1, A_2 имеют одинаковый ранг.

(d) Число $\cos(2\pi/13)$ не построимо.

11. Число $\cos(2\pi/p)$ не построимо для

(a) $p = 3 \cdot 2^k + 1$ простого.

(b) p простого, $p \neq 2^m + 1$.

(c) $p = 289$.

(d) числа p, не являющегоеся произведением степени двойки и различных простых чисел вида $2^m + 1$.

Идея еще одного доказательства невозможности в теореме Гаусса выражается понятиями *поля* и *размерности поля*.

13. *Полем* (числовым) называется подмножество множества $\mathbb{C}$ комплексных чисел, замкнутое относительно сложения, вычитания, умножения и деления.

(a) Следующие множества являются полями: $\mathbb{Q}$, множество построимых чисел, множество вещественных чисел, $\mathbb{Q}[\sqrt{2}] := \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}\}$, каждое Q_k в цепочке квадратичных расширений и

$$\mathbb{Q}[e] := \{\alpha_0 + \alpha_1 e + \alpha_2 e^2 + \alpha_3 e^3 + \cdots + \alpha_{12} e^{12} \mid \alpha_i \in \mathbb{Q}\}, \quad \text{где} \quad e = \cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}.$$

(b) Любое поле содержит поле $\mathbb{Q}$.

(c) Любое поле, содержащее $\sqrt{2}$, содержит $\mathbb{Q}[\sqrt{2}]$.

(d) Любое поле, содержащее e, содержит $\mathbb{Q}[e]$.

14. *Размерностью* $\dim F$ поля F называется наименьшее k, для которого существуют такие

$$b_2, b_3 \dots, b_k \in F, \quad \text{что} \quad F = \{\alpha_1 + \alpha_2 b_2 + \alpha_3 b_3 + \cdots + \alpha_k b_k \mid \alpha_i \in \mathbb{Q}\},$$

если такое k существует.

(a) $\dim \mathbb{Q} = 1$.

(b) $\dim \mathbb{Q}[\sqrt{2}] = 2$.

(c) В цепочке квадратичных расширений $\dim Q_k = 2 \dim Q_{k-1}$ при $k \geq 1$.

(d) В цепочке квадратичных расширений $\dim Q_k = 2^{k-1}$.

(e)* Если $G \subset F$ — поля, то $\dim F$ делится на $\dim G$.

15. (a) $\dim \mathbb{Q}[\cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}] \le 12$.

(b) Если $\dim \mathbb{Q}[\cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}] < 12$, то $P(e) = 0$ для некоторого многочлена P с рациональными коэффициентами степени меньше 12.

(c) Выведите из предыдущих пунктов, что число $\cos(2\pi/13)$ не построимо.

16. (a) $\dim \mathbb{Q}[\cos\frac{2\pi}{289} + i\sin\frac{2\pi}{289}] = 272$.

(b) Выведите из предыдущих пунктов, что число $\cos(2\pi/289)$ не построимо.

(c) Докажите невозможность в теореме Гаусса.

17. (a) Многочлены P и Q с рациональными коэффициентами имеют общий корень, $\deg P = 3$, $\deg Q = 2$. Докажите, что многочлен P имеет рациональный корень.

(b) То же с заменой рациональных коэффициентов и корня на коэффициенты и корень из произвольного поля.

(c) Если все корни неприводимого многочлена нечетной степени с рациональными коэффициентами построимы, то один из них рационален.

(d)* Корни многочлена 4-ой степени с рациональными коэффициентами построимы тогда и только тогда, когда его *кубическая резольвента* [Ko, Pr] имеет рациональный корень.

18. Любое построимое число является алгебраическим, т.е. корнем некоторого многочлена с целыми коэффициентами. (Из этого и доказанной в 1883 г. Линдеманом трансцендентности числа π, влекущей трансцендентность числа $\sqrt{\pi}$, вытекает, что задача о квадратуре круга неразрешима циркулем и линейкой.)

19. (a) (Г. Челноков) Лешин калькулятор получается из комплексного гауссова добавлением кнопки извлечения кубического корня из комплексных чисел (которая дает все три значения корня). Гришин калькулятор получается из комплексного гауссова добавлением кнопки нахождения по комплексному числу a всех трех комплексных корней уравнения $a = \dfrac{3x - 4x^3}{1 - 3x^2}$. Будет ли множество 'Лешиных' чисел совпадать с множеством 'Гришиных'?

(b) (Г. Челноков) Неприводимый над $\mathbb{Q}$ многочлен раскладывается над $\mathbb{Q}[\sqrt[4]{2}]$ ровно на четыре множителя. Докажите, что степень этого многочлена делится на 8.

Указания и решения к некоторым задачам о невозможности.

Указание к 1c. Домножьте на сопряженное.

Указание к 2a. Индукция по количеству операций калькулятора, необходимых для получения числа, с применением домножения на сопряженное.

Указание к 2b. Это несложное следствие задачи 2a.

Решение 2c. Предположим, что $\sqrt[3]{2}$ построимо. Тогда существует такая цепочка квадратичных расширений

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \ldots \subset Q_{r-1} \subset Q_r, \quad \text{что} \quad \sqrt[3]{2} \in Q_r \setminus Q_{r-1}.$$

Поскольку $\sqrt[3]{2} \notin \mathbb{Q}$, то $r \ge 2$. Значит,

$$\sqrt[3]{2} = \alpha + \beta\sqrt{a}, \quad \text{где} \quad \alpha, \beta, a \in Q_{r-1}, \quad \sqrt{a} \notin Q_{r-1} \quad \text{и} \quad \beta \ne 0.$$

Отсюда

$$2 = (\sqrt[3]{2})^3 = (\alpha^3 + 3\alpha\beta^2 a) + (3\alpha^2\beta + \beta^3 a)\sqrt{a} = u + v\sqrt{a}.$$

Поскольку $2 \in \mathbb{Q} \subset Q_{r-1}$, то $2 - u \in Q_{r-1}$. Так как

$$v\sqrt{a} = 2 - u \quad \text{и} \quad v \in Q_{r-1}, \quad \text{то} \quad 0 = v = 3\alpha^2\beta + \beta^3 a.$$

Так как $3\alpha^2+\beta^2 a>0$, получаем $\beta=0$ — противоречие!

Указание к 3a. Выразите $\cos 3\alpha$ через $\cos\alpha$.

Указание к 3b. Если $\cos(2\pi/9)=a+\sqrt{b}$, то число $a-\sqrt{b}$ тоже является корнем уравнения $8x^3-6x+1=0$. Тогда по теореме Виета третий корень равен $-(a+\sqrt{b})-(a-\sqrt{b})=-2a\in\mathbb{Q}$.

Решение 3c. Следует из 3a и 3d.

Доказательство теоремы 3d о кубических уравнениях для уравнений, все три корня которых вещественны (этот частный случай достаточен для непостроимости правильного 9-угольника). Часть 'тогда' очевидна. Чтобы доказать часть 'только тогда', предположим, что хотя бы один из корней построим. Для каждого из построимых корней z рассмотрим минимальную цепочку расширений

$$\mathbb{Q}=Q_1\subset Q_2\subset Q_3\subset\ldots\subset Q_{r-1}\subset Q_r,\quad \text{для которой}\quad z_1\in Q_r\setminus Q_{r-1}.$$

Возьмем корень $z=z_1$ с наименьшей длиной минимальной цепочки l.

Если уравнение не имеет рациональных корней, то $l\geq 2$. Значит,

$$z_1=\alpha+\beta\sqrt{a},\quad \text{где}\quad \alpha,\beta\in Q_{l-1},\quad \sqrt{a}\notin Q_{r-1}\qquad \text{и}\quad \beta\neq 0.$$

Тогда число $\overline{z}_1=\alpha-\beta\sqrt{a}$ также является корнем рассматриваемого уравнения (по лемме о сопряжении). Поскольку $\beta\neq 0$, то $\alpha-\beta\sqrt{a}\neq\alpha+\beta\sqrt{a}$, т. е. $\overline{z}_1\neq z_1$. Обозначим $z_2:=\overline{z}_1$. Из первой формулы Виета для нашего уравнения находим:

$$z_1+z_2+z_3=(\alpha+\beta\sqrt{a})+(\alpha-\beta\sqrt{a})+z_3=2\alpha+z_3\in\mathbb{Q},\quad \text{поэтому}\quad z_3\in Q_{l-1}.$$

Следовательно, для корня z_3 существует цепочка меньшей длины, чем для z_1. Противоречие. $\square$

Указание к 5a. Примените признак Эйзенштейна к многочлену $((x+1)^{13}-1)/x$ и лемму Гаусса.

Решение 5b. Рассмотрим цепочку квадратичных расширений $\mathbb{Q}=Q_1\subset Q_2\subset\ldots\subset Q_{r-1}\subset Q_r\supset e$. Заметим, что многочлен Φ приводим над Q_r (поскольку имеет корень e). Поэтому существует l, для которого многочлен Φ приводим над Q_{l+1}. Обозначим через k наименьшее такое l. Из пункта 5a следует, что $k\geq 1$. Теперь легко видеть, что цепочка $\mathbb{Q}=Q_1\subset Q_2\subset\ldots\subset Q_k\subset Q_{k+1}$ искомая.

Указание к 5c. Сопрягите относительно Q_k равенство $\Phi(x)=P(x)R(x)$.

Указание к 5d. Достаточно доказать, что если многочлен P с коэффициентами в Q_{k+1} делит Φ, то P и $\overline{P}$ взаимно просты. Для этого покажите, что НОД$(P,\overline{P})$ имеет коэффициенты из Q_k и воспользуйтесь неприводимостью многочлена Φ в Q_k.

Решение 5e. Аналогично решению 5b.

Указание к 5f. Докажите, что указанное в пункте 5d разложение многочлена $\Phi(x)$ состоит ровно из двух множителей (воспользуйтесь тем, что если коэффициенты многочлена P лежат в Q_{k+1}, то коэффициенты многочлена $P\overline{P}$ лежат в Q_k). То же самое будет верно и для разложения получившихся множителей и т.д. Исходя из этого получите, что степень многочлена $\Phi(x)$ должна быть степенью двойки.

Указание к 5g. Аналогично 5f.

Указание к 6b. Предположите противное и воспользуйтесь методом неопределённых коэффициентов.

Указание к 7a. Примените признак Эйзенштейна к многочлену $\Phi(x+1)$ и лемму Гаусса.

Указание к 7b. Аналогично решению задачи 5 докажите, что если число $\cos\dfrac{2\pi}{289}$ построимо, то степень многочлена $\Phi(x)$ должна быть степенью двойки. А это неверно.

Решение 8. Рассмотрим комплексное число $e=\cos(2\pi/7)+i\sin(2\pi/7)$. Так как $e\neq 1$, то число e удовлетворяет уравнению 6-ой степени $e^6+e^5+e^4+e^3+e^2+e+1=0$. Разделим обе части уравнения на e^3. Положим

$$f:=e+e^{-1},\quad \text{тогда}\quad e^2+e^{-2}=f^2-2\quad\text{и}\quad e^3+e^{-3}=f(e^2+e^{-2}-1).$$

Получим кубическое уравнение

$$f(f^2-3)+(f^2-2)+f+1=0,\quad \text{то есть}\quad f^3+f^2-2f-1=0.$$

Кандидаты на рациональные корни этого уравнения $f=\pm 1$ отвергаются проверкой. Согласно теореме 3d о кубических уравнениях число $f=e+e^{-1}$ не построимо. Поэтому и e не построимо (поясните).

Указание к 9a. Индукция по k.

Указание к 9b. Следует из пункта 9a и из того, что любой симметрический многочлен от переменных $f_1,f_2,\dots,f_{(p-1)/2}$ рационально выражается через многочлены вида $f_1^k+f_2^k+\dots+f_{(p-1)/2}^k$.

Решение 9c. Так как для любых $s,t\in\{1,2,\dots,p-1\}$ существует такое k, что $e^s=(e^t)^k$, то ранги чисел $e,e^2,\dots,e^{p-1}$ одинаковы.

Решение 9d. Так как e^s+e^{-s} рационально выражается через $e+e^{-1}$, то для любых $s,t\in\{1,2,\dots,p-1\}$ число e^s+e^{-s} рационально выражается через e^t+e^{-t} (аналогично приведенному решению задачи 8). Поэтому ранги чисел $f_1,\dots,f_{(p-1)/2}$ одинаковы.

(Заметим, что $rk(e+e^{-1})=rke-1$.)

Решение 9e. Пусть $r:=\operatorname{rk} f_s$. Значит, для некоторой цепочки квадратичных рассширений

$$f_s=\alpha_s+\beta_s\sqrt{a},\quad\text{где}\quad \alpha_s,\beta_s,a\in Q_{r-1},\quad \sqrt{a}\notin Q_{r-1}\quad\text{и}\quad \beta_s\neq 0.$$

Тогда число $\overline{f}_s=\alpha_s-\beta_s\sqrt{a}$ также является корнем рассматриваемого многочлена (по лемме о сопряжении). Поскольку

$$\beta_s\neq 0,\quad\text{то}\quad \alpha_s-\beta_s\sqrt{a}\neq\alpha_s+\beta_s\sqrt{a},\quad\text{т. е.}\quad \overline{f}_s\neq f_s.$$

Итак, корни $f_1,\dots,f_{(p-1)/2}$ разбиваются на пары сопряженных. Значит, $(p-1)/2$ четно — противоречие.

Другое окончание решения. Числа $f_1,\dots,f_{(p-1)/2}$ являются корнями многочлена с рациональными коэффициентами. Так как $p=4k+3$, то по задаче 17c одно из них f_s является рациональным. Но тогда e^s является корнем квадратного уравнения с рациональными коэффициентами. Значит, многочлен $1+x+x^2+x^3+\dots+x^{p-1}$ приводим над $\mathbb{Q}$ — противоречие. (Видимо, достаточное здесь отсутствие делителей степени 2 у многочлена $1+x+x^2+x^3+\dots+x^{p-1}$ можно доказать проще.)

Решение 10a. Докажем первую фомулу (остальные доказываются аналогично). Заметим, что $g^6=-1$. Поэтому

$$A_0^2=((e^{g^0}+e^{-g^0})+(e^{g^3}+e^{-g^3}))^2=$$

$$\underset{(*)}{=}2+e^{g^1}+e^{-g^1}+2+e^{g^4}+e^{-g^4}+2(e^{g^0}+e^{g^6})(e^{g^3}+e^{g^9})=4+A_1+2A_2.$$

Последнее равенство верно, поскольку

$$(e^{g^0}+e^{g^6})(e^{g^3}+e^{g^9}) = e^{g^0+g^3}+e^{g^3+g^6}+e^{g^6+g^9}+e^{g^9+g^0} = e^{g^0+g^3}A_0 \underset{(*)}{=} e^{g^8}A_0 = A_2.$$

(Равенства $(*)$ выполнены, поскольку $g = 2$.)

Указание к 10b. Докажите, что $A_0+A_1+A_2$, $A_0^2+A_1^2+A_2^2$, $A_0^3+A_1^3+A_2^3$ рациональны.

Указание к 10c. Пользуясь пунктом 10a и тем, что $A_0 + A_1 + A_2 = -1$, докажите, что любое A_i рационально выражается через любое A_j.

Указание к 10d. Решение получается из пунктов 10b и 10c аналогично решению задачи 9e.

Вот идея другого решения, не использующего пункт 10c. Пусть число A_0 имеет ранг r. Сопряжём его относительно Q_{r-1}. Полученное число будет одним из чисел A_i (поясните). Теперь легко понять, что числа A_i разбиваются на пары сопряжённых, т.е. их чётное число, что неверно.

Указание к 11a. Аналогично задаче 10.

Указание к 11b. Предположите, что для $p = 2^k r + 1$ число $\cos\dfrac{2\pi}{p}$ построимо (где $r > 1$ — нечетное число). Выведите из этого, что числа

$$A_i = e^{g^i} + e^{g^{r+i}} + \cdots + e^{g^{(2^k-1)r+i}}, \quad 0 \le i \le r-1$$

имеют одинаковый ранг и являются корнями мнгочлена степени r с рациональными коэффициентами.

Указание к 11c. Рассмотрите числа

$$A_0 = e^{g^0} + e^{g^{17}} + \cdots + e^{g^{272}}, \quad A_1 = e^{g^1} + e^{g^{18}} + \cdots + e^{g^{273}}, \quad A_{16} = e^{g^{16}} + e^{g^{33}} + \cdots + e^{g^{288}}.$$

Указание к 12. Решение аналогично решению задачи 5.

Указание к 14c. Докажите, что

$$Q_k = \{\alpha_1 + \alpha_2 b \mid \alpha_1, \alpha_2 \in Q_{k-1}\} \quad \text{для любого} \quad b \in Q_k - Q_{k-1}.$$

Указание к 14d. Следует из 14a и 14c.

Указание к 14e. *Размерностью* $\dim(F : G)$ поля F над полем G называется наименьшее k, для которого существуют такие

$$b_1, b_2, \ldots, b_k \in F, \quad \text{что} \quad F = \{\alpha_1 b_1 + \alpha_2 b_2 + \alpha_3 b_3 + \cdots + \alpha_k b_k \mid \alpha_i \in G\},$$

если такое k существует. Докажите, что $\dim F = \dim G \dim(F : G)$.

Указание к 15b. Докажем, что существуют такие рациональные $a_0, a_1, \ldots, a_{12}$, не все равные 0, что

$$a_0 + a_1 e + \cdots + a_{11} e^{11} = 0. \qquad (*)$$

По определению размерности существуют такие $b_1, \ldots, b_{11} \in \mathbb{Q}[\cos\dfrac{2\pi}{13} + i\sin\dfrac{2\pi}{13}]$ и $\alpha_{kl} \in \mathbb{Q}$, что

$$e^{j-1} = \alpha_{j,1} b_1 + \alpha_{j,2} b_2 + \cdots + \alpha_{j,11} b_{11} \quad \text{для} \quad j = 1, 2, \ldots, 12.$$

Подставьте эти значения e^i в $(*)$. Теперь приравняйте к 0 коэффициенты при $b_1, \dots, b_{11}$. Наконец, докажите, что полученная система уравнений имеет нетривиальное рациональное решение.

Указание к 16a. Решение аналогично решению задач 15ab. Воспользуйтесь неприводимостью многочлена $\Phi(x) = 1 + x^{17} + x^{34} + x^{51} + \dots + x^{272}$.

Указание к 17a. Пусть $a{=}a_1$ и $b{=}b_1$ — построимые числа, а P и Q — многочлены с рациональными коэффициентами минимальной степени, корнями которых являются соответственно a и b. Пусть $a_2, \dots, a_m$ — все остальные комплексные корни многочлена P, а $b_2, \dots, b_n$ — все остальные комплексные корни многочлена Q. Заметим, что

$a + b$ — корень многочлена $P(x - b_1) \dots P(x - b_n)$,

$a - b$ — корень многочлена $P(x + b_1) \dots P(x + b_n)$,

ab — корень многочлена $P(\frac{x}{b_1}) \dots P(\frac{x}{b_n})$,

$\frac{a}{b}$ — корень многочлена $P(xb_1) \dots P(xb_n)$,

$\sqrt{a}$ — корень многочлена $P(x^2)$.

Осталось доказать следующее вспомогательное утверждение.

Лемма. Пусть $R(x, y)$ — многочлен от двух переменных с рациональными коэффициентами, а $b_1, b_2, \dots, b_n$ — все комплексные корни многочлена Q с рациональными коэффициентами. Тогда многочлен от одной переменной $R(x, b_1)R(x, b_2) \dots R(x, b_n)$ также имеет рациональные коэффициенты.

Решение задачи 17b аналогично решению задач 5bc.

Литература

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

[Ch] Н. Н. Чеботарев, Основы теории Галуа, 1934.

[Ga] К. Ф. Гаусс, Арифметические исследования.

[Gi] С. Гиндикин, Дебют Гаусса, Квант, 1972 N1.

[Ka] А. Я. Канель, готовится.

[Ki] А. А. Кириллов, О правильных многоугольниках, функции Эйлера и числах Ферма, Квант, 1977 N7 или 1994 N6.

[Ko] В. А. Колосов, Теоремы и задачи алгебры, теории чисел и комбинаторики (М: Гелиос, 2001).

[Li] Дж. Литлвуд, Математическая смесь.

[Po] М. М. Постников, Теория Галуа.

[Pr] В. В. Прасолов, Многочлены (М: МЦНМО, 1999, 2001, 2003)

[PS] В. В. Прасолов и Ю. П. Соловьев, Эллиптические функции и алгебраические уравнения (М.: Факториал, 1997).

[Va] Б. Л. Ван дер Варден, Алгебра.

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