Построения циркулем и линейкой и теория Галуа.

В.А. Кириченко

Летняя школа в Дубне, 2005

Введение

Эти заметки являются элементарным введением в теорию Галуа. Главный вопрос, который решает теория Галуа, можно сформулировать следующим образом. Пусть задан многочлен f степени n с рациональными коэффициентами

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0.$$

Можно ли решить уравнение $f(x) = 0$, последовательно решая только вспомогательные уравнения некоторого специального вида? Например, только квадратные уравнения (или уравнения степени не выше $m < n$), или только уравнения вида $x^k - a = 0$? В последнем случае речь идёт о разрешимости уравнения $f(x) = 0$ в радикалах. При этом коэффициенты каждого последующего вспомогательного уравнения находятся из решения предыдущих уравнений, и уже не обязаны быть рациональными.

Рассмотрим несколько примеров, которые будут подробно разобраны в последующих разделах. Чтобы решить квадратное уравнение, достаточно уметь извлекать только квадратные корни. При решении произвольного кубического уравнения квадратными корнями уже не обойтись (это мы докажем во втором разделе). А вот уравнения $x^5 - 1 = 0$ и $x^{17} - 1 = 0$ можно решить, используя только квадратные корни.

Вообще, уравнения которые можно решить, извлекая только квадратные корни, естественно возникают при геометрических построениях циркулем и линейкой. Поэтому мы начнём знакомство с теорией Галуа с обсуждения некоторых задач на построение. В частности, мы докажем неразрешимость классических задач древности о трисекции угла и удвоении куба. Мы также выясним, какие правильные многоугольники можно построить циркулем и линейкой. Эту задачу первым решил Гаусс [1]. Решение существенно использует арифметические свойства вычетов по модулю числа n. В третьем и четвёртом разделах мы подробно разберём решение Гаусса а также его более общий результат, касающийся решения уравнений вида $x^n - 1 = 0$. Например, в четвёртом разделе мы докажем методами Гаусса, что для решения уравнения $x^{13} - 1 = 0$ достаточно уметь решать только квадратные и кубические уравнения, и найдём эти уравнения явно.

В последнем разделе, мы сначала сформулируем результат Гаусса для уравнений вида $x^n - 1 = 0$ на языке теории Галуа. Для таких уравнений Гаусс разработал теорию Галуа (конечно, не под таким названием) за 30 лет до Галуа. Затем мы построим теорию Галуа для кубических уравнений. Ни Гаусс, ни Галуа не использовали понятия *поля*, *расширения* *поля* и *степени расширения*. Однако, при изложении их методов удобно использовать эти понятия. Поэтому второй и частично третий разделы посвящены определению и обсуждению этих и некоторых других понятий, таких как *квадратичные* и *круговые поля*.

Ещё одна цель этих заметок — реклама замечательной книги Гаусса "Арифметические исследования" [1]. В заметках частично переизложена седьмая (последняя) часть этой книги, посящённая уравнениям деления круга. Книга Гаусса содержит много других интересных и глубоких результатов. При этом изложение очень понятное и не использует никаких сведений, выходящих за рамки школьной программы.

Заметки рассчитаны на школьников старших классов и на всех, интересующихся теорией Галуа или теорией чисел. Полезно некоторое знакомство с комплексными числами, хотя все необходимые сведения о них приводятся в первом разделе. Полезно также знакомство с вычетами по модулю простого числа.

Многие утверждения сформулированы в виде задач. Решение большинства задач существенно для понимания дальнейшего материала (номера этих задач набраны прямым шрифтом). Эти задачи достаточны просты, и часто снабжены указаниями, которые нужно самостоятельно продумать, чтобы получить полное решение. Сложные задачи помечены звёздочкой.

1 Построения циркулем и линейкой

В этом разделе обсуждаются построения правильных многоугольников и другие построения циркулем и линейкой, которые были придуманы математиками Древней Греции. В основном, раздел состоит из задач. Для того, чтобы их решить, полезно помнить, как строить биссектрису угла, делить отрезок пополам и опускать перпендикуляр с помощью циркуля и линейки. Обсуждаются также комплексные числа и геометрическая интерпретация их сложения и умножения. Часть задач снабжена указаниями.

Здесь и далее, точки плоскости мы будем отождествлять с комплексными числами таким образом: точке с вещественными координатами (a, b) соответствует комплексное число $a + bi$, где i — *мнимая единица*. Например, точки $(0, 0)$ и $(1, 0)$ отождествляются с 0 и 1, соответственно, а точка $(0, 1)$ — с числом i.

Правила пользования циркулем и линейкой.

Определим, что значит построить точку с помощью циркуля и линейки:

0. Пусть на плоскости отмечено несколько точек — это *база* построения (в дальнейшем, если об этом ничего не сказано, то в качестве базы берутся точки 0 и 1).

Многократное повторение следующих трёх действий позволяет строить новые точки из уже построенных (к которым отнесём и точки, данные в качестве базы).

1. Можно провести прямую через любые две ранее построенные точки.

2. Можно провести окружность с центром в одной из ранее построенных точек, проходящую через другую уже построенную точку.

3. Можно построить точки пересечения двух прямых, прямой и окружности или двух окружностей, полученных в результате действий 1 и 2.

Построение циркулем и линейкой — это любая последовательность действий 1, 2 и 3. Новые точки появляются только в результате действия 3 (конечно, они могут совпасть с уже построенными).

Задачи:

1.1. Постройте с помощью циркуля и линейки

(a) равносторонний треугольник,

(b) квадрат,

(c) правильный шестиугольник,

(d) правильный пятиугольник,

Указание: Рассмотрим равнобедренный треугольник ABC с основанием AC и с углом при вершине B в $36° = \pi/5$ (углы при основании тогда равны $72°$). Пусть AD — биссектриса угла A. Тогда треугольники ABC и CAD подобны! При этом треугольник BDA тоже равнобедренный, поэтому $AC = AD = BD$. Отсюда можно найти отношение длин $\frac{AC}{AB}$, а оно равно $2\cos(2\pi/5)$.

(e) правильный 2^n-угольник,

(f) правильный 15-угольник.

В этих задачах интересно также найти минимальное число действий 1 и 2, которые необходимы для построения. Для определённости потребуем чтобы правильный многоугольник был вписан в единичную окружность с центром в нуле. При этом правильный n-угольник считается построенным, если построены две его соседние вершины. Для равностороннего треугольника, очевидно, необходимо всего два действия: нужно построить две окружности единичного радиуса с центрами в 0 и 1 и взять их точки пересечения — это и будут две вершины равностороннего треугольника. Для квадрата достаточно проделать пять действий, но доказать, что нельзя обойтись меньшим числом, уже не так просто. Ниже приведено построение правильного пятиугольника, для которого требуется девять действий.

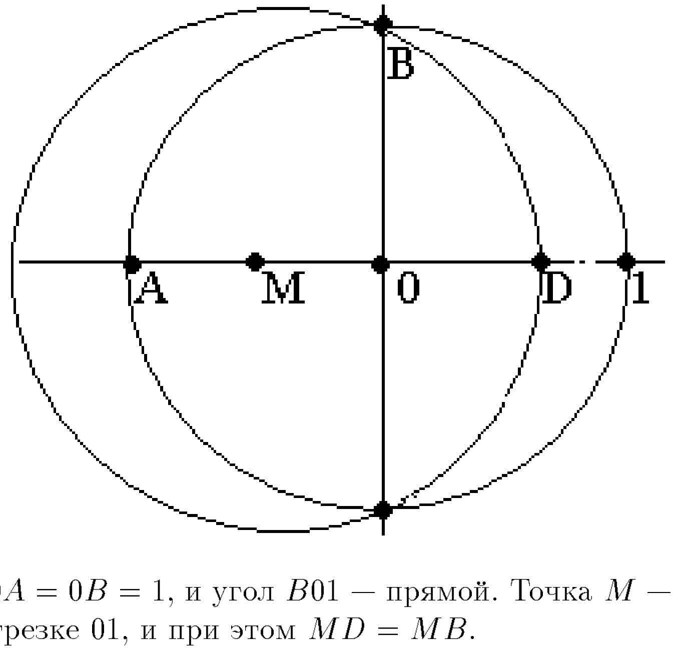

Рис. 1: Здесь $0A = 0B = 1$, и угол $B01$ — прямой. Точка M — середина отрезка $A0$. Точка D лежит на отрезке 01, и при этом $MD = MB$.

Длина отрезка BD равна длине стороны правильного пятиугольника, вписанного в окружность единичного радиуса (докажите!).

1.2. Пусть m натуральное число, такое что правильный m-угольник можно построить циркулем и линейкой. Докажите что с помощью циркуля и линейки можно построить и правильный $2^n m$-угольник.

1.3. **(a)** Пусть n и m — взаимно простые натуральные числа, такие что правильные n-угольник и m-угольник можно построить с помощью циркуля и линейки. Докажите, что правильный mn-угольник тоже можно построить циркулем и линейкой. Останется ли утверждение задачи верным, если m и n не взаимно просты?

(b) Пусть m — натуральное число, такое что правильный m-угольник нельзя построить циркулем и линейкой. Докажите, что тогда нельзя построить и правильный mn-угольник для любого натурального n.

Уже математики Древней Греции были убеждены, что трисекция угла с помощью циркуля и линейки в общем случае невозможна. Однако доказано это было только в начале XIX столетия Гауссом. Мы докажем это в разделе 2. Тем не менее, для некоторых углов трисекция выполнима.

1.4. (Трисекция угла)

(a) Разделить угол в 27 градусов на три равных угла с помощью циркуля и линейки.

(b*) Найдите все углы в целое число градусов, которые можно разделить на три равных угла с помощью циркуля и линейки.

Построимые числа. Пусть на комплексной плоскости отмечены точки 0 и 1. Используя эти две точки как базу, какие ещё точки можно построить циркулем и линейкой? Назовём точку и соответствующее ей комплексное число *построимыми*, если их можно так построить.

1.5. Докажите, что все точки с рациональными координатами построимы.

1.6. Докажите, что если можно построить циркулем и линейкой отрезок длины a и отрезок длины b, то можно построить и некоторые отрезки длины

(a) ab и a/b,

Указание: Воспользуйтесь теоремой Фалеса.

(b) $\sqrt{a}$,

Указание: Воспользуйтесь тем, что в прямоугольном треугольнике квадрат высоты, опущенной из прямого угла, равен произведению проекций катетов на гипотенузу.

Напомним, что если отождествить каждое комплексное число z с вектором с началом в точке 0 и концом в точке z, то сложение комплексных чисел соответствует сложению векторов на плоскости. Умножение тоже можно описать геометрически таким образом. Для каждого комплексного числа z можно определить его модуль $|z|$ и аргумент $\arg(z)$. Модуль — это длина вектора z, а аргумент — угол между этим вектором и осью абсцисс, измеренный против часовой стрелки (при этом, как и в тригонометрии, величина угла определена с точностью до $2\pi k$, где k — любое целое число). Таким образом, модуль — функция однозначная, а аргумент — многозначная. При умножении двух комплексных чисел их модули перемножаются, а аргументы складываются. Последнее следует понимать так: если φ — любое из значений $\arg(z)$, а — ψ любое из значений $\arg(w)$, то $\varphi + \psi$ — одно из значений $\arg(zw)$.

Эта геометрическая интерпретация полезна при решении следующей задачи.

1.7. Докажите, что если комплексные числа z и w построимы, то построимы и числа
(a) $z+w$ и $z-w$,
(b) zw и z/w, где $w \neq 0$,
(c) $\sqrt{z}$.

Сложение и умножение комплексных чисел можно определить и алгебраически, исходя из того, что $i^2 = -1$. Если $z = a + bi$, $w = u + vi$, то

$$z + w = (a + u) + (b + v)i,$$

$$zw = (au - bv) + (av + bu)i.$$

1.8. Докажите, что геометрическое определение сложения и умножения комплексных чисел эквивалентно алгебраическому.

Из геометрической интерпретации умножения комплексных чисел также легко вывести, что комплексные корни n-ой степени из единицы совпадают с вершинами некоторого правильного n-угольника, вписанного в единичную окружность. Это даёт следующий способ доказательства построимости правильного пятиугольника.

Найдём все корни уравнения $x^5 - 1 = 0$. После деления на $x - 1$, уравнение сводится к *возвратному* уравнению $x^4 + x^3 + x^2 + x + 1 = 0$. Уравнение чётной степени $2n$ называется *возвратным*, если коэффициенты при x^{2n-i} и при x^i совпадают для всех $i = 0, 1 \ldots, n$. Возвратное уравнение можно свести к уравнению степени n, поделив его на x^n и сделав подстановку $t = x + x^{-1}$. Проделав это в нашем случае, получим уравнение $t^2 + t - 1 = 0$. Его корни строятся циркулем и линейкой по задаче 1.7. Теперь, чтобы найти x, нужно построить корни квадратного уравнения $x^2 - tx + 1 = 0$, что снова выполнимо циркулем и линейкой.

2 Расширения полей

Утверждения из предыдущего раздела о построимости циркулем и линейкой были хорошо известны уже математикам Древней Греции. Сейчас мы перепрыгнем на две тысячи лет вперёд, во времена Гаусса, и докажем, что некоторые построения выполнить циркулем и линейкой невозможно. Например, нельзя построить правильный семиугольник. Для этого мы от геометрии перейдём к алгебре, и изучим такие понятия как расширение поля и степень расширения.

Расширения полей. Из результата задачи 1.7 следует, что множество всех построимых комплексных чисел замкнуто относительно операций сложения, умножения и деления. В таком случае говорят, что множество является *полем*. Например, множества всех рациональных или комплексных чисел являются полями. Обозначим эти поля через $\mathbb{Q}$ и $\mathbb{C}$ соответственно. *Подполем* поля K называется любое подмножество поля K замкнутое относительно операций сложения, умножения и деления. В дальнейшем, мы будем рассматривать только поля, являющиеся подполями поля комплексных чисел.

Как описать поле всех построимых чисел? Для каждого конкретного числа, например, для $\sqrt[3]{2}$, как узнать, построимо оно или нет?

Чтобы ответить на первый вопрос, можно рассмотреть подполя в поле всех построимых чисел, состоящие только из чисел, построенных в результате фиксированного числа действий 3. В качестве базы при этом берутся все рациональные числа. Например, какие новые (иррациональные) числа можно построить однократным применением действия 3, используя рациональные числа как базу? При этом действия 1 и 2 разрешены в любом количестве.

2.1. **(a)** Докажите, что если в качестве базы взять все рациональные числа, то применяя действие 3 один раз, можно построить любое число вида $p + \sqrt{q}$, где p и q рациональны, причём $q \leq 0$, и ничего больше.

(b) Найдите все числа, которые можно построить, применяя действие 3 один раз, если в качестве базы взять все комплексные числа с рациональными координатами.

Указание: Чтобы найти точку пересечения двух прямых, нужно решить систему линейных уравнений. Чтобы найти точки пересечения прямой и окружности или двух окружностей, нужно решить квадратное уравнение.

Построим с помощью циркуля и линейки одну новую (иррациональную) точку, скажем, $\alpha = \sqrt{r}$, где r рациональное число. Тогда мы можем построить все точки вида $p + q\alpha$, где p и q рациональны. Все такие числа тоже образуют подполе поля комплексных чисел. Оно называется *квадратичным расширением* поля рациональных чисел и обозначается через $\mathbb{Q}(\alpha)$. Например, базой в задаче 2.1(b) было квадратичное расширение $\mathbb{Q}(i)$. Аналогично можно определить квадратичное расширение $K(\alpha)$ любого подполя $K \subset \mathbb{C}$. А именно: пусть $\alpha \in \mathbb{C}$ — число, такое что α не лежит в K, а α^2 лежит. Тогда $K(\alpha)$ состоит из всех чисел вида $a + b\alpha$, таких что a и b лежат в поле K.

2.2. Докажите, что это определение корректно, то есть $K(\alpha)$ замкнуто относительно сложения, умножения и деления.

2.3. Докажите, что комплексное число α построимо тогда и только тогда, когда существует цепочка полей $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$, такая что каждое поле K_i является квадратичным расширением предыдущего поля K_{i-1}, и α содержится в K_n.

Расширения поля рациональных чисел, которые получаются описанным в задаче 2.3 способом, называются *поликвадратичными*. Таким образом, любое построимое число содержится в некотором поликвадратичном расширении.

Когда построение циркулем и линейкой невыполнимо. Напомним, что многочлен с рациональными коэффициентами называется *неприводимым* если его нельзя разложить в произведение многочленов меньшей степени с рациональными коэффициентами. Например, кубический многочлен неприводим тогда и только тогда, когда он не имеет рациональных корней.

2.4. Пусть комплексное число α является корнем неприводимого кубического многочлена с рациональными коэффициентами. Докажите, что α нельзя построить с помощью циркуля и линейки.

Указание: Можно рассуждать от противного. Рассмотрим поликвадратичное поле K, содержащее α, для которого длина n цепочки $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n = K$ квадратичных расширений минимальна (это, в частности, означает, что α не лежит в K_{n-1}). Тогда $\alpha = a + b\beta$, где a, b и β^2 лежат в K_{n-1}, а β — нет. Если $a + b\beta$ — корень *кубического многочлена x^3+px^2+qx+r с рациональными коэффициентами, то $a-b\beta$ — корень этого же многочлена! По теореме Виета, третий корень равен $p-2a$, то есть лежит в K_{n-1}.*

Ниже мы докажем другими методами, что если степень неприводимого многочлена имеет нечётный делитель, то ни один из его корней непостроим. Интересно, можно ли придумать элементарное доказательство этого утверждения, похожее на доказательство в случае кубического многочлена. Например, для многочленов степени 5, или любой другой нечётной степени.

2.5. **(a)** Приведите пример угла, для которого трисекция невозможна.

(b) Докажите, что нельзя удвоить единичный куб (то есть построить ребро куба, объём которого равен двум) с помощью циркуля и линейки.

(c) Докажите, что с помощью циркуля и линейки нельзя построить правильный семиугольник и правильный девятиугольник.

Указание: Сведите уравнение $x^7-1=0$ к кубическому.

Для каждого комплексного числа α можно определить поле $\mathbb{Q}(\alpha)$ как множество всех чисел вида $(p_0+p_1\alpha^{i_1}+\dots p_k\alpha^{i_k})/(q_0+q_1\alpha^{j_1}+\dots q_l\alpha^{j_l})$, где $p_0, \dots, p_k, q_0, \dots, q_l$ — рациональные, а $i_1, \dots, i_k, j_1, \dots, j_l$ — натуральные числа. При этом знаменатель, конечно, не должен быть равен нулю. Такое поле называется *расширением* поля рациональных чисел, полученным присоединением числа α. Важную роль в вопросах неразрешимости построений циркулем и линейкой играет понятие *степени* такого расширения. *Степень* расширения $\mathbb{Q}(\alpha)$ — это натуральное число n, такое что любой элемент поля представляется *единственным* образом в виде $p_0+p_1\alpha+\dots+p_{n-1}\alpha^{n-1}$, где $p_0, p_1, \dots, p_{n-1}$ рациональны. Если такого числа не существует, то расширение называется *трансцендентным*. Если существует, то расширение называется *алгебраическим*.

Те, кто знаком с понятиями *векторного пространства*, *базиса* и *размерности*, могут проверить, что степень расширения $\mathbb{Q}(\alpha)$ — это его размерность как векторного пространства над полем рациональных чисел.

2.6. (a) Докажите, что степень любого квадратичного расширения равна двум.

(b) Найдите степень расширения $\mathbb{Q}(\sqrt[3]{2})$.

(c) Докажите, что расширение $\mathbb{Q}(\alpha)$ является алгебраическим, если и только если α — корень многочлена с рациональными коэффициентами.

В общем случае, степень расширения $\mathbb{Q}(\alpha)$ равна степени *минимального многочлена* для α. Многочлен f с рациональными коэффициентами называется *минимальным многочленом* для α, если α является корнем многочлена f, но не является корнем никакого ненулевого многочлена меньшей степени с рациональными коэффициентами.

2.7. Пусть f — многочлен с рациональными коэффициентами и корнем α. Докажите, что f — минимальный многочлен для α, если и только если f неприводим.

Предложение 1. *Если α является корнем неприводимого многочлена степени d с рациональными коэффициентами, то степень расширения $\mathbb{Q}(\alpha)$ равна d.*

Доказательство. Обозначим минимальный многочлен для α через f. Докажем, что любой элемент поля $\mathbb{Q}(\alpha)$ представляется как многочлен от α с рациональными коэффициентами и степени меньше, чем d. Во-первых, значение в α любого многочлена равно значению в α его остатка при делении на f. Во-вторых, число вида $1/g(\alpha)$, где g — многочлен с рациональными коэффициентами, такой что $g(\alpha) \neq 0$, тоже представляется как многочлен от α. Действительно, поскольку f неприводим, то g либо делится на f, либо взаимно прост с f. Во втором случае, по алгоритму Евклида, найдутся многочлены h_1 и h_2 такие, что $h_1 f + h_2 g = 1$. Тогда $h_2(\alpha)g(\alpha) = 1$, то есть $1/g(\alpha) = h_2(\alpha)$. Из этих двух утверждений следует, что любое число вида $h(\alpha)/g(\alpha)$, где h и g — многочлены с рациональными коэффициентами, и $g(\alpha) \neq 0$, представляется как многочлен от α степени меньше d с рациональными коэффициентами.

Теперь для каждого элемента $\beta \in \mathbb{Q}(\alpha)$ докажем единственность его представления в виде $\beta = p_0 + p_1\alpha + \ldots + p_{d-1}\alpha^{d-1}$, где p_0, p_1, ..., p_{d-1} рациональны. Если $\beta = q_0 + q_1\alpha + \ldots + q_{d-1}\alpha^{d-1}$ — второе такое представление, то взяв их разность, мы получим $0 = (p_0 - q_0) + (p_1 - q_1)\alpha + \ldots + (p_{d-1} - q_{d-1})\alpha^{d-1}$. Так как α не может быть корнем ненулевого многочлена степени меньше d, отсюда следует, что $p_i = q_i$. $\square$

В определении степени мы использовали число $\alpha \in \mathbb{Q}(\alpha)$. На самом деле, определение зависит только от самого поля $K = \mathbb{Q}(\alpha)$, но не от выбора числа α. На языке линейной алгебры, это утверждение о том, что все *базисы* в *векторном пространстве* состоят из одинакового числа элементов. Для его доказательства полезно уметь исключать неизвестные из систем линейных уравнений.

2.8. Пусть β — любой элемент поля $\mathbb{Q}(\alpha)$. Докажите, что если α является корнем неприводимого многочлена степени d с рациональными коэффициентами, то β является корнем многочлена степени не выше d с рациональными коэффициентами.

Указание: Представим каждую из степеней β, β^2,...,β^{d-1} *как сумму чисел* 1, α, α^2,..., α^{d-1}, *взятых с рациональными коэффициентами. Получим* $d-1$ *уравнений. Например, при* $d = 2$*:*

$$\begin{cases} \beta = p_{10} + p_{11}\alpha \\ \beta^2 = p_{20} + p_{21}\alpha. \end{cases}$$

Последовательно исключая α, α^2,..., α^{d-1} *из этих уравнений, мы получим, что для некоторых рациональных чисел* q_1,q_2, ... ,q_{d-1}, *не равных одновременно нулю, число* $q_1\beta + q_2\beta^2 + \ldots + q_{d-1}\beta^{d-1}$ *рационально.*

В частности, если $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ (так будет, например, если $\beta = \alpha - 1$), то степени расширения K, измеренные с помощью α и с помощью β, совпадают. Более того, точно так же можно доказать, что если набор чисел α_1, α_2,..., α_k из K обладает свойством, что любой элемент поля K записывается единственным образом в виде $p_1\alpha_1 + p_2\alpha_2 + \ldots + p_k\alpha_k$, где p_1, ... , p_k рациональны, то обязательно $k = d$. Поэтому, чтобы найти степень расширения, достаточно найти любой набор с таким свойством и посчитать, сколько в нём элементов. Это и будет степень.

В определении понятий расширения и его степени можно заменить поле рациональных чисел на произвольное подполе $K \subset \mathbb{C}$ (просто везде вместо слова "рациональный" напишем "принадлежащий полю K"). Будем обозначать степень поля $L = K(\alpha)$, рассматриваемого как расширение поля K, через $[L : K]$.

В дальнейшем, если это не оговаривается, под степенью поля подразумевается степень этого поля как расширения поля рациональных чисел.

2.9. **(a)** Проверьте, что $\mathbb{Q}(\sqrt{2})$ содержится в $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, и найти $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})]$.
(b) Пусть $K = \mathbb{Q}(\sqrt{2})$. Найдите $[K(\sqrt[3]{2}) : \mathbb{Q}]$ и $[K(\sqrt[3]{2}) : K]$.
(c) Пусть $K = \mathbb{Q}(\alpha)$, $L = \mathbb{Q}(\beta)$ и при этом L содержит K. Докажите, что

$$[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}].$$

Указание: Обозначим $[K : \mathbb{Q}]$ через m, а $[L : K]$ — через n. Докажите, что любой элемент поля L представляется единственным образом в виде суммы

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} p_{ij} \alpha^i \beta^j,$$

где числа p_{ij} рациональны.

Таким образом, если поле K содержится в поле L, то степень $[K : \mathbb{Q}]$ делит степень $[L : \mathbb{Q}]$. Получаем такое следствие:

Пусть комплексное число α является корнем неприводимого многочлена степени d с рациональными коэффициентами. Если d не является степенью двойки, то α нельзя построить с помощью циркуля и линейки.

Действительно, степень любого поликвадратичного поля равна 2^n. Если α лежит в поликвадратичном поле L, то поле $\mathbb{Q}(a)$ содержится в L. Поэтому число d, которое равно степени поля $\mathbb{Q}(\alpha)$, делит 2^n.

Обратное не всегда верно. Можно привести пример многочлена четвёртой степени, корни которого нельзя построить циркулем и линейкой. Однако верно следующее:

Пусть комплексное число α является корнем неприводимого многочлена степени 2^n с рациональными коэффициентами. Если все остальные корни этого многочлена лежат в $\mathbb{Q}(\alpha)$, то α можно построить циркулем и линейкой.

Доказательство этого утверждения использует теорию Галуа и теорию групп (см. [4]).

3 Круговые поля

В этом и следующем разделах мы вслед за Гауссом выясним, какие правильные многоугольники построимы циркулем и линейкой, а какие нет. Для этого мы изучим устройство *круговых полей*.

Комплексное число η называется *первообразным* корнем степени n из единицы, если $\eta^n = 1$, но $\eta^k \neq 1$ для любого натурального $k < n$. Например, из корней 4-ой степени из единицы два (i и $-i$) — первообразные, а два (1 и -1) — нет.

3.1. Докажите, что все корни степени n из единицы являются степенями любого первообразного корня.

Пусть η — некоторый первообразный корень степени n из единицы. Расширение $\mathbb{Q}(\eta)$ называется *круговым полем*, или *полем деления круга*. Свойства круговых полей тесно связаны с построимостью правильных многоугольников, так как построить первообразный корень степени n из единицы и все его степени — это всё равно, что поделить дугу окружности на n равных частей, то есть построить правильный n-угольник.

3.2. Найдите степень кругового поля $\mathbb{Q}(\eta)$, где η первообразный корень степени n из единицы для

(a) $n = 3$,
(b) $n = 4$,
(c) $n = 5$,
(d) $n = 6$,

Чтобы найти степень кругового поля для произвольного n, достаточно найти минимальный многочлен $\Phi_n(x)$ для η, то есть неприводимый многочлен, корнем которого является η. Такой многочлен называется *круговым*. По предложению 1, степень этого многочлена и есть степень кругового поля. Понятно, что многочлен $\Phi_n(x)$ делит многочлен x^n-1, поэтому можно попробовать найти $\Phi_n(x)$, поделив x^n-1 на остальные неприводимые делители.

3.3. Проверьте, что если число d делит число n, то многочлен $x^d - 1$ делит многочлен $x^n - 1$.

В частности, из этой задачи следует, что $x^n - 1$ делится на круговой многочлен Φ_d, если d — делитель числа n. Так как все круговые многочлены неприводимы, то $x^n - 1$ делится и на произведение таких круговых многочленов по всем делителям n. Оказывается, что других делителей у $x^n - 1$ нет.

Предложение 2. *Круговой многочлен $\Phi_n(x)$ равен многочлену*

$$\frac{(x^n - 1)}{\prod\limits_{d|n, d\neq n} \Phi_d(x)}. \tag{1}$$

Например, при $n = 6$:

$$\Phi_6(x) = (x^6 - 1)/[\Phi_3(x)\Phi_2(x)\Phi_1(x)] = (x^6 - 1)/[(x^2 + x + 1)(x + 1)(x - 1)] = x^2 - x + 1$$

Чтобы доказать предложение 2, нужно проверить, что многочлен (1) неприводим. Мы это сделаем в случае, когда $n = p^k$ является степенью простого числа p, и предложением 2 будем пользоваться только в этом случае.

Доказательство. Доказательство использует критерий Эйзенштейна.

Критерий Эйзенштейна: Если $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ — многочлен с целыми коэффициентами, такой что $a_1, \ldots, a_n$ делятся на p, но свободный член a_n не делится на p^2, то f неприводим.

3.4. Докажите критерий Эйзенштейна.

Указание: Проверьте, что если $f(x) = g(x)h(x)$ для некоторых многочленов g и h с целыми коэффициентами, то все коэффициенты многочленов g и h, кроме старших, тоже делятся на p. Далее докажите, что любое разложение многочлена f в произведение многочленов с рациональными коэффициентами можно свести к разложению в произведение многочленов с целыми коэффициентами.

Пусть сначала $n = p$. Тогда нужно доказать неприводимость многочлена

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + 1.$$

Чтобы применить критерий Эйзенштейна, сделаем подстановку $y = x - 1$. Получим:

$$\frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = y^{p-1} + py^{p-2} + \frac{p(p-1)}{2!}y^{p-3} + \ldots + p.$$

Коэффициент при y^i имеет вид $\frac{p!}{(i+1)!(p-i-1)!}$ для $i = 0, \ldots, p-1$, то есть делится на p для всех $i = 0, \ldots, p-2$.

3.5. Докажите, что это рассуждение работает и в случае $n = p^k$.

$\square$

Теперь несложно найти связь между степенью многочлена Φ_n и *функцией Эйлера*. Функция Эйлера φ сопоставляет натуральному числу n количество натуральных чисел d, таких что $d < n$ и d взаимно просто с n.

3.6. (a) Докажите, что корнями многочлена Φ_n являются в точности все первообразные корни степени n из единицы.

(b) Докажите, что степень многочлена $\Phi_n(x)$ равна $\varphi(n)$.

(c) Докажите, что $\varphi(p^k) = p^{k-1}(p-1)$, если p — простое число.

Отсюда заключаем, что при $k > 1$ правильный p^k-угольник можно построить, если и только если $p = 2$. Чтобы правильный p-угольник можно было построить циркулем и линейкой необходимо, чтобы $p-1$ являлось степенью двойки. Оказывается, что это условие одновременно и достаточное, то есть правильный p-угольник можно построить циркулем и линейкой тогда и только тогда, когда $p = 2^k + 1$. Такие простые числа называются *числами Ферма*. Поэтому окончательный ответ такой.

Правильный n-угольник можно построить циркулем и линейкой если и только если $n = 2^m p_1 p_2 \ldots p_k$, где p_1, p_2,..., p_k — попарно различные простые числа Ферма, а m — любое неотрицательное целое число.

3.7. Докажите, что если число $2^k + 1$ простое, то k обязательно должно быть степенью двойки.

Периоды с шагом 2. Нам осталось доказать, что если p — простое число Ферма, то правильный p-угольник можно построить циркулем и линейкой. Это было впервые доказано Гауссом [1]. В переводе на алгебраический язык, нам достаточно построить цепочку расширений $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_k = \mathbb{Q}(\eta)$, такую что $[K_i : K_{i-1}] = 2$ для всех $i = 1, \ldots, k$. Здесь и в дальнейшем, η — некоторый первообразный корень степени p из единицы.

В частности, для построения поля K_1 нам нужно найти в поле $\mathbb{Q}(\eta)$ квадратичную иррациональность. В оставшейся части этого раздела мы найдём такую квадратичную иррациональность в случае, когда p — произвольное нечётное простое число. Мы докажем следующее утверждение.

Предложение 3. *Круговое поле, полученное присоединением первообразного корня степени p из единицы, содержит либо $\sqrt{p}$, либо $\sqrt{-p}$.*

Мы применим метод, который придумал Гаусс.

Сначала проиллюстрируем этот метод на примере $p = 5$ (метод похож на алгебраический метод построения правильного пятиугольника). Рассмотрим числа $x_1 =$

$\eta+\eta^4$ и $x_2 = \eta^2+\eta^3$. Докажем, что они являются корнями квадратного уравнения с целыми коэффициентами. Для этого найдём их сумму

$$x_1 + x_2 = \eta + \eta^2 + \eta^3 + \eta^4,$$

и произведение

$$x_1x_2 = (\eta + \eta^4)(\eta^2 + \eta^3) = \eta^3 + \eta^4 + \eta^6 + \eta^7 = \eta + \eta^2 + \eta^3 + \eta^4.$$

Здесь мы воспользовались тем, что $\eta^5 = 1$, так что $\eta^6 = \eta$ и $\eta^7 = \eta^2$. Осталось воспользоваться тем, что

$$1 + \eta + \eta^2 + \ldots + \eta^{n-1} = \frac{\eta^n - 1}{\eta - 1}$$

по формуле для суммы геометрической прогрессии, поэтому, если η — корень степени n из единицы, то $\eta + \eta^2 + \ldots \eta^{n-1} = -1$. Получаем, что $x_1 + x_2 = x_1x_2 = -1$, то есть x_1 и x_2 — корни уравнения

$$x^2 + x - 1 = 0.$$

Поэтому $x_{1,2} = \frac{-1\pm\sqrt{5}}{2}$, и $\pm\sqrt{5} = x_1 - x_2 \in \mathbb{Q}(\eta)$.

Как обобщить это рассуждение на случай произвольного простого p? Для начала поймём, почему разбиение корней на две группы $\{\eta, \eta^4\}$ и $\{\eta^2, \eta^3\}$ оказалось удачным. Чем, например, хуже разбиение на $\{\eta^1, \eta^3\}$ и $\{\eta^2, \eta^4\}$? Тем, что оно зависит от выбора первообразного корня η, и разрушается при выборе другого корня. Действительно, если вместо η подставить, например, $\varepsilon = \eta^2$, то первое (удачное) разбиение выживает (группы $\{\eta, \eta^4\}$ и $\{\eta^2, \eta^3\}$ просто меняются местами), а второе разбиение переходит в совсем другое разбиение на $\{\eta^2 = \varepsilon, \eta = \varepsilon^3\}$ и $\{\eta^4 = \varepsilon^2, \eta^3 = \varepsilon^4\}$. Тем самым, разбиение удачно, если оно сохраняется при любом выборе первообразного корня (то есть группы, из которых состоит разбиение, или меняются местами, или сохраняются). Теперь мы попытаемся найти такое разбиение для произвольного p.

Пусть мы разбили корни η, η^2, $\ldots$, η^{p-1} на две равные группы $\{\eta^{i_1}, \ldots, \eta^{i_{(p-1)/2}}\}$ и $\{\eta^{j_1}, \ldots, \eta^{j_{(p-1)/2}}\}$. Легко видеть, что при подстановке вместо η любого другого корня $\varepsilon = \eta^k$, не равного единице, эти группы перейдут в группы $\{\eta^{ki_1}, \ldots, \eta^{ki_{(p-1/2)}}\}$ и $\{\eta^{kj_1}, \ldots, \eta^{kj_{(p-1)/2}}\}$. Понятно, что вместо показателей $i_1, \ldots, i_{(p-1)/2}$ можно взять только их остатки при делении на p (так как $\eta^p = 1$), то есть *вычеты по модулю* p. Таким образом, нам нужно разбить вычеты по модулю p на две группы, которые при умножении на любой ненулевой вычет k или меняются местами, или сохраняются. Для этого нам понадобится следующий факт из теории чисел.

Факт. Для каждого простого p существует такое натуральное число $q < p$, что все числа 1, q, q^2,..., q^{p-2} имеют попарно различные остатки при делении на p (тем самым каждый ненулевой остаток встречается среди этих чисел ровно один раз). Такое число q называется *первообразным вычетом* по модулю p.

Этот факт был замечен и доказан Эйлером. Два доказательства придумал Гаусс (см. [1], Раздел III, или любой учебник по элементарной теории чисел).

3.8. Найдите первообразный вычет по модулю

(a) 5, **(b)** 7, **(c)** 13, **(d)** 17.

Теперь легко видеть, что разбиение ненулевых вычетов на степени $\{1, q^2, \dots, q^{p-3}\}$ с чётными показателями и на степени $\{q, q^3, \dots, q^{p-2}\}$ с нечётными показателями сохраняется при умножении на любой ненулевой вычет k. В самом деле, если $k = q^l$, то $kq^i = q^{i+l}$, и умножение на k просто сдвигает показатели степеней на l. Поэтому, если l чётно, то чётные показатели переходят в чётные, а нечётные в нечётные, а если l нечётно, то чётные становятся нечётными, и наоборот. При этом мы используем, что $q^{p-1} = 1$ по малой теореме Ферма.

Вернёмся к доказательству предложения 3. Пусть r — произвольный остаток по модулю p. Назовём *периодом* $(2, r)$ сумму

$$\eta^{(rq^2)} + \eta^{(rq^4)} + \dots + \eta^{(rq^{p-1})}.$$

Сумма содержит $\frac{p-1}{2}$ членов. Например, при $p = 5$ это уже знакомые нам выражения: период $(2, 0) = 2$, период $(2, 1) = \eta + \eta^4$, а период $(2, 2) = \eta^2 + \eta^3$.

Перечислим некоторые полезные свойства периодов.

(1) Период $(2, r)$ для любого $r \neq 0$ совпадает либо с периодом $(2, 1)$ (если r равно q в чётной степени), либо с периодом $(2, q)$ (если r равно q в нечётной степени). Период $(2, 0) = \frac{p-1}{2}$.

(2) Произведение двух периодов $(2, r_1)$ и $(2, r_2)$ равно сумме периодов

$$(2, r_1 + r_2) + (2, r_1 + q^2 r_2) + (2, r_1 + q^4 r_2) + \dots + (2, r_1 + q^{p-1} r_2).$$

Это проще всего проверить, воспользовавшись такой картинкой. Возьмём правильный $(p-1)$-угольник с последовательно занумерованными вершинами и поместим каждый корень η^{q^i} в его i-тую вершину (заметим, что это не соответствует расположению корней на комплексной плоскости). Тогда корни, входящие в период $(2, r_i)$, лежат в вершинах правильного $\frac{p-1}{2}$-угольника.

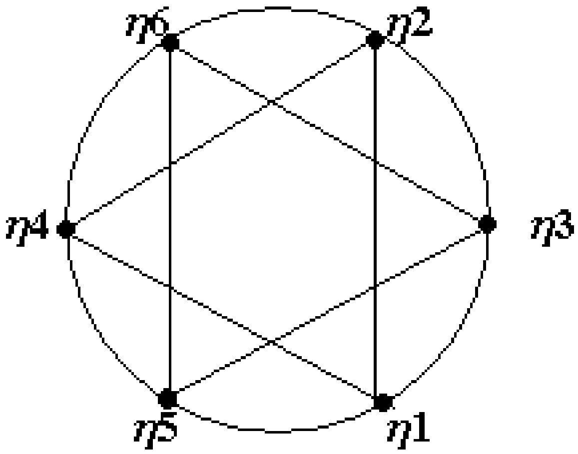

Рис. 2: $p = 7$, $q = 3$.

Теперь, если раскрыть скобки в произведении $(2, r_1) \cdot (2, r_2)$, то получим $\frac{(p-1)^2}{4}$ членов вида $\eta^{r_1 q^i + r_2 q^j}$, где i и j пробегают все чётные числа от 2 до $p-1$. Их можно сгруппировать в $(p-1)/2$ групп по $(p-1)/2$ членов в каждой, объединяя в одну группу произведения тех корней $\eta^{r_1 q^i}$ и $\eta^{r_2 q^j}$, для которых расстояние между соответствующими вершинами одно и то же (иными словами, разность $(i-j)$, рассматриваемая по модулю $(p-1)$, постоянна). Тогда сумма корней в каждой такой группе даст период $(2, r_1 + q^{i-j} r_2)$.

Из свойства (2) следует, что если r_1 и r_2 умножить на одно и то же число r, то

$$(2, rr_1) \cdot (2, rr_2) = (2, r(r_1 + r_2)) + (2, r(r_1 + q^2 r_2)) + (2, r(r_1 + q^4 r_2)) + \ldots + (2, r(r_1 + q^{p-1} r_2))$$

Заметим, что уже из свойства (2) следует, что множество F_2 всех чисел вида $p_1(2,1) + p_2(2,q)$, где p_1 и p_2 рациональны, образует квадратичное расширение поля рациональных чисел. Мы же хотим теперь доказать, что это расширение совпадает с $\mathbb{Q}(\sqrt{\pm p})$. Для этого мы найдём сумму и произведение периодов $(2,1)$ и $(2,q)$, и тем самым по теореме Виета найдём квадратное уравнение, корнями которого они являются.

(3) В произведении

$$(2,1) \cdot (2,q) = (2, 1+q) + (2, 1+q^3) + \ldots + (2, 1+q^{p-2})$$

число периодов $(2,1)$ в правой части равно числу периодов $(2,q)$.

В этом можно убедиться, разбив вычеты $(1+q)$, $(1+q^3)$,..., $(1+q^{p-2})$ на пары $\{(1+q), (1+q^{-1})\}$, $\{(1+q^3), (1+q^{-3})\}$ и т.д. Здесь мы используем, что $q^{p-1} = 1$, так что $q^{-1} = q^{p-2}$ $q^{-3} = q^{p-4}$ и т.д. При этом, если $\frac{p-1}{2}$ нечётно, то один вычет, а именно $(1+q^{(p-1)/2})$, останется без пары. Но этот вычет равен нулю, так как $q^{(p-1)/2} = -1$.

3.9. Докажите, что $q^{(p-1)/2} = -1$.

Каждая неупорядоченная пара периодов $\{(2, q^1), (2, q^{-1})\}$, $\{(2, 1+q^3), (2, 1+q^{-3})\}$ и т.д., как легко видеть, совпадает с парой $\{(2,1), (2,q)\}$. Например, если $(2, 1+q^{-1}) = (2,1)$, то $(2, 1+q) = (2, q(1+q^{-1})) = (2, q)$, и наоборот.

Гаусс доказывал это иначе (его доказательство очень похоже на основные рассуждения в теории Галуа). Он заметил, что по свойству (2)

$$(2,1) \cdot (2,q) = A(2,1) + B(2,q) + C(2,0),$$

где A, B и C — целые неотрицательные числа. При этом

$$(2, 1 \cdot q) \cdot (2, q \cdot q) = A(2, 1 \cdot q) + B(2, q \cdot q) + C(2,0) = A(2,q) + B(2,1) + C(2,0),$$

а так как левые части обоих равенств совпадают, то отсюда можно вывести, что $A = B$. В самом деле, вычитая второе равенство из первого мы получим, что

$$(A-B)(2,1) + (B-A)(2,q) = 0.$$

3.10. Докажите, что если $s(2,1) + t(2,q) = 0$, где s и t рациональны, то $s = t = 0$.

Напомним, что вычет r называется *квадратичным вычетом*, если $r \equiv x^2 \pmod{p}$ для некоторого вычета x. Если такого x не существует, то r называется *квадратичным невычетом*. Проверьте, что q^2, ..., q^{p-1} — квадратичные вычеты, а q, q^3,..., q^{p-2} — невычеты. Доказывая свойство (3), мы попутно получили интересный результат из теории чисел.

Если r — любой квадратичный вычет, а r_1, r_2,..., $r_{(p-1)/2}$ — все квадратичные невычеты, то среди чисел $r+r_1$, $r+r_2$,..., $r+r_{(p-1)/2}$ ненулевых квадратичных вычетов столько же, сколько и невычетов.

Теперь несложно найти произведение $(2,1)\cdot(2,q)$. Из свойства 2 следует, что

$$(2,1)\cdot(2,q) = A(2,1) + B(2,q) + C,$$

где A, B и C — целые числа, в сумме дающие $\frac{p-1}{2}$. Из свойства 3 следует, что $A = B$. При этом C может быть равно только нулю или единице. Действительно, так как вычеты $1+q$, $1+q^3$, ... , $1+q^{p-2}$ попарно различны, то только один из них может быть равен нулю. Поскольку $\frac{p-1}{2} - C = 2A$ — чётное число, получаем, что $C = 1$, если $\frac{p-1}{2}$ нечётно, и $C = 0$, если $\frac{p-1}{2}$ чётно. Попутно мы доказали такой результат.

Число -1 — квадратичный вычет по модулю p тогда и только тогда, когда $(p-1)/2$ чётно.

Теперь находим A, и получаем, что

$$(2,1)\cdot(2,q) = \begin{cases} \frac{1-p}{4}, & \text{если } p = 4k+1 \\ \frac{1+p}{4}, & \text{если } p = 4k+3. \end{cases}$$

(4) Сумма периодов $(2,1)+(2,q)$ равна -1.

Доказывается это так же, как и в случае $p = 5$.

Таким образом, периоды $(2,1)$ и $(2,q)$ — корни квадратного уравнения:

$$\begin{cases} x^2 - x - \frac{p-1}{4} = 0, & \text{если } p = 4k+1 \\ x^2 - x + \frac{p+1}{4} = 0, & \text{если } p = 4k+3, \end{cases}$$

то есть $(2,1)$ и $(2,q)$ совпадают с числами

$$\frac{1 \pm i^{(p-1)/2}\sqrt{p}}{2}.$$

Правда, мы не выяснили какой из корней уравнения какому периоду равен (об этом ещё будет сказано чуть дальше). Но в любом случае, квадрат разности периодов $((2,1)-(2,q))^2$ равен $(-1)^{(p-1)/2}p$, поэтому поле $\mathbb{Q}(\eta)$ содержит $\sqrt{p}$, если $p = 4k+1$, или $\sqrt{-p}$, если $p = 4k+3$.

Разность периодов $G(p) = ((2,1)-(2,q))$ называется *гауссовой суммой*. Другое её определение (уже для произвольного, не обязательно простого n) такое:

$$G(n) = \sum_{i=0}^{n-1} \eta^{(i^2)},$$

где η — первообразный корень степени n из единицы.

3.11. Проверьте, что для простого n, эти определения эквивалентны.

Гауссовы суммы играют важную роль в теории чисел. Например, мы доказали, что $G(p) = \pm i^{(p-1)/2}\sqrt{p}$, но точное определение знака — совсем не простая проблема (попробуйте над ней подумать!). Гауссу после многолетних размышлений удалось доказать, что знак положителен, и получить как следствие ещё одно доказательство *квадратичного закона взаимности* [1]. Очень понятное изложение этого закона с доказательством (правда, другим) дано в [2].

4 Периоды с произвольным шагом

Пусть p — простое число, а d — произвольный делитель числа $p-1$. Так же как и в случае $d = 2$, можно по делителю d построить *периоды* (d, r) следующим образом. Пусть r — произвольный остаток по модулю p. Назовём *периодом* (d, r) сумму

$$\eta^{(rq^d)} + \eta^{(rq^{2d})} + \ldots + \eta^{(rq^{p-1})}.$$

Число d назовём *шагом периода* (d, r), а вычет r — *базой*. Сумма содержит $f = \frac{p-1}{d}$ членов. Если воспользоваться картинкой, аналогичной рисунку 2, то период (d, r) при $r \neq 0$ есть сумма всех корней, стоящих в вершинах правильного f-угольника, вписанного в правильный $(p-1)$-угольник. Всего можно вписать d различных правильных f-угольников. Получаем d различных периодов $(d, 1)$, (d, q),..., (d, q^{d-1}). Точно так же, как в случае $d = 2$, можно доказать, что периоды $(d, 1)$, (d, q),..., (d, q^{d-1}) содержатся в расширении степени d поля рациональных чисел.

В самом деле, произведение любых двух периодов (d, r_1) и (d, r_2) равно сумме периодов с тем же шагом:

$$(d, r_1) \cdot (d, r_2) = (d, r_1 + r_2) + (d, r_1 + q^d r_2) + (d, r_1 + q^{2d} r_2) + \ldots + (d, r_1 + q^{(f-1)d} r_2). \quad (2)$$

4.1. Докажите это утверждение. Проверьте также, что равенство (2) останется верным, если базу во всех участвующих в нём периодах умножить на произвольный вычет r.

Тогда произведение любого числа периодов с шагом d тоже представляется как сумма периодов $(d, 1)$, (d, q), $\ldots$, (d, q^{d-1}) с целыми коэффициентами. Тем самым, множество чисел вида $p_1(d, 1) + p_2(d, q) + \ldots + p_d(d, q^{d-1})$, где $p_1, p_2, \ldots , p_d$ рациональны, является полем. Обозначим это поле через F_d.

Легко убедиться, что степень $[F_d : \mathbb{Q}]$ этого поля как расширения поля рациональных чисел равна d. Действительно, любой элемент F_d единственным образом записывается как сумма периодов $(d, 1)$,..., (d, q^{d-1}) с рациональными коэффициентами. Иначе мы получили бы, что $p_1(d, 1) + p_2(d, q) + \ldots + p_d(d, q^{d-1}) = 0$ для некоторых не равных одновременно нулю рациональных $p_1, p_2, \ldots , p_d$, а это означает (если расписать каждый период как сумму степеней корня η), что η — корень ненулевого многочлена $g(x)$ степени $\leq p-1$ с рациональными коэффициентами и нулевым свободным членом. Поделив многочлен $g(x)$ на x, получим многочлен степени $\leq p-2$, корнем которого опять является η. Но мы знаем, что минимальный многочлен для η — это круговой многочлен $x^{p-1} + x^{p-2} + \ldots + 1 = 0$, степень которого равна $p-1 > p-2$. Противоречие.

Тем самым доказано такое утверждение.

Предложение 4. *Пусть p — простое число, а d — делитель числа $p-1$. Круговое поле, полученное присоединением первообразного корня степени p из единицы, содержит подполе степени d.*

4.2. Докажите, что если F — симметрический многочлен от d переменных, то при подстановке в F периодов $(d, 1)$, (d, q), $\ldots$,(d, q^{d-1}) получится целое число. Более точно,

$$F((d, 1), (d, q), \ldots , (d, q^{d-1})) = A((d, 1) + (d, q) + \ldots + (d, q^{d-1})) + Bf = -A + Bf,$$

где A и B — целые неотрицательные числа.

Указание: воспользуйтесь методом Гаусса, который мы обсуждали в предыдущем разделе для $d = 2$ и задачей 4.1.

Из задачи следует, что периоды $(d, 1)$, (d, q),...,(d, q^{d-1}) — корни уравнения степени d с рациональными коэффициентами. Можно также найти явную формулу для коэффициентов этого уравнения (так же, как мы это сделали в случае $d = 2$) и в случае $d = 3$. Это тоже сделал Гаусс. Задача нахождения коэффициентов тесно связана со свойствами простого числа p. Например, как мы видели, при $d = 2$ ответ зависит от того, является ли -1 полным квадратом по модулю p.

Заметим, что если d' — другой делитель числа $p - 1$, и при этом d' делит d, то F_d содержит $F_{d'}$. Это следует из того, что если $d = d' \cdot f$, то $(d', r) = (d, r) + (d, rq^f) + \ldots + (d, rq^{f(d'-1)})$.

Построимость правильных p-угольников. Продолжим построение правильного p-угольника в случае когда $p = 2^k + 1$ — простое число Ферма. Выше мы убедились, что в качестве первого поля K_1 в цепочке $K_0 = \mathbb{Q} \subset K_1 \subset \ldots \subset K_k = \mathbb{Q}(\eta)$ можно взять квадратичное расширение $\mathbb{Q}(i^{\frac{p-1}{2}}\sqrt{p})$. Метод, с помощью которого мы нашли K_1, годится для нахождения и всех остальных полей. Для каждого i от 1 до k рассмотрим поле F_{2^i}, полученное присоединением всех периодов вида $(2^i, r)$.

Докажем, что если в качестве K_i взять расширение F_{2^i}, то поле K_i будет квадратичным расширением поля K_{i-1}. Это прямо следует из задачи 2.9(c), по которой $[K_i : K_{i-1}] \cdot [K_{i-1} : \mathbb{Q}] = [K_i : \mathbb{Q}]$, и того, что $[F_{2^i} : \mathbb{Q}] = 2^i$. Однако можно это доказать и непосредственно, получив при этом конкретный алгоритм построения, а не только доказательство его существования. Например, можно показать (так же, как мы это проделали при $i = 1$), что сумма и произведение периодов $(2^i, 1)$ и $(2^i, q^{2^{i-1}})$ лежат в K_{i-1}. Мы это сделаем на примере правильного 17-угольника.

Пример (p = 17). Построим циркулем и линейкой правильный 17-угольник. Для этого последовательно найдём периоды $(2, 1)$, $(4, 1)$, $(8, 1)$ и $(16, 1) = \eta$. В качестве первообразного корня η возьмём корень $\cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}$.

Сначала проверим, что 3 — первообразный вычет по модулю 17. Действительно, в следующей таблице (где в i-том столбце записаны показатель i и остаток числа 3^i при делении на 17) встречаются все остатки от 1 до 16.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Эта таблица пригодится нам в вычислениях.

Периоды $(2, 1)$ и $(2, 3)$ — корни уравнения $x^2 + x - 4 = 0$ (см. вычисление из предыдущего раздела). При этом, легко проверить, глядя на рисунок 3, что $(2, 1) > (2, 3)$, поэтому

$$(2, 1) = \frac{-1 + \sqrt{17}}{2}; \quad (2, 3) = \frac{-1 - \sqrt{17}}{2},$$

а не наоборот. На рисунке 3 изображены все первообразные корни 17-ой степени из единицы так, как они расположены на комплексной плоскости.

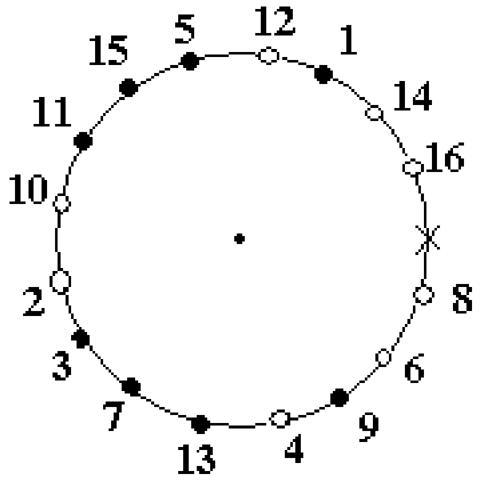

Рис. 3: Корень с номером i равен η^{3^i}.

Найдём уравнение, корнями которого являются периоды $(4,1)$ и $(4,3^2)$. Понятно, что

$$(4,1)+(4,3^2)=(2,1).$$

По формуле для произведения периодов,

$$(4,1)\cdot(4,3^2)=(4,1+3^2)+(4,1+3^6)+(4,1+3^{10})+(4,1+3^{14}).$$

При этом периоды в правой части разбиваются на пары $\{(4,1+3^2),(4,1+3^{-2})\}$ и $\{(4,1+3^6),(4,1+3^{-6})\}$, так что сумма периодов в каждой паре равна периоду с шагом 2. Таким образом,

$$(4,1)\cdot(4,3^2)=(2,1+3^2)+(2,1+3^6).$$

Воспользовавшись таблицей, получаем

$$(2,1+3^2)=(2,10)=(2,3^3)=(2,3); \qquad (2,1+3^6)=(2,16)=(2,3^8)=(2,1).$$

Получается, что

$$(4,1)\cdot(4,3^2)=(2,1)+(2,3)=-1,$$

и периоды $(4,1)$ и $(4,3^2)$ — корни уравнения $x^2-(2,1)x-1=0$. Точно так же можно показать, что периоды $(4,3)$ и $(4,3^2)$ — корни уравнения $x^2-(2,3)-1=0$.

Для периодов $(8,1)$ и $(8,3^4)$ получаем, что

$$(8,1)+(8,3^4)=(4,1)$$

$$(8,1)\cdot(8,3^4)=(8,1+3^4)+(8,1+3^{12})=(4,1+3^4)=(4,14)=(4,3^9)=(4,3),$$

поэтому они удовлетворяют уравнению $x^2-(4,1)x+(4,3)=0$. Наконец, первообразные корни 17-ой степени из единицы $\eta=(16,1)$ и $\eta^{-1}=(16,3^8)$ удовлетворяют уравнению $x^2-(8,1)+1=0$. Таким образом, чтобы найти η, нужно последовательно решить 5 квадратных уравнений. При этом надо каждый раз определять, какой из корней уравнения какому периоду равен, но это в данном случае несложно (нужно опять воспользоваться рисунком 3).

Основная теорема теории Галуа для круговых полей. Теперь уже видно, что теми же методами можно доказать более общее утверждение. Пусть p — произвольное простое число. Напомним, что через F_d мы обозначили поле, полученное присоединением всех периодов с шагом d. Тогда любому разложению на множители числа $(p-1) = d_1 d_2 \ldots d_k$ можно сопоставить цепочку расширений $\mathbb{Q} \subset F_{d_1} \subset F_{d_1 d_2} \subset \ldots \subset F_{p-1} = \mathbb{Q}(\eta)$. При этом степень i-того расширения над предыдущим будет равна d_i. Чтобы минимизировать эти степени (и тем самым упростить нахождение корня η), разумно взять разложение на простые делители.

Теорема 1. (Гаусс [1]) *Пусть p — простое число. Для того, чтобы построить правильный p-угольник, достаточно уметь строить только корни тех уравнений, степени которых равны простым делителям числа $p-1$.*

Эта теорема заключает в себе теорию Галуа для кругового поля, полученного присоединением первообразного корня степени p из единицы, и была доказана Гауссом (ей посвящена седьмая часть его "Арифметических исследований" [1]) за 30 лет до создания общей теории Галуа. Выше мы повторили путь, который проделал Гаусс для доказательства этой теоремы. Галуа внимательно изучил работу Гаусса и понял, что основной принцип, стоящий за рассуждениями Гаусса, работает не только для кругового многочлена, но и для гораздо более общего класса многочленов. Ниже мы разберём этот принцип на примере круговых полей и *поля разложения* кубического многочлена.

Следующий по простоте случай после простых чисел Ферма — это простые числа вида $p = 2^k 3^l + 1$. В этом случае, чтобы построить правильный p-угольник, достаточно уметь строить корни всех кубических уравнений. Если к циркулю и линейке добавить прибор, позволяющий строить корни кубических уравнений, коэффициенты которых уже построены, то можно будет построить правильные p-угольники для всех простых $p = 2^k 3^l + 1$. Например, можно построить правильные 7-угольник, 13-угольник(см. пример в конце этого раздела) и 19-угольник.

Построения с помощью других инструментов. Сейчас мы обсудим построения с помощью дополнительных приспособлений. Все утверждения будут сформулированы в виде задач, некоторые из которых довольно сложные. Решения части задач можно найти в [3] и [5].

Математики Древней Греции придумали множество инструментов, с помощью которых можно проводить трисекцию угла, удвоение куба и разные другие построения, невыполнимые циркулем и линейкой. Иногда вместо дополнительных инструментов использовалась плоскость, на которой помимо базы построения была нарисована вспомогательная кривая.

4.3*. Назовём *парабольной плоскостью* плоскость, на которой нарисована парабола. Докажите, что на парабольной плоскости можно построить с помощью циркуля и линейки:

(a) ось симметрии параболы;

Указание: Сначала докажите, что если окружность пересекает параболу в четырёх точках, то центр тяжести этих точек лежит на оси параболы.

(b) правильный семиугольник;

(c) правильный девятиугольник.

(d) Опишите все правильные n-угольники, которые можно построить на парабольной плоскости.

(e) Докажите, что любой угол на парабольной плоскости можно поделить на три равные части.

(f) Докажите, что на парабольной плоскости можно построить корень любого кубического многочлена, если его коэффициенты уже построены.

*4.4.** Возьмём плоскость, на которой нарисована одна единственная окружность и отмечен также центр окружности.

(a) Докажите, что на такой плоскости с помощью одной только линейки можно построить любую точку, построимую циркулем и линейкой.

(b) Останется ли утверждение пункта (а) верным, если центр окружности не отмечен?

Список возможных построений сильно расширится, если вместо обычной линейки взять линейку с двумя делениями. Для определённости будем считать, что расстояние между делениями равно единице. Линейка с двумя делениями, в отличие от обычной линейки, позволяет проводить также следующее построение. Пусть на плоскости уже построены две прямых, прямая и окружность или две окружности. Обозначим их через l_1 и l_2. Пусть также задана точка P. Тогда с помощью линейки с двумя делениями можно провести через точку P прямую l, так чтобы кривые l_1 и l_2 высекали на l отрезок единичной длины. Однако, с практической точки зрения, линейкой с двумя делениями пользоваться сложно: нужно следить, чтобы одно деление скользило по кривой l_1, второе — по кривой l_2, пока линейка не пройдёт через точку P.

*4.5.** Докажите, что с помощью линейки с двумя делениями и циркуля, можно разделить любой угол на три равные части.

Такая трисекция угла была проведена Архимедом.

Пример (p = 13). Построим на парабольной плоскости правильный 13-угольник с помощью циркуля и линейки.

Сначала проверим, что 2 является первообразным вычетом по модулю 13.

1	2	3	4	5	6	7	8	9	10	11	12
2	4	8	3	6	12	11	9	5	10	7	1

Теперь последовательно найдём периоды $(3,1)$, $(6,1)$ и $(12,1)=\eta$. Найдём коэффициенты уравнения, корнями которого будут $(3,1)$, $(3,2)$ и $(3,4)$. Во-первых,

$$(3,1)+(3,2)+(3,4)=-1$$

Во-вторых, по задаче 4.1

$$(3,1)\cdot(3,2)+(3,2)\cdot(3,4)+(3,1)\cdot(3,4)=A(3,1)+B(3,2)+C(3,4)+D(3,0), \qquad (3)$$

где A, B, C и D — целые неотрицательные числа. Из задачи 4.2 следует, что $A=B=C$. Следующие пояснения предназначаются главным образом читателю, ещё не решившему задачу 4.2. Левая часть равенства (3) не изменится, если базу во всех периодах умножить на 2. Поэтому и правая часть не изменится, но при этом (3,1) переходит в $(3,2)$, $(3,2)$ — в

$(3,4)$, а $(3,4)$ — в $(3,1)$). Получаем, что $A(3,1)+B(3,2)+C(3,4) = C(3,1)+A(3,2)+B(3,4)$. Отсюда уже легко вывести, что $A = B = C$.

Кроме того, $A + B + C + D = 12$, поскольку каждое из попарных произведений равно сумме четырёх периодов с шагом 3. Покажем, что $D = 0$. С одной стороны, любой период в правой части имеет вид $(3, 2^i + 2^j)$, где i и j дают разные остатки при делении на 3. С другой стороны, равенство $2^i + 2^j \equiv 0 \pmod{13}$ означает, что $2^{i-j} \equiv -1 \pmod{13}$, то есть $i - j$ сравнимо с 6 по модулю 12, и тем самым должно делиться на 3. Отсюда получаем, что $D = 0$. Тогда $3A = 12$, то есть $A = 4$.

В-третьих, из тех же соображений,

$$(3,1)\cdot(3,2)\cdot(3,4) = A[(3,1)+(3,2)+(3,4)] + B(3,0),$$

где $3A + B = 4^2$, а B равно числу таких пар (i,j), где $0 \le i,j < 4$, для которых $1 + 2^{1+3i} + 2^{2+3i} \equiv 0 \pmod{13}$. Перебором можно убедиться, что такая пара всего одна, откуда $B = 1$, $A = 5$, а

$$(3,1)\cdot(3,2)\cdot(3,4) = 5\cdot(-1) + 1\cdot 4 = -1.$$

Таким образом, $(3,1)$, $(3,2)$ и $(3,4)$ — корни кубического уравнения

$$x^3 + x^2 - 4x + 1 = 0.$$

По задаче 4.3, мы можем построить его корни.

Заметим, что и для произвольного простого p вида $3k+1$ коэффициенты при x^2 и x в уравнении на периоды $(3,1)$, $(3,q)$ и $(3,q^2)$ находятся тем же способом. Они равны 1 и $-k$, соответственно. Найти можно и свободный член (см. [1]), при этом ответ получается из представления числа $4p$ в виде суммы $x^2 + 27y^2$, где x и y целые. Мы это сделаем в конце следующего раздела, немного иначе, чем Гаусс.

4.6. Докажите, что если N — свободный член в уравнении на периоды $(3,1)$, $(3,q)$ и $(3,q^2)$, то $27N - 1$ делится на p.

Теперь найдём уравнение на периоды $(6,1)$ и $(6,2^3)$. Поскольку,

$$(6,1) + (6,2^3) = (3,1),$$

$$(6,1)\cdot(6,2^3) = (6, 1+2^3) + (6, 1+2^9) = (3, 1+2^3) = (3,4),$$

периоды будут корнями квадратного уравнения $x^2 - (3,1)x + (3,4) = 0$.

Наконец, корни $\eta = (12,1)$ и $\eta^{-1} = (12,2^6)$ удовлетворяют квадратному уравнению $x^2 - (6,1) + 1 = 0$.

5 Теория Галуа

Теперь мы сформулируем основную идею, стоящую за рассуждениями Гаусса для кругового поля, и покажем, как эта же идея работает в случае *поля разложения* кубического многочлена.

Круговое поле. Для каждого простого числа p мы рассматриваем круговое поле $K = \mathbb{Q}(\eta)$, полученное присоединением всех корней степени p из единицы. Наши предыдущие конструкции зависели от выбора первообразного корня, но мы старались эту зависимость свести к минимуму (например, когда разбивали корни на две группы). Сейчас мы сформулируем эту же стратегию более строго. Пусть η и $\zeta = \eta^i$ — два первообразных корня. Определим отображение g_i поля K в себя: для любого элемента $r_0 + r_1\eta + \ldots + \eta^{r-1}$, где r_0, r_1,..., r_{p-1} рациональны, положим

$$g_i(r_0 + r_1\eta + \ldots + r_{p-1}\eta^{p-1}) = r_0 + r_1\zeta + \ldots + r_{p-1}\zeta^{p-1}.$$

Вместо η мы всюду написали ζ. Легко проверить, что отображение g_i взаимно-однозначно, и что для любых двух элементов x и y из K

$$g_i(x+y) = g_i(x) + g_i(y),$$

$$g_i(xy) = g_i(x)g_i(y).$$

Всякое взаимно-однозначное отображения поля в себя с такими свойствами называется *автоморфизмом* поля.

5.1. **(a)** Докажите, что у поля рациональных чисел есть только тривиальный автоморфизм (то есть автоморфизм, переводящий каждый элемент в себя).

(b) Докажите, что автоморфизм любого расширения поля рациональных чисел оставляет все рациональные числа на месте.

5.2. Докажите, что любой автоморфизм кругового поля $K = \mathbb{Q}(\eta)$ совпадает с g_i для некоторого целого i взаимно простого с p, и что g_i совпадает с g_j если и только если i сравнимо с j по модулю p. Таким образом, существует всего $p-1$ различных автоморфизмов.

Легко проверить, что для каждого автоморфизма поля обратное отображение тоже будет автоморфизмом, и что композиция двух автоморфизмов — автоморфизм. Эти свойства означают, что все автоморфизмы поля образуют *группу* относительно операции композиции. Эта группа называется *группой Галуа* поля.

5.3. Обозначим через k^{-1} такой вычет по модулю p, для которого $kk^{-1} \equiv 1 \pmod{p}$. Докажите, что отображение кругового поля в себя, обратное к g_k, совпадает с $g_{k^{-1}}$, и что композиция автоморфизмов g_i и g_j равна g_{ij}.

Тем самым группа автоморфизмов кругового поля (обозначим её через $Gal(K)$ в честь Галуа) совпадает с *мультипликативной группой* $(\mathbb{Z}/p\mathbb{Z})^*$ ненулевых вычетов по модулю p. Композиции автоморфизмов соответствует произведение вычетов. В частности, группа автоморфизмов тоже циклическая: если $i = q^k$ для некоторого первообразного вычета q, то $g_i = (g_q)^k$. Если пронумеровать корни из единицы вычетами по модулю p так, чтобы i-тый корень был равен η^{q^i}, то автоморфизм g_q будет просто сдвигать нумерацию на один вперёд.

Важную роль в теории Галуа играет понятие *инвариантов* автоморфизма. Элемент поля называется *инвариантом* автоморфизма, если этот автоморфизм переводит элемент в себя. Легко проверить, что множество инвариантов фиксированного автоморфизма является подполем. Для автоморфизма g поля $K = \mathbb{Q}(\eta)$ обозначим подполе его инвариантов через K^g.

5.4. **(a)** Докажите, что инвариантами автоморфизма g_q являются все рациональные числа и ничего больше.

(b) Докажите, что если $i = q^2$, то K^{g_i} совпадает с подполем $F_2 \subset K$, полученным присоединением периодов вида $(2, r)$.

(c) Пусть d — делитель числа $p-1$, и $i = q^d$. Докажите, что K^{g_i} совпадает с подполем $F_d \subset K$, полученным присоединением периодов вида (d, r).

(d) Для произвольного целого числа d' докажите, что если $i = q^{d'}$, то K^{g_i} совпадает с подполем $F_d \subset K$, где $d = \text{НОД}(d', p-1)$.

Из пункта (a) немедленно следует очень простое доказательство того, что периоды $(d, 1)$, $\ldots, (d, q^{d-1})$ — корни некоторого многочлена степени d с рациональными коэффициентами. Действительно, элементарные симметрические функции от $(d, 1)$, $\ldots, (d, q^{d-1})$ — инварианты автоморфизма g_q. Поэтому, они рациональны. Правда, такое доказательство не даёт никаких конкретной формулы для коэффициентов уравнения, вроде той, которую мы вывели при $d = 2$ вслед за Гауссом.

Обратно, для каждого подполя $F_d \subset K$ можно рассмотреть множество всех автоморфизмов, которые оставляют на месте все элементы подполя F_d. Легко убедиться, что это множество является *подгруппой* в группе Галуа, то есть оно замкнуто относительно операций композиции и взятия обратного.

5.5. Докажите, что всякий автоморфизм, сохраняющий поле F_d является степенью автоморфизма g_{q^d}, то есть имеет вид $g_{q^{kd}}$, где $k = 1, \ldots, \frac{p-1}{d}$.

Таким образом, группа автоморфизмов, оставляющих на месте все элементы поля F_d, состоит из $\frac{p-1}{d}$ элементов. Основная теорема теории Галуа для круговых полей(см. теорему 1 из предыдущего раздела) теперь может быть переформулирована так.

Теорема 2. *Существует взаимно однозначное соответствие между подполями поля K и подгруппами его группы Галуа, устроенное следующим образом.*

(1) Каждому подполю соответствует группа всех автоморфизмов, переводящих в себя каждый элемент подполя.

(2) Каждой подгруппе соответствует подполе из тех элементов поля K, которые являются инвариантами для каждого элемента подгруппы.

(3) Степень $[K : F]$ поля K над подполем F равна числу элементов в подгруппе, соответствующей F.

Например, самому полю K соответствует подгруппа $\{1\} \subset Gal(K)$ из одного элемента. Заметим, что в таком виде теорема уже может быть сформулирована и для других полей. Класс полей, для которых эта теорема верна, состоит из *полей Галуа*. *Поле Галуа* — это поле, полученное присоединением к полю рациональных чисел *всех* корней какого-либо неприводимого многочлена с рациональными коэффициентами. Оно называется также *полем разложения* этого многочлена. Все подполя кругового поля тоже являются полями Галуа, однако в общем случае это совсем не так. То есть поле Галуа может содержать подполя, не являющиеся полями Галуа (в следующем примере мы это увидим). Отсутствие достаточного числа подполей Галуа в поле разложения многочлена часто приводит к тому, что корни этого многочлена не выражаются в радикалах.

Можно доказать теорему, не используя специфики кругового поля, так что доказательство будет работать для всех полей Галуа. Это доказательство здесь не приводится.

Теорема значительно облегчает доказательство существования цепочек расширений $\mathbb{Q} \subset K_1 \subset \ldots \subset K_n = K$ с заданными степенями. Достаточно построить цепочку подгрупп $Gal(K) \supset G_1 \supset \ldots \supset G_n = \{1\}$ с заданным числом элементов в каждой подгруппе. То есть вместо того, чтобы искать подполе степени d в поле из бесконечного числа элементов, нужно всего лишь найти подгруппу из $\frac{p-1}{d}$ элементов в группе из конечного числа элементов. Например, доказательство построимости правильного 17-угольника циркулем и линейкой проводится в одну строчку. Цепочке подгрупп

$$(\mathbb{Z}/17\mathbb{Z})^* = \{q^i : 1 \le i \le 16\} \supset \{q^{2i} : 1 \le i \le 8\} \supset \{q^{4i} : 1 \le i \le 4\} \supset \{q^{8i} : i = 1, 2\} \supset \{1\}$$

соответствует цепочка подполей, каждое из которых имеет степень 2 над предыдущим. Правда, такое доказательство опять же не даёт никакого конкретного рецепта построения.

Поле разложения кубического многочлена. Пусть теперь поле K — это *поле разложения* неприводимого кубического многочлена $f(x) = x^3 + px^2 + qx + r$ с рациональными коэффициентами, то есть поле, полученное из $\mathbb{Q}$ присоединением всех корней многочлена f. Иначе говоря, это минимальное по включению поле, в котором f раскладывается на линейные множители.

В отличие от кругового многочлена, у f не обязательно существует корень, через степени которого можно выразить остальные корни. Например, поле разложения многочлена $f(x) = x^3 - 2$ может быть получено присоединением $\sqrt[3]{2}$ и первообразного кубического корня ω из единицы. Поэтому его степень равна шести, в то время как степень расширения, полученного присоединением любого из трёх корней многочлена f равна 3. Кстати, отсюда следует, что подполе $\mathbb{Q}(\sqrt[3]{2}) \subset K$ само не является полем Галуа. В общем случае, верно следующее утверждение.

Степень поля разложения неприводимого кубического многочлена равна либо трём, либо шести.

Сейчас мы это докажем. Пусть α — любой из корней многочлена f. Тогда K содержит поле $\mathbb{Q}(\alpha)$, имеющее степень 3. Поэтому степень K делится на 3. Если при этом $K = \mathbb{Q}(\alpha)$, то это значит, что остальные два корня представляются в виде $p_0 + p_1\alpha + p_2\alpha^2$, где p_0, p_1 и p_2 — рациональные числа. Пусть теперь $K \neq \mathbb{Q}(\alpha)$. Это означает, что над полем $\mathbb{Q}(\alpha)$ многочлен f раскладывается в произведение линейного многочлена $x - \alpha$ и неприводимого над $\mathbb{Q}(\alpha)$ квадратичного многочлена, корнями которого являются остальные два корня многочлена f. Поэтому K — квадратичное расширение поля $\mathbb{Q}(\alpha)$, то есть $[K : \mathbb{Q}(\alpha)]{=}2$. Отсюда $[K : \mathbb{Q}] = 6$.

Приведём пример, когда $[K : \mathbb{Q}]{=}3$. Пусть η — первообразный корень седьмой степени из единицы, а $x_1 = \eta + \eta^{-1}$, $x_2 = \eta^2 + \eta^{-2}$ и $x_3 = \eta^3 + \eta^{-3}$ — периоды с шагом 3. Как легко проверить, периоды — корни многочлена $f(x) = x^3 + x^2 - 2x - 1$ (который возникает при попытках построить правильный семиугольник). Поэтому степень поля разложения многочлена f равна трём.

Остаётся вопрос: как по коэффициентам многочлена f понять, какой из двух случаев имеет место? На этот вопрос мы ответим чуть позже, а пока найдём группу Галуа поля K. Пусть x_1, x_2 и x_3 — корни многочлена f.

5.6. Докажите, что любой автоморфизм поля K переводит корни многочлена f друг в друга.

5.7. Докажите, что если для автоморфизмов g и h верно, что $g(x_i) = h(x_i)$ при всех $i = 1, 2, 3$, то $g = h$.

Таким образом, каждый элемент группы Галуа $Gal(K)$ полностью определяется тем, как он переставляет корни многочлена f. Перестановок трёх элементов всего 6, и они образуют группу относительно операции композиции. Эта группа обозначается через S_3. Перестановки из S_3 мы будем обозначать так. Пусть $\{i, j, k\} = \{1, 2, 3\}$. Тогда e — тождественная перестановка, $(i\ j)$ — перестановка, меняющая местами x_i и x_j (таких перестановок три, и они называются *транспозициями*), $(i\ j\ k)$ — перестановка, переводящая x_i в x_j, x_j в x_k и x_k в x_j (таких перестановок две, и они называются *циклами* длины 3).

Мы доказали, что группа Галуа $Gal(K)$ — подгруппа группы S_3. Посмотрим, какие подгруппы бывают у группы S_3. Во-первых, есть три подгруппы из двух элементов: $\{e, (1\ 2)\}$, $\{e, (2\ 3)\}$ и $\{e, (1\ 3)\}$. Действительно, поскольку композиция транспозиции $(i\ j)$ с самой собой равна тождественной перестановке, все эти множества замкнуты относительно умножения и деления. Во-вторых, есть одна подгруппа из трёх элементов $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$. Обозначим эту подгруппу через A_3. В-третьих, есть очевидные подгруппы S_3 и $\{e\}$.

5.8. Проверьте, что $(1\ 2\ 3)^2 = (1\ 3\ 2)$ и $(1\ 2\ 3)^3 = e$.

5.9. **(a)** Пусть s_1 и s_2 — две различные транспозиции из S_3. Проверьте, что любая перестановка из S_3 представляется как композиция нескольких транспозиций, каждая из которых совпадает либо с s_1, либо с s_2.

(b) Докажите то же самое в случае, если s_1 — транспозиция, а s_2 — цикл длины 3.

Из этой задачи следует, что других подгрупп в S_3 нет.

Пример: Пусть $f(x) = x^3 - 2$. Найдём группу Галуа поля разложения многочлена f. Докажем, что любая перестановка корней многочлена f реализуется некоторым элементом группы Галуа. Действительно, пусть $x_1 = \sqrt[3]{2}$, $x_2 = \sqrt[3]{2}\omega$ и $x_3 = \sqrt[3]{2}\omega^2$. Тогда автоморфизм s_1, переводящий $\sqrt[3]{2}$ в себя, а ω — в ω^2, оставляет x_1 на месте, а x_2 и x_3 меняет местами. Автоморфизм s_2, переводящий $\sqrt[3]{2}$ в $\sqrt[3]{2}\omega$, а ω — в ω^2, меняет местами x_1 и x_2. Действительно, $s_2(x_2) = s_2(\sqrt[3]{2}\omega) = s_2(\sqrt[3]{2})$, $s_2(\omega) = \sqrt[3]{2}\omega^3 = x_1$. Тем самым группа Галуа содержит две различных транспозиции и совпадает с S_3 по задаче 5.9.

5.10. Проверьте, что это рассуждение работает для любого кубического многочлена f, такого что степень его поля разложения равна шести.

Таким образом, если степень поля K равна шести, то его группа Галуа совпадает с S_3.

Теперь найдём группу Галуа в случае, когда степень поля K равна 3. В этом случае группа Галуа состоит из трёх элементов. Действительно, корень x_1 может перейти либо в себя, либо в x_2, либо в x_3. Задание образа x_1 полностью определяет автоморфизм на остальных элементах поля (так как любой элемент поля K представляется в виде $p_0 + p_1x_1 + p_2x_1^2$, где p_0, p_1 и p_2 — рациональные числа). Единственная подгруппа в S_3 из трёх элементов — подгруппа A_3. Поэтому если степень поля K равна трём, то его группа Галуа совпадает с A_3.

Заметим, что в обоих случаях элементов в группе Галуа ровно столько, какова степень поля K. Это верно и для произвольных полей Галуа.

Пусть степень поля K равна шести. Используем группу Галуа, чтобы найти квадратичное расширение поля рациональных чисел, содержащееся в K. Основная идея та же, что и в случае кругового поля: построить цепочку расширений $\mathbb{Q} \subset K_1 \subset K$, по цепочке подгрупп $\{e\} \subset A_3 \subset S_3$ группы Галуа. Для этого найдём инварианты группы A_3. Поскольку все неединичные элементы группы A_3 циклически переставляют корни x_1, x_2, x_3, то они циклически переставляют и разности $x_1 - x_2$, $x_2 - x_3$, $x_3 - x_1$ (в отличие от элемента $(1\ 2)$, который меняет знак у разности $x_1 - x_2$). В частности, произведение $D(f) = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ является инвариантом подгруппы A_3.

5.11. Докажите, что $-D(f)^2$ является многочленом с целыми коэффициентами от p, q и r, и найдите его коэффициенты. Этот многочлен называется *дискриминантом* многочлена f.

Указание: Воспользуйтесь тем, что $D(f)^2 = 0$ тогда и только тогда, когда два корня многочлена f совпадают. Пусть совпадающие корни равны a, а оставшийся корень равен b. Получаем параметризацию коэффициентов $p = 2a + b$, $q = a(a + 2b)$ и $r = a^2 b$. Отсюда можно найти полиномиальное соотношение между p, q и r. Его проще всего найти при $p = 0$, чего можно добиться заменой $y = x + \frac{p}{3}$, так как при такой замене значение дискриминанта не изменится.

Отсюда мы сразу получаем ответ на поставленный выше вопрос: как найти степень поля K по его коэффициентам? Нужно вычислить $D(f)^2$. Если из полученного рационального числа нельзя извлечь рациональный квадратный корень, то $[K : \mathbb{Q}] = 6$, а если можно, то $[K : \mathbb{Q}] = 3$. Действительно, в первом случае K содержит квадратичное подполе $\mathbb{Q}(D(f))$, полученное присоединением числа $D(f)$, поэтому степень поля K должна быть чётной. Во втором случае (когда $D(f)$ рационально) разность корней $x_2 - x_3$ лежит в $\mathbb{Q}(x_1)$, так как

$$x_3 - x_2 = \frac{D(f)}{(x_1 - x_2)(x_1 - x_3)},$$

$$(x_1 - x_2)(x_1 - x_3) = x_1^2 - (x_2 + x_3)x + x_2 x_3 = x_1^2 + (p + x_1)x_1 + \frac{r}{x_1}.$$

Здесь мы воспользовались теоремой Виета: $x_1 + x_2 + x_3 = -p$ и $x_1 x_2 x_3 = r$. Поскольку сумма корней $x_2 + x_3 = -p - x_1$ тоже лежит в $\mathbb{Q}(x_1)$, то и сами корни там лежат.

Уравнение на периоды с шагом 3. Закончим вывод формулы для коэффициентов уравнения на периоды с шагом 3, которую мы начали выводить в конце раздела 4. Пусть p — простое число вида $3k + 1$. Мы уже выяснили, что уравнение на периоды имеет вид:

$$x^3 - x^2 + kx + N. \tag{$*$}$$

Нам осталось найти свободный член N. При этом мы знаем, что N — целое число, и, кроме того, $27N - 1$ делится на p (см. задачу 4.6). Так как поле разложения уравнения $(*)$ совпадает с F_3, то его степень равна 3. Поэтому дискриминант уравнения является полным квадратом.

5.12. Докажите, что дискриминант уравнения $(*)$ равен

$$\frac{1}{27}(4p^3 - (3p + 27N - 1)^2).$$

Поскольку дискриминант — целое число, отсюда следует, что $4p^3 - (3p-1)^2$ делится на 27, что впрочем легко проверить и непосредственно. Таким образом, мы получаем, что

$$27M^2 = 4p^3 - (3p + 27N - 1)^2$$

для некоторого целого числа M. При этом, поскольку $27N-1$ делится на p, то и M делится на p, поэтому можно всё уравнение поделить на p^2. Обозначим $3 + (27N-1)/p$ через x_0, а M/p через y_0. Тогда x_0 и y_0 удовлетворяют уравнению

$$4p = x^2 + 27y^2. \qquad (**)$$

В частности, мы доказали, что для всех простых чисел p вида $3k+1$ уравнение $(**)$ разрешимо в целых числах!

5.13. Докажите, что уравнение $(**)$ не может иметь двух разных решений в натуральных числах.

Указание: Проверьте, что если (s,t) и (s',t') — два решения, то $(st'+s't)(st'-s't) = 4p(t'^2-t^2)$. Тогда либо $(st'+s't)$, либо $(st'-s't)$ делится на p. При этом оба числа меньше p. В этом можно убедиться, доказав такие равенства:

$$(ss' \pm 27tt')^2 + 27(st' \mp s't)^2 = 16p^2.$$

Обозначим через (s,t) решение уравнения $(**)$ в натуральных числах. Тогда $x_0 = \pm s$, причём знак определяется однозначно из того, что $p(x_0-3)+1 = 27N$ делится на 27. Например, при $p=7$ имеем $s=t=1$, откуда $x_0=-1$ и $N=-1$.

Список литературы

[1] К.Ф. Гаусс, “Арифметические исследования”, Серия “Классики науки”, Издательство Академии Наук СССР, 1959

[2] С.Г. Гиндикин, “Рассказы о физиках и математиках”, Библиотечка “Квант”, 1981, **14**, сс. 141-158

[3] “Энциклопедия элементарной математики”, Наука, 1963, том **4**

[4] М.М. Постников, “Теория Галуа”, Физматгиз, 1963

[5] В.В. Прасолов, “Три классические задачи на построение”, Серия “Популярные лекции по математике”, Наука 1992