Лекция 4. Построения циркулем и линейкой

1 Представление чисел в виде суммы двух квадратов

1.1 Одна из задач Эрдёша

Одно из классических диофантовых уравнений второй степени записывается как $x^2 + y^2 = m, m \in \mathbb{N}$ и ставит вопрос о количестве целых точек на окружности радиуса $\sqrt{m}$. Одним из интересных приложений, мотивирующих задачу, является открытая проблема, поставленная впервые Палом Эрдёшем.

Задача. Пусть P_n — набор, состоящий из точек плоскости $p_1, \ldots, p_n$, а $f(P_n)$ есть наибольшее количество одинаковых расстояний между какими-либо двумя точками. Какова асимптотическая скорость роста $f(P)$ при $n \to \infty$, если из всех конфигураций точек в качестве P_n берется та, у которой наибольшее значение $f(P_n)$?

Перебрав некоторые простые конструкции, легко получить примеры линейного роста искомой величины. Содержательный же вопрос в том, можно ли построить серию конфигураций со сверхлинейным ростом. Наилучшую известную на сегодня конструкцию построил сам Эрдёш. Его утверждение заключалось в том, что на обычной квадратной сетке $\sqrt{n} \times \sqrt{n}$ можно найти расстояние m (зависящее от n), которое будет встречаться асимптотически чаще, чем $c \cdot n$ раз для любого $c > 0$. В качестве такого значения m берется как раз то, для которого на окружности радиуса $\sqrt{m}$ лежит много целых точек. Эрдёш показал, что при правильном выборе m в зависимости от n, можно найти асимптотически $n \cdot \frac{\log n}{\log \log n}$ расстояний, равных n, сняв тем самым вопрос о возможности сверхлинейного роста. Остаётся, однако, открытым вопрос о том, можно ли получить рост быстрее, чем n^α для какого-либо $\alpha > 1$.

1.2 Решение задачи о сумме двух квадратов

Утверждение 1. Для простого числа $p > 2$ следующие три утверждения равносильны:

(1) p имеет вид $4k + 1, k > 0$.

(2) p не является простым элементом кольца гауссовых чисел $\mathbb{Z}[i]$.

(3) p представляется в виде суммы двух квадратов натуральных чисел, притом единственным образом.

Доказательство. Легче всего установить равносильность (2) и (3). В самом деле, если $p = x^2 + y^2$, то в гауссовых числах можно записать $p = (x + yi)(x - yi)$. Поскольку $x, y \in \mathbb{N}$, то оба элемента из правой части необратимы, то есть p разложим в гауссовых числах и не является простым элементом кольца.

Если $p = (a+bi)(c+di)$, то $p = (a-bi)(c-di)$ и $p^2 = (a^2+b^2)(c^2+d^2)$. Последнее равенство не выходит за пределы целых чисел, поэтому в силу простоты p и необратимости множителей, каждый из них равен p. То есть $p = a^2+b^2 = c^2+d^2$. Каждое из чисел $a \pm bi, c \pm di$ является простым в $\mathbb{Z}[i]$, так как имеет норму p, поэтому из основной теоремы арифметики получается, что либо $(a+bi) \mid (a-bi), (c+di) \mid (c-di)$, либо $(a+bi) \mid (c-di), (c+di) \mid (a-bi)$.

Упражнение 1. $(a+bi) \sim (a-bi) \Leftrightarrow (a+bi) \sim (1+i)$.

Первый случай влечёт $(a+bi) \sim (a-bi)$, то есть $p = 2$, что противоречит условию. Второй случай влечет $(a+bi) \sim (c+di)$, что означает, что разложения a^2+b^2 и c^2+d^2 совпадают. Аналогично, любое разложение p в сумму двух квадратом совпадает с a^2+b^2.

Так как p вида $4k+3$ не может быть суммой двух квадратов, то остается доказать, что любое число вида $4k+1$ раскладывается в гауссовых числах. Для этого нужно доказать, что -1 является квадратичным вычетом по модулю p, что можно сделать, вычислив символ Лежандра или же воспользовавшись более общей теоремой.

Теорема 1. *Пусть $p-1 = r \cdot l, r, l > 1$. Тогда $0 \neq a \in \mathbb{Z}_p$ является r-й степенью ($\exists x : x^r \equiv a \pmod{p}$) тогда и только тогда, когда $a^l \equiv 1 \pmod{p}$.*

Так как $p-1 = 2r$, то -1 является квадратичным вычетом тогда и только тогда, когда $(-1)^r \equiv 1 \pmod{p}$, то есть $r = 2k$ и $p = 4k+1$. Итак, $\exists x : p \mid (x^2+1)$, что в гауссовых числах записывается как $p \mid (x+i)(x-i)$. Если бы p было простым числом, то из этого следовало бы, что $p \mid (x+i)$ или $p \mid (x-i)$. Легко видеть, что это противоречие при $p > 2$, так как если $p \mid (a+bi)$, то $p \mid a$ и $p \mid b$. Итак, число вида $4k+1$ простым в гауссовых числах быть не может, что завершает доказательство утверждения. $\square$

Упражнение 2. Пусть $n = l^2 \cdot p_1 \cdot \ldots \cdot p_m$, где p_i — различные простые. Тогда n представимо в виде суммы двух квадратов, если все p_i имеют вид $4k+1$, притом количество разложений равно 2^{m-1}.

В связи с тем, что по доказанному простые пары p, $p+2$ не могут существовать в $\mathbb{Z}[i]$, можно поставить задачу о простых близнецах в гауссовых числах по-другому.

Упражнение 3 (задача для исследования)**.** Выяснить, конечно ли число пар простых вида $(a \pm 1) + (b \pm 1)i$ в гауссовых числах.

2 Построения циркулем и линейкой

2.1 Стандартная постановка задач на построение

Задаваясь вопросом о построимости того или иного геометрического объекта, неоходимо предельно строго сформулировать задачу. К примеру, если ставить вопрос о построимости отрезка длиной x^2, если дан отрезок длины x, необходимо оговорить, дан ли единичный отрезок. Если, к примеру, дан отрезок длины 1, то важно оговорить, где лежат его конечные точки, потому что если один из его концов имеет координаты $(\sqrt[3]{2}, 0)$, то отрезок длины $\sqrt[3]{2}$ легко построим, однако построить его не удастся, если единичный отрезок дан на оси абсцисс с одним из концов в начале координат.

Устоявшаяся формулировка начальных условий и список разрешённых действий в задачах на построение подразумевает следующие условия:

- Даны координатные оси, перпендикулярные друг другу, и точка их пересечения.
- Слова «дан единичный отрезок» трактуются как «отмечена точка $(1, 0)$».
- Если в процессе построения используется произвольная точка (прямая), то координаты выбираемой точки (коэффициенты уравнения прямой) подразумеваются какими-либо рациональными числами. Это необходимо, так как в результате выбора произвольной точки может быть получена, к примеру, точка $(\pi, 0)$, построить которую в стандартных условиях невозможно.
- Алгоритм построения конечен.
- Одним шагом алгоритма считается одно из следующих действий:
  - Проведение прямой через две уже построенные точки.
  - Проведение окружности с одной из построенных точек в качетсве центра через другую построенную точку.
  - Взятие пересечения двух уже построенных прямых или окружностей или же взятие пересечения уже построенной прямой и уже построенной окружности.
  - Взятие «произвольной» точки или прямой в смысле, оговоренном выше.

Только формализовав таким образом круг возможных действий, можно перейти к доказательству содержательных теорем о непостроимости. В их числе: непостроимость отрезка длины $\sqrt[3]{2}$, непостроимость углов величиной $\frac{\pi}{18}$ (что опровергает возможность трисекции угла в 30 градусов) и $\frac{2\pi}{7}$ (опровергает возможность построения правильного 7-угольника), непостроимость отрезка длины π.

Замечание. Стоит оговориться, что поскольку построение любого отрезка длины x эквивалентно построению его на оси абсцисс, то можно вести речь попросту о «построимости числа».

Если рассматривать координатную плоскость как комплексную, то практически все задачи могут быть сформулированы как построение какого-то определенного числа $z \in \mathbb{C}$ или же набора чисел.

2.2 Поле построимых чисел

Уточнив постановку задачи, можно сформулировать несколько простых наблюдений. Первое из них состоит в том, что задача о построении некоторой точки на плоскости эквивалентна построению обеих её координат (проекций на оси или любых отрезков, равных проекциям по длине). Второе же заключается в том, что множество чисел, построимых, например, на оси абсцисс замкнуто относительно операций сложения, умножения и обратных к ним (для каждой операции можно поредъявить свое несложное геометрическое построеное), то есть представляет собой поле. Эти два наблюдения подитоживаются следующим предложением.

Утверждение 2. Множество построимых комплексных чисел $\widetilde{P}$ является полем и представимо как множество пар построимых вещественных чисел $\{(x, y) \mid x, y \in P\}$, которые также образуют поле.

Замечание. Аналогичное утверждение можно сформулировать в случае, если в задаче на уже даны какие-то числа, отрезки или углы. Множество построимых чисел по-прежнему останется полем, структура которого, как выяснится, устроена похожим образом.

2.3 Расширения полей. Квадратичные расширения

Определение 1. Ситуацию, когда поле K_1 является подполем поля K_2, называют *расширением* полей. Одно или несколько последовательных расширений $K_1 \subset \ldots \subset K_n$ называют *башней* расширений.

Замечание. Важное свойство расширения $K_1 \subset K_2$ состоит в том, что K_2 представляет собой линейное пространство над K_1. Размерность такого линейного пространства называется *степенью* расширения.

Определение 2. Расширение $K_1 \subset K_2$ называется квадратичным, если его степень равна 2 (пишут $[K_2 \colon K_1] = 2$).

Утверждение 3. Пусть есть некоторое поле K, являющееся для простоты подполем $\mathbb{C}$ и задано уравнение квадратное уравнение $x^2 = a$, которое не имеет решений в K. Пусть $\sqrt{a}$ — это какое-то из решений уравнения в $\mathbb{C}$. Тогда минимальное поле $\widetilde{K}$, содержащее K и $\sqrt{a}$ (обозначается $K[\sqrt{a}]$), можно представить как $\widetilde{K} = \{x + y\sqrt{a} \mid x, y \in K\}$, причём все такие линейные комбинации различны.

Доказательство. Очевидно, что все такие линейные комбинации должны лежать в $K[\sqrt{a}]$ в силу того, что оно замкнуто и содержит K и $\sqrt{a}$. Достаточно непосредственно проверить, что $\widetilde{K}$ является полем, тогда по стандартному рассуждению оно и будет минимальным.

Если же какие-то из линейных комбинаций $x + y\sqrt{a}$ совпадают, то это бы значило, что $\sqrt{a}$ выражается через элементы K, то есть лежит в K, что противоречит посылке. $\square$

Замечание. Расширение $K \subset K[\sqrt{a}]$ квадратично.

Замечание. В доказательстве мы использовали то, что $\frac{x+y\sqrt{a}}{p+q\sqrt{a}} \in \widetilde{K}$. Приём, использующийся для доказательства этого простого утверждения, называется домножением на «сопряжённое».*

Следующее наблюдение состоит в том, что любое квадратичное расширение поля K может быть получено добавлением квадратного корня некоторого числа $x \in K$. В самом деле, в качестве базиса в $L \supset K$ могут быть выбраны числа $1, x$, притом известно, что число $(1+x)(1-x) = 1 - x^2 \in L$, что означает, существует квадратное уравнение, имеющее x своим корнем. Тогда x лежит в $K[\sqrt{D}]$, где D — дискриминант этого уравнения.

Имея число a, простым геометрическим пострением можно получить число $\sqrt{a}$, поэтому любое число из любой башни квадратичных расширений сторится циркулем и линейкой.

С другой стороны, в соответствии с описанием алгоритма построения циркулем и линейкой, получение новых точек на каких-то шагах алгоритма происходит с помощью пересечения прямых и окружностей, параметры которых (угловые коэффициенты, центры и радиусы) лежат в некотором поле чисел, которые можно считать уже построенными (в комплексной семантике это минимальное поле, содержащее $\mathbb{C}$ и все точки, отмеченные в ходе алгоритма до рассматриваемого шага).

Самый простой случай — пресечение двух прямых. Легкая выкладка показывает, что точка пересечения двух прямых, заданных уравнениями с коэффициентами в K, лежит в K. Пересечение прямой и окружности же сводится к решению квадратного уравнения, корни которого лежат в $K[\sqrt{D}]$. Наконец, пересечение двух окружностей может быть сведено к пересечению прямой и окружности, так как разность уравенений вида $(x-a)^2+(y-b)^2 = c^2$ будет линейным уравенинем. Итого, точка, построенная на следующем шаге алгоритма либо лежит в K, либо в квадратичном расширении K.

Итого, сделанные наблюдения позволяют сформулировать следующее утверждение, характеризующее поле построимых чисел.

---

*В общем случае операция сопряжения в расширении $K_1 \subset K_2$ — это автоморфизм K_2, сохраняющий K_1.

Легко убедиться, что единственный нетривиальный автоморфизм в расширении $K \subset K[\sqrt{a}]$ переводит $x + y\sqrt{a}$ в $x - y\sqrt{a}$.

Как устанавливается в теории Галуа, для широкого класса расширений количество таких автоморфизмов совпадает со степенью расширения (если она конечна), а их группа, называемая группой Галуа, заключает в себе много информации о свойствах расширения. В частности со свойствами группы Галуа связана выразимость корней уравнений высших степеней в радикалах.

Утверждение 4. Поле построимых чисел P состоит из всех чисел α, для которых $\exists K_0 \subset K_1 \subset \ldots \subset K_n, K_0 = \mathbb{Q}, [K_{i+1} : K_i] = 2, \alpha \in K_n$.

Иными словами, построимы только элементы, лежащие в какой-либо башне квадратичных расширений.

Следующее важное наблюдение описывает строение башен квадратичных расишрений.

Теорема 2. *Пусть $K \subset L \subset T$ — двухэтажная башня конечных расширений полей, причем элементы $\{x_1, \ldots, x_{[L:K]}\}$ представляют собой базис L над K, а $\{y_1, \ldots, y_{[T:L]}\}$ — базис T над L. Тогда расширение $K \subset T$ конечно, имеет базис $\{x_i y_j \mid 1 \leqslant i \leqslant [L : K], 1 \leqslant j \leqslant [T : L]\}$ и степень $[T : K] = [T : L] \cdot [L : K]$.*

Упражнение 4. Доказать теорему.

Замечание. Простое, но очень важное следствие теоремы: если каждое расширение в башне $K_1 \subset \ldots \subset K_n$ конечно, то $K_1 \subset K_n$ тоже конечно.

Несмотря на простоту, теорема представляет собой мощный инструмент: она позволяет по-другому доказать то, что построимые числа образуют поле, а также, например, то, что полем являются все алгебриаические числа.

Другим немедленным следствием теоремы является такое утверждение:

Утверждение 5. Любое построимое число $\alpha \in P$ обладает свойством $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 2^r$ для некоторого натурального r.

Доказательство. По характеристическому свойству построимых чисел получаем, что существует башня расширений $K_0 \subset \ldots K_n$, $[K_{i+1} : K_i] = 2$, $\alpha \in K_n, K_0 = \mathbb{Q}$. Из того, что $\alpha \in K_n$ следует, что $\mathbb{Q}[\alpha] \subset K_n$, то есть имеет место башня расширений $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset K_n$. По тоереме о степени расширения, $2^n = [K_n : \mathbb{Q}] = [\mathbb{Q}[\alpha] : \mathbb{Q}] \cdot [K_n : \mathbb{Q}[\alpha]]$, откуда немедленно следует, что $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ является степенью двойки. □

Замечание. Утверждение можно использовать как инструмент для доказательства непостроимости каких-либо чисел. Так, если показать, что $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ не является степенью двойки, то из характеристического свойства и утверждения выше немедленно получается, что $\alpha \notin P$.

Теперь задача о построимости числа α практически свелась к задаче о подсчёте степени расширения $\mathbb{Q}[\alpha]$. Мощным инструментом для поиска степени расширения оказывается следующая теорема:

Теорема 3. *Пусть K — поле, $f(x) \in K[x]$ — неразложимый многочлен, $\deg f = l, \alpha$ — корень* $f(x)$. Тогда $[K[\alpha] : K] = l$.*

*В этом месте стоит оговориться, откуда берётся α. Например, если K является подполем $\mathbb{C}$, то α можно брать из $\mathbb{C}$. В общем же случае можно показать, что существует конструкция поля, являющаяся расширением K, в котором у f есть один корень или даже все l. Здесь и далее неявно полагается, что $K \subset \mathbb{C}$, однако соответсвующие рассуждения можно провести и в общем случае

Доказательство. Покажем, что $K[\alpha] = \{a_0 + \ldots + a_{l-1}\alpha^{l-1} \mid a_0, \ldots, a_{l-1} \in K\}$. Тогда теорема будет доказана, так как такие выражения $K[\alpha]$ содержать обязано. Осталось показать, что они образуют поле.

Проверка замкнутости относительно сложения и вычитания тривиальна. Для проверки умножения можно без потери общности считать, что старший коэффициент многочлена f равен единице (он не может быть нулём, так как $\deg f = l$). Пользуясь тем, что $f(\alpha) = 0$, можно выразить α^l как линейную комбинацию $1, \alpha, \ldots, \alpha^{l-1}$. Поэтому в произведении двух линейных комбинаций вида $\sum a_i\alpha^i$ от всех степеней выше l можно избавиться.

Осталось проверить наличие обратного по умножению элемента. Для этого как минимум нужно показать, что для никакая нетривиальная линейная комбинация $1, \alpha, \ldots, \alpha^{l-1}$ не равна нулю. Такое равенство повлекло бы существование многочлена степени меньше l, у которого α является корнем. Пусть $g(x)$ — многочлен минимальной степени среди всех многочленов, обнуляющих $\alpha, \deg g < l$. Пусть также f даёт остаток σ при делении на g: $f = gh + \sigma$. Но тогда, так как $f(\alpha) = 0, g(\alpha) = 0$, то $\sigma(\alpha) = 0$. Если $\sigma \not\equiv 0$, то $\deg \sigma < r$ по определению деления с остатком, что противоречит определению g. Значит $\sigma \equiv 0$, что в свою очередь влечёт противоречие с неразложимостью f.

Таким образом, все линейные комбинации в $K[x]$ различны. Осталось предъявить обратный по умножению элемент к $h(\alpha) = v_0 + \ldots + v_{l-1}\alpha^{l-1}$. Пусть $h(x) = v_0 + \ldots + v_{l-1}x^{l-1}$, тогда, очевидно, что $(f, h) = 1$, так как иначе f разложим. Но в таком случае $\exists g_1, g_2 \in K[x] : f(x)g_1(x)+h(x)g_2(x) \equiv 1$. При подставлении α получается, что $h(\alpha)g_2(\alpha) \equiv 1$, что означает, что $g_2(\alpha)$ и будет обратным к $h(\alpha)$ (если $\deg g_2 \geqslant l$, то от членов с α в степени выше, чем $l - 1$ можно избавиться стандартным способом). $\square$

2.4 Примеры непостроимых чисел

Утверждение 6. $x^3 - 2$ является неразложимым над $\mathbb{Q}$ многочленом.

Доказательство. Пусть это неверно, тогда $x^3 - 2 = (x - a)h(x)$, тогда $a \in \mathbb{Q}$ зануляет левую часть, то есть у $x^3 - 2$ есть рациональный корень, что невозможно. $\square$

Итак, $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$ и число $\sqrt[3]{2}$ непостроимо.

Упражнение 5. Записать минимальный многочлен для числа $\alpha = \sin\frac{\pi}{18}$ и доказать его неразложимость.

2.5 Построимость правильных многоугольников

2.5.1 Правильный 7-угольник

Вопрос о построимости правильного n-угольника равносилен вопросу о построимости комплексного числа $\xi = e^{\frac{2\pi}{n}}$ с помощью циркуля и линейки. Несложно заметить, что $2\cos\frac{2\pi}{n} = \xi + \xi^{-1}$.

Пусть n нечётно и $\sigma_r = \xi^r + \xi^{-r} = 2\cos(\frac{2\pi r}{n})$ для $r = 1, \ldots, \frac{n-1}{2}$. Для решения вопроса о построимости ξ или, что тоже самое, σ_1, нужно исследовать строение расширения $\mathbb{Q} \subset \mathbb{Q}[\sigma_1]$.

Сперва можно исследовать арифметические свойства чисел σ_n для $n = 7$. Как несложно посчитать, $\sigma_1^2 = \sigma_2 + 2, \sigma_2^2 = \sigma_4 + 2, \sigma_4^2 = \sigma_1 + 2$. Вообще, таблица умножения в $\mathbb{Q}[\sigma_1]$ выглядит следующим образом.

	σ_1	σ_2	σ_3
σ_1	$\sigma_2 + 2$	$\sigma_1 + \sigma_3$	$\sigma_2 + \sigma_3$
σ_2	$\sigma_1 + \sigma_3$	$\sigma_4 + 2$	$\sigma_1 + \sigma_2$
σ_3	$\sigma_2 + \sigma_3$	$\sigma_1 + \sigma_2$	$\sigma_1 + 2$

Также $\sigma_1 + \sigma_2 + \sigma_3 = -1$.

Упражнение 6. Пользуясь полученной таблицей, показать, что σ_1 удовлетворяет уравнению $\sigma_1^3 + \sigma_1^2 - 2\sigma_1 - 1 = 0$.

Таким образом вопрос о построимости правильного семиугольника сведен к вопросу о разложимости многочлена $x^3 + x^2 - 2x - 1$. Однако рациональных корней у него нет (так как числитель рационального корня должен делить свободный член, а знаменатель — старший коэффициент), поэтому приводимым он быть не может и степень расширения $[\mathbb{Q}[\sigma_1] : \mathbb{Q}] = 3$ при $n = 7$. Итак, правильный семиугольник непосторим с помощью циркуля и линейки.

2.5.2 Правильный 17-угольник

Как было доказано Гауссом в своё время, для правильного 17-угольника алгоритм построения циркулем и линейкой существует. Поэтому целью здесь будет являться не просто нахождение степени расширения $\mathbb{Q}[\sigma_1]$, а построение конкретной башни квадратичных расширений, последнее из которых содержит σ_1. Для начала стоит снова немного изучить арифметические свойства чисел σ_i.

Пусть $\tau_1 = \sigma_1 + \sigma_2 + \sigma_4 + \sigma_8, \tau_2 = \sigma_3 + \sigma_5 + \sigma_6 + \sigma_7, \tau_1 + \tau_2 = -1$.

Тогда $\tau_1^2 = \tau_1 + 8 + 2(\sigma_1 + \sigma_3 + \sigma_3 + \sigma_5 + \sigma_7 + \sigma_8 + \sigma_2 + \sigma_6 + \sigma_6 + \sigma_7 + \sigma_4 + \sigma_5) = \tau_1 + 8 + 2(\tau_1 + 2\tau_2) = 8 + \tau_1 + 2\tau_1 + 4(-1 - \tau_1) = 4 - \tau_1$. Значит, числа τ_1 и τ_2 строятся циркулем и линейкой (лежат в $\mathbb{Q}[\sqrt{17}]$).

Далее нужно разбить τ_1 и τ_2 следующим образом:

$$\tau_1 = \underbrace{\sigma_1 + \sigma_4}_{\beta_1} + \underbrace{\sigma_2 + \sigma_8}_{\beta_2},$$
$$\tau_2 = \underbrace{\sigma_3 + \sigma_5}_{\beta_3} + \underbrace{\sigma_6 + \sigma_7}_{\beta_4}.$$

Число $\beta_1 + \beta_2$ уже построено, поэтому нужно понять, чему равно произведение $\beta_1\beta_2 = (\sigma_1 + \sigma_4)(\sigma_2 + \sigma_8) = \sigma_1 + \sigma_3 + \sigma_2 + \sigma_6 + \sigma_7 + \sigma_8 + \sigma_4 + \sigma_5 = -1$.

Тогда по теореме Виетта, числа β_1, β_2 также будут построимыми. Аналогично, $\beta_3\beta_4 = -1$, поэтому все β_i будут построимы, притом добавить надо числа $\sqrt{\tau_1^2 + 4}$ и $\sqrt{\tau_2^2 + 4}$.

Осталось вычислить, что такое $\sigma_1\sigma_4 = \sigma_3 + \sigma_5 = \beta_3$. Тогда сумма и произведение чисел σ_1 и σ_4 оказываются уже построены, то есть при расширении поля корнем $\sqrt{\beta_1^2 - 4\beta_3}$, получается поле, содержащее σ_1.

Итак, алгоритм построения правильного 17-угольника полностью описан.