А. Г. Хованский, Построения циркулем и линейкой, *Матем. просв.*, 2013, выпуск 17, 42–60

Алгебра геометрических построений

Построения циркулем и линейкой

А. Г. Хованский

Древние греки решили много красивых задач на построение циркулем и линейкой и обнаружили несколько проблем, которые стали чрезвычайно знаменитыми из-за многочисленных безуспешных попыток их решения, предпринимавшихся на протяжении многих веков. Древние греки построили правильные n-угольники для $n = 2^k \cdot 3$, $2^k \cdot 4$, $2^k \cdot 5$, $2^k \cdot 15$, где k — любое неотрицательное число. Построить правильный n-угольник для какого-либо другого n никому не удавалось до тех пор, пока Гаусс не построил правильный 17-угольник и не описал полностью числа n, для которых задача построения разрешима. Гаусс получил этот замечательный результат еще до возникновения теории Галуа. Его удивительное открытие оказало огромное влияние на развитие ряда областей математики. Здесь мы рассказываем об этой задаче и о других задачах на построение.

Задачи на построение — самые старые задачи о «разрешимости в явном виде». Мы различаем три класса построений. В первом, самом простом, классе допускается лишь построение прямой, проходящей через две заданные точки, окружности данного радиуса с данным центром и точки пересечения данных прямых и окружностей.

В третьем, самом сложном, классе кроме перечисленных построений допускается выбор произвольных точек, но требуется, чтобы результат построения не зависел от сделанных произвольных выборов.

Во втором, промежуточном, классе произвольный выбор не допускается, но разрешаются два построения, осуществляемые при помощи этой операции: построение центра данной окружности и построение перпендикуляра к данной прямой, проходящего через данную точку, не лежащую на прямой.

Математическое просвещение, сер. 3, вып. 17, 2013(42–60)

Логически построения третьего класса отличаются от построений остальных классов: промежуточные объекты, получающиеся в процессе построения, могут зависеть от произвольного выбора. В этом случае они не считаются построенными циркулем и линейкой. Мы стараемся обойтись, когда это возможно, без операции выбора произвольной точки. Мы доказываем, что использование этой операции в большинстве задач на построение не добавляет ничего нового (все, что строится при помощи этой операции, можно построить и без нее). Часть классических задач на построение вполне удовлетворительно формулируется и решается внутри первого класса построений.

Задача о трисекции угла нуждается в операции выбора произвольной точки: по двум данным прямым, проходящим через данную точку, остальными операциями вообще нельзя построить ничего нового. Мы показываем, что если к двум данным прямым добавить произвольно выбранную точку на одной из них, то по этим новым данным операциями первого класса можно построить все, что строится операциями третьего класса по двум данным прямым.

Второй класс построений нужен, чтобы расширить исходное множество начальных данных. Например, операции первого класса построений не позволяют построить ничего нового, если множество начальных данных — несколько непересекающихся окружностей. Но если к окружностям добавить их центры, то по этим новым данным операциями первого класса можно построить все, что строится операциями третьего класса по исходным данным (если среди окружностей есть две с разными центрами).

В первом параграфе мы обсуждаем задачу о разрешимости алгебраических уравнений при помощи квадратных корней, нужную для задач на построение. Мы делаем это даже в большей общности, чем необходимо (мы не предполагаем, что основное поле совершенно и что его характеристика не равна двум). Эта задача интересна сама по себе, а лишняя общность не добавляет больших хлопот. Второй параграф посвящен задачам на построение.

§1. Разрешимость уравнений в квадратных корнях

В этом параграфе мы обсуждаем следующий вопрос о разрешимости уравнений в конечном виде: когда неприводимое алгебраическое уравнение над полем K решается при помощи арифметических операций и извлечения корней степени два? Теория Галуа отвечает на этот вопрос, если поле K совершенно и его характеристика не равна двум. Простые дополнительные рассуждения позволяют ответить на этот вопрос, не делая никаких предположений о поле K.

О расположении материала. В п. 1.1 собран нужный вспомогательный материал. В п. 1.2 приводится необходимое и достаточное условие разрешимости уравнения при помощи квадратных корней, если характеристика поля K не равна двум. В п. 1.3 тот же вопрос решается для полей характеристики два. В пп. 1.4–1.5 приводятся результаты Гаусса о корнях степени n из единицы (нужные для задачи о правильном n-угольнике).

1.1. Вспомогательный материал

Напомним несколько элементарных утверждений. Если поле K содержится в поле F, то F является векторным пространством над K. Если $\dim_K F < \infty$, то поле F называется *конечным расширением* поля K, размерность $\dim_K F$ называется *степенью* расширения и обозначается символом $[F : K]$.

Теорема 1. *Если $K \subset F$ и $F \subset M$ — конечные расширения, то*:
1) *$K \subset M$ — конечное расширение*;
2) $[M : K] = [M : F][F : K]$.

Доказательство. Пусть $u_1, \ldots, u_n$ — базис F над K и $v_1, \ldots, v_m$ — базис M над F. Легко видеть, что элементы $u_i v_j$, где $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$, образуют базис M над K. Откуда вытекают оба утверждения теоремы.

Утверждение 2. 1) *Если $[F : K] = n$ и $a \in F$, то существует полином Q над полем K степени, не большей чем n, такой, что $Q(a) = 0$.*
2) *Если Q — неприводимый над K полином и $Q(a) = 0$, то $[K(a) : K] = \deg Q$.*

Доказательство. 1) Так как $\dim_K F = n$, то элементы 1, a, $\ldots$, a^n зависимы, т. е. найдутся $\lambda_i \in K$, такие, что $\lambda_n a^n + \lambda_{n-1} a^{n-1} + \cdots + \lambda_0 = 0$, причем для некоторого $i > 0$ коэффициент λ_i не равен нулю.
2) Поле $K(a)$ изоморфно полю $K[x]/I$, где I — идеал, порожденный полиномом Q степени n.

Утверждение 3. *Если степень неприводимого полинома над полем характеристики $p > 0$ не делится на p, то все его корни некратны.*

Доказательство. Кратный корень полинома Q является корнем его производной Q'. Неприводимый полином Q не может иметь общего корня с ненулевым полиномом меньшей степени. Поэтому если Q имеет кратный корень, то $Q' \equiv 0$, т. е. $Q(x) = R(x^p)$, где R некоторый полином. В этом случае $\deg Q = p \cdot \deg R$ и, следовательно, $\deg Q$ делится на p.

1.2. 2-радикальные расширения.

Вернемся к вопросу о разрешимости уравнений при помощи квадратных корней.

Определение. Расширение $K \subset F$ называется 2-*радикальным*, если существует башня полей $K = F_0 \subset F_1 \subset \cdots \subset F_n$, такая, что $F \subset F_n$ и $F_i = F_{i-1}(a_i)$ при $1 \leqslant i \leqslant n$, где $a_i^2 \in F_{i-1}$ и $a_i \notin F_{i-1}$.

Теорема 4. *Если $K \subset F$ — 2-радикальное расширение, то $[F : K] = 2^k$.*

Доказательство. Для $K = F_0 \subset F_1 \subset \cdots \subset F_n$ имеем $[F_n : K] = [F_n : F_{n-1}] \cdot \ldots \cdot [F_1 : F_0] = 2^n$. Если $K \subset F \subset F_n$, то $[F : K] \cdot [F_n : F] = 2^n$. Поэтому $[F : K]$ — степень двойки.

Следствие 5. *Если неприводимый над K полином P имеет корень в некотором 2-радикальном расширении поля K, то $\deg P = 2^k$.*

Доказательство. Если $P(a) = 0$, то $[K(a) : K] = \deg P$.

Следствие 6. *Пусть характеристика поля K не равна двум. Кубическое уравнение $P = 0$ над полем K решается в квадратных корнях, если и только если один из корней уравнения содержится в поле K.*

Доказательство. Если $a \in K$ и $P(a) = 0$, то $P = (x - a)Q$, где $Q \in K[x]$. Квадратное уравнение $Q = 0$ решается в квадратных корнях, так как характеристика поля K не равна двум. Если кубический полином не имеет корня в K, то он неприводим и можно воспользоваться следствием 5.

Замечание. Для $K = \mathbb{Q}$ следствие 6 принимает явный вид: для полинома $P \in \mathbb{Q}[x]$ можно явно найти все его рациональные корни (в частности, можно явно проверить, что таких корней нет). Если корень a найден, то квадратное уравнение $0 = Q(x) = P/(x - a)$ решается явно.

Обозначим через E_P поле разложения полинома P над полем K.

Следствие 7. *Если неприводимый над K полином P имеет корень в некотором 2-радикальном расширении поля K, то $[E_P : K] = 2^m$.*

Доказательство. Расширение $K \subset E_P$ в условиях следствия 2-радикально.

Следствие 7 допускает следующее частичное обращение.

Теорема 8. *Если для неприводимого полинома P над полем K, характеристика которого не равна двум, выполняется равенство $[E_P : K] = 2^m$, то расширение $K \subset E_P$ является 2-радикальным.*

Доказательство. Степень расширения $[E_P : K]$ делится на степень полинома P, поэтому $\deg P = 2^k$. Следовательно, по утверждению 3, уравнение $P = 0$ сепарабельно и к нему применима теория Галуа. Порядок группы Галуа G поля E_P над полем K равен числу $[E_P : K] = 2^m$. Так как порядок группы G является степенью двойки, то существует нормальная башня подгрупп $G = G_0 \supset G_1 \supset \cdots \supset G_m = e$, такая, что $G_i/G_{i-1} = \mathbb{Z}_2$ при $1 \leqslant i \leqslant k$. Для башни полей $K = K_0 \subset K_1 \subset \cdots \subset K_m = E_P$, соответствующей этой башне подгрупп, имеем $[K_i : K_{i-1}] = 2$. Так как характеристика поля K (а, значит, и поля K_i) не равна двум, то поле K_i получается из поля K_{i-1} присоединением квадратного корня.

1.3. 2-радикальные расширения полей характеристики два

В этом пункте мы будем обозначать символом K некоторое поле характеристики два и символом $\overline{K}$ — его алгебраическое замыкание. Нас интересуют лишь алгебраические элементы над полем K и алгебраические расширения поля K. Не ограничивая общности, можно считать, что эти элементы и расширения содержатся в поле $\overline{K}$.

Лемма 9. *Множество элементов y, таких, что $y^2 \in K$, является полем.*

Доказательство. Лемма вытекает из равенства $(a + b)^2 = a^2 + b^2$, справедливого в полях характеристики два.

Определим цепочку подполей $K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \ldots$ поля $\overline{K}$ при помощи соотношения $y \in K_{i+1}$, если и только если $y^2 \in K_i$. Поле $\widetilde{K} = \bigcup K_i$ будем называть *совершенным замыканием* поля K. Легко видеть, что поле $\widetilde{K}$ является минимальным совершенным полем, содержащим поле K.

Теорема 10. *Конечное расширение $K \subset M$ поля K является 2-радикальным, если и только если $M \subset \widetilde{K}$.*

Доказательство. Если для башни полей $K = F_0 \subset F_1 \subset \cdots \subset F_n$ имеем $F_i = F_{i-1}(a_i)$, где $a_i^2 \in F_{i-1}$, то $F_i \subset K_i$.

Полином $P \in K[x]$ называется *минимальным полиномом* алгебраического элемента a над K, если $P(a) = 0$, полином P неприводим и унимодален (т. е. старший коэффициент полинома P равен единице).

Теорема 11. *Полином P является минимальным полиномом некоторого элемента $a \in K_n \setminus K_{n-1}$, если и только если $P(x) = x^{2^n} - b$, где $b \in K$ и $b \neq c^2$ для всякого $c \in K$.*

Доказательство. Элемент $a \in K_n$ является единственным (кратным) корнем полинома $x^{2^n} - b$, где $b = a^{2^n} \in K$, поэтому минимальный

полином P элемента a имеет единственный корень a. Числа m, такие, что $a^m \in K$, образуют аддитивную подгруппу в $\mathbb{Z}$. Если $a \in K_n \setminus K_{n-1}$, то $a^m \in K$, только если m делится на 2^n. Откуда видно, что $P(x) = x^{2^n} - b$.

Следствие 12. *Если $P \in K[x]$ — унимодальный и неприводимый над K, то уравнение $P(x) = 0$ разрешимо в квадратных корнях, если и только если $P(x) = x^{2^n} - b$, где $b \in K$ и $b \neq c^2$ для всякого $c \in K$. В частности, всякое неприводимое уравнение степени большей единицы над совершенным полем K не решается при помощи квадратных корней.*

1.4. Корни из единицы

Здесь мы напоминаем классические результаты Гаусса, открытые еще до возникновения теории Галуа.

Пусть $\Omega_n \subset \mathbb{C}$ — множество чисел x, таких, что $x^n = 1$, и Ω_n^* — множество всех *примитивных корней из единицы* степени n, т. е. множество чисел $a \in \Omega_n$, таких, что $a^m \neq 1$ при $0 < m < n$. Если $\omega \in \Omega_n^*$, то: 1) $a \in \Omega_n$, если и только если $a = \omega^k$ для некоторого целого k; 2) $a \in \Omega^*$, если и только если $a = \omega^k$, где k взаимно просто с n, т. е. вычет k по модулю n лежит в мультипликативной группе $U(n)$ обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$. *Циклотомическим полиномом* степени n называется полином $\Phi_n(x) = \prod_{a \in \Omega_n^*} (x - a)$.

Лемма 13. *Справедливо равенство $x^n - 1 = \prod_{d|n} \Phi_d(x)$, где произведение берется по всем делителям d числа n.*

Доказательство. Вытекает из соотношений

$$\Omega_n = \bigcup_{d|n} \Omega_d^* \quad \text{и} \quad \Omega_{d_1}^* \bigcap \Omega_{d_2}^* = \varnothing \text{ при } d_1 \neq d_2.$$

Следствие 14. *Полином Φ_n унимодален и имеет целые коэффициенты.*

Доказательство. Если P, $Q \in \mathbb{Z}[x]$ — унимодальные полиномы, то: 1) полином PQ унимодален и $PQ \in \mathbb{Z}[x]$; 2) если $T = P/Q$ — полином, то полином T унимодален и $T \in \mathbb{Z}[x]$. Мы используем очевидные факты 1)–2) для индукционного доказательства следствия. Для $n = 1$ следствие верно, так как $\Phi_1(x) = x - 1$. Положим $\Psi_n = \prod \Phi_{d'}$, где произведение берется по делителям d' числа n, меньшим чем n. Если следствие верно для $d' < n$, то, согласно 1), полином Ψ_n унимодален и $\Psi_n \in \mathbb{Z}[x]$. По лемме 13 $\Phi_n(x) = (x^n - 1)/\Psi_n(x)$. Согласно 2), следствие верно для $d = n$.

Полином $f \in \mathbb{Z}[x]$ называется *примитивным*, если его коэффициенты не имеют общего делителя. *Произведение примитивных полиномов является примитивным полиномом*. Из этого факта и теоремы Гаусса

автоматически вытекает следующее *свойство целочисленности*: если для $f_1 = f_2 f_3$, где f_1, f_2 — унимодальные полиномы, $f_1 \in \mathbb{Z}[x]$ и $f_2, f_3 \in \mathbb{Q}[x]$, то полиномы f_2, f_3 имеют целые коэффициенты и полином f_3 унимодален.

Напомним также, что если p взаимно просто с n, то полином $x^n - 1 \in \mathbb{Z}_p[x]$ не имеет кратных корней (так как $n \neq 0 \mod p$, то производная nx^{n-1} полинома $x^n - 1$ не имеет ненулевых корней).

Теорема 15 (Гаусс). *Полином Φ_n неприводим над $\mathbb{Z}$.*

Лемма 16 (Гаусс). *Пусть $\omega \in \Omega_n^*$, f — минимальный полином числа ω и p — простое число, взаимно простое с n. Тогда $f(\omega^p) = 0$.*

Доказательство. Число ω — корень полинома Φ_n. Поэтому $\Phi_n = fg$, где $g \in \mathbb{Q}[x]$. Согласно свойству целочисленности, $g \in \mathbb{Z}[x]$ и полином g унимодален. Допустим, что $f(\omega^p) \neq 0$. Тогда $g(\omega^p) = 0$, так как $0 = \Phi_n(\omega^p) = f(\omega^p)g(\omega^p)$. В этом случае ω — корень полинома $g(x^p)$, поэтому $g(x^p) = fh$, где $h \in \mathbb{Q}[x]$. Согласно свойству целочисленности, $h \in \mathbb{Z}[x]$ и полином h унимодален. Пусть $\pi\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ — гомоморфизм, продолжающий на кольцо полиномов естественное отображение $\mathbb{Z} \to \mathbb{Z}_p$. Имеем $(\pi g)(x^p) = (\pi f)(\pi h)$. В кольце $\mathbb{Z}_p[x]$ для всякого полинома φ справедливо тождество $\varphi(x^p) = \varphi^p(x)$ (оно вытекает из тождества $a^p = a$ в $\mathbb{Z}_p$ и из тождества $(\varphi + \psi)^p = \varphi^p + \psi^p$ в $\mathbb{Z}_p[x]$), поэтому $(\pi g)^p = (\pi f)(\pi h)$. Следовательно, полиномы $\pi(g)$ и $\pi(f)$ имеют общий множитель, поэтому полином $\pi(f)\pi(g)$ имеет кратный корень. Но полином $\pi(\Phi_n) = \pi(f)\pi(g)$ является делителем полинома $\pi(x^n - 1) = (x^n - 1) \in \mathbb{Z}_p[x]$, который не имеет кратных корней. Противоречие доказывает лемму Гаусса.

Доказательство теоремы Гаусса. Пусть $(\omega,\ f,\ p)$ такие, как в лемме Гаусса. Для тройки $(\omega_1,\ f,\ p_2)$, где $\omega_1 = \omega^{p_1}$, $p_1 = p$ и p_2 любое простое число, взаимно простое с n, применима лемма Гаусса. Действительно, $\omega_1 \in \Omega_n^*$ и $f(\omega_1) = 0$. Аналогично $f(\omega^{p_1 \cdot \ldots \cdot p_m}) = 0$ для любой последовательности простых чисел $p_1, \ldots, p_m$, взаимно простых с n. Каждый элемент $\alpha \in \Omega_n^*$ представим в виде $\alpha = \omega^m$, где m — произведение простых чисел, взаимно простых с n. Унимодальный полином Φ_n имеет те же корни, что и унимодальный полином f. Поэтому $\Phi_n = f$ и полином Φ_n неприводим.

Следствие 17. *Группа Галуа G поля E_n разложения полинома $x^n - 1$ над полем $\mathbb{Q}$ изоморфна мультипликативной группе $U(n)$ кольца $\mathbb{Z}/n\mathbb{Z}$.*

Доказательство. Легко видеть, что группа G является подгруппой группы $U(n)$. Корни неприводимого полинома Φ_n лежат в поле разложения полинома $x^n - 1 = 0$, поэтому $\#G \geqslant \deg \Phi_n$. Но $\deg \Phi_n = \#U(n)$. Поэтому группа G совпадает с группой $U(n)$.

Замечание. Пусть $\mathbb{Q} \subset E$ расширение Галуа и пусть $E \subset E_n$. Тогда группа Галуа G расширения $\mathbb{Q} \subset E$ коммутативна, так как G — факторгруппа группы $U(n)$. Согласно знаменитой теореме Кронекера – Вебера, верно и обратное утверждение: *если группа Галуа расширения $\mathbb{Q} \subset E$ коммутативна, то E содержится в поле E_n при некотором n.*

1.5. Разрешимость уравнения $x^n - 1 = 0$

Здесь описываются числа n, для которых 2-радикально расширение $\mathbb{Q} \subset E_n$.

Утверждение 18. *Пусть $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ — разложение n на простые множители. Тогда $U(n) = U(p_1)^{k_1} \times \cdots \times U(p_m)^{k_m}$ и $\#U(n) = \prod(p_i^k - p^{k_i - 1})$.*

Доказательство. Вытекает из китайской теоремы об остатках и из того, что в кольце $\mathbb{Z}/p^k\mathbb{Z}$ есть ровно p^{k-1} необратимых элементов.

Простое число p называется *простым числом Ферма*, если $p = 2^n + 1$. Для нечетного m число $2^{km} + 1$ делится на $2^k + 1$ и является составным. Поэтому простые числа Ферма представимы в виде $p = 2^{2^q} + 1$. Числа 3, 5, 17, 257, 65537 доставляют примеры простых чисел Ферма. Неизвестно, является ли множество простых чисел Ферма бесконечным. Целое число n будем называть *числом Гаусса*, если $n = 2^k p_1 \cdot \ldots \cdot p_m$, где $k \geqslant 0$, а $p_1, \ldots, p_m$ — различные простые числа Ферма.

Теорема 19 (Гаусс). *Расширение $\mathbb{Q} \subset E_n$ 2-радикально, если и только если n — число Гаусса.*

Доказательство. Действительно, $\deg \Phi(n) = \#U(n)$. Из утверждения 18 видно, что $\#U(n) = 2^k$, если и только если число n — число Гаусса.

Пример. Решим уравнение $\Phi_5(x) = 0$. Имеем

$$\Phi_5(x) = (x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1 = 0.$$

Далее,

$$x^{-2}\Phi_5(x) = x^2 + x + 1 + x^{-1} + x^{-2} = u^2 + u - 1,$$

где $u = x + x^{-1}$. Чтобы найти x, достаточно сначала решить квадратное уравнение $u^2 + u - 1 = 0$ и затем решить квадратное уравнение $xu = x^2 + 1$.

Явное решение уравнения $\Phi_{17}(x) = 0$ было найдено Гауссом. Оно послужило отправной точкой и для других его замечательных открытий. И сейчас, владея теорией Галуа, самостоятельно решить это уравнение далеко не просто. Моим студентам Ю. Бурда и Л. Кадец это удалось (см. [1]).

§2. Что можно построить циркулем и линейкой?

Этот параграф посвящен вопросам разрешимости и неразрешимости задач на построение. Несколько слов о расположении материала.

В пп. 2.1–2.2 описан класс точек, прямых и окружностей, которые могут быть построены при помощи операций из первого класса построений по начальным данным, являющимся конечным множеством точек: в п. 2.1 даны необходимые условия принадлежности этому классу, в п. 2.2 достаточные. В п. 2.3 мы обсуждаем несколько классических задач на построение (включая задачу о построении правильного n-угольника), которые укладываются в картину, разобранную в пп. 2.1–2.2.

В п. 2.4 выделены два построения, использующие выбор произвольных точек, которые позже рассматриваются как две новые операции. В п. 2.6 описано, что можно построить по любым (кроме нескольких исключительных типов) начальным данным с использованием операции выбора произвольных точек. Оказывается, что все, что можно построить с ее использованием, можно построить и без нее, пользуясь двумя новыми операциями и построениями из пп. 2.1–2.2.

В п. 2.7 мы описываем, что можно построить по множеству начальных данных одного исключительного типа, связанного с задачей о трисекции угла, и подробно обсуждаем вопрос о разрешимости этой задачи.

В п. 2.8 доказана одна теорема из вещественной аффинной геометрии, связанная с выполнимостью арифметических операций над вещественными числами при помощи геометрических построений.

2.1. Неразрешимость некоторых задач на построение

Прежде чем доказывать невозможность того или иного построения, нужно точно определить, что это такое. Пусть M — множество всех точек, прямых и окружностей на плоскости (только такие объекты можно строить циркулем и линейкой). Можно задать некоторый *допустимый класс* $\mathcal{M} \subset M$ и сказать, что точка, прямая или окружность могут быть построены, если они принадлежат этому классу. Класс $\mathcal{M}$ можно определить, задав начальные данные и допустимые операции.

Список допустимых операций (начало списка)

1. *Операция построения прямой* сопоставляет паре различных точек проходящую через них прямую.

2. *Операция построения окружности* сопоставляет точкам P, Q, O, где $P \neq Q$, окружность с центром O и радиусом, равным $[P, Q]$.

3. *Операция пересечения* сопоставляет паре несовпадающих пересекающихся кривых Γ_1, Γ_2, где Γ_i — либо прямая, либо окружность,

их точки пересечения (пересечение может содержать одну или две точки).

Определение. Класс $\mathcal{M}(\mathcal{D}) \subset M$ точек, прямых и окружностей, которые *строятся по начальным данным* $\mathcal{D} \subset M$, — это минимальный класс, содержащий $\mathcal{D}$ и замкнутый относительно допустимых операций 1)–3).

Замкнутость класса $\mathcal{M}(\mathcal{D})$ относительно пересечения означает, что если $\Gamma_1, \Gamma_2 \in \mathcal{M}(\mathcal{D})$, кривые Γ_1, Γ_2 не совпадают и $P \in \Gamma_1 \cap \Gamma_2$, то $P \in \mathcal{M}(\mathcal{D})$. Аналогично определяется замкнутость относительно других операций.

Теоремы о невозможности тех или иных построений основаны на формулируемой ниже простой алгебраической теореме 20.

Определение. *Класс* $\mathcal{M}_T$ — это класс всех точек, прямых и окружностей на координатной плоскости, определенных *над некоторым вещественным полем* T (точка определена над T, если обе ее координаты лежат в T, прямая или окружность определены над T, если их можно задать уравнениями $ax + by + c = 0$ или $(x-a)^2 + (y-b)^2 + c = 0$, где $a, b, c \in T$).

Если *вещественное поле* $T \subset \mathbb{R}$ *замкнуто относительно извлечения квадратных корней*, т. е. если $a \in \mathbb{R}$ и $a^2 \in T$, то $a \in T$, то класс $\mathcal{M}_T$ вместе с каждой окружностью содержит ее центр и расстояние между точками $P, Q \in \mathcal{M}_T$ лежит в поле T.

Теорема 20. *Если вещественное поле* $T \subset \mathbb{R}$ *замкнуто относительно извлечения квадратных корней, то класс* $\mathcal{M}_T$ *замкнут относительно допустимых операций* 1)–3).

Доказательство. В координатах плоскости $\mathbb{R}^2$ операции 1)–3) сводятся к нахождению вещественных решений линейных и квадратных уравнений. Решение таких уравнений не выводит из поля T, так как оно замкнуто относительно извлечения вещественных квадратных корней.

Пусть $\mathcal{D}_0$ — некоторое множество точек на плоскости, содержащее не менее двух точек. Евклидовы движения и гомотетии переводят прямую в прямую, окружность с отмеченным центром в окружность с отмеченным центром. Такие движения согласованы с задачами построения.

Определение. *Полем, соответствующим* $\mathcal{D}_0$, назовем наименьшее вещественное поле $T(\mathcal{D}_0)$, замкнутое относительно извлечения квадратных корней и содержащее отношения длин отрезков, концы которых лежат в $\mathcal{D}_0$.

Выберем две разные точки $O, E \in \mathcal{D}_0$ и нормируем расстояние так, чтобы длина отрезка $[O, E]$ равнялась единице. Скажем, что ортонормированная система координат *согласована с* $\mathcal{D}_0$, если $O = (0, 0)$ и $E = (0, 1)$.

Теорема 21. *В согласованной с $\mathcal{D}_0$ системе координат справедливо включение $\mathcal{M}(\mathcal{D}_0) \subset \mathcal{M}_T$, где $T = T(\mathcal{D}_0)$.*

Другими словами, если точка, прямая или окружность не определены над полем T, то их нельзя построить при помощи операций 1)–3) по точкам из множества $\mathcal{D}_0$.

Доказательство. В условиях теоремы координаты точек множества $\mathcal{D}_0$ лежат в поле $T(\mathcal{D}_0)$. Теперь теорема вытекает из теоремы 20.

2.2. Несколько явных построений

Для выполнения тех или иных построений в качестве «строительных кирпичиков» нужны решения нескольких школьных задач на построения. Напомним их.

1) *По точкам A, B построить точку, лежащую вне прямой AB, и середину P отрезка $[A, B]$.* Пусть Q, R — точки пересечения окружностей с центрами A и B и радиусами, равными $[A, B]$. Каждая из точек Q, R лежит вне AB, и P — точка пересечения AB и QR.

2) *Восстановить перпендикуляр к прямой l из точки $P \in L$.* В нашей ситуации требуется по точкам $A, P \in l$ построить точки Q, R, такие, что прямые AP и QR перпендикулярны и $P \in AQ$. Пусть $B \neq A$ — точка пересечения прямой AP с окружностью с центром P и с радиусом, равным $[P, A]$. В качестве искомых точек можно взять точки Q, R из предыдущего построения.

3) *На прямую l опустить перпендикуляр из точки $P \notin l$.* В нашей ситуации требуется по трем точкам A, B, P, не лежащим на одной прямой, построить точку Q, такую, что прямые AB и PQ перпендикулярны. В качестве Q можно взять точку пересечения $Q \neq P$ окружностей с центрами A и B, проходящими через P.

4) *построить прямую l_1, параллельную прямой l и проходящую через точку $P \notin l$.* Достаточно из точки P опустить перпендикуляр l_2 к прямой l и затем восстановить перпендикуляр l_1 к прямой l_2.

Пусть $O \neq E$ — две точки. Рассмотрим систему координат на плоскости, согласованную с множеством $\mathcal{D}_0 = \{O, E\}$. Первая координата на плоскости задает координату на прямой $l_0 = OE$. Отождествим точку на l_0 с числом, равным ее координате. При этом O и E отождествятся с 0 и 1.

Лемма 22. *Пусть $a, b \in l_0 \cap \mathcal{M}(\mathcal{D}_0)$. Тогда*: 1) *$-a$, a^{-1}, $a + b$, $ab \in l_0 \cap \mathcal{M}(M_0)$;* 2) *если $ab > 0$, то $(ab)^{1/2} \in l_0 \cap \mathcal{M}(\mathcal{D}_0)$.*

Ограничимся картинками, поясняющими доказательство, см. рис. 1.

Замечание. При построении прямой, параллельной данной и проходящей через данную точку, мы пользовались циркулем и линейкой. Это построение можно рассматривать как единую операцию. Такой операции

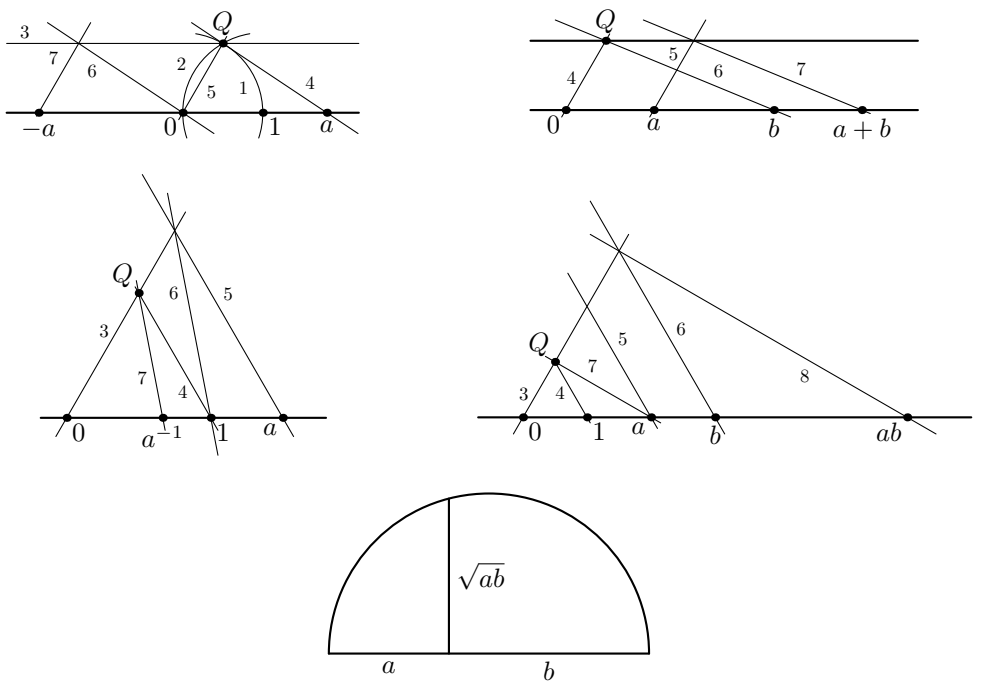

Рис. 1. Линии занумерованы в порядке построения

достаточно, чтобы, имея точки 0 и 1, построить точки $-a$, a^{-1}, $a+b$, ab по точкам a, b на числовой прямой (смотри рис. 1, точка Q в этом случае выбирается произвольно). Этот факт имеет красивое применение в аффинной геометрии (см. п. 2.8).

Теорема 23. *В условиях теоремы* 21 *справедливо равенство* $\mathcal{M}(\mathcal{D}_0) = \mathcal{M}_T$.

Доказательство. Достаточно показать, что $\mathcal{M}(\mathcal{D}_0) \supset \mathcal{M}_T$, т. е. что можно построить любой элемент из $\mathcal{M}_T$. Если P, $Q \in \mathcal{D}_0$, то класс $\mathcal{M}(\mathcal{D}_0)$ содержит точку $\rho \in l_0$, где ρ — отношение длин отрезков $[P,Q]$ и $[O,E]$: это одна из точек пересечения прямой l_0 с окружностью с центром O и радиусом, равным $[P,Q]$. Согласно лемме 22, каждая точка $(a,0)$, где $a \in T$, лежит в $\mathcal{M}(\mathcal{D}_0)$. Точка $(0,b)$, где $b \in T$, тоже лежит в $\mathcal{M}(\mathcal{D}_0)$: ее можно построить, пересекая ось y с окружностью с центром O, проходящую через точку $(b,0)$. Строя прямые, перпендикулярные к осям, убеждаемся, что при $a, b \in T$ точка (a,b) лежит в $\mathcal{M}(\mathcal{D}_0)$. Прямая l, определенная над T, содержит пару точек, определенных над T, поэтому $l \in \mathcal{M}(D_0)$. Окружность S, определенная над T, содержит точку, определенную над T. Ее центр тоже определен над T, поэтому $S \in \mathcal{M}(D_0)$.

2.3. Классические задачи на построение

В нескольких классических задачах на построение начальным данным является отрезок, или, что то же самое, пара его концов O, E. В этом пункте символом T мы будем обозначать *поле конструируемых чисел*, соответствующее множеству $\mathcal{D}_0 = \{O, E\}$. По теореме 23 в системе координат, согласованной с $\mathcal{D}_0$, справедливо равенство $\mathcal{M}(\mathcal{D}_0) = \mathcal{M}_T$.

Квадратура круга. *По точкам O, E построить отрезок I такой, что площадь круга радиуса $[OE]$ равна площади квадрата со стороной I.*

Теорема 24. *Для любых точек $P, Q \in \mathcal{M}_T$ отрезок $[PQ]$ не равен отрезку I. Другими словами, в классе $\mathcal{M}_T$ квадратура круга не осуществима.*

Доказательство. Расстояние между точками $P, Q \in \mathcal{M}_T$ — конструируемое число, а длина отрезка I — трансцендентное число $\pi^{1/2}$.

Удвоение куба. *По точкам O, E построить отрезок J такой, что объем куба со стороной J в два раза больше объема куба со стороной I.*

Теорема 25. *Для любых точек $P, Q \in \mathcal{M}_T$ отрезок $[PQ]$ не равен отрезку J. Другими словами, в классе $\mathcal{M}_T$ удвоение куба не осуществимо.*

Доказательство. Расстояние между точками $P, Q \in \mathcal{M}_T$ — конструируемое число, а длина отрезка J равна $2^{1/3}$. Уравнение $x^3 - 2 = 0$ неприводимо над $\mathbb{Q}$ и не решается при помощи квадратных корней.

Задача о правильном n-угольнике. *Построить правильный n-угольник с данной стороной $[OE]$.*

Теорема 26 (Гаусс). *Правильный n-угольник можно построить* (т. е. его вершины лежат в классе $\mathcal{M}_T$), *если и только если n — число Гаусса.*

Доказательство. Несложно видеть, что задача эквивалентна следующей: построить вершины правильного n-угольника с центром O, одна из вершин которого — точка E. При отождествлении плоскости с комплексной прямой вершины этого n-угольника — корни уравнения $z^n = 1$. Это уравнение решается при помощи квадратных корней (в поле комплексных чисел), если и только если n — число Гаусса. Осталось заметить, что комплексное число выражается над полем $\mathbb{Q}$ при помощи квадратных корней, если и только если его вещественная и мнимая части — конструируемые числа.

2.4. Два специальных построения

Выделим два простых построения, использующие выбор произвольной точки из континуального множества. Эти построения невозможно

осуществить при помощи операций 1)–3), и их можно рассматривать как новые операции (что позже мы и будем делать).

Задача 1. *По прямой l и точке $P \notin l$ найти точку $E \in l$, такую, что прямые l и EP перпендикулярны.*

Класс $\mathcal{M}(\mathcal{D})$, где множество начальных данных $\mathcal{D}$ состоит из прямой l и точки $P \notin l$, совпадает с множеством $\mathcal{D}$: применение допустимых операций не увеличивает множества $\mathcal{D}$. Однако если на прямой l *произвольным образом* выбрать две различные точки A, B, то такое построение легко выполнить (см. п. 2.2). Его результатом являются перпендикуляр l_P и точка $E = l \cap l_P$, которые *не зависят от сделанного произвольного выбора*.

По точкам $O = P$ и E можно построить все объекты класса $\mathcal{M}_T$. Результат каждого из этих построений не зависит от выбранных произвольно точек A, $B \in l$, $A \neq B$, которые использовались в построении.

Задача 2. *Построить центр данной окружности S.*

Класс $\mathcal{M}(\mathcal{D})$, где $\mathcal{D} = \{S\}$, совпадает с множеством $\mathcal{D}$. Однако если выбрать две разные точки A, $B \in S$, то перпендикуляр к прямой AB, делящий отрезок $[A, B]$ пополам, проходит через центр окружности. Находя середину построенного диаметра, получим центр окружности O.

Чтобы включить такие конструкции в нашу схему, нужно допустить выбор *произвольных точек*, лежащих в одном из множеств (стратов), на которые разбивается плоскость уже построенными точками, прямыми и окружностями. Но при этом считать построенными лишь объекты, которые не зависят от сделанных произвольных выборов. Ниже мы покажем, что такая расширенная интерпретация процесса построения циркулем и линейкой не меняет уже полученных результатов и позволяет рассматривать и другие задачи, в частности, задачу о трисекции угла.

Начнем с рассмотрения стратификации плоскости, связанной с конечным подмножеством множества M всех точек, прямых и окружностей.

2.5. Стратификация плоскости

Пусть $V \subset M$ — конечное подмножество. С V связана *стратификация* Σ_V плоскости, т. е. ее разбиение на *страты* $S_\alpha \in \Sigma_V$ разных размерностей. (Если точки, прямые и окружности из V нарисованы, то стратификация Σ_V видна на картинке.)

Нульмерный страт в Σ_V — любая точка множества V_0 всех точек пересечения различных прямых и окружностей из V и любое из одноточечных множеств, содержащихся в V.

Одномерный страт в Σ_V — любая компонента связности множества $\Gamma_i \setminus (\Gamma_i \cap V_0)$, где Γ_i — любая прямая или окружность из V.

Двумерный страт в Σ_V — любая компонента связности дополнения плоскости к объединению всех точек, прямых и окружностей из V.

Пусть T — вещественное поле, замкнутое относительно извлечения квадратных корней. Из теоремы 20 вытекает следующее следствие.

Следствие 27. *Если $V \subset \mathcal{M}_T$ и P — нульмерный страт в Σ_V, то $P \subset \mathcal{M}_T$.*

Утверждение 28. *Точки, определенные над T, плотны на*: 1) *плоскости*; 2) *прямой, определенной над T*; 3) *окружности, определенной над T.*

Доказательство. Пункты 1) и 2) очевидны. Прямые вида $y = c$, где $c \in T$, плотны в $\mathbb{R}^2$. Они пересекают окружность, определенную над T, в точках, определенных над T. Множество таких точек всюду плотно на окружности.

Следствие 29. *Если $V \subset \mathcal{M}_T$, то точки, определенные над T, плотны в каждом страте положительной размерности стратификации Σ_V.*

2.6. Классы построений, допускающие произвольный выбор

Результат применения операции пересечения зависит от выбора одной из точек пересечения двух кривых. Определим операцию 4), зависящую не только от дискретного, но и от континуального выбора. При ее помощи можно выполнить два простых построения (см. п. 2.4), которые можно принять за новые операции 5) и 6).

Продолжение списка допустимых операций

4. *Операция выбора точки* применима к конечному множеству $V \subset M$ и заключается в выборе страта $S_\alpha \in \Sigma_V$ положительной размерности и точки P из этого страта.

5. *Операция построения основания перпендикуляра* сопоставляет прямой l и точке $P \notin l$ точку $E \in l$ такую, что прямые EP и l перпендикулярны.

6. *Операция восстановления центра* сопоставляет окружности ее центр.

Определим класс $\mathcal{M}_G(\mathcal{D})$ элементов, которые можно *в обобщенном смысле построить* по конечному множеству $\mathcal{D}$. Скажем, что $v \in \mathcal{M}_G(\mathcal{D})$, если существует конечный алгоритм (т. е. правило, описывающее все дискретные выборы), k-й шаг которого — переход от одного конечного множества $V_k \subset M$ к следующему $V_{k+1} \subset M$. При этом: 1) $V_1 = \mathcal{D}$; 2) $V_{k+1} = V_k \cup \{a\}$, где a или получается применением к некоторым элементам множества V_k одной из операций 1)–3) (см. п. 2.1), или $a = P$ и точка P

получена при помощи операции выбора из множества V_k; 3) элемент v содержится в некотором из множеств V_N вне зависимости от континуальных выборов, которые встречались на предыдущих шагах.

Теорема 30. *Пусть T — вещественное поле, замкнутое относительно извлечения квадратных корней и $\mathcal{D} \subset \mathcal{M}_T$ — конечное множество. Тогда $\mathcal{M}_G(\mathcal{D}) \subset \mathcal{M}_T$.*

Доказательство. Если $v \in \mathcal{M}_G(\mathcal{D})$, то континуальным выбором, встречающимся в процессе построения v, можно распорядиться по своему усмотрению. По условию $V_1 = \mathcal{D} \subset \mathcal{M}_T$ и $V_2 = V_1 \bigcup \{a\}$. Если первый шаг состоит в присоединении точки a из страта положительной размерности в стратификации Σ_{V_1}, то выберем точку a, определенную над T. По следствию 29 это можно сделать. При таком выборе $V_2 \subset \mathcal{M}_T$. Если точка, прямая или окружность a получаются применением к некоторым элементам множества V_1 одной из операций 1)–3), то $V_2 \subset \mathcal{M}_T$ по теореме 20. Будем последовательно на каждом шаге построения, состоящем в присоединении произвольно выбранной точки, выбирать точку, определенную над T. При применении это правила выбора $V_k \subset \mathcal{M}_T$ для любого $k > 0$.

Следствие 31. *Если $\mathcal{D}_0$ — конечное множество точек, содержащее не менее двух точек, то $\mathcal{M}_G(\mathcal{D}_0) = \mathcal{M}(\mathcal{D}_0)$. В частности, операция* 4) *не помогает решить задачи о квадратуре круга и об удвоения куба. С ее помощью можно построить только те правильные n-угольники, которые строятся и без нее.*

Определение. Минимальный класс $\mathcal{M}_r(\mathcal{D})$, содержащий $\mathcal{D}$ и замкнутый относительно операций 1)–3) и 5), 6), будем называть классом объектов, которые *в расширенном смысле строятся по начальным данным $\mathcal{D}$.*

Скажем, что D — *исключительное множество типа R_i*, если D содержит:

для типа R_1 — *единственную точку*;
для типа R_2 — *единственную прямую*;
для типа R_3 — $k > 1$ *параллельных прямых*;
для типа R_4 — $k > 0$ *прямых, проходящих через точку O*;
для типа R_5 — $k > 0$ *прямых, проходящих через точку O, и точку O*;
для типа R_6 — $k > 0$ *окружностей с общим центром O*;
для типа R_7 — $k > 0$ *окружностей с общим центром O и точку O.*

Утверждение 32. *Для конечного неисключительного множества $\mathcal{D}$ существует конечное множество $\mathcal{D}_0 \subset \mathcal{M}_r(\mathcal{D})$, содержащее только точки плоскости, и такое, что $\mathcal{D} \subset \mathcal{M}(\mathcal{D}_0)$* (более того, для данного $\mathcal{D}$ множества $\mathcal{D}_0$ можно предъявить явно).

Например, для $\mathcal{D} = \{S, l\}$, где S — окружность с центром O, l — прямая и $O \notin l$, достаточно положить $\mathcal{D}_0 = \{O, E, P\}$, где $E \in l$ — основание перпендикуляра, опущенного из O на l, и $P \in S \cap l$. Для других неисключительных множеств D множество $\mathcal{D}_0$ предъявляется столь же явно.

Следствие 33. *Для конечного неисключительного множества начальных данных $\mathcal{D} \subset M$ справедливы равенства $\mathcal{M}_G(\mathcal{D}) = \mathcal{M}_r(\mathcal{D}) = \mathcal{M}(\mathcal{D}_0) = \mathcal{M}_T$, где T — поле, согласованное с $\mathcal{D}_0$.*

Доказательство. Согласно утверждению, $\mathcal{D} \subset \mathcal{M}(\mathcal{D}_0)$. Но $\mathcal{M}(\mathcal{D}_0) = \mathcal{M}_T$ (см. теорему 23) и $\mathcal{M}_G(\mathcal{D}) \subset \mathcal{M}_T$ (см. теорему 30). Справедливы включения $\mathcal{M}_G(\mathcal{D}) \supset \mathcal{M}_r(\mathcal{D}) \supset \mathcal{M}(\mathcal{D}_0)$. Следствие доказано.

Мы описали класс $\mathcal{M}_G(\mathcal{D})$ для неисключительных $\mathcal{D}$ и показали, что для построения его объектов операция 4) не требуется: $\mathcal{M}_G(\mathcal{D}) = \mathcal{M}_r(\mathcal{D})$.

2.7. Трисекция угла

Следующая классическая задача связана с классом $\mathcal{M}_G(\mathcal{D})$ для исключительного множества $\mathcal{D}$ типа R_4.

Задача о трисекции угла. *Разделить данный угол на три равных части.*

Опишем класс $\mathcal{M}_G(\mathcal{D})$ для множества $\mathcal{D}$ типа R_4 (классы $\mathcal{M}_G(\mathcal{D})$ для исключительных множеств $\mathcal{D}$ других типов описываются также). Итак, пусть $\mathcal{D}$ — это $k > 0$ прямых, проходящих через точку O. Фиксируем любую окружность S с центром O. Будем пользоваться следующими обозначениями: $\mathcal{D}'$ — множество точек, равное $\bigcup_{l \in \mathcal{D}} (S \cap l)$; T — поле, согласованное с $\mathcal{D}'$; $l_0 \in \mathcal{D}$ — фиксированная прямая.

Теорема 34. *Класс $\mathcal{M}_G(\mathcal{D})$ состоит из точки O и из всех прямых l, проходящих через O и таких, что $|\cos(l, l_0)| \in T$* (здесь (l, l_0) — любой и из двух углов, образованных прямыми l и l_0).

Доказательство. Выберем любую точку $E \in l_0 \setminus O$, пользуясь операцией 4). Построим окружность S с центром O и радиусом, равным $[O, E]$. Вместе с S построим множество $\mathcal{D}'$. Класс $\mathcal{M}(\mathcal{D}') = \mathcal{M}_T$ содержит все прямые l, проходящие через O, такие, что $|\cos(l, l_0)| \in T$, и не содержит других прямых, проходящих через O. Класс $\mathcal{M}_G(\mathcal{D})$ принадлежит классу $\mathcal{M}(T)$ и тоже не содержит других прямых, проходящих через O.

Объекты множества $\mathcal{D}$ инвариантны относительно группы G_O гомотетий с центром O, поэтому все объекты класса $\mathcal{M}_G(\mathcal{D})$ тоже инвариантны относительно G_O. Действительно, при гомотетии построение переходит в гомотетичное построение, если произвольные точки выбирать гомотетичными точкам в исходном построении. Но объекты класса $\mathcal{M}_G(\mathcal{D})$ не

зависят от произвольных выборов, сделанных при их построении, т. е. они инвариантны относительно группы G_O. Только прямые, проходящие через O, и точка O инвариантны относительно этой группы.

Разрешимость задачи о трисекции угла существенно зависит от величины этого угла (см. следствия 35–38).

Следствие 35. *Если $\mathcal{D} = \{l_0, l_1\}$, где l_0, l_1 — прямые, проходящие через O, и $a = |\cos(l_0, l_1)|$, то класс $\mathcal{M}_G(\mathcal{D})$ состоит из O и из прямых l, таких, что $O \in l$ и $|\cos(l, l_0)| \in T$, где T — минимальное вещественное поле, содержащее a и замкнутое относительно извлечения квадратных корней.*

Следствие 36. *В условиях следствия* 35 *можно построить прямые, делящие угол (l_0, l_1) на n равных частей, если и только если уравнение $P_n(x) = a$, где P_n — полином Чебышёва степени n, разрешимо в 2-радикалах над T.*

Отметим, что *если a — трансцендентное число, то уравнение $P_n(x) = a$ неприводимо над полем $\mathbb{Q}(a)$*. Действительно, поле $\mathbb{Q}(a)$ изоморфно полю рациональных функций $\mathbb{Q}(t)$ над $\mathbb{Q}$, а уравнение $P_n(x) = t$ неприводимо даже над полем $\mathbb{C}(t)$ (риманова поверхность алгебраической функции $x(t)$, определенной этим уравнением, — сфера Римана).

Следствие 37. *Если в условиях следствия* 36 *число a трансцендентно, то угол можно поделить на n равных частей циркулем и линейкой, если и только если $n = 2^k$. В частности, трисекция такого угла невозможна.*

Действительно, если неприводимое уравнение решается в 2-радикалах, то его степень равна 2^k. С другой стороны, угол можно поделить на 2^k частей, последовательно строя биссектрисы.

Следствие 38. *Если в условиях следствия* 35 *число a рационально, то трисекция угла возможна, если и только если уравнение $4x^3 - 3x = a$ имеет рациональный корень.*

Следствие 38 доставляет явно проверяемый критерий разрешимости задачи о трисекции угла, косинус которого рационален. В частности, легко видеть, что трисекция угла в 60° невозможна.

2.8. Одна теорема из аффинной геометрии

Формулируемая ниже теорема показывает, что для построения вещественной аффинной геометрии на плоскости нужны лишь точки и прямые,

а понятие непрерывности не нужно. Ее доказательство основано на возможности выполнения арифметических операций с помощью параллельных прямых (см. п. 2.2).

Теорема 39. *Пусть* $F\colon \mathbb{R}^2 \to \mathbb{R}^2$ *— взаимно однозначное отображение, переводящее каждую прямую в прямую. Тогда* F *— аффинное преобразование.*

Лемма 40. *Если* $\varphi\colon \mathbb{R} \to \mathbb{R}$ *автоморфизм поля* $\mathbb{R}$, *то* $\varphi(x) = x$ *при* $x \in \mathbb{R}$.

Доказательство. Если $x \in \mathbb{Q}$, то очевидно $\varphi(x) = x$. Если $x \geqslant 0$, то $x = a^2$ и $\varphi(x) = \varphi^2(a) \geqslant 0$, т. е. φ монотонно. Значит, $\varphi(x) = x$ при $x \in \mathbb{R}$.

Лемма 41. *Если в условиях теоремы* $F(O) = O$ *и* $F(E) = E$, *где* $O \neq E$, *то ограничение* F *на прямую* OE *— тождественное отображение.*

Доказательство. Введем координату на прямой OE, отождествляя O с нулем, а E с единицей. Отображение F переводит непересекающиеся прямые в непересекающиеся прямые, т. е. оно сохраняет соотношение параллельности между прямыми. Используя параллельные прямые и точки $O = 0$ и $E = 1$, по точкам $a, b \in OE$ можно построить точки $-a, a^{-1}, a + b, ab$ (см. лемму 22). Поэтому ограничение F на OE задает автоморфизм числовой прямой. Осталось воспользоваться леммой 40.

Доказательство теоремы. Отображения, удовлетворяющие условию теоремы, образуют группу G, содержащую группу аффинных преобразований. Подгруппа G_0, фиксирующая точки A, B, C, не лежащие на одной и прямой, тривиальна. Действительно, если $\Psi \in G_0$, то по лемме 41 ограничение Ψ на продолжения сторон треугольника ABC является тождественным преобразованием (так как Ψ фиксирует вершины треугольника). Через каждую точку P можно провести прямую l_P, пересекающую стороны треугольника ABC в двух разных точках (которые Ψ фиксирует). Применяя лемму 41 к прямой l_P, получим $\Psi(P) = P$, т. е. группа G_0 тривиальна. Следовательно, группа G содержит не более одного преобразования, переводящего A, B, C в точки A', B', C', не лежащие на одной прямой. Но среди таких преобразований есть аффинное преобразование. Теорема доказана.

Список литературы

[1] Бурда Ю., Кадец Л. *Семнадцатиугольник и закон взаимности Гаусса* // Математическое просвещение. Сер. 3. Вып. 17. 2013. С. 61–67.

А. Г. Хованский, Univ. of Toronto