Циркуль, линейка и расширение полей

Скорее всего, в вашей жизни уже были некоторые построения циркулем и линейкой. Наверняка вы умеете проводить параллельные прямые, серединные перпендикуляры, биссектриссы и т.д.

Однако задумывались ли вы, над следующим вопросом: а что вообще **можно** построить циркулем и линейкой, а что **нельзя**? Этот вопрос вы и будете сегодня исследовать.

Напоминание. Построение циркулем и линейкой — это любая последовательность из действий ниже.

- Можно провести прямую через две заданные точки.
- Можно провести окружность с центром в данной точке, проходящую через другую заданную точку.
- Можно построить пересечение двух прямых, прямой и окружности или двух окружностей, построенных ранее.

1. Что можно построить?

Правильные n-угольники, однако, весьма конкретные фигуры.
Попытаемся, все-таки, описать, а что мы вообще умеем строить. Пусть дана координатная плоскость и на ней отмечена точка с координатами $(1, 0)$ и центр координат $(0, 0)$.

Определение. Назовем число $a \in \mathbb{R}$ *построимым*, если с помощью циркуля и линейки можно построить точку, у которой одна из координат a.

Цель. Попытаться описать все построимые числа.

1. Покажите, что все рациональные числа построимы.

2. Докажите, что если a и b построимы, то построимы и числа:
(а) $a + b$ и $a - b$;
(б) ab;
(в) a/b.

3. Докажите, что если a, b, c построимы, то построимы и числа:
(а) $\sqrt{ab}$;
(б) $b + c\sqrt{a}$;

4. Пусть K — некоторое множество построимых чисел. Докажите, что все числа, являющиеся корнями квадратных уравнений с коэффициентами из K тоже построимы.

2. Поля и кольца

Числа из секции 2 отнюдь не случайны: они описывают структуру, которая довольно часто встречается в математике. Пора и вам с ней познакомиться.

Определение. Пусть A множество с двумя операциями: сложение $(a + b)$ и умножения $(a \cdot b)$. Пусть в A заданы элементы 1 (единица) и 0 (ноль). Говорят, что A является *кольцом*, если выполнены следующие свойства:

- Сложение коммутативно: $a + b = b + a$;
- Сложение обратимо: для каждого элемента $a \in A$ существует элемент $b \in A$, такой что $a + b = 0$ (иными словами, есть «$-a$»).
- Умножение ассоциативно: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- $1 \cdot a = a \cdot 1 = a$ для любого элемента $a \in A$.
- $0 \cdot a = a \cdot 0 = 0, 0 + a = a + 0 = a$ для любого элемента $a \in A$.
- Операции сложения и умножения дистрибутивны:

$$a \cdot (b + c) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c$$

Определение. Говорят, что множество A является *полем*, если выполняются следующие свойства:

- A является кольцом;
- Умножение коммутативно: $a \cdot b = b \cdot a$;
- У каждого элемента $a \in A$, кроме нулевого, есть обратный элемент: $a \cdot b = b \cdot a = 1$ (иными словами, есть «$\frac{1}{a}$»).

Пересказ. Если говорить грубо, то кольца — это то, где можно складывать и умножать (как учили в школе), а поля — это то, где можно складывать, умножать и делить (но не на ноль).

Примеры колец. Например, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. А вот $\mathbb{N}$ кольцом не является — не выполняется второе свойство: нет отрицательных чисел. Пример кольца, которое при этом не является полем — многочлены с коэффициентами из любого кольца: $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$.

Примеры полей. Например, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Целые числа $\mathbb{Z}$ полем не являются — нет обратных элементов по умножению.

5. Покажите, что любое кольцо содержит в себе $\mathbb{Z}$, а любое поле — $\mathbb{Q}$.

6. Является ли полем множество
(а) $A = \{a + b\sqrt{2}, \text{где } a, b \in \mathbb{Q}\}$;
(б) $A = \{a + b\sqrt{2} + c\sqrt{3}, \text{где } a, b, c \in \mathbb{Q}\}$;
(в) $A = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \text{где } a, b, c \in \mathbb{Q}\}$

7. Докажите, что множество построимых чисел является полем.

8. Пусть мы умеем строить числа из некоторого поля K. Докажите, что,
(а) используя одну линейку, мы не выйдем за пределы поля K.
(б) проведя только одну окружность, мы получим только числа вида $a + b\sqrt{c}$, где $a, b, c \in K$.

3. Расширения

Вот если бы у нас была только линейка — тогда бы мы оставались в том поле, что и были. Однако окружности добавляют нам некие квадратные корни, или, иными словами, корни квадратных уравнений с коэффициентами из поля. Однако эта структура тоже довольно классическая.

Определение. Даны поля K и L, причем $K \subset L$. Тогда L называется *расширением поля* K.

Определение. Будем обозначать как $K(\alpha)$ минимальное поле (по включению) поле, содержащее элемент α и поле K).

Определение. Если α является корнем квадратного трехчлена с коэффициентами из K, расширение $K(\alpha)$ называется *квадратичным расширением*.

9. Покажите, что если $K(\alpha)$ — квадратичное расширение поля K, то его элементы — это дроби вида $\dfrac{a + b \cdot \alpha}{c + d \cdot \alpha}$, где $a, b, c, d \in K$.

10. **Теорема**. Докажите, что если число b можно построить циркулем и линейкой, то найдется такая цепочка (башня) квадратичных расширений:
$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset ... \subset F_n$ такая, что $b \in F_n$.

Определение. Множество элементов $a_1, ... a_n$ называется *линейно зависимым* над кольцом K, если существуют числа $\lambda_1, ... \lambda_n$ из кольца K, причем не все они равны нулю, такие, что $\lambda_1 a_1 + ... + \lambda_n a_n = 0$.

Определение. Множество, не являющееся линейно зависимым, называется *линейно независимым.* Максимальное подмножество элементов, являющееся линейно независимым множеством, называется базисом исходного множества.

11. Докажите, что если $a_1, ... a_n$ — базис множества K, то любой элемент $b \in K$ представляется в виде $b = \lambda_1 a_1 + ... + \lambda_n a_n$.

Определение Даны поле K и его расширение L. Рассмотрим базис L над кольцом K (то есть коэффициенты λ берутся из K). Количество элементов базиса называется *степенью расширения* и обозначается как $[L : K]$ (возможно, равное ∞).

12. **(а)** Дана цепочка расширений $K \subset L \subset M$. Причем $[L : K], [M : L] < \infty$. Покажите, что $[M : L][L : K] = [M : K]$.
(б) Покажите, что в условиях **Теоремы** из пункта 10 $[F_n : \mathbb{Q}] = 2^n$.

13. **Теорема.** Корень не разложимого многочлена нечетной степени не может быть построен с помощью циркуля и линейки.

4. Финишная прямая

Теперь осталось пожинать плоды теоремы и решить легендарные задачи Древней Греции. Уже тогда геометры предполагали, что построить эти конструкции невозможно, однако доказано это было только в конце *XIX* века.

14. **Удвоение куба.** Докажите, что нельзя построить по ребру куба ребро куба вдвое большего объема.

15. **Трисекция угла.** Докажите, что нельзя разделить произвольный угол на 3 равные части (например, угол в 30°!).

16. **Квадратура круга.** Докажите, что нельзя построить квадрат той же площади, что и данный круг.

17.* Докажите, что правильный семиугольник нельзя построить с помощтю циркуля и линейки.