Алгебра 4
02.10.97

# Расширения полей

## Часть 1. Построения многоугольников циркулем и линейкой.

Перед началом построений на плоскости отмечены только точки с координатами $(0, 0)$ и $(1, 0)$. Рассмотрим некоторую конечную последовательность построений и рассмотрим поле, натянутое на координаты всех построенных точек.

Назовем поле $K$ *поликвадратичным*, если существует последовательность вложенных расширений $\mathbb{Q} \subset K_1 \subset \ldots \subset K_n \subset K$, каждое из которых квадратично.

**Теорема.** Поля, получающиеся посредством построений циркулем и линейкой, поликвадратичны.

Доказательство — индукция по числу построений. После каждого построения к полю добавляются координаты всех новых точек пересечения. Возможны два случая:

1. Добавляется точка пересечения двух прямых. Ее координаты получаются решением системы линейных уравнений, поле не меняется.
2. Добавляются точки пересечения двух окружностей или точки пересечения прямой и окружности. Ее координаты получаются решением квадратного уравнения, поэтому поле либо не меняется, либо получается присоединением корней квадратного уравнения.

Поэтому поле, полученное после очередного построения, поликвадратично над предыдущим. Доказательство окончено.

**Утверждение.** Если $K \subset M \subset L$, то $[L : K] = [L : M] \cdot [M : K]$.

Если $f_1, \ldots, f_n$ — базис $L$ над $M$, $g_1, \ldots, g_k$ — базис $M$ над $K$, то $\{ f_i g_j \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant k \}$ — базис $L$ над $K$.

**Следствие.** Не существует поликвадратичного поля, содержащего подполе, изоморфное $\mathbb{Q}(\sqrt[18]{1})$.

Если бы такое поле существовало, то его размерность над $\mathbb{Q}$ делилась бы на $[\mathbb{Q}(\sqrt[18]{1}) : \mathbb{Q}] = 6$, чего не может быть.

Поэтому правильный восемнадцатиугольник нельзя построить циркулем и линейкой. По такой же причине нельзя осуществить трисекцию угла или удвоение куба — придется строить корни кубического уравнения.

## Часть 2. Нормальные расширения

Расширение $K$ поля $L$ называется *нормальным*, если любой многочлен, неприводимый над $L$ и имеющий корень в $K$, разлагается в $K$ на линейные множители.

**Лемма.** Любые два минимальных поля разложения многочлена $f(x) \in L[x]$ изоморфны.

Доказательство леммы. Обозначим эти поля через $K_1, K_2$. Пусть $f(x) = f_1(x) \cdot \ldots \cdot f_k(x)$ — разложение на неприводимые множители в $L[x]$. Пусть $\alpha_1$ (соотв. $\beta_1$) — некоторый корень $f_1(x)$ в $K_1$ (соотв. $K_2$). Можно построить изоморфизм $L(\alpha_1) \xrightarrow{\sim} L(\beta_1)$, переводящий $\alpha_1$ в $\beta_1$, так как оба этих поля изоморфны $L[x]/(f_1(x))$. Пользуясь этим изоморфизмом, отождествим $L(\alpha_1)$ и $L(\beta_1)$ и обозначим это поле $L^{(1)}$. Разложим $f(x)$ на неприводимые множители над $L^{(1)}$ и обозначим через $f^{(1)} \in L^{(1)}[x]$ произведение нелинейных сомножителей. Тогда $K_1, K_2 \supset L^{(1)}$ — минимальные поля разложения $f^{(1)}(x)$. Однако $\deg f^{(1)}(x) < \deg f(x)$, и доказательство завершается индукцией по степени.

**Теорема.** Если $K : L$ — минимальное поле разложения $f(x) \in L[x]$, то $K$ нормально.

Доказательство теоремы. Пусть $g(x) \in L[x]$ и $\beta_1$ — корень $g(x)$ в $K$. Пусть $M$ — поле разложения $fg$. Предположим, теорема неверна и $M \neq K$, тогда пусть $\beta_2$ — корень $g(x)$, не принадлежащий $K$.

Пусть $\alpha_1$, $\alpha_2$, $\ldots$, $\alpha_n$ — корни многочлена $f(x)$.

Поля $L(\beta_1)$ и $L(\beta_2)$ изоморфны, так как они получаются присоединением корня $g(x)$. По лемме этот изоморфизм можно продолжить на поля $L(\beta_1, \alpha_1, \ldots, \alpha_n)$ и $L(\beta_2, \alpha_1, \ldots, \alpha_n)$ — минимальные поля разложения $f(x) \in L(\beta_1)[x] \simeq L(\beta_2)[x]$. Но первое поле есть $K$, а второе по предположению является строгим надмножеством $K$. Противоречие.

## Часть 3. Сепарабельные расширения.

Элемент $\varkappa$ расширения $K : L$ называется *сепарабельным*, если его минимальный многочлен $f(x) \in L[x]$ не имеет кратных корней, то есть $f'(x) \neq 0$.

Расширение называется сепарабельным, если все его элементы сепарабельны.

Пример несепарабельного элемента: $\sqrt[p]{t}$ в расширении поля $\mathbb{F}_p(t)$.

Если поле конечно или имеет характеристику 0, то любое его конечное расширение сепарабельно.

**Теорема о примитивном элементе.** Пусть $K : L$ — конечное сепарабельное расширение. Тогда существует $\theta \in K$, такое что $K = L(\theta)$.

Доказательство. Пусть $K = L(\alpha_1, \ldots, \alpha_n)$. Очевидно, индукцией по $n$, достаточно доказать эту теорему для $n = 2$, когда $K = L(\alpha, \beta)$.

Возможны два случая:

1) $L$ конечно, тогда теорема верна, так как всякое конечное поле получается присоединением примитивного корня из единицы.

2) $L$ бесконечно.

Пусть $\alpha = \alpha_1$ — корень многочлена $f(x)$, а $\alpha_2, \dots, \alpha_n$ — остальные его корни; $\beta = \beta_1$ — корень $g(x)$ и $\beta_2, \dots, \beta_k$ — остальные корни. Так как расширение сепарабельно, то кратных корней нет.

Будем искать $\theta$ в виде $\alpha + c\beta$, где $c$ — элемент $L$, а именно, выберем $c$ так, что $\alpha_i + c\beta_j \neq \alpha + c\beta$, если $i \neq 1 \neq j$. Поскольку $L$ бесконечно, это всегда можно сделать. Тогда

$$g(\beta) = 0$$
$$f(\theta - c\beta) = 0$$

Многочлены $g(x), f(\theta - cx) \in L(\theta)[x]$ имеют общий корень $\beta$, а других общих корней нет, так как $\alpha_i + c\beta_j \neq \alpha + c\beta$. Поэтому НОД$(g(x), f(\theta - cx)) = x - \beta$. Поскольку коэффициенты обоих многочленов принадлежат $L(\theta)$, то $\beta \in L(\theta)$. Отсюда и $\alpha \in L(\theta)$, и теорема доказана.

Конечное сепарабельное нормальное расширение называется *расширением Галуа*.

Пусть $K : L$ — расширение Галуа степени $n$. Тогда $K \cong L(\theta) = L[x]/(P(x))$. Есть ровно $n$ автоморфизмов $K$ над $L$, а именно, каждый автоморфизм свободно и однозначно определяется значением $\sigma(\theta) = \theta'$, где $\theta'$ — один из корней $P(x)$. Таким образом,

$$\#Gal[K : L] = n.$$