КОРЕНЬ КУБИЧЕСКИЙ ИЗ ДВУХ

МНОГОЧЛЕН $x^3 - 2$ — НЕРАЗЛОЖИМЫЙ В $\mathbb{Q}[x]$

ЛЕММА 1

Многочлен $x^3 - 2$ является неразложимым в $\mathbb{Q}[x]$ (простым).

ДОКАЗАТЕЛЬСТВО

От противного. Пусть $x^3 - 2 = f(x)g(x)$. Тогда степени $f(x)$, $g(x)$ должны быть меньше 2. Подставим $x = \sqrt[3]{2}$:

$0 = f(\sqrt[3]{2})g(\sqrt[3]{2}) \Rightarrow f(\sqrt[3]{2}) = 0$ либо $g(\sqrt[3]{2}) = 0$, но это противоречит тому, что $x^3 - 2$ — минимальный.

Доказано.

ЛЕММА 2

НОД $(x^3 - 2, ax^2 + bx + c) = 1$ для любого многочлена $ax^2 + bx + c \in \mathbb{Q}[x]$.

Очевидно следует из леммы 1.

ЛЕММА 3

Для любого ненулевого многочлена $ax^2 + bx + c \in \mathbb{Q}[x]$ существуют такие многочлены $h_1, h_2 \in \mathbb{Q}[x]$, что $h_1(x^3 - 2) + h_2(ax^2 + bx + c) = 1$.

ЛЕММА 4

Пусть $g(x) \in \mathbb{Q}[x]$ — многочлен произвольной степени. Тогда существует многочлен $ax^2 + bx + c$ такой, что $g(\sqrt[3]{2}) = a(\sqrt[3]{2})^2 + b\sqrt[3]{2} + c$.

ДОКАЗАТЕЛЬСТВО

Разделим $g(x)$ с остатком на $x^3 - 2$:
$g(x) = l(x)(x^3 - 2) + ax^2 + bx + c$, где $ax^2 + bx + c$ — некоторый многочлен.

Подставим $x = \sqrt[3]{2}$:
$g(\sqrt[3]{2}) = l(x) \cdot 0 + a(\sqrt[3]{2})^2 + b\sqrt[3]{2} + c$. Доказано.

УТВЕРЖДЕНИЕ

$g(\sqrt[3]{2}) = 0 \Leftrightarrow g(x)$ делится нацело на $x^3 - 2$ в кольце многочленов $\mathbb{Q}[x]$.

ЛЮБОЕ ЧИСЛО ИЗ $\mathbb{Q}(\sqrt[3]{2})$ ВЫРАЖАЕТСЯ ЧЕРЕЗ 3 ЭЛЕМЕНТА

Возьмем произвольное число $\beta \in \mathbb{Q}(\sqrt{2})$.

Оно имеет вид $\beta = \dfrac{a\sqrt[3]{4} + b\sqrt[3]{2} + c}{p\sqrt[3]{4} + q\sqrt[3]{2} + r}$.

Но по лемме 3 для многочлена, который находится в знаменателе, существует представление:

$h_1(x^3 - 2) + h_2(px^2 + qx + r) = 1$.

Подставим $x = \sqrt[3]{2}$:

$h_1 \cdot 0 + h_2(\sqrt[3]{2})(p\sqrt[3]{4} + q\sqrt[3]{2} + r) = 1 \Rightarrow$

$\beta = (a\sqrt[3]{4} + b\sqrt[3]{2} + c)h_2(\sqrt[3]{2})$, а это снова многочлен такого же вида. Следовательно, для описания любого $\beta \in \mathbb{Q}(\sqrt[3]{2})$ служит базис, состоящий из трех элементов: $1, \sqrt[3]{2}, \sqrt[3]{4}$.

Таким образом, теорема об устройстве поля $\mathbb{Q}(\sqrt[3]{2})$ полностью доказана.

ОБОБЩЕНИЕ ДЛЯ ЛЮБОГО АЛГЕБРАИЧЕСКОГО ЧИСЛА

Пусть α — алгебраическое число степени r. То есть существует многочлен $f(x)$ степени r такой, что $f(\alpha) = 0$, и при этом $g(\alpha) \neq 0 \; \forall \, g(x) \in \mathbb{Q}[x]$, если $deg\ g < r$.

Убедимся, что $f(x)$ — единственный. Пусть есть еще один минимальный многочлен $f_1(x)$ для числа α. Разделим с остатком один на другой. Получим, что при $x = \alpha$: $0 = 0 \cdot l(\alpha) + q(\alpha)$, откуда остаток $q(\alpha) = 0$, но это невозможно, т.к. $deg\ q < deg\ f$.

Очевидно, что $f(x)$ неразложимый в $\mathbb{Q}[x]$.
Тогда НОД $(f, g) = 1 \; \forall \, g$, $deg\ g < r$.

Следовательно, $\exists \, h_1, h_2 \in \mathbb{Q}[x]$ такие, что $h_1(x)f(x) + h_2(x)g(x) = 1$.

При $x = \alpha$ получаем:

$h_1(\alpha) \cdot 0 + h_2(\alpha)g(\alpha) = 1 \Rightarrow \dfrac{1}{g(\alpha)} = h_2(\alpha)$ — обратное значение.

Таким образом все элементы поля $\mathbb{Q}(\alpha)$ имеют вид значения в точке α некоторого многочлена, степень которого меньше r:

$\beta \, \forall \in \mathbb{Q}(\alpha) \quad \beta = s_0 + s_1\alpha + s_2\alpha^2 + \ldots + s_{r-1}\alpha^{r-1}$.

А это, в свою очередь, означает, что для задания любого элемента $\beta \in \mathbb{Q}(\alpha)$ требуется базис, состоящий из r элементов: $1, \alpha, \alpha^2, \ldots, r - 1$.

ТЕОРЕМА О БАЗИСЕ

ТЕОРЕМА

Все базисы поля $k \subset K$ имеют одинаковое число элементов.

ДОКАЗАТЕЛЬСТВО

От противного. Пусть есть два базиса $\alpha_1, \alpha_2, \ldots, \alpha_r$ и $\beta_1, \beta_2, \ldots, \beta_l$, и $l < r$. Для наглядности проведем рассуждения для $r = 3$, $l = 2$.

Выразим элементы «большого» базиса через «маленький» базис:

$\alpha_1 = r_{11}\beta_1 + r_{21}\beta_2$

$\alpha_2 = r_{12}\beta_1 + r_{22}\beta_2$

$\alpha_3 = r_{13}\beta_1 + r_{23}\beta_2$

Домножим эти равенства, соответственно, на x_1, x_2, x_3, сложим и приравняем сумму к нулю.
Перегруппировав, получим:

$\beta_1(r_{11}x_1 + r_{12}x_2 + r_{13}x_3) + \beta_2(r_{21}x_1 + r_{22}x_2 + r_{23}x_3) = 0$.

Так как в любом базисе 0 должен выражаться единственным образом с коэффициентами, равными 0, получаем:

$r_{11}x_1 + r_{12}x_2 + r_{13}x_3 = 0$,

$r_{21}x_1 + r_{22}x_2 + r_{23}x_3 = 0$.

Такая система уравнений всегда разрешима, при этом один элемент из x_1, x_2, x_3 выражается через другие два. А значит, в нашем базисе из 3-х элементов один выражается через другие два, т.е. по сути базис содержит 2 элемента, а набор из 3-х элементов уже не является базисом. Противоречие.

Для произвольных размерностей базисов $r > l$ рассуждения полностью аналогичны.

Теорема доказана.