

Определение. *Характеристика поля K* – это наименьшее число $p \in \mathbb{N}$, такое что

$$\underbrace{1 + 1 + \dots + 1}_p = 0$$

Если такого p не существует, то говорят, что характеристика равна 0.

Обозначение: $\text{char } K$.

Предложение. K – поле \Rightarrow либо $\text{char } K = 0$, либо $\text{char } K = p > 0$, где p – простое число.

Определение. K, F – поля и $K \subseteq F \Rightarrow F$ называется расширением поля K (« $K \subseteq F$ » – расширение полей).

Замечание. $K \subseteq F$ – расширение полей $\Rightarrow F$ является векторным пространством над K .

Определение. *Степенью расширения $K \subseteq F$* называется размерность F как векторного пространства.

Обозначение: $[F : K]$

Определение. Расширение $K \subseteq F$ называется *конечным*, если $[F : K] < \infty$.

Лемма. Пусть $K \subseteq F, F \subseteq L$ – конечные расширения полей, тогда $K \subseteq L$ – тоже конечное расширение полей, причём $[L : K] = [L : F] \cdot [F : K]$.

K – поле, $h \in K[x]$ и $\deg h = n$

$$F = K[x]/(h), f \in K[x] \rightsquigarrow \bar{f} = f + (h) \in F$$

F – поле $\Leftrightarrow h$ – неприводим

Пусть h – неприводим, то есть F – поле, тогда для $K \subseteq F$ верно $[F : K] = n$ и \bar{x} является корнем h в поле F , в частности h имеет корни в поле F .

Следствие. $f \in K[x], \deg f > 1 \Rightarrow \exists$ конечное расширение $K \subseteq F$, такое что f имеет корень в F .

Следствие. $f \in K[x], \deg f > 1 \Rightarrow \exists$ конечное расширение $K \subseteq F$, такое что f разлагается на линейные множители.

$K \subseteq F$ – расширение полей, $\alpha \in F$

Определение. Элемент $\alpha \in F$ называется *алгебраическим* над K , если существует $f \in K[x], f \neq 0$, такой что $f(\alpha) = 0$. Иначе α называется *трансцендентным* над K .

Определение. *Минимальным многочленом* элемента $\alpha \in F$, алгебраическим над K , называется такой многочлен $h \in K[x]$, что

(а) $h(\alpha) = 0$

(б) h имеет наименьшую степень

Лемма. Пусть $K \subseteq F$ – расширение полей, $\alpha \in F$ – элемент, алгебраический над K , и $h \in K[x]$ – его минимальный многочлен. Тогда

- (а) h определён однозначно с точностью до пропорциональности
- (б) для всякого $f \in K[x]$ имеем $f(\alpha) = 0 \Leftrightarrow f \div h$
- (в) h неприводим над K

$K \subseteq F$ – расширение полей, $\alpha \in F$ – элемент, алгебраический над K и h_α – его минимальный многочлен

Обозначение: $K(\alpha)$ – пересечение всех подполей F , содержащих K и α .

Замечание. $K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f, g \in K[x], g(\alpha) \neq 0 \right\}$.

Предложение. Существует изоморфизм $\psi : K[x]/(h_\alpha) \xrightarrow{\sim} K(\alpha)$, такой что $\psi(\bar{x}) = \alpha$.

Следствие. $\forall y \in K(\alpha)$ существует единственное представление в виде $y = \beta_0 + \beta_1\alpha + \dots + \beta_{n-1}\alpha^{n-1}$, где $\beta_i \in K$.

Обозначение. K – поле $\Rightarrow K^\times = (K \setminus \{0\}, \times)$ – мультипликативная группа K .

K – конечно поле $\Rightarrow \text{char } K = p > 0$ – простое число. Пусть $\langle 1 \rangle \subseteq K$ – циклическая прод группа по сложению, порождённая 1. Тогда $\langle 1 \rangle$ – подкольцо в K и $\langle 1 \rangle = \mathbb{Z}_p \Rightarrow \langle 1 \rangle$ – подполе в K .

Будем отождествлять \mathbb{Z}_p с $\langle 1 \rangle$ и считать, что $\mathbb{Z}_p \subseteq K$.

Теорема. $|K| = p^n$, где $n = \dim_{\mathbb{Z}_p} K$.

Конструкция поля из p^n элементов. Выберем неприводимый многочлен $h \in \mathbb{Z}_p[x]$, $\deg h = n$. Тогда $F = \mathbb{Z}_p/(h)$ – поле и $[F : \mathbb{Z}_p] = n \Rightarrow$ получаем $|F| = p^n$.

Задание 1. Избавьтесь от иррациональности в знаменателе дроби $\frac{9 - 40\sqrt[3]{6} - 6\sqrt[3]{36}}{1 - \sqrt[3]{6} - 3\sqrt[3]{36}}$ и упростите полученное выражение.

1. Пусть $\alpha = \sqrt[3]{6}$, тогда описанная дробь представляется в следующем виде:

$$\frac{9 - 40\alpha - 6\alpha^2}{1 - \alpha - 3\alpha^2} = \frac{f(\alpha)}{g(\alpha)} \in \mathbb{Q}(\alpha)$$

Известно, что $\mathbb{Q}(\alpha) \xrightarrow{\sim} \mathbb{Q}[x]/(x^3 - 6)$, многочлен $x^3 - 6$ неприводим над \mathbb{Q} и является минимальным для α . Таким образом, задача сводится к делению в факторкольце $\mathbb{Q}[x]/(x^3 - 6)$. В данном случае формула понижения степени будет равна $\alpha^3 = 6$.

2. Каждый элемент $\mathbb{Q}(\alpha)$ единственным образом представляется в виде $A\alpha^2 + B\alpha + C$, тогда

$$\begin{aligned} \frac{9 - 40\alpha - 6\alpha^2}{1 - \alpha - 3\alpha^2} &= A\alpha^2 + B\alpha + C \\ 9 - 40\alpha - 6\alpha^2 &= (A\alpha^2 + B\alpha + C)(1 - \alpha - 3\alpha^2) = \\ &= A\alpha^2 + B\alpha + C - A\alpha^3 - B\alpha^2 - C\alpha - 3A\alpha^4 - 3B\alpha^3 - 3C\alpha^2 = \\ &= -3A\alpha^4 - (A + 3B)\alpha^3 + (A - B - 3C)\alpha^2 + (B - C)\alpha + C = \\ &= (A - B - 3C)\alpha^2 + (-18A + B - C)\alpha + (-6A - 18B + C) \end{aligned}$$

Таким образом, $-6\alpha^2 - 40\alpha + 9 = (A - B - 3C)\alpha^2 + (-18A + B - C)\alpha + (-6A - 18B + C)$. Получаем следующую СЛУ на неизвестные A , B и C :

$$\begin{aligned} \left(\begin{array}{ccc|c} 1 & -1 & -3 & -6 \\ -18 & 1 & -1 & -40 \\ -6 & -18 & 1 & 9 \end{array} \right) &\rightsquigarrow \left(\begin{array}{ccc|c} 1 & -1 & -3 & -6 \\ 0 & -17 & -55 & -148 \\ 0 & -24 & -17 & -27 \end{array} \right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & -1 & -3 & -6 \\ 0 & -17 & -55 & -148 \\ 0 & 408 & 289 & 459 \end{array} \right) \rightsquigarrow \\ \left(\begin{array}{ccc|c} 1 & -1 & -3 & -6 \\ 0 & -17 & -55 & -148 \\ 0 & 0 & 1031 & 3039 \end{array} \right) &\rightsquigarrow \left(\begin{array}{ccc|c} 1 & -1 & 0 & 3 \\ 0 & -17 & 0 & 17 \\ 0 & 0 & 1 & 3 \end{array} \right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 3 \end{array} \right) \Rightarrow \begin{cases} A = 2 \\ B = -1 \\ C = 3 \end{cases} \end{aligned}$$

3. Получаем, что данная дробь может быть представлена в следующем виде:

$$\frac{9 - 40\sqrt[3]{6} - 6\sqrt[3]{36}}{1 - \sqrt[3]{6} - 3\sqrt[3]{36}} = 3 - \sqrt[3]{6} + 2\sqrt[3]{36}$$

Ответ: $3 - \sqrt[3]{6} + 2\sqrt[3]{36}$

Задание 2. Найдите минимальный многочлен для числа $\sqrt{7} - \sqrt{3} + 1$ над \mathbb{Q} .

1. Пусть $\alpha = \sqrt{7} - \sqrt{3} + 1$. Рассмотрим следующие преобразования:

$$\begin{aligned}\alpha &= \sqrt{7} - \sqrt{3} + 1 \Leftrightarrow \alpha - 1 = \sqrt{7} - \sqrt{3} \\ (\alpha - 1)^2 &= (\sqrt{7} - \sqrt{3})^2 \Leftrightarrow \alpha^2 - 2\alpha - 9 = -2\sqrt{21} \\ (\alpha^2 - 2\alpha - 9)^2 &= 84 \Leftrightarrow \alpha^4 - 4\alpha^3 - 14\alpha^2 + 36\alpha - 3 = 0\end{aligned}$$

2. Получен аннулирующий многочлен $f = x^4 - 4x^3 - 14x^2 + 36x - 3 \in \mathbb{Q}[x]$, $f(\alpha) = 0$. Покажем, что он минимальный.

Рассмотрим расширение $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$. Известно, что $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ равно степени минимального многочлена, то есть достаточно показать, что $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Последовательно присоединим $\sqrt{3}$ и $\sqrt{7}$ к \mathbb{Q} , то есть рассмотрим цепочку $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3})(\sqrt{7})$.

3. Ясно, что для $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$ минимальный многочлен имеет вторую степень (этот многочлен равен $x^2 - 3$). Если он имеет первую степень, то есть равен $f = ax + b$, $a, b \in \mathbb{Q}$, то по определению $f(\sqrt{3}) = a\sqrt{3} + b = 0 \Leftrightarrow a\sqrt{3} = -b$, что неверно: левая часть иррациональна, а правая рациональна. Получаем: $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.

4. Присоединим к $\mathbb{Q}(\sqrt{3})$ элемент $\sqrt{7}$, то есть рассмотрим $\mathbb{Q}(\sqrt{3})(\sqrt{7})$. Покажем, что минимальный многочлен $\sqrt{7}$ над $\mathbb{Q}(\sqrt{3})$ имеет степень равную 2. Такой многочлен найдётся: $x^2 - 7$.

Пусть элемент $\sqrt{7}$ обнуляется многочленом первой степени, то есть $\sqrt{7} \in \mathbb{Q}(\sqrt{3})$. Тогда верно, что $\sqrt{7} = a\sqrt{3} + b$, $a, b \in \mathbb{Q}$. Возведя обе части в квадрат, получим $7 = 3a^2 + b^2 + 2ab\sqrt{3}$, что равносильно $7 = 3a^2 + b^2$ и $2ab\sqrt{3} = 0$. Из последнего получаем, что $a = 0$ или $b = 0$, но тогда $7 = b^2$ или $7 = 3a^2$ соответственно, что неразрешимо в \mathbb{Q} .

Таким образом, минимальная степень многочлена равна двум и $[\mathbb{Q}(\sqrt{3})(\sqrt{7}) : \mathbb{Q}(\sqrt{3})] = 2$.

5. По лемме $[\mathbb{Q}(\sqrt{3})(\sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3})(\sqrt{7}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$. Более того, $1, \sqrt{3}, \sqrt{7}, \sqrt{21}$ – базис векторного пространства $\mathbb{Q}(\sqrt{3})(\sqrt{7})$ над \mathbb{Q} . Докажем, что поле $\mathbb{Q}(\sqrt{3})(\sqrt{7}) = \mathbb{Q}(\sqrt{7} - \sqrt{3} + 1) = \mathbb{Q}(\alpha)$. Несложно увидеть, что $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{3})(\sqrt{7})$, так как $\alpha \in \mathbb{Q}(\sqrt{3})(\sqrt{7})$.

Покажем, что каждый базисный вектор $\mathbb{Q}(\sqrt{3})(\sqrt{7})$ лежит в $\mathbb{Q}(\alpha)$. Так как $\alpha \in \mathbb{Q}(\alpha)$, элемент $\alpha^2 = 11 - 2\sqrt{3} + 2\sqrt{7} - 2\sqrt{21} = 9 + 2\alpha - 2\sqrt{21} \in \mathbb{Q}(\alpha) \Rightarrow \sqrt{21} \in \mathbb{Q}(\alpha)$. Рассмотрим элемент $\sqrt{21}\alpha \in \mathbb{Q}(\alpha)$: $7\sqrt{3} - 3\sqrt{7} + \sqrt{21} \in \mathbb{Q}(\alpha) \Rightarrow 7\sqrt{3} - 3\sqrt{7} \in \mathbb{Q}(\alpha)$. Складывая этот элемент с 7α и 3α , получим, что $\sqrt{7}$ и $\sqrt{3}$ лежат в $\mathbb{Q}(\alpha)$. Единица лежит в $\mathbb{Q}(\alpha)$, так как $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$.

Базис $\mathbb{Q}(\sqrt{3})(\sqrt{7})$ лежит в $\mathbb{Q}(\alpha)$, значит, $\mathbb{Q}(\sqrt{3})(\sqrt{7}) \subseteq \mathbb{Q}(\alpha)$, но $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{3})(\sqrt{7})$, тогда $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3})(\sqrt{7})$. Получаем, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

6. Таким образом, степень минимального многочлена для $\sqrt{7} - \sqrt{3} + 1$ над \mathbb{Q} равна 4. Такой многочлен уже найден – это $f = x^4 - 4x^3 - 14x^2 + 36x - 3$

Ответ: $f = x^4 - 4x^3 - 14x^2 + 36x - 3$

Задание 3. Постройте явно \mathbb{F}_8 и составьте для него таблицы сложения и умножения.

1. Конструкция поля из p^n элементов: выберем неприводимый многочлен $h \in \mathbb{Z}_p[x]$, $\deg h = n$. Тогда $F = \mathbb{Z}_p/(h)$ – поле и $[F : \mathbb{Z}_p] = n \Rightarrow$ получаем $|F| = p^n$.
2. Поле \mathbb{F}_8 состоит из $8 = 2^3$ элементов. Из предыдущего пункта следует, что для того, чтобы его построить, нужно взять неприводимый многочлен $h \in \mathbb{Z}_2[x]$, такой что $\deg h = 3$. В $\mathbb{Z}_2[x]$ всего два неприводимых многочлена степени три: $h_1 = 1 + x + x^3$, $h_2 = 1 + x^2 + x^3$. Многочлены неприводимы над \mathbb{Z}_2 , так как $h_1(0) = h_1(1) = 1 \neq 0$ и $h_2(0) = h_2(1) = 1 \neq 0$. Для реализации поля возьмём первый многочлен $h = h_1$.
3. Положим $\mathbb{F}_8 = \mathbb{Z}_2[x]/(h) = \{\bar{0}, \bar{1}, \bar{x}, \bar{x} + \bar{1}, \bar{x}^2, \bar{x}^2 + \bar{1}, \bar{x}^2 + \bar{x}, \bar{x}^2 + \bar{x} + \bar{1}\}$ (это все многочлены в $\mathbb{Z}_2[x]$ степени меньше 3). Нетрудно заметить, что условие $|\mathbb{F}_8| = 8$ выполнено.
4. Составим таблицу сложения для данного поля. Так как в поле сложение коммутативно, таблица будет симметрична относительно главной диагонали. Все операции производятся по модулю 2.

+	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{x} + \bar{1}$	\bar{x}^2	$\bar{x}^2 + \bar{1}$	$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{x} + \bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{x} + \bar{1}$	\bar{x}^2	$\bar{x}^2 + \bar{1}$	$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{x} + \bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{x} + \bar{1}$	\bar{x}	$\bar{x}^2 + \bar{1}$	\bar{x}^2	$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{x}^2 + \bar{x}$
\bar{x}	\bar{x}	$\bar{x} + \bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{x} + \bar{1}$	\bar{x}^2	$\bar{x}^2 + \bar{1}$
$\bar{x} + \bar{1}$	$\bar{x} + \bar{1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{1}$	\bar{x}^2
\bar{x}^2	\bar{x}^2	$\bar{x}^2 + \bar{1}$	$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{x} + \bar{1}$
$\bar{x}^2 + \bar{1}$	$\bar{x}^2 + \bar{1}$	\bar{x}^2	$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{x}^2 + \bar{x}$	$\bar{1}$	$\bar{0}$	$\bar{x} + \bar{1}$	\bar{x}
$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{x} + \bar{1}$	\bar{x}^2	$\bar{x}^2 + \bar{1}$	\bar{x}	$\bar{x} + \bar{1}$	$\bar{0}$	$\bar{1}$
$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{1}$	\bar{x}^2	$\bar{x} + \bar{1}$	\bar{x}	$\bar{1}$	$\bar{0}$

5. Составим таблицу умножения для данного поля. Так как в поле умножение коммутативно, таблица будет симметрична относительно главной диагонали. При умножении будем применять формулу понижения степени: $x^3 = x + 1$. Все операции производятся по модулю 2.

\times	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{x} + \bar{1}$	\bar{x}^2	$\bar{x}^2 + \bar{1}$	$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{x} + \bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{x} + \bar{1}$	\bar{x}^2	$\bar{x}^2 + \bar{1}$	$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{x} + \bar{1}$
\bar{x}	$\bar{0}$	\bar{x}	\bar{x}^2	$\bar{x}^2 + \bar{x}$	$\bar{x} + \bar{1}$	\bar{x}	$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{x}^2 + \bar{1}$
$\bar{x} + \bar{1}$	$\bar{0}$	$\bar{x} + \bar{1}$	$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{1}$	$\bar{x}^2 + \bar{x} + \bar{1}$	\bar{x}^2	$\bar{1}$	\bar{x}
\bar{x}^2	$\bar{0}$	\bar{x}^2	$\bar{x} + \bar{1}$	$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{x}^2 + \bar{x}$	\bar{x}	$\bar{x}^2 + \bar{1}$	$\bar{1}$
$\bar{x}^2 + \bar{1}$	$\bar{0}$	$\bar{x}^2 + \bar{1}$	\bar{x}	\bar{x}^2	\bar{x}	$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{x} + \bar{1}$	$\bar{x}^2 + \bar{x}$
$\bar{x}^2 + \bar{x}$	$\bar{0}$	$\bar{x}^2 + \bar{x}$	$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{1}$	$\bar{x}^2 + \bar{1}$	$\bar{x} + \bar{1}$	\bar{x}	\bar{x}^2
$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{0}$	$\bar{x}^2 + \bar{x} + \bar{1}$	$\bar{x}^2 + \bar{1}$	\bar{x}	$\bar{1}$	$\bar{x}^2 + \bar{x}$	\bar{x}^2	$\bar{x} + \bar{1}$

Задание 4. Пусть $K \subseteq F$ – расширение полей и $\alpha \in F$. Положим $K[\alpha] = \{f(\alpha) \mid f \in K[x]\}$. Докажите, что если $K[\alpha]$ конечномерное векторное пространство над K , то $K[\alpha] = K(\alpha)$.

1. Докажем, что α алгебраический над K . По условию $K[\alpha]$ – конечномерное векторное пространство над $K \Rightarrow \dim K[\alpha] = n < \infty$, тогда векторы $1, \alpha, \alpha^2, \dots, \alpha^n$ – линейно зависимы (их $n + 1$ штука). Получаем, что существует нетривиальная линейная комбинация $f = a_0 + a_1\alpha + \dots + a_n\alpha^n$, где $a_i \in K$, $n \in \mathbb{N}$, равная нулю, то есть α – корень многочлена f в поле F .

Получаем, что α – алгебраичен над K .

2. Элементы $K[\alpha]$ – выражения вида $a_0 + a_1\alpha + \dots + a_n\alpha^n$, где $a_i \in K$, $n \in \mathbb{N}$. Поле $K(\alpha)$ содержит $\alpha, \alpha^2, \dots, \alpha^n$, а значит, все выражения вида $a_0 + a_1\alpha + \dots + a_n\alpha^n$, $a_i \in K$. Значит, $K[\alpha] \subseteq K(\alpha)$.

3. Пусть h – минимальный многочлен α , тогда h – неприводим над K и $h(\alpha) = 0$.

Докажем, что $K[\alpha]$ – поле. В данном кольце $1 \neq 0$ (K – поле). Покажем, что всякий ненулевой элемент $f(\alpha)$ кольца обратим. Рассмотрим многочлен $f \in K[x]$. Так как $f(\alpha) \neq 0$, f не делится на h . В то же время h не делится на f , так как h неприводим $\Rightarrow \text{НОД}(f, h) = 1 \Leftrightarrow$ существуют $v, u \in K[x] : vf + uh = 1$. Переходя в $K[\alpha]$, получим $1 = v(\alpha)f(\alpha) + u(\alpha)h(\alpha) \Rightarrow v(\alpha)f(\alpha) = 1$, то есть $v(\alpha)$ является обратным к $f(\alpha)$ в $K[\alpha]$.

Таким образом, кольцо $K[\alpha]$ – поле.

4. Известно, что $K(\alpha)$ – наименьшее поле содержащее K и α . Но $K[\alpha]$ – поле, содержащее K и α , лежащее в $K(\alpha)$. Значит, $K(\alpha) = K[\alpha]$.