Алгебра

Сидоров Дмитрий

Группа БПМИ 219

June 6, 2022

№1

Избавьтесь от иррациональности в знаменателе дроби $\frac{3-63\sqrt[3]{7}-8\sqrt[3]{49}}{1-2\sqrt[3]{7}-4\sqrt[3]{49}}$ и упростите полученное выражение.

Решение:

Обозначим $\alpha = \sqrt[3]{7}$ $(\alpha^3 = 7), f(\alpha) = 3 - 63\sqrt[3]{7} - 8\sqrt[3]{49}, g(\alpha) = 1 - 2\sqrt[3]{7} - 4\sqrt[3]{49} \Rightarrow \frac{3-63\sqrt[3]{7}-8\sqrt[3]{49}}{1-2\sqrt[3]{7}-4\sqrt[3]{49}} = \frac{f(\alpha)}{g(\alpha)} \in \mathbb{Q}(\alpha)$. Тогда, тк $[\mathbb{Q}(a) : \mathbb{Q}] = 3$ (доказано на семинаре, что если α - действительный корень уравнения $x^3 = a$ $(a \in \mathbb{Q})$, то $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 1$, если a - куб рационального числа, и $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ иначе), то каждый элемент $\mathbb{Q}(\alpha)$ можно единственным образом представить в виде $a_0 \cdot 1 + a_1 \cdot \sqrt[3]{7} + a_2 \cdot \sqrt[3]{49}$. Значит $\frac{3-63\sqrt[3]{7}-8\sqrt[3]{49}}{1-2\sqrt[3]{7}-4\sqrt[3]{49}} = a_0 \cdot 1 + a_1 \cdot \sqrt[3]{7} + a_2 \cdot \sqrt[3]{49} \Rightarrow$ $3 - 63\sqrt[3]{7} - 8\sqrt[3]{49} = (1 - 2\sqrt[3]{7} - 4\sqrt[3]{49})(a_0 + a_1 \cdot \sqrt[3]{7} + a_2 \cdot \sqrt[3]{49}) = a_0 - 2\sqrt[3]{7}a_0 - 4\sqrt[3]{49}a_0 + a_1\sqrt[3]{7} - a_1 \cdot 2\sqrt[3]{49} - 28a_1 + a_2\sqrt[3]{49} - 14a_2 - 28a_2\sqrt[3]{7} = (a_0 - 28a_1 - 14a_2) + \sqrt[3]{7}(-2a_0 + a_1 - 28a_2) + \sqrt[3]{49}(-4a_0 - 2a_1 + a_2) \Rightarrow$

$$\begin{pmatrix} 1 & -28 & -14 & 3 \\ -2 & 1 & -28 & -63 \\ -4 & -2 & 1 & -8 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -28 & -14 & 3 \\ 0 & -55 & -56 & -57 \\ 0 & -114 & -55 & -4 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -28 & -14 & 3 \\ 0 & -55 & -56 & -57 \\ 0 & -4 & 57 & -110 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -28 & -14 & 3 \\ 0 & 1 & -742 & 1483 \\ 0 & -4 & 57 & 110 \end{pmatrix} \rightarrow$$

$$\begin{pmatrix} 1 & 0 & 20762 & 41527 \\ 0 & 1 & -742 & 1483 \\ 0 & 0 & -2911 & -5822 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 20762 & 41527 \\ 0 & 1 & -742 & 1483 \\ 0 & 0 & 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix} \Rightarrow \frac{3-63\sqrt[3]{7}-8\sqrt[3]{49}}{1-2\sqrt[3]{7}-4\sqrt[3]{49}} = 3 - \sqrt[3]{7} + 2\sqrt[3]{49}$$

Ответ: $\frac{3-63\sqrt[3]{7}-8\sqrt[3]{49}}{1-2\sqrt[3]{7}-4\sqrt[3]{49}} = 3 - \sqrt[3]{7} + 2\sqrt[3]{49}$

№2

Найдите минимальный многочлен для числа $\sqrt{6} - \sqrt{5} - 1$ над $\mathbb{Q}$.

Решение:

Обозначим $\sqrt{6} - \sqrt{5} - 1$ как a. Тогда $\sqrt{6} - \sqrt{5} - 1 = a \Rightarrow a + 1 = \sqrt{6} - \sqrt{5} \Rightarrow (a+1)^2 = a^2 + 2a + 1 = (\sqrt{6} - \sqrt{5})^2 = 11 - 2\sqrt{30} \Rightarrow -2\sqrt{30} = a^2 + 2a - 10 \Rightarrow 120 = (a^2 + 2a - 10)^2 = a^4 + 4a^3 - 16a^2 - 40a + 100 \Rightarrow a^4 + 4a^3 - 16a^2 - 40a - 20 = 0$. Значит многочлен $f = x^4 + 4x^3 - 16x^2 - 40x - 20 \in \mathbb{Q}[x]$ является аннулирующим, тк $f(a) = 0$. Теперь докажем, что найденный многочлен f является минимальным. Для этого для расширения $\mathbb{Q} \subseteq \mathbb{Q}(a)$, тк $[\mathbb{Q}(a) : Q] = \deg f_{\min}$ (равно степени минимального многочлена) и $\deg f = 4$, покажем, что $[\mathbb{Q}(a) : Q] = 4$. Для этого рассмотрим $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{5})(\sqrt{6})$.

Покажем, что $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$. Пусть $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 1$, тогда минимальный многочлен иметт степень 1, те имеет вид $g = ax + b,\ a, b \in \mathbb{Q} \Rightarrow g(\sqrt{5}) = a\sqrt{5} + b \Rightarrow a\sqrt{3} = -b \Rightarrow$ противоречие, тк правая часть является рациональным числом, а левая иррациональным. При этом существует минимальный многочлен, который имеет вторую степень $(x^2 - 5)$, значит $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$.

Теперь покажем, что $[\mathbb{Q}(\sqrt{5})(\sqrt{6}) : \mathbb{Q}(\sqrt{5})] = 2$. Существует многочлен $(x^2 - 6)$ такой, что он имеет степень 2, и он является минимальным для $\sqrt{6}$ над $\mathbb{Q}(\sqrt{5})$. Пусть существует многочлен степени 1, который обнуляет $\sqrt{6}$, тогда $\sqrt{6} \in \mathbb{Q}(\sqrt{5})$ и $\sqrt{6} = a\sqrt{5} + b,\ a, b \in \mathbb{Q} \Rightarrow 6 = 5a^2 + b^2 + 2ab\sqrt{5} \Rightarrow$ либо $a = 0$, либо $b = 0$ (тк иначе правая часть рациональна, а левая иррациональна). Но тогда либо $6 = 5a^2$, либо $6 = b^2$, оба уравнения не имеют решений в $\mathbb{Q}$. Таким образом, $[\mathbb{Q}(\sqrt{5})(\sqrt{6}) : \mathbb{Q}(\sqrt{5})] = 2$.

Известно, что для произвольных конечных расширений полей $K \subseteq F \subseteq L$ выполняется $[L : K] = [L : F] \cdot [F : K]$, значит $[\mathbb{Q}(\sqrt{5})(\sqrt{6}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5})(\sqrt{6}) : \mathbb{Q}(\sqrt{5})] \cdot [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4$. Теперь докажем, что $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{5})(\sqrt{6})$.

1) $1, \sqrt{5}, \sqrt{6}, \sqrt{30}$ - базис векторного пространства $\mathbb{Q}(\sqrt{5})(\sqrt{6})$ над $\mathbb{Q} \Rightarrow$ тк $a \in \mathbb{Q}(\sqrt{5})(\sqrt{6})$, то $\mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{5})(\sqrt{6})$

2) Покажем, что базис $\mathbb{Q}(\sqrt{5})(\sqrt{6})$ лежит в $\mathbb{Q}(a)$. $a = \sqrt{6} - \sqrt{5} - 1 \in \mathbb{Q}(a) \Rightarrow a^2 = (\sqrt{6} - \sqrt{5} - 1)^2 \in \mathbb{Q}(a)$ и при этом $(\sqrt{6} - \sqrt{5} - 1)^2 = 12 - 2\sqrt{30} - 2\sqrt{6} + 2\sqrt{5} = -2a + 10 - 2\sqrt{30} \Rightarrow \sqrt{30} \in \mathbb{Q}(a)$. В том числе $\sqrt{30}a \in \mathbb{Q}(a) \Rightarrow 6\sqrt{5} - 5\sqrt{6} - \sqrt{30} \in \mathbb{Q}(a) \Rightarrow 6\sqrt{5} - 5\sqrt{6} = b \in \mathbb{Q}(a)$ (тк$\sqrt{30} \in \mathbb{Q}(a)$). Тогда, тк $5a, 6a \in \mathbb{Q}(a)$ и $a+b \in \mathbb{Q}(a)$ (тк $a, b \in \mathbb{Q}(a)$), то $b + 5a \in \mathbb{Q}(a) \Rightarrow b + 5a = \sqrt{5} - 5 \in \mathbb{Q}(a) \Rightarrow \sqrt{5} \in \mathbb{Q}(a)$. Аналогично $b + 6a = \sqrt{6} - 6 \in \mathbb{Q}(a) \Rightarrow \sqrt{6} \in \mathbb{Q}(a)$. При этом, тк $Q \subseteq \mathbb{Q}(a)$ по построению $1 \in \mathbb{Q}(a)$ (в том числе для других целых чисел этот факт использовался ранее). Таким образом, $1, \sqrt{5}, \sqrt{6}, \sqrt{30}$ лежат в $\mathbb{Q}(a)$, а значит $\mathbb{Q}(\sqrt{5})(\sqrt{6}) \subseteq Q(a)$ (тк $1, \sqrt{5}, \sqrt{6}, \sqrt{30}$ - базис векторного пространства $\mathbb{Q}(\sqrt{5})(\sqrt{6})$ над $\mathbb{Q}$).

Таким образом, $\mathbb{Q} = \mathbb{Q}(\sqrt{5})(\sqrt{6})$, а значит $[\mathbb{Q}(a) : Q] = 4$. Итого, $f = x^4 + 4x^3 - 16x^2 - 40x - 20$ - искомый минимальный многочлен для числа $\sqrt{6} - \sqrt{5} - 1$ над $\mathbb{Q}$.

Ответ: $f = x^4 + 4x^3 - 16x^2 - 40x - 20$

№3

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

Решение:

Тк $8 = 2^3$, то в нашем случае для $\mathbb{F}_8 = \mathbb{F}_{p^n}$ $p = 2, n = 3$ (p - простое, $n \in \mathbb{N}$). Тогда, чтобы построить поле $\mathbb{F}_8$ нужно взять неприводимый многочлен $f \in \mathbb{Z}_2[x]$, степень которого равна $n = 3$. Значит, можно взять многочлен $f = x^3 + x + 1$, тк для него $f(0) = 1 \neq 0, f(1) = 1 \neq 0$. Положим $\mathbb{F}_8 = \mathbb{Z}_2[x]/(f)$. Тогда $\mathbb{F}_8$ состоит из всех многочленов в $\mathbb{Z}_2[x]/(f)$, степень которых меньше 3, те $\mathbb{F}_8 = \{\bar{0}, \bar{1}, \bar{x}, \bar{x} + \bar{1}, \bar{x}^2, \bar{x}^2 + \bar{1}, \bar{x}^2 + \bar{x}, \bar{x}^2 + \bar{x} + \bar{1}\}$.

Таблицы сложения и умножения для этого поля см в конце документа (обе операции коммутативны в поле, те таблицы симметричны относительно главной диагонали, а так же для умножения используем факт, что $x^3 = -x - 1 = x + 1$).

№4

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

Доказательство:

Пусть $\dim K[\alpha] = n < \infty$ (по условию $K[\alpha]$ конечномерно как векторное пространство над K). Тогда векторы $1, \alpha, \dots, \alpha^n$ линейно завсимы, тк их $n + 1 > n$ штук. Таким образом, существует i такой, что линейная комбинация $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$ при $a_i \neq 0,\ a_i \in K \Rightarrow \alpha-$ это корень многочлена $f = a_0 + a_1\alpha + \dots + a_n\alpha^n$ в поле F, а значит α является алгебраическим над K. При этом элементы $K[\alpha]$ имеют вид $a_0 + a_1\alpha + \dots + a_n\alpha^n$ $(a_i \in K)$ и $\alpha^j \in K(\alpha), 1 \leq j \leq n \Rightarrow a_0 + a_1\alpha + \dots + a_n\alpha^n \in K(\alpha) \Rightarrow K[\alpha] \subseteq K(\alpha)$.

Известно, что если $K \subseteq F$ - расширение полей и $\alpha \in F$ - элемент, алгебраический над K и h - его минимальный многочлен, то $K(\alpha)$ - пересечение всех подполей F, содержащих K и α, значит $K(\alpha)$ - наименьшее поле, содержащее

K и α. Докажем, что $K[\alpha]$ - поле (тогда, тк $K[\alpha]$ содержит K и α и $K[\alpha] \subseteq K(\alpha)$, $K(\alpha) = K[\alpha]$). Пусть $h \in K[x]$ - минимальный многочлен α, тогда $h(\alpha) = 0$, и по лемме из лекции h неприводим над K. По определению поле - коммутативное в кольцо, в котором $0 \neq 1$ и всякий ненулевой элемент обратим. В $K[\alpha]$ $0 \neq 1$, тк K - поле. Докажем, что всякий ненулевой элемент в $K[\alpha]$ обратим. Рассмотрим многочлен $f \in K[x]$, для которого выполняется $f(\alpha) \neq 0$. Тогда по лемме из лекции получаем, что f не делится на h (тк иначе $f(\alpha) = 0$). При этом, тк h неприводим, он не делится на f. Таким образом, их НОД равен 1, а значит $\exists u, v \in K[x] : uh + vf = 1 \Rightarrow u(\alpha)h(\alpha) + v(\alpha)f(\alpha) = 1 \Rightarrow v(\alpha)f(\alpha) = 1$, тк $h(\alpha) = 0 \Rightarrow f(\alpha)$ обратим, а значит всякий ненулевой элемент в $K[\alpha]$ обратим, и $K[\alpha]$ является полем. Таким образом, $K[\alpha] = K(\alpha)$. ■