Типичные ошибки в решениях задач 2 и 3.

№2 3) Нужно помнить, что поле, над которым рассматривается матрица конечно. В нем нет отношения "$\leq$", к которому вы привыкли в $\mathbb{R}$.

Поэтому, например, при $\alpha, \beta \in \mathbb{F}_5$

$$\det\begin{pmatrix}\alpha & \beta\\ -\beta & \alpha\end{pmatrix} = \begin{vmatrix}\alpha & \beta\\ -\beta & \alpha\end{vmatrix} = \alpha^2+\beta^2 = \bar{0} \text{ не только при } \alpha=\beta=\bar{0},$$

а еще при $\begin{cases}\alpha=2\\ \beta=1\end{cases}, \begin{cases}\alpha=-2\\ \beta=-1\end{cases}, \begin{cases}\alpha=2\\ \beta=-1\end{cases}, \begin{cases}\alpha=-2\\ \beta=1\end{cases}, \begin{cases}\alpha=1\\ \beta=2\end{cases}, \begin{cases}\alpha=-1\\ \beta=2\end{cases}, \begin{cases}\alpha=1\\ \beta=-2\end{cases}, \begin{cases}\alpha=-1\\ \beta=-2\end{cases}$

Также в конечном поле обманчивы выражения, содержащие радикалы, т.к. элементами такого поля является не целое число, а вычет. Например, $\sqrt{2} \in \mathbb{F}_7$, поскольку $3^2=2$ в $\mathbb{F}_7$.

№2 В7) В разобранной задаче мы видели, что $\langle E, B\rangle$-базис R над $\mathbb{F}_5$, $B=\begin{pmatrix}0&1\\2&0\end{pmatrix}$, $B^2=2E \Rightarrow B$-корень многочлена x^2-2. Было доказано, что он и является минимальным, ибо $\operatorname{ord} B=8 \Rightarrow B$-корень x^8-1. $x^8-1 \in \mathbb{F}_5[x]$ – это многочлен, аннулирующий B, наименьшей степени из многочленов вида x^n-1. Но минимальной многочлен – это любого вида (со старшим коэффициентом 1), аннулирующий многочлен минимальной степени (со старшим коэффициентом 1). минимальный многочлен неприводим, а $x^8-1 \vdots m_B(x)=x^2-2$.

$$R = \mathbb{F}_5[B] \simeq \mathbb{F}_5[x]/(x^2-2) \neq \mathbb{F}_5[x]/(x^8-1)$$

↑ поле, т.к. $m_B(x)=x^2-2$ – неприводимый мн-к

↑ не поле, т.к. x^8-1 – приводимый мн-к

N35) Многие не понимают, как доказать, что $\mathbb{Q}[\alpha] \subset Quot\,\mathbb{Z}[\alpha]$.

Вообще $Quot\,A = \left\{ \frac{a_1}{a_2} ; a_1, a_2 \in A, a_2 \neq \bar{0} \right\}$.

Пусть α – корень $x^3 - d$.

$$Quot\,\mathbb{Z}[\alpha] = \left\{ \frac{a_1 + b_1\alpha + c_1\alpha^2}{a_2 + b_2 + c_2\alpha^2} ; a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{Z}, a_2^2 + b_2^2 + c_2^2 \neq 0 \right\},$$

т. к. $\mathbb{Z}[\alpha] = \{ a + b\alpha + c\alpha^2 ; a, b, c \in \mathbb{Z} \}$.

$$\mathbb{Q}[\alpha] = \{ a + b\alpha + c\alpha^2 ; a, b, c \in \mathbb{Q} \} =$$

$$= \left\{ \frac{m_1}{n_1} + \frac{m_2}{n_2}\alpha + \frac{m_3}{n_3}\alpha^2 ; m_i, n_i \in \mathbb{Z}, n_i \neq 0, i = 1,2,3 \right\} =$$

$$= \left\{ \frac{m_1 n_2 n_3 + n_1 m_2 n_3 \alpha + n_1 n_2 m_3 \alpha^2}{n_1 n_2 n_3 + 0\alpha + 0\alpha^2}, m_i, n_i \in \mathbb{Z}, n_i \neq 0\ i = 1,2,3 \right\}$$

Теперь очевидно, что $\mathbb{Q}[\alpha] \subset Quot\,\mathbb{Z}[\alpha]$.

Случай: α – корень $x^2 - d$ еще проще.

Проверьте себя с помощью теста.

Выберите правильный ответ.

Пусть K – конечное поле, $|K| = p^n$. α – примитивный элемент расширения K над простым подполем. Чему равна $\deg m_\alpha(x)$?

1) p
2) $ord\,\alpha$
3) n