

Решение задач к экзамену по алгебре

Задача 1

Пусть $F \subset K \subset L$. Если L/F алгебраическое, то и L/K , и K/F алгебраические (сразу следует из определения). В обратную сторону, пусть $\alpha \in L$. Пусть $f = x^n + a_{n-1}x^{n-1} + \dots + a_0$ — минимальный многочлен α над K , тогда $F(a_0, a_1, \dots, a_{n-1}, \alpha)$ — конечное, а значит α алгебраический над F . Второе условие, очевидно, верно, т. к. если элемент алгебраический над F , он алгебраический и над любым расширением.

Задача 2

Докажем по индукции, $n = 1$ — очевидно. Пусть $x^2 - a_n$ имеет корень над $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, a_{n-1})$, т. е. $(a + b\sqrt{a_{n-1}})^2 = a_n$, где $a, b \in \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_{n-2}})$, т. е. $a^2 + a_{n-1}b^2 + 2ab\sqrt{a_{n-1}} = a_n$, в частности $ab = 0$, если $a = 0$, противоречие, иначе $b^2 = \frac{a_n a_{n-1}}{a^2}$. Противоречие, ведь $\{\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_{n-2}}, \frac{\sqrt{a_n a_{n-1}}}{a_{n-1}}\}$ тоже удовлетворяет условию.

Задача 3

Очевидно из мультипликативности степени расширений.

Задача 4

Пусть $\alpha = a + b\sqrt{-3} \in \mathcal{O}_K$, где $a, b \in \mathbb{Q}$, тогда, в частности, $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$, и $\text{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$, т. е. $2a \in \mathbb{Z}$, и $a^2 + 3b^2 \in \mathbb{Z}$, а значит $2a$ и $2b$ — целые одной четности. Но α — корень многочлена $x^2 - \text{Tr}_{K/\mathbb{Q}}(\alpha)x + N_{K/\mathbb{Q}}(\alpha)$, т. е. условие достаточно.

Задача 5

Пусть $F = \mathbb{F}_p(x^p)$, $L = \mathbb{F}_p(x)$. $\text{Tr}_{L/K}(1) = [L : F] = p = 0$. Минимальный многочлен x^k для $p \nmid k$ равен $t^p - x^{pk}$, из совпадения степеней, он равен характеристическому, т. е., в частности, $\text{Tr}_{L/K}(x^k) = 0$ для $k = 0, 1, \dots, p-1$, но это базис, а значит $\text{Tr}_{L/K} = 0$.

Задача 6

$\text{Tr}(\theta) = 0$. Характеристический θ^{-1} равен $t^3 + \frac{a}{b}t^2 + \frac{1}{b}$ ($b \neq 0$ из неприводимости).
Т. е. $\text{Tr}(\theta^{-1}) = -\frac{a}{b}$. $\text{Tr}(\theta^2) = -a \text{Tr}(1) - b \text{Tr}(\theta^{-1}) = -2a$, аналогично
 $\text{Tr}(\theta^3) = -3b$, $\text{Tr}(\theta^4) = 2a^2$.

$$\text{disc}\{1, \theta, \theta^2\} = \det \begin{pmatrix} 3 & 0 & -2a \\ 0 & -2a & -3b \\ -2a & -3b & 2a^2 \end{pmatrix} = -12a^3 - 27b^2 + 8a^3 = -4a^3 - 27b^2$$

Альтернативное доказательство:

$$\det \begin{pmatrix} \text{Tr}(1) & \text{Tr}(\theta) & \text{Tr}(\theta^2) \\ \text{Tr}(\theta) & \text{Tr}(\theta^2) & \text{Tr}(\theta^3) \\ \text{Tr}(\theta^2) & \text{Tr}(\theta^3) & \text{Tr}(\theta^4) \end{pmatrix} = \det \left(\begin{pmatrix} 1 & 1 & 1 \\ \theta & \theta' & \theta'' \\ \theta^2 & \theta'^2 & \theta''^2 \end{pmatrix} \begin{pmatrix} 1 & \theta & \theta^2 \\ 1 & \theta' & \theta'^2 \\ 1 & \theta'' & \theta''^2 \end{pmatrix} \right) =$$

$$= \det \left(\begin{pmatrix} 1 & 1 & 1 \\ \theta & \theta' & \theta'' \\ \theta^2 & \theta'^2 & \theta''^2 \end{pmatrix} \right)^2$$

Т. е. искомым дискриминант — дискриминант в многочлена в стандартном смысле.

Задача 7

1) \implies 2) Пусть f — минимальный многочлен α над F . Пусть $F \subset L \subset F$ и g — минимальный многочлен α над L , тогда $g \mid f$, причём, из факториальности кольца многочленов, таких g конечной число (g должен быть унитарным), при этом g однозначно определяет L . Действительно, L — минимальное поле, содержащее коэффициенты g , из совпадения степеней расширений и вложенности последнего в L .

2) \implies 1) Считаем F бесконечным, для конечных полей утверждение очевидно из цикличности мультипликативной группы. Пусть $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$. Достаточно доказать утверждение для $n = 2$. Действительно, для $n \geq 3$ можно рассмотреть $F' = F(\alpha_3, \alpha_4, \dots, \alpha_n)$ и воспользоваться индукцией. $K = F(\alpha, \beta)$. Рассмотрим промежуточные поля вида $F(\alpha + c\beta)$, где $c \in F$. Из условия, для каких-то $c_1, c_2 \in K$ $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$, а значит это расширение содержит α и β , т. е. $F(\alpha + c_1\beta) = K$.

Задача 8

Пусть $\alpha = \sqrt[k]{\frac{b_i}{b_j}}$, $i \neq j$, $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, r — наименьшее число, т. ч. $\alpha^r \in \mathbb{Q}$. Пусть $x^r = c$. Тогда $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)^r = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(c) = c^d$, значит $c = q^{\frac{r}{gcd(r,d)}}$, где $q \in \mathbb{Q}$, т. е. $x^{gcd(r,d)} \in \mathbb{Q}$, а значит $d = r$. $\text{Tr}_{K/\mathbb{Q}}(\alpha) = s \text{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = 0$ т. к.

минимальный многочлен $\alpha = x^r + c$. Деля равенство из условия на $\sqrt[k]{b_i}$ и применяя след, получаем $a_i = 0$.

Задача 9

Многочлен $\Phi(x) = x^{p-1} + x^{p-2} + \dots + 1$ неразложим по критерию Эйзенштейна. Действительно, $\Phi(x+1) = \frac{(x+1)^p - 1}{x+1-1} = x^{p-1} \pmod{p}$, при этом $\Phi(x+1) = x^{p-1} + \dots + p$. Значит $\{1, \xi, \dots, \xi^{p-2}\}$ — базис. $\text{Tr}(\xi^k) = -1$, при $p \nmid k$; $p-1$ — иначе. Итого:

$$\begin{aligned} \text{disc}\{1, \xi, \dots, \xi^{p-2}\} &= \det \begin{pmatrix} p-1 & -1 & -1 & \dots & -1 \\ -1 & -1 & -1 & \dots & -1 \\ -1 & -1 & -1 & \dots & p-1 \\ \dots & \dots & \dots & \dots & \dots \\ -1 & -1 & p-1 & \dots & -1 \end{pmatrix} = \\ &= \det \begin{pmatrix} 1 & 1-p & 1 & \dots & 1 \\ -1 & -1 & -1 & \dots & -1 \\ -1 & -1 & -1 & \dots & p-1 \\ \dots & \dots & \dots & \dots & \dots \\ -1 & -1 & p-1 & \dots & -1 \end{pmatrix} = \det \begin{pmatrix} 1 & 1-p & 1 & \dots & 1 \\ 0 & -p & 0 & \dots & 0 \\ 0 & -p & 0 & \dots & p \\ \dots & \dots & \dots & \dots & \dots \\ 0 & -p & p & \dots & 0 \end{pmatrix} = \\ &= (-1)^{\frac{p-1}{2}} p^{p-2} \end{aligned}$$

Алтернативное доказательство:

$$\begin{aligned} \text{disc}\{1, \xi, \dots, \xi^{p-2}\} &= \text{disc}_{\Phi} = \frac{\text{disc}_{x^p-1}}{\Phi(1)^2} = (-1)^{\frac{p(p-1)}{2}} \frac{\text{Res}(x^p - 1, px^{p-1})}{p^2} = \\ &= (-1)^{\frac{p-1}{2}} p^{p-2} (-1)^{p-1} = (-1)^{\frac{p-1}{2}} p^{p-2} \end{aligned}$$

Задача 10

Пусть $\{\sigma_i\}$ — различные вложения K над F в алгебраическое замыкание L , продолженные на алгебраическое замыкание, $\{\tau_j\}$ — различные вложения L над K . Тогда любое вложение L над F представляется единственным образом в виде $\sigma_i \tau_j$, т. к. если σ — вложение, найдётся i , т. ч. F неподвижно относительно $\sigma_i^{-1} \sigma$. Значит $\sigma_i^{-1} \sigma = \tau_j$ на L для какого-то j . Отсюда утверждение задачи получается группировкой членов суммы или произведения.

Задача 11

Из одной из предыдущих задач мы знаем, что степень расширения — 2^n , вложения переворачивают знак у произвольного подмножества порождающих. Действительно, добавляем корни по одному, на каждом шаге продолжаем вложение, либо переворачивая знак, либо оставляя. Эти вложения, очевидно различны и на сумме, т. к. порождающие линейно независимы, а значит степень расширения хотя бы 2^n . Отсюда расширения совпадают.

Задача 12

Пусть $F = \mathbb{F}_q$, $L = \mathbb{F}_{q^n}$, L/F — нормальное и сепарабельное, как разбивающее расширение многочлена $x^{q^n} - x$, не имеющего кратных корней (его производная равна -1), утверждается, что $\sigma(x) = x^q$ порождает группу Галуа. Действительно, σ — автоморфизм с периодом n , пусть его порядок равен d , тогда $X^{p^d} - X = 0$ для любого элемента L , следовательно, $d = n$.

Пусть ζ порождает мультипликативную группу L . $N(\zeta) = \zeta^{1+p+\dots+p^{n-1}} = \zeta^{\frac{p^n-1}{p-1}} \in F$, т. е. порядок образа ζ равен $p-1$. Значит он порождает мультипликативную группу F .

Задача 13

Минимальный, очевидно, делит $f(x) = \Phi_p(x^{p^{n-1}})$, но степень минимального равна $\varphi(p^n) = p^{n-1}(p-1)$, значит $f = \Phi_{p^n}$.

Задача 14

S_n — очевидно, разрешима, при $n < 4$. При $n = 4$ $\{id\} \subset V_4 \subset A_4 \subset S_4$ — искомая цепь. Пусть $n > 4$, тогда $[A_n, A_n] = A_n$. Действительно, $[(mik), (klj)] = (kim)(jlk)(mik)(klj) = (ijk)$, где все индексы различны. Но 3-циклы порождают A_n .

Задача 15

Пусть $x^2 + bx + a^2$ — минимальный многочлен β . Будем искать $c, d \in F$, т. ч. $c(\beta + d)^2 = \beta$. $c(-b\beta + 2\beta d - a^2 + d^2) = \beta$, т. е. $2cd - cb = 1$ и $a^2 = d^2$. Т. к. $a \neq 0$, и $\text{char } F \neq 2$, $2a - b$ или $-2a - b$ не равно 0. Итого $\beta = \frac{1}{-b+2a}(\beta + a)^2$, или $\beta = \frac{1}{-b-2a}(\beta - a)^2$, в зависимости от того, какой из знаменателей не равен 0.

Задача 16

Расширение сепарабельно, т. к. $\text{char } F \neq 2, 3$, и нормально, по определению. Будем рассматривать действие группы Галуа на корнях f , т. е. вложение в S_3 , т. к. образ корней однозначно задаёт автоморфизм. Если $\text{disc } F \in (F^*)^2$, $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ неподвижен относительно всех автоморфизмов, значит автоморфизмы допускают только чётные перестановки корней, при этом $3 \mid |G|$, значит $G = A_3$. Пусть теперь $G = A_3$, тогда G действует на корнях как A_3 , т. к. $2 \nmid |G|$, значит элемент $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \in F_f$ неподвижен, значит лежит в F .

Задача 17

Пусть L/K — циклическое расширение Галуа, σ — образующая, $\theta = \sqrt{x + y\sqrt{a}}$. Тогда $\sigma^2|_{K(\sqrt{a})} = \text{id}$, значит $\sigma^2(\theta) = -\theta$, при этом $\sigma(\theta) = \sqrt{x - y\sqrt{a}}$. Действительно, применим σ к равенству $\theta^2 = x + y\sqrt{a}$. Пусть $\alpha = \theta\sigma(\theta)$, тогда $\sigma(\alpha) = -\alpha$, в частности $\sigma^2(\alpha) = \alpha$, т. е. $\alpha \in K(\sqrt{a})$, значит $\alpha = z\sqrt{a}$, итого $\alpha^2 = x^2 - ay^2 = az^2$. В обратную сторону рассуждение полностью аналогично.

Задача 18

Пусть $H = \text{Gal}(F/K_1K_2)$, тогда, очевидно, $H = H_1 \cap H_2$, при этом $K_1K_2 = F^H$. Пусть теперь $H' = \text{Gal}(F/(K_1 \cap K_2))$, тогда $H_1, H_2 \subset H'$, но $K^{H_1H_2} \subset K^{H_1} \cap K^{H_2} = K_1 \cap K_2$, т. е. $H' \subset H_1H_2$, а значит $H' = H_1H_2$, по определению.

Задача 19

Рассмотрим действие $G = S_n$ на корнях, т. е. вложение $G \hookrightarrow \text{Perm}\{x_1, x_2, \dots, x_n\}$. Тогда образ A_n — нечётные перестановки корней. Действительно, при $n \geq 5$, $[S_n, S_n] = A_n$, при $n < 5$, 3-циклы переходят в 3-циклы и порождают A_n . Тогда $L^{A_n} = K(\sqrt{\Delta})$, где Δ — дискриминант f . Действительно, $\sqrt{\Delta}$ неподвижен относительно чётных перестановок корней и меняет знак под действием нечётных, при этом $[L^{A_n} : K] = 2$.

Задача 20

Рассмотрим многочлен $f(x) = x^4 - x + 1$. Он неприводим, т. к. у него нет корней и $x^4 - x + 1 = (x+1)(x^3 - x^2 + x + 1) \pmod{3}$, где последний неприводим по модулю 3, т. к. у него нет корней. Рассмотрим кубическую резольвенту f , $g(x) = x^3 - 4x + 1$. $g(x)$ неразложим, т. к. не имеет корней. При этом дискриминант g равен дискриминанту f , значит $\text{disc}_f = 256 - 27 = 229 \neq n^2$.

Итого, $12 \mid |G|$ и $G \neq A_4$, но $|G| \neq 12$. Действительно, ведь тогда подгруппа чётных перестановок G имеет порядок 6 и её действие на множестве из 4-х элементов разбивает его на 2 орбиты из 2 элементов, но в этой подгруппе есть элемент порядка 3. Противоречие. Отсюда, $G = S_4$.

Задача 21

$$\begin{aligned} g(x) &= (x - (x_1 + x_2)(x_3 + x_4))(x - (x_1 + x_3)(x_2 + x_4))(x - (x_1 + x_4)(x_2 + x_3)) = x^3 - \\ &\quad - 2\sigma_2 x^2 + (\sigma_{02} + 3\sigma_{21} + 6\sigma_4)x - (\sigma_{111} + 2\sigma_{301} + 2\sigma_{03} + 4\sigma_{22}) = x^3 - 2\sigma_2 x^2 + \\ &\quad + (\sigma_2^2 + \sigma_{21})x - (\sigma_3\sigma_2\sigma_1 - \sigma_{301} - \sigma_{03} - 4\sigma_{22}) = x^3 - 2\sigma_2 x^2 + (\sigma_2^2 + \sigma_3\sigma_1 - 4\sigma_4)x - \\ &\quad - (\sigma_3\sigma_2\sigma_1 - \sigma_4(\sigma_1^2 - 2\sigma_2) - (\sigma_3^2 - 2\sigma_4\sigma_2) - 4\sigma_2\sigma_2) = x^3 - 2\sigma_2 x^2 + (\sigma_2^2 + \sigma_3\sigma_1 - 4\sigma_4)x + \\ &\quad + \sigma_4\sigma_1^2 + \sigma_3^2 - \sigma_3\sigma_2\sigma_1 \end{aligned}$$

Задача 22

Минимальный многочлен σ равен $x^n - 1$, т. к. $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ линейно независимы, как попарно различные характеры. Рассмотрим гомоморфизм $\varphi : K[x] \rightarrow \text{End}_K(L)$, т. ч. $\varphi(x) = \sigma$. Ядро φ нетривиально, т. к. $\text{End}_K(L)$ конечномерно над K . Из структурной теоремы,

$$L \simeq \bigoplus_{i=1}^m K[x]/(f_i),$$

где $f_i \mid f_{i+1}$. Тогда f_m — минимальный многочлен, по определению. Но $\dim_K K[x]/(x^n - 1) = n$, значит $L \simeq K[x]/(x^n - 1)$. Тогда найдётся u , т. ч. $u, \sigma u, \sigma^2 u, \dots, \sigma^{n-1} u$ — базис L над K .

Задача 23

G — конечнопорождённая абелева, из структурной теоремы

$$G \simeq \mathbb{Z}^r \oplus \left(\bigoplus_{i=1}^n \mathbb{Z}/q_i \mathbb{Z} \right)$$

Рассмотрим $k[x, y] := k[x_1, x_1^{-1}, x_2, x_2^{-1}, \dots, x_r, x_r^{-1}, y_1, y_2, \dots, y_n]$. Пусть $I = (y_1^{q_1} - 1, y_2^{q_2} - 1, \dots, y_n^{q_n} - 1)$. Пусть теперь $\varphi : k[x, y] \rightarrow G$, т. ч. $p_j(\varphi(x_i)) = \delta_{ij}$, $p_{j+r}(\varphi(y_i)) = \delta_{ij}$, тогда $I \subset \ker \varphi$, значит определено $\psi : k[x, y]/I \rightarrow G$. ψ , очевидно, изоморфизм, т. к. переводит разные мономы в разные.

Задача 24

Пусть π_1 и π_2 — соответствующие проекции, i_1 и i_2 — соответствующие вложения. Тогда $\pi_1 \circ i_1 = id$, $\pi_2 \circ i_2 = id$, $\pi_2 \circ i_1 = 0$, $\pi_1 \circ i_2 = 0$ и $i_1 \circ \pi_1 + i_2 \circ \pi_2 = id$. Все эти равенства сохраняются при применении тензорного произведения. Отсюда $(M \oplus N) \otimes P$ — прямая сумма $M \otimes P$ и $N \otimes P$.

Задача 25

$(f, w) \mapsto (v \mapsto f(v)w)$, очевидно, билинейно, значит определено $\varphi : f \otimes w \mapsto (v \mapsto f(v)w)$. Пусть $\{v_1, v_2, \dots, v_n\}$ — базис V , $\{w_1, w_2, \dots, w_m\}$ — W , тогда $\{v^i \otimes w_j\}_{i,j}$ — базис $V^* \otimes W$. Пусть $u = \sum_{i,j} a_{ij} v^i \otimes w_j \in \ker \varphi$. Тогда $0 = \varphi(u)(v_i) = \sum_j a_{ij} w_j$, по определению двойственного базиса. Тогда все $a_{ij} = 0$. Пусть теперь $f \in \text{Hom}(V, W)$, тогда $f = \varphi(\sum_i e^i \otimes f(e_i))$. Итого, ϕ — изоморфизм.

Задача 25

$$\begin{array}{ccccccc} M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow d' & & \downarrow d & & \downarrow d'' \\ 0 & \longrightarrow & N' & \xrightarrow{f} & N & \xrightarrow{g} & N'' \end{array}$$

Утверждается, что $\delta : \ker d'' \rightarrow \text{coker } d'$, т. ч. $\delta = f^{-1} \circ d \circ g^{-1}$ корректно определён и последовательность

$$\ker d' \longrightarrow \ker d \xrightarrow{g^*} \ker d'' \xrightarrow{\delta} \text{coker } d' \xrightarrow{f^*} \text{coker } d \longrightarrow \text{coker } d''$$

точна. Действительно, $f^{-1} \circ d \circ g^{-1} m'' = f^{-1} \circ d(m + \ker g) = f^{-1} \circ d(m + \text{Im } f) = f^{-1}(n + \text{Im } d \circ f) = f^{-1}(n + \text{Im } f \circ d') = n' + \text{Im } d'$. Здесь $f^{-1}(n)$ определено, т. к. $g(n) = 0$ из коммутативности диаграммы. Точность в $\ker d$ и $\text{coker } d$ очевидна. Докажем точность в $\ker d''$. Вложение $\text{Im } g^* \subseteq \ker \delta$ сразу следует из инъективности $f : N' \rightarrow N$ и определения δ . Пусть теперь m'' оказался в ядре, тогда $n' = d'x$. Отсюда $d(f(x) - m) = d \circ f x - n = f \circ d'x - n = 0$, но $g(f(x) - m) = m''$, значит $m'' \in g^*$. Проверим точность в $\text{coker } d'$. Вложение $\text{Im } \delta \subseteq \ker f^*$ очевидно из определения δ . Пусть теперь $f(n') = d(x)$, тогда $n' - \delta \circ g x \in \text{Im } d'$ из инъективности $f : N' \rightarrow N$. Итого, получаем диаграмму

$$\begin{array}{ccccccc}
& \ker d' & \longrightarrow & \ker d & \longrightarrow & \ker d'' & \\
& \downarrow & & \downarrow & & \downarrow & \\
& M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow 0 \\
& \downarrow & & \downarrow & & \downarrow & \\
0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' \\
& \downarrow & & \downarrow & & \downarrow & \\
& \text{coker } d' & \longrightarrow & \text{coker } d & \longrightarrow & \text{coker } d'' &
\end{array}$$

A commutative diagram showing a sequence of maps between kernels and cokernels. The top row consists of $\ker d' \rightarrow \ker d \rightarrow \ker d''$. The middle row consists of $M' \rightarrow M \rightarrow M'' \rightarrow 0$. The bottom row consists of $0 \rightarrow N' \rightarrow N \rightarrow N''$. The bottom-most row consists of $\text{coker } d' \rightarrow \text{coker } d \rightarrow \text{coker } d''$. Vertical arrows point down from each of the first five terms: $\ker d' \rightarrow M' \rightarrow N' \rightarrow \text{coker } d'$, $\ker d \rightarrow M \rightarrow N \rightarrow \text{coker } d$, and $\ker d'' \rightarrow M'' \rightarrow N'' \rightarrow \text{coker } d''$. A horizontal arrow points from 0 to N' . A curved arrow connects the 0 on the left to the 0 on the right, passing above the $N' \rightarrow N \rightarrow N''$ sequence.