Алгебра 7: матрицы и определители

В этом листке предполагается, что все векторные пространства заданы над полем k.

Задача 7.1. Пусть $v_1, \dots, v_n \in V$, $w_1, \dots, w_m \in W$ – базисы в векторных пространствах V и W. Рассмотрим гомоморфизм e_i^j из V в W, переводящий v_i в w_j, все остальные v_i в ноль. Докажите, что e_j^i задают базис в пространстве гомоморфизмов $\operatorname{Hom}(V, W)$.

Определение 7.1. В условиях предыдущей задачи, пусть задан гомоморфизм $\gamma \in \operatorname{Hom}(V, W)$. Запишем $\gamma = \gamma_j^i e_j^i$, $\gamma_j^i \in k$. Матрица

$$\begin{pmatrix} \gamma_1^1 & \dots & \gamma_n^1 \\ \vdots & \ddots & \vdots \\ \gamma_1^m & \dots & \gamma_n^m \end{pmatrix}$$

называется **матрицей гомоморфизма** γ.

Задача 7.2. Даны гомоморфизмы $a \in \operatorname{Hom}(U, V)$, $b \in \operatorname{Hom}(V, W)$. с матрицами (a_j^i), (b_l^k). Докажите, что композиция a и b задается матрицей $c_k^i = \sum_j a_j^i b_k^j$.

Замечание. Заметим, что формула произведения матриц имеет смысл также и для матриц с элементами из произвольного кольца.

Задача 7.3. Рассмотрим пространство A квадратных матриц $n \times n$, с умножением $A \times A \longrightarrow A$, которое задается по формуле $(a_j^i) \circ (b_l^k) \longrightarrow \sum_j a_j^i b_k^j$. Докажите, что это алгебра с единицей. Докажите, что эта алгебра изоморфна алгебре линейных операторов из k^n в k^n.

Определение 7.2. Эта алгебра называется **алгеброй матриц**, обозначается $\operatorname{Mat}(n)$. Единица этой матрицы (диагональная матрица с $a_i^i = 1$) называется **единичной матрицей**, обозначается Id.

Задача 7.4. Пусть дан линейный оператор $f \in \operatorname{Hom}(V, V)$, $v_1, \dots, v_n$ – базис в V, а (f_j^i) – матрица f. Пусть задан другой базис $v_1', \dots, v_n'$ в V. Докажите, что существует единственный оператор g, переводящий v_i в v_i', и g обратим. Запишем g, g^{-1} матрицами (g_j^i), $((g^{-1})_j^i)$ Докажите, что f записывается в базисе $v_1', \dots, v_n'$ матрицей $h_j^i := (g_j^i) \circ (f_j^i) \circ ((g^{-1})_j^i)$.

Определение 7.3. В такой ситуации, говорится, что матрицы (h_j^i), (f_j^i) **эквивалентны**.

Задача 7.5. Найдите все матрицы, эквивалентные $c\,\mathsf{Id}$, где $c \in k$

Задача 7.6 (!). Пусть $E(i, j)$ - матрица

$$\begin{pmatrix} 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix},$$

у которой на i, j-м месте стоит 1, а на всех остальных местах – 0. Для каких i, j, i', j', матрицы $E(i, j)$ и $E(i', j')$ эквивалентны?

Задача 7.7 (!). Пусть A – матрица, эквивалентная $E(i,j)$. Докажите, что все строки A пропорциональны. Докажите, что все столбцы A пропорциональны.

Задача 7.8 (*). Докажите, что если все строки и столбцы A пропорциональны, то A эквивалентна $E(i,j)$.

Определение 7.4. Пусть V – векторное пространство, $A \in \operatorname{End}(V)$ – его эндоморфизм (т.е. гомоморфизм из V в себя), а V^* – двойственное пространство. Рассмотрим оператор $A^* : V^* \longrightarrow V^*$, отображающий линейный функционал $\gamma \in V^*$ в функционал $A^*(\gamma)(v) = \gamma(A(v))$ Оператор A^* называется **сопряженным оператором** для A.

Задача 7.9. Пусть V – конечномерное векторное пространство, V^* двойственное пространство. Постройте естественный изоморфизм между $\Lambda^k(V)^*$ и $\Lambda^k(V^*)$.

Замечание. "Естественный" значит: не требующий дополнительного выбора (выбора базиса, например). В подобной ситуации, естественный изоморфизм $\Lambda^k(V)^* \cong \Lambda^k(V^*)$ перестановочен с стандартным действием $GL(V)$ на $\Lambda^k(V)^*$, $\Lambda^k(V^*)$. Пространства V и V^* изоморфны, но можно доказать, что не существует $GL(V)$-инвариантного изоморфизма $V \cong V^*$. Иначе говоря, построить естественный изоморфизм $V \cong V^*$ *нельзя.*

Задача 7.10 (!). Пусть V – векторное пространство, $A \in \operatorname{End}(V)$ – его эндоморфизм, а A^* – сопряженный оператор к A. Докажите, что $\det A^* = \det A$

Указание. Воспользуйтесь предыдущей задачей.

Определение 7.5. Пусть дана квадратная матрица (A^i_j), а (B^i_j) получена из (A^i_j) отражением относительно диагонали: $B^i_j = A^j_i$. Тогда (B^i_j) называется **транспонированной матрицей** для (A^i_j), и обозначается через $(A^i_j)^\perp$.

Задача 7.11 (!). Пусть $v_1, \ldots, v_n$, – базис в V, а $v^1, \ldots, v^n$ – двойственный базис в V^* (v^i отображает v_i в 1, все остальные v_j в ноль). Рассмотрим оператор $A \in \operatorname{End}(V)$ и его матрицу (A^i_j). Докажите, что A^* задается матрицей $(A^i_j)^\perp$.

Определение 7.6. Пусть на векторном пространстве V задана невырожденная билинейная симметрическая форма g. Оператор $A \in \operatorname{End}(V)$ называется **ортогональным относительно** g (или просто ортогональным) тогда и только тогда, когда $g(Av, Av) = g(v, v)$, для любого $v \in V$.

Задача 7.12 (!). Докажите, что ортогональный оператор всегда обратим.

Задача 7.13 (!). Пусть $A \in \operatorname{End}(V)$ – линейный оператор на векторном пространстве, наделенном невырожденной билинейной симметрической формой g. Используя g, отождествим V и V^*. Тогда двойственный оператор A^* можно рассматривать как эндоморфизм V. Докажите, что линейный оператор A ортогонален тогда и только тогда, когда $A^{-1} = A^*$.

Задача 7.14 (!). Докажите, что определитель ортогонального оператора равен ± 1.

Определение 7.7. Невырожденная билинейная кососимметрическая форма (см. листок Алгебра 3) называется **симплектической**.

Задача 7.15 (*). Пусть V – векторное пространство с заданной на нем симплектической формой ω. Оператор $A \in \mathrm{End}(V)$ называется **симплектическим**, если он сохраняет ω, т.е., если $\omega(Av, Av) = \omega(v, v)$. Докажите, что симплектический оператор всегда имеет определитель 1.

Задача 7.16 (!). Пусть V двумерное векторное пространство над $\mathbb{R}$, а A – матрица

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Рассмотрим матрицу

$$A' = \begin{pmatrix} d & b \\ -c & a \end{pmatrix}.$$

Докажите, что $AA' = \Delta \, \mathsf{Id}$, где $\Delta \in k$ – число, равное $\Delta = ad - bc$. Докажите, что A обратима тогда и только тогда, когда $\Delta \neq 0$.

Задача 7.17 (!). В условиях предыдущей задачи, докажите, что Δ равно определителю A.

Задача 7.18. Пусть V – двумерное векторное пространство над $\mathbb{R}$ с положительно определенной билинейной симметрической формой, A – ортогональный оператор, и пусть его матрица записывается в ортогонормированном базисе как

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Из задачи 7.14 следует, что $\det A = \pm 1$.

а. Пусть $\det A = 1$. Докажите, что $b = -c$, $a = d$, и $a^2 + b^2 = 1$.

б. Пусть $\det A = -1$. Докажите, что $b = c$, $a = -d$, и $a^2 + b^2 = 1$.

Задача 7.19 (*). Используя предыдущую задачу, опишите группу движений плоскости, сохраняющих начало координат, в терминах матриц 2 на 2. Докажите, что это диэдральная группа (см. листок Алгебра 1).

Определение 7.8. Пусть дана матрица (A^i_j). Мы говорим, что матрица (B^i_j) получена из (A^i_j) **преобразованием Гаусса по строкам**, если $(B^i_j) = (A^i_j) \circ E$, где E это матрица такого вида:

$$\begin{pmatrix}
1 & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
. \;\; 1 & \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots \; 0 \; \ldots \; 1 \; \ldots\ldots \\
\vdots \; \vdots \; \vdots \; \vdots \; \ddots \; \vdots \; \vdots \; \vdots \; \vdots \\
\ldots\ldots \; 1 \; \ldots \; 0 \; \ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots \; 1 \;\; . \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \; 1
\end{pmatrix}, \tag{7.1}$$

либо такого:

$$\begin{pmatrix}
1 & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
. \;\; 1 & \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\; 1 & \ldots \;\; \lambda \;\; \ldots\ldots \\
\vdots \;\; \vdots \;\; \vdots \;\; \vdots & \ddots \;\; \vdots \;\; \vdots \;\; \vdots \;\; \vdots \\
\ldots\ldots\; 0 & \ldots \;\; 1 \;\; \ldots\ldots \\
\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots \;\; 1 \;\; . \\
\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots \;\; 1
\end{pmatrix} \tag{7.2}$$

(точками обозначаются нули). Если $(B_j^i) = E \circ (A_j^i)$, где E такие же, как выше, то говорят, что (B_j^i) получена из (A_j^i) **преобразованием Гаусса по столбцам**.

Задача 7.20. Докажите, что преобразования Гаусса по строкам описываются следующими операциями на матрицах: (B_j^i) получается из (A_j^i) перестановкой строк, либо добавлением к i-й строке j-й строки, почленно умноженной на λ. Какими операциями описываются преобразования Гаусса по столбцам?

Задача 7.21. Докажите, что матрица вида (7.1) имеет определитель -1, а матрица вида (7.2) имеет определитель 1.

Задача 7.22 (!). Докажите, что преобразования Гаусса вида (7.2) не меняют определитель матрицы, а преобразования вида (7.1) умножают его на -1.

Определение 7.9. Матрица (A_j^i) называется **верхнетреугольной**, если $A_j^i = 0$ при $i < j$:

$$\begin{pmatrix}
* & * & * & \ldots & * & * & * \\
0 & * & * & \ldots & * & * & * \\
0 & 0 & * & \ldots & * & * & * \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & * & * & * \\
0 & 0 & 0 & \ldots & 0 & * & * \\
0 & 0 & 0 & \ldots & 0 & 0 & *
\end{pmatrix}.$$

Матрица называется **диагональной**, если $A_j^i = 0$ при $i \neq j$.

Задача 7.23 (!). Пусть (A_j^i) – верхнетреугольная матрица $n \times n$. Докажите, что $\det(A_j^i)$ равен произведению всех диагональных коэффициентов:

$$\det(A_j^i) = \prod_i A_i^i.$$

Задача 7.24. а. Докажите, что преобразованиями Гаусса по строкам любую матрицу можно привести к верхнетреугольному виду.

б. Докажите, что преобразованиями Гаусса по строкам и по столбцам любую матрицу можно привести к диагональному виду.

Замечание. Поскольку преобразования Гаусса не меняют определителя (с точностью до ± 1), определитель квадратной матрицы можно вычислить, приведя ее к верхнетреугольному виду и перемножив диагональные коэффициенты.

Задача 7.25 (*). Пусть A – кольцо с алгоритмом Евклида (см. листок Алгебра 2), и пусть у любого элемента $a \in A$ существует разложение на простые сомножители. Решите задачу 7.24 для матриц с элементами из A.

Указание. Сначала рассмотрите матрицы (a^i_j) размера 1×2, потом по индукции матрицы размера $1 \times n$ (и тем самым $n \times 1$). Докажите к тому же, что после приведения единственный оставшийся ненулевой элемент матрицы будет равен НОД$(a^1_1, \dots, a^1_n)$. Для матрицы произвольного размера $m \times n$, переставьте сначала строки и столбцы так, чтобы a^1_1 стало ненулевым. В пункте (б) затем, применяя преобразования по строкам, потом по столбцам, потом вновь по строкам, и так далее, добейтесь того, что $a^1_1 \neq 0$, и в то же время все остальные элементы первого столбца и первой строки равны нулю.

Грассманова алгебра и миноры матриц

Задача 7.26 (!). Пусть $v_1, \dots, v_n$ – базис векторного пространства V, а $v_{i_1} \wedge v_{i_2} \wedge \dots \wedge v_{i_k}$, $i_1 < i_2 < \dots < i_k$ – соответствующий базис в $\Lambda^k(V)$. Рассмотрим матрицу $A \in \operatorname{End} V$, и пусть $A(i_1, i_2, \dots, i_k; i'_1, i'_2, \dots i'_k)$ – коэффициенты матрицы эндоморфизма, индуцированного A на $\Lambda^k(V)$, в вышеописанном базисе. Докажите, что $A(i_1, i_2, \dots, i_k; i'_1, i'_2, \dots, i'_k)$ это определитель матрицы, полученной из A выкидыванием всех строк, кроме i_1-й, i_2-й, ... , i_k-й, и всех столбцов, кроме i'_1-го, i'_2-го, ... , i'_k-го.

Замечание. Такой определитель называется **минором** матрицы A.

Указание. Взяв композицию A с оператором, который переводит v_{i_l} в $v_{i'_l}$, сведите задачу к случаю $i_l = i'_l$. Докажите, что коэффициенты $A(i_1, i_2, \dots, i_k; i'_1, i'_2, \dots, i'_k)$ не зависят от строк, кроме i_1-й, i_2-й, ... , i_k-й, и столбцов, кроме i'_1-го, i'_2-го, ... , i'_k-го, и положите $A^i_j = 0$, если i и j не принадлежат $\{i_1, i_2, \dots, i_k\}$. Это сводит задачу к случаю, когда $V = V_1 \oplus V_2$, а A имеет вид $B \oplus 0_{V_2}$, где $B \in \operatorname{End}(V_1)$, а 0_{V_2} действует нулем на V_2. В этой ситуации можно применить формулу $\Lambda^*(V) = \Lambda^*(V_1) \otimes \Lambda^*(V_2)$, и получить искомое.

Определение 7.10. Пусть $A \in \operatorname{End}(V)$ – линейный оператор. Рассмотрим эндоморфизм, который индуцируется A на $\Lambda^*(V)$. Рассмотрим самое большое число N, для которого этот эндоморфизм не равен нулю на $\Lambda^N(V)$. Это число N называется **рангом линейного оператора** A (записывается $\operatorname{rk} A$). Если A выражается матрицей (A^i_j), то $\operatorname{rk} A$ называется рангом этой матрицы.

Задача 7.27 (!). Пусть A действует нулем на $\Lambda^k(V)$. Докажите, что A действует нулем на $\Lambda^l(V)$, для любого $l > k$.

Задача 7.28. Докажите, что ранг матрицы – это размер ее самого большого ненулевого минора.

Задача 7.29. Докажите, что ранг оператора A равен самому большому числу N, для которого найдутся такие вектора $v_1, \dots, v_N$, что $A(v_1), \dots, A(v_N)$ линейно независимы.

Задача 7.30 (!). Докажите, что ранг оператора A равен размерности его образа.

Задача 7.31. Пусть задана матрица ранга 1. Докажите, что все ее строки пропорциональны. Докажите, что все ее столбцы пропорциональны.

Задача 7.32. Докажите, что $\operatorname{rk} A = \operatorname{rk} A^*$.

Указание. Воспользуйтесь задачей 7.9.

Определение 7.11. Билинейная форма $\mu : \quad V_1 \otimes V_2 \longrightarrow k$ называется **невырожденным спариванием**, если для каждого ненулевого $v_1 \in V_1$ найдется такой вектор $v_1' \in V_2$, что $\mu(v_1, v_1') \neq 0$, и для каждого ненулевобо $v_2 \in V_2$ найдется такой вектор $v_2' \in V_1$, что $\mu(v_2, v_2') \neq 0$.

Задача 7.33. Пусть V_1, V_2 конечномерны. Докажите, что невырожденное спаривание $\mu : V_1 \otimes V_2 \longrightarrow k$ задает изоморфизм между V_1 и V_2^*, и любой изоморфизм между этими пространствами задается таким образом.

Задача 7.34 (!). Пусть V – n-мерное векторное пространство. Постройте естественный изоморфизм

$$\Lambda^k(V)^* \cong \Lambda^{n-k}(V) \otimes \det V^*$$

(через $\det V$ обозначается одномерное пространство $\Lambda^n(V)$).

Указание. Воспользуйтесь предыдущей задачей.

Задача 7.35. Пусть V – n-мерное векторное пространство с базисом $v_1, v_2, \ldots, v_n$, и дано $A \in \operatorname{End} V$. Рассмотрим базис $w_1, w_2, \ldots, w_n$ в $\Lambda^{n-1}(V)$, где $w_k = v_1 \wedge v_2 \wedge \ldots v_{k-1} \wedge v_{k+1} \wedge \ldots$ (перемножаются все v_i, кроме одного). Запишем A матрицей (A_j^i), и пусть $\check{A}_j^i$ – минор, полученный из A выкидыванием i-й строки и j-го столбца. Докажите, что A действует на $\Lambda^{n-1}(V)$ матрицей $(\check{A}_j^i)$.

Задача 7.36. В условиях предыдущей задачи, рассмотрим невырожденное билинейное спаривание

$$V \otimes \Lambda^{n-1}(V) \longrightarrow \det V,$$

заданное формулой $v \otimes w \longrightarrow v \wedge w$. Выберем изоморфизм $k \cong \det V$ таким образом, что $v_1 \wedge v_2 \wedge \cdots \wedge v_n$ переходит в 1. Это задает невырожденное спаривание между V и $\Lambda^{n-1}(V)$. Докажите, что базис в $\Lambda^{n-1}(V)$, двойственный к $v_1, v_2, \ldots, v_n$, равен $w_1, -w_2, w_3, -w_4, \ldots$. Докажите, что в этом базисе A действует на $\Lambda^{n-1}(V)$ матрицей $((-1)^{i+j} \check{A}_j^i)$.

Задача 7.37. Пусть $\mu : \ V \otimes V' \longrightarrow k$ – невырожденное билинейное спаривание, а $A \in \operatorname{End} V$ и $B \in \operatorname{End} V'$ – такие эндоморфизмы, что $\mu(Av, Bv') = \mu(v, v')$ для любых $v, v' \in V, V'$. Выберем двойственные базисы в V, V', и пусть (α_j^i) и (β_j^i) – их матрицы. Докажите, что $(\alpha_j^i) \circ (\beta_j^i)^\perp = \mathsf{Id}$.

Задача 7.38 (!). Пусть $A \in \operatorname{End} V$, где V – n-мерное векторное пространство с базисом $v_1, v_2, \ldots, v_n$, а (A_j^i) – матрица оператора A. Докажите, что A обратим тогда и только тогда, когда $\det A \neq 0$. Докажите, что

$$A^{-1} = \frac{1}{\det A}((-1)^{i+j} \check{A}_j^i)^\perp.$$

Указание. Докажите, что для естественного спаривания

$$V \otimes \Lambda^{n-1}(V) \xrightarrow{\mu} \det V,$$

мы имеем $\mu(A(v), A(w)) = \det A \mu(v, w)$, где $A(w)$ обозначает естественное действие A на $\Lambda^{n-1}(V)$. Затем воспользуйтесь предыдущей задачей для $(A_j^i) = (\alpha_j^i)$, $\frac{1}{\det A}((-1)^i \check{A}_j^i) = (\beta_j^i)^\perp$.

Замечание. Мы получили хорошо известную формулу вычисления обратной матрицы через миноры. Геометрический смысл этой формулы можно объяснить так – миноры матрицы суть (по определению) матричные коэффициенты действия этой матрицы на $\Lambda^{n-1}(V)$, а естественное спаривание между V и $\Lambda^{n-1}(V)$ при действии A умножается на $\det A$, что позволяет вычислить A^{-1} через $\det A$ и $\check{A}$.

Вычисление определителя

Задача 7.39 (!). Пусть (A^i_j) – матрица линейного оператора A. Докажите, что $\det A$ равен

$$\sum_{\sigma\in S_n} \mathsf{sgn}(\sigma) A^1_{\sigma_1} A^2_{\sigma_2} \dots A^n_{\sigma_n}$$

где $(\sigma_1, \sigma_2, \dots, \sigma_n) \in S_n$ – перестановка, суммирование происходит по группе всех перестановок, а sgn – снак перестановки σ.

Указание. Воспользуйтесь явной формой тензора $v_1 \wedge v_2 \wedge \dots \wedge v_n$, который выписан в листке Алгебра 6 через суммирование по группе S_n.

Замечание. Обыкновенно детерминант определяют посредством этой формулы.

Задача 7.40. Пусть (A^i_j) матрица линейного оператора A. Докажите, что $\det A$ может быть вычислен как

$$A^1_1 \check{A}^1_1 - A^1_2 \check{A}^1_2 + A^1_3 \check{A}^1_3 \dots$$

где $\check{A}^i_j$ – миноры, полученные выкидыванием i-й строки и j-го столбца.

Замечание. Эта процедура называется **разложением определителя по столбцам**.

Задача 7.41 (*). (определитель Вандермонда) Рассмотрим матрицу

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ t_1 & t_2 & t_3 & \dots & t_n \\ t_1^2 & t_2^2 & t_3^2 & \dots & t_n^2 \\ \dots & \dots & \dots & \dots & \dots \\ t_1^{n-1} & t_2^{n-1} & t_3^{n-1} & \dots & t_n^{n-1} \end{pmatrix},$$

$n > 1$. Докажите, что ее определитель равен $\prod_{i<j}(t_i - t_j)$.

Задача 7.42 (*). Рассмотрим матрицу

$$\begin{pmatrix} t & x_1 & x_2 & x_3 & \dots & x_n \\ t^2 & x_1^2 & x_2^2 & x_3^2 & \dots & x_n^2 \\ t^4 & x_1^4 & x_2^4 & x_3^4 & \dots & x_n^4 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ t^{2^n} & x_1^{2^n} & x_2^{2^n} & x_3^{2^n} & \dots & x_n^{2^n} \end{pmatrix},$$

и обозначим ее детерминант через $P_n(t, x_1, ...x_n)$. Пусть основное поле равно $\mathbb{Z}/2\mathbb{Z}$. Докажите, что $P_n(t, x_1, \dots, x_n)$ обращается в ноль, если взять в качестве $t = \sum \alpha_i x_i$ произвольную линейную комбинацию x_i. Выведите из теоремы Безу, что

$$P_n(t, x_1, \dots, x_n) = Q(x_1, \dots, x_n) \prod (t - \sum \alpha_i x_i),$$

где $\alpha_i \in \mathbb{Z}/2\mathbb{Z}$, а $Q \in \mathbb{Z}/2\mathbb{Z}[x_1, \dots, x_n]$ есть некий полином.

Указание. Разделите P_n в столбик на $t - \sum \alpha_i x_i$. Если получится не ноль, то и при подстановке в $P(t)$ значения $t = \sum \alpha_i x_i$ тоже будет не ноль.

Задача 7.43 (*). Докажите, что в условиях предыдущей задачи $Q = P_{n-1}(x_n)$.

Задача 7.44 (*). Выведите из предыдущей задачи, что $Q(x_1, \ldots, x_n) \neq 0$.

Задача 7.45 (*). (теорема Диксона) Рассмотрим полином

$$F_n(t) = \prod (t - \sum \alpha_i x_i) \in \mathbb{Z}/2\mathbb{Z}[x_1, \ldots, x_n].$$

Докажите, что

$$F_n(t) = t^{2^n} + \sum_{i=0}^{n-1} c_{n,i} t^{2^i},$$

где $c_{n,i} \in \mathbb{Z}/2\mathbb{Z}[x_1, \ldots, x_n]$ – полиномы от $x_1, \ldots, x_n$.

Указание. Воспользуйтесь предыдущей задачей и задачей 7.42.

Замечание. Полиномы $c_{n,i} \in \mathbb{Z}/2\mathbb{Z}[x_1, \ldots, x_n]$ называются **инвариантами Диксона**.

Задача 7.46 (*). Рассмотрим коэффициенты Q_r (равные, по теореме Диксона, $c_{n,i}$) полинома $F_n(t)$ как элементы симметрической алгебры $S^*(V)$, где V - векторное пространство над полем $\mathbb{Z}/2\mathbb{Z}$ с базисом $x_1, \ldots, x_n$. Рассмотрим действие группы $GL(V)$ обратимых линейных операторов на V, и продолжим его естественным образом (по мультипликативности) на симметрическую алгебру. Докажите, что Q_r инвариантен относительно $GL(V)$:

$$Q_r(x_1, x_2, \ldots, x_n) = Q_r(h(x_1), h(x_2), \ldots, h(x_n))$$

где $h \in GL(V)$ – любой обратимый эндоморфизм.

Замечание. Рассмотрим в кольце полиномов $S^*(V)$ подкольцо $GL(V)$-инвариантных полиномов. Диксон (1911) доказал, что это кольцо есть кольцо полиномов от образующих $c_{n,i}$. Подробности см. в статье

A PRIMER ON THE DICKSON INVARIANTS, Contemporary Mathematics 19 (1983), 421-434. `http://www.math.purdue.edu/~ wilker/papers/dickson.pdf`