Алгебра — I

Листок 0

Под “кольцом” в этом листке понимается коммутативное ассоциативное кольцо с единицей.

(1) (a) Докажите, что для любых двух элементов a, b кольца A уравнение $x + b = a$ имеет единственное решение. (Это решение обозначается $a - b$.)
(b) Докажите, что для любых элементов a и $b \neq 0$ поля $\Bbbk$ уравнение $bx = a$ имеет единственное решение. (Это решение обозначается a/b.)
(c) Докажите, что для любого элемента a кольца A выполнено равенство $0 \cdot a = 0$.
(d) Докажите, что для любого элемента a кольца A выполнено равенство $(-1) \cdot a = -a$.

(2) (a) Постройте поле из 3 элементов.
(b) Постройте поле из 5 элементов.
(c) Постройте поле из 4 элементов.
(d) Существует ли поле из 6 элементов?

(3) Раскройте скобки у $(a_1 + \dots + a_m)^2$ и $(a + b + c)^3$.

(4) Чему равен коэффициент при $a_1^{k_1} \dots a_m^{k_m}$ после раскрытия скобок и приведения подобных членов в выражении $(a_1 + \dots + a_m)^n$?

(5) Вычислите:
(a) $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n}$;
(b) $\binom{n}{0} - \binom{n}{1} + \dots + (-1)^n \binom{n}{n}$;
(c) $\binom{n}{0}^2 + \binom{n}{1}^2 + \dots + \binom{n}{n}^2$;
(d) $\binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \binom{n}{6} + \dots$;
(e) $\binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \dots$.

(6) Выразите $\sin^4 x$ и $\cos^5 x$ через первые степени $\sin$ и $\cos$ от кратных аргументов.

(7) Выразите $\cos nx$ и $\sin nx$ через $\cos x$ и $\sin x$.

(8) Вычислите:
(a) $\sin x + \sin 2x + \dots + \sin nx$;
(b) $\sin^2 x + \sin^2 3x + \dots + \sin^2(2n-1)x$;
(c) $\cos x + 2\cos 2x + \dots + n \cos nx$.

(9) Найдите модуль и аргумент следующих комплексных чисел:

$$-4, \quad 1+i, \quad 1 - i\sqrt{3}, \quad \sin\alpha + i\cos\alpha, \quad \frac{1 + i\operatorname{tg}\alpha}{1 - i\operatorname{tg}\alpha}, \quad 1 + \cos\alpha + i\sin\alpha.$$

(10) Вычислите

$$\frac{(5+i)(7-6i)}{3+i}; \quad \frac{(1+i)^5}{(1-i)^3}; \quad \frac{(1+3i)(8-i)}{(2+i)^2}.$$

(11) Найдите x и y, считая их вещественными:

$$(1+2i)x + (3-5i)y = 1 - 3i.$$

(12) Решите уравнения:

$$z^2 = i; \qquad z^2 = 5 - 12i; \qquad z^2 + (2i-7)z + 13 - i = 0.$$

(13) Найдите все z:

$$\bar{z} = z^2; \qquad \bar{z} = z^3.$$

(14) Вычислите

$$(1 + i\sqrt{3})^{150}; \qquad \left(\frac{\sqrt{3}+i}{1-i}\right)^{30}; \qquad (1 + \cos\alpha + i\sin\alpha)^k.$$

Алгебра — I

Листок 1

(1) Пусть $V \subset \mathbb{R}^n$ - множество всех векторов, сумма координат которых равна 0.
  (a) Докажите, что V является векторным подпространством в $\mathbb{R}^n$
  (b) Найдите размерность V, укажите какой-нибудь базис.

(2) Докажите, что система линейных уравнений $AX = B$ с трехдиагональной квадратной матрицей коэффициентов

$$A = \begin{pmatrix} -2 & 1 & 0 & \dots & 0 \\ 1 & -2 & 1 & \dots & 0 \\ 0 & 1 & -2 & \dots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \dots & -2 \end{pmatrix}$$

имеет единственное решение в вещественных числах при любой правой части B.

(3) Сколько всего в n-мерном векторном пространстве над полем из q элементов
  (a) векторов?
  (b) упорядоченных наборов из k линейно независимых векторов?
  (c) k-мерных подпространств?

(4) (a) Докажите, что в любом конечном поле есть подполе из p элементов, где p — некоторое простое число.
  (b) Докажите, что число элементов любого конечного поля является степенью простого числа.

(5) Пусть векторное пространство $V \subset \mathbb{k}[x]$ содержит по многочлену каждой из степеней $d = 0, 1, \dots, m$. Верно ли, что оно содержит все многочлены степени $\leqslant m$?

(6) Пусть $\mathbb{k} \subset \mathbb{F}$ — два поля, и $\mathbb{F}$ конечномерно как векторное пространство над $\mathbb{k}$. Обязательно ли любой элемент поля $\mathbb{F}$ является корнем некоторого ненулевого многочлена из $\mathbb{k}[x]$?

(7) Дано несколько разных точек $p_0, p_1, \dots, p_m \in \mathbb{k}$. Постройте в пространстве $\mathbb{k}[x]_{\leqslant m}$ многочленов от x степени $\leqslant m$ базис, координатами многочлена f в котором являются значения $f(p_i)$.

(8) Производной многочлена $f(x) = \sum\limits_{k=0}^{n} a_k x^k$ над полем $\mathbb{k}$ называется многочлен $f'(x) = \sum\limits_{k=1}^{n} k a_k x^{k-1}$. Постройте в пространстве $\mathbb{k}[x]_{\leqslant m}$ многочленов от x степени $\leqslant m$ базис, координатами многочлена f в котором являются значения производных $f^{(k)}(p)$ для некоторой фиксированной точки $p \in \mathbb{k}$ и $k = 0, 1, \dots, m$.

(9) Пусть V — множество всех подмножеств некоторого множества M. Для $X, Y \in V$ определим их сумму как симметрическую разность $X \triangle Y = (X \cup Y) \setminus (X \cap Y)$. Кроме того, для $X \in V$ положим $0 \cdot X = \varnothing$ и $1 \cdot X = X$, где $0, 1$ — соответственно, ноль и единица поля $\mathbb{F}_2$ из двух элементов.
  (a) Докажите, что таким образом на V определена структура векторного пространства над полем $\mathbb{F}_2$.
  (b) Какова размерность этого пространства (для конечного множества M)? Укажите какой-нибудь базис V.
  (c) Обязательно ли семейство подмножеств $X_1, \dots, X_n$ линейно независимо, если $X_i \not\subset \bigcup\limits_{j \neq i} X_j$ для любого i?
  (d) Обязательно ли семейство подмножеств $X_1, \dots, X_n$ линейно независимо, если $X_1 \not\subset X_2 \not\subset \dots \not\subset X_n$?

(10) В стаде 101 корова. Если увести любую одну, то оставшихся можно разделить на две части по 50 коров в каждой так, что суммарный вес коров первой части равен суммарному весу коров другой части. Рассмотрите эти равенства как систему линейных уравнений на веса коров и докажите, что все коровы весят одинаково,
  (a) если вес каждой коровы — натуральное число;
  (a') если вес каждой коровы — элемент поля $\mathbb{F}_2$;
  (b) если вес каждой коровы — целое число;
  (c) если вес каждой коровы — рациональное число;
  (d) если вес каждой коровы — вещественное число;
  (e) если вес каждой коровы — комплексное число.

Алгебра — I

Листок 2

(1) Для каждого из определенных ниже отображений D пространства $\Bbbk[x]_{\leqslant m}$ (многочленов от x степени $\leqslant m$) в себя докажите, что D является линейным оператором, напишите его матрицу в стандартном базисе $(1, x, \ldots, x^m)$, и найдите базис, в котором матрица оператора D имеет вид

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

(a) D переводит каждый многочлен $f(x) = \sum\limits_{k=0}^{n} a_k x^k$ в его производную $f'(x) = \sum\limits_{k=1}^{n} k a_k x^{k-1}$.

(b) D переводит каждый многочлен $f(x) = \sum\limits_{k=0}^{n} a_k x^k$ в его первую разность $f(x+1) - f(x)$.

(2) Докажите, что ранг $m \times n$ матрицы $A = (a_{ij})$ равен 1 тогда и только тогда, когда существуют числа $x_1, \ldots, x_m$ (не все из которых равны нулю) и числа $y_1, \ldots, y_n$ (не все из которых равны нулю) такие, что $a_{ij} = x_i y_j$ для любых i, j.

(3) Как изменится определитель матрицы, если ее симметрично отразить относительно побочной диагонали?

(4) Докажите, что если сумма всех элементов матрицы в каждой строке равна нулю, то определитель матрицы равен нулю.

(5) (a) Пусть квадратная матрица X представляется в блочном виде с нулевым угловым блоком: $X = \left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)$. Докажите, что если матрицы A и C — квадратные, то $\det X = \det A \det C$.

(b) Пусть A и B — матрицы $n \times n$ над произвольным полем $\Bbbk$. Покажите, что матрицу $C = \left(\begin{smallmatrix} E & B \\ -A & 0 \end{smallmatrix}\right)$ можно привести элементарными преобразованиями к матрице $D = \left(\begin{smallmatrix} E & B \\ 0 & AB \end{smallmatrix}\right)$, и получите тем самым другое доказательство того, что $\det AB = \det A \det B$.

(6) Сколько над полем из q элементов

(a) невырожденных матриц размера $n \times n$?

(b) матриц размера $n \times n$ с фиксированным определителем $d \neq 0$?

(c) матриц размера $m \times n$ ранга m, где $m < n$?

(7) Квадратная матрица называется *кососимметрической*, если $a_{ij} = -a_{ji}$ для любых i, j.

(a) Докажите, что определитель кососимметрической матрицы нечетного порядка равен нулю.

(b) Докажите, что определитель кососимметрической матрицы четвертого порядка является полным квадратом (как многочлен от матричных элементов).

(c) * Докажите, что определитель кососимметрической матрицы любого четного порядка является полным квадратом.

(8) Пусть дана квадратная $n \times n$ матрица $A = (a_{ij})$. Обозначим через $\hat{A}$ матрицу из алгебраических дополнений к элементам матрицы A (она называется *присоединенной* матрицей).

(a) Докажите, что при применении к матрице A элементарного преобразования (прибавления к i-й строке j-й, умноженной на λ) матрица $\hat{A}$ также подвергается элементарному преобразованию. Какому?

(b) Докажите, что если $\det A = 0$, то и $\det \hat{A} = 0$.

(c) * Докажите, что $\det \hat{A} = \det A^{n-1}$.

(9) *Решеткой подпространств* в векторном пространстве V называется любое множество его подпространств, замкнутое относительно операций пересечения и суммы. Решетка подпространств L называется *дистрибутивной*, если для любых $V_1, V_2, V_3 \in L$ выполнено равенство $V_1 \cap (V_2 + V_3) = V_1 \cap V_2 + V_1 \cap V_3$.

(a) Пусть в пространстве V выбран базис $(v_1, \ldots, v_n)$. Докажите, что всевозможные линейные оболочки подмножеств базиса образуют дистрибутивную решетку подпространств в V.

(b) При каких n решетка всех подпространств в $\mathbb{R}^n$ является дистрибутивной?

(c) * Докажите, что для любой дистрибутивной решетки подпространств в конечномерном пространстве V существует такой базис $(v_1, \ldots, v_n)$, что каждое подпространство из решетки является линейной оболочкой некоторого множества базисных векторов v_i.

Алгебра — I

Листок 3

Внимание! Срок сдачи 13 ноября.

1. Представьте цикл $(1\,2\,3\,\ldots,n)$ в виде произведения $n-1$ транспозиции.

2. Пусть $\sigma\in S_n$ — нечетная перестановка и N — ее порядок в группе S_n. Что можно сказать про четность N?

3. Докажите, что если порядок любого неединичного элемента группы G равен двум, то группа G — абелева. Приведите пример такой группы более чем из двух элементов.

4. Пусть G — произвольная группа, $a,b\in G$, причем порядок элемента $ab\in G$ равен n. Каким может быть порядок элемента ba?

5. Докажите, что непустое подмножество H конечной группы G является подгруппой, если H замкнуто относительно умножения (т. е. в данном случае требование существования в H обратных элементов излишне). Верно ли это для бесконечной группы G?

6. Рассмотрим четыре матрицы из $\mathrm{SL}(2,\mathbb{C})$:

$$E=\begin{pmatrix}1&0\\0&1\end{pmatrix},I=\begin{pmatrix}i&0\\0&-i\end{pmatrix},J=\begin{pmatrix}0&1\\-1&0\end{pmatrix},K=\begin{pmatrix}0&i\\i&0\end{pmatrix}.$$

   Докажите, что множество $Q_8=\{\pm E,\pm I,\pm J,\pm K\}$ является подгруппой в $\mathrm{SL}(2,\mathbb{C})$ (Q_8 называется группой кватернионов). Найдите порядки всех элементов в Q_8. Докажите, что группа диэдра D_4 и группа кватернионов Q_8 не изоморфны.

Алгебра — I

Листок $3'$ (дополнительный)

Внимание! Срок сдачи 20 ноября.

(1) Пусть $\{1,\dots,n\} = I_1 \sqcup I_2 \sqcup \dots \sqcup I_k$ — разбиение множества $\{1,\dots,n\}$ на орбиты перестановки $\sigma \in S_n$. Определим *декремент* перестановки формулой

$$d(\sigma) = \sum_{l=1}^{k}(|I_l| - 1) = n - k.$$

  (a) Докажите, что знак перестановки σ равен $(-1)^{d(\sigma)}$.
  (b) Докажите, что перестановку σ можно представить в виде произведения $d(\sigma)$ транспозиций.
  (c) Докажите, что перестановку σ нельзя представить в виде произведения менее чем $d(\sigma)$ транспозиций.

(2) Под группой многогранника мы будем понимать группу *вращений* многогранника. Найдите порядок стационарной группы вершины и порядок самой группы для
  (a) группы диэдра;
  (b) группы тетраэдра;
  (c) группы куба;
  (d) группы икосаэдра.

(3) Докажите, что
  (a) группа диэдра D_3 изоморфна симметрической группе S_3;
  (b) группа тетраэдра T изоморфна знакопеременной группе A_4;
  (c) группа куба C изоморфна симметрической группе S_4;
  (d) группа икосаэдра I изоморфна знакопеременной группе A_5.

(4) Сколько существует различных ожерелий из 6 бусин, каждая из которых может быть красного, синего или желтого цвета? (Указание: используйте формулу Бернсайда).

(5) Докажите, что знакопеременная группа A_n, $n \geqslant 3$, порождается циклами длины 3, причем на самом деле

$$A_n = \langle (123), (124), \dots, (12n) \rangle.$$

Алгебра — I

Листок 4

Внимание! Срок сдачи 27 ноября.

1. Докажите, что если подгруппа $H \subset G$ имеет индекс 2, то она нормальна (группа G не обязательно конечна; индекс подгруппы — число левых смежных классов по ней).

2. Какие подгруппы имеет группа S_3? Найдите для них левые и правые смежные классы. Какие подгруппы группы S_3 являются нормальными?

3. Докажите, что группа S_4 имеет, кроме себя самой и единичной подгруппы, лишь следующие нормальные подгруппы: знакопеременная группа A_4 и "четверная группа Клейна" V_4, состоящая из перестановок:
$$e, \quad (12)(34), \quad (13)(24), \quad (14)(23).$$
Покажите, что последняя группа абелева.

4. Докажите, что $S_4/V_4 \cong S_3$.

5. Пусть p — простое число. Найдите число подгрупп порядка p в симметрической группе S_n, если (a) $p \leqslant n < 2p$; (b) $2p \leqslant n < 3p$.

6. Докажите, что
   (a) симметрическая группа S_3 изоморфна группе, заданной образующими s_1, s_2 и соотношениями $s_1^2 = e, s_2^2 = e$, $(s_1 s_2)^3 = e$;
   (b) симметрическая группа S_4 изоморфна группе, заданной образующими s_1, s_2, s_3 и соотношениями $s_1^2 = e, s_2^2 = e, s_3^2 = e$, $(s_1 s_2)^3 = e$, $(s_1 s_3)^2 = e$, $(s_2 s_3)^3 = e$.

Алгебра — I

Листок 5

Внимание! Срок сдачи 11 декабря.

1. Назовем два отрезка соизмеримыми, если существует третий, который укладывается в каждом из них целое число раз.

   (a) Верно ли, что два отрезка соизмеримы тогда и только тогда, когда найдется третий, в котором каждый из них укладывается целое число раз?

   (b) От прямоугольника со сторонами a и b отрезают (пока это возможно) квадраты со стороной, равной меньшей из сторон прямоугольника (назовем эту операцию операцией Евклида). К полученному прямоугольнику применим снова операцию Евклида, и т.д.

   Докажите, что a и b соизмеримы тогда и только тогда, когда прямоугольник разрежут на конечное количество квадратов, причем сторона наименьшего квадрата является их общей мерой.

   Верно ли, что сторона наименьшего квадрата является наибольшей общей мерой?

2. Докажите, что в конечной абелевой группе порядка n для любого $d \mid n$ существует хотя бы одна подгруппа порядка d.

3. Сколько попарно неизоморфных групп здесь выписано: $\mathbb{Z}_{24}$, $\mathbb{Z}_{12} \oplus \mathbb{Z}_2$, $\mathbb{Z}_8 \oplus \mathbb{Z}_3$, $\mathbb{Z}_6 \oplus \mathbb{Z}_4$, $\mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$, $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$?

4. (a) Найдите все такие $x \in \mathbb{Z}_p$ (p — простое), что $x^2 = 1$.

   (b) Чему равно произведение всех ненулевых элементов $\mathbb{Z}_p$ (p — простое)?

   (c) Докажите терему Вильсона: Число p является простым тогда и только тогда, когда $(p-1)!+1 \equiv 0 \pmod{p}$.

5. Докажите, что ровно половина элементов $\mathbb{Z}_p^*$ является квадратами (p — простое, $p > 2$, $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \mid x \neq 0\}$).

6. Обозначим через $\varphi(m)$ число обратимых элементов в кольце $\mathbb{Z}_m$ (то есть количество натуральных чисел, меньших m и взаимно простых с m). Эта функция называется функцией Эйлера. Докажите теорему Эйлера:

   Если класс вычетов $[a]_m$ обратим, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Алгебра — I

Листок $5'$ (дополнительный)

Внимание! Срок сдачи 19 декабря.

1. Докажите, что значение функции Эйлера $\varphi(m)$ для $m = p_1^{k_1} \cdot \dots \cdot p_n^{k_n}$ (p_i — различные простые числа) задается формулой
$$\varphi(m) = m \cdot (1 - \frac{1}{p_1}) \cdot \dots \cdot (1 - \frac{1}{p_n}).$$

2. (a) Пусть d, n — натуральные числа, причем d делит n. Сколько в циклической группе порядка n элементов порядка d?

   (b) Докажите, что $\sum_{d|m} \varphi(d) = m$.

3. Приведите примеры делителей нуля в кольце непрерывных функций на $[0, 1]$.

4. Докажите, что кольцо $\Bbbk[x, y]$ многочленов от двух переменных не является кольцом главных идеалов.

5. Докажите, что кольцо $\Bbbk[[x]]$ формальных степенных рядов над полем $\Bbbk$ является кольцом главных идеалов (и даже евклидовым). Какие элементы этого кольца неприводимы (просты)?

6. Пусть $f(x) = x^3 + b \in \mathbb{F}_7[x]$. Для каких $b \in \mathbb{F}_7$ существует ненулевой гомоморфизм колец $\mathbb{F}_7[x]/(f(x)) \to \mathbb{F}_7$?

7. (a) Сколько неприводимых многочленов степени 2 и 3 над полем $\mathbb{F}_q$?

   (b) Пусть n_k — число неприводимых многочленов степени k со старшим коэффициентом 1 над полем $\mathbb{F}_q$. Докажите, что в кольце формальных степенных рядов $\mathbb{Q}[[x]]$ выполнено равенство
$$1 - qx = \prod_{k=1}^{\infty} (1 - x^k)^{n_k}.$$

Алгебра — I

Листок 6

Срок сдачи 24 января.

1. Пусть операторы F и G в конечномерном векторном пространстве коммутируют. Докажите, что $\operatorname{Ker} G$ и $\operatorname{Im} G$ — инвариантные подпространства оператора F.

2. Пусть W — подпространство векторного пространства V; и пусть $v_1, \ldots, v_k \in V$. Рассмотрим смежные классы $\bar{v}_i = v_i + W \in V/W$.

   (a) Верно ли, что если $v_1, \ldots, v_k$ линейно независимы, то и $\bar{v}_1, \ldots, \bar{v}_k$ тоже линейно независимы?

   (b) Верно ли, что если $\bar{v}_1, \ldots, \bar{v}_k$ линейно независимы, то и $v_1, \ldots, v_k$ тоже линейно независимы?

3. Пусть F — идемпотентный линейный оператор (то есть $F^2 = F$). Какими могут быть характеристический и минимальный многочлены оператора F? Докажите, что у оператора F есть собственный базис. Как выглядит матрица оператора F в собственном базисе?

4. Пусть линейный оператор F имеет собственные векторы $v_1, \ldots, v_k$ с различными собственными значениями.

   (a) Докажите, что эти собственные векторы линейно независимы.

   (b) Докажите, что если k равно размерности пространства, то любое инвариантное подпространство оператора F является линейной оболочкой некоторых из этих собственных векторов.

5. Докажите, что любое (возможно, бесконечное) семейство попарно коммутирующих операторов в конечномерном комплексном векторном пространстве имеет общий собственный вектор.

6. Пусть линейный оператор F в конечномерном векторном пространстве над полем $\mathbb{C}$ удовлетворяет уравнению $F^n = \mathrm{id}$.

   (a) Докажите, что все собственные значения этого оператора являются степенями числа $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

   (b) Докажите, что если все собственные значения этого оператора равны, то он скалярен (то есть пропорционален тождественному оператору).

Алгебра — I

Листок 7

Срок сдачи 12 февраля.

1. Множество $c_{00} = \{(\ldots, z_{-1}, z_0, z_1, z_2, \ldots) \mid z_i \in \mathbb{C}, z_k \neq 0$ лишь для конечного числа индексов $k\}$ всех финитных двусторонних последовательностей комплексных чисел рассмотрим как векторное пространство над $\mathbb{C}$. Приведите пример обратимого линейного оператора в c_{00}, не имеющего ни одного собственного вектора.

2. Какие из следующих утверждений верны?

   (a) Если оператор на конечномерном векторном пространстве обратим, то он диагонализуем.

   (b) Если квадрат оператора на конечномерном векторном пространстве диагонализуем, то сам он тоже диагонализуем.

3. Пусть $A \in \mathrm{Mat}(n, \Bbbk)$ (где $\mathrm{Mat}(n, \Bbbk)$ — пространство $n \times n$ матриц с коэффициентами из $\Bbbk$) — фиксированная диагональная матрица, причем все ее собственные значения различны. Найдите все собственные значения и собственные векторы оператора $f\colon \mathrm{Mat}(n, \Bbbk) \to \mathrm{Mat}(n, \Bbbk)$ для следующих случаев:

   (a) $f(X) = AX$;

   (b) $f(X) = [A, X] = AX - XA$;

   (c) $f(X) = A^{-1}XA$ (в этом пункте предполагаем невырожденность матрицы A).

4. Решите предыдущую задачу в случае, когда A — произвольная матрица, имеющая n различных собственных значений.

5. Докажите, что следующие свойства линейного оператора F в конечномерном комплексном векторном пространстве V равносильны:

   - Для каждого собственного значения оператора F соответствующее собственное подпространство одномерно.
   - Каждому собственному значению оператора F в его жордановой нормальной форме отвечает ровно одна жорданова клетка.
   - Минимальный многочлен оператора F совпадает с характеристическим.
   - Фробениусова нормальная форма оператора F состоит из единственного циклического блока.
   - Всякий оператор, перестановочный с F, выражается как многочлен от F.

6. Пусть две вещественные матрицы подобны над $\mathbb{C}$. Верно ли, что они подобны и над $\mathbb{R}$?

Алгебра — I

Листок $7'$

1. Всякая ли матрица подобна своей транспонированной

   (a) над полем $\mathbb{C}$?

   (b) над произвольным полем?

2. (a) Пусть F — линейный оператор в произвольном векторном пространстве V над полем $\Bbbk$, локально нильпотентный в том смысле, что для любого $v \in V$ найдется натуральное число N такое, что $F^N v = 0$. Докажите, что для каждого формального степенного ряда $g(t) = \sum a_k t^k \in \Bbbk[[t]]$ корректно определен линейный оператор $g(F) = \sum a_k F^k$, причем такое сопоставление формальному степенному ряду линейного оператора определяет гомоморфизм алгебры формальных степенных рядов $\Bbbk[[t]]$ в алгебру линейных операторов $\operatorname{End}_{\Bbbk} V$.

   (b) Пусть $\operatorname{char}\Bbbk = 0$. Докажите, что $V = \Bbbk[x]$, $F = \partial/\partial x$, $g(t) = \exp(t) = \sum \frac{t^k}{k!}$ удовлетворяют условиям предыдущего пункта, причем для любого многочлена $P(x) \in \Bbbk[x]$ имеет место равенство $\exp(\partial/\partial x)P(x) = P(x+1)$.

   (c) Докажите, что для любого многочлена $P(x) \in \Bbbk[x]$ линейное дифференциальное уравнение $f(x)+a_1 f'(x)+a_2 f''(x)+\cdots+a_n f^{(n)}(x) = P(x)$ (где $a_1 \ldots, a_n \in \Bbbk$) имеет единственное решение в $\Bbbk[x]$.

3. Пусть F — линейный оператор в конечномерном пространстве V над полем $\Bbbk$. Обозначим через $\operatorname{End}_F(V)$ алгебру линейных операторов в V, перестановочных с F. Докажите, что существует разложение пространства V в прямую сумму ненулевых F-инвариантных подпространств V_1, V_2 тогда и только тогда, когда существуют ненулевые операторы $P_1, P_2 \in \operatorname{End}_F(V)$, удовлетворяющие условиям $P_1^2 = P_1$, $P_2^2 = P_2$, $P_1P_2 = P_2P_1 = 0$, $P_1 + P_2 = 1$.

4. Пусть V — конечномерное векторное пространство над полем $\Bbbk$. Линейный оператор $F : V \to V$ называется *полупростым*, если у каждого его инвариантного подпространства $U \subset V$ есть инвариантное прямое дополнение, то есть существует F-инвариантное подпространство $W \subset V$ такое, что $V = U \oplus W$.

   (a) Докажите, что при $\Bbbk = \mathbb{C}$ (и вообще, для любого алгебраически замкнутого поля $\Bbbk$) оператор F полупрост тогда и только тогда, когда он диагонализуем.

   (b) Докажите, что для любого алгебраически замкнутого поля $\Bbbk$ любой оператор F можно представить как сумму $F = F_s + F_n$, где оператор F_s полупрост, оператор F_n нильпотентен, причем $F_sF_n = F_nF_s$. (Такое разложение оператора в сумму называется *разложением Жордана.*

   (c) Докажите, что разложение Жордана любого оператора над алгебраически замкнутым полем единственно.

   (d) Пусть F, G — пара коммутирующих (перестановочных) операторов в векторном пространстве над алгебраически замкнутым полем. Докажите, что $(F+G)_s = F_s + G_s$ и $(F+G)_n = F_n + G_n$.

   (e) ** Верно ли, что разложение Жордана существует и единственно над произвольным полем?

5. Найдите максимально возможное число попарно перестановочных линейно независимых полупростых линейных операторов в $\mathbb{C}^n$.

Алгебра — I

Листок 8–8′

Срок сдачи первых пяти задач — 5 марта.

1. Пусть V — конечномерное векторное пространство над полем $\Bbbk$, и пусть $W \subset V$ — подпространство. Обозначим через $\mathrm{Ann}(W)$ аннулятор W в V^*. Постройте канонические изоморфизмы $(V/W)^* \cong \mathrm{Ann}(W)$ и $W^* \cong V^*/Ann(W)$.

2. (a) Пусть W — векторное пространство над $\mathbb{C}$. Постройте канонический изоморфизм $(W^*)_{\mathbb{R}} \cong (W_{\mathbb{R}})^*$.

   (b) Пусть V — векторное пространство над $\mathbb{R}$. Постройте канонический изоморфизм $(V^*)^{\mathbb{C}} \cong (V^{\mathbb{C}})^*$.

3. Пусть b — билинейная форма на конечномерном векторном пространстве V над полем $\Bbbk$. Определим *левую корреляцию* b_L и *правую корреляцию* b_R формы b как линейные операторы $V \to V^*$, переводящие произвольный вектор $v \in V$ в линейные функции $b(v, \bullet)$ и $b(\bullet, v)$, соответственно. (Жирная точка $\bullet$ отмечает место, в которое вставляется аргумент линейной функции.) Отождествим пространство V с дважды двойственным V^{**} посредством канонического изоморфизма. Докажите, что сопряженный оператор $b_L^* : V^{**}(= V) \to V^*$ к левой корреляции $b_L : V \to V^*$ совпадает с оператором правой корреляции $b_R : V \to V^*$.

4. Пусть V — n-мерное векторное пространство над конечным полем $\mathbb{F}_q$, где $q = p^k$ нечетно, и пусть b — невырожденная симметричная билинейная форма в V.

   (a) Докажите, что если $n > 1$, то существует вектор $v \in V$ такой, что $b(v, v) = 1$.

   (b) **(Закон инерции над конечным полем.)** Выберем элемент $\eta \in \mathbb{F}_q^*$, не являющийся квадратом. Докажите, что заменой базиса матрица формы b может быть приведена либо к виду $\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$, либо к виду $\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & \eta \end{pmatrix}$, но только к одному из них.

5. Пусть b — билинейная форма на n-мерном векторном пространстве V над полем $\Bbbk$. Подпространство $W \subseteq V$ называется изотропным, если ограничение b на W равно нулю.

   (a) Найдите в $\mathbb{C}^n$ для формы $b(x, y) = \sum x_k y_k$ изотропное подпространство максимальной возможной размерности.

   (b) Может ли максимальная размерность изотропного подпространства невырожденной билинейной формы быть больше, чем $n/2$?

   (c) Пусть b — кососимметрическая билинейная форма, а основное поле $\Bbbk = \mathbb{R}$. Какова может быть максимальная размерность изотропного подпространства в зависимости от ранга формы b?

   (d) Пусть b — симметрическая билинейная форма, а основное поле $\Bbbk = \mathbb{R}$. Какова может быть максимальная размерность изотропного подпространства в зависимости от индексов инерции формы b?

6. * Докажите, что если в симметрической матрице некоторый главный минор порядка r отличен от нуля, а все окаймляющие его главные миноры порядка $r + 1$ и $r + 2$ равны нулю, то ранг этой матрицы равен r.

7. * Сопоставим каждому (неориентированному) графу Γ с вершинами $v_1, \ldots, v_n$ квадратичную функцию $q_\Gamma(x) = \sum_{i,j=1}^n a_{ij} x_i x_j$, положив

$$a_{ij} = \begin{cases} 2, & \text{если } i = j, \\ -1, & \text{если } v_i \text{ и } v_j \text{ соединены ребром}, \\ 0, & \text{если } v_i \text{ и } v_j \text{ не соединены ребром}. \end{cases}$$

   (a) Докажите, что если функция q_Γ положительно определена, то граф Γ не содержит циклов, то есть каждая связная компонента его является деревом.

   (b) Докажите, что если функция q_Γ неотрицательно определена, то каждая связная компонента графа Γ — либо дерево, либо замкнутая цепочка.

   (c) * Опишите все связные графы, для которых функция q_Γ положительно определена; неотрицательно определена.

Алгебра — I

Листок 9

Симметрические функции и корни многочленов.

Срок сдачи — 27 апреля.

1. Назовем многочлен $f(x_1,\dots,x_n)\in\Bbbk[x_1,\dots,x_n]$ *кососимметрическим*, если для любой перестановки $\sigma\in S_n$ мы имеем $f(x_{\sigma(1)},\dots,x_{\sigma(n)})=\operatorname{sgn}(\sigma)f(x_1,\dots,x_n)$. Докажите, что если $\Bbbk$ — поле, причем $\operatorname{char}\Bbbk\neq 2$, то любой кососимметрический многочлен однозначно представляется в виде $f(x_1,\dots,x_n)=g(x_1,\dots,x_n)\Delta$, где $g(x_1,\dots,x_n)$ — симметрический многочлен, а $\Delta=\prod_{i>j}(x_i-x_j)$ — определитель Вандермонда.

2. Докажите, что если следы первых n степеней $n\times n$-матрицы A равны нулю, то матрица A нильпотентна.

3. Стандартный (ортонормированный) базис в евклидовом пространстве $\mathbb{R}^n$ обозначим $(e_1,\dots,e_n)$. Пусть A — симметричная положительно определенная вещественная $n\times n$-матрица, рассматриваемая как оператор в $\mathbb{R}^n$. Докажите, что длины главных осей эллипсоида $(x,Ax)=1$ однозначно определяются набором чисел $\nu_k=\sum_{i=1}^n|A^ke_i|^2$, где k пробегает числа $1,\dots,n$.

4. Выразите через p и q дискриминант многочлена x^n+px+q.

5. Пусть $f(x)$ — многочлен степени n со старшим коэффициентом 1, и пусть $y_1,\dots,y_{n-1}$ — все корни его производной. Докажите, что для дискриминанта $D(f)$ имеет место следующая формула:
$$D(f)=n^n(-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n-1}f(y_i).$$

6. Пусть $f(x)=a_0x^n+a_1x^{n-1}+\dots+a_n$. Рассмотрим дискриминант $D(f)$ как многочлен от $a_0,\dots,a_n$. Докажите следующее дифференциальное соотношение:
$$na_0\frac{\partial D}{\partial a_1}+(n-1)a_1\frac{\partial D}{\partial a_2}+\dots+a_{n-1}\frac{\partial D}{\partial a_n}=0.$$
(Указание: как меняется дискриминант при сдвиге аргумента $x\mapsto x+h$?)

7. (a) Докажите, что многочлены x^4+1 и x^6+x^3+1 неприводимы над полем рациональных чисел.
   (b) Докажите, что многочлен степени 3 над полем либо неприводим, либо имеет корень. Является ли многочлен x^3-5x^2+1 неприводимым над полем рациональных чисел?
   (c) Докажите, что многочлен от двух переменных x^2+y^2+1 неприводим над полем рациональных чисел. Остается ли он неприводимым над полем комплексных чисел?

8. Пусть p — простое число, k и n — натуральные числа.
   (a) Докажите что многочлен $x^{p^n-1}-1$ делится на многочлен $x^{p^k-1}-1$ в $\mathbb{F}_p[x]$ тогда и только тогда, когда n делится на k.
   (b) Докажите, что поле $\mathbb{F}_{p^k}$ вкладывается в поле $\mathbb{F}_{p^n}$ тогда и только тогда, когда n делится на k.

Алгебра — I

Листок 9′ (дополнительный)

Расширения полей.

1. (a) Пусть p — простое, $q = p^k$. Докажите, что поле $\mathbb{F}_q$ порождено над $\mathbb{F}_p$ одним элементом.

   (b) Докажите, что для любого натурального k существует неприводимый многочлен степени k над $\mathbb{F}_p$.

2. Докажите, что группа автоморфизмов конечного поля $\mathbb{F}_q$ порождена автоморфизмом Фробениуса $a \mapsto a^p$, где p — простое число и $q = p^k$. Каков порядок этой группы?

3. Докажите, что любой неприводимый многочлен $f(x) \in \mathbb{F}_p[x]$, имеющий корень в $\mathbb{F}_{p^k}$, разлагается в $\mathbb{F}_{p^k}[x]$ на линейные множители.

4. Пусть $\Bbbk \subset \mathbb{F}$ — расширение полей. Элемент $a \in \mathbb{F}$ называется *алгебраическим* над $\Bbbk$, если он является корнем некоторого ненулевого многочлена $f(x) \in \Bbbk[x]$, и *трансцендентным* над $\Bbbk$ в противном случае.

   (a) Докажите, что элемент $a \in \mathbb{F}$ является алгебраическим над $\Bbbk$ тогда и только тогда, когда $\Bbbk(a)$ (наименьшее подполе поля $\mathbb{F}$, содержащее $\Bbbk$ и a) конечномерно, как векторное пространство над $\Bbbk$.

   (b) Докажите, что если элемент $a \in \mathbb{F}$ является алгебраическим над $\Bbbk$, то $\Bbbk(a)$ изоморфно $\Bbbk[x]/(g_a)$, где $g_a \in \Bbbk[x]$ — минимальный многочлен элемента a, а если элемент $a \in \mathbb{F}$ трансцендентен над $\Bbbk$, то $\Bbbk(a)$ изоморфно полю рациональных функций $\Bbbk(x)$.

5. Расширение полей $\Bbbk \subset \mathbb{F}$ называется *алгебраическим*, если все элементы поля $\mathbb{F}$ алгебраические над $\Bbbk$. Поле называется *алгебраически замкнутым*, если любой многочлен над ним имеет в нем корень.

   (a) Пусть имеются три поля $\Bbbk \subset \mathbb{F} \subset \mathbb{L}$. Докажите, что если два из расширений $\Bbbk \subset \mathbb{F}$, $\mathbb{F} \subset \mathbb{L}$, $\Bbbk \subset \mathbb{L}$ являются алгебраическими, то и третье тоже является алгебраическим.

   (b) Докажите, что алгебраически замкнутое поле не имеет нетривиальных алгебраических расширений (то есть алгебраических расширений степени, большей 1).

   (c) * Докажите, что у каждого поля $\Bbbk$ есть *алгебраическое замыкание* $\overline{\Bbbk}$ — алгебраически замкнутое поле, являющееся алгебраическим расширением $\Bbbk$.

6. Пусть $\Bbbk \subset \mathbb{F}$ — расширение полей. Элементы $a_1, \ldots, a_n \in \mathbb{F}$ называются *алгебраически независимыми* над $\Bbbk$, если для любого ненулевого многочлена $f(x_1, \ldots, x_n) \in \Bbbk[x_1, \ldots, x_n]$ его значение $f(a_1, \ldots, a_n)$ не равно 0 в поле $\mathbb{F}$, и *алгебраически зависимыми* в противном случае. Рассмотрим множество $\mathcal{C}$ минимальных (по включению) подмножеств множества $\mathbb{F}$, алгебраически зависимых над $\Bbbk$, множество $\mathcal{I}$ подмножеств множества $\mathbb{F}$, алгебраически независимых над $\Bbbk$, и множество $\mathcal{B}$ максимальных (по включению) подмножеств множества $\mathbb{F}$, алгебраически независимых над $\Bbbk$.

   (a) Докажите, что если $C_1, C_2 \in \mathcal{C}$, причем $C_1 \neq C_2$, и $e \in C_1 \cap C_2$, то существует $C_3 \in \mathcal{C}$, $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.

   (b) Докажите, что если $I_1, I_2 \in \mathcal{I}$, причем $|I_1| < |I_2| < \infty$, то существует $e \in I_2 \setminus I_1$, для которого $I_1 \cup \{e\} \in \mathcal{I}$.

   (c) Докажите, что если множество $\mathcal{B}$ содержит конечное подмножество $B \subset \mathbb{F}$, $|B| = n$, то все элементы $\mathcal{B}$ являются конечными множествами с одинаковым числом элементов n. (В этом случае n называется степенью трансцендентности $\mathbb{F}$ над $\Bbbk$; в противном случае говорят, что степень трансцендентности бесконечна.)

   (d) * Докажите, что множество $\mathcal{B}$ непусто, причем для любых $B_1, B_2 \in \mathcal{B}$ и любого $a \in B_1 \setminus B_2$ существует $b \in B_2 \setminus B_1$ такой, что $(B_1 \setminus \{a\}) \cup \{b\} \in \mathcal{B}$.

   (e) * Пусть все элементы $\mathcal{B}$ — бесконечные множества (то есть степень трансцендентности $\mathbb{F}$ над $\Bbbk$ бесконечна). Докажите, что все они равномощны.

7. (a) Докажите, что степень трансцендентности $\mathbb{C}$ над $\mathbb{Q}$ бесконечна.

   (b) Докажите, что любое поле характеристики ноль, чья степень трансцендентности над $\mathbb{Q}$ конечна (или даже счетна), можно вложить в $\mathbb{C}$.

   (c) Докажите теорему Гамильтона–Кэли (для произвольного поля), используя только то, что матрица любого комплексного линейного оператора приводится к верхнетреугольному виду, и то, что $n \times n$ матрица, характеристический многочлен которой имеет n разных корней, диагонализуема.

   (Указания: теорема Гамильтона–Кэли состоит в том, что некоторый определенный набор из n^2 многочленов с целыми коэффициентами от коэффициентов матрицы $A = (a_{ij})$ (а именно, коэффициенты матрицы $\chi_A(A)$) обращается в ноль тождественно на элементах поля. Для диагональных и, следовательно, для диагонализуемых матриц это верно. Проверьте, что диагонализуемые матрицы плотны в пространстве всех комплексных $n \times n$ матриц, и что полином, обращающийся в ноль на всюду плотном подмножестве пространства $\mathbb{C}^N$, тождественно равен нулю. Воспользуйтесь вложением поля частных кольца многочленов $\mathbb{Z}[a_{11}, \ldots, a_{nn}]$ в поле комплексных чисел, чтобы установить, что упомянутые целочисленные многочлены — нулевые и, следовательно, обращаются в нуль на элементах любого поля.)

Алгебра — I

Листок 10

Тензорные произведения.

Срок сдачи задач без звездочек — 25 мая.

1. Докажите, что в тензорном произведении векторных пространств над полем $\Bbbk$ тензорное произведение векторов равно нулю тогда и только тогда, когда один из векторов–сомножителей равен нулю.

2. Пусть (e_i) — базис n-мерного пространства V, а (e^i) — двойственный базис пространства V^*. Докажите, что тензор $\sum\limits_{i=1}^{n} e_i \otimes e^i \in V \otimes V^*$ не зависит от выбора базиса (e_i).

3. Обозначим через ϕ изоморфизм $\mathrm{Hom}(V,V) \xrightarrow{\sim} \mathrm{Hom}(V,V)^*$, получающийся композицией канонических изоморфизмов $\mathrm{Hom}(V,V) \xrightarrow{\sim} V^* \otimes V \xrightarrow{\sim} V \otimes V^* \xrightarrow{\sim} V^{**} \otimes V^* \xrightarrow{\sim} (V^* \otimes V)^* \xrightarrow{\sim} \mathrm{Hom}(V,V)^*$. Сопоставим ему билинейную форму Φ на пространстве $\mathrm{Hom}(V,V)$, заданную формулой $\Phi(F_1,F_2) = (\phi(F_1))(F_2)$. Является ли эта форма симметрической? Как она вычисляется в терминах матриц операторов F_1, F_2?

4. Докажите, что любое $GL(V)$-эквивариантное (то есть перестановочное с действием $GL(V)$) линейное отображение $V^* \otimes V \to \Bbbk$ пропорционально отображению свертки. (Элемент $g \in GL(V)$ действует в $\Bbbk$ тождественным оператором, а в $V^* \otimes V$ — линейным оператором $(g^{-1})^* \otimes g$.)

5. Докажите, что тензор $t \in V^* \otimes W$ представляется в виде суммы k разложимых тензоров тогда и только тогда, когда ранг соответствующего линейного оператора из $\mathrm{Hom}(V,W)$ не превосходит k.

6. Пусть V, W — векторные пространства над полем комплексных чисел, $\dim V = n$, $\dim W = k$.
   (a) Сколько орбит у действия $GL(V) \times GL(W)$ на $V \otimes W$?
   (b) Сколько орбит у действия $GL(V)$ на $V^* \otimes V$? (Элемент $g \in GL(V)$ действует в $V^* \otimes V$ линейным оператором $(g^{-1})^* \otimes g$.)
   (c) Сколько орбит у действия $GL(V)$ на S^2V^*? (Элемент $g \in GL(V)$ действует в S^2V^* линейным оператором $S^2(g^{-1})^*$.)

7. * Вычислите $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/3\mathbb{Z})$.

8. * **(Инвариант Дена)** Пусть P — выпуклый многогранник в $\mathbb{R}^3$. Обозначим через l_i длины ребер многогранника P, а через α_i — величины соответствующих двугранных углов. *Инвариантом Дена* многогранника P называется $\mathrm{Dehn}(P) = \sum l_i \otimes \alpha_i \in \mathbb{R} \otimes_{\mathbb{Q}} \mathbb{R}/\pi\mathbb{Q}$.
   (a) Докажите, что если многогранник P разбит плоскостью на два многогранника P_1 и P_2, то $\mathrm{Dehn}(P) = \mathrm{Dehn}(P_1) + \mathrm{Dehn}(P_2)$.
   (b) Докажите, что если два многогранника P_1 и P_2 равносоставлены (то есть P_1 может быть разбит на меньшие многогранники, из которых можно составить P_2), то $\mathrm{Dehn}(P_1) = \mathrm{Dehn}(P_2)$.
   (c) Докажите, что $\cos n\varphi$ выражается как многочлен от $\cos\varphi$ (этот многочлен называется n-м многочленом Чебышева). Чему равен его старший коэффициент? Докажите, что $\arccos\frac{1}{3}$ не является рациональным кратным π.
   (d) Докажите, что куб и правильный тетраэдр одного объема не являются равносоставленными.

Алгебра — II

Листок 1

Группы.

Срок сдачи задач 1–9 — 26 сентября.

1. Докажите, что любая подгруппа, содержащая коммутант группы, нормальна.

2. Докажите, что центр группы порядка p^n содержит более одного элемента (p — простое число, $n \in \mathbb{N}$).

3. Существуют ли неабелевы группы порядка p^2?

4. Пусть G — группа верхних унитреугольных матриц порядка 3 с элементами из поля $\mathbb{F}_3$. Найдите порядок группы G, ее центр и классы сопряженных элементов.

5. Может ли быть циклической
   (a) факторгруппа некоммутативной группы по ее центру?
   (b) группа всех автоморфизмов некоммутативной группы?

6. Сколько силовских p-подгрупп в (a) $GL_2(\mathbb{F}_p)$? (b) $GL_n(\mathbb{F}_p)$?

7. Найдите коммутанты групп (a) S_3; (b) A_4; (c) D_4; (d) S_4; (e) Q_8 (группа Гамильтона); (f) D_5.

8. (a) Докажите, что коммутант любой нормальной подгруппы группы G является нормальной подгруппой группы G.
   (b) Верно ли, что любая нормальная подгруппа коммутанта группы G является нормальной подгруппой группы G?

9. Пусть p, q — простые числа, $p < q$.
   (a) Докажите, что если p не делит $q - 1$, то любая группа порядка pq — абелева. Сколько их (с точностью до изоморфизма)?
   (b) Докажите, что если p делит $q - 1$, то существует неабелева группа порядка pq. Сколько их (с точностью до изоморфизма)?

10. Докажите разрешимость любой группы порядка
   (a) p^n, где p — простое число, $n \in \mathbb{N}$;
   (b) pq, где p, q — различные простые числа;
   (c) p^2q, где p, q — различные простые числа;
   (d) $n < 60$.

11. Пусть порядок группы G равен 60.
   (a) Докажите, что если число силовских 2-подгрупп в группе G не равно 5, то группа G разрешима.
   (b) Докажите, что если группа G проста, то она изоморфна группе A_5.

Алгебра — II

Листок 1′ (дополнительный)

Автоморфизмы симметрических групп.

1. (a) Опишите классы сопряженности в знакопеременной группе A_n.

   (b) Докажите, что при $n \geq 5$ группа A_n проста.

2. (a) Докажите, что любой автоморфизм группы переводит классы сопряженности в классы сопряженности.

   (b) Докажите, что если автоморфизм симметрической группы S_n переводит транспозиции в транспозиции, то он является внутренним.

   (c) Докажите, что при $n \neq 6$ все автоморфизмы группы S_n являются внутренними.

3. (a) Пусть H — подгруппа индекса 6 в S_6. Тогда действие S_6 на множестве смежных классов S_6/H задает гомоморфизм $S_6 \to S_6$. Докажите, что это автоморфизм.

   (b) Докажите, что любая подгруппа индекса 6 в S_6 изоморфна S_5.

4. Напомним, что для любого поля $\Bbbk$ группа $PGL_n(\Bbbk)$ определяется как факторгруппа группы $GL_n(\Bbbk)$ по подгруппе скалярных матриц.

   (a) Докажите, что действие группы $PGL_2(\mathbb{F}_5)$ на $\mathbb{P}^1(\mathbb{F}_5)$ задает вложение этой группы в S_6.

   (b) Обозначим через H образ этого вложения. Докажите, что H — подгруппа индекса 6 в S_6.

   (c) Рассмотрим S_5 как подгруппу в S_6, состоящую из всех перестановок, оставляющих элемент 6 на месте. Опишите все подгруппы в S_6, сопряженные с ней, и докажите, что подгруппа H не сопряжена с S_5.

   (d) Докажите, что автоморфизм группы S_6, задаваемый по предыдущей задаче подгруппой H, не является внутренним.

   (e) Куда этот автоморфизм переводит транспозиции?

5. (a) Докажите, что факторгруппа $\mathrm{Aut}(S_6)/\mathrm{Int}(S_6)$ группы всех автоморфизмов группы S_6 по подгруппе ее внутренних автоморфизмов изоморфна $\mathbb{Z}/2\mathbb{Z}$.

   (b) Верно ли, что $\mathrm{Aut}(S_6) \cong \mathrm{Int}(S_6) \times \mathbb{Z}/2\mathbb{Z}$?

Алгебра — II

Листок 2

Представления.

Срок сдачи задач 1–8 — 6 ноября.

1. Какие собственные значения могут иметь операторы представления группы движений треугольника D_3?

2. Как действует оператор, представляющий симметрию треугольника, на собственных подпространствах оператора, представляющего поворот?

3. Докажите, что группа D_3 имеет всего три неприводимых комплексных представления: два одномерных и одно двумерное.

4. Классифицируйте простые модули над ассоциативной алгеброй A, где
   (a) $A = \mathbb{C}[x]/(x^2 - 3x + 2)$;
   (b) $A = \mathbb{C}[x]/(x^2 - 2x + 1)$.

5. Является ли полупростым любой конечномерный модуль над алгеброй A из предыдущей задачи?

6. Найдите все такие группы G, для которых $\mathbb{C}G = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$ (прямая сумма алгебр).

7. Перечислите все (с точностью до изоморфизма) конечные группы G, для которых групповая алгебра $\mathbb{C}G$ изоморфна
   (a) прямой сумме двух матричных алгебр;
   (b) прямой сумме трех матричных алгебр.

8. Пусть $V = \mathbb{C}^2$ и (e_1, e_2) — стандартный базис V. Рассмотрим в тензорной алгебре $T(V)$ двусторонний идеал I, порожденный $(e_1 \otimes e_1)$, $(e_2 \otimes e_2)$ и $(e_1 \otimes e_2 + e_2 \otimes e_1 - 1)$. Обозначим через C факторалгебру $T(V)/I$.
   (a) Чему равна размерность алгебры C?
   (b) Пусть $X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ и $Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Докажите, что существует матричное представление алгебры C, переводящее e_1 в X, а e_2 в Y. Является ли оно неприводимым?
   (c) Перечислите все (с точностью до эквивалентности) неприводимые представления алгебры C.

9. Пусть V — n-мерное векторное пространство над полем $\mathbb{C}$, а q — квадратичная форма на V. *Алгеброй Клиффорда* $C(q)$ называется факторалгебра тензорной алгебры пространства V по двустороннему идеалу, порожденному элементами вида $v \otimes v - q(v)$. Чему равна размерность $C(q)$?

10. Пусть $V = W^* \oplus W$ и q — квадратичная форма на V, заданная формулой $q((\varphi, w)) = \varphi(w)$. Положим $M = \Lambda(W)$.
    (a) Докажите, что существует неприводимое представление алгебры Клиффорда $C(q)$ в пространстве M, переводящее $(\varphi, 0) \in V$ в оператор внутреннего умножения на $\varphi \in W^*$, а $(0, w)$ — в оператор внешнего умножения на $w \in W$.
    (b) Докажите, что любое неприводимое представление алгебры $C(q)$ эквивалентно этому представлению.

Алгебра — II

Листок 3

Характеры.

Срок сдачи задач с 1 по 7 — 30 ноября.

1. Докажите, что представление конечной группы изоморфно своему сопряженному тогда и только тогда, когда все значения его характера вещественны.

2. Докажите, что для любого элемента g неединичной конечной группы G существует такой нетривиальный неприводимый комплексный характер χ группы G, что $\chi(g) \neq 0$.

3. Пусть ε — одномерное представление группы S_4, в котором каждая перестановка действует умножением на свой знак, ρ — ее представление вращениями куба, а τ — ее представление симметриями тетраэдра. Докажите, что $\rho \otimes \varepsilon \simeq \tau$ и $\tau \otimes \varepsilon \simeq \rho$.

4. Разложите на неприводимые представление S_4 в пространстве функций на ребрах тетраэдра.

5. Пусть ρ — неприводимое двумерное представление группы S_3.

   (a) Разложите $S^2\rho$ и $S^3\rho$ в прямую сумму неприводимых представлений.

   (b) Докажите, что $S^{n+6}\rho \simeq S^n\rho \oplus \varkappa$, где через $\varkappa$ обозначено регулярное представление группы G, а $n \in \mathbb{N}$.

   (c) Опишите разложение $S^n\rho$ в прямую сумму неприводимых для любого $n \in \mathbb{N}$.

   (d) Опишите алгебру всех G-инвариантных полиномов на V, где V — пространство представления ρ.

6. Пусть G — конечная группа, $H \subset G$ — подгруппа (не обязательно нормальная), $X = G/H$ — множество левых смежных классов, на котором группа G действует левыми умножениями. Докажите, что характер представления группы G в пространстве $\mathbb{C}X$ вычисляется по формуле:
$$\chi(C) = \frac{|G| \cdot |C \cap H|}{|C| \cdot |H|},$$
где C — класс сопряженных элементов группы G. (Напомним, что такие представления называются квазирегулярными.)

7. Пусть пересечение класса сопряженных элементов $C \subset G$ с подгруппой $H \subset G$ раскладывается в дизъюнктное объединение $C \cap H = D_1 \sqcup \dots \sqcup D_s$ классов H-сопряженности. Докажите, что значение на C характера представления группы G, индуцированного с произвольного представления ρ подгруппы H, вычисляется по формуле:
$$\chi_{\mathrm{Ind}\,\rho}(C) = \frac{|G|}{|C| \cdot |H|} \sum_{i=1}^{s} |D_i| \cdot \chi_\rho(D_i).$$

8*. Пусть $\rho : G \to GL(V)$ — точное представление конечной группы G (то есть $G \simeq \rho(G)$). Докажите, что в разложениях его тензорных степеней встречаются все неприводимые представления группы G.

Алгебра — II

Листок 4

Представления симметрических групп.

Срок сдачи 18 декабря.

Условимся называть *тавтологическим* n-мерное представление симметрической группы S_n в пространстве $\mathbb{C}^n$, при котором переставляются базисные векторы стандартного базиса. Тавтологическое представление является прямой суммой тривиального одномерного представления и $(n-1)$-мерного представления группой (несобственных) движений стандартного правильного $(n-1)$-мерного симплекса. Это последнее представление мы будем называть *симплициальным*.

(1) Докажите, что симплициальное представление симметрической группы неприводимо, и вычислите его характер.

(2) Вычислите скалярный квадрат (относительно стандартной эрмитовой структуры на $\mathbb{C}[S_n]$) характера k-той внешней степени тавтологического представления симметрической группы а) S_4; б) S_n.

(3) Выведите из предыдущей задачи, что все внешние степени симплициального представления симметрической группы неприводимы (для этого разложите внешнюю степень тавтологического представления в сумму подходящих внешних степеней симплициального представления).

(4) Обозначим через $\mathrm{Sym}_k : V^{\otimes k} \to V^{\otimes k}$ (соответственно, $\mathrm{Alt}_k : V^{\otimes k} \to V^{\otimes k}$) оператор симметризации (соответственно, антисимметризации). Укажите явно такой ненулевой тензор $\tau \in V^{\otimes 3}$, для которого
$$\mathrm{Sym}_3(\tau) = \mathrm{Alt}_3(\tau) = 0.$$

(5) С каждой таблицей Юнга, построенной по диаграмме Юнга λ, свяжем следующие три элемента групповой алгебры $\mathbb{C}S_n$:
$$a_\lambda = \sum_{\sigma \in R} \sigma, \qquad b_\lambda = \sum_{\sigma \in C} \mathrm{sgn}(\sigma) \cdot \sigma, \qquad c_\lambda = a_\lambda \cdot b_\lambda$$
где $R, C \subseteq G$ — подгруппы, сохраняющие соответственно строки и столбцы выбранной таблицы Юнга. Элемент c_λ называется *симметризатором Юнга*. Обозначим через V_λ левый идеал, порожденный c_λ в $\mathbb{C}S_n$. Докажите, что V_λ — единственный (с точностью до изоморфизма) простой $\mathbb{C}S_n$-модуль, входящий как в $\mathrm{Ind}_R^{S_n} \mathbb{C}_1$, так и в $\mathrm{Ind}_C^{S_n} \mathbb{C}_\varepsilon$, где $\mathbb{C}_1$ — тривиальный одномерный $\mathbb{C}R$-модуль, а $\mathbb{C}_\varepsilon$ — знакопеременный одномерный $\mathbb{C}C$-модуль.

Процедура построения по диаграмме Юнга λ неприводимого представления группы S_n в пространстве V_λ (соответствующего естественной структуре $\mathbb{C}S_n$-модуля на V_λ) называется *конструкцией Шура*.

(6) Докажите, что одномерные тривиальное и знакопеременное представления симметрической группы получаются применением конструкции Шура к диаграммам
$$\underbrace{\square\square\cdots\square\square}_{n} \qquad \text{и} \qquad n\left\{\begin{array}{c}\square\\ \square\\ \vdots\\ \square\\ \square\end{array}\right.$$
соответственно.

(7) Докажите, что при применении конструкции Шура к транспонированным диаграммам Юнга получатся представления, отличающиеся друг от друга тензорным умножением на одномерное знакопеременное представление.

(8) Установите соответствие между представлениями Шура групп S_3 и S_4 и неприводимыми представлениями этих групп, описанными геометрически в задачах из прошлых листков.

(9) Докажите, что k-тая внешняя степень симплициального представления симметрической группы получается применением конструкции Шура к диаграмме-крюку
$$k{+}1\left\{\begin{array}{l}\square\square\square\square\\ \square\\ \square\\ \square\\ \square\\ \square\end{array}\right. \qquad .$$

Алгебра-2 (матфак ВШЭ 2015-2016): расширения полей листок 1

Срок сдачи листка 1 февраля (сданные позже задачи учитываются с коэффициентом 1/2). Вклад листков в оценку - половина (другая половина - оценка за контрольную, или средний балл по контрольным, если вдруг их окажется несколько). В каждом листке есть простой теорвопрос, он стоит двух задач, но пока он не сдан, баллы за листок не засчитываются.

1 (этот самый вопрос) Пусть K поле, x – элемент некоторого расширения K. Докажите, что следующие утверждения эквивалентны: а) x алгебраичен над K (т.е. удовлетворяет полиномиальному уравнению с коэффициентами из K) б) $K[x]$ – конечномерное векторное пространство над K в) $K[x]$ – поле г) $K[x] = K(x)$.

2 Пусть R – коммутативное ассоциативное кольцо с единицей без делителей нуля, а x удовлетворяет полиномиальному уравнению с коэффициентами из R. Верно ли, что $R[x]$ конечно порождено как R-модуль? При каком (разумном) условии на коэффициенты уравнения это окажется верным?

3 Пусть $\mathbb{Q}(x)$ – поле рациональных функций от одной переменной, а f, g взаимно простые многочлены (не константы). Рассмотрим подполе $\mathbb{Q}(\frac{f(x)}{g(x)})$. Покажите, что $\mathbb{Q}(x)$ алгебраично над $\mathbb{Q}(\frac{f(x)}{g(x)})$, а $\mathbb{Q}(\frac{f(x)}{g(x)})$ трансцедентно над $\mathbb{Q}$. Найдите степень расширения $[\mathbb{Q}(x) : \mathbb{Q}(\frac{f(x)}{g(x)})]$.

4 Пусть L – алгебраическое расширение K и $f : L \to L$ – гомоморфизм над K. Докажите, что f изоморфизм (указание: выведите это из соответствующего факта для конечных расширений). Верно ли это утверждение, если L не является алгебраическим?

5 Найдите минимальный многочлен $e^{\frac{2\pi i}{5}}$ над $\mathbb{Q}$, над $\mathbb{Q}(i)$ и над $\mathbb{Q}(\sqrt{5})$.

6 Пусть m, n положительные числа, не являющиеся квадратами. Проверьте, что $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n})$, найдите $[\mathbb{Q}(\sqrt{m} + \sqrt{n}) : \mathbb{Q}]$ и минимальный многочлен $\sqrt{m} + \sqrt{n}$ над $\mathbb{Q}$.

В дальнейшем $\mathbb{F}_q$ обозначает конечное поле из q элементов.

7 Пусть q – степень простого числа. Докажите эквивалентность следующих утверждений: $X^3 - 1$ распадается на линейные множители над $\mathbb{F}_q$; -3 является квадратом в $\mathbb{F}_q$; $q \equiv 1 \pmod 3$.

8 Докажите, что многочлен f степени d приводим над $\mathbb{F}_q$ тогда и только тогда, когда он имеет корень в $\mathbb{F}_{q^l}$ для некоторого $l \leq d/2$.

9 Докажите, что многочлен $X^4 + 1$ приводим над полем $\mathbb{F}_p$ для любого простого p, но неприводим над $\mathbb{Z}$ (для приводимости воспользуйтесь предыдущим упражнением).

10 Пусть p простое. Докажите, что многочлен $X^p - a$ неприводим над полем K тогда и только тогда, когда у него нет корня в K (указание: как может выглядеть какой-либо сомножитель? воспользуйтесь тождеством Безу.)

11 Пусть p простое. Докажите, что $X^p - X - 1$ неприводим над $\mathbb{F}_p$.

Алгебра-2 (матфак ВШЭ 2015-2016): расширения полей, листок 2

Срок сдачи листка 26 февраля (просроченная задача оценивается как ползадачи, сданные в срок).

1 Сформулируйте и докажите теорему о продолжении гомоморфизмов в алгебраически замкнутое поле.

2 Найдите степень поля разложения $X^5 - 7$ над $\mathbb{Q}$ и $(X^2-3)(X^3-2)$ над $\mathbb{Q}$.

3 Найдите степень поля разложения $X^6 + X^3 + 1$ над $\mathbb{F}_p, p \equiv 1(9)$; над $\mathbb{F}_p, p \equiv 7(9)$; над $\mathbb{F}_p, p \equiv 2(9)$.

4 Пусть K поле характеристики p и a алгебраичен над K. Покажите, что a сепарабелен тогда и только тогда, когда $K(a) = K(a^{p^n})$ для всех $n \in \mathbb{N}$.

Поле характеристики p называется совершенным, если все его элементы - p-е степени. Например, конечные поля совершенны (почему?). Все расширения совершенного поля сепарабельны.

5 а) Пусть k алгебраически замкнутое поле характеристики p, и $K = k(T)$. Обозначим u_n корень многочлена $X^{p^n} - T$ в $\overline{K}$, и пусть $K_n = K(u_n)$.

Какова степень K_n над K? Покажите, что $K_n = (K_{n+1})^p$ (здесь L^p обозначает подполе p-х степеней в L).

б) Выведите отсюда, что $K(u_1, ...u_n, ...)$ совершенное поле, и что все конечные чисто несепарабельные расширения K - это K_n.

6 Какие из следующих алгебр являются полями? произведениями полей? опишите эти поля.

$\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[4]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$.

7 Тот же вопрос для $\mathbb{F}_2(\sqrt{T}) \otimes_{\mathbb{F}_2(T)} \mathbb{F}_2(\sqrt{T})$, $\mathbb{F}_4(\sqrt[3]{T}) \otimes_{\mathbb{F}_4(T)} \mathbb{F}_4(\sqrt[3]{T})$.

Расширение L поля K называется нормальным, если это поле разложения семейства многочленов над K, и расширением Галуа, если оно нормально и сепарабельно. В этом случае группа автоморфизмов L над K называется группой Галуа.

8 Пусть $a = \sqrt[4]{5}$. Покажите, что $\mathbb{Q}(ia^2)$ нормально над $\mathbb{Q}$, что $\mathbb{Q}(a+ia)$ нормально над $\mathbb{Q}(ia^2)$, но $\mathbb{Q}(a+ia)$ не является нормальным над $\mathbb{Q}$.

9 Покажите, что $cos(\frac{2\pi}{9})$ алгебраичен над $\mathbb{Q}$, и что $\mathbb{Q}(cos(\frac{2\pi}{9}))$ – нормальное расширение $\mathbb{Q}$.

10 а) Пусть группа G транзитивно действует на множестве из p элементов, где p простое число. Докажите, что образ G в группе подстановок S_p содержит p-цикл.

б) Выведите отсюда, что группа Галуа поля разложения неприводимого многочлена $P \in \mathbb{Q}[X]$ простой степени p, у которого ровно $p-2$ вещественных корня, есть S_p.

11 Пусть $S \subset F(X_1, ..., X_n)$ поле симметрических рациональных функций от n переменных с коэффициентами в поле F. Покажите, что $F(X_1, ..., X_n)$ – расширение Галуа поля S, степени $n!$.

Алгебра-2 (2015-2016): расширения полей, листок 3

Сдавать листок можно вплоть до 25 марта. Каждый пункт оценивается отдельно (а теорвопрос, как обычно, в 2 пункта).

1 Пусть поле L конечное расширение поля K. Докажите, что $|Aut_K L| \leq [L:K]$. В каком случае достигается равенство и почему?

2 Пусть E расширение Галуа F, а $P \in F[x]$ неприводим над F. Покажите, что все неприводимые сомножители P над E имеют одну и ту же степень.

3 Пусть K поле разложения $X^4 - 2$ над $\mathbb{Q}$, и $G = Gal(K/\mathbb{Q})$.

а) Покажите, что $G \cong D_4$, и найдите неподвижное подполе K^C, где C центр G.

б) Какие подгруппы порядка 4 есть в G? Опишите квадратичные расширения $\mathbb{Q}$, содержащиеся в K.

в) Опишите подрасширения K степени 4 над $\mathbb{Q}$. Какие из них - расширения Галуа?

4

а) Пусть F поле характеристики $\neq 2$ и E расширение Галуа степени 4 над F. Докажите, что имеется квадратичное над F подрасширение $K \subset E$, и что существуют такие $a, b, \epsilon \in F$, что $E = F(\sqrt{a + b\sqrt{\epsilon}})$.

б) Пусть теперь $a, b, \epsilon \in F$ таковы, что $\sqrt{\epsilon} \notin F$ и $\sqrt{a + b\sqrt{\epsilon}} \notin F(\sqrt{\epsilon})$. Покажите, что $E = F(\sqrt{a + b\sqrt{\epsilon}})$ нормально над F тогда и только тогда, когда $a^2 - \epsilon b^2$ является квадратом в $F(\sqrt{\epsilon})$.

в) Выведите отсюда, что если E расширение Галуа F, то $a^2 - \epsilon b^2 = u^2$ или $a^2 - \epsilon b^2 = \epsilon u^2$ для некоторого $u \in F$, и укажите группу Галуа в каждом из этих двух случаев.

5

С помощью теории Галуа покажем, что $\mathbb{C}$ алгебраически замкнуто. Из анализа используем только теорему о промежуточном значении: из нее следует, что любой многочлен нечетной степени в $\mathbb{R}[X]$ имеет корень в $\mathbb{R}$.

Пусть K - конечное расширение Галуа $\mathbb{R}$, содержащее $\mathbb{C}$, и $G = Gal(K/\mathbb{R})$.

а) Покажите, что порядок G - степень двойки и выведите из этого, что в $Gal(K/\mathbb{C})$, если она нетривиальна, есть подгруппа индекса 2.

б) Покажите, что $\mathbb{C} = \mathbb{R}(i)$ не имеет расширений степени 2, и выведите отсюда, что $\mathbb{C}$ алгебраически замкнуто.

6

а) Пусть p простое число, K поле характеристики p. Обозначим $\Phi : K \to K$ отображение $\Phi(x) = x^p - x$, и пусть L_a $(a \in K)$ поле разложения $X^p - X - a$. Покажите, что $L_a = L_b$ тогда и только тогда, когда существует такой $l \in \mathbb{F}_p^*$, что $b - al \in Im\Phi$ (указание: посмотрите на действие группы Галуа на корнях соответствующих многочленов).

б) Пусть теперь $car(K) \neq p$, и K содержит все корни $X^p - 1$. Пусть M_a $(a \in K^*)$ поле разложения $X^p - a$. Покажите, что $M_a = M_b$ $(b \in K^*)$ тогда и только тогда, когда существует такое целое l, $(l, p) = 1$, что $\frac{b}{a^l}$ – p-я степень в K.