Элементы комбинаторики.

A1◇1. Сколько разных слов (не обязательно осмысленных) можно получить переставляя буквы в словах

а) рок; **б)** урок; **в)** шнурок; **г)** курок; **д)** колобок;
е) $\underbrace{\text{аа}\ldots\text{а}}_{a}\underbrace{\text{бб}\ldots\text{б}}_{b}$; **ж)** $\underbrace{\text{б}_1\text{б}_1\ldots\text{б}_1}_{k_1}\underbrace{\text{б}_2\text{б}_2\ldots\text{б}_2}_{k_2}\ldots\ldots\ldots\underbrace{\text{б}_m\text{б}_m\ldots\text{б}_m}_{k_m}$;.

A1◇2. Раскройте скобки и прведите подобные слагаемые в выражениях
а) $(a_1+a_2+\cdots+a_m)^2$; **б)** $(a+b+c)^3$; **в)** $(a+b)^n$; **г)** $(a_1+a_2+\cdots+a_m)^n$.

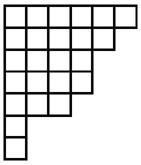
A1◇3. Имеются: 4 попарно отличающихся друг от друга чашки, 4 совершенно одинаковых гранёных стакана, 10 совершенно одинаковых кусков сахара и 7 попарно разноцветных соломинок. Сколькими способами можно разложить:
а) соломинки по чашкам **б)** сахар по чашкам **в)** сахар по стаканам
г) соломинки по стаканам

A1◇4. Как изменятся ответы в предыдущей задаче, если потребовать, чтобы после раскладывания пустых ёмкостей не оставалось?

A1◇5. Сколько решений имеет уравнение $x_1+x_2+\cdots+x_m=n$ (где m,n – фиксированные натуральные числа) **а)** в натуральных **б)** в целых неотрицательных числах?

A1◇6. Сколько существует различных отображений из m-элементного множества в n-элементное?

A1◇7. Фигурка типа



(состоящая из выравненных по правому краю клетчатых горизонтальных полосок, длина которых невозрастает сверху вниз) называется *диаграммой Юнга*. Общее число клеток в диаграмме называется её *весом*. Сколько существует диаграмм Юнга
а) веса 6; **б)** веса 7, имеющих не более 3 строк;
в) произвольного веса, но имеющих не более p строк и не более q столбцов.

Мультиномиальные коэффициенты. Если $N=n_1+n_2+\cdots+n_\nu$ (все n_i – целые неотрицательные) то мы полагаем
$$\binom{N}{n_1,n_2,\ldots,n_\nu}\stackrel{\text{def}}{=}\frac{N!}{n_1!\cdot n_2!\cdot\cdots\cdot n_\nu!}.$$
При $\nu=2$ число $\binom{n}{k,(n-k)}=\frac{n!}{k!(n-k)!}$ обозначается ерез $\binom{n}{k}$ и называется (n,k)-тым *биномиальным коэффициентом* или *числом сочетаний* из n по k). Отметим, что
$$\binom{n}{k}=\binom{n}{n-k}.$$

A1◇8. Докажите, что все описанные выше числа (например, число $1000!/100!^{10}$) являются целыми.

A1◇9. Докажите реккурентное соотношение $\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-1}{k}$.

A1◇10. Вычислите: **а)** $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n}$

б) $\binom{k}{k} + \binom{k+1}{k} + \cdots + \binom{k+n}{k}$ **в*)** $\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2$.

А1⋄11. Пусть p – простое число. Покажите, что $\binom{p}{k}$ либо равно 1 либо делится на p, и выясните

а) когда $\binom{2p}{k} \not\equiv 0 \mod p$?

б*) верно ли, что $\binom{b_0 + b_1 p + \cdots + b_k p^k}{a_0 + a_1 p + \cdots + a_k p^k} \equiv \binom{b_0}{a_0}\binom{b_1}{a_1}\cdots\binom{b_k}{a_k} \mod p$?

А1⋄12. Обозначим через $\binom{n}{k}_m$ количество всех чисел в m-ичной системе счисления с суммой цифр, равной k. Покажите, что $\binom{n}{k}_2$ совпадает с биномиальным коэффициентом $\binom{n}{k}$, а в общем случае равно коэффициенту при x^k после раскрытия скобок и приведения подобных слагаемых в выражении $(1 + x + x^2 + \cdots + x^{m-1})^n$, и докажите следующие соотношения, обобщающие предыдущие факты о числах сочетаний:

а*) $\binom{n}{k}_m = \binom{n}{n(m-1)-k}_m$

б*) $\binom{n}{k}_m = \underbrace{\binom{n-1}{k}_m + \binom{n-1}{k-1}_m + \cdots + \binom{n-1}{k-m+1}_m}_{m}$

в*) при любом фиксированном s выполнено соотношение

$$\binom{n}{k}_m = \binom{s}{0}_m \binom{n-s}{k}_m + \binom{s}{1}_m \binom{n-s}{k-1}_m + \cdots + \binom{s}{k}_m \binom{n-s}{0}_m$$

г*) $\binom{n}{0}_m^2 + \binom{n}{1}_m^2 + \cdots + \binom{n}{n(m-1)}_m^2 = \binom{2n}{n(m-1)}_m$

А1⋄13*. Подсчитайте количество счастливых автобусных таллонов[1].

[1]автобусный таллон называется счастливым, если сумма первых трёх цифр написанного на нём шестизначного номера равна сумме последних трёх цифр

Комплексные числа.

Основные понятия. Поле *комплексных чисел* $\mathbb{C}$ — это плоскость с фиксированной декартовой системой координат XOY (как на рис. 2.1). Точки $z \in \mathbb{C}$ называются *комплексными числами*. С ними связаны следующие понятия: *вещественная часть* $x = \mathrm{Re}(z)$ – координата точки z по оси $[OX)$; *мнтмая часть* $y = \mathrm{Im}(z)$ – координата точки z по оси $[OY)$; *радиус-вектор* z – вектор Oz с концом в z и началом в начале координат; *модуль* $|z|$ – длина радиус-вектора z; *аргумент* $\mathrm{Arg}(z)$ – ориентированная длина дуги, которую надо пройти по единичной окружности от луча $[OX)$ до луча $[OZ)$ (знак "+" соответствует движению против ЧС). Подчеркнём, что $\mathrm{Arg}(z)$ является *многозначной* функцией от z, поскольку определён с точностью до любого целого числа оборотов.

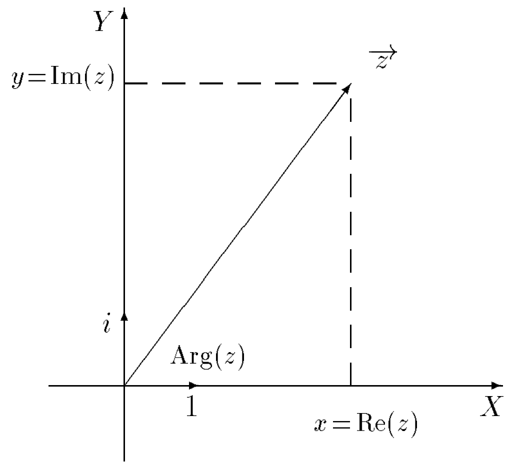


Рис. 2.1. Атрибуты комплексного числа.

Определение операций: *сложение* комплексных чисел— это сложение их радиус-векторов по праилу параллелограмма; *умножение* комплексных чисел — это перемножение их модулей с одновременным сложением аргументов[1].

Алгебраическая запись комплексных чисел. Числа с координатами $(1,0)$ и $(0,1)$ обозначаются 1 и i соответственно. Таким образом, каждое комплексное число можно алгебраически записывать в виде $z = x + iy = x \cdot 1 + y \cdot i$, где $x = \mathrm{Re}(z) = |z| \cos(\mathrm{Arg}(z))$, $y = \mathrm{Im}(z) = |z| \sin(\mathrm{Arg}(z))$.

A2◇1°. Чему равны i^2, i^3, i^4, …, i^n ?

A2◇2°. Проверьте выполнение аксиом поля для $\mathbb{C}$ (особенно обратите внимание корректность определения умножения и на дистрибутивность) и выразите действительную и мнимую части произведения и суммы двух комплексных чисел через действительную и мнимую части самих этих чисел.

A2◇3°. Выразите вещественную и мнимую часть, модуль и аргумент числа $(x+iy)^n$, где $x = \cos\varphi, y = \sin\varphi$, **а)** через z и y; **б)** через φ.

A2◇4. Вычислите (т. е. найдите вещественную и мнимые чати, модуль и аргумент):

а) $\dfrac{(5+i)(7-6i)}{3+i}$; **б)** $\dfrac{(1+i)^5}{(1-i)^3}$; **в)** $\left(\dfrac{\sqrt{3}+i}{1-i}\right)^{30}$; **г)** $(1+\cos\alpha + i\sin\alpha)^k$.

A2◇5. Решите уравнения: **а)** $z^2 + (2i-7)z + (13-i) = 0$; **б)** $z^3 = i$; **в)** $(z+1)^n - (z-1)^n = 0$; **г)** $(z+i)^n + (z-i)^n = 0$; **д)** $\overline{z} = z^3$.

A2◇6. Выразите $\cos\dfrac{2\pi}{5}$ и $\sin\dfrac{4\pi}{5}$ в радикалах.

A2◇7. Всегда ли вещественная и мнимая части корня квадратного уравнения с комплексными коэффициентами выражаются в радикалах через вещественные и мнимые части коэффициентов уравнения?

A2◇8. Вычислите сумму и произведение **а)** всех корней **б)** s-тых степеней всех корней степени n из 1.

A2◇9. Вычислите суммы: **а)** $\binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \cdots$; **б)** $\binom{n}{1} + \binom{n}{5} + \binom{n}{9} + \cdots$;
в) $\binom{n}{1} - \dfrac{1}{3}\binom{n}{5} + \dfrac{1}{9}\binom{n}{9} + \cdots$; **г)** $\sin x + \sin 2x + \cdots + \sin nx$;
д) $\sin^2 x + \sin^2 3x + \cdots + \sin^2(2n-1)$; **е)** $\cos x + 2\cos 2x + \cdots + n\cos nx$.

A2◇10. Пусть $m \in \mathbb{N}$ — нечётно. Убедитесь, что $\dfrac{\sin mx}{\sin x}$ является многочленом от $\sin^2 x$, найдите его степень, корни и старший коэффициент и докажите тождества:

а) $\dfrac{\sin(mx)}{\sin\, x} = (-4)^{\frac{m-1}{2}} \prod\limits_{j=0}^{\frac{m-1}{2}} \left(\sin^2 x - \sin^2\left({}^{2\pi j}\!\big/_{m}\right)\right)$;

б) $(-1)^{\frac{m-1}{2}} \sin(mx) = 2^{m-1} \prod\limits_{j=0}^{m-1} \sin\left(x + {}^{2\pi j}\!\big/_{m}\right)$.

А2◇11. Вычмслите $z^m + 1/z^m$, если $z + 1/z = 2\cos\theta$.

А2◇12. Куда отображения $z \longmapsto z^2$ и $z \longmapsto 1/z$ переводят:
а) прямую $y = kx$; **б)** окружность $|z+i| = 1$;
в) координатную сетку; **г)** кошечку с рис. 2.2?

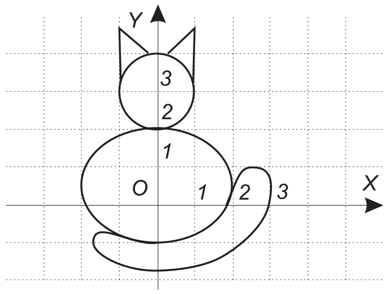


Рис. 2.2. Комплексная кошечка

А2◇13. Верно ли, что попарно разные $z_1,\ z_2,\ z_3 \in \mathbb{C}$ тогда и только тогда лежат на одной прямой, когда $\dfrac{z_1 - z_3}{z_2 - z_3}$ вещественно?

А2◇14. Верно ли, что четыре попарно разные точки $z_1,\ z_2,\ z_3,\ z_4 \in \mathbb{C}$, не лежащие на одной прямой, тогда и только тогда лежат на одной окружности, когда их *двойное отношение* $\dfrac{(z_1 - z_3) : (z_2 - z_3)}{(z_1 - z_4) : (z_2 - z_4)}$ вещественно?

А2◇15. Докажите, что отображение $z \longmapsto (az+b)/(cz+d)$ (где $a, b, c, d \in \mathbb{C}$) переводит окружности и прямые или в окружности или в прямые, сохраняя при этом углы.

А2◇16. Верно ли, что всякое комплексное число $z \neq -1$ с $|z| = 1$ можно представить в виде $z = \dfrac{1+ti}{1-ti}$ с $t \in \mathbb{R}$?

Сравнения и вычеты.

А3◇1. Докажите, что уравнение $15x^2 - 7y^2 = 9$ не имеет решений в целых числах.

А3◇2. Докажите, что уравнения $x^2 + y^2 + z^2 = 2xyz$ и $5x^3 + 11y^3 + 13z^3 = 0$ не имеют целочисленных решений, кроме $x = y = z = 0$.

Кольцо вычетов $\mathbb{Z}/n\mathbb{Z}$ состоит, по определению, из n остатков $0, 1, \dots, (n-1)$ от деления на n. Элементы кольца вычетов можно складывать и умножать — результатами этих опреаций , по определению, считаются остаток от суммы и остаток от произведения остатков-операндов.

А3◇3°. Проверьте, что $\mathbb{Z}/n\mathbb{Z}$ удовлетворяет аксиомам коммутативного кольца с единицей.

А3◇4. Составьте таблицы умножения для колец $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ и $\mathbb{Z}/8\mathbb{Z}$. В каждом из этих колец найдите все обратимые элементы, все квадраты, все делители нуля и все нильпотенты.

А3◇5°. Проверьте, что отображение $\mathbb{Z} \xrightarrow{res_n} \mathbb{Z}/n\mathbb{Z}$, переводящее число $m \in \mathbb{Z}$ в его остаток от деления на n является *гомоморфизмом колец*, т. е. переводит суммы в суммы, а произведения – в произведения.

Редукция по модулю n — это научное название для гомоморфизма из предыдущей задачи. Применяя редукцию по модулю n к какому-либо уравнению в кольце $\mathbb{Z}$ мы получаем уравнение $\mathbb{Z}/n\mathbb{Z}$, причём из его неразрешимости в $\mathbb{Z}/n\mathbb{Z}$ вытекает, очевидно, неразрешимость исходного уравнения в $\mathbb{Z}$. Ввиду конечности кольца $\mathbb{Z}/n\mathbb{Z}$, анализ разрешимости уравнений часто резко упрощается при редукции по подходящему модулю. Имея это в виду вернитесь ещё раз к зад. А3◇1 и зад. А3◇2.

Алгоритм Евклида есть процедура, позволяющая быстро отыскать *НОД* пары натуральных чисел A, B (или многочленов A, B от одной переменной над полем) и состоящая в следующем. Пусть $A > B$ (соотв. $\deg A > \deg B$). Положим

$$E_1 = A\ , \quad E_2 = B\ , \quad E_\nu = \text{остаток от деления } E_{\nu-2} \text{ на } E_{\nu-1} \quad .$$

Последовательность E_ν (соотв. $\deg E_\nu$) строго монотонно убывает до тех пор, пока очередной E_ν не будет нулевым. Последний ненулевой элемент последовательности E_ν равен *НОД*(A, B).

А3◇6. Докажите это и убедитесь, что *НОД* делится нацело на любой другой общий делитель.

А3◇7. Пусть A, B – целые числа (соотв. многочлены). Докажите, что всегда можно подобрать такие целые числа (соотв. многочлены) a, b, что $aA + bB =$ *НОД*(A, B). Подберите такие a, b и вычислите *НОД*(A, B) для **а)** $A = 1537,\ B = 1387$; **б)** $A = x^5 - 1,\ B = x^4 + x^2 + 1$.

А3◇8. Пусть m – произвольное, а a, b – взаимно простые числа (или элементы $k[x]$). Докажите, что **а)** m делится и на ab, если m делится и на a и на b; **б)** a делит m, если a делит mb.

А3◇9. Докажите, что класс $k \mod n$ тогда и тоько тогда обратим в $\mathbb{Z}/n\mathbb{Z}$, когда n и k взаимно просты в $\mathbb{Z}$.

А3◇10. Пусть p – простое число. Будет ли $\mathbb{Z}/p\mathbb{Z}$ полем? Найдите все $x \in \mathbb{Z}/p\mathbb{Z}$, такие что $x^2 = 1$, и вычислите произведение всех ненулевых чисел в $\mathbb{Z}/p\mathbb{Z}$.

А3◇11 (теорема Вильсона). Докажите, что натуральное $p \geqslant 2$ является простым тогда и только тогда, когда $(p-1)! + 1 \equiv 0 (\mod p)$.

А3◇12 (малая теорема Ферма). Докажите, что для любого целого числа m, не делящегося на простое число p, выполнено сравнение $m^{p-1} \equiv 1 \mod p$.

А3◇13. Пусть p – простое число. Выясните, сколько всего ненулевых квадратов в $\mathbb{Z}/p\mathbb{Z}$ и всегда ли в $\mathbb{Z}/p\mathbb{Z}$ разрешимо уравнение $x^2 + y^2 = -1$.

А3◇14. Какие значения может принимать функция $y = x^{\frac{p-1}{2}}$ на ненулевых элементах $\mathbb{Z}/p\mathbb{Z}$ при простом p? Верно ли, что ненулевой $x \in \mathbb{Z}/p\mathbb{Z}$ тогда и только тогда является квадратом, когда $x^{\frac{p-1}{2}} = 1$?

А3⋄15[*] (лемма Гаусса). Запишем все числа из $\mathbb{Z}/p\mathbb{Z}$ (где p – простое) по порядку в виде

$$-\frac{p-1}{2}\,,\ \ldots\,,\ -1\,,\ 0\,,\ 1\,,\ \ldots\,,\ \frac{p-1}{2}\,.$$

Докажите, что

а) a тогда и только тогда квадрат в $\mathbb{Z}/p\mathbb{Z}$, когда в предыдущей записи чётное число положительных чисел меняет знак при умножении на a;

б) -1 квадрат в $\mathbb{Z}/p\mathbb{Z}$ тогда и только тогда, когда $p \equiv 1 \pmod 4$ или $p = 2$;

в) 2 квадрат в $\mathbb{Z}/p\mathbb{Z}$ тогда и только тогда, когда $(p^2-1)/8$ чётно.

Квадратичная взаимность. Пусть p – простое число. Сопоставим каждому $n \in \mathbb{Z}$ *символ Лежандра - Якоби* $\left(\frac{n}{p}\right) \in \{-1\,,0\,,1\,\}$, значение которого равно нулю, если n делится на p, единице – если n является ненулевым квадратом в $\mathbb{Z}/p\mathbb{Z}$, и -1 — в остальных случаях.

А3⋄16. Докажите, что $\left(\frac{n}{p}\right)$ — мультипликативный характер[1] и что $\sum\limits_{i=1}^{p-1}\left(\frac{i}{p}\right) = 0$.

А3⋄17[*]. Докажите, что знак $\left(\frac{m}{p}\right)$ совпадает со знаком произведения $\prod\limits_{j=1}^{(p-1)/2}\dfrac{\sin\left(m\cdot 2\pi j/p\right)}{\sin\left(2\pi j/p\right)}$.

Указание. воспользуйтесь леммой Гаусса

А3⋄18[*] (квадратичный закон взаимности). Докажите, что для любых простых чисел p, q

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\,.$$

Указание. воспользуйтесь предыдущей задачей и разложите все перемножаемые дроби на множители по формулам из листка «Комплексные числа».

А3⋄19. Найдите $\left(\frac{43}{109}\right)$.

[1]функция $\mathbb{Z} \xrightarrow{f} \mathbb{C}$ называется *мультипликативным характером*, если $f(mn) = f(m)f(n)$ всякий раз, когда $\text{нод}(m,n) = 1$

Коммутативные кольца, гомоморфизмы и идеалы

Терминология. Отображение $A \xrightarrow{\varphi} B$ называется *гомоморфизмом колец*[1] если $\forall\, a_1, a_2 \in A$ в кольце B выполнены соотношения $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$ и $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2)$. Взаимно однозначные гомомоморфизмы называются *изоморфизмами*, а изоморфизмы на себя называются *автоморфизмами*.

А4◇1. Пусть $A \xrightarrow{\varphi} B$ – ненулевой гомоморфизм коммутативных колец с единицами. Верно ли, что $\varphi(1) = 1$? Изменится ли ответ, если в B нет делителей нуля?

А4◇2. Найдите все автоморфизмы

а) поля $\mathbb{C}$, оставляющие элементы из $\mathbb{R}$ неподвижными.

б*) поля $\mathbb{Q}[\sqrt[3]{2}] \stackrel{\text{def}}{=} \mathbb{Q}[x]/(x^3 - 2)$.

А4◇3°. Проверьте, что *образ* $\operatorname{im}\varphi \stackrel{\text{def}}{=} \{\, b \in B \mid \exists a \in A \varphi(a) = b \,\}$ гомоморфизма колец $A \xrightarrow{\varphi} B$ является подкольцом в B, а *ядро* $\ker\varphi \stackrel{\text{def}}{=} \{\, a \in A \mid \varphi(a) = 0 \,\}$ является *идеалом*[2] в A, причём $\ker\varphi = \{0\}$ тогда и только тогда, когда φ – вложение.

А4◇4°. Докажите, что кольцо является полем тогда и только тогда, когда оно не имеет идеалов, отличных от (0) и самого кольца.

Китайская теорема об остатках. Прямой суммой $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ колец[3] называется кольцо, элементами которого являются упорядоченные наборы $(a_1, a_2, \ldots, a_n)$ из $a_\nu \in A_\nu$ с *покоординатным* сложением и умножением.

А4◇5. Докажите, что если $m = rs$ и $НОД(r, s) = 1$, то $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/r\mathbb{Z} \oplus \mathbb{Z}/s\mathbb{Z}$, и выведите из этого, что если число m разложено на простые множители: $m = p_1^{k_1} \cdot \cdots \cdot p_n^{k_n}$, то имеется изоморфизм колец $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{k_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{k_n}\mathbb{Z}$.

А4◇6. Сформулируйте и докажите аналог предыдущей задачи для кольца многочленов $k[x]$, где k — произвольное поле.

А4◇7. Решите в $\mathbb{Z}/360\mathbb{Z}$ уравнения **а)** $x^2 = 1$ **б)** $x^3 = 1$ **в)** $x^2 = 49$.

А4◇8. Опишите все многочлены $f \in \mathbb{Q}[x]$, имеющие остатки $1 + x$, $1 + x^3$ и $1 + x^5$ от деления на $1 + x^2$, $1 + x^4$ и $1 + x^8$ соответственно.

Евклидовость. Кольцо A называется *евклидовым*, если в нём нет делителей нуля и имеется *функция высоты* λ из множества ненулевых элементов A в множество целых неотрицательных чисел, обладающая свойством $\lambda(ab) \geqslant \max\bigl(\lambda(a), \lambda(b)\bigr)$ и такая, что $\forall\, a, b \in A,\ b \neq 0$ найдутся q и r из A такие, что $a = bq + r$ и либо $r = 0$, либо $\lambda(r) < \lambda(b)$. Кольцо A называется *кольцом главных идеалов*, если все идеаля в A имеют вид $(a) \stackrel{\text{def}}{=} aA = \{ax \mid x \in A\}$ с $a \in A$.

А4◇9°. Убедитесь, что кольца $\mathbb{Z}$ и $k[x]$, где k – поле, евклидовы.

А4◇10. Докажите, что всякое евклидово кольцо является кольцом главных идеалов.

А4◇11. Докажите, что кольцо $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$, где $\omega \neq 1$ – один из комплексных корней уравнеия $z^3 = 1$, является евклидовым относительно высоты $\lambda(z) = |z|^2$ и опишите множество обратимых элементов этого кольца.

А4◇12. Докажите, что кольца $\mathbb{Q}[x, y]$ и $\mathbb{Z}[x]$ не являются кольцами главных идеалов.

Терминология. Идеал $\mathfrak{a}$ в коммутативном кольце A с единицей называется *простым*, если в кольце $A/\mathfrak{a}$ нет делителей нуля, и *максимальным*, — если $A/\mathfrak{a}$ – поле. Элемент $a \in A$ называется *простым*, если идеал (a) прост, и *неприводимым*, — если a не представим в виде произведения двух необратимых элементов.

---

[1] что такое *коммутативное кольцо с единицей* и что такое *поле* см. в каом-нибудь учебнике алгебры, например в записках лекций

[2] подкольцо $\mathfrak{i} \subset A$ называется *идеалом*, если $a\mathfrak{i} \stackrel{\text{def}}{=} \{ax \mid x \in \mathfrak{i}\} \subset \mathfrak{i} \quad \forall\, a \in, A$

[3] иногда вместо «прямая сумма» говорят «прямое произведение» и пишут $A_1 \times A_2 \times \cdots \times A_n$, что более правильно с «общекатегорной» точки зрения, но в рассматриваемых нами случаях обозначает в точности то же самое

A4◇13°. Докажите, что максимальные идеалы просты, а простые элементы неприводимы.

A4◇14. Докажите, что в евклидовом кольце простота элемента равносильна его неприводимости.

A4◇15*. Глядя на равенство $2 \cdot 2 = (\sqrt{5}+1)\cdot(\sqrt{5}-1)$ в кольце $\mathbb{Z}[\sqrt{5}]$, укажите в этом кольце неприводимый непростой элемент.

A4◇16°. Докажите, что простота элемента p равносильно тому, что при произвольных $a, b \in A$ элемент p делит произведение ab лишь при условии, что он делит хотя бы один из сомножителей.

A4◇17°. Докажите, что идеал является максимальным тогда и только тогда, когда он не содержится ни в каком строго большем идеале, отличном от всего кольца.

A4◇18. Будет ли факторкольцо $\mathbb{R}[x]/(f(x))$ полем при $f = x^4+1$, $f = x^3+1$ и $f = x^2+3$?

A4◇19. Докажите, что многочлен $x^{p-1} + ... + x + 1$ неприводим над $\mathbb{Q}$ при простом $p > 1$.
Указание: воспользуйтесь *критерием Эйзенштейна*.

A4◇20. Пусть $f(x)$ - неприводимый многочлен степени n над полем $\mathbb{Z}/p\mathbb{Z}$ (p - простое число). Докажите, что фактор-кольцо $(\mathbb{Z}/p\mathbb{Z})\,[x]\big/(f)$ есть конечное поле и найдите число его элементов.

A4◇21. Пусть $f, g \in \mathbb{Z}[x]$ не имеют общих делителей, отличных от ± 1. Докажите, что факторкольцо $\mathbb{Z}[x]/(f, g)$ конечно.

A4◇22. Докажите, что в кольце главных идеалов всякий элемент является произведением конечного числа неприводимых элементов.
Указание: воспользуйтесь тем, что в кольце главных идеалов нельзя построить бесконечной возрастающей цепочки строго вложенных друг в друга идеалов.

A4◇23. Докажите, что в кольце $k[x]$ многочленов над *любым* полем имеется бесконечно много неприводимых многочленов.

A4◇24. В кольце $k[[x]]$ формальных степенных рядов над полем k опишите все идеалы и все максимальные идеалы.

A4◇25. Гауссовы целые числа. Пусть $\Gamma = \{m + ni \in \mathbb{C} \mid m, n \in \mathbb{Z}\}$ — кольцо *целых гауссовых чисел*. Докажите, что

- **а)** Γ – евклидово кольцо относительно высоты $\lambda(z) = |z|^2$;
- **б)** если числа m_1 и m_2 представимы в виде суммы квадратов двух неотрицательных целых чисел, то и их произведение $m_1 m_2$ тоже представимо;
- **в)** следующие условия на простое число $p \in \mathbb{Z}$ попарно равносильны:
  - (a) $p \in \mathbb{Z}$ перестаёт быть простым в Γ;
  - (b) p представимо в виде суммы квадратов двух неотрицательных целых чисел;
  - (c) -1 является квадратом в $\mathbb{Z}/p\mathbb{Z}$;
  - (d)* $p \not\equiv 3 \pmod 4$.

A4◇26*. Докажите, что натуральное число тогда и только тогда не является квадратом и не представляется в виде суммы двух квадратов, когда в его разложении на простые множители участвует хотя бы одно простое число вида $4k+3$ в нечётной степени.

A4◇27. Существует ли в кольце гауссовых целых чисел Γ такой идеал $\mathfrak{a} \subset \Gamma$, что факторкольцо $\Gamma/\mathfrak{a}$ является **а)** полем характеристики 2? **б)** полем характеристики 3?
(в случае положительного ответа укажите, сколько элементов может быть в этом поле).

Примеры на делимость

Функция Эйлера. Для каждого $n \in \mathbb{Z}$ обозначим через $\varphi(n)$ *функцию Эйлера* — число обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$ (т. е. количество всех взаимно простых с n чисел $k \in \mathbb{N}$, не превосходящих $n-1$).

А$4\frac{1}{2}\diamond$1. Проверьте, что функция Эйлера является мультипликативным характером, и что если $m = p_1^{k_1} \cdot \dots \cdot p_n^{k_n}$ — разложение на простые множители, то

а) $\varphi(m) = \varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_n^{k_n})$; **б)** $\varphi(m) = m \cdot \left(1 - \dfrac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \dfrac{1}{p_n}\right)$.

А$4\frac{1}{2}\diamond$2. Найдите все m такие, что $\varphi(m) = 10$.

А$4\frac{1}{2}\diamond$3 (теорема Эйлера). Выясните, чему равно произведение всех обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$ и вычислите $a^{\varphi(m)}$ для данного обратимого $a \in \mathbb{Z}/n\mathbb{Z}$.

Функция Мёбиуса. Пусть $m \in \mathbb{Z}$ разложено на простые множители: $m = p_1^{k_1} \cdot \dots \cdot p_n^{k_n}$; значение *функции Мёбиуса* $\mu(m)$ на числе m по определению равно 0, если хоть один из показателей $k_i \geqslant 2$ (т. е. если m делится на ненулевой квадрат), и равно $(-1)^n$, если все показатели $k_1, k_2, \dots, k_n$ равны 1. В частности, при $m = 0$ имеем $\mu(1) \stackrel{\text{def}}{=} 1$.

А$4\frac{1}{2}\diamond$4. Убедитесь, что $\mu(m)$ является мультипликативным характером, и докажите тождество $\sum\limits_{d|n} \mu(d) = \begin{cases} 1, & \text{при } n = 1 \\ 0, & \text{при } n > 1 \end{cases}$.

А$4\frac{1}{2}\diamond$5 (обращение Мёбиуса). Пусть для функции $\mathbb{N} \xrightarrow{g} \mathbb{C}$ при каждом $n \in \mathbb{N}$ известно значение суммы $\sigma(n) = \sum\limits_{d|n} g(d)$. Докажите, что тогда функцию g можно восстановить по функции σ при помощи формулы $g(n) = \sum\limits_{d|n} \mu(n/d)\sigma(d)$.

А$4\frac{1}{2}\diamond$6. Для данного $m \in \mathbb{N}$ вычислите $\sum\limits_{d|m} \varphi(d)$.

Круговые многочлены. Комплексное число $\zeta \in \mathbb{C}$ называется *первообразным корнем n-той степени*, если все комплексные решения уравнеия $z^n = 1$ являются степенями ζ. Многочлен $f_n(x) \stackrel{\text{def}}{=} \prod\limits_{\zeta}(x - \zeta) \in \mathbb{C}[x]$, где ζ пробегает все различные первообразные корни степени n, называется *n-тым круговым многочленом*.

А$4\frac{1}{2}\diamond$7. Для любого ли $n \in \mathbb{N}$ существуют первообразные корни n-той степени?

А$4\frac{1}{2}\diamond$8. Правда ли, что $x^n - 1 = \prod\limits_{d|n} f_d(x)$? Используя подходящую модификацию обращения Мёбиуса, докажите, что $f_n(x) = \prod\limits_{d|n}(x^{n/d} - 1)^{\mu(d)}$.

А$4\frac{1}{2}\diamond$9. Докажите, что при всех $n \in \mathbb{N}$ n-тый круговой многочлен f_n имеет степень $\varphi(n)$, целые коэффициенты и неприводим над $\mathbb{Z}$.

А$4\frac{1}{2}\diamond$10. Пусть $p \in \mathbb{N}$ – простое. Верно ли, что: **а)** $f_{2n}(x) = f_n(-x)$ при нечётном n;

б) $f_p(x) = x^{p-1} + \dots + x + 1$; **в)** $f_{p^k}(x) = f_p\left(x^{p^{k-1}}\right)$ **г)** $f_{pm}(x) = \dfrac{f_m(x^p)}{f_m(x)}$ при $p \not| m$.

А$4\frac{1}{2}\diamond$11. Докажите, что если $m = p_1^{k_1} \cdot \dots \cdot p_n^{k_n}$ (p_i — различные простые числа), то

$$f_m(x) = f_{p_1 p_2 \cdots p_n}\left(x^{p_1^{k_1-1} \cdots p_n^{k_n-1}}\right).$$

Первообразные корни в кольце вычетов. Пусть a – обратимый элемент кольца $\mathbb{Z}/n\mathbb{Z}$. Назовём *порядком* вычета a наименьшее натуральное число k такое, что $a^k = 1$. Элемент a называется *первообразным корнем по модулю n*, если все прочие обратимые вычеты являются его степенями.

A$4\frac{1}{2}\diamond$12. Пусть порядки $k_1, k_2, \ldots, k_n$ вычетов $a_1, a_2, \ldots, a_n$ попарно взаимно просты. Чему равен порядок вычета $a = a_1 \cdot \cdots \cdot a_n$?

A$4\frac{1}{2}\diamond$13. Пусть вычеты порядков k и l существуют. Существует ли вычет порядка $HOK(k,l)$?

A$4\frac{1}{2}\diamond$14. Докажите, что для существования первообразного корня необходимо и достаточно существование обратимого вычета порядка $\varphi(n)$. По любому ли простому модулю существует первообразный корень?

A$4\frac{1}{2}\diamond$15*. Пусть ϱ — первообразный корень по простому модулю $p > 2$. Докажите, что существует $\vartheta \in \mathbb{N}$, такое что $(\varrho + p\vartheta)^{p-1} \equiv 1 \mod p$, но $(\varrho + p\vartheta)^{p-1} \not\equiv 1 \mod p^2$. Верно ли, что класс $\varrho + p\vartheta$ является первообразным корнем по модулю p^k для всех $k \in \mathbb{N}$?

A$4\frac{1}{2}\diamond$16*. Докажите существование первообразного корня $\bmod 2\,p^k$ $\forall\, k \in \mathbb{N}$ и простого p.

A$4\frac{1}{2}\diamond$17. Существует ли первообразный корень по модулю 21?

Комбинаторика обращения Мёбиуса

ЧУМЫ. Множество $\mathfrak{P}$, для *некоторых* пар элементов которого задано отношение порядка $\leqslant$ со свойствами:

$$(1)\quad (x \leqslant y \quad \& \quad y \leqslant x) \Leftrightarrow (x = y); \qquad\qquad (2)\quad (x \leqslant y \quad \& \quad y \leqslant z) \Rightarrow (x \leqslant z)\ .$$

частично упорядоченным множеством (сокращённо ЧУМом). ЧУМ называется *локально конечным*, если для всех $x, y \in \mathfrak{P} \times \mathfrak{P}$ множество $[x,y] \stackrel{\text{def}}{=} \{\, z \mid x \leqslant z \leqslant y \,\}$ – конечно. Множество функций $\varrho(x,y)$: $\mathfrak{P} \times \mathfrak{P} \longrightarrow \mathbb{C}$, удовлетворяющих условию $\varrho(x,y) = 0$ при $x > y$, с операциями

$$[\varrho_1 + \varrho_2]\,(x,y) \stackrel{\text{def}}{=} \varrho_1(x,y) + \varrho_2(x,y) \qquad \text{и} \qquad [\varrho_1 \star \varrho_2]\,(x,y) \stackrel{\text{def}}{=} \sum_{x \leqslant z \leqslant y} r_1(x,z) r_2(z,y)$$

называется *агеброй инцидентности* ЧУМа $\mathfrak{P}$ и обозначается через $\mathcal{A}(\mathfrak{P})$.

A$4\frac{1}{2}\diamond$18. Будет ли локально конечным ЧУМом множество: **а)** $\mathbb{Z}$ с отношением $n|m$.
б) конечных подмножеств данного множества с отношением $X \subseteq Y$;
в) вершин ориентированного графа ($x \leqslant y$ если имеется ориентированный путь из x в y);

A$4\frac{1}{2}\diamond$19. Проверьте, что $\mathcal{A}(\mathfrak{P})$ является (некоммутативным) кольцом с единицей и докажите, что $\varrho(x,y) \in \mathcal{A}(\mathfrak{P})$ обратим тогда и только тогда, когда $\varrho(x,x) \neq 0 \quad \forall\, x \in \mathfrak{P}$.

Обращение Мёбиуса. Функция $\zeta(x,y) \stackrel{\text{def}}{=} \begin{cases} 1\,, & \text{при} \quad x \leqslant y \\ 0\,, & \text{при} \quad x > y \end{cases}$ называется *функцией инцидентности* (или ζ-*функцией*), а функция $\mu(x,y)$, обратная к $\zeta(x,y)$ в $\mathcal{A}(\mathfrak{P})$, — *функцией Мебиуса* ЧУМа $\mathfrak{P}$.

A$4\frac{1}{2}\diamond$20. Докажите равенства: **а)** $\mu(x,y) = -\sum\limits_{x \leqslant z < y} \mu(x,z)$; **б)** $\mu(x,y) = -\sum\limits_{x < z \leqslant y} \mu(z,y)$.

A$4\frac{1}{2}\diamond$21. Постройте функцию Мебиуса для $\mathbb{Z}$ с отношением $x|y$, для множества всех подмножеств данного n-элементного множества и для ориентированного дерева.

A$4\frac{1}{2}\diamond$22 (формула обращения). Пусть для функции $\mathfrak{P} \xrightarrow{g} \mathbb{C}$ известны значения всех сумм $\sigma(x) = \sum\limits_{y<x} g(y)$. Верно ли, что g восстанавливается из σ по формуле $g(x) = \sum\limits_{y<x} \sigma(y)\mu(y,x)$?

Письменная контрольная работа по темам «поля», «кольца», «делимость».

А5◇1. Вычислите $НОД(A, B)$ и представьте его в виде $Ax + By$ с $x, y \in K$ для

а) $A = 10013$, $B = 6213$ в $K = \mathbb{Z}$;

б) $A = 57 + 2i$, $B = 91 + 444i$ в $K = \Gamma$.

А5◇2. Сколько решений имеет уравнение $x^7 = 35$ в $\mathbb{Z}/601\mathbb{Z}$?

А5◇3. Решите сравнение $6x^3 + 27x^2 + 17x + 20 \equiv 0 (\mod 30)$.

А5◇4. Выясните:

а) будет ли кольцо $\mathbb{Q}[\vartheta]$, где $\vartheta^5 = 1$, (т. е факторкольцо $\mathbb{Q}[x]/(x^5 - 1)$) полем?

б) будет ли $1 + \vartheta^2 + \vartheta^4$ обратим в нём (если да, то найдите обратный к нему элемент, если нет, объясните почему)?

А5◇5. Найдите все неприводимые многочлены степени 2 и выясните сколько имеется неприводимых многочленов степени 3 над полями $\mathbb{Z}/2\mathbb{Z}$ и $\mathbb{Z}/3\mathbb{Z}$.

А5◇6. В кольце $\mathbb{Z}[x]$ разложите на неприводимые множители или докажите неприводимость многочленов:

а) $t^4 + t + 1$,

б) $t^5 + t^4 + t^2 + t + 2$,

в) $t^6 + t^3 + 1$.

Матричная алгебра

А6◇1. Найти все матрицы, коммутирующие с матрицей $\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$.

А6◇2. Найти все квадратные матрицы размера $n \times n$, коммутирующие с любой матрицей того же размера.

А6◇3. Вычислите: **а)** $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n$; **б)** $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}^n$; **в)** $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^n$; **г)** $\begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix}^n$;

А6◇4. Вычислите значения многочленов $f(x) = 2x^2 - 3x + x^0$ и $g(x) = a_0x^n + a_1x^{n-1} + ... + a_nx^0$ на матрицах **а)** $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$; **б)** $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$; **в*)** $\begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix}$; **г*)** $\begin{pmatrix} a & 1 & 0 \\ 0 & b & 1 \\ 0 & 0 & c \end{pmatrix}$.

А6◇5. Пусть $a_1, a_2, \ldots, a_n$ — целые положительные числа, $\varepsilon_k = \cos\dfrac{2\pi}{a_k} + i\sin\dfrac{2\pi}{a_k}$. В какой наименьшей степени матрица $\begin{pmatrix} 0 & & \varepsilon_1 \\ & \iddots & \\ \varepsilon_n & & 0 \end{pmatrix}$ будет равна E?

А6◇6. Напишите уравние, корнем которого является матрица $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

А6◇7. Пусть матрица $A \in \mathrm{Mat}_2(\mathbb{Z})$ является решением уравнения $x^2 = 2$. Будет ли $K[A]$ полем при: **а)** $K = \mathbb{Z}$; **б)** $K = \mathbb{Q}$; **в)** $K = \mathbb{R}$.

А6◇8*. Для какого класса матриц A из $M_2(\mathbb{R})$ кольцо $\mathbb{R}[A]$ изоморфно полю комплексных чисел?

А6◇9. Образуют ли кольца квадратные матрицы вида

а) $\begin{pmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{pmatrix}$ (верхнетреугольные); **б)** $\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ (диагональные)

А6◇10. Образуют ли группы (по умножению) квадратные матрицы вида

а) $\begin{pmatrix} 1 & & & & \\ & 1 & & a_{ij} & \\ & & \ddots & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}$ с $a_{ij} \in \mathbb{C}$ и нулями в остальных местах;

б) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & \cos\alpha & 0 & -\sin\alpha \\ 0 & 0 & 1 & 0 \\ 0 & \sin\alpha & 0 & \cos\alpha \end{pmatrix}$; **в)** $\begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix}$ (верхнетреугольные унипотентные)

А6◇11. Докажите, что множество матриц $H = \left\{ \begin{pmatrix} a & b & c & d \\ b & -a & -d & c \\ c & d & -a & -b \\ d & -c & b & -a \end{pmatrix} \right\}$ образует группу по умножению и сложению.

А6◇12. Пусть A, B, …, C_1, D_1 - квадратные матрицы одного порядка. Выразите блоки произведения матриц $\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$ через исходные восемь матриц и обобщите полученную формулу на неквадратные матрицы.

A6◇13*. Напишите явную формулу для (ij)-того элемента матрицы, обратной к верхнетреугольной унипотентной матрице (h_{ij}) (где $h_{ii} = 1$ и $h_{ji} = 0$ при $j > i$).

A6◇14*. Пусть A, B, C, D - невырожденные матрицы. Докажите, что

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1} = \begin{pmatrix} (A - BD^{-1}C)^{-1} & (C - DB^{-1}A)^{-1} \\ (B - AC^{-1}D)^{-1} & (D - CA^{-1}B)^{-1} \end{pmatrix}.$$

Терминология. Пусть A и B - квадратные матрицы; матрица $[A, B] \stackrel{\text{def}}{=} AB - BA$ называтся их *коммутатором*. Число $\vartriangle A \stackrel{\text{def}}{=} \sum\limits_i a_{ii}$ называется *следом* квадратной матрицы A. Матрица $A \neq 0$ называется *нильпотентной*, если $A^n = 0$ для некоторого $n \in \mathbb{N}$. Матрица A называется *унипотентной*, если $A = E + N$, где N — нильпотентная матрица.

A6◇15. Докажите, что $\vartriangle[A, B] = 0$ для любых квадратных матриц A, B.

A6◇16. Докажите, что для любых квадратных матриц A, B, C выполняются *правила Лейбница*:
а) $[A, BC] = [A, B]C + B[A, C]$, **б)** $[A, [B, C]] = [[A, B], C] + [B, [A, C]]$.

A6◇17. Выразите $(A + B)^n$ через $A^i B^j$, если **а)** $[A, B] = 0$; **б*)** $[A, B] = B$,; **в*)** $[A, B] = A$.

A6◇18. Верно ли, что сумма двух нильпотентных матриц A и B нильпотентна? Докажите, что это так, если матрицы **а)** A и B **б)** A и $[A, B]$ перестановочны.

A6◇19. Верно ли, что если A – нильпотентна, то то матрица $E \pm A$ обратима?

A6◇20. Для ненулевого $a \in \mathbb{C}$ вычислите: **а)** $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1}$; **б)** $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}^{-1}$; **в)** $\begin{pmatrix} a & 1 & 1 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}^{-1}$.

A6◇21. Пусть A - нильпотентная матрица, G - множество матриц вида $f(A)$, где f - формальный степенной ряд от одной переменной без свободного члена. Докажите, что G - группа относительно операции $f(A) * g(A) \stackrel{\text{def}}{=} f(A) + g(A) - f(A)g(A)$.

A6◇22*. Докажите, что матрица A над полем конечной характеристики унипотентна тогда и только тогда, когда $A^n = E$ для некоторого $n \in \mathbb{N}$.

A6◇23*. Докажите, что пары матриц

а) $\begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$ и $\begin{pmatrix} 0 & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix}$;

б) $\begin{pmatrix} 1 & & & 0 \\ & 2 & & \\ & & \ddots & \\ 0 & & & n \end{pmatrix}$ и $\begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & 0 & \ddots & 1 \\ 1 & & & 0 \end{pmatrix}$

порождают алгебру матриц $\mathrm{Mat}_n(\mathbb{C})$ над полем $\mathbb{C}$, т.е. любая матрица из $\mathrm{Mat}_n(\mathbb{C})$ может быть получена из них конечным числом операций умножения, сложения и умножения на число.

Векторные пространства и модули

А7◇1. Множество W многочленов из $\mathbb{Z}[x]$ с четным свободным членом является модулем над $\mathbb{Z}[x]$. Является ли этот модуль: **а)** конечно порожденным? **б)** свободным?

А7◇2. Убедитесь, что всякий конечно порожденный модуль является гомоморфным образом конечно порожденного свободного модуля. Задайте этот гомоморфизм явно и найдите его ядро для модуля W из предыдущей задачи.

А7◇3. Обозначим через $\mathbb{F}_p$ поле вычетов $\mathbb{Z}/p\mathbb{Z}$, где p – простое. Сколько одномерных и двумерных подпространств имеется в векторном пространстве ${\mathbb{F}_p}^3$ и сколько прямых и плоскостей имеется в аффинном пространстве ${\mathbb{F}_p}^3$?

А7◇4. Те же вопросы про n-мерные пространства над конечным полем $\mathbb{F}_q$ из q элементов.

А7◇5. Пусть $A = (a_{ij})$ есть $n \times n$ матрица, у которой

$$a_{ni} = \sum_{j=1}^{n-1} \lambda_j a_{ji}$$

Решите систему линейных уравнений $Ax = 0$.

А7◇6*. Целозначные многочлены. Пусть $M \subset \mathbb{Q}[t]$ – множество всех многочленов, принимающих целые значения при всех целых t (такие многочлены иногда называют *целозначными*). Убедитесь, что они составляют $\mathbb{Z}$-модуль и докажите, что

а) многочлены $\gamma_k(t) \stackrel{\text{def}}{=} \binom{t+k}{k} = \dfrac{\overbrace{(t+1)(t+2)\cdots(t+k)}^{k}}{k!}$ с $k = 0,\ 1,\ 2,\ \ldots$ составляют базис этого модуля (над $\mathbb{Z}$);

б) $\mathbb{Z}$-линейные гомоморфизмы $M \longrightarrow M$, перестановочные со всеми сдвигами

$$T_a :\ f(t) \longmapsto T_a f(t) \stackrel{\text{def}}{=} f(t+a)$$

составляют коммутативное кольцо, изоморфное $\mathbb{Z}[[\nabla]]$, где $M \xrightarrow{\nabla} M$ — разностный оператор, переводящий $f(t)$ в $\nabla f(t) \stackrel{\text{def}}{=} f(t) - f(t-1)$.

Приложение: расширения полей

А7◇7. Докажите, что число элементов конечного поля является степенью простого числа.

А7◇8. Пусть число p – простое, $q = p^n$, $s = p^m$, $\mathbb{F}_q$ и $\mathbb{F}_s$ — поля из q и s элементов соответственно. Пусть имеется ненулевой гомоморфизм $\mathbb{F}_q \longrightarrow \mathbb{F}_s$. Что можно сказать про n и m ?

А7◇9. Убедитесь, что множество решений уравнения $x^{p^k} - x = 0$ в поле характеристики p является подполем.

А7◇10. Какова максимальная степень неприводимого многочлена над $\mathbb{F}_p$, делящего $x^{p^k} - x$?

А7◇11. Докажите, что имеются единственные с точностью до изоморфизмф поля из 4 и из 8 элементов. Укажите явные конструкции этих полей в виде алгебраических расширений их простого подполя $\mathbb{F}_2$.

А7◇12. Пусть L - поле характеристики p . Докажите, что сопоставление $x \mapsto x^p$ (называемое *гомоморфизмом Фробениуса*)

а) является гомоморфным вложением поля в себя;

б) оставляет на месте все элементы простого подполя;

в) является *автоморфизмом* (т. е. изоморфизмом на себя), если поле L конечно;

A7⋄13*. Докажите, что для любого натурального n и любого простого p существует поле $\mathbb{F}_q$ из $q = p^n$ элементов.

A7⋄14*. Докажите, что два конечных поля $\mathbb{F}_{q_1}$ и $\mathbb{F}_{q_2}$ изоморфны тогда и только тогда, когда $q_1 = q_2$.

A7⋄15*. Докажите, что всякий автоморфизм конечного поля является итерацией автомоморфизма Фробениуса. Сколько всего имеется автоморфизмов у поля $\mathbb{F}_{p^n}$?

A7⋄16*. Докажите, что если неприводимый многочлен из $\mathbb{F}_p[x]$ имеет корень в $\mathbb{F}_{p^n}$, то он полностью разлагается на линейные множители в $\mathbb{F}_{p^n}[x]$.

A7⋄17*. Используя надлежащую версию обращения Мёбиуса, докажите, что число неприводимых многочленов степени n над полем $\mathbb{Z}/p\mathbb{Z}$ равно $\dfrac{1}{n}\sum\limits_{d|n}\mu\left(\dfrac{n}{d}\right)p^d$.

Определители

A8◇1. Найдите знак перестановки $(n\,,\ (n-1)\,,\ \dots\,,\ 2\,,\ 1\,)$.

A8◇2. Числа $1, 2, 3, \dots, n^2$ всевозможными способами организуются в квадратные матрицы размера $n \times n$. Найдите сумму определителей всех этих матриц.

A8◇3. Вычислите:

а) $\begin{pmatrix} 1 & 1 \\ 1 & a+1 \end{pmatrix}^{-1}$; **б)** $\begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix}^{-1}$; **в)** $\begin{pmatrix} a & 1 & 1 \\ 0 & b & 1 \\ 0 & 0 & c \end{pmatrix}^{-1}$; **г)** $\begin{pmatrix} 1 & b & 0 \\ 0 & 1 & 0 \\ 0 & c & 1 \end{pmatrix}^{-1}$.

A8◇4. При каких условиях матрица $\begin{pmatrix} a & 1 & 1 \\ 0 & b & 1 \\ 0 & 0 & c \end{pmatrix}$ с $a, b, c \in \mathbb{Z}$ обратима над $\mathbb{Z}$?

A8◇5. Пусть A есть $n \times n$ матрица. Выразите коэффициенты характеристического многочлена $\chi_A(t) = \det(tE - A) = 0$ через миноры матрицы A.

A8◇6. Обозначим через A_{ij} с $1 \leqslant i < j \leqslant 4$ 2×2-минор матрицы

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \end{pmatrix},$$

образованный i-тым и j-тым столбцами. Найдите квадратичное тождество, связывающее шесть величин A_{ij} (оно называется *соотношением Плюккера*).

A8◇7*. Докажите, что шесть чисел тогда и только тогда реализуются как шесть 2×2-миноров некоей 2×4-матрицы, когда они удовлетворяют квадратичному соотношению Плюккера из предыдущей задачи.

Указание. Дополните 2×4-матрицу до матрицы 4×4, дописав к ней снизу ещё один экземпляр её же самой, и примените соотношения Лапласа.

A8◇8. Пусть

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}$$

Напишите условие существования такого λ, при котором пространство решений системы

$$(A + \lambda B)x = 0$$

становится 2-мерным.

A8◇9. Рядом Фибоначчи називается последовательность, которая начинается числами 1, 1 и в которой каждое следующее число равно сумме двух предыдущих. Докажите, что $(n+1)$-й член ряда Фибоначчи равен определителю:

$$\begin{vmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ -1 & 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 1 & 1 & \dots & 0 & 0 \\ & \dots & & & \dots & & \\ 0 & 0 & 0 & 0 & \dots & -1 & 1 \end{vmatrix}.$$

Кое-что о группах.

А9◇1°. Верно ли, что отображение множества M в множество N тогда и только тогда
а) инъективно, когда оно имеет левое обратное отображение?
б) сюръективно, когда оно имеет правое обратное отображение?

А9◇2°. Пусть $\sigma \in \mathfrak{S}_n$ — цикл длины k, а $\tau \in \mathfrak{S}_n$ — произвольная перестановка. Убедитесь, что $\tau\sigma\tau^{-1}$ есть цикл длины k и выясните, какие элементы входят в этот цикл, если $\sigma = (1, 2, \ldots, k)$?

А9◇3. Пусть $\sigma \in \mathfrak{S}_n$ — нечётная перестановка и N — её порядок в группе $\mathfrak{S}_n$. Что можно сказать про чётность N?

А9◇4. Рассмотрим перестановку $\sigma = (\,3\,,\ 5\,,\ 4\,,\ 1\,,\ 2\,) \in \mathfrak{S}_5$. Найдите σ^{100}.

Группа фигуры. Множество всех движений пространства, переводящих данную фигуру $\mathfrak{F}$ в себя называется *собственной* (или *несобственной*) *группой* фигуры $\mathfrak{F}$, смотря по тому, допускаются ли при этом несобственные (т. е. меняющие ориентацию) движения. Группа правильного плоского n-угольника в пространстве называется *группой диэдра* и обозначается $\mathfrak{D}_n$. Специальный частный случай – группа «двуугольника» $\mathfrak{D}_2$ называется *квадратичной группой Клейна* и обозначается $\mathfrak{V}_4$ (двуугольник можно представлять себе либо как отрезок с «квадратным поперечным сечением[1]», либо как «дольку» с рис. 9.1).

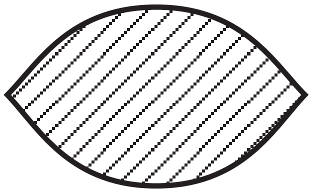


Рис. 9.1. Двуугольник

А9◇5°. Пусть $\mathfrak{G}$ — несобственная группа ромба, не являющегося квадратом. Найдите порядок группы $\mathfrak{G}$ и опишите орбиты и стационарные подгруппы вершин ромба.

А9◇6. Изоморфна ли симметрическая группа $\mathfrak{S}_3$ (несобственной) группе треугольника $\mathfrak{D}_3$?

А9◇7. Найдите порядок группы $\mathfrak{D}_n$ и все точки плоскости, для которых порядок стабилизатора в группе $\mathfrak{D}_n$ больше 1.

А9◇8. Найдите порядок стационарной подгруппы вершины и порядок всей группы для собственных и несобственных групп:
а) тетраэдра; **б)** куба; **в)** октаэдра; **г)** икосаэдра; **д)** додекаэдра.

А9◇9. Изоморфна ли несобственная группа тетраэдра группе $\mathfrak{S}_4$?

А9◇10. Сколько элементов симметрической группы $\mathfrak{S}_4$ остаются неподвижными при сопряжении перестановкой $(1, 2)(3, 4)$?

А9◇11. Постройте геометрический изоморфизмы собственной группы
а) тетраэдра с $\mathfrak{A}_4$; **б)** куба и октаэдра с $\mathfrak{S}_4$; **в)** икосаэдра и додекаэдра с $\mathfrak{A}_5$.

А9◇12. Изоморфна ли несобственная группа икосаэдра группе $\mathfrak{S}_5$?

А9◇13. Используя предыдущие геометрические образы юостройте эпиморфизм $\mathfrak{S}_4 \longrightarrow \mathfrak{S}_3$ и опишите его ядро (подсказка: ядро есть стабилизатор естественно ассоциированного с кубом пространственного двуугольника).

А9◇14. Во всякой ли конечной абелевой группе порядка n для любого $d \mid n$ найдётся хотя бы одна подгруппа порядка d?

А9◇15. Может ли конечная мультипликативная подгруппа поля не быть циклической?

Добрый совет: когда речь идёт о взаимодествии некоей нормальной подгруппы в $\mathfrak{G}$ с какой-либо другой подгруппой или фактор-группой группы $\mathfrak{G}$, полезно ьывает рассмотреть естественное действие этой другой подгруппы сопряжениями на нормальной подгруппе.

А9◇16. Пусть $\mathfrak{G}$– группа из шести элементов. Докажите, что:
а) в $\mathfrak{G}$ имеется подгруппа, изоморфная $\mathbb{Z}/3\mathbb{Z}$;

[1] т. е. имеюжим низ, верх, право и лево

б) эта подгруппа нормальна;
в) в $\mathfrak{G}$ имеется подгруппа, изоморфная $\mathbb{Z}/2\mathbb{Z}$;
г) если она нормльна, то $\mathfrak{G} \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, а если нет, то $\mathfrak{G} \cong \mathfrak{S}_3 \cong \mathfrak{D}_3$.

А9◇17. Пусть $\mathfrak{G}$ – группа из 15-ти элементов. Верно ли, что:
а) в $\mathfrak{G}$ имеется подгруппа, изоморфная $\mathbb{Z}/5\mathbb{Z}$;
б) в $\mathfrak{G}$ имеется подгруппа, изоморфная $\mathbb{Z}/3\mathbb{Z}$;
в) обе эти подгруппы нормальны;
г) $\mathfrak{G} \cong \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

А9◇18. Всегда ли инъективный гомоморфизм групп имеет левый обратный гомоморфизм, и всегда ли сюръективный гомоморфизм групп имеет правый обратный гомоморфизм?

А9◇19. Пусть произведение любых двух левых смежных классов группы $\mathfrak{G}$ по подгруппе $\mathfrak{H}$ снова является левым смежным классом. Верно ли, что $\mathfrak{H}$ нормальна?

А9◇20. Пусть $\mathfrak{H}_1$ и $\mathfrak{H}_2$ — две нормальные подгруппы группы $\mathfrak{G}$, и $\mathfrak{H}_1 \cap \mathfrak{H}_2 = \{e\}$. Докажите, что $ab = ba$ для любых $a \in \mathfrak{H}_1$, $b \in \mathfrak{H}_2$.

А9◇21. Пусть $\mathfrak{H} \subset \mathfrak{G}$ – подгруппа, индекс которой совпадает с наименьшим простым делителем p порядка группы. Докажите, что $\mathfrak{H}$ – нормальная подгруппа (рассмотрите случай $p = 2$, если общий случай вызывает у Вас затруднения).

А9◇22. Опишите центр $\mathrm{Z}(\mathfrak{G})$, группу внутренних автоморфизмов $\mathrm{Int}(\mathfrak{G})$ и группу всех автоморфизмов $\mathrm{Aut}(\mathfrak{G})$ для группы $\mathfrak{G}$
а) комплексных корней степени n из единицы для $n = 2, 3, 4, 5, 6$;
б) диэдральной $\mathfrak{D}_n$ (хотя бы для $n = 3, 4$);
в) симметрической $\mathfrak{S}_4$; **г)** знакопеременной $\mathfrak{A}_4$; **д)** знакопеременной $\mathfrak{A}_5$.

А9◇23. Порождается ли симметрическая группа $\mathfrak{S}_n$ транспозицией (12) и циклом $(1\,2\,3\,\dots\,n)$?

А9◇24. Порождается ли знакопеременная группа $\mathfrak{A}_n$ 3-циклами (123), (124), ..., $(12n)$?

А9◇25. Постройте эпиморфизм из свободной группы порождённой двумя элементами на группу диэдра $\mathfrak{D}_n$ и опишите его ядро (хотя бы для $n = 3,\ 4$).

А9◇26. Докажите, что группа треугольника порождается двумя отражениями, и опишите соотношения между ними.

А9◇27*. Тот же вопрос про симетрическую группу $\mathfrak{S}_4$ и три отражения (на самом деле, подобное описание имеется для всех групп $\mathfrak{S}_n$).

А9◇28. Пусть $\mathfrak{G}$ — произвольная группа, $a, b \in \mathfrak{G}$, причём порядок их произведения ab равен n. Каким может быть порядок элемента ba?

А9◇29. Каков порядок группы с образующими a, b и соотношениями $ab^2 = ba$, $ba^2 = ab$. $\mathfrak{G}$?