Для зачета по каждому листку достаточно сдать все задачи со звездочками, либо все задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

АЛГЕБРА 1: определение группы, кольца, поля

Группы

Произведением $A \times B$ множеств A и B называется множество пар (a, b), где a – элемент A, а b – элемент B. Отображение $f : A \to B$ множества A в множество B называется **инъективным**, или **инъекцией**, или **вложением** (это все синонимы), если оно переводит разные элементы множества A в разные элементы множества B. Отображение называется **сюръективным**, или **сюръекцией**, или **наложением**, если в каждый элемент множества B переходит хотя бы один элемент множества A. Отображение называется **биективным** (биекцией, взаимно однозначным), если оно инъективно и сюръективно.

Пусть A - некоторое множество (конечное или нет). Обозначим через $S(A)$ множество биективных отображений из A в себя. Если f, g – два таких отображения, их можно "перемножить", взяв композицию $f \circ g$:

$$f \circ g(a) = f(g(a)).$$

Множество $S(A)$, наделенное такой операцией, называется "группа подстановок (или перестановок) элементов из A". Тождественная подстановка обозначается 1_A (часто также пишут Id_A, от слова identity).

Также $S(A)$ называется **симметрической группой**. Если A – конечное множество из n элементов, $S(A)$ обозначается S_n.

Подстановки можно записывать в виде таблиц; например, подстановка $1 \mapsto 3$, $2 \mapsto 4$, $3 \mapsto 1$, $4 \mapsto 2$ чисел $1, 2, 3, 4$ записывается как $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$. В верхней строке пишут числа в порядке возрастания, в нижней – их образы.

Задача 1.1. Найти произведение

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

Задача 1.2. а. Сколько существует подстановок чисел $1, 2, \ldots, 5$? Сколько из них оставляют число 1 на месте?

б. Сколько из них переводят 1 в 5?

в. Для скольких из них $\sigma(1) < \sigma(2)$?

г. Для скольких из них $\sigma(1) < \sigma(2) < \sigma(3)$?

Задача 1.3. Сколько элементов в $S(A)$, если A – конечное множество из n элементов?

Задача 1.4. Верно ли что $f \circ g = g \circ f$ для любых f, g?

Для каждой подстановки $f \in S(A)$ (через "$\in$" обозначается элемент множества) существует и единственна "обратная подстановка" f^{-1}, т.е. такая подстановка, что $f \circ f^{-1} = f^{-1} \circ f = 1_A$.

Циклическая перестановка множества $a, b, c, d, \dots, w$ отображает a в b, b в c, c в d и так далее по кругу. Такая перестановка обозначается $(a, b, c, d, \dots, w)$. Ее порядок – это количество элементов в скобках. **Транспозиция** – это циклическая перестановка порядка 2; она переставляет два элемента и оставляет на месте все остальные.

Задача 1.5. Пусть $\sigma = (123)$, $\tau = (34)$. Чему равно $\tau \circ \sigma \circ \tau^{-1}$?

Задача 1.6. Доказать, что каждая подстановка представима как произведение транспозиций.

Задача 1.7 (*). Может ли произведение нечетного числа транспозиций быть тождественной перестановкой?

Указание. Что произойдет с многочленом $(x_1 - x_2)(x_1 - x_3) \dots (x_1 - x_n)(x_2 - x_3) \dots$ (произведение $(x_i - x_j)$ по всем $i > j$), если поменять местами x_i и x_j?

На группе подстановок $S(A)$ заданы следующие структуры: произведение, взятие обратной подстановки, тождественная подстановка. Эту ситуацию удобно аксиоматизировать.

Определение 1.1. Пусть G – множество, где задана операция "произведения" $f, g \mapsto f \cdot g$, "взятие обратного" $f \mapsto f^{-1}$, и задан "единичный элемент" 1_G, и все это удовлетворяет следующим аксиомам.

а. "Ассоциативность": $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ для всех f, g, h.

б. "Единица": $f \cdot 1_G = 1_G \cdot f = f$ для всех f.

в. "Обратный элемент": $f \cdot f^{-1} = f^{-1} \cdot f = 1_G$ для всех f.

Тогда G называется **группой**.

Подмножество G, замкнутое относительно этих операций, называется **подгруппой в** G.

Задача 1.8. Дана группа G.

а. Если $fg = f$ или $gf = f$, то $g = 1$.

б. Если $fg = 1$ или $gf = 1$, то $g = f^{-1}$.

Замечание. Тем самым, для того, чтобы полностью определить структуру группы на множестве G, достаточно задать операцию умножения. Единица и обратный элемент, если они существуют, восстанавливаются по умножению однозначно.

Задача 1.9. Являются ли группами следующие множества, с указанными операциями.

а. Натуральные числа с операцией сложения.

б. Целые числа с операцией сложения.

в. Целые числа с операцией умножения.

г. Рациональные числа с операцией умножения.

д. Вещественные числа с операцией сложения.

е. Вещественные числа с операцией умножения.

ж. **(*)**Движения плоскости с операцией композиции.

з. Числа строго больше -1 и строго меньше 1, с операцией $u*v = (u+v)/(1+uv)$ (проверьте также, что операция корректно определена).

и. Фигуры (множества точек) на плоскости с операцией оъединения.

к. **(*)**Фигуры (множества точек) на плоскости с операцией симметрической разности: $A*B$ состоит из точек, принадлежащих ровно одной из фигур A, B.

л. **(*)**Отображения из фиксированного множества C в фиксированную гриппу G, с операцией $(f \cdot g)(s) = f(s)g(s)$.

"Произведение групп" G_1 и G_2 есть множество пар (g_1, g_2), $g_1 \in G_1, g_2 \in G_2$, с групповой операцией
$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2')$$
Отображение $f : G \to G'$ из группы G в группу G' называется **гомоморфизмом**, если оно сохраняет умножение: $f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2)$. Гомоморфизм называется **мономорфизмом**, если он инъективен, **эпиморфизмом** если он сюръективен, и **изоморфизмом** если он биективен. Группы G, G' **изоморфны** если между ними существует изоморфизм. Изоморфизм группы в себя называется **автоморфизмом**.

Задача 1.10. Докажите, что если $f : G \to G'$ – гомоморфизм групп, то $f(1_G) = 1_{G'}$ и $f(g^{-1}) = (f(g)^{-1})$ для любого $g \in G$.

Определение 1.2. Если задан гомоморфизм $G \to S(A)$ группы G в группу $S(A)$ перестановок множества A, то говорят, что G **действует на множестве** A (в самом деле, в этом случае каждый элемент G каким-то образом переставляет элементы A). Действие G на A можно записать как отображение $G \times A \xrightarrow{\rho} A$, $a, g \mapsto \rho(g, a)$. Иногда действие группы на множестве записывается проще: $a, g \mapsto g(a)$.

Задача 1.11. Докажите, что любая группа допускает иньективный гомоморфизм в группу подстановок (не обязательно конечного множества).

Указание. Подумайте, в чем может быть смысл фразы "Группа G действует на себе умножениями слева".

Задача 1.12. Верно ли, что

а. Любая группа из двух элементов изоморфна группе перестановок S_2.

б. Любая группа из шести элементов изоморфна или группе перестановок S_3, или произведению двух нетривиальных групп.

Задача 1.13 (*). Докажите, что группа перестановок S_n не изоморфна произведению двух нетривиальных групп.

Задача 1.14. Пусть G – группа, $g \in G$ – ее элемент. Верно ли, что последовательность $g, g^2, g^3, \dots$ периодическая? Верно ли это, если G – конечная группа?

Пусть n – натуральное число. Говорят, что $g \in G$ – **элемент порядка** n в группе G, если $g^n = 1_G$, но $g^k \neq 1_G$ для $k < n$.

Задача 1.15 (!). Дана конечная группа из n элементов. Докажите, что порядок любого элемента группы делит n.

Указание. Рассмотрите действие группы на себе умножениями слева.

Задача 1.16 (*). Дана группа с четным числом элементов. Докажите, что в ней есть элемент порядка 2.

Задача 1.17 (*). Верно ли, что

а. Группа D_{12} движений правильного 12-угольника изоморфна произведению $D_6 \times S_2$, где D_6 – это группа движений шестиугольника.

б. Группа D_6 изоморфна произведению $D_3 \times S_2$, где D_3 – это группа движений треугольника.

Группа называется **коммутативной**, или **абелевой**, если $f \cdot g = g \cdot f$ для всех f, g. Два элемента f, g **коммутируют**, если $f \cdot g = g \cdot f$.

Задача 1.18. Какие из групп, рассмотренных в задаче 1.9, коммутативны?

Задача 1.19 (*). а. **Центром** группы G называется подмножество, состоящее из всех элементов $g \in G$ таких, что $gg' = g'g$ для всех $g' \in G$. Докажите, что центр - это подгруппа.

б. Дана группа G, в которой есть элементы порядка > 2. В ней дана подгруппа G' такая, что все элементы $g \in G$, не принадлежащие G', имеют порядок 2. Приведите пример такой ситуации (или докажите, что она невозможна). Всегда ли в такой ситуации G конечна?

в. Докажите, что в такой ситуации G' абелева.

г. Пусть G' содержит центр G. Докажите, что группа G единственным образом (с точностью до изоморфизма) задается условием из пункта (2) и подгруппой G'.

(Такая группа называется диэдральной группой).

д. Дана диэдральная группа G, связанная с абелевой группой G' как выше. Пусть G' - произведение S_2 и еще одной абелевой группы: $G' = S_2 \times G''$. Докажите, что G – произведение S_2 и диэдральной группы.

Кольца и поля

Рассмотрим вещественные числа, целые числа или конечные десятичные дроби. На этих множествах заданы

а. Сложение, которое коммутативно и превращает наше множество в группу (обозначается плюсом; взятие обратного относительно сложения обозначается минусом)

б. Умножение, которое коммутативно, но группы не задает, потому что не все числа обратимы (обозначается точкой; точку часто опускают для краткости и пишут просто xy вместо $x \cdot y$).

Эти структуры полезно аксиоматизировать.

Определение 1.3. Пусть R – множество с двумя операциями $a, b \mapsto a + b$ (сложение) и $a, b \mapsto a \cdot b$ (умножение). Пусть в R заданы элементы 0 и 1 (ноль и единица). Если следующие свойства выполнены, R называется **кольцом**.

а. R является коммутативной группой относительно операции сложения, 0 есть единица в этой групповой структуре

б. 1 является единицей относительно умножения: $1 \cdot a = a \cdot 1 = a$ для всех a.

в. Ассоциативность по умножению: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

г. Дистрибутивность: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Если умножение коммутативно, говорят, что кольцо R коммутативно. Если к тому же умножение обратимо для всех $a \neq 0$, т.е. $R \backslash \{0\}$ есть группа относительно умножения, то R называется **полем**.

В этом и нескольких следующих листках, мы будем рассматривать только коммутативные кольца, и слово "коммутативный" будем для краткости опускать; если явно не указано обратное, все кольца предполагаются коммутативными.

Задача 1.20. Являются ли кольцами следующие множества (с естественными операциями, если они не указаны явно):

а. Натуральные числа.

б. Целые числа.

в. Четные целые числа.

г. Рациональные числа.

д. Иррациональные числа.

е. Конечные десятичные дроби.

ж. Пары целых чисел, сложение и умножение покоординатные.

з. Пары целых чисел, сложение покоординатное, умножение задается формулой $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

и. **(*)** Пары рациональных чисел, сложение покоординатное, умножение задается формулой $(a, b) \cdot (c, d) = (ac + 2bd, ad + bc)$.

к. **(*)**Фигуры на плоскости (сложение – симметрическая разность, умножение – пересечение).

л. **(*)**Отображения из фиксированного множества C в фиксированную гриппу G, с операцией $(f \cdot g)(s) = f(s)g(s)$.

Задача 1.21. Какие из колец, рассмотренных в задаче 1.20, являются полями?

Задача 1.22. Дано кольцо R. Рассмотрим множество последовательностей

$$a = (a_0, a_1, \dots, a_i, \dots, 0, 0, \dots)$$

элементов R с конечным числом ненулевых элементов. Опеределим операции в этом множестве как

$$(a + b)_i = a_i + b_i,$$
$$(a \cdots b)_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

Докажите, что это множество является кольцом (в частности, проверьте, что умножение ассоциативно).

Кольцо, определенное в задаче 1.22, называется **кольцом полиномов от одной переменной** над R, и обозначается через $R[x]$. Элементы $R[x]$ называются "полиномы" или "многочлены". Они обычно записываются как $a_0 + a_1 x + \dots + a_i x^i$ (все a_j с $j > i$ нулевые).

В курсе алгебры мы будем предполагать понятие вещественного числа известным (например, можно думать про вещественные числа как про бесконечные десятичные дроби с обычными операциями "в столбик"). Строгое определение дается в курсе геометрии, топологии и анализа. Все, что нам нужно в курсе алгебры, это

Важное замечание: Вещественные числа образуют поле.

Это "важное замечание" также доказывается в курсе геометрии, топологии и анализа. Кроме того, нужно следующее свойство:

Задача 1.23 (*). Докажите, что каждое уравнение вида

$$x^{2n+1} + a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + ... + a_1 x + a_0 = 0$$

имеет вещественное решение.

Эту задачу надо решать, когда вы узнаете из курса анализа определение вещественных чисел, или выучите его самостоятельно по книгам.

Задача 1.24 (*). Будет ли полем кольцо, определенное в задаче 1.20 9, если в определении вместо "рациональные числа" сказать "вещественные числа"?

Задача 1.25. Зафиксируем целое число n. При делении на n другие числа дают остатки 0, 1, 2, ... $n-1$. Обозначим эту операцию за $\mod n$. Два числа, у которых равны остатки $\mod n$, называются сравнимыми по модулю n. Определим сумму и произведение на множестве чисел $\mathrm{mod}\ n$ таким образом, чтобы

$$(x \mod n) + (y \mod n) = ((x + y) \mod n),$$
$$(x \mod n) \cdot (y \mod n) = (xy \mod n)$$

выполнялось для любых целых чисел x, y. Докажите, что это определение корректно, и множество остатков образует кольцо.

Задача 1.26 (*). Докажите, что множество остатков $\mod n$ со сложением и умножением, определенными выше, образует поле тогда и только тогда, когда число n простое.

Замечание. Если вы сейчас не можете решить эту задачу, отложите ее: через некоторое время, после введения полезных промежуточных понятий, та же задача будет без звездочки.

Задача 1.27. Постройте поля из

а. 2-х,

б. 3-х,

в. (*)4-х элементов.

Задача 1.28 (*). Докажите, что не существует поля из шести элементов.

Задача 1.29. Докажите, что если p – простое число, то поле из p элементов единственно с точностью до изоморфизма.

Определение 1.4. Характеристикой поля k называется число 0, если $1 \in k$ имеет бесконечный порядок относительно сложения, или порядок p элемента $1 \in k$, если он конечен.

Задача 1.30. Докажите, что если характеристика p поля k ненулевая, то p простое.

Задача 1.31 (*). Дано поле характетристики p. Докажите, что отображение Фробениуса $x \mapsto x^p$ сохраняет умножение и сложение (как и для групп, такое отображение называется гомоморфизм).

Указание. Воспользуйтесь формулой бинома.

Задача 1.32 (*). Выведите из этого малую теорему Ферма: для любого целого числа x, x^p сравнимо с x по модулю p.

Пусть $P = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ – многочлен с коэффициентами в поле k. **Корень** P – это такой элемент α в поле k, что $P(\alpha) = 0$.

Задача 1.33. Пусть α – корень многочлена P над полем k. Докажите, что многочлен P делится на $z - \alpha$ в кольце $k[z]$

Указание. Воспользуйтесь делением многочленов в столбик:

$$\begin{array}{rrr|l}
x^2 & +2x & -12 & x+5 \\ \cline{4-4}
\underline{x^2} & \underline{+5x} & & x-3 \\
 & -3x & -12 & \\
 & \underline{-3x} & \underline{-15} & \\
 & & 3 &
\end{array}$$

Задача 1.34. Докажите, что ненулевой многочлен степени n над полем не может иметь больше n разных корней.

Указание. Воспользуйтесь предыдущей задачей.

Пусть P – ненулевой многочлен над полем k. Многочлен P называется **неприводимым**, если его нельзя представить в виде произведения многочленов меньшей степени.

Воспользовавшись делением многочленов в столбик, рассмотрим множество остатков в кольце $k[x]$ по модулю P.

Задача 1.35. Докажите, что это множество образует кольцо (мы обозначим его за $k[x] \bmod P$).

Комплексные числа.

Множество целых чисел обозначается за $\mathbb{Z}$, а вещественных чисел – за $\mathbb{R}$. Пусть $\mathbb{C}$ – множество пар вещественных чисел (a, b), со сложением, определенным как $(a, b) + (c, d) = (a + c, b + d)$ и с умножением, определенным формулой

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Элементы $\mathbb{C}$ называются комплексными числами.

Задача 1.36. Проверьте, что $\mathbb{C}$ – кольцо. Докажите, что уравнение $x^2 + 1 = 0$ имеет решение в $\mathbb{C}$. Сколько решений оно имеет?

Задача 1.37. Выберем решение уравнения $x^2 + 1$ в $\mathbb{C}$ и обозначим его за $\sqrt{-1}$. Докажите, что любое комплексное число можно единстнвенным образом представить в виде $a + b\sqrt{-1}$, $a, b \in \mathbb{R}$.

Задача 1.38. Постройте изоморфизм $\mathbb{C} \cong (\mathbb{R}[x] \mod P)$, где P – многочлен $P = x^2 + 1$.

Задача 1.39. Дано комплексное число $z := a + b\sqrt{-1}$. Сопряженное z число — это $\overline{z} := a - b\sqrt{-1}$. Докажите, что комплексное сопряжение сохраняет умножение и сложение в $\mathbb{C}$ (такие отображения называются автоморфизмами поля $\mathbb{C}$).

Задача 1.40. Дано комплексное число $z := a + b\sqrt{-1}$. Докажите, что $z\overline{z}$ вещественно (это значит, что в представлении комплексного числа в виде (x, y) компонента y равна нулю).

Задача 1.41. Дано комплексное число $z := a+b\sqrt{-1}$. Докажите, что $z\overline{z} = a^2+b^2$. В частности, это число всегда неотрицательно, и равно нулю только если $z = 0$. Часто $z\overline{z}$ записывают как $|z|^2$, поскольку длина вектора (a, b) на плоскости это $\sqrt{a^2 + b^2}$ ($|z|$, расстояние на плоскости от z до 0, называется модулем z).

Задача 1.42. Выведите из предыдущей задачи, что комплексные числа образуют поле.

Указание. $z^{-1} = \overline{z}|z|^{-2}$

Задача 1.43. Докажите "неравенство треугольника": $|z_1| - |z_2| \leqslant |z_1 + z_2| \leqslant |z_1| + |z_2|$

Задача 1.44. Докажите, что $|z_1 z_2| = |z_1||z_2|$.

Задача 1.45 (!). Пусть $z = a + b\sqrt{-1}$ – комплексное число с модулем 1: $|z| = 1$. Рассмотрим умножение на z как преобразование плоскости $\mathbb{R}^2$, отождествленной естественным образом с $\mathbb{C}$. Докажите, что если $z \neq 1$, то это преобразование — движение с единственной неподвижной точкой $0 \in \mathbb{R}^2$.

Задача 1.46 (!). Из геометрии известно, что движение с единственной неподвижной точкой $0 \in \mathbb{R}^2$ — это поворот на какой-то угол φ вокруг 0. Для движения из задачи 1.45, как найти a и b, зная φ?

Замечание. Угол φ называется **аргументом** комплексного числа z.

Задача 1.47 (!). Докажите формулу косинусов $\cos(\varphi + \psi) = \cos\varphi \sin\psi + \sin\varphi \cos\psi$.

Указание. Воспользуйтесь предыдущей задачей.

Задача 1.48 (!). Докажите, что уравнение $z^n = 1$ имеет ровно n решений в комплексных числах.

Указание. Воспользуйтесь тригонометрической интерпретацией комплексных чисел.

Задача 1.49 (*). Дан полином P степени меньше n, и пусть $\zeta_1, \dots, \zeta_n$ – "корни n-й степени из 1", иначе говоря, все комплексные решения уравнения $z^n = 1$. Докажите, что среднее $\frac{1}{n}\sum P(\zeta_i)$ значений P по всем ζ_i равно $P(0)$.

Указание. Воспользуйтесь тригонометрической интерпретацией комплексных чисел.

Задача 1.50 (*). Дан полином P степени меньше n. Пусть Ξ – правильный n-угольник на комплексной плоскости $\mathbb{C} = \mathbb{R}^2$. Докажите, что значение P в центре Ξ равно среднему значений P в вершинах Ξ.

Указание. Воспользуйтесь предыдущей задачей.

Замечание. Архимед определил периметр окружности как предел периметров вписанных в нее многоугольников. Если следовать примеру Архимеда, то средним значением функции f, определенной на окружности, можно считать предел (по n) средних $\frac{1}{n}\sum f(\zeta_i)$, где z_i – вершины правильных n-угольников, вписанных в эту окружность. Из предыдущей задачи можно вывести, что среднее значений полиномиальной функции P в единичной окружности $|z| = 1$ равно значению P в ее центре.

Задача 1.51. Вычислите группу автоморфизмов $\mathbb{C}$,

а. **(*)**переводящих в себя подполе $\mathbb{R} \subset \mathbb{C}$.

б. переводящих в себя подполе $\mathbb{R} \subset \mathbb{C}$, и оставляющих на месте все его элементы.

Задача 1.52 (!). В определении комплексных чисел заменим

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

на

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc).$$

Обозначим получившееся за $\mathbb{R}_2$. Будет ли $\mathbb{R}_2$ кольцом? А полем? Найти все решения уравнения $z^2 = 1$ в $\mathbb{R}_2$. Найти все решения уравнения $z^2 = 0$ в $\mathbb{R}_2$.

Задача 1.53 (!). В определении комплексных чисел заменим

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

на

$$(a, b) \cdot (c, d) = (ac, ad + bc).$$

Обозначим его за $\mathbb{R}_\varepsilon$. Будет ли $\mathbb{R}_\varepsilon$ кольцом? А полем? Будет ли оно изоморфно $\mathbb{R}_2$ из предыдущей задачи? Найти все решения уравнения $z^2 = 1$.

Задача 1.54 (*). В предыдущих двух задачах, найдите также все решения уравнения $z^2 = z$.

Задача 1.55 (*). Пусть $P = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ полином степени n, у которого n корней, лежащих снаружи единичной окружности. Докажите, что $\frac{a_k}{a_0} < C_n^k$, где $C_n^k = \frac{n!}{k!(n-k)!}$ – биномиальный коэффициент.