

Г р у п п ы

Пусть в некотором множестве G определены: (1) операция $*$, ставящая в соответствие любым двум элементам $x, y \in G$ некоторый элемент $x * y$; (2) операция i , ставящая в соответствие любому $x \in G$ некоторый элемент $i(x)$; (3) некоторый элемент $n \in G$, причем выполняются такие свойства (для любых $x, y, z \in G$):

$$(1) \quad x * (y * z) = (x * y) * z$$

$$(2) \quad x * n = n * x = x$$

$$(3) \quad x * i(x) = i(x) * x = n$$

В этом случае множество G называется группой.

В приводимых далее примерах групп мы иногда указываем лишь операцию $*$.

(1) Пусть $G = \mathbb{R}$, $x * y = x + y$, $n = 0$, $i(x) = -x$. Получается аддитивная группа \mathbb{R} .

(2) Заменяя \mathbb{R} на \mathbb{Q} , \mathbb{Z} или \mathbb{C} , получаем аддитивные группы рациональных, целых или комплексных чисел.

(3) Пусть $G = \mathbb{R} \setminus \{0\}$, $x * y = x \cdot y$. Получается мультипликативная группа \mathbb{R}^* . (Здесь \mathbb{R} также можно заменить на \mathbb{C} или \mathbb{Q} - но не на \mathbb{Z} !)

(4) Пусть M - некоторое множество, G - множество всех взаимно однозначных функций из M в M , $f * g$ - композиция f и g . Получается группа перестановок множества M .

(5) Группа движений плоскости состоит из всех движений (взаимно однозначных функций, сохраняющих расстояние), операция $*$ - композиция движений.

(6) Если рассматривать не все движения плоскости, а лишь те, которые отображают некоторое множество M точек плоскости на себя, получим группу симметрий множества M .

(7) Пусть $m \geq 1$ - некоторое натуральное число. Рассмотрим множество G всех возможных остатков при делении на m : $G = \{0, 1, \dots, m-1\}$. Через $x * y$ обозначим остаток, который дает при делении на m сумма чисел с остатками x и y (напомним, что остаток от деления суммы определяется остатками слагаемых). Получающаяся группа обозначается $\mathbb{Z} / m\mathbb{Z}$.

(8) Пусть m - натуральное число. Рассмотрим остатки от деления на m , взаимно простые с m .

(При $m = 4$ это 1 и 3, при простом m - 1, 2, ...,

$m-1$.) Через $x * y$ обозначим остаток, который дает при делении на m произведение чисел с остатками x и y . Оказывается,

$a \backslash b$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$a * b$ $\mathbb{Z}/3\mathbb{Z}$

$a \backslash b$	1	3
1	1	3
3	3	1

$a * b$ $(\mathbb{Z}/4\mathbb{Z})^*$

что $x * y$ лежит в нашем множестве. Возникающая группа обозначается $(\mathbb{Z}/m\mathbb{Z})^*$.

1. Указать, как нужно определить элемент n и операцию i в тех примерах, где это не указано.

2. Доказать, что (1) $x * (y * (z * t)) = ((x * y) * z) * t$;
 (2) если $x * y = x * z$, то $y = z$; (3) $i(x * y) = i(y) * i(x)$,
 $i(i(a)) = a$, $i(n) = n$; (4) $(a * x = b) \Leftrightarrow (x = i(a) * b)$.

3. Доказать, что если $n_1 * x = x$ при всех $x \in G$, то $n_1 = n$ ("единственность нейтрального элемента"). Доказать, что если $x * y = n$, то $y = i(x)$ ("единственность").

4. Доказать, что для любого $a \in G$ функция $\ell_a: G \rightarrow G$, для которой $\ell_a(x) = a * x$, является взаимно однозначным отображением G в G . Чему равны $\ell_a \circ \ell_b$ и $(\ell_a)^{-1}$?

5. Доказать, что если операция $*$ на множестве G такова, что $x * (y * z) = (x * y) * z$ и для любых a и $b \in G$ найдутся такие x и y , что $a * x = b$, $y * a = b$, то можно определить функцию i и элемент n , превращающие G в группу.

Обычно операция в группе обозначается не $*$, а \cdot или $+$ ("мультипликативная" и "аддитивная" записи). В соответствии с этим n обозначается через 1 или 0 , а $i(x)$ — через $-x$ или x^{-1} . Аддитивная запись применяется для коммутативных (=абелевых) групп, в которых $x * y = y * x$.

6. Доказать, что если $x * x = n$ при всех $x \in G$, то G коммутативна.

В дальнейшем мы будем пользоваться в основном мультипликативной записью. Через x^n обозначается $x \cdot x \cdot \dots \cdot x$ (n раз).

Говорят, что элемент a группы G имеет конечный порядок, если существует такое n , что $a^n = 1$. Наименьшее из таких n называется порядком элемента a .

7. Указать все элементы конечного порядка в (1) аддитивной группе \mathbb{R} ; (2) мультипликативных группах \mathbb{R}^* , \mathbb{C}^* ; (3) группе поворотов плоскости вокруг данной точки; (4) группе всех движений плоскости.

8. Доказать, что в конечной группе всякий элемент имеет конечный порядок. (Указание. В последовательности $1, a, a^2, \dots$ есть совпадающие элементы.)

9. Элемент a имеет порядок k . Доказать, что $(a^n = 1) \Leftrightarrow (n \text{ делится на } k)$.

10. Какие порядки могут иметь элементы группы перестановок множества из 9 элементов?

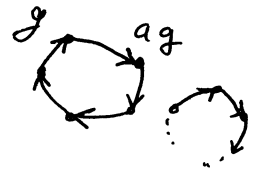
11. Найти порядки всех элементов $\mathbb{Z}/n\mathbb{Z}$

12. Доказать, что порядки элементов a и a^{-1} равны. Доказать, что порядки элементов ab и ba равны. Доказать, что порядки элементов abc , bca и cab равны.

13. Элементы a и b группы G имеют конечный порядок. Можно ли утверждать, что элемент ab имеет конечный порядок?

14. Порядок элемента a равен k . Чему равен порядок элемента a^n .

15. Пусть a — элемент конечной группы G . Изобразим элементы G точками и проведем из каждого g стрелку в ag . Доказать, что стрелки образуют несколько циклов, не связанных друг с другом и содержащих одинаковое количество элементов.



16. Пусть a — элемент конечной группы G . Доказать, что число элементов G (порядок G) делится на порядок a .

17. (Теорема Ферма — Эйлера.) Пусть m — натуральное число, $\varphi(m)$ — количество чисел от 0 до $m-1$, взаимно простых с m , а число a взаимно просто с m . Доказать, что $a^{\varphi(m)} - 1$ делится на m . (Указание. См. предыдущую задачу.)

18. Вывести из утверждения предыдущей задачи "малую теорему Ферма": если p простое, то $a^p - a$ делится на p .

19. Придумать бесконечную группу, в которой каждый элемент имел бы конечный порядок (например, 2).

20. Существует ли группа из 4 элементов, в которой каждый элемент имел бы порядок 2?

21. Доказать, что при простом p в группе $(\mathbb{Z}/p\mathbb{Z})^*$ имеется элемент порядка $p-1$.

22. Будем многократно применять одно и то же преобразование к "кубику Рубика". Доказать, что рано или поздно он вернется в первоначальное положение.

Группа перестановок

23. Пусть M — конечное множество из n элементов. Сколько элементов содержит группа перестановок множества M ?

24. Коммутативна ли эта группа?

25. Назовем транспозицией перестановку M , меняющую два элемента местами и оставляющую остальные элементы на месте:

$a \mapsto b$, $b \mapsto a$, $x \mapsto x$ при $x \neq a, b$. Доказать,

что всякая перестановка представляется в виде произведения транспозиций. (Расположенные в ряд предметы можно переложить как угодно, несколько раз поменяв местами пары предметов.)

26. Имеется n расположенных в ряд бирок, на которых написаны числа от 1 до n . Назовем числом беспорядков количество таких пар $\langle i, j \rangle$, что $i < j$, а i -ая бирка находится правее j -ой. Доказать, что при перестановке двух бирок четность числа беспорядков меняется (из четного оно делается нечетным и наоборот).



27. Доказать, что произведение нечетного числа транспозиций не может быть равно тождественной перестановке. (Указание. См. предыдущую задачу.)

Перестановка называется четной, если она представима как произведение четного числа транспозиций, и нечетной, если она представима как произведение нечетного числа транспозиций.

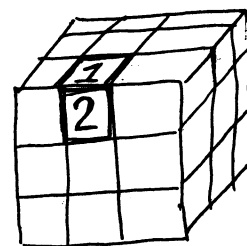
28. Доказать, что никакая перестановка не является четной и нечетной одновременно, что произведение двух четных или двух нечетных четно, а произведение нечетной и четной перестановок нечетно.

29. Доказать, что количество четных перестановок равно количеству нечетных перестановок.

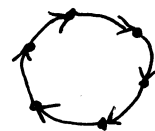
30. Доказать, что в игре "15" нельзя поменять местами фишки "14" и "15", оставив остальные на месте и не нарушая правил игры.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

31. Доказать, что нельзя, играя с кубиком Рубика, добиться того, чтобы (1) указанные на рисунке грани 1 и 2 поменялись бы местами, а остальные грани остались бы на месте; (2) угловые кубики одной из граней циклически переставились, а все остальные кубики остались бы на местах (возможно, повернувшись!).



32. Циклом порядка k называется перестановка такого вида: k элементов переходят друг в друга по кругу, остальные переходят в себя. Доказать, что всякая перестановка представима в виде произведения независимых циклов (два цикла называются независимыми, если элементы, сдвигаемые одним, оставляются на месте другим).



33. Доказать, что всякая четная перестановка представима в виде произведения нескольких циклов длины 3.

34. Два элемента группы x и y называются сопряженными, если $x = h y h^{-1}$ для некоторого элемента h этой группы. Какие элементы сопряжены в группе перестановок?

Подгруппы

Пусть G - группа, H - некоторое подмножество G . Оно называется подгруппой, если $n \in H$; $i(x) \in H$ для любого $x \in H$ и $x * y \in H$ для любых $x, y \in H$.

Например, \mathbb{Z} - подгруппа аддитивной группы \mathbb{R} .

35. Доказать, что для любого n множество $n\mathbb{Z}$ всех кратных n является подгруппой в \mathbb{Z} . Есть ли в \mathbb{Z} другие подгруппы?

36. Является ли подгруппой группы перестановок множества M множество перестановок, имеющих неподвижную точку (таких перестановок σ , что $\sigma(x) = x$ для некоторого $x \in M$)? Образуют ли подгруппу перестановки, оставляющие на месте данный элемент $x \in M$?

37. Найти все подгруппы группы $\mathbb{Z}/n\mathbb{Z}$.

38. Найти все конечные подгруппы группы \mathbb{C}^* ненулевых комплексных чисел по умножению.

39. Найти все подгруппы в группах симметрий правильного треугольника и квадрата.

40. Доказать, что для конечной группы G в определении подгруппы можно опустить условия $n \in H$ и $i(x) \in H$: если $x * y \in H$ для любых $x, y \in H$, то H - подгруппа. Существенна ли конечность G ?

41. Пусть G - группа, $H \subset G$ - подгруппа. Для каждого элемента $a \in G$ через Ha обозначим все элементы G , которые можно получить, умножая какой-то элемент H на a : $Ha = \{ha \mid h \in H\}$. Доказать, что для любых a и b либо $Ha = Hb$, либо Ha не пересекается с Hb .

42. (Теорема Лагранжа.) Пусть G - конечная группа, H - ее подгруппа. Доказать, что порядок G делится на порядок H . (Порядок = число элементов.) (Указание. См. предыдущую задачу.)

43. Вывести из теоремы Лагранжа утверждение задачи 9.

44. Пусть H - подгруппа аддитивной группы \mathbb{R} . Доказать, что либо H состоит из всех кратных некоторого действительного числа α , либо H всюду плотно в \mathbb{R} (т.е. в любом интервале есть элемент H).

45. Вывести из предыдущей задачи, что дробная часть числа $n\sqrt{2}$ при некотором $n \neq 0$ меньше 0.0001. (Указание. Числа $m + n\sqrt{2}$ ($m, n \in \mathbb{Z}$) образуют подгруппу в \mathbb{R} .)

46. Найти все конечные подгруппы (1) группы поворотов плоскости вокруг данной точки; (2) группы всех движений плоскости, для которых данная точка неподвижна.

Изоморфизм

Группа $\mathbb{Z}/2\mathbb{Z}$ остатков от деления на 2 по существу тождественна группе $\{+1, -1\}$ по умножению. Можно считать, что мы имеем дело по существу с одной и той же группой, а различаются лишь обозначения элементов: $0 \leftrightarrow 1, 1 \leftrightarrow (-1)$. Говорят, что эти группы изоморфны, а функция $0 \mapsto 1, 1 \mapsto -1$ есть их изоморфизм.

$$\left. \begin{array}{l|l} \begin{array}{c|c} a & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \\ \hline a & 0 & 1 \\ \hline 0 & 1 & \end{array} & a * b \\ \hline \mathbb{Z}/2\mathbb{Z} & \end{array} \right\} \begin{array}{c|c} \begin{array}{c|c} a & 1 & -1 \\ \hline 1 & 1 & -1 \\ -1 & -1 & 1 \\ \hline a & 1 & -1 \\ \hline -1 & -1 & \end{array} & a * b \\ \hline \{+1, -1\} & \end{array} \right\} i(a)$$

Определение. Пусть G и H - две группы. Функция $f: G \rightarrow H$ называется изоморфизмом, если f взаимно однозначна и выполнены такие свойства: (1) $f(n_G) = n_H$; (2) $f(i_G(a)) = i_H(f(a))$; (3) $f(a *_G b) = f(a) *_H f(b)$.
Здесь n_G, i_G и $*_G$ - операции в G , а $n_H, i_H, *_H$ - операции в H . Группы называются изоморфными, если существует изоморфизм одной из них в другую (тогда обратное отображение - также изоморфизм).

47. Указать изоморфные среди следующих групп: группа симметрий треугольника, $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/3\mathbb{Z})^*, \mathbb{Z}/6\mathbb{Z}$, группа перестановок множества из 3 элементов, группа кубических комплексных корней из 1 по умножению.

48. Две группы изоморфны третьей. Можно ли утверждать, что они изоморфны между собой?

49. Очевидно, изоморфные группы имеют одинаковое число элементов. Верно ли обратное?

50. Доказать, что любая группа из 2 элементов изоморфна $\mathbb{Z}/2\mathbb{Z}$, а любая группа из 3 элементов изоморфна $\mathbb{Z}/3\mathbb{Z}$.

51. Верно ли аналогичное утверждение для групп из 4 и 5 элементов?

52. Изоморфны ли группы (1) \mathbb{R} и \mathbb{Q} (по сложению); (2) \mathbb{Q} и \mathbb{Z} (по сложению); (3) \mathbb{R} по сложению и \mathbb{R}^* (ненулевые действительные числа по умножению); (4) \mathbb{R} по сложению и \mathbb{R}^+ (положительные действительные числа по умножению)?

53. Рассмотрим группу $\mathbb{Q} \oplus \mathbb{Q}$ пар рациональных чисел по сложению (сложение - покомпонентное). Изоморфна ли она группе \mathbb{Q} ? Изоморфна ли группа $\mathbb{Z} \oplus \mathbb{Z}$ (определенная аналогичным образом) группе \mathbb{Z} ?

54. Изоморфна ли группа $\mathbb{R} \oplus \mathbb{R}$ группе \mathbb{R} ?

55. Найти подгруппу группы \mathbb{C}^* (ненулевые комплексные числа по умножению), изоморфную группе поворотов плоскости вокруг фиксированной точки.

56. Существуют ли в \mathbb{Q} и \mathbb{R} подгруппы, изоморфные $\mathbb{Z} \oplus \mathbb{Z}$?

57. Доказать, что всякая группа, содержащая неединичный элемент, содержит подгруппу, изоморфную $\mathbb{Z}/n\mathbb{Z}$ при некотором $n > 1$ или изоморфную \mathbb{Z} .

58. Найти в группе перестановок множества из n элементов подгруппу, изоморфную $\mathbb{Z}/n\mathbb{Z}$

59. Доказать, что всякая группа G изоморфна некоторой подгруппе группы перестановок множества G . (Указание. См. задачу 4.)

60. Обозначим через \mathbb{Z}^n группу, элементами которой являются кортежи из n целых чисел, $\langle a_1, \dots, a_n \rangle + \langle b_1, \dots, b_n \rangle = \langle a_1 + b_1, \dots, a_n + b_n \rangle$. Доказать, что всякая подгруппа группы \mathbb{Z}^n изоморфна \mathbb{Z}^k при некотором k , причем $k \leq n$.

61. Доказать, что \mathbb{Z}^m и \mathbb{Z}^n не изоморфны при $m \neq n$.

62. Доказать, что все группы данного простого порядка p изоморфны (следовательно, изоморфны $\mathbb{Z}/p\mathbb{Z}$ и, следовательно, коммутативны).

63. Определим прямую сумму групп G и H как группу $G \oplus H$, элементами которой являются пары $\langle g, h \rangle$ с $g \in G$, $h \in H$, операции — покомпонентные. Доказать, что $(\mathbb{Z}/a\mathbb{Z}) \oplus (\mathbb{Z}/b\mathbb{Z})$ изоморфно $\mathbb{Z}/ab\mathbb{Z}$, если a и b взаимно просты.

64. Доказать, что для любого элемента g группы G отображение $S_g: h \mapsto ghg^{-1}$ является изоморфизмом группы G на себя.

Гомоморфизмы

Пусть G, H группы. Функция $f: G \rightarrow H$ называется гомоморфизмом, если $f(g_1 *_{G} g_2) = f(g_1) *_{H} f(g_2)$, $f(i_G(g)) = i_H(f(g))$ и $f(n_G) = n_H$. (Ср. определение изоморфизма.) Тривиальный пример гомоморфизма: $f(g) = n_H$ для всех $g \in G$.

65. Придумать примеры нетривиальных гомоморфизмов (I) группы перестановок в группу $\mathbb{Z}/2\mathbb{Z}$; (2) $\mathbb{Z}/6\mathbb{Z}$ в $\mathbb{Z}/12\mathbb{Z}$; (3) $\mathbb{Z}/12\mathbb{Z}$ в $\mathbb{Z}/6\mathbb{Z}$; (4) группы \mathbb{R}^* ненулевых действительных чисел по умножению в группу $\mathbb{Z}/2\mathbb{Z}$; (5) группы \mathbb{R}^* в группу \mathbb{R}^+ положительных действительных чисел по умножению; (6) группы \mathbb{C}^* ненулевых комплексных чисел по умножению в \mathbb{R}^+ ; (7) группы \mathbb{C}^* в группу $T = \{z \mid |z| = 1\}$ по умножению; (8) группы \mathbb{R} по сложению в группу T ; (9) группы движений плоскости в группу всех движений плоскости, оставляющих данную точку неподвижной; (10) аддитивной группы \mathbb{R} в \mathbb{R}^+ .

66. Найти все гомоморфизмы $\mathbb{Z}/n\mathbb{Z}$ в \mathbb{Z} .

67. Сколько имеется различных гомоморфизмов $\mathbb{Z}/n\mathbb{Z}$ в \mathbb{C}^* ?

68. Группа \mathbb{Z} и элемент $1 \in \mathbb{Z}$ обладают следующим свойством: для всякой группы G и элемента $a \in G$ существует единственный гомоморфизм $f: \mathbb{Z} \rightarrow G$, при котором $f(1) = a$. Доказать.

69. Придумать группу S и два элемента $m, n \in S$ так, чтобы выполнялось следующее свойство (см. предыдущую задачу): для всякой группы G и элементов $a, b \in G$ существует единственный гомоморфизм $f: S \rightarrow G$, для которого $f(m) = a$, $f(n) = b$. Группа с таким свойством называется свободной группой с двумя образующими.

70. Доказать, что любые две свободные группы с двумя образующими изоморфны.

71. Пусть $f: G \rightarrow H$ - гомоморфизм. Доказать, что ядро $\ker f = \{g \in G \mid f(g) = e_H\}$ и образ $\operatorname{im} f$ (= множество значений f) являются подгруппами групп G и H .

72. Пусть $f_1: G \rightarrow H_1$ и $f_2: G \rightarrow H_2$ - гомоморфизмы, причем $\ker f_1 = \ker f_2$. Доказать, что группы $\operatorname{im} f_1$ и $\operatorname{im} f_2$ изоморфны.

73. Пусть $f: G \rightarrow H$ - гомоморфизм. Доказать, что прообразы всех элементов $\operatorname{im} f$ содержат равное число элементов.

74. Доказать, что если $f: G \rightarrow H$ - гомоморфизм, G конечна, то (число элементов G) = (число элементов $\operatorname{im} f$) · (число элементов $\ker f$).

Задача 72 показывает, что образ гомоморфизма $f: G \rightarrow H$ определяется (с точностью до изоморфизма) самой группой G и ядром гомоморфизма. Пусть G - группа. Подгруппа $N \subset G$ называется нормальным делителем, если N есть ядро некоторого гомоморфизма f группы G в некоторую другую группу G' . Образ этого гомоморфизма (определяемый однозначно с точностью до изоморфизма) называется факторгруппой G по N и обозначается G/N .

75. Доказать, что для любой группы G подгруппы $\{e\}$ и G - нормальные делители и найти факторгруппы.

76. Найти факторгруппу аддитивной группы \mathbb{R} по подгруппе \mathbb{Z} целых чисел. (Ответ: \mathbb{T} .)

77. Найти факторгруппы \mathbb{C}^* по \mathbb{T} , \mathbb{C}^* по \mathbb{R}^+ , \mathbb{R}^* по \mathbb{R}^+ .

78. Найти факторгруппу группы движений плоскости по подгруппе параллельных переносов.

79. Пусть $f: G \rightarrow H$ - гомоморфизм. Доказать, что $f(g_1) = f(g_2) \Leftrightarrow g_1^{-1} \cdot g_2 \in \ker f$.

80. Доказать, что если N - нормальный делитель G , то $g_1^{-1} \cdot g_2 \in N \Leftrightarrow g_2 \cdot g_1^{-1} \in N$.

81. Пусть H - нормальный делитель G . Будем говорить, что $x \in G$ эквивалентно $y \in G$ по H , если $x^{-1}y \in H$. Показать, что разбивается на классы эквивалентных друг другу элементов, и множество этих классов находится во взаимно однозначном соответствии с группой G/H .

82. Доказать, что если подгруппа $H \subset G$ такова, что $g_1^{-1}g_2 \in H$ равносильно $g_2g_1^{-1} \in H$, то H - нормальный делитель. (Указание. См. предыдущую задачу.)

83. Доказать, что следующие свойства подгруппы H группы G равносильны: (1) H - нормальный делитель G ; (2) $xy \in H \Leftrightarrow yx \in H$; (3) $h \in H, g \in G \Rightarrow ghg^{-1} \in H$; (4) для всякого элемента $g \in G$ множества $Hg = \{hg \mid h \in H\}$ и $gH = \{gh \mid h \in H\}$ совпадают.

84. Доказать, что в коммутативной группе всякая подгруппа является нормальным делителем.

85. Какие подгруппы группы S_3 перестановок трехэлементного множества - нормальные делители? Найти соответствующие факторгруппы.

86. Подгруппа конечной группы содержит ровно половину её элементов. Доказать, что эта подгруппа - нормальный делитель и найти факторгруппу.

87. Найти факторгруппу группы T по подгруппе корней степени n из единицы. (Указание. Какие существуют гомоморфизмы T в себя?)

88. Доказать, что единственной нормальной подгруппой группы перестановок множества из n элементов при $n \geq 5$ является подгруппа четных перестановок.

Действие групп на множествах

Пусть G - группа, M - некоторое множество. Действием G на M называет гомоморфизм G в группу перестановок множества M . Перестановка, соответствующая элементу g , будет обозначаться T_g . (Таким образом, согласно определению гомоморфизма, $T_{gh}(m) = T_g \circ T_h(m)$.)

Пример. Каждая группа G действует на себе "левыми сдвигами":
 $T_g(x) = gx$.

89. Проверить, что это действительно действие. Можно ли заменить левые сдвиги на правые (т.е. положить $T_g(x) = xg$)?

Пусть G действует на множестве M : Назовем орбитой точки $m \in M$ множество всех точек, в которые она может перейти под действием преобразований, соответствующих элементам g : $O(m) = \{T_g(m) \mid g \in G\}$

90. Доказать, что орбиты разных точек множества M либо не пересекаются, либо совпадают.

91. Группа T (комплексных чисел с модулем 1 по умножению) действует на множестве C умножениями: $T_g(m) = g \cdot m$ ($g \in T, m \in C$). Каковы будут орбиты?

92. Пусть H - подгруппа G . Рассмотрим действие H на G левыми сдвигами: $T_h(g) = hg$. Что будет орбитами?

Пусть G действует на M , $m \in M$. Рассмотрим множество тех $g \in G$, при которых $T_g(m) = m$.

93. Доказать, что это - подгруппа (называемая стабилизатором точки m).

94. Конечная группа G действует на M , $m \in M$. Доказать, что (число элементов G) = (число элементов орбиты m) · (число элементов стабилизатора m).

95. Рассмотрим естественное действие группы S_{10} (перестановок десятиэлементного множества) на множестве всех последовательностей русских букв длины 10. Подсчитать величины, входящие в равенство предыдущей задачи, если $m = \text{"МАТЕМАТИКА"}$.

96. Пусть G - группа. Рассмотрим действие G на себе сопряжениями: $T_g(h) = ghg^{-1}$. Орбиты этого действия называются классами сопряженных элементов. Каковы они, если G коммутативна? если G - группа перестановок?

97. Доказать, что если число элементов группы G равно p^k , где p - простое, то количество элементов ее центра (множества элементов, коммутирующих со всеми элементами G , т.е. таких x , что $xy = yx$ для всех $y \in G$) кратно p (и, в частности, больше 1). (Указание. См. предыдущую задачу.)

98. Доказать, что всякая группа порядка p^2 , где p - простое число, коммутативна.

99. Доказать, что всякая конечная коммутативная группа изоморфна прямой сумме нескольких групп вида $\mathbb{Z}/n\mathbb{Z}$.

100. Назовем коммутатором элементов группы a, b элемент $[a, b] = a b a^{-1} b^{-1}$. Доказать, что $ab = ba \Leftrightarrow [a, b] = 1$. Доказать, что множество всевозможных произведений коммутаторов - нормальный делитель, называемый коммутантом. Доказать, что для любого нормального делителя N группы G (G/N коммутативна) $\Leftrightarrow (N$ содержит коммутант $G)$

101. Доказать, что группа, в которой $x^2 = 1$ при всех x , либо бесконечна, либо имеет порядок, равный степени 2. Доказать, любые две группы с таким свойством и одинаковым числом элементов изоморфны.