Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Московский педагогический государственный университет»

И. А. Шилин

КОМПЬЮТЕРНАЯ АЛГЕБРА В ЗАДАЧАХ

Учебное пособие

МПГУ
Москва • 2018

УДК 512.6(076.1)
ББК 22.14-4
Ш 578

Рецензенты:
А. В. Царев, доктор физико-математических наук (кафедра алгебры МПГУ);
А. А. Туганбаев, доктор физико-математических наук, профессор (кафедра высшей математики НИУ «МЭИ»)

Шилин, Илья Анатольевич.
Ш578 Компьютерная алгебра в задачах : учебное пособие / И. А. Шилин. – Москва : МПГУ, 2018. – 56 с.

ISBN 978-5-4263-0664-6

Учебное пособие содержит подборку практических задач с решениями для изучения дисциплины «Компьютерная алгебра» и адресовано всем студентам Института математики и информатики МПГУ, изучающим эту дисциплину.

УДК 512.6(076.1)
ББК 22.14-4

ISBN 978-5-4263-0664-6

Содержание

ВВЕДЕНИЕ

Компьютерная алгебра — это учебная дисциплина, призванная продемонстрировать и научить, как с помощью компьютеров можно решать математические задачи, относящиеся к общей алгебре. Под словом «решать» здесь следует понимать «решать точно», поскольку, например, задачу о вычислении корня полинома, принадлежащего заданному отрезку, на концах которого полином принимает значения разных знаков, относят к другой дисциплине — «Численным методам», где как раз достаточно найти приближенное решение с заданной точностью.

Эта небольшая книга написана автором в том же духе, в каком написаны подавляющее число толстых книг по компьютерным наукам: отсутствует методически выверенное последовательное изложение от самых азов до сложных изысканностей и вместо этого читателю предлагается изучать дисциплину через разобранные в книге примеры, то есть, по сути, девизом книги является название некогда популярной телепередачи «Делай с нами, делай как мы, делай лучше нас».

Почти все рассмотренные в книге задачи относятся к теории групп. В наше время существует немало вычислительных пакетов, с помощью которых можно найти точные решения теоретико-групповых задач. Наряду с обычными (Maple, Mathematica, MathCad, REDUCE, Derive, MATLAB) существуют специализированные вычислительные пакеты, целиком предназначенные именно для этой цели: свободно распространяемые GAP, Sage, FGB и коммерческие CAYLEY и Magma, созданные в Университете Сиднея[1]. Однако в этой книге, возможно, наперекор духу времени, под решением задач с помощью компьютера подразумевается их решение с помощью программирования, а не использования уже готовых пакетов. Изучению возможностей пакетов компьютерной алгебры должен, по всей видимости, быть посвещен отдельный курс, итогом которого должно быть, например, знание команды `NormalSubgroups` в GAP, которая выводит на экран список всех нормальных делителей заданной группы. Пользуясь пакетом GAP, с помощью всего лишь одной командной строки

```
gap> NormalSubgroups(SymmetriGroup(4));
```

удается вывести на экран все нормальные делители симметрической группы $\mathbf{S}_4$:

```
[Group(()), Group([(1,4)(2, 3),(1,3)(2,4)]),
```

[1] Автору довелось побывать в Лаборатории компьютерной алгебры Университета Сиднея, которую возглавляет создатель CAYLEY и Magma Джон Кэннон.

```
Group([(2,4,3),(1,4)(2, 3),(1,3)(2,4)]), Sym([1..4])],
```

то есть подгруппы $\{\mathrm{id}\}$, $\mathbf{K}$, $\mathbf{A}_4$ и $\mathbf{S}_4$, где $\mathbf{K}$ — так называемая подгруппа Клейна, состоящая из подстановок id, $(1\,2)(3\,4)$, $(1\,3)(2\,4)$ и $(1\,4)(2\,3)$ и изоморфная группе $\mathbb{Z}_2^2$. Но такой способ использования компьютера непригоден для нашего курса, цель которого научить мыслить алгоритмически при решении алгебраических задач, переводить задачу с языка математики на язык программных кодов и результаты программы обратно на математический язык.

При решении алгебраических задач с помощью программирования на первый план выступает задача реализации исследуемого математического объекта в программном коде. Подобный прием мы встречаем и в самой математике, например:

а) множество $\mathbb{C}$ реализуется как плоскость $\Pi = \mathbb{R}^2$ посредством взаимно однозначного отображения $z \longmapsto (\mathrm{re}\, z, \mathrm{im}\, z)$;

б) расширенная комплексная плоскость $\overline{\mathbb{C}}$ реализуется как сфера Римана $S : \xi^2 + \nu^2 + \zeta^2 = \zeta$: совместив плоскость $\zeta = 0$ с Π так, что ось $\xi = 0$ совпадает с осью $y = 0$ и ось $\nu = 0$ — с осью $x = 0$, используем взаимно однозначное отображение

$$a + b\mathbf{i} \longmapsto \left(\frac{a}{a^2+b^2+1}, \frac{b}{a^2+b^2+1}, \frac{a^2+b^2}{a^2+b^2+1}\right),$$
$$\infty \longmapsto (0, 0, 1);$$

в) скалярное $\mathbf{v} \cdot \mathbf{w}$ и векторное $\mathbf{v} \times \mathbf{w}$ произведение векторов $\mathbf{v} = (x_1, x_2, x_3)$ и $\mathbf{w} = (y_1, y_2, y_3)$ реализуется как произведение чисто мнимых кватернионов $h_1 = x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$ и $h_2 = y_1\mathbf{i} + y_2\mathbf{j} + y_3\mathbf{k}$, а именно

$$h_1 h_2 = -\mathbf{v} \cdot \mathbf{w} + (\mathbf{v} \times \mathbf{w}) \cdot \mathfrak{h},$$

где под $\mathfrak{h}$ подразумевается символический вектор $(\mathbf{i}, \mathbf{j}, \mathbf{k})$;

г) группа G реализутся в некотором линейном пространстве L в виде подгруппы мультипликативной группы невырожденных линейных операторов этого пространства посредством гомоморфизма $G \longrightarrow GL(L)$, а для конечной группы G, стало быть, в виде подгруппы мультипликативной группы невырожденных матриц (над соответствующем полем Φ) посредством гомоморфизма $G \longrightarrow \mathrm{Mat}(\dim L, \Phi)$. Такую реализацию называют представлением группы G. Например, группа $\mathbf{S}_n$ реализутся в виде подгруппы в $\mathrm{Mat}(n, \mathbb{Z}_2)$ посредством гомоморфизма $T : \sigma \longmapsto m(\sigma)$, где $m(\sigma) = e_{[1,\sigma(1)]} + \ldots + e_{[n,\sigma(n)]}$ и под $e_{[s,t]}$ понимается матрица (a_{ij}) над

полем $\mathbb{Z}_2$, матричные элементы которой определены правилом

$$a_{ij} = \begin{cases} 0, & \text{если } s \neq i \text{ или } t \neq j, \\ 1, & \text{если } s = i \text{ и } t = j; \end{cases}$$

д) подмножество A непустого множества B реализуется как характеристическая функция (индикатор) $\chi_A : B \longrightarrow \{0, 1\}$, где

$$\chi_A(x) = \begin{cases} 0, & \text{если } x \notin A, \\ 1, & \text{если } x \in A \end{cases}$$

(обобщая эту реализацию, Заде определил в 1965 году нечеткое подмножество в B как отображение $\varphi : B \longrightarrow [0; 1]$).

Если множество B конечно, а именно, $B = \{b_1, \ldots, b_n\}$, то, выписывая друг за другом значения характеристической функции χ_A, получаем двоичное число $\overline{c_1 c_2 \ldots c_n}$, где $c_i = \chi_A(b_i)$. Мы будем использовать этот прием, то есть реализовывать подмножества множества B в виде целых двоичных чисел от 0 (пустое подмножество) до $2^n - 1$ (само B), на протяжении всей книги. Аналогичную реализацию будем применять для отображений $B \longrightarrow D$, где D состоит из m элементов: в кодах программ эти отображения будут заменяться целыми числами в m-ичной системе счисления, записанными с помощью n цифр (разрядов).

К каждой из разобранных задач в качестве примера приведен программный код на языке PASCAL.

1. Вычисление образующих элементов мультипликативной группы поля вычетов и индексов по ним

Напомним, что факторкольцо кольца $\mathbb{Z}$ по идеалу $n\mathbb{Z}$, состоящему из чисел, делящихся на n, состоит из элементов $\overline{0}, 1, \ldots, \overline{n}$, являющихся в кольце $\mathbb{Z}$ классами чисел с равными остатками, получающимися при делении на n. Это кольцо обозначается $\mathbb{Z}_n$ и называется кольцом вычетов по модулю n. Элемент $\overline{a}$ обратим в том и только том случае, если НОД$(a, n) = 1$. Обратимые элементы образуют группу относительно умножения — ее называют мультипликативной группой кольца $\mathbb{Z}_n$. Будем обозначать ее $\operatorname{Inv}\mathbb{Z}_n$. Понятно, что в случае простого n все не равные нулю элементы кольца обратимы и $\mathbb{Z}_n$ является полем. Более того, можно доказать, что в случае простого n группа $\operatorname{Inv}\mathbb{Z}_n = \{\overline{1}, \ldots, \overline{n-1}\}$ циклическая. Как известно, число образующих элементов циклической группы порядка k равно $\Phi(k)$, где Φ — функция Эйлера, поэтому число образующих элементов мультипликативной группы поля вычетов вычисляется по формуле $\Phi(\Phi(n)) = \Phi(n-1)$.

Пусть $\overline{a}$ — один из таких образующих элементов. Тогда группу $\operatorname{Inv}\mathbb{Z}_n$ можно представить в виде

$$\operatorname{Inv}\mathbb{Z}_n = \langle\overline{a}\rangle = \{\overline{a}, \overline{a}^2, \ldots, \overline{a}^{n-2}, \overline{a}^{n-1} = \overline{1}\}.$$

Например, в циклической мультипликативной группе $\operatorname{Inv}\mathbb{Z}_{17} = \{\overline{1}, \overline{2}, \ldots, \overline{16}\}$ поля $\mathbb{Z}_{17}$ элемент $\overline{3}$ является образующим, поскольку

$$\begin{array}{llll} \overline{3}^1 = \overline{3} & \overline{3}^5 = \overline{5} & \overline{3}^9 = \overline{14} & \overline{3}^{13} = \overline{12} \\ \overline{3}^2 = \overline{9} & \overline{3}^6 = \overline{15} & \overline{3}^{10} = \overline{8} & \overline{3}^{14} = \overline{2} \\ \overline{3}^3 = \overline{10} & \overline{3}^7 = \overline{11} & \overline{3}^{11} = \overline{7} & \overline{3}^{15} = \overline{6} \\ \overline{3}^4 = \overline{13} & \overline{3}^8 = \overline{16} & \overline{3}^{12} = \overline{4} & \overline{3}^{16} = \overline{1} \end{array}$$

Напомним, что если элемент g циклической группы порядка k является образующим элементом, то элемент g^s тоже является образующим элементом в том и только том случае, когда НОД$(s, k) = 1$. Так, в приведенном примере числа $3, 5, 7, 9, 11, 13, 15$ взаимно просты с 16 и, следовательно, элементы

$$\overline{3}^3 = \overline{10}, \quad \overline{3}^5 = \overline{5}, \quad \overline{3}^7 = \overline{11}, \quad \overline{3}^9 = \overline{14},$$
$$\overline{3}^{11} = \overline{7}, \quad \overline{3}^{13} = \overline{12}, \quad \overline{3}^{15} = \overline{6}$$

группы $\operatorname{Inv}\mathbb{Z}_{17}$, то есть элементы $\overline{5}$, $\overline{6}$, $\overline{7}$, $\overline{10}$, $\overline{11}$, $\overline{12}$, $\overline{14}$ тоже являются образующими элементами.

Пусть $\overline{a}$ — образующий элемент группы $\operatorname{Inv}\mathbb{Z}_n$ (n — простое число). Индексом элемента $\overline{b} \in \operatorname{Inv}\mathbb{Z}_n$ по основанию $\overline{a}$ называют такое наименьшее неотрицательное целое число s, что $\overline{a}^s = \overline{b}$. Обозначают индекс так: $\operatorname{ind}_{\overline{a}}\overline{b}$. Так, возвращаясь к рассмотренному примеру, имеем

$$\begin{array}{llll}
\operatorname{ind}_{\overline{3}}\overline{1}=\overline{0} & \operatorname{ind}_{\overline{3}}\overline{5}=\overline{5} & \operatorname{ind}_{\overline{3}}\overline{9}=\overline{2} & \operatorname{ind}_{\overline{3}}\overline{13}=\overline{4} \\
\operatorname{ind}_{\overline{3}}\overline{2}=\overline{14} & \operatorname{ind}_{\overline{3}}\overline{6}=\overline{15} & \operatorname{ind}_{\overline{3}}\overline{10}=\overline{3} & \operatorname{ind}_{\overline{3}}\overline{14}=\overline{9} \\
\operatorname{ind}_{\overline{3}}\overline{3}=\overline{1} & \operatorname{ind}_{\overline{3}}\overline{7}=\overline{11} & \operatorname{ind}_{\overline{3}}\overline{11}=\overline{7} & \operatorname{ind}_{\overline{3}}\overline{15}=\overline{6} \\
\operatorname{ind}_{\overline{3}}\overline{4}=\overline{12} & \operatorname{ind}_{\overline{3}}\overline{8}=\overline{10} & \operatorname{ind}_{\overline{3}}\overline{12}=\overline{13} & \operatorname{ind}_{\overline{3}}\overline{16}=\overline{8}
\end{array}$$

Отображение

$$\operatorname{Ind}:\ \operatorname{Inv}\mathbb{Z}_n \longrightarrow \mathbb{Z}_{n-1},\ \overline{b} \longmapsto \operatorname{ind}_{\overline{a}}\overline{b}$$

является изоморфизмом мультипликативной группы $\operatorname{Inv}\mathbb{Z}_n$ в аддитивную группу $\mathbb{Z}_{n-1}$, аналогом изоморфизма $\ln : \mathbb{R}_+ \longrightarrow \mathbb{R}$, $b \longmapsto \ln b$ мультипликативной группы положительных действительных чисел в аддитивную группу действительных чисел, и применяется для решения степенных и показательных уравнений над полем $\mathbb{Z}_n$.

Компьютерная программа, которая спрашивает пользователя простое число n и выводит на экран образующие элементы группы $\operatorname{Inv}\mathbb{Z}_n$ и таблицу индексов по одному из образующих элементов, может быть составлена по следующей схеме:

а) производится отбор целых чисел $i \in \{1, \ldots, n-1\}$, взаимно простых с n — для этого используется включенная в программу функция `gcd`, вычисляющая наибольший общий делитель двух чисел;

б) если i — одно из отобранных чисел, то программа определяет его наименьшую степень s, такую, что остаток от деления i^s на n равен 1. Если $s = n-1$, то $\overline{i}$ — образующий элемент. При этом остатки от деления чисел $i^1, i^2, \ldots, i^{n-1}$ на n записываются в массив. Программе достаточно найти всего один образующий элемент: пробегая целые числа s от 2 до $n-1$, взаимно простые с $n-1$, программа выводит на экран остатки от деления чисел i^s на n — эти числа суть все остальные образующие элементы;

в) используя массив, программа выводит на экран таблицу индексов.

Соответствующий программный код может быть таким:

```
program zn;
var i,j,n : integer;
inv,d : array[1..100] of integer;
function gcd (x,y : integer) : integer;
begin
if x=0 then gcd:=y else gcd:=gcd(y mod x,x)
```

```
end;
BEGIN
writeln(); write('Input n => ');read(n);
i:=2;
repeat
      d[1]:=i; j:=1;
      repeat
          j:=j+1; d[j]:=(d[j-1]*i) mod n
      until d[j]=1;
      i:=i+1
until j=n-1;
writeln(); write('Generators: ');
for i:=1 to n-2 do if gcd(i,n-1)=1
        then if i>2 then write('; ',d[i]) else write(d[i]);
write('.'); writeln();
for i:=1 to n-1 do
begin    j:=1;
     while d[j]<>i do j:=j+1;
     writeln('ind(',i,')=',j mod (n-1))
end
END.
```

Упражнение 1. Составьте программу, которая спрашивает у пользователя n, коэффициенты $\overline{a}$ и $\overline{b}$ и выводит на экран решения линейного уравнения $\overline{a}x = \overline{b}$ над кольцом $\mathbb{Z}_n$.

Как известно, если $\overline{a} \in \operatorname{Inv}\mathbb{Z}_n$, то уравнение $\overline{a}x = \overline{b}$ имеет единственное решение $x = \overline{a}^{-1}\overline{b}$.

При $\overline{a} \notin \operatorname{Inv}\mathbb{Z}_n$ могут быть два случая:

- Если $d = \text{НОД}(a, n)$ является делителем числа b, то уравнение имеет d

$$x_1 = \overline{c},\ \ x_2 = \overline{c + \tilde{n}},\ \ \ldots, x_d = \overline{c + (d-1)\tilde{n}},$$

  где $\tilde{n} = \frac{n}{d}$ и $\overline{c}$ — единственное решение уравнения $\overline{\tilde{a}}x = \overline{\tilde{b}}$, $\tilde{a} = \frac{a}{d}$, $\tilde{b} = \frac{b}{d}$, над кольцом $\mathbb{Z}_{\tilde{n}}$;

- Если b не делится на d, то уравнение $\overline{a}x = \overline{b}$ не имеет решений.

Замечание. Поскольку порядок элемента конечной группы является делителем порядка группы, то число $|\operatorname{Inv}\mathbb{Z}_n| = \Phi(n)$ делится на порядок s элемента $\overline{a}$. Тогда $\Phi(n) = ks$ и, следовательно, $\overline{a}^{\Phi(n)} = (\overline{a}^s)^k = \overline{1}^k = \overline{1}$. Отсюда $\overline{a}\overline{a}^{\Phi(n)-1} = \overline{1}$, то есть

$$\overline{a}^{-1} = \overline{a}^{\Phi(n)-1}. \tag{1}$$

При решении уравнения $\overline{a}x = \overline{b}$ вручную при больших n гораздо проще использовать формулу (1), однако компьютерная программа совершит гораздо меньше операций, если найдет элемент $\overline{a}^{-1}$ методом перебора.

Упражнение 2. Составьте программу, которая спрашивает у пользователя n, коэффициенты $\overline{a}$ и $\overline{b}$ и выводит на экран решения линейного уравнения $\overline{a}x = \overline{b}$ над кольцом $\mathbb{Z}_n$, найденное с помощью цепных дробей.

Разделим n на a с остатком:

$$n = aq_0 + r_1, \;\; 0 \leqslant r_1 < |a|.$$

Если $r_1 \neq 0$, разделим a на r_1 с остатком:

$$a = r_1q_1 + r_2, \;\; 0 \leqslant r_2 < r_1.$$

Если $r_2 \neq 0$, разделим r_1 на r_2 с остатком:

$$r_1 = r_2q_2 + r_3, \;\; 0 \leqslant r_3 < r_2.$$

Последовательность $r_1, r_2, r_3, \ldots$ строго убывает и ограничена снизу числом ноль, поэтому, продолжая процесс деления с остатком далее, получим на некотором шаге равный нулю остаток и запись

$$\frac{n}{a} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_m}}}},$$

которую называют представлением числа $\frac{n}{a}$ в виде цепной (или непрерывной) дроби. Для цепной дроби используется компактная запись $[q_0; q_1, q_2, \ldots, q_m]$. Цепные дроби

$$\delta_0 := [q_0], \;\; \delta_1 := [q_0; q_1], \;\; \delta_2 := [q_0; q_1, q_2], \ldots,$$
$$\delta_{m-1} := [q_0; q_1, \ldots, q_{m-1}], \;\; \delta_m := [q_0; q_1, q_2, \ldots, q_m]$$

называют подходящими к дроби $[q_0; q_1, q_2, \ldots, q_n]$. Обозначим числитель и знаменатель подходящей дроби δ_i соответственно P_i и Q_i. Если a и n взаимно просты, то единственным решением уравнения $\overline{a}x = \overline{b}$ является класс целых чисел, содержащий число $(-1)^m P_{m-1} b$.

Упражнение 3. Составьте программу, которая спрашивает у пользователя простое число n, коэффициенты $\overline{a}$, k, c и $\overline{b}$ и выводит на экран решения показательного уравнения $\overline{a}^{kx+c} = \overline{b}$ над полем $\mathbb{Z}_n$.

Пусть $\overline{z}$ — образующий элемент группы $\operatorname{Inv}\mathbb{Z}_n$. Тогда

$$\operatorname{ind}_{\overline{z}} \overline{a}^{kx+c} = \operatorname{ind}_{\overline{z}} \overline{b},$$
$$(kx + c)\operatorname{ind}_{\overline{z}} \overline{a} = \operatorname{ind}_{\overline{z}} \overline{b},$$
$$(k \operatorname{ind}_{\overline{z}} \overline{a})x + (c \operatorname{ind}_{\overline{z}} \overline{a}) = \operatorname{ind}_{\overline{z}} \overline{b},$$

то есть задача свелась к решению линейного уравнения над кольцом $\mathbb{Z}_{n-1}$.

Упражнение 4. Составьте программу, которая спрашивает у пользователя простое число n, коэффициенты $\overline{a}$ и $\overline{b}$ и показатель степени k и выводит на экран решения степенного уравнения $\overline{a}x^k = \overline{b}$ над полем $\mathbb{Z}_n$.

Если $\operatorname{Inv}\mathbb{Z}_n = \langle\overline{z}\rangle$, то

$$\operatorname{ind}_{\overline{z}}(\overline{a}x^k) = \operatorname{ind}_{\overline{z}}\overline{b},$$
$$\operatorname{ind}_{\overline{z}}\overline{a} + k\operatorname{ind}_{\overline{z}}x = \operatorname{ind}_{\overline{z}}\overline{b},$$
$$k\operatorname{ind}_{\overline{z}}x = \operatorname{ind}_{\overline{z}}\overline{b} - \operatorname{ind}_{\overline{z}}\overline{a},$$

то есть задача свелась к решению линейного уравнения над кольцом $\mathbb{Z}_{n-1}$.

2. Вычисление коэффициентов унитарного комплексного многочлена по его корням, являющимися целыми гауссовыми числами

Пусть f — унитарный многочлен над полем $\mathbb{C}$ и $\deg f = n \geqslant 1$. Тогда существует комплексный корень многочлена f (теорема Гаусса). Более того, существуют комплексные корни $\alpha_1, \ldots, \alpha_k$ кратности $m_1, \ldots, m_k$, где $m_1 + \ldots + m_k = n$. Если f имеет вид

$$f = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

то его коэффициенты и корни связаны равенствами

$$\begin{cases} a_{n-1} = -(\underbrace{\alpha_1 + \ldots + \alpha_n}_{C_n^1 = n \text{ слагаемых}}), \\ a_{n-2} = \underbrace{\alpha_1\alpha_2 + \ldots + \alpha_{n-1}\alpha_n}_{C_n^2 \text{ слагаемых}}, \\ \ldots \\ a_{n-i} = (-1)^i(\underbrace{\alpha_1\alpha_2\ldots\alpha_i + \ldots + \alpha_{n-i+1}\ldots\alpha_n}_{C_n^i \text{ слагаемых}}), \\ \ldots \\ a_0 = (-1)^n \underbrace{\alpha_1\alpha_2\ldots\alpha_n}_{C_n^n = 1 \text{ слагаемое}} \end{cases} \tag{2}$$

(теорема Виета).

Подмножество $\mathbb{Z}[\mathbf{i}]$ поля $\mathbb{C}$, состоящее из чисел, действительная и мнимая часть которых суть целые числа, является подкольцом и называется кольцом целых гауссовых чисел. Составим программу, которая спрашивает у пользователя степень n многочлена f, действительные и мнимые части корней $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}[\mathbf{i}]$ многочлена f и выводит на экран коэффициенты $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ указанного многочлена.

Заметим, что $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ являются однородными симметрическими многочленами, принадлежащими кольцу $\mathbb{C}[\alpha_1, \ldots, \alpha_n]$. Каждому моному

$$\mu_{p_1\ldots p_n} = \alpha_1^{p_1}\alpha_2^{p_2}\ldots\alpha_n^{p_n}, \qquad p_i \in \{0, 1\},$$

входящему в эти многочлены, поставим в соответствие целое двоичное число $z = \overline{p_1 p_2 \ldots p_n}$. Тем самым установлено взаимно однозначное отображение множества мономов, встречающихся в равенствах (2), и множеством $\{1, 2, \ldots, 2^n - 1\}$. Иными словами, по числу z можно восстановить моном $\mu_{p_1\ldots p_n}$ и определить, к какому из многочленов

$a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ относится этот моном. Принимая это во внимание, программу можно составить по следующей схеме:

а) программа спрашивает n, $\operatorname{re}\boldsymbol{\alpha}_i$ и $\operatorname{im}\boldsymbol{\alpha}_i$ для $i \in \{1, \ldots, n\}$;

б) каждое целое число i от 1 до $2^n - 1$ программа переводит в двоичную систему счисления, находит значение соответствующего ему монома и добавляет это значение к переменной $a_{p_1+\ldots+p_n}$. Например, если пользователем введены числа $n = 4$, $\boldsymbol{\alpha}_1 = 3 - 2\mathbf{i}$, $\boldsymbol{\alpha}_2 = 3 + 2\mathbf{i}$, $\boldsymbol{\alpha}_3 = -4$ и $\boldsymbol{\alpha}_4 = \mathbf{i}$, то числу $11_{10} = 1011_2$ соответствует моном $\boldsymbol{\mu}_{1011} = \boldsymbol{\alpha}_1\boldsymbol{\alpha}_3\boldsymbol{\alpha}_4$, при этом

$$\boldsymbol{\mu}_{1011}(3 - 2\mathbf{i}, -4, \mathbf{i}) = -8 - 12\mathbf{i};$$

в) программа выводит на экран коэффициенты $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$. Например, коэффициент a_1 вычисляется по формуле

$$\begin{aligned} a_1 = -[&\boldsymbol{\mu}_{1110}(3 - 2\mathbf{i}, 3 + 2\mathbf{i}, -4) + \boldsymbol{\mu}_{1101}(3 - 2\mathbf{i}, 3 + 2\mathbf{i}, \mathbf{i}) + \\ &+ \boldsymbol{\mu}_{1011}(3 - 2\mathbf{i}, -4, \mathbf{i}) + \boldsymbol{\mu}_{0111}(3 + 2\mathbf{i}, -4, \mathbf{i})] = \\ &= -[(-52) + (13\mathbf{i}) + (-8 - 12\mathbf{i}) + (8 - 12\mathbf{i})] = 52 + 11\mathbf{i}. \end{aligned}$$

В приведенной ниже программе (с ограничением $n \leqslant 6$) массивы `re` и `im` предназначены для записи действительной и мнимой части корней многочлена, массивы `ar` и `ai` — для записи действительной и мнимой части коэффициентов, а массив `d` — для записи целого числа в двоиной системе счисления:

```
program polynomials;
var n,i,j,k,l,p,kr,ki : integer;
   re,im : array[1..6] of integer;
   ar,ai : array[0..5] of integer;
   d: array[0..64] of integer;
   s : string;
BEGIN
writeln('Input the number of the roots'); readln(n);
k:=1;
for i:=1 to n do
begin
     k:=2*k;
     writeln(' Root ',i,': Input the real part'); readln(re[i]);
     writeln(' Input the imagine part'); readln(im[i]);
     ar[i-1]:=0; ai[i-1]:=0
end;
for i:=1 to k-1 do
begin
     l:=i;
     for j:=1 to n do
     begin
          d[j]:=l mod 2;
```

```
            l:=l div 2
        end;
        p:=0; kr:=1; ki:=0;
        for j:=1 to n do
        begin
            p:=p+d[j];
            if d[j]=1 then
            begin
                l:=kr;
                kr:=kr*re[j]-ki*im[j];
                ki:=l*im[j]+ki*re[j]
            end
        end;
        p:=n-p;
        ar[p]:=ar[p]+kr; ai[p]:=ai[p]+ki
    end;
    for i:=0 to n-1 do if (((n-1-i) mod 2) = 0) then
    begin
        ar[i]:=-ar[i]; ai[i]:=-ai[i]
    end;
    for i:=0 to n-1 do
    begin
        if ai[n-1-i]>=0 then s:='+' else s:='';
        writeln();
        write('a(',n-1-i,') = ',ar[n-1-i],s,ai[n-1-i],'i')
    end
    END.
```

В частности, для $n = 4$ и корней $\alpha_1 = 3 - 2\mathbf{i}$, $\alpha_2 = 3 + 2\mathbf{i}$, $\alpha_3 = -4$ и $\alpha_4 = \mathbf{i}$ программа находит, что

$$a_3 = -2 - \mathbf{i}, \quad a_2 - 11 + 2\mathbf{i}, \quad a_1 = 52 + 11\mathbf{i}, \quad a_0 = -52\mathbf{i}.$$

3. Вычисление числа транзитивных отношений

Число элементов пустого или конечного множества A называется порядком этого множества и обозначается $|A|$. Множество, элементами которого являются подмножества множества A, называется булеаном множества A и обозначается 2^A, поскольку $\left|2^A\right| = 2^{|A|}$.

Пусть $A_1, A_2 \ldots, A_n$ — непустые множества. Прямым произведением этих множеств называется множество

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i\}.$$

Если множества $A_1, \ldots, A_n$ конечны, то

$$|A_1 \times \ldots \times A_n| = \prod_{i=1}^{n} |A_i|.$$

Вместо $\underbrace{A \times \ldots \times A}_{n}$ пишут A^n. Множество A^2 называют квадратом множества A, множество A^3 — кубом, A^4 — четвертой степенью множества A и т. д.

n-арным отношением на множестве A называется подмножество в A^n. Специальное название имеет отношение $\Delta(A^n) = \{(a, \ldots, a)\}$ — оно называется диагональю. Если $n = 2$, то отношение называют *бинарным*.

Бинарное отношение Ω на множестве A называют:

а) рефлексивным, если $\Delta(A^2) \subset \Omega$;

б) симметричным, если из включения $(a, b) \in \Omega$ следует включение $(b, a) \in \Omega$;

в) антисимметричным, если из включений $(a, b) \in \Omega$ и $(b, a) \in \Omega$ следует $a = b$;

г) транзитивным, если из $(a, b) \in \Omega, (b, c) \in \Omega$ следует $(a, c) \in \Omega$;

д) отношением эквивалентности, если Ω рефлексивно, симметрично и тразитивно;

е) отношением частичного порядка, если Ω рефлексивно, антисимметрично и транзитивно.

Выделим во множестве A непустые подмножества, такие, что каждый элемент множества A принадлежит, причем только одному, такому подмножеству. В этом случае выбранные подмножества называют классами и говорят, что множество A разбито на классы. Если множество A разбито на классы, то можно считать, что на A задано некоторое отношение эквивалентности Ω, а именно: $(a, b) \in \Omega$ в том и только в том

случае, если элементы a и b принадлежат одному классу. И наоборот, если Ω — отношение эквивалентности на множестве A, то можно считать, что множество A разбито на классы: любой элемент $a \in A$ принадлежит классу $C_a = \{b \in A \mid (a, b) \in \Omega\}$.

Пусть $|A| = n$. Так как для нас не является важным, из каких элементов состоит A, будем считать, что A состоит из чисел $1, \ldots, n$, то есть $A = \{1, \ldots, n\}$. Бинарному отношению Ω на множестве A поставим в соответствие матрицу (a_{ij}), матричные элементы a_{ij} в которой определяются формулой

$$a_{ij} = \begin{cases} 0, & \text{если } (i, j) \notin \Omega, \\ 1, & \text{если } (i, j) \in \Omega. \end{cases}$$

Так, в частном случае $n = 3$ рефлексивному отношению

$$\Omega_1 = \{(1, 1), (1, 3), (2, 2), (3, 3)\}$$

и симметричному отношению

$$\Omega_2 = \{(1, 1), (1, 2), (2, 1)(2, 3), (3, 2)\}$$

соответствуют матрицы

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Если отношение Ω рефлексивно, то в соответствующей ему матрице все матричные элементы главной диагонали равны единице. Так как число элементов, находящихся вне главной диагонали, равно $n^2 - n$, то существует 2^{n^2-n} рефлексивных отношений.

Симметричному отношению соответствует симметрическая матрица или, что то же самое, *полу*матрица, к которой относятся матричные элементы, находящиеся не ниже главной диагонали. Например, рассмотренному выше отношению Ω_2 соответствует полуматрица

$$\begin{pmatrix} 1 & 1 & 0 \\ & 0 & 1 \\ & & 0 \end{pmatrix}.$$

Так как число элементов в полуматрице равно

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2} = C_{n+1}^2,$$

то существует $2^{C_{n+1}^2}$ симметричных отношений.

Обозначим S_n^k число разбиений множества, состоящего из n элементов, на k классов. Число S_n^k называют числом Стирлинга второго рода. Из определения следует, что $S_n^1 = S_n^n = 1$. Для общего случая доказана формула

$$S_n^k = \frac{1}{k!} \sum_{i=0}^{k-1} (-1)^i C_k^i (k-i)^n.$$

Число B_n разбиений множества, состоящего из n элементов, на классы или, что то же самое, число отношений эквивалентности на таком множестве вычисляется, очевидно, по формуле $B_n = \sum\limits_{k=1}^{n} S_n^k$. Число B_n называют числом Белла.

Так как антисимметричному отношению Ω соответствует матрица (a_{ij}), матричные элементы главной диагонали которой могут быть любыми, а все остальные $(i \neq j)$ удовлетворяют условию

$$\text{если } a_{ij} = 1, \text{ то } a_{ji} \neq 1,$$

то можно считать, что отношению Ω поставлена в соответствие полуматрица (b_{ij}), $i \leqslant j$, на главной диагонали которой стоят нули или единицы, а матричные элементы, расположенные выше главной диагонали, равны α, β или γ, где

$$\begin{gathered} b_{ij} = \alpha \text{ означает, что } a_{ij} = a_{ji} = 0, \\ b_{ij} = \beta \text{ означает, что } a_{ij} = 1 \text{ и } a_{ji} = 0, \\ b_{ij} = \gamma \text{ означает, что } a_{ij} = 0 \text{ и } a_{ji} = 1. \end{gathered}$$

Например, антисимметричному отношению $\Omega = \{(1,2),(1,3),(3,2)\}$ на множестве $\{1,2,3\}$ соответствует полуматрица

$$\begin{pmatrix} 1 & \alpha & \beta \\ & 0 & \gamma \\ & & 0 \end{pmatrix}.$$

Так как число матричных элементов главной диагонали равно n, а число матричных элементов полуматрицы, расположенных над главной диагональю, равно

$$1 + \ldots + (n-1) = \frac{n(n-1)}{2} = C_n^2,$$

то на множестве порядка n существует $2^n \cdot 3^{C_n^2}$ антисимметричных отношений.

Формулы для числа $t(n)$ транзитивных отношений и числа $p(n)$ отношений частичного порядка на множестве из n элементов в настоящее время неизвестны, но числа $t(n)$ и $p(n)$ связаны между собой равенством

$$t(n) = \sum_{k=0}^{n} \left(\sum_{l=0}^{k} C_n^l \, S_{n-l}^{k-l} \right) p(n).$$

Программа, которая спрашивает порядок множества и выводит на экран число транзитивных отношений на этом множестве, может быть составлена по следующей схеме:

а) программа спрашивает n и обнуляет счетчик `v` транзитивных отношений;

б) переводит всякое целое число i, удовлетворяющее неравенству $1 \leqslant i \leqslant 2^{n^2} - 1$, в двоичную систему счисления. Из цифр числа i программа формирует матрицу размера $n \times n$: например, в случае $n = 3$ числу

$$i = 219_{10} = 011011011_2$$

соответствует матрица

$$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Далее обнуляется счетчик `w` и происходит следующая проверка матрицы. Для каждого равного единице матричного элемента a_{ij} и каждого номера столбца k в случае, если матричный элемент a_{jk} тоже отличен от нуля, рассматривается матричный элемент a_{ik} — если он равен нулю, то значение счетчика `w` увеличивается на единицу.

```
program transitiverel;
var i,j,n,m,l,k,w,v,s : integer;
   d: array[0..64] of integer;
   a: array[1..8,1..8] of integer;
BEGIN
writeln(); write('Input n: '); read(n);
m:=1; v:=0; s:=n*n;
for i:=1 to s do m:=2*m;
for i:=1 to m-1 do
begin
     l:=i;
     for j:=1 to s do
     begin
          d[j]:=l mod 2;
```

```
        l:=l div 2
    end;
    l:=0;
    for j:=1 to n do for k:=1 to n do
    begin
        l:=l+1;
        a[j,k]:=d[l]
    end;
    w:=0;
    j:=0;
    repeat
         j:=j+1;
         k:=0;
         repeat
             k:=k+1;
             if a[j,k]=1 then
             begin
                 l:=1;
                 repeat
                     if a[k,l]=1 then if a[j,l]<1 then w:=1;
                     l:=l+1
                 until ((l>n) or (w=1))
             end
         until ((k>n) or (w=1))
    until ((j>n) or (w=1));
    if w=0 then v:=v+1
end;
writeln(); write('t(',n,')=',v)
END.
```

Упражнение 5. Напишите программу, спрашивающую n и вычисляющую число отношений эквивалентности на множестве порядка n.

Упражнение 6. Напишите программу, спрашивающую n и вычисляющую число отношений частичного порядка на множестве порядка n.

Упражнение 7. Топологией произвольного множества M называют подмножество $\mathfrak{T}$ в 2^M, удовлетворяющее условиям: а) $\emptyset, M \in \mathfrak{T}$; б) для любых $A_1, \ldots, A_s \in \mathfrak{T}$ выполняется включение $\bigcap\limits_{i=1}^{s} A_s \in \mathfrak{T}$; в) для всякого $\mathfrak{A} \subset \mathfrak{T}$ выполняется включение $\bigcup\limits_{A \in \mathfrak{A}} A \in \mathfrak{T}$. Так, топологиями в M являются множество $\mathfrak{T}_0 = \{\emptyset, M\}$ (тривиальная) и 2^M (дискретная).

Элементы топологии $\mathfrak{T}$ называются открытыми подмножествами в M. Если $A \in \mathfrak{T}$, то его дополнение $M \setminus A$ называется замкнутым подмножеством в M.

Составьте программу, спрашивающую n и выводящую на экран число всех топологий на множестве порядка n.

Топологию множества M можно задать, указав не открытые, а замкнутые подмножества в M. Понятно, что замена замкнутых подмножеств на открытые приводит к «двойственному» определению, не меняя алгоритм вычисления топологий по сути, а самым сложным в этом алгоритме является проверка последнего условия из определения топологии. Однако можно поступить так: замкнутые множества будем рассматривать как неподвижные точки особого отображения $2^M \longrightarrow 2^M$, которое назовем замыканием. Иными словами, топологическое пространство определим следующимм образом.

Множество M называют топологическим пространством, если задано отображение $\boldsymbol{\tau} : 2^M \longrightarrow 2^M$, удовлетворяющее условиям:

а) пустое множество является неподвижной точкой отображения $\boldsymbol{\tau}$, то есть $\boldsymbol{\tau}(\emptyset) = \emptyset$;

б) $A \subset \boldsymbol{\tau}(A)$;

в) $\boldsymbol{\tau}(A \cup B) = \boldsymbol{\tau}(A) \cup \boldsymbol{\tau}(B)$;

г) $\boldsymbol{\tau}^2 = \boldsymbol{\tau}$.

Отображение $\boldsymbol{\tau}$ называют замыканием.

Задача, таким образом, заключается в отыскании всех замыканий. Для сокращения вычислений в программе целесообразно рассматривать только такие отображения $\boldsymbol{\tau} : 2^M \longrightarrow 2^M$, для которых аксиома **а** выполнена. Создать более эффективный алгоритм можно, опираясь на следующие соображения.

Множеству M, состоящему из n элементов, поставим в соответствие одномерный массив длины n, ячейки которого будем нумеровать числами от 1 до n справа налево. Заполняя эти ячейки числами 0 и 1, мы получаем характеристические функции на множестве $\{1, \ldots, n\}$, то есть перечисляем подмножества в $\{1, \ldots, n\}$:

$$
\begin{array}{lcl}
\emptyset & \longleftrightarrow & \boxed{0}\boxed{0}\ldots\boxed{0}\boxed{0} \\
\{1\} & \longleftrightarrow & \boxed{0}\boxed{0}\ldots\boxed{0}\boxed{1} \\
 & \ldots & \\
\{1, \ldots, n\} & \longleftrightarrow & \boxed{1}\boxed{1}\ldots\boxed{1}\boxed{1}
\end{array}
$$

Занумеруем эти подмножества числами от 1 до 2^n сверху вниз. Вместо того чтобы рассматривать $(2^n)^{2^n}$ отображений $\boldsymbol{\tau} : 2^M \longrightarrow 2^M$ и проверять каждое из них на выполнимость аксиом **б** – **г** замыкания, поступим следующим образом. Для каждого k поставим k-ому подмножеству M_k в M в соответствие подмножество $\mathfrak{M}_k$ булеана 2^M, состоящее из возможных образов подмножества M_k, которые могут получиться при отображениях $\boldsymbol{\tau}$, удовлетворяющих аксиоме **b**. Для этого заметим, что в силу аксиомы **b** получается, что если k-ое подмножество содержит элемент $p \in \{1, \ldots, n\}$, то его образом при отображении могут быть только подмножества, номера $s_{p,q,r}$ которых определяются формулой

$$s_{p,q,r} := 2^{p-1} + q + 2^p(r-1),$$

где $q \in \{1, \ldots, 2^{p-1}\}$ и $r \in \{1, \ldots, 2^{n-p}\}$, то есть определяются первыми 2^{n-p} членами 2^{p-1} арифметических прогрессий, разность в которых равна 2^p, а первый член вычисляется по формуле $s_{p,q,1} = 2^{p-1} + q$. Составим из этих подмножеств подмножество

$\mathfrak{M}_{k,p}$ в булеане 2^M. Множество $\mathfrak{M}_k$ получается тогда по формуле $\mathfrak{M}_k := \bigcap\limits_{p\in M_k} \mathfrak{M}_{k,p}$.

Например, при нахождении топологий на множестве $M = \{1,2,3,4\}$ для его седьмого подмножества $M = \{2,3\}$, которое задается массивом $\boxed{0}\boxed{1}\boxed{1}\boxed{0}$, получаем последовательности

$$\begin{gathered}
s_{2,1,1} = 3,\ s_{2,1,2} = 7,\ s_{2,1,3} = 11,\ s_{2,1,4} = 15,\ldots\\
s_{2,2,1} = 4,\ s_{2,2,2} = 8,\ s_{2,2,3} = 12,\ s_{2,2,4} = 16,\ldots\\
s_{3,1,1} = 5,\ s_{3,1,2} = 13,\ldots\\
s_{3,2,1} = 6,\ s_{3,2,2} = 14,\ldots\\
s_{3,3,1} = 7,\ s_{3,3,2} = 15,\ldots\\
s_{3,4,1} = 8, s_{3,4,2} = 16,\ldots,
\end{gathered}$$

откуда

$$\begin{gathered}
\mathfrak{M}_{7,2} = \{M_3, M_4, M_7, M_8, M_{11}, M_{12}, M_{15}, M_{16}\},\\
\mathfrak{M}_{7,3} = \{M_5, M_6, M_7, M_8, M_{13}, M_{14}, M_{15}, M_{16}\}
\end{gathered}$$

и, следовательно, $\mathfrak{M}_7 = \{M_7, M_8, M_{15}, M_{16}\}$.

4. Вложение конечной группы в группу преобразований этой группы

Преобразованием непустого множества A называется взаимно однозначное отображение $A \longrightarrow A$. Множество преобразований множества A будем обозначать $\operatorname{Symm} A$. Композицией преобразований $\varphi, \psi \in \operatorname{Symm} A$ называют отображение

$$\varphi\psi : \ A \longrightarrow A, \ a \longmapsto \varphi(\psi(a)).$$

Легко показать, что $\varphi\psi \in \operatorname{Symm} A$ и для любых $\varphi, \psi, \gamma \in \operatorname{Symm} A$ выполняется равенство $(\varphi\psi)\gamma = \varphi(\psi\gamma)$, таким образом, композиция является ассоциативной бинарной операцией на множестве $\operatorname{Symm} A$. Во множестве $\operatorname{Symm} A$ относительно копозиции имеется нейтральный элемент — им является тождественное преобразование $\mathrm{id} : \ a \longmapsto a$. Кроме того, для каждого преобразования $\varphi \in \operatorname{Symm} A$ отображение φ^{-1} существует и тоже является преобразованием множества A. Следовательно, $\operatorname{Symm} A$ является группой относительно композиции.

Если множество A конечно, то конечна и группа $\operatorname{Symm} A$. Если $|A| = n$, то группу $\operatorname{Symm} A$ называют симметрической группой и обозначают $\mathbf{S}_n$. Элементы группы $\mathbf{S}_n$ (то есть преобразования конечного множества) называют подстановками. Без потери общности можно считать, что A состоит из чисел: $A = \{1, \ldots, n\}$. Наглядно произвольную подстановку $\sigma \in \mathbf{S}_n$ можно представить в виде матрицы

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Еще удобнее записывать подстановку в виде произведения независимых циклов. Например, пусть

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 7 & 3 & 5 & 2 & 1 & 9 & 8 \end{pmatrix}.$$

Тот факт, что

$$\begin{gathered} 1 \longmapsto 4 \longmapsto 3 \longmapsto 7 \longmapsto 1, \\ 2 \longmapsto 6 \longmapsto 2, \\ 8 \longmapsto 9 \longmapsto 8, \\ 5 \longmapsto 5, \end{gathered}$$

принято записывать так:

$$\sigma = (1\,4\,3\,7)(2\,6)(8\,9)(5).$$

Слово «цикл» означает, что $(1\,4\,3\,7)$ мы можем переписать в виде $(4\,3\,7\,1)$, или $(3\,7\,1\,4)$, или $(7\,1\,4\,3)$, то есть

$$\sigma = (3\,7\,1\,4)(2\,6)(9\,8)(5)$$

или

$$\sigma = (4\,3\,7\,1)(6\,2)(8\,9)(5)$$

и т. д. Слово «независимый» означает, что каждый элемент области определения подстановки σ принадлежит только одному циклу. Таким образом, каждая подстановка разлагается в произведение независимых циклов однозначно — с точностью до порядка записи циклов и элементов, с которых начинается запись циклов. Предположим, что σ раскладывается в произведение s циклов. Разумеется, можно считать, что длины $l_1, \ldots, l_s$ циклов удовлетворяют неравенству $l_1 \leqslant l_2 \leqslant \ldots \leqslant l_s$. Набор $\operatorname{pow}\sigma = (l_1, \ldots, l_s)$ назовем показателем. Подстановки $\sigma, \tau \in \mathbf{S}_n$ называются сопряженными, если существует такой внутренний автоморфизм[2] φ_g, что $\varphi_g(\sigma) = \tau$. Оказывается, σ и τ сопряжены в том и только том случае, если $\operatorname{pow}\sigma = \operatorname{pow}\tau$. Бинарное отношение сопряженности является отношением эквивалентности на группе $\mathbf{S}_n$. Если среди чисел $l_1, \ldots, l_s$ имеются равные, а именно

$$\operatorname{pow}\sigma = (\underbrace{l_1, \ldots, l_{m_1}}_{m_1 \text{ чисел}}, \overbrace{l_{m_1+1}, \ldots, l_{m_1+m_2}}^{m_2 \text{ чисел}}, \ldots, \underbrace{l_{m_1+\ldots+m_{r-1}+1}, \ldots, l_s}_{m_r \text{ чисел}})$$

и

$$l_1 = \ldots = l_{m_1}, \quad l_{m_1+1} = \ldots = l_{m_1+m_2}, \quad \ldots, \quad l_{m_1+\ldots+m_{r-1}+1} = \ldots = l_s,$$

то порядок класса $\operatorname{Cgnt}_{l_1,\ldots,l_s}$ сопряженных подстановок с показателем $(l_1, \ldots, l_s)$ вычисляется по формуле

$$|\operatorname{Cgnt}_{1,\ldots,l_s}| = \frac{n!}{(l_1)^{m_1}(l_{m_1+1})^{m_2}\ldots(l_{m_1+\ldots+m_{r-1}+1})^{m_r}\, m_1! m_2! \ldots m_r!}.$$

Так, группа

$$\mathbf{S}_3 = \{\mathrm{id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$$

[2]По поводу определения внутреннего автоморфизма смотрите следующую задачу.

разбивается на следующие классы сопряженности:

$$\{\mathrm{id}\},\quad \{(1\,2),(1\,3),(2\,3)\},\quad \{(1\,2\,3),(1\,3\,2)\}.$$

Первый класс состоит из единственной подстановки $\mathrm{id} = (1)(2)(3)$ с показателем $\operatorname{pow}\mathrm{id} = (1,1,1)$; второй класс состоит из подстановок

$$\begin{gathered}(1\,2) = (3)(1\,2),\\ (1\,3) = (2)(1\,3),\\ (2\,3) = (1)(2\,3),\end{gathered}$$

показатель которых равен $(1,2)$; третий класс состоит из двух подстановок с показателем $\operatorname{pow}(1\,2\,3) = \operatorname{pow}(1\,3\,2) = (1)$. При этом

$$\begin{gathered}|\mathrm{Cgnt}_{1,1,1}| = \frac{3!}{1^3\cdot 3!} = 1,\\ |\mathrm{Cgnt}_{1,2}| = \frac{3!}{1^1\cdot 2^1\cdot 1!\cdot 1!} = 3,\\ |\mathrm{Cgnt}_{1}| = \frac{3!}{3^1\cdot 1!} = 2.\end{gathered}$$

Для непустых множеств A и B будем обозначать B^A множество отображений A в B. Пусть G — группа и $|G| = n$. Каждому элементу $g \in G$ поставим в соответствие отображение $\psi_g : G \longrightarrow G$, $a \longmapsto ga$, которое естественно называть левым сдвигом группы G на элемент g. Легко проверить, что отображение ψ_g взаимно однозначно и отображение $\varphi : G \longrightarrow \operatorname{Symm} G$, $g \longmapsto \psi_g$ является вложением (инъективным гомоморфизмом) группы G в группу $\operatorname{Symm} G$. Так как $\operatorname{Symm} G \simeq \mathbf{S}_n$, то φ можно считать вложением группы G в группу $\mathbf{S}_n$. Таким образом, каждая группа порядка n с точностью до изоморфизма является подгруппой симметрической группы $\mathbf{S}_n$ и, следовательно, элементы группы G можно представить подстановками.

Пусть $k \in \mathbb{N}$. k-ой степенью подстановки $\sigma \in \mathbf{S}_n$ называют подстановку $\sigma^k = \underbrace{\sigma\ldots\sigma}_{k}$. Порядком подстановки σ называется ее наименьшая степень $\operatorname{ord}\sigma$, совпадающая с тождественной подстановкой, то есть $\operatorname{ord}\sigma = \min\{k \in \mathbb{N} \mid \sigma^k = \mathrm{id}\}$. Если подстановка σ раскладывается в произведение s независимых циклов, длины которых равны соответственно $l_1,\ldots,l_s$, то $\operatorname{ord}\sigma = \mathrm{НОК}(l_1,\ldots,l_s)$.

Конечная группа может быть задана генетическим кодом, то есть указанием ее порождающих элементов и определяющих соотношений

между ними. Рассмотрим, например, группу

$$G = \langle s, t \mid s^8 = t^2 = e,\, ts = s^5 t \rangle$$

порядка 16. Она состоит из элементов e, s, s^2, s^3, s^4, s^5, s^6, s^7, t, st, s^2t, s^3t, s^4t, s^5t, s^6t и s^7t и не является абелевой группой, поскольку

$$\begin{aligned} s^3 \cdot t &= s^3 t, \\ t \cdot s^3 &= s^5 t s^2 s^2 t s = s^7 t \neq s^3 t. \end{aligned}$$

Занумеровав все элементы группы G числами от 1 до 16 в том порядке, в котором они перечислены выше, получаем следующую таблицу Кэли для группы G:

	e	s	s^2	s^3	s^4	s^5	s^6	s^7	t	st	s^2t	s^3t	s^4t	s^5t	s^6t	s^7t
e	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
s	2	3	4	5	6	7	8	1	10	11	12	13	14	15	16	9
s^2	3	4	5	6	7	8	1	2	11	12	13	14	15	16	9	10
s^3	4	5	6	7	8	1	2	3	12	13	14	15	16	9	10	11
s^4	5	6	7	8	1	2	3	4	13	14	15	16	9	10	11	12
s^5	6	7	8	1	2	3	4	5	14	15	16	9	10	11	12	13
s^6	7	8	1	2	3	4	5	6	15	16	9	10	11	12	13	14
s^7	8	1	2	3	4	5	6	7	16	9	10	11	12	13	14	15
t	9	14	11	16	13	10	15	12	1	6	3	8	5	2	7	4
st	10	15	12	9	14	11	16	13	2	7	4	1	6	3	8	5
s^2t	11	16	13	10	15	12	9	14	3	8	5	2	7	4	1	6
s^3t	12	9	14	11	16	13	10	15	4	1	6	3	8	5	2	7
s^4t	13	10	15	12	9	14	11	16	5	2	7	4	1	6	3	8
s^5t	14	11	16	13	10	15	12	9	6	3	8	5	2	7	4	1
s^6t	15	12	9	14	11	16	13	10	7	4	1	6	3	8	5	2
s^7t	16	13	10	15	12	9	14	11	8	5	2	7	4	1	6	3

Так как, например, при отображении ψ_{s^4t} имеем

$$\begin{gathered} e \longmapsto s^4t \longmapsto e, \quad s \longmapsto st \longmapsto s, \quad s^2 \longmapsto s^6t \longmapsto s^2, \\ s^3 \longmapsto s^3t \longmapsto s^3, \quad s^4 \longmapsto t \longmapsto s^4, \quad s^5 \longmapsto s^5t \longmapsto s^5, \\ s^6 \longmapsto s^2t \longmapsto s^6, \quad s^7 \longmapsto s^7t \longmapsto s^7, \end{gathered}$$

то при вложении $\varphi : \; G \longrightarrow \mathbf{S}_{16}, \; g \longmapsto \psi_g$ имеем

$$s^4t \;\longmapsto\; (1\ 13)(2\ 10)(3\ 15)(4\ 12)(5\,9)(6\ 14)(7\ 11)(8\ 16).$$

Точно так же получаем, что

$$s \;\longmapsto\; (1\,2\,3\,4\,5\,6\,7\,8)(9\ 10\ 11\ 12\ 13\ 14\ 15\ 16)$$

и т. д. При этом $\operatorname{pow} s^4t = (2,2,2,2,2,2,2,2)$ и $\operatorname{pow} s = (8,8)$, $\operatorname{ord} s^4t = 2$ и $\operatorname{ord} s = 8$.

Ниже приведен код программы, находящей образ группы G при вложении в группу $\mathbf{S}_{16}$ по правилу $g \longmapsto \psi_g$ и вычисляющей для каждой подстановки ψ_g порядок и показатель.

```
   program cycles;
   var i,j,s,t,m,p,q,k: integer;
      u,v,mas: array[1..16] of integer;
   const g: array[1..16,1..16] of integer =
   ((1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16),
   (2,3,4,5,6,7,8,1,10,11,12,13,14,15,16,9),
   (3,4,5,6,7,8,1,2,11,12,13,14,15,16,9,10),
   (4,5,6,7,8,1,2,3,12,13,14,15,16,9,10,11),
   (5,6,7,8,1,2,3,4,13,14,15,16,9,10,11,12),
   (6,7,8,1,2,3,4,5,14,15,16,9,10,11,12,13),
   (7,8,1,2,3,4,5,6,15,16,9,10,11,12,13,14),
   (8,1,2,3,4,5,6,7,16,9,10,11,12,13,14,15),
   (9,14,11,16,13,10,15,12,1,6,3,8,5,2,7,4),
   (10,15,12,9,14,11,16,13,2,7,4,1,6,3,8,5),
   (11,16,13,10,15,12,9,14,3,8,5,2,7,4,1,6),
   (12,9,14,11,16,13,10,15,4,1,6,3,8,5,2,7),
   (13,10,15,12,9,14,11,16,5,2,7,4,1,6,3,8),
   (14,11,16,13,10,15,12,9,6,3,8,5,2,7,4,1),
   (15,12,9,14,11,16,13,10,7,4,1,6,3,8,5,2),
   (16,13,10,15,12,9,14,11,8,5,2,7,4,1,6,3));
   function gcd (x,y : integer) : integer;
   begin
        if x=0 then gcd:=y else gcd:=gcd(y mod x,x)
   end;
   BEGIN
   k:=0;
   for i:=1 to 16 do
   begin
        writeln();
        writeln('Permutation ',i,': ');
        write('('); s:=1; k:=0;
        for j:=1 to 16 do
        begin
             mas[j]:=0; u[j]:=0; v[j]:=0
        end;
        j:=1; p:=0; q:=1
        repeat
             if mas[s]=0
                 then begin
                        if q=1 then q:=2 else write(' '); write(s);
mas[s]:=1;
                        s:=g[i,s]; p:=p+1
                    end
```

```
                else begin
                        write(')('); m:=1; t:=0;
                        repeat
                            if mas[m]=0 then
                            begin
                                s:=m; mas[s]:=1; if q=1 then q:=2 else
write(' '); write(s); t:=t+1;
                                u[p]:=1; k:=k+1; v[k]:=p; p:=1
                            end;
                            m:=m+1;
                            s:=g[i,s]
                        until t=1;
                   end;
                j:=j+1
        until j=17;
        write(') '); writeln('');
        for j:=1 to k do v[k+1]:=v[k+1]+v[j];
        v[k+1]:=16-v[k+1]; p:=v[1]; s:=v[1];
        for j:=2 to k+1 do
        begin
            p:=gcd(p,v[j]); s:=(s*v[j]) div p;
        end;
        write('order = ',s); writeln(''); write('power is ('); m:=1;
        repeat
            t:=1;
            for j:=1 to k do if v[t]<v[j+1] then t:=j+1;
            begin
                if m>1 then write(',');
                write(v[t]); if m=1 then m:=2
            end;
            v[t]:=0; s:=0;
            for j:=1 to k+1 do s:=s+v[j]
        until s=0;
        write(')')
    end
    END.
```

Вот какие результаты выводит на экран программа:

```
Permutation 1:
(1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)(13)(14)(15)(16)
order = 1
power is (1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1)
Permutation 2:
(1 2 3 4 5 6 7 8)(9 10 11 12 13 14 15 16)
order = 8
power is (8,8)
Permutation 3:
(1 3 5 7)(2 4 6 8)(9 11 13 15)(10 12 14 16)
order = 4
```

```
power is (4,4,4,4)
Permutation 4:
(1 4 7 2 5 8 3 6)(9 12 15 10 13 16 11 14)
order = 8
power is (8,8)
Permutation 5:
(15)(2 6)(3 7)(4 8)(9 13)(10 14)(11 15)(12 16)
order = 2
power is (2,2,2,2,2,2,2,2)
Permutation 6:
(1 6 3 8 5 2 7 4)(9 14 11 16 13 10 15 12)
order = 8
power is (8,8)
Permutation 7:
(1 7 5 3)(2 8 6 4)(9 15 13 11)(10 16 14 12)
order = 4
power is (4,4,4,4)
Permutation 8:
(1 8 7 6 5 4 3 2 )(9 16 15 14 13 12 11 10)
order = 8
power is (8,8)
Permutation 9:
(1 9)(2 14)(3 11)(4 16)(5 13)(6 10)(7 15)(8 12)
order = 2
power is (2,2,2,2,2,2,2,2)
Permutation 10:
(1 10 7 16 5 14 3 12)(2 15 8 13 6 11 4 9)
order = 8
power is (8,8)
Permutation 11:
(1 11 5 15 )(2 16 6 12 )(3 13 7 9 )(4 10 8 14 )
order = 4
power is (4,4,4,4)
Permutation 12:
(1 12 3 14 5 16 7 10)(2 9 4 11 6 13 8 15)
order = 8
power is (8,8)
Permutation 13:
(1 13)(2 10)(3 15)(4 12)(5 9)(6 14)(7 11)(8 16)
order = 2
power is (2,2,2,2,2,2,2,2)
Permutation 14:
(1 14 7 12 5 10 3 16)(2 11 8 9 6 15 4 13)
order = 8
power is (8,8)
Permutation 15:
(1 15 5 11)(2 12 6 16)(3 9 7 13)(4 14 8 10)
order = 4
power is (4,4,4,4)
Permutation 16:
```

```
(1 16 3 10 5 12 7 14)(2 13 4 15 6 9 8 11)
order = 8
power is (8,8)
```

Упражнение 8. Составьте программу, выводящую для группы G на экран не подстановки ψ_g, как было сделано в рассмотренной задаче, а матрицы $m(\psi_g)$ (см. Введение).

5. Вычисление подгрупп и выделение нормальных делителей конечной группы

Напомним, что подмножество H группы G называется подгруппой, если для любых элементов $a, b \in H$ выполняется включение

$$ab^{-1} \in H \tag{3}$$

(мы используем мультипликативные обозначения). Легко проверить, что для всякого $g \in G$ отображение

$$\varphi_g : \ G \longrightarrow G, \ a \longmapsto g^{-1}ag$$

является автоморфизмом группы G — его называют внутренним автоморфизмом. Подгруппу H называют нормальным делителем, если для всякого внутреннего автоморфизма φ_g выполняется включение $\varphi_g(H) \subset H$. Так как отображение φ_g взаимно однозначно, то это приводит к равенствам $\varphi_g(H) = H$. В абелевой группе G для всякого $g \in G$ выполняется равенство $\varphi_g = \mathrm{id}$, поэтому всякая подгруппа в G является нормальным делителем.

Задать группу — означает ввести групповую операцию на некотором множестве. Рассмотрим пример. Пусть ABC — правильный треугольник на плоскости Π и точка O — его центр. Рассмотрим следующие преобразования плоскости Π: тождественное преобразование id, повороты r_{120} и r_{240} по часовой стрелке относительно точки O на углы 120 и 240 градусов, симметрии s_1, s_2 и s_3 относительно прямых, содержащих высоты треугольника ABC, выходящие соответственно из вершин A, B и C. Множество $\mathbf{D}_3$, состоящее из этих шести преобразований, является группой (ее называют диэдральной группой) относительно композиции преобразований — точнее, подгруппой в $\mathrm{Symm}\,\Pi$. Групповая операция в $\mathbf{D}_3$ наглядно представляется таблицей Кэли:

	id	r_{120}	r_{240}	s_1	s_2	s_3
id	id	r_{120}	r_{240}	s_1	s_2	s_3
r_{120}	r_{120}	r_{240}	id	s_3	s_1	s_2
r_{240}	r_{240}	id	r_{120}	s_2	s_3	s_1
s_1	s_1	s_2	s_3	id	r_{120}	r_{240}
s_2	s_2	s_3	s_1	r_{240}	id	r_{120}
s_3	s_3	s_1	s_2	r_{120}	r_{240}	id

Занумеровав элементы $\mathrm{id}, r_{120}, r_{240}, s_1, s_2, s_3$ соотвественно числами $1, 2, 3, 4, 5, 6$, перепишем таблицу Кэли в виде массива:

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	6	4	5
3	3	1	2	5	6	4
4	4	5	6	1	2	3
5	5	6	4	3	1	2
3	3	4	5	2	3	1

Этот массив используется для описания группы $\mathbf{D}_3$ в приведенной ниже программе, которая вычисляет все подгруппы и нормальные делители в $\mathbf{D}_3$. Программа должна проверить достаточное условие (3) для всех непустых подмножеств группы $\mathbf{D}_3$. Но каждое такое подмножество можно реализовать в виде не равного нулю двоичного числа $\nu = \overline{c_1c_2c_3c_4c_5c_6}$, где

$$c_1 = \chi(\mathrm{id}),\ c_2 = \chi(r_{120}),\ c_3 = \chi(r_{240}),$$
$$c_4 = \chi(s_A),\ c_5 = \chi(s_B),\ c_6 = \chi(s_C)$$

и χ — характеристическая функция (индикатор) на группе $\mathbf{D}_3$. Поскольку для всякой подгруппы H в $\mathbf{D}_3$ должно выполняться включение $\mathrm{id} \in H$, программе достаточно работать с числами ν, в которых $c_1 = 1$.

Программа работает следующим образом:

а) создается массив `inv` из шести ячеек, в котором в i-ую ячейку записывается номер элемента группы $\mathbf{D}_3$, обратного ее i-ому элементу;

б) для каждого непустого подмножества группы, содержащего нейтральный элемент, проверяется условие (3) — если оно выполнено, то на экран выводится обнаруженная подгруппа H;

в) если для подгруппы H выполняется включения $\varphi_g(H) \subset H$ для всех $g \in \mathbf{D}_n$, программа отмечает, что H — нормальный делитель.

```
program subgroups;
var i,j,k,p,q,csg,w,u,sg: integer;
s,m, inv: array[1..6] of integer;
const g: array[1..6,1..6] of integer = ((1,2,3,4,5,6), (2,3,1,6,4,5),
(3,1,2,5,6,4), (4,5,6,1,2,3), (5,6,4,3,1,2), (6,4,5,2,3,1));
sy: array[1..6] of string =
('id','r120','r240','s1','s2','s3');
BEGIN
p:=1; csg:=0; s[1]:=1;
for i:=1 to 6 do
begin
     j:=1;
     while g[i,j]<>1 do j:=j+1;
     inv[i]:=j
end;
for i:=1 to 5 do p:=p*2;
for i:=0 to p-1 do
```

```
begin
     q:=i; s[1]:=1;
     for j:=1 to 4 do
     begin
          s[j+1]:=q-((q div 2)*2);
          q:=q div 2;
     end;
     s[6]:=q;
     q:=0;
     for j:=1 to 6 do q:=q+s[j];
     if (6 mod q)=0 then
     begin
          j:=1;
          for p:=1 to 6 do
          for q:=1 to 6 do
             if s[p]=1 then if s[q]=1
               then if s[g[p,inv[q]]]=0 then j:=0;
          if j=1 then
          begin
              csg:=csg+1; k:=1;
              for p:=2 to 6 do
              for q:=2 to 6 do if s[q]=1 then
                if s[g[g[inv[p],q],p]]=0 then k:=0;
              writeln('');
              write('subgroup ',csg,': ');
              for j:=1 to 6 do if s[j]>0 then
              begin
                   if j>1 then write(',');
                   write(sy[j])
             end;
              write('');
              if k=1 then write(' - normal')
          end
     end
end
END.
```

Вот результаты, которые программа выводит на экран:

```
subgroup 1: {id,} - normal
subgroup 2: {id,r120,r240,} - normal
subgroup 3: {id,s1,}
subgroup 4: {id,s2,}
subgroup 5: {id,s3}
subgroup 6: {id,r120,r240,s1,s2,s3} - normal
```

Упражнение 9. Группу G называют T-группой, если «отношение

нормальности на G транзитивно», то есть для любых подгрупп H_1 и H_2, таких, что H_1 является нормальным делителем в H_2, а H_2 нормальным делителем в G, подгруппа H_1 нормальна в G.

Составьте программу, проверяющую, является ли заданная группа T-группой.

6. Вычисление централизаторов и нормализаторов подгрупп конечных неабелевых групп

Централизатором подмножества S группы G называют подмножество $\operatorname{Cnt} S$ таких элементов в G, которые коммутируют с любым элементом из S, то есть

$$\operatorname{Cnt} S = \{g \mid ag = ga,\ a \in S\}.$$

Централизатор самой группы называют ее центром. Если $g, \hat{g} \in \operatorname{Cnt} G$ и $a \in G$, то

$$(g\hat{g}^{-1})a = g(\hat{g}^{-1}a) = g(a^{-1}\hat{g})^{-1} = (a^{-1}\hat{g})^{-1}g = \\ = (\hat{g}a^{-1})^{-1}g = (a\hat{g}^{-1})g = a(\hat{g}^{-1}g) = a(g\hat{g}^{-1}),$$

то есть $g\hat{g}^{-1} \in \operatorname{Cnt} G$ и, следовательно, $\operatorname{Cnt} G$ является подгруппой в G. Более того, если $h \in \operatorname{Cnt} G$, то для любого внутреннего автоморфизма φ_g группы G и любого $a \in G$ получаем

$$\varphi_g(h)a = (g^{-1}hg) = ha,$$
$$a\varphi_g(h) = a(g^{-1}hg) = ah = ha.$$

Это означает, что $\operatorname{Cnt} G$ является нормальным делителем.

Понятно, что в абелевой группе G для любого подмножества $S \subset G$ выполняется равенство $\operatorname{Cnt} S = G$, то есть централизаторы являются «мерой абелевости» группы.

Нормализатором подмножества S группы G назовем подмножество

$$\operatorname{Nm} S = \{g \in G \mid \varphi_g(S) = S\}.$$

Так как для любых $g, \hat{g} \in \operatorname{Nm} S$

$$\varphi_{g\hat{g}}(S) = (g\hat{g})^{-1}S(g\hat{g}) = (\hat{g}^{-1}g^{-1})S(g\hat{g}) = \hat{g}^{-1}(g^{-1}Sg)\hat{g} = \hat{g}^{-1}S\hat{g} = S,$$

то $\varphi_{g\hat{g}} \in \operatorname{Nm} S$. Умножив обе части равенства $g^{-1}Sg = S$ слева на g и справа на g^{-1}, получим $S = gSg^{-1}$, то есть $S = \varphi_{g^{-1}}$, что означает $g^{-1} \in \operatorname{Nm} S$. Таким образом, $\operatorname{Nm} S$ является подгруппой в G.

Из определения получается, что подгруппа H в G в том и только том случае является нормальным делителем, если $\operatorname{Nm} H = G$. Таким образом, $\operatorname{Nm} S$ является «мерой «нормальности» подгруппы H.

Приведем пример программы, которая вычисляет нормализаторы и централизаторы подгрупп группы

$$W = \langle s, t \mid s^4 = t^5 = e,\ \varphi_s(t) = t^{-1} \rangle,$$

состоящей из 20 элементов.

```
program normcent;
var i,j,k,l,p,q,r,csg: integer;
   s,v,w,inv: array[1..20] of integer;
const g: array[1..12,1..12] of integer =
((1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20),
(2,3,4,1,9,10,11,12,13,14,15,16,17,18,19,20,5,6,7,8),
(3,4,1,2,13,14,15,16,17,18,19,20,5,6,7,8,9,10,11,12),
(4,1,2,3,17,18,19,20,5,6,7,8,9,10,11,12,13,14,15,16),
(5,12,13,20,6,7,8,1,2,9,10,11,14,15,16,3,4,17,18,19),
(6,11,14,19,7,8,1,5,12,2,9,10,15,16,3,13,20,4,17,18),
(7,10,15,18,8,1,5,6,11,12,2,9,16,3,13,14,19,20,4,17),
(8,9,16,17,1,5,6,7,10,11,12,2,3,13,14,15,18,19,20,4),
(9,16,17,8,10,11,12,2,3,13,14,15,18,19,20,4,1,5,6,7),
(10,15,18,7,11,12,2,9,16,3,13,14,19,20,4,17,8,1,5,6),
(11,14,19,6,12,2,9,10,15,16,3,13,20,4,17,18,7,8,1,5),
(12,13,20,5,2,9,10,11,14,15,16,3,4,17,18,19,6,7,8,1),
(13,20,5,12,14,15,16,3,4,17,18,19,6,7,8,1,2,9,10,11),
(14,19,6,11,15,16,3,13,20,4,17,18,7,8,1,5,12,2,9,10),
(15,18,7,10,16,3,13,14,19,20,4,17,8,1,5,6,11,12,2,9),
(16,17,8,9,3,13,14,15,18,19,20,4,1,5,6,7,10,11,12,2),
(17,8,9,16,18,19,20,4,1,5,6,7,10,11,12,2,3,13,14,15),
(18,7,10,15,19,20,4,17,8,1,5,6,11,12,2,9,16,3,13,14),
(19,6,11,14,20,4,17,18,7,8,1,5,12,2,9,10,15,16,3,13),
(20,5,12,13,4,17,18,19,6,7,8,1,2,9,10,11,14,15,16,3));
sy: array[1..20] of string =
('e','s','s2','s3','t','t2','t3','t4','st','st2','st3','st4',
's2t','s2t2','s2t3','s2t4','s3t','s3t2','s3t3','s3t4');
BEGIN
for i:=1 to 20 do
begin
     j:=1; while g[i,j]<>1 do j:=j+1; inv[i]:=j
end;
p:=1; csg:=0; s[1]:=1;
for i:=1 to 19 do p:=p*2;
for i:=0 to p-1 do
begin
     q:=i; s[1]:=1;
     for j:=1 to 18 do
     begin
          s[j+1]:=q-((q div 2)*2);
          q:=q div 2;
     end;
```

```
        s[20]:=q; q:=0;
        for j:=1 to 20 do q:=q+s[j];
        if (20 mod q)=0 then
                begin
                    j:=1;
                    for p:=1 to 20 do
                    for q:=1 to 20 do
                      if s[p]=1 then if s[q]=1
                       then if s[g[p,inv[q]]]=0 then j:=0;
                    if j=1 then
                      begin
                          csg:=csg+1; writeln('');
                          write('subgroup ',csg,': ');
                          for j:=1 to 20 do if s[j]>0 then
                              begin
                                  if j>1 then write(','); write(sy[j])
                              end;
                          write('');
                          for k:=1 to 20 do
                          begin
                              v[k]:=1; w[k]:=1
                          end;
                          for p:=2 to 20 do
                          begin
                              for q:=2 to 20 do
                              if s[q]=1 then
                              begin
                                  if s[g[g[inv[p],q],p]]=0 then v[p]:=0;
                                  if g[p,q]<>g[q,p] then w[p]:=0
                              end;
                          end;
                          writeln('');
                          write('Normalizer: e');
                          for k:=2 to 20 do if v[k]=1 then
write(',',sy[k]);
                          write(''); writeln('');
                          write('Centralizer: e');
                          for k:=2 to 20 do if w[k]=1 then
write(',',sy[k]);
                          write('');
                      end
                end
    end
    END.
```

Программа выводит на экран следующие результаты:

```
subgroup 1: e
Normalizer:
e,s,s2,s3,t,t2,t3,t4,st,st2,st3,st4,s2t,s2t2,s2t3,s2t4,s3t,s3t2,s3t3,s3t4
```

```
Centralizer:
e,s,s2,s3,t,t2,t3,t4,st,st2,st3,st4,s2t,s2t2,s2t3,s2t4,s3t,s3t2,s3t3,s3t4
subgroup 2: e,s2
Normalizer:
e,s,s2,s3,t,t2,t3,t4,st,st2,st3,st4,s2t,s2t2,s2t3,s2t4,s3t,s3t2,s3t3,s3t4
Centralizer:
e,s,s2,s3,t,t2,t3,t4,st,st2,st3,st4,s2t,s2t2,s2t3,s2t4,s3t,s3t2,s3t3,s3t4
subgroup 3: e,s,s2,s3
Normalizer:
e,s,s2,s3
Centralizer:
e,s,s2,s3
subgroup 4: e,t,t2,t3,t4
Normalizer:
e,s,s2,s3,t,t2,t3,t4,st,st2,st3,st4,s2t,s2t2,s2t3,s2t4,s3t,s3t2,s3t3,s3t4
Centralizer:
e,s2,t,t2,t3,t4,s2t,s2t2,s2t3,s2t4
subgroup 5: e,s2,t,t2,t3,t4,s2t,s2t2,s2t3,s2t4
Normalizer:
e,s,s2,s3,t,t2,t3,t4,st,st2,st3,st4,s2t,s2t2,s2t3,s2t4,s3t,s3t2,s3t3,s3t4
Centralizer:
e,s2,t,t2,t3,t4,s2t,s2t2,s2t3,s2t4
subgroup 6: e,s2,st,s3t
Normalizer:
e,s2,st,s3t
Centralizer:
e,s2,st,s3t
subgroup 7: e,s2,st2,s3t2
Normalizer:
e,s2,st2,s3t2
Centralizer:
e,s2,st2,s3t2
subgroup 8: e,s2,st3,s3t3
Normalizer:
e,s2,st3,s3t3
Centralizer:
e,s2,st3,s3t3
subgroup 9: e,s2,st4,s3t4
Normalizer:
e,s2,st4,s3t4
Centralizer:
e,s2,st4,s3t4
subgroup 10: e,s,s2,s3,t,t2,t3,t4,st,st2,st3,st4,s2t,s2t2,s2t3,s2t4,s3t,
s3t2,s3t3,s3t4
Normalizer:
e,s,s2,s3,t,t2,t3,t4,st,st2,st3,st4,s2t,s2t2,s2t3,s2t4,s3t,s3t2,s3t3,s3t4
Centralizer:
e,s2
```

Эти результаты можно представить таблицей

H	$\mathrm{Nm}\, H$	$\mathrm{Cnt}\, H$	H	$\mathrm{Nm}\, H$	$\mathrm{Cnt}\, H$
$\{e\}$	W	W	$\langle st \rangle$	$\langle st \rangle$	$\langle st \rangle$
$\langle s^2 \rangle$	W	W	$\langle st^2 \rangle$	$\langle st^2 \rangle$	$\langle st^2 \rangle$
$\langle s \rangle$	$\langle s \rangle$	$\langle s \rangle$	$\langle st^3 \rangle$	$\langle st^3 \rangle$	$\langle st^3 \rangle$
$\langle t \rangle$	W	$\langle s^2, t \rangle$	$\langle st^4 \rangle$	$\langle st^4 \rangle$	$\langle st^4 \rangle$
$\langle s^2, t \rangle$	W	$\langle s^2, t \rangle$	W	W	$\langle s^2 \rangle$

7. Представление подстановки в виде композиции транспозиций

Рассмотрим подстановку $\tau \in \mathbf{S}_n$, удовлетворяющую условию: существуют такие числа $p, q \in \{1, \ldots, n\}$, что

$$\tau(x) = \begin{cases} x, & \text{если } x \notin \{p, q\}, \\ p, & \text{если } x = q. \end{cases}$$

Ясно, что $\tau(p) = q$. Подстановка τ называется транспозицией. Без потери общности можно считать, что $p < q$. Тогда τ имеет вид:

$$\tau = (p\,q)(1)\ldots(p-1)(p+1)\ldots(q-1)(q+1)\ldots(n).$$

Транспозицию, по договоренности, записывают проще: $\tau = (p\,q)$, то есть опускают циклы длины 1. Ясно, что $\tau^2 = \mathrm{id}$.

Покажем, что любая подстановка $\sigma \in \mathbf{S}_n$ может быть представлена в виде композиции транспозиций. Введем обозначение: $\sigma_0 = \sigma$. В случае $\sigma_0(1) \neq 1$ определим транспозицию $\tau_1 = (1\,\sigma_0(1))$ и подстановку

$$\sigma_1 = \begin{cases} \sigma_0, & \text{если } \sigma_0(1) = 1, \\ \tau_1\sigma_0, & \text{если } \sigma_0(1) \neq 1. \end{cases}$$

Если $\sigma_1(2) \neq 2$, то определим транспозицию $\tau_2 = (2\,\sigma_1(2))$ и подстановку

$$\sigma_2 = \begin{cases} \sigma_1, & \text{если } \sigma_1(2) = 2, \\ \tau_2\sigma_1, & \text{если } \sigma_1(2) \neq 2. \end{cases}$$

И т. д.

После нескольких таких шагов получим $\sigma_k = \mathrm{id}$, то есть существуют транспозиции $\tau_1, \ldots, \tau_k$, такие, что $\tau_k(\tau_{k-1}(\ldots(\tau_1\sigma)\ldots) = \mathrm{id}$. Поскольку композиция подстановок является ассоциативной операцией, мы можем переписать полученный результат в виде: $\tau_k \ldots \tau_1\sigma = \mathrm{id}$. Тогда

$$\tau_k(\tau_k \ldots \tau_1\sigma) = \mathrm{id},$$
$$(\tau_k\tau_k)(\tau_{k-1} \ldots \tau_1\sigma) = \tau_k\,\mathrm{id},$$

$$\mathrm{id}(\tau_{k-1}\dots\tau_1\sigma) = \tau_k,$$
$$(\tau_{k-1}\dots\tau_1\sigma) = \tau_k,$$
$$\dots$$
$$\sigma = \tau_1\dots\tau_k.$$

В качестве примера рассмотрим подстановку $\sigma = (2\,6\,5)(7\,1\,4) \in \mathbf{S}_7$. Так как $\sigma(1) = 4$, то $\tau_1 = (1\,4)$ и $\sigma_1 = \tau_1\sigma = (1)(2\,6\,5)(7\,4)$. Далее, поскольку $\sigma_1(2) = 6$, то $\tau_2 = (2\,6)$ и $\sigma_2 = \tau_2\sigma_1 = (1)(2)(7\,4)(5\,6)$. Ввиду того, что $\sigma_2(3) = 3$, полагаем $\sigma_3 = \sigma(2)$. Снова поскольку $\sigma_3(4) = 7$, то $\tau_3 = (4\,7)$ и $\sigma_4 = \tau_3\sigma_3 = (1)(2)(3)(4)(5\,6)(7)$. Полагаем, наконец, что $\tau_4 = (5\,6)$. Тогда $\tau_4\tau_3\tau_2\tau_1\sigma = \mathrm{id}$, таким образом,

$$\sigma = (1\,4)(2\,6)(4\,7)(5\,6).$$

Пусть $\sigma \in \mathbf{S}_n$ где , $n \geqslant 2, i, j \in \{1,\dots,n\}$ и $i < j$. Будем говорить, что σ содержит (i,j)-инверсию, если $\sigma(i) > \sigma(j)$. Число инверсий, которые содержит подстановка σ, назовем четностью и обозначим $\Pi(\sigma)$. Число $\operatorname{sign}\sigma := (-1)^{\Pi(\sigma)}$ называют знаком подстановки σ. Так, тождественная подстановка не содержит инверсий, поэтому $\Pi(\mathrm{id}) = 0$ и $\operatorname{sign}\mathrm{id} = 1$, а подстановка

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 7 & 3 & 5 & 2 & 1 & 9 & 8 \end{pmatrix}$$

содержит $(1,4)$-, $(1,6)$-, $(1,7)$-, $(2,4)$-, $(2,6)$-, $(2,7)$-, $(3,4)$-, $(3,5)$-, $(3,6)$-$(3,7)$-, $(4,6)$-, $(4,7)$-, $(5,6)$-, $(5,7)$-, $(6,7)$- и $(8,9)$-инверсии и никаких других инверсий не содержит, поэтому $\Pi(\gamma) = 16$ и, как и для тождественной подстановки, $\operatorname{sign}\gamma = 1$.

Можно показать, что транспозиция является нечетной подстановкой и, более того, если равенство $\sigma = \tau_1\dots\tau_s$ является представлением подстановки σ в виде композиции транспозиций, то $\operatorname{sign}\sigma = (-1)^s$.

Приведем код программы, которая записывает все, кроме тождественной, подстановки ψ_g, получающиеся при вложении группы $\mathbf{D}_3$ в группу $\mathbf{S}_6$ по правилу $g \mapsto \psi_g$, в виде композиции транспозиций и вычисляет четность этих подстановок.

```
program transpositions;
var i,j,k: integer;
   p: array[1..6] of integer;
const g: array[1..6,1..6] of integer = ((1,2,3,4,5,6), (2,3,1,6,4,5),
(3,1,2,5,6,4), (4,5,6,1,2,3), (5,6,4,3,1,2), (6,4,5,2,3,1));
BEGIN
for i:=2 to 6 do
```

```
begin
     j:=0; writeln('');
     write('PERMUTATION ',i);
     writeln('');
     begin
          for k:=1 to 6 do p[k]:=g[i,k];
          for k:=1 to 6 do if p[k]<>k then
               begin
                    write('(',k,' ',p[k],')'); p[p[k]]:=p[k]; j:=j+1;
          end
     end;
     writeln(''); write('parity = ',j);
end
END.
```

Программа выводит на экран следующие результаты:

```
PERMUTATION 2
(1 2)(3 1)(4 6)(5 4)
parity = 4
PERMUTATION 3
(1 3)(2 1)(4 5)(6 4)
parity = 4
PERMUTATION 4
(1 4)(2 5)(3 6)
parity = 3
PERMUTATION 5
(1 5)(2 6)(3 4)
parity = 3
PERMUTATION 6
(1 6)(2 4)(3 5)
parity = 3
```

Упражнение 10. Составьте программу, представляющую подстановки в виде композиции транспозиций специального вида — например, вида $(1\,j)$.

Упражнение 11. Составьте программу, которая представляет подстановки в виде композиции транспозиций $(1\,2)$ и подстановок $(1\,2\,\ldots\,n)$.

Упражнение 12. Составьте программу, которая представляет подстановки в виде композиции транспозиций $(1\,2)$, $(2\,3)$, $\ldots$, $(n-1\;\,n)$.

Упражнение 13. Составьте программу, которая представляет подстановки в виде композиции циклов длины 3.

Упражнение 14. Составьте программу, которая представляет подстановки в виде композиции циклов $(1\,2\,3)$, $(1\,2\,4), \ldots, (1\,2\,n)$.

8. Вычисление групп гомоморфизмов конечных групп

Обозначим $\mathrm{Hom}(G,H)$ множество гомоморфизмов группы G в абелеву группу H. Поставим гомоморфизмам $\varphi,\psi\in\mathrm{Hom}(G,H)$ в соответствие отображение

$$\varphi\star\psi:\ G\longrightarrow H,\ a\longmapsto\varphi(a)\psi(a).$$

Равенства $(\varphi\star\psi)(ab)=\varphi(ab)\psi(ab)$ и

$$(\varphi\star\psi)(a)\cdot(\varphi\star\psi)(b)=\varphi(a)\psi(a)\varphi(b)\psi(b)=\\ =\varphi(a)\varphi(b)\psi(a)\psi(b)=\varphi(ab)\psi(ab)$$

показывают, что $\varphi\star\psi\in\mathrm{Hom}(G,H)$, то есть $\star$ является бинарной операцией на множестве $\mathrm{Hom}(G,H)$. Из равенств

$$[(\varphi\star\psi)\star\theta](a)=(\varphi\star\psi)(a)\theta(a)=(\varphi(a)\psi(a))\theta(a),\\ [\varphi\star(\psi\star\theta)](a)=\varphi(a)(\psi\star\theta(a))=\varphi(a)(\psi(a)\theta(a))=(\varphi(a)\psi(a))\theta(a)$$

заключаем, что операция $\star$ ассоциативна.

Обозначим e_H нейтральный элемент группы H и рассмотрим отображение $\varepsilon:\ G\longrightarrow H,\ a\longmapsto e_H$. Так как $\varepsilon(ab)=e_H=e_He_H=\varepsilon(a)\varepsilon(b)$, то $\varepsilon\in\mathrm{Hom}(G,H)$ Для любого $a\in G$

$$(\varphi\star\varepsilon)(a)=\varphi(a)\varepsilon(a)=\varphi(a)e_H=\varphi(a),\\ (\varepsilon\star\varphi)(a)=\varepsilon(a)\varphi(a)=e_H\varphi(a)=\varphi(a),$$

поэтому $\varphi\star\varepsilon=\varepsilon\star\varphi=\varphi$, то есть гомоморфизм ε «играет нейтральную роль» относительно операции $\star$.

По отношению к гомоморфизму $\varphi\in\mathrm{Hom}(G,H)$ отображение $\hat\varphi(a)=[\varphi(a)]^{-1}$ «выполняет обратную роль»:

$$(\varphi\star\hat\varphi)(a)=\varphi(a)\hat\varphi(a)=\varphi(a)[\varphi(a)]^{-1}=e_H,\\ (\hat\varphi\star\varphi)(a)=\hat\varphi(a)\varphi(a)=[\varphi(a)]^{-1}\varphi(a)=e_H,$$

то есть $\varphi\star\hat\varphi=\hat\varphi\star\varphi=\varepsilon$. Кроме того,

$$\hat\varphi(ab)=[\varphi(ab)]^{-1}=[\varphi(a)\varphi(b)]^{-1}=[\varphi(b)]^{-1}[\varphi(a)]^{-1}=\\ =[\varphi(a)]^{-1}[\varphi(b)]^{-1}=\hat\varphi(a)\hat\varphi(b),$$

поэтому $\hat\varphi\in\mathrm{Hom}(G,H)$.

Таким образом, множество $\mathrm{Hom}(G, H)$ является группой относительно операции $\star$, причем, как видно, абелевой.

Рассмотрим пример. Кватернионом называют математический объект вида $h = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, где $a, b, c, d \in \mathbb{R}$ и $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ — значки. Множество кватернионов обозначают $\mathbb{H}$, а множество отличных от нуля кватернионов — символом $\mathbb{H}^*$. Кватернионы складываются и перемножаются так же, как складываются и перемножаются многочлены, но при умножении должны соблюдаться правила

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Легко проверить, что $\mathbb{H}^*$ является (неабелевой) группой относительно умножения, причем

$$h^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2}(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}),$$

а подмножество

$$Q = \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$$

в $\mathbb{H}^*$ является подгруппой.

В приведенной ниже программе, вычисляющей группу $\mathrm{Hom}(Q, \mathbb{Z}_4)$, массивы `g` и `h` описывают групповые операции в Q и $\mathbb{Z}_4$, выражая таблицы Кэли

	1	-1	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{i}$
1	1	2	3	4	5	6	7	8
-1	2	1	4	3	6	5	8	7
$\mathbf{i}$	3	4	2	1	7	8	6	5
$-\mathbf{i}$	4	3	1	2	8	7	5	6
$\mathbf{j}$	5	6	8	7	2	1	3	4
$-\mathbf{j}$	6	5	7	8	1	2	4	3
$\mathbf{k}$	7	8	5	6	4	3	2	1
$-\mathbf{k}$	8	7	6	5	3	4	1	2

и

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	1	2	3	4
$\overline{1}$	2	3	4	1
$\overline{2}$	3	4	1	2
$\overline{3}$	4	1	2	3

Массив `inv` служит для записи элементов, обратных элементам группы Q. Используя массив `d`, программа просматривает только такие из отображений $\varphi : Q \longrightarrow \mathbb{Z}_4$ (их существует 4^8), которые удовлетворяют необходимым условиям гомоморфизма $\varphi(1) = \overline{0}$ и $\varphi(a^{-1}) = -\varphi(a)$, и отби-

рают среди них те, которые удовлетворяют определению гомоморфизма.

```
   program homomorphisms;
   var i,j,k,m,t,v : integer;
      d,inv: array[1..8] of integer;
   const g: array[1..8,1..8] of integer = ((1,2,3,4,5,6,7,8),
(2,1,4,3,6,5,8,7), (3,4,2,1,7,8,6,5), (4,3,1,2,8,7,5,6),
   (5,6,8,7,2,1,3,4), (6,5,7,8,1,2,4,3), (7,8,5,6,4,3,2,1),
(8,7,6,5,3,4,1,2));
        h: array[1..4,1..4] of integer =
   ((1,2,3,4),(2,3,4,1),(3,4,1,2),(4,1,2,3));
   BEGIN
   inv[1]:=1; m:=1; d[1]:=1; v:=0;
   for i:=2 to 8 do
   begin
        j:=1;
        repeat j:=j+1 until g[i,j]=1;
        inv[i]:=j;
        m:=m*4
   end;
   for i:=1 to m-1 do
   begin
        m:=i; t:=1;
        for j:=2 to 8 do
        begin
            d[j]:=m mod 4; m:=m div 4;
        end;
        j:=1;
        repeat
             j:=j+1; if h[d[j],d[inv[j]]]<>1 then t:=0
        until ((t=0) or (j=8));
        if t=1 then
             begin
                 j:=1;
                 repeat
                      k:=1; j:=j+1;
                      repeat
                           k:=k+1;
                           if d[g[j,k]]<>h[d[j],d[k]] then t:=0
                      until ((t=0) or (k=8));
                 until ((t=0) or (j=8));
             end;
        if t=1 then
             begin
                 v:=v+1;
                 writeln();
                 write('homomorphism ',v,': 1');
                 for j:=2 to 8 do write('-',d[j])
             end
   end
```

```
END.
```

Программа выводит на экран результаты:

```
homomorphism 1: 1-1-1-1-1-1-1-1
homomorphism 2: 1-1-3-3-3-3-1-1
homomorphism 3: 1-1-3-3-1-1-3-3
homomorphism 4: 1-1-1-1-3-3-3-3
```

Эти результаты означают, что найдены 4 гомоморфизма $Q \longrightarrow \mathbb{Z}_4$:

i	$\varphi_i(1)$	$\varphi_i(-1)$	$\varphi_i(\mathbf{i})$	$\varphi_i(-\mathbf{i})$	$\varphi_i(\mathbf{j})$	$\varphi_i(-\mathbf{j})$	$\varphi_i(\mathbf{k})$	$\varphi_i(-\mathbf{k})$
1	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
2	$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{2}$	$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{0}$
3	$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{2}$
4	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{2}$	$\overline{2}$	$\overline{2}$

Таким образом, группа $\mathrm{Hom}(Q, \mathbb{Z}_4)$ состоит из четырех элементов. С точностью до изоморфизма существует две группы порядка 4 — это циклическая группа $\mathbb{Z}_4$ и группа $\mathbb{Z}_2^2$, являющаяся прямым произведением циклической группы $\mathbb{Z}_2$ на себя. Так как $\operatorname{ord} \varphi_i = 2$ для всех i, а в группе $\mathbb{Z}_4$ имеется элемент порядка 4 ($\operatorname{ord} \overline{1} = 4$), то $\mathrm{Hom}(Q, \mathbb{Z}_4) \simeq \mathbb{Z}_2^2$.

Упражнение 15. Пусть G и H — произвольные группы, $\mathfrak{H}$ — множество гомоморфизмов $G \longrightarrow H$. Легко показать, что $\bigcap\limits_{\varphi \in \mathfrak{H}} \operatorname{Im} \varphi$ является подгруппой в H (здесь $\operatorname{Im} \varphi$ обозначает образ гомоморфизма φ). Пару групп (G, H) назовем гомоморфно устойчивой, если $\bigcup\limits_{\varphi \in \mathfrak{H}} \operatorname{Im} \varphi$ есть подгруппа в H.

Составьте программу, проверяющую гомоморфную устойчивость пары заданных групп.

9. Вычисление групп автоморфизмов и внутренних автоморфизмов конечных групп

Обозначим $\operatorname{Aut} G$ множество автоморфизмов группы G. Если $\varphi, \psi \in \operatorname{Aut} G$, то существует отображение $\psi^{-1} \in \operatorname{Symm} G$ и для произвольных $a, b \in G$ найдутся такие $c, d \in G$, что $\psi(c) = a$ и $\psi(d) = b$. Поэтому

$$\varphi\psi^{-1}(ab) = \varphi(\psi^{-1}(ab)) = \varphi(\psi^{-1}(\psi(c)\psi(d)) = \varphi(\psi^{-1}(\psi(cd)) = \varphi(cd),$$
$$\varphi\psi^{-1}(a)\varphi\psi^{-1}(b) = \varphi(\psi^{-1}(\psi(c))\varphi(\psi^{-1}(\psi(d)) = \varphi(c)\varphi(d) = \varphi(cd).$$

Таким образом, $(\varphi\psi^{-1})(ab) = (\varphi\psi^{-1})(a)(\varphi\psi^{-1})(b)$, то есть $\varphi\psi^{-1} \in \operatorname{Aut} G$. Это означает, что $\operatorname{Aut} G$ является подгруппой группы $\operatorname{Symm} G$. Группу $\operatorname{Aut} G$ называют группой автоморфизмов группы G.

Рассмотрим теперь произвольные внутренние автоморфизмы $\varphi_g, \varphi_{\hat{g}} \in \operatorname{Aut} G$. Так как

$$(\varphi_g\varphi_{\hat{g}})(a) = \varphi_g(\varphi_{\hat{g}}(a)) = \varphi_g(\hat{g}^{-1}a\hat{g}) = g^{-1}(\hat{g}^{-1}a\hat{g})g = \\ = (g^{-1}\hat{g}^{-1})a(\hat{g}g) = (\hat{g}g)^{-1}a(\hat{g}g) = \varphi_{g\hat{g}},$$

то $\varphi_g\varphi_{\hat{g}} = \varphi_{g\hat{g}}$, то есть композиция внутренних автоморфизмов снова является внутренним автоморфизмом. Так как

$$(\varphi_g\varphi_{g^{-1}})(a) = \varphi_g(\varphi_{g^{-1}}(a)) = \varphi_g(gag^{-1}) = \\ = g^{-1}(gag^{-1})g = (g^{-1}g)a(g^{-1}g) = a,$$

$$(\varphi_{g^{-1}}\varphi_g)(a) = \varphi_{g^{-1}}(\varphi_g(a)) = \varphi_{g^{-1}}(g^{-1}ag) = \\ = g(g^{-1}ag)g^{-1} = (gg^{-1})a(gg^{-1}) = a,$$

то $\varphi_g^{-1} = g_{g^{-1}} \in \operatorname{Inn} G$. Таким образом, подмножество $\operatorname{Inn} G$ в $\operatorname{Aut} G$, состоящее из внутренних автоморфизмов, является подгруппой — ее называют группой внутренних автоморфизмов группы G. Очевидно, что для абелевой группы G выполняется равенство $\operatorname{Inn} G = \{\mathrm{id}\}$.

Ниже приведена программа, вычисляющая группы $\operatorname{Aut} \mathbf{D}_5$ и $\operatorname{Inn} \mathbf{D}_5$. Группа $\mathbf{D}_5$, как и рассмотренная выше группа $\mathbf{D}_3$, является частным случаем диэдральной группы $\mathbf{D}_k = \langle s, t \mid s^k = t^2 = e, ts = s^{k-1}t \rangle$, которая реализуется как группа преобразований плоскости, переводящих правильный k-угольник $A_1A_2\ldots A_k$ в себя. Обозначим r_α поворот плоскости относительно центра многоугольника на угол α. Если k нечетно, обозначим s_n, $1 \leqslant n \leqslant k$, симметрию плоскости относительно прямой, проходящей через вершину A_n и середину противоположной стороны. В случае четного k при $1 \leqslant n \leqslant \frac{k}{2}$ обозначим s_n симметрию плоскости

относительно прямой $A_nA_{n+\frac{k}{2}}$ и s_n^* симметрию относительно прямой, проходящей через середины сторон A_nA_{n+1} и $A_{n+\frac{k}{2}}A_{n+\frac{k}{2}+1}$. Тогда

$$\mathbf{D}_k = \{\mathrm{id}, r_{\frac{360}{k}}, r_{\frac{360}{k}\cdot 2}, \ldots, r_{\frac{360}{k}\cdot(k-1)}, s_1, \ldots, s_k\},\ k \text{ — нечетное},$$

$$\mathbf{D}_k = \{\mathrm{id}, r_{\frac{360}{k}}, r_{\frac{360}{k}\cdot 2}, \ldots, r_{\frac{360}{k}\cdot(k-1)}, s_1, \ldots, s_{\frac{k}{2}}, s_1^*, \ldots, s_{\frac{k}{2}}^*\},\ k \text{ — четное}.$$

В этих обозначениях таблица Кэли для группы $\mathbf{D}_5$ имеет вид:

	id	r_{72}	r_{144}	r_{216}	r_{288}	s_1	s_2	s_3	s_4	s_5
id	1	2	3	4	5	6	7	8	9	10
r_{72}	2	3	4	5	1	8	9	10	6	7
r_{144}	3	4	5	1	2	10	6	7	8	9
r_{216}	4	5	1	2	3	7	8	9	10	6
r_{288}	5	1	2	3	4	9	10	6	7	8
s_1	6	9	7	10	8	1	3	5	2	4
s_2	7	10	8	6	9	4	1	3	5	2
s_3	8	6	9	7	10	2	4	1	3	5
s_4	9	7	10	8	6	5	2	4	1	3
s_5	10	8	6	9	7	3	5	2	4	1

Алгоритм поиска автоморфизмов в этой программе похож на алгоритм вычисления гомоморфизмов из предыдущей задачи, но имеются и отличия: добавлены проверка взаимной однозначности отображения, проверка определения внутреннего автоморфизма и вычисление порядка автоморфизма.

```
   program automorphisms;
   var i,j,k,m,t,v,w : integer;
      d,inv: array[1..10] of integer;
   const g: array[1..10,1..10] of integer =((1,2,3,4,5,6,7,8,9,10),
   (2,3,4,5,1,8,9,10,6,7), (3,4,5,1,2,10,6,7,8,9), (4,5,1,2,3,7,8,9,10,6),
   (5,1,2,3,4,9,10,6,7,8), (6,9,7,10,8,1,3,5,2,4), (7,10,8,6,9,4,1,3,5,2),
   (8,6,9,7,10,2,4,1,3,5), (9,7,10,8,6,5,2,4,1,3),
(10,8,6,9,7,3,5,2,4,1));
   BEGIN
   inv[1]:=1; m:=1; d[1]:=1; v:=0;
   for i:=2 to 10 do
   begin
        j:=1;
        repeat j:=j+1 until g[i,j]=1;
        inv[i]:=j;
        m:=m*10
   end;
   for i:=0 to m-1 do
   begin
        m:=i; t:=1;
        for j:=2 to 10 do
        begin
             d[j]:=(m mod 10)+1;
```

```
     m:=m div 10;
end;
j:=1;
repeat
      j:=j+1; w:=0; k:=1;
      repeat
           k:=k+1; if j=d[k] then w:=1
      until ((w=1) or (k=10));
      if w=0 then t:=0
until ((t=0) or (j=10));
if t=1 then
       begin
           j:=1;
           repeat
                j:=j+1; if g[d[j],d[inv[j]]]<>1 then t:=0
           until ((t=0) or (j=10));
           if t=1 then
                 begin
                      j:=1;
                      repeat
                           k:=1; j:=j+1;
                           repeat
                                k:=k+1;
                                if d[g[j,k]]<>g[d[j],d[k]] then t:=0
                           until ((t=0) or (k=10));
                      until ((t=0) or (j=10))
                 end
       end;
if t=1 then
       begin
            v:=v+1; writeln();
            write('automorphism ',v,': 1');
            for j:=2 to 10 do write('-',d[j])
            k:=0;
            repeat
                 k:=k+1; w:=1; j:=1;
                 repeat
                      j:=j+1;
                      if g[g[inv[k],j],k]<>d[j] then w:=0
                 until ((j=10) or (w=0));
                 if w=0 then t:=0
            until ((k=10) or (t=0));
            if t=1 then write(' - inner');
            k:=1; j:=1;
            repeat
                 j:=j+1;
                 if d[j]<>j then k:=0
            until ((j=10) or (k=0));
            if k=0 then
                  begin
```

```
                        k:=1; w:=0;
                        repeat
                             k:=k+1;
                             for j:=2 to 10 do
                             begin
                                  d[j]:=d[d[j]];
                                  if d[j]<>j then w:=w+1
                             end
                        until (w=9);
                        write(' (ord=',k,')')
                   end
          end
     end
END.
```

Программа выводит на экран следующие результаты:

```
homomorphism 1: 1-2-3-4-5-6-7-8-9-10 - inner
homomorphism 2: 1-2-3-4-5-7-8-9-10-6 - inner (ord=5)
homomorphism 3: 1-2-3-4-5-8-9-10-6-7 - inner (ord=5)
homomorphism 4: 1-2-3-4-5-9-10-6-7-8 - inner (ord=5)
homomorphism 5: 1-2-3-4-5-10-6-7-8-9 - inner (ord=5)
homomorphism 6: 1-3-5-2-4-6-8-10-7-9 (ord=4)
homomorphism 7: 1-3-5-2-4-7-9-6-8-10 (ord=4)
homomorphism 8: 1-3-5-2-4-8-10-7-9-6 (ord=4)
homomorphism 9: 1-3-5-2-4-9-6-8-10-7 (ord=4)
homomorphism 10: 1-3-5-2-4-10-7-9-6-8 (ord=4)
homomorphism 11: 1-4-2-5-3-6-9-7-10-8 (ord=4)
homomorphism 12: 1-4-2-5-3-7-10-8-6-9 (ord=4)
homomorphism 13: 1-4-2-5-3-8-6-9-7-10 (ord=4)
homomorphism 14: 1-4-2-5-3-9-7-10-8-6 (ord=4)
homomorphism 15: 1-4-2-5-3-10-8-6-9-7 (ord=4)
homomorphism 16: 1-5-4-3-2-6-10-9-8-7 - inner (ord=2)
homomorphism 17: 1-5-4-3-2-7-6-10-9-8 - inner (ord=2)
homomorphism 18: 1-5-4-3-2-8-7-6-10-9 - inner (ord=2)
homomorphism 19: 1-5-4-3-2-9-8-7-6-10 - inner (ord=2)
homomorphism 20: 1-5-4-3-2-10-9-8-7-6 - inner (ord=2)
```

Как видно, группа $\operatorname{Inn}\mathbf{D}_5$ состоит из 10 элементов, но с точностью до изоморфизма существуют только две группы порядка 10 — циклическая группа $\mathbb{Z}_{10}$, порядки элементов которой равны 1, 2, 5 и 10, и неабелева группа $\mathbf{D}_5$, порядками элементов которой являются числа 1, 2 и 5. Отсюда делаем вывод, что $\operatorname{Inn}\mathbf{D}_5 \simeq \mathbf{D}_5$. Этот же вывод следует из того, что $\operatorname{Inn}\mathbf{D}_5$ не является абелевой группой: для этого достаточно, например, заметить, что $[\varphi_{16}\varphi_{17}](s_5) = s_4$ и $[\varphi_{17}\varphi_{16}](s_5) = s_2$ (где φ_{16} и φ_{17} суть 16-ый и 17-ый автоморфизмы), то есть $\varphi_{16}\varphi_{17} \neq \varphi_{17}\varphi_{16}$.

Неабелева группа $\operatorname{Aut}\mathbf{D}_5$ состоит из 20 элементов. С точностью до изоморфизма существует три таких группы: $\mathbf{D}_{10}$,

$$H = \langle s, t \mid s^4 = t^5 = e,\ \varphi_s(t) = t^{-1} \rangle$$

и

$$F = \langle s, t \mid s^4 = t^5 = e,\ \varphi_s(t) = t^2 \rangle.$$

$\operatorname{Aut}\mathbf{D}_5 \not\simeq \mathbf{D}_{10}$, поскольку в $\mathbf{D}_{10}$ существует элемент (например, r_{36}) порядка 10. Покажем, что элемент порядка 10 существует и в группе H. Из ее определяющего соотношения получаем, что $s^2t = ts^2$. Так как s^2 и t коммутируют друг с другом, $\operatorname{ord} s^2 = 2$, $\operatorname{ord} t = 5$ и $\text{НОД}(2,5) = 1$, получаем $\operatorname{ord}(s^2t) = \text{НОК}(2,5) = 10$. Таким образом, $\operatorname{Aut}\mathbf{D}_5 \simeq F$.

Упражнение 16. Составьте программу, спрашивающую n и выводящую на экран таблицу Кэли диэдральной группы $\mathbf{D}_n$.

Упражнение 17. Запишем в ячейки строкового массива определяющие соотношения для группы G из Задачи 4:

```
const g: array[1..3] of string = ('s8=e','t2=e','s5t=ts');.
```

Составьте программу, которая по этим соотношениям строит таблицу Кэли для группы G.

10. Решение линейного дифференциального уравнения второго порядка с постоянными коэффициентами

Пусть L — линейное пространство над полем Φ. Подмножество V в L, для любых векторов a и b которого и любого $\alpha \in \Phi$ выполняются включения $a + b \in V$ и $\alpha a \in V$, называют линейным подпространством в L. Для всякого $h \in L$ смежный класс группы $(L, +)$ по подгруппе V, порожденный вектором h, называют линейным многообразием. Вектор h называют вектором сдвига, а V — направляющим подпространством.

Пусть имеется дифференциальное уравнение $y'' + py' + qy = f(x)$, в котором коэффициенты p и q являются постоянными функциями. Перепишем его в операторном виде: $\left\{\frac{\mathrm{d}^2}{\mathrm{d}x^2} + p\frac{\mathrm{d}}{\mathrm{d}x} + q\right\} y = f$. Обозначая линейный оператор, заключенный в фигурные скобки, буквой φ, перепишем уравнение кратко: $\varphi(y) = f$. Если функция f тождественно равна нулю, то уравнение означает, что мы ищем ядро оператора φ; в этом случае множество V решений уравнения, как и ядро всякого линейного оператора, является линейным подпространством. Можно показать, что дефект оператора равен двум. По корням алгебраического уравнения $x^2 + px + q = 0$, которое называют характеристическим, можно найти базис ядра $\operatorname{Ker}\varphi$ следующим образом. Если корни характеристического уравнения действительны и различны, то, обозначив их r_1 и r_2, получаем, что $\operatorname{Ker}\varphi = \operatorname{Span}(\mathrm{e}^{r_1 x}, \mathrm{e}^{r_2 x})$. Если характеристическое уравнение имеет только один (двукратный) корень r, то $\operatorname{Ker}\varphi = \operatorname{Span}(\mathrm{e}^{rx}, x\mathrm{e}^{rx})$. Наконец, если корни характеристического уравнения являются сопряженными комплексными числами $\alpha + \mathbf{i}\beta$ и $\alpha - \mathbf{i}\beta$, то в качестве базисных векторов подпространства V можно взять функции $\mathrm{e}^{\alpha x}\cos\beta x$ и $\mathrm{e}^{\alpha x}\sin\beta x$.

Рассмотрим теперь случай, когда $f(x)$ «не является нулевым вектором». Тогда множество решений указанного выше дифференциального уравнения является линейным многообразием, направляющим подпространством для которого служит V, а в качестве вектора сдвига можно указать произвольное частное решение h уравнения. Если f имеет вид

$$f(x) = \mathrm{e}^{ax}(P_m(x)\cos bx + Q_n(x)\sin bx), \tag{4}$$

где P_m и Q_n — многочлены степени m и n, а комплексное число $a + b\mathbf{i}$ является корнем кратности s характеристического уравнения, то в качестве h можно взять функцию

$$x^s\mathrm{e}^{ax}(\tilde{P}_l(x)\cos bx + \tilde{Q}_l(x)\sin bx),$$

где $l = \max\{m, n\}$.

Например, множество решений уравнения $y'' - 6y' + 9y = 0$ является линейной оболочкой функций e^{3x} и $x\mathrm{e}^{3x}$, а множество решений уравнения $y'' - 6y' + 9y = \mathrm{e}^{3x}$, правую часть которого можно переписать в виде $\mathrm{e}^{3x}(1\cos 0x + 7\sin 0x)$, является линейным многообразием $\alpha\mathrm{e}^{3x}x^2 + \mathrm{Span}\left(\mathrm{e}^{3x}, x\mathrm{e}^{3x}\right)$, числовой коэффициент α в котором можно найти методом неопределенных коэффициентов.

Упражнение 18. Предположим, что коэффициенты p и q характеристического уравнения являются целыми числами, его корни — целыми или целыми гауссовыми числами, а правую часть уравнения $y'' + py' + qy = f(x)$ можно переписать в виде (4). Составьте программу, которая спрашивающую p, q, a, b, многочлены P_m и Q_n и выводит на экран множество решений дифференциального уравнения.

Для заметок

Для заметок

Учебное издание

Шилин Илья Анатольевич

КОМПЬЮТЕРНАЯ АЛГЕБРА В ЗАДАЧАХ

Учебное пособие

Редактор *Алексеева А. А.*
Оформление обложки *Удовенко В. Г.*
Компьютерная верстка *Шилин И. А.*

Управление издательской деятельности
и инновационного проектирования МПГУ
119571, Москва, Вернадского пр-т, д. 88, оф. 446.
Тел.: (499) 730–38–61
E-mail: izdat@mpgu.edu

Подписано в печать 20.09.2018. Формат $60 \times 90/16$.
Бум. офсетная. Печать цифровая. Объем $3,5$ п.л.
Тираж 500 экз. Заказ № 841

ISBN 978-5-4263-0664-6