ГЛАВА VII

ТЕОРИЯ ГРУПП

§ 1. Аксиомы полугруппы и группы, простейшие свойства, примеры

***830.** Правым (левым) нулем полугруппы называется такой элемент z, что $az = z$ ($za = z$) при любом a. Доказать, что если в полугруппе имеются как правые, так и левые нули, то все они совпадают, так что существует единственный двусторонний нуль.

***831.** Правой (левой) единицей полугруппы называется такой элемент u, что $au = a$ ($ua = a$) при любом a. Доказать, что если в полугруппе имеются как правые так и левые единицы, то все они совпадают, так что существует единственная двусторонняя единица.

832. Может ли элемент полугруппы быть одновременно правым нулем и левой единицей?

833. Перечислить (с точностью до изоморфизма) все полугруппы, состоящие из двух элементов.

834. Перечислить (с точностью до изоморфизма) все полугруппы с одной образующей.

***835.** Доказать, что конечная полугруппа с правыми сокращениями (т. е из $ba = ca$ следует $b = c$) и хотя бы с одной левой единицей есть группа.

836. Построить пример конечной полугруппы с правыми сокращениями, не являющейся группой.

837. Построить пример бесконечной коммутативной полугруппы с единицей и с сокращениями, не являющейся группой.

838. Доказать, что квадратные невырожденные матрицы порядка n с элементами из данного поля K образуют группу (она называется полной линейной группой степени n над полем K и обозначается $\mathrm{GL}(n, K)$).

839. Доказать, что квадратные матрицы порядка n с элементами из поля K, имеющие определитель, равный 1, образуют группу (она называется специальной линейной группой и обозначается $\mathrm{SL}(n, K)$).

840. Доказать, что квадратные матрицы порядка n, в каждой строке и в каждом столбце которых один элемент равен 1, а остальные нули, образуют группу (симметрическая группа S_n.

841. Доказать, что квадратные матрицы порядка n, в каждой строке и в каждом столбце которых имеется не более чем один элемент, равный 1, а остальные нули, образуют полугруппу.

842. Доказать, что для каждого элемента a полугруппы задачи 841 существует единственный элемент a^+ такой, что $aa^+a=a$, $a^+aa^+=a^+$ (полугруппы с таким свойством называются инверсными).

843. Доказать, что ортогональные матрицы порядка n образуют группу (полная ортогональная группа $\mathrm{GO}(n)$), группу же составляют собственно ортогональные матрицы (специальная ортогональная группа $\mathrm{SO}(n)$).

844. Доказать, что целочисленные матрицы с определителями 1 образуют группу.

845. Доказать, что пересечение групп задач 843 и 844 есть конечная группа и найти ее порядок.

846. Доказать, что пары (a, b) элементов поля K, $a\neq 0$, составляют группу относительно умножения, определяемого формулой

$$(a_1, b_1)(a_2, b_2)=(a_1a_2, a_1b_2+b_1).$$

847. Доказать, что линейные функции $ax+b$, $a\neq 0$, образуют группу относительно суперпозиции, изоморфную группе задачи 846.

848. Доказать, что непрерывные строго возрастающие на отрезке $[0, 1]$ функции φ со значениями $\varphi(0)=0$, $\varphi(1)=1$ составляют группу относительно суперпозиции.

849. Доказать, что комплексные числа, изображения которых заполняют логарифмическую спираль $r=e^{k\varphi}$, $k\neq 0$, образуют группу относительно умножения.

850. Доказать, что подстановки n элементов составляют группу, изоморфную группе задачи 840.

851. Установить изоморфизм группы вещественных чисел относительно сложения и группы задачи 849.

852. Установить изоморфизм группы вещественных чисел относительно сложения и группы положительных чисел относительно умножения.

853. Доказать, что группа движений и отражений плоскости, совмещающих с собой равносторонний треугольник, изоморфна группе S_3 подстановок трех элементов.

854. Доказать, что группа движений (без отражений) трехмерного пространства, совмещающих с собой куб, изоморфна группе S_4 подстановок четырех элементов.

***855.** Доказать, что группа, порожденная движениями и отражениями трехмерного пространства, совмещающими с собой правильный икосаэдр, изоморфна группе S_5 подстановок пяти элементов.

856. Чему равен порядок группы движений, совмещающих с собой плоскую пластину, имеющую вид правильного n-угольника (группа диэдра).

857. Пусть все элементы группы, кроме единицы, имеют порядок 2. Доказать, что группа абелева.

§ 2. Подгруппа, нормальный делитель, факторгруппа, гомоморфизм

858. Описать правые классы смежности при разложении группы G по подгруппе H:

a) G — циклическая группа Z_8 восьмого порядка, H — ее подгруппа четвертого порядка;

b) $G=S_3$, H — подгруппа, порожденная транспозицией (12);

c) G — группа вращений куба, H — ее подгруппа, совмещающая с собой одну из граней куба;

d) G — группа всех невырожденных вещественных матриц, H — подгруппа матриц с определителем 1.

859. Доказать, что в конечной группе нечетного порядка любой элемент является квадратом другого, однозначно определенного, элемента.

860. Чему равен наибольший порядок элемента симметрической группы S_{12}?

861. Сколько подгрупп имеет группа S_3. Которые из них сопряжены?

862. Доказать, что если число правых классов смежности в разложении бесконечной группы G по подгруппе H конечно, то и число левых классов смежности конечно и равно числу правых классов.

863. Доказать, что подгруппа H индекса 2 в группе G является ее нормальным делителем.

***864.** Доказать, что если H — подгруппа конечного индекса в группе G и K — промежуточная подгруппа, т. е. такая, что $H \subset K \subset G$, то индекс K в G есть делитель индекса H в G.

***865.** Доказать, что пересечение двух подгрупп H_1 и H_2 конечного индекса в группе G есть подгруппа конечного индекса, не превосходящего произведения индексов H_1 и H_2.

866. Центром группы называется множество всех элементов, коммутирующих со всеми элементами группы. Доказать, что центр есть нормальный делитель.

***867.** Доказать, что группа, порядок которой есть степень простого числа p, имеет нетривиальный центр.

868. Доказать, что существуют две группы (с точностью до изоморфизма) порядка p^2, где p — простое число, обе абелевы.

869. Перечислить группы восьмого порядка.

870. Показать, что отображение $\varphi \longrightarrow \cos\varphi + i\sin\varphi$ есть гомоморфное отображение аддитивной группы вещественных чисел на мультипликативную группу комплексных чисел модуля 1. Найти ядро гомоморфизма.

871. Рассмотрим аддитивную группу G полиномов с вещественными коэффициентами, степени которых не превосходят $n-1$. Каждому полиному $f \in G$ сопоставим строку $(f(x_1), f(x_2), \ldots, f(x_n))$, где $x_1, x_2, \ldots, x_n$ — данные попарно различные числа. Доказать, что это отображение есть изоморфизм.

872. То же отображение применить к аддитивной группе всех полиномов над $\mathbb{R}$, без ограничения степени. Доказать, что это отображение есть гомоморфизм и найти его ядро.

873. Пусть G — конечная группа, $H = \varphi(G)$ — ее гомоморфный образ. Доказать, что порядок $x \in G$ делится на порядок $\varphi(x) \in H$.

***874.** Доказать, что если порядок конечной абелевой группы делится на простое число p, то в группе найдется элемент порядка p.

***875.** Доказать, что для конечной группы число элементов в любом классе сопряженных элементов есть делитель порядка группы.

876. Что представляют собой классы сопряженных элементов в симметрической группе S_n.

877. Пусть H — абелева группа нечетного порядка. Рассмотрим множество $G = H \cup Ha$, где a — новый символ, и определим в G умножение по правилам: $x_1 \cdot x_2 = x_1 x_2$, $x_1 \cdot x_2 a = x_1 x_2 a$, $x_1 a \cdot x_2 = x_1 x_2^{-1} a$, $x_1 a \cdot x_2 a = x_1 x_2^{-1}$. Доказать, что G есть группа и все элементы из Ha сопряжены.

***878.** Описать конечные группы G порядка $2m$, в которых существует класс сопряженных элементов, содержащий половину элементов G.

***879.** Найти группы, имеющие три класса сопряженных элементов.

***880.** Найти группы, имеющие четыре класса сопряженных элементов.

***881.** Доказать, что если H — подгруппа группы G конечного индекса n, то существует лишь конечное число подгрупп, сопряженных с H, и это число делит n.

882. Доказать, что если группа G содержит подгруппу H конечного индекса, то содержит и нормальный делитель конечного индекса.

***883.** Доказать, что если подгруппа G содержит подгруппу H индекса n, то она содержит нормальный делитель, индекс которого делит $n!$.

884. Коммутатором элементов a и b группы G называется $aba^{-1}b^{-1}$. Подгруппа, порожденная коммутаторами, называется коммутантом группы G. Доказать, что:

a) коммутатор a и b равен 1 тогда и только тогда, когда a и b коммутируют;

b) конечные произведения коммутаторов составляют коммутант;

c) коммутант является нормальным делителем;

d) факторгруппа по коммутанту абелева;

e) если G/H — абелева группа, то H содержит коммутант G.

885. Доказать, что если A и B — нормальные делители группы G и $a \in A$, $b \in B$, то $aba^{-1}b^{-1} \in A \cap B$.

886. Доказать, что если A и B — нормальные делители G и $A \cap B = 1$, то элементы из A коммутируют с элементами из B.

***887.** Доказать, что если порядок конечной группы делится на простое число p, то в ней существует элемент порядка p (теорема Коши).

888. Дать описание групп порядка $2p$, где p — простое число.

***889.** Перечислить группы порядка pq, где p и q — простые числа.

***890.** Пусть группа $G=\mathrm{SL}(n, \mathbb{Z})$ есть группа целочисленных матриц порядка n с определителем 1 и m — натуральное число. Переход от кольца $\mathbb{Z}$ к кольцу вычетов $\mathbb{Z}_m$ по модулю m определяет, очевидно, гомоморфизм группы $\mathrm{SL}(n, \mathbb{Z})$ в группу $\mathrm{SL}(n, \mathbb{Z}_m)$ — группу матриц с определителем 1 над кольцом $\mathbb{Z}_m$. Доказать, что это отображение является эпиморфизмом.

***891.** Пусть G — конечная группа целочисленных матриц и m — натуральное число, $m \geqslant 3$. Доказать, что редукция по модулю m осуществляет мономорфное отображение G в $\mathrm{GL}(n, \mathbb{Z}_m)$.

***892.** Что представляют собой классы сопряженных элементов в группе $SO(3)$ вращений трехмерного пространства (или, что то же самое, в группе собственно ортогональных матриц третьего порядка).

***893.** Доказать, что группа $SO(3)$ простая, т.е. она не содержит нормальных делителей, кроме всей группы и единичной подгруппы.

894. Пусть G — конечная группа. Каждому $x \in G$ сопоставим подстановку σ_x: $a \to ax$ элементов группы G. Ясно, что произведению элементов групп соответствует произведение сопоставленных им подстановок (если считать первым действующим левый множитель) и группа G изоморфна так построенной группе подстановок. Сопоставление $x \to \sigma_x$ называется регулярным представлением конечной группы подстановками.

Доказать, что любая подстановка σ_x регулярного представления разбивается на циклы одинаковой длины, равной порядку элемента x.

895. Для того чтобы среди подстановок регулярного представления конечной группы G нашлась нечетная подстановка, необходимо и достаточно, чтобы порядок n группы G был четным числом и, если $n=2^k n_1$, при нечетном n_1, чтобы в G существовал элемент порядка 2^k.

***896.** Доказать, что если в группе G четного порядка $n=2^k n_1$, при нечетном n_1, имеется элемент порядка 2^k, то элементы нечетного порядка составляют подгруппу порядка n_1, являющуюся нормальным делителем группы G.

***897.** Показать, что симметрическая группа S_5 подстановок пяти элементов изоморфна некоторой транзитивной группе подстановок шести элементов.

898. Пусть G — группа, H — ее подгруппа конечного индекса. Умножение справа всех правых классов смежности G по H порождает гомоморфное представление группы G подстановками. Доказать, что ядро гомоморфизма есть пересечение группы H со всеми сопряженными.

899. Найти группу автоморфизмов циклической группы.

900. Найти группу автоморфизмов группы диэдра.

***901.** Найти группу автоморфизмов элементарной абелевой группы, т.е. прямого произведения конечного числа циклических групп простого порядка.

902. Найти группу автоморфизмов группы кватернионов.

903. Даны две группы G и H и дано гомоморфное отображение группы G в группу автоморфизмов группы H. Показать, что множество пар (g, h), где $g \in G$, $h \in H$, с правилом умножения $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1^{g_2} h_2)$ является группой. Здесь h^g — результат действия автоморфизма, сопоставленного g, на элемент h (так построенная группа называется полупрямым произведением групп G и H).

904. Пусть F и H — две подгруппы группы G, причем H — нормальный делитель. Доказать, что произведение FH есть подгруппа в G, являющаяся гомоморфным образом полупрямого произведения F и H, при $h^f = f^{-1} h f$.

***905.** Даны группы G и H. Рассматривается группа F функций f, определенных на G со значениями в H, с естественным умножением. В группе F определены автоморфизмы, сопоставляемые элементам G по формуле $f^{g_1}(g_2) = f(g_1 g_2)$. Полупрямое произведение GF называется сплетением групп G и H.

Доказать, что сплетение конечных групп допускает изоморфное транзитивное представление подстановками mk элементов, где m — порядок группы G, а k — порядок группы H.

906. Если группа H абелева и G конечна, то любое полупрямое произведение GH (т.е. при любом отображении группы G в группу автоморфизмов группы H) есть гомоморфный образ сплетения.

***907.** Подпрямым произведением групп H_1 и H_2 называется подгруппа F их прямого произведения, проекции которой на H_1 и H_2 заполняют H_1 и H_2.

Что представляют собой пары (h_1, h_2), составляющие подпрямое произведение?

§ 3. Свободная группа и свободное произведение

908. В свободной группе с k образующими взята подгруппа, образованная словами, в которых сумма показателей делится на m. Показать, что она является нормальным делителем и найти факторгруппу.

909. В свободной группе G с k образующими взято множество H элементов, в которых сумма показателей при каждом образующем равна нулю. Показать, что это множество есть нормальный делитель, именно, коммутант группы G, и найти факторгруппу.

***910.** Пусть G — свободное произведение $n+1$ групп второго порядка. Доказать, что элементы четной длины составляют нормальный делитель индекса 2, являющийся свободной группой с n образующими.

***911.** Доказать, что если образующие $u_1, \ldots, u_k$ группы H связаны такими соотношениями, что из $w_1 w_2 \ldots \ldots w_m = 1$ следует $w_m \ldots w_2 w_1 = 1$ (здесь w_i принимают значения $u_1, \ldots, u_k, u_1^{-1}, \ldots, u_k^{-1}$), то группа H может быть вложена как подгруппа индекса 2 в группу G, порожденную образующими $v_0, v_1, \ldots, v_k$ второго порядка.

***912.** В трехмерном пространстве дана поверхность с уравнением $x^2+y^2+z^2=axyz$, $a>0$. Рассматривается ее часть S, лежащая в октанте $x>0$, $y>0$, $z>0$. Преобразование σ_x: $(x, y, z) \longrightarrow \left(\frac{y^2+z^2}{x}, y, z\right)$, очевидно, преобразует S на себя (геометрический смысл σ_x ясен: прямые, параллельные Ox, пересекают S, вообще говоря, в двух точках и σ_x переводит одну из этих точек в другую). Аналогично определяются σ_y и σ_z.

Доказать, что группа, порожденная σ_x, σ_y, σ_z, есть свободное произведение трех групп второго порядка.

***913.** Доказать, что неопределенное уравнение $x^2 + y^2 + z^2 = axyz$, при целом $a>0$, не имеет решений в целых числах при $a \neq 1$ и $a \neq 3$. При $a=1$ все решения получаются из решения (3, 3, 3), а при $a=3$ — из решения (1, 1, 1) посредством применения преобразований из группы, порожденной преобразованиями σ_x, σ_y, σ_z (см. задачу 912).

***914.** Доказать, что множество целочисленных матриц $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, элементы которых удовлетворяют условиям $ad -$

$-bc=1$, $a\equiv d\equiv 1 \pmod 4$, $b\equiv c\equiv 0 \pmod 2$, составляет свободную группу с двумя образующими $\sigma=\begin{pmatrix}1&2\\0&1\end{pmatrix}$ и $\tau=\begin{pmatrix}1&0\\2&1\end{pmatrix}$.

§ 4. Инвариантные полиномы. Применения к исследованию уравнений низших степеней

915. Доказать, что если полином не меняется при четных перестановках и меняет знак при нечетных, то он делится на определитель Вандермонда, составленный из переменных, и частное от деления есть симметрический полином.

916. Доказать, что каждый полином, не меняющийся при четных перестановках переменных, может быть представлен в виде

$$F_1+F_2\Delta,$$

где F_1 и F_2 — симметрические полиномы и Δ — определитель Вандермонда из переменных.

917. Доказать, что каждый полином от n переменных $x_1, x_2, \ldots, x_n$, не изменяющийся при круговых перестановках переменных, можно представить в виде

$$\sum Af_1^{\alpha_0}\eta_1^{\alpha_1}\eta_2^{\alpha_2}\ldots\eta_{n-1}^{\alpha_{n-1}},$$

где $\eta_1, \eta_2, \ldots, \eta_{n-1}$ суть линейные формы:

$$\eta_1=x_1\varepsilon+x_2\varepsilon^2+\ldots+x_n,$$
$$\eta_2=x_1\varepsilon^2+x_2\varepsilon^4+\ldots+x_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\eta_{n-1}=x_1\varepsilon^{n-1}+x_2\varepsilon^{2n-2}+\ldots+x_n;$$
$$\varepsilon=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n},$$

причем показатели $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ удовлетворяют условию: $\alpha_1+2\alpha_2+\ldots+(n-1)\alpha_{n-1}$ делится на n.

918. Для рациональных функций, не меняющихся при круговых перестановках переменных, указать n основных (дробных и с нерациональными коэффициентами), через которые все выражаются рационально.

919. Для рациональных функций от трех переменных, не меняющихся при круговых перестановках, указать три основные функции с рациональными коэффициентами.

920. Для рациональных функций от четырех переменных, не меняющихся при круговых перестановках, указать четыре основные функции с рациональными коэффициентами.

921. Для рациональных функций от пяти переменных, не меняющихся при круговых перестановках, указать пять основных функций с рациональными коэффициентами.

922. Пусть $g(x_1, \ldots, x_n)$ — полином, не меняющийся при подстановках из группы H, и $f(x)$ — полином степени n с корнями $x_1^0, \ldots, x_n^0$. Доказать, что существует полином, степень которого равна индексу H в симметрической группе, одним из корней которого является $g(x_1^0, \ldots, x_n^0)$, а коэффициенты являются полиномами от коэффициентов f и g, с коэффициентами из $\mathbb{Z}$.

923. Найти уравнение, корнями которого являются

$$(x_1 + x_2\varepsilon + x_3\varepsilon^2)^3 \text{ и } (x_1 + x_2\varepsilon^2 + x_3\varepsilon)^3,$$

где $\varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, x_1, x_2, x_3 — корни уравнения

$$x^3 + ax^2 + bx + c = 0.$$

924. Найти уравнение наименьшей степени с коэффициентами, выражающимися рационально через коэффициенты данного уравнения $x^4 + ax^3 + bx^2 + cx + d = 0$, принимая за один из корней искомого уравнения:

a) $x_1x_2 + x_3x_4$; b) $(x_1 + x_2 - x_3 - x_4)^2$.

***925.** Написать формулу для решения уравнения

$$x^4 - 6ax^2 + bx - 3a^2 = 0.$$

926. Составить уравнение, одним из корней которого является

$$(x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1) \times \\ \times (x_1x_3 + x_3x_5 + x_5x_2 + x_2x_4 + x_4x_1),$$

где x_1, x_2, x_3, x_4, x_5 — корни уравнения

$$x^5 + ax + b = 0.$$