Основы алгебры (ФРТК, 3 семестр)

Линдеманн Никита, МФТИ

26 декабря 2019 г.

Содержание

1 Программа **2**

2 Теория **3**
2.1 Основные понятия и определения 3

3 Задачи **4**
3.1 Группы, их подгруппы. Циклические группы. 4
3.2 Изоморфизмы групп 7
3.3 Гомоморизмы, нормальные подгруппы и факторгруппы 9
3.4 Конечнопорождённые абелевы группы 11

Литература **12**

1 Программа

1. Группы, подгруппы, изоморфизмы групп. Циклические группы и порядки элементов. Группы классов вычетов по модулю n.

2. Смежные классы по подгруппе. Теорема Лагранжа. Нормальные подгруппы и факторгруппы.

3. Гомоморфизмы групп. Основная теорема о гомоморфизме. Теорема о соответствии подгрупп при гомоморфизмах.

4. Примеры групп: группы вращений плоскости, группы диэдра, группа кватернионов.

5. Симметрические группы. Разложение подстановок в произведение транспозиций и независимых циклов. Знакопеременные группы. Строение групп степеней 3, 4.

6. Прямые произведеения и прямые суммы групп и подгрупп.

7. Свободные абелевы группы конечного ранга. Теорема о согласованных базисах.

8. Разложение конечнопораждённых абелевых групп в прямую сумму циклических групп и примарных циклических групп.

9. Поле комплексных чисел. Алгебраическая и тригонометрическая запись комплексных чисел. Формула Муавра. Корни из комплексных чисел. Мультипликативная группа C^* и ее подгруппы.

2 Теория

2.1 Основные понятия и определения

Определение 2.1.1. Внутренней бинарной операцией на множестве X называется отображение $f : X \times X \to X$.

Определение 2.1.2. При заданном множестве Y внешней бинарной операцией на множестве X называется отображение $f : X \times Y \to X$.

Определение 2.1.3. Непустое множество G с заданной на нем внутренней бинарной операцией $* : G \times G \to G$ называется коммутативной (абелевой) группой $(G, *)$, если выполнены следующие аксиомы:

1. Ассоциотивность: $\forall\, a, b, c \in G$ выполнено $(a * b) * c = a * (b * c)$
2. Наличие нейтрального элемента: $\exists\, e \in G : \forall\, a \in G$ выполнено $e * a = a * e = a$
3. Наличие обратного элемента: $\forall\, a \in G\ \exists\, a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$
4. Коммутативность: $\forall\, a, b \in G$ выполнено $a * b = b * a$

Если на непустом множестве G просто задана одна внутреняя бинарная операция, то такое множество называется группойд, если выполнена только аксиома 1, то такое множество называется полугруппой, если выполнены аксиомы 1-2, то это монойд, а если выполнены аксиомы 1-3, то такое множество называется группой.

Далее мы будем использовать мультипликативную форму записи, то есть вместо операции $*$ писать обычное умножение $\cdot$ (часто будем опускать этот знак, как в арифметике).

Определение 2.1.4. Порядок группы G – это количество элементов группы $|G|$, а порядок элемента группы $a \in G$ – это наименьшее положительное целое число m, такое что m-кратное умножение данного элемента на себя даёт нейтральный элемент: $\operatorname{ord}(a) = |a| = m$, $a^m = e$.

Определение 2.1.5. Центр группы G – множество элементов данной группы, которые коммутируют со всеми её элементами: $Z(G) = \{a \in G \mid \forall\, b \in G\ ab = ba\}$.

Определение 2.1.6. Непустое множество $H \subset G$ является подгруппой $H < G$, если $\forall\, a, b \in H$ выполнено

1. $ab \in H$
2. $a^{-1} \in H$

Определение 2.1.7. Пусть $H < G$ и $x \in G$, тогда левый (так как умножение на x происходит слево) смежный класс группы G по подгруппе H, порожденный элементом x – это $xH = \{xh \mid h \in H\}$ (то есть произведение понимается в смысле Минковского).

3 Задачи

3.1 Группы, их подгруппы. Циклические группы.

Задача 3.1.1. Образует ли группу относительно сложения:

1. Множество всех действительных чисел.

   Да, так как из аксиоматического определения $\mathbb{R}$ следует, что вещественные числа являются абелевой группой по сложению (более того $\mathbb{R}$ – поле, а значит у него есть аддитивная и мультипликативная группа поля).

2. Множество всех неотрицательных действительных чисел.

   Нет, так как ни для одного элемента из этого множества нет противоположного.

3. Множество всех рациональных чисел.

   Да, так как выполнены все аксиомы группы: сумма двух рациональных чисел есть рациональное число, для каждого рационального $q \in \mathbb{Q}$ существует противоположное $-q \in \mathbb{Q}$, и в $\mathbb{Q}$ есть нейтральный по сложению элемент 0 (как и в случае с вещественными числами, $\mathbb{Q}$ – поле).

4. Множество всех нечетных чисел.

   Очевидно, что это множество не является группой, так как сумма двух нечетных чисел есть четное число.

5. Множество всех мнимых чисто комплексных чисел.

   Да, так как это множество с точки зрения теории групп ничем не отличается от аддитивной группы вещественных чисел (то есть они изоморфны: $\mathbb{C}_i \cong \mathbb{R}$, здесь $\mathbb{C}_i = \{ai \mid a \in \mathbb{R}\}$).

Задача 3.1.2. Образует ли группу относительно умножения:

1. Множество всех рациональных чисел.

   Нет, так как в этом множестве присутствует необратимый элемент: $0 \in \mathbb{Q}$ (это единственная причина, почему это множество не является группой по умножению: $\mathbb{Q}^* = \mathbb{Q} \setminus 0$ уже является мультипликативной группой).

2. Множество всех положительных действительных чисел.

   Да, так как выполнены все аксиомы мультипликативной группы: произведение двух положительных действительных чисел есть положительное вещественное число, для каждого $a \in \mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$ существует обратный $\dfrac{1}{a} \in \mathbb{R}_+$, и этому множеству принадлежит еденица $1 \in \mathbb{R}_+$.

3. Множество всех ненулевых комплексных чисел.

   Да, так как $\mathbb{C}$ – поле, то $\mathbb{C}^*$ – его мультипликативная группа.

4. Множество всех комплексных чисел, равных по модулю 1.

   Да: из того, что $z_1, z_2 \in \mathbb{C}_1 = \{z \in \mathbb{C} \mid |z| = 1\}$, следует, что $z_1 z_2 \in \mathbb{C}_1$ так как $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$; если $z \in \mathbb{C}_1$, то $z^{-1} \in \mathbb{C}_1$ так как $|z^{-1}| = |z|^{-1}$, и в этом множестве есть нейтральный по умножению элемент $1 \in \mathbb{C}_1$.

5. Множество всех ненулевых чисто мнимых комплексных чисел.

   Нет, так как произведение двух чисто мнимых комплексных чисел всегда вещественное число.

Задача 3.1.3. Образует ли группу данное множество квадратных матриц порядка n:

1. Относительно сложения:

   (a) Множество всех верхних треугольных матриц.

   Да, так как сумма двух верхних треугольных матриц тоже является верхней треугольной матрицей, обратная к такой матрице тоже верхняя треугольная, и нулевая матрица, являющаяся нулем группы тоже частный случай верхней треугольной матрицы.

   (b) Множество всех матриц с нулевым следом.

   Да, так как достаточно очевидно, что если $\mathrm{tr}(A) = 0, \mathrm{tr}(B) = 0$, то $\mathrm{tr}(A+B) = 0$, если $\mathrm{tr}(A) = 0$, то $\mathrm{tr}(-A) = 0$, и в качестве нуля выступают матрицы, у которых на главной диагонали стоят нули, такие матрицы тоже имеют нулевой след.

   (c) Множество всех вырожденных матриц.

   Нет, так как суммой двух вырожденных матриц может быть матрица с ненулевым определителем:
   $$\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

2. Относительно умножения:

   (a) Множество всех невырожденных матриц.

   Да, так как по свойству определителя $|A^{-1}| = |A|^{-1}$, $|A \cdot B| = |A| \cdot |B|$, и нейтральный элемент по умножению E принадлежит этому множеству.

   (b) Множество всех матриц, в каждой строке и столбце которых один элемент равен 1, а все остальные – нулю.

   Конечно, нет, так как ни одна такая матрица не обратима и в этом множестве не существует единичного элемента.

Задача 3.1.4. Доказать, что если квадрат любого элемента группы равен единичному элементу, то группа абелева.

Доказательство. Действительно, если $\forall\, a \in G\ a \cdot a = e$, то каждый элемент группы является обратным к самому себе: $a = a^{-1}$. Тогда $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ для любых $a, b \in G$, откуда и следует коммутативность группы. □

Задача 3.1.5. Доказать, что группа простого порядка является циклической.

Доказательство. Сначала покажем, что порядок элемента делит порядок группы: пусть $g \in G$, тогда $|g| = |\langle g \rangle|$, а по теорема Ланранжа порядк подгруппы делит порядок группы. Далее, пусть $|G| = p$, где p – простое число, тогда рассмотрим $g \neq e \in G$. Так как $|g| > 1$ и $|g|$ делит простое p, то $|g| = p$, а значит $|\langle g \rangle| = p \Rightarrow G = \langle g \rangle$. □

Задача 3.1.6. Найти порядки элементов и подгрупп в группах:

1. $\mathbb{Z}/_{6\mathbb{Z}} = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

   Очевидно, что 1 – порождающий элемент, значит $\langle 1 \rangle = \mathbb{Z}_6$ и $|\langle 1 \rangle| = |\mathbb{Z}_6| = 6$. Двойка образует подгруппу четных чисел: $\langle 2 \rangle = \{0, 2, 4\} \lhd \mathbb{Z}_6$ (все подгруппы данной группы нормальные так как сама группа абелева), а значит, $|\langle 2 \rangle| = |\langle 4 \rangle| = 3$. Следующая подгруппа – подгруппа состоящая из двух элементом $\langle 3 \rangle = \{0, 3\} \Rightarrow |\langle 3 \rangle| = 2$. И последняя подгруппа – подгруппа с образующим элементом 5: $\langle 5 \rangle = \langle 1 \rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6$, следовательно, $|\langle 5 \rangle| = 6$. Заметим, что порядки всех подгрупп делят порядок группы, в соответствии с теоремой Лагранжа.

2. $\left(\mathbb{Z}/_{7\mathbb{Z}}\right)^* = \{1, 2, 3, 4, 5, 6\}$.

   Здесь уже не так очевидно, какие элементы являются образующими. Будем строить подгруппы, выбирая каждый раз в качестве образующего новый элемент, начиная с двойки:
   $2 \to 4 \to 1$, значит, $\langle 2 \rangle = \langle 4 \rangle = \{1, 2, 4\}$.
   $3 \to 2 \to 6 \to 4 \to 5 \to 1$, значит, элементы 5 и 3 – образующие: $\langle 3 \rangle = \langle 5 \rangle = \left(\mathbb{Z}/_{7\mathbb{Z}}\right)^*$.
   $6 \to 1$, следовательно, $\langle 6 \rangle = \{1, 6\}$.

Задача 3.1.7. Доказать, что в группе G порядки сопряженных элементов x и gxg^{-1} ($x, g \in G$) равны.

Доказательство. Действительно, если $\mathrm{ord}(x) = n$, значит $x^n = e$, но тогда $(gxg^{-1})^n = (gxg^{-1})(gxg^{-1}) \ldots (gxg^{-1}) = gx^n g^{-1} = gg^{-1} = e$, откуда следует, что $\mathrm{ord}(gxg^{-1}) = \mathrm{ord}(x) = n$. □

3.2 Изоморфизмы групп

Задача 3.2.1. Доказать, что мультипликативная группа $\left(\mathbb{Z}/_{8\mathbb{Z}}\right)^*$ не изоморфна аддитивной группе $\mathbb{Z}/_{4\mathbb{Z}} = \mathbb{Z}_4$, хотя в обеих группах по 4 элемента.

Доказательство. Мы знаем, что $\left(\mathbb{Z}/_{8\mathbb{Z}}\right)^* = \{1, 3, 5, 7\}$ и $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Установить отсутствие изоморфизма можно, перебрав все возможные $4! = 24$ взаимно-однозначные отображения (биекции) между группами, но мы сделаем проще. Пусть все-таки изоморфизм $\varphi : \mathbb{Z}_4 \to \left(\mathbb{Z}/_{8\mathbb{Z}}\right)^*$ существует, тогда $\varphi(0) = 1$. Рассмотрим, куда может перейти $1 \in \mathbb{Z}_4$. Очевидно, что $1 + 1 = 2 \neq 0 \in \mathbb{Z}_4$, но это значит, что $1 \in \mathbb{Z}_4$ не может при изоморфизме переходить ни в один элемент группы $\left(\mathbb{Z}/_{8\mathbb{Z}}\right)^*$: если $\varphi(1) = 3$, то $\varphi(1 + 1) = \varphi(2) = \varphi(1)\varphi(1) = 3 \cdot 3 = 1$, что при биекции невозможно, так как в единицу группы $\left(\mathbb{Z}/_{8\mathbb{Z}}\right)^*$ переходит ноль группы $\mathbb{Z}_4$, если предположить, что $\varphi(1) = 5$, то тоже легко прийти к противоречию таким же способом $\varphi(1 + 1) = \varphi(2) = \varphi(1)\varphi(1) = 5 \cdot 5 = 1$, аналогично и при $\varphi(1) = 7$ противоречие – $\varphi(1 + 1) = \varphi(2) = \varphi(1)\varphi(1) = 7 \cdot 7 = 1$. Значит, $\left(\mathbb{Z}/_{8\mathbb{Z}}\right)^* \ncong \mathbb{Z}/_{4\mathbb{Z}}$ □

Задача 3.2.2. Доказать, что существует только две неизоморфные группы, содержащие по 4 элемента.

Доказательство. Путь $|G| = 4$. Тогда возможны два случая. Во-первых, в группе G может быть элемент порядка 4, тогда группа G изоморфна циклической группе $\mathbb{Z}_4$ соответствующего порядка.

Пусть теперь в группе G четвертого порядка нет элементов четвертого порядка. Это означает, что все отличные от единицы элементы группы G имеют порядок 2 (это следует из теоремы Лагранжа – порядок подгруппы должен делить порядок группы), откуда следует, что группа G является коммутативной. Пусть $G = \{1, a, b, c\}$ — коммутативная группа и $a^2 = b^2 = c^2$ Найдем, чему равно ab. Если $ab = 1$, то $a = b$, что невозможно так как элементы a и b различны. Далее, если $ab = a$, то $b = 1$, а если $ab = b$, то $a = 1$, что также невозможно. Остается только одна возможность, а именно, $ab = c$. Циклические подгруппы $\langle a\rangle$ и $\langle b\rangle$ нормальны в G (так как G коммутативна, то все подгруппы в ней нормальные). Заметим также, что $\langle a\rangle \cap \langle b\rangle = \{1\}$ и $\langle a\rangle \cdot \langle b\rangle = \{1, a, b, ab\} = G$. Значит, $G \cong \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (это следует из теоремы, которая утверждает, что если $H \lhd G$ и $K \lhd G$ – нормальные подгруппы группы G, такие, что $H \cap K = \{1\}$ и $HK = G$, то $H \times K \cong G$).

Итак, существуют только две (с точностью до изоморфизма) группы порядка 4: циклическая группа $\mathbb{Z}_4$ и группа $\mathbb{Z}_2 \times \mathbb{Z}_2$. □

Задача 3.2.3. Доказать, что матрицы вида $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$, где $x, y \in \mathbb{R}$ образуют аддитивную группу, изоморфную $(\mathbb{C}, +)$, а ненулевые матрицы того же вида – мультипликативную группу, изоморфную $(\mathbb{C}^*, \cdot)$.

Доказательство. Для доказательства изоморфности аддитивных групп построим в явном виде изоморфизм $\varphi : (M_2, +) \to (\mathbb{C}, +)$, где $(M_2, +)$ – группа, состоящая из матриц указанного вида. Сопоставим каждому комплексному числу матрицу по правилу: $\varphi(z) = \varphi(x + iy) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$. Биективность такого отображения очевидна, проверим, что это гомоморфизм: $\varphi(z_1 + z_2) = \varphi((x_1 + iy_1) + (x_2 + iy_2)) = \varphi((x_1 + x_2) + (y_1 + y_2)i) = \begin{pmatrix} x_1 + x_2 & -y_1 - y_2 \\ y_1 + y_2 & x_1 + x_2 \end{pmatrix} = \begin{pmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{pmatrix} + \begin{pmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{pmatrix} = \varphi(z_1) + \varphi(z_2)$.

Аналогично докажем второй факт. Покажем, что отображение $\varphi(z) = \varphi(x + iy) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$ является гомомрфизмом и мультипликативных групп $(M_2, \cdot)$ и $(\mathbb{C}, \cdot)$. Действительно:

$$\varphi(z_1 z_2) = \varphi((x_1 + iy_1)(x_2 + iy_2)) = \varphi((x_1x_2 - y_1y_2) + (x_2y_1 + x_1y_2)i) =$$
$$\begin{pmatrix} x_1x_2 - y_1y_2 & -x_1y_2 - x_2y_1 \\ x_2y_1 + x_1y_2 & x_1x_2 - y_1y_2 \end{pmatrix} = \begin{pmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{pmatrix} = \varphi(z_1)\varphi(z_2).$$

□

Задача 3.2.4. Доказать, что группа диэдра D_4 степени 4 (группа преобразований плоскости, сохранующих квадрат) и мультипликативная группа кватернионов Q_8 не изоморфны.

Доказательство. Известно, что $Q_8 = \{\pm 1, \pm i, \pm j, \pm k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1\}$ и $D_4 = \{\mathrm{Id}, \mathrm{R}_{\frac{\pi}{2}}, \mathrm{R}_\pi, \mathrm{R}_{\frac{3\pi}{2}}, \mathrm{S}_1, \mathrm{S}_2, \mathrm{S}_3, \mathrm{S}_4\}$, где Id – тождественное преобразование, R_α – поворот вокруг центра квадрата на угол α, а $\mathrm{S}_1, \mathrm{S}_2, \mathrm{S}_3, \mathrm{S}_4$ – четыре отражения (два относительно диоганалей и два относительно серединных перпедикуляров квадрата).

Рассмотрим порядки элементов в группе Q_8: $|\pm i| = |\pm j| = |\pm k| = 4$, $|-1| = 2$. Для группы D_4: $|\mathrm{S}_1| = |\mathrm{S}_2| = |\mathrm{S}_3| = |\mathrm{S}_4| = 2$, $|\mathrm{R}_{\frac{\pi}{2}}| = 4$, $|\mathrm{R}_\pi| = 2$, $|\mathrm{R}_{\frac{3\pi}{2}}| = 4$. Из того факта, что в Q_8 только один элемент порядка два, в то время как в группе D_4 целых пять элементов второго порядка, делаем вывод, что данные группы не могут быть изоморфны: $D_4 \ncong Q_8$. □

3.3 Гомоморизмы, нормальные подгруппы и факторгруппы

Задача 3.3.1. Доказать, что при гомоморфизме групп $\varphi : G \to S$ нейтральный элемент первой группы переходит в нейтральный элемент второй группы: $\varphi(e_G) = e_S$, а так же, что $\forall\, g \in G$ верно $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Доказательство. Рассмторим произвольный элемент $a \in G$, для него выполнено $\varphi(a) = \varphi(e_G \cdot a) = \varphi(e_G)\varphi(a)$, значит $\varphi(e_G) \in S$ – нейтральный элемент в группе S, то есть $\varphi(e_G) = e_S$. Для доказательства второго факта положим $\varphi(g) = s \in S$ и рассмотрим $e_S = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) = s\varphi(g^{-1})$, откуда следует, что $\varphi(g^{-1}) = s^{-1} = \varphi(g)^{-1}$. □

Задача 3.3.2. Доказать, что ядро любого гомоморфизма является нормальной подгруппой в группе, из которой он действует.

Доказательство. Пусть $\varphi : G \to S$ – заданный гомоморфизм групп. По определению $\operatorname{Ker}\varphi = \{g \in G \mid \varphi(g) = e_S \in S\}$. Покажем, что ядро – подгруппа: действительно, $\forall\, k_1, k_2 \in \operatorname{Ker}\varphi$ верно, что $k_1k_2, k_1^{-1} \in \operatorname{Ker}\varphi$ так как если $\varphi(k_1) = \varphi(k_2) = e_S$, то $\varphi(k_1k_2) = \varphi(k_1)\varphi(k_2) = e_S \in \operatorname{Ker}\varphi$ и $\varphi(k_1^{-1}) = \varphi(k_1)^{-1} = e_S^{-1} = e_S \in \operatorname{Ker}\varphi$. Нормальность этой подгруппы следует из того факта, что нейтральный элемент коммутирует со всеми элементами группы: $\forall\, g \in G$ и $\forall\, k \in \operatorname{Ker}\varphi$ верно, что $gk = kg$, так как $\varphi(gk) = \varphi(g)\varphi(k) = \varphi(g)e_S = \varphi(g)$ и аналогично $\varphi(kg) = \varphi(k)\varphi(g) = e_S\varphi(g) = \varphi(g)$, это и означает, что $\operatorname{Ker}\varphi \lhd G$. □

Задача 3.3.3. Определить разбиение группы S_3 на левые и правые смежные классы:

1. По подгруппе $H = \{e, (23)\}$.

   По определению правый смежный класс группы S_3 по подгруппе H – это множество $Hg = \{hg \mid h \in H\}$ (аналогично определяется и левый смежный класс), где представитель смежного класса g пробегает всю группу S_3.

   Пусть $g \in S_3 = \{e, (12), (13), (23), (123), (321)\}$. Построим смежные классы по подгруппе H с разными представителями:

$$g = e \Rightarrow \quad He = eH = H$$

$$g = (12) \Rightarrow \quad H(12) = \{(12), (132)\},\ (12)H = \{(12), (231)\}$$
$$g = (13) \Rightarrow \quad H(13) = \{(13), (123)\},\ (12)H = \{(12), (213)\}$$
$$g = (23) \Rightarrow \quad H(23) = \{(23), e\},\ (23)H = \{(23), e\}$$
$$g = (123) \Rightarrow \quad H(123) = \{(123), (13)\},\ (123)H = \{(123), (21)\}$$
$$g = (321) \Rightarrow \quad H(321) = \{(321), (12)\},\ (321)H = \{(321), (13)\}$$

2. По подгруппе $K = \{e, (123), (321)\}$.

   Пусть $g \in S_3 = \{e, (12), (13), (23), (123), (321)\}$. Аналогично предыдущему пункту построим смежные классы по подгруппе K с разными представителями:

$$g = e \Rightarrow \quad Ke = eK = K$$

$$g = (12) \Rightarrow \quad K(12) = \{(12), (13), (23)\},\ (12)K = \{(12), (23), (13)\}$$
$$g = (13) \Rightarrow \quad K(13) = \{(13), (32), (12)\},\ (13)K = \{(13), (21), (23)\}$$
$$g = (23) \Rightarrow \quad K(23) = \{(23), (21), (31)\},\ (23)K = \{(23), (13), (21)\}$$
$$g = (123) \Rightarrow \quad K(123) = \{(123), (132), e\},\ (123)K = \{(123), (132), e\}$$
$$g = (213) \Rightarrow \quad K(213) = \{(213), 3, (123)\},\ (213)K = \{(213), e, (123)\}$$

   Так как $\forall\, g \in S_3$ правые и левые межные классы по подгруппе K совпадают $gK = Kg$, то, по определению, K является нормальной подгруппой в S_3: $S_3 \rhd K$.

Задача 3.3.4. Установить изоморфизмы групп:

1. $\mathbb{C}/_{\mathbb{R}} \cong \mathbb{R}$.

   Воспользуемся первой теоремой об изоморфизме, которая гласит, что гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма. Постороим такой гомоморфизм $\varphi : \mathbb{C} \to \mathbb{R}$, чтобы его ядро совпадало со множеством вещественных чисел $\operatorname{Ker}\varphi = \mathbb{R}$. Нетрудно видеть, что эпиморфизм (сюръективный гомоморфизм), заданный правилом $\varphi(z) = \varphi(x + iy) = y$ удовлетворяет этому условию, причем $\varphi(\mathbb{C}) = \mathbb{R}$. Тогда по первой теореме об изоморфизме $\varphi(\mathbb{C}) \cong \mathbb{C}/_{\operatorname{Ker}\varphi}$, что равносильно тому, что $\mathbb{R} \cong \mathbb{C}/_{\mathbb{R}}$.

2. $\mathbb{C}^*/_U \cong \mathbb{R}_+$ (здесь $U = \{z \in \mathbb{C} \mid |z| = 1\}$, а $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$).

   Опять же воспользуемся первой теоремой об изоморфизме. Пусть $\varphi : \mathbb{C}^* \to \mathbb{R}_+$ задано правилом $\varphi(z) = \varphi(x+iy) = x^2+y^2$. Проверим, что это гомомрфизм: $\varphi(z_1z_2) = \varphi((x_1+iy_1)(x_2+iy_2)) = \varphi((x_1x_2-y_1y_2)+i(x_1y_2+x_2y_1)) = (x_1x_2-y_1y_2)^2+(x_1y_2+x_2y_1)^2 = x_1^2(x_2^2+y_2^2)+y_1^2(x_2^2+y_2^2) = (x_1^2+y_1^2)(x_2^2+y_2^2) = \varphi(z_1)\varphi(z_2)$, причем $\varphi(\mathbb{C}^*) = \mathbb{R}_+$. Ядро этого гомоморфизма – все элементы, переходящие в единицу, то есть $\operatorname{Ker}\varphi = U$. Значит, $\varphi(\mathbb{C}^*) \cong \mathbb{C}^*/_{\operatorname{Ker}\varphi}$ по первой теореме об изоморфизме, а следовательно $\mathbb{C}^*/_U \cong \mathbb{R}_+$.

3. $U/_{U_n} \cong U$ (здесь U_n – группа комплексных корней n-ой степени из единицы).

   Зададим гомомрфизм $\varphi : U \to U$ правилом $\varphi(z) = z^n$. Очевидно, что $\operatorname{Ker}\varphi = U_n$ и $\varphi(U) = U$. Значит, по первой теореме об изоморфизме, $U/_{U_n} \cong U$.

4. $\mathbb{Z}_{36}/_{\mathbb{Z}_6} \cong \mathbb{Z}_6$. Верно ли, что $\mathbb{Z}_6 \oplus \mathbb{Z}_6 \cong \mathbb{Z}_{36}$?

   Построим гомоморфизм $\varphi : \mathbb{Z}_{36} \to \mathbb{Z}_6$ следующим образом: $\varphi(n) = \dfrac{n}{36} \mod 6$, где $\mod$ означает взятие остатка от делния (в данном случае на 6). Нетрудно видеть, что $\operatorname{Ker}\varphi = \mathbb{Z}_6$ и $\varphi(\mathbb{Z}_{36}) = \mathbb{Z}_6$, значит, по первой теореме об изоморфизме, $\mathbb{Z}_{36}/_{\mathbb{Z}_6} \cong \mathbb{Z}_6$.

3.4 Конечнопорождённые абелевы группы

Задача 3.4.1. Разложить в прямую сумму подгрупп группы:

1. $\mathbb{Z}_{12}$
2. $\mathbb{Z}_{16}$
3. $\mathbb{Z}$

Задача 3.4.2. Определить с точностью до изоморфизма все абелевы группы порядка 48.

Задача 3.4.3. Изоморфны ли группы $\mathbb{Z}_6 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{10}$ и $\mathbb{Z}_{30} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$?

Задача 3.4.4. Разложить в прямую сумму циклических групп факторгруппу $A/_B$, где A – свободная вбелева группа с базисом x_1, x_2, x_3, а B – ее подгруппа с образующими y_1, y_2, y_3, причем:

$$\begin{cases} y_1 = 2x_1 + 6x_2 - 2x_3 \\ y_2 = 2x_1 + 8x_2 - 4x_3 \\ y_3 = 4x_1 + 12x_2 - 2x_3 \end{cases}$$

Задача 3.4.5. Разложить в прямое произведение примарных циклических погрупп мультипликативную группу $\mathbb{Z}_{18}^*$ обратимых классов вычетов по модулю 18.

Список литературы

[1] И.И. Богданов. Курс видеолекций «Теория групп». https://www.youtube.com/playlist?list=PLyBWNG-pZKx6pWlAfPRo2X_kPWyzq1ebj.

[2] Т.М. Банникова, Н.А. Баранова. Теория групп в задачах и упражнениях

[3] К.Ю. Федоровский. Алгебра. Введение в теорию групп