МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

АЛГЕБРА. ЧАСТЬ 2

ТИМАШЁВ
ДМИТРИЙ АНДРЕЕВИЧ

МЕХМАТ МГУ

Оглавление

Лекция 1. Начала теории групп: определение, примеры, гомоморфизм

Первая лекция в нашем курсе будет вводной – мы будет вспоминать основные сведения из теории групп, которые освещались в первой части курса.

Определение. Группа – это множество G, на котором задана бинарная операция $G \times G \to G$ (т.е. сопоставляющая двум элементам группы третий: $(x, y) \mapsto x \cdot y$), обычно называемая умножением и удовлетворяющая аксиомам группы:
1) ассоциативность

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \forall x, y, z \in G$$

2) существование нейтрального элемента e:

$$\exists e \in G \ \ \forall x \in G: \ \ x \cdot e = e \cdot x = x$$

3) существование обратного элемента:

$$\forall x \in G \ \ \exists y \in G: \ x \cdot y = y \cdot x = e$$

Отметим, что из аксиом следует, что нейтральный элемент e определен однозначно, и для $\forall x \in G$ обратный элемент к x (обозначается x^{-1}) определен однозначно – эти свойства мы доказывали в прошлом семестре.

Если добавить условие коммутативности бинарной операции, то получим важный класс групп – коммутативные, или абелевы группы.

Определение. Группа G называется коммутативной (абелевой), если она удовлетворяет аксиоме коммутативности умножения:

4) коммутативность

$$x \cdot y = y \cdot x \quad \forall x, y \in G$$

Замечание: в общем случае мы будем называть операцию в группе умножением (мультипликативная терминология), но нередко операцию в группе называют не умножением, а сложением (аддитивная терминология – используется только для абелевых групп). В зависимости от терминологии меняются названия некоторых объектов и понятий, связанных с группами:

Терминология	**Мультипликативная**	**Аддитивная**
операция	умножение: $x \cdot y$	сложение: $x + y$
нейтральный элемент	единица: e или 1	нуль: 0
	обратный элемент: x^{-1}	противоположный элемент: $-x$
	степень: $\forall k \in \mathbb{Z}$ $x^k = \begin{cases} x \cdot \ldots \cdot x, & k > 0 \\ x^{-1} \cdot \ldots \cdot x^{-1}, & k < 0 \\ e, & k = 0 \end{cases}$	кратные: $k \cdot x$

После того, как мы вспомнили основные термины, связанные с группами, вспомним и даже расширим список примеров групп.

Примеры групп:

1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$; операция – сложение.
Это абелевы группы, и все они являются частными случаями одного более общего примера: пусть A – кольцо, тогда аддитивная группа кольца $(A, +)$, т.е. множество A с операцией сложения – это абелева группа (по сложению).

2) $\mathbb{Q}\backslash\{0\}, \mathbb{R}\backslash\{0\}, \mathbb{C}\backslash\{0\}$; операция – умножение.
Это абелевы группы, и все они являются частными случаями одного более общего примера: пусть A – ассоциативное кольцо с единицей, тогда мультипликативная группа кольца $A^\times = \{x \in A \mid \exists y \in A\colon\ x \cdot y = y \cdot x = 1\}$, т.е. множество всех обратимых элементов A – это абелева группа (по умножению).
Если мы по аналогии рассмотрим кольцо целых чисел $\mathbb{Z}$, то увидим, что мультипликативная группа этого кольца содержит только два элемента: $\mathbb{Z}^\times = \{1, -1\}$, то есть, мультипликативная группа кольца может быть довольно маленькой.
Если же вместо кольца рассмотреть некоторое поле K, то группа обратимых элементов поля (по определению) состоит из всех ненулевых элементов поля: $K^\times = K\backslash\{0\}$. Требование коммутативности здесь даже необязательно, т.е. достаточно рассмотреть тело, а не поле.

3) Матричные группы.
Пусть K – поле. Во всех матричных группах (если специально не оговорено иное) в качестве операции рассматривается операция умножения матриц.
Полная матричная группа (т.е. группа, состоящая из всех невырожденных матриц над данным полем):

$$GL_n(K) = \{A \in Mat_n(K) \mid \det A \neq 0\}$$

Так как множество невырожденных матриц совпадает с множеством обратимых матриц, то можно рассматривать эту группу как мультипликативную группу кольца всех квадратных матриц данного размера, т.е. $GL_n(K) = Mat_n(K)^\times$.
Существует множество широко изучающихся подгрупп $GL_n(K)$, укажем некоторые из них.
Специальная линейная группа (группа, состоящая из матриц с определителем 1):

$$SL_n(K) = \{A \in Mat_n(K) \mid \det A = 1\}$$

Ортогональная группа (состоит из всех ортогональных матриц данного размера):

$$O_n(K) = \{A \in Mat_n(K) \mid A \cdot A^T = E\}$$

Специальная ортогональная группа:

$$SO_n(K) = O_n(K) \cap SL_n(K)$$

4) Линейные группы.
Если мы посмотрим на предыдущую серию примеров с безкоординатной точки зрения, то получим линейные группы – аналоги матричных групп.
Пусть V – векторное пространство над полем K, $dim\, V = n < \infty$. Рассмотрим множество линейных операторов пространства V. При фиксированном базисе V всякий линейный оператор однозначно задается квадратной матрицей размера $n \times n$, и наоборот – всякая квадратная матрица $n \times n$ задает некий линейный оператор пространства V. Таким образом, мы получаем взаимно-однозначное соответствие между квадратными матрицами и линейными операторами (очевидно, это соответствие зависит от выбора базиса). Поэтому при фиксированном базисе вместо соответствующих матричных групп мы можем рассматривать группы линейных операторов (в качестве операции рассматривается операция умножения (композиции) линейных операторов).
Полная линейная группа:

$$GL(V) = \{\text{обратимые линейные операторы на } V\}$$

Также можно рассматривать эту группу как мультипликативную группу кольца всех линейных операторов на пространстве V, т.е. $GL(V) = L(V)^\times$.
В этой группе можно рассматривать подгруппы:

Специальная линейная группа (группа, состоящая из операторов с определителем 1):

$$SL(V) = \{\mathcal{A}: V \to V \;\; \det \mathcal{A} = 1\}$$

Пусть V – евклидово векторное пространство над полем действительных чисел (т.е. $K = \mathbb{R}$ и на V задано скалярное произведение). Рассмотрим операторы на V,

сохраняющие скалярное произведение (т.е. сохраняющие длины векторов) – получим ортогональную группу.

Ортогональная группа:

$$O(V) = \{\text{ортогональные линейные операторы на } V\}$$

Специальная ортогональная группа

$$SO(V) = O(V) \cap SL(V)$$

Можно модифицировать понятие скалярного умножения и рассматривать невырожденную симметрическую билинейную функцию на векторном пространстве над произвольным полем. В этом случае получим псевдоортогональные группы – не будем подробно о них говорить, для примеров ограничимся евклидовым случаем.

5) Группы движений (изометрий).
Продолжим серию геометрических примеров. Пусть E – евклидово аффинное пространство и $F \subseteq E$ – геометрическая фигура. Назовем группой движений (изометрий) фигуры F множество тех движений аффинного пространства E, которые фигуру F переводят в себя:

Группа движений фигуры F:

$$Isom(F) = \{\varphi: E \to E, \varphi - \text{движение}, \varphi(F) = F\}$$

В качестве групповой операции рассматривается операция композиции движений. В этой группе можно рассмотреть подгруппу собственных движений.

Группа собственных движений фигуры F:

$$Isom(F)^+ = \{\varphi: E \to E, \varphi - \text{собственное движение}, \varphi(F) = F\}$$

Пример.
Пусть E – евклидова плоскость, в качестве фигуры F рассмотрим правильный n-угольник $\Delta_n \subset E$. Группа движений правильного n-угольника носит специальное название – *группа диэдра:*

$$D_n = Isom\,(\Delta_n)$$

Обсудим, как устроена группа диэдра. Рассмотрим два случая – четного и нечетного n. В качестве примера рассмотрим правильный 5-угольник и правильный 6-угольник и посмотрим, какие движения плоскости их сохраняют.
Во-первых, такие движения должны сохранять на месте центры правильных n-угольников, т.е. центр – это неподвижная точка движения. Поэтому все искомые

движения – это повороты и отражения относительно прямых. Посмотрим, какие из них сохраняют Δ_n.

Начнем с поворотов. Δ_n переходит в себя только при поворотах вокруг центра на угол, кратный $\frac{2\pi}{n}$.

Так как отражения должны сохранять Δ_n, то они должны быть относительно осей симметрии Δ_n. В случае нечетного n любая ось симметрии проходит через центр Δ_n и одну из вершин, в случае четного n любая ось симметрии проходит либо через противоположные вершины, либо через середины противоположных сторон. В обоих случаях получаем n симметрий.

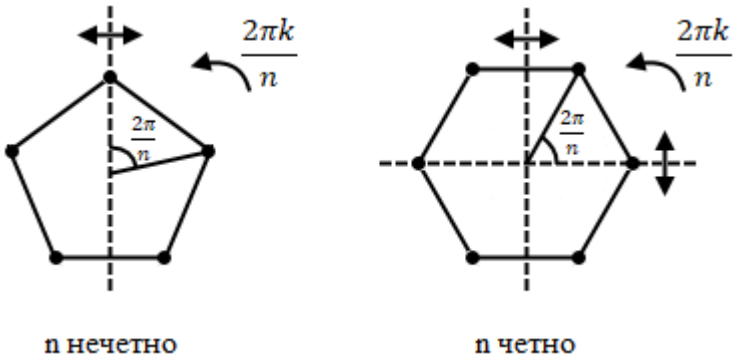


Рис. 1.1. Случай четного и нечетного Δ_n

$$D_n = Isom\,(\Delta_n) = \{\text{повороты на углы } \frac{2\pi k}{n} \text{ вокруг центра } \Delta_n\ (k = 0, \dots, n-1);$$
$$\text{отражения относительно осей симметрии } \Delta_n\ (n \text{ штук})\}$$

Итак, $|D_n| = 2n$. Нетрудно видеть, что группа собственных движений Δ_n содержит только повороты:

$$Isom(D_n)^+ = \{\text{повороты на углы } \frac{2\pi k}{n} \text{ вокруг центра } \Delta_n\ (k = 0, \dots, n-1)\} = R_n$$

6) Группа преобразований (подстановок) множества X.

Пусть X – произвольное множество. Рассмотрим все преобразования этого множества (т.е. все взаимно-однозначные отображения этого множества в себя):

Группа преобразований множества X:

$$S(X) = \{\varphi: X \to X, \varphi \ - \text{ биекция}\}$$

В качестве групповой операции рассматривается операция композиции преобразований. Если множество X конечно, то можно пронумеровать его элементы и считать, что оно содержит натуральные числа от 1 до n: $X = \{1, \dots, n\}$. Тогда группа преобразований превращается в группу подстановок:

Группа подстановок (симметрическая группа):

$$S(X) = S_n$$

В этой группе заслуживает внимания подгруппа четных постановок A_n (знакопеременная группа):

Группа четных подстановок:

$$A_n = \{\sigma \in S_n, \sigma - \text{ четная}\}$$

На этом пока закончим рассмотрение основных примеров групп. Из указанных выше примеров видно, насколько богатой является область приложения теории групп. Важно уметь различать группы и сравнивать их между собой по различным свойствам.

Похожая задача возникает не только в теории групп, но и в других областях математики (сравнение между собой разных алгебраические структуры одного типа). Общее решение, которое математика придумала для решения такого рода вопросов – рассматривать отображения из одной структуры в другую, которые определенным образом согласованы со свойствами структур данного типа. Термин “согласованность” в каждом конкретном случае определяется по-разному. Например, в топологии (при рассмотрении структур топологического пространства) в качестве таких согласованных отображений рассматриваются непрерывные отображения из одного топологического пространства в другое. В математическом анализе (при рассмотрении например многомерных пространств, многообразий) рассматриваются дифференцируемые отображения. В линейной алгебре основной структурой является структура векторного пространства и отображения, согласованные с этой структурой – это линейные отображения. А для произвольных алгебраических структур (группы, кольца ,поля...) используется понятие гомоморфизма. Дадим определение гомоморфизма в категории групп (в категории других алгебраических структур определение будет аналогичным).

Определение. Гомоморфизм групп – это отображение $\varphi: G \to H$ (где G и H – группы), удовлетворяющее свойству:

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y), \forall x, y \in G$$

Проиллюстрируем это определение на нескольких простых примерах.

Примеры гомоморфизмов:

1) Знак подстановки можно рассматривать как гомоморфизм из группы подстановок в мультипликативную группу действительных чисел:

$$sgn: S_n \to \mathbb{R}^\times$$

2) Определитель матрицы – гомоморфизм из полной матричной группы в мультипликативную группу поля K:

$$\det: GL_n(K) \to K^\times$$

Отметим несколько простейших свойств гомоморфизма, непосредственно вытекающих из определения.

1) Единица переходит в единицу:

$$\varphi(e) = e$$

- здесь единица e в группах G и H обозначена одинаково – это не вызывает путаницы, так как каждый раз из контекста понятно, о какой группе идет речь. Строго говоря, нужно писать так:

$$\varphi(e_G) = e_H$$

Доказательство.

$$\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e)$$

Умножив обе части полученного равенства на $\varphi(e)^{-1}$, получим $e = \varphi(e)$, что и требовалось.

2) Обратный элемент переходит в обратный:

$$\varphi(g^{-1}) = \varphi(g)^{-1}, \forall g \in G$$

Доказательство.

$$\varphi(g) \cdot \varphi(g^{-1}) = \varphi(g \cdot g^{-1}) = \varphi(e) = e$$

Аналогично

$$\varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1} \cdot g) = \varphi(e) = e$$

Значит, $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Напомним, что в первом семестре мы рассматривали частный случай гомоморфизма – изоморфизм (т.е. биективный гомоморфизм $G \to H$). В этом случае существует обратное отображение

$$\varphi^{-1}: H \to G$$

- тоже изоморфизм. Обозначение:

$$G \rightleftharpoons H$$

Определение. Группы изоморфны, если между ними существует изоморфизм. Обозначение:

$$G \simeq H$$

Изоморфные группы с точки зрения тории групп неразличимы. Вообще, изоморфные математические структуры в рамках теории структур данного типа нельзя отличить друг от друга. С помощью же гомоморфизма можно сравнивать различные алгебраические

структуры одного и того же типа (например, группы) друг с другом. Например, можно исследовать структуру сложно устроенных групп, с помощью гомоморфизма отображая их в более простые группы.

Примеры.
1) Рассмотрим три группы:

- $(\mathbb{Z}_n, +)$ – аддитивную группу кольца вычетов по модулю n с операцией сложения
- $(\mathbb{U}_n, \cdot)$ – группу корней степени n из в $\mathbb{C}$
- R_n – группу поворотов плоскости вокруг неподвижной точки на углы, кратные $\frac{2\pi}{n}$

Все эти группы изоморфны между собой: $(\mathbb{Z}_n, +) \simeq (\mathbb{U}_n, \cdot) \simeq R_n$. Изоморфизм устанавливается просто:

$$k \bmod n \leftrightarrow \varepsilon_k = e^{\frac{2\pi k i}{n}} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} \leftrightarrow \text{поворот на угол } \frac{2\pi k}{n} \text{ против ч. с.}$$

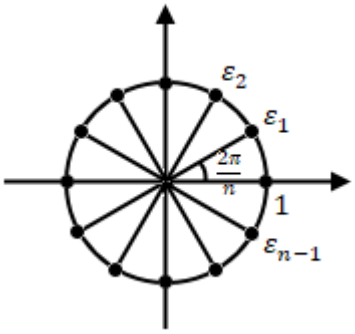


Рис. 1.2. Иллюстрация изоморфизма групп

При перемножении комплексных корней из 1 их аргументы складываются (т.е. складываются углы поворота), но складываются по модулю 2π, поэтому можно сказать, что операция сложения вычетов соответствует операции умножения соответствующих корней из 1 и соответствует операции сложения углов поворота (т.е. композиции поворотов).

2) Рассмотрим три группы:

- $(\mathbb{Z}_6, +)$ – аддитивную группу кольца вычетов по модулю n с операцией сложения
- S_3 – группу подстановок с операцией умножения подстановок
- D_3 – группа движений правильного треугольника

Группы $(\mathbb{Z}_6, +)$ и S_3 не изоморфны между собой. Действительно, группа $(\mathbb{Z}_6, +)$ – абелева, а группа S_3 неабелева (замечание: единственный способ доказать неизоморфность групп – предъявить некоторое теоретико-групповое свойство, которое выполняется в одной группе, но не выполняется в другой).

Группы S_3 и D_3 изоморфны между собой. Группа D_3 содержит 6 элементов: поворот на 0 (тождественное преобразование), повороты на $\pm\frac{2\pi}{3}$ и три симметрии, проходящих через вершины треугольника. Пронумеруем вершины треугольника, как показано на рис. 1.3:

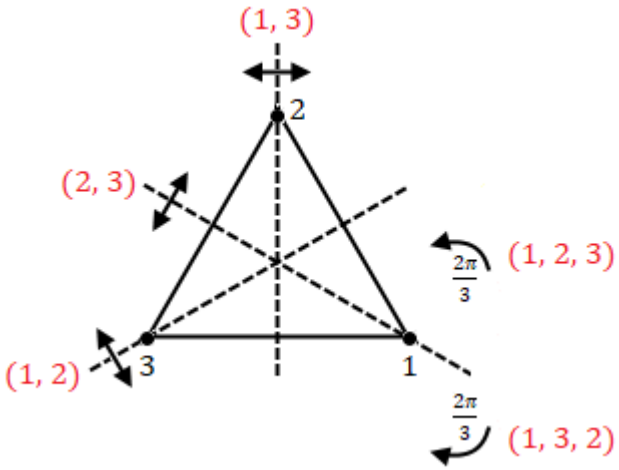


Рис. 1.3. Изоморфизм групп S_3 и D_3

и каждому движению, сохраняющему треугольник, поставим в соответствие соответствующую перестановку вершин этого треугольника (см. рис. 1.3, повороту на 0 соответствует тождественная перестановка). Понятно, что композиции движений соответствует композиция перестановок вершин.

Лекция 2. Нормальные подгруппы, факторгруппы. Основная теорема о гомоморфизмах.

Еще немного поговорим о теме, которую мы изучали в первой части курса – о подгруппах. На первой лекции мы уже использовали это понятие, но для аккуратности вспомним определение.

Определение. Подгруппа в группе G – это подмножество $H \subseteq G$, удовлетворяющее условиям:
1) Замкнутость относительно умножения:

$$g, h \in H \Rightarrow g \cdot h \in H$$

2) Содержит нейтральный элемент:

$$e \in H$$

3) Замкнутость относительно взятия обратного элемента:

$$g \in H \Rightarrow g^{-1} \in H$$

Условие 2) можно заменить на условие $H \neq \emptyset$. В самом деле, если H непусто и существует $g \in H$, то из условия 3) следует, что и $g^{-1} \in H$. Но тогда из свойства 1) следует, что и $g \cdot g^{-1} = e \in H$.

Подгруппа $H \subseteq G$ сама является группой относительно операции умножения в G, ограниченной на H.

Упражнение 1. Доказать, что если группа G конечна, то условия 2) и 3) в определении подгруппы требовать необязательно – любое непустое ее подмножество H, удовлетворяющее условию 1) является подгруппой.

Вспомним примеры подгрупп в группах, которые мы рассматривали на прошлой лекции.

Примеры подгрупп:
1) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$; операция – сложение.
2) $\mathbb{Z}^\times \subset \mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times$; операция – умножение.
3) $GL_n(K) \supset O_n(K) \supset SO_n(K)$, $GL_n(K) \supset SL_n(K)$
4) $Isom(F) \supset Isom(F)^+$, в частности, $D_n \supset R_n$
5) $S_n \supset A_n$
6) В первой половине курса также рассматривалась следующая конструкция построения подгруппы: фиксируем $g \in G$ и рассмотрим циклическую подгруппу, порожденную этим элементом:

$$H = < g > = < g^k \mid k \in \mathbb{Z} >$$

Определение. Группа G называется циклической, если она совпадает с циклической подгруппой, порожденной некоторым элементом: $G =< g >$ для некоторого $g \in G$. Элемент g называется порождающим элементом.

Вспомним основный свойства циклических групп.

Свойства циклических (под)групп:
1) Порядок циклической подгруппы равен порядку порождающего элемента (по определению, порядок элемента g – это наименьшее $m \in \mathbb{N}$, такое, что $g^m = e$, или ∞, если таких m нет):

$$H =< g > \Rightarrow |H| = o(g)$$

2) Если подгруппа имеет конечный порядок, то она изоморфна аддитивной группе кольца вычетов, а если порядок равен бесконечности, то она изоморфна $\mathbb{Z}$:

$$|H| = m < \infty \Rightarrow H = \{e, g, g^2, \cdots, g^{m-1}\} \simeq \mathbb{Z}_m$$
$$|H| = \infty \Rightarrow H \simeq \mathbb{Z}$$

3) Любая подгруппа в циклической группе – циклическая.

Продолжим вспоминать понятия, связанные с подгруппами. Если в группе G задана подгруппа H, то мы можем определить на множестве G отношение эквивалентности – отношение смежности слева по подгруппе.

Определение (смежность слева по подгруппе). Говорят, что элемент g смежен элементу g' по подгруппе H (обозначение: $g \underset{H}{\sim} g'$), если $\exists h \in H$: $g \cdot h = g'$.

В прошлом семестре мы доказывали, что смежность слева является отношением эквивалентности на G. Как любое отношение эквивалентности, оно разбивает G на попарно непересекающиеся классы эквивалентности – левые смежные классы группы G по подгруппе H:

$$g \cdot H = \{g \cdot h \mid h \in H\}$$

Свойства смежных классов:
1) Они образуют разбиение G на попарно непересекающиеся подмножества.
2) Существует биекция (сопоставляющая элементу $h \in H$ элемент $g \cdot h \in g \cdot H$):

$$H \leftrightarrow g \cdot H$$

Множество всех левых смежных классов группы G по подгруппе H обозначается G/H. Разбиение группы на смежные классы иллюстрирует рис. 2.1:

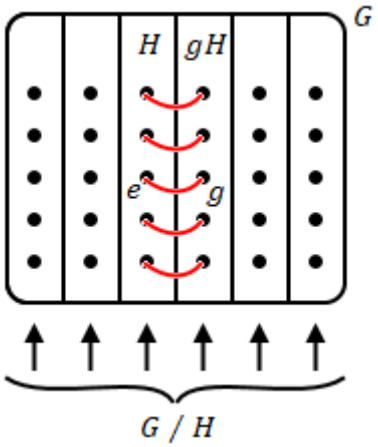


Рис. 2.1. Разбиение группы на смежные классы

Глядя на рис. 2.1, совершенно очевидной становится еще одна теорема из теории конечных групп (которая была доказана в прошлом семестре) – теорема Лагранжа.

Теорема Лагранжа. Пусть G – конечная группа, $H \subseteq G$ – подгруппа. Тогда

$$|G| = |H| \cdot |G \,/\, H|$$

Число $|G \,/\, H|$ называется индексом подгруппы H.

Из теоремы Лагранжа вытекает несколько важных следствий.

Следствие 1. Порядок подгруппы делит порядок группы: $|H|$ делит $|G|$.

Следствие 2. Порядок любого элемента в конечной группе делит порядок группы: $\forall g \in G$: $o(g)$ делит $|G|$.

Следствие 3. Если $|G| = n$, то $\forall g \in G$ выполнено $g^n = e$.

Следствие 4. Если $|G| = p$ – простое число, то $G \simeq \mathbb{Z}_p$.

Доказательство.
Выберем $g \in G, g \neq e$ и рассмотрим $H =< g >$ - циклическую подгруппу, порожденную g. Ее порядок (по следствию 1) делит порядок группы: $|H|$ делит $|G| = p$, откуда следует, что $|H| = 1$ или $|H| = p$. Вариант $|H| = 1$ невозможен, так как $H \neq \{e\}$, значит, $|H| = p$, то есть, в группе H столько же элементов, сколько и в G, поэтому $H = G$. Таким образом, G – циклическая группа порядка p. Так как все циклические группы одного порядка изоморфны друг другу, то $G \simeq \mathbb{Z}_p$. ■

Отметим, что вместо смежности слева можно рассматривать смежность справа по подгруппе H и правые смежные классы группы G по подгруппе H:

$$H \cdot g = \{h \cdot g \mid h \in H\}$$

При этом, естественно, все то, что было сказано выше про левые смежные классы, будет верно и для правых смежных классов, включая теорему Лагранжа:

$$|G| = |H| \cdot |H \setminus G|,$$

где $H \setminus G$ – множество правых смежных классов.
Отсюда сразу же следует, что количество левых смежных классов и правых смежных классов для конечных групп совпадает. На самом деле, это утверждение верно и для бесконечных групп.

Упражнение 2. Доказать, что даже для бесконечной группы G выполнено следующее: если $G \,/\, H$ конечно, то и $H \setminus G$ конечно и $|G \,/\, H| = |H \setminus G|$.

Теперь от повторения материала первой части курса перейдем к новым понятиям.

Определение. Подгруппа $H \subseteq G$ называется нормальной, если $\forall g \in G\colon\ g \cdot H = H \cdot g$. Обозначение: $H \lhd G$.

Замечание. Очевидно, что понятие нормальности содержательно только для некоммутативных групп – в абелевой группе любая подгруппа будет нормальной.

Предложение. Следующие условия эквивалентны:
1) $H \lhd G$,
2) $g \cdot H \cdot g^{-1} = H,\ \forall g \in G$
3) $g \cdot h \cdot g^{-1} \in H,\ \forall h \in H, g \in G$
Терминология: элемент $g \cdot h \cdot g^{-1}$ называется элементом, сопряженным к h, элемент g называется сопрягающим элементом.

Доказательство.
1) $\Leftrightarrow$ 2):
$\Rightarrow$: домножим равенство $g \cdot H = H \cdot g$ на g^{-1} справа, получим $g \cdot H \cdot g^{-1} = H$.
$\Leftarrow$: домножим равенство $g \cdot H \cdot g^{-1} = H$ на g справа, получим $g \cdot H = H \cdot g$.

2) $\Leftrightarrow$ 3):
$\Rightarrow$: условие 3) означает, что $g \cdot H \cdot g^{-1} \subseteq H,\ \forall g \in G$, поэтому очевидно, что 2) $\Rightarrow$ 3).
$\Leftarrow$: условие 3) означает, что $g \cdot H \cdot g^{-1} \subseteq H,\ \forall g \in G$, в частности, это условие должно выполняться и для элемента g^{-1}, то есть, $g^{-1} \cdot H \cdot g \subseteq H$. Сопрягая с g, получаем $H \subseteq g \cdot H \cdot g^{-1}$. Отсюда следует, что $g \cdot H \cdot g^{-1} = H$. ■

Свойство 3) наиболее удобно для проверки нормальности конкретной подгруппы.

Важность нормальных подгрупп заключается в том, что с их помощью можно строить новые группы из уже имеющихся в нашем распоряжении.

Определение. Факторгруппа группы G по нормальной подгруппе H – это множество смежных классов $G\ /\ H$ с операцией перемножения смежных классов как подмножеств в группе G:

$$A \cdot B = \{a \cdot b \mid a \in A, b \in B\}$$

Проверим корректность данного определения, т.е. проверим, что в результате так определенного перемножения смежных классов получается смежный класс – пусть

$$A = g \cdot H, B = g' \cdot H,$$

тогда

$$A \cdot B = g \cdot H \cdot g' \cdot H$$

Так как подгруппа H нормальная, то $H \cdot g' = g' \cdot H$, поэтому

$$A \cdot B = g \cdot g' \cdot H \cdot H = g \cdot g' \cdot H$$

- действительно получили смежный класс элемента $g \cdot g'$.

Остальные аксиомы группы (ассоциативность умножения смежных классов, наличие нейтрального и обратного элементов) вытекают из соответствующих аксиом в самой группе G. Проверим ассоциативность: пусть

$$A = g \cdot H, B = g' \cdot H, C = g'' \cdot H$$

Получаем

$$(A \cdot B) \cdot C = (gg' \cdot H) \cdot (g'' \cdot H) = (gg') \cdot g'' \cdot H = g \cdot (g'g'') \cdot H = gH \cdot (g'g'' \cdot H) =$$
$$= A \cdot (B \cdot C)$$

Нейтральный элемент:

$$e \cdot H = H$$

Обратный элемент:

$$(g \cdot H)^{-1} = g^{-1} \cdot H$$

Пример. $G = \mathbb{Z}$ - абелева циклическая группа, поэтому любая (нормальная) подгруппа в G имеет вид $H = m \cdot \mathbb{Z}$. Смежные классы – классы вычетов по модулю m:

$$k + m \cdot \mathbb{Z} = \{k + m \cdot n \mid n \in \mathbb{Z}\}$$

Факторгруппа $\mathbb{Z}/m\mathbb{Z}$ – группа вычетов по модулю m.

Отметим, что нормальные подгруппы естественно возникают в связи с гомоморфизмами групп.

Определение. Пусть $\varphi: G \to H$ – гомоморфизм групп. Его образ:

$$Im\,\varphi = \{h = \varphi(g) \mid g \in G\},$$

ядро гомоморфизма:

$$Ker\,\varphi = \{g \in G \mid \varphi(g) = e\}$$

Свойства:
1) $Im\,\varphi$ – подгруппа в H,
2) $Ker\,\varphi$ – нормальная подгруппа в G.

Доказательство.
1) Проверим, что $Im\,\varphi$ действительно подгруппа в H:

- $h, h' \in Im\,\varphi \Rightarrow h = \varphi(g), h' = \varphi(g') \Rightarrow h \cdot h' = \varphi(g \cdot g') \in Im\,\varphi$
- $h^{-1} = \varphi(g^{-1}) \in Im\,\varphi$
- $e = \varphi(e) \in Im\,\varphi$

2) Аналогично проверим, что $Ker\,\varphi$ – подгруппа в G:

- $g, g' \in Ker\,\varphi \Rightarrow \varphi(g \cdot g') = \varphi(g) \cdot \varphi(g') = e \cdot e = e \Rightarrow g \cdot g' \in Ker\,\varphi$
- $g \in Ker\,\varphi \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1} = e^{-1} = e \Rightarrow g^{-1} \in Ker\,\varphi$
- $\varphi(e) = e \Rightarrow e \in Ker\,\varphi$

Нормальность – проверим, что при сопряжении мы не выходим за пределы $Ker\,\varphi$:

$$\forall x \in Ker\,\varphi, \forall g \in G \quad \varphi(g \cdot x \cdot g^{-1}) = \varphi(g) \cdot \varphi(x) \cdot \varphi(g)^{-1} = \varphi(g) \cdot e \cdot \varphi(g)^{-1} = e$$

Таким образом, $g \cdot x \cdot g^{-1} \in Ker\,\varphi$, значит, $Ker\,\varphi$ – нормальная подгруппа в G. ■

Примеры.
1) $\varphi: \mathbb{R} \to \mathbb{C}^{\times}$, $\varphi(x) = cos(2\pi x) + i\,sin(2\pi x) = e^{2\pi i x}$
$Im\,\varphi = \{z \mid |z| = 1\} = \mathbb{U}$ – единичная окружность,
$Ker\,\varphi = \mathbb{Z}$
Этот гомоморфизм можно геометрически представить так: мы как бы наматываем действительную прямую на единичную окружность в комплексной плоскости, причем каждый отрезок длины 1 полностью наматывается на окружность без перекрытий:

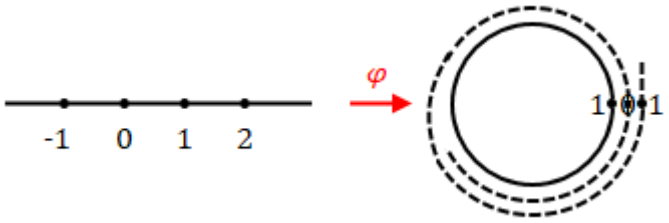


Рис. 2.2. Гомоморфизм $\varphi(x) = e^{2\pi i x}$

2) $sgn\colon S_n \to \mathbb{R}^\times$ - отображение знака подстановки в $\mathbb{R}^\times$
$Im(sgn) = \{\pm 1\}$
$Ker(sgn) = A_n$

3) $det\colon GL_n(K) \to K^\times$ - определитель
$Im(det) = K^\times$
$Ker(det) = SL_n(K)$

4) Пусть $H \lhd G$. Каноническая проекция:

$$\pi\colon G \to G \,/\, H$$
$$g \mapsto g \cdot H$$

(т.е. мы каждому элементу группы ставим в соответствие смежный класс, которому он принадлежит). Каноническая проекция является гомоморфизмом групп (следует из правила перемножения смежных классов).

$$Im\,\pi = G \,/\, H$$
$$Ker\,\pi = H$$

Таким образом, любая нормальная подгруппа является ядром некого гомоморфизма. Ранее мы доказали, что ядро любого гомоморфизма является нормальной подгруппой. Это дает нам еще одну характеризацию нормальных подгрупп: нормальные подгруппы – это то же самое, что и ядра гомоморфизмов.
Закончим лекцию теоремой, которая описывает структуру любого гомоморфизма.

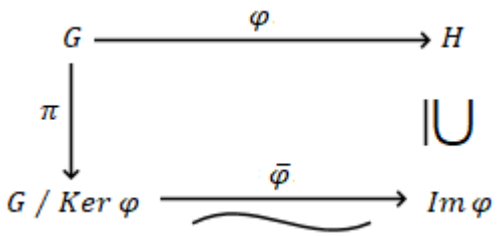
Основная теорема о гомоморфизмах групп. Пусть $\varphi\colon G \to H$ – гомоморфизм групп. Тогда $\exists!$ изоморфизм

$$\bar{\varphi}\colon\ G \,/\, Ker\,\varphi \Rightarrow Im\,\varphi,$$

для которого $\varphi = \bar{\varphi} \circ \pi$, где $\pi\colon G \to G \,/\, Ker\,\varphi$ – каноническая проекция. Другими словами,

$$\varphi(g) = \bar{\varphi}(g \cdot Ker\,\varphi)$$

Еще короче теорему можно сформулировать с помощью коммутативной диаграммы:



Доказательство.
Для краткости обозначим $K = Ker\,\varphi$.

Утверждение. Прообразы элементов группы H при отображении φ – это то же самое, что и смежные классы по ядру гомоморфизма φ:

$$h \in Im\,\varphi\,, h = \varphi(g) \Rightarrow \varphi^{-1}(h) = g \cdot K$$

Доказательство утверждения.
$\forall g' \in G$ рассмотрим $k = g^{-1} \cdot g'$. Тогда $g' = g \cdot k$. Поймем, при каком условии g' лежит в прообразе элемента h:

$$\varphi(g') = \varphi(g) \cdot \varphi(k) = h \cdot \varphi(k) = h \Leftrightarrow \varphi(k) = e \Leftrightarrow k \in K$$

- тогда и только тогда, когда k лежит в ядре гомоморфизма φ. Таким образом, элементы из прообраза h - это в точности элементы из $g \cdot K$ и утверждение доказано.
Проиллюстрируем:

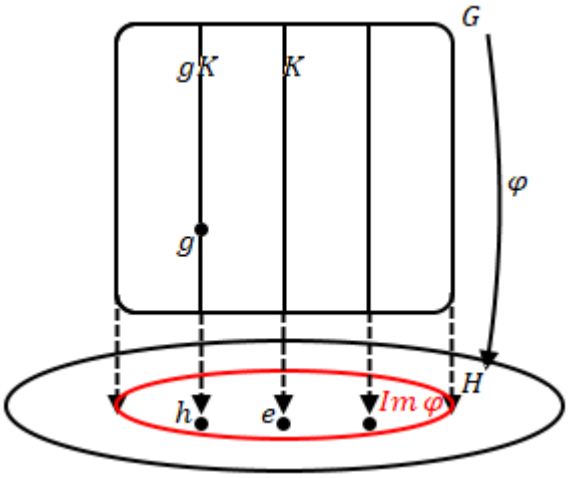


Рис. 2.3. Иллюстрация к основной теореме о гомоморфизмах

- группа G “расслаивается” на смежные классы, которые соответствуют точкам из образа φ. Отсюда следует существование отображения $\bar{\varphi}$: $G\,/\,K \to Im\,\varphi$, его биективность и единственность (так как формула $\varphi(g) = \bar{\varphi}(g \cdot Ker\,\varphi)$ задает $\bar{\varphi}$ однозначно). Осталось проверить, что $\bar{\varphi}$ – гомоморфизм, но это вытекает из определения умножения в факторгруппе – так как:

$$gK \cdot g'K = gg' \cdot K,$$

то

$$\bar{\varphi}(gg' \cdot K) = \varphi(gg') = \varphi(g) \cdot \varphi(g') = \bar{\varphi}(gK) \cdot \bar{\varphi}(g'K)$$

Таким образом, $\bar{\varphi}$ – биективный гомоморфизм, т.е. изоморфизм. ■

Лекция 3. Основная теорема о гомоморфизмах. Автоморфизмы групп.

На прошлой лекции мы доказали основную теорему о гомоморфизмах – она, в частности, утверждает, что

$$G \,/\, Ker\,\varphi \simeq Im\,\varphi$$

Этот факт удобно использовать для вычисления факторгрупп (т.е. для понимания, каким группам понятной структуры изоморфна факторгруппа).

Вычисление факторгрупп: пусть $G \rhd K$, $G \,/\, K \simeq ?$

1) Строим гомоморфизм $\varphi: G \to H$ так, чтобы $Ker\,\varphi = K$.
2) Ищем образ этого гомоморфизма $Im\,\varphi \subseteq H$ – это будет подгруппа в группе H.
3) $G \,/\, K \simeq Im\,\varphi$.

Рассмотрим, что получается в примерах из прошлой лекции.

Примеры.
1) $\mathbb{R} \,/\, \mathbb{Z} \simeq ?$
Для вычисления факторгруппы необходимо рассмотреть гомоморфизм из $\mathbb{R}$ в какую-то группу, ядром которого является $\mathbb{Z}$. Такой гомоморфизм мы строили на прошлой лекции:

$$\varphi: \mathbb{R} \to \mathbb{C}^{\times}, \quad \varphi(x) = e^{2\pi i x}$$

Его ядро и образ:
$Ker\,\varphi = \mathbb{Z}$,
$Im\,\varphi = \{z \mid |z| = 1\} = \mathbb{U}$ – единичная окружность на комплексной плоскости.
По основной теореме о гомоморфизмах,

$$\mathbb{R} \,/\, \mathbb{Z} \simeq \mathbb{U}$$

2) $S_n \,/\, A_n \simeq ?$
Конечно, ответ на этот вопрос затруднений не вызывает – это группа из двух элементов (по теореме Лагранжа). Так как группа простого порядка, то она циклическая. Для наглядности применим основную теорему о гомоморфизмах – рассмотрим гомоморфизм

$$sgn: S_n \to \mathbb{R}^{\times}$$

Его ядро и образ:
$Ker(sgn) = A_n$,
$Im(sgn) = \{\pm 1\}$
По основной теореме о гомоморфизмах,

$$S_n \,/\, A_n \simeq \{\pm 1\}$$

3) $GL_n(K) \,/\, SL_n(K) \simeq ?$
Для вычисления факторгруппы необходимо рассмотреть гомоморфизм из $GL_n(K)$ в какую-то группу, ядром которого является $SL_n(K)$. Такой гомоморфизм мы строили на прошлой лекции:

$$det: GL_n(K) \to K^{\times}$$

Его ядро и образ:
$Ker(det) = SL_n(K)$
$Im(det) = K^\times$
По основной теореме о гомоморфизмах,

$$GL_n(K) \,/\, SL_n(K) \simeq K^\times$$

Рассмотрим еще несколько примеров:

4) Пусть $\varphi\colon \mathbb{Z} \to \mathbb{C}^\times$ - гомоморфизм, который ставит в соответствие целому числу k k-ый по счету корень степени m из единицы ($m \in \mathbb{N}$ фиксировано):

$$\varphi(k) = \cos\frac{2\pi k}{m} + i\sin\frac{2\pi k}{m} = e^{\frac{2\pi k i}{m}}$$

Образ φ – это группа всех комплексных корней степени m из единицы:
$Im\,\varphi = \mathbb{U}_m$
Ядро φ – это целые числа, кратные m:
$Ker\,\varphi = m\mathbb{Z}$
По основной теореме о гомоморфизмах,

$$\mathbb{Z} \,/\, m\mathbb{Z} = \mathbb{Z}_m \simeq \mathbb{U}_m$$

5) $\mathbb{C}^\times \,/\, \mathbb{U} \simeq ?$
Для вычисления факторгруппы необходимо рассмотреть гомоморфизм из $\mathbb{C}^\times$ в какую-то группу, ядром которого является $\mathbb{U}$. В качестве такого гомоморфизма рассмотрим

$$\varphi\colon \mathbb{C}^\times \to \mathbb{R}^\times, \varphi(z) = |z|$$

- это действительно гомоморфизм групп (по свойству модуля комплексных чисел).
Его ядро и образ:
$Ker\,\varphi = \mathbb{U}$
$Im(det) = \mathbb{R}^+$ - все положительные действительные числа
По основной теореме о гомоморфизмах,

$$\mathbb{C}^\times \,/\, \mathbb{U} \simeq \mathbb{R}^+$$

Рассмотрим еще одно применение основной теоремы о гомоморфизмах – докажем с помощью нее теорему, которую удобно применять при изучении структуры групп. Эту теорему иногда называют второй теоремой об изоморфизме групп, а основную теорему о гомоморфизмах групп – первой теоремой об изоморфизме групп.

Теорема. Пусть G – группа, $H, N \subseteq G$ – подгруппы, причем $N \lhd G$. Тогда:

- $H \cdot N = \{h \cdot n \mid h \in H, n \in N\} = N \cdot H$ –наименьшая подгруппа, содержащая H и N
- $H \cdot N \,/\, N \simeq H \,/\, H \cap N$

Доказательство.
Поймем, что $H \cdot N = N \cdot H$. Рассмотрим $H \cdot N = \{h \cdot n \mid h \in H, n \in N\}$. Зафиксировав h и меняя n, получим левый смежный класс элемента h по подгруппе N. Тогда $H \cdot N$ есть объединение таких левых смежных классов:

$$H \cdot N = \bigcup_{h \in H} h \cdot N$$

Так как подгруппа N нормальна, то $h \cdot N = N \cdot h$ и

$$H \cdot N = \bigcup_{h \in H} h \cdot N = \bigcup_{h \in H} N \cdot h \; = N \cdot H$$

Докажем, что $H \cdot N$ – подгруппа:
1) содержит единицу:

$$H \cdot N \ni e \cdot e = e,$$

2) замкнутость относительно умножения:

$$(H \cdot N) \cdot (H \cdot N) = H \cdot (N \cdot H) \cdot N = H \cdot (N \cdot H) \cdot N = (H \cdot H) \cdot (N \cdot N) = H \cdot N$$

3) замкнутость относительно взятия обратного элемента:

$\forall g \in H \cdot N$ выполнено $g = h \cdot n$, где $h \in H, n \in N$. Тогда $g^{-1} = n^{-1} \cdot h^{-1} \in N \cdot H = H \cdot N$

Очевидно, что $H \cdot N$ содержится в любой подгруппе, содержащей H и N. Так как $H \cdot N$ – подгруппа, то это – наименьшая подгруппа, содержащая H и N.

Для доказательства теоремы осталось доказать, что $H \cdot N \,/\, N \simeq H \,/\, H \cap N$. Для этого воспользуемся основной теоремой о гомоморфизмах. Рассмотрим каноническую проекцию

$$G \xrightarrow{\pi} G \,/\, N$$

Образ подгруппы $H \cdot N \subseteq G$ при ограничении гомоморфизма π на эту подгруппу равен:

$$\pi(H \cdot N) = H \cdot N \,/\, N$$

Образ подгруппы $H \subseteq H \cdot N$ при ограничении гомоморфизма π на эту подгруппу равен:

$$\pi(H) = \pi(H \cdot N) = H \cdot N \,/\, N$$

(так как в любом смежном классе элемента из $H \cdot N$ есть представитель, лежащий в H).

Изобразим происходящее на диаграмме:

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G\,/\,N \\ \cup & & \cup \\ H \cdot N & \xrightarrow{\pi|_{H\cdot N}} & \pi(H \cdot N) = H \cdot N\,/\,N \\ \cup & & \| \\ H & \xrightarrow{\pi|_{H}} & \pi(H) \end{array}$$

Теперь можно применить основную теорему о гомоморфизмах, так как $Ker\,\pi|_H = H \cap N$ (в самом деле, элементы, лежащие в $Ker\,\pi|_H$ – это элементы, которые отображаются в единицу группы $G\,/\,N$, но элементы, которые отображаются в единицу при канонической проекции – это элементы группы N, но они также должны лежать и в H, так как мы рассматриваем $\pi|_H$).
По основной теореме о гомоморфизмах,

$$Im(\pi|_H) = \pi(H) \simeq H\,/\,H \cap N$$

Теорема доказана. ■

Продолжим изучение гомоморфизмов – рассмотрим гомоморфизмы группы в себя.

Определение. Эндоморфизм группы G – это гомоморфизм $\varphi\colon G \to G$.

Определение. Автоморфизм группы G – это изоморфизм $\varphi\colon G \twoheadrightarrow G$.

Множество всех автоморфизмов группы G (обозначение: $Aut\ G$) само является группой относительно операции композиции автоморфизмов – это подгруппа в группе всех преобразований множества G: $Aut\ G \subseteq S(G)$. Группа $Aut\ G$ является важной характеристикой группы G – она показывает, какими внутренними симметриями обладает группа G (т.е. преобразованиями, которые сохраняют структуру группы). Посмотрим, как устроены автоморфизмы простейших групп – циклических.

Предложение 1.

1)Конечные циклические группы.
Все конечные циклические группы одного порядка изоморфны друг другу, поэтому в качестве представителя можно взять группу $\mathbb{Z}_m$ вычетов по модулю m с операцией сложения. Тогда

$$Aut\ \mathbb{Z}_m \simeq \mathbb{Z}_m{}^{\times} = \{k\ mod\ m \mid \text{НОД}\ (k, m) = 1\}$$

2) Бесконечные циклические группы

Все бесконечные циклические группы изоморфны группе целых чисел $\mathbb{Z}$ с операцией сложения. Тогда

$$Aut\,\mathbb{Z} \simeq \mathbb{Z}^{\times} = \{\pm 1\}$$

Доказательство.

1) Для краткости вместо $k\,mod\,m$ будем писать $\bar{k}$. Рассмотрим произвольный эндоморфизм

$$\varphi\colon \mathbb{Z}_m \to \mathbb{Z}_m$$

Пусть при этом эндоморфизме порождающий элемент $\mathbb{Z}_m$ переходит в $\bar{k}$: $\varphi(1) = \bar{k}$. Тогда произвольный вычет $\bar{n}$ этот эндоморфизм отображает в $\bar{k} \cdot \bar{n}$ (можно считать, что $0 \le n \le m-1$):

$$\varphi(\bar{n}) = \varphi(\bar{1} + \cdots + \bar{1}) = \varphi(\bar{1}) + \cdots + \varphi(\bar{1}) = \bar{k} + \cdots + \bar{k} = \overline{k \cdot n} = \bar{k} \cdot \bar{n}$$

- таким образом, φ – умножение на $\bar{k}$. Иными словами, если мы знаем, куда при энодоморфизме переходит порождающий элемент циклической группы, то этот эндоморфизм определен однозначно – это эндоморфизм умножения на образ порождающего элемента.

Обратно, для $\forall \bar{k} \in \mathbb{Z}_m$ операция умножения на этот элемент (то есть, отображение $\varphi\colon \mathbb{Z}_m \to \mathbb{Z}_m$, которое задается правилом $\varphi(\bar{n}) = \bar{k} \cdot \bar{n}$) всегда будет эндоморфизмом. Действительно,

$$\varphi(\bar{n}_1 + \bar{n}_2) = \bar{k} \cdot (\bar{n}_1 + \bar{n}_2) = \bar{k} \cdot \bar{n}_1 + \bar{k} \cdot \bar{n}_2 = \varphi(\bar{n}_1) + \varphi(\bar{n}_2)$$

Пусть $\psi\colon \mathbb{Z}_m \to \mathbb{Z}_m$ – другой эндоморфизм. Это тоже будет операция умножения на фиксированный вычет:

$$\psi(\bar{n}) = \bar{l} \cdot \bar{n}$$

Тогда

$$\varphi \circ \psi(\bar{n}) = \bar{k} \cdot \left(\bar{l} \cdot \bar{n}\right) = \left(\bar{k} \cdot \bar{l}\right) \cdot \bar{n}$$

То есть, $\varphi \circ \psi$ – умножение на $\bar{k} \cdot \bar{l}$. Таким образом, мы получили взаимно-однозначное соответствие между всеми эндоморфизмами и всеми вычетами, причем произведению соответствует произведение.

φ – автоморфизм $\Leftrightarrow \exists \psi = \varphi^{-1}\colon\ \varphi \circ \psi = \psi \circ \varphi = id$. Если φ задается множителем $\bar{k}$, а ψ задается множителем $\bar{l}$, то их композиция задается множителем $\bar{k} \cdot \bar{l}$. Равенство $\varphi \circ \psi = \psi \circ \varphi = id$ будет выполнено при условии $\bar{k} \cdot \bar{l} = 1$. Таким образом, обратный эндоморфизм к φ существует тогда и только тогда, когда в кольце вычетов существует множитель, обратный к вычету $\bar{k}$ (когда вычет $\bar{k}$ обратим: $\bar{k} \in \mathbb{Z}_m{}^{\times}$).

Таким образом, мы получаем биекцию между всеми автоморфизмами и всеми обратимыми вычетами:

$$Aut\,\mathbb{Z}_m \simeq \mathbb{Z}_m{}^{\times}$$
$$\varphi \leftrightarrow \varphi(\bar{1}) = \bar{k}$$

- изоморфизм групп.

2) Для случая бесконечных циклических групп доказательство проводится аналогично. Не будем проводить его подробно, остановимся лишь на нескольких ключевых моментах.
Любой эндоморфизм $\varphi: \mathbb{Z} \to \mathbb{Z}$ задается умножением на некоторый множитель: пусть $\varphi(1) = k$, тогда
при $n > 0$:

$$\varphi(n) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = k + \cdots + k = k \cdot n$$

при $n < 0$:

$$\varphi(n) = \varphi(-1 + \cdots + (-1)) = \varphi(-1) + \cdots + \varphi(-1) = -k + \cdots + (-k) = -k \cdot n$$

при $n = 0$:

$$\varphi(n) = 0 = k \cdot 0$$

Таким образом, получаем что $\varphi(n)$ – операция умножения на $k = \varphi(1)$.

Далее аналогично пункту 1) доказываем, что φ – автоморфизм $\Leftrightarrow k \in \mathbb{Z}^{\times} = \{\pm 1\}$.

Наконец, аналогично пункту 1) доказываем, что композиции авто- (эндо-) морфизмов соответствует произведение множителей, которые задают эти эндоморфизмы. ■

Итак, мы рассмотрели, как устроены автоморфизмы простейших групп – циклических. В общем случае группа автоморфизмов устроена более сложно, однако среди всех автоморфизмов данной группы G можно выделить такие, которые задаются как бы самой структурой группы G.

Определение. Пусть $g \in G$. Внутренний автоморфизм $i_g: G \Rightarrow G$ определяется следующим образом:

$$i_g(x) = g \cdot x \cdot g^{-1}, \forall x \in G$$

Другими словами, внутренний автоморфизм, задаваемый элементом $g \in G$ – это операция сопряжения с этим элементом. Убедимся, что это действительно автоморфизм:

- биективность: $(i_g)^{-1} = i_{g^{-1}}$
- эндоморфизм: $i_g(x \cdot y) = g \cdot x \cdot y \cdot g^{-1} = g \cdot x \cdot g^{-1} \cdot g \cdot y \cdot g^{-1} = i_g(x) \cdot i_g(y)$

- действительно, каждая операция сопряжения является биективным гомоморфизмом группы на себя, то есть, автоморфизмом.

Предложение 2.
1) Отображение

$$i: G \to Aut\ G$$
$$g \mapsto i_g$$

- гомоморфизм групп.

2)

$$Im\, i = Inn\, G \lhd Aut\, G$$

3)

$$Ker\, i = Z(G) = \{g \in G \mid g \cdot x = x \cdot g, \forall x \in G\}$$

- центр группы G.

4)

$$Inn\, G \simeq G/Z(G)$$

Доказательство.

1) Проверим, что отображение i является гомоморфизмом групп:

$$i_{gh}(x) = (gh) \cdot x \cdot (gh)^{-1} = g \cdot h \cdot x \cdot h^{-1} \cdot g^{-1} = i_g(i_h(x)), \qquad \forall x \in G$$

Следовательно,

$$i_{gh} = i_g \circ i_h$$

- отображение i переводит произведение элементов группы G в композицию соответствующих внутренних автоморфизмов, значит, i - гомоморфизм.

2) Для проверки нормальности группы $Inn\, G$ воспользуемся следующим свойством: вместе с каждым элементом нормальная подгруппа должна содержать и все его сопряженные.

$\forall g \in G, \forall \varphi \in Aut\, G$

$$\varphi \circ i_g \circ \varphi^{-1}(x) = \varphi(g \cdot \varphi^{-1}(x) \cdot g^{-1}) = \varphi(g) \cdot \varphi\left(\varphi^{-1}(x)\right) \cdot \varphi(g^{-1}) =$$
$$= \varphi(g) \cdot x \cdot \varphi(g)^{-1} = i_{\varphi(g)}(x)$$

Следовательно,

$$\varphi \circ i_g \circ \varphi^{-1} = i_{\varphi(g)} \in Inn\, G \Rightarrow Inn\, G \lhd Aut\, G$$

3)

$$g \in Ker\, i \Leftrightarrow i_g = id$$

Другими словами,

$$g \cdot x \cdot g^{-1} = x, \qquad \forall x \in G$$

Домножим справа на g:

$$g \cdot x = x \cdot g, \qquad \forall x \in G$$

Следовательно, $Ker\, i = Z(G)$.

4) Следует из пункта 3) и основной теоремы о гомоморфизмах. ■

Замечание 1. Рассмотрим группу “внешних автоморфизмов”:

$$Aut\, G/Inn\, G \simeq Out\, G$$

Эта группа “измеряет”, какие у группы G есть симметрии, которые не происходят непосредственно из умножения в группе G (которые не являются внутренними автоморфизмами).

Замечание 2. Если группа G абелева, то ее центр совпадает со всей группой и внутренних автоморфизмов нет (кроме тождественного).
Обратное тоже верно: поскольку $Inn\ G \simeq G/Z(G)$, то $Inn\ G$ является тривиальной тогда и только тогда, когда $Z(G) = G$, а это эквивалентно тому, что группа G является абелевой:

$$G \text{ абелева} \Leftrightarrow Z(G) = G \Leftrightarrow Inn\ G = \{id\}$$

Таким образом, интерес представляет только группа внутренних изоморфизмов у неабелевых групп. Устройство этой группы может быть разнообразным – например, если центр тривиален, то $Inn\ G \simeq G$ – группа внутренних изоморфизмов устроена так же, как и сама группа G. Однако, можно указать одно общее свойство.

Предложение 3. Если группа G неабелева, то ее группа внутренних изоморфизмов $Inn\ G$ не может быть циклической.

Доказательство.
Для краткости обозначим центр группы $Z(G) = Z$. Тогда (следует из п.4 предложения 2) $Inn\ G \simeq G/Z$. Докажем от противного, что G/Z не циклическая.
Пусть $G/Z =< gZ >$. Тогда любой элемент G/Z является некоторой степенью gZ:

$$\forall x \in G\ \exists k \in \mathbb{Z}\colon\ xZ = (gZ)^k = g^kZ$$

То есть, если G/Z циклическая, то всякий элемент группы G представляется в виде произведения некоторого элемента из центра на степень фиксированного элемента: $x = g^k \cdot z$. Это невозможно, так как все элементы такого вида коммутируют между собой: пусть $x_1, x_2 \in G$, тогда $x_1 = g^{k_1} \cdot z_1$, $x_2 = g^{k_2} \cdot z_2$, $k_i \in \mathbb{Z}, z_i \in Z$ и

$$x_1 \cdot x_2 = g^{k_1} \cdot z_1 \cdot g^{k_2} \cdot z_2 = g^{k_1} \cdot g^{k_2} \cdot z_1 \cdot z_2 = g^{k_1+k_2} \cdot z_1 \cdot z_2 = g^{k_2} \cdot g^{k_1} \cdot z_2 \cdot z_1 = \\ = g^{k_2} \cdot z_2 \cdot g^{k_1} \cdot z_1 = x_2 \cdot x_1$$

Следовательно, G абелева, что противоречит условию. ■

Лекция 4. Прямое произведение.

На этой лекции мы рассмотрим структуру прямого произведения, которая позволяет сводить изучение более сложных групп к более простым и строить новые группы из уже имеющихся.

Определение. Пусть G – группа, $A, B \subseteq G$ – подгруппы. G есть прямое произведение (внутреннее) подгрупп A и B (обозначение: $G = A \times B$), если:

- $G = A \cdot B$,
- $A, B \lhd G$,
- $A \cap B = \{e\}$

Свойства разложения группы в прямое произведение:

Свойство 1. A и B коммутируют между собой: $\forall a \in A, b \in B\colon\ a \cdot b = b \cdot a$

Доказательство.
Рассмотрим элемент $a \cdot b \cdot a^{-1} \cdot b^{-1} = [a, b]$ – коммутатор элементов a и b.
Основное свойство коммутатора:

$$a \cdot b = [a, b] \cdot b \cdot a$$

Другими словами, коммутатор – “поправочный множитель”, который нужно добавить, чтобы равенство $a \cdot b = b \cdot a$ сохранялось для некоммутирующих элементов. В частности, из основного свойства коммутатора вытекает, что $a \cdot b = b \cdot a \Leftrightarrow [a, b] = e$.

Для доказательства нашего свойства сгруппируем множители в коммутаторе двумя способами:
1) $[a, b] = a \cdot (b \cdot a^{-1} \cdot b^{-1})$
Рассмотрим произведение $b \cdot a^{-1} \cdot b^{-1}$ – это сопряжение элемента a^{-1}, значит, $b \cdot a^{-1} \cdot b^{-1} \in A$, так как $A \lhd G$. Так как $a \in A$, то и $[a, b] = a \cdot b \cdot a^{-1} \cdot b^{-1} \in A$.
2) $[a, b] = (a \cdot b \cdot a^{-1}) \cdot b^{-1}$
Рассмотрим произведение $a \cdot b \cdot a^{-1}$ – это сопряжение элемента b, значит, $a \cdot b \cdot a^{-1} \in B$, так как $B \lhd G$. Так как $b \in B$, то и $[a, b] = a \cdot b \cdot a^{-1} \cdot b^{-1} \in B$.

Таким образом, $[a, b] \in A \cap B = \{e\}$, поэтому $a \cdot b = b \cdot a$ для $\forall a \in A, b \in B$. ■

Свойство 2. Любой элемент группы G единственным способом разлагается в произведение элементов из A и B: $\forall g \in G\ \exists!\ a \in A, b \in B\colon\ g = a \cdot b$.

Доказательство.
Существование такого разложения следует из определения прямого произведения: $G = A \cdot B$. Единственность разложения доказывается следующим образом: предположим, существует два разложения:

$$g = a \cdot b = a' \cdot b', \text{ где } a, a' \in A,\ b, b' \in B$$

Домножив слева на $(a')^{-1}$, справа на b^{-1}, получим

$$(a')^{-1} \cdot a = b' \cdot b^{-1}$$

В левой части равенства находится элемент из A, в правой части равенства – из B, значит, оба этих элемента находятся в пересечении $A \cap B = \{e\}$, из чего можно заключить, что $a' = a$ и $b' = b$, то есть, разложение единственно. ■

Свойство 3. Если $g_1 = a_1 \cdot b_1, g_2 = a_2 \cdot b_2\ \ (a_i \in A, b_i \in B, i = 1,2)$, то (по свойству 1):

$$g_1 \cdot g_2 = a_1 \cdot b_1 \cdot a_2 \cdot b_2 = (a_1 \cdot a_2) \cdot (b_1 \cdot b_2)$$

Другими словами, при перемножении двух элементов группы G, разложенных по сомножителям прямого произведения, достаточно отдельно перемножить компоненты этого разложения.

Из этих свойств следует, что структура умножения в группе G полностью определяется тем, как устроено умножение в подгруппах A и B. Сама группа G также полностью задается подгруппами A и B в том смысле, что каждый элемент $g \in G$ однозначно задается парой элементов из этих подгрупп. Таким образом, структура G полностью сводится к структурам A и B, и это наблюдение подсказывает другой вариант определения прямого произведения – мы можем определить прямое произведение не подгрупп в какой-то объемлющей группе, а отдельно взятых групп.

Определение. Прямое произведение (внешнее) групп A и B – это множество пар:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

на котором задана структура группы с помощью операции умножения:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

Проверим корректность определения (т.е. что так определенное множество действительно является группой):

- Ассоциативность: следует из ассоциативности умножения в A и B
- Нейтральный элемент: (e_A, e_B)
- Обратный элемент: $(a, b)^{-1} = (a^{-1}, b^{-1})$

Понятия внутреннего и внешнего прямого произведения эквивалентны:

а) Внутреннее прямое произведение $G = A \cdot B$ изоморфно внешнему – следует из свойств 2) и 3) внутреннего прямого произведения
б) Внешнее прямое произведение $A \times B$ является и внутренним:

$$A \times B = (A \times \{e\}) \times (\{e\} \times B)$$

Действительно:

- $(a, b) = (a, e) \cdot (e, b)$
- Нормальность A и B следует из того, что при сопряжении пар (a, e) всегда получаются пары того же вида; аналогично с парами вида (e, b)
- $(A \times \{e\}) \cap (\{e\} \times B) = (e_A, e_B)$

Говоря о прямых произведениях, мы использовали мультипликативную терминологию теории групп, можно использовать и аддитивную терминологию – тогда вместо прямого произведения $A \times B$ говорят о прямой сумме групп $A \oplus B$.

Предупреждение: не путать прямое произведение × с тензорным произведением $\otimes$.

Примеры.
1) Аддитивная группа комплексных чисел является прямой суммой группы действительных чисел и группы чисто мнимых чисел:

$$\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$$

Это действительно будет прямой суммой:

- любое комплексное число z разлагается в сумму действительного и чисто мнимого (алгебраическая форма записи комплексных чисел: $z = x + iy$, $x = Re(z), y = Im(z)$)
- подгруппы $\mathbb{R}$ и $i\mathbb{R}$ нормальны, так как $\mathbb{C}$ - абелева группа
- $\mathbb{R}$ и $i\mathbb{R}$ пересекаются только по нейтральному элементу 0 – очевидно

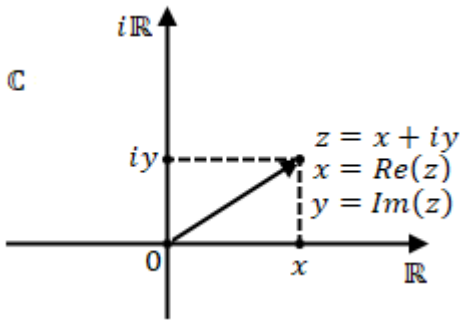


Рис. 4.1. $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$

2) Аналогично мультипликативная группа комплексных чисел раскладывается в прямое произведение групп $\mathbb{R}^+$ и $\mathbb{U}$:

$$\mathbb{C}^\times = \mathbb{R}^+ \times \mathbb{U}$$

Действительно:

- каждое ненулевое комплексное число может быть представлено в виде произведения модуля (положительного числа $r = |z|$) и тригонометрической части ($e^{i\varphi}$ – числа, по модулю равного 1, $\varphi = Arg(z)$) – это тригонометрическая форма записи комплексных чисел: $z = r \cdot e^{i\varphi}$
- подгруппы $\mathbb{R}^+$ и $\mathbb{U}$ нормальны, так как $\mathbb{C}^\times$ - абелева группа
- $\mathbb{R}^+$ и $\mathbb{U}$ пересекаются только по нейтральному элементу 1 – очевидно (пересечение единичной окружности с положительным лучом)

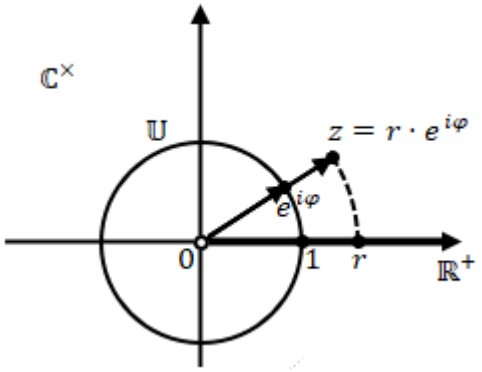


Рис. 4.2. $\mathbb{C} = \mathbb{R}^+ \times \mathbb{U}$

Заметим, что понятие прямого произведения (как внутреннего, так и внешнего) обобщается на случай любого конечного числа сомножителей.

Определение. Группа G есть (внутреннее) прямое произведение своих подгрупп $G_1, \dots, G_s$, (обозначение: $G = G_1 \times \dots \times G_s$), если:

- $\forall g \in G \quad \exists!\ g_1 \in G_1, \dots, g_s \in G_s\colon\ g = g_1 \cdot \dots \cdot g_S$
- $\forall g_i \in G_i, g_j \in G_j,\ \ i, j \in \{1, \dots, s\}, i \neq j$ выполнено $g_i \cdot g_j = g_j \cdot g_i$

Свойства прямого произведения:

Свойство 1. Если $g = g_1 \cdot \dots \cdot g_S$ и $h = h_1 \cdot \dots \cdot h_S$, где $g_i, h_i \in G_i, \forall i = 1, \dots, s$, то (так как сомножители из разных подгрупп коммутируют):

$$g \cdot h = g_1 \cdot \dots \cdot g_S \cdot h_1 \cdot \dots \cdot h_S = (g_1 \cdot h_1) \cdot \dots \cdot (g_S \cdot h_S)$$

Другими словами, при перемножении двух элементов группы G, разложенных по сомножителям прямого произведения, достаточно отдельно перемножить компоненты этого разложения.

Свойство 2. $G_i \lhd G$ $(\forall i = 1, \dots, s)$.

Доказательство.
Достаточно проверить, что вместе с каждым элементом $h \in G_i$ в G_i содержится и сопряженный ему элемент. Для $\forall h \in G_i, \forall g \in G, g = g_1 \cdot \ldots \cdot g_S$ $(g_j \in G_j)$ выполнено:

$$g \cdot h \cdot g^{-1} = g_1 \cdot \ldots \cdot g_i \cdot \ldots \cdot g_S \cdot h \cdot {g_S}^{-1} \cdot \ldots \cdot {g_i}^{-1} \cdot \ldots \cdot {g_1}^{-1}$$

Теперь воспользуемся свойством 1 (сгруппируем сомножители):

$$g \cdot h \cdot g^{-1} = (g_1 \cdot {g_1}^{-1}) \cdot \ldots \cdot (g_i \cdot h \cdot {g_i}^{-1}) \cdot \ldots \cdot (g_S \cdot {g_S}^{-1}) = g_i \cdot h \cdot {g_i}^{-1} \in G_i \ \blacksquare$$

Свойство 3. $G_i \cap G_j = \{e\}$ при $i \neq j$.

Доказательство.
Пусть $g \in G_i \cap G_j$. Тогда

$$\begin{array}{ccccccccccccccc} g & = & e & \cdot \ldots \cdot & g & \cdot \ldots \cdot & e & \cdot \ldots \cdot & e & = & e & \cdot \ldots \cdot & e & \cdot \ldots \cdot & g & \cdot \ldots \cdot & e \\ & & \cap & & \cap & & \cap & & \cap & & \cap & & \cap & & \cap & & \cap \\ & & G_1 & & G_i & & G_j & & G_s & & G_1 & & G_i & & G_j & & G_s \end{array}$$

Так как каждый элемент $g \in G$ единственным образом разлагается в произведение сомножителей из G_k, то оба этих разложения должны совпадать, поэтому $g = e$. ■

Замечание. При $S > 2$ свойств 2 и 3 недостаточно, чтобы произведение $G = G_1 \cdot \ldots \cdot G_s$ было прямым. Контрпример: $G = \mathbb{R}^2$ с операцией сложения.

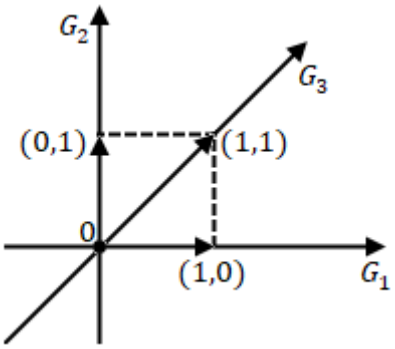


Рис. 4.3. Контрпример: $G = G_1 + G_2 + G_3$

Очевидно, что $G = G_1 + G_2 + G_3$, где G_1 – ось абсцисс, G_2 – ось ординат, G_3 – биссектриса первой и третьей четверти (любой вектор плоскости может быть представлен в виде суммы векторов из G_1, G_2 и G_3) и выполнены условия 2 и 3: эти группы нормальны, так как группа G абелева и $G_i \cap G_j = \{e\}$ при $i \neq j$. Но $G \neq G_1 \oplus G_2 \oplus G_3$, так как разложение по слагаемым не единственно, например:

$$(1,0) + (0,1) + (0,0) = (0,0) + (0,0) + (1,1)$$

- два разных разложения одного и того же элемента.

Упражнение 1. Произведение $G = G_1 \cdot \ldots \cdot G_s$ является прямым ,если выполнены свойства 2 и 3′: $G_i \cap G_1 \cdot \ldots \cdot G_{i-1} \cdot G_{i+1} \cdot \ldots \cdot G_s = \{e\}$ для $\forall i = 1, \ldots, s$.

Свойство 4. Прямое произведение можно определять индуктивно:

$$G_1 \times \ldots \times G_s = (G_1 \times \ldots \times G_{s-1}) \times G_s$$

Доказательство.
Строгое доказательство оставляется читателю. Идеи: во-первых, очевидно, что

$$G_1 \cdot \ldots \cdot G_s = (G_1 \cdot \ldots \cdot G_{s-1}) \cdot G_s$$

Далее проверим, что если левая часть этого равенства – прямое произведение, то правая – тоже прямое произведение (и наоборот).

Условие 2 из определения прямого произведения ($\forall g_i \in G_i, g_j \in G_j,\ \ i,j \in \{1,\ldots,s\}, i \neq j$ выполнено $g_i \cdot g_j = g_j \cdot g_i$) слева и справа равносильно.
Условие 1 из определения прямого произведения (единственность разложения $g = g_1 \cdot \ldots \cdot g_{s-1} \cdot g_s$) также слева и справа равносильно – сгруппируем первые $s-1$ сомножителей: пусть $g' = g_1 \cdot \ldots \cdot g_{s-1}$, тогда $g = g' \cdot g_s$. Ясно, что единственность разложения элемента g в произведение s сомножителей равносильна единственности разложения элемента g в произведение $g' \cdot g_s$ и разложения g' в произведение $g_1 \cdot \ldots \cdot g_{s-1}$.

Определение. (Внешнее) прямое произведение групп $G_1, \ldots, G_s$:

$$G_1 \times \ldots \times G_s = \{(g_1, \ldots, g_s) \mid g_j \in G_j, i = 1, \ldots, s\}$$

- группа с операцией

$$(g_1, \ldots, g_i, \ldots, g_s) \cdot (g_1', \ldots, g_i', \ldots, g_s') = (g_1 \cdot g_1', \ldots, g_i \cdot g_i', \ldots, g_s \cdot g_s')$$

Аналогично случаю двух сомножителей, внешнее прямое произведение эквивалентно внутреннему.

Для конечных групп порядок прямого произведения групп равен произведению порядков сомножителей:

$$|G_1 \times \ldots \times G_s| = |G_1| \cdot \ldots \cdot |G_s|$$

(это вытекает, например, из определения внешнего прямого произведения – порядок декартова произведения нескольких множеств равен произведению порядков сомножителей).

Теперь обсудим применения понятия прямого произведения к доказательству китайской теоремы об остатках.

Китайская теорема об остатках.
Классическая формулировка: пусть $m_1, \ldots, m_s \in \mathbb{N}$ попарно взаимно просты, $m = m_1 \cdot \ldots \cdot m_s$. Тогда $\forall n_1, \ldots, n_s \in \mathbb{Z}\ \ \exists n \in \mathbb{Z}$:

$$n \equiv n_1 (mod\, m_1)$$
$$\dots$$
$$n \equiv n_s (mod\, m_s)$$

причем n определено однозначно по модулю m.

Теоретико-групповая формулировка:

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s}$$

Доказательство.
Рассмотрим отображение

$$\varphi: \mathbb{Z} \to \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s}$$
$$\varphi(n) = (n\, mod\, m_1, \dots, n\, mod\, m_s)$$

Это гомоморфизм групп (так как при сложении целых чисел вычеты этих чисел по соответствующим модулям тоже складываются, а наборы вычетов складываются покомпонентно).
Ядро этого гомоморфизма состоит из целых чисел, которые отображаются в нейтральный элемент, т.е. в $(0\, mod\, m_1, \dots, 0\, mod\, m_s)$ – это числа, кратные m (так как m_i попарно взаимно просты):

$$Ker\, \varphi = \{n \in \mathbb{Z} \mid n \vdots m_1, \dots, m_s\} = \{n \in \mathbb{Z} \mid n \vdots m = m_1 \cdot \dots \cdot m_s\} = m\mathbb{Z}$$

По основной теореме о гомоморфизмах,

$$Im\, \varphi \simeq \mathbb{Z}/\, Ker\, \varphi = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$$

С другой стороны, по построению

$$Im\, \varphi \subseteq \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s}$$

- группа порядка $m_1 \cdot \dots \cdot m_s = m$. Но $Im\, \varphi$ – тоже группа порядка m. Значит,

$$\mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s} = Im\, \varphi \simeq \mathbb{Z}_m$$

и φ сюръективен. Это и есть классическая формулировка китайской теоремы об остатках. ■

Следствие. Если $m = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$, где p_i – простые числа, попарно различные, то

$$\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{k_s}}$$

Упражнение 2. Доказать, что примарные циклические группы (группы вида $\mathbb{Z}_{p^k}$, p – простое) нельзя разложить в прямую сумму нетривиальных подгрупп.

Теперь научимся вычислять факторгруппы прямого произведения групп по прямому произведению подгрупп.

Теорема. Пусть

$$G = G_1 \times \ldots \times G_s \supseteq H = H_1 \times \ldots \times H_s,$$

причем $H_i \lhd G_i$. Тогда $H \lhd G$ и

$$G/H \simeq G_1/H_1 \times \ldots \times G_s/H_s$$

Доказательство.
Будем работать с внешним прямым произведением. Рассмотрим отображение

$$\varphi: G \to G_1/H_1 \times \ldots \times G_s/H_s$$
$$\varphi(g_1, \ldots, g_s) = (g_1H_1, \ldots, g_sH_s)$$

Ясно, что φ – гомоморфизм, так как перемножение наборов $(g_1, \ldots, g_s)$ происходит покомпонентно, перемножение смежных классов также происходит покомпонентно. По каждой компоненте будет гомоморфизм канонической проекции, который g_i сопоставляет смежный класс g_iH_i, а произведению элементов соответствует произведение смежных классов.
Ядро этого гомоморфизма состоит из наборов $(g_1, \ldots, g_s)$, которые отображаются в нейтральный элемент, т.е. в $(H_1, \ldots, H_s)$. Получаем

$$\varphi(g_1, \ldots, g_s) = (H_1, \ldots, H_s) \Leftrightarrow g_i \in H_i, \qquad \forall i = 1, \ldots, s.$$

Таким образом,

$$Ker\, \varphi = H_1 \times \ldots \times H_s = H$$

Как легко видеть из определения, φ – сюръективен, поэтому

$$Im\, \varphi = G_1/H_1 \times \ldots \times G_s/H_s$$

По основной теореме о гомоморфизмах,

$$Im\, \varphi \simeq G/\, Ker\, \varphi = G/H$$

■

Следствие. Если $G = G_1 \times \ldots \times G_s$, то

$$G/G_i \simeq G_1 \times \ldots \times G_{i-1} \times G_{i+1} \times \ldots \times G_s$$

Доказательство.
Сразу вытекает из предыдущей теоремы. Возьмем $H = \{e\} \times \ldots \times G_i \times \ldots \times \{e\} = G_i$. Тогда

$$G/G_i \simeq G_1/\{e\} \times \ldots \times G_i/G_i \times \ldots \times G_s/\{e\}$$

Так как $G_i/\{e\} \simeq G_i$ и $G_i/G_i \simeq \{e\}$, получаем

$$G/G_i \simeq G_1 \times \ldots \times \{e\} \times \ldots \times G_s = G_1 \times \ldots \times G_{i-1} \times G_{i+1} \times \ldots \times G_s$$

■

Лекция 5. Группы, порожденные семейством элементов.

Начнем с обсуждения способа построения подгрупп по данной системе элементов – подгруппу можно породить некоторым семейством элементов группы.

Определение. Пусть G – группа. Подгруппа, порожденная семейством элементов $g_i \in G$, $i \in I$: $H =< g_i \mid i \in I >$ - наименьшая подгруппа в G, содержащая g_i, $\forall i \in I$.

Такая подгруппа существует - это пересечение всех подгрупп в G, содержащих g_i,$\forall i \in I$.

В случае конечного семейства $g_i, i \in I = \{1, \dots, n\}$ пишут $H =< g_1, \dots, g_n >$. Такие подгруппы называются конечно порожденными.

Предложение. Подгруппа, порожденная семейством $g_i \mid i \in I$ – это множество вида:

$$< g_i \mid i \in I > = \{g_{i_1}^{\varepsilon_1} \cdot g_{i_2}^{\varepsilon_2} \cdot \dots \cdot g_{i_N}^{\varepsilon_N} \mid i_1, \dots, i_N \in I, \varepsilon_1, \dots, \varepsilon_N = \pm 1\}$$

Доказательство.
Для краткости обозначим множество в правой части равенства через H_0. Пусть $H \subseteq G$ – подгруппа, содержащая все элементы семейства: $H \ni g_i, \forall i \in I$. Тогда (в силу определения подгруппы) H содержит и все обратные к ним элементы: $H \ni g_i^{-1}, \forall i \in I$. Но тогда H содержит и всевозможные произведения этих элементов:

$$H \ni g_{i_1}^{\varepsilon_1} \cdot g_{i_2}^{\varepsilon_2} \cdot \dots \cdot g_{i_N}^{\varepsilon_N}, \forall\, i_1, \dots, i_N \in I, \forall \varepsilon_1, \dots, \varepsilon_N = \{\pm 1\},$$

то есть, $H \ni H_0$.
С другой стороны, H_0 – подгруппа:

- $e = g_i \cdot g_i^{-1} \in H_0$
- $(g_{i_1}^{\varepsilon_1} \cdot \dots \cdot g_{i_N}^{\varepsilon_N}) \cdot (g_{j_1}^{\delta_1} \cdot \dots \cdot g_{j_M}^{\delta_M}) = g_{i_1}^{\varepsilon_1} \cdot \dots \cdot g_{i_N}^{\varepsilon_N} \cdot g_{j_1}^{\delta_1} \cdot \dots \cdot g_{j_M}^{\delta_M} \in H_0$
- $\left(g_{i_1}^{\varepsilon_1} \cdot \dots \cdot g_{i_N}^{\varepsilon_N}\right)^{-1} = g_{i_N}^{-\varepsilon_N} \cdot \dots \cdot g_{i_1}^{-\varepsilon_1} \in H_0$

Таким образом, H_0 является подгруппой, содержащей все элементы семейства $g_i, i \in I$, и она содержится в любой другой подгруппе такого вида, значит, $H_0 =< g_i \mid i \in I >$. ■

Примеры подгрупп, порожденных семейством элементов:
1) Циклическая подгруппа:

$$H =< g >$$

По определению, циклическая подгруппа содержит порождающий элемент g и состоит из всех степеней этого элемента. Любая другая подгруппа, содержащая g, содержит и все степени g, значит, циклическая подгруппа является наименьшей подгруппой, обладающей этим свойством.

2) Группа подстановок S_n:

$$S_n = < (i,j) \mid 1 \leq i < j \leq n >$$

Группа подстановок порождена транспозициями (этот факт был доказан в первой части курса). Всего транспозиций на множестве из n элементов $C_n^2 = \frac{n(n-1)}{2}$, но количество порождающих элементов можно уменьшить – можно брать транспозиции только соседних номеров:

$$S_n = < (1,2), (2,3), \dots, (n-1, n) >$$

- любую перестановку номеров можно получить, переставляя по очереди соседние номера между собой: получаем $n-1$ порождающих элементов.

Упражнение. Доказать, что S_n может быть порождена двумя элементами, например:

$$S_n = < (1,2), (1,2, \dots, n) >$$

Это наименьшее количество порождающих элементов – одним элементом группу S_n породить нельзя (кроме случая $n = 1,2$), так как тогда S_n была бы циклической, а значит, коммутативной, но S_n некоммутативна при $n > 2$.

3) Группа четных подстановок (знакопеременная группа) A_n:

$$A_n = < (i,j,k) \mid 1 \leq i,j,k \leq n, \text{попарно различны} >$$

Утверждение. Группа четных подстановок порождается тройными циклами при $n \geq 3$. При $n \geq 5$ группа A_n порождена произведениями двух независимых транспозиций:

$$A_n = < (i,j)(k,l) \mid 1 \leq i,j,k,l \leq n, \text{попарно различны} >$$

Доказательство.
Заметим, что четную подстановку (как и любую подстановку) можно разложить в произведение транспозиций τ_i:

$$\forall \sigma \in A_n: \sigma = \tau_1 \cdot \tau_2 \cdot \dots \cdot \tau_{N-1} \cdot \tau_N$$

Так как σ – четная подстановка, то количество множителей должно быть четным, и транспозиции можно разбить на пары:

$$\forall \sigma \in A_n: \sigma = \tau_1 \cdot \tau_2 \cdot \dots \cdot \tau_{N-1} \cdot \tau_N = (\tau_1 \cdot \tau_2) \cdot \dots \cdot (\tau_{N-1} \cdot \tau_N)$$

Таким образом, A_n порождается произведениями пар транспозиций. Если эти транспозиции зависимы, то их произведение будет тройным циклом:

$$(i,j) \cdot (j,k) = (i,j,k)$$

Если транспозиции независимы, то посчитаем их произведение следующим образом: дважды "вклеим" между этими транспозициями транспозицию (j,k) – это не изменит результат:

$$(i,j)\cdot(k,l) = (i,j)\cdot(j,k)\cdot(j,k)\cdot(k,l) = (i,j,k)\cdot(j,k,l)$$

- получили произведение двух тройных циклов.
Итак, любое произведение двух транспозиций выражается через тройные циклы, значит, любая четная подстановка представима в виде произведения тройных циклов при $n \geq 3$.

При $n \geq 5$ мы можем каждый тройной цикл выразить через пары независимых транспозиций: снова дважды "вклеим" между множителями транспозицию (l,m) – мы можем это сделать, так как $n \geq 5$, и можно выбрать попарно различные $i,j,k,l,m \in \{1,2,\dots,n\}$:

$$(i,j,k) = (i,j)\cdot(j,k) = (i,j)\cdot(l,m)\cdot(l,m)\cdot(j,k)$$

- получили произведение двух пар независимых транспозиций. ■

4) Группа невырожденных матриц $GL_n(K)$:

$$GL_n(K) = <\text{элементарные матрицы}>$$

Группа $GL_n(K)$ порождается элементарными матрицами, т.е. матрицами, которые можно получить из единичной матрицы с помощью одного элементарного преобразования (строк или столбцов). Это следует из факта, который был доказан в первой половине курса: любую невырожденную матрицу можно разложить в произведение элементарных матриц.

5) Группа $SL_n(K)$:

$$SL_n(K) = <\text{элементарные матрицы } 1-\text{го типа}>$$

Утверждение. Группа $SL_n(K)$ порождается элементарными матрицами первого типа (т.е. матрицами, соответствующими преобразованию 1-го типа: прибавлению к одной строке матрицы другой строки, умноженной на некоторый коэффициент).

Доказательство.
Докажем индукцией по n, что любую матрицу $A \in SL_n(K)$ можно привести к единичной матрице E, пользуясь только элементарными преобразованиями строк 1-го типа.

База индукции: $n = 1$ – доказывать нечего (в этом случае сразу $A = E$).

Шаг индукции: пусть $A \in SL_n(K)$. Так как A невырождена, то в первом столбце найдется ненулевой элемент (обозначим его *). Тогда:

1) Прибавим строку, содержащую элемент * к первой строке с подходящим коэффициентом (так, чтобы в левом верхнем углу оказался ненулевой элемент). Если в первом столбце был только один ненулевой элемент в левом верхнем углу, то этот шаг пропускаем.

2) Если требуется, прибавим первую строку к какой-нибудь другой строке с подходящим коэффициентом (так, чтобы первый элемент в этой строке стал ненулевым) – получим два ненулевых элемента в первом столбце.

3) Прибавим нижнюю строку с ненулевым элементом в первом столбце к первой строке с подходящим коэффициентом (так, чтобы в левом верхнем углу получилась 1).

4) Пользуясь только элементарными преобразованиями 1-го типа, обнуляем все элементы первого столбца, кроме стоящего в левом верхнем углу. Получаем матрицу с углом нулей из $SL_n(K)$, состоящую из блоков размера 1×1 и $n-1 \times n-1$ – матрицы из $SL_{n-1}(K)$, к которой применимо предположение индукции.

5) Значит, пользуясь только элементарными преобразованиями 1-го типа, мы можем получить матрицу, отличающуюся от единичной только первой строкой.

6) Обнуляем элементы первой строки, вычитая из первой строки остальные строки с подходящими коэффициентами – получаем единичную матрицу.

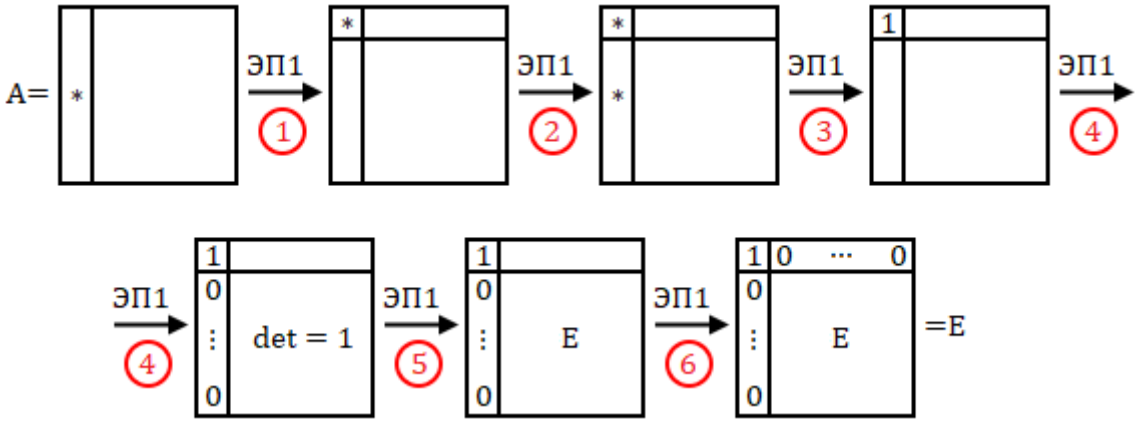


Рис. 5.1. Преобразования, приводящие A к E

Но каждое элементарное преобразование строк равносильно умножению слева на соответствующую элементарную матрицу. Следовательно, взяв матрицу A и умножив ее слева на матрицы элементарных преобразований 1-го типа, описанных выше, мы получим единичную матрицу:

$$U_N \cdot \ldots \cdot U_1 \cdot A = E$$

Тогда

$$A = U_1^{-1} \cdot \ldots \cdot U_N^{-1}$$

Но матрица, обратная к элементарной матрице первого типа, тоже является элементарной матрицей 1-го типа (соответствует обратному преобразованию). Таким образом, любую матрицу $A \in SL_n(K)$ можно разложить в произведение элементарных матриц 1-го типа. ■

Конечно порожденные абелевы группы

Заметим, что особую роль в теории групп играют конечно порожденные группы, так как любое утверждение теории групп, в котором участвует конечное число элементов, достаточно доказать для всех конечно порожденных подгрупп данной группы.
Займемся изучением простейшего класса конечно порожденных групп – конечно порожденных абелевых групп.
Пусть $G =< g_1, \dots, g_n >$ - абелева. Тогда $\forall g \in G: g = g_{i_1}^{\varepsilon_1} \cdot g_{i_2}^{\varepsilon_2} \cdot \dots \cdot g_{i_N}^{\varepsilon_N}$. Так как G абелева, то в этом произведении можно привести подобные члены:

$$\forall g \in G: g = g_1^{k_1} \cdot g_2^{k_2} \cdot \dots \cdot g_n^{k_n}, k_i \in \mathbb{Z}$$

в аддитивной терминологии:

$$\forall g \in G: g = k_1 g_1 + k_2 g_2 + \dots + k_n g_n, k_i \in \mathbb{Z}$$

- произвольный элемент группы G представляется в виде целочисленной линейной комбинации порождающих элементов. Это похоже на разложение вектора по базису в конечномерном векторном пространстве. Вообще, между конечнопорожденными абелевыми группами и конечномерными векторными пространствами есть довольно много аналогий – и в терминологии, и в их свойствах. Чтобы эти аналогии были видны, далее для конечно порожденных абелевых групп будем пользоваться аддитивной терминологией.

Определение. Система элементов $h_1, \dots, h_m \in G$ называется линейно зависимой, если существует целочисленная линейная комбинация элементов этой системы, равная нулю:

$$\exists l_1, \dots, l_m \in \mathbb{Z}, \exists l_i \neq 0: \quad l_1 h_1 + k_2 g_2 + \dots + l_m h_m = 0$$

Система $g_1, \dots, g_n \in G$ – *базис* группы G, если $G =< g_1, \dots, g_n >$ и $g_1, \dots, g_n$ линейно независима.

Как и для векторных пространств, можно переформулировать это определение эквивалентным образом: система $g_1, \dots, g_n \in G$ – базис группы G, тогда и только тогда, когда каждый элемент группы G представляется в виде линейной комбинации элементов $g_1, \dots, g_n$ единственным образом:

$$\forall g \in G \ \exists! \ k_1, \dots, k_n \in \mathbb{Z}: \ g = k_1 g_1 + k_2 g_2 + \dots + k_n g_n$$

Как и в случае векторных пространств, $k_1, \dots, k_n$ – координаты g в базисе $g_1, \dots, g_n$.

Определение. Абелева группа, имеющая базис, называется свободной.

Примеры:
1) Группа вычетов $\mathbb{Z}_m$
$\mathbb{Z}_m$ конечно порождена (так как она циклическая), но не свободна: любая конечная система элементов в этой группе линейно зависима:

$$\forall g_1, \dots, g_n \in \mathbb{Z}_m: \ mg_1 + \dots + mg_n = 0$$

Этот пример показывает, что аналогия между конечно порожденными абелевыми группами и конечномерными векторными пространствами не совсем полная.

2) Группа целочисленных векторов длины n: $\mathbb{Z}^n = \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$
$\mathbb{Z}^n$ свободна, в качестве базиса можно выбрать стандартный базис:

$$e_1, \dots, e_n, e_i = (0, \dots, \underset{\nearrow\ i-\text{ое место}}{1}, \dots, 0)$$

Основная лемма о линейной зависимости для абелевых групп.
Пусть G – абелева группа, $g_1, \dots, g_n, h_1, \dots, h_m \in G$ и $\forall j = 1, \dots, m \ \exists\ k_{1j}, \dots, k_{nj} \in \mathbb{Z}$:

$$h_j = k_{1j}g_1 + \dots + k_{nj}g_n,$$

причем $m > n$. Тогда $h_1, \dots, h_m$ линейно зависима.

Доказательство.
Рассмотрим однородную систему линейных уравнений с матрицей коэффициентов, составленных из k_{ij}:

$$\begin{cases} k_{11}x_1 + \dots + k_{1m}x_m = 0 \\ \dots \\ k_{n1}x_1 + \dots + k_{nm}x_m = 0 \end{cases}$$

Так как все $k_{ij} \in \mathbb{Z}$, то можно считать, что это система линейных уравнений над $\mathbb{Q}$. Так как $n < m$, то система имеет ненулевое решение: $(l_1, \dots, l_m) \in \mathbb{Q}^m$. Домножив на общий знаменатель, можно считать, что $l_1, \dots, l_m \in \mathbb{Z}$.
Рассмотрим $l_1h_1 + \dots + l_mh_m$ – нетривиальную линейную комбинацию $h_1, \dots, h_m$. Перепишем ее в виде

$$l_1h_1 + \dots + l_mh_m = \sum_j l_jh_j = \sum_j l_j \sum_i k_{ij}g_i = \sum_i (\sum_j k_{ij}l_j)g_i$$

Заметим, что коэффициент при g_i – это результат подстановки $l_1, \dots, l_m$ в j-ое уравнение системы, то есть, 0 (так как $l_1, \dots, l_m$ – решение системы). Следовательно,

$$l_1 h_1 + \cdots + l_m h_m = 0$$

и система $h_1, \dots, h_m$ линейно зависима. ■

Следствие. Как и в случае векторных пространств, из основной леммы о линейной зависимости вытекает, что во всех базисах свободной абелевой группы F одинаковое число элементов (так как базисы выражаются друг через друга). Это число называется *рангом* свободной группы F и обозначается $rk\ F$.

Теорема 1. Все свободные абелевы группы одного ранга изоморфны друг другу.

Доказательство.
Достаточно рассмотреть фиксированную свободную абелеву группу данного ранга, и доказать, что любая другая ей изоморфна. В качестве такой группы ранга n рассмотрим

$$\mathbb{Z}^n = \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$$

Пусть F – свободная абелева группа, $rk\ F = n$ и пусть $f_1, \dots, f_n$ – ее базис. Рассмотрим отображение

$$\varphi\colon \mathbb{Z}^n \to F$$
$$\varphi(k_1, \dots, k_n) = k_1 f_1 + \cdots + k_n f_n$$

- гомоморфизм (очевидно). Его биективность вытекает из того, что набор $f_1, \dots, f_n$ является базисом (сюръективность: любой элемент группы F можно выразить в виде линейной комбинации базисных элементов, поэтому любой элемент группы F является образом какого-то набора из $\mathbb{Z}^n$; инъективность: это выражение единственно, поэтому различные элементы из $\mathbb{Z}^n$ переходят в различные). Поэтому φ – изоморфизм. ■

Таким образом, для изучения свободных абелевых групп достаточно ограничиться изучением групп вида $\mathbb{Z}^n$.

Докажем еще одну теорему (аналог известного результата из линейной алгебры: в конечномерном векторном пространстве размерность подпространства не превышает размерности самого пространства).

Теорема 2. Пусть F – свободная абелева группа, $H \subseteq F$ – подгруппа. Тогда H свободна и $rk\ H \leq rk\ F$.

Доказательство.
Пусть $rk\ F = n$. Без ограничения общности (см. предыдущую теорему) можно считать, что $F = \mathbb{Z}^n$. Доказательство будем проводить индукцией по n.

База индукции: $n = 1$ – в этом случае $H \subseteq \mathbb{Z}$. Так как $\mathbb{Z}$ - циклическая группа, то любая ее подгруппа также будет циклической: $H = m\mathbb{Z}$.

Базис группы H: $\begin{matrix}\{m\} \text{ при } m \neq 0 \\ \emptyset \text{ при } m = 0\end{matrix}$ $\Rightarrow H$ свободна, $rk\ H = \begin{cases}1 \text{ при } m \neq 0 \\ 0 \text{ при } m = 0\end{cases}$ и неравенство

$$rk\ H \leq rk\ F$$

выполнено, так как $rk\ F = 1$.

Шаг индукции (переход от $n-1$ к n): рассмотрим отображение проекции $\mathbb{Z}^n$ на последнюю координатную ось

$$\pi\colon \mathbb{Z}^n \to F$$
$$\pi(k_1, \dots, k_n) = k_n$$

- гомоморфизм.

$$Ker\ \pi = \mathbb{Z}^{n-1} \oplus \{0\} \simeq \mathbb{Z}^{n-1}$$

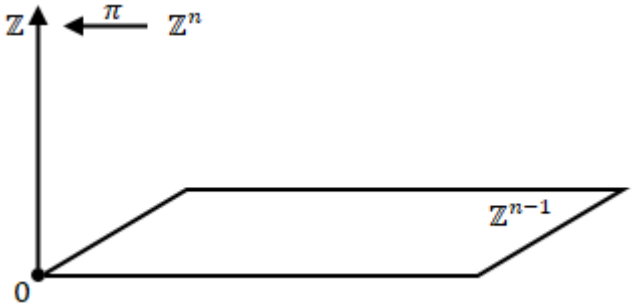


Рис. 5.2. Отображение π

Теперь рассмотрим подгруппу $H \subseteq \mathbb{Z}^n$ – ограничим π на H, и рассмотрим ядро $Ker\ (\pi|_H)$ получившегося гомоморфизма – это будет подгруппа в ядре гомоморфизма π:

$$K = Ker\ (\pi|_H) = H \cap \mathbb{Z}^{n-1} \subseteq \mathbb{Z}^{n-1}$$

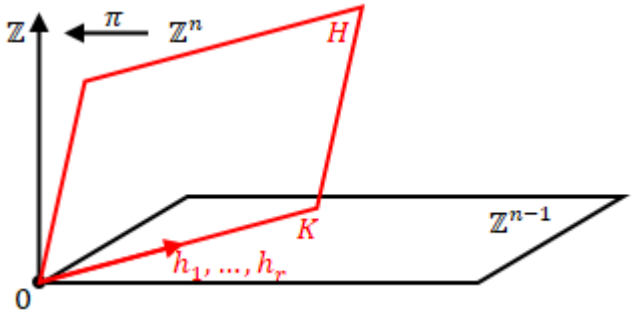


Рис. 5.3. $H \subseteq \mathbb{Z}^n$ и $K = Ker\ (\pi|_H)$

K – подгруппа в свободной абелевой группе ранга $n-1$, следовательно, по предположению индукции, K свободна, и $rk\ K = r \leq n-1$. Пусть $h_1, \dots, h_r$ – базис K. Образ гомоморфизма $\pi|_H$ – подгруппа в группе $\mathbb{Z}$:

$$Im(\pi|_H) = \pi(H) \subseteq \mathbb{Z}$$

По базе индукции, эта группа является свободной и либо порождена одним элементом, либо является нулевой:

$$\pi(H) = m\mathbb{Z}$$

1) $m = 0 \Rightarrow H = K \subseteq \mathbb{Z}^{n-1}$. Следовательно, H – свободная абелева группа, $rk\, H = r \leq n-1 < n$.

2) $m \neq 0$. Выберем $h_{r+1} \in H$, $\pi(h_{r+1}) = m$ и докажем, что $h_1, \dots, h_r, h_{r+1}$ – базис H, т.е. что произвольный элемент из H выражается в виде линейной комбинации этих элементов, и что они линейно независимы.

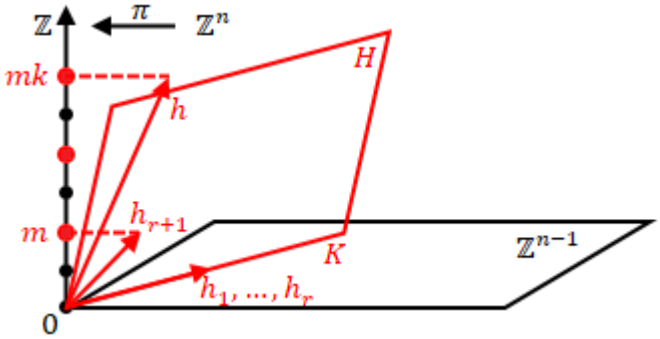


Рис. 5.4. $h_1, \dots, h_r, h_{r+1}$ – базис H

$\forall h \in H$ мы можем рассмотреть его образ при проекции: $\pi(h) = mk$. Тогда

$$\pi(h - kh_{r+1}) = \pi(h) - k\pi(h_{r+1}) = mk - km = 0$$

Следовательно, $h - kh_{r+1} \in K$, и выражается через базис K:

$$h - kh_{r+1} = k_1h_1 + \dots + k_rh_r,$$

откуда

$$h = k_1h_1 + \dots + k_rh_r + kh_{r+1}$$

т.е. произвольный элемент из H выражается в виде линейной комбинации $h_1, \dots, h_r, h_{r+1}$. Осталось проверить линейную независимость: если

$$l_1h_1 + \dots + l_rh_r + l_{r+1}h_{r+1} = 0,$$

то применив к левой и правой части гомоморфизм π, получим (т.к. $l_1h_1 + \dots + l_rh_r \in K$):

$$\pi(l_1h_1 + \dots + l_rh_r + l_{r+1}h_{r+1}) = \pi(l_{r+1}h_{r+1}) = l_{r+1}\pi(h_{r+1}) = l_{r+1} \cdot m = 0$$

Отсюда, так как $m \neq 0$, получаем, что $l_{r+1} = 0$, но тогда $l_1h_1 + \dots + l_rh_r = 0$. Так как $h_1, \dots, h_r$ – базис K, то $l_1 = \dots = l_r = 0$. Таким образом, набор $h_1, \dots, h_r, h_{r+1}$ линейно независим, значит, $h_1, \dots, h_r, h_{r+1}$ – базис.

Так как $rk\ H = r < n$, то $rk\ H = r + 1 \leq n$. ■

Замечание. Если $H \subset F$, то необязательно $rk\ H < rk\ F$. В качестве контрпримера можно рассмотреть группы $F = \mathbb{Z}^2$ (целочисленные векторы на плоскости) и $H = \{(k_1, k_2) \mid k_1 + k_2 \vdots 2\}$ (целочисленные векторы на плоскости с четной суммой координат).
Подгруппа H не является собственной, но она свободна и $rk\ H = 2$, в качестве базиса можно выбрать h_1, h_2 как показано на рис. 5.5:

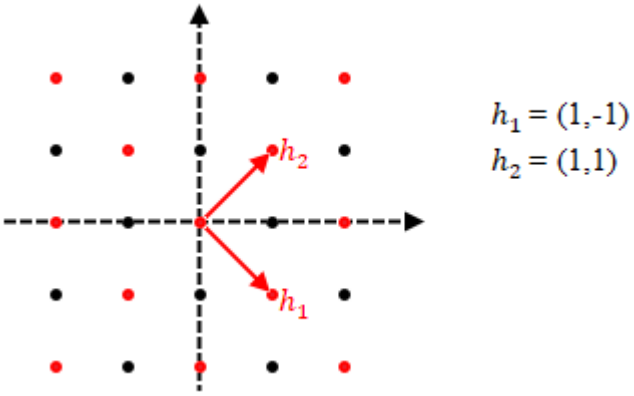


Рис. 5.5. $H \subset \mathbb{Z}^2$, $rk\ H = rk\ \mathbb{Z}^2$

Лекция 6. Свободные абелевы группы. Структура конечнопорожденных абелевых групп.

Обсудим, как свободные абелевы группы появляются в геометрии.

Определение. Пусть V – евклидово векторное пространство. Подмножество $S \subset V$ называется дискретным, если для любой ограниченной области $B \subset V$ пересечение $S \cap B$ конечно.

Пример. $S = \mathbb{Z}^n \subset V = \mathbb{R}^n$.

Теорема 1. Любая дискретная (аддитивная) подгруппа $L \subset V$ свободна и любой базис L является линейно независимой системой векторов в V.

Доказательство.
Заменив V на $\langle L \rangle_{\mathbb{R}}$ можно считать, что L порождает V как векторное пространство. Такие дискретные подгруппы называются решетками (пример: $V = \mathbb{R}^n$, $L = \mathbb{Z}^n$). Можно выбрать базис пространства V, состоящий из векторов решетки: $v_1, \dots, v_n \in L$. Если мы рассмотрим все целочисленные линейные комбинации этих векторов, то они породят подрешетку в этой решетке: $L \supseteq L_0 = \langle v_1, \dots, v_n \rangle$.
Введем понятие фундаментального параллелепипеда:

Фундаментальный параллелепипед

$$\Pi = \{v = t_1 v_1 + \cdots + t_n v_n \mid 0 \le t_1, \dots, t_n \le 1\}$$

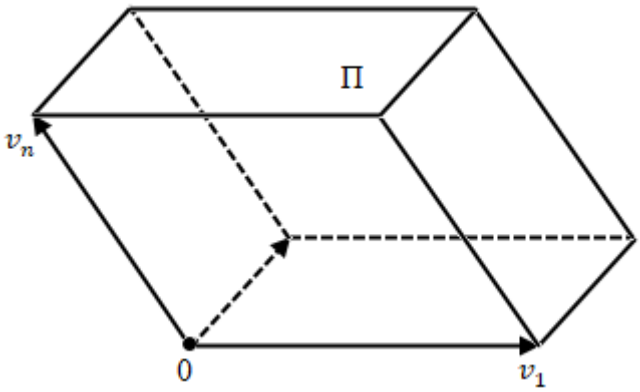


Рис. 6.1. Фундаментальный параллелепипед

Любой вектор $v \in L$ мы можем разложить в линейную комбинацию базисных векторов пространства V:

$$v = x_1 v_1 + \cdots + x_n v_n \ (x_i \in \mathbb{R})$$

Положим

$$k_i = [x_i] \in \mathbb{Z},$$
$$t_i = x_i - [x_i] = \{x_i\} \in [0,1).$$

Тогда

$$v_0 = k_1 v_1 + \cdots + k_n v_n \in L_0$$
$$v' = v - v_0 = t_1 v_1 + \cdots + t_n v_n \in \Pi \cap L$$

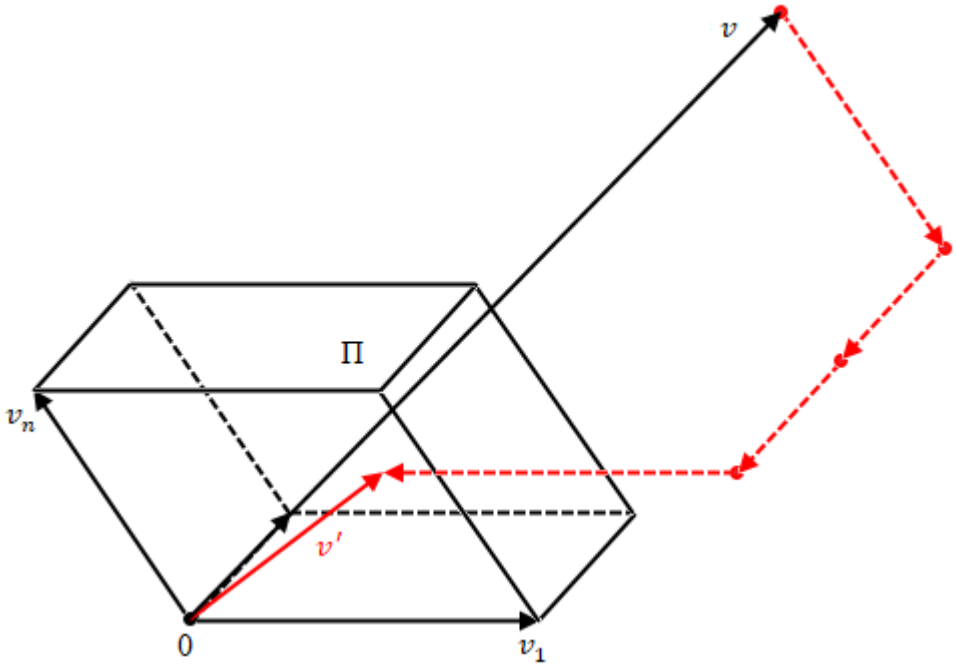


Рис. 6.2. Иллюстрация к разложению $v = v' + v_0$

Следовательно, любой смежный класс $v + L_0$ пересекает фундаментальный параллелепипед Π. Так как Π ограничен, то $\Pi \cap L$ конечно. Но каждый смежный класс по подгруппе L_0 имеет представителя, лежащего в $\Pi \cap L$. Поскольку разные смежные классы между собой не пересекаются, то у разных смежных классов будут разные представители. Следовательно, число смежных классов тоже конечно, т.е.

$$|L \,/\, L_0| = m < \infty$$

Тогда (по следствию из теоремы Лагранжа) $\forall v \in L$: $m(v + L_0) = L_0$. Отсюда следует, что $mv \in L_0$.
Следовательно,

$$L_0 \subseteq L \subseteq \frac{1}{m} L_0$$

L_0 – свободная абелева группа, ее базис: $v_1, \dots, v_n$, но $\frac{1}{m} L_0$ – тоже свободная абелева группа, ее базис: $\frac{1}{m} v_1, \dots, \frac{1}{m} v_n$. Из теоремы, доказанной на прошлой лекции (см. теорема 2) вытекает, что L тоже свободная абелева группа (как подгруппа в свободной абелевой группе) и

$$n = rk\, L_0 \leq rk\, L \leq rk\, (\frac{1}{m} L_0) = n,$$

откуда $rk\, L = n$.

Осталось доказать, что любой базис группы L является линейно независимой системой векторов в пространстве V. Пусть $w_1, \dots, w_n$ – базис абелевой группы L. Тогда векторы $v_1, \dots, v_n$, образующие базис подгруппы $L_0 \subseteq L$ линейно выражаются (с целыми коэффициентами) через $w_1, \dots, w_n$. Отсюда вытекает, что $w_1, \dots, w_n$ линейно независимы (как векторы) над $\mathbb{R}$ (иначе $rk\{v_1, \dots, v_n\} \leq rk\{w_1, \dots, w_n\} < n$, но тогда $v_1, \dots, v_n$ тоже были бы линейно зависимы – противоречие). ■

Теперь вернемся к общей теории свободных конечно порожденных абелевых групп и докажем теорему, которая является аналогом теоремы из линейной алгебры (о выборе базиса векторного пространства, согласованного с подпространством).

Теорема 2 (о согласованных базисах). Пусть F – свободная абелева группа, $H \subseteq F$ – подгруппа. Тогда существуют базисы $f_1, \dots, f_n$ для F и $h_1, \dots, h_r$ для H ($r \leq n$), такие что $h_i = m_i f_i$, $m_i \in \mathbb{N}, \forall i = 1, \dots, r$.

Пример. $F = \mathbb{Z}^2$, $H = \langle h_1, h_2 \rangle$, $h_1 = (1, -1)$, $h_2 = (2,1)$. Векторы h_1 и h_2 образуют базис, который не согласован со стандартным базисом e_1, e_2 решетки F.

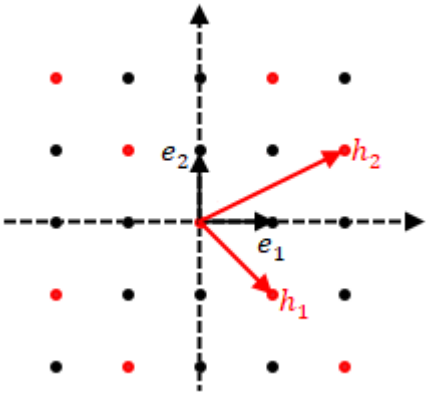


Рис. 6.3. Базис h_1, h_2 не согласован с базисом e_1, e_2

Однако, мы можем подобрать два других базиса, которые будут согласованы: h_1, $h_2' = h_2 - 2h_1$ – базис группы H будет согласован с новым базисом группы F: $f_1 = e_1 - e_2, f_2 = e_2$. Теперь $h_1 = f_1, h_2' = 3f_2$:

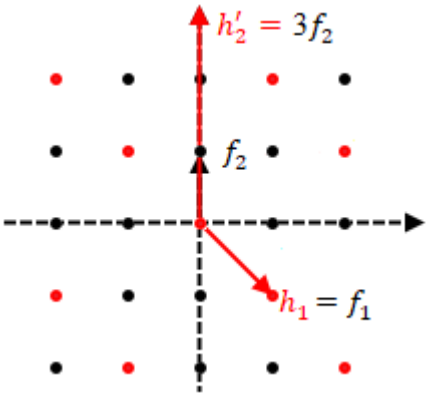


Рис. 6.4. h_1, h_2' согласован с базисом f_1, f_2

Доказательство.
Выберем произвольный базис $f_1, \dots, f_n$ для F и систему порождающих $h_1, \dots, h_l$ для H. Так как H – подгруппа F, то $\forall j = 1, \dots, l$ выполнено $h_j = k_{1j}f_1 + \dots + k_{nj}f_n$, где $k_{ij} \in \mathbb{Z}$. Рассмотрим матрицу (матрица перехода от базиса $f_1, \dots, f_n$ к системе порождающих $h_1, \dots, h_l$):

$$K = \begin{pmatrix} k_{11} & \cdots & k_{1l} \\ \vdots & \ddots & \vdots \\ k_{n1} & \cdots & k_{nl} \end{pmatrix}$$

- целочисленная матрица, по столбцам которой стоят координаты элемента h_j в базисе $f_1, \dots, f_n$, а по строкам – координаты по f_i.

Менять $f_1, \dots, f_n$ и $h_1, \dots, h_l$ будем с помощью элементарных замен.

Элементарные замены базиса F: $(f_1, \dots, f_n) \to (f_1', \dots, f_n')$:
1) К одному из базисных векторов прибавляем другой с каким-то целым коэффициентом:

$$f_i' = f_i + m \cdot f_j' \ \ (m \in \mathbb{Z})$$

2) Переставляем два базисных вектора местами:

$$f_i' = f_j, \qquad f_j' = f_i$$

3) Замена знака (умножаем базисный вектор на обратимое целое число, т.е. на -1):

$$f_i' = -f_i$$

Элементарным заменам базиса будет соответствовать переход от матрицы K к матрице K' с помощью целочисленного элементарного преобразования строк.
Аналогично элементарные замены системы порождающих в группе H: $(h_1, \dots, h_l) \to (h_1', \dots, h_l')$ эквивалентны переходу от матрицы K к матрице K' с помощью целочисленного элементарного преобразования столбцов.

Лемма. С помощью целочисленных элементарных преобразований строк и столбцов любую целочисленную матрицу $K \in Mat_{n \times l} \in \mathbb{Z}$ можно привести к виду

$$K^* = \begin{pmatrix} m_1 & & 0 & 0 & \dots & 0 \\ & \ddots & & \dots & \dots & \dots \\ 0 & & m_r & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \ddots & \dots \\ 0 & \dots & 0 & \dots & \dots & 0 \end{pmatrix}, m_i \in \mathbb{N}$$

Если мы докажем эту лемму, то докажем, что переход $K \to K^*$ равносилен замене базиса: $(f_1, \dots, f_n) \to (f_1^*, \dots, f_n^*)$ и замене системы порождающих: $(h_1, \dots, h_l) \to (h_1^*, \dots, h_l^*)$, которая выражается через базис $(f_1^*, \dots, f_n^*)$ в соответствии со столбцами матрицы K^*, т.е.

$$h_i^* = \begin{cases} m \cdot f_i^* \text{ при } i \le r \\ 0 \text{ при } i > r \end{cases}$$

Базисы $(f_1^*, \dots, f_n^*)$ и $(h_1^*, \dots, h_r^*)$ групп F и H – искомые.

Тем самым мы доказали теорему о согласованных базисах по модулю этой леммы, которую мы докажем.

Доказательство леммы.
Будем доказывать лемму индукцией по $max\ \{n, l\}$.
База индукции: $n = l = 1$ – доказывать нечего.

Шаг индукции: $K = 0$ – доказывать нечего. Иначе (если матрица ненулевая):

- Выберем ненулевой элемент $k_{ij} \neq 0$ с самым маленьким модулем: $|k_{ij}| = min = m \in \mathbb{N}$. Далее переставим m в левый верхний угол (целочисленное преобразование 2-го типа), получим матрицу K'.
- Разделим элементы матрицы K', лежащие в первой строке или в первом столбце с остатком на m:

$$k_{i1} = p_{i1}m + {k_{i1}}''$$
$$k_{1j} = q_{1j}m + {k_{1j}}''$$

  Затем заменяем эти элементы на их остатки (вычитаем из соответствующей строки (столбца) первую строку (столбец) с подходящим коэффициентом) – получим матрицу K'' из матрицы K' элементарными целочисленными преобразованиями строк и столбцов 1-го типа. В первом столбце и первой строке K'' стоят числа, меньшие по модулю, чем m.
- Далее: либо все ${k_{i1}}''$ и ${k_{1j}}''$ равны нулю, либо среди них есть хотя бы один ненулевой элемент. В этом случае ($\exists {k_{i1}}'' \neq 0$ или $\exists {k_{1j}}'' \neq 0$) применяем предыдущий шаг еще раз – снова выбираем элемент с самым маленьким модулем, переставляем его на позицию (1,1) и т.д. Так мы будем уменьшать наименьший модуль ненулевого элемента и рано или поздно получим матрицу K''' вида:

$$K''' = \left(\begin{array}{c|ccc} \pm m_1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \dots & & \bar{K} & \\ 0 & & & \end{array}\right)$$

- Матрица $\overline{K}$ тоже целочисленная, но меньших размеров – по предположению индукции мы можем привести ее к псевдодиагональному виду целочисленными элементарными преобразованиями строк и столбцов – получим матрицу $\widetilde{K}$, которая выглядит ,как показано на рис. 6.5.
- При необходимости поменяем знак у первой строки (столбца), т.е. применим целочисленное элементарное преобразование 3-го типа и получим матрицу K^* нужного вида. ■

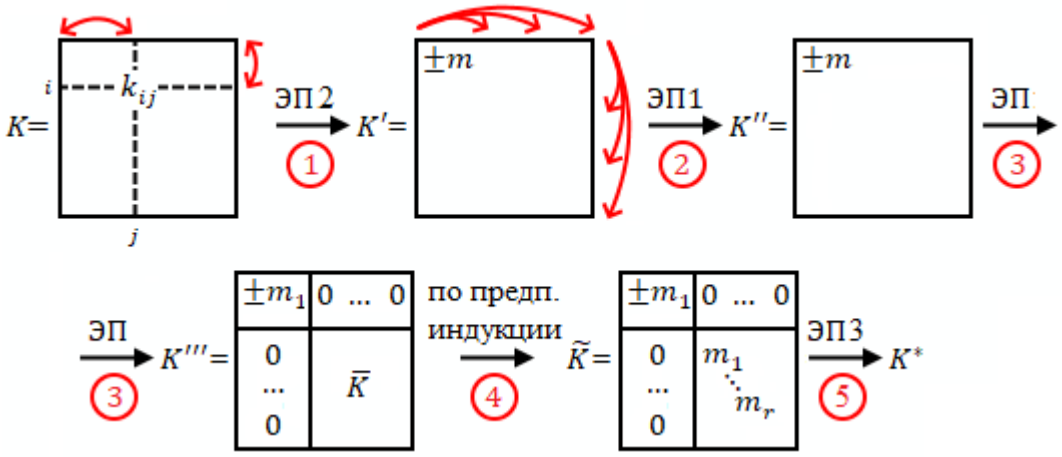


Рис. 6.5. Преобразования, приводящие K к K^*

Следующую теорему можно назвать универсальным свойством свободной абелевой группы.

Теорема 3 (универсальное свойство свободной абелевой группы). Пусть F – свободная абелева группа с базисом $f_1, \dots, f_n$ и G – абелева группа с элементами $g_1, \dots, g_n$. Тогда ∃! гомоморфизм

$$\varphi: F \to G$$
$$\varphi(f_i) = g_i, \forall i = 1, \dots, n$$

Другими словами, гомоморфизмы из свободной абелевой группы можно задавать на базисных элементах как угодно (поэтому группа и называется свободной).

Доказательство.
Единственность. Любой элемент группы F единственным образом разлагается в целочисленную линейную комбинацию базисных векторов: $\forall f \in F \ \exists!\ k_1, \dots, k_n \in \mathbb{Z}$:

$$f = k_1 f_1 + \dots + k_n f_n$$

Тогда

$$\varphi(f) = \varphi(k_1 f_1 + \dots + k_n f_n) = k_1 \varphi(f_1) + \dots + k_n \varphi(f_n) = k_1 g_1 + \dots + k_n g_n$$

Существование. Из доказательства единственности понятно, как задать φ: формула

$$\varphi(f) = k_1 g_1 + \cdots + k_n g_n$$

задает отображение $\varphi: F \to G$ корректно (так как разложение $\forall f \in F$ по $f_1, \dots, f_n$ единственно). Несложно проверить, что это гомоморфизм: пусть

$$f = k_1 f_1 + \cdots + k_n f_n,$$
$$f' = k_1' f_1 + \cdots + k_n' f_n$$

Тогда

$$f + f' = (k_1 + k_1')f_1 + \cdots + (k_n + k_n')f_n$$

Тогда по определению отображения φ:

$$\varphi(f + f') = (k_1 + k_1')g_1 + \cdots + (k_n + k_n')g_n =$$
$$= k_1 g_1 + \cdots + k_n g_n + k_1' g_1 + \cdots + k_n' g_n = \varphi(f) + \varphi(f')$$

По построению очевидно, что $\varphi(f_i) = g_i$. ■

Замечание. Выбор базиса $f_1, \dots, f_n$ в свободной абелевой группе F позволяет, как мы видели на прошлой лекции, отождествить ее с решеткой целочисленных векторов $\mathbb{Z}^n$:

$$F \simeq \mathbb{Z}^n$$

При этом отождествлении

$$Ker\,\varphi \simeq \{(k_1, \dots, k_n) \mid k_i \in \mathbb{Z},\ k_1 g_1 + \cdots + k_n g_n = 0\}$$

Другими словами, ядро гомоморфизма φ – это группа всех линейных зависимостей между элементами $g_1, \dots, g_n$.
Образ φ – подгруппа в группе G, состоящая из всех таких линейных комбинаций, т.е. подгруппа, порожденная элементами $g_1, \dots, g_n$:

$$Im\,\varphi < g_1, \dots, g_n >$$

Теперь все готово для того, чтобы сформулировать основную теорему о структуре произвольных конечно порожденных абелевых групп.

Теорема 4 (о структуре произвольных конечно порожденных абелевых групп). Всякая конечно порожденная абелева группа изоморфна одной из групп следующего вида:

$$\underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{r} \oplus \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{k_s}}$$

$r, s \in \mathbb{Z}_+$, $p_1, \dots, p_s$ – простые числа (не обязательно попарно различные), $k_1, \dots, k_s \in \mathbb{N}$. Более того, r (*ранг* группы) и неупорядоченный набор $(p_1^{k_1}, \dots, p_s^{k_s})$ (*тип кручения*) определены однозначно для данной конечно порожденной абелевой группы.

Следствием из этой теоремы является классификация конечных абелевых групп.

Следствие. Всякая конечная абелева группа изоморфна прямой сумме нескольких примарных циклических групп: $\mathbb{Z}_{p_1^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_s}}$, причем набор $(p_1^{k_1}, \ldots, p_s^{k_s})$ (mun конечной абелевой группы) определен однозначно.

Предупреждение. Само разложение конечно порожденной абелевой группы G во внутреннюю прямую сумму бесконечных и примарных циклических подгрупп определено неоднозначно.

Примеры.
1) Для свободной абелевой группы G ее разложение в прямую сумму n бесконечных циклических подгрупп:

$$G \simeq \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \simeq \mathbb{Z}^n$$

задается выбором базиса в группе G (а базисов много).

2) Модель группы Клейна. Рассмотрим $G = (\mathbb{Z}_2)^2$ – векторное пространство размерности 2 над полем $\mathbb{Z}_2$. Оно содержит 4 элемента. В этой группе есть 3 подгруппы: ось абсцисс A, ось ординат B, биссектриса координатной четверти C. Каждая из этих подгрупп состоит из двух элементов (т.е. изоморфна $\mathbb{Z}_2$).

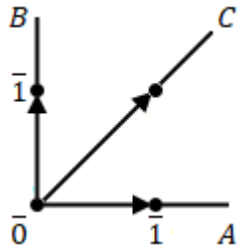


Рис. 6.6. $V_4 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Легко видеть, что группа G равна прямой сумме любых двух из этих подгрупп:

$$G = A \oplus B = A \oplus C = B \oplus C \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Лекция 7. Структура конечнопорожденных абелевых групп. Экспонента группы.

Доказательство теоремы 4 (о структуре произвольных конечно порожденных абелевых групп).
Вначале докажем существование такого разложения. Пусть $G = < g_1, \dots, g_n >$ - конечно порожденная абелева группа. Рассмотрим свободную абелеву группу F ранга n: $rk\ F = n$, $f_1, \dots, f_n$ – базис F.
По универсальному свойству свободных групп, ∃! гомоморфизм

$$\varphi: F \to G$$
$$\varphi(f_i) = g_i, \forall i = 1, \dots, n$$

Образ φ – вся группа G, так как G порождена элементами g_i, которые являются образами базисных векторов:

$$Im\,\varphi = G$$

Ядро φ – подгруппа в группе F:

$$Ker\,\varphi = H \subseteq F$$

По основной теореме о гомоморфизмах,

$$G \simeq F/H$$

Таким образом, задача сводится к разложению факторгруппы F/H в прямую сумму циклических групп. По теореме о согласованных базисах, в свободной группе F и ее подгруппе H (тоже свободной) можно выбрать согласованные базисы: ∃ базисы $f_1^*, \dots, f_n^*$ для F и $h_1^*, \dots, h_l^*$ для группы H ($l \leq n$), такие что:

$$\forall i = 1, \dots, n: \quad h_i^* = m_i f_i^*, \qquad m_i \in \mathbb{N}$$

Выбор базиса в F означает, что мы разложили F в прямую сумму циклических подгрупп, порожденных базисными элементами $f_1^*, \dots, f_n^*$ (т.к. каждый элемент свободной абелевой группы единственным образом выражается через базисные элементы). Аналогично подгруппа H разлагается в прямую сумму циклических подгрупп, порожденных базисными элементами $h_1^*, \dots, h_l^*$. Тогда

$$G \simeq F/H = < f_1^* > \oplus \dots \oplus < f_n^* > / < h_1^* > \oplus \dots \oplus < h_l^* >$$

Если мы каждую из бесконечных циклических групп $< f_i^* >$ отождествим с группой $\mathbb{Z}$, то $< h_i^* >$ отождествится с $m_i\mathbb{Z}$. Получаем, что

$$G \simeq F/H = \mathbb{Z} \oplus \dots \oplus \mathbb{Z} \,/\, m_1\mathbb{Z} \oplus \dots \oplus m_l\mathbb{Z}$$

Здесь $\mathbb{Z} \oplus ... \oplus \mathbb{Z}$ содержит n слагаемых, $m_1\mathbb{Z} \oplus ... \oplus m_l\mathbb{Z}$ содержит l слагаемых. Добавим для равного количества слагаемых прямую сумму $n - l = r$ нулевых слагаемых $\{0\} \oplus ... \oplus \{0\}$:

$$G \simeq F/H = \mathbb{Z} \oplus ... \oplus \mathbb{Z} \,/\, m_1\mathbb{Z} \oplus ... \oplus m_l\mathbb{Z} \oplus \{0\} \oplus ... \oplus \{0\}$$

Тогда

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/m_l\mathbb{Z} \oplus \mathbb{Z}/\{0\} \oplus ... \oplus \mathbb{Z}/\{0\}$$

Получаем

$$G \simeq \mathbb{Z}_{m_1} \oplus ... \oplus \mathbb{Z}_{m_l} \oplus \mathbb{Z}^r$$

- разложили G в прямую сумму бесконечных и конечных циклических групп. Дальнейшее уже несложно – разложим $\mathbb{Z}_{m_i}$ в прямую сумму примарных циклических групп (это можно сделать по следствию из китайской теоремы об остатках). Получим

$$G \simeq \mathbb{Z}_{p_1^{k_1}} \oplus ... \oplus \mathbb{Z}_{p_s^{k_s}} \oplus \mathbb{Z}^r$$

Тем самым мы доказали существование такого разложения. Докажем единственность вида этого разложения.

Лемма 1. Пусть G – абелева группа. Множество $Tor\,(G)$ элементов конечного порядка в группе G – подгруппа в G. Она называется *подгруппой кручения* или *периодической частью* группы G.

Доказательство леммы 1.

- Нейтральный элемент 0 – элемент порядка 1, поэтому $0 \in Tor\,(G)$
- Пусть $g, h \in Tor\,(G) \Rightarrow \exists m, n \in \mathbb{N}$: $mg = nh = 0$. Тогда
$$mn(g + h) = nmg + mnh = n \cdot 0 + m \cdot 0 = 0 \Rightarrow g + h \in Tor\,(G)$$
- $m(-g) = -mg = 0 \Rightarrow -g \in Tor\,(G)$

Значит, $Tor\,(G)$ – подгруппа G. Лемма доказана. ■

Если G конечно порождена, то как мы доказали выше,

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{p_1^{k_1}} \oplus ... \oplus \mathbb{Z}_{p_s^{k_s}} \quad (*)$$

Тогда легко видеть, что подгруппа кручения $Tor\,(G)$ изоморфна прямой сумме конечных циклических слагаемых в этом разложении:

$$Tor\,(G) \simeq \mathbb{Z}_{p_1^{k_1}} \oplus ... \oplus \mathbb{Z}_{p_s^{k_s}}$$

- конечная группа.

В самом деле, рассмотрим произвольный элемент $g \in G$. В силу разложения (*) его можно понимать как набор r целых чисел и s вычетов по соответствующим модулям. Его порядок конечен тогда и только тогда, когда все r целых чисел равны нулю:

$$o(n_1, \dots, n_r, \bar{n}_{r+1}, \dots, \bar{n}_{r+s}) < \infty \Leftrightarrow n_1 = \dots = n_r = 0$$

Тогда

$$G/Tor\ (G) \simeq \mathbb{Z}^r$$

- свободная абелева группа ранга r.

Заметим, что подгруппа кручения $Tor\ (G)$ не зависит от разложения (*), так как $Tor\ (G)$ определяется по самой группе G. Но тогда и факторгруппа по группе кручения $G/Tor\ (G)$ также не зависит от разложения (*). В частности, отсюда следует ,что ранг r не зависит от разложения (*), потому что ранг свободной абелевой группы определен однозначно.

Осталось доказать, что набор $(p_1^{k_1}, \dots, p_s^{k_s})$ (тип кручения) определен однозначно. Начнем с того, что уточним лемму 1 – в лемме 1 мы рассматривали множество всех элементов конечного порядка, теперь рассмотрим множество элементов, порядок которых равен степени заданного простого числа.

Лемма 2. Пусть G – абелева группа, p – простое число. Множество $Tor_p\ (G)$ элементов порядка p^k $(p \geq 0)$ в группе G – подгруппа в G. Она называется *подгруппой p-кручения* или *p-периодической частью* группы G.

Доказательство леммы 2 аналогично доказательству леммы 1 ($m = p^k, n = p^l$). ■

Тогда для конечно порожденной абелевой группы G с разложением (*) легко видеть, что подгруппа p-кручения изоморфна прямой сумме примарных циклических слагаемых, для которых $p_i = p$:

$$Tor_p\ (G) \simeq \mathbb{Z}_{p^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p^{k_q}}$$

Действительно, включение $\supseteq$ следует из леммы 2, так как каждое из слагаемых $\mathbb{Z}_{p^{k_i}}$ состоит из элементов порядков p^l (следует из теоремы Лагранжа – порядок элемента должен делить порядок группы) $\Rightarrow$ их сумма тоже лежит в $Tor_p\ (G)$.
Включение $\subseteq$: рассмотрим произвольный элемент $g \in G$, который в силу разложения (*) может быть представлен как набор r целых чисел и s вычетов по соответствующим модулям:

$$o(n_1, \dots, n_r, \bar{n}_{r+1}, \dots, \bar{n}_{r+s}) = p^l$$

Порядок g равен p^l, если: $n_1 = \dots = n_r = 0$ и $p^l \cdot n_{r+i} \vdots p_i^{k_i}$. Отсюда следует, что $n_{r+i} \vdots p_i^{k_i}$ при $p_i \neq p$.

Теперь заметим, что точно так же, как и вся подгруппа кручения, подгруппа p-кручения также не зависит от разложения (*), так как подгруппа кручения разлагается в прямую сумму подгрупп p-кручений по всем простым числам, входящим в разложение (*). Осталось для каждой подгруппы p-кручения доказать, что вид ее разложения в прямую сумму примарных циклических слагаемых определен однозначно.
Таким образом, заменив группу G на ее подгруппу p-кручения $Tor_p\ (G)$, дальше можем считать, что G является p-примарной конечной абелевой группой:

$$|G| = p^n, \qquad G \simeq \mathbb{Z}_{p^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p^{k_s}}, \qquad k_1 + \dots + k_s = n,$$

также без ограничения общности можем считать, что $k_1 \leq k_2 \dots \leq k_s$. Докажем индукцией по n, что набор $(k_1, \dots, k_s)$ определен однозначно по группе G.

База индукции: $n = 0$. В этом случае $G = \{0\}$ – разложение не содержит ни одного слагаемого.

Шаг индукции: пусть $k_1 = \dots = k_t = 1 < k_{t+1} \dots \leq k_s$. Рассмотрим множество всех p-ых кратных элементов группы:

$$pG = \{pg \mid g \in G\}$$

- это подгруппа:

- $p \cdot 0 = 0 \in pG$
- $pg_1 + pg_1 = p(g_1 + g_2) \in pG$
- $-pg = p(-g) \in pG$

Заметим, что если G разложено в прямую сумму $G \simeq \mathbb{Z}_{p^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p^{k_s}}$, то

$$pG \simeq p\mathbb{Z}_{p^{k_1}} \oplus \dots \oplus p\mathbb{Z}_{p^{k_s}}$$

Подгруппа $p\mathbb{Z}_{p^k}$ будет состоять из всех вычетов по модулю p^k чисел, делящихся на p, т.е. это будет циклическая группа, порожденная вычетом $\bar{p}$. Ее порядок равен p^{k-1}, т.е. $p\mathbb{Z}_{p^k}$ изоморфна $\mathbb{Z}_{p^{k-1}}$:

$$p\mathbb{Z}_{p^k} = <\bar{p}> \simeq \mathbb{Z}_{p^{k-1}}$$

Заметим, что если $k = 1$, то

$$p\mathbb{Z}_{p^k} \simeq \{0\}$$

Таким образом,

$$pG \simeq p\mathbb{Z}_{p^{k_1-1}} \oplus \dots \oplus p\mathbb{Z}_{p^{k_s-1}} \simeq p\mathbb{Z}_{p^{k_{t+1}-1}} \oplus \dots \oplus p\mathbb{Z}_{p^{k_s-1}}$$

Поскольку pG не зависит от разложения (*) и определяется самой группой G, то мы можем применить предположение индукции: набор $(k_{t+1} - 1, \dots, k_s - 1)$ определен однозначно ⇒ определен однозначно набор $(k_{t+1}, \dots, k_s) \Rightarrow t = n - (k_{t+1} + \dots + k_s)$ тоже определено однозначно. Значит, и вид исходного разложения группы G определен однозначно. Теорема полностью доказана. ■

Обсудим еще одно понятие теории групп – экспоненту группы. Как мы знаем, порядок элемента группы – это наименьшая натуральная степень, в которую его нужно возвести, чтобы получить единицу. Если задаться вопросом – в какой наименьшей степени все элементы группы равны единице, мы приходим к понятию экспоненты группы.

Определение. Пусть G – группа (в мультипликативной записи). Ее *экспонента* – наименьшее $m \in \mathbb{N}$ такое, что $\forall g \in G\colon\ g^m = e$, или ∞, если таких m не существует. Обозначение: $m = e(G)$.

Замечания.
1). Если $e(G) < \infty$, то она равна наименьшему общему кратному порядков всех элементов группы: $e(G) = \text{НОК}(o(g) \mid g \in G$, поскольку $g^m = e \Leftrightarrow m \vdots o(g)$.
2). Если $|G| = n < \infty$, тогда по теореме Лагранжа $\forall g \in G\colon\ g^n = e \Rightarrow e(G) < \infty$ и $\forall g \in G\ \ o(g) \vdots n$, также (по предыдущему замечанию) $e(G)$ делит $n = |G|$.

Как мы видим, если группа конечна, то и ее экспонента конечна. Возникает вопрос – верно ли обратное, т.е. следует ли из конечности экспоненты группы конечность самой группы? В такой формулировке это, конечно же, неверно. Однако ,если добавить условие конечной порожденности группы, то мы получим интересную и трудную проблему теории групп, которая долгое время не была решена (проблема Бернсайда).

Проблема Бернсайда (ограниченная). Пусть G конечно порождена, $e(G) < \infty$. Верно ли, что $|G| < \infty$?

Условие конечной порожденности необходимо, иначе в качестве контрпримера можно рассмотреть, например, $G = \mathbb{Z}_m \times \mathbb{Z}_m \times \ldots = \mathbb{Z}_m^\infty$ - группу, состоящую из бесконечных наборов вычетов по модулю m – ясно, что $|G| = \infty$, но $e(G) = m$.

Также можно рассматривать неограниченную проблему Бернсайда: верно ли, что если все элементы конечно порожденной группы имеют конечный порядок (неограниченно большой), то такая группа конечна?
Ответ: нет (П. С. Новиков, С. И. Адян, 1968 г).
Ограниченную проблему Бернсайда чуть ранее решил (ответ также отрицательный) Е. С. Голод, учившийся и работавший, (как и П. С. Новиков, С. И. Адян) на мехмате МГУ.

Однако, для абелевых групп ответ: да – конечно порожденная абелева группа с конечной экспонентой обязательно конечна. Это следует из теоремы о структуре конечно порожденных абелевых групп, которую мы только что доказали: подгруппа p-кручения (множество элементов конечного порядка) в конечно порожденной абелевой группе – конечная группа, поэтому если группа имеет конечную экспоненту (т.е. все элементы имеют конечный порядок), то она конечна.
С помощью этой же теоремы легко найти экспоненту любой конечной абелевой группы.

Лемма 3. Для конечной абелевой группы $G \simeq \mathbb{Z}_{m_1} \oplus ... \oplus \mathbb{Z}_{m_s}$ верно равенство

$$e(G) = \text{НОК}(m_1, \dots, m_s).$$

Доказательство.
Пусть для краткости $m = \text{НОК}(m_1, \dots, m_s)$ и заметим, что $\forall g = (\bar{n}_1, \dots, \bar{n}_s) \in G$, $\bar{n}_i = n_i \bmod m_i$ выполнено

$$m \cdot g = (\overline{mn}_1, \dots, \overline{mn}_s) = (\bar{0}, \dots, \bar{0}) = 0,$$

так как $m = \text{НОК}(m_1, \dots, m_s)$ и $mn_i \vdots m_i$ для всех $i = 1, \dots, s$. Отсюда следует, что $e(G) \leq m$.
С другой стороны, для $g = (\bar{1}, \dots, \bar{1})$ имеем:

$$n \cdot g = (\bar{n}, \dots, \bar{n}) = 0 \Leftrightarrow n \vdots m_i, \forall i = 1, \dots, s \Leftrightarrow n \vdots m$$

Следовательно,

$$o(g) = m \Rightarrow e(G) \geq m$$

Таким образом,

$$e(G) = m$$

■
Следующая теорема дает критерий цикличности конечной абелевой группы с помощью экспоненты.

Теорема 1. Для конечной абелевой группы G следующие условия эквивалентны:
1) G циклична,
2) $e(G) = |G|$.

Доказательство.
1) ⇒ 2): если G циклична, то $G = < g >$, $o(g) = |G|$. Отсюда следует, что $e(G) \geq |G|$. Но (см. замечание 2 на предыдущей странице) $e(G)$ делит $|G|$, поэтому $e(G) = |G|$.

2) ⇒ 1): так как G – конечная абелева группа, то $G \simeq \mathbb{Z}_{m_1} \oplus ... \oplus \mathbb{Z}_{m_s}$. Тогда

$$|G| = m_1 \cdot \dots \cdot m_s = n$$
$$e(G) = \text{НОК}(m_1, \dots, m_s) = m$$

Если $m = n$, то числа $m_1, \dots, m_s$ попарно взаимно просты. Тогда (по китайской теореме об остатках) $G \simeq \mathbb{Z}_n$. ■

У этой теоремы есть одно замечательное приложение в теории полей – оказывается, любая конечная подгруппа в мультипликативной группе поля всегда будет циклической.

Теорема 2. Пусть K – поле. Тогда ∀ конечная подгруппа $G \subseteq K^\times$ - циклическая.

Доказательство.

Заметим, что группа G абелева, так как $K^\times$ абелева. Пусть $|G| = n, e(G) = m < n$. Имеем: $\forall g \in G\colon\ g^m = 1$, откуда следует, что многочлен $x^m - 1 \in K[x]$ имеет как минимум n различных корней (так как его корнями являются как минимум $x = g \in G$). Поэтому $n \leq m$. Следовательно, $m = n$. Тогда (по теореме 1) группа G циклическая. ■

Следствие. K конечно ⇒ $K^\times$ циклическая.

Пример: $K = \mathbb{Z}_p$ (p простое) ⇒ $K^\times \simeq \mathbb{Z}_{p-1}$ (так как $K^\times$ - группа порядка $p - 1$).

$p = 2,3 \Rightarrow p - 1 = 1,2$ – можно понять, что $K^\times$ циклическая и без теоремы 2.
$p = 5 \Rightarrow |K^\times| = 4$. Из классификации конечных абелевых групп следует, что может быть два варианта:

$$K^\times \simeq \mathbb{Z}_4 \text{ или } K^\times \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Но из теоремы 2 следует, что $K^\times \simeq \mathbb{Z}_4$: действительно, $K^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, в качестве порождающего элемента можно взять $\overline{2}$.

Лекция 8. Действия групп на множествах.

Начнем с небольшого экскурса в историю. Группы возникли в математике как группы преобразований некоторых множеств. Впервые понятие группы появилось в работах Галуа по разрешимости алгебраических уравнений (т.н. группы Галуа), затем появились группы линейных и других преобразований различных пространств и т.д. Группы преобразований занимают особое место и в теории групп, и в ее приложениях за пределами алгебры.
Элементы группы преобразований можно применять к точкам множества, на котором эти преобразования действуют. Не всегда бывает удобно считать, что разные элементы группы задают разные преобразования, однако важно, чтобы произведению элементов группы соответствовала композиция преобразований. Все эти наблюдения ведут к определению понятия действия группы на множестве как гомоморфизма из данной группы в группу преобразований этого множества.

Определение 1. Действие группы G на множестве X – это гомоморфизм

$$\alpha\colon\ G \to S(X)$$
$$g \mapsto \alpha_g$$

Гомоморфизм α задает операцию действия элемента группы G на точку множества X:

$$g \circ x = \alpha_g(x), \qquad \forall g \in G, x \in X$$

Если обратить внимание на свойства, которым удовлетворяет α, можно прийти к альтернативному определению действия:

Определение 2. Действие группы G на множестве X – это отображение

$$G \times X \to X$$
$$(g, x) \mapsto g \circ x$$

со следующими свойствами: $\forall g_1, g_2 \in G, x \in X$
1) $g_1 \circ (g_2 \circ x) = (g_1 g_2) \circ x$
2) $e \circ x = x$

Определения 1 и 2 эквивалентны:
1) $\Rightarrow$ 2): с помощью гомоморфизма $\alpha\colon\ G \to S(X)$ мы уже определили соответствующую операцию $g \circ x = \alpha_g(x)$. Проверим, что она удовлетворяет свойствам из определения 2):

1) $g_1 \circ (g_2 \circ x) = \alpha_{g_1}(\alpha_{g_2}(x)) = (\alpha_{g_1} \circ \alpha_{g_2})(x) = \alpha_{g_1 g_2}(x) = (g_1 g_2) \circ x$
2) $\alpha_e = id_X$ (т.к. α - гомоморфизм), поэтому $e \circ x = x$, $\forall x \in X$

2) $\Rightarrow$ 1): $\forall g \in G$ определим отображение $\alpha_g: X \to X$ по формуле $\alpha_g(x) = g \circ x$, $\forall x \in X$.
Свойства α_g:
а) $\alpha_{g_1} \circ \alpha_{g_2} = \alpha_{g_1 g_2}$ (следует из свойства 1) определения 2)
б) $\alpha_e = id_X$ (следует из свойства 2) определения 2)
в) $\forall g \in G$: α_g – биекция (так как существует обратное отображение $(\alpha_g)^{-1} = \alpha_{g^{-1}}$ – это вытекает из свойств а) и б): $\alpha_g \circ \alpha_{g^{-1}} = \alpha_{g^{-1}} \circ \alpha_g = \alpha_{gg^{-1}} = \alpha_e = id_X$)
Следовательно, отображение

$$\alpha: G \to S(X)$$
$$g \mapsto \alpha_g$$

- гомоморфизм. ■

Обозначение действия:

$$G \curvearrowright X$$

Примеры действий.
1) $S(X) \curvearrowright X$ – тавтологическое действие: $\varphi \circ x = \varphi(x)$

$$\alpha = id: S(X) \to S(X)$$

2) $GL_n(K) \curvearrowright K^n$ – умножение матрицы на столбец: $A \circ Y = A \cdot Y$, $\forall A \in GL_n(K)$, $\forall Y \in K^n$

$$\alpha_A: K^n \to K^n$$

- линейный оператор, задаваемый матрицей A.

3) Обсудим, как группа G действует на себе самой. Приведем три стандартных примера.

- $G \curvearrowright G$ умножениями слева: $g \circ x = g \cdot x$

Если мы аналогично определим действие умножениями справа: $g \circ x = x \cdot g$, то не будет выполняться первое свойство определения 2) действия группы: проверим свойство 1) для умножения справа:

$$g_1 \circ (g_2 \circ x) = (x \cdot g_2) \cdot g_1 = x \cdot (g_2 g_1)$$

результат должен быть равен

$$(g_1 g_2) \circ x = x \cdot (g_1 g_2)$$

т.е. свойство 1) не выполняется, если элементы g_1 и g_2 не коммутируют. Чтобы это свойство выполнялось, нужно определить умножение справа как $g \circ x = x \cdot g^{-1}$:

- $G \curvearrowright G$ умножениями справа: $g \circ x = x \cdot g^{-1}$

Тогда

$$g_1 \circ (g_2 \circ x) = (x \cdot {g_2}^{-1}) \cdot {g_1}^{-1} = x \cdot ({g_2}^{-1} {g_1}^{-1}) = x \cdot (g_1 g_2)^{-1} = (g_1 g_2) \circ x$$

- $G \curvearrowright G$ сопряжениями: $g \circ x = g \cdot x \cdot g^{-1}$
  $\alpha_g = i_g$ – внутренний автоморфизм

Оказывается, само понятие действия группы на множестве приводит к некоторым нетривиальным результатам – с его помощь можно доказывать вполне содержательные теоремы. Первая теорема, которую мы рассмотрим и которая иллюстрирует применение понятия действия группы – это теорема Кэли.

Теорема Кэли. Любая группа G изоморфна подгруппе в $S(G)$.

Следствие. Если $|G| = n < \infty$, то G изоморфна некоторой подгруппе в S_n (другими словами, группы подстановок – универсальные группы, в которые вкладывается любая другая группа).

Доказательство.
Действие $G \curvearrowright G$ умножениями слева задает гомоморфизм

$$\alpha\colon\ G \to S(G)$$
$$g \mapsto \alpha_g$$
$$\alpha_g(x) = g \cdot x$$

α инъективен: если $g_1 \neq g_2$, то и $\alpha_{g_1} \neq \alpha_{g_2}$. Действительно,

$$\alpha_{g_1}(e) = g_1 \cdot e = g_1 \neq g_2 = g_2 \cdot e = \alpha_{g_2}(e)$$

Следовательно, $G \simeq Im(\alpha) \subset S(G)$. ■

Рассмотрим еще некоторые общие понятия теории действий. Пусть задано действие $G \curvearrowright X$, задающее гомоморфизм $\alpha\colon\ G \to S(X)$.

Определение 3. $Ker(\alpha)$ – ядро неэффективности действия (т.е. это элементы группы G, которые действуют на точки X тривиально). Действие эффективно, если $Ker(\alpha) = \{e\}$.

Любое действие сводится к эффективному путем факторизации по ядру неэффективности: по основной теореме о гомоморфизмах

$$\alpha \overset{\pi}{\to} G/Ker(\alpha) = \bar{G} \twoheadrightarrow Im(\alpha) \subseteq S(X)$$

Если задано действие $G \curvearrowright X$, то можно задать эффективное действие $\bar{G} \curvearrowright X$ по следующему правилу:

$$\forall \bar{g} = g \cdot Ker(\alpha), \forall x \in X\colon\quad \bar{g} \circ x = g \cdot x$$

Для эффективного действия $G \curvearrowright X$ выполнено $G \twoheadrightarrow Im(\alpha) \subseteq S(X)$.

Далее будем как правило обозначать операцию действия как умножение: "$\cdot$" вместо "$\circ$".

Пусть задано $G \curvearrowright X$.
Определение. Эквивалентность точек множества относительно действия группы:

$$x \underset{G}{\sim} y \to y, \text{ если } \exists g \in G\colon\ g \cdot x = y$$

Проверим, что это действительно отношение эквивалентности:

- Рефлексивность: $x \underset{G}{\sim} x = e \cdot x$
- Симметричность: $x \underset{G}{\sim} y = g \cdot x \Rightarrow y \underset{G}{\sim} x = g^{-1} \cdot y$
- Транзитивность: $x \underset{G}{\sim} y \underset{G}{\sim} z \ \Rightarrow\ y = g \cdot x,\ z = g' \cdot y = g' \cdot (g \cdot x) = (g'g) \cdot x \ \Rightarrow\ x \underset{G}{\sim} z$

Отношение эквивалентности по действию группы G разбивает множество X на попарно непересекающиеся классы эквивалентности, которые называются *орбитами* для действия группы G на множестве X:

$$G \cdot x = \{y = g \cdot x \mid g \in G\}$$

- орбита точки $x \in X$.

Основное свойство орбит: орбиты образуют разбиение X на попарно непересекающиеся подмножества.

Определение. Действие $G \curvearrowright X$ называется транзитивным, если X состоит из одной орбиты.

Примеры орбит.
1) $SO_2(\mathbb{R}) \curvearrowright \mathbb{R}^2$ умножениями матриц на столбцы.
Матрицы $A \in SO_2(\mathbb{R})$ имеют вид:

$$A = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

Преобразование α_A множества $\mathbb{R}^2$, соответствующее этой матрице – это поворот плоскости вокруг начала координат на угол φ:

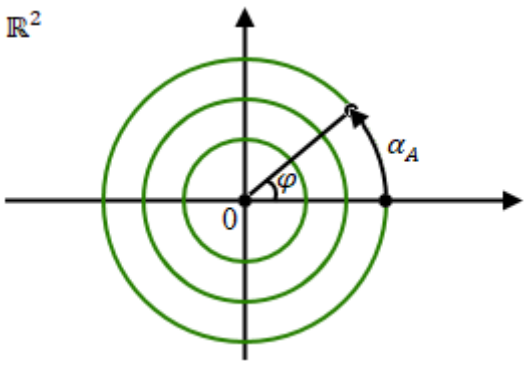


Рис.8.1. Орбиты – концентрические окружности

Орбиты – концентрические окружности $\{x^2 + y^2 = const\}$ и неподвижная точка $\{0\}$. Этот пример хорошо объясняет название “орбита”.

2) $GL_n(K) \curvearrowright Mat_n(K)$ сопряжениями:

$$C \circ A = C \cdot A \cdot C^{-1}$$

С каждой квадратной матрицей A связан линейный оператор $\mathcal{A}$: $K^n \to K^n$, который задается матрицей A в стандартном базисе. Как известно из линейной алгебры, $C \cdot A \cdot C^{-1}$ – это матрица оператора $\mathcal{A}$ в другом базисе, C – матрица перехода (любая невырожденная матрица).

Орбита матрицы A = {матрицы оператора $\mathcal{A}$ во всевозможных базисах K^n}.

3) Пусть

$$S_n \ni \sigma = (i_1, \dots, i_l) \cdot (j_1, \dots, j_k) \cdot \dots \cdot (k_1, \dots, k_m)$$

– разложение подстановки σ на независимые циклы. Рассмотрим

$$G = <\sigma> \curvearrowright X = \{1, \dots, n\}$$

Пусть

$$\{1, \dots, n\} = \{i_1, \dots, i_l, j_1, \dots, j_k, \dots, k_1, \dots, k_m, l_1, \dots, l_r\}$$

т.е. множество $\{1, \dots, n\}$ состоит из номеров, которые входят в независимые циклы и неподвижных элементов $l_1, \dots, l_r$. Орбиты:

$$O_1 = \{i_1, \dots, i_l\},$$
$$O_2 = \{j_1, \dots, j_k\},$$
$$\dots$$
$$O_s = \{k_1, \dots, k_m\},$$
$$O_{s+1} = \{l_1\}, \dots, O_{s+r} = \{l_r\}$$

Таким образом, понятие орбиты цикла, которое мы ввели в первом семестре, является частным случаем понятия орбиты действия группы на множестве.

4) Пусть $H \subseteq G$ – подгруппа. Рассмотрим $H \curvearrowright G$ умножениями слева/справа: $h \circ g = h \cdot g$ или $g \cdot h^{-1}$.
Орбиты – это правые / левые смежные классы по подгруппе H.

С понятием орбиты связано еще одно важное понятие в теории действий – понятие стабилизатора.

Определение. Пусть задано $G \curvearrowright X$. Стабилизатор точки $x \in X$ (обозначение: G_x) – это множество всех элементов группы G, действие которых оставляет точку x на месте:

$$G_x = \{g \in G:\ g \cdot x = x\}$$

Предложение. 1) $H = G_x$ – подгруппа в G, 2) Если $x \underset{G}{\sim} y = g \cdot x$, то $G_y = g \cdot H \cdot g^{-1}$.

Доказательство.
1)

- $e \in H$, так как $e \cdot x = x$
- Пусть $g, g' \in H$. Тогда $(gg') \cdot x = g \cdot (g' \cdot x) = g \cdot x = x$. Значит, $gg' \in H$.
- $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$. Значит, $g^{-1} \in H$.

2) Пусть элемент $h \in H$ оставляет точку y на месте: $h \cdot y = y$. Запишем это как $h \cdot (g \cdot x) = g \cdot x$ и подействуем на обе части получившегося равенства элементом g^{-1}, получим:

$$g^{-1} \cdot h \cdot g \cdot x = x \Leftrightarrow g^{-1}hg \in H \Leftrightarrow h \in g \cdot H \cdot g^{-1}$$

■

Теорема. Существует взаимно-однозначное соответствие между точками орбиты точки x и множеством левых смежных классов группы G по стабилизатору точки x:

$$G \cdot x \leftrightarrow\ G/G_x$$
$$y = g \cdot x \leftrightarrow g \cdot G_x$$

Доказательство.
Рассмотрим отображение

$$G \cdot x \to\ G/G_x$$
$$y = g \cdot x \mapsto g \cdot G_x$$

Поймем, почему это отображение корректно определено (одна и та же точка y может получаться из x действием разных элементов группы G – нужно проверить, что все они соответствуют одному и тому же смежному классу справа).
Пусть

$$y = g \cdot x = g' \cdot x$$

- подействуем на обе части равенства элементом g^{-1}:

$$g^{-1} \cdot g' \cdot x = x \Rightarrow g^{-1} \cdot g' = h \in G_x \Rightarrow g' = g \cdot h, h \in G_x$$

т.е. элементы g и g' принадлежат одному и тому же смежному классу: $g \cdot G_x = g' \cdot G_x$. Поэтому отображение определено корректно, кроме того, оно инъективно: предположим, что

$$g \cdot G_x = g' \cdot G_x$$

Тогда $g' = g \cdot h$ для некоторого $h \in G_x$, откуда $g' \cdot x = g \cdot h \cdot x$. Но $h \in G_x$, поэтому $h \cdot x = x$ и $g' \cdot x = g \cdot x$. Таким образом, если два элемента лежат в одном смежном

классе по стабилизатору, то при действии этих элементов на некоторую точку x мы получим одну и ту же точку из орбиты.
Сюръективность отображения очевидна. Следовательно, мы установили взаимно-однозначное соответствие

$$G \cdot x \leftrightarrow G/G_x$$
$$y = g \cdot x \leftrightarrow g \cdot G_x$$

■

Следствие. Для действий конечной группы:

$$|G \cdot x| = \frac{|G|}{|G_x|}$$

(следует из предыдущей теоремы и теоремы Лагранжа).

Пример. Проиллюстрируем применение этого следствия. Пусть $C \subset E^3$ – куб. Рассмотрим группу его собственных движений $G = Isom^+C$. Всякое движение, оставляющее куб на месте, имеет неподвижную точку (центр куба), поэтому все собственные движения куба – это вращения относительно прямых, проходящих через центр куба, т.е. $G = Isom^+C$ – группа вращений куба.

а) При движении, оставляющем на месте куб, вершины куба каким-то образом переставляются, поэтому можно говорить о действии группы G на множество вершин куба:

$$G \curvearrowright X = \{\text{вершины } C\}$$

Это действие, очевидно, транзитивно (любую вершину некоторой последовательностью вращений можно перевести в любую другую).
Зафиксируем некоторую вершину $x \in X$ и найдем ее стабилизатор (т.е. найдем вращения куба, оставляющие x на месте) - это должно быть вращение относительно оси, проходящей через точку x и через центр куба. Куб переходит в себя при поворотах на $\frac{2\pi k}{3}, k \in \mathbb{Z}$ относительно этой оси:

$$G_x = \{\text{повороты на } \frac{2\pi k}{3} \text{ вокруг } l = \overline{Ox}\} \simeq \mathbb{Z}_3$$

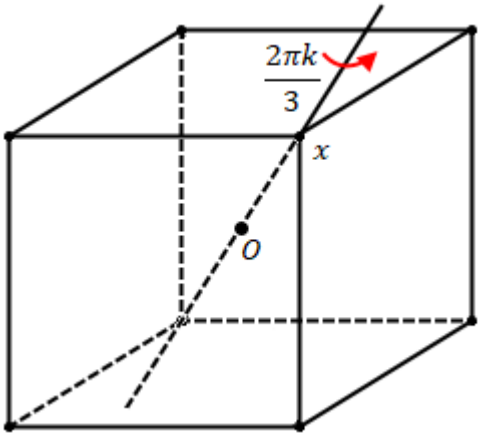


Рис. 8.2. Стабилизатор вершины x

Так как действие транзитивно, то орбита x – это все вершины куба:

$$G \cdot x = X$$

Тогда

$$|G| = |G \cdot x| \cdot |G_x| = |X| \cdot |G_x| = 8 \cdot 3 = 24$$

Таким образом, группа вращений куба состоит из 24 элементов. Поймем, как она устроена.

б) рассмотрим действие группы G на множестве диагоналей куба:

$$G \curvearrowright Y = \{\text{диагонали } C\}$$

Поскольку действие можно рассматривать как гомоморфизм группы перестановок данного множества, то

$$\alpha\colon\ G \to S(Y) \simeq S_4$$

Таким образом, $|S_4| = |G| = 24$. Докажем, что α – изоморфизм: его ядро (т.е. те вращения куба, которые каждую диагональ оставляют на месте) – это тождественное преобразование, так как диагонали куба – четыре не взаимно перпендикулярных прямых:

$$Ker\,\alpha = \{e\}$$

Таким образом, гомоморфизм α инъективен и $G \approx Im(\alpha)$. Так как $|G| = 24$, то и $|Im(\alpha)| = 24$. Но и $|S_4| = 24$, поэтому $Im(\alpha) = S_4$.

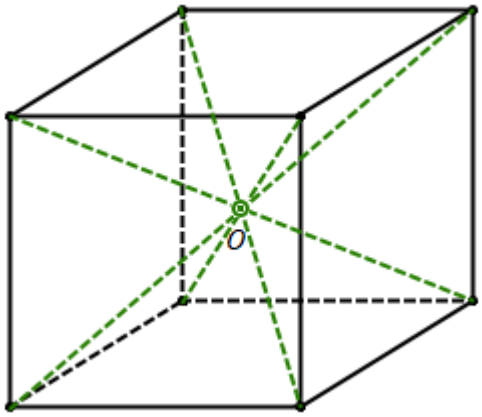


Рис. 8.3. $G \simeq S_4$

Вывод: группа вращений куба $G = Isom^+C$ изоморфна группе S_4 – каждому вращению куба можно сопоставить перестановку его диагоналей.

Лекция 9. Действие произвольной группы на себе самой сопряжениями. Коммутант.

Продолжим обсуждение группы вращений куба, начатое на прошлой лекции. Рассмотрим действие группы G на множестве прямых, соединяющих центры противоположных граней куба:

$$G \curvearrowright Z = \{\text{прямые, соединяющие центры противоположных граней } C\}$$

Это действие задает гомоморфизм

$$\beta: Isom^+ C \to S(Z) \simeq S_3$$

Ядро этого гомоморфизма состоит из всех вращений куба, которые оставляют прямые из Z на месте. Если вращение оставляет на месте прямую, то это либо вращение вокруг этой прямой, либо вращение вокруг перпендикулярной ей прямой на 180^0, поэтому ядро β состоит из вращений на πk вокруг прямых из Z:

$$Ker\,\beta = \{\text{повороты на } \pi k \ (k = 0,1) \text{ вокруг } l \in \mathbb{Z}\}$$

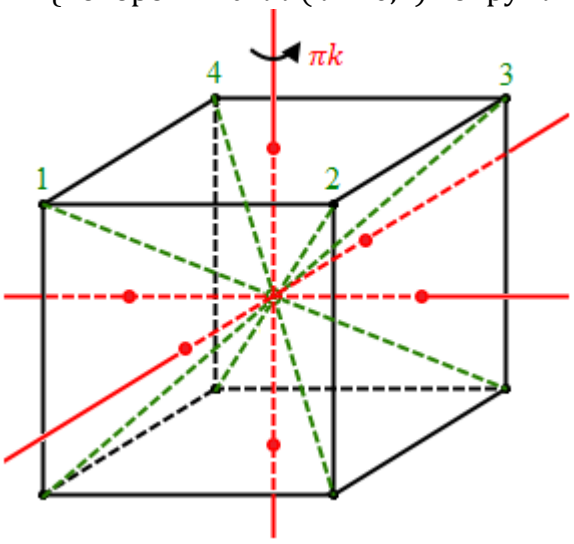


Рис. 9.1. К примеру $G \curvearrowright Z$

Поймем, какие подстановки на диагоналях куба соответствуют таким поворотам. В силу симметричности куба рассмотрим поворот относительно одной из осей (см. рис. 9.1) – повороту вокруг такой оси на πk $(k = 0,1)$ соответствуют перестановки диагоналей ε и $(1,3)(2,4)$. Поворотам относительно других осей $l \in \mathbb{Z}$ соответствуют перестановки $(1,2)(3,4)$ и $(1,4)(2,3)$. Таким образом, при изоморфизме α:

$$Ker\,\beta \twoheadrightarrow \{\varepsilon, (1,3)(2,4), (1,2)(3,4), (1,4)(2,3)\} = V_4 \lhd S_4$$

- нормальная подгруппа в S_4. Эта группа V_4 называется *четверной группой Клейна*. Ее особенность заключается в том, что каждый элемент в квадрате дает нейтральный. Также

V_4 является абелевой группой и является прямым произведением своих подгрупп порядка 2. Отсюда следует, что

$$V_4 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Теперь найдем $Im\,\beta$. Это подгруппа в S_3 – по основной теореме о гомоморфизмах,

$$S_3 \supseteq Im\,\beta \simeq Isom^+C / Ker\,\beta \simeq S_4/V_4$$

Так как $|S_3| = 6$, то $|Im\,\beta| \leq 6$. С другой стороны, $|S_4/V_4| = 24/4 = 6$. Отсюда следует, что $Im\,\beta = S_3$ – гомоморфизм β сюръективен.

В результате:

$$\varphi = \beta \circ \alpha^{-1}\colon\ S_4 \to S_3$$

- *эпиморфизм* (сюръективный гомоморфизм),

$$Ker\,\varphi = V_4$$
$$S_4/V_4 \simeq S_3$$

На прошлой лекции мы обсуждали примеры действий, рассмотрим один из них более подробно.

Действие $G \curvearrowright G$ сопряжениями.

$$g \circ x = g \cdot x \cdot g^{-1}$$

Орбиты – *классы сопряженности*:

$$C_G(x) = C(x) = \{y = g \cdot x \cdot g^{-1} \mid g \in G\}$$

Стабилизаторы – *централизаторы*:

$$Z_G(x) = Z(x) = \{g \in G \mid g \cdot x \cdot g^{-1} = x\} \Leftrightarrow \{g \in G \mid g \cdot x = x \cdot g\}$$

Другими словами, централизатор элемента x – это множество всех элементов группы, которые коммутируют с элементом x.

Гомоморфизм действия:

$$i\colon G \to Aut(G) \subseteq S(G)$$
$$g \mapsto i_g$$ – внутренний автоморфизм

Ядро неэффективности:

$$Ker\,i = Z(G) = \{g \in G \mid g \cdot h \cdot g^{-1} = h, \forall h \in G\}$$

– это центр группы (т.е. элементы, которые при сопряжении оставляют любую точку на месте). Также центр группы – это те элементы, которые коммутируют со всеми элементами группы:

$$Z(G) = \{g \in G \mid g \cdot h = h \cdot g, \forall h \in G\},$$

что равносильно еще одному определению:

$$Z(G) = \{g \in G \mid h \cdot g \cdot h^{-1} = g, \forall h \in G\}\} \Leftrightarrow \{g \in G \mid C(g) = \{g\}\}$$

- центр состоит из элементов g, для которых класс сопряженности состоит из одного элемента $\{g\}$.

Таким образом, центр группы – это множество неподвижных точек действия. Также можно сказать, что центр группы – это множество элементов, централизатор которых совпадает со всей группой:

$$Z(G) = \{g \in G \mid Z(g) = G\}$$

Примеры:

1) $G = GL_n(\mathbb{C})$.

Классы сопряженности состоят из всех матриц с одинаковой жордановой нормальной формой (как известно из линейной алгебры, две комплексных матрицы сопряжены тогда и только тогда, когда их ЖНФ совпадают)

2) $Z\big(GL_n(K)\big) = \{\lambda \cdot E \mid \lambda \in K^{\times}\}$

Центр группы невырожденных матриц – это группа скалярных матриц. Действительно, скалярные матрицы коммутируют с произвольной матрицей – включение $\supseteq$ очевидно. Докажем включение $\subseteq$: пусть $A \in Z\big(GL_n(K)\big)$, т.е.

$$A \cdot B = B \cdot A, \qquad \forall B \in Z\big(GL_n(K)\big)$$

Возьмем $B = E + E_{ij}$ $(i \neq j)$, где E_{ij} – матрица, с единственным ненулевым элементом 1, стоящим в i-ой строке и j-ом столбце. Другими словами, B – матрица элементарного преобразования 1-го типа, соответствующая прибавлению к i-ой строке j-ой строки. Тогда (так как единичная матрица E коммутирует с любой матрицей):

$$A \cdot B = B \cdot A \Leftrightarrow A \cdot E_{ij} = E_{ij} \cdot A$$

Но результат произведения $A \cdot E_{ij}$ – это матрица, j-ый столбец которой равен i-ому столбцу матрицы A (остальные элементы будут нулевыми), а результат произведения $A \cdot E_{ij}$ – это матрица, i-ая строка которой равна j-ой строке матрицы A (остальные элементы будут нулевыми).

$$A \cdot E_{ij} = \begin{array}{c} \\ i \\ \\ \end{array}\!\!\begin{array}{|c|c|c|}\hline 0 & a_{1i} & 0 \\ \hline \vdots & \vdots & \vdots \\ \hline 0 & a_{ni} & 0 \\ \hline \end{array} = \begin{array}{c} \\ i \\ \\ \end{array}\!\!\begin{array}{|c|c|c|}\hline 0 & \vdots & 0 \\ \hline a_{j1} \cdots & * & \cdots a_{jn} \\ \hline 0 & \vdots & 0 \\ \hline \end{array} = E_{ij} \cdot A$$

j $\qquad$ j

Рис. 9.2. Иллюстрация к равенству $A \cdot E_{ij} = E_{ij} \cdot A$

Отсюда следует, что

$$a_{ii} = a_{jj},$$
$$a_{ki} = 0, \forall k \neq i,$$
$$a_{jl} = 0, \forall l \neq j,$$

что и означает, что $A = \lambda \cdot E$.

3) $G = S_n$

Рассмотрим, как устроены классы сопряженности в группе подстановок. По определению,

$$C(\sigma) = \{\pi \cdot \sigma \cdot \pi^{-1} \mid \pi \in S_n\}$$

а) $\sigma = (i_1, \dots, i_l)$ – цикл.

Для наглядности изобразим цикл графически. Цикл – это подстановка, которая циклически переставляет элементы орбиты, а все номера, не вошедшие в орбиту этого цикла, переходят сами в себя:

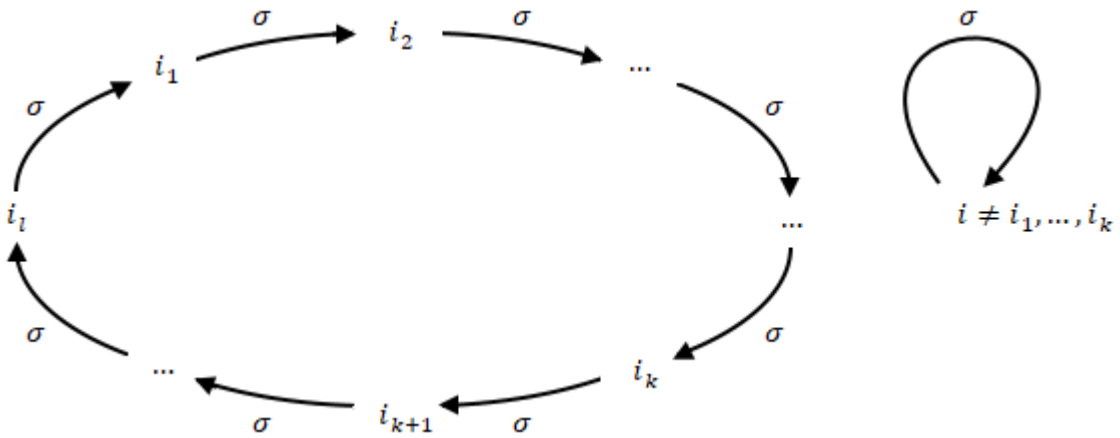


Рис. 9.3. Цикл

Поймем, куда переводит перестановка $\pi \cdot \sigma \cdot \pi^{-1}$ произвольный номер j. Рассмотрим два случая:

1) $\pi^{-1}(j)$ не попал в орбиту цикла σ, т.е. $j \notin \{\pi(i_1), \dots, \pi(i_l)\}$. Тогда (см. рис. 9.4):

$$\pi \cdot \sigma \cdot \pi^{-1}(j) = j$$

2) $\pi^{-1}(j)$ попал в орбиту цикла σ, т.е. $j = \pi(i_k)$. Тогда (см. рис. 9.4):

$$\pi \cdot \sigma \cdot \pi^{-1}(j) = \pi(i_{k+1})$$

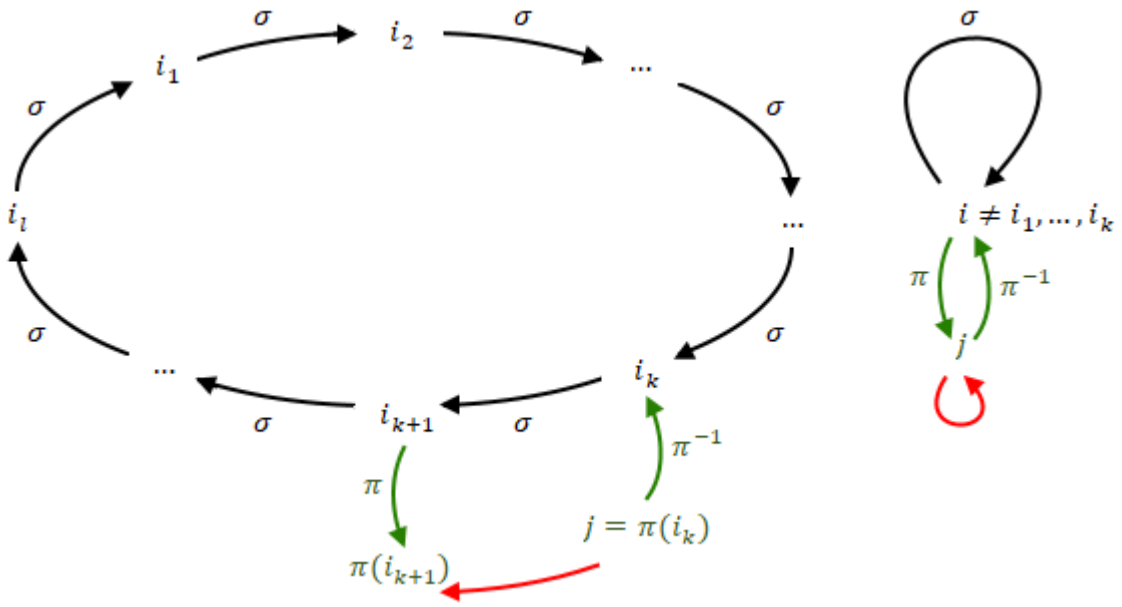


Рис. 9.4. $\pi \cdot \sigma \cdot \pi^{-1}(j) = \pi(i_{k+1})$ и $\pi \cdot \sigma \cdot \pi^{-1}(j) = j$

Таким образом,

$$\pi \cdot \sigma \cdot \pi^{-1} = (\pi(i_1), \dots, \pi(i_l))$$

- цикл той же длины.

б) Общий случай. Разложим подстановку σ в произведение независимых циклов:

$$\sigma = (i_1, \dots, i_l) \cdot (j_1, \dots, j_m) \cdot \dots \cdot (k_1, \dots, k_p)$$

Так как операция сопряжения является автоморфизмом, то сопряженное к произведению подстановок является произведением сопряженных к каждому сомножителю:

$$\pi \cdot \sigma \cdot \pi^{-1} = \pi \cdot (i_1, \dots, i_l) \cdot \pi^{-1} \cdot \pi \cdot (j_1, \dots, j_m) \cdot \pi^{-1} \cdot \dots \cdot \pi \cdot (k_1, \dots, k_p) \cdot \pi^{-1} =$$
$$= (\pi(i_1), \dots, \pi(i_l)) \cdot (\pi(j_1), \dots, \pi(j_m)) \cdot \dots \cdot (\pi(k_1), \dots, \pi(k_p))$$

- получили разложение подстановки $\pi \cdot \sigma \cdot \pi^{-1}$ в произведение независимых циклов (циклы будут независимыми, так как подстановка π является взаимно-однозначным отображением, а циклы, в произведение которых мы разложили подстановку σ, не пересекались).
Таким образом, сопряженная подстановка $\pi \cdot \sigma \cdot \pi^{-1}$ разлагается в произведение стольких же циклов таких же длин, на которые разлагается исходная подстановка σ, т.е. имеет ту же цикловую структуру.

в) Обратно, если

$$\sigma' = (i'_1, \dots, i'_l) \cdot (j'_1, \dots, j'_m) \cdot \dots \cdot (k'_1, \dots, k'_p)$$

- подстановка σ' имеет ту же цикловую структуру, что и σ, то

$$\sigma' = \pi \cdot \sigma \cdot \pi^{-1},$$

где

$$\pi = \begin{pmatrix} i_1 & \dots & i_l & j_1 & \dots & j_m & \dots & k_1 & \dots & k_p & l_1 & \dots & l_q \\ i'_1 & \dots & i'_l & j'_1 & \dots & j'_m & \dots & k'_1 & \dots & k'_p & l'_1 & \dots & l'_q \end{pmatrix}$$

($l_1, \dots, l_q$ и $l'_1, \dots, l'_q$ - оставшиеся номера). Таким образом, любые две подстановки с одинаковой цикловой структурой сопряжены между собой. Сопрягающая подстановка определена неоднозначно (например, цикл можно начинать с другого места и менять циклы одинаковой длины местами).

Вывод: классы сопряженности в группе подстановок S_n состоят из всех подстановок одинаковой цикловой структуры.

С помощью этого результата мы можем ответить на вопрос, как устроен центр S_n. Воспользуемся следующим определением центра:

$$Z(S_n) = \{\sigma \in S_n \mid C(\sigma) = \{\sigma\}\}$$

- центр S_n состоит из подстановок, класс сопряженности которых состоит только из нее самой. Другими словами, σ – единственная подстановка с данной цикловой структурой. Предположим, что в разложении σ на циклы есть цикл длины, большей 2:

$$\sigma = (i_1, i_2, \dots, i_l) \cdot (\dots) \cdot \dots \quad , l > 2$$

Тогда легко можно предъявить другую подстановку той же самой цикловой структуры (просто поменяв местами i_1 и i_2):

$$\sigma = (i_2, i_1, \dots, i_l) \cdot (\dots) \cdot \dots$$

- таким образом, σ не может содержать в своем разложении циклы длиной больше двух. Пусть σ является произведением нескольких независимых транспозиций:

$$\sigma = (i_1, i_2) \cdot (j_1, j_2) \cdot \dots$$

Тогда, если таких транспозиций хотя бы две, мы снова можем переставить элементы местами и получить другую подстановку той же самой цикловой структуры:

$$\sigma = (i_1, j_1) \cdot (j_2, i_2) \cdot \dots$$

Значит, такие подстановки тоже не лежат в центре S_n. Если же σ состоит только из одной транспозиции, при этом $n > 2$:

$$\sigma = (i_1, i_2) \cdot i_3 \dots,$$

то мы также можем поменять элементы местами и получить другую подстановку той же самой цикловой структуры:

$$\sigma = (i_1, i_3) \cdot i_2 \dots$$

Во всех этих случаях мы можем заменить σ с сохранением ее цикловой структуры. Таким образом, при $n > 2$ центр состоит только из тождественной подстановки, а при $n = 2$ группа S_2 состоит из двух подстановок – это коммутативная группа и ее центр совпадает с ней самой:

$$Z(S_n) = \begin{cases} \{\varepsilon\}, & n \neq 2 \\ S_2, & n = 2 \end{cases}$$

Теперь от примеров перейдем к некоторым теоретическим результатам, которые вытекают из рассмотрения сопряженности в группе.

Предложение 1. Пусть G – конечная группа. Тогда:

1) $\forall x \in G\colon |C(x)| = \frac{|G|}{|Z(x)|}$
2) $|G| = |Z(G)| + \sum_{i=1}^{s} \frac{|G|}{|Z(x_i)|}$, где x_i – представители всех нецентральных классов сопряженности.

Формула 2) называется *формулой классов*.

Доказательство.
1) Следует из общей формулы для порядка орбиты при действии произвольной конечной группы на произвольном множестве.
2) Следует из разбиения группы G на попарно непересекающиеся классы сопряженности:

$$G = C_1 \sqcup \dots \sqcup C_m \Rightarrow |G| = |C_1| + \dots + |C_m|$$

Пусть $|C_1| = \dots = |C_r| = 1$, а $|C_j| > 1$ при $j > r$. Классы сопряженности, состоящие из одного элемента – это в точности центр группы, поэтому $C_1 \cup \dots \cup C_r = Z(G)$ и

$$|G| = |C_1| + \dots + |C_r| + \sum_{i=1}^{m-r} |C_{r+i}| = |Z(G)| + \sum_{i=1}^{m-r} |C_{r+i}|$$

Из пункта 1) следует, что

$$|C_{r+i}| = \frac{|G|}{|Z(x_i)|}, \text{где } x_i \in C_{r+i}$$

Получаем

$$|G| = |Z(G)| + \sum_{i=1}^{s} \frac{|G|}{|Z(x_i)|}$$

■

Несмотря на то, что формула классов тривиальна, из нее вытекает несколько важных следствий.

Предложение 2. Пусть G – *p-примарная* конечная группа, т.е. $|G| = p^n$, $n > 0$, p-простое. Тогда центр G нетривиален: $Z(G) \neq \{e\}$.

Доказательство.
Формула классов:

$$|G| = |Z(G)| + \sum_{i=1}^{s} \frac{|G|}{|Z(x_i)|}$$

Имеем:

$$|G| = p^n, \qquad \frac{|G|}{|Z(x_i)|} = \frac{p^n}{p^k} = p^{n-k} \vdots p, \text{так как } k < n$$

Тогда $|Z(G)| \vdots p$ (так как все остальные слагаемые в формуле классов делятся на p), т.е. $|Z(G)| > 1$ и $Z(G) \neq \{e\}$. ■

Предложение 3. Если $|G| = p^2$, p-простое, то G – абелева.

Доказательство.
От противного: пусть G не абелева. Рассмотрим центр G – по предложению 2 он нетривиален: $Z(G) \neq \{e\}$. По теореме Лагранжа, $|Z(G)|$ делит $|G| = p^2$, откуда $|Z(G)| = p$ или $|Z(G)| = p^2$. Если $|Z(G)| = p^2$, то $Z(G) = G$ и G – абелева: противоречие.

Если $|Z(G)| = p$, то

$$|G/Z(G)| = p^2/p = p.$$

Но группа простого порядка всегда циклическая (см. лекцию 2), поэтому $G/Z(G) \simeq Inn(G)$ – циклическая. Но группа внутренних автоморфизмов $Inn(G)$ неабелевой группы не может быть циклической – противоречие. Стало быть, G – абелева. ■

Следствие. Любая группа порядка p^2 изоморфна $\mathbb{Z}_{p^2}$ или $\mathbb{Z}_P \oplus \mathbb{Z}_p$.

Отметим, что для групп порядка p^3 (p-простое), коммутативность уже не обязательна. В качестве примера можно рассмотреть группу диэдра D_4: ее порядок равен $8 = 2^3$, но она (как и любая группа диэдра при $n > 2$) некоммутативна. Однако, группы порядка p^3 все же можно классифицировать.

Задача. Классифицировать с точностью до изоморфизма все группы порядка p^3, p-простое.

На этом мы закончим изучение сопряженности в группах и перейдем к следующей теме.

Коммутант.

Напоминание: пусть G – произвольная группа, $x, y \in G$. Коммутатор:

$$[x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1}$$

Свойства коммутатора:

1)
$$x \cdot y = [x, y] \cdot y \cdot x$$

2)
$$x \cdot y = y \cdot x \Leftrightarrow [x, y] = e$$

3)
$$[x, y]^{-1} = (x \cdot y \cdot x^{-1} \cdot y^{-1})^{-1} = y \cdot x \cdot y^{-1} \cdot x^{-1} = [y, x]$$

4) Пусть $\varphi\colon\ G \to H$ – гомоморфизм. Тогда

$$\varphi([x, y]) = \varphi(x \cdot y \cdot x^{-1} \cdot y^{-1}) = \varphi(x) \cdot \varphi(y) \cdot \varphi(x)^{-1} \cdot \varphi(y)^{-1} = [\varphi(x), \varphi(y)]$$

Множество всех коммутаторов элементов данной группы не обязано быть группой, однако оно порождает подгруппу в исходной группе G – коммутант группы G.

Определение. Коммутант (производная группа) группы G – подгруппа, порожденная всеми коммутаторами. Обозначение: $[G, G]$, или G'.

$$[G, G] = G' = < [x, y] \mid x, y \in G >$$

Простейшие свойства коммутанта:

1) Коммутант – это множество всех произведений коммутаторов:

$$[G, G] = \{[x_1, y_1] \cdot \ldots \cdot [x_N, y_N] \mid x_i, y_i \in G, \quad i = 1, \ldots, N, \quad N \geq 0\}$$

Доказательство.
По определению, $[G, G]$ состоит из всевозможных элементов вида $[x_1, y_1]^{\pm 1} \cdot \ldots \cdot [x_N, y_N]^{\pm 1}$. Но $[x_i, y_i]^{-1} = [y_i, x_i]$, поэтому степени -1 можно не рассматривать. ■

2) G – абелева $\Leftrightarrow [G, G] = \{e\}$.

Доказательство.
$\Rightarrow$: так как G – абелева, то $[x, y] = e$, $\forall x, y \in G$. Тогда $[G, G] = < e > = \{e\}$.
$\Leftarrow$: если $[G, G] = \{e\}$, то $[x, y] = e$, $\forall x, y \in G$, поэтому G – абелева. ■

Таким образом, коммутант – мера некоммутативности умножения в группе: чем больше пар элементов не коммутируют между собой, тем больше коммутант.

Лекция 10. Коммутант. Разрешимые группы.

Теорема 1.
1) Пусть $\varphi\colon\ G \to H$ – эпиморфизм. Тогда $\varphi(G') = H'$.
2) Коммутант – нормальная подгруппа: $G' \lhd G$.
3) G/G' - абелева.
4) Пусть $K \lhd G$, G/K – абелева. Тогда $K \supseteq G'$.

Доказательство.
1) Заметим, что при гомоморфизме коммутатор переходит в коммутатор (см. свойство 4 коммутатора из предыдущей лекции):

$$\varphi([x,y]) = [\varphi(x), \varphi(y)]$$

Отсюда следует, что

$$\varphi([x_1,y_1]\cdot \ldots \cdot [x_N,y_N]) = \varphi([x_1,y_1])\cdot \ldots \cdot \varphi([x_N,y_N]) = \\ = [\varphi(x_1),\varphi(y_1)]\cdot \ldots \cdot [\varphi(x_N),\varphi(y_N)]$$

Таким образом (так как гомоморфизм φ сюръективен): $\varphi(G') = (\varphi(G))' = H'$. Остальные свойства выводятся из свойства 1).

2) $\forall g \in G$ рассмотрим внутренний автоморфизм $i_g\colon\ G \Rightarrow G$ и применим свойство 1) к случаю $H = G$, $\varphi = i_g$. Тогда

$$i_g(G') = g \cdot G' \cdot g^{-1} = G'.$$

Следовательно, $G' \lhd G$.

3) Применим свойство 1) к канонической проекции $\pi\colon\ G \to G\ /\ G'$. Так как π – эпиморфизм, то

$$(G\ /\ G')' = \pi(G') = \{e \cdot G'\}$$

Отсюда следует, что G/G' - абелева (т.к. ее коммутант тривиален – см. свойство 2) коммутанта из предыдущей лекции)

4) Применим свойство 1) к канонической проекции $\pi\colon\ G \to G/K$. Снова получаем, что

$$\pi(G') = (G/K)' = \{e \cdot K\}$$

(второе равенство следует из того, что G/K – абелева). Таким образом, $G' \subseteq Ker\,\pi = K$. ■

Приведенными свойствами удобно пользоваться при вычислении коммутантов различных групп. Рассмотрим несколько примеров.

Предложение 1. 1) $S_n' = A_n$, 2) $A_n' = A_n$ при $n \geq 5$.

Доказательство.
1) Как мы знаем, группа S_n порождается транспозициями. Если транспозиции независимы, то они коммутируют между собой и их коммутатор тривиален, а если транспозиции зависимы, то:

$$[(i,j),(j,k)] = (i,j)\cdot(j,k)\cdot(i,j)^{-1}\cdot(j,k)^{-1} = (i,j,k)\cdot(i,j,k) = (i,k,j)$$

Так как тройные циклы порождают группу A_n при $n \geq 3$, то $S_n' \supseteq A_n$. Это включение верно и при $n = 1{,}2$, так как в этих случаях $A_n = \{\varepsilon\}$.
С другой стороны, $A_n \lhd S_n$, и (как мы вычисляли ранее) $S_n/A_n \simeq \{\pm 1\}$ абелева. Тогда из пункта 4 теоремы 1 следует, что $S_n' \subseteq A_n$. Таким образом, $S_n' = A_n$.

2) Пусть $i,j,k,l,m \in \{1,\dots,5\}$ попарно различны. Тогда

$$[(i,j)\cdot(l,m),(j,k)\cdot(l,m)] = (i,j)\cdot(l,m)\cdot(j,k)\cdot(l,m)\cdot(i,j)\cdot(l,m)\cdot(j,k)\cdot(l,m) = \\ = (i,j)\cdot(j,k)\cdot(i,j)\cdot(j,k)\cdot(l,m)^4 = (i,k,j)$$

Итак, при $n \geq 5$ любой тройной цикл можно получить как коммутатор четных подстановок, т.е. A_n' содержит все тройные циклы, которые порождают A_n при $n \geq 3$. Отсюда следует, что $A_n' = A_n$ при $n \geq 5$. ■

Замечание: при $n = 1{,}2$ имеем: $A_n = \{\varepsilon\} = A_n'$, при $n = 3$: $|A_3| = \frac{3!}{2} = 3$, поэтому A_3 циклическая (как группа простого порядка) и абелева: $A_3 \simeq \mathbb{Z}_3$, поэтому $A_3' = \{\varepsilon\}$. Случай $n = 4$ остается читателю в качестве упражнения.

Упражнение. Доказать, что $A_4' = V_4$ (четверная группа Клейна).

Предложение 2.
1) $GL_n(K)' = SL_n(K)$, кроме случая $n = 2$, $|K| = 2$.
2) $SL_n(K)' = SL_n(K)$, кроме случая $n = 2$, $|K| \leq 3$.

Доказательство.
Как было доказано на предыдущих лекциях, $SL_n(K) \lhd GL_n(K)$ как ядро гомоморфизма $det\colon GL_n(K) \to K$. Тогда (по основной теореме о гомоморфизмах),

$$GL_n(K)/SL_n(K) \simeq K^\times$$

- абелева группа (так как умножение в поле коммутативно). Тогда (по свойству 4 теоремы 1)

$$SL_n(K) \supseteq GL_n(K)'$$

и тем более

$$SL_n(K) \supseteq GL_n(K)' \supseteq SL_n(K)'$$

Докажем обратное включение. Как было доказано ранее, группа $SL_n(K)$ порождена элементарными матрицами 1-го типа: $U_{ij}(\lambda) = E + \lambda E_{ij}$. Вычислим коммутатор двух таких матриц при $n \geq 3$:

$$\left[U_{ik}(\alpha), U_{kj}(\beta)\right] = U_{ik}(\alpha) \cdot U_{kj}(\beta) \cdot U_{ik}(\alpha)^{-1} \cdot U_{kj}(\beta)^{-1} =$$
$$= U_{ik}(\alpha) \cdot U_{kj}(\beta) \cdot U_{ik}(-\alpha) \cdot U_{kj}(-\beta) = U_{ij}(\alpha\beta)$$

- последнее равенство получается последовательным применением элементарных преобразований, соответствующих элементарным матрицам (начиная с $U_{kj}(-\beta)$) к единичной матрице.

Так как $n \geq 3$, то $\forall i,j \in \{1,\dots,n\}$ можно выбрать $k \neq i,j$ и $\forall \lambda \in K$ можно подобрать $\alpha, \beta \in K$ такие, что $\alpha \cdot \beta = \lambda$. Следовательно, $SL_n(K)'$ содержит все элементарные матрицы 1-го типа, а поскольку такие матрицы порождают $SL_n(K)$, то группа $SL_n(K)$ совпадает со своим коммутантом:

$$SL_n(K) = SL_n(K)'$$

Тогда (используя ранее доказанное включение $SL_n(K) \supseteq GL_n(K)' \supseteq SL_n(K)'$) можно сделать вывод, что

$$SL_n(K) = SL_n(K)' = GL_n(K)'$$

При $n = 2$ уже нельзя подобрать $k \neq i,j$. Элементарных матриц 1-го типа будет всего две: $U_{12}(\alpha)$ и $U_{21}(\alpha)$, выберем $U_{12}(\alpha)$ и прокоммутируем с диагональной матрицей ($U_{21}(\alpha)$ рассматривается аналогично):

$$\left[\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix}, \begin{pmatrix}\beta & 0\\ 0 & \gamma\end{pmatrix}\right] = \begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}\beta & 0\\ 0 & \gamma\end{pmatrix} \cdot \begin{pmatrix}1 & -\alpha\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}1/\beta & 0\\ 0 & 1/\gamma\end{pmatrix} = \begin{pmatrix}1 & \alpha(1-\frac{\beta}{\gamma})\\ 0 & 1\end{pmatrix}$$

- в результате получили матрицу $U_{12}\left(\alpha(1-\frac{\beta}{\gamma})\right)$.

Теперь рассмотрим ограничения на поле K. Если K содержит хотя бы 3 элемента: $|K| > 2$, то можно подобрать $\beta, \gamma \neq 0$, $\beta \neq \gamma$, что $1 - \frac{\beta}{\gamma} \neq 0$. Тогда $\forall \lambda \in K\ \exists \alpha \in K$: $\alpha(1-\frac{\beta}{\gamma}) = \lambda$. Отсюда следует, что $U_{12}(\lambda) \in GL_2(K)'$. Аналогично $U_{21}(\lambda) \in GL_2(K)'$. Следовательно, $GL_2(K)'$ содержит все элементарные матрицы 1-го типа, а значит, содержит и $SL_2(K)$, которая ими порождается: $GL_2(K)' \supseteq SL_2(K)$. Таким образом,

$$GL_2(K)' = SL_2(K)$$

При $|K| > 3$ можно найти $\beta \neq 0,\ \beta^2 \neq 1$ (так как у уравнения $\beta^2 = 1$ не больше двух корней). Тогда для $\gamma = \frac{1}{\beta}$ имеем:

$$\begin{pmatrix} \beta & 0 \\ 0 & \gamma \end{pmatrix} \in SL_2(K) \text{ и } 1 - \frac{\beta}{\gamma} = 1 - \beta^2 \neq 0$$

и далее можно провести аналогичное рассуждение: $\forall \lambda \in K\ \exists \alpha \in K\colon\ \alpha(1 - \frac{\beta}{\gamma}) = \lambda$, поэтому $U_{12}(\lambda) \in SL_2(K)'$ (так как обе матрицы $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} \beta & 0 \\ 0 & \gamma \end{pmatrix}$ имеют определитель, равный 1). Аналогично $U_{21}(\lambda) \in SL_2(K)'$. Следовательно, $SL_2(K)'$ содержит все элементарные матрицы 1-го типа, а значит, содержит и $SL_2(K)$, которая ими порождается: $SL_2(K)' \supseteq SL_2(K)$. Таким образом,

$$SL_2(K)' = SL_2(K)$$

Предложение доказано. ■

Определение. *Кратные коммутанты* группы G определяются по индукции: k-ый коммутант – это коммутант $(k-1)$-го коммутанта:

$$G^{(k)} = \left[G^{(k-1)}, G^{(k-1)}\right],\ \ G^{(0)} = G$$

Предложение 3.
1) Пусть $\varphi\colon\ G \to H$ – эпиморфизм. Тогда $\varphi(G^{(k)}) = H^{(k)}$.
2) Если φ – автоморфизм, то $\varphi(G^{(k)}) = G^{(k)}$.
3) Кратный коммутант – нормальная подгруппа: $G^{(k)} \lhd G$.

Доказательство.
1) Докажем индукцией по k.
База индукции: при $k = 0$ доказывать нечего (т.к. $G^{(0)} = G$ и $H^{(0)} = H$).
Шаг индукции: по предположению индукции, $\varphi\colon\ G^{(k-1)} \to H^{(k-1)}$ – эпиморфизм. Тогда по свойству коммутанта (п.1 теоремы 1 – при эпиморфизме коммутант переходит в коммутант):

$$\varphi(G^{(k)}) = H^{(k)}$$

2) Сразу следует из пункта 1), если взять $H = G$, φ – автоморфизм.

3) Применим пункт 2) к $\varphi = i_G, \forall g \in G$ (внутренний автоморфизм). Тогда

$$g \cdot G^{(k)} \cdot g^{-1} = G^{(k)},\ \ \forall g \in G$$

Отсюда следует, что $G^{(k)} \lhd G$. ■

Определение. Подгруппа $H \subseteq G$ называется характеристической, если она переходит в себя при любых автоморфизмах группы G:

$$\varphi(H) = H, \ \ \forall \varphi \in Aut(G)$$

Примеры характеристических подгрупп: 1) $G^{(k)}, \forall k$, 2) $Z(G)$.

Замечание: всякая характеристическая подгруппа является нормальной (доказательство как для свойства 3) кратных коммутантов).

Кратные коммутанты образуют ряд (возможно, бесконечный) вложенных друг в друга подгрупп – *производный ряд*: $G \rhd G' \rhd \cdots \rhd G^{(k-1)} \rhd G^{(k)} \rhd \cdots$

Определение. Группа G разрешима, если $\exists n$: $G^{(n)} = \{e\}$. Наименьшее такое n называется *ступенью (классом) разрешимости* группы G.
Ступень 0: $G = \{e\}$.
Ступень 1: G абелева.

Вообще, можно сказать, что разрешимые группы – следующий по сложности класс групп после абелевых. Разрешимые группы как бы собраны в башню из абелевых этажей: умножение в группе G коммутативно в первом приближении (т.е. факторгруппа G/G' абелева, значит умножение в группе G коммутативно с точностью до поправок из коммутанта), группа G' коммутативна с точностью до поправок из G'' (по модулю G'') и так далее. Если группа разрешима, то в конце концов мы получим $\{e\}$.
Разрешимость группы удобно проверять с помощью следующей теоремы:

Теорема 2.
1) Подгруппа разрешимой группы разрешима,
2) Пусть $H \lhd G$. Тогда: G разрешима $\Leftrightarrow$ H и G/H разрешимы.

Доказательство.
1) Пусть $H \subseteq G$, тогда $H' \subseteq G'$ (так как H' порожден коммутаторами элементов из H, которые лежат также и в G). По тем же соображениям $H'' \subseteq G''$ и так далее: $H^{(k)} \subseteq G^{(k)}$ (доказывается индукцией по k).
Если G разрешима ступени n, тогда $G^{(n)} = \{e\}$, значит тем более $H^{(n)} = \{e\}$, то есть, H разрешима ступени не больше n.

2) Пусть $\pi: \ G \to G/H$ – каноническая проекция. Это эпиморфизм, следовательно,

$$\pi(G^{(k)}) = (G/H)^{(k)}, \ \ \forall k.$$

Если G разрешима ступени n, то $G^{(n)} = \{e\}$, значит (см. пункт 1) $H^{(n)} = \{e\}$ и

$$(G/H)^{(n)} = \pi(G^{(n)}) = \{eH\}.$$

Поэтому H и G/H разрешимы ступени $\leq n$.

Обратно, пусть H разрешима ступени k, а G/H разрешима ступени l. Это значит, что

$$\pi(G^{(l)}) = (G/H)^{(l)} = \{eH\} \Rightarrow G^{(l)} \subseteq Ker\,\pi = H$$

Но тогда

$$G^{(l+1)} \subseteq H', G^{(l+2)} \subseteq H'', \dots, G^{(l+k)} \subseteq H^{(k)} = \{e\}$$

т.е. G разрешима ступени $\leq k + l$. ■

Примеры.
1) $G = S_n$.
$n = 1$: $S_1 = \{\varepsilon\}$ – разрешима ступени 0.
$n = 2$: $S_2 \simeq \mathbb{Z}_2$ – абелева ⇒ разрешима ступени 1.
$n = 3$: $S_3' = A_3$ – абелева, $A_3' = \{\varepsilon\} \Rightarrow S_3$ разрешима ступени 2.
$n = 4$: $S_4 \triangleleft V_4$ (см. прошлую лекцию). V_4 абелева ⇒ разрешима. $S_4/V_4 \simeq S_3$ (см. прошлую лекцию). Как мы только что доказали, S_3 разрешима. Значит, по теореме 2 п.2) S_4 разрешима.

Упражнение. Доказать, что S_4 разрешима ступени 3 (указание: решить предыдущее упражнение - доказать, что $A_4' = V_4$ и воспользоваться тем, что $S_4' = A_4$ и $V_4' = \{\varepsilon\}$).

При $n \geq 5$ группа S_n неразрешима, так как в этом случае $S_n \supseteq A_n = A_n' = A_n'' = \cdots$ - неразрешимая подгруппа.

В связи с этим примером скажем несколько слов о происхождении термина “разрешимая группа”. Он возник в связи с решением алгебраических уравнений в радикалах, а именно: пусть f – многочлен: $f \in K[x],\ K \subseteq \mathbb{C}$. Возникает вопрос – можно ли корни f выразить через элементы поля K с помощью арифметических операций и операции извлечения корня.
С каждым многочленом можно связать $Gal(f)$ – группу Галуа этого многочлена. Она состоит из всех перестановок комплексных корней многочлена f, которые сохраняют все алгебраические выражения от этих корней с коэффициентами и значениями в поле K. Оказывается, корни $x_1, \dots, x_n$ многочлена f выражаются в радикалах через элементы поля K тогда и только тогда, когда $Gal(f)$ разрешима.
Почти для всех многочленов группа $Gal(f)$ совпадает с группой подстановок на его корнях, т.е. группой S_n. Поэтому $\forall f,\ deg\, f = n$, его корни $x_1, \dots, x_n$ выражаются в радикалах через коэффициенты f тогда и только тогда, когда S_n разрешима.
Таким образом, любые алгебраические уравнения степени не выше 4 разрешимы в радикалах, а начиная с 5, вообще говоря, нет.

2) $GL_n(K)$ и $SL_n(K)$ неразрешимы, кроме случая $n = 2$, $|K| \leq 3$. Действительно:

$$GL_n(K) \supset SL_n(K) = SL_n(K)' = SL_n(K)'' = \cdots$$

- неразрешима.

Предложение 4. Всякая конечная p-группа, т.е. группа G порядка p^n (p – простое) разрешима.

Доказательство.
Докажем индукцией по n.

База индукции: $n = 0$ – доказывать нечего: $G = \{e\}$ разрешима.

Шаг индукции: всякая конечная p-группа порядка большего 1, имеет нетривиальный центр: $Z(G) \neq \{e\}$. Но $Z(G)$ абелева группа, а значит разрешимая. Так как $Z(G)$ – подгруппа G, то

$$|Z(G)| = p^k, k > 0.$$

Тогда

$$|G/Z(G)| = p^{n-k} < p^n,$$

т.е. $G/Z(G)$ - p-группа меньшего порядка. Следовательно, по предположению индукции, $G/Z(G)$ разрешима. Значит (по теореме 2) группа G разрешима. ■

Лекция 11. Простые группы.

На прошлой лекции мы выяснили, что группы $GL_n(K)$ и $SL_n(K)$ неразрешимы, кроме случая $n = 2, |K| \leq 3$. Приведем пример разрешимой матричной группы.

Предложение. Группа невырожденных верхнетреугольных матриц $B_n(K)$ разрешима.

Доказательство.
Докажем с помощью теоремы 2 из предыдущей лекции (критерий разрешимости группы)
1) Рассмотрим отображение

$$\varphi\colon B_n(K) \to K^\times \times \ldots \times K^\times$$

$$\varphi\left(\begin{pmatrix} \lambda_1 & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix}\right) = (\lambda_1, \ldots, \lambda_n)$$

т.е. отображение φ, ставящее в соответствие верхнетреугольной матрице вектор, состоящий из ее диагональных элементов.
Это гомоморфизм. Действительно, результат перемножения двух верхнетреугольных матриц с элементами $(\lambda_1, \ldots, \lambda_n)$ и $(\mu_1, \ldots, \mu_n)$ на диагонали – это снова верхнетреугольная матрица с элементами $(\mu_1\lambda_1, \ldots, \mu_n\lambda_n)$ на диагонали, т.е.

$$\varphi(A \cdot B) = (\mu_1\lambda_1, \ldots, \mu_n\lambda_n) = (\lambda_1, \ldots, \lambda_n) \cdot (\mu_1, \ldots, \mu_n) = \varphi(A) \cdot \varphi(B)$$

Ядром гомоморфизма φ является группа унитреугольных матриц (т.е. верхнетреугольных матриц с единицами на диагонали):

$$Ker\,\varphi = U_n(K)$$

Так как гомоморфизм φ сюръективен (очевидно – в качестве диагональных элементов можно выбрать любой набор $(\lambda_1, \ldots, \lambda_n) \in K^\times \times \ldots \times K^\times$), то по основной теореме о гомоморфизмах

$$B_n(K)/U_n(K) \simeq Im\,\varphi = K^\times \times \ldots \times K^\times = (K^\times)^n$$

Но группа $(K^\times)^n$ абелева, а значит, разрешима. Осталось доказать, что $U_n(K)$ разрешима.

2) Разрешимость группы $U_n(K)$.
Докажем индукцией по n.
База индукции: $n = 1 \Rightarrow U_1(K) = \{1\}$ разрешима.

Шаг индукции: рассмотрим отображение

$$\psi\colon U_n(K) \to U_{n-1}(K)$$

$$\left(\begin{array}{ccc|c} & \bar{A} & & \begin{matrix}*\\ \cdots \\ *\end{matrix} \\ \hline 0 & \cdots & 0 & 1 \end{array}\right) \mapsto \bar{A}$$

т.е. отображение, ставящее в соответствие матрице $A \in U_n(K)$ матрицу $\bar{A} \in U_{n-1}(K)$, получающуюся из матрицы A удалением последней строки и последнего столбца.
Это гомоморфизм:

$$\psi(A \cdot B) = \bar{A} \cdot \bar{B} = \psi(A) \cdot \psi(B)$$

$$\left(\begin{array}{ccc|c} & \bar{A} & & \begin{matrix}*\\ \cdots \\ *\end{matrix} \\ \hline 0 & \cdots & 0 & 1 \end{array}\right) \cdot \left(\begin{array}{ccc|c} & \bar{B} & & \begin{matrix}*\\ \cdots \\ *\end{matrix} \\ \hline 0 & \cdots & 0 & 1 \end{array}\right) = \left(\begin{array}{ccc|c} & \bar{A} \cdot \bar{B} & & \begin{matrix}*\\ \cdots \\ *\end{matrix} \\ \hline 0 & \cdots & 0 & 1 \end{array}\right)$$

A B $A \cdot B$

Ядро гомоморфизма ψ – это группа, состоящая из унитреугольных матриц A, у которых $\bar{A} = E$:

$$Ker\,\psi = V_n(K) = \left\{ \begin{pmatrix} 1 & & 0 & a_1 \\ & \ddots & & \vdots \\ & & 1 & a_{n-1} \\ 0 & & & 1 \end{pmatrix},\ a_1, \dots, a_{n-1} \in K \right\}$$

Существует изоморфизм:

$$V_n(K) \simeq K^{n-1}$$

$$A = \begin{pmatrix} 1 & & 0 & a_1 \\ & \ddots & & \vdots \\ & & 1 & a_{n-1} \\ 0 & & & 1 \end{pmatrix} \leftrightarrow (a_1, \dots, a_{n-1})$$

Ясно, что это взаимно-однозначное соответствие. Проверим, что это гомоморфизм:

$$\begin{pmatrix} 1 & & 0 & a_1 \\ & \ddots & & \vdots \\ & & 1 & a_{n-1} \\ 0 & & & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & & 0 & b_1 \\ & \ddots & & \vdots \\ & & 1 & b_{n-1} \\ 0 & & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & 0 & a_1 + b_1 \\ & \ddots & & \vdots \\ & & 1 & a_{n-1} + b_{n-1} \\ 0 & & & 1 \end{pmatrix}$$

A B $A \cdot B$

Таким образом,

$$A \cdot B \leftrightarrow (a_1 + b_1, \dots, a_{n-1} + b_{n-1}) = (a_1, \dots, a_{n-1}) + (b_1, \dots, b_{n-1})$$

и данное отображение действительно является изоморфизмом. Следовательно, $V_n(K)$ абелева ⇒ разрешима. По основной теореме о гомоморфизмах,

$$U_n(K)/V_n(K) \simeq Im\,\psi = U_{n-1}(K)$$

Но группа $U_{n-1}(K)$ разрешима по предположению индукции, следовательно (см. критерий разрешимости – теорема 2 лекции 10) группа $U_n(K)$ также разрешима. ■

На этом закончим обсуждение разрешимых групп и перейдем к рассмотрению класса групп, которые в каком-то смысле противоположны разрешимым – к простым группам.

Простые группы.

Определение. Группа G называется *простой*, если она не тривиальна и не содержит собственных нормальных подгрупп: $G \neq \{e\}$ и $\nexists H \lhd G$ кроме $H = G$ или $\{e\}$.

Можно сказать, что простые группы – это элементарные строительные блоки, из которых строятся произвольные группы (можно провести аналогию с простыми числами). Что имеется в виду – рассмотрим в произвольной группе G *нормальный ряд* подгрупп (длины n):

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{k-1} \rhd G_k \rhd \cdots \rhd G_n = \{e\}$$

и рассмотрим факторгруппы соседних членов этого ряда: если G_{k-1}/G_k не проста, то нормальный ряд можно "уплотнить": действительно, так как G_{k-1}/G_k не проста, то существует $H \lhd G_{k-1}/G_k$. Рассмотрим прообраз H при канонической проекции:

$$\widetilde{H} = \pi^{-1}(H) \lhd G_{k-1} \xrightarrow{\pi} G_{k-1}/G_k \rhd H$$

$\widetilde{H}$ – нормальная подгруппа, тогда $G_{k-1} \rhd \widetilde{H} \rhd G_k$. Таким образом, мы можем "уплотнять" нормальный ряд до тех пор, пока это возможно, и если группа G конечна, то рано или поздно этот процесс прекратится (так как каждый раз при "уплотнениии" мы получаем группу промежуточного порядка по сравнению с G_{k-1} и G_k) – мы придем к "неуплотняемому" нормальному ряду, в котором все факторгруппы просты – такой ряд называется *композиционным*:

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{k-1} \rhd G_k \rhd \cdots \rhd G_n = \{e\}, \qquad G_{k-1}/G_k \text{ просты } \forall k = 1, \dots, n$$

Приведем без доказательства следующую теорему.

Теорема Жордана-Гёльдера. Если у группы G существует композиционный ряд , то его длина n и набор простых факторов G_{k-1}/G_k $(k = 1, \dots, n)$ определены однозначно с точностью до изоморфизма и до перестановки.

Композиционный ряд позволяет сводить изучение произвольной группы G к простым группам в той же степени, в какой производный ряд позволяет сводить изучение разрешимых групп к абелевым группам. В этой связи можно поставить вопрос о том, какую роль играют простые группы в общей задаче классификации конечных групп.

Классификация конечных групп.

Классификация конечных групп сводится к:

- классификации простых групп
- классификации групп с заданным набором простых факторов композиционного ряда

Классификации групп с заданным набором простых факторов композиционного ряда вряд ли возможна, мы не будем ее обсуждать. Задача же классификации простых групп решена относительно недавно (1981 г), однако сама классификация очень сложна и труднопроверяема, а ее объем настолько велик, что не все математики верят в ее истинность. Мы, разумеется, не будем пытаться провести полную классификацию простых групп, однако рассмотрим некоторые важные частные случаи и примеры. Начнем со случая абелевых групп.

Теорема 1. Простые абелевы группы – это циклические группы простого порядка.

Доказательство.
1) Если $|G| = p$ – простое число, то $G \simeq \mathbb{Z}_p$ и любая подгруппа $H \subseteq G$ имеет порядок $|H| = 1$ или p (по теореме Лагранжа) $\Rightarrow H = \{e\}$ или G. Следовательно, G проста.

2) Обратно: пусть G – простая абелева группа. Возьмем $g \in G$, $g \neq e$. Рассмотрим $H = < g > \lhd G$ – так как G абелева, то H нормальна, также $H \neq \{e\}$ (потому что $g \neq e$), следовательно (так как G – простая группа), $H = G$. Отсюда следует, что G – циклическая группа.

3) Если $|G| = \infty$, то можно считать, что $G = \mathbb{Z}$. Но группа $\mathbb{Z}$, очевидно, не является простой – легко указать ее нетривиальную нормальную подгруппу: например, $H = 2\mathbb{Z}$ - группа четных чисел.

4) Если $|G| = m$, то можно считать, что $G = \mathbb{Z}_m$. Если m не является простым: $m = k \cdot l$, $k, l > 1$, то рассмотрим $H = < k \bmod m > = \{\bar{0}, \bar{k}, \overline{2k}, \dots, \overline{(l-1)k}\} \lhd G$. Так как H не тривиальна и не совпадает с G, то группа G не проста. Следовательно, m – простое. ■

Для случая неабелевых групп ограничимся рассмотрением одного важного примера конечной простой группы – группы четных подстановок.

Теорема 2. Группа A_n проста при $n \geq 5$.

Отметим, что $n \leq 3$ группа A_n абелева, а группа A_4 разрешима (т.о. не является простой).

Доказательство.
Пусть $H \lhd A_n$, $H \neq \{\varepsilon\}$. Докажем, что $H = A_n$.

1) Если $\sigma \in H, \pi \in A_n$, то

$$[\pi, \sigma] = \pi \cdot \sigma \cdot \pi^{-1} \cdot \sigma^{-1} \in H$$

- действительно, $\pi \cdot \sigma \cdot \pi^{-1}$ – это элемент, сопряженный к σ, значит (т.к. $H \lhd A_n$), $\pi \cdot \sigma \cdot \pi^{-1} \in H$. Также $\sigma^{-1} \in H$, значит, и $\pi \cdot \sigma \cdot \pi^{-1} \cdot \sigma^{-1} \in H$.

2) Выберем $\sigma \in H$, $\sigma \neq \varepsilon$ и разложим σ в произведение независимых циклов. Пусть l – наибольшая длина цикла в этом разложении. Далее рассмотрим случаи:

а) Пусть $l \geq 4$, тогда

$$\sigma = (i_1, i_2, i_3, i_4, \dots, i_l) \cdot \dots$$

Возьмем $\pi = (i_1, i_2, i_3)$, тогда (см. пример 3 глава 9 – как устроены классы сопряженности в группе подстановок):

$$[\pi, \sigma] = \pi\sigma\pi^{-1} \cdot \sigma^{-1} = (i_2, i_3, i_1, i_4, \dots, i_l) \cdot (i_l, \dots, i_4, i_3, i_2, i_1) = (i_1, i_2, i_4) \in H$$

б) Пусть $l = 3$, причем в разложении σ присутствует не менее двух тройных циклов:

$$\sigma = (i_1, i_2, i_3) \cdot (j_1, j_2, j_3) \cdot \dots$$

Возьмем $\pi = (i_1, j_1) \cdot (i_2, j_2)$, тогда:

$$[\pi, \sigma] = \pi\sigma\pi^{-1} \cdot \sigma^{-1} = (j_1, j_2, i_3) \cdot (i_1, i_2, j_3) \cdot (j_3, j_2, j_1) \cdot (i_3, i_2, j_1) = (i_1, j_1) \cdot (i_3, j_3) \in H$$

в) Пусть $l \leq 3$, причем в разложении σ присутствует не более одного тройного цикла. Тогда возможны два варианта:

- σ – тройной цикл
- $\sigma = (i_1, i_2) \cdot (j_1, j_2) \cdot \dots$

Во второй ситуации возьмем $\pi = (i_1, i_2, j_1)$, тогда:

$$[\pi, \sigma] = \pi\sigma\pi^{-1} \cdot \sigma^{-1} = (i_2, j_1) \cdot (i_1, j_2) \cdot (j_2, j_1) \cdot (i_2, i_1) = (i_1, j_1) \cdot (i_2, j_2) \in H$$

Во всех случаях H содержит либо тройной цикл, либо пару независимых транспозиций.

3) Все тройные циклы сопряжены в A_n при $n \geq 5$. Действительно, пусть (i_1, i_2, i_3) – произвольный тройной цикл. Тогда его с помощью сопряжения можно получить из любого фиксированного тройного цикла, например, цикла $(1, 2, 3)$:

$$(i_1, i_2, i_3) = \pi \cdot (1, 2, 3) \cdot \pi^{-1}, \text{ где } \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ i_1 & i_2 & i_3 & i_4 & \dots & i_n \end{pmatrix}$$

Если подстановка π оказалась нечетной, просто переставим в нижней строке два элемента местами, не трогая i_1, i_2, i_3 (мы можем это сделать, так как $n \geq 5$) – получим четную подстановку.

4) Все пары независимых транспозиций сопряжены в A_n при $n \geq 5$. Действительно, пусть $(i_1, i_2) \cdot (i_3, i_4)$ – пара независимых транспозиций. Тогда ее с помощью сопряжения можно получить из любой фиксированной пары независимых транспозиций, например, из $(1,2) \cdot (3,4)$:

$$(i_1, i_2) \cdot (i_3, i_4) = \pi \cdot (1,2) \cdot (3,4) \cdot \pi^{-1}, \text{ где } \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ i_1 & i_2 & i_3 & i_4 & \dots & i_n \end{pmatrix}$$

Если подстановка π оказалась нечетной, просто переставим в нижней строке два первых элемента местами – получим четную подстановку.

5) Следовательно, H содержит все тройные циклы или все пары независимых транспозиций. Но оба этих множества порождают A_n при $n \geq 5$, поэтому $H = A_n$. ■

Приведем еще один пример простой группы, на этот раз бесконечной.

Теорема 3. Группа $SO_3(\mathbb{R})$ проста.

Доказательство.
1) Геометрические соображения:

$$SO_3(\mathbb{R}) = \{\text{матрицы поворотов в } 3-\text{мерном евклидовом пространстве } V \text{ в ортонормированных базисах}\}$$

Из линейной алгебры известно, что если A – матрица оператора $\mathcal{A}\colon V \to V$ в базисе (e_1, e_2, e_3), то CAC^{-1} – матрица $\mathcal{A}$ в базисе (e_1', e_2', e_3'), причем C – матрица перехода от нового базиса к старому:

$$(e_1', e_2', e_3') \xrightarrow{C} (e_1, e_2, e_3)$$

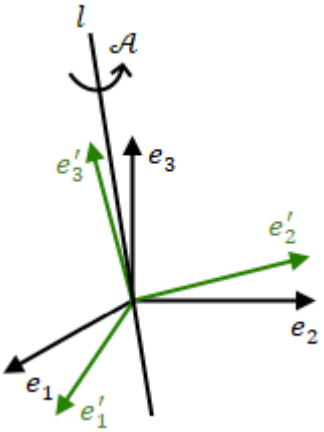


Рис. 11.1. CAC^{-1} – матрица $\mathcal{A}$ в базисе (e_1', e_2', e_3')

С другой стороны, матрицу CAC^{-1} можно рассматривать как матрицу оператора $\mathcal{A}' = \mathcal{C}\mathcal{A}\mathcal{C}^{-1}$ в старом базисе (e_1, e_2, e_3), где $\mathcal{C}$ – оператор, отображающий новый базис в старый, т.е. $\mathcal{C}(e_i') = e_i$, $i = 1,2,3$. Иными словами, оператор $\mathcal{A}'$ поворачивает пространство V по отношению к базису (e_1, e_2, e_3) так же, как оператор $\mathcal{A}$ поворачивает пространство V по отношению к базису (e_1', e_2', e_3'), так как в этих базисах у операторов одинаковые матрицы: CAC^{-1} и $\mathcal{C}\mathcal{A}\mathcal{C}^{-1}$. Поэтому геометрические объекты, задающие оператор $\mathcal{A}'$, по отношению к старому базису выглядят так же, как геометрические объекты, задающие оператор $\mathcal{A}$, по отношению к новому базису.
Например, если $\mathcal{A}$ – поворот вокруг оси l на угол φ, тогда $\mathcal{A}'$ - поворот вокруг оси $l' = \mathcal{C}(l)$ на угол φ.

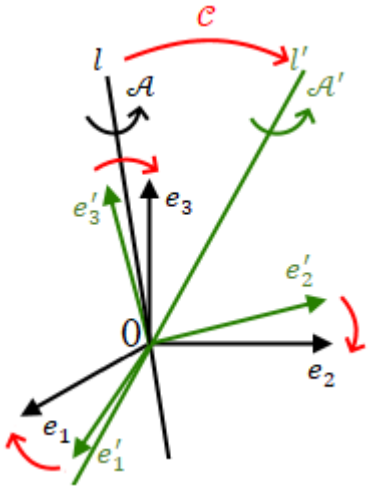


Рис. 11.2. Операторы $\mathcal{A}$ и $\mathcal{A}'$

Эти геометрические рассуждения подсказывают правильный подход к операции сопряжения в группе $SO_3(\mathbb{R})$. Теперь докажем простоту $SO_3(\mathbb{R})$. Пусть $H \lhd SO_3(\mathbb{R})$, $H \neq \{E\}$. Докажем, что $H = SO_3(\mathbb{R})$.

2) Выберем $A \in H$, $A \neq E$. Тогда A – матрица поворота на ненулевой угол φ. Но в H содержатся и все сопряженные матрицы CAC^{-1} – всевозможные матрицы поворотов на угол φ вокруг различных осей, в частности, вокруг третьей координатной оси:

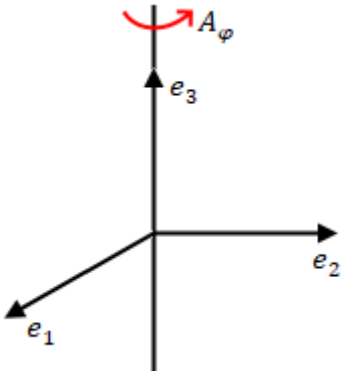


Рис. 11.3. A_φ – поворот вокруг третьей координатной оси

$$H \ni A_\varphi = \begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

3) Теперь будем поворачивать ось Oe_3 вокруг оси Oe_1 в плоскости Oe_2e_3. Матрица, задающая этот поворот:

$$C_\alpha = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix}$$

Тогда

$$C_\alpha A_\varphi {C_\alpha}^{-1} = B_\varphi(\alpha) \in H$$

- угол поворота вокруг Oe_3'.

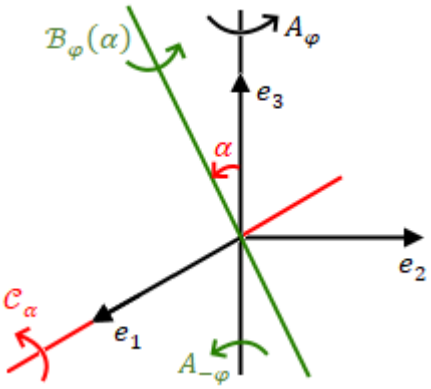


Рис. 11.4. ${C_\alpha A_\varphi C_\alpha}^{-1} = B_\varphi(\alpha)$

Заметим, что

$$B_\varphi(0) = A_\varphi$$
$$B_\varphi(\pi) = A_{-\varphi} = A_\varphi^{-1}$$

4) Рассмотрим произведение

$$B_\varphi(\alpha) \cdot A_\varphi = R_\psi \in H$$

– это матрица поворота на некоторый угол $\psi = \psi(\alpha)$. Тогда

$$\psi(\pi) = 0$$
$$\psi(\alpha) \neq 0, \text{ при } 0 < \alpha < \pi$$

5) Докажем, что $\psi(\alpha)$ – непрерывная функция.

$$tr\, R_\psi = 2\cos\psi + 1 \Rightarrow \psi = arccos\left(\frac{tr\, R_\psi - 1}{2}\right)$$

т.е. ψ – непрерывная функция от элементов матрицы R_ψ, которые, в свою очередь, являются непрерывными функциями от α (так как $B_\varphi(\alpha) \cdot A_\varphi = R_\psi$, а элементы $B_\varphi(\alpha)$ и A_φ непрерывно зависят от α). Таким образом, $\psi(\alpha)$ – непрерывная функция.

Но тогда $\psi(\alpha)$ принимает все промежуточные значения на отрезке $[0, \psi_0]$, где $\psi_0 = \psi(\alpha_0),\ 0 < \alpha_0 < \pi$. Следовательно (в силу нормальности), H содержит все повороты на углы $\in [0, \psi_0]$.

6) Пусть $S \in SO_3(\mathbb{R})$. Тогда $S = S_\beta$ – поворот вокруг оси l на угол β. Выберем n: $0 < \frac{\beta}{n} < \psi_0$. Тогда (так как $S_{\frac{\beta}{n}} \in H$)

$$S = \left(S_{\frac{\beta}{n}}\right)^n \in H$$

Следовательно, $H = SO_3(\mathbb{R})$ и группа $SO_3(\mathbb{R})$ проста. ■

Лекция 12. Силовские подгруппы.

При изучении структур групп важно знать, какие в них имеются подгруппы и как они устроены. В случае конечных групп теорема Лагранжа дает ограничение на порядок подгруппы: если $|G| = n < \infty$, $H \subseteq G$, то $|H|$ делит n. Верно ли обратное: если $m \mid n$, то в группе G существует подгруппа порядка m?

Для циклических групп утверждение верно (соответствующая теорема была доказана в первой части курса), также оно верно для абелевых групп (доказательство этого факта останется за рамками нашего курса), однако в общем случае утверждение неверно – в качестве контрпримера можно рассмотреть группу A_5:

Контрпример. $|A_5| = \frac{5!}{2} = 60$, но в группе A_5 не существует подгрупп порядка 30. Это вытекает из следующей леммы, которая представляет самостоятельный интерес:

Лемма. Пусть G – группа, $H \subset G$, $(H: G) = 2$. Тогда $H \lhd G$.

Доказательство.
Рассмотрим левые смежные классы по H: их два, один из них $e \cdot H = H$. Так как эти смежные классы не пересекаются, а их объединение – это вся группа G, то второй смежный класс – это $g \cdot H = G \setminus H, \forall g \notin H$.
Рассмотрим правые смежные классы по H: как и в случае левых смежных классов, это $H \cdot e = H$ и $H \cdot g = G \setminus H, \forall g \notin H$.
Итак, левые и правые смежные классы по H совпадают, то есть, $H \lhd G$. ■

Как мы знаем, группа A_5 проста – в ней нет нетривиальных нормальных подгрупп, поэтому не может быть и подгрупп порядка 30.

Итак, мы видим, что вопрос о подгруппах в произвольной конечной группе не тривиален – теорема Лагранжа дает лишь необходимое условие на порядок подгруппы, но не достаточное. Тем не менее, оказывается, что в любой конечной группе заведомо существуют подгруппы, порядок которых равен некоторым делителям порядка группы. Такие подгруппы называются *силовскими*.

Силовские подгруппы.

Определение. Пусть G – конечная группа, $|G| = n = p^k m$, p – простое, m не делится на p. Тогда подгруппа $P \subseteq G$ порядка $|P| = p^k$ называется *силовской* p-подгруппой.

Силовские подгруппы названы так в честь норвежского математика П. Л. Силова (P. L. Sylow, 1832-1918), который ввел в рассмотрение этот класс подгрупп и доказал основные утверждения, связанные с ними. Сформулируем и докажем три теоремы Силова.

1-ая теорема Силова. В любой конечной группе G для любого простого p существует силовская p-подгруппа $P \subseteq G$.

Доказательство.
Заметим, что формулировка корректна: если p не входит в разложение $n = |G|$, то силовская p-подгруппа, очевидно, существует (возьмем $k = 0$). Содержательным утверждение теоремы становится для простых чисел, которые являются делителями $n = |G|$.

Вначале расмотрим частный случай: G – абелева.
Как было доказано ранее (см. следствие из теоремы 4 лекции 6), всякая конечная абелева группа разлагается в прямую сумму примарных циклических групп:

$$G \simeq \mathbb{Z}_{p_1^{l_1}} \oplus \ldots \oplus \mathbb{Z}_{p_t^{l_t}}, \text{ где } p_1, \ldots, p_t - \text{простые}$$

Рассмотрим подгруппу p-кручения (элементы, порядок которых равен некоторой степени p):

$$Tor_p(G) \simeq \mathbb{Z}_{p^{l_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{l_q}}$$

Из этой формулы видно, что G – это прямая сумма подгрупп p-кручения для различных p:

$$G = Tor_{p_1}(G) \oplus \ldots \oplus Tor_{p_s}(G), \ p_1, \ldots, p_{p_s} \text{ попарно различны}$$

Так как

$$\left|Tor_{p_j}(G)\right| = p_j^{k_j}, \qquad |G| = n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s},$$

то каждая из подгрупп p-кручения является силовской подгруппой:

$$P = Tor_p(G)$$

- силовская подгруппа.

Общий случай.
Докажем индукцией по $|G| = n = p^k m$ (m не делится на p). Используем формулу классов (см. лекция 9 предложение 1):

$$|G| = |Z(G)| + \sum_{i=1}^{s} \frac{|G|}{|Z(x_i)|}$$

где $x_1, \ldots, x_s$ – представители всех нецентральных классов сопряженности.

Возможны две ситуации:
1) $\exists i\colon \ |Z(x_i)| \vdots p^k$,
2) $\forall i\colon \ |Z(x_i)| = p^{k_i} \cdot m_i$, где m_i не делится на p, $k_i < k$.

- 1) Так как $x_i \notin Z(G)$, то $|Z(x_i)| < |G|$, тогда по предположению индукции $\exists\, P \subseteq Z(x_i)$, $|P| = p^k$, то есть, P – силовская подгруппа в G.
- 2) В этом случае

$$\frac{|G|}{|Z(x_i)|} = p^{k-k_i} \cdot \frac{m}{m_i} \vdots p$$

Тогда из формулы классов следует, что

$$|Z(G)| \vdots p$$

Но $Z(G)$ абелев, поэтому существует силовская p-подгруппа $P_0 \subseteq Z(G)$, $|P_0| = p^{k_0}$, $k_0 > 0$. P_0 нормальна в G (как центральная подгруппа):

$$P_0 \lhd G$$

и

$$|G/P_0| = p^{k-k_0} \cdot m < n$$

По предположению индукции, существует силовская подгруппа $\bar{P} \subseteq G/P_0$, $|\bar{P}| = p^{k-k_0}$. Рассмотрим прообраз $\bar{P}$ при канонической проекции:

$$\pi\colon\ G \to G/P_0$$
$$P = \pi^{-1}(\bar{P})$$

- подгруппа в G. Тогда

$$\pi(P) = \bar{P} \simeq P/P_0,$$

откуда следует, что

$$|P| = |\bar{P}| \cdot |P_0| = p^{k-k_0} \cdot p^{k_0} = p^k$$

Таким образом, P – силовская p-подгруппа в G. ■

Итак, силовские p-подгруппы существуют. Для данного простого числа p их может быть несколько, тем не менее, все они устроены одинаково.

2-ая теорема Силова.
1) Все силовские p-подгруппы в G сопряжены друг другу (при данном p).
2) Любая p-подгруппа группы G содержится в некоторой силовской p-подгруппе.

Доказательство.
2) Пусть $P \subseteq G$ – фиксированная силовская p-подгруппа, $H \subseteq G$ – произвольная p-подгруппа. Рассмотрим действие $H \curvearrowright G/P$ умножениями слева:

$$h \circ gP = hgP$$

Данное действие задает разбиение G/P на орбиты:

$$G/P = \boldsymbol{\mathcal{O}}_1 \sqcup \ldots \sqcup \mathcal{O}_s$$

Пусть $|G| = n = p^k m$, p – простое, m не делится на p. Тогда $|P| = p^k$, $|H| = p^l$, $l < k$. Из разбиения G/P на орбиты вытекает, что

$$|G/P| = |\boldsymbol{\mathcal{O}}_1| + \cdots + |\mathcal{O}_s|$$

Здесь $|G/P| = m$ не делится на p, откуда следует, что не все порядки орбит делятся на p. Но порядок каждой орбиты должен делить $|H| = p^l$, поэтому существует i: $|\mathcal{O}_i| = 1$, т.е. $\mathcal{O}_i = \{gP\}$. Тогда $\forall h \in H$:

$$hgP = gP \Rightarrow g^{-1}hgP = P \Rightarrow g^{-1}hg \in P \Rightarrow h \in gPg^{-1}$$

Следовательно,

$$H \subseteq gPg^{-1} \simeq P,$$

где gPg^{-1} – тоже силовская p-подгруппа (действительно, $gPg^{-1} \simeq P$ следует из того, что сопряжение – это автоморфизм, тогда $|gPg^{-1}| = |P| = p^k$).

1) Пусть H сама является силовской p-подгруппой. Тогда

$$|H| = p^k = |P| = |gPg^{-1}|$$

откуда следует, что

$$H = gPg^{-1}$$

■

Следствие. Силовская p-подгруппа $P \subseteq G$ нормальна $\Leftrightarrow$ P – единственная силовская p-подгруппа в G.

Доказательство.
По 2-ой теореме Силова все силовские p-подгруппы в G имеют вид gPg^{-1} ($g \in G$). Но

$$P \lhd G \Leftrightarrow gPg^{-1} = P, \ \ \forall g \in G$$

$\Leftrightarrow P$ – единственная силовская p-подгруппа в G. ■

Прежде чем переходить к 3-ей теореме Силова, обсудим некоторые общие понятия. Пусть S – множество всех подгрупп в G. $G \curvearrowright$ S сопряжениями:

$$g \circ H = g \cdot H \cdot g^{-1}, \ \ \forall g \in G, H \in \mathrm{S}$$

Стабилизатор подгруппы – *нормализатор*:

$$N_G(H) = N(H) = \{g \in G \mid g \cdot H \cdot g^{-1} = H\}$$

- наибольшая подгруппа в G, в которой H нормальна.

Свойства нормализатора:
1)
$$N_G(H) \supseteq H$$
2)
$$H \lhd G \Leftrightarrow N_G(H) = G$$

3-ая теорема Силова.
1) Количество $n_p(G)$ силовских p-подгрупп равно:

$$n_p(G) = \frac{|G|}{|N_G(P)|}$$

где $P \subseteq G$ – фиксированная силовская p-подгруппа. В частности, если $|G| = n = p^k m$, m не делится на p, то $n_p(G)$ делит m.
2)
$$n_p(G) \equiv 1 (\mathrm{mod}\, p)$$
Доказательство.
1) Пусть S_p – множество всех силовских p-подгрупп в G. Из 2-ой теоремы Силова следует, что $G \curvearrowright \mathrm{S}_p$ сопряжениями транзитивно. Тогда

$$n_p(G) = \left|\mathrm{S}_p\right| = \frac{|G|}{|N_G(P)|}$$

- частный случай формулы для порядка орбиты. Так как $N_G(P) \supseteq P$, то $|N_G(P)| = p^k d$, где d – делитель m. Тогда $n_p(G) = \frac{m}{d}$ делит m.

2) Рассмотрим $P \curvearrowright \mathrm{S}_p$ сопряжениями. Оно задает разбиение S_p на орбиты:

$$\mathrm{S}_p = \boldsymbol{\mathcal{O}}_1 \sqcup \ldots \sqcup \mathcal{O}_s$$

При действии $P \curvearrowright \mathrm{S}_p$ сопряжениями на P мы получим P, поэтому одна из орбит состоит из одной точки (можно считать, что $\mathcal{O}_1 = \{P\}$). Докажем, что $|\mathcal{O}_i| > 1$ при $i > 1$. В самом деле, пусть $\mathcal{O}_i = \{Q\}$. Тогда

$$g \cdot Q \cdot g^{-1} = Q, \ \ \forall g \in P \Rightarrow N_G(Q) \supseteq P, Q$$

- в $N_G(Q)$ содержатся две силовские p-подгруппы P, Q. Но $Q \lhd N_G(Q)$, значит, $P = Q$ (по следствию из 2-ой теоремы Силова). Из разбиения S_p на орбиты следует, что

$$n_p(G) = \left|\mathrm{S}_p\right| = |\boldsymbol{\mathcal{O}}_1| + \cdots + |\mathcal{O}_s|$$

Здесь $|\mathcal{O}_1| = 1$, а порядки всех остальных орбит больше 1. Так как порядок подгруппы делит порядок группы, то $|\mathcal{O}_i|$ делится на p при $i > 2$, значит, $n_p(G) \equiv 1 (\mathrm{mod}\, p)$. ■

Проиллюстрируем применение теорем Силова на примерах.

Пример. $G = A_5$.
Опишем силовские подгруппы в A_5. Так как $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$, то силовские подгруппы в A_5 существуют для $p = 2,3,5$.

$p = 2 \Rightarrow |P| = 4$:
Силовская 2-подгруппа в A_5 имеет порядок 4. Тогда $\forall \sigma \in P$ имеем:

$$o(\sigma) = 1,2, \text{или } 4$$

Порядки элементов в A_5:

- если $\sigma = \varepsilon$ – тождественная подстановка, то $o(\sigma) = 1$,
- если σ – тройной цикл: $\sigma = (i,j,k)$, то $o(\sigma) = 3$,
- если σ – пятерной цикл: $\sigma = (i,j,k,l,m)$, то $o(\sigma) = 5$,
- если σ – произведение транспозиций: $\sigma = (i,j)(k,l)$, то $o(\sigma) = 2$.

Таким образом, в силовской 2-подгруппе в A_5 содержатся только элементы порядка 1 и 2: тождественная перестановка и произведение транспозиций. Однако, не каждая пара произведений транспозиций может лежать в одной силовской 2-группе: если умножить пару независимых транспозиций $(i,j)(k,l)$ на пару независимых транспозиций, содержащих номер m:

$$(i,j)(k,l) \cdot (i,j)(l,m) = (k,l,m)$$

- получим тройной цикл (элемент порядка 3), значит, такие две пары не могут одновременно входить в P. Аналогично

$$(i,j)(k,l) \cdot (j,k)(l,m) = (k,i,j,l,m)$$

- получим пятерной цикл (элемент порядка 5), поэтому такие две пары также не могут одновременно входить в P.

Другими словами, группа P может быть составлена из пар независмых транспозиций, в которых участвуют только 4 номера:

$$P = \{\varepsilon, (i,j)(k,l), (i,k)(j,l), (i,l)(j,k)\} = P_m$$

Подобную подгруппу мы рассматривали в A_4 – это группа Клейна: $P_m \simeq V_4$. Всего таких подгрупп в A_5 будет 5. Итак, все силовские 2-подгруппы в A_5 – это P_1, P_2, P_3, P_4, P_5.
В соответствии с 3-ей теоремой Силова,

$$n_2 = 5 \equiv 1 (\mathrm{mod}\, 2).$$

Сопряженность:

$$\sigma \cdot P_m \cdot \sigma^{-1} = P_{\sigma(m)}$$

Все подгруппы P_m будут сопряжены: $\forall m, n \in \{1,2,3,4,5\} \quad \exists \sigma \in A_5 \colon \ \sigma(m) = n$.

Нормализатор $N(P_m)$ состоит из подстановок $\sigma \in A_5$, оставляющих на месте P_m, т.е. удовлетворяющих условию $\sigma(m) = m$. Таким образом,

$$N(P_m) \simeq A_4.$$

В соответствии с 3-ей теоремой Силова,

$$n_2 = \frac{|G|}{|N(P_m)|} = \frac{60}{12} = 5$$

$p = 3 \Rightarrow |P| = 3$:
Силовская 3-подгруппа в A_5 имеет порядок 3, следовательно, это циклическая группа:

$$P = < \sigma >$$

Она порождается элементом $\sigma, \ o(\sigma) = 3$, поэтому $\sigma = (i, j, k)$ – тройной цикл. Тогда

$$P = < \varepsilon, (i, j, k), (k, j, i) \ > = P_{i,j,k}$$

Всего таких подгрупп в A_5 будет $C_5^3 = 10$. В соответствии с 3-ей теоремой Силова,

$$n_3 = 10 \equiv 1 (\mathrm{mod}\, 3).$$

В группе A_5 все тройные циклы сопряжены (см. прошлую лекцию), поэтому (так как каждая силовская 3-подгруппа порождается тройным циклом), все силовские 3-подгруппы будут сопряжены.

Упражнение 1. Найти $N(P_{i,j,k})$.

$p = 5 \Rightarrow |P| = 5$:
Силовская 5-подгруппа в A_5 имеет порядок 5, следовательно, это циклическая группа:

$$P = < \sigma >$$

Она порождается элементом $\sigma, \ o(\sigma) = 5$, поэтому $\sigma = (i, j, k, l, m)$ – пятерной цикл. Тогда

$$P = < \varepsilon, \sigma, \sigma^2, \sigma^3, \sigma^4 >$$

Всего пятерных циклов в A_5 будет $4! = 24$, они разбиваются на группы по 4 элемента, каждая из которых дает силовскую 5-подгруппу. Поэтому количество силовских 5-подгрупп в A_5 равно

$$n_5 = \frac{4!}{4} = 6$$

В соответствии с 3-ей теоремой Силова,

$$n_5 = 6 \equiv 1 (\mathrm{mod}\, 5).$$

Упражнение 2. Доказать сопряженность всех силовских 5-подгрупп в A_5 и найти нормализатор какой-нибудь из них.

В заключение рассмотрим один из многочисленных примеров приложения силовских подгрупп в теории конечных групп. Как известно, группы простого порядка p – это циклические группы, а группы порядка p^2 всегда абелевы (для каждого простого p их две с точностью до изоморфизма – это следует из классификации абелевых групп). С помощью теорем Силова можно описать группы, порядок которых равен произведению двух простых чисел.

Теорема. Пусть $|G| = pq$, p, q – простые, $p > q$. Тогда:
1) G разрешима,
2) если $p - 1$ не делится на q, то G – циклическая: $G \simeq \mathbb{Z}_{pq}$.

Доказательство.
1) Пусть $P \subset G$ – силовская p-подгруппа. По 3-ей теореме Силова,

$$n_p(G) \equiv 1 (\mathrm{mod}\, p),$$
$$n_p(G) \text{ делит } q.$$

Так как $p > q$, то возможен лишь один вариант: $n_p(G) = 1$. Тогда по следствию из 2-ой теоремы Силова, $P \lhd G$. Имеем:

$$|P| = p, \;\; |G/P| = q$$

- порядки групп P и G/P являются простыми числами, значит, P и G/P – циклические, откуда следует, что они абелевы, а значит, разрешимые. Из критерия разрешимости следует, что и группа G также будет разрешимой.

2) Пусть $Q \subset G$ – силовская q-подгруппа. По 3-ей теореме Силова,

$$n_q(G) \equiv 1 (\mathrm{mod}\, q),$$
$$n_q(G) \text{ делит } p.$$

Так как p – простое, то либо $n_q(G) = 1$, либо $n_q(G) = p$. Так как по условию $p - 1$ не делится на q, то вариант $n_q(G) = p$ невозможен (противоречит условию $n_q(G) \equiv 1 (\mathrm{mod}\, q)$), значит, $n_q(G) = 1$.

Тогда по следствию из 2-ой теоремы Силова, $Q \lhd G$ и в группе G есть две нормальные подгруппы P и Q. Рассмотрим их пересечение:

$$|P \cap Q| \text{ делит } p = |P| \text{ и } q = |Q|$$

Так как p и q – два различных простых числа, то $P \cap Q = \{e\}$. Таким образом, в G содержатся две нормальные подгруппы, пересекающиеся по единице, значит, G содержит и их прямое произведение:

$$G \supseteq P \times Q.$$

Но

$$|P \times Q| = pq = |G|.$$

Следовательно,

$$G = P \times Q \simeq \mathbb{Z}_p \bigoplus \mathbb{Z}_q \simeq \mathbb{Z}_{pq}$$

■

Лекция 13. Линейные представления групп.

При изучении свойств группы и ее элементов бывает удобно вложить группу (или хотя бы гомоморфно отобразить ее) в какую-нибудь другую группу, более нам знакомую. В таком случае говорят о представлении одной группы в другой. Чаще всего в качестве более знакомой группы берется группа невырожденных матриц или линейных операторов в каком-нибудь векторном пространстве – про эти группы мы довольно много знаем.

Определение. *Линейное представление* группы G в векторном пространстве V над полем K – это гомоморфизм из группы G в группу невырожденных линейных операторов над V:

$$\mathcal{R}\colon\ G \to GL_n(V)$$

Иначе можно сказать, что это действие G на V с помощью линейных преобразований.

Размерностью линейного представления: $dim\,\mathcal{R}$ называется размерность векторного пространства, на котором задано линейное представление:

$$dim\,\mathcal{R} = dim\,V$$

В нашем курсе мы чаще будем рассматривать конечномерные представления.

Параллельно с линейными можно рассматривать матричные представления. *Матричное представление* группы G над полем K – это гомоморфизм из группы G в группу невырожденных матриц:

$$R\colon\ G \to GL_n(K)$$

Его размерность:

$$dim\,R = n$$

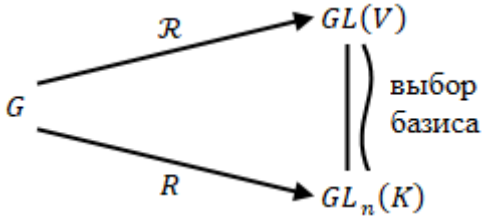
Между матричными и линейными представлениями существует естественная связь, а именно – выбор базиса $(e_1, \dots, e_n)$ в пространстве V устанавливает взаимно-однозначное соответствие между линейными операторами и матрицами размера $n \times n$. В частности, невырожденным линейным операторам соответствуют невырожденные матрицы, т.е. выбор базиса в пространстве V задает изоморфизм между группой невырожденных линейных операторов на V и группой невырожденных матриц размера $n \times n$ над полем K:

$$GL(V) \simeq GL_n(K)$$

Таким образом, возникает взаимно-однозначное соответствие между линейными и матричными представлениями соответствующей размерности:

$$\mathcal{R} \leftrightarrow R$$

Подчеркнем, однако, что это соответствие не каноническое, а зависит от базиса в пространстве V:



Соглашения по обозначениям: линейные операторы и линейные представления будем обозначать рукописными заглавными латинскими буквами:

$$\mathcal{A}, \mathcal{R}, \ldots$$

А соответствующие матрицы и матричные представления – теми же печатными заглавными латинскими буквами:

$$A, R, \ldots$$

Примеры линейных представлений:

1) Линейное представление бесконечной циклической группы:

$$\mathcal{R}\colon \mathbb{Z} \to GL(V)$$

задается одним невырожденным линейным оператором $\mathcal{A} = \mathcal{R}(1)$:

$$\mathcal{R}(n) = \mathcal{A}^n, \ \ \forall n \in \mathbb{Z}$$

- чтобы задать линейное представление группы целых чисел, достаточно задать один линейный оператор, поэтому можно сказать, что теория представлений группы целых чисел – это то же самое, что теория линейных операторов.

2) Линейное представление конечной циклической группы:

$$\mathcal{R}\colon \mathbb{Z}_m \to GL(V)$$

также задается одним невырожденным линейным оператором $\mathcal{A} = \mathcal{R}(\overline{1})$, но уже не произвольным (так как $\overline{1}$ – элемент конечного порядка m в $\mathbb{Z}_m$), а таким, что $\mathcal{A}^m = \mathcal{E}$:

$$\mathcal{R}(\overline{n}) = \mathcal{A}^n, \ \ \forall \overline{n} \in \mathbb{Z}_m$$

Таким образом, теория представлений конечных циклических групп – это теория линейных операторов конечного порядка.

3) Мономиальное представление симметрической группы

$$\mathcal{R}\colon S_n \to GL(K^n)$$

Это представление задается следующим образом: для любой подстановки $\sigma \in S_n$ оператор $\mathcal{R}(\sigma)$ действует на базисные векторы стандартного базиса в K^n перестановкой σ, т.е.

$$\forall \sigma \in S_n, \forall i = 1, \dots, n\colon \quad \mathcal{R}(\sigma)e_i = e_{\sigma(i)}$$

На произвольный вектор $x = \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} \in K^n$ оператор $\mathcal{R}(\sigma)$ действует следующим образом:

$$\mathcal{R}(\sigma)x = \mathcal{R}(\sigma)(x_1e_1 + \cdots + x_ne_n) = x_1e_{\sigma(1)} + \cdots + x_ne_{\sigma(n)} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ \cdots \\ x_{\sigma^{-1}(n)} \end{pmatrix}$$

- так как $i = \sigma(j)$, то при i-ом базисном векторе будет координата $j = \sigma^{-1}(i)$.

Матричная реализация этого линейного представления в стандартном базисе с помощью мономиальных матриц (матриц, у которых в каждой строке и каждом столбце ровно одна единица, а остальные элементы равны нулю):

$n = 2$:

$$R(\varepsilon) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad R((1,2)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$n = 3$:

$$R(\varepsilon) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ R((1,2)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ R((1,3)) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$R((2,3)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \ R((1,2,3)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \ R((1,3,2)) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

4) Пусть V – евклидово пространство, $dim\, V = 2$. Рассмотрим представление группы действительных чисел поворотами:

$$\mathcal{R}\colon \mathbb{R} \to GL(V),$$
$$\mathcal{R}(t) \text{ – поворот на угол } t$$

Это действительно будет линейным представлением, так как при композиции поворотов углы поворотов складываются. Матричная реализация этого линейного представления в некотором ортонормированном базисе (e_1, e_2):

$$R\colon \mathbb{R} \to GL_2(\mathbb{R})$$

$$R(t) = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

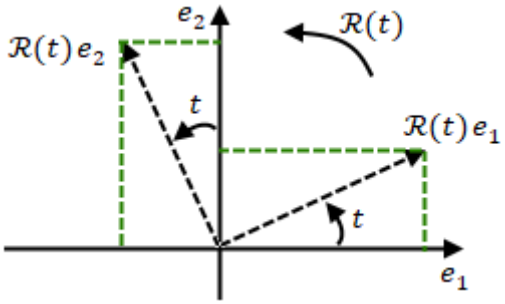


Рис. 13.1. К примеру 4)

5) Пусть задано действие $G \curvearrowright X$. По этому действию можно построить линейное представление группы G в

$$V = \mathcal{F}(X, K) = \{f\colon X \to K\}$$

– пространстве функций на множестве X.

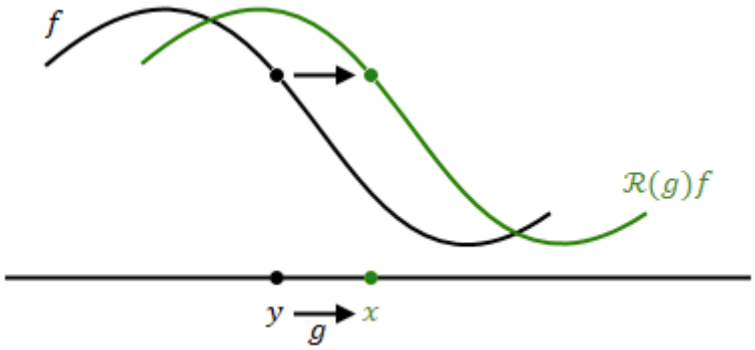


Рис. 13.2. К примеру 5)

Будем рассуждать следующим образом: элемент $g \in G$ как-то двигает точки множества X. В соответствии с этим движением сдвинем график функции f (см. рис. 13.2).

Пусть точка x под действием $g \in G$ перешла в точку y:

$$g \cdot y = x,$$

тогда

$$y = g^{-1} \cdot x.$$

Значение функции $\mathcal{R}(g)f$ в точке x положим равным значению функции f в точке y:

$$[\mathcal{R}(g)f](x) = f(g^{-1} \cdot x)$$

- формула, определяющая действие группы G на множестве функций.

Проверим, что это действительно линейное представление.

Линейность:
1)

$$[\mathcal{R}(g)(f_1+f_2)](x) = (f_1+f_2)(g^{-1}\cdot x) = f_1(g^{-1}\cdot x) + f_2(g^{-1}\cdot x) =$$

$$= [\mathcal{R}(g)f_1](x) + [\mathcal{R}(g)f_2](x) \Rightarrow \mathcal{R}(g)(f_1+f_2) = \mathcal{R}(g)f_1 + \mathcal{R}(g)f_2$$

2) Аналогично проверяется, что

$$[\mathcal{R}(g)(\lambda f)](x) = \lambda\mathcal{R}(g)f$$

Гомоморфизм:

$$[\mathcal{R}(g_1g_2)f](x) = f((g_1g_2)^{-1}\cdot x) = f({g_2}^{-1}{g_1}^{-1}\cdot x) = f({g_2}^{-1}\cdot y) = [\mathcal{R}(g_2)f](y) =$$

$$= \tilde{f}({g_1}^{-1}\cdot x) = \left[\mathcal{R}(g_1)\tilde{f}\right](x) = [\mathcal{R}(g_1)\mathcal{R}(g_2)f](x) \Rightarrow \mathcal{R}(g_1g_2) = \mathcal{R}(g_1)\mathcal{R}(g_2)$$

(при доказательстве для краткости ввели обозначения $y = {g_1}^{-1}\cdot x,\ \ \tilde{f} = \mathcal{R}(g_2)f$).

Осталось заметить, что это гомоморфизм в группу невырожденных операторов – очевидно, что $\mathcal{R}(e) = \mathcal{E}$, откуда следует, что у каждого оператора $\mathcal{R}(g)$ существует обратный:

$$\mathcal{R}(g)^{-1} = \mathcal{R}(g^{-1}),\ \ \forall g \in G,$$

так как

$$\mathcal{E} = \mathcal{R}(e) = \mathcal{R}(gg^{-1}) = \mathcal{R}(g)\mathcal{R}(g^{-1})$$

■

Частный случай:

$$|X| = n < \infty$$

В качестве примера рассмотрим случай конечного множества X. Каждая функция на X задается конечным множеством значений, поэтому функции на конечном множестве можно отождествить с конечным набором элементов поля K.

Отождествим стандартный базис в пространстве функций $\mathcal{F}(X,K) = \{f\colon X \to K\}$ со стандартным базисом пространства строк (столбцов) K^n, а именно: i-ый базисный вектор в пространстве K^n отождествим с функцией $\varepsilon_y(x)$, принимающей в точке x значение 1, а во всех остальных точках – значение 0:

$$\varepsilon_y(x) = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases}$$

Тогда $\forall f \in \mathcal{F}(X,K)$:

$$f = \sum_{y\in X} f(y)\varepsilon_y$$

В этом базисе линейное представление $\mathcal{R}$ устроено следующим образом:

$$\forall g \in G,\ \ \forall y \in X\colon \quad \mathcal{R}(g)\varepsilon_y = \varepsilon_{gy}$$

Другими словами, базисные функции переставляются – это похоже на мономиальное представление, которое является частным случаем линейного представления конечного множества.

Пример.

$$X = \{1, \dots, n\},\ \ G = S_n,$$

тогда

$$\mathcal{F}(X, K) = K^n,\ \ \mathcal{R} \text{ - мономиальное представление}$$

В общем случае (как видно из формулы $\mathcal{R}(g)\varepsilon_y = \varepsilon_{gy}$) произвольное представление группы G в $\mathcal{F}(X, K)$ может быть представлено в виде композиции:

$$\mathcal{R}\colon \quad G \xrightarrow[\text{действия}]{\text{гомоморфизм}} S(X) \xrightarrow[\text{представление}]{\text{мономиальное}} GL(V)$$

6) Рассмотрим еще один частный случай представления группы G в $V = \mathcal{F}(X, K)$. Положив $X = G$, получим т.н. *регулярное представление* группы G. Регулярное представление бывает левым и правым.

Левое регулярное представление:

$$\mathcal{L}\colon\ G \to GL(V)$$

- задается с помощью действия $G \curvearrowright G$ умножениями слева. Согласно общей формуле, определяющей действие группы G на множестве функций $\mathcal{F}(X, K)$:

$$[\mathcal{L}(g)f](x) = f(g^{-1} \cdot x), \qquad \forall f \in \mathcal{F}(G, K),\ \ \forall g, x \in G$$

Правое регулярное представление:

$$\mathcal{R}\colon\ G \to GL(V)$$

- задается с помощью действия $G \curvearrowright G$ умножениями справа. Согласно общей формуле, определяющей действие группы G на множестве функций $\mathcal{F}(X, K)$:

$$[\mathcal{R}(g)f](x) = f(x \cdot g), \qquad \forall f \in \mathcal{F}(G, K),\ \ \forall g, x \in G$$

Гомоморфизмы линейных представлений.

Как и сами группы, линейные представления удобно сравнивать между собой с помощью гомоморфизмов.

Определение. Пусть

$$\mathcal{R}\colon\ G \to GL(V),$$
$$\mathcal{R}'\colon\ G \to GL(V')$$

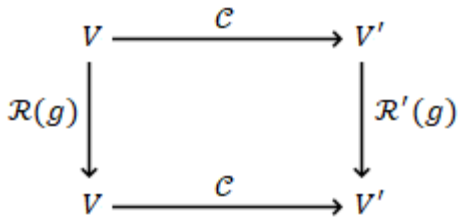
- два линейных представления группы G. *Гомоморфизм* $\mathcal{R} \to \mathcal{R}'$ - это линейное отображение

$$\mathcal{C}\colon V \to V',$$

для которого $\forall g \in G$:

$$\mathcal{C} \cdot \mathcal{R}(g) = \mathcal{R}'(g) \cdot \mathcal{C}$$

Другими словами, перестановка оператора представления через гомоморфизм $\mathcal{C}$ превращает одно представление в другое. Происходящее можно изобразить в виде коммутативной диаграммы:



Таким образом, линейное представление – это линейное отображение векторных пространств, перестановочное с действием группы G на этих пространствах.

Изоморфизм линейных представлений – это биективный гомоморфизм. Изоморфизм

$$\mathcal{C}\colon V \xrightarrow{\sim} V'$$

позволяет отождествить V с V', а поскольку диаграмма, изображенная выше, коммутативна, то он позволяет отождествить также $\mathcal{R}$ с $\mathcal{R}'$.

Определение. Пусть

$$R\colon\ G \to GL_n(K),$$
$$R'\colon\ G \to GL_m(K)$$

- два матричных представления группы G. *Гомоморфизм* $R \to R'$ - это матрица

$$C \in Mat_{m\times n}(K),$$

для которой $\forall g \in G$:

$$C \cdot R(g) = R'(g) \cdot C$$

Изоморфизм матричных представлений – это гомоморфизм, для которого $m = n$ и матрица C невырождена. В этом случае

$$R'(g) = C \cdot R(g) \cdot C^{-1},$$

т.е. матрицы представления R' сопряжены матрицам представления R с помощью одной и той же сопрягащей матрицы.

Это наблюдение позволяет правильно интерпретировать геометрический смысл изоморфизма матричных представлений – замена матрицы на сопряженную означает замену базиса, т.е. если R – матричная реализация линейного представления $\mathcal{R}$ в базисе $(e_1, \dots, e_n)$, то тогда матричная реализация изоморфного ему представления $\mathcal{R}'$ – это матричная реализация того же самого линейного представления $\mathcal{R}$ в другом базисе $(e_1', \dots, e_n')$, а C – матрица перехода от $(e_1', \dots, e_n')$ к $(e_1, \dots, e_n)$.

Таким образом, изоморфные матричные представления – это записи одного и того же линейного представления в разных базисах.

Инвариантное подпространство.

Возникает естественный вопрос – к какому наиболее простому виду можно привести матричную запись линейного представления (представление, естественно, предполагается конечномерным) путем удачного выбора базиса? В линейной алгебре мы уже сталкивались с похожим вопросом (приведение матрицы линейного оператора к жордановой форме), и одно из понятий, которое мы для этого использовали – это инвариантное подпространство. То же самое понятие возникает и для линейных представлений.

Определение. Пусть

$$\mathcal{R}\colon\ G \to GL(V)$$

- линейное представление. Подпространство $U \subseteq V$ инвариантно относительно представления $\mathcal{R}$, если применяя операторы представления к векторам из этого подпространства, мы остаемся в нем:

$$\forall g \in G, \forall u \in U\colon \quad \mathcal{R}(g) \cdot u \in U$$

В этом случае (поскольку операторы представления обратимы, и обратные к ним тоже являются операторами представления, соответствующие обратным элементам группы G):

$$\forall g \in G, \forall v \in U \ \ \exists u \in U\colon \quad \mathcal{R}(g) \cdot u = v,$$

где

$$u = \mathcal{R}(g^{-1}) \cdot v.$$

Другими словами,

$$\mathcal{R}(g)U = U$$

- оператор $\mathcal{R}(g)$ переводит подпространство U в себя.

Рассмотрим $\mathcal{R}(g)|_U$ – ограничение оператора $\mathcal{R}(g)$ на U. В силу сказанного выше, это будет сюръективное отображение ($Im(\mathcal{R}(g)|_U) = U$), но оно будет также и инъективным, потому что оператор $\mathcal{R}(g)$ – невырожденный, а значит, инъективный на всем пространстве V, тем более на U. Следовательно, $\mathcal{R}(g)|_U$ – обратимый линейный оператор на U.

Таким образом, каждый оператор представления мы можем ограничить на инвариантное подпространство и получить обратимый линейный оператор на этом инвариантном подпространстве. Возникает *подпредставление*:

$$\mathcal{R}|_U\colon\ G \to GL(U)$$
$$\mathcal{R}|_U(g) = \mathcal{R}(g)|_U$$

Пусть $(e_1, \dots, e_k, \dots, e_n)$ – базис V, согласованный с U (т.е. $(e_1, \dots, e_k)$ – базис U). В этом базисе матрица оператора $\mathcal{R}(g)$ выглядит следующим образом:

$$R(g) = \begin{array}{c|cc} & k & n-k \\ k & \mathcal{R}|_U(g) & * \\ n-k & 0 & * \end{array}$$

Приводимые, неприводимые и вполне приводимые линейные представления.

Определение. Линейное представление

$$\mathcal{R}\colon\ G \to GL(V)$$

- *приводимо*, если существует нетривиальное инвариантное подпространство $U \subseteq V$ (т.е. $U \neq \{0\}, V$),
- *неприводимо*, если $V \neq \{0\}$ и $\mathcal{R}$ не является приводимым (т.е. в V нет нетривиальных инвариантных подпространств),
- *вполне приводимо*, если для любого инвариантного подпространства $U \subseteq V$ существует инвариантное дополнительное подпространство $W \subseteq V$, такое что $V = U \oplus W$.

В базисе $(e_1, \dots, e_k, e_{k+1}, \dots, e_n)$ пространства V, согласованном с U, W (т.е. $(e_1, \dots, e_k)$ – базис U, $(e_{k+1}, \dots, e_n)$ – базис W) матрица оператора $\mathcal{R}(g)$, $\forall g \in G$ будет блочно-диагональной:

$$R(g) = \begin{array}{c|cc} & k & n-k \\ k & \mathcal{R}|_U(g) & 0 \\ n-k & 0 & \mathcal{R}|_W(g) \end{array}$$

Примеры:

1) Представление $\mathcal{R}$ группы $\mathbb{R}$ в двумерном евклидовом пространстве V поворотами неприводимо (так как в V нет инвариантых подпространств – любая прямая под действием поворота на угол, не кратный π, перейдет в другую прямую):

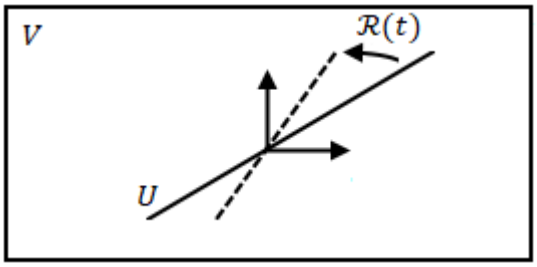


Рис. 13.3. В V нет инвариантых подпространств

2) Представление $\mathcal{R}$ группы $\mathbb{R}$ в двумерном евклидовом пространстве V, которое в матричной реализации выглядит следующим образом:

$$R(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

Легко проверить, что это действительно представление:

$$R(t_1)R(t_2) = \begin{pmatrix} 1 & t_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & t_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & t_1 + t_2 \\ 0 & 1 \end{pmatrix} = R(t_1 + t_2)$$

Представление $\mathcal{R}$ приводимо, в качестве нетривиального инвариантного подпространства можно выбрать

$$U = < e_1 >$$

- прямую, натянутую на e_1.

Однако, $\mathcal{R}$ не вполне приводимо: действительно, в противном случае имело бы место разложение

$$V = U \oplus W,$$

где

$$W = < e_2' >$$

- тоже инвариантное подпространство.

Тогда в базисе (e_1, e_2') матрица $R'(t)$ была бы диагональной:

$$R'(t) = \begin{pmatrix} 1 & 0 \\ 0 & \lambda(t) \end{pmatrix}$$

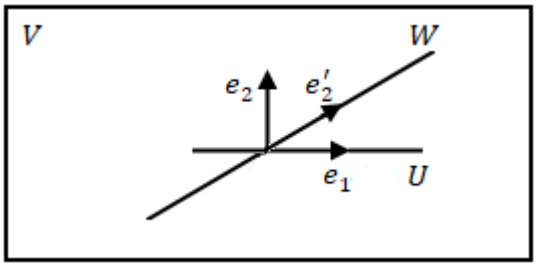


Рис. 13.4. $V = U \oplus W$, где $W = < e_2' >$

С другой стороны, базис (e_1, e_2) связан с базисом (e_1, e_2') с помощью матрицы перехода C, тогда

$$R'(t) = C \cdot R(t) \cdot C^{-1}.$$

Отсюда следует, что

$$det\, R'(t) = det\, R(t) \Leftrightarrow \lambda(t) = 1,$$

то есть,

$$R'(t) = E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

и

$$\mathcal{R}(t) = \mathcal{E}, \ \ \forall t \in \mathbb{R}$$

- противоречие (так как единичный оператор должен иметь единичную матрицу в любом базисе, но в базисе e_1, e_2 его матрица таковой не является).

Лекция 14. Вполне приводимые линейные представления.

На прошлой лекции мы познакомились с понятием приводимости линейных представлений. Докажем, что свойство полной приводимости наследуется при переходе к подпредставлениям.

Предложение 1. Подпредставление вполне приводимого представления вполне приводимо.

Доказательство.
Пусть

$$\mathcal{R}\colon\ G \to GL(V)$$

- вполне приводимое представление, $V' \subseteq V$ – инвариантное подпространство. Рассмотрим подпредставление

$$\mathcal{R}|_{V'}\colon\ G \to GL(V')$$

Докажем его полную приводимость. Пусть $U \subseteq V'$ – инвариантное подпространство для этого подпредставления. Существует $W \subseteq V$, такое что

$$V = U \oplus W.$$

Рассмотрим

$$W' = W \cap V'$$

- инвариантное подпространство (как пересечение двух инвариантных подпространств). Докажем, что

$$V' = U \oplus W'$$

Происходящее иллюстрирует рис. 14.1:

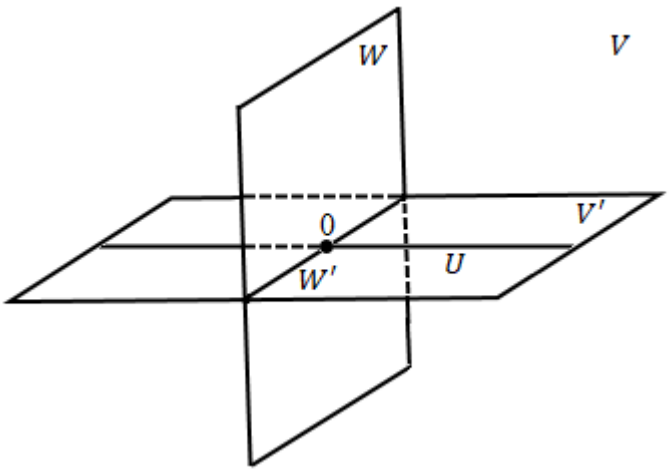


Рис. 14.1. Иллюстрация к предложению 1

Нужно доказать, что любой вектор из V' единственным способом разлагается в сумму векторов из U и W'. В самом деле, так как $V = U \oplus W$, то $\forall v \in V'$ существует единственное разложение

$$v = u + w, \ \ u \in U, w \in W$$

Так как $v \in V'$ и $u \in U \subseteq V'$, то и $v - u = w \in V'$. Тогда

$$v - u = w \in V' \cap W = W'$$

- это и означает, что

$$V' = U \oplus W'.$$

Следовательно, W' - инвариантное дополнение к подпространству U в V', поэтому $\mathcal{R}|_{V'}$ вполне приводимо. ■

Определение. Говорят, что представление $\mathcal{R}\colon \ G \to GL(V)$ разлагается в *прямую сумму линейных представлений*:

$$\mathcal{R} = \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_s$$

если V разлагается в прямую сумму инвариантных подпространств:

$$V = V_1 \oplus \ldots \oplus V_s$$

и

$$\mathcal{R}|_{V_i} = \mathcal{R}_i \quad (i = 1, \ldots, s).$$

В базисе, согласованном с $V_1, \ldots, V_s$ матрица оператора $\mathcal{R}(g)$ будет иметь блочно-диагональный вид (блоки – матрицы операторов $\mathcal{R}_i(g)$):

$$R(g) = \begin{pmatrix} \mathcal{R}_1(g) & & 0 \\ & \ddots & \\ 0 & & \mathcal{R}_s(g) \end{pmatrix}$$

Если мы разложили вполне приводимое представление $\mathcal{R}$ в прямую сумму линейных представлений, то (так как подпредставление вполне приводимого представления вполне приводимо) мы можем продолжить этот процесс – разлагать подпредставления в прямую сумму подпредставлений меньшей размерности. Так как пространство V конечномерно, рано или поздно мы остановимся. Это соображение приводит нас к следущему утверждению (которое верно также и для бесконечномерных пространств V, но доказательство этого факта выходит за рамки нашего курса).

Предложение 2. Всякое конечномерное вполне приводимое представление является прямой суммой неприводимых представлений.

Доказательство.

Пусть $\mathcal{R}\colon\ G \to GL(V)$ – вполне приводимое представление. Докажем утверждение индукцией по размерности представления $dim\ \mathcal{R}$.

База индукции: $dim\ \mathcal{R} = 0$ – доказывать нечего (нулевое пространство является прямой суммой нулевого числа слагаемых).

Шаг индукции: либо $\mathcal{R}$ неприводимо, тогда доказывать нечего (прямая сумма состоит из одного слагаемого $\mathcal{R}$), либо $\mathcal{R}$ приводимо – тогда существует нетривиальное инвариантное подпространство $V' \subset V,\ V' \neq \{0\}, V$. Так как $\mathcal{R}$ вполне приводимо, то существует дополнительное инвариантное подпространство

$$V'' \subset V = V' \oplus V''.$$

Рассмотрим

$$\mathcal{R}' = \mathcal{R}|_{V'} \text{ и } \mathcal{R}'' = \mathcal{R}|_{V''}$$

- вполне приводимые представления (по предложению 1). По предположению индукции, каждое из них разлагается в прямую сумму неприводимых представлений:

$$\mathcal{R}' = \mathcal{R}_1 \oplus \dots \oplus \mathcal{R}_t$$

и

$$\mathcal{R}'' = \mathcal{R}_{t+1} \oplus \dots \oplus \mathcal{R}_s$$

где $\mathcal{R}_i$ – неприводимые представления $(i = 1, \dots, s)$. Тогда

$$\mathcal{R} = \mathcal{R}_1 \oplus \dots \oplus \mathcal{R}_t \oplus \mathcal{R}_{t+1} \oplus \dots \oplus \mathcal{R}_s$$

■

Таким образом, изучение вполне приводимых линейных представлений полностью сводится к изучению неприводимых представлений, которые нельзя упростить. Можно сказать, что неприводимые представления – это элементарные “кирпичики”, из которых складывается любое вполне приводимое представление. Возникает естественный вопрос – какие представления можно свести к неприводимым, т.е. какие представления являются вполне приводимыми ? Можно поставить вопрос более точно – при каких условия все представления данной группы вполне приводимы ? Оказывается, это свойство выполнено по крайней мере для конечных групп (при некотором ограничении на характеристику поля, но нулевой характеристики поля достаточно).

Теорема Машке (H. Maschke, 1853-1908). Всякое (конечномерное) линейное представление конечной группы над полем нулевой характеристики вполне приводимо.

Доказательство.
Пусть G – конечная группа,

$$\mathcal{R}\colon\ G \to GL(V)$$

- конечномерное линейное представление в векторном пространстве V над полем K, $char\ K = 0$. Докажем, что $\mathcal{R}$ вполне приводимо.

Пусть $U \subseteq V$ – инвариантное подпространство. Нужно построить дополнительное инвариантное подпространство.

1) Построим просто дополнительное подпространство – выберем в U базис $(e_1, \dots, e_k)$ и дополним его до $(e_1, \dots, e_k, e_{k+1}, \dots, e_n)$ – базиса пространства V. Тогда $(e_{k+1}, \dots, e_n)$ – базис некоторого подпространства W, и V разлагается в прямую сумму:

$$V = U \oplus W$$

Рассмотрим проектор на U вдоль W:

$$\mathcal{P}\colon V \to V$$
$$v = u + w,\ \ u \in U, w \in W\ \Rightarrow\ \mathcal{P}(v) = u$$

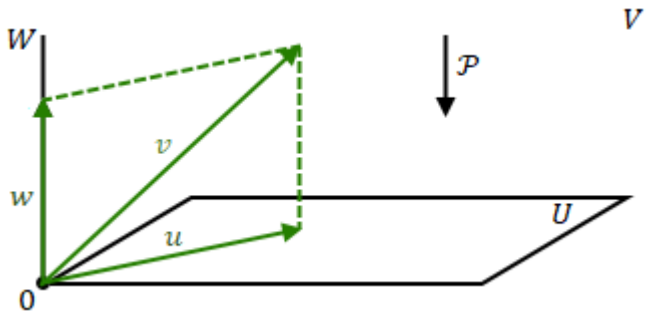


Рис. 14.2. $\mathcal{P}$ – проектор на U вдоль W

Определяющие свойства $\mathcal{P}$:

а)
$$Ker\ \mathcal{P} = W,$$

б)
$$Im\ \mathcal{P} = U,$$

в)
$$\mathcal{P}|_U = \mathcal{E}.$$

То, что эти свойства выполнены и однозначно задают оператор $\mathcal{P}$, следует из определения оператора $\mathcal{P}$.

Обратно, если линейный оператор $\mathcal{P}\colon V \to V$ удовлетворяет свойствам б) и в), и $W = Ker\ \mathcal{P}$, то

$$V = U \oplus W,$$

и $\mathcal{P}$ – проектор на U.
В самом деле, по свойству б):

$$v \in V \Rightarrow \mathcal{P}(v) = u \in U.$$

Тогда по свойству в):

$$w = v - u \Rightarrow \mathcal{P}(w) = \mathcal{P}(v) - \mathcal{P}(u) = u - u = 0 \Rightarrow w \in W$$

Получаем, что любой вектор $v \in V$ представляется в виде суммы $v = u + w$ векторов из U и W. Осталось доказать, что такое представление единственно. Применяя оператор $\mathcal{P}$ к обеим частям равенства, получаем (по свойству в) и потому, что $w \in Ker\ \mathcal{P}$):

$$\mathcal{P}(v) = \mathcal{P}(u) + \mathcal{P}(w) = u + 0 = u$$

Таким образом, первое слагаемое в разложении вектора v определено однозначно, значит, и второе слагаемое тоже определено однозначно: $w = v - u$. Также из равенства

$$\mathcal{P}(v) = \mathcal{P}(u + w) = u$$

следует, что $\mathcal{P}$ – проектор на U.

Другими словами, задать дополнительное подпространство к U – это то же самое, что задать проектор на U, то есть, оператор $\mathcal{P}$, удовлетворяющий свойствам б) и в).

Теперь поймем, как в терминах проектора переформулировать то, что его ядро является инвариантным дополнительным подпространством.

2) Докажем, что

$W = Ker\ \mathcal{P}$ - инвариантное подпространство $\Leftrightarrow$ $\mathcal{P}$ – эндоморфизм представления $\mathcal{R}$,

то есть,

$$\mathcal{P} \cdot \mathcal{R}(g) = \mathcal{R}(g) \cdot \mathcal{P}, \ \ \forall g \in G$$

Доказательство.
$\Rightarrow$:
для произвольного $v \in V$ рассмотрим $\mathcal{P} \cdot \mathcal{R}(g)(v)$. Так как $\mathcal{P}$ – проектор, то v представляется в виде:

$$v = u + w, \ \ u \in U, w \in W.$$

Тогда

$$\mathcal{P} \cdot \mathcal{R}(g)(v) = \mathcal{P}(\mathcal{R}(g)u + \mathcal{R}(g)w) = \mathcal{R}(g)u = \mathcal{R}(g) \cdot \mathcal{P}v$$

(предпоследнее равенство выполнено, так как U и W – инвариантные подпространства, поэтому $\mathcal{R}(g)u \in U$ и $\mathcal{R}(g)w \in W$). Следовательно, $\mathcal{P} \cdot \mathcal{R}(g) = \mathcal{R}(g) \cdot \mathcal{P}, \ \ \forall g \in G$.

$\Leftarrow$:
для произвольных $w \in W$, $g \in G$ убедимся, что $\mathcal{R}(g)w \in W$. Так как $W = Ker\ \mathcal{P}$, то это то же самое, что и

$$\mathcal{P} \cdot \mathcal{R}(g)w = 0.$$

Так как $\mathcal{P}$ коммутирует с $\mathcal{R}(g)$ и $w \in W = Ker\ \mathcal{P}$, то

$$\mathcal{P} \cdot \mathcal{R}(g)w = \mathcal{R}(g) \cdot \mathcal{P}w = \mathcal{R}(g)0 = 0.$$

Отсюда следует, что

$$\mathcal{R}(g)w \in W,$$

то есть, $W = Ker\ \mathcal{P}$ - инвариантное подпространство. ■

3) Изменим W так, чтобы оно стало инвариантным. Для этого изменим $\mathcal{P}$ с помощью операции усреднения по группе, а именно, рассмотрим:

$$\tilde{\mathcal{P}} = \frac{1}{|G|}\sum_{g\in G} \mathcal{R}(g) \cdot \mathcal{P} \cdot \mathcal{R}(g)^{-1}$$

- обратите внимание, что здесь существенна нулевая характеристика поля K, так как мы делим на $|G|$.

Оператор $\tilde{\mathcal{P}}$ тоже является проектором. Чтобы доказать это, нужно проверить, что выполняются свойства б) $Im\ \tilde{\mathcal{P}} = U$ и в) $\tilde{\mathcal{P}}\big|_U = \mathcal{E}$.

б) В самом деле,

$$\forall v \in V\colon\quad \tilde{\mathcal{P}}(v) = \frac{1}{|G|}\sum_{g\in G} \mathcal{R}(g) \cdot \mathcal{P} \cdot \mathcal{R}(g)^{-1}\, v \in U,$$

так как

$$\mathcal{P} \cdot \mathcal{R}(g)^{-1} v \in U,$$

потому что $\mathcal{P}$ – проектор на U. Тогда

$$\mathcal{R}(g) \cdot \mathcal{P} \cdot \mathcal{R}(g)^{-1} v \in U,$$

так как U – инвариантное подпространство.

Чтобы доказать, что $Im\ \tilde{\mathcal{P}} = U$, осталось показать, что так можно получить любой вектор из U – это будет следовать из проверки свойства в):

в)

$$\forall u \in U\colon\ \tilde{\mathcal{P}}(u) = \frac{1}{|G|}\sum_{g\in G} \mathcal{R}(g) \cdot \mathcal{P} \cdot \mathcal{R}(g)^{-1}\, u = \frac{1}{|G|}\sum_{g\in G} \mathcal{R}(g) \cdot \mathcal{P} \cdot \mathcal{R}(g^{-1})\, u =$$

$$= \frac{1}{|G|}\sum_{g\in G} \mathcal{R}(g) \cdot \mathcal{R}(g^{-1})\, u = \frac{1}{|G|}\sum_{g\in G} u = u$$

Следовательно, $\tilde{\mathcal{P}}$ – тоже проектор на U.

Докажем, что $\tilde{\mathcal{P}}$ – эндоморфизм. $\forall g_0 \in G$:

$$\mathcal{R}(g_0)\cdot\tilde{\mathcal{P}}=\frac{1}{|G|}\sum_{g\in G}\mathcal{R}(g_0)\cdot\mathcal{R}(g)\cdot\mathcal{P}\cdot\mathcal{R}(g)^{-1}=\frac{1}{|G|}\sum_{g\in G}\mathcal{R}(g_0 g)\cdot\mathcal{P}\cdot\mathcal{R}(g^{-1})$$

Пусть $h=g_0 g$. Если g пробегает все элементы G, то и h пробегает все элементы G, так как $g={g_0}^{-1}h$. Поэтому можно суммировать не по g, а по h:

$$\mathcal{R}(g_0)\cdot\tilde{\mathcal{P}}=\frac{1}{|G|}\sum_{h\in G}\mathcal{R}(h)\cdot\mathcal{P}\cdot\mathcal{R}(h^{-1}g_0)=\frac{1}{|G|}\sum_{h\in G}\mathcal{R}(h)\cdot\mathcal{P}\cdot\mathcal{R}(h^{-1})\cdot\mathcal{R}(g_0)=\tilde{\mathcal{P}}\cdot\mathcal{R}(g_0)$$

Таким образом, оператор $\tilde{\mathcal{P}}$ перестановочен с любым оператором вида $\mathcal{R}(g_0)$. Значит, $\tilde{\mathcal{P}}$ – эндоморфизм. Следовательно (так как $\tilde{\mathcal{P}}$ является проектором и эндоморфизмом), $\widetilde{W}=Ker\,\tilde{\mathcal{P}}$ – инвариантное подпространство и

$$V=U\oplus\widetilde{W}$$

Теорема Машке полностью доказана. ■

Пример. Мономиальное представление симметрической группы:

$$\mathcal{R}\colon S_n\to GL(K^n)$$

Как обсуждалось на прошлой лекции, $\forall\sigma\in S_n,\forall i=1,\dots,n$ оператор $\mathcal{R}(\sigma)$ действует на базисные векторы стандартного базиса в K^n перестановкой σ, т.е.

$$\mathcal{R}(\sigma)e_i=e_{\sigma(i)}$$

Если поле K имеет нулевую характеристику, то применима теорема Машке – это представление вполне приводимо, значит, его можно разложить в прямую сумму неприводимых представлений. Для этого нужно найти в S_n инвариантное подпространство – оно угадывается очень легко: при любой перестановке базисных векторов их сумма всегда остается на месте, следовательно,

$$U=<e_1+\dots+e_n>=\{x=\begin{pmatrix}x_1\\\dots\\x_n\end{pmatrix}\in K^n\mid x_1=\dots=x_n\}$$

- инвариантное подпространство.

В качестве дополнительного инвариантного подпространства W выберем

$$W=\{x\in K^n\mid x_1+\dots+x_n=0\}.$$

В самом деле:

$$x\in U\cap W\Rightarrow x=\begin{pmatrix}t\\\dots\\t\end{pmatrix},\quad x_1+\dots+x_n=nt=0\Rightarrow t=0\Rightarrow x=\bar{0}$$

(здесь существенно, что $char\ K = 0$). Следовательно, $U \cap W = \{0\}$. Также

$$dim\ (U \oplus W) = dim\ (U) + dim\ (W) = 1 + (n-1) = n.$$

Значит,

$$K^n = U \oplus W$$

Итак, мы разложили K^n в прямую сумму двух инвариантных подпространств. Но первое из них (U) одномерно, значит, представление $\mathcal{R}|_U$ неприводимо (в одномерном пространстве нет нетривиальных подпространств). Докажем, что и представление $\mathcal{R}|_W$ также будет неприводимым (представление $S = \mathcal{R}|_W$ также называется стандартным линейным представлением группы S_n, $dim\ S = n - 1$).

Пусть $W' \subseteq W$ – ненулевое инвариантное подпространство. Выберем $x \in W', x \neq 0$. Сумма координат ненулевого вектора x равна нулю, следовательно, у него есть координаты разных знаков, в частности, $\exists i, j\colon\ x_i \neq x_j$. Подействем на x транспозицией номеров i и j:

$$\mathcal{R}(i,j) \cdot x = \begin{pmatrix} x_1 \\ \dots \\ x_j \\ \dots \\ x_i \\ \dots \\ x_n \end{pmatrix} \in W'$$

Но тогда и разность векторов x и $\mathcal{R}(i,j) \cdot x$ также должна лежать в W':

$$x - \mathcal{R}(i,j)x = \begin{pmatrix} 0 \\ \dots \\ x_i - x_j \\ \dots \\ x_i - x_j \\ \dots \\ 0 \end{pmatrix} = (x_i - x_j)(e_i - e_j) \in W' \Rightarrow e_i - e_j \in W'$$

- получили, что разность $e_i - e_j$ лежит в W'. Понятно, что тогда все такие разности обязаны лежать в W' (всегда можно подобрать подстановку, переводящую i в k, а j в l):

$$\forall k, l \in \{1, \dots, n\},\ \ k \neq l \quad \exists \sigma = \begin{pmatrix} \dots & i & \dots & j & \dots \\ \dots & k & \dots & l & \dots \end{pmatrix} \in S_n \Rightarrow$$

$$\Rightarrow \mathcal{R}(\sigma)(e_i - e_j) = e_k - e_l \in W'$$

Но разности $e_k - e_l$ ($k, l \in \{1, \dots, n\},\ \ k \neq l$) порождают пространство W, следовательно,

$$W' = W,$$

откуда следует, что представление $\mathcal{R}|_W$ неприводимо. ■

Ортогональные и унитарные линейные представления.

Над полями $\mathbb{R}$ и $\mathbb{C}$ для изучения линейных представлений можно использовать некоторые дополнительные геометрические соображения из линейной алгебры. Над этими полями существуют пространства со скалярным умножением – евклидовы в действительном случае и эрмитовы в комплексном случае.

Определение. Пусть V – евклидово или эрмитово векторное пространство над $\mathbb{R}$ или $\mathbb{C}$ соответственно, и $(x \mid y)$ – скалярное произведение векторов $x, y \in V$. Линейное представление

$$\mathcal{R}\colon\ G \to GL(V)$$

называется *ортогональным* (соответственно *унитарным*), если все $\mathcal{R}(g)$ являются ортогональными (соответственно унитарными) операторами ($\forall g \in G$). Другими словами, $\mathcal{R}(g)$ сохраняют скалярное произведение:

$$(x \mid y) = (\mathcal{R}(g)x \mid \mathcal{R}(g)y), \qquad \forall x, y \in V,\ \ \forall g \in G$$

Предложение 3. Всякое ортогональное или унитарное представление вполне приводимо.

Доказательство.
Пусть $U \subseteq V$ – инвариантное подпространство. Тогда

$$V = U \oplus U^{\perp}$$

и $U^{\perp}$ инвариантно. В самом деле:

$$x \in U^{\perp} \Rightarrow (x \mid y) = 0,\ \ \forall y \in U$$

Докажем, что $\forall g \in G$ выполнено $\mathcal{R}(g)x \in U^{\perp}$:

$$\forall g \in G\colon\quad (\mathcal{R}(g)x \mid y) = \ (x \mid \mathcal{R}(g^{-1})y) = 0,$$

так как U – инвариантное подпространство и $\mathcal{R}(g^{-1})y \in U$. Значит, $\mathcal{R}(g)x \in U^{\perp}$.

Это и означает, что ортогональное дополнение $U^{\perp}$ является инвариантным подпространством. ■

Предложение 4. Для любого конечномерного линейного представления

$$\mathcal{R}\colon\ G \to GL(V)$$

конечной группы G в конечномерном пространстве V над $\mathbb{R}$ или $\mathbb{C}$ существует евклидова или эрмитова структура на V, для которой $\mathcal{R}$ ортогонально или унитарно.

Иными словами, всякое конечномерное линейное представление конечной группы над $\mathbb{R}$ или $\mathbb{C}$ ортогонализуемо (унитаризуемо).

Доказательство.
Пусть $(\cdot \mid \cdot)$ – какое-то скалярное умножение на V. Усредним по группе – определим функцию $(\cdot \mid\mid \cdot)$ следующим образом:

$$(x \mid\mid y) = \frac{1}{|G|}\sum_{g\in G}(\mathcal{R}(g)x \mid \mathcal{R}(g)y)$$

- это тоже билинейная симметрическая или полуторалинейная эрмитова функция на V (так как каждое слагаемое обладает этими свойствами).

Проверим, что $(\cdot \mid\mid \cdot)$ положительно определена: так как $\mathcal{R}(g)$ невырожден, то из $x \neq 0$ следует, что $\mathcal{R}(g)x \neq 0$. Тогда

$$x \neq 0 \Rightarrow (x \mid\mid x) = \frac{1}{|G|}\sum_{g\in G}(\mathcal{R}(g)x \mid \mathcal{R}(g)x) > 0$$

Таким образом, функция $(\cdot \mid\mid \cdot)$ – скалярное умножение. Проверим, что оно сохраняется под действием операторов представления $\mathcal{R}$. Действительно, $\forall g_0 \in G, \forall x, y \in V$:

$$(\mathcal{R}(g_0)x \mid\mid \mathcal{R}(g_0)y) = \frac{1}{|G|}\sum_{g\in G}(\mathcal{R}(g)\mathcal{R}(g_0)x \mid \mathcal{R}(g)\mathcal{R}(g_0)y)$$

как и в доказательстве теоремы Машке, обозначив $h = gg_0$, получим:

$$\frac{1}{|G|}\sum_{g\in G}(\mathcal{R}(g)\mathcal{R}(g_0)x \mid \mathcal{R}(g)\mathcal{R}(g_0)y) = \frac{1}{|G|}\sum_{h\in G}(\mathcal{R}(h)x \mid \mathcal{R}(h)y) = (x \mid\mid y)$$

Следовательно, представление $\mathcal{R}$ ортогонально или унитарно по отношению к $(\cdot \mid\mid \cdot)$. ■

Следствие. Короткое доказательство теоремы Машке над $\mathbb{R}$ или $\mathbb{C}$.

Лекция 15. Лемма Шура. Неприводимые представления абелевых групп.

Напоминание: ранее мы вводили понятие гомоморфизма линейных представлений. Пусть

$$\mathcal{R}\colon\ G \to GL(V),$$
$$\mathcal{R}'\colon\ G \to GL(V')$$

- два линейных представления группы G.

Гомоморфизм из $\mathcal{R}$ в $\mathcal{R}'$ - это линейное отображение

$$\mathcal{C}\colon\ V \to V',$$

для которого $\forall g \in G$:

$$\mathcal{C} \cdot \mathcal{R}(g) = \mathcal{R}'(g) \cdot \mathcal{C}$$

Эндоморфизм – это гомоморфизм из $\mathcal{R}$ в $\mathcal{R}$, т.е. линейный оператор

$$\mathcal{C}\colon\ V \to V,$$

для которого $\forall g \in G$:

$$\mathcal{C} \cdot \mathcal{R}(g) = \mathcal{R}(g) \cdot \mathcal{C}$$

Гомоморфизмы из $\mathcal{R}$ в $\mathcal{R}'$ образуют подпространство $Hom\,(\mathcal{R}, \mathcal{R}')$ в пространстве всех линейных отображений из V в V'.

Эндоморфизмы представления $\mathcal{R}$ образуют подкольцо $End\,(\mathcal{R})$ в кольце всех линейных операторов на пространстве V.

Исследуем, как устроены гомоморфизмы и эндоморфизмы линейных представлений. Начнем со следующей простой леммы.

Лемма 1. Пусть

$$\mathcal{C} \in Hom\,(\mathcal{R}, \mathcal{R}').$$

Тогда $Ker\,\mathcal{C} \subseteq V$ и $Im\,\mathcal{C} \subseteq V'$ - инвариантные подпространства.

Доказательство.
Пусть $v \in Ker\,\mathcal{C}$, тогда $\mathcal{C} \cdot v = 0$. Но тогда и $\mathcal{R}(g)v \in Ker\,\mathcal{C}$. В самом деле, $\forall g \in G$:

$$\mathcal{C} \cdot \mathcal{R}(g)v = \mathcal{R}'(g) \cdot \mathcal{C} \cdot v = \mathcal{R}'(g) \cdot 0 = 0.$$

Если $v' \in Im\,\mathcal{C}$, то $v' = \mathcal{C} \cdot v$ для некоторого $v \in V$. Тогда $\forall g \in G$:

$$\mathcal{R}'(g)\cdot v' = \mathcal{R}'(g)\cdot\mathcal{C}\cdot v = \mathcal{C}\cdot\mathcal{R}(g)\cdot v$$

т.е. $\mathcal{R}'(g)\cdot v' \in Im\,\mathcal{C}$ – он является образом вектора $\mathcal{R}(g)\cdot v$. ■

Лемма Шура. (I. Schur, 1875-1941).

1) Пусть

$$\mathcal{R}:\ G \to GL(V),$$
$$\mathcal{R}':\ G \to GL(V')$$

- два неприводимых представления группы G, $\mathcal{C} \in Hom\,(\mathcal{R},\mathcal{R}')$. Тогда либо $\mathcal{C}$ – изоморфизм, либо $\mathcal{C} = 0$.

2) Пусть

$$\mathcal{R}:\ G \to GL(V)$$

- конечномерное неприводимое представление над $\mathbb{C}$. Тогда любой эндоморфизм этого представления является скалярным оператором (т.е. оператором умножения на некоторую константу $\lambda \in \mathbb{C}$):

$$\mathcal{C} \in End\,(\mathcal{R}) \Rightarrow \mathcal{C} = \lambda\cdot\mathcal{E}$$

Доказательство.
1) Рассмотрим $Ker\,\mathcal{C} \subseteq V$ и $Im\,\mathcal{C} \subseteq V'$ - инвариантные подпространства. Так как представления $\mathcal{R}$ и $\mathcal{R}'$ неприводимы, то каждое из этих подпространств либо нулевое, либо совпадает со всем пространством.

Но если $Ker\,\mathcal{C} = \{0\}$, то $Im\,\mathcal{C} \neq \{0\}$, следовательно, $Im\,\mathcal{C} = V'$. Отсюда следует, что $\mathcal{C}$ - изоморфизм:

$$\mathcal{C}:\ V \twoheadrightarrow V'$$

А если $Ker\,\mathcal{C} = V$, то $Im\,\mathcal{C} = \{0\}$, следовательно, $\mathcal{C} = 0$.

2) Рассмотрим характеристический многочлен оператора $\mathcal{C}$ (степени $n = dim\,\mathcal{R}$):

$$\chi_{\mathcal{C}}(t) = det\,(t\mathcal{E} - \mathcal{C}) = t^n - (tr\,\mathcal{C})t^{n-1} + \cdots + (-1)^n det\,\mathcal{C}$$

У этого многочлена есть корень в $\mathbb{C}$:

$$\exists\lambda \in \mathbb{C}:\ \chi_{\mathcal{C}}(\lambda) = 0$$

Значит, оператор $\lambda\mathcal{E} - \mathcal{C}$ вырожден. Но он также является эндоморфизмом: $\lambda\mathcal{E} - \mathcal{C} \in End\,(\mathcal{R})$, так как $\mathcal{C} \in End\,(\mathcal{R})$ и $\mathcal{E} \in End\,(\mathcal{R})$. Следовательно (по первой части леммы Шура),

$$\lambda\mathcal{E} - \mathcal{C} = 0 \Rightarrow \mathcal{C} = \lambda\mathcal{E}$$

■

Замечание: из доказательства леммы Шура видно, что в ее формулировке поле $\mathbb{C}$ можно заменить на любое алгебраически замкнутое поле.

Следующая лемма показывает, как из любого линейного отображения между линейными представлениями сделать гомоморфизм.

Лемма 2 (об усреднении линейного отображения по группе). Пусть

$$\mathcal{R}\colon\ G \to GL(V),$$
$$\mathcal{R}'\colon\ G \to GL(V')$$

- два линейных представления конечной группы G на полем K нулевой характеристики.
1) Пусть

$$\mathcal{C}\colon\ V \to V'$$

- линейное отображение. Тогда

$$\tilde{\mathcal{C}} = \frac{1}{|G|}\sum_{g\in G} \mathcal{R}'(g)\cdot \mathcal{C}\cdot \mathcal{R}(g)^{-1}$$

- гомоморфизм из $\mathcal{R}$ в $\mathcal{R}'$.

2) Пусть $\mathcal{R} = \mathcal{R}'$ - конечномерное неприводимое представление, $K = \mathbb{C}$ (или любое алгебраически замкнутое поле нулевой характеристики). Тогда

$$\tilde{\mathcal{C}} = \frac{tr\ \mathcal{C}}{dim\ \mathcal{R}}\cdot \mathcal{E}$$

Доказательство.
1) Для того, чтобы доказать, что $\tilde{\mathcal{C}}$ – гомоморфизм, нужно проверить, что $\tilde{\mathcal{C}}$ коммутирует с операторами представления. $\forall g_0 \in G$:

$$\mathcal{R}'(g_0)\cdot\tilde{\mathcal{C}} = \frac{1}{|G|}\sum_{g\in G}\mathcal{R}'(g_0)\cdot\mathcal{R}'(g)\cdot\mathcal{C}\cdot\mathcal{R}(g)^{-1} = \frac{1}{|G|}\sum_{g\in G}\mathcal{R}'(g_0 g)\cdot\mathcal{C}\cdot\mathcal{R}(g^{-1})$$

как и в доказательстве теоремы Машке, обозначив $h = gg_0$, получим:

$$\frac{1}{|G|}\sum_{h\in G}\mathcal{R}'(h)\cdot\mathcal{C}\cdot\mathcal{R}(h^{-1}g_0) = \frac{1}{|G|}\sum_{h\in G}\mathcal{R}'(h)\cdot\mathcal{C}\cdot\mathcal{R}(h^{-1})\cdot\mathcal{R}(g_0) = \tilde{\mathcal{C}}\cdot\mathcal{R}'(g_0)$$

2) По лемме Шура, оператор $\tilde{\mathcal{C}}$ – скалярный:

$$\tilde{\mathcal{C}} = \lambda\cdot\mathcal{E},$$

его матрица $\tilde{C}$:

$$\tilde{C} = \begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$$

След оператора $\tilde{\mathcal{C}}$, очевидно, равен λ, умноженному на размер матрицы, т.е. $\lambda \cdot dim\, \mathcal{R}$. С другой стороны, так как след – линейная функция, получаем:

$$tr\, \tilde{\mathcal{C}} = \frac{1}{|G|} \sum_{g \in G} tr\, (\mathcal{R}(g) \cdot \mathcal{C} \cdot \mathcal{R}(g)^{-1}) = \frac{1}{|G|} \sum_{g \in G} tr\, \mathcal{C} = tr\, \mathcal{C}$$

(здесь мы использовали тот факт, что след оператора равен следу сопряженного оператора). Тогда

$$\lambda = \frac{tr\, \mathcal{C}}{dim\, \mathcal{R}}$$

■

Далее будем рассматривать только конечномерные представления.

Пусть $\mathcal{R}$ - вполне приводимое представление группы G над полем K. Тогда $\mathcal{R}$ может быть разложено в прямую сумму неприводимых представлений:

$$\mathcal{R} = \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_s$$

Пусть $\mathcal{R}_0$ - неприводимое представление группы G над полем K.

Определение. *Кратность* $\mathcal{R}_0$ в разложении $\mathcal{R} = \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_s$ – количество слагаемых $\mathcal{R}_i \simeq \mathcal{R}_0$.

Предложение 1. Пусть $K = \mathbb{C}$ (или любое алгебраически замкнутое поле). Тогда кратность $\mathcal{R}_0$ в разложении $\mathcal{R}$ равна $dim\, Hom\, (\mathcal{R}, \mathcal{R}_0)$.

Доказательство.
Пусть

$$\mathcal{R}\colon\ G \to GL(V),$$
$$V = V_1 \oplus \ldots \oplus V_s,$$
$$\mathcal{R}|_{V_i} = \mathcal{R}_i,$$
$$\mathcal{R}_0\colon\ G \to GL(V_0).$$

Пусть

$$\mathcal{C}\colon\ V \to V_0$$

- гомоморфизм из $\mathcal{R}$ в $\mathcal{R}_0$.
Для произвольного вектора $v \in V$ существует единственное разложение

$$v = v_1 + \cdots + v_s,\ \ v_i \in V_i$$

Тогда

$$\mathcal{C} \cdot v = \mathcal{C} \cdot v_1 + \cdots + \mathcal{C} \cdot v_s = \mathcal{C}_1 \cdot v_1 + \cdots + \mathcal{C}_s \cdot v_s, \qquad \mathcal{C}_i = \mathcal{C}|_{V_i}$$

Таким образом, мы по гомоморфизму из $\mathcal{R}$ в $\mathcal{R}_0$ построили набор $\mathcal{C}_i$ гомоморфизмов из $\mathcal{R}_i$ в $\mathcal{R}_0$, которые однозначно определяют гомоморфизм $\mathcal{R}$. И обратно, любой набор гомоморфизмов $\mathcal{C}_i \in Hom\,(\mathcal{R}, \mathcal{R}_0)$, $i = 1, \dots, s$ задает гомоморфизм $\mathcal{C} \in Hom\,(\mathcal{R}, \mathcal{R}_0)$. Следовательно,

$$Hom\,(\mathcal{R}, \mathcal{R}_0) \simeq Hom\,(\mathcal{R}_1, \mathcal{R}_0) \oplus \dots \oplus Hom\,(\mathcal{R}_s, \mathcal{R}_0).$$

По лемме Шура:

$$Hom\,(\mathcal{R}_i, \mathcal{R}_0) = \begin{cases} \{0\} & \text{при } \mathcal{R}_i \simeq \mathcal{R}_0 \\ \simeq \mathbb{C} & \text{при } \mathcal{R}_i \simeq \mathcal{R}_0 \end{cases}$$

$$Hom\,(\mathcal{R}_i, \mathcal{R}_0) = \begin{cases} \{0\} & \text{при } \mathcal{R}_i \not\simeq \mathcal{R}_0 \\ \simeq \mathbb{C} & \text{при } \mathcal{R}_i \simeq \mathcal{R}_0 \end{cases}$$

Таким образом, в разложении $Hom\,(\mathcal{R}_i, \mathcal{R}_0)$ в прямую сумму присутствуют только нулевые и одномерные слагаемые, причем одномерные слагаемые соответствуют $\mathcal{R}_i \simeq \mathcal{R}_0$. Значит,

$$Hom\,(\mathcal{R}, \mathcal{R}_0) \simeq \mathbb{C}^m,$$

где m – количество $\mathcal{R}_i \simeq \mathcal{R}_0$. Таким образом,

$$dim\ Hom\,(\mathcal{R}, \mathcal{R}_0) = m \text{ – кратность } \mathcal{R}_0 \text{ в разложении } \mathcal{R}.$$

■

Упражнение. Доказать, что для произвольного поля K кратность $\mathcal{R}_0$ в разложении $\mathcal{R}$ равна

$$\frac{dim\ Hom\,(\mathcal{R}, \mathcal{R}_0)}{dim\ End\,(\mathcal{R}_0)}$$

Следствие. Разложение вполне приводимого представления над полем $\mathbb{C}$ (из упражнения следует, что и над произвольным полем K) в прямую сумму неприводимых представлений единственно с точностью до изоморфизма.

Неприводимые представления групп.

Перейдем к изучению неприводимых представлений групп. Начнем со случая абелевых групп. Имеет место следующая теорема.

Теорема. Все неприводимые представления абелевой группы G над полем $\mathbb{C}$ (и над любым алгебраически замкнутым полем) одномерны.

Доказательство.
Пусть

$$\mathcal{R}\colon\ G \to GL(V)$$

- неприводимое представление.

Так как G – абелева, то

$$\forall g,h \in G\colon\ gh = hg \Rightarrow \mathcal{R}(g)\cdot\mathcal{R}(h) = \mathcal{R}(h)\cdot\mathcal{R}(g)$$

Таким образом, все операторы представления абелевой группы коммутируют между собой, в частности, любой из них является эндоморфизмом: $\forall g \in G\colon\ \mathcal{R}(g) \in End\,(\mathcal{R})$. Но по лемме Шура такой эндоморфизм должен быть скалярным: $\forall g \in G\colon \mathcal{R}(g) = \lambda\cdot\mathcal{E}$ для некоторого $\lambda \in \mathbb{C}$.

Но для скалярных операторов любое подпространство в V является инвариантным, в частности, они сохраняют любое одномерное подпространство. Тогда из неприводимости $\mathcal{R}$ следует, что $dim\,V = 1$. ■

Замечания.
1) Верно и обратное – одномерное представление любой группы G над произвольным полем K неприводимо (так как в одномерном пространстве нет нетривиальных подпространств).

2) Если $dim\,\mathcal{R} = 1$, то любой линейный оператор в одномерном пространстве – это оператор умножения на ненулевой скаляр:

$$\forall g \in G\colon\ \mathcal{R}(g) = \lambda(g)\cdot\mathcal{E},\ \ \lambda(g) \in K^{\times}$$

Соответствующее матричное представление:

$$R\colon\ G \to GL_1(K) \simeq K^{\times}$$
$$R(g) = (\lambda(g))$$

Таким образом, одномерные представления группы G над полем K – то же, что и гомоморфизмы

$$R\colon\ G \to K^{\times}$$

Описание неприводимых комплексных представлений конечных абелевых групп.

Пусть G – конечная абелева группа. Тогда, как мы знаем, G разлагается в прямое произведение (примарных) циклических групп:

$$G = \langle g_1\rangle_{m_1} \times \cdots \times \langle g_s\rangle_{m_s}.$$

Пусть

$$R\colon\ G \to \mathbb{C}^{\times}$$

- неприводимое (а значит, одномерное) комплексное представление. Посмотрим, куда отображаются элементы, порождающие $\langle g_i\rangle$. Обозначим $R(g_i) = \varepsilon_i \in \mathbb{C}^{\times}$. Так как $g_i^{m_i} = e$, а R – гомоморфизм, то

$$R\left(g_i^{m_i}\right) = R(e) \Leftrightarrow \varepsilon_i^{m_i} = 1$$

То есть, ε_i являются корнями соответствующей степени из единицы. Тогда $\forall g \in G$:

$$g = g_1^{k_1} \cdots g_s^{k_s} \Rightarrow R(g) = \varepsilon_1^{k_1} \cdots \varepsilon_s^{k_s} \qquad (*)$$

Таким образом, представление $R = R_{\varepsilon_1,\ldots,\varepsilon_s}$ однозначно опередляется набором $(\varepsilon_1, \ldots, \varepsilon_s)$.

Обратно, для любого набора $(\varepsilon_1, \ldots, \varepsilon_s) \in \mathbb{U}_{m_1} \times \ldots \times \mathbb{U}_{m_s}$ формула $(*)$ определяет одномерное представление

$$R\colon\ G \to \mathbb{C}^\times$$

Корректность: если

$$g = g_1^{k_1} \cdots g_s^{k_s} = g = g_1^{l_1} \cdots g_s^{l_s},$$

то (так как $G = \langle g_1 \rangle_{m_1} \times \ldots \times \langle g_s \rangle_{m_s}$):

$$g_i^{k_i} = g_i^{l_i},\ \ \forall i = 1, \ldots, s,$$

а поскольку g_i – элемент порядка m_i, то показатели степеней равны по модулю m_i:

$$k_i = l_i + m_i q_i$$

откуда

$$\varepsilon_i^{k_i} = \varepsilon_i^{l_i}\left(\varepsilon_i^{m_i}\right)^{q_i} = \varepsilon_i^{l_i} \Rightarrow \varepsilon_1^{k_1} \cdots \varepsilon_s^{k_s} = \varepsilon_1^{l_1} \cdots \varepsilon_s^{l_s},$$

т.е. так заданное отображение $R\colon\ G \to \mathbb{C}^\times$ определено корректно.

Гомоморфность: пусть

$$g = g_1^{k_1} \cdots g_s^{k_s},$$
$$h = g_1^{n_1} \cdots g_s^{n_s},$$

тогда

$$gh = g_1^{k_1+n_1} \cdots g_s^{k_s+n_s}$$

и

$$R(g) \cdot R(h) = \varepsilon_1^{k_1} \cdots \varepsilon_s^{k_s} \cdot \varepsilon_1^{n_1} \cdots \varepsilon_s^{n_s} = \varepsilon_1^{k_1+n_1} \cdots \varepsilon_s^{k_s+n_s} = R(g \cdot h)$$

Таким образом, все неприводимые (= одномерные) комплексные представления конечной абелевой группы G имеют вид $R_{\varepsilon_1,\ldots,\varepsilon_s}$.

Следствие. Количество неприводимых комплексных представлений конечной абелевой группы G равно $m_1 \cdot m_1 \cdot \ldots \cdot m_s = |G|$.

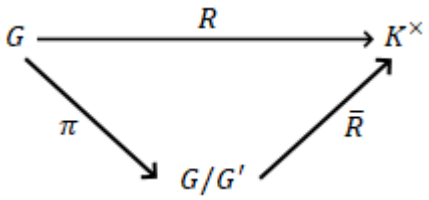
Одномерные представления групп.

Теперь от абелевых групп перейдем к произвольным. Начнем с одномерных представлений. Одномерные представления произвольных групп можно свести к абелевым группам.

Предложение 2. Существует взаимно-однозначное соответствие между одномерными линейными представлениями группы G и одномерными линейными представлениями группы G/G' (которая является абелевой):

$$R\colon\ G \to K^{\times} \ \leftrightarrow\ \bar{R}\colon\ G/G' \to K^{\times},$$
$$R = \bar{R} \circ \pi, \text{ где } \pi\colon G \to G/G' \text{ - каноническая проекция.}$$

Коммутативная диаграмма:



Доказательство.
Пусть

$$R\colon\ G \to K^{\times}$$

- одномерное представление. Тогда

$$G/Ker\ R \simeq Im\ R \subseteq K^{\times},$$

т.е. $G/Ker\ R$ – абелева. Тогда по основному свойству коммутанта, отсюда следует, что

$$Ker\ R \supseteq G'.$$

Определим $\bar{R}$ формулой:

$$\bar{R}\colon\ G/G' \to K^{\times}$$
$$\bar{R}(g \cdot G') = R(g)$$

Корректность: (докажем, что данная формула корректна – результат $\bar{R}(g \cdot G')$ не зависит от выбора представителя смежного класса). Пусть элементы g и g' лежат в одном и том же смежном классе:

$$g \cdot G' = g' \cdot G' \Rightarrow g = g' \cdot h, \text{ где } h \in G'.$$

Тогда

$$R(g) = R(g') \cdot R(h), \text{ где } R(h) \in Ker\ R.$$

Так как $R(h) \in Ker\ R$, то $R(h) = 1$, поэтому $R(g) = R(g')$ и отображение $\bar{R}$ определено корректно.

Гомоморфность: $\bar{R}$ – гомоморфизм, так как R – гомоморфизм.

По построению $R = \bar{R} \circ \pi$, где $\pi: G \to G/G'$ - каноническая проекция.

Обратно, для любого одномерного представления $\bar{R}: \ G/G' \to K^\times$ можно построить одномерное представление

$$R = \bar{R} \circ \pi: \ G \to K^\times$$

Следовательно, изучение одномерных представлений сводится к случаю абелевых групп. ■

Следствие. Количество одномерных комплексных представлений конечной группы G равно $|G/G'|$.

Пример. Пусть $G = S_n$. Опишем ее одномерные линейные представления. Коммутант S_n – это группа четных подстановок: $G' = A_n$, тогда

$$G/G' = S_n/A_n = \{\text{четные подстановки, нечетные подстановки}\} \simeq \mathbb{Z}_2$$

Класс четных подстановок будет нейтральным элементом в G/G', класс нечетных подстановок будет порождающим элементом (порядка 2) в G/G'.

Количество одномерных представлений группы S_n равно $|S_n/A_n| = 2$. Чтобы их описать, нужно задать отображение порождающего элемента S_n/A_n, то есть, задать, куда отображаются нечетные подстановки. Так как S_n/A_n – циклическая группа порядка 2, то нечетные подстановки будут отображаться в корень степени 2 из единицы, т.е. в ± 1. Четные подстановки (как нейтральный элемент) будут отображаться в 1. Получаем следующие одномерные представления $\bar{R}_1$ и $\bar{R}_2$:

$$\bar{R}_1(\text{нечетные подстановки}) = 1, \ \ \bar{R}_1(\text{четные подстановки}) = 1 \ \Rightarrow R_1(\sigma) = 1$$

$$\bar{R}_2(\text{нечетные подстановки}) = -1, \ \ \bar{R}_2(\text{четные подстановки}) = 1 \ \Rightarrow R_2(\sigma) = sgn(\sigma)$$

Таким образом, мы описали все одномерные представления группы S_n – это тривиальное представление и знаковое представление.

Лекция 16. Линейные представления конечных групп.

С этого момента мы будем рассматривать только конечномерные комплексные линейные представления конечных групп.

Пусть G – конечная группа. По теореме Машке любое представление G вполне приводимо и раскладывается в прямую сумму неприводимых представлений единственным образом (с точностью до изоморфизма). Таким образом, изучение представлений группы G сводится к изучению неприводимых представлений.

Напоминание. Левое регулярное представление $\mathcal{L}\colon\ G \to GL(V)$ в пространстве функций $V = \mathcal{F}(G, \mathbb{C})$ задается с помощью действия $G \curvearrowright G$ умножениями слева. Согласно общей формуле, определяющей действие группы G на множестве функций $\mathcal{F}(X, K)$:

$$[\mathcal{L}(g)f](x) = f(g^{-1} \cdot x), \qquad \forall f \in \mathcal{F}(G, \mathbb{C}),\ \forall g, x \in G$$

Стандартный базис пространства функций $\mathcal{F}(G, \mathbb{C})$: $\varepsilon_y(x) = \begin{cases} 1 \text{ при } x = y \\ 0 \text{ при } x \neq y \end{cases}$ $(y \in G)$.

Таким образом, $dim\ \mathcal{L} = |G|$. Как было показано ранее,

$$\mathcal{L}(g)\varepsilon_y = \varepsilon_{g \cdot y}$$

- другими словами, представление $\mathcal{L}$ переставляет базисные функции по вышеуказанному правилу.

Регулярные представления играют важную роль в теории представлений конечных групп.

Теорема 1. Для любого неприводимого представления $\mathcal{R}\colon\ G \to GL(V)$ его кратность в регулярном представлении $\mathcal{L}$ равна $dim\ \mathcal{R}$.

Доказательство.
Кратность $\mathcal{R}$ в $\mathcal{L}$ равна $dim\ Hom\ (\mathcal{L}, \mathcal{R})$ – см. предыдущую лекцию. Пусть

$$\mathcal{C}\colon\ \mathcal{F}(G, \mathbb{C}) \to V$$

- гомоморфизм из $\mathcal{L}$ в $\mathcal{R}$. Подействуем им на базисные функции. Пусть $\mathcal{C}(\varepsilon_e) = v$. Тогда

$$\forall h \in G\colon\ \mathcal{C}(\varepsilon_h) = \mathcal{C} \cdot \mathcal{L}(h)\varepsilon_e = \mathcal{R}(h) \cdot \mathcal{C}(\varepsilon_e) = \mathcal{R}(h)v$$

(первое равенство следует из того, что $\mathcal{L}(h)\varepsilon_e = \varepsilon_{h \cdot e} = \varepsilon_h$, второе равенство – из того, что $\mathcal{C}$ - гомоморфизм, поэтому перестановочен с $\mathcal{L}$). Таким образом, зная образ базисной функции, отвечающей единичному элементу, мы можем найти образы остальных

базисных функций. Другими словами, гомоморфизм $\mathcal{C} = \mathcal{C}_v$ однозначно определяется вектором v.

Обратно, для любого $v \in V$ можно определить линейное отображение:

$$\mathcal{C}_v\colon \mathcal{F}(G, \mathbb{C}) \to V$$
$$\varepsilon_h \mapsto \mathcal{R}(h) \cdot v$$

Это гомоморфизм из $\mathcal{L}$ в $\mathcal{R}$, так как $\forall g, h \in G$ отображение $\mathcal{C}_v$ перестановочно с операторами представления:

$$\mathcal{C}_v \cdot \mathcal{L}(g)\varepsilon_h = \mathcal{C}_v\left(\varepsilon_{gh}\right) = \mathcal{R}(gh)v = \mathcal{R}(g)\mathcal{R}(h)v = \mathcal{R}(g) \cdot \mathcal{C}_v(\varepsilon_h) \Rightarrow$$
$$\mathcal{C}_v \cdot \mathcal{L}(g) = \mathcal{R}(g) \cdot \mathcal{C}_v.$$

Возникает отображение

$$V \to Hom\,(\mathcal{L}, \mathcal{R})$$
$$v \mapsto \mathcal{C}_v,$$

которое является изоморфизмом векторных пространств: биективность V вытекает из вышесказанного, а линейность V – из конструкции отображения $\mathcal{C}_v$. Следовательно,

$$dim\, Hom\,(\mathcal{L}, \mathcal{R}) = dim\, V = dim\, \mathcal{R}$$

■

Следствие 1. У конечной группы имеется лишь конечное число неприводимых представлений (с точностью до изоморфизма), и все они являются подпредставлениями регулярного представления.

Следствие 2. Пусть $\mathcal{R}_1, \dots, \mathcal{R}_s$ – полный список неприводимых представлений группы G с точностью до изоморфизма. Тогда

$$(dim\, \mathcal{R}_1)^2 + \cdots + (dim\, \mathcal{R}_s)^2 = |G|$$

Доказательство.
Разложим регулярное представление в прямую сумму неприводимых слагаемых:

$$\mathcal{L} \simeq \underbrace{\mathcal{R}_1 \oplus \cdots \oplus \mathcal{R}_1}_{m_1} \oplus \underbrace{\mathcal{R}_2 \oplus \cdots \oplus \mathcal{R}_2}_{m_2} \oplus \cdots \oplus \underbrace{\mathcal{R}_s \oplus \cdots \oplus \mathcal{R}_s}_{m_s}$$

Тогда

$$dim\, \mathcal{L} = |G| = \sum_{i=1}^{s} (dim\, \mathcal{R}_i) \cdot m_i = \sum_{i=1}^{s} (dim\, \mathcal{R}_i)^2$$

■

Регулярное представление – элемент пространства функций на группе. Среди всех функций на группе можно выделить функции специального вида – матричные элементы линейных представлений.

Определение. Пусть $\mathcal{R}\colon\ G \to GL(V)$ – линейное представление, $(e_1, \dots, e_n)$ – базис V, а $R\colon\ G \to GL_n(\mathbb{C})$ - соответствующее матричное представление. Тогда всякому $g \in G$ соответствует

$$R(g) = \begin{pmatrix} r_{11}(g) & \cdots & r_{1n}(g) \\ \vdots & \ddots & \vdots \\ r_{n1}(g) & \cdots & r_{nn}(g) \end{pmatrix}$$

- матрица оператора $\mathcal{R}(g)$ в базисе $(e_1, \dots, e_n)$. Функции $r_{ij}(g)\colon G \to \mathbb{C}$ называются *матричными элементами* представления $\mathcal{R}$ в базисе $(e_1, \dots, e_n)$.

Определение. Линейная оболочка функций r_{ij} называется *пространством матричных элементов*.

Предложение 1. Пространство матричных элементов

$$Mat\ (\mathcal{R}) = < r_{ij} \mid i,j = 1, \dots, dim\ \mathcal{R} = n > \subseteq \mathcal{F}(G, \mathbb{C})$$

не зависит от выбора базиса.

Доказательство.
Посмотрим, что происходит при замене базиса:

$$(e_1, \dots, e_n) \xrightarrow{C} (e_1', \dots, e_n')$$

В новом базисе:

$$R'(g) = C^{-1} \cdot R(g) \cdot C$$

$$r_{ij}'(g) = \sum_{k,l=1}^{n} \tilde{c}_{ik} \cdot r_{kl}(g) \cdot c_{lj}(g),$$

где $\tilde{c}_{ik}$ – элементы C^{-1}. Тогда

$$r_{ij}' = \sum_{k,l=1}^{n} \tilde{c}_{ik} \cdot c_{lj} \cdot r_{kl}$$

т.е. матричные элементы в новом базисе являются линейными комбинациями матричных элементов в старом базисе. Отсюда следует, что линейная облочка r_{ij}' содержится в линейной оболочке r_{ij}:

$$< r_{ij}' \mid i,j = 1, \dots, n > \subseteq < r_{kl} \mid k,l = 1, \dots, n >$$

Обратное включение доказывается аналогично (перейдем от нового базиса к старому, матрица перехода C^{-1}, тогда $R(g) = C \cdot R'(g) \cdot C^{-1}$, и так далее).

Таким образом, линейные облочки r_{ij} и r'_{ij} совпадают, следовательно, пространство матричных элементов не зависит от выбора базиса. ■

Пример. Матричные элементы для регулярного представления в стандартном базисе:

$$\varepsilon_y(x) = \begin{cases} 1 \text{ при } x = y \\ 0 \text{ при } x \neq y \end{cases} \quad (y \in G)$$

- здесь матричные элементы нумеруются не числами, а элементами группы. Соответствующий матричный элемент будем обозначать $l_{a,b}$ $(a, b \in G)$. Тогда

$$l_{a,b} = \text{координата } \mathcal{L}(g) \cdot \varepsilon_b \text{ при } \varepsilon_a$$

Но $\mathcal{L}(g) \cdot \varepsilon_b = \varepsilon_{gb}$, поэтому

$$l_{a,b} = \begin{cases} 1 \text{ при } gb = a \Leftrightarrow g = ab^{-1} \\ 0 \text{ иначе} \end{cases}$$

- мы получили функцию, равную 1 на одном элементе группы $g = ab^{-1}$, и равную 0 на всех остальных, т.е. это функция из стандартного базиса:

$$l_{a,b} = \varepsilon_{ab^{-1}}$$

- таким образом, в данном случае пространство представления и пространство матричных элементов - это одно и то же пространство:

$$Mat\ (\mathcal{L}) = \mathcal{F}(G, \mathbb{C})$$

Предложение 2. Пусть

$$\mathcal{R}_i\colon\ G \to GL(V_i), \qquad i = 1, \dots, s$$

- полный список неприводимых представлений группы G. Выберем базисы $(e_{i,1}, \dots, e_{i,n_i})$ в пространствах V_i, $n_i = dim\, \mathcal{R}_i$. Тогда соответствующие матричные элементы $r_{i,kl}$ $(i = 1, \dots, s,\ \ k, l = 1, \dots, n_i)$ образуют базис пространства $\mathcal{F}(G, \mathbb{C})$.

Доказательство.
Разложим регулярное представление в прямую сумму неприводимых слагаемых:

$$\mathcal{L} \simeq \underbrace{\mathcal{R}_1 \oplus \cdots \oplus \mathcal{R}_1}_{m_1} \oplus \underbrace{\mathcal{R}_2 \oplus \cdots \oplus \mathcal{R}_2}_{m_2} \oplus \cdots \oplus \underbrace{\mathcal{R}_s \oplus \cdots \oplus \mathcal{R}_s}_{m_s}$$

В базисе, согласованном с этим разложением, матрицы операторов представления $\mathcal{L}$ будут иметь блочно-диагональный вид:

$$L(g) = \begin{pmatrix} \boxed{R_1(g)} & & & & & \\ & \ddots & & & & \\ & & \boxed{R_1(g)} & & & \\ & & & \ddots & & \\ & & & & \boxed{R_i(g)} & \\ & & & & & \ddots \\ & & & & & & \boxed{R_s(g)} \end{pmatrix}$$

А поскольку пространство матричных элементов от выбора базиса не зависит, то

$$Mat\ (\mathcal{L}) = \mathcal{F}(G, \mathbb{C}) = < r_{i,kl} \mid i = 1, \dots, s,\ \ k, l = 1, \dots, n_i >$$

Но количество функций $r_{i,kl}$ равно

$$n_1^2 + \cdots + n_s^2 = dim\ \mathcal{L} = dim\ \mathcal{F}(G, \mathbb{C}).$$

То есть, пространство $\mathcal{F}(G, \mathbb{C})$ порождено набором функций $r_{i,kl}$, количество которых равно размерности пространства $\mathcal{F}(G, \mathbb{C})$. Отсюда следует, что функции $r_{i,kl}$ линейно независимы и образуют базис пространства $\mathcal{F}(G, \mathbb{C})$. ■

Следствие.

$$\mathcal{F}(G, \mathbb{C}) = Mat\ (\mathcal{R}_1) \oplus \cdots \oplus Mat\ (\mathcal{R}_s)$$

- поскольку подпространства $\mathcal{R}_1, \dots, \mathcal{R}_s$ порождаются попарно непересекающимися группами базисных функций $r_{i,kl}$.

Таким образом, в некотором смысле мы свели изучение всех функций на группе к изучению матричных элементов различных неприводимых представлений.

В этой лекции мы рассматривали левое регулярное представление $\mathcal{L}\colon\ G \to GL(V)$ в пространстве функций $V = \mathcal{F}(G, \mathbb{C})$, с таким же успехом можно было рассматривать и правое регулярное представление. Эти два представления возникают из действия группы самой на себе умножениями слева или справа. Рассмотрим еще одно действие группы на себе – действие сопряжениями. Представление $\mathcal{A}$ в пространстве $\mathcal{F}(G, \mathbb{C})$:

$$[\mathcal{A}(g)f](h) = f(g^{-1} \cdot h \cdot g), \qquad \forall f \in \mathcal{F}(G, \mathbb{C}),\ \ \forall g, h \in G$$

Предложение 3. Для любого линейного представления $\mathcal{R}\colon\ G \to GL(V)$ пространство $Mat\ (\mathcal{R}) \subseteq \mathcal{F}(G, \mathbb{C})$ инвариантно относительно представления $\mathcal{A}$.

Доказательство.
Выберем базис $(e_1, \dots, e_n)$ в пространстве V. В этом базисе:

$$R(g^{-1} \cdot h \cdot g) = R(g^{-1}) \cdot R(h) \cdot R(g),$$

откуда следует, что

$$r_{ij}(g^{-1} \cdot h \cdot g) = \sum_{k,l=1}^{n} r_{ik}(g^{-1}) \cdot r_{kl}(h) \cdot r_{lj}(g).$$

Если зафиксировать g, и рассматривать правую и левую части этого равенства как функции от h, получим $\forall g \in G,\ \ \forall i,j = 1, \dots, n$:

$$\mathcal{A}(g) r_{ij} = \sum_{k,l=1}^{n} r_{ik}(g^{-1}) \cdot r_{lj}(g) \cdot r_{kl} \ \in Mat(R)$$

- отсюда следует, что $\mathcal{A}(g)$ сохраняет $Mat(R)$ для любого $g \in G$. ■

Центральные функции.

Определение. Функция $f \in \mathcal{F}(G, \mathbb{C})$ называется *центральной*, если все операторы $\mathcal{A}(g)$ ее сохраняют:

$$\mathcal{A}(g) f = f,\ \ \forall g \in G,$$

то есть,

$$f(g^{-1} h g) = f(h),\ \ \forall g, h \in G$$

Таким образом, центральные функции – это функции, постоянные на классах сопряженности (принимающие одинаковые значения на сопряженных элементах группы).

Пример. Пусть $\mathcal{R}\colon\ \ G \to GL(V)$ - линейное представление. Его характер:

$$\chi_{\mathcal{R}}(g) = tr\, \mathcal{R}(g) = tr\, R(g) = r_{11}(g) + \dots + r_{nn}(g)$$

- сумма диагональных матричных элементов представления $\mathcal{R}$ в некотором базисе. Характер – центральная функция. В самом деле:

$$\chi_{\mathcal{R}}(g^{-1} h g) = tr\, \mathcal{R}(g^{-1} h g) = tr\big(\mathcal{R}(g^{-1}) \cdot \mathcal{R}(h) \cdot \mathcal{R}(g)\big) =$$

$$= tr\big(R(g^{-1}) \cdot R(h) \cdot R(g)\big) = tr\, R(h) = \chi_{\mathcal{R}}(h)$$

Центральные функции образуют подпространство $\mathcal{Z}(G, \mathbb{C}) \in \mathcal{F}(G, \mathbb{C})$. Его базис образуют функции следующего вида:

$$\varepsilon_C(x) = \begin{cases} 1 \text{ на } C \\ 0 \text{ на } G \backslash C \end{cases} = \sum_{g \in C} \varepsilon_g$$

где C – класс сопряженности.
Соответственно, размерность пространства центральных функций равна количеству базисных функций, то есть, количеству классов сопряженности:

$$dim\ \mathcal{Z}(G, \mathbb{C}) = \text{количество классов сопряженности в } G$$

Предложение 4. Пусть $\mathcal{R}$ - неприводимое представление. Тогда $\chi_{\mathcal{R}}$ - единственная (с точностью до пропорциональности) центральная функция в $Mat\ (\mathcal{R})$.

Доказательство.
Матричные элементы r_{ij} линейно независимы (следует из неприводимости представления $\mathcal{R}$), значит, для любой функции $f \in Mat\ (\mathcal{R})$ существует единственное разложение f в линейную комбинацию матричных элементов:

$$f = \sum_{i,j=1}^{n} c_{ji} \cdot r_{lj}$$

Тогда $\forall h \in G$:

$$f(h) = \sum_{i,j=1}^{n} c_{ji} \cdot r_{lj}(h) = \sum_{j=1}^{n} (\sum_{i=1}^{n} c_{ji} \cdot r_{lj}(h))$$

Сумма, стоящая в скобках – это элемент произведения матриц $C \cdot R(h)$, стоящий на месте (j, j), т.е. на диагонали. Суммируя по j, получаем след $C \cdot R(h)$:

$$f(h) = tr\ (C \cdot R(h))$$

Переходя от матриц к операторам:

$$f(h) = tr\ (\mathcal{C} \cdot \mathcal{R}(h)),$$

где $\mathcal{C}$ – линейный оператор на V с матрицей C в том базисе, в котором мы рассматриваем матричные элементы.

Запишем условие того, что функция центральна, с учетом полученной формулы:

$$f(g^{-1}hg) = tr\ (\mathcal{C} \cdot \mathcal{R}(g^{-1}hg)) = tr\ (\mathcal{C} \cdot \mathcal{R}(g)^{-1} \cdot \mathcal{R}(h) \cdot \mathcal{R}(g)) =$$

$$= tr\ (\mathcal{R}(g) \cdot \mathcal{C} \cdot \mathcal{R}(g)^{-1} \cdot \mathcal{R}(h)).$$

Так как

$$f(h) = tr\ (\mathcal{C} \cdot \mathcal{R}(h)),$$

то функция f является центральной тогда и только тогда, когда эти выражения равны:

$$tr\,(\mathcal{R}(g)\cdot\mathcal{C}\cdot\mathcal{R}(g)^{-1}\cdot\mathcal{R}(h)) = tr\,(\mathcal{C}\cdot\mathcal{R}(h)) \Leftrightarrow$$

$$\Leftrightarrow \mathcal{R}(g)\cdot\mathcal{C}\cdot\mathcal{R}(g)^{-1} = \mathcal{C} \Leftrightarrow \mathcal{R}(g)\cdot\mathcal{C} = \mathcal{C}\cdot\mathcal{R}(g), \qquad \forall g\in G$$

- получили, что $\mathcal{C}$ коммутриует с $\mathcal{R}(g),\ \forall g\in G$, то есть, $\mathcal{C}$ – эндоморфизм: $\mathcal{C}\in End\,(\mathcal{R})$.

Итак, функция $f\in Mat\,(\mathcal{R})$ является центральной тогда и только тогда, когда задающий эту функцию линейный оператор $\mathcal{C}$ является эндоморфизмом. Тогда по лемме Шура, $\mathcal{C}$ – это скалярный оператор:

$$\mathcal{C} = \lambda\cdot\mathcal{E},\ \ \lambda\in\mathbb{C}.$$

Получаем

$$f(h) = tr\,(\lambda\cdot\mathcal{E}\cdot\mathcal{R}(h)) = \lambda\cdot tr\,\mathcal{R}(h) = \lambda\cdot\chi_{\mathcal{R}}(h).$$

Таким образом, любая центральная функция в $Mat\,(\mathcal{R})$, где $\mathcal{R}$ неприводимо, пропорциональна характеру представления $\mathcal{R}$. ■

Из доказанных утверждений вытекает следующая теорема.

Теорема 2. Характеры всех неприводимых представлений группы G образуют базис пространства $\mathcal{Z}(G,\mathbb{C})$.

Доказательство.
Как было доказано ранее (см. следствие из предложения 2):

$$\mathcal{F}(G,\mathbb{C}) = Mat\,(\mathcal{R}_1)\oplus\cdots\oplus Mat\,(\mathcal{R}_s),$$

где $\mathcal{R}_1,\dots,\mathcal{R}_s$ – все неприводимые представления G. Значит, любая функция $f\in\mathcal{F}(G,\mathbb{C})$ единственным способом разлагается в сумму функций из пространств $Mat\,(\mathcal{R}_1),\dots,Mat\,(\mathcal{R}_s)$:

$$f = f_1+\cdots+f_s,\ \ f_i\in Mat\,(\mathcal{R}_i).$$

Тогда

$$\mathcal{A}(g)f = \mathcal{A}(g)f_1+\cdots+\mathcal{A}(g)f_s$$

Как было доказано ранее (см. предложение 3), пространство матричных элементов инвариантно относительно представления $\mathcal{A}$, поэтому $\mathcal{A}(g)f_i\in Mat\,(\mathcal{R}_i),\ \forall i=1,\dots,s$. Поэтому

$$\mathcal{A}(g)f = f \Leftrightarrow \mathcal{A}(g)f_i = f_i,\ \ \forall i=1,\dots,s.$$

Отсюда следует, что

$$f\in\mathcal{Z}(G,\mathbb{C}) \Leftrightarrow f_i\in\mathcal{Z}(G,\mathbb{C}),\ \ \forall i=1,\dots,s.$$

По предложению 4:

$$f_i\in\mathcal{Z}(G,\mathbb{C}) \Leftrightarrow f_i = \lambda_i\cdot\chi_{\mathcal{R}_i},\ \ \forall i=1,\dots,s.$$

То есть, функция f – это линейная комбинация характеров $\chi_{\mathcal{R}_i}$:

$$f = \lambda_1 \cdot \chi_{\mathcal{R}_1} + \cdots + \lambda_n \cdot \chi_{\mathcal{R}_n}$$

Отсюда следует, что характеры неприводимых представлений $\chi_{\mathcal{R}_i}$ порождают пространство центральных функций $\mathcal{Z}(G, \mathbb{C})$, при этом $\chi_{\mathcal{R}_i} \neq 0$ (это следует, например, из того, что $\chi_{\mathcal{R}_i}(e) = tr\ \mathcal{E} = dim\ \mathcal{R}_i \neq 0$).
Так как $\chi_{\mathcal{R}_i}$ линейно независимы (потому что они лежат в разных прямых слагаемых $Mat\ (\mathcal{R}_i)$), то они образуют базис пространства $\mathcal{Z}(G, \mathbb{C})$. ■

Следствие. Количество неприводимых представлений группы G (с точностью до изоморфизма) равно количеству классов сопряженности в G.

Доказательство.
Оба этих числа равны $dim\ \mathcal{Z}(G, \mathbb{C})$. ■

Подведем итоги: конечномерных неприводимых представлений конечной группы конечное число, сумма квадратов их размерностей равна порядку группы, а их количество равно количеству классов сопряженности группы.

Лекция 17. Неприводимые линейные представления конечных групп.

На прошлой лекции мы познакомились с понятием характера линейного представления. Пусть $\mathcal{R}$: $G \to GL(V)$ - линейное представление. Его характер:

$$\chi_{\mathcal{R}}(g) = tr\ \mathcal{R}(g) = tr\ R(g) = r_{11}(g) + \cdots + r_{nn}(g)$$

- сумма диагональных матричных элементов представления $\mathcal{R}$ в некотором базисе.

Характеры – это удобный вычислительный инструмент для теории представлений – свойства представлений отражаются в алгебраических свойствах их характеров, и наоборот.

Предложение 1. Пусть

$$\mathcal{R} = \mathcal{R}_1 \oplus \cdots \oplus \mathcal{R}_m,$$

тогда

$$\chi_{\mathcal{R}} = \chi_{\mathcal{R}_1} + \cdots + \chi_{\mathcal{R}_m}.$$

Доказательство.
В базисе, согласованном с разложением $\mathcal{R}$ в прямую сумму его матрица имеет вид:

$$R(g) = \begin{pmatrix} R_1(g) & & 0 \\ & \ddots & \\ 0 & & R_m(g) \end{pmatrix}$$

Тогда

$$\chi_{\mathcal{R}}(g) = tr\ R(g) = tr\ \mathcal{R}_1(g) + \cdots + tr\ \mathcal{R}_m(g) = \chi_{\mathcal{R}_1} + \cdots + \chi_{\mathcal{R}_m}$$

■

Структура эрмитова пространства на $\mathcal{F}(G, \mathbb{C})$.

Дальнейшие свойства характеров, которые мы будем обсуждать, имеют метрическую природу, т.е. связаны со структурой эрмитова пространства на $\mathcal{F}(G, \mathbb{C})$.

Скалярное произведение:

$$(f_1 \mid f_2) = \frac{1}{|G|} \sum_{g \in G} f_1(g) \cdot \overline{f_2(g)}$$

- несложно проверить, что это действительно полуторалинейная эрмитова положительно определенная функция.

Замечание. Регулярное представление $\mathcal{L}$ в пространстве $\mathcal{F}(G, \mathbb{C})$ унитарно по отношению к этой эрмитовой структуре (т.е. все операторы $\mathcal{L}(g)$ будут сохранять скалярное умножение):

$$(\mathcal{L}(g_0)\, f_1 \mid \mathcal{L}(g_0) f_2) = \frac{1}{|G|} \sum_{g \in G} f_1(g_0^{-1} g) \cdot \overline{f_2(g_0^{-1} g)}$$

Пусть $h = g_0^{-1} g$. Если g пробегает все элементы G, то и h пробегает все элементы G, так как $g = g_0 h$. Поэтому можно суммировать не по g, а по h:

$$(\mathcal{L}(g_0)\, f_1 \mid \mathcal{L}(g_0) f_2) = \frac{1}{|G|} \sum_{h \in G} f_1(h) \cdot \overline{f_2(h)} = (f_1 \mid f_2)$$

т.е. $\mathcal{L}$ унитарно.

Теорема (соотношения ортогональности).
Пусть

$$\mathcal{R}_i\colon\ G \to GL(V_i)$$
$$(i = 1, \dots, s)$$

- полный список всех неприводимых представлений группы G с точностью до изоморфизма. Введем на каждом V_i эрмитову структуру так, чтобы $\mathcal{R}_i$ стало унитарным, и выберем в V_i ортонормированный базис $(e_{i,1}, \dots, e_{i,n_i})$, где $n_i = dim\, \mathcal{R}_i$. Тогда:

1) Матричные элементы $r_{i,kl}$ в выбранных базисах $(i = 1, \dots, s,\ k, l = 1, \dots, n_i)$ образуют ортогональный базис пространства $\mathcal{F}(G, \mathbb{C})$.
2) Характеры $\chi_{\mathcal{R}_1}, \dots, \chi_{\mathcal{R}_s}$ образуют ортонормированный базис пространства $\mathcal{Z}(G, \mathbb{C})$.

Доказательство.
1) То, что $r_{i,kl}$ образуют базис $\mathcal{F}(G, \mathbb{C})$, уже было доказано (см. предложение 2 прошлой лекции). Докажем его ортогональность. Пусть

$$\mathcal{R}\colon\ G \to GL(V)$$
$$\mathcal{R}'\colon\ G \to GL(V')$$

- два неприводимых унитарных представления, $(e_1, \dots, e_n)$ и $(e'_1, \dots, e'_m)$ – ортонормированные базисы в V и V'.
Рассмотрим линейный оператор

$$\mathcal{E}_{ij}\colon\ V' \to V$$

с матрицей

$$E_{ij} = \begin{pmatrix} 0 & \vdots & 0 \\ \cdots & 1 & \cdots \\ 0 & \vdots & 0 \end{pmatrix} \begin{matrix} \\ i \\ \\ \end{matrix}$$
$$\qquad\qquad\quad j$$

Его усреднение по группе G:

$$\tilde{\mathcal{E}}_{ij} = \frac{1}{|G|}\sum_{g\in G} \mathcal{R}(g)\cdot \mathcal{E}_{ij}\cdot \mathcal{R}'(g)^{-1}$$

Так как $\mathcal{R}$ и $\mathcal{R}'$ - унитарные представления, значит, их матрицы в ортонормированных базисах будут унитарными матрицами, т.е. $\mathcal{R}'(g)^{-1} = \mathcal{R}'(g)^*$ - обратная матрица совпадает с эрмитово сопряженной. Поэтому

$$\tilde{\mathcal{E}}_{ij} = \frac{1}{|G|}\sum_{g\in G} \mathcal{R}(g)\cdot \mathcal{E}_{ij}\cdot \mathcal{R}'(g)^*$$

Матрица $\tilde{E}_{ij}$ оператора $\tilde{\mathcal{E}}_{ij}$ будет выглядеть следующим образом: на месте (k,l) стоит

$$\frac{1}{|G|}\sum_{g\in G}\sum_{p=1}^{n}\sum_{q=1}^{m} r_{kp}(g)\cdot \delta_{p_i}\cdot \delta_{q_j}\cdot \overline{r'_{lq}(g)}$$

- здесь мы записали (p,q)-ый элемент матрицы E_{ij} как $\delta_{p_i}\cdot\delta_{q_j}$, а также воспользовались тем, что (q,l)-ом месте матрицы $R'(g)^*$ стоит элемент $\overline{r'_{lq}(g)}$.

Так как в сумме присутствует множители δ_{p_i} и δ_{q_j}, то от суммирования по p и по q останутся лишь слагаемые, соответствующие $p=i$ и $q=j$. Таким образом, в матрице $\tilde{E}_{ij}$ на месте (k,l) стоит

$$\frac{1}{|G|}\sum_{g\in G} r_{ki}(g)\cdot \overline{r'_{lj}(g)} = \left(r_{ki}\mid r'_{lj}\right)$$

То есть, произведение любых двух матричных элементов представлений $\mathcal{R}$ и $\mathcal{R}'$ можно интерпретировать как матричный элемент линейного оператора $\tilde{\mathcal{E}}_{ij}$.

По лемме об усреднении, $\tilde{\mathcal{E}}_{ij}$ – гомоморфизм представлений. Но представления $\mathcal{R}$ и $\mathcal{R}'$ неприводимы, поэтому если $\mathcal{R}$ и $\mathcal{R}'$ не изоморфны, то по лемме Шура $\tilde{\mathcal{E}}_{ij}=0$, а если $\mathcal{R}$ и $\mathcal{R}'$ изоморфны, то по лемме Шура, и по лемме об усреднении $\tilde{\mathcal{E}}_{ij}$ – скалярный оператор:

$$\tilde{\mathcal{E}}_{ij} = \frac{tr\ \mathcal{E}_{ij}}{dim\ \mathcal{R}}\cdot \mathcal{E} = \begin{cases} 0 \text{ при } i\neq j \\ \dfrac{1}{n}\cdot\mathcal{E} \text{ при } i=j \end{cases}$$

Следовательно, если $\mathcal{R}$ и $\mathcal{R}'$ не изоморфны, то $\left(r_{ki}\mid r'_{lj}\right)=0 \quad \forall i,j,k,l$ – матричные элементы представлений $\mathcal{R}$ и $\mathcal{R}'$ ортогональны, а если $\mathcal{R}$ и $\mathcal{R}'$ изоморфны (можно считать, что $\mathcal{R}=\mathcal{R}'$), то $\left(r_{ki}\mid r_{lj}\right)$ – элемент матрицы $\tilde{E}_{ij}$,стоящий на месте (k,l), удовлетворяет соотношению:

$$(r_{ki} \mid r_{lj}) = \begin{cases} \frac{1}{n} \text{ при } i = j, k = l \\ 0 \text{ иначе} \end{cases}$$

т.е. разные матричные элементы одного и того же неприводимого представления также ортогональны.

2) То, что характеры $\chi_{\mathcal{R}_1}, \dots, \chi_{\mathcal{R}_s}$ образуют базис $\mathcal{Z}(G, \mathbb{C})$, уже было доказано (см. теорему 2 прошлой лекции). Докажем его ортогональность. Пусть

$$\mathcal{R}\colon\ G \to GL(V)$$
$$\mathcal{R}'\colon\ G \to GL(V')$$

- два неприводимых унитарных представления, $(e_1, \dots, e_n)$ и $(e'_1, \dots, e'_m)$ – ортонормированные базисы в V и V'. Их характеры:

$$\chi_{\mathcal{R}}(g) = tr\ R(g) = r_{11}(g) + \dots + r_{nn}(g)$$
$$\chi_{\mathcal{R}'}(g) = tr\ R'(g) = r'_{11}(g) + \dots + r'_{nn}(g)$$

Если $\mathcal{R}$ и $\mathcal{R}'$ не изоморфны, то:

$$(\chi_{\mathcal{R}} \mid \chi_{\mathcal{R}'}) = \sum_{\substack{i=1,\dots,n \\ j=1,\dots,m}} (r_{ii} \mid r'_{jj}) = 0,$$

так как матричные элементы разных неприводимых представлений ортогональны друг другу.

Ортонормированность.

Если $\mathcal{R}$ и $\mathcal{R}'$ изоморфны (можно считать, что $\mathcal{R} = \mathcal{R}'$), то $(r_{ii} \mid r_{jj}) = \begin{cases} 0 \text{ при } i \neq j, \\ \frac{1}{n} \text{ при } i = j \end{cases}$ и

$$(\chi_{\mathcal{R}} \mid \chi_{\mathcal{R}}) = \sum_{i,j=1}^{n} (r_{ii} \mid r_{jj}) = \sum_{i=1}^{n} (r_{ii} \mid r_{ii}) = \sum_{i=1}^{n} \frac{1}{n} = 1$$

Теорема полностью доказана. ■

Предложение 2. Кратность неприводимого представления $\mathcal{R}_i$ в произвольном представлении $\mathcal{R}$ равна $(\chi_{\mathcal{R}_i} \mid \chi_{\mathcal{R}})$.

Доказательство.
Разложим представление $\mathcal{R}$ в прямую сумму неприводимых слагаемых:

$$\mathcal{R} \simeq \underbrace{\mathcal{R}_1 \oplus \cdots \oplus \mathcal{R}_1}_{m_1} \oplus \underbrace{\mathcal{R}_2 \oplus \cdots \oplus \mathcal{R}_2}_{m_2} \oplus \cdots \oplus \underbrace{\mathcal{R}_s \oplus \cdots \oplus \mathcal{R}_s}_{m_s}$$

Тогда

$$\chi_{\mathcal{R}} = m_1 \cdot \chi_{\mathcal{R}_1} + \cdots + m_s \cdot \chi_{\mathcal{R}_s}$$

Скалярно умножим это равенство на $\chi_{\mathcal{R}_i}$. Так как характеры $\chi_{\mathcal{R}_1}, \dots, \chi_{\mathcal{R}_s}$ образуют ортонормированный базис пространства $\mathcal{Z}(G, \mathbb{C})$, получим:

$$(\chi_{\mathcal{R}_i} \mid \chi_{\mathcal{R}}) = m_1 \cdot (\chi_{\mathcal{R}_i} \mid \chi_{\mathcal{R}_1}) + \cdots + m_s \cdot (\chi_{\mathcal{R}_i} \mid \chi_{\mathcal{R}_s}) = m_i$$

■

Следствие. Линейное представление конечной группы однозначно определяется своим характером.

Упражнение. Вычислить характер регулярного представления $\chi_{\mathcal{L}}$ и с помощью предложения 2 доказать, что кратность $\mathcal{R}_i$ в $\mathcal{L}$ равна $dim\ \mathcal{R}_i$.

Подведем итоги того, что мы знаем про неприводимые конечномерные комплексные линейные представления конечных групп.

Итоги.

1) У конечной группы G есть лишь конечное число неприводимых представлений $\mathcal{R}_1, \dots, \mathcal{R}_s$ с точностью до изоморфизма. Их количество s равно количеству классов сопряженности в G.

2) Пусть $dim\ \mathcal{R}_i = n_i$. Тогда

$$n_1^2 + \cdots + n_s^2 = |G|$$

3) Количество $n_i = 1$ равно $|G/G'|$.

Пример. Описание неприводимых представлений S_n при малых n.

$n = 1,2$: в этих случаях S_n абелева, поэтому все ее неприводимые представления одномерны, их описание мы уже знаем (у группы S_1 существует только тривиальное представление, у S_2 – тривиальное и представление sgn).

$n = 3$: неприводимых представлений S_3 столько же, сколько классов сопряженности, а классы сопряженности в S_3 (как и вообще в S_n) задаются цикловыми структурами: $e, (i,j), (i,j,k)$ – получаем три класса сопряженности.
Следовательно, имеется три неприводимых представления $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3$, их размерности обозначим n_1, n_2, n_3 (можно считать, что $n_1 \le n_2 \le n_3$).

Далее, мы знаем количество одномерных представлений S_3 (одномерные представления группы S_n мы описывали на лекции 15) – их два: тривиальное и представление sgn:

$$\mathcal{R}_1, \mathcal{R}_2\colon\ S_3 \to \mathbb{C}^*$$
$$\mathcal{R}_1(\sigma) = 1,\ \ \mathcal{R}_2(\sigma) = sgn(\sigma),\ \ \forall \sigma \in S_3$$

Поэтому $n_1 = n_2 = 1$. Так как

$$n_1^2 + n_2^2 + n_3^2 = |S_3| = 6,$$

то $n_3 = 2$.
Но мы уже знаем двумерное неприводимое представление группы S_3, так как у группы S_n всегда есть стандартное неприводимое представление размерности $n - 1$:

Стандартное представление:

$$\mathcal{R}_3\colon\ S_3 \to GL(V),\ \ V = \{x \in \mathbb{C}^3 \mid x_1 + x_2 + x_3 = 0\}$$

Геометрический смысл стандартного представления: в пространстве V рассмотрим подпространство $V_{\mathbb{R}}$, состоящее из тех же векторов, но с вещественными координатами:

$$V_{\mathbb{R}} = \{x \in \mathbb{R}^3 \mid x_1 + x_2 + x_3 = 0\}$$

- инвариантное вещественное подпространство. Тогда $\mathbb{R}^3$ можно разложить в прямую сумму:

$$\mathbb{R}^3 = V_{\mathbb{R}} \oplus U_{\mathbb{R}},$$

где

$$U_{\mathbb{R}} = \{x \in \mathbb{R}^3 \mid x_1 = x_2 = x_3 = 0\}.$$

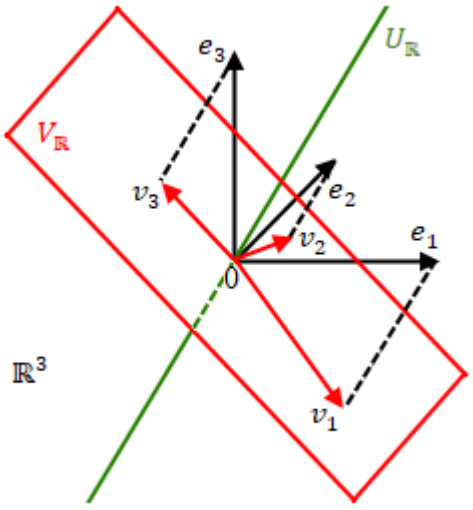


Рис. 17.1. $\mathbb{R}^3 = V_{\mathbb{R}} \oplus U_{\mathbb{R}}$

Спроектируем базисные векторы e_1, e_2, e_3 на плоскость $V_{\mathbb{R}}$ - получим векторы v_1, v_2, v_3 (см. рис. 17.1). Каждый базисный вектор e_i представляется в виде суммы своей проекции

v_i на плоскость $V_{\mathbb{R}}$ и проекции на прямую $U_{\mathbb{R}}$. Но проекция векторов e_i на прямую $U_{\mathbb{R}}$ равна вектору с концом в точке пересечения прямой $U_{\mathbb{R}}$ с треугольником, вершины которого являются вершинами векторов e_1, e_2, e_3, то есть, $\frac{1}{3}(e_1 + e_2 + e_3)$. Получаем

$$e_i = v_i + \frac{1}{3}(e_1 + e_2 + e_3)$$

Концы векторов v_i на плоскости $V_{\mathbb{R}}$ образуют вершины правильного треугольника:

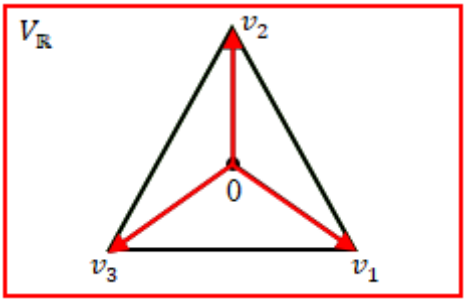


Рис. 17.2. Концы векторов v_i лежат в вершинах Δ_3

Поскольку представление $\mathcal{R}_3$ является подпредставлением мономиального представления, действующего в пространстве $\mathbb{R}^3$, то сответствующие операторы $\mathcal{R}_3(\sigma)$ переставляют базисные векторы в соответствии с перестановкой номеров под действием σ. При перестановке базисных векторов e_i их сумма остается неизменной, значит, будут переставляться и векторы v_i. Следовательно, представление $\mathcal{R}_3$ в пространстве $V_{\mathbb{R}}$ действует линейными преобразованиями, которые переставляют вершины правильного треугольника всеми возможными способами. Таким образом:

$$\mathcal{R}_3\colon\ S_3 \twoheadrightarrow Isom\,\Delta_3 = D_3 \subseteq GL(V_{\mathbb{R}})$$

- получаем уже знакомый нам изоморфизм групп S_3 и D_3.

$\underline{n = 4}$: неприводимых представлений S_4 столько же, сколько классов сопряженности, а классы сопряженности в S_4 (как и вообще в S_n) задаются цикловыми структурами: $e, (i,j), (i,j,k), (i,j,k,l), (i,j)(k,l)$ – получаем пять классов сопряженности.
Следовательно, имеется пять неприводимых представлений $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3, \mathcal{R}_4, \mathcal{R}_5$, их размерности обозначим n_1, n_2, n_3, n_4, n_5 (можно считать, что $n_1 \le n_2 \le n_3 \le n_4 \le n_5$).

Далее, как уже отмечалось ранее, существует два одномерных представления группы S_n – тривиальное и представление sgn:

$$\mathcal{R}_1, \mathcal{R}_2\colon\ S_4 \to \mathbb{C}^*$$
$$\mathcal{R}_1(\sigma) = 1,\ \ \mathcal{R}_2(\sigma) = sgn(\sigma),\ \ \forall \sigma \in S_3$$

Поэтому $n_1 = n_2 = 1$, а $1 < n_3 \le n_4 \le n_5$.

Далее воспользуемся формулой для суммы квадратов размерностей:

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = |S_4| = 24,$$

откуда

$$n_3^2 + n_4^2 + n_5^2 = 22.$$

Отсюда следует, что (так как 22 четно и не делится на 4) среди n_3, n_4, n_5 есть четное количество нечетных чисел. Это возможно лишь когда $n_3 = 2$, а $n_4 = n_5 = 3$.

Начнем с построения представлений размерности 3. Как уже отмечалось в случае S_3, можно рассмотреть стандартное представление:

$$\mathcal{R}_4\colon\ S_4 \to GL(W),\ \ W = \{x \in \mathbb{C}^4 \mid x_1 + x_2 + x_3 + x_4 = 0\}.$$

В качестве $\mathcal{R}_5$ рассмотрим

$$\mathcal{R}_5\colon\ S_4 \to GL(W)$$
$$\mathcal{R}_5(\sigma) = \mathcal{R}_4(\sigma) \cdot sgn(\sigma),\ \ \forall \sigma \in S_4$$

- это неприводимое представление, так как у операторов $\mathcal{R}_5(\sigma)$ те же инвариантные подпространства, что и у операторов $\mathcal{R}_4(\sigma)$. При этом $\mathcal{R}_5$ не изоморфно $\mathcal{R}_4$, так как

$$det\, \mathcal{R}_4(\sigma) = det\, \mathcal{M}(\sigma) = sgn(\sigma)$$

- действительно, оператор $\mathcal{M}(\sigma)$ имеет матрицу следующего вида:

$$M(\sigma) = \begin{pmatrix} & R_4(\sigma) & & 0 \\ & & & 0 \\ & & & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Но

$$det\, \mathcal{R}_5(\sigma) = sgn(\sigma) \cdot sgn^3(\sigma) = sgn^4(\sigma) = 1$$

Геометрический смысл представлений $\mathcal{R}_4$ и $\mathcal{R}_5$ аналогичен геометрическому смыслу стандартного представления $\mathcal{R}_3$, которое мы рассматривали в случае группы S_3, только пространство будет уже не трехмерным, а четырехмерным, соответственно, будет уже четыре стандартных базисных вектора e_1, e_2, e_3, e_4, которые при проекции на гиперплоскость $W_{\mathbb{R}}$ будут давать вершины не треугольника, а правильного тетраэдра T, вписанного в куб C (вершины тетраэдра T отмечены на рис. 17.3 зеленым цветом).

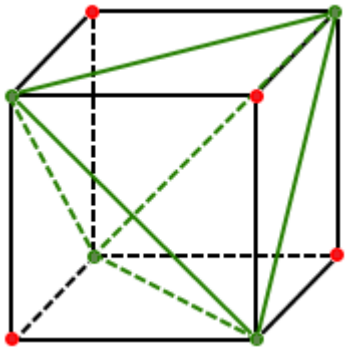


Рис. 17.3. Тетраэдр T, вписанный в куб C

Представление $\mathcal{R}_4$ изоморфно отображает группу S_4 на группу движений правильного тетраэдра:

$$\mathcal{R}_4\colon\ S_4 \twoheadrightarrow Isom\,T \subset Isom\,C$$

При движении куба C тетраэдр T также может перейти в тетраэдр, вершины которого отмечены на рис. 17.3 красным цветом. Так как $det\,\mathcal{R}_5(\sigma) = 1$, то операторы представления $\mathcal{R}_5$ могут переводить зеленый тетраэдр в красный, но вершины куба будут оставлять на месте, т.е. представление $\mathcal{R}_5$ изоморфно отображает группу S_4 на группу собственных движений куба:

$$\mathcal{R}_5\colon\ S_4 \twoheadrightarrow Isom^{+}C$$

Итак, для описания неприводимых представлений S_4 осталось построить неприводимое представление $\mathcal{R}_3$ размерности 2. Его можно построить следующим образом: ранее мы строили эпиморфизм из S_4 на S_3, рассматривая группу движений куба на множестве прямых, соединяющих цетнры противоположных граней. Но у группы S_3 есть неприводимое двумерное представление – это стандартное представление группы S_3, которое мы построили выше, когда описывали неприводимые представления S_3. Тогда композиция этих двух гомомрфизмов и будет неприводимым представлением группы S_4 размерности 2.

$$\mathcal{R}_3\colon\quad S_4 \xrightarrow{\text{эпиморфизм}} S_3 \xrightarrow[\text{представление}]{\text{стандартное}} GL(V)$$

Таким образом, мы получили полное описание всех неприводимых представлений группы S_4.

Отметим, что существует описание неприводимых представлений S_n для любого n над любым полем нулевой характеристики.

Закончим знакомство с представлениями групп задачей, которая иллюстрирует, как работает теория представлений в других областях математики.

Модельная задача. В вершинах куба записаны 8 чисел. За один шаг число в каждой вершине мы заменяем на среднее арифметическое чисел в соседних вершинах. Как будет примерно выглядеть распределение чисел по вершинам через много шагов?

Решение.
Обозначим x_1, x_2, x_3, x_4 вершины зеленого тетраэдра, $x_{-1}, x_{-2}, x_{-3}, x_{-4}$ вершины красного тетраэдра:

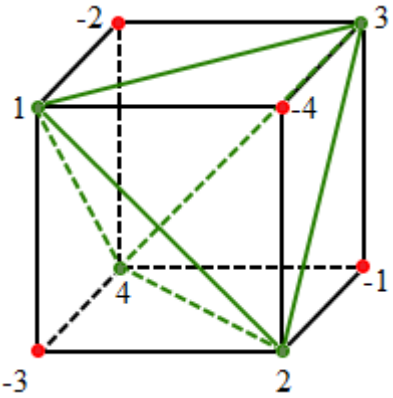


Рис. 17.4. К модельной задаче

Множество вершин:

$$X = \{x_1, x_2, x_3, x_4, x_{-1}, x_{-2}, x_{-3}, x_{-4}\}$$

Группа $S_4 \simeq Isom^+ C$ действует на множестве X, и возникает линейное представление $\mathcal{R}$ группы S_4 в пространство $\mathcal{F}(X, \mathbb{C})$ функций на множестве вершин куба. Но функция на конечном множестве полностью определяется своим набором значений на этом множестве, поэтому {8 чисел в вершинах} – то же, что и $f \in \mathcal{F}(X, \mathbb{C})$. Наша операция S (замена числа в вершине на среднее арифметическое) – линейный оператор в пространстве $\mathcal{F}(X, \mathbb{C})$:

$$S\colon\ \mathcal{F}(X, \mathbb{C}) \to \mathcal{F}(X, \mathbb{C})$$

$$Sf(x_i) = \frac{1}{3}\left(f(x_{-j}) + f(x_{-k}) + f(x_{-l})\right),$$

где $\{i, j, k, l\} = \{1,2,3,4\}$.

Заметим, что S перестановочен с действием S_4 на множестве X, т.е. S – эндоморфизм представления $\mathcal{R}$. Попробуем понять, как S действует в $\mathcal{F}(X, \mathbb{C})$. Разложим представление $\mathcal{R}$ на неприводимые слагаемые.

Вначале разложим $\mathcal{F}(X, \mathbb{C})$ в прямую сумму двух инвариантных подпространств – четных и нечетных функций (четная функция на противоположных вершинах принимает одинаковые значения, а нечетная на противоположных вершинах принимает противоположные значения):

$$\mathcal{F}(X, \mathbb{C}) = \mathcal{F}^+ \oplus \mathcal{F}^-,$$

$$\mathcal{F}^\pm = \{f \mid f(x_{-i}) = \pm f(x_i),\ \ \forall i\}$$

Посмотрим, как ограничивается представление $\mathcal{R}$ на эти два подпространства:

$\mathcal{R}|_{\mathcal{F}^+} = \mathcal{M}$ - мономиальное представление
$\mathcal{R}|_{\mathcal{F}^-} = \mathcal{M} \cdot sgn$

Пространства $\mathcal{F}^+$ и $\mathcal{F}^-$, в свою очередь, разлагаются в прямую сумму подпространств:

$$\mathcal{F}^+ = U^+ \oplus W^+,$$

где

$$U^+ = \{f \mid f(x_1) = \cdots = f(x_4)\}$$
$$W^+ = \{f \mid f(x_1) + \cdots + f(x_4) = 0\}$$

- U^+ состоит из функций, которые во всех вершинах принимают одинаковые значения, а W^+ состоит из функций, сумма значений которых во всех вершинах равна нулю.

Аналогично

$$\mathcal{F}^- = U^- \oplus W^-$$

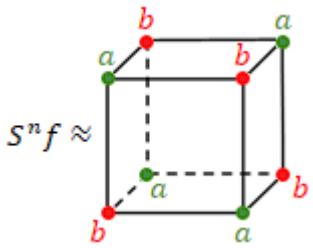
В итоге, представление $\mathcal{R}$ раскладывается в сумму четырех неприводимых представлений: $\mathcal{R}_1$ на U^+ (тривиальное), $\mathcal{R}_2$ на U^- (знаковое), $\mathcal{R}_4$ на W^+ (представление $\mathcal{R}_4$ из классификации неприводимых представлений группы S_4), $\mathcal{R}_5$ на W^- (представление $\mathcal{R}_5$ из классификации неприводимых представлений группы S_4):

$$\mathcal{R} = \mathcal{R}_1 \oplus \mathcal{R}_2 \oplus \mathcal{R}_4 \oplus \mathcal{R}_5$$

По лемме Шура, S действует на каждом из этих подпространств скалярно:

- на U^+: $S = \mathcal{E}$,
- на U^-: $S = -\mathcal{E}$,
- на W^+: $S = -\frac{1}{3}\mathcal{E}$,
- на W^-: $S = \frac{1}{3}\mathcal{E}$.

Отсюда видно, что $S^n \to 0$ на пространствах W^+ и W^-, т.е. когда мы применяем много раз оператор S к произвольной функции $f \in \mathcal{F}(X, \mathbb{C})$, то “выживают” только те части этой функции, которые лежат в пространствах U^+ и U^-. Поэтому при $n \gg 0$



Легко понять, что за один шаг a и b меняются местами.

Лекция 18. Кольца и алгебры. Часть 1.

Определение. *Кольцо* – это множество A с двумя бинарными операциями (сложением и умножением), для которых выполнены следующие аксиомы:

1) относительно сложения, A – абелева группа,
2) умножение дистрибутивно:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

Определение. *Алгебра* над полем K – это множество A с тремя операциями: сложение, умножение, умножение на элементы поля K (скаляры), для которых выполнены следующие аксиомы:

1) относительно сложения и умножения на скаляры, A – векторное пространство над K,
2) умножение билинейно, т.е. выполнены свойства:

- дистрибутивность:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

- однородность: $\forall a, b \in A,\ \forall \lambda \in K$

$$(\lambda \cdot a) \cdot b = a \cdot (\lambda \cdot b) = \lambda \cdot (a \cdot b)$$

В зависимости от дополнительных свойств умножения, выделяют разные классы колец и алгебр: коммутативные, ассоциативные, с единицей, и т.д.

Примеры.

1) $\mathbb{Z}$ (целые числа) - коммутативное, ассоциативное кольцо с единицей без делителей нуля (область целостности).

2) $\mathbb{Z}_m$ (вычеты по модулю m) - коммутативное, ассоциативное кольцо с единицей. Если m – простое число, то $\mathbb{Z}_m$ является полем (поле – ненулевое коммутативное ассоциативное кольцо с единицей, каждый ненулевой элемент которого обратим).

3) $K[x_1, \dots, x_n]$ (многочлены от n переменных над полем K) – коммутативная, ассоциативная алгебра с единицей без делителей нуля.

4) $\mathcal{F}(X, K)$ (функции на множестве X со значениями в поле K) – коммутативная, ассоциативная алгебра с единицей.

5) $Mat_n(K)$ (матрицы $n \times n$ над полем K) – некоммутативная, ассоциативная алгебра с единицей.

6) E (трехмерное евклидово пространство) с операцией векторного умножения:

$$(a, b) \mapsto [a, b]$$

Свойства векторного умножения:

1) билинейность
2) антикоммутативность:

$$[a, b] = -[b, a]$$

3) тождество Якоби: $\forall a, b, c \in E$:

$$[[a, b], c] + [[b, c], a] + [[c, a], b] = 0$$

E – *алгебра Ли* над $\mathbb{R}$ (алгебра Ли – алгебра, в которой умножение антикоммутативно и удовлетворяет тождеству Якоби). Названа так в честь Софуса Ли (M. S. Lie, 1842-1899) – норвежского математика 19 века.

Замечание. Если A – ненулевая алгебра с единицей над полем K, то $1 \neq 0$ (действительно, если бы выполнялось равенство $1 = 0$, то $\forall a \in A$: $a = a \cdot 1 = a \cdot 0 = 0$). Тогда существует вложение поля K в качестве подалгебры в алгебру A:

$$K \hookrightarrow A$$
$$\lambda \mapsto \lambda \cdot 1$$

Это действительно вложение, так как если $\lambda \cdot 1 = \mu \cdot 1$, то $(\lambda - \mu) \cdot 1 = 0$, откуда следует, что $\lambda - \mu = 0$, то есть, $\lambda = \mu$.

Таким образом, мы можем рассматривать ненулевую алгебру с единицей над полем K как кольцо с единицей, которое содержит K в качестве подкольца.

Возникает вопрос о необходимости введения понятия алгебры. Дело в том, что алгебры удобнее колец – с ними проще работать, поскольку в алгебре есть дополнительная структура векторного пространства и можно использовать мощные методы линейной алгебры. Особенно это удобно в конечномерной ситуации.

Структурные константы.

Определение. Пусть A – конечномерная алгебра над полем K, $dim\, A = n$. Выберем в A базис $(e_1, \dots, e_n)$. Тогда $\forall i, j \in \{1, \dots, n\}$:

$$e_i \cdot e_j = c_{ij}^1 e_1 + \dots + c_{ij}^n e_n$$

Коэффициенты $c_{ij}^{\mathrm{k}} \in K \ \ (i,j,k \in \{1,\dots,n\})$ называются *структурными константами* алгебры A в базисе $(e_1,\dots,e_n)$.

Структурные константы однозначно определяют умножение в алгебре A. В самом деле, $\forall x,y \in A$:

$$x = x_1e_1 + \cdots + x_ne_n$$
$$y = y_1e_1 + \cdots + y_ne_n$$
$$x \cdot y = \sum_{i,j=1}^{n} x_iy_j \cdot e_i \cdot e_j = \sum_{i,j,k=1}^{n} c_{ij}^{k} \cdot x_iy_j \cdot e_k$$

Так как структурные константы однозначно определяют умножение, то они однозначно определяют и все свойства этого умножения. Например:

коммутативность $\Leftrightarrow e_i \cdot e_j = e_j \cdot e_i \ \ \forall i,j \in \{1,\dots,n\} \Leftrightarrow c_{ij}^{k} = c_{ji}^{k} \ \ \forall i,j,k \in \{1,\dots,n\}$
антикоммутативность $\Leftrightarrow e_i \cdot e_j = -e_j \cdot e_i \ \forall i,j \in \{1,\dots,n\} \Leftrightarrow c_{ij}^{k} = -c_{ji}^{k} \ \forall i,j,k \in \{1,\dots,n\}$

Упражнение. Охарактеризовать ассоциативность и тождество Якоби в терминах структурных констант.

Примеры.

1) $A = Mat_n(K)$. Базис – матричные единицы E_{ij} $(i,j = 1,\dots,n)$:

$$E_{ij} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & 1 & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \begin{matrix} \\ i \\ \\ \end{matrix}$$
$$\qquad\qquad\quad j$$

Матричные единицы перемножаются по правилу: $E_{ij} \cdot E_{kl} = \begin{cases} E_{il} \text{ при } j = k \\ 0 \text{ при } \ j \neq k \end{cases}$

Структурные константы:

$$c_{ij,kl}^{pq} = \begin{cases} 1 \text{ при } i = p, j = k, q = l \\ 0, \text{иначе} \end{cases}$$

2) Пусть G – конечная группа. *Групповая алгебра* $K \cdot G$ – векторное пространство с базисом e_g $(g \in G)$ и билинейным умножением, заданным на базисе правилом:

$$e_g \cdot e_h = e_{g \cdot h}$$

т.е. базисные элементы перемножаются в соответствии с тем, как перемножаются элементы группы, которые нумеруют эти базисные векторы.

Структурные константы:

$$c_{g,h}^{u} = \begin{cases} 1 \text{ при } u = g \cdot h \\ 0, \text{ иначе} \end{cases}$$

Таким образом, всякий элемент a групповой алгебры $K \cdot G$ единственным способом разлагается в линейную комбинацию базисных:

$$a = \sum_{g \in G} \lambda_g \cdot e_g = \sum_{g \in G} \lambda_g \cdot g$$

где $\lambda_g \in K$ (для краткости иногда вместо e_g пишут соответствующий ему элемент $g \in G$ – получаем формальные линейные комбинации элементов группы).

Можно воспринимать групповую алгебру как множество формальных линейных комбинаций элементов конечной группы G с коэффициентами из поля K, которые складываются и перемножаются по формальным правилам.

$K \cdot G$ – ассоциативная алгебра с единицей $1 = e$ (нейтральный элемент в G), $dim\, K \cdot G = |G|$, алгебра $K \cdot G$ коммутативна $\Leftrightarrow$ G абелева.

3) *Алгебра кватернионов* $\mathbb{H}$ - четырехмерная алгебра над $\mathbb{R}$ с базисом $(1, i, j, k)$, причем 1 – единица в $\mathbb{H}$ (нейтральный элемент по умножению), i, j, k – кватернионные единицы. В $\mathbb{H}$ операция умножения задана на базисе по правилам:

$$\begin{gathered} i^2 = j^2 = k^2 = -1, \\ i \cdot j = k, \qquad j \cdot i = -k \\ j \cdot k = i, \qquad k \cdot j = -i \\ k \cdot i = j, \qquad i \cdot k = -j \end{gathered}$$

Таблицу умножения в $\mathbb{H}$ можно запомнить с помощью следующей картинки:

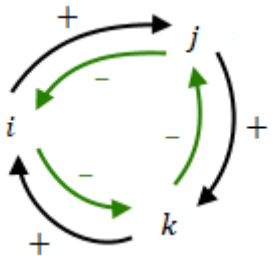


Рис. 18.1. Умножение кватернионных единиц

- произведение двух кватернионных единиц равно третьей, следующей за ними по циклу, причем если мы идем по часовой стрелке, то произведение будет со знаком “+”, а если против часовой стрелки, то со знаком “−“.

Кватернионы придумал английский математик Гамильтон (W.R. Hamilton, 1805-1865) как обобщение комплексных чисел. Однако, при этом не все свойства комплексных чисел удается сохранить: алгебра кватернионов $\mathbb{H}$ - некоммутативная ассоциативная алгебра с единицей над $\mathbb{R}$. Свойство ассоциативности (не вполне очевидное) можно проверить перебором на базисных векторах. Мы построим матричную модель алгебры кватернионов (т.е. алгебру, изоморфную алгебре кватернионов), про которую заранее известно, что умножение в ней ассоциативно.

Модель алгебры кватернионов

$$\mathbb{H} \simeq \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \subset Mat_2(\mathbb{C})$$

- вещественное четырехмерное подпространство в пространстве $Mat_2(\mathbb{C})$. Изоморфизм задается на базисе следующим соответствием:

$$1 \leftrightarrow E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad i \leftrightarrow I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad j \leftrightarrow J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad k \leftrightarrow K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Матрицы E, I, J, K действительно образуют базис в пространстве матриц вида $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, $a, b \in \mathbb{C}$, так как они соответствуют выбору вместо чисел a и b соответствующих базисных элементов $1, i$.

Упражнение. Проверить, что для матриц E, I, J, K выполнены правила умножения кватернионных единиц $1, i, j, k$.

Следовательно, множество матриц вида $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, $a, b \in \mathbb{C}$ образует подалгебру (над $\mathbb{R}$) в алгебре $Mat_2(\mathbb{C})$, изоморфную $\mathbb{H}$. Умножение матриц ассоциативно, поэтому и умножение в $\mathbb{H}$ ассоциативно. Исследуем и другие свойства алгебры кватернионов.

Определение. Пусть $q = \alpha \cdot 1 + \beta \cdot i + \gamma \cdot j + \delta \cdot k$, где $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ - произвольный кватернион. *Сопряженным кватернионом* называется $\bar{q} = \alpha \cdot 1 - \beta \cdot i - \gamma \cdot j - \delta \cdot k$. *Кватернионная норма*:

$$N(q) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

Сопряженный кватернион – аналог сопряженного комплексного числа, кватернионная норма – аналог квадрата модуля комплексного числа.

Свойства кватернионного сопряжения и кватернионной нормы:

1) $\bar{\bar{q}} = q$,
2) $\bar{q} = q \Leftrightarrow q \in \mathbb{R}$,
3) $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$,

4) $\overline{q_1 \cdot q_2} = \overline{q_2} \cdot \overline{q_1}$

Доказательство.
Левая и правая части билинейно (над $\mathbb{R}$) зависят от q_1 и q_2, поэтому достаточно проверить свойство 4 для базисных кватернионов q_1 и q_2. Если один из них равен 1 ,то равенство $\overline{q_1 \cdot q_2} = \overline{q_2} \cdot \overline{q_1}$ очевидно, а если оба кватерниона равны мнимым кватернионным единицам, то рассмотрим два случая:
а) если $q_1 = q_2$, то

$$\overline{q_1 \cdot q_2} = \overline{q_1^2} = \overline{-1} = -1,$$
$$\overline{q_2} \cdot \overline{q_1} = \overline{q_1} \cdot \overline{q_1} = (-q_1) \cdot (-q_1) = q_1^2 = -1$$

б) если $q_1 \neq q_2$, например, $q_1 = i$, $q_2 = j$, то

$$\overline{q_1 \cdot q_2} = \overline{i \cdot j} = \bar{k} = -k$$
$$\overline{q_2} \cdot \overline{q_1} = \bar{j} \cdot \bar{i} = (-j) \cdot (-i) = j \cdot i = -k$$

5) $N(q) = q \cdot \bar{q} = \bar{q} \cdot q$ – проверяется непосредственно.

6) Если $q \neq 0$, то $N(q) \neq 0$ и существует обратный кватернион:

$$q^{-1} = \frac{\bar{q}}{N(q)}$$

Итак, в алгебре кватернионов любой ненулевой элемент имеет обратный. Такие алгебры (кольца) называются телами.

Определение. Назовем *телом* ненулевое ассоциативное кольцо с единицей, в котором каждый ненулевой элемент имеет обратный (иными словами, тело – это некоммутативное поле).

Определение. *Алгебра с делением* – это алгебра, являющаяся телом.

Таким образом, $\mathbb{H}$ - конечномерная алгебра с делением над $\mathbb{R}$.

Идеалы.

В теории групп особую роль играют нормальные подгруппы. Аналогичное понятие присутствует и в теории колец и алгебр – это идеал.

Определение. Пусть A – кольцо/алгебра. *Идеалом* в A называется подмножество $I \subseteq A$, для которого:
1) I – подгруппа относительно сложения (для колец),
– векторное подпространство (для алгебр).

2) $A \cdot I \subseteq I$ – *левый* идеал,
$I \cdot A \subseteq I$ – *правый* идеал.

Если идеал одновременно является левым и правым, то говорят, что он *двусторонний*. Именно двусторонние идеалы являются полным аналогом нормальных подгрупп в теории групп. В коммутативном кольце/алгебре все идеалы – двусторонние.

Обозначение для двустороннего идеала: $I \lhd A$.

Примеры идеалов.

1) $A = \mathbb{Z}$. Идеал – это подгруппа относительно сложения, поэтому любой идеал имеет вид

$$I = m \cdot \mathbb{Z} \ (m \geq 0).$$

Это двусторонний идеал: $m \cdot \mathbb{Z} \lhd \mathbb{Z}$.

2) Нулевой идеал $I = \{0\}$. Это двусторонний идеал : $\{0\} \lhd A$.

3) Наибольший идеал $I = A$. Очевидно, что это двусторонний идеал: $A \lhd A$. Наибольший и нулевой идеалы называются тривиальными.

4) $A = Mat_n(K) \supset I = \{\text{матрицы, у которых все столбцы, кроме первого, нулевые}\}$ – левый идеал (очевидно, что I – подпространство в $Mat_n(K)$, и при умножении матрицы из I слева на произвольную матрицу из $Mat_n(K)$ мы снова получим матрицу из I). Аналогично

$$A = Mat_n(K) \supset I = \{\text{матрицы, у которых все строки, кроме первой, нулевые}\}$$

- правый идеал. Отметим, что двусторонних идеалов в алгебре матриц нет.

5) $A = \mathcal{F}(X, K)$. Для любой точки $x_0 \in X$ рассмотрим $I(x_0)$ – множество функций, которые в этой точке обращаются в ноль:

$$I(x_0) = \{f \in \mathcal{F}(X, K) \mid f(x_0) = 0\}$$

Легко видеть, что $I(x_0)$ является подпространством в $\mathcal{F}(X, K)$ и $I(x_0)$ – двусторонний идеал: $I(x_0) \lhd \mathcal{F}(X, K)$.

Факторкольцо и факторалгебра.

В теории групп нормальные подгруппы используются для построения новых групп – мы можем строить по ним факторгруппы. Аналогичная конструкция есть и в теории колец и в теории алгебр.

Определение. Пусть A – кольцо или алгебра, $I \lhd A$. *Факторкольцо/факторалгебра*:

$$A/I = \{a + I \mid a \in A\}$$

- факторгруппа по сложению. Умножение смежных классов и умножение на скаляры определяется естественно: $\forall a, b \in A,\ \forall \lambda \in K$:

$$(a + I)(b + I) = ab + I$$
$$\lambda(a + I) = \lambda a + I$$

Проверим корректность так заданного умножения смежных классов, т.е. что результат умножения не зависит от выбора представителей смежных классов: пусть

$$a + I = a' + I \Rightarrow a' = a + u,\ \ u \in I,$$
$$b + I = b' + I \Rightarrow b' = b + v,\ \ v \in I,$$

тогда

$$a'b' = (a + u)(b + v) = ab + av + ub + uv.$$

Здесь $av \in I,\ ub \in I, uv \in I$, значит и $av + ub + uv \in I$, то есть, $ab + I = a'b' + I$.

Аналогично проверяется корректность умножения смежных классов на скаляры (в случае алгебры):

$$\lambda a' = \lambda a + \lambda u,\ \ u \in I,$$

- здесь $\lambda u \in I$, значит $\lambda a + I = \lambda a' + I$.

Пример. $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ – кольцо вычетов.

В связи с тем, что кольцо вычетов является общим случаем факторкольца, в общем случае принята та же терминология, что и для колец вычетов.

Терминология:

смежные классы по идеалу = классы вычетов:

$$a + I = a \bmod I$$

принадлежность одному смежному классу = сравнимость по модулю идеала:

$$a \equiv b \ (mod\ I) \Leftrightarrow a - b\ \in I \Leftrightarrow a + I = b + I$$

Лекция 19. Кольца и алгебры. Часть 2.

Продолжим изучение колец и алгебр. Как и в теории групп, для сравнения разных алгебраических объектов, принадлежащих к одному классу, используется понятие гомоморфизма.

Определение. *Гомоморфизм колец (алгебр)* – это отображение $\varphi\colon A \to B$ (где A и B – кольца/алгебры), для которого: $\forall x, y \in A$:

- $\varphi(x + y) = \varphi(x) + \varphi(y)$
- $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

для алгебр добавляется еще одно свойство: $\forall \lambda \in K$:

- $\varphi(\lambda \cdot x) = \lambda \cdot \varphi(x)$

для колец/алгебр с единицей требуется выполнения еще одного условия (единица в A переходит в единицу в B):

- $\varphi(1) = 1$

Образ гомоморфизма:

$$Im\ \varphi = \{b = \varphi(a) \mid a \in A\}$$

Ядро гомоморфизма:

$$Ker\ \varphi = \{a \in A \mid \varphi(a) = 0\}$$

В частности, если рассматривать A и B как группы по сложению, то получаем привычные понятия образа и ядра гомоморфизма групп. Если A и B алгебры, то φ является линейным отображением – получаем понятия образа и ядра линейного отображения, знакомые из линейной алгебры. Как и для групп, верно следующее утверждение.

Предложение 1. Для любого гомоморфизма колец/алгебр $\varphi\colon A \to B$:

- $Im\ \varphi \subseteq B$ – подкольцо/подалгебра
- $Ker\ \varphi \lhd A$ – двусторонний идеал

Доказательство.
1) Как мы знаем из теории групп, $Im\ \varphi$ и $Ker\ \varphi$ – подгруппы по сложению. Для того, чтобы доказать, что $Im\ \varphi$ – подкольцо, остается проверить замкнутость относительно умножения:

$$b, b' \in Im\ \varphi \Rightarrow b = \varphi(a), b' = \varphi(a') \Rightarrow bb' = \varphi(aa') \in Im\ \varphi$$

Если $Im\ \varphi$ – подалгебра, нужно еще проверить замкнутость относительно умножения на скаляры:

$$b \in Im\ \varphi \Rightarrow \lambda b = \varphi(\lambda a) \in Im\ \varphi$$

Таким образом, $Im\ \varphi$ – подкольцо/подалгебра в B.

2) Для того, чтобы доказать, что $Ker\ \varphi$ – двусторонний идеал, остается проверить замкнутость относительно умножения справа и слева на любые элементы A:

$$a \in Ker\ \varphi, a' \in A \Rightarrow \varphi(aa') = \varphi(a)\varphi(a') = 0 \cdot \varphi(a') = 0 \Rightarrow aa' \in Ker\ \varphi$$
$$a \in Ker\ \varphi, a' \in A \Rightarrow \varphi(a'a) = \varphi(a')\varphi(a) = \varphi(a') \cdot 0 = 0 \Rightarrow a'a \in Ker\ \varphi$$

Если A – алгебра, нужно еще проверить замкнутость относительно умножения на скаляры:

$$\varphi(\lambda a) = \lambda \cdot \varphi(a) = \lambda \cdot 0 = 0 \Rightarrow \lambda a \in Ker\ \varphi$$

Следовательно, $Ker\ \varphi \lhd A$. ■

Таким образом, идеалы естественно возникают как ядра гомоморфизмов колец/алгебр. Верно и обратное. Пусть $I \lhd A$, тогда, как и для групп, можно рассмотреть каноническую проекцию из A в факторкольцо/факторалгебру A/I, которая каждому элементу ставит в соответствие его смежный класс (класс вычетов) по модулю идеала I.

Каноническая проекция:

$$\pi\colon\ A \to A/I$$
$$a \mapsto a + I$$

Каноническая проекция – гомоморфизм (следует из определения операций в A/I: операции над смежными классами определяются через операции над представителями этих смежных классов). Ядром этого гомоморфизма является сам идеал I, а образ совпадает с A/I:

$$Ker\ \pi = I$$
$$Im\ \pi = A/I$$

Таким образом, двусторонние идеалы = ядра гомоморфизмов. По аналогии с теорией групп, существует и следующая теорема.

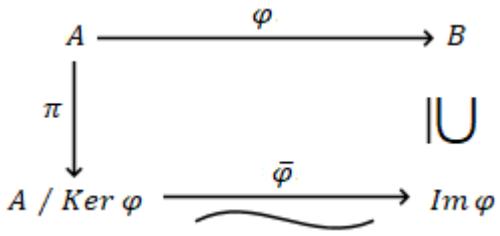
Основная теорема о гомоморфизмах колец/алгебр. Пусть $\varphi\colon\ A \to B$ – гомоморфизм колец/алгебр. Тогда ∃! изоморфизм

$$\bar{\varphi}\colon\ A/\ Ker\ \varphi \twoheadrightarrow Im\ \varphi,$$

для которого $\varphi = \bar{\varphi} \circ \pi$, где $\pi\colon\ A \to A\ /\ Ker\ \varphi$ – каноническая проекция. Другими словами,

$$\varphi(a) = \bar{\varphi}(a + Ker\ \varphi)$$

Еще короче теорему можно сформулировать с помощью коммутативной диаграммы:



Доказательство.
Из теории групп мы знаем, что существует единственный изоморфизм аддитивных групп $\bar{\varphi}$ с нужными свойствами (см. основную теорему о гомоморфизмах групп, лекция 2). Остается проверить, что $\bar{\varphi}$ – гомоморфизм колец/алгебр.

$\bar{\varphi}$ – гомоморфизм колец:

$$\bar{\varphi}\big((x + Ker\,\varphi) \cdot (y + Ker\,\varphi)\big) = \bar{\varphi}(xy + Ker\,\varphi) = \varphi(xy) = \varphi(x) \cdot \varphi(y) =$$

$$= \bar{\varphi}(x + Ker\,\varphi) \cdot \bar{\varphi}(y + Ker\,\varphi)$$

$\bar{\varphi}$ – гомоморфизм алгебр:

$$\bar{\varphi}\big(\lambda \cdot (x + Ker\,\varphi)\big) = \bar{\varphi}(\lambda x + Ker\,\varphi) = \varphi(\lambda x) = \lambda \cdot \varphi(x) = \lambda \cdot \varphi(x + Ker\,\varphi)$$

■

Пример. Рассмотрим алгебру $\mathcal{F}(X, K)$. Выберем $x_0 \in X$ и рассмотрим гомоморфизм вычисления значения функции в данной точке:

$$\varphi\colon \mathcal{F}(X, K) \to K$$
$$f \mapsto f(x_0)$$

Его ядро и образ:

$$Ker\,\varphi = I(x_0)$$
$$Im\,\varphi = K$$

По основной теореме о гомоморфизмах,

$$\mathcal{F}(X, K)/I(x_0) \simeq K$$

Еще одно понятие, которое можно перенести из теории групп в теорию колец/алгебр – это понятие прямой суммы.

Определение. Прямая сумма колец/алгебр

$$A = A_1 \oplus \cdots \oplus A_s$$

- их прямая сумма как аддитивных групп (если A – кольцо), или как векторных пространств (если A – алгебра) с умножением по правилу: $\forall a_i, b_i \in A_i$ $(i = 1, \dots, s)$:

для внутренней прямой суммы: если

$$a = a_1 + \cdots + a_s$$
$$b = b_1 + \cdots + b_s$$

то

$$ab = a_1 b_1 + \cdots + a_s b_s$$

для внешней прямой суммы: если

$$a = (a_1, \dots, a_s)$$
$$b = (b_1, \dots, b_s)$$

то

$$ab = (a_1 b_1, \dots, a_s b_s)$$

Как и в случае групп, понятия внешней и внутренней прямой суммы колец/алгебр эквивалентны. Прямая сумма колец/алгебр данного типа (коммутативные, ассоциативные, с единицей и т.д.) часто имеет тот же тип. В частности, имеет место следующий факт: пусть $A_1, \dots, A_s$ – ассоциативные кольца с единицей, тогда $A_1 \oplus \cdots \oplus A_s$ – ассоциативное кольцо/алгебра с единицей $(1, \dots, 1)$.

Лемма. Мультипликативная группа прямой суммы ассоциативных колец с единицей изоморфна прямому произведению мультипликативных групп этих колец:

$$(A_1 \oplus \cdots \oplus A_s)^\times \simeq A_1^\times \times \cdots \times A_s^\times$$

Доказательство.
Элемент $(a_1, \dots, a_s)$ обратим в $A_1 \oplus \cdots \oplus A_s \Leftrightarrow \exists b_i \in A_i$:

$$(a_1, \dots, a_s)(b_1, \dots, b_s) = (a_1 b_1, \dots, a_s b_s) = (1, \dots, 1) \Leftrightarrow \forall i\colon\ a_i b_i = 1$$
$$(b_1, \dots, b_s)(a_1, \dots, a_s) = (b_1 a_1, \dots, b_s a_s) = (1, \dots, 1) \Leftrightarrow \forall i\colon\ b_i a_i = 1$$

То есть, $\forall i\colon\ a_i b_i = b_i a_i = 1$, что равносильно тому, что $\forall i\ a_i$ обратим в A_i. Таким образом, элемент прямой суммы обратим тогда и только тогда, когда обратимы его компоненты. Это и устанавливает изоморфизм между $(A_1 \oplus \cdots \oplus A_s)^\times$ и $A_1^\times \times \cdots \times A_s^\times$ (так как в обоих случаях умножение происходит покомпонентно). ■

Китайская теорема об остатках для колец вычетов.

Пусть $m_1, \dots, m_s \in \mathbb{N}$ попарно взаимно просты, $m = m_1 \cdot \ldots \cdot m_s$. Тогда

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$

- изоморфизм колец.

Доказательство.
Рассмотрим отображение

$$\psi\colon\ \mathbb{Z} \to \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$
$$\psi(n) = (n \bmod m_1, \dots, n \bmod m_s)$$

Это гомоморфизм колец (так как при сложении и умножении целых чисел вычеты этих чисел по соответствующим модулям тоже складываются (соответственно, перемножаются), а наборы вычетов складываются покомпонентно).

Как было показано ранее (при доказательстве китайской теоремы об остатках для групп – см. лекцию 4):

$$Ker\,\psi = m\mathbb{Z}$$
$$Im\,\psi = \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$

По основной теореме о гомоморфизмах колец,

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$
$$\bar{\psi}(n\ mod\ m) = (n\ mod\ m_1, \dots, n\ mod\ m_s)$$

■

Следствие (мультипликативное свойство функции Эйлера). Функция Эйлера мультипликативна:

$$\varphi(m) = \varphi(m_1) \cdot \ldots \cdot \varphi(m_s)$$

В частности, если $m = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$, где $p_1, \dots, p_s$ – различные простые числа, $k_1, \dots, k_s \in \mathbb{N}$, то

$$\varphi(m) = \varphi\left(p_1^{k_1}\right) \cdot \ldots \cdot \varphi\left(p_s^{k_s}\right) = \left(p_1^{k_1} - p_1^{k_1-1}\right) \cdot \ldots \cdot \left(p_s^{k_s} - p_s^{k_s-1}\right)$$

Доказательство.
По китайской теореме об остатках для колец:

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$

тогда по лемме

$$\mathbb{Z}_m^\times \simeq \mathbb{Z}_{m_1}^\times \times \cdots \times \mathbb{Z}_{m_s}^\times.$$

Следовательно,

$$\varphi(m) = |\mathbb{Z}_m^\times| = \left|\mathbb{Z}_{m_1}^\times\right| \cdot \ldots \cdot \left|\mathbb{Z}_{m_s}^\times\right| = \varphi(m_1) \cdot \ldots \cdot \varphi(m_s)$$

■

В теории групп было понятие простой группы (т.е. группы, в которой нет нетривиальных нормальных подгрупп). Аналогичное понятие можно определить и для колец/алгебр.

Определение. Кольцо/алгебра A называется *простым*, если $A \neq \{0\}$ и в A не существует нетривиальных двусторонних идеалов $I \lhd A$, кроме тривиальных: $I = \{0\}$ и $I = A$.

Теорема 1. Коммутативное ассоциативное кольцо с единицей A просто $\Leftrightarrow$ A – поле.

Доказательство.

⇒:
Пусть $x \in A$, $x \neq 0$. Рассмотрим множество элементов, кратных x:

$$I = \{a \cdot x \mid a \in A\} = A \cdot x$$

Легко видеть, что это идеал: $I \lhd A$, при этом $I \neq \{0\}$, так как I содержит по крайней мере $x = 1 \cdot x$. Следовательно (так как A просто), $I = A$. Отсюда следует, что существует $y \in A$: $y \cdot x = 1$, т.е. x обратим. Таким образом, A – поле.

⇐:
Пусть $I \lhd A$, $I \neq \{0\}$. Выберем $x \in A$, $x \neq 0$. Тогда $x \cdot x^{-1} = 1 \in I$. Но если идеал содержит 1, тогда он содержит и любой элемент кольца A, так как $\forall a \in A$: $a = a \cdot 1 \in I$. Следовательно, $I = A$, т.е. A – простое кольцо. ■

Отметим, что в случае некоммутативных колец аналогичное утверждение верно только в одну сторону: всякое тело является простым ассоциативным кольцом с единицей. Обратное неверно – существуют простые некоммутативные ассоциативные кольца с единицей, которые не являются телами, и важный пример такого кольца (и алгебры) доставляет следующая теорема.

Теорема 2. Алгебра $Mat_n(K)$ проста.

Доказательство.
Пусть $I \lhd Mat_n(K), I \neq \{0\}$. Выберем $A \in I, A \neq \{0\}$. Разложим матрицу A по базису, т.е. представим в виде линейной комбинации матричных единиц:

$$A = \sum_{i,j=1}^{n} a_{ij} E_{ij}$$

Так как $A \neq \{0\}$, то $\exists k, l$: $a_{kl} \neq 0$.

Умножим A слева и справа на матричные единицы: $\forall p, q \in \{1, \dots, n\}$ рассмотрим произведение:

$$E_{pk} \cdot A \cdot E_{lq} = a_{kl} \cdot E_{pk} \cdot E_{kl} \cdot E_{lq} = a_{kl} \cdot E_{pq} \in I$$

- таким образом, если в ненулевом идеале лежит какая-то ненулевая матрица, то там лежит и матричная единица: $E_{pq} \in I$ для произвольных $p, q \in \{1, \dots, n\}$. Следовательно, I содержит все матричные единицы, которые образуют базис алгебры матриц, т.е. $I = Mat_n(K)$. ■

Коммутативная алгебра.

Далее сосредоточим внимание на изучении коммутативных ассоциативных колец с единицей. Наука, их изучающая, называется коммутативной алгеброй.

Пусть A – коммутативное ассоциативное кольцо с единицей. Пусть задано семейство элементов $f_j \in A \quad (j \in J)$. По аналогии с определением подгруппы, порожденной семейством элементов, можно ввести понятие идеала, порожденного семейством элементов.

Определение. Идеал, *порожденный семейством элементов* кольца/алгебры $I = (f_j \mid j \in J) \lhd A$ – наименьший идеал, содержащий это семейство.

Такой идеал существует, так как его можно представить в виде пересечения всех идеалов, содержащих семейство $f_j \in A$ (хотя бы один такой идеал найдется – это само кольцо/алгебра A). Можно дать его явное описание:

$$I = \{a_1 f_{j_1} + \cdots + a_s f_{j_s} \mid j_1, \ldots, j_s \in J, \;\; a_1, \ldots, a_s \in A\}$$

В самом деле, любой идеал, содержащий элементы $f_j, \;\; j \in J$, содержит и все выражения вида $a_1 f_{j_1} + \cdots + a_s f_{j_s}$ (так как идеал замкнут относительно сложения и умножения на произвольные элементы кольца), но множество всех таких выражений само является идеалом.

Определение. *Конечно порожденный* идеал – идеал, порожденный конечным семейством элементов:

$$I = (f_1, \ldots, f_m) = \{a_1 f_1 + \cdots + a_m f_m \mid a_i \in A\} = Af_1 + \cdots + Af_m$$

Существуют кольца/алгебры, в которых каждый идеал является конечно порожденным. Приведем без доказательства один из важных результатов, касающихся таких колец/алгебр.

Теорема Гильберта о базисе идеала. В алгебре многочленов $K[x_1, \ldots, x_n]$ над полем K любой идеал конечно порожден.

Немного упростим ситуацию, и будем рассматривать среди конечно порожденных идеалов самые простые – а именно, идеалы, порожденные одним элементом. Такие идеалы называются главными.

Определение. *Главный* идеал – идеал вида

$$I = (f) = \{af \mid a \in A\} = Af$$

Определение. *Кольцо главных идеалов* – целостное кольцо, в котором все идеалы главные.

Напоминание: евклидово кольцо – целостностное кольцо A, на котором задана евклидова норма:

$$N: A\backslash\{0\} \to \mathbb{Z}_+$$

со свойствами:

1) $N(a \cdot b) \geq N(a)$, равенство достигается только при $b \in A^\times$,
2) $\forall a, b \in A, b \neq 0$ существуют $q, r \in A$: $a = b \cdot q + r$ и $N(r) < N(b)$, или $r = 0$ (деление с остатком).

Примеры евклидовых колец:

1) $A = \mathbb{Z}$, норма: $N(a) = |a|$,

2) $A = K[x]$, K – поле, норма: $N(f) = deg\ f$.

Теорема 3. Всякое евклидово кольцо (в частности, $\mathbb{Z}$ и $K[x]$, K – поле) является кольцом главных идеалов.

Доказательство.
Пусть A – евклидово кольцо, $I \lhd A$. Если $I = \{0\}$, то $I = (0)$ – главный идеал. Иначе выберем $b \in I$, $b \neq 0$ с наименьшей нормой среди ненулевых элементов идеала I: $N(b) = min$ (среди элементов I).
Теперь воспользуемся вторым свойством евклидовой нормы (деление с остатком): $\forall a \in I$: $a = b \cdot q + r$, причем $N(r) < N(b)$, или $r = 0$. Но $a \in I$, $b \cdot q \in I$, следовательно, и $a - b \cdot q = r \in I$, значит, $r = 0$ (иначе это противоречит выбору b). Получаем, что $a = b \cdot q$.
Следовательно, $I = (b)$. ■

Теория делимости в евклидовых кольцах, которую мы развили в первой части курса, практически без изменений переносится на любые кольца главных идеалов. Отметим, что не всякое целостное (и даже факториальное) кольцо является кольцом главных идеалов.

Пример. $K[x_1, \dots, x_n]$ – не кольцо главных идеалов при $n > 1$.

В самом деле, рассмотрим

$$I = \{f \in K[x_1, \dots, x_n] \mid f(0, \dots, 0) = 0$$

- идеал многочленов без свободного члена. Если бы $I = (f)$, то $x_1, \dots, x_n$ должны были бы делиться на f (так как $x_1, \dots, x_n \in I$), откуда следует, что $f = c \in K$. Но если $c = 0$, то $I = \{0\}$, а если $c \neq 0$, то $I = K[x_1, \dots, x_n]$ – противоречие. Следовательно, I – не главный идеал.

Лекция 20. Структура факторалгебр алгебры многочленов от одной переменной.

На прошлой лекции мы ввели понятие кольца главных идеалов (к этому классу колец относятся, в частности, все евклидовы кольца) и рассмотрели два основных примера колец главных идеалов: кольцо целых чисел $\mathbb{Z}$ и кольцо многочленов от одной переменной $K[x]$ над полем K.

Идеалы в $\mathbb{Z}$: $(m) = m\mathbb{Z}$, факторкольца: $\mathbb{Z}/(m) = \mathbb{Z}_m$. С устройство колец вычетов мы уже довольно подробно познакомились, теперь обратимся к изучению факторалгебр алгебры многочленов от одной переменной. Как будет видно далее, их структура очень похожа на структуру колец вычетов (и на структуру факторколец любых колец главных идеалов).

Пусть $f \in K[x],\ deg\ f = n > 0$. Изучим, как устроена факторалгебра $K[x]/(f)$.

Предложение 1. В любом классе вычетов $mod\,(f)$ существует и единственный многочлен степени меньше n.

Доказательство.
Существование: пусть $g \in K[x]$. Поделим g на f с остатком:

$$g = f \cdot q + h, \quad deg\ h < n \text{ (считаем } deg\ 0 = -\infty)$$

Тогда

$$g\ mod\ (f) = h\ mod\ (f).$$

Единственность: пусть

$$h\ mod(f) = \tilde{h}\ mod(f),$$
$$deg\ h < n,\ \ deg\ \tilde{h} < n.$$

Тогда

$$h - \tilde{h} \in (f) \Rightarrow h - \tilde{h} \vdots f \Rightarrow h - \tilde{h} = 0 \Rightarrow h = \tilde{h}$$

■

Доказанное предложение позволяет наглядно представить, как устроена $K[x]/(f)$.

Следствие 1. $K[x]/(f)$ можно отождествить с пространством $K[x]_{<n}$ всех многочленов степени меньше n:

$$g \in K[x]_{<n} \leftrightarrow \bar{g} = g\ mod\ (f)$$

Операции в факторалгебре: $\forall g, h \in K[x]_{<n},\ \forall \lambda \in K$:

$$\bar{g} + \bar{h} = \overline{g + h}$$
$$\lambda \cdot \bar{g} = \overline{\lambda \cdot g}$$
$$\bar{g} \cdot \bar{h} = \bar{r},$$

где r – остаток при делении gh на f.

Следствие 2. $dim\ K[x]/(f) = n$.

Доказательство.
По следствию 1, $K[x]/(f) \simeq K[x]_{<n}$ как векторное пространство. Базис в $K[x]/(f)$:

$$\bar{1},\ \bar{x},\ \bar{x}^2, \dots, \bar{x}^{n-1}.$$

■

Как известно, кольцо вычетов по модулю n является полем тогда и только тогда, когда n – простое. Аналогичное утверждение имеет место и для $K[x]/(f)$.

Предложение 2. $K[x]/(f)$ – поле $\Leftrightarrow f$ неприводим.

Доказательство.
$\Rightarrow$:
От противного: пусть

$$f = g \cdot h, \quad deg\ g, deg\ h < n,$$

тогда

$$\bar{g} \cdot \bar{h} = \bar{0}$$

Но $\bar{g} \neq \bar{0}$ и $\bar{h} \neq \bar{0}$, таким образом, в $K[x]/(\bar{f})$ есть делители нуля, т.е. $K[x]/(f)$ не является полем – противоречие. Значит, f неприводим.

$\Leftarrow$:
Рассмотрим каноническую проекцию:

$$\pi\colon\ K[x] \to K[x]/(f)$$
$$g \mapsto \bar{g}$$

Пусть $I \lhd K[x]/(f)$. Тогда $\pi^{-1}(I) \lhd K[x]$. Но всякий идеал в кольце $K[x]$ является главным, поэтому $\pi^{-1}(I) = (h)$. Но $\pi^{-1}(I)$ содержит, в частности, ядро гомоморфизма π, то есть (f), поэтому

$$\pi^{-1}(I) = (h) \supseteq (f).$$

Это означает, что $f \vdots h$. Но f неприводим, поэтому возможны два случая:

- $h = \lambda \in K^\times \Rightarrow \pi^{-1}(I) = K[x] \Rightarrow I = K[x]/(f)$
- $h = \lambda \cdot f \Rightarrow \pi^{-1}(I) = (f) \Rightarrow I = \{\bar{0}\}$ (так как f – ядро, а I – образ гомоморфизма π)

Следовательно, в $K[x]/(f)$ нет идеалов, отличных от тривиальных, т.е. $K[x]/(f)$ – простое коммутативное ассоциативное кольцо с единицей, т.е. поле (см. теорему 1 прошлой лекции). ■

Пусть A = произвольная ассоциативная алгебра с единицей над K, $a \in A$. Тогда для любого $f \in K[x]$, $f = c_0 + c_1 x + \cdots + c_n x^n$ можно определить $f(a)$:

$$f(a) = c_0 \cdot 1 + c_1 \cdot a + \cdots + c_n \cdot a^n \in A$$

Пример. $A = Mat_n(K) \supseteq C$. Тогда

$$f(C) = c_0 \cdot E + c_1 \cdot C + \cdots + c_n \cdot C^n$$

Эта операция подстановки фиксированного элемента алгебры в многочлен задает φ_a – гомоморфизм вычисления значения многочлена на элементе a:

$$\varphi_a \colon K[x] \to A$$
$$f \mapsto f(a)$$

Его ядро и образ:

$$Im\,(\varphi_a) = K[a] \subseteq A$$
$$Ker\,(\varphi_a) \lhd K[x]$$

$Im\,(\varphi_a)$ – наименьшая подалгебра с единицей, содержащая элемент a, $Ker\,(\varphi_a)$ – идеал аннулирующих многочленов для элемента a.

Определение. Элемент a *алгебраичен* (над K), если $Ker\,(\varphi_a) \neq \{0\}$, т.е. существует ненулевой аннулирующий многочлен $f \in K[x]$: $f(a) = 0$, $deg\, f > 0$. В противном случае элемент a *трансцендентен*.

Если a алгебраичен, то $Ker\,(\varphi_a) = (\mu_a)$, где μ_a – многочлен положительной степени со старшим коэффициентом 1. Многочлен μ_a называется *минимальным многочленом* элемента a.

Свойства минимального многочлена.

1) μ_a – ненулевой аннулирующий многочлен наименьшей степени со старшим коэффициентом 1.
2) μ_a делит все аннулирующие многочлены.
3) μ_a определен однозначно.

Доказательство.
2) $f(a) = 0 \Rightarrow f \in Ker\,(\varphi_a) \Rightarrow f \vdots \mu_a$.

1) $f(a) = 0, f \neq 0 \Rightarrow f \vdots \mu_a \Rightarrow deg\, f \geq deg\, \mu_a$.

3) Пусть $\tilde{\mu}_a$ – другой минимальный многочлен элемента a. Тогда по свойству 1) оба многочлена μ_a и $\tilde{\mu}_a$ имеют одинаковую степень (минимальную среди всех степеней аннулирующих многочленов для элемента a) и старший коэффициент 1. Тогда $\mu_a - \tilde{\mu}_a$

– тоже аннулирующий многочлен: $\mu_a - \tilde{\mu}_a \in Ker\ (\varphi_a), deg\ (\mu_a - \tilde{\mu}_a) < deg\ \mu_a$. Отсюда следует, что $\mu_a - \tilde{\mu}_a = 0$, т.е. $\mu_a = \tilde{\mu}_a$. ■

Примеры минимальных многочленов.

1) Минимальный многочлен матрицы (линейного оператора).

2) $K = \mathbb{Q}$, $A = \mathbb{R}$.
$\sqrt{2} \in \mathbb{R}$ алгебраичен над $\mathbb{Q}$, его минимальный многочлен: $\mu_{\sqrt{2}}(x) = x^2 - 2$,
$e \in \mathbb{R}$ трансцендентно над $\mathbb{Q}$ (результат из теории чисел).

Предложение 3. Любой многочлен $f \in K[x]$ положительной степени со старшим коэффициентом 1 является минимальным многочленом элемента $\bar{x} = x\ mod\ (f)$ алгебры $K[x]/(f)$.

Доказательство.
Для любого $g \in K[x],\ g = c_0 + c_1 x + c_2 x^2 + \cdots$ выполнено:

$$g(\bar{x}) = c_0 \cdot 1 + c_1 \cdot \bar{x} + c_2 \cdot \bar{x}^2 + \cdots = \overline{c_0 + c_1 x + c_2 x^2 + \cdots} = \bar{g}$$

Итак, подставить класс вычетов $\bar{x}$ в многочлен g – это все равно что перейти к классу вычетов многочлена g. Тогда

$$g(\bar{x}) = \bar{0} \Leftrightarrow g \in (f)$$

Следовательно,

$$Ker\ (\varphi_{\bar{x}}) = (f) \Rightarrow f = \mu_{\bar{x}}$$

■

Свойства алгебраических и трансцендентных элементов.

1) a трансцендентен $\Rightarrow K[a] \simeq K[x]$ (трансцендентный элемент можно рассматривать как переменную); a алгебраичен $\Rightarrow K[a] \simeq K[x]/(\mu_a)$.

Доказательство.
По основной теореме о гомоморфизмах колец/алгебр

$$K[a] = Im\ (\varphi_a) \simeq K[x]/Ker\ (\varphi_a)$$

Если a трансцендентен, то $Ker\ (\varphi_a) = \{0\}$ и $K[a] \simeq K[x]$, а если a алгебраичен, то $Ker\ (\varphi_a) = \{\mu_a\}$ и $K[a] \simeq K[x]/(\mu_a)$. ■

2) В конечномерной алгебре A все элементы алгебраичны и $deg\ \mu_a \leq dim\ A$.

Доказательство.

Выберем произвольный элемент $a \in A$ и рассмотрим его степени: $1, a, a^2, \dots, a^n$. Так как алгебра A конечномерна, то полученный набор элементов будет линейно зависим при $n = dim\ A$, т.е. существует нетривиальная линейная комбинация

$$c_0 \cdot 1 + c_1 \cdot a + \cdots + c_n \cdot a^n = 0.$$

Тогда (т.к. $\exists c_i \neq 0$):

$$f = c_0 + c_1 \cdot x + c_2 \cdot x^2 + \cdots + c_n \cdot x^n \neq 0$$

- ненулевой аннулирующий многочлен элемента a. Значит, a алгебраичен и

$$deg\ \mu_a \leq deg\ f \leq n = dim\ A$$

■

3) Если алгебра A не имеет делителей нуля, и $a \in A$ – алгебраический элемент, то его минимальный многочлен μ_a неприводим в $K[x]$ и подалгебра $K[a]$ – поле.

Доказательство.
Если бы μ_a был приводим: $\mu_a = f \cdot g$ $(deg\ f, deg\ g < deg\ \mu_a)$, то имело бы место равенство:

$$f(a) \cdot g(a) = \mu_a(a) = 0,$$

при этом $f(a) \neq 0$ и $g(a) \neq 0$, так как $deg\ f, deg\ g < deg\ \mu_a$. Следовательно, f и g – делители нуля – противоречие. Следовательно, μ_a неприводим в $K[x]$.

По свойству 1) $K[a] \simeq K[x]/(\mu_a)$. А ранее было доказано (см. предложение 2), что факторалгебра по идеалу, порожденному неприводимым многочленом, является полем, следовательно, $K[a]$ – поле. ■

Теорема. Для любого неприводимого многочлена $f \in K[x]$ существует единственное (с точностью до изоморфизма) поле $L \supseteq K$, в котором f имеет корень a, и L не содержит подполей $L \supset M \supseteq K$, содержащих a. При этом $f = \lambda \cdot \mu_a$ $(\lambda \in K^\times)$ и $L = K[a] \simeq K[x]/(f)$.
Говорят, что поле L получается из поля K *присоединением корня* a многочлена f.

Доказательство.
Существование: положим $L = K[x]/(f)$. Поскольку многочлен f неприводим, то из предложения 2 следует, что L является полем, а из предложения 3 следует, что в L многочлен f имеет корень $a = x\ mod\ (f)$.
По построению, любой элемент L имеет вид $g\ mod\ (f) = g(a)$ (см. предложение 3). Следовательно, $L = K[a]$. Отсюда сразу следует, что нет промежуточных подполей, содержащих a (так как $K[a]$ – наименьшая подалгебра с единицей, содержащая a).

Теперь докажем, что $f = \lambda \cdot \mu_a$ $(\lambda \in K^\times)$. По условию, многочлен f является аннулирующим для a, поэтому $f \vdots \mu_a$. Но f неприводим, поэтому $f = \lambda \cdot \mu_a$ $(\lambda \in K^\times)$.

Единственность: рассмотрим гомоморфизм вычисления значения многочлена на элементе a:

$$\varphi_a\colon K[x] \to L$$
$$f \mapsto f(a)$$

Его ядро

$$Ker\,(\varphi_a) = (\mu_a) = (f)$$

– идеал, порожденный f.
Отсюда следует, что

$$M = Im\,(\varphi_a) = K[a] \simeq K[x]/(f)$$

- поле, так как f неприводим (см. предложение 2). Итак, $L \supseteq M \supseteq K$, $a \in M$ – получили промежуточное поле, содержащее a. Но в силу минимальности расширения L получаем, что $L = M \simeq K[x]/(f)$. ■

Пример. $\mathbb{C} = \mathbb{R}[i] \simeq \mathbb{R}[x]/(x^2+1)$ – все комплексные числа являются значениями многочленов с вещественными коэффициентами на элементе i (достаточно взять многочлены первой степени – следует из алгебраической формы записи комплексных чисел).
Воспользуемся тем, что

$$\mathbb{R}[x]/(x^2+1) \simeq \mathbb{R}[x]_{<1}$$

при этом

$$i \leftrightarrow \bar{x} = x\ mod\ (x^2+1)$$
$$\alpha + \beta i \leftrightarrow \alpha \cdot \bar{1} + \beta \cdot \bar{x} \leftrightarrow \alpha + \beta x$$

Т.е. можно считать, что комплексные числа – это многочлены с действительными коэффициентами степени не выше 1, при этом складывать и умножать на числа их можно как обычные многочлены, а произведение нужно рассматривать по модулю x^2+1.

Теория полей.

Терминология: пусть L – поле, $L \supseteq K$ – подполе. Говорят, что L – *расширение* поля K. В этом случае L – векторное пространство (и даже алгебра) над K.

Определение. Расширение полей $L \supseteq K$ называется конечным, если L конечномерно над K. *Степень* расширения $(L\colon K) = dim_K L$.

Примеры.

1) $\mathbb{C} \supset \mathbb{R}$ - конечное расширение, $(\mathbb{C}\colon \mathbb{R}) = 2$. Базис: $1, i$.

2) $\mathbb{R} \supset \mathbb{Q}$ - бесконечное расширение. В самом деле, для любого конечного расширения $L \supset \mathbb{Q}$ выполнено $L \simeq \mathbb{Q}^n$, $n = (L\colon \mathbb{Q})$ (здесь под изоморфизмом понимается изоморфизм векторных пространств, а не полей). Но L счетно, а $\mathbb{R}$ - нет.

3) Пусть $M \supseteq K$ – расширение полей, элемент $a \in M$ – алгебраический над полем K. Тогда $L = K[a]$ – поле, и $L \supset K$ – конечное расширение. При этом $(L{:}\,K) = deg\ \mu_a$.

В самом деле: так как M – поле, то в M нет делителей нуля, поэтому μ_a неприводим. Следовательно, алгебра $L \simeq K[x]/(\mu_a)$ – поле, и $dim\ L = deg\ \mu_a$.

4) Обратно, если $L \supseteq K$ – конечное расширение полей, тогда любой $a \in L$ алгебраичен над K (по свойству 2 алгебраических элементов).

Лекция 21. Теория полей. Часть 1.

На прошлой лекции мы ввели понятие конечного расширения полей. Докажем, что свойство конечности передается “по цепочке”.

Теорема о башне расширений. Пусть $K \subset L \subset M$ – расширения полей. Тогда расширение $M \supset K$ конечно тогда и только тогда, когда $L \supset K$ и $M \supset L$ конечны. При этом $(M:K) = (M:L) \cdot (L:K)$.

Доказательство.
$\Rightarrow$:
Пусть $M \supset K$ конечно и $\mu_1, \dots, \mu_n$ порождают M как векторное пространство над K. Но тогда $\mu_1, \dots, \mu_n$ тем более порождают M как векторное пространство над L. Другими словами, $(M:L) \leq (M:K)$. Но $(M:K)$ конечно, значит, и $(M:L)$ конечно.

$L \subseteq M$ – векторное подпространство над K, поэтому $(L:K) \leq (M:K)$. Следовательно, $(L:K)$ конечно (так как $(M:K)$ конечно).

$\Leftarrow$:
Пусть $L \supset K$ и $M \supset L$ конечны, и $e_1, \dots, e_m$ – базис M над L, а $f_1, \dots, f_l$ – базис L над K. Тогда для любого $\mu \in M$ существуют $\lambda_1, \dots, \lambda_m \in L$:

$$\mu = \lambda_1 e_1 + \dots + \lambda_m e_m$$

Каждый из коэффициентов λ_i, в свою очередь, разлагается в линейную комбинацию $f_1, \dots, f_l$, с коэффициентами из K (как элемент поля L): $\forall i = 1, \dots, m \ \ \exists \alpha_{i1}, \dots, \alpha_{il} \in K$:

$$\lambda_i = \alpha_{i1} f_1 + \dots + \alpha_{il} f_l$$

Тогда

$$\mu = \sum_i \lambda_i e_i = \sum_{i,j} \alpha_{ij} f_j e_i$$

Таким образом, всевозможные попарные произведения $e_i f_j$ $(i = 1, \dots, m, \quad j = 1, \dots, l)$ порождают M как векторное пространство над K. Докажем, что они являются линейно независимыми над полем K.

Линейная независимость: пусть

$$\sum_{i,j} \beta_{ij} e_i f_j = 0, \ \ \beta_{ij} \in K.$$

Перепишем это равенство как:

$$\sum_{i,j} \beta_{ij} e_i f_j = \sum_i \left(\sum_j \beta_{ij} f_j \right) e_i = 0$$

Поскольку $e_1, \dots, e_m$ линейно независимы над L, а коэффициенты $\sum_j \beta_{ij} f_j$ – элементы поля L, то $\forall i$:

$$\sum_j \beta_{ij} f_j = 0$$

Но $\beta_{ij} \in K$, а $f_1, \dots, f_l$ линейно независимы над K, следовательно, $\forall i, j\colon \beta_{ij} = 0$.

Итак, мы доказали, что $e_i f_j$ $(i = 1, \dots, m, \quad j = 1, \dots, l)$ линейно независимы над K, следовательно, $e_i f_j$ образуют базис M как векторного пространства над K. Отсюда следует, что:
во-первых, расширение $M \supset K$ конечно,
во-вторых, $(M\colon K) = m \cdot l = (M\colon L) \cdot (L\colon K)$. ■

Следствие. Пусть $K_0 \subseteq K_1 \subseteq \dots \subseteq K_s$ – башня расширений полей. Тогда расширение $K_0 \subseteq K_s$ конечно тогда и только тогда, когда $K_{i-1} \subseteq K_i$ конечны, $\forall i = 1, \dots, s$. При этом

$$(K_s\colon K_0) = (K_s\colon K_{s-1}) \cdot (K_{s-1}\colon K_{s-2}) \cdot \dots \cdot (K_1\colon K_0).$$

Доказательство – индукцией по s.

Наряду с конечными расширениями в теории полей рассматриваются конечно порожденные расширения.

Определение. Пусть $K \subseteq L$ – расширение полей и $a_1, \dots, a_n \in L$. Расширение поля K, порожденное элементами $a_1, \dots, a_n$ – это наименьшее подполе $M \subseteq L$, такое что $M \supseteq K$ и $M \ni a_1, \dots, a_n$ (иными словами, это пересечение всех подполей, содержащих K и $a_1, \dots, a_n$). Обозначение: $M = K(a_1, \dots, a_n)$.

Конструктивное описание:

$$K(a_1, \dots, a_n) = \left\{ \frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)} \mid f, g \in K[x_1, \dots, x_n],\ \ g(a_1, \dots, a_n) \neq 0 \right\}$$

Терминология: говорят, что расширение $K(a_1, \dots, a_n)$ – конечно порожденное расширение поля K, получаемое *присоединением* элементов $a_1, \dots, a_n$ к полю K.

Рассмотрим случай расширения, порожденного одним элементом.

Предложение 1. Пусть $K \subseteq L$ – расширение полей, $a \in L$. Тогда:
а) если a алгебраичен над K, то $K(a) = K[a] \simeq K[x]/(\mu_a)$,
б) если a трансцендентен над K, то $K(a) \simeq K(x)$, где $K(x)$ – поле рациональных дробей от одной переменной.

Доказательство.
а) Ясно, что $K(a) \supseteq K[a] \simeq K[x]/(\mu_a)$ (включение $\supseteq$ верно, так как $K(a)$ состоит из всех рациональных дробей на элементе a, а $K[a]$ состоит из всех многочленов на элементе a; изоморфность $K[a]$ и $K[x]/(\mu_a)$ мы доказали ранее – см. теорему лекции 20). При этом $K[x]/(\mu_a)$ – поле, так как μ_a неприводим.

Тогда $K[a]$ – поле, которое содержит поле K и элемент a, поэтому $K[a] \supseteq K(a)$, так как $K(a)$ – наименьшее поле, удовлетворяющее этим свойствам. Следовательно, $K(a) = K[a]$.

б) Докажем, что отображение

$$\begin{gathered} K(x) \to K(a) \\ \frac{f}{g} \mapsto \frac{f(a)}{g(a)} \end{gathered}$$

взаимно-однозначно (заметим, что так определенное отображение корректно, так как в силу трансцендентности a, $g(a) \neq 0$).
Пусть

$$\frac{f_1(a)}{g_1(a)} = \frac{f_2(a)}{g_2(a)},$$

тогда

$$f_1(a) \cdot g_2(a) = f_2(a) \cdot g_1(a)$$

Но $K[a] \simeq K[x]$ (см. свойство 1 алгебраических и трансцендентных элементов, доказанное на прошлой лекции). Поэтому

$$f_1 \cdot g_2 = f_2 \cdot g_1 \Rightarrow \frac{f_1}{g_1} = \frac{f_2}{g_2}$$

Следовательно, отображение $K(x) \to K(a)$ инъективно, а его сюръективность очевидна. Поэтому $K(a) \simeq K(x)$. ■

Из только что доказанного предложения видно, что при присоединении к полю алгебраического элемента получается конечное расширение, а при присоединении трансцендентного элемента – бесконечное расширение. Это наблюдение обобщается на случай присоединения к полю нескольких элементов.

Предложение 2. Конечно порожденное расширение $K(a_1, \dots, a_n) \supseteq K$ конечно тогда и только тогда, когда $a_1, \dots, a_n$ алгебраичны над K (иными словами, конечные расширения – то же самое, что и конечно порожденные расширения, которые порождены конечным числом алгебраических элементов).

Доказательство.
$\Rightarrow$:
$\forall i = 1, \dots, n$ рассмотрим

$$K(a_1, \dots, a_n) \supseteq K(a_i) \supseteq K$$

По теореме о башне расширений, $(K(a_i) : K) \leq (K(a_1, \dots, a_n) : K)$. Отсюда следует, что $(K(a_i) : K) < \infty$ (так как $(K(a_1, \dots, a_n) : K) < \infty$). Следовательно, $K(a_i) \supseteq K$ – конечное расширение. Тогда по предложению 1, a_i алгебраичен над K.

⇐:
Пусть $a_1, \dots, a_n$ алгебраичны над K. Рассмотрим башню расширений:

$$K \subseteq K(a_1) \subseteq K(a_1, a_2) \subseteq \cdots \subseteq K(a_1, \dots, a_n)$$

Каждый a_i алгебраичен над K, и тем более алгебраичен над $K(a_1, \dots, a_{i-1})$, т.е. на каждом шаге мы присоединяем алгебраический элемент. Тогда по предложению 1, все расширения $K(a_1, \dots, a_{i-1}) \subseteq K(a_1, \dots, a_i)$ конечны. Поэтому (по следствию из теоремы о башне расширений), $K \subseteq K(a_1, \dots, a_n)$ – конечное расширение. ■

Теорема 1. Пусть $K \subseteq L$ – расширение полей. Все элементы L, алгебраичные над K, образуют подполе $\overline{K} \subseteq L$, называемое *алгебраическим замыканием* поля K в L. При этом $\overline{\overline{K}} = \overline{K}$.

Доказательство.
Пусть $a, b \in \overline{K}$. Рассмотрим расширение поля K, порожденное этими элементами: $K(a, b) \supseteq K$ – конечное расширение (по предложению 2). В $K(a, b)$ содержатся элементы $a \pm b$, $a \cdot b$, a/b (если $b \neq 0$), следовательно, $a \pm b$, $a \cdot b$, a/b (если $b \neq 0$) являются алгебраическими над K, т.е. лежат в $\overline{K}$. Это и означает, что $\overline{K}$ – подполе.

Докажем, что $\overline{K}$ алгебраически замкнуто. Пусть $c \in \overline{\overline{K}}$, т.е. c – корень некоторого многочлена с коэффициентами из $\overline{K}$:

$$f = c_0 + c_1 x + \cdots + c_n x^n, \quad c_0, \dots, c_n \in \overline{K}$$

Рассмотрим башню расширений:

$$K \subseteq K(c_0, \dots, c_n) \subseteq K(c_0, \dots, c_n, c)$$

Оба расширения $K \subseteq K(c_0, \dots, c_n)$ и $K(c_0, \dots, c_n) \subseteq K(c_0, \dots, c_n, c)$ будут конечны (по предложению 2). Тогда по теореме о башне расширений, расширение $K \subseteq K(c_0, \dots, c_n, c)$ также будет конечным, следовательно, $c \in \overline{K}$. ■

Определение. Число $a \in \mathbb{C}$ называется *алгебраическим*, если a алгебраично над $\mathbb{Q}$. Число $a \in \mathbb{C}$ называется *трансцендентным*, если a трансцендентно над $\mathbb{Q}$.

Поле (всех) алгебраических чисел $\overline{\mathbb{Q}}$ - подполе в $\mathbb{C}$.

Теорема 2. Поле алгебраических чисел $\overline{\mathbb{Q}}$ счетно.

Доказательство.
Множество алгебраических чисел – это объединение множеств комплексных корней всех многочленов положительной степени с рациональными коэффициентами:

$$\overline{\mathbb{Q}} = \bigcup_{\substack{f \in \mathbb{Q}[x], \\ deg\, f > 0}} \{ a \in \mathbb{C} \mid f(a) = 0 \}$$

Каждое из этих множеств конечно, а множество всех многочленов положительной степени с рациональными коэффициентами можно представить в виде объединения пространств многочленов степени не выше данной:

$$\mathbb{Q}[x] = \bigcup_{n=0}^{\infty} \mathbb{Q}\,[x]_{\leq n}$$

Каждое из пространств $\mathbb{Q}[x]_{\leq n}$ как векторное пространство изоморфно $\mathbb{Q}^{n+1}$, поэтому $\mathbb{Q}[x]_{\leq n}$ – счетное множество для $\forall n$. Так как счетное объединение счетных множеств счетно, то и $\mathbb{Q}[x]$ также будет счетным множеством. Тогда и $\overline{\mathbb{Q}}$ будет счетным множеством (как счетное объединение конечных множеств). ■

Следствие. Существуют трансцендентные числа. Их подавляющее большинство (так как $\overline{\mathbb{Q}}$ счетно, а $\mathbb{C}$ несчетно, то $\mathbb{C} \backslash \overline{\mathbb{Q}}$ несчетно).

Замечание. Пусть $K \subseteq L$ – расширение полей, L алгебраически замкнуто. Тогда $\overline{K}$ тоже алгебраически замкнуто: любой многочлен положительной степени с коэффициентами из $\overline{K}$ можно рассматривать как многочлен с коэффициентами из L – он имеет корень $a \in L$. Но поскольку $\overline{K}$ алгебраически замкнуто в L (по теореме 1), то $a \in \overline{K}$.
В этом случае $\overline{K}$ – минимальное алгебраически замкнутое расширение поля K. Оно называется *алгебраическим замыканием* поля K.

Примеры алгебраических замыканий.

1) Поле алгебраических чисел $\overline{\mathbb{Q}}$ - алгебраическое замыкание поля $\mathbb{Q}$.

2) $\mathbb{C}$ - алгебраическое замыкание поля $\mathbb{R}$

Теорема. У любого поля существует единственное с точностью до изоморфизма алгебраическое замыкание.

Мы не будем доказывать эту теорему, на практике обычно достаточно более слабого утверждения (см. теорему 3).

Определение. Пусть K – поле, $f \in K[x]$, $deg\ f > 0$. *Поле разложения* многочлена f над полем K – это такое расширение $F \supseteq K$, для которого f разлагается на линейные множители над F и не существует промежуточных подполей $F \supset M \supset K$ с тем же свойством.

Теорема 3. Для любого многочлена $f \in K[x]$, $deg\ f > 0$ существует единственное с точностью до изоморфизма поле разложения f над K.

Доказательство.
Существование. Построим башню расширений

$$L_0 \subseteq L_1 \subseteq \cdots \subseteq L_i \subseteq L_{i+1} \subseteq \cdots,$$

где $L_0 = K,\ L_i = K(a_1, \dots, a_i), \dots$ так, чтобы на каждом шаге

$$f(x) = (x - a_1) \cdot \dots \cdot (x - a_i) \cdot f_i(x) \text{ над } L_i$$

Докажем, что это можно сделать, индукцией по i, начиная с $i = 0$.

База индукции: $L_0 = K$, $f_0 = f$.
Шаг индукции: если f_i разлагается на линейные множители над L_i, то построение закончено. Иначе $f_i = p_i \cdot q_i$, где p_i неприводим над L_i, $deg\ p_i > 1$. Присоединим корень:

$$L_{i+1} = L_i(a_{i+1}), \text{ где } p_i(a_{i+1}) = 0$$

Присоединив корень, мы выделим в p_i, а значит и в f_i еще один линейный множитель $(x - a_{i+1})$ и продолжим построение башни расширений.

Так как степень многочлена конечна, то рано или поздно мы дойдем до поля $F = K(a_1, \dots, a_n)$, над которым f разлагается на линейные множители. Это и будет поле разложения многочлена f (по построению).

Единственность. Пусть $\tilde{F}$ – другое поле разложения. Построим изоморфизм $\varphi\colon\ F \to \tilde{F}$ по цепочке: из доказательства существования поля разложения f следует существование башни расширений

$$L_0 \subseteq L_1 \subseteq \cdots \subseteq L_i \subseteq L_{i+1} \subseteq \cdots \subseteq F$$

Тогда $\varphi_0 = id$ – тождественное вложение поля $L_0 = K$ в $\tilde{F}$. Продолжим φ_0 на L_1, затем на L_2 и т.д. по индукции. Пусть уже построено

$$\varphi_i\colon\ L_i \twoheadrightarrow \tilde{L}_i \subseteq \tilde{F}$$
$$a \mapsto \varphi_i(a) = \tilde{a}$$

Тогда каждому многочлену $g(x) = c_0 + c_1x + \cdots + c_mx^m \in L_i[x]$ можно поставить в соответствие многочлен с коэффициентами из $\tilde{L}_i$, заменив коэффициенты многочлена $g(x) \in L_i[x]$ на их образы при изоморфизме: $\tilde{g}(x) = \tilde{c}_0 + \tilde{c}_1x + \cdots + \tilde{c}_mx^m \in \tilde{L}_i[x]$. Таким образом,

$$L_i[x] \twoheadrightarrow \tilde{L}_i[x]$$

Над L_i:

$$f(x) = (x - a_1) \cdot \ldots \cdot (x - a_i) \cdot f_i(x),$$

$f_i = p_i \cdot q_i$, где p_i неприводим над L_i, $deg\ p_i > 1$. В силу изоморфизма полей, то же самое разложение имеет место и в $\tilde{L}_i$: многочлен $\tilde{p_i}$ неприводим над $\tilde{L}_i$. Но так как $\tilde{F}$ – поле разложения, то $\tilde{p_i}$ имеет корень $\tilde{a}_{i+1} \in \tilde{F}$. Присоединим $\tilde{a}_{i+1}$ к $\tilde{L}_i$: положим

$$\tilde{L}_{i+1} = \tilde{L}_i(\tilde{a}_{i+1})$$

Но $\tilde{L}_i(\tilde{a}_{i+1}) \simeq L_i(a_{i+1})$, так как расширения поля, получаемые присоединением корня данного неприводимого многочлена изоморфны друг другу. Так как $L_i(a_{i+1}) = L_{i+1}$, то мы построили изоморфизм:

$$\varphi_{i+1}\colon\ L_{i+1} \twoheadrightarrow \tilde{L}_{i+1}$$

В итоге построим вложение полей:

$$\varphi\colon\ F \hookrightarrow \tilde{F}$$

Данное вложение будет являться изоморфизмом, так как $Im\,\varphi \simeq F$ – подполе $\tilde{F}$, над которым f разлагается на линейные множители. Из минимальности следует, что $Im\,\varphi = \tilde{F}$, то есть, $F \simeq \tilde{F}$. ■

Лекция 22. Теория полей. Часть 2.

Определение. Простое поле – это поле K, в котором не содержится меньших подполей $L \subset K$.

Замечание. В каждом поле K содержится единственное простое подполе $K_0 \subseteq K$, которое является пересечением всех подполей в K.

Предложение 1. Пусть K – простое поле, $char\ K = p$.
а) если $p = 0$, то $K \simeq \mathbb{Q}$,
б) если $p > 0$, то $K \simeq \mathbb{Z}_p$.

Доказательство.
Рассмотрим гомоморфизм

$$\varphi\colon \mathbb{Z} \to K$$

$$\varphi(n) = \begin{cases} 1 + \cdots + 1, & n > 0 \\ (-1) + \cdots + (-1), & n < 0 \\ 0, & n = 0 \end{cases}$$

Его ядро:

$$Ker\ \varphi = p\mathbb{Z}$$

а) если $p = 0$, то $Ker\ \varphi = \{0\}$ и φ инъективен. Продолжим φ до гомоморфизма $\mathbb{Q} \to K$ по правилу:

$$\varphi\left(\frac{m}{n}\right) = \frac{\varphi(m)}{\varphi(n)}$$

Нужно проверить корректность, так как разные дроби могут соответствовать одному и тому же рациональному числу. Проверим одновременно корректность и инъективность данного отображения: пусть

$$\frac{m_1}{n_1} = \frac{m_2}{n_2} \Leftrightarrow m_1 \cdot n_2 = m_2 \cdot n_1$$

Поскольку гомоморфизм φ на целых числах инъективен, то

$$m_1 \cdot n_2 = m_2 \cdot n_1 \Leftrightarrow \varphi(m_1 \cdot n_2) = \varphi(m_2 \cdot n_1) \Leftrightarrow \varphi(m_1) \cdot \varphi(n_2) = \varphi(m_2) \cdot \varphi(n_1) \Leftrightarrow$$

$$\Leftrightarrow \frac{\varphi(m_1)}{\varphi(n_1)} = \frac{\varphi(m_2)}{\varphi(n_2)}$$

Это одновременно доказывает корректность и инъективность φ. Следовательно, $\mathbb{Q} \simeq \varphi(\mathbb{Q})$ – подполе в K. Но поскольку K простое, то $\varphi(\mathbb{Q}) = K$.

б) если $p > 0$, то $Ker\ \varphi = p\mathbb{Z}$. По основной теореме о гомоморфизмах,

$$\varphi(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$$

Так как p простое (как характеристика поля), то $\mathbb{Z}_p$ – поле. Тогда $\varphi(\mathbb{Z})$ – подполе в K, но поскольку K простое, то $\varphi(\mathbb{Z}) = K$. ■

Следствие. Любое поле K содержит подполе, изоморфное $\mathbb{Q}$ (если $char\ K = 0$) или изоморфное $\mathbb{Z}_p$ (если $char\ K = p > 0$).

Без ограничения общности, можно считать, что любое поле K содержит $\mathbb{Q}$ или $\mathbb{Z}_p$.

Конечные поля.

Предложение 2. Пусть F – конечное поле. Тогда $char\ F = p > 0$, p – простое, и $|F| = p^n$ для некоторого $n \in \mathbb{N}$.

Доказательство.
Так как F конечно, то $F \not\supseteq \mathbb{Q}$, следовательно, $char\ F = p > 0$, p – простое, и $F \supseteq \mathbb{Z}_p$ (по следствию из предложения 1). Так как F конечно, то $F \supseteq \mathbb{Z}_p$ – конечное расширение полей. Обозначим $(F: \mathbb{Z}_p) = n$. Тогда

$$F \simeq \left(\mathbb{Z}_p\right)^n$$

как векторное пространство над $\mathbb{Z}_p$ – этот изоморфизм задается выбором базиса в F над полем $\mathbb{Z}_p$. Следовательно,

$$|F| = \left|\left(\mathbb{Z}_p\right)^n\right| = p^n$$

■

Отметим, что поля положительной характеристики p (к которым, в частности, относятся все конечные поля) обладают одним необычным свойством – в таких полях операция возведения в степень p является гомоморфизмом (т.е. переводит не только произведение в произведение, но и сумму в сумму). Этот гомоморфизм называется гомоморфизмом (эндоморфизмом) Фробениуса.

Определение. Пусть K – поле, $char\ K = p > 0$. *Эндоморфизм Фробениуса* Φ: $K \to K$ задается формулой:

$$\Phi(x) = x^p$$

Назван так в честь выдающегося немецкого математика Фердинанда Фробениуса (F.G. Frobenius, 1849-1917).

Убедимся, что Φ – гомоморфизм:

$$\Phi(x \cdot y) = (x \cdot y)^p = x^p \cdot y^p = \Phi(x) \cdot \Phi(y)$$

$$\Phi(x + y) = (x + y)^p = x^p + \cdots + C_p^k x^{p-k} y^k + \cdots + y^p$$

Заметим, что

$$C_p^k = \frac{p!}{k!\,(p-k)!} \vdots p \text{ при } 0 < k < p$$

Отсюда вытекает, что сумма C_p^k единиц в поле K равна нулю. Тогда

$$C_p^k x^{p-k} y^k = (1 + \cdots + 1) x^{p-k} y^k = 0 \text{ при } 0 < k < p$$

и

$$\Phi(x + y) = (x + y)^p = x^p + y^p = \Phi(x) + \Phi(y)$$

Итак, Φ – гомоморфизм. Поскольку K – поле, то $Ker\ \Phi = \{0\}$, т.е. Φ инъективен. А если K – конечное поле, то Φ – автоморфизм (так как инъективное отображение конечного множества в себя является также и сюръективным).

Теорема (основная теорема о структуре конечных полей). Для любого простого числа p и $n \in \mathbb{N}$ существует единственное (с точностью до изоморфизма) конечное поле F, порядок которого равен p^n.
Обозначение: $F = \mathbb{F}_q$ – *поле Галуа*, где $q = p^n$.

Пример: $\mathbb{F}_p = \mathbb{Z}_p$.

Доказательство.
Единственность (как часто бывает, из доказательства единственности станет понятно, как доказать существование).
Так как $|F| = p^n$, то $char\ F = p$, следовательно, $F \supseteq \mathbb{Z}_p$.
$|F^\times| = q - 1$, тогда по теореме Лагранжа $\forall a \in F^\times$ выполнено $a^{q-1} = 1$. Домножив это равенство на a, получим, что $\forall a \in F$ выполнено $a^q = a$.

Рассмотрим многочлен

$$f(x) = x^q - x \in \mathbb{Z}_p[x]$$

- он имеет в F q различных корней (все элементы поля F) и его степень равна q, следовательно, $f(x)$ разлагается в произведение q линейных множителей:

$$f(x) = \prod_{a \in F} (x - a)$$

Отсюда следует, что F – поле разложения для f над $\mathbb{Z}_p$. Оно единственно с точностью до изоморфизма.

Существование.
Пусть L – поле разложения для $f(x) = x^q - x$ над $\mathbb{Z}_p$, и $L \supseteq F$ – множество корней f в L. Заметим, что $\forall a \in L$:

$$a^q = a^{p^n} = \Phi^n(a)$$

- тоже гомоморфизм, т.е. $\forall a, b \in L$:

$$(a \pm b)^q = a^q \pm b^q$$
$$(a \cdot b)^q = a^q \cdot b^q$$
$$\left(\frac{a}{b}\right)^q = \frac{a^q}{b^q} \text{ (при } b \neq 0)$$

Следовательно, $F = \{a \in L \mid a^q = a\}$ – подполе в L. Оно содержит все корни многочлена f, значит, f разлагается в F на линейные множители. Из минимальности поля разложения вытекает, что $F = L$.

Осталось понять, сколько в F элементов. Заметим, что так как $q = 0$ в $\mathbb{Z}_p$, то производная многочлена $f(x) = x^q - x$ постоянна:

$$f'(x) = q \cdot x^{q-1} - 1 = -1$$

Это, в частности, означает, что f и f' взаимно просты, то есть, f не имеет кратных корней. Так как f разлагается на линейные множители над F, то f имеет q различных корней в F. Но F – это множество корней f в L, следовательно, $|F| = q$. ■

Отметим, что на практике построение конечного поля как поля разложения многочлена не очень удобно (из-за необходимости построения башни расширений). Гораздо удобнее присоединять корень одного неприводимого многочлена к исходному полю (используя конструкцию факторалгебры по идеалу, порожденному этим неприводимым многочленом). Возникает вопрос – можно ли любое конечное поле построить с помощь такой конструкции (для этого нужно, чтобы для любого n существовал неприводимый многочлен степени n над $\mathbb{Z}_p$). Оказывается, такой многочлен всегда существует.

Предложение 3. Для любого $n \in \mathbb{N}$ существует неприводимый многочлен степени n в $\mathbb{Z}_p[x]$.

Доказательство.
Рассмотрим мультипликативную группу поля Галуа $\mathbb{F}_{p^n}^\times$. Это циклическая группа (как мультипликативная группа конечного поля). Пусть $a \in \mathbb{F}_{p^n}^\times$ - некоторый порождающий элемент. Тогда

$$\mathbb{F}_{p^n}^\times = \mathbb{Z}_p[a] \simeq \mathbb{Z}_p[x]/(\mu_a).$$

μ_a неприводим над $\mathbb{Z}_p$ и

$$\deg \mu_a = (\mathbb{F}_{p^n} : \mathbb{Z}_p) = n$$

Итак, в качестве неприводимого многочлена степени n в $\mathbb{Z}_p[x]$ можно взять минимальный многочлен порождающего элемента $\mathbb{F}_{p^n}^{\times}$. ■

Теперь можно предложить следующую конструкцию построения поля из n элементов.

Конструкция построения поля из n элементов:

$$\mathbb{F}_{p^n} = \mathbb{Z}_p[x]/(g),$$

где g – неприводимый многочлен степени n.

Так как $\mathbb{Z}_p[x]/(g) \simeq \mathbb{Z}_p[x]_{<n}$ как векторное пространство над $\mathbb{Z}_p$, то можно рассматривать модель $\mathbb{F}_{p^n}$ как множество всех многочленов степени меньше n над полем $\mathbb{Z}_p$ с обычной операцией сложения и операцией умножения, которая ставит в соответствие двум таким многочленам остаток, получающийся при делении их произведения на g.

Пример. Построим поле $\mathbb{F}_4$.
Рассмотрим $\mathbb{Z}_2[x]$ и найдем в нем неприводимые многочлены второй степени. В $\mathbb{Z}_2[x]$ не так много многочленов второй степени: это

$$x^2, \quad x^2 + \bar{1}, \quad x^2 + x, \quad x^2 + x + \bar{1}$$

Многочлен x^2 имеет корень $\bar{0}$, многочлен $x^2 + \bar{1}$ имеет корень $\bar{1}$, многочлен $x^2 + \bar{1}$ имеет корни $\bar{0}$ и $\bar{1}$. Многочлен $x^2 + x + \bar{1}$ корней не имеет – он неприводим. Тогда

$$\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2 + x + \bar{1}) \simeq \mathbb{Z}_2[x]_{<n} = \{\bar{0},\ \bar{1},\ x,\ x + \bar{1}\}$$

Операции:

$$\bar{1} + \bar{1} = \bar{0}$$
$$x + x = \bar{0}$$
$$x \cdot x = x + \bar{1}$$
$$x \cdot (x + \bar{1}) = \bar{1}$$
$$(x + \bar{1}) \cdot (x + \bar{1}) = x,$$

остальные операции как для многочленов.

Предложение 4. Поле $\mathbb{F}_q$ содержит подполе $F \simeq \mathbb{F}_r$ тогда и только тогда, когда $q = p^n$, $r = p^m$ и $n \vdots m$. При этом такое подполе F единственно.

Доказательство.
⇒:
Пусть $\mathbb{F}_q$ содержит $F \simeq \mathbb{F}_r$. Так как $\mathbb{F}_q$ конечно, то оно является расширением F.

Обозначим $(\mathbb{F}_q : F) = d$. Тогда $\mathbb{F}_q \simeq F^d$ как векторное пространство над F. Отсюда, в частности, следует, что

$$\left|\mathbb{F}_q\right| = |F|^d \Rightarrow q = r^d$$

Так как r – количество элементов в $\mathbb{F}_r$, то $r = p^m$, тогда $q = r^{md}$.

$\Leftarrow$:
Пусть $n = m \cdot d$, тогда $q = r^d$. Отсюда следует, что $q - 1$ делится на $r - 1$:

$$q - 1 = r^d - 1 = (r - 1)(r^{d-1} + r^{d-2} + \cdots + r + 1)$$

Для краткости обозначим $r^{d-1} + r^{d-2} + \cdots + r + 1 = s$ и рассмотрим многочлен $x^q - x$:

$$x^q - x = x(x^{q-1} - 1) = x\left(x^{(r-1)s} - 1\right) =$$

$$= x(x^{r-1} - 1)\left(x^{(r-1)(s-1)} + x^{(r-1)(s-2)} + \cdots + x^{r-1} + 1\right) =$$

$$= (x^r - x)\left(x^{(r-1)(s-1)} + x^{(r-1)(s-2)} + \cdots + x^{r-1} + 1\right)$$

То есть, $x^q - x$ делится на $x^r - x$. Рассмотрим поле $\mathbb{F}_q$ – оно является полем разложения для многочлена $x^q - x$, но тогда $\mathbb{F}_q$ содержит и поле разложения F для $x^r - x$. Но $F \simeq \mathbb{F}_r$, также F состоит из всех корней многочлена $x^r - x$, откуда вытекает единственность F. ■

Лекция 23. Конечномерные алгебры.

Перейдем от изучения полей к телам и алгебрам, которые является телами, т.е. к алгебрам с делением. Принципиальной разницы между телом и алгеброй с делением нет, поскольку любое тело можно рассматривать как алгебру с делением над своим центром.

Определение. Пусть A – ассоциативное кольцо/алгебра с единицей над полем K. Его *центр* – это множество элементов, коммутирующих со всеми остальными:

$$Z(A) = \{a \in A \mid ab = ba, \ \ \forall b \in A\}$$

Предложение 1.
а) $Z(A)$ – подкольцо/подалгебра с единицей,
б) если A – тело, то $Z(A)$ – поле.

Доказательство.
а) Очевидно, что $Z(A) \ni 1$. Далее, если $a, a' \in A$, то $\forall b \in A$:

$$(a \pm a')b = ab \pm a'b = ba \pm ba' = b(a \pm a') \ \ \Rightarrow \ \ a \pm a' \in Z(A)$$

$$(aa')b = a(a'b) = a(ba') = (ab)a' = (ba)a' = b(aa') \ \ \Rightarrow \ \ aa' \in Z(A)$$

Таким образом, $Z(A)$ – подкольцо с единицей. Для случая алгебр: $\forall \lambda \in K$:

$$(\lambda a)b = \lambda(ab) = \lambda(ba) = b(\lambda a) \ \ \Rightarrow \ \ \lambda a \in Z(A)$$

б) Если A – тело, то убедимся, что вместе с каждым элементом a в $Z(A)$ лежит и a^{-1}. Если $a \in Z(A)$, то $\forall b \in A$:

$$ab = ba$$

Домножим это равенство слева и справа на a^{-1} $(a \neq 0)$, получим:

$$ba^{-1} = a^{-1}b$$

Таким образом, элемент a^{-1} также перестановочен с $\forall b \in A$, то есть, $a^{-1} \in Z(A)$. ■

Следствие. Всякое тело является алгеброй с делением над своим центром.

Пусть A – ассоциативная алгебра с единицей над полем K. Тогда очевидно, что $Z(A)$ содержит подалгебру, изоморфную полю K: $Z(A) \supseteq K \cdot 1 \simeq K$, где 1 – единица в A, т.е. можно считать, что A содержит K в качестве подполя. Алгебры, центр которых состоит только из поля K, называются центральными.

Определение. Пусть A – ассоциативная алгебра с единицей над полем K. Алгебра A называется *центральной*, если $Z(A) = K$.

Примеры центральных алгебр.

1) Алгебра $Mat_n(K)$ центральна (см. также лекция 9, пример 2).

Доказательство.
Пусть $C \in Z(Mat_n(K))$, тогда C должна коммутировать со всеми матрицами из $Mat_n(K)$ – достаточно проверить это для матричных единиц: $\forall i, j = 1, \dots, n$:

$$C \cdot E_{ij} = E_{ij} \cdot C$$

Но

$$C \cdot E_{ij} = \sum_{k,l} c_{kl} E_{kl} \cdot E_{ij} = \sum_{k} c_{ki} E_{kj},$$

а

$$E_{ij} \cdot C = \sum_{k,l} c_{kl} E_{ij} \cdot E_{kl} = \sum_{l} c_{jl} E_{il}$$

- нетрудно видеть, что в первом случае получается матрица с одним ненулевым (j-ым) столбцом, который совпадает с i-ым столбцом матрицы C, а во втором случае получается матрица с одной ненулевой (i-ой) строкой, которая совпадает с j-ой строкой матрицы C:

$$C \cdot E_{ij} = \begin{array}{c} \\ i \\ \\ \end{array} \left[\begin{array}{c|c|c} 0 & c_{1i} & 0 \\ \hline & \vdots & \\ \hline 0 & c_{ni} & 0 \end{array}\right] = \begin{array}{c} \\ i \\ \\ \end{array} \left[\begin{array}{c:c} 0 & 0 \\ \hline c_{j1} \cdots * \cdots c_{jn} & \\ \hline 0 & 0 \end{array}\right] = E_{ij} \cdot C$$
$$\qquad\qquad\qquad\quad j \qquad\qquad\qquad\qquad\quad j$$

Отсюда следует, что

$$c_{ii} = c_{jj},$$
$$c_{ki} = 0, \forall k \neq i,$$
$$c_{jl} = 0, \forall l \neq j,$$

что означает, что $A = \lambda \cdot E$ для некоторого $\lambda \in K$. Следовательно,

$$Z(Mat_n(K)) = K \cdot E$$

■

2) $\mathbb{R}, \mathbb{C}, \mathbb{H}$ - алгебры с делением над $\mathbb{R}$. Ясно, что $\mathbb{C}$ не является центральной алгеброй, так как она коммутативна и ее центр совпадает с ней самой, а $\mathbb{C} \supset \mathbb{R}$. Также очевидно, что $\mathbb{R}$ центральна, так как в этом случае поле совпадает с алгеброй. Докажем, что $\mathbb{H}$ - центральная алгебра.

Доказательство.
Пусть

$$q = \alpha + \beta i + \gamma j + \delta k \in Z(\mathbb{H})$$

Тогда q коммутирует со всеми кватернионами, в частности, с кватернионными единицами, например:

$$q \cdot i = \alpha i - \beta - \gamma k + \delta j$$
$$i \cdot q = \alpha i - \beta + \gamma k - \delta j$$

Отсюда следует, что $\gamma = \delta = 0$, аналогично проверяется, что и $\beta = 0$. Следовательно, $q = \alpha \in \mathbb{R}$. ■

Конечномерные алгебры с делением.

Пусть A – конечномерная ассоциативная алгебра с единицей над K. Напоминание:

- Любой элемент $a \in A$ алгебраичен и $deg\ \mu_a \leq dim\ A$
- Если A без делителей нуля, тогда $\forall a \in A$: μ_a неприводим в $K[x]$

Упражнение. Доказать, что если конечномерная ассоциативная алгебра с единицей не имеет делителей нуля, то это – алгебра с делением.

Можно сказать, что конечномерные алгебры с делением – это некоммутативный аналог конечных расширений полей.

Предложение 2. Если K алгебраически замкнуто, то любая конечномерная алгебра с делением над K изоморфна K.

Доказательство.
Пусть A – конечномерная алгебра с делением над K. Тогда μ_a неприводим над K для любого $a \in A$. Но поле K алгебраически замкнуто, и над ним неприводимы только многочлены первой степени, следовательно,

$$\mu_a(x) = x - \lambda\ \ (\lambda \in K)\ \Rightarrow\ a = \lambda \cdot \overline{1}$$

Таким образом,

$$A = K \cdot \overline{1} \simeq K$$

■

Итак, если поле K алгебраически замкнуто, то мы знаем устройство любой конечномерной алгебры с делением над этим полем. Над полями, которые не являются алгебраически замкнутыми, существуют нетривиальные алгебры с делением – например, можно присоединить к полю K корень какого-нибудь неприводимого многочлена над этим полем – так мы получим расширение поля K, которое является алгеброй с делением над K (более того, она будет коммутативна, т.е. полем), но эта алгебра не будет центральной (так как ее центр совпадает с ней самой, а не с K).

Но именно центральные конечномерные алгебры с делением представляют интерес (т.к. если алгебра не центральна, можно заменить поле K на центр этой алгебры, тем самым

превратив алгебру в центральную). Мы, однако, не будем углубляться в изучение центральных алгебр, а вместо этого исследуем, какие бывают конечномерные алгебры с делением над $\mathbb{R}$. Мы уже знаем три примера таких алгебр: $\mathbb{R}, \mathbb{C}, \mathbb{H}$. Оказывается, других нет.

Теорема Фробениуса. Всякая конечномерная алгебра с делением над $\mathbb{R}$ изоморфна либо $\mathbb{R}$, либо $\mathbb{C}$, либо $\mathbb{H}$.

Доказательство.
Пусть A – конечномерная алгебра с делением над $\mathbb{R}$.

0) Если $A = \mathbb{R} \cdot 1 \simeq \mathbb{R}$, то доказывать нечего.

1) Пусть $A \neq \mathbb{R}$ (эту запись следует понимать как то, что A не совпадает с вложением поля $\mathbb{R}$ в алгебру A в виде множества элементов вида $\mathbb{R} \cdot 1$).
Возьмем $a \in A$, $a \notin \mathbb{R}$. Тогда $deg\ \mu_a > 1$, μ_a неприводим над $\mathbb{R}$, следовательно,

$$\mu_a(x) = x^2 + \alpha \cdot x + \beta,$$

где $\alpha, \beta \in \mathbb{R}$ и $D = \alpha^2 - 4\beta < 0$.
Многочлен μ_a – аннулирующий для a, то есть:

$$a^2 + \alpha \cdot a + \beta = 0 \Leftrightarrow \left(a + \frac{\alpha}{2}\right)^2 + \beta - \frac{\alpha^2}{4} = 0$$

Обозначим для краткости

$$a + \frac{\alpha}{2} = b, \ \ \beta - \frac{\alpha^2}{4} = \delta.$$

Заметим, что $\delta = -\frac{D}{4} > 0$, тогда

$$b^2 = -\delta < 0$$

- мы нашли в алгебре A элемент, квадрат которого равен отрицательному числу. Положим

$$i = \frac{b}{\sqrt{\delta}} \Rightarrow i^2 = -1$$

Тогда

$$\mu_i(x) = x^2 + 1$$

Присоединяя корень этого многочлена (т.е. i) к $\mathbb{R}$, получаем, что

$$A \supseteq \mathbb{R}[i] \simeq \mathbb{C}$$

2) Рассмотрим A как векторное пространство над $\mathbb{C} \simeq \mathbb{R}[i]$ относительно умножения на скаляры слева (мы должны определить, с какой стороны умножаем на скаляры, так как $\mathbb{C} \simeq \mathbb{R}[i]$ уже не обязано лежать в центре алгебры A). Умножение на скаляры справа будет коммутировать с умножением слева, так как операция умножения в алгебре ассоциативна, поэтому операции умножения на скаляры справа (как и умножение на любые элементы алгебры A справа) будут линейными операторами на A. Рассмотрим оператор умножения справа на i:

$$\mathcal{I}\colon A \to A$$
$$a \mapsto a \cdot i$$

- линейный оператор над $\mathbb{C}$. Он удовлетворяет соотношению:

$$\mathcal{I}^2 = -\mathcal{E} \Rightarrow \mathcal{I}^4 = \mathcal{E},$$

т.е. $\mathcal{I}$ - оператор конечного порядка. Тогда (факт из линейной алгебры) оператор $\mathcal{I}$ диагонализуем с собственными значениями $\lambda \in \mathbb{C},\ \lambda^2 = -1$, т.е. $\lambda = \pm i$. Следовательно, пространство A распадается в прямую сумму двух собственных подпространств, отвечающих собственным значениям оператора $\mathcal{I}$:

$$A = A_+ \oplus A_-$$

В явном виде: $\forall a \in A$ существует единственное разложение

$$a = a_+ + a_-$$

где $a_+ \in A_+,\ a_- \in A_-$ - действительно, подействуем на это равенство оператором $\mathcal{I}$, получим

$$\mathcal{I}(a) = i \cdot a_+ - i \cdot a_- \Leftrightarrow i \cdot \mathcal{I}(a) = -a_+ + a_-$$

Тогда

$$a_+ = \frac{a - i \cdot \mathcal{I}(a)}{2}, \qquad a_- = \frac{a + i \cdot \mathcal{I}(a)}{2}$$

- легко видеть, что эти элементы действительно лежат в A_+ и A_- соответственно.

3) Свойства A_+ и A_-:
а) По определению собственных подпространств:

$$a \in A_+ \Rightarrow a \cdot i = i \cdot a$$
$$a \in A_- \Rightarrow a \cdot i = -i \cdot a$$

б)

$$A_+ \cdot A_+ \subseteq A_+$$
$$A_- \cdot A_- \subseteq A_+$$
$$A_+ \cdot A_- \subseteq A_-$$
$$A_- \cdot A_+ \subseteq A_-$$

- это следует из пункта а): например, пусть $a \in A_+$, $b \in A_-$, тогда:

$$(a \cdot b) \cdot i = a \cdot (-i \cdot b) = -(i \cdot a) \cdot b = -i \cdot (a \cdot b) \Rightarrow a \cdot b \in A_-$$

в)

$$a \in A_\pm, \ \ a \neq 0 \Rightarrow a^{-1} \in A_\pm$$

- это также следует из пункта а): умножим равенство $a \cdot i = \pm i \cdot a$ слева и справа на a^{-1}, получим:

$$i \cdot a^{-1} = \pm a^{-1} \cdot i \Rightarrow a^{-1} \in A_\pm$$

4) Из свойств а), б), в) вытекает, что A_+ является алгеброй с делением над $\mathbb{C}$. В самом деле, A_+ - подпространство A, замкнутое относительно умножения и взятия обратного элемента, кроме того, элементы из A_+ коммутируют с элементами из $\mathbb{C}$.

Но $\mathbb{C}$ - алгебраически замкнутое поле, тогда из предложения 2 следует, что $A_+ \simeq \mathbb{C}$. Если $A_- = \{0\}$, то доказательство закончено: $A = A_+ \simeq \mathbb{C}$.

5) Пусть $A_- \neq \{0\}$. Возьмем произвольный $b \in A_-, \ \ b \neq 0$ и (как и на первом этапе доказательства) рассмотрим его минимальный многочлен: так как $b \notin \mathbb{R}$, то $deg\ \mu_b > 1$, μ_a неприводим над $\mathbb{R}$, следовательно,

$$\mu_b(x) = x^2 + \lambda \cdot x + \mu,$$

где $\lambda, \mu \in \mathbb{R}$ и $D = \lambda^2 - 4\mu < 0$.
Многочлен μ_b – аннулирующий для b, то есть:

$$b^2 + \lambda \cdot b + \mu = 0$$

Так как $b \in A_-$, то $b^2 \in A_+$, а $\lambda \cdot b \in A_-$. Кроме того, $\mu \in A_+$. Так как пространство A есть прямая сумма подпространств A_+ и A_-, то $\lambda = 0$ и

$$b^2 + \mu = 0.$$

Так как $D = \lambda^2 - 4\mu < 0$, то $\mu > 0$.
Положим

$$j = \frac{\mu}{\sqrt{\delta}} \in A_- \Rightarrow j^2 = -1$$

6) Как и на втором этапе доказательства, рассмотрим оператор умножения справа на j:

$$\mathcal{J}\colon A \to A$$
$$a \mapsto a \cdot j$$

- линейный оператор над A. Он удовлетворяет соотношению:

$$\mathcal{J}^2 = -\mathcal{E},$$

т.е. $\mathcal{J}$ – невырожденный оператор. Кроме того, по свойству б) пункта 3:

$$\mathcal{J}(A_+) \subseteq A_-$$
$$\mathcal{J}(A_-) \subseteq A_+$$

Но из невырожденности оператора $\mathcal{J}$ следует, что включения – это равенства:

$$\mathcal{J}(A_+) = A_-$$
$$\mathcal{J}(A_-) = A_+$$

- действительно, если бы например имело место строгое включение $\mathcal{J}(A_+) \subset A_-$, тогда применив к обеим частям равенства оператор $\mathcal{J}$, мы бы получили

$$\mathcal{J}^2(A_+) \subset \mathcal{J}(A_-) \Leftrightarrow -\mathcal{E}(A_+) \subset \mathcal{J}(A_-) \Leftrightarrow A_+ \subset \mathcal{J}(A_-) = A_+$$

- противоречие.

Таким образом, оператор $\mathcal{J}$ переставляет подпространства A_+ и A_-. Теперь для того, чтобы доказать, что $A \simeq \mathbb{H}$, нужно предъявить в A базис, умножение в котором устроено так же, как умножение в базисе пространства $\mathbb{H}$.

Подалгебра A_+ имеет базис $(1, i)$ над $\mathbb{R}$. Тогда $A_- = \mathcal{J}(A_+)$ имеет базис $\mathcal{J}(1) = 1 \cdot j = j$ и $\mathcal{J}(i) = i \cdot j = k$. Значит, $A = A_+ \bigoplus A_-$ имеет базис $(1, i, j, k)$ над $\mathbb{R}$. Умножение на базисе устроено следующим образом:

$$i^2 = j^2 = -1 \text{ по построению,}$$
$$k^2 = (i \cdot j)^2 = i \cdot j \cdot i \cdot j = i \cdot (-i \cdot j) \cdot j = -i^2 \cdot j^2 = -(-1) \cdot (-1) = -1$$
$$i \cdot j = k \text{ по построению,}$$
$$j \cdot i = -i \cdot j = -k,$$
$$j \cdot k = j \cdot i \cdot j = -i \cdot j^2 = -i \cdot (-1) = i,$$
$$k \cdot j = i \cdot j^2 = i \cdot (-1) = -i,$$
$$k \cdot i = i \cdot j \cdot i = -i^2 \cdot j = j,$$
$$i \cdot k = i \cdot i \cdot j = i^2 \cdot j = (-1) \cdot j = -j.$$

Итак, умножение в этом базисе устроено в точности так, как умножение в базисе $\mathbb{H}$, следовательно, $A \simeq \mathbb{H}$. ■

Итак, мы выяснили, как устроены конечномерные алгебры с делением над $\mathbb{R}$. Теперь рассмотрим, как устроены алгебры с делением над конечным полем, т.е. как устроены конечные тела. Оказывается, конечные тела – это конечные поля.

Теорема Веддербарна (J. H. Wedderburn, 1882-1948). Всякое конечное тело является полем.

Доказательство.
1) Пусть D – конечное тело. Рассмотрим его центр $F = Z(D)$ – это конечное поле, $|F| = q$. Тело D является конечномерным векторным пространством над F: обозначим $dim\ D = n$, тогда

$$D \simeq F^n,$$
$$|D| = q^n.$$

Рассмотрим мультипликативную группу тела: $D^\times$ - конечная группа, $Z(D^\times) = F^\times$. Воспользуемся формулой классов:

$$|G| = |F^\times| + \sum_{i=1}^{s} \frac{|D^\times|}{|Z(x_i)|}$$

где x_i – представители нецентральных классов сопряженности в $D^\times$.
Рассмотрим

$$F(x_i) = \{y \in D \mid x_i \cdot y = y \cdot x_i\} = Z(x_i) \cup \{0\}$$

- подтело в D. Оно содержится в центре D:

$$F(x_i) \supseteq F$$

Так как $F(x_i)$ – векторное пространство над F, то

$$|F(x_i)| = q^{d_i}$$

Будем доказывать индукцией по n, что D – поле. Так как $d_i < n$, то по предположению индукции $F(x_i)$ – подполе в D. Тогда

$$|D| = |F(x_i)|^k \Leftrightarrow q^n = q^{k \cdot d_i},$$

где $k = dim\ D$ над $F(x_i)$. Таким образом, d_i является делителем d.

Подставляя порядки соответствующих множеств в формулу классов, получаем следующую формулу:

$$q^n - 1 = q - 1 + \sum_{i=1}^{s} \frac{q^n - 1}{q^{d_i} - 1}$$

2) Рассмотрим многочлен $x^n - 1$ над $\mathbb{C}$. Его корнями являются всевозможные корни степени n из единицы:

$$x^n - 1 = \prod_{k=0}^{n-1}(x - \varepsilon_k),$$

где

$$\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \;\; k = 0, \dots, n-1.$$

Многочлен деления круга на n частей:

$$\Phi_n(x) = \prod(x - \varepsilon_k),$$

где ε_k – первообразные корни степени n из единицы (как было доказано в первой части курса, ε_k – первообразный корень степени n из единицы $\Leftrightarrow (n, k) = 1$).

Лемма.
а)

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

б)

$\Phi_n(x) \in \mathbb{Z}[x]$, со старшим коэффициентом 1

Доказательство леммы.
а) Очевидно, так как любой ε_k является первообразным для некоторого $d|n$.

б) Доказывается индукцией по n.
База индукции: $\Phi_1(x) = x - 1$.
Шаг индукции: из пункта а) следует, что

$$x^n - 1 = \Phi_n(x) \cdot \prod_{\substack{d|n, \\ d<n}} \Phi_d(x)$$

Так как каждый из $\Phi_d(x)$ по предположению индукции – целочисленный со старшим коэффициентом 1, то и $\prod_{\substack{d|n, \\ d<n}} \Phi_d(x) \in \mathbb{Z}[x]$, со старшим коэффициентом 1. Тогда и $\Phi_n(x) \in \mathbb{Z}[x]$, со старшим коэффициентом 1. ■

3) Из этой леммы и формулы классов следует, что

$$q^n - 1 \vdots \Phi_n(q)$$

Также (в силу пункта а) леммы) $\forall q$:

$$\frac{q^n-1}{q^{d_i}-1} \vdots \Phi_n(q)$$

Следовательно (из формулы классов)

$$q-1 \vdots \Phi_n(q)$$

- но это возможно лишь при $n=1$:

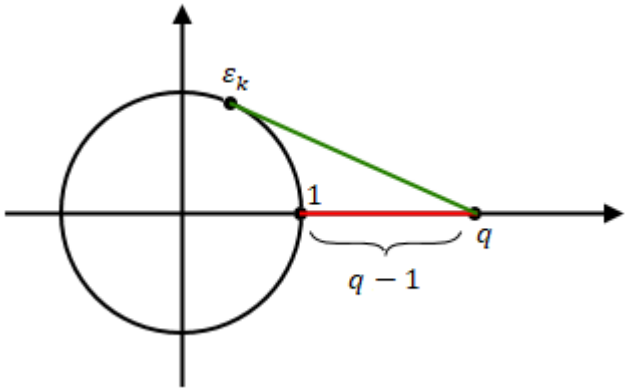


Рис. 23.1. $|q-\varepsilon_k| > q-1$

- при $n>1$, если ε_k – первообразный корень степени n из единицы, то $|q-\varepsilon_k| > q-1$, следовательно, $|\Phi_n(q)| > q-1$.

Так как $n=1$, то $D=F$. ■

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in

ЛЕКЦИИ УЧЕНЫХ МГУ