Основы высшей алгебры и теории кодирования.

Автор: Пук-пук Стесняшка

Оглавление

Глава 1

Теоритическое введение

1.1 Группа

Определение 1. Группа $G = \langle M, * \rangle$ – это такая пара из множества M и бинарной операции $*$ на этом множестве, что выполняются следующие свойства (аксиомы группы):
G1: $(x * y) * z = x * (y * z)$ (ассоциативность);
G2: (аксиома единицы) существует единственный *нейтральный* (или единичный) элемент e такой, что для любого x выполняется $e * x = x * e = x$;
G3: для любого элемента x существует ровно один *обратный элемент*, то есть такой элемент y, для которого $y * x = x * y = e$ (обратный элемент обозначается x^{-1}).

Пример 1. (Числовые группы). Числовые системы: целые числа $\mathbb{Z}$, рациональные числа $\mathbb{Q}$, действительные числа $\mathbb{R}$, комплексные числа $\mathbb{C}$, образуют группы относительно операции сложения.
Множества отличных от нуля чисел (рациональных $\mathbb{Q}^*$, действительных $\mathbb{R}^*$, комплексных $\mathbb{C}^*$) образуют группу относительно операции умножения.

Все числовые группы удовлетворяют дополнительному свойству коммутативности: $a*b = b*a$ для любых a, b из группы. Группы со свойством коммутативности называются *абелевыми* или *коммутативными*.
Группа называется *конечной*, если в ней (а точнее — в множестве M) конечное число элементов. Это число называется *порядком* группы.

1.2 Примеры групп

1.2.1 Аддитивная группа вычетов по модулю n

Определение 2. Вычеты по модулю n с операцией сложения образуют группу. Обозначается эта группа Z_n. Это конечная абелева группа. Её порядок, то есть количество вычетов, равен n.

1.2.2 Мультипликативная группа вычетов

Определение 3. Взаимно простые с n вычеты по модулю n (то есть отвечающие взаимно простым с n остаткам), с операцией умножения образуют группу.

Нейтральным элементом является вычет $[1]$: $[1]_n \cdot [x]_n = [1 \cdot x]_n = [x]_n$ для любого вычета x, даже необязательно взаимно простого с n.
Мультипликативная группа вычетов по модулю n обозначается Z_n^*. Её порядок, то есть количество остатков по модулю n, которые взаимно просты с n, обозначается $\varphi(n)$ и называется *функцией Эйлера*.

1.2.3 Группа перестановок (симметрическая группа)

Определение 4. Перестановки множества $\{1, 2, \ldots, n\}$ с операцией композиции перестановок образуют группу. Обозначается группа перестановок n элементов как S_n. Другое её название – *симметрическая группа*.

Перестановки образуют конечную группу. Её порядок, то есть количество перестановок, нетрудно найти обычными методами элементарной перечислительной комбинаторики. Он равен $n! = 1 \cdot 2 \cdot \ldots \cdot n$.

1.2.4 Знакопеременная группа

Определение 5. Подгруппа чётных перестановок (ядро гомоморфизма знака перестановки) обозначается A_n и называется *знакопеременной группой*.

1.2.5 Циклическая группа

Определение 6. Группа называется *циклической*, если она порождена одним элементом: $G = \langle a \rangle, a \in G$. Любой элемент с таким свойством называется *порождающим* циклической группы.

1.2.6 Группа диэдра

Определение 7. Движения пространства также образуют группу, как и симметрии многоугольников и многогранников. Обычно группа симметрий правильного n-угольника (как собственных, так и несобственных) обозначается D_n и называется *группой диэдра*. В этой группе $2n$ элементов.

1.3 Порядок группы, порядок элемента группы

1.3.1 Порядок группы

Определение 8. Группа называется *конечной*, если в ней (а точнее — в множестве M) конечное число элементов. Это число называется *порядком* группы.

1.3.2 Порядок элемента группы

Если подгруппа H, порожденная одним элементом, $H = \langle h \rangle$, то в этом случае порядок $\langle h \rangle$ называется также *порядком элемента* h, общее обозначение $ord\, h$. Более традиционное определение:

Определение 9. Порядок $ord_G h$ элемента h группы G – это наименьшее среди тех положительных чисел d, для которых $h^d = e$. Если таких чисел нет, порядок считается бесконечным (у группы $\langle h \rangle$ в этом случае также бесконечный порядок).

1.4 Отображения, композиции

Определение 10. *Отображением* множества A в множество B (другое название: функция из множества A в множество B) называется произвольное соответствие, которое каждому элементу множества A сопоставляет ровно один элемент множества B.

Определение 11. Для двух отображений $f: A \to B$ и $g: B \to C$ определена операция *композиции* (обозначение $g \circ f$, порядок существенный). Это такое отображение из множества A в множество C, которое элементу $x \in A$ сопоставляет тот элемент $z \in C$, для которого выполняются равенства $z = g(y)$, $y = f(x)$.

Утвержение 1. *Операция композиции обладает свойством ассоциативности: для любых отображений $f: A \in B$, $g: B \to C$, $h: C \to D$ выполняется равенство*

$$(h \circ (g \circ f)) = ((h \circ g) \circ f), \text{ то есть } (h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$$

для любого $x \in A$.

Определение 12. Отображение $f: X \to Y$ называется *инъективным* (инъекция), если из равенства $f(x_1) = f(x_2)$ следует равенство $x_1 = x_2$.
Отображение $f: X \to Y$ называется *сюръективным* (сюръекция), если для любого y существует такое x, что $f(x) = y$.
Отображение $f: X \to Y$ называется *биективным* (биекция или взаимно однозначное отображение), если для любого y существует ровно одно такое x, что $f(x) = y$ (то есть отображение является одновременно сюръективным и инъективным).

1.5 Четность перестановки

Определение 13. Перестановкой *называется взаимно однозначное отображение конечного множества на себя.*

Найдём гомоморфизмы $\sigma : S_n \to C_2$ из группы перестановок n элементов в циклическую группу порядка 2. Нам будет удобно представлять эту циклическую группу как $\{\pm 1, \cdot\}$, то есть подгруппу группы ненулевых действительных чисел по умножению.
Один гомоморфизм очевиден: он переводит все перестановки в $+1$.
Вспомним, что транспозиции порождают S_n. Поэтому если все транспозиции лежат в ядре σ, то и любая перестановка лежит в ядре σ.
Из коммутативности C_2 можно вывести и другой факт: если хотя бы одна транспозиция лежит в ядре, то и все транспозиции лежат в ядре. Для этого посмотрим на равенство:

$$(k\,\ell) = (i\,k)(j\,\ell) \circ (i\,j) \circ (i\,k)(j\,\ell).$$

Применим к этому равенству гомоморфизм σ:

$$\sigma((k\,\ell)) = \sigma((i\,k)(j\,\ell) \circ (i\,j) \circ (i\,k)(j\,\ell)) = \sigma((i\,k)(j\,\ell))\sigma((i\,j))\sigma((i\,k)(j\,\ell)) =$$

$$= \sigma((i\,k)(j\,\ell))^2\sigma((i\,j)) = \sigma((i\,j))$$

Это означает, что образы всех транспозиций при гомоморфизме σ одинаковы. Итак, если гомоморфизм нетривиальный (есть прообраз $y-1$), то образы всех транспозиций равны -1. Чтобы найти образ произвольной перестановки, нужно представить её как композицию N транспозиций и отобразить в $(1)^N$. Это означает, что нетривиальный гомоморфизм $\sigma : S_n \to C_2$ единственный.

Однако мы не закончили анализ. Пока неясно, существует ли этот нетривиальный гомоморфизм. Могло бы так случиться, что одна и та же перестановка раскладывалась и в композицию чётного числа транспозиций, и в композицию позицию нечётного числа транспозиций. Это дало бы два противоречивых условия на образ такой перестановки и означало бы, что нетривиального гомоморфизма нет.

Оказывается, что такого противоречия не возникает, и нетривиальный гомоморфизм $\sigma : S_n \to$ $\to C_2$ существует. Он сопоставляет перестановке *знак*. Перестановки знака $+1$ называются чётными, а знака -1 называются нечётными.

1.6 Цикловое разложение перестановки. Формула для порядка перестановки

Определение 14. *Перестановкой* называется взаимно однозначное отображение конечного множества на себя.

Пример 2. Перестановка, которая задаётся последовательностью $2, 1, 4, 5, 3$ записывается в виде таблицы как:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \text{ или } \begin{pmatrix} 5 & 2 & 4 & 1 & 3 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$$

Табличная запись длиннее, но зато позволяет легко вычислять композицию перестановок. Чтобы вычислить композицию перестановок σ и π, нужно написать таблицу для π, под ней написать такую таблицу для σ, в которой первая строка совпадает со второй строкой таблицы для π (в каждой строке таблицы записаны ровно по одному разу числа от до n, так что такая таблица существует). После этого нужно взять первую строку первой таблицы и вторую строку второй таблицы. Это и будет таблица для композиции перестановок. Правило звучит громоздко, его легко записать в виде формулы:

$$\begin{pmatrix} t_1 & t_2 & t_3 & \dots & t_i & \dots & t_n \\ v_1 & v_2 & v_3 & \dots & v_i & \dots & v_n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \dots & i & \dots & n \\ t_1 & t_2 & t_3 & \dots & t_i & \dots & t_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \dots & i & \dots & n \\ v_1 & v_2 & v_3 & \dots & v_i & \dots & v_n \end{pmatrix}$$

1.6.1 Цикловое разложение перестановки

В качестве полезного промежуточного шага построим граф перестановки. Это ориентированный граф на множестве вершин $1, 2, \dots, n$, в котором из вершины i исходит ровно одно ребро в вершину $\pi(i)$. В силу биективности в каждую вершину этого графа также входит ровно одно ребро. Пример графа перестановки из примера выше:

В графе перестановки возможны петли, они возникают в тех вершинах, для которых $\pi(i) = i$. В любом случае ориентированный граф, входящие и исходящие степени вершин которого равны 1, разбивается на непересекающиеся циклы (петли считаем циклами длины 1). Записывая

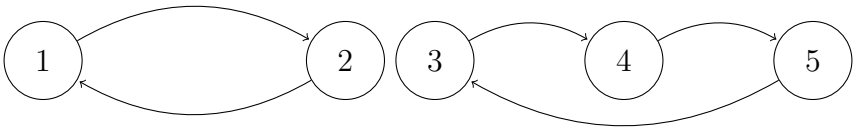

Рис. 1.1: Граф перестановки

вершины в порядке обхода этих циклов и разделяя циклы скобками, получаем цикловое разложение перестановки. Для перестановки из примера выше цикловое разложение выглядит как:

$$(1\,2)(3\,4\,5), \text{ или } (2\,1)(4\,5\,3), \text{ или } (3\,4\,5)(2\,1).$$

Порядок циклов в записи циклового разложения несущественен. Внутри каждого цикла важен лишь циклический порядок: неважно, какой именно элемент цикла стоит на первом месте.

1.6.2 Формула для порядка перестановки

Рассмотрим группу перестановок S_n. Общее определение порядка элемента в группе для перестановок пересказывается так: порядок перестановки π – это такое наименьшее положительное k, что перестановка

$$\pi^k = \underbrace{\pi \circ \pi \circ \cdots \circ \pi}_{k \text{ композиций}}$$

является тождественной (тождественная перестановка – это нейтральный элемент в группе S_n).

Утверждение 2. *Порядок цикла $(a_1\, a_2\, \ldots\, a_\ell)$ равен ℓ.*

Лемма 1. *Пусть цикловое разложение перестановки π состоит из циклов длин $\ell_1, \ell_2, \ldots, \ell_s$. Тогда порядок перестановки π равен* $\mathrm{HOK}(\ell_1, \ell_2, \ldots, \ell_s)$.

1.7 Подгруппа

Определение 15. Подмножество H элементов группы G называется *подгруппой*, если для него выполняются следующие свойства
1. если a,$b \in H$, то $a \cdot b \in H$;
2. $e \in H$;
3. если $a \in H$, то $a^{-1} \in H$.
Обозначение $H < G$ указывает, что H – подгруппа G.

Лемма 2. *Подмножество H является подгруппой тогда и только тогда, когда ограничение H является группой относительно ограничения групповой операции на G.*

Теорема 1. *Множество H является подгруппой группы G тогда и только тогда, когда для любых a,$b \in H$ выполнено $ab^{-1} \in H$.*

Лемма 3. *Пересечение подгрупп – подгруппа.*

Лемма 4. *Пусть G – конечная группа. Множество $H \subseteq G$ является подгруппой группы G тогда и только тогда, когда H замкнуто относительно групповой операции.*

1.8 Описание подгрупп циклической группы порядка n

Лемма 5. *Для каждого делителя k порядка n циклической группы C_n существует элемент порядка k. Всякая подгруппа циклической группы циклическая. Подгруппа порядка $k \mid n$ в циклической группе C_n единственна.*

1.9 Описание подгрупп бесконечной циклической группы

Лемма 6. *Всякая нетривиальная подгруппа бесконечной циклической группы бесконечная циклическая и имеет конечный индекс. Подгруппа индекса k в бесконечной циклической группе единственна.*

1.10 Смежные классы по подгруппе

Опредление 16. Пусть $H < G$ – подгруппа группы G, а x – некоторый элемент группы G.

Левый смежный класс по подгруппе H с представителем x – это множество

$$xH = \{y : y = xh, h \in H\}.$$

Аналогично, *правый смежный класс* по подгруппе H с представителем x – это множество

$$Hx = \{y : y = hx, h \in H\}$$

Ясно, что всегда $x \in xH$ и $x \in Hx$. Для абелевых групп разницы между левыми и правыми смежными классами нет. В этом случае говорят просто о смежном классе (так же говорят и в неабелевом случае, когда выбор левого или правого смежного класса ясен из контекста).

Теорема 2 (Теорема о смежных классах)**.** *Смежные классы xH и yH либо не пересекаются, либо совпадают.*

Лемма 7. *Элементы x, y группы G принадлежат одному левому смежному классу по подгруппе H тогда и только тогда, когда $y^{-1}x$ принадлежит H.*
Элементы x, y группы G принадлежат одному правому смежному классу по подгруппе H тогда и только тогда, когда xy^{-1} принадлежит H.

1.11 Теорема Лагранжа. Малая теорема Ферма. Теорема Эйлера

Лемма 8. *Пусть $H < G$ – подгруппа группы G, а x – некоторый элемент группы G. Тогда отображение «сдвига» $f : h \mapsto xh$ задаёт биекцию между подгруппой H и смежным классом с представителем H.*

Следствие 1. *Если в подгруппе H конечное количество элементов, то $|H| = |xH|$ для любого x.*

Количество смежных классов группы G по подгруппе H называется *индексом подгруппы* и обозначается через $(G : H)$. (Если смежных классов по H бесконечно много, то H называется подгруппой бесконечного индекса.)

Теорема 3 (Теорема Лагранжа)**.**

Пусть H – подгруппа конечной группы G. Тогда порядок H является делителем порядка G и, более того,

$$|G| = (G : H) \cdot |H|.$$

Следствие 2. *Группа простого порядка не имеет несобственных подгрупп.*

Утвержение 3. *Порождённая элементом h подгруппа совпадает с множеством целых степеней h. Все различные степени имеют показатели $0, 1, \ldots, ord\, h - 1$.*

По теореме Лагранжа порядок элемента (как и порядок любой подгруппы) делит порядок группы. Приведём несколько следствий из этого утверждения. Первое выполняется для любых конечных групп.

Следствие 3. *Пусть x – элемент группы G из n элементов. Тогда $x^n = e$.*

Теорема 4 (Малая теорема Ферма)**.**

Если p – простое число, то для любого $a \not\equiv 0 \ (mod\, p)$ выполняется сравнение $a^{p-1} = 1 \ (mod\, p)$.

Теорема 5 (Малая теорема Ферма для всех вычето)**.**

Если p – простое число, то для любого a выполняется сравнение $a^p = a \ (mod\, p)$.

Определение 17. *Функция Эйлера $\varphi(m)$ – это количество натуральных чисел от 1 до m, взаимно простых с m.*

Теорема 6 (Теорема Эйлера)**.**

Пусть a взаимно просто с n. Тогда $a^{\varphi(n)} \equiv 1 \pmod{n}$, где $\varphi(n)$ — функция Эйлера.

1.12 Изоморфизмы и автоморфизмы групп

Определение 18. *Изоморфизм групп* $(G, *)$ и $(G', \circ)$ – это отображение $\varphi G \to G'$, которое (1) биективно; (2) сохраняет операцию, то есть для любых элементов a, bгруппы G выполняется равенство

$$\varphi(a * b) = \varphi(a) \circ \varphi(b)$$

(образ произведения равен произведению образов).

Группы называются *изоморфными*, если между ними существует изоморфизм. Обозначение $G \cong G'$.

Утверждение 4. *Пусть* $: G \to G'$ *– изоморфизм групп* $(G, *)$ *и* $(G', \circ)$. *Тогда:*
1. $\varphi(e)$ *– нейтральный элемент группы* G' *(изоморфизм сохраняет единицу);*
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ *(образ обратного элемента – обратный элемент к образу); 3. обратное отображение* φ^{-1} *является изоморфизмом; 4. композиция изоморфизмов является изоморфизмом.*

Опредление 19. Изоморфизм группы с самой собой называется *автоморфизмом.*

Тривиальный пример автоморфизма — тождественное отображение, однако автоморфизмов групп может быть гораздо больше.

Утверждение 5. *Автоморфизмы любой группы* G *образуют относительно композиции группу, которая называется* группой автоморфизмов *группы* G.

Группу автоморфизмов группы G будем обозначать $Aut\, G$

1.13 Прямое произведение групп

Опредление 20. *Прямое произведение* групп G и H обозначается $G \times H$ и состоит из всех возможных пар (g, h), $g \in G,\ h \in H$. Операция в G – это покомпонентное выполнение операций в G и H:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2)$$

.

Утверждение 6. $G \times H$ *является группой.*

Утверждение 7. $G \times H \cong G \times H$

Утверждение 8. *Если* G_i *– конечные группы, то*

$$|G_1 \times G_2 \times \cdots \times G_n| = |G_1| \cdot |G_2| \cdot \ldots \cdot |G_n|$$

(в правой части обычное произведение чисел).

Утверждение 9. *Если* $G_i \cong H_i$, *то* $G_1 \times G_2 \times \cdots \times G_n \cong H_1 \times H_2 \times \cdots \times H_n$.

Лемма 9. *Порядок элемента* $(g_1, g_2, \ldots, g_n) \in G_1 \times G_2 \times \cdots \times G_n$ *равен* НОК *порядков элементов* g_i.

Утверждение 10. $H \cong C_{\ell_1} \times C_{\ell_2} \times \cdots \times C_{\ell_k}$.

1.14 Сопряженные элементы. Сопряженные подгруппы. Нормальные подгруппы

1.14.1 Сопряженные элементы

Опредление 21. Будем называть элемент b группы G *сопряжённым* с элементом a посредством элемента g, если $b = gag^{-1}$.

Два элемента группы называются *сопряжёнными*, если один сопряжён с другим посредством некоторого элемента g. Отношение сопряжённости будем обозначать $\sim$.

Лемма 10. *Отношение сопряжённости является отношением эквивалентности.*

Утверждение 11. *Перестановка, которая получается переименованием* α *из перестановки* π, *– это перестановка, сопряжённая* π *посредством* α.

1.14.2 Сопряженные подгруппы

Определение 22. Подгруппы H_1 и H_2 группы G называются *сопряжёнными*, если $H_2 = gH_1g^{-1}$ для некоторого $g \in G$.

1.14.3 Нормальные подгруппы

Определение 23. Если для любого $x \in G$ левый смежный класс по подгруппе H совпадает с правым, $xH = Hx$, то такая подгруппа называется *нормальной*.
Для нормальных подгрупп используется специальное обозначение $H \lhd G$.

Свойство нормальности подгруппы переформулируется в терминах сопряжений: подгруппа H группы G *нормальна* тогда и только тогда, она не изменяется при сопряжении посредством любого элемента $g \in G$, то есть $gHg^{-1} = H$. Это условие очевидно равносильно совпадению левых и правых смежных классов $gH = Hg$ (умножение справа на g^{-1} превращает второе равенство в первое).

Определение 24. *Группа, в которой нет нормальных подгрупп, кроме единичной и самой группы, называется* простой.

Самым очевидным примером простой группы является группа простого порядка. В ней вообще всего две подгруппы в силу теоремы Лагранжа.

Теорема 7. *Знакопеременная группа A_5 простая.*

1.15 Критерий сопряженности перестановок

Лемма 11. *Перестановки сопряжены тогда и только тогда, когда их цикловые типы совпадают.*

1.16 Гомоморфизмы групп

1.16.1 Гомоморфизмы групп

Определение изоморфизма групп указывает на два свойства: биективность и сохранение операции. Если оставить только второе, получаем понятие гомоморфизма.

Определение 25. Отображение $\varphi : G \to G'$, где $(G, *)$, $(G', \circ)$ – две группы, называется гомоморфизмом, если $\varphi(a * b) = \varphi(a) \circ \varphi(b)$.

Утвержение 12. *Композиция гомоморфизмов – гомоморфизм.*

Утвержение 13. *Пусть $\varphi : G \to G'$ – гомоморфизм групп $(G, *)$ и $(G', \circ)$. Тогда*
1. *$\varphi(e)$ – нейтральный элемент группы G' (изоморфизм сохраняет единицу);*
2. *$\varphi(a^{-1}) = \varphi(a)^{-1}$ (образ обратного элемента – обратный элемент к образу).*

1.17 Ядро гомоморфизма

Определение 26. Пусть $\varphi: G \to G'$ – гомоморфизм групп. Тогда *образ* $Im\,\varphi = \varphi(G)$ состоит из тех элементов $g' \in G'$, для которых есть прообраз (такой элемент $g \in G$, что $\varphi(g) = g'$). Это общее определение для любого отображения.

Определение 27. *Ядром* $Ker\,\varphi$ гомоморфизма называется множество $\{g \in G: \varphi(g) = e_{G'}\}$. Другими словами, элемент принадлежит ядру, если он отображается гомоморфизмом в нейтральный элемент.

Утверждение 14. *Ядро и образ являются подгруппами.*

Утверждение 15. *Пусть $\varphi: G \to G'$ – гомоморфизм групп, H – подгруппа G'. Тогда $^{-1}(H)$ является подгруппой G.*

Утверждение 16. *Пусть $\varphi: G \to G'$ – гомоморфизм групп. Тогда элементы (левого или правого) смежного класса по $Ker\,\varphi$ переходят в один и тот же элемент группы G'. И обратно: если $g' \in G'$, то $\varphi^{-1}(g')$ является смежным классом (левым и правым) по ядру.*

Лемма 12. *У ядра любого гомоморфизма левые классы смежности совпадают с правыми.*

Лемма 13. *Для гомоморфизма конечных групп $\varphi: G \to G'$ выполняется равенство*

$$|G| = |Ker\,\varphi| \cdot |Im\,\varphi|$$

.

1.18 Факторгруппа

Определение 28. *ет Пусть H/G – нормальная подгруппа группы G.*
Факторгруппа G/H *состоит из смежных классов по H. Групповая операция в факторгруппе определяется как*

$$(xH) \cdot (yH) = (xy)H.$$

1.19 Теорема о гомоморфизмах групп

Теорема 8 (Теорема о гомоморфизмах групп)**.**

Пусть $\varphi: G \to H$. Тогда $Im\,\varphi \cong G/Ker\,\varphi$.

1.20 Действия групп. Орбита, стабилизатор

1.20.1 Действия групп

Определение 29. *Действием группы G* на множестве X называется гомоморфизм $\varphi: G \to S(X)$ группы G в группу $S(X)$ биекций множества X (взаимно однозначных отображений множества X на себя). Говорят также, что группа G действует на множестве X.

Определение 30. Если гомоморфизм $G \to S(X)$ инъективный, то действие называется *точным.*

1.20.2 Орбита, стабилизатор

Определение 31. Пусть группа G действует на множестве X. Для любого $x \in X$ множество $Stab_x(G)$ элементов группы G, оставляющих точку x неподвижной, называется *стабилизатором* точки x:

$$Stab_x(G) = \{g \in G : \ g(x) = x\}.$$

Утвержение 17. *Стабилизатор $Stab_x(G)$ – подгруппа G.*

Определение 32. Пусть группа G действует на множестве X. *Орбитой действия* называется множество образов некоторой точки x:

$$Orb_x(G) = \{y \in X : \ y = g(x),\ g \in G\}.$$

Утвержение 18. *Орбиты действия разбивают точки множества X на непересекающиеся множества (классы эквивалентности отношения «точка x принадлежит орбите точки y»).*

Определение 33. Действие называется *транзитивным*, если у него ровно одна орбита. (То есть любая точка переводится в любую другую действием какого-нибудь элемента группы.)

Лемма 14. *Пусть группа G действует на множестве X. Отображение φ : уß$\{g \in G : \ g(x) = y\}$ сопоставляет каждой точке орбиты Orb_x левый смежный класс по стабилизатору $Stab_x$. Это соответствие взаимно однозначно.*
В частности, для порядков группы, стабилизатора и размера орбиты выполняется соотношение

$$|G| = |Stab_x| \cdot |Orb_x|.$$

1.21 Теорема Кэли

Теорема 9 (Теорема Кэли)**.**

Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.

1.22 Лемма Бернсайда

Лемма 15 (Лемма Бернсайда)**.**

Пусть конечная группа G действует на конечном множестве X. Количество орбит действия даётся формулой:

$$\#\text{орбит} = \frac{1}{|G|} \sum_{g \in G} |X_g|,$$

где $X_g = \{x \in X \mid gx = x\}$ – множество неподвижных точек действия элемента g.

1.23 Кольцо

Определение 34. Кольцо – это множество R с двумя бинарными операциями сложения (обозначается $+$) и умножения (обозначается $\cdot$, иногда опускается, как это принято в формулах элементарной алгебры), для которых выполняются следующие свойства (аксиомы кольца):
R1: относительно сложения R – коммутативная группа (которая называется аддитивной группой кольца), нейтральный элемент относительно сложения называется нулём и обозначается обычно как 0;
R2: умножение ассоциативно;
R3: $a \cdot (b + c) = a \cdot b + a \cdot c$; $(b + c) \cdot a = b \cdot a + c \cdot a$ (дистрибутивность умножения относительно сложения слева и справа).

Определение 35. Кольцо называется коммутативным, если умножение в кольце коммутативно: $xy = yx$ для любых элементов кольца.

Определение 36. Кольцо называется кольцом с единицей, если в нём есть нейтральный элемент относительно умножения. Этот элемент называется единицей и обозначается 1. Таким образом, $a \cdot 1 = 1 \cdot a = a$ для любого элемента a кольца.

Определение 37. Элемент $a \neq 0$ кольца R называется *левым делителем нуля*, если существует такой $b \neq 0$, что $ab = 0$. Аналогично, a называется *правым делителем нуля*, если существует такой $b \neq 0$, что $ba = 0$.

Определение 38. Вычитание в кольце – это сложение с противоположным, то есть $x - y = x + (-y)$, где в правой части $-y$ обозначает противоположный к y элемент кольца: $y + (-y) = 0$.

Глава 2

Решение задач из канонического задания

2.1 Обязательные задачи

2.1.1 Задача №1

Корни уравнения $x^n = 1$ как действительные, так и комплексные называются корнями n-й степени из единицы. Проверить, что корни n-й степени образуют группу по умножению.
а) *Верно ли, что всякий корень 35-й степени из единицы является кубом некоторого корня 35-й степени из единицы?*
б) *Тот же вопрос про корни 36-й степени из единицы.*

Решение:

Корни n-ой степени из 1 имеют вид:

$$x_1 = 1 \cdot (\cos\frac{2\pi k_1}{n} + i \cdot \sin\frac{2\pi k_1}{n})$$

Проверим, что они образуют группу по умножению:

$$x_1 \cdot x_2 = 1 \cdot 1 \cdot (\cos\frac{2\pi(k_1+k_2)}{n} + i \cdot \sin\frac{2\pi(k_1+k_2)}{n}) \text{ – также корень из 1;}$$
$$(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3) \tag{2.1}$$

Пункт 2.1 вып-ся в силу ассоциативности умножения компл-ных чисел;

$$\exists\ e = 1 \cdot (\cos 2\pi + i \cdot \sin 2\pi) : \forall x \hookrightarrow x \cdot 1 = 1 \cdot x = x$$

$$\forall x = 1 \cdot (\cos\frac{2\pi k}{n} + i \cdot \sin\frac{2\pi k}{n})\ \exists\ x^{-1} = 1 \cdot (\cos\frac{2\pi(n-k)}{n} + i \cdot \sin\frac{2\pi(n-k)}{n}) :$$
$$x^{-1} \cdot x = x \cdot x^{-1} = 1$$

Следовательно они образуют группу;

а) Рассмотрим корень 35 степени из 1: $x = 1 \cdot (\cos\frac{2\pi k}{35} + i \cdot \sin\frac{2\pi k}{35})$
Пусть: $x_1 = 1 \cdot (\cos\frac{2\pi k_1}{35} + i \cdot \sin\frac{2\pi k_1}{35})$ – корень 3 степени из $x \Rightarrow$

$$\Rightarrow x_1^3 = 1 \cdot (\cos\frac{2\pi(3k_1)}{35} + i \cdot \sin\frac{2\pi(3k_1)}{35}) = 1 \cdot (\cos\frac{2\pi k}{35} + i \cdot \sin\frac{2\pi k}{35}) = x \Rightarrow$$

$$\Rightarrow \frac{2\pi(3k_1)}{35} = \frac{2\pi k}{35} + 2\pi q \Rightarrow k_1 = \frac{1}{3}(k + 35q)$$

Т.к. $35 \equiv 2\, mod\, 3$, то $\forall k\ \exists q \hookrightarrow k + 35\, q \vdots 3\ (\equiv \exists k_1) \Rightarrow$ любой корень 35-ой степени из единицы является корнем 3-ей степени некоторого корня 35-ой степени из единицы.
Ответ: *да, верно;*

б) Проведем такие же рассуждения, что и в пункте (а), в результате получим что:

$$k_1 = \frac{1}{3}(k + 36q)$$

Теперь: $36 \equiv 0\ mod\ 3 \Rightarrow \forall k\ \neg(\vdots)\ : \nexists k_1 \in \mathbb{Z} \hookrightarrow x = \sqrt[36]{1} \Rightarrow$ утверждение не верно для $n = 36$.
Ответ: *нет, не верно;*

2.1.2 Задача №2

C_{360} - циклическая группа порядка 360. *Найти число решений уравнения $x^k = e$ и количество элементов порядка k в группе C_{360} при:*
а) $k = 7$;
б) $k = 12$;
в) $k = 48$. *Сколько в C_{360} порождающих элементов*?

Решение:

C_{360} - циклическая группа порядка 360. Пусть x_0 - порождающий элемент.
Заметим, что элемент x_0^q является порождающим $\Leftrightarrow$ НОД(360,q) = 1.
Следовательно, всего порождающих элементов $\varphi(360) = 96$.

а) Дано: $x^7 = e$. Если элемент x_0^q ($q \in \mathbb{Z}$, $q < 360$) является решением данного уравнения, то должно выполняться равенство:

$$(x_0^q)^7 = x_0^{360p} \text{где } p \in \mathbb{N}_{\nvdash} \Rightarrow$$
$$\Rightarrow \left.\begin{array}{r} 7q = 360p \Rightarrow q = \dfrac{360}{7}p \\ q < 360 \end{array}\right\} \Rightarrow \frac{360}{7}p < 360 \Rightarrow p < 7$$

Заметим, что $q \in \mathbb{Z}$ только при $p = 0$, т.е. для $x = e \Rightarrow$ данное уравнение имеет 1 решение.
Элементов порядка 7 нет.
Ответ: *решений:* 1, *элементов порядка 7:* $\emptyset$

б) Дпно: $x^{12} = e \Rightarrow$

$$\Rightarrow \left.\begin{array}{r} (x_0^q)^{12} = x_0^{360p} \Rightarrow 12q = 360p \Rightarrow q = \dfrac{360}{12}p = 30p \\ q < 360 \end{array}\right\} \Rightarrow 30p < 360 \Rightarrow p < 12$$

Заметим, что $q \in \mathbb{Z}$ при всех $p = 0, 1, 2, \ldots, 11 \Rightarrow$ данное уравнение имеет 12 решений.
Элементов порядка 12 четыре: $x_0^{30}, x_0^{150}, x_0^{210}, x_0^{330}$.

Ответ: *решений:* 12, *элементов порядка 12:* $x_0^{30}, x_0^{150}, x_0^{210}, x_0^{330}$

в) Найдем $i_{min} \in (0; 360]$:

$$(a^{i_{min}})^{48} = e = a^{48i_{min}},$$

$$\text{т.е найдем:} \quad a^{48i_{\min}} = \frac{360}{\gcd(48i_{min},360)} = 1 \Rightarrow i_{min} = 15$$

Кол-во эл-тов порядка 48:

$$e = (a^x)^{48}$$

Порядок элемента циклической группы:

$$\text{ord } a^x = \frac{360}{\gcd(x, 360)} = 48 \Rightarrow x \gcd(x, 360) = 7{,}5 \Rightarrow$$

$$\Rightarrow \text{искомых элементов нет.}$$

Ответ: : $360/i_{min} = 24$, *элементов порядка:* $48 : \ 0$, кол-во пораждающих элем-тов в данной группе: 96.

2.1.3 Задача №3

Уравнение $x^{12} = e$ *имеет* 14 *решений в группе* G. *Доказать, что группа* G *не является циклической.*

Решение:

Допустим, что группа G – циклическая, и пусть g^i – минимальный x, удовлетворяющий

$$g^{12} = e \tag{2.2}$$

Тогда из условия следует, что все корни уравнения можно представить следующим образом:

$$g^i, g^{2i} \dots g^{14i}$$

Из 2.2 $\Rightarrow g^{12i} = e \Rightarrow g^{13i} = g^i$ – противоречие, т.к нет 14-ого корня.

2.1.4 Задача №4

Доказать, что в группе S_8 *нет элементов порядка* 56.

Решение:

Рассмотрим элемент группы S_8, т.е. перестановку из 8 чисел. Пусть внутри этой группы есть k циклов длиной $l_1, \dots, l_k$. Порядок перестановки равен НОКу длин циклов. Допустим, что в этой группе есть перестановка порядка 56, тогда $\text{НОК}(l_1, \dots, l_k) = 56 = 7 \cdot 8$. Значит в данной перестановке обязательно есть цикл длиной 7. Но тогда оставшееся число образует цикл длиной 1 и $\text{НОК}(l_1, \dots, l_k) = 7 \cdot 1 = 7 \neq 56$. Пришли к противоречию. Следовательно, в этой группе нет элемента порядка 56.

2.1.5 Задача №5

Найти порядок перестановки $(123)(4567)(89)$ *и количество сопряженных ей перестановок в группе* S_9. *Является ли эта перестановка четной?*

Решение:

Порядок перестановки $(123)(4567)(89) = \sigma$ опр-ся формулой:

$$\text{ord } \sigma = \text{НОК}(l_1,..l_n), \text{где } l_i - \text{длина } i\text{-ого цикла перестановки.} \tag{2.3}$$

Подставим в эту формулу длины наших циклов: $3, 4, 2,$ получим: ord σ = НОК(3,4,2) = 12. Заметим, что сопряженная перестановка - перестановка, имеющая ту же циклическую структуру, что и данная $\Rightarrow$ их кол-во будет опр-ся формулой:

$$amount = \frac{9!}{3 \cdot 4 \cdot 2} = 15120$$

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

В заданной перестановке σ кол-во циклов четной длины – четно, т.к. в ней $2 + 3 + 1 = 6$ инверсий:

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

$\Rightarrow \sigma$ –четная перестановка (перестановка чётна тогда и только тогда, когда в её цикловом разложении количество циклов чётной длины чётно).
Ответ: порядок перестановки: 12; кол-во сопряженных ей перестановок: $\frac{9!}{3 \cdot 4 \cdot 2}$; да, является.

2.1.6 Задача №6

Доказать, что все элементы порядка 11 сопряжены в S_{11}.

Доказательство:

Рассмотрим перестановки порядка 11 из группы S_{11}. Порядок перестановок равен НОКу длин циклов. Но 11 - простое число. Значит, в перестановках порядка 11 обязательно присутствует цикл длиной 11. Но элементы данной группы являются перестановками 11 чисел. Значит, перестановки порядка 11 имеют единственный цикл, следовательно, имеют одинаковую циклическую структуру и сопряжены друг с другом.

2.1.7 Задача №7

Порождают ли перестановки порядка 11 *группу* S_{11}?

Доказательство:

В предыдущей задаче было доказано, что в S_{11} все перестановки порядка 11 состоят из одного цикла. Значит, знак этих перестановок равен $(-1)^{11+1} = 1$, т.е. они четные. При произведении перестановок их знаки перемножаются. Значит, любая композиция перестановок порядка 11 будет четной. Но в группе S_{11} есть и нечетные перестановки. Например: (1 2 3 4 5 6 7 8 9 10)(11). Значит, перестановки порядка 11 не могут породить S_{11}.

2.1.8 Задача №8

Построить некоммутативную группу минимального порядка.

Решение:

Рассмотрим группу S_3, докажем, что она является некоммутативной группой минимального порядка 6:
S_3 - некомм-вна, приведем следующий пример: $(12)3 \times (123) = (213) \neq (23)1 = (123) \times (12)3$
Докажем, что группы порядка 1, 2, 3, и 5 являются комм-вными:
Заметим, что если порядок группы равен простому числу p, то всякий неединичный элемент имеет порядок p, тогда порождённая им циклическая подгруппа совпадает со всей группой $\Rightarrow$ эта группа – циклична $\Rightarrow$ группа – коммутативна.
Докажем теперь, что группа порядка 4 – комм-вна:
По теореме Лагранжа порядок любого эл-та либо 4, либо 2, либо 1. Если есть элемент порядка 4, то случай аналоген случаю выше. Рассомтрим случай, когда группа образована двумя пораждающими x и y порядка 2. Такакя группа всегда комм-вна: т.к. $x = x^{-1}$; $y = y^{-1}$, то $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$ – абелева группа. Получаем, что порядок 6 – минимальный для некоммутативных групп.

2.1.9 Задача №9

Вычислить:
а)12^{257} *mod* 17*;*
б)10^{111} *mod* 121.

Решение:

а) Заметим, что, из Теоремы (4) $\Rightarrow 12^{16} = 1 \ mod\ 17 \Rightarrow 12^{256} = 1 \ mod\ 17 \Rightarrow 12^{257} = 12 \ mod\ 17$.

Ответ: 12 *mod* 17

б) Из Теоремы (6) $\Rightarrow 10^{\phi(121)} = 1 \ mod\ 121$, $\phi(121) = 110 \Rightarrow 10^{110} = 1 \ mod\ 121 \Rightarrow 10^{111} = = 10 \ mod\ 121$.

Ответ: 10 *mod* 121

2.1.10 Задача №10

Найти порядок элемента (2,5) *в прямом произведении циклических групп* $C_{16} \times C_{12}$.

Решение:

Заметим, что у эл-нта 2 в группе C_{16} порядок – 8, а у эл-нта 5 в C_{12} – 12 $\Rightarrow$ ord (2,5) = НОК$(12, 8) = 24$ –это и будет искомый порядок эл-та (2,5) в циклической группе $C_{16} \times C_{12}$.
Ответ: 24.

2.1.11 Задача №11

Доказать, что группа вращений трехмерного куба изоморфна группе S_4.

Доказательство:

При поворотах куба место нижней грани может занять любая из 6 граней куба. Для каждого такого поворота имеется 4 различных расположения куба, соответствующих его поворотам вокруг оси, проходящей через центры верхней и нижней граней, на углы: 0, $\frac{\pi}{2}, \pi, \frac{3\pi}{2}$. Таким образом, получаем, что: $6 \cdot 4 = 24$ вращений куба $\Rightarrow ord D_4 = 24$, но $ord S_4 = 24 \Rightarrow$ можно построить биекцию между D_4 и S_4.

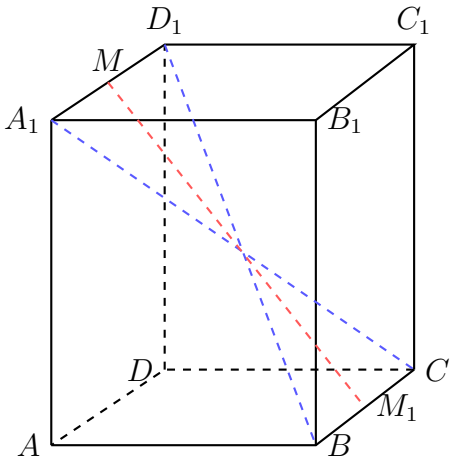

Рис. 2.1: Прямоугольный параллелепипед

При повороте относительно прямой MM_1, где M, M_1 - середины сторон A_1D_1, BC (см. Рис. 2.1). Диагонали A_1C, D_1B перейдут в себя, а другие главные диагонали поменяются - это соответсвует транспозиции в $S_4 \Rightarrow$ таким поворотом можно задать все транспозиции из $S_4 \Rightarrow$ и все перестановки в S_4, ч.т.д.

2.1.12 Задача №12

Пусть G – группа вращений трехмерного куба, а H_v – ее подгруппа, состоящая из тех вращений, которые оставляют вершину v на месте. Указать повороты на 90° и на 180° из одного левого смежного класса по подгруппе H_v .

Решение:

Пусть вершина v соответствует диагонали 1. H_v состоит из вращений, оставляющих данную вершину на месте, т.е. $H_v = \{e,(2\ 3),(2\ 4),(3\ 4),(2\ 3\ 4),(2\ 4\ 3)\}$.
Рассмотрим левый смежный класс по H_v с представителем $g = (1\ 2\ 3\ 4)$:
1. $(1\ 2\ 3\ 4)() = (1\ 2\ 3\ 4)$ – поворот на 90°
2. $(1\ 2\ 3\ 4)(2\ 3) = (1\ 2\ 4)$ – не поворот
3. $(1\ 2\ 3\ 4)(2\ 4) = (1\ 2)(3\ 4)$ – поворот на 180°
4. $(1\ 2\ 3\ 4)(3\ 4) = (1\ 2\ 3)$ – не поворот
5. $(1\ 2\ 3\ 4)(2\ 3\ 4) = (1\ 2\ 4\ 3)$ – поворот на 90°
6. $(1\ 2\ 3\ 4)(2\ 4\ 3) = (1\ 2)$ – поворот на 180°
$gH_v = \{(1\ 2\ 3\ 4),(1\ 2\ 4),(1\ 2)(3\ 4),(1\ 2\ 3),(1\ 2\ 4\ 3),(1\ 2)\}$.

Ответ: повороты на 90°: 1-ый и 5-ый элементы; повороты на 180° - 3-ий и 6-ой элементы.

2.1.13 Задача №13

Существует ли сюръективный гомоморфизм а) C_{2418} *на* C_{16}; б) $C_{25} \times C_{18}$ *на* C_{15}?

Решение:

а) $C_{24} \times C_{18} = C_8 \times C_3 \times C_9 \times C_2, C_{16}$
Предположим, что есть гомоморфизм $\varphi : C_{24} \times C_{18} \to C_{16}$. Тогда для $a \in C_{16}$ – порождающего элемента C_{16} $\exists\, x \in C_{24} \times C_{18} : \varphi(x) = a$. Тогда:

$$\left.\begin{aligned} \varphi(x^{ord\ x}) = \varphi(e) = e_1 \\ \varphi(x^{ord\ x}) = a^{ord\ x} \end{aligned}\right\} \implies ord\ x \vdots 16,$$

но в $C_{24} \times C_{18}$ нет элемента с таким порядком. Значит, гомоморфизма нет.
б)$C_{25} \times C_{18}, C_{15} = C_5 \times C_3$
Рассмотрим элемент $C_{25} \times C_{18}$ $g = (a,b) : a \in C_{25}, b \in C_{18}$. Введем покоординатные гомоморфизмы $\varphi_1 : C_{25} \to C_5$, $\varphi_2 : C_{18} \to C_3 : \varphi_1(a) = a^5, \varphi_2(b) = b^6$. Таким образом, задан гомоморфизм $\varphi : C_{25} \times C_{18} \to C_{15}$.

Ответ: а) нет, не существует; **б)** да, существует.

2.1.14 Задача №14

Доказать, что подгруппа, порожденная некоторым классом сопряженных элементов группы G, является нормальным делителем группы G.

Доказательство:

Рассмотрим подгруппу H, порожденную некоторым классом сопряженных элементов группы G, тогда $\forall h \in H \ \forall g \in G \hookrightarrow ghg^{-1} \in H$ (т.к. в H есть начальный элемент, из которого получена H, а при умножении на все остальные мы не выйдем за H в силу замкнутости)$\Leftrightarrow$ $\Leftrightarrow \forall g \in G \hookrightarrow gHg^{-1} = H \Leftrightarrow \forall g \in G \hookrightarrow gH = Hg$, т.е. H - нормальная подгруппа.

2.1.15 Задача №15

Найти число различных раскрасок ребер трехмерного куба в два цвета. Две раскраски считаются различными, если нельзя добиться совпадения цветов ребер вращениями куба.

Решение:

Решение задачи состоит в применении леммы Бернсайда. Группа вращений куба имеет порядок $|G| = 24$ и, как мы выяснили ранее, изоморфна S_4. Пусть X – множество всех раскрасок зафиксированного кубика. Найдем число орбит действия G. Для этого необходимо для каждого элемента группы G найти количество раскрасок, которые он оставляет на месте.
1. Тождественное преобразование оставляет на месте любую раскраску. Таких преобразований 1, $|X^2| = 2^{12}$.
2. Поворот вокруг оси, перпендикулярной грани куба, на 180° задает 6 транспозиций, в каждой по 2 ребра. Таких преобразований 3, $|X^3| = 2^6$.
3).Поворот вокруг оси, перпендикулярной грани куба, на 90° задает 3 цикла, в каждом по 4 ребра. Таких преобразований 6, $|X^2| = 2^3$.
4).Поворотов вокруг оси, перпендикулярной паре ребер, на 180° задает 5 транспозиций, в каждой по 2 ребра, и еще оставляет 2 ребра на месте. Таких преобразований 6, $|X^4| = 2^7$.
6).Поворот вокруг главной диагонали куба на 120° задает четыре цикла, в каждом по 3 ребра. Всего таких преобразований 8, $|X^5| = 2^4$.
Значит, всего таких раскрасок:

$$\frac{2^{12} + 3 \cdot 2^6 + 6 \cdot 2^3 + 6 \cdot 2^7 + 8 \cdot 2^4}{24} = 218$$

2.1.16 Задача №16

а) *Построить гомоморфизм φ аддитивной группы рациональных чисел $(Q,+)$, ядром которого является подгруппа целых чисел $(Z,+)$.*
б) *Проверить, что $(Q,+)/Ker\varphi$ бесконечна, но все ее элементы имеют конечный порядок.*

Решение:

Построим гомоморфизм из $(\mathbb{Q},+)$ в группу корней из единицы $(A,\cdot)$ по правилу:
$\forall q \in \mathbb{Q}\ \exists m \in \mathbb{Z}, n \in \mathbb{N} : q = \frac{m}{n} \Rightarrow \varphi(q) = \varphi(\frac{m}{n}) = \cos(\frac{2\pi m}{n}) + i\sin(\frac{2\pi m}{n})$
Тогда $\forall z \in \mathbb{Z} \to \varphi(z) = \cos(2\pi z) + i\sin(2\pi z) = 1$ - нейтральный в $(A,\cdot)$, т.е. $(\mathbb{Z},+) = Ker\varphi$.
По теореме о гомоморфизмах $(\mathbb{Q},+)/Ker\varphi \cong (A,\cdot)$, а группа $(A,\cdot)$, очевидно, бесконечна.
Понятно, что порядок любого элемента $|\cos(\frac{2\pi m}{n}) + i\sin(\frac{2\pi m}{n})| \leq n \in \mathbb{Z}$, т.е. конечен.

2.1.17 Задача №17

Доказать, что если элемент a кольца R не является делителем нуля, то из $ax = ay$ следует $x = y$. И наоборот: если элемент a кольца R является делителем нуля, то для некоторых $x \neq y$ выполняется $ax = ay$.

Доказательство:

Пусть $a \neq 0 \in R$ не является делителем нуля и выполнено равенство $ax = ay$. Тогда, воспользовавшись дистрибутивностью вычитания, получим $ax - ay = a(x-y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$.
Пусть $a \neq 0 \in R$ – делитель нуля. Тогда по определению $\exists\ x \neq 0 : ax = 0$. С другой стороны $\exists\ y = 0 : ay = 0$. Таким образом, $\exists\ x,y : x \neq y, ax = ay$.

2.1.18 Задача №18

Ненулевой элемент кольца называется нильпотентным, если $x^n = 0$ при некотором n. Показать, что:
а)*нильпотентность x влечет обратимость $1 - x$, если K – кольцо с единицей;*
б)*кольцо $Z_m = Z/m$ Z содержит нильпотентные элементы в том и только том случае, если m делится на квадрат натурального числа, большего единицы;*
в)*множество нильпотентных элементов коммутативного кольца вместе с нулевым элементом образует подкольцо. Привести опровергающий пример в некоммутативном случае.*

Решение:

а) $x^n = 0 \Leftrightarrow 1 - x^k = (1-x)(1 + x + x^2 + \ldots + x^{n-1}) = 1 \Leftrightarrow 1 - x$ - левый обратный,
аналогично, $1 - x$ - правый обратный, значит $1 - x$ обратим.

б) т.к. $a^n = 0, n > 1 \Leftrightarrow m|a^n \Leftrightarrow p_i|a$, $p_j|a$, где p_i, p_j – простые делители m, $p_i \neq p_j \Leftrightarrow m|a^2$.

в) Пусть $a^k = 0$, $b^n = 0$ - нильпотенты $\Rightarrow (a+b)^{n+k} = 0$, т.к. в каждом слагаемом степень a или b будет больше k или n, соответсвенно, $\Rightarrow$ все они раны $0 \Rightarrow$ нильпотенты образуют группу по умножению.

Проверим замкнутость относительно сложения, для этого покажем замнутость взятия противоположного:
Т.к. кольцо коммутативно, то:

$$(ab)(a+b) = a^2 + (b)a + ab + (b)b = a^2 + (b)b + a((b) + b) = a^2 + (b)b,$$
$$\text{т.к.} - b^2 = (b)b, \left(b^2 - b^2 = b^2 + (-b)b = (b-b)b = 0\right)$$
$$\Rightarrow a^2 + (-a)^2 = (a + (-a))(a - (-a)) = 0 \cdot 2a = 0$$
$$\text{учитывая, что } a^n = 0 \Rightarrow (-a)^{2n} = ((-a)^2)^n = a^{2n} = 0.$$

2.1.19 Задача №19

Является ли кольцом главных идеалов кольцо Z_{72}?

Решение:

Пусть есть произвольный идеал $I \in Z_{72}$. Рассмотрим n - минимальный элемент этого идеала.
1. По определению $nZ_{72} \subset I$.
2. Докажем, что $nZ_{72} \supset I$. Предположим противное: $\exists m : m \in I \wedge m \notin nZ_{72}$. Разделив m на n с остатком, получим:

$$\left.\begin{array}{r} m = pn + r, 0 < r < n \\ m \in I \wedge n \in I \end{array}\right\} \Rightarrow r \in I$$

Таким образом, мы нашли число, лежащее в I и меньшее n. Пришли к противоречию. Значит, $nZ_{72} \supset I$.
Таким образом, $nZ_{72} \subset I$ и $nZ_{72} \supset I \Rightarrow nZ_{72} = I \Rightarrow I = (n)$, т.е. произвольный идеал оказался главным $\Rightarrow Z_{72}$ – кольцо главных идеалов.

2.1.20 Задача №20

Решить линейное диофантово уравнение $33x + 23y = 4$.

Решение:

$$\begin{cases} a_0 = 33 \\ a_1 = 23 \end{cases} \Rightarrow \begin{cases} a_2 = 1 \cdot 33 - 1 \cdot 23 = 10 \\ a_3 = 1 \cdot 23 - 2 \cdot 10 = 3 \\ a_4 = 1 \cdot 10 - 3 \cdot 3 = 1 \end{cases}$$

$1 = 1 \cdot 10 - 3 \cdot 3 = 1 \cdot 10 - 3(23 - 2 \cdot 10) = 7 \cdot 10 - 3 \cdot 23 = 7(33 - 23) - 3 \cdot 23 = 7 \cdot 33 - 10 \cdot 23 \Rightarrow$
$4 = 28 \cdot 33 - 40 \cdot 23 \Rightarrow$

$$\Rightarrow x = 28 + 23c,\ y = -40 - 33c.$$

2.1.21 Задача №21

Решить сравнения: $21x \equiv 13 \ mod\ 34$, $7x \equiv 2 \ mod\ 73$.

Решение:

а) $21x \equiv 13 \bmod 34 \Rightarrow 21x + 34y = 13$:

$$\begin{cases} a_0 = 34 \\ a_1 = 21 \end{cases} \Rightarrow a_2 = 1 \cdot 34 - 1 \cdot 21 = 13 \Rightarrow 34 - 21 = 13 \Rightarrow$$

$$\Rightarrow x = 34k - 1.$$

б) $7x \equiv 2 \bmod 73 \Rightarrow 7x + 73y = 2$:

$$\begin{cases} a_0 = 73 \\ a_1 = 7 \end{cases} \Rightarrow \begin{cases} a_2 = 1 \cdot 73 - 10 \cdot 7 = 3 \\ a_3 = 1 \cdot 7 - 2 \cdot 3 = 1 \end{cases} \Rightarrow 2 = 2 \cdot 7 - 4 \cdot 3 = 2 \cdot 7 - 4(73 - 10 \cdot 7) = 42 \cdot 7 - 4 \cdot 73 \Rightarrow$$

$$\Rightarrow x = 73k + 42$$

2.1.22 Задача №22

Решить систему сравнений

a. $x \equiv 1 \bmod 33$,

b. $x \equiv -1 \bmod 23$.

Решение:

$$\begin{cases} x \equiv 1 \ mod\ 33 \\ x \equiv -1 \ mod\ 23 \end{cases} \Rightarrow \begin{cases} x = 33k + 1 \\ x = 23n - 1 \end{cases} \Rightarrow 33k \equiv -2 \ mod\ 23 \Rightarrow 33k \equiv 21 \ mod\ 23 \Rightarrow 11k \equiv$$

$\equiv 7 \ mod\ 23 \Rightarrow 11k \equiv 99 \ mod\ 23 \Rightarrow k \equiv 9 \ mod\ 23 \Rightarrow k = 23c{+}9 \Rightarrow x = 33(23c{+}9){+}1 = 759c{+}298$

2.1.23 Задача №23

Найти наибольший общий делитель многочленов $x^{48} - 1$ *и* $x^{20} - 1$.

Решение:

Пусть $f(x) = x^{48} - 1$, $g(x) = x^{20} - 1$
Будем пользоваться алгоритмом Евклида:

$$x^{48} - 1 = (x^{20} - 1)(x^{28} + x^8) + (x^8 - 1)$$
$$x^{20} - 1 = (x^8 - 1)(x^{12} + x^4) + (x^4 - 1)$$
$$x^8 - 1 = (x^4 - 1)(x^4 + 1) + 0$$
$$\Rightarrow \text{НОД}(f(x),g(x)) = x^4 - 1$$

2.1.24 Задача №24

Найти порядок группы обратимых элементов кольца Z_{72}.

Решение:

Пусть элемент x кольца вычетов Z_p обратим, т.е. существует такое целое число a, что $xa = 1 + pq, q \in \mathbb{Z} \Rightarrow a = \frac{1+pq}{x}$. Пусть p и x не взаимно просты, т.е. $p = bp_1, x = bx_1$. Тогда $bp_1q \equiv 0 \bmod b \Rightarrow bp_1q + 1 \equiv 1 \bmod b \Rightarrow$ такого a не существует. Если p и x взаимно просты, то всегда найдется такое q, что $x|(1 + pq)$. Пришли к следующему утверждению: элемент x кольца вычетов Z_p обратим $\Leftrightarrow x$ и p взаимно просты, т.е. НОД(x,p) = 1. Количество элементов x, меньших p и взаимно простых с ним, равно функции Эйлера $\varphi(p) = \varphi(72) = 24$. Значит, порядок группы обратимых элементов данного кольца равен 24.

2.1.25 Задача №25

Сумма идеалов $I_1 + I_2$ – это идеал, порожденный всеми суммами элементов из идеалов I_1, I_2 . Аналогично, произведение идеалов I_1I_2 – это идеал, порожденный всеми произведениями элементов из I_1, I_2 . Пусть I_1 порожден в $Q[x]$ многочленом $x^2 - x$, а I_2 порожден многочленом $x^2 + x$. Найти $I_1 + I_2, I_1I_2, I1 \cap I2$.

Решение:

Дано:

$$I_1 = \{(x^2 - x)p(x) \mid p(x) \in Q[x]\}$$
$$I_2 = \{(x^2 + x)p(x) \mid p(x) \in Q[x]\}$$

1. Любая сумма элементов из I_1 и I_2 делится на x

$$\Rightarrow I_1 + I_2 \subseteq (x)$$

Рассмотрим произвольный элемент $x \cdot r \in (x)$:

$$x \cdot r = \frac{1}{2}(x^2 + x) \cdot r - \frac{1}{2}(x^2 - x) \cdot r \in I_1 + I_2$$

Получается, что:

$$I_1 + I_2 \supseteq (x) \Rightarrow I_1 + I_2 = (x).$$

2. Каждый элемент из I_1I_2 имеет вид $(x^2 + x)(x^2 - x)p(x)q(x) \Rightarrow$

$$\Rightarrow I_1I_2 \subseteq (x^4 - x^2)$$

Произвольный элемент $(x^4 - x^2)p(x) \in (x^4 - x^2)$ может быть представлен как

$$(x^4 - x^2)p(x) = (x^2 + x) \cdot (x^2 - x) \cdot p(x) \Rightarrow$$

$$\Rightarrow I_1I_2 \supseteq (x^4 - x^2)$$

То есть:

$$I_1I_2 = (x^4 - x^2).$$

3. Эл-нт прин-жит $I_1 \Leftrightarrow$ он дел-ся на $x(x-1)$.
Эл-нт прин-жит $I_2 \Leftrightarrow$ он дел-ся на $x(x+1)$.
Если эл-нт имеет вид $x(x^2-1)p(x)$, то он лежит в $I_1 \cap I_2$.
Обратно, если эл-нт $\in I_1 \cap I_2$, то он имеет такой вид, поскольку дел-ся на (x^2-x) и $(x^2+x) \Rightarrow$

$$\Rightarrow I_1 \cap I_2 = (x^3 - x).$$

2.1.26 Задача №26

Являются ли полями следующие кольца вычетов:
а) $Q[x]/(x^3+1)$; б) $F_3[x]/(x^3+2)$; в) $F_7[x]/(x^3+3)$;
г) $Q[x]/(x^4+1)$; д) $F_3[x]/(x^4+1)$; е) $F_{17}[x]/(x^4+1)$?

Решение:

Кольцо вычетов по модулю идеала является полем тогда и только тогда, когда идеал максимален. Задача сводится к проверке максимальности идеалов.

а) В кольце Q вып-тся:

$$(x^3+1) \subset (x+1)$$

Следует заметить, что обратного включения нет $\Rightarrow$ идеал не максимален $\Rightarrow$ кольцо $Q[x]/(x^3+$ $+1)$ не яв-тся полем.
б) В поле F_3 вып-тся:

$$x^3+2 = (x+2)(x^2+x+1) \Rightarrow (x^3+2) \subset (x+2)$$

Заметим, что обратоного включения нет $\Rightarrow$ идеал не максимален $\Rightarrow$ кольцо $F_3/(x^3+2)$ не яв-тся полем.
в) Многочлен x^3+3 не имеет корней в поле $F_7 \Rightarrow$ он неприводим, т.к. он 3 степени $\Rightarrow$ порождаемый им идеал максимален $\Rightarrow$ кольцо $F_7/(x^3+3)$ яв-тся полем.
г) Многочлен x^4+1 не имеет корней в Q. Докажем, что он неприводим. Предположим, что существует разложение:

$$x^4+1 = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(b+ac+d)x^2+(bc+ad)x+bd$$

Полученная система их четырех уравнений с 4-мя неизвестными имеет 1 решение в действительных числах:

$$a = \sqrt{2}, b = 1, c = -\sqrt{2}, d = 1$$

Что означает, что система не имеет решений в рациональных числах $\Rightarrow$ идеал максимален $\Rightarrow$ кольцо $Q[x]/(x^4+1)$ яв-тся полем.
д) Непосредственной подстановкой убеждаемся, что x^4+1 не имеет корней в F_3. Но при этом выполняется:

$$x^4+1 = (x^2+2x+2)(x^2+x+2)$$

$\Rightarrow$ идеал не максимален, а кольцо $F_3/(x^4+1)$ не яв-тся полем.
е) В поле F_{17} выполняется:

$$x^4+1 = (x+15)(x^3+2x^2+4x+8)$$

Идеал не максимален, поэтому кольцо $F_{17}/(x^4+1)$ не является полем.

2.1.27 Задача №27

Многочлен $f(x)$ над полем F_5 степени 2 принимает значение 1 в точке 1, значение 2 в точке 3 и значение 3 в точке 4. Найти $f(x)$.

Решение:

Пусть:

$$f(x) = ax^2 + bx + c$$

Подставляем известные точки и воспользуемся свойствами поля F_5:

$$f(1) = a + b + c = 1;$$

$$f(3) = 9a + 3b + c = 4a + 3b + c = 2;$$

$$f(4) = 16a + 4b + c = a + 4b + c = 3$$

Вычтем из третьего уравнения первое и второе:

$$-4a - c = a - c = 0 \Rightarrow a = c$$

Подставим полученное во второе уравнение:

$$5a + 3b = 3b = 2 \Rightarrow b = 4$$

Теперь подставим полученное в первое уравнение:

$$2a = -3 = 2 \Rightarrow a = c = 1$$

Итак, искомый многочлен:

$$f(x) = x^2 + 4x + 1$$

2.1.28 Задача №28

Ненулевой элемент a поля $Z_p = Z/p\ Z$ называется квадратичным вычетом по модулю p, если уравнение $x^2 = a$ имеет решение в поле Z_p. В противном случае a называется квадратичным невычетом. а) *Найти сумму всех квадратичных вычетов по модулю* 73. б) *Найти произведение всех квадратичных невычетов по модулю* 103.

Решение:

а) квадратичные вычеты – квадраты чисел от 0 до $(p-1)/2 = 36$.

$$0^2 + 1^2 + \ldots + 36^2 = \frac{36 \cdot 37 \cdot 73}{6} \equiv 0(mod 73)$$

б) Найдем сначала произведение всех ненулевых квадратичных вычетов. Воспользуемся теоремой Вильсона. Оно будет равно:

$$\prod_{i=1}^{51} i^2 = (-1)^5 1 \cdot \prod_{i=1}^{102} i = 102! \cdot (-1)^5 1 = (-1)^5 2 = 1$$

Теперь найдем произведение всех ненулевых остатков:

$$\prod_{i=1}^{102} i = 102! = -1;$$

Если x - искомое произведение всех квадратичных невычетов, то выполняется:

$$-1 = 1 \cdot x$$

Итак, получается:

$$x = -1$$

2.2 Дополнительные задачи

2.2.1 Задача №1

Построить группу G, в которой уравнение $x^12 = e$ имеет ровно 14 решений.

Решение:

Докажем, что группа $G = C_{84} \cdot C_2$ имеет ровно 14 решений уравнеия $x^{12} = e$.
Давайте найдем кол-во решений данного уравнения в C_{84} и C_2:

В C_{84} это все элементы у которых порядок $\vdots 12$, различных решений ровно 7.
В то время как в C_2 очевидным образом все 2 эл-та явл-ся решениями.
Элемент из $C_{84} \cdot C_2$ это пара $(a, b),\ a \in C_{84},\ b \in C_2$.
Кол-во решений исходного ур-ия - это произведение подгруп решений в C_{84} и C_2:

$$C_7 \cdot C_2 = C_{14} - 14 \text{ различных решений.}$$

2.2.2 Задача №2

Пусть G – группа, порожденная элементами и b, для которых выполняются соотношения $ab = ba$, $a^2 = b^2$, $a^4b^4 = e$. Найти порядок группы G. Является ли эта группа циклической?

Решение:

Будем использовать операотр сложения вместо оператора $\times$ оператор $+$. Запишим эти соотношения в матричном виде: $A = \begin{pmatrix} 4 & 4 \\ 2 & -2 \end{pmatrix} \Rightarrow |detA| = 16 \Rightarrow$ порядок данной группы 16.

2.2.3 Задача №3

Построить подгруппу порядка 56 группы S_8. (Указание: исполь- зуйте поле из 8 элементов.)?

Решение:

Нам дано поле F_8 из 8-ми элементов, рассмотрим его и отображение в себя $f : f(x) = ax + b$, где $a \in F^*, b$,$x \in F$. Так как есть правило деления (существования обратного эл-та) для полей $\Rightarrow\ \exists$ обратная функция. Заметим, что для того чтобы $\exists$ обратная функция необходимо, чтобы f была биективной $\Rightarrow$ это преобразование задает некоторую перестановку элементов этого поля. Заметим, что всего таких функций возможно: $|f| = |F * ||F| = 56$. Остается доказать, что это группа:
Замкнутость и ассоциативность очевидна;
Существование нейтральной – $f_0 = 1x + 0$; Существование обратной – $f^{-1} = a^{-1}x + (-a)b^{-1}$
Т.к все четыре условия вып-ны $\Rightarrow$ это группа порядка 56, которая переставляет 8 эл-тов, т.е подгруппа в S_8.

2.2.4 Задача №4

Указать две несопряженные изоморфные подгруппы порядка 12 в S_{11}.

Решение:

Рассмотрим группу A_4: $A_4 \subseteq S_4 \subseteq S_{11}$
Т.к. A_4 - четные перестановки на {1, 2, 3, 4} - $\phi(g)$, то можно рассмотреть так же A_4 как четные перестановки на {5, 6, 7, 8} - $\psi(g)$.
Рассмотрим их как независмые перестановки $\Rightarrow$ они коммутируют $\Rightarrow \psi(g)\phi(g) \subseteq S_{11}$.
Такие подгруппы не будут сопряжены, так как в S_n сопряжённые элементы имеют одинаковое циклическое строение. Поэтому произведение двух тройных циклов не будет сопряжено S_4.

2.2.5 Задача №5

Доказать, что если – собственная подгруппа конечной группы G, то объединение сопряженных с подгрупп не содержит всех элементов группы.

Решение:

Пусть $H_1, \dots H_m$ - сопряженные с , в каждой такой подгруппе $h \leq |G|$ элментов, тогда в обединении mh элементов, но $|G| = n \cdot h$, где n - индекс группы G.
От противного: $G = H_1 \cup \dots \cup H_m \Rightarrow |G| \leq |H_1| + \dots |H_m| \Rightarrow |G| = nh \leq m \cdot h \Rightarrow m \leq n$
Если объединение сопряженных с H групп содержит все элементы, то $m = n$ и нет пересечений у подмножеств.
Но, как минимум, единичный элемент входит во все сопряженные группы, значит мы его посчитали m раз $\Rightarrow$ равенство точно не может достигаться. Предположение неверно.

2.2.6 Задача №6

Пусть G – абелева группа и – подгруппа всех ее элементов конечного порядка. Тогда в фактор–группе G/H все неединичные элементы имеют бесконечный порядок.

Решение:

Пусть gH - элемент факторгруппы G/H.
$gH \neq e$ ($gH \neq H$) $\Leftrightarrow$ g $\notin H$
(Если $g \notin H$, то $g \in gH(ge) \Rightarrow$ по Th. Лагранжа H и gH не пересекаются).
Предположим, что $\exists\ g \notin H$, $h \in H:\ ord(gh) = n \in Z$
$\exists n:\ (gh)^n = e = g^n h^n \Rightarrow g^n = (h^n)^{-1} \in H$.
Получили противоречие, предположение неверно, значит, элементы не имеют конечного порядка.

2.2.7 Задача №7

Укажите такую абелеву группу G и две такие ее изоморфные подгруппы H_1, H_2, что фактор–группы G/H_1 и G/H_2 неизоморфны.

Решение:

Фактор-группа G/H абелева $\Leftrightarrow \forall x,y \in G \to Hxy = Hyx \Leftrightarrow \forall x,y \in G \to Hxyx^{-1}y^{-1} = H \Leftrightarrow \forall x,y \in G \to xyx^{-1}y^{-1} \in H \Leftrightarrow$ H содержит коммутант группы G.

2.2.8 Задача №8

Доказать, что группа автоморфизмов циклической группы абелева. Найти порядок группы автоморфизмов циклической группы порядка 12. *Является ли эта группа циклической*?

Доказательство:

Автоморфизм циклической группы однозначно задается образом порождающего ($\phi(a) = a^p$, следовтельно, из свойств изоморфизма $\phi(a^t) = a^{qt}$). Рассмотрим два автоморфизма: $\phi_1(a) = a^p$, и $\phi_2(a) = a^q$. Покажем, что группа таких автоморфизмов - абелева:

$$\phi_1\phi_2(a) = \phi_1(a^p) = a^{pq} = \phi_2(a^q) = \phi_2\phi_1(a)$$

Таким образом группа автоморфизмов абелева (факт, что это группа - очевиден).
Чтобы $\phi(a) = a^p$, где a – порождающий, был автоморыизмом необходимо и лдостаточно, чтобы a^p был также порождающим (в ином случае при отображении мы не получим всю группу – нарушается биекция). В группе C_{12} – 4 порождающих, т.к, как было выяснено, автоморфизм однозначно задается отображением порождающего в порождающий следует, что порядок группы автоморфизмов C_{12} равен 4.
Рассморим эту группу автоморфизмов C_{12}: $\{\phi_1(a) = a, \phi_5(a) = a^5, \phi_7(a) = a^7, \phi_{11}(a) = a11$. Порядок элементов $\phi_1, \phi_5, \phi_7, \phi_1 1$ равны 2, так как $\phi_1^2(a) = a = \phi_5^2(a) = a^{25} = \phi_7(a) = a^{49} = \phi_{11}^2(a) = a^{121}$, откуда следует, что данная группа автоморфизмов не циклическая – нет элемента порядка группы – элемента порядка 4.

2.2.9 Задача №9

Доказать, что нормальная подгруппа индекса k содержит все элементы, порядки которых взаимно просты с k.

Доказательство:

Пусть у нас есть H – нормальная подгруппа G, причем ее индекс равен m. Пусть у нас также есть x, порядок которого n, НОД(n,m) = 1:

$$x^n = e \in H$$

Фактор-группа G/H имеет порядок m, поэтому $(xH)^m = H$. Воспользуемся нормальностью подгруппы:

$$(xH)^m = x^m H = H \implies x^m \in H$$

Поскольку m и n взаимно просты, существует такие целые числа x, y, что

$$mx + ny = 1$$

Возведем в эту степень x:

$$x = x^1 = (x^m)^x \cdot (x^n)^y \in H$$

Утверждение доказано.

2.2.10 Задача №11

Доказать, число элементов, сопряженных с элементом a в группе G, равно индексу $N(a)$ в группе G, т.е. числу смежных классов по подгруппе $N(a)$ – нормализатору элемента a:

$$N(a) = (g|\ ga = ag\ \forall g \in G).$$

Доказательство:

Требуется доказать, что число элементов, сопряженных с a, равно индексу $N(a)$. Рассмотрим действие группы G на элемент a: $g(a) = gag^{-1}$. Размер орбиты данного действия равен числу элементов, сопряженных с элементом a. Рассмотрим стабилизатор действия: $Stab_a = \{g \in G : gag^{-1} = a\} = \{g \in G : ga = ag\} = N(a) \Rightarrow |N(a)| = |Stab_a|$. Тогда в силу соотношения $|G| = |Stab_a||Orb_a|$ и теоремы Лагранжа получаем:

$$(G : N(a)) = \frac{|G|}{|N(a)|} = \frac{|G|}{|Stab_a|} = |Orb_a|$$

что и требовалось доказать.

2.2.11 Задача №12

Коммутант группы – это подгруппа, порожденная коммутаторами, то есть элементами вида $xyx^{-1}y^{-1}$. Доказать, что коммутант является нормальной подгруппой.

Доказательство:

Подгруппа H является нормальной $\Leftrightarrow \forall g \in G \hookrightarrow gH = Hg \Leftrightarrow \forall g \in G \hookrightarrow gHg^{-1} = H \Leftrightarrow \forall g \in$
$\in G\ \forall h \in H \hookrightarrow ghg^{-1} \in H$
Докажем последнее утверждение для коммутанта группы:
$\forall g \in G\, \forall h = xyx^{-1}y^{-1} \in H \hookrightarrow g(xyx^{-1}y^{-1})g^{-1} = gxeyex^{-1}ey^{-1}g^{-1} = gx(g^{-1}g)y(g^{-1}g)x^{-1}(g^{-1}g)y^{-1}g^{-1} =$
$= (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} \in H$, что и требовалось доказать.

2.2.12 Задача №13

Доказать, что фактор–группа G/H абелева тогда и только тогда, когда H содержит коммутант K группы G.

Доказательство:

Фактор-группа G/H абелева $\Leftrightarrow \forall x,y \in G \hookrightarrow Hxy = Hyx \Leftrightarrow \forall x,y \in G \hookrightarrow Hxyx^{-1}y^{-1} = H \Leftrightarrow$ $\Leftrightarrow \forall x,y \in G \hookrightarrow xyx^{-1}y^{-1} \in H \Leftrightarrow$ H содержит коммутант группы G.

2.2.13 Задача №15

Группа называется p–группой, если ее порядок является степенью простого числа p. Центром группы называется множество элементов, коммутирующих со всеми элементами группы. Доказать, что центр p–группы состоит не только из единичного элемента.

Доказательство:

Обозначим центр как Z. Рассмотрим разбиение группы G на классы сопряженности. Они не пересекаются, и при этом в объединении дают всю группу. Кроме того, элемент принадлежит центру $\Leftrightarrow$ его класс состоит только из него самого:

$$h^{-1}gh = g \Leftrightarrow hg = gh \ \forall h \in G$$

Нам нужно доказать, что есть больше одного класса сопряженности из одного элемента. Докажем, что мощность класса сопряженности делит порядок группы. Рассмотрим произвольный элемент x. Докажем, что каждый элемент, сопряженный ему, задает свой смежный класс по его централизатору. Пусть есть такие h_1, h_2, что

$$h_1^{-1}xh_1 = h_2^{-1}xh_2 \Leftrightarrow xh_1h_2^{-1} = h_1h_2^{-1}x \Leftrightarrow h_1h_2^{-1} \in C(x) \Leftrightarrow C(x)h_1 = C(x)h_2$$

Отсюда следует, что число элементов в классе сопряженности x равно индексу централизатора, который делит порядок группы. Мы получили, что порядок группыы представляется в виде суммы:

$$|G| = a_0 + a_1p + a_2p^2 + \ldots = p^n$$

При этом в центре лежит e, поэтому $a_0 > 0$. Получается, что $a_0 = kp, k > 0$, т.е. $a_0 > 1$, что и требовалось доказать.

2.2.14 Задача №16

Доказать, что всякая группа порядка p^2, где p – простое число, абелева.

Доказательство:

Мы знаем, что у такой группы нетривиальный центр. Его порядок делит p^2, т.е. он равен или p, или p^2. Второй случай равносилен тому, что группа абелева. Осталось рассмотреть первый случай. Факторгруппа G/Z будет иметь порядок p, т.е. будет циклической. У нее есть образующий элемент gZ. Докажем, что тогда любая пара элементов G перестановочна. Пусть есть $h_1 \in G, h_2 \in Z$. Они представимы как

$$h_1 = g^i z_1, h_2 = g^j z_2, z_1, z_2 \in Z$$

$$h_1 h_2 = g^i z_1 g^j z_2 = g^j z_2 g^i z_1 = h_2 h_1$$

Откуда следует, что центр должен совпадать со всей группой, что дает противоречие. Утверждение доказано.

2.2.15 Задача №19

Указать пример коммутативного кольца с единицей R и его под кольца R_1 таких, что R_1 также является кольцом с единицей и, но $1 \neq u$.

Решение:

Рассмотрим декартово произведение $R = \mathbb{Z} \times \mathbb{Z} = \{(x, y) \mid x, y \in \mathbb{Z}\}$. Введем на нем операции $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ и $(x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot x_2, y_1 \cdot y_2)$. Получили кольцо с единицей $(1, 1)$. Теперь рассмотрим его подкольцо $R_1 = \{(x, 0) \mid x \in \mathbb{Z}\}$. Единицей данного подкольца является элемент (1,0) $\neq$ (1,1).

2.2.16 Задача №20

Построить кольцо из 21 элемента, в котором произведения принимают ровно три различных значения.

Решение:

Введем кольцо:

$\mathbb{Z}_7^{'} = (\{0,1,2,3,4,5,6\}, +\, mod\, 7, \times')$, где операция$\times'$ каждой паре элементов ставит в соответствие 0 :

$$\forall a,b \in \mathbb{Z}_7^{'} \to a \times' b = 0$$

Это кольцо, т.к. выполняются свойства полугруппы по умножению и дистрибутивность.
Умножим кольцо R на кольцо $\mathbb{Z}_3$ и обозначим полученное через $R^{'}$. Тогда в кольце $R^{'}$ будет ровно $7 \cdot 3 = 21$ элемент, и произведения в нем будут принимать 3 значения:

$$\forall a,b \in R^{'} \to a \cdot b \in \{(0,0),(0,1),(0,2)\}$$

2.2.17 Задача №21

В коммутативном кольце R с $0 \neq 1$ $x^2 = 2$ имеет три различных решения. Доказать, что в R есть делители нуля.

Решение:

Пусть y - одно из решений уравнения $x^2 = 2$. Тогда $x^2 = y^2 \Leftrightarrow x^2 - y^2 = 0 \Leftrightarrow (x-y)(x+y) = 0$. Если в R нет делителей нуля, то $x = y$ или $x = -y$, т.е. уравнение $x^2 = 2$ имеет всего лишь 2 корня, что противоречит условию. Значит, в кольце R есть делители нуля.

2.2.18 Задача №22

Доказать, что кольцо гауссовых целых чисел

$$Z(i) = \{a + bi : \ a, b - -\text{целые}\}, i^2 = -1,$$

евклидово.

Доказательство:

Введем норму в $Z(i)$:
$N(a + bi) = a^2 + b^2$
$N((a + bi)(c + di)) = N((ac - bd) + i(bc + ad)) = (ac - bd)^2 + (bc + ad)^2 = a^2c^2 - 2abcd + b^2d^2 +$
$+ b^2c^2 + 2abcd + a^2d^2 = (a^2 + b^2)(c^2 + d^2) = N(a + bi)N(c + di)$
Теперь определим деление с остатком. Пусть нужно разделить два числа:

$$\frac{a + bi}{c + di} = \frac{(ac + bd) + i(bc - ad)}{c^2 + d^2}$$

Разделим оба слагаемых с остатком как обычные целые числа. Тогда норма остатка будет удовлетворять неравенству:

$$N(r) < \frac{N(c^2 + d^2)}{N(c + di)} = N(c + di)$$

Что и требуется при делении с остатком. Итак, $Z(i)$ - евклидово кольцо.

2.2.19 Задача №23

Проверить простоту элементов $17, 11, 2 + 3i$ *в кольце* $Z(i)$.

Решение:

Обратные элементы в кольце: $Z(i)^* = \{\pm 1, \pm i\}$.
17: Разложим 17 на необратимые множители:
$17 = (4 + i)(4 - i)$
17 – составное число.
11: Предположим, что
$11 = (a + bi)(c + di)$
$121 = (a^2 + b^2)(c^2 + d^2)$

11 не раскладывается в сумму двух полных квадратов $\Rightarrow$ обе скобки не могут быть равны 11. Если одна скобка равна 1, то соответствующий элемент будет обратим. Таким образом, 11 – простое число.
2 + 3i: Аналогично:
$2 + 3i = (a + bi)(c + di)$
$13 = (a^2 + b^2)(c^2 + d^2)$
Один из множителей должен быть равен 1, что влечет за собой обратимость элемента. Значит, $2 + 3i$ – простое число.

2.2.20 Задача №24

Является ли кольцо $Z(j) = \{a + bj : \ a, b -$ целые$\}, j^2 = -6$, *евклидовым кольцом*?

Решение:

Обратимые элементы в кольце $Z(j)$ – множество $\{\pm 1\}$. Рассмотрим число 10:

$$10 = 2 \cdot 5 = (2 - j)(2 + j)$$

Проверим, что число 2 не кратно ни одной из этих скобок:

$$2 = (2 - j)(a + bj) = 2a + 6b + j(2b - a) = 5a$$

Не имеет решений в целых числах:

$$2 = (2 + j)(a + bj) = 2a - 6b + j(2b + a) = 5a$$

Опять же не имеет делителей в целых числах.Проверим то же для 5:

$$5 = (2 - j)(a + bj) = 5a = 10b$$

Не имеет решений в целых числах.

$$5 = (2 + j)(a + bj) = 5a = -10b$$

Аналогично не имеет решений.
Итак, получили два разных разложения 10 на простые множители(сами множители простые, но именно их разложения разные, как было показано выше).
Отсюда следует, что кольцо $Z(j)$ не является евклидовым.

2.2.21 Задача №25

Доказать, что любой элемент кольца $Z/143Z$ является суммой двух делителей нуля. Найти представление в виде суммы двух делителей нуля для элемента 17.

Доказательство:

Делителями нуля в этом кольце являются все элементы, кратные либо 11, либо 13. Найдем для каждого элемента разложение в сумму делителей нуля.
1) Если элемент кратен 13, то его можно разложить в сумму двух ненулевых элементов, кратных 13.
2) Если элемент кратен 11, то действуем аналогично предыдущему пункту.
3) Иначе, если элемент a не делится на 11 и 13, то найдутся два числа x,y такие, что:

$$11x + 13y = a$$

При этом x не кратен 13, а y не кратен 11. Тогда $11x$ и $13y$ и есть искомые делители нуля $\Rightarrow$ найдем такие x,y для 17:

$$11x + 13y = 17$$

$$x = -2, y = 3$$

$$11x = -22 = 121, 13y = 39$$

Итак, $17 = 121 + 39$

2.2.22 Задача №26

Найти все идеалы в кольце F_2^n (n-я прямая степень поля F_2).

Решение:

F_2^n – множество последовательностей битов длины n с операциями побитового XOR и AND. Свойством втягивания относительно AND обладает нулевой бит:

$$0 \ \& \ x = 0$$

Это означет, что каждый идеал однозначно задается набором битов, которые будут нулевыми у каждого элемента идеала. Иначе говоря, каждый идеал представим как:

$$I = (1 \dots 101 \dots \dots 101 \dots 1)$$

То есть он порожден элементом с нулями на местах, в которых стоит 0 у всех элементов идеала.

2.2.23 Задача №27

Доказать, что идеал (x) в кольце многочленов $Z[x]$ над кольцом целых чисел Z имеет в качестве собственного делителя идеал $(2, x)$. Показать, что оба идеала при этом являются простыми.

Доказательство:

Рассмотрим идеал $(x) = \{x \cdot p(x) \mid p(x) \in Z[x]\}$, который представляет из себя множество всех многочленов без свободного члена.
$(2,x) = \{2 \cdot p(x) + x \cdot q(x) \mid p(x), q(x) \in Z[x]\}$ – множество всех многочленов с четным свободным членом.
Ноль – четное число $\Rightarrow (2,x) \supset (x)$, что и требовалось доказать.
Теперь докажем, что оба идеала простые.
Если элемент идеала (x) раскладывается в произведение, то один из множителей обязан делиться на x, т.е. содержаться в идеале $\Rightarrow (x)$ прост.
Четное число не представимо в виде произведения двух нечетных $\Rightarrow$ любое разложение элемента идеала $(2,x)$ в виде произведения содержит элемент с четным свободным членом, что эквивалентно тому, что он принадлежит идеалу $\Rightarrow$ идеал $(2,x)$ – простой.

2.2.24 Задача №28

Доказать, что кольцо многочленов $Z[x]$ над кольцом целых чисел Z не является евклидовым.

Доказательство:

В евклидовом кольце каждый идеал является главным в силу того, что имеет место алгоритм, аналогичный алгоритму Евклида. В $Z[x]$ есть идеал $(2,x)$. Общими делителями порождающих элементов являются ± 1. Они не являются четными, а, значит, не принадлежат идеалу. Таким образом, этот идеал не является главным $\Rightarrow$ кольцо не является евклидовым.

2.2.25 Задача №29

а) *Привести пример коммутативного кольца с единицей, в котором некоторый простой элемент порождает идеал, не являющийся простым.*
б) *Привести пример коммутативного кольца с единицей, в котором некоторый простой идеал не является идеалом, порожденным простым элементом.*

Решение:

а) Рассмотрим кольцо $Z[i\sqrt{7}]$. В данном кольце 2 – простое число, т.к.
$2 = (a + ib\sqrt{7})(c + id\sqrt{7}) \Rightarrow 4 = (a^2 + 7b^2)(c^2 + 7d^2)$
Одна из этих скобок должна быть равной 1 $\Rightarrow$ соответствующий элемент будет обратим.
Идеал (2) – множество всех чисел с четными коэффициентами.
$(1 + i\sqrt{7})(1 - i\sqrt{7}) = 1 + 7 = 8 \in (2)$
Оба множителя не принадлежат идеалу $\Rightarrow$ идеал не является простым.
б) Из предыдущих задач мы знаем, что идеал $(2,x)$ в кольце $Z[x]$ простой и при этом он не порожден одним элементом.

2.2.26 Задача №30

Построить пример коммутативного кольца с единицей, в котором разложение на простые множители неоднозначно.

Решение:

Рассмотрим кольцо $Z[i\sqrt{3}]$. Обратимыми элементами в нем являются $\{\pm 1\}$.
Число 4 имеет два разложения:
$4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$
$4 = 2 \cdot 2$
Числа $\{1 + i\sqrt{3}, 1 - i\sqrt{3}, 2\}$ имеют модуль 4.
Скобки не могут принимать значение 2 в целых числах $\Rightarrow$ одна из них равна 1 $\Rightarrow$ есть обратимость соответствующего элемента, и все 3 элемента просты. Таким образом, имеем 2 различных разложения числа 4, т.е. разложение на простые неоднозначно.

2.2.27 Задача №31

Найти наибольший порядок элемента мультипликативной группы кольца Z_{72}.

Решение:

Числа 8 и 9 взаимно простые $\Rightarrow$ по китайской теореме об остатках $Z_{72} \cong Z_8 \times Z_9 \Rightarrow$ в силу свойств изоморфизма $Z_{72}^* \cong Z_8^* \times Z_9^*$
В группе $Z_8^* = \{1,3,5,7\}$ каждый неединичный элемент имеет порядок 2:
$3^2 = 9 \equiv 1 \bmod 8$
$5^2 = 25 \equiv 1 \bmod 8$
$7^2 = 49 \equiv 1 \bmod 8$
Группа $Z_9^* = \{1,2,4,5,7,8\}$ циклична с порождающим элементом 2:
$1 = 2^6$
$2 = 2^1$
$4 = 2^2$
$5 = 2^5$
$7 = 2^4$
$8 = 2^3$
Порядок элемента прямого произведения равен НОКу порядков компонент элемента. Значит, максимальный порядок элемента в Z_{72} не превосходит НОК(2,6) = 6. Приведем пример:
$11^1 = 11$
$11^2 = 49$
$11^3 = 35$
$11^4 = 25$
$11^5 = 59$
$11^6 = 1$

2.2.28 Задача №32

Найти количество нильпотентных элементов в кольце

$$F_7[x]/(x^{14}+x^7+2).$$

Решение:

$x^{14}+x^7+2 = x^{14}-6x^7+9 = (x^7-3)^2 =<$ теорема Лагранжа $>= (x^7-3^7)^2 = (x-3)^{14}$
Опишем множество нильпотентных элементов кольца $F_7[x]/(x-3)^{14}$. Понятно, что каждый многочлен, кратный $(x-3)$, нильпотентен. Обратно, если многочлен не кратен $(x-3)$, то он ни в какой степени не будет кратен $(x-3)^{14}$. Получается, что элемент нильпотентен $\Leftrightarrow$ он кратен $(x-3)$. Эти элементы представимы как $(x-3)\cdot p(x)$, при этом степень не больше 13. Всего таких элементов столько же, сколько существует многочленов степени не больше 12, т.е. 7^{13}. Итак, количество нильпотентных элементов равно 7^{13}.

2.2.29 Задача №33

Найти порядок группы обратимых элементов колец

$$\text{а)}F_7[x]/(x^2+3x-5);\ \text{б)}F_3[x]/(x^2+x+1).$$

Решение:

а) $x^2 \mapsto -3x+5 = 4x+5$
Пусть у нас есть элемент $ax+b$. Попробуем найти для него обратный:
$(ax+b)(cx+d) = 1$
$(bc+ad+4ac)x + (bd+5ac) = 0\cdot x + 1$
Преобразуя имеющуюся систему, получаем
$c(5a^2-4ab-b^2) = a$
Итак, элемент необратим $\Leftrightarrow 5a^2-4ab-b^2 = 0 \Leftrightarrow (b+5a)(b-a) = 0 \Leftrightarrow (b-2a)(b-a) = 0$
Необратимы все элементы, кратные или $(x+1)$, или $(x+2)$. Тогда порядок группы обратимых элементов равен $7^2-2\cdot 6-1 = 36$.
б) $x^2 \mapsto -x-1 = 2x+2$
Пусть у нас есть элемент $ax+b$. Попробуем найти для него обратный:
$(ax+b)(cx+d) = 1$
$(bc+ad+2ac)x + (bd+2ac) = 0\cdot x + 1$
Преобразуя имеющуюся систему, получаем
$c(2a^2-2ab-b^2) = a$
Итак, элемент необратим $\Leftrightarrow 2a^2-2ab-b^2 = 0 \Leftrightarrow a^2+b^2+2ab = 0 \Leftrightarrow a = -b$
Необратимы все элементы, кратные $(x-1)$. Тогда порядок группы обратимых элементов равен $3^2-3 = 6$.

2.2.30 Задача №34

Построить изоморфизм полей $F_5[x]/(x^2-2)$ *и* $F_5[x]/(x^2-3)$.

Решение:

$F_5[x]/(x^2-2) \cong F_5[\sqrt{2}]$
$F_5[x]/(x^2-3) \cong F_5[\sqrt{3}]$
Рассмотрим отображение $\varphi : a + b\sqrt{2} \mapsto a + b2\sqrt{3}$
Докажем, что данное отображение является изоморфизмом.
Биективность очевидна. Проверим свойства операции:
$\varphi(a + b\sqrt{2}) + \varphi(c + d\sqrt{2}) = (a + c) + 2(b + d)\sqrt{3} = \varphi(a + c + (b + d)\sqrt{2})$
$\varphi(a+b\sqrt{2})\cdot\varphi(c+d\sqrt{2}) = (a+b2\sqrt{3})\cdot(c+d2\sqrt{3}) = (ac+2bd)+2(bc+ad)\sqrt{3} = \varphi(ac+2bd+(bc+ad)\sqrt{2})$
Итак, отображение биективно и сохраняет операции, т.е. является изоморфизмом.

2.2.31 Задача №35

Найти наименьшее конечное поле характеристики 2, *в котором многочлен* $x^{14}+1$ *раскладывается на линейные множители.*

Решение:

Воспользуемся характеристикой, равной двойке:
$x^{14} + 1 = (x^7 + 1)^2 = (x + 1)^2(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^2$
Последний множитель не раскладывается в линейные в поле F_2, поскольку никакой элемент не является его корнем.
Он не раскладывается в линейные в поле F_4, т.к. 0 не является его корнем, а для любого элемента этого поля выполняется $x^3 = 1$, откуда следует
$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 1 + x^2 + x + 1 + x^2 + x + 1 = 1$
Докажем теперь, что он раскладывается на линейные множители в поле F_8. Многочлен $x^8 - x$ в этом поле имеет 8 различных корней, откуда следует, что $x^7 - 1 = x^7 + 1$ имеет 7 различных корней, т.е. разложим на линейные множители. Тогда $x^{14} + 1$ тоже разложим на линейные множители. Итак, искомым полем является F_8.

2.2.32 Задача №36

Сколько различных решений имеет уравнение $1+x^2+x^8++x^{26} = 0$ *в поле* F_{81} *из* 81 *элемента*?

Решение:

Каждый элемент F_{81} является корнем многочлена $x^{81} - x$.
Рассмотрим фактор-кольцо $F_{81}[x]/(x^{26} + x^8 + x^2 + 1)$.
В нем $x^{27} = -x^9 - x^3 - x \Rightarrow x^{81} = -x^{27} - x^9 - x^3 \Rightarrow x^{81} - x = 0 \Rightarrow (x^{26} + x^8 + x^2 + 1) | (x^{81} - x) \Rightarrow$ многочлен раскладывается на различные линейные множители, т.е. имеет 26 различных корней.

2.2.33 Задача №37

Элемент a порождает мультипликативную группу поля F из 343 элементов. Является ли многочлен $x^2 + ax - a + 2a^2$ неприводимым в кольце многочленов $F[x]$?

Решение:

Предположим, что многочлен приводим
$x^2 + ax - a + 2a^2 = (x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2 \Rightarrow$
$x_1 + x_2 = -a$
$x_1x_2 = 2a^2 - a$
Воспользуемся тем, что характеристика равна 7
$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = a^2 - 8a^2 + 4a = 4a$
$(3x_1 - 3x_2)^2 = 9(x_1 - x_2)^2 = 36a = a$
$a = b^2$
$b^{342} = 1 \Rightarrow a^{171} = 1$
Получили противоречие с тем, что a является порождающим $\Rightarrow$ многочлен неприводим.