Дисклеймер.

Автор не несет ответственности за любой ущерб, причиненный Вам при использовании данного документа. Автор напоминает, что данный документ может содержать ошибки и опечатки, недостоверную и/или непроверенную информацию. Если Вы желаете помочь в развитии проекта или сообщить об ошибке/опечатке/неточности:

GitHub проекта

Автор в ВК

Внимание: данный документ не поддерживается и поддерживаться не будет! Сообщения об ошибках НЕ рассматриваются, пулл реквесты НЕ принимаются! Если Вы хотите поддерживать этот документ - форкните проект на Github. Благодарю за понимание.

Словарь терминов

Ассоциативность: $a * (b * c) = (a * b) * c$;

Коммутативность (коммутативная группа также называется абелевой): $a * b = b * a$;

Полугруппа — множество с заданной на нём ассоциативной бинарной операцией.

Моноид — множество с заданной на нём ассоциативной бинарной операцией и содержащее нейтральный элемент.

Группа — множество с заданной на нём ассоциативной бинарной операцией, содержащее нейтральный элемент и имеющее в своем составе обратные элементы для любых элементов. При этом результат применения бинарной операции к любым двум элементам группы должен входить в группу. (Пример — целые числа с операцией сложения являются группой)

Мощность группы $(cardG, |G|)$ — число элементов в группе.

Подгруппа — множество, заданное относительно операций в группе и само являющееся группой. Собственная подгруппа — подгруппа, не равная группе или нейтральному элементу, т.е. имеющая в составе более одного (нейтрального) элемента, но менее элементов, чем содержится в группе.

Обратимые элементы — элементы, имеющие в данной группе/кольце/ подгруппе/итд обратный к себе элемент.

Группа по сложению называется аддитивной (аддитивность).

Группа по умножению называется мультипликативной (мультипликативность).

Циклическая группа, (порожденная элементом a) — группа, любой элемент которой можно записать в виде $g = a^n$, где a называется образующим группы. Обозначение: $G =< a >$.

Порядок группы — количество элементов в группе.

Факторгруппа — множество смежных классов группы по её нормальной подгруппе, само являющееся группой.

Тривиальные нормальные подгруппы G — e и G, при этом если других нормальных подгрупп нет, то G называется простой.

Идеал (подразумевается двусторонний идеал, если это не оговорено отдельно): Аддитивная подгруппа $I \subseteq R$ называется двусторонним идеалом, если $\forall r \in R, i \in I$ выполняется $ri \in R$ (левый идеал) или $ir \in R$ (правый идеал). Двусторонний идеал подразумевает, что $ri \in R, ir \in R$. ($3\mathbb{Z}$ — идеал для кольца $\mathbb{Z}$)).

Собственный идеал кольца — идеал, не равный самому кольцу.

Простой идеал — идеал, образованный двумя элементами, один из которых должен лежать в этом идеале (Не знаю, насколько верна такая формулировка, но простые идеалы — идеалы, образованные простыми числами?)

Сумма идеалов — множество, содержащее объединение суммируемых идеалов (чаще всего данное множество идеалом не является).

Произведение взаимно простых (и только взаимно простых) идеалов — пересечение данных идеалов.

Пересечение идеалов — идеал, состоящий из элементов, принадлежащих пересекаемым идеалам.

Максимальный идеал — идеал, который не содержится ни в одном из других собственных идеалов кольца. К примеру, в $\mathbb{Z}$ идеалы: $2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}$. При этом $2\mathbb{Z}$ и $3\mathbb{Z}$ являются максимальными идеалами (так как не являются подмножествами никаких других идеалов), а $4\mathbb{Z}$ максимальным не является, так как содержится в идеале $2\mathbb{Z}$. В $\mathbb{Z}$ все простые идеалы являются максимальными.

Главный идеал — идеал, порожденный одним элементом.

Фактормножество — множество всех смежных классов ($G \setminus H$).

Факторкольцо — множество классов смежности элементов R по модулю I, на котором следующим образом определены операции сложения и умножения: $(a+I)+(b+I) = (a+b)+I$. $(a+I)\cdot(b+I) = ab+I$.

Факторкольцо R/I — $\{r+I|r \in R\}$.

Класс эквивалентности — множество всех элементов, эквивалентных одному.

Ядро гомоморфизма φ ($\ker\varphi$) — полный прообраз подгруппы $\{e\}$ (нейтрального элемента то есть) группы G.

R^* — множество обратимых элементов.

Область целостности — коммутативное кольцо без делителей нуля.

Кольцо называется факториальным, когда каждый ненулевой и не ассоциированный с единицей элемент можно разложить на простые множители единственным образом с точностью до порядка и ассоциированности элементов.

Нормальные подгруппы и идеалы. Гомоморфизм групп и колец. Свойства ядра и образа

Вопрос 1

Теория

G — множество, $*$ — бинарная операция.

$G, *$ — группа, если:

1) $a*(b*c) = (a*b)*c \ \forall a,b,c \in G$;

2) $\exists e \in G : e*a = a*e = a \ \forall a \in G$;

3) $\forall a \in G \ \exists a^{-1} \in G : a*a^{-1} = e$

$(G,*)$, удовлетворяющее аксиоме (1) называется полугруппой, а $(G,*)$, удовлетворяющее аксиомам (1) и (2) — моноидом.

4) $a*b = b*a \ \forall a,b \in G$

Если $(G, *)$ удовлетворяет аксиомам (1), (2), (3), (4), то группа называется коммутативной (абелевой).

R — множество, «+» «·» — бинарные операции на R.

R — кольцо, если:

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

2) $\exists 0 \in R : a + 0 = a$;

3) $\forall a \ \exists(-a) : a + (-a) = 0$;

4) $a + b = b + a$;

5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

6) $a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$;

—

7) $\exists 1 \in R : 1 \cdot a = a \cdot 1 = a$ (кольцо с единицей);

8) $a \cdot b = b \cdot a$ (коммутативное кольцо);

9) $\forall a \neq 0 \ \exists a^{-1} \in F : a \cdot a^{-1} = 1$;

10) $0 \neq 1$;

Множество $((R, +, \cdot))$, удовлетворяющее всем 10 аксиомам называется полем.

Примеры:

$\mathbb{Z}$ — кольцо целых чисел.

$F[x]$ — кольцо многочленов из поля F.

$0 \cdot a = 0$ ($\forall$ кольца).

Ответы

Нормальные подгруппы и идеалы:

Определение: X — группа или кольцо.

$Y \subseteq X$:

Y называется подгруппой или подкольцом, если оно является группой или кольцом относительно операций, заданных в X. При этом выполняется:

1) $\forall a, b \in Y : a * b \in Y$

2) $\forall a \in Y, a^{-1} \cdot a = e$
3) $a^{-1} \in Y$.

Примеры подгрупп:

1) Сама группа G и её подмножество, состоящее из одного нейтрального элемента, являются подгруппами, причем группа, состоящая из нейтрального элемента, является тривиальной.

2) Множество целых чисел, кратных числу m является подгруппой в группе целых чисел с заданной операцией сложения.

3) Числа $\{-1; 1\}$ образуют подгруппу в группе ненулевых рациональных чисел относительно умножения.

H называется нормальной подгруппой группы G, если $\forall h \in H$ и $\forall g \in G$ выполняется $g^{-1}hg \in G$ (для коммутативных групп все группы нормальные). Также нормальность подгруппы означает равенство правых и левых смежных классов: $gH = Hg$.

В коммутативной группе все подгруппы нормальные:

$g^{-1}hg = (g^{-1}h)g = g(g^{-1}h) = gg^{-1}h = eh = h, h \in H, g \in G$.

Примеры: $\{1\}$, G — нормальные подгруппы.

Идеал (подразумевается двусторонний идеал, если это не оговорено отдельно): Аддитивная подгруппа $I \subseteq R$ называется двусторонним идеалом, если $\forall r \in R, i \in I$ выполняется $ri \in I$ (левый идеал) или $ir \in I$ (правый идеал). Двусторонний идеал подразумевает, что $ri \in I, ir \in I$. ($3\mathbb{Z}$ — идеал для кольца $\mathbb{Z}$)).

Примеры:

1) R — коммутативное кольцо, $r \in R$, rR — идеал. При

этом идеал выдерживает умножение на элементы кольца (при умножении всего идеала на произвольный элемент кольца идеал останется идеалом).

2) Любое множество $n\mathbb{Z}$ — идеал кольца $\mathbb{Z}$.

3) В любом кольце R само кольцо R и элемент $\{0\}$ являются идеалами.

Определение: φ — гомоморфизм, если $\varphi(a *_x b) = \varphi(a) *_y \varphi(b)$ $\forall$ бинарной операции $*$. (При этом $*_x$ НЕ ОБЯЗАТЕЛЬНО ТА ЖЕ ОПЕРАЦИЯ, что и $*_y$)

Гомоморфизм групп и колец

Свойства гомоморфизма:

Группы:

Гомоморфизм групп переводит нейтральный элемент в нейтральный: $\varphi(e_x) = e_y$;

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

Умножим на обратный элемент с обеих сторон: $\varphi(e_x) \times \varphi(e_x) \times (\varphi(e_x))^{-1} = \varphi(e_y) \times (\varphi(e_y))^{-1} \Leftrightarrow \varphi(e_x) \times e_x = \varphi(e_x) = e_y$. Отсюда $\varphi(e_x) = e_y$.

Гомоморфизм групп переводит обратный элемент в обратный: $\varphi(a^{-1}) = \varphi(a)^{-1}$.

$\varphi(a) \times \varphi(a^{-1}) = \varphi(a \cdot a^{-1}) = \varphi(e) = \varphi(a \cdot a^{-1}) = \varphi(a) \times \varphi(a)^{-1}$.

Таким образом, φ «сохраняет групповую структуру».

Примеры групп: $(\mathbb{Z}, +)$,

Кольца:

$\varphi(0) = 0$;

$\varphi(-a) = -\varphi(a)$

Для колец с единицей необязательно $\varphi(1) = 1$ (но часто требуется).

Гомоморфизм колец сохраняет операции сложения и умножения, т.е.:

$\varphi(a+b) = \varphi(a) + \varphi(b)$;

$\varphi(ab) = \varphi(a) \cdot \varphi(b) \ \forall a, b \in R$

$\begin{cases} \varphi(r) = (r, r) \\ \psi(r) = (0, r) \end{cases}$ — гомоморфизм.

Примеры:

$(\mathbb{Z}, +)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{R}^* = \mathbb{R} \setminus \{0\})$

$\varphi : X \to Y$, $\varphi(n) = (-1)^n$

$\varphi(m+n) = (-1)^{m+n} \Leftrightarrow (-1)^m \cdot (-1)^n = \varphi(m) \cdot \varphi(n)$, следовательно, φ — гомоморфизм. При этом $\ker \varphi = 2\mathbb{Z}$.

Виды гомоморфизма:

Мономорфизм — инъективный гомоморфизм;

Эпиморфизм — сюръективный гомоморфизм;

Изоморфизм — биективный гомоморфизм;

Эндоморфизм — гомоморфизм в себя $(X \to X)$;

Автоморфизм — изоморфизм в себя.

Свойства ядра и образа

Свойства образа:

$\varphi : X \to Y$;

Ядро (Kernel)

$\ker \varphi = \{x \in X | \varphi(x) = e_y \text{ (для группы) }, \varphi(x) = 0 \text{ (для кольца) }\}$.

Для:

$\{\varphi : X \to Y; \varphi(n) = (-1)^n\} \Rightarrow \ker \varphi = 2Z$

Решение:

$\varphi(n) = 1 \Leftrightarrow (-1)^n = 1 \Leftrightarrow n$ —четное.

Свойства ядра:

1) Ядро гомоморфизма групп является нормальной подгруппой.

$H = \ker\varphi = \{g \in G | \varphi(g) = e\} = \varphi^{-1}(e)$.

Утверждаем, что: $\forall h_1, h_2 \in H$, $h_1^{-1} \in H$, $g^{-1}hg \in H$

Докажем:

$\varphi(h_1) = \varphi(h_2) = e$;

1) $\varphi(h_1 \cdot h_2) = \varphi(h_1) \cdot \varphi(h_2) = e \cdot e = e$. $\varphi(h_1 \cdot h_2) = e \Rightarrow h_1 \cdot h_2 \in H$.

2) $\varphi(h_1)^{-1} = \varphi(h_1^{-1})$ по свойству гомоморфизма групп.

3) $(\varphi(h_1))^{-1} = e^{-1}$, $\varphi(e) = 1$ ($\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e) \Rightarrow \varphi(e) = \varphi(e) \cdot \varphi(e)$, разделим обе части на $\varphi(e)$, получим $1 = \varphi(e)$).

$\varphi(h_1)^{-1} = \varphi(h_1^{-1}) = e$.

2) Ядро гомоморфизма колец всегда является двусторонним идеалом.

$\varphi : X \to Y$

$\ker\varphi = \{x \in X | \varphi(x) = 0\}$

Для $r \in X$:

1) $\varphi(x + y) = 0$, так как $\varphi(x + y) = \varphi(x) + \varphi(y) = 0 + 0 = 0$

2) $\varphi(-x) = 0$, так как $\varphi(-x) = -\varphi(x) = -0 = 0$.

3) $\varphi(xr) = \varphi(x) \cdot \varphi(r) = 0 \cdot 0 = 0$;

$\varphi(rx) = \varphi(r) \cdot \varphi(x) = 0 \cdot 0 = 0$.

$\Rightarrow \ker\varphi$ — двусторонний идеал.

3) Ядро всегда содержит нейтральный элемент.

$\varphi(e) = x$; $x \cdot x = \varphi(e) \cdot \varphi(e) = \varphi(e + e) = \varphi(e) = x$. Если $x^2 = x$, то, применив умножение на обратный элемент, получим $x^2 = x \Rightarrow x^{-1}x^2 = x^{-1}x \Rightarrow x = e$.

Свойства образа:

Образ гомоморфизма = образ функции.

$Im\varphi = \{\varphi(x)|x \in X\} \subseteq Y$ (определен на множестве Y. Является подмножеством множества. Если построить ограниченный график функции, то его $y = f(x)$ будут образом функции f на множестве Y)

Образ гомоморфизма группы является подгруппой.

Доказательство:

1) $\forall a, b \in Imf :\ ab \in Imf$

$\exists x_a, x_b \in X : f(x_a) = a,\ f(x_b) = b$

$ab = f(x_a)f(x_b) = f(x_a x_b);\ f(x_a x_b) \in Imf$

2) $e_y \in Imf$. $f^{-1}(e_y) = e_x$

3) Если $y \in Imf$, то $f^{-1}(e_y) = e_x$

$\exists x \in X : f(x) = y; \exists x^{-1} \in X : xx^{-1} = e_x$

$e_y = f(e_x) = f(xx^{-1}) = f(x)f(x^{-1}) = yf(x^{-1})$

$yf(x^{-1}) = ey_1 \Rightarrow f(x^{-1})$ — обратный элемент к y.

Образ гомоморфизма колец является подкольцом.

Существование эпиморфизма групп с данным ядром.

$H \trianglelefteq G$. Пусть $G \setminus H$ — множество смежных классов G по H. Определим в $G \setminus H$ бинарную операцию по следующему правилу:

Произведение смежных классов aH и bH — смежный класс abH. Определение произведения смежных классов корректно, т.е. не зависит от выбранных представителей a и b.

Докажем это: $aH, bH \in G/H$. $a_1 = a \cdot h_a \in aH$, $b_1 = b \cdot h_b \in bH$. Докажем, что $a_1 b_1 H = abH$, достаточно доказать $a_1 b_1 \in abH$. $a_1 b_1 = ah_a bh_b = abh_a h_b \in abH$

Теорема: $H \trianglelefteq G$, H — нормальная подгруппа, G группа.

Существует эпиморфизм $\varphi : G \twoheadrightarrow F$, такой, что $\ker \varphi = H$. (F — тоже группа)

Диаграмма (ориентированный граф, вершины помечены математическими объектами, а стрелки - отображениями этих объектов) называется коммутативной, если для любых вершин A, B и любых двух путей из A в B композиции отображений по каждому из них равны.

Лемма: $\varphi : G \to F$, $H = \ker \varphi$

$\varphi(g) = f$,

$\varphi^{-1}(f) = gH = Hg$ — нет левых или правых классов, так как ядро является нормальной подгруппой(конец леммы).

Доказательство единственности:

$F = G \setminus H = \{gH : g \in G\}$ — множество смежных классов.

Множество $G \setminus H$ является группой, т.к. нейтральным элементом служит eH, а обратным элементом к классу aH — класс $a^{-1}H$.

Правило: $\varphi(g) = gH = Hg$ (так как F — множество смежных классов). Так как $\varphi(g)\varphi(g_1) = gHg_1H = gg_1(H \cdot H)$ (так как группа ассоциативна) $= gg_1H = \varphi(gg_1)$ — гомоморфизм.

φ — сюръективный гомоморфизм, так как каждый смежный класс gH — образ элемента в $g \in G$: $\varphi : G \to G/H$ — эпиморфизм.

Существование эпиморфизма колец с данным ядром.

$I \trianglelefteq R$, I — идеал, R — кольцо.

Существует эпиморфизм $\varphi : R \twoheadrightarrow A$ — гомоморфизм колец, $\ker \varphi = I$. Если $\varphi' : R \twoheadrightarrow A'$, $\ker \varphi = I$, то существует единственный изоморфизм $\Theta : A \to A'$, такой, что $\varphi' = \Theta \circ \varphi$.

Отношение эквивалентности на кольце $a \sim b \Leftrightarrow a - b \in I(2 \equiv 5(\mod 3), 2 - 5 \in 3\mathbb{Z}), b - a \in I(5 - 2 \in \mathbb{Z})$, по классу смежности. $\begin{cases} a \in b + I \\ b \in a + I \end{cases}$ для $a, b \in R$.

Проверка корректности:

1) Пусть $a_1 \in a + I,\ b_1 \in b + I$.

Тогда $a_1 = a + i_1,\ b_1 = b + i_2,\ i_1, i_2 \in I$

$a_1 + b_1 = a + i_1 + b + i_2 = a + b + i_1 + i_2$.

$i_1+i_2 \in I$ по свойствам кольца, следовательно, $a+b+i_1+i_2 \in a + b + I \Rightarrow$ определение корректно (не зависит от выбора конкретного представителя класса смежности).

2) $a_1 b_1 = (a + i_1)(b + i_2) = ab + ai_2 + i_1 b + i_1 i_2$

$ai_2, i_1 b, i_1 i_2 \in I$ по свойствам кольца $\Rightarrow ab+ai_2+i_1b+i_1i_2 \in ab + I$

(Идеал является подкольцом без единицы, потому что аддитивная подгруппа выдерживает умножение на элементы кольца)

1) $(a + I) + (b + I) = (a + b) + I$, так как $\forall R$ является подгруппой по сложению.

$\varphi(a) = a + I,\ \varphi(b) = b + I$

$\varphi(a) + \varphi(b) = \varphi(a + b)$ — гомоморфизм.

2) Определяем операцию умножения:

$(a + I)(b + I) = ab + I$, следовательно, $\varphi(a)\varphi(b) = (a + I)(b + I) = ab + aI + bI + II = ab + I$. $\varphi(ab) = ab + I$. — тоже гомоморфизм.

Следовательно, по (1) и (2) φ — гомоморфизм кольца.

$(A = R/I)$

$\varphi : R \twoheadrightarrow A$ — сюръекция, так как каждый элемент $r \in R$ переходит в элемент $r + I \in R/I$ — факторкольцо.

Единственность эпиморфизма с данным ядром

X, Y, Z — группы. $f : X \to Y; g : X \to Z$.

f, g — эпиморфизмы. $\ker f = \ker g$. Тогда $\exists$ изоморфизм $h : Y \to Z$, такой, что $g = h \circ f$.

Доказательство:

$\ker f = A = \ker g$

$y \in Y \Rightarrow \exists x \in X : f(x) = y$ (по свойству эпиморфизма).

$\forall a \in A$ $f(xa) = f(x)f(a) = yf(a) = ye_y = y$ (e_y — нейтральный элемент в Y, т.к. гомоморфизм переводит ядро в нейтральный элемент, а A — ядро).

xA содержится во множестве всех прообразов y (1).

$x_1 \in X;\ f(x_1) = y. \quad f(x^{-1}x_1) = f(x^{-1})f(x_1) = f(x)^{-1}y = y^{-1}y = e_y \Rightarrow x^{-1}x_1 \in A$, $x_1 \in xA$.

Значит, множество всех прообразов y содержится в xA. (2)

Из (1) и (2) следует, что для каждого элемента $y \in Y$ можно взаимно однозначно определить смежный класс xA, такой, что $\forall a \in A \;\; f(xa) = y$.

Пусть $g(x) = z$. Аналогично доказывается, что множество прообразов z равно xA.

Построим функцию $h : Y \to Z$, такую, что :

$\forall y \in Y (f^{-1}(y) = x),\ h(y) = h(f(x)) = g(x) = z$, так как $g = h \circ f$ по условию задания.

Докажем, что заданная функция единственна:

Допустим, существует $h' : Y \to Z$, такая, что $g = h' \circ f$ и существует $y \in Y : h'(y) \neq h(y)$.

$h(y) = h(f(x)) = g(x) = z,$

$h'(y) = h(f(x')) = g(x') = z'.$

$z \neq z' \Rightarrow xA \neq x'A$. Но тогда $\forall a \in A :$

$f(xa) \neq f(x'a) \Rightarrow y \neq y$ — противоречие. Значит, h' и h совпадают.

Докажем, что h — изоморфизм.

$y_1, y_2 \in Y$:

$f^{-1}(y_1) = x_1;\ g(x_1) = z_1;$

$f^{-1}(y_2) = x_2;\ g(x_2) = z_2.$

$h(y_1y_2) = h(f(x_1x_2)) = g(x_1x_2) = g(x_1)g(x_2) = z_1z_2$

$h(y_1)h(y_2) = h(f(x_1))h(f(x_2)) = g(x_1)g(x_2) = z_1z_2 \Rightarrow h$ — гомоморфизм.

Если $y_1 \neq y_2$, то $x_1A \neq x_2A(f(x_1) = y_1,\ f(x_2) = y_2) \Rightarrow g(x_1) \neq g(x_2)$.

Другими словами, если $y_1 \neq y_2$, то $h(y_1) \neq h(y_2) \Rightarrow h$ — мономорфизм. То, что h — эпиморфизм, очевидно: $\forall z \in Z\ \exists x \in X : g(x) = z$, а, значит, существует и $f(x)$; $f(x) = y$.

Т.е. $\forall z \in Z$ найдется прообраз в Y.

h — гомоморфизм и эпиморфизм $\Rightarrow h$ — изоморфизм.

Следствие (теорема о гомоморфизме):

X, Y — группы; $f : X \to Y$.

Тогда $Imf \cong X/\ker f$.

Доказательство:

Пусть $f' : X \to Imf$; $f'(x) = f(x), \forall x \in X$. По определению f' — эпиморфизм.

Из теоремы о существовании эпиморфизма с данным ядром: $\exists g : x \to F$, F — группа, g — эпиморфизм; $\ker g = \ker f$. Из этой же теоремы известно, что $F = X/\ker g = X/\ker f$. Таким образом f', g — эпиморфизмы с одинаковым ядром и одинаковой областью задания, следовательно, условие теоремы о гомоморфизмах сводятся к условию предыдущей теоремы, следовательно, $\exists h : Imf \to X/\ker f$, такая, что h — изоморфизм.

Смежные классы по подгруппе, теорема Лагранжа

Для элемента $g \in G$ левый класс смежности по подгруппе H — множество $gH = \{gh \in G, h \in H\}$, правый класс смежности по подгруппе H — множество $Hg = \{hg \in G, h \in H\}$.

Класс смежности: зафиксирвали элемент группы и умножаем его на все элементы подгруппы (Запись: gH, где g — элемент группы, H — подгруппа.)

В каждом классе смежности содержится столько же элементов, сколько содержится в подгруппе.

Лемма: $H \trianglelefteq G$ — группа
$\forall g_1, g_2 \in G$, $g_1 H$ равномощно $g_2 H$.
Доказательство:
$\varphi : H \to g_1 H$, $\varphi(h) = g_1 h, h \in H$ — биекция, так как $\varphi^{-1}(x) = g_1^{-1} x$.

Лемма: $H \leq G, g_1, g_2 \in G$
$g_1 H \cap g_2 H = \varnothing$ или $g_1 H = g_2 H$
Доказательство:
Допустим, $g \in g_1 H \cap g_2 H$,
$g = g_1 h_1 = g_2 h_2$ для $h_1, h_2 \in H$, тогда
$g_1 = g_2 h_2 h_1^{-1}$
$\forall h \in H : g_1 h = g_2 \underbrace{(h_2 h_1^{-1} h)}_{\in H} \in g_2 H \Rightarrow g_1 H \subseteq g_2 H$

Обратное ($g_2 H \subseteq g_1 H$) доказывается аналогично. Таким образом, $g_1 H = g_2 H$ либо $g_1 H \cap g_2 H = \varnothing$.

Теорема Лагранжа:
Порядок подгруппы является делителем порядка группы.
$H \leq G$
$|G| = |H| \cdot |G : H|$, где $|G : H|$ — количество смежных классов.

Доказательство т. Лагранжа: $H \leq G$, $|G| < \infty$
$H_i = H_1, H_2, ..., H_m$ — левые смежные классы по H.

$$G = \sqcup_{i=1}^m H_i \Rightarrow |G| = \underbrace{\sum_{i=1}^m |H_i| = \sum_{i=1}^m |H|}_{|H_i|=|H|} = m \cdot |H|, \text{ а } m =$$

$|G : H| = |G/H| = |H\backslash G|$ — количество смежных классов.

$\sqcup$ — дизъюнктное (непересекающееся) объединение.

Взаимно простые идеалы, их пересечение и произведение

Определение: Идеал I — простой, если выполнено следующее условие: $ab \in I \Rightarrow a \in I$ или $b \in I$.

Идеал $6\mathbb{Z}$ не является простым, т.к. $2 \cdot 3 \in 6\mathbb{Z}$, $2, 3 \notin 6\mathbb{Z}$.

Ответы

Идеалы называются взаимно простыми, если сумма двух идеалов равна кольцу: $I_j + I_l = R \; \forall j \neq l$

Внимание, правило: идеал выдерживает умножение на элементы кольца, то есть если перемножить все элементы идеала на элемент кольца — в итоге получим идеал, который является подмножеством данного идеала.

Лемма: Если $I_1, ..., I_k$ — попарно взаимно простые, то $I_1 \cdot ... \cdot I_k = I_1 \cap ... \cap I_k$.

Доказательство: Достаточно доказать для $k = 2$ и дальше применить индукционный переход:

$I_1 + I_2 = R$. Заметим, что произведение идеалов всегда содержатся в пересечении. $I_1 \cdot I_2 \subseteq I_1 \cap I_2$.

$x \in I_1 \cap I_2$. $\exists a_1 \in I_1, a_2 \in I_2 : a_1 + a_2 = 1$.

$x = x \cdot 1 = x(a_1 + a_2) = xa_1 + xa_2$, где $x \in I_2,\ a_1 \in I_1,\ x \in I_1,\ a_2 \in I_2 \Rightarrow xa_1 + xa_2 \in I_2 I_1 + I_1 I_2 = I_1 I_2$.

Далее перейдем по индукции с использованием следующей леммы:

Лемма Если I_1 взаимно прост с каждым из $I_2, ..., I_k$, то он взаимно прост с их произведением.

Доказательство:

Пусть $k = 3$, $I_1 + I_2 = R$, $I_1 + I_3 = R$. Отсюда $R = I_1 + I_2 \cdot R = I_1 + I_2 \cdot (I_1 + I_3) = \underbrace{I_1 + I_2 I_1}_{\subseteq I_1} + I_2 I_3 \subseteq I_1 + I_2 \cdot I_3 \subseteq R$.

Дальше индукция по k:

Пусть верно для k: $I_1 \cdot ... \cdot I_n + J = R$. Докажем, что верно для $k+1$:

$I_1 \cdot ... \cdot I_k + J = R$

$I_{k+1} + J = R$.

$(I_1 \cdot ... \cdot I_k + J)(I_{k+1} + J) = I_1 \cdot ... \cdot I_k \cdot I_{k+1} + \underbrace{I_1 \cdot ... \cdot I_k \cdot J}_{\subseteq J} + \underbrace{J \cdot I_{k+1}}_{\subseteq J} + \underbrace{JJ}_{\subseteq J} = J + I_1 \cdot ... \cdot I_{k+1} \Rightarrow$

J взаимно прост с $I_1 \cdot ... \cdot I_{k+1}$

Китайская теорема об остатках

Теорема: $I_1, ..., I_k$ — идеалы кольца R, где R (здесь и далее) — коммутативное кольцо с единицей.

Предполагается, что каждая пара идеалов взаимно простая: $I_j + I_l = R \ \forall j \neq l = 1, ..., k$.

Теорема говорит о том, что $R/(I_1 \cdot ... \cdot I_k) = \oplus_{j=1}^k R/I_j$, где $\oplus_{j=1}^k R/I_j$ — набор остатков от деления на $r_1, ..., r_k$.

Если

$x \equiv 1 \mod 3$

$x \equiv 2 \mod 5$

$x \equiv ? \mod 15$, где $15 = 3 \cdot 5$

Доказательство:

$\varphi : R \to R/(I_1 \cdot ... \cdot I_n)$ — эпиморфизм с ядром $(I_1 \cdot ... \cdot I_n)$ (по теореме о существовании эпиморфизма с данной ядром).

$\psi : R \to \oplus_{j=1}^{k} R/I_j$;

$\psi(r) = (r + I_1, ..., r + I_n)\ \forall r \in R$

ψ — гомоморфизм.

$\psi(r + k) = (r + k + I_1, ..., r + k + I_n)\ \ r, k \in R$

$\psi(r) + \psi(k) = (r + I_1, ..., r + I_n) + (k + I_1, ..., k + I_n) = (r + I_1 + k + I_1, ..., r + I_n + k + I_n) = (r + k + I_1, ..., r + k + I_n)$.

$\psi(r + k) = \psi(r) + \psi(k)\ \ \forall r, k \in R$.

$\psi(r) = 0 \Leftrightarrow r \in I_j\ \forall j \Leftrightarrow r \in I_1 \cap ... \cap I_n$ — по лемме один это равно $(I_1 \cdot ... \cdot I_n) \Rightarrow$

$\ker \psi = \ker \varphi$.

Докажем, что ψ — эпиморфизм.

ψ — эпиморфизм, если $\forall \psi' \in \oplus_{j=1}^{n} R/I_j$

$\exists x \in R : \psi(x) = \psi'$.

Пусть $\psi' = (r_1 + i_1, ..., r_n + i_n) \in \oplus_{j=1}^{n} R/I_j$, где $r_1, ..., r_n \in R$; j — любой элемент из I_j.

$I_j + \prod\limits_{k=1, k \neq j}^{n} I_k = R$, так как I_j, I_k — взаимно просты, $\Rightarrow$ $\exists b_j \in I_j; c_j \in \prod\limits_{k=1, k \neq j}^{n} I_k = I_1 \cap ... \cap I_{j-1} \cap I_{j+1} \cap ... \cap I_n$, так что:

$b_j + c_j = 1$. $(c_j = 1 - b_j \Rightarrow c_j \in 1 + I_j)$

$r_j \cdot c_j = r_j + r_j \cdot i_j\ (i_j \in I_j) \Rightarrow r_j c_j \in r_j + I_j$

$\forall k \neq j\ c_j \in I_k \Rightarrow r_j c_j \in I_k$

Тогда $\psi(r_j c_j) = (0_1, 0_2, ..., r_j, 0_{j+1}, ..., 0_n)$

Пусть $x = \sum\limits_{k=1}^{n} r_k c_k$. Тогда $\psi(x) = \sum\limits_{k=1}^{n} \psi(r_k c_k) = (r_1, ..., r_n) \Rightarrow$ ψ — эпиморфизм

φ, ψ — эпиморфизмы с одинаковым ядром $\Rightarrow \exists$ изоморфизм $\xi : R/(I_1 \cdot ... \cdot I_n) \to \oplus_{j=1}^{n} R/I_j$

То есть наше отображение сюръективно, поэтому по теореме о гомоморфизме мы получаем, что образ изоморфен факторкольцу.

Простые и максимальные идеалы

R — кольцо, I — идеал в R.

Идеал I называется простым, если из $ab \in I$ следует, что $a \in I$ или $b \in I$.

R — кольцо, I — идеал в R.

Определение: I — максимальный идеал, если он не содержится ни в каком другом собственном идеале R.

Лемма 1: Любой максимальный идеал является простым идеалом.

Доказательство: $a, b \in R$, такие, что $ab \in M$ (M — максимальный идеал). Предположим, что $a \notin M$.

Рассмотрим идеал $M \supsetneqq M + aR \Rightarrow$т.к. M — максимальный идеал, то $M + aR = R$ (так как M — максимальный идеал, он содержится только во всем кольце).

$bR = bM + baR$.

$bM \subseteq M;\ ba \in M \Rightarrow baR \subseteq M; b \in bR \Rightarrow b \in bM + baR \subseteq M \Rightarrow b \in M$.

Лемма 2: Идеал I — максимальный тогда и только тогда, когда R/I — поле.

Доказательство: R/I — поле. Пусть I — не максимальный идеал, тогда $I \subsetneqq J,\ J$ — идеал в R (т.е. I содержится в собственном идеале J).

Элемент $r \in J \setminus I$.

Ни один из собственных идеалов не содержит 1, следовательно, J не содержит 1. Но $I \subsetneqq J$, следовательно, класс элемента r в факторкольце R/I необратим (т.е. не имеет обратного по 1), следовательно, R/I не является полем. Противоречие.

Лемма 3: Любой собственный идеал кольца содержится в каком-либо максимальном идеале.

I — максимальный идеал.

Неприводимые элементы и простота главного идеала

Теория:

R — кольцо, $a, b \in R$.

Определение: Элементы a, b — ассоциированные, если $a \in bR$ и $b \in aR \Leftrightarrow aR = bR$ $(a \vdots b, b \vdots a)$.

Определение: Элемент $p \in R$ называется неприводимым, если p необратим и если выполнено следующее условие: $p = ab$ влечёт: p ассоциировано с a или с b ($p = ab$ влечёт: a или b — обратимо) (для всех колец).

Определение: Элемент кольца $p \in R$ называется простым, если идеал pR — простой.

Лемма: Если pR — простой идеал, то p — неприводимый элемент.

Доказательство:

$a, b \in R,\ ab = p,\ ab \in pR \Rightarrow a \in pR$ или $b \in pR$.

Пусть, для определенности, $a \in pR \Rightarrow \exists r \in R:\ a = pr;\ p = ar^{-1} \in aR$.

$a \in pR,\ p \in a? \Rightarrow$ по определению p и a — ассоциированные элементы.

То есть, из $p = ab$ следует, что p и a — ассоциированы — тогда, по определению, p — неприводимый элемент.

Определение: Главный идеал — идеал, порожденный одним элементом, то есть идеал вида aR.

Определение: R — кольцо главных идеалов, если любой идеал в R — главный.

Лемма: R — кольцо главных идеалов, $a, c \in R$; c — неприводимый, a не делится на c.Тогда $aR+cR = R$ (т.е. aR взаимно прост с cR).

Доказательство:

$aR + cR$ — идеал.

Так как R — кольцо главных идеалов, $aR+cR = bR$, $b \in R$ и $cR \subseteq bR \Rightarrow c \in bR \Rightarrow bR = cR$ или $bR = R$.

Если $bR = cR$, то $aR \subseteq cR \Rightarrow a \in cR$ — противоречие. Следовательно, $aR + cR = R$.

Лемма: R — кольцо главных идеалов, область целостности. Если p — неприводимый элемент, то pR — простой идеал.

Доказательство:

$a, b \in R$. Пусть $aB \in pR$. Докажем, что тогда $a \in pR$ или $b \in pR$:

Допустим, $\begin{cases} a \notin pR \\ b \notin pR \end{cases}$.

$a \notin pR \Rightarrow aR + xR = a'R \Rightarrow x \in a'R \Rightarrow \exists r \in R : x = a'r$.

x — неприводимый элемент, aR — область целостности, следовательно, a' обратимо или r обратимо. Либо обратимо a', и тогда $a'R = R$. Либо $x'R$ обратимо, то $a'R = xR$, тогда $a \in a'R = xR$ — противоречие. Следовательно, что $aR+xR = a'R = R$.

Факториальные кольца

Кольцо называется факториальным, когда каждый нулевой и не ассоциированный с единицей элемент можно разложить на простые множители единственным образом с точностью до порядка и ассоциированности элементов.

Достаточное условие факториальности.

Пусть R — область главных идеалов, то есть каждый идеал порожден одним элементом. Тогда $\forall r \in R$ $\exists$ неприводимые элементы $p_1, ..., p_m \in R$ и $\varepsilon \in R^* : r = \varepsilon p_1, ..., p_m$.

При этом: $\varepsilon p_1, ..., p_m = \delta q_1 \cdot ... \cdot g_n$, $\varepsilon, \delta \in R^*$, а p_i, q_i неприводимы, то $m = n$ и $\exists \sigma \in S_n : p_i$ ассоциировано с $q_{\sigma(i)} \forall i = 1, ..., n$.

Факториальность кольца главных идеалов

Если R — область главных идеалов, то каждый необратимый элемент раскладывается в произведение неприводимых.

Т.е. кольцо главных идеалов R — факториально.

Доказательство:

Пусть $r \in R$ — необратимый элемент. $rR \subseteq M$ — максимальный идеал.

Так как любой идеал главный, то $rR \subseteq p_1 R$ — максимальный. Так как максимальный идеал по лемме является простым, то тогда p_1 — неприводимый (по лемме).

Таким образом, $r = p_1 r_1$, где p_1 — неприводимый.

Если r_1 обратим,то всё доказано, так как r будет неприводимым, т.е. простым и p_1 простой $\Rightarrow$ —?

Иначе понимаем, что $r = p_1 r_1$, $r_1 = p_2 r_2$, $r_2 \in R$, p_2 — неприводим.

и так далее: $r_k = r_{k+1}p_{k+1}$

Сейчас докажем, что такой процесс обязательно прервется. Предположим обратное: ни один $r_k \notin R^*$

$rR \subseteq r_1R$ (т.к. r содержится в идеале r_1R, порожденном r). Получили строго возрастающую цепочку идеалов:

$rR \subseteq r_1R \subseteq r_2R \subseteq ... \subseteq r_kR \subseteq ....$

$I = \cap_{k=1}^{\infty} r_kR$ — идеал, причем $I = qR$ для некоторого $q \in R$. $q \in$ какому-то множеству из объединения: $q \in r_jR, j \in \mathbb{N} \Rightarrow qR \subseteq r_jR$.

С другой стороны, $r_jR \subseteq I = qR \Rightarrow qR = r_jR = r_{j+1}R \Rightarrow q, r_j$ — ассоциированы между собой, следовательно, все остальные идеалы большие r_jR тоже будут равны qR. Цепочка оборвалась на каком-то шаге. $r_j = r_{j+1}p_{j+1}$. Так как r_j и r_{j+1} ассоциированы, то $p_{j+1} \in R^*$ — обратим. Приходим к противоречию, так как p_{j+1} — не приводим по условию. Значит, процесс прервется, значит, необратимый элемент $r \in R$ раскладывается в произведение неприводимых.

Евклидовы кольца и кольца главных идеалов

Теория:

Алгоритм деления с остатком:

в $\mathbb{Z} : \forall a, b\ \exists c, r : a = bc + r, |r| < |b|$;

В кольце многочленов, где $F[x]$ — поле:

$F[x] : \forall a, b \neq 0\ \exists c, r : a = bc + r,\ \deg r < \deg b,\ a, b$ — многочлены, deg — степень многочлена.

Рассмотрим произвольное Евклидово кольцо:

Будем считать, что у нас задано: пусть кольцо R — коммутативная область целостности с единицей.

Область целостности — это кольцо, в котором можно сокращать на элементы. В области целостности $\forall r \neq 0\ ra = rb \Leftrightarrow$

$a = b$. Доказательство: $r(a-b) = 0 \Leftrightarrow a - b = 0$.

Замечание:

Два элемента кольца называются ассоциированными, если a делится на b и наоборот: $a, b \in R$, a ассоциировано с b если $a \in bR$, и $b \in aR$ или, что то же самое, $aR = bR$ ($aR,\ bR$ — идеалы).

Если $aR = bR$, R — область целостности (при $a \neq 0$), то:

$a = bx$, $b = ay$, $\Rightarrow a = ayx \Leftrightarrow yx = 1$. ($x, y$ — обратимые элементы).

А при $a = 0$:

$bR = \{0\} \Rightarrow b = 0 \Rightarrow a = b \cdot 1$.

Ответы:

Пусть $f : R \to \mathbb{N}_0 \cup \{-\infty\}$, такая, что:

1) $f(0) < f(r)\ \forall r \in R \setminus \{0\}$

2) $\forall a, b \in R\ \exists c, r \in R :\ f(r) < f(b)$ и $a = bc + r$.

Если такая функция существует, то R называется евклидовым кольцом, ну а f называется евклидовой нормой.

Определение: Главный идеал кольца — идеал, порожденный одним элементом, то есть идеал вида aR. R называется кольцом главных идеалов, если любой идеал является главным.

Теорема: Любое евклидово кольцо является кольцом главных идеалов.

Доказательство: $I \trianglelefteq R$ (произвольный идеал). Пусть a — ненулевой элемент идеала I, такой, что $f(a) \leq f(b)\ \forall b \in I \setminus \{0\}$

Возьмем произвольный элемент $d \in I \setminus \{0\}$. Тогда по условию евк. кольца, $\exists c, r \in R : d = ac + r,\ f(r) < f(a)$.

Но $r = d - ac$ (a лежит в идеале, соответственно, ac также лежит в идеале, d лежит в идеале, ну, значит, r тоже лежит в идеале)

Если $r \neq 0$, то $f(r) < f(a) \leq f(r)$ — противоречие. ($r = 0$, то есть $d = ac \in aR$).

Из всего предыдущего мы получили, что:

$I \subseteq aR$, $a \in R \Rightarrow aR \subseteq I \Rightarrow I = aR$

Наибольший общий делитель и его линейное представление

Определение: $a, b \in R$, R — коммутативное с единицей, $\gcd(a, b)$ — это такой общий делитель a, b, который делится на все остальные общие делители. Другими словами, если $a \in cR,\ b \in cR \Rightarrow \gcd(a, b) \in cR$, кроме того, $a, b \in \gcd(a, b)R$.

Предупреждение: gcd существует не в любом кольце. В кольце главных идеалов наибольший общий делитель существует всегда.

НОД соответствует наименьшему главному идеалу (чем больше делитель, тем меньше идеал).

Еще раз то же самое, но опять другими словами: $d = \gcd(a, b) \Leftrightarrow dR$ — наименьший главный идеал, содержащий a и b.

НОД — не число! НОД — идеал. $2\mathbb{Z}\ \ -2\mathbb{Z}$, так как 2 и -2 являются ассоциированными элементами. Ассоциированные элементы порождают одинаковые идеалы, следовательно, НОД определен с точностью до ассоциированности.

Линейное представление НОД:

$a \vdots b \Rightarrow a \in b\mathbb{Z}$

$n \vdots b \Rightarrow n \in b\mathbb{Z}$

Если существует любой другой идеал, содержащий a и n, то он содержит идеал $a\mathbb{Z} + n\mathbb{Z} \Rightarrow b\mathbb{Z} \subseteq c\mathbb{Z} \Rightarrow \begin{cases} a \vdots b \\ n \vdots b \end{cases}$

$\forall c : \begin{cases} a \vdots c \\ n \vdots c \end{cases} \Rightarrow b \vdots c \Rightarrow b =$ НОД, т.е. $b = d$.

Пример: $6\mathbb{Z} + 9\mathbb{Z} \subseteq 3\mathbb{Z} \subseteq 1\mathbb{Z}$: $6 \vdots 3, 9 \vdots 3$, $6 \vdots 1$ и $9 \vdots 1 \Rightarrow 3 \vdots 1$.

Теорема: Если R —кольцо главных идеалов, то $\forall a, b \in R\ \exists x, y \in R :\ ax + by = \gcd(a, b)$.

Доказательство:

$aR + bR = \{au + bv | u, v \in R\}$ — наименьший идеал, содержащий a, b. А, так как R — кольцо главных идеалов, то этот идеал — главный: $\exists d : aR + bR = dR$.

dR — наименьший главный идеал, содержащий a, b, т.е. $d = \gcd(a, b)$. Т.к. $d \in aR + bR$, то $\exists x, y \in R : d = ax + by$.

Функция Эйлера

$(\mathbb{Z}/n\mathbb{Z})$. $a \in (\mathbb{Z}/n\mathbb{Z})^*$

$\exists a' : a \cdot a' = 1$ в $\mathbb{Z}/n\mathbb{Z}$ $(aa' \equiv 1 \mod n)$

$\exists x : a \cdot a' = 1 + nx$ в целых числах.

$aa' - nx = 1$ имеет решение тогда и только тогда, когда $\gcd(a, n) = 1$.

Тогда $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}_n)^* = \{a | \gcd(a, n) = 1\}$, где $0 \leq a \leq n - 1$.

Поэтому функция эйлера есть ни что иное, как порядок группы: $\varphi = |\mathbb{Z}_n^*|$

Теорема:

1) $\varphi(ab) = \varphi(a)\varphi(b)$ при $\gcd(a,b) = 1$;

2) $\varphi(\prod\limits_{i=1}^{m}(p_i^{k_i})) = \prod\limits_{i=1}^{m}\varphi(p_i^{k_i})$;

3) $\varphi(p^k) = p^k - p^{k-1}$, где p — простое.

Доказательство:

1) $\gcd(a,b) = 1$, идеалы $aR + bR = R$ (взаимно простые, т.к. a и b взаимно простые).

По китайской теореме об остатках $R/abR \cong R/aR \oplus R/bR$.

(x,y) обратимы, $\Leftrightarrow \exists x', y'$, такие, что $(x,y)\cdot(x',y') = (1,1)$.

$xx' = 1$ и $yy' = 1 \Rightarrow x, y$ обратимы в R/aR и R/bR.

Мы можем произвести замену:

$(R/abR)^* \cong (R/aR)^* \times (R/bR)^*$, так как отличия прямой суммы от прямого произведения проявляются лишь на бесконечных множествах.

$\varphi(ab) = \varphi(a)\cdot\varphi(b)$ $(\varphi(ab) = |(R/abR)^*|)$.

2) Индукция по количеству сомножителей:

$n = \prod\limits_{i=1}^{m}(p_i^{k_i})$. $\varphi(n) = \prod\limits_{i=1}^{m}\varphi(p_i^{k_i})$, где p_i — различные простые.

База при $m = 1$ — левые и правые части совпадают.

Индукционный переход: $m > 1$, $a = \prod\limits_{i=1}^{m-1}(p_i^{k_i})$, $b = p_m^{k_m}$, $n = ab$.

$\gcd(a,b) = 1$, $\varphi(n) = \varphi(a)\varphi(b)$. У a на 1 множитель меньше, следовательно, воспользуемся индукционным переходом: $\varphi(a) = \prod\limits_{i=1}^{m-1}\varphi(p_i^{k_i})$, $\varphi(n) = \prod\limits_{i=1}^{m-1}\varphi(p_i^{k_i})\cdot\varphi(p_m^{k_m}) = \prod\limits_{i=1}^{m}(p_i^{k_i}) = \varphi(p_m^{k_m})$.

3) $\gcd(m, p^k) \neq 1 \Leftrightarrow m \vdots p$.

Таких чисел от 1 до p^k в p раз меньше, чем p^k, т.е. p^{k-1}. Это числа не взаимно просты. Тогда взаимно простых чисел

$p^k - p^{k-1}$, т.е.

$\varphi(p^k)$(взаимно простые с p^k) $= p^k$(всего)$-p^{k-1}$(не взаимно простые)

Например, $\varphi(60) = \varphi(2^2 \cdot 3 \cdot 5) = \varphi(2^2)\varphi(3)\varphi(5) = (2^2 - 2) \cdot (3 - 1) \cdot (5 - 1) = 2 \cdot 2 \cdot 4 = 16$.

Теорема Эйлера. Порядок элемента группы.

Определение: $a \in G$ — группа.

$< a >= \{1, a, a^2, ...a^{m-1}\}$ — циклическая группа.

$ord\ a = | < a > |$ (количество элементов в $\{1, a, a^2, ...a^{m-1}\}$) $=$ наименьшее m, т.к. $a^m = 1$ (порядок элемента)

Лемма: $a^k = 1 \Leftrightarrow k \vdots ord\ a$.

Доказательство: Пусть $k = ord\ a \cdot l \Rightarrow a^k = (a^{ord\ a})^l = 1^l = 1$. $(a^{ord\ a} = 1)$

В обратную сторону: пусть $k = ord\ a \cdot l + r,\ 0 \leq r < ord\ a$

$a^k = a^(ord\ a)^l \cdot a^r = a^r$.

Если $r \neq 0$, то $a^r = 1$ противоречит минимальности $ord\ a$. Таким образом, $r = 0$.

Если $a^m = 1$, то для $< a >$ выполняется: $a^{m-1} = a^{-1}, a^{m-2} = a^{-2}$, так как подгруппа — циклическая.

Циклическая группа изоморфна либо $\mathbb{Z}$, либо $\mathbb{Z}n$

$\{1, a, a^2, ...a^{m-1}\} \cong \mathbb{Z}n \cong \mathbb{Z}/n\mathbb{Z}$.

Следствие теоремы Лагранжа:

Порядок элемента группы равен порядку циклической подгруппы, образованной этим элементом, следовательно, порядок любого элемента a конечной группы G делит порядок G:

$|G| \vdots ord\ a$.

Теорема Эйлера:

$a^{\varphi(n)} \equiv 1 \mod n$. (Если $\gcd(a, n) = 1$)

Доказательство:

$a \in (\mathbb{Z}n)^* \Rightarrow |(\mathbb{Z}n)^*| \vdots ord\ a \Rightarrow \varphi(n) \vdots ord\ a$. Отсюда, по лемме, $a^{\varphi(n)} = 1$ в $\mathbb{Z} \ltimes^* \Leftrightarrow a^{\varphi(n)} \equiv 1 \mod n$.

Экспонента группы, теорема Кармайкла. Точное значение функции Кармайкла

Гипотеза Кармайкла:

Первые 10 значений функции Эйлера $\{1, 1, 2, 2, 4, 2, 6, 4, 6, 4\}$ многократно повторяются, следовательно, нет такого значения m, которое функция Эйлера принимает только один раз.

$n \in \mathbb{N}, \exists m \neq n : \varphi(n) = \varphi(m)$

Или: $\nexists m \in \mathbb{N} : \dim(\varphi^{-1}(m)) = 1$.

$(\mathbb{Z}/n\mathbb{Z})*$

G — группа. Экспонентой группы G называется наименьшее натуральное число l (l — НОК для всех элементов из G), такое, что $g^l = e$ (нейтральный) $\forall g \in G$. При этом l делится на порядок G.

$l = lcm(ord\ g)$ (lcm — НОК)

Функция Кармайкла — экспонента группы $(\mathbb{Z}/n\mathbb{Z})*$

Обозначаем $\lambda(n)$

Функция Кармайкла (без доказательства):

$\lambda(n) = \varphi'(n)$, если $n \not\vdots 8$

$\lambda(n) = \frac{1}{2}\varphi'(n)$, если $n \vdots 8$

$(\mathbb{Z}/2^k\mathbb{Z})^* \cong C_2 \times C_{2^{k-2}}\ \forall k \geq 3$, где C — циклическая группа.

Теорема Кармайкла:

$a^{\varphi(n)} \equiv 1 \mod n$

$\varphi(60) = \varphi(2^2 \cdot 3 \cdot 5) = \varphi(2^2)\varphi(3)\varphi(5) = (2^2 - 2) \cdot (3-1) \cdot (5-1) = 2 \cdot 2 \cdot 4 = 16$

$\varphi'(60) = lcm(\varphi(2^2)\varphi(3), \varphi(5)) = 4$

$\mathbb{Z}/n\mathbb{Z} \cong \oplus_{i=1}^{m} \mathbb{Z}/p_i^{k_i}\mathbb{Z}$

Лемма $\times_{i=1}^{m} G_i$ (G — произвольные группы)

$(x_1, ..., x_m), x_i \in G_i$.

Пусть $d_i = ord\ x_i$.

$(x_1, ..., x_m)^l = (x_1^l, ..., x_m^l) = (e_{G_1}, ..., e_{G_m}) \Rightarrow x_i^l = e \forall i \Rightarrow e$ — НОК, то есть $l = (lcm d_i)_{i=1}^{m}$

$ord\ (x_1, ..., x_m) = lcm(d_1, ..., d_m)$.

Таким образом, если $(x_1, ..., x_m)^l \in \times_{i=1}^{m} (\mathbb{Z}/p_i^{k_i}\mathbb{Z})*$, то $(x_1, ..., x_m)^l = (1, ..., 1)$ при $l = lcm(\varphi(p_i^{k_i}))$.

Обозначим $\varphi'(p_i^{k_i}, ..., p_m^{k_m}) = lcm(\varphi(p_i^{k_i}))$.

По китайской теореме об остатках $\mathbb{Z}/n\mathbb{Z} \cong \oplus_{i=1}^{m} \mathbb{Z}/p_i^{k_i}\mathbb{Z}$, где $n = \prod\limits_{i=1}^{m} p_i^{k_i}$, p_i — различные простые.

Многочлены. Теорема о делении с остатком

F — поле. $F[t]$ — кольцо многочленов над полем F.

($F[t] = \{a_0 + ... + a_n t^n | a_i \in F, a_n \neq 0$ при $n \neq 0\}$ (где t — просто символ, не переменная!)

$$(a_1, ..., a_n) \cdot (b_0, ..., b_n) = (c_0, ..., c_{n+m}), C_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

С многочленом $p(t) = a_0 + ... + a_n t^n$ связана полиномиальная функция $f_p : F \to F$.

$f_p(x) = a_0 + ... + a_n x^n \ \forall x \in F$.

Если $F = F_2 = \mathbb{Z}/2\mathbb{Z}$, то многочлены t и t^2 не равны, но соответствующие полиномиальные функции равны. (F_2 — поле из двух элементов).

$\deg(a_0 + ... + a_n t^n) := n$ при этом $a_n \neq 0$.

$\deg(0) = -\infty$;

$\deg(pq) = \deg p + \deg q$;

$\deg(p + q) \leq \deg q$.

Теорема (о делении с остатком):

deg является евклидовой нормой на $F[x]$, а само $F[x]$ — евклидово кольцо.

Доказательство:

1) $\deg 0 < \deg p \ \forall p \neq 0$

2) $p, q \neq 0 \in F[t]$

$X = \{p - qf || f \in F[t]\}$.

Пусть $p - qf$ — многочлен наименьшей возможной степени из X.

Если $r > \deg q$:

$q = a_m t^m + ...$

$r = b_{m+k} t^{m+k} + ...$

$r - qt^k \frac{b_{m+k}}{a_m} < \deg r$, но $r - qt^k \frac{bm+k}{a_m} \in X$

Противоречие показывает, что $\deg r < \deg q \Rightarrow p = qf + r, \ \deg r < \deg q$.

(мы доказали, что $F[x]$ является евклидовым кольцом)