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.

Содержание

1 Нормальные подгруппы и идеалы. Свойства гомоморфизма

Нормальная подгруппа – подгруппа, для которой выполняется $\forall g \in G, h \in H$ верно $ghg^{-1} \in H$ или, аналогично, $gH = Hg$.

В абелевой группе все подгруппы нормальные.

Идеал — аддитивная подгруппа I кольца R, для которой выполняется $\forall r \in R, i \in I$ верно $ri \in I$ (левый идеал), $ir \in I$ (правый идеал). Идеал выдерживает умножение на элементы кольца.

Гомоморфизм групп — отображение группы $(G, *)$ в группу $(H, \#)$, такое, что $f(g * g') = f(g) \# f(g')$.

Гомоморфизм колец — гомоморфизм, сохраняющий операции (т.е. переводящий сложение в сложение, умножение в умножение).

Свойства гомоморфизма групп:

1) $f(e_x) = e_y$ (рассмотреть перевод произведения двух $f(e_x)$ в одну $f(e_x)$ и домножить на обратный);

2) $f(a^{-1}) = (f(a))^-1$ (представить перемножение элемента и обратного, получится e, дальше понятно);

Свойства гомоморфизма колец:

1) $f(0) = 0$;

2) $f(-a) = -f(a)$;

3) $f(a + b) = f(a) + f(b)$;

4) $f(ab) = f(a)f(b)$.

Образ гомоморфизма — его образ как функции.

Свойства:

Образ гомоморфизма групп всегда является подгруппой. Доказывается на изи, потому что гомоморфизм сохраняет операции, нейтральный и обратный.

Ядро гомоморфизма — все такие элементы, которые гомоморфизм обращает в нейтральный.

Свойства:

1) Ядро гомоморфизма всегда содержит нейтральный элемент (так как гомоморфизм переводит нейтральный в нейтральный).

2) Ядро гомоморфизма групп/колец является нормальной подгруппой/двусторонним идеалом (гомоморфим $g^{-1}hg$).

2 Существование эпиморфизма групп с данным ядром

Теорема: $H \trianglelefteq G$, группы по умножению. Тогда существует группа F и эпиморфизм φ, такой, что $\ker\varphi = H$.

Доказательство:

Задаем $F = \{gH | g \in G\}$, $\varphi(g) = gH$, обратная $\varphi^{-1} = gH = Hg$.

Проверяем корректность операций ($ahbh \in abH$).

Доказываем, что F — группа (ассоциативность непосредственно, нейтральный H, так как $gHH = gH$, обратный аналогично через нейтральный eH и предположение существования g^1H).

Доказываем, что H — $\ker\varphi$: берем элемент из H, доказываем, что он лежит в ядре ($\varphi(h) = hH = H$). Затем берем какой-то элемент $g \in \ker\varphi$, гомоморфируем, получаем $gH = H \Rightarrow gh_1 = h_2 \Rightarrow g = h_1^{-1}h_2 \Rightarrow g \in H$. То есть любой элемент из ядра лежит в H следовательно, $H = \ker\varphi$.

Говорим, что структура G/H называется факторгруппой.

3 Существование эпиморфизма колец с данным ядром

Теорема: I — двусторонний идеал, R и A — кольца. Тогда существует эпиморфизм с ядром I.

Доказательство:

Определяем $\varphi(a) = a + I$ и $\varphi(b) = b + I$. Проверяем корректность при сложении и умножении, при этом не забываем о том, что идеал выдерживает умножение на элементы кольца.

Аналогично группам доказываем, что I нейтральный по сложению в A.

Также аналогично доказываем, что $I = \ker\varphi$.

Не забываем сказать, что R/I — факторкольцо.

4 Теорема о гомоморфизме

Теорема: G, G', G'' — группы. $f : G \to G'$ — эпиморфизм, $g : G \to G''$ — гомоморфизм. Если $\ker f = \ker g$, тогда существует единственный мономорфизм $h : G' \to G''$, такой, что $g = h \circ f$.

Если g — эпиморфизм, то h — гомоморфизм.

Доказательство: задаем $x' \in G'$, тогда в силу сюръективности существует $x \in G$, являющийся его прообразом. Задаем $h(x') = g(x)$, проверяем корректность данного определения, взяв $y \in G$ такой, что $f(y) = x'$. Тогда $f(y) = f(x) \Rightarrow y = xt, t \in \ker f \Rightarrow g(y) = g(t)g(x) = g(x)$, что показывает корректность определения.

Доказываем, что h — гомоморфизм. Берем $x', z' \in G'$, тогда есть $x, z \in G$. Тогда, в силу гомоморфности f, g: $f(xz) = f(x)f(z)$, $h(xz) = g(xz) = g(x)g(z) = h(x')h(z')$, то есть h — гомоморфизм. Положим теперь $f(x') = h(z')$ и аналогично проверке корректности получаем $x' = f(x) = f(z)f(t) = f(z) = z'$, то есть h — инъекция.

Если $g = h \circ f$ — сюрьекция, то h также сюръекция, а, следовательно, биекция.

Теорема о гомоморфизме: Гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма.

Доказательство: функция f, задающая образ, сюръективна по определению. Она - эпиморфизм с ядром $\ker f$ по теореме о существовании эпиморфизма с данным ядром. Тогда f обладает теми же свойствами, что и группы в теореме выше, следовательно, существует изоморфизм $Imf \cong G/\ker f$.

5 Смежные по подгруппе, Лагранж

Смежный класс — $gH = \{gh | h \in H\}$ для некоторого $g \in G$.

Лемма: Смежные классы равномощны подгруппе, по которой образованы.

Доказательство: $f : H \to gH$ — биекция. Сюръекция по определению, инъекция, т.к. из $gh_1 = gh_2$ следует $h_1 = h_2$.

Лемма: Смежные классы либо не пересекаются, либо совпадают.

Доказательство: Предполагаем, что существует $g \in g_1H \cap g_2H$, тогда $g = g_1h_1 = g_2h_2 \Leftrightarrow g_1 = g_2h_1^{-1}h_2 \Rightarrow g_1H \subset g_2H$, так же в обратную сторону, тогда смежные классы равны.

Теорема: Порядок подгруппы является делителем порядка группы.

Доказательство: Вводим левые смежные классы по подгруппе, их непересекающееся объединение составляет группу, следовательно, порядок группы равен сумме порядков каждого смежного класса, классы равномощны.

6 Взаимно простые идеалы, их пересечение и произведение

Идеал I — **простой**, если из $ab \in I$ следует $a \in I$ или $b \in I$.

Идеалы называются взаимно простыми, если $I_1 + I_2 = R$. При этом, соответственно, найдутся такие $i_1 \in I_1, i_2 \in I_2$, что $i_1 + i_2 = 1$.

Лемма: Если все идеалы $I_1, ..., I_n$ — попарно взаимно простые, то $I_1 \cap ... \cap I_n = I_1 \cdot ... \cdot I_n$. Доказывается по индукции, в обе стороны:

$\begin{cases} \forall i_1 \in I_1 \ \ i_1 I_2 \subseteq I_2 & \forall i_2 \in I_2 \ \ i_2 I_1 \subseteq I_1 \end{cases} \Rightarrow \begin{cases} I_1 I_2 \subseteq I_2 & I_2 I_1 \subseteq I_1 \end{cases} \Rightarrow I_1 I_2 \subseteq I_1 \cdot I_2$.

Обратно: берем $i_1 \in I_1, i_2 \in I_2$, для них верно, что $i_1 + i_2 = 1$, берем $x \in I_1 \cap I_2$, для него $x = x \cdot 1 = x(i_1 + i_2) = xi_1 + xi_2$. Это элементы идеалов, следовательно, x лежит в сумме идеалов, а $I_2 I_1 + I_1 I_2 = I_1 I_2$. Значит, любой элемент пересечения лежит в произведении, следовательно, пересечение равно произведению.

Переходим по индукции с использованием

Леммы: Если I_1 взаимно прост с $I_2 ..., I_k$, то он взаимно прост с их произведением.

Доказываем опять по индукции, берем $k = 3$, расписываем $R = I_1 + I_2$ и $= I_2 + I_3$, затем $I_1 + I_2 = I_1 + I_2 R = I_1 + I_2(I_2 + I_3) = I_1 + I_2 I_3 = R$. Индукция по k: $I_1 \cdot ... \cdot I_k = R$ и $I_{k+1} + J = R$, перемножаем, все классно

Возвращаемся к предыдущей лемме, доказываем для нее ИП.

7 Китайская теорема об остатках

Теорема: R — коммутативное с 1. Если $I_1, ..., I_n$ — взаимно простые, то $R/I_1 \cdot ... \cdot I_n \cong \oplus_{i=1}^n R/I_i$.

Доказательство по индукции для $k = 2$. $R/I_1 \cdot I_2 \cong R/I_1 \oplus R/I_2$. Строим гомоморфизм $\varphi : R \to R/I_1 \oplus R/I_2$. $\varphi(r) = (r + I_1, r + I_2)$. Проверим, что это гомоморфизм. Затем говорим, что, раз идеалы взаимно просты, то $I_1 + I_2 = R \Rightarrow i_1 + i_2 = 1$. Тогда прообразом элемента $(x + I_1, y + I_2)$ будет являться элемент $xi_1 + yi_2$. Доказываем это, взяв гомоморфизм (не забываем, что элементы вида $xi_1 \in I_1$!!!). Получаем, что это верно. Таким образом, имеем два эпиморфизма, первый мы доказали, второй очевиден по теореме о существовании эпиморфизма с данным ядром. По теореме о гомоморфизме между их образами существует изоморфизм.

Индукция осуществляется аналогично, $R/I_1 \cdot ... \cdot I_{n+1} \cong R/I_1 \cdot ... \cdot I_n \oplus R/I_{n+1}$.

8 Простые и максимальные идеалы

Идеал I — **простой**, если из $ab \in I$ следует, что либо $a \in I$, либо $b \in I$.

Максимальный идеал — идеал, который не содержится ни в каком другом идеале.

Лемма: Для любого идеала существует максимальный идеал, который его содержит. (без доказательства)

Лемма: Любой максимальный идеал является простым.

Доказательство через расписывание определения простого идеала. Для определенности говорим, что $a \notin I$, значит, должно выполняться $b \in I$. Затем рассматриваем структуру $I + aR = R$. Домножаем на b с обоих сторон, получаем хренюшку $bR = bI + baR$, откуда следует, что $bI \subseteq I;\ ba \in I \Rightarrow baR \subseteq I; b \in bR \Rightarrow b \in bI + baR \subseteq I \Rightarrow b \in I$

Лемма:

1) Идеал I — простой $\Leftrightarrow$ R/I — область целостности

2) Идеал I — простой $\Leftrightarrow$ R/I — поле.

Доказательство 1 вправо: допускаем, что R/I — не область целостности, следовательно, существуют $a, b \neq I, a, b \in R/I$, такие, что $ab = eI$. Расписываем $ab = I$, умножаем, получаем $r_1r_2 + I \in I \Rightarrow r_1r_2 \in I$, что по определению простого идеала дает $a \in I$ или $b \in I$, что противоречит тому, что R/I — не область целостности. Ура.

Доказательство 1 влево: говорим, что если $ab = I$, то либо $a = I$, либо $b = I$. Расписываем их, получаем что $r_1 \in I$ или $r_2 \in I$, затем расписываем $ab = I \Rightarrow r_1r_2 \in I$.

Доказательство 2 вправо: расписываем a, b, получаем $r_1r_2 + I = R$, так как I — максимальный, $r_1r_2 + i = 1$, добавим и вычтем с каждой стороны по I, чтобы избавиться от i, получим, что $r_1r_2 = 1$, то есть любой элемент имеет обратный.

Доказательство 2 влево: расписываем a, b, перемножаем, приравниваем к 1, так как каждый элемент имеет обратный, откуда следует, что $r_1r_2 + I = 1$, значит, I — максимальный.

9 Неприводимые элементы и простота главного идеала

Элементы $a, b \in R$ называются **ассоциированными**, если $a \in bR$ и $b \in aR$, или, иначе говоря, a делит b и b делит a, то есть они отличаются на обратимый элемент.

Элемент $p \in R$ называется **неприводимым**, если из $p = ab$ следует, что либо a ассоциировано с p, либо b ассоциировано с p.

Элемент p простой, если pR — простой идеал.

Лемма: если pR простой идеал, то p неприводим.

Доказательство: $ab = p$, либо $a \in pR$, либо $b \in pR$ по свойству простых идеалов. Пусть $a \in pR$. Тогда $a = pr \Leftrightarrow p = ar^{-1} \Rightarrow p \in aR$. Значит, p ассоциировано с a.

Главный идеал — идеал, образованный одним элементом, идеал вида aR.

Кольцо главных идеалов — кольцо, в котором любой идеал главный (кольцо целых чисел является кольцом главных идеалов).

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

Доказательство: если $ab \in pR$ и pR простой, то $a \in pR$ или $b \in pR$. Предположим, что это не так, и оба элемента не лежат в pR. Тогда $aR + pR = a'R$, отсюда $p = a'r$. Расписываем p по условию неприводимости, говорим, что либо a', либо r обратимы. Если обратим $a'R = R$. Если обратим r, то $a' = pr^{-1} \Rightarrow prr^{-1} = a'r \Rightarrow pR = a'R$. То есть p ассоциирован с a', следовательно, $a \in pR$, противоречие, значит, верно что $a'R = R$. Аналогично с b. $R = aR+pR = a(bR+pR)+pR = abR+pR = pR$. $pR = R$, значит, p обратимый, противоречие условию, следовательно, $a \in pR$ или $p \in pR$.

10 Факториальные кольца. Достаточное условие факториальности

Кольцо R **факториально**, если существуют неприводимые элементы $p_1, ..., p_m \in R$ и обратимый элемент $\epsilon \in R$, такие, что $r = \epsilon p_1 ... p_m$ и если $\epsilon p_1 ... p_m = \delta q_1 ... q_n$, то $m = n$ и существует такая перестановка σ, что p_i ассоциировано с $q_\sigma(i)$.

Лемма: Пусть R — кольцо, область целостности, в которой каждый элемент порождает простой идеал. Если каждый необратимый раскладывается в произведение неприводимых, то кольцо R факториально.

Доказательство: говорим, что $\epsilon p_1 ... p_m = \theta q_1 ... q_n$. Индукцией по $\min(m, n)$ докажем, что $m = n$ и p_i ассоциировано с $q_{\sigma(i)}$. База индукции $n = 0$, $\epsilon = \theta q_1 ... q_m$ тоже обратимо, тогда $\epsilon = \theta$, значит, $m = n = 0$.

ИП: $p_m R$ — простой, тогда $\exists l$, т.ч. $q_l = p_m R \Rightarrow \exists \delta$, т.ч. $q_l = \delta p_m$, причем, т.к. q_l неприводим, то δ обратим. Подставим это в равенство для m: $\theta q_1 ... q_n = \theta q_1 ... q_{l-1} p_n \delta q_{l+1} ... q_m = \epsilon p_1 ... p_n$. Сократим на p_n, для этой конструкции будет выполняться условие индукции, значит, $m = n$ и искомая перестановка $\sigma(m) = l$.

11 Факториальность кольца главных идеалов

Теорема: Область главных идеалов является факториальным кольцом

Доказательство: пусть $r \in R$ — необратимый. Идеал $rR \subseteq p_1R$, где p_1R максимальный, значит, $r = r_1p_1$, при этом p_1 неприводим. Будем раскладывать так каждый r_i. Если на одном из этапов r_i обратим, то теорема доказана. Иначе рассмотрим объединение идеалов $I = \cup r_iR$, он идеал, значит, $I = qR$. Тогда $q \in r_jR$, так как I — объединение всех идеалов вида r_iR. То есть $qR \subseteq r_jR$, но одновременно $r_jR \subseteq qR$. Значит, r_j ассоциировано с q. Еще $r_jR \subseteq r_{j+1}R$ и $r_{j+1}R \subseteq qR = r_jR$. Тогда $r_{j+1}R = qR$, $r_{j+1}R$ ассоциировано с r_jR, тогда они отличаются на обратимый. Мы знаем, что $r_j = r_{j+1}p_{j+1}$, значит, либо p_{j+1} обратим, либо r_{j+1} обратим. p_{j+1} неприводим, и, значит, необратим, следовательно, r_{j+1} обратим.

12 Евклидовы кольца и кольца главных идеалов

R — область целостности. Если $\exists f : R \to \mathbb{N} \cup \{-\infty\}$, обладающая следующими свойствам:

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

2) $\forall a \neq 0$ и $b \neq 0$, $ab \in R$ существуют такие r, q, что $a = bq + r$, причем $f(r) < f(b)$,

то такое кольцо называется **евклидовым**, а функция - евклидовой нормой.

Теорема: Евклидово кольцо является кольцом главных идеалов.

Доказательство: берем нетривиальный идеал, берем из него такое b, чтобы его евклидова норма была минимальной. Затем берем $a \in I$, тогда, по условию евклидового кольца, выполняется $a = bq + r$, (такие q и r существуют), откуда $r = a - bq$, оба слагаемых лежат в идеале, значит, r лежит в идеале и его евклидова норма 0, т.к. у b евклидова норма минимальна. Тогда a делит b и, следовательно, $I \subseteq bR$, но $b \in I \Rightarrow bR \subseteq I \Rightarrow bR = I$, значит, любой идеал в R — главный.

13 НОД и его линейное представление

Элемент $d = \gcd(a, b)$, если он делит и a, и b и он делит любой другой общий делитель a и b.

Таким образом, $aR + bR \subseteq dR$.

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

Доказательство: на изи. $aR + bR = dR$ — главный, следовательно, $\exists x \in R, y \in R$, такие, что $d = ax + by$.

14 Функция Эйлера

Функция Эйлера от n — количество элементов от 1 до n, которые взаимно просты с n .

Лемма: $\gcd(a,n) = d$, $aZ + n\mathbb{Z}$ — максимальный, тогда $a\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$.

Доказываем от противного, предполагая, что $a\mathbb{Z} + n\mathbb{Z} = b\mathbb{Z}$.

Тогда b делится на a и n, если a делится на c и b делится на c, то aR и bR подмножества cR, то есть $bR \subseteq cR$, то есть b делится на c, следовательно, $b = d$.

Свойства функции Эйлера:

1) Если $\gcd(a,b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$.

Доказательство: $aR + bR = R$. Применяем КТО, $R/abR \cong R/aR \oplus R/bR \Rightarrow (R/abR)^* \cong (R/aR)^* \times (R/bR)^*$, И тогда получаем, что $\varphi(a,b) = (R/abR)^*$ (по определению), $\varphi(a) = (R/aR)^*$, $\varphi(b) = (R/bR)^*$, следовательно, $\varphi(a)\varphi(b) = \varphi(ab)$.

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

Доказательство: индукция по количеству сомножителей. Индукционный переход раскрыть по предыдущему свойству как $\varphi(p_i^{k_m}) \cdot \prod\limits_{i=1}^{m-1}\varphi(p_i^{k_i}) = \prod\limits_{i=1}^{m}\varphi(p_i^{k_i})$.

3) $\varphi(p^k) = p^k - p^{k-1}$.

Доказательство: $\gcd(m, p^k) \neq 1$, следовательно, m делит p. Таких m от 1 до p^k будет в p раз меньше, так как каждое число m имеет с p^k общий делитель.

15 Порядок элемента группы, теорема Эйлера

Пусть $a \in \mathbb{Z}_n^*$; $a^m = 1(mod\ n)$.

$< a >$ — циклическая группа, порожденная элементом a.

Порядком элемента a называется наименьшая степень, в которую надо возвести a, чтобы получить 1. Если такого числа не существует, то порядок группы равен бесконечности. Обозначается $\operatorname{ord} a$.

Лемма: $\varphi(n) = |(\mathbb{Z}_n)^*|$.

Доказательство: пусть a из группы. Для него существует такой a', что $aa' = 1(mod\ n)$, значит, существует x, такой, что $xn = aa' - 1 \Rightarrow aa' - xn = 1$, отсюда $\gcd(a, n) = 1$, по определению функции Эйлера она — количество элементов взаимно простых с n, а такие в нашей группе все, так как доказанное условие выполняется для любого a.

Лемма: $a^k \equiv 1 \Leftrightarrow k \vdots \operatorname{ord} a$.

Доказательство: Если k делит $\operatorname{ord} a$, то $k \geq \operatorname{ord} a \Rightarrow k = (\operatorname{ord} a)b + r$, где $0 < r < \operatorname{ord} a$.

Перепишем как $a^{(\operatorname{ord} a)b+r} = 1 \Rightarrow (a^{\operatorname{ord} a})^b \cdot a^r = 1 \Rightarrow 1^b a^r = 1 \Rightarrow a^r = 1 \Rightarrow r = 0 \Rightarrow k \vdots \operatorname{ord} a$.

В обратную сторону: $k \vdots \operatorname{ord} a \Rightarrow k = (\operatorname{ord} a)b \Rightarrow (a^{\operatorname{ord} a})^b = 1$.

Следствие из теоремы Лагранжа:

Т.к. $\operatorname{ord} a = | < a > |$, а $< a >$ — подгруппа в G, то $|G|$ делится на $\operatorname{ord} a$.

Теорема Эйлера:

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

Доказательство: По следствию из теоремы Лагранжа $|(Z_n)^*| \vdots \operatorname{ord} a \Rightarrow \varphi(n) \vdots \operatorname{ord} a \Rightarrow \varphi(n) = (\operatorname{ord} a)b \Rightarrow (a^{\operatorname{ord} a})^b = 1$.

16 Экспонента группы, теорема Кармайкла

Экспонента группы — наименьшее натуральное число d, такое, что $\forall g \in G$ будет верно $g^d = e$. Экспонента существует для всех конечных групп.

$g^d = e \Rightarrow d \vdots \operatorname{ord} g \ \forall g \in G \Rightarrow d = \operatorname{lcm}(\operatorname{ord} g_1, ..., g_m)$, где $m = |G|$.

Теорема Кармайкла:

Пусть $n = \prod\limits_{i=1}^{m} p_i^{k_i}$, где p_i — взаимно простые множители.

$\varphi'(n) = \operatorname{lcm}(\varphi(p_1^{k_1}), ..., \varphi(p_m^{k_m}))$.

Если $\gcd(a, n) = 1$, то $\varphi'(n) \equiv 1 (mod\ n)$.

Доказательство: $\gcd(a, n) = 1$, то $\gcd(a, p_i) = 1$. Пусть $a \equiv x_i (mod\ p_i)$. Тогда $a = (x_1, ..., x_m) \in \times_{i=1}^{m} (Z/p_i^{k_i} Z)^*$

$\varphi'(n) = \operatorname{lcm}(\varphi(p_1^{k_1}), ..., \varphi(p_m^{k_m})) \Rightarrow \varphi'(n) \vdots \varphi(p_i^{k_i})$.

$\varphi(p_i^{k_i}) = |(Z/p_i^{k_i} Z)^*|$ по определению функции Эйлера от простого числа.

$|(Z/p_i^{k_i} Z)^*| = |(Z_{p_i^{k_i}})^*| \vdots \operatorname{ord} x$ по следствию из теоремы Лагранжа.

$x^{\operatorname{ord} x} \equiv 1 (mod p_i^{k_i}) \Rightarrow x^{|(Z_{p_i^{k_i}})^*|} = 1 (mod p_i^{k_i}) \Rightarrow x^{\varphi(p_i^{k_i})} = 1 (mod p_i^{k_i}) \Rightarrow x^{\varphi'(n)} = 1 (mod p_i^{k_i})$

$a^{\varphi'(n)} = (x_1, ..., x_m)^{\varphi'(n)} = (1, ..., 1) = 1 (mod p_i^{k_i})$.

17 Многочлены. Теорема о делении с остатком

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

$F[t] = \{a_0 + a_1t^1 + ... + a_nt^n | a_i \in R; a_n \neq 0\}$.

Многочлены можно представить в виде множества коэффициентов $F[n] = (a_0, ..., a_n)$.

Сложение многочленов определено стандартно.

Умножение многочленов: каждый элемент множества коэффициентов представляется в виде суммы $\sum\limits_{i=0}^{n} a_ib_{n-i}$.

Полиномиальная функция — значение многочлена в точке x.

Теорема о делении с остатком:

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

Доказательство: зададим условия евклидовости:

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

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

Пусть $X = \{p - qf | f \in F[t]\}$. Берем $r \in X$, такое, что $\deg(r) \leq \deg(r')\forall r' \in F[t]$. Тогда $p = fq + r$.

Допустим, что $\deg(q) \leq \deg(r)$. Распишем их по коэффициентам (коэффициенты большего многочлена задавать как $m+n$), $m \geq n$, умножим q на t^m и на $\frac{b_{n+m}}{a_n}$, отсюда $\deg(r - q \cdot t^m \cdot \frac{b_{n+m}}{a_n}) < \deg(r)$. Но $r - q \cdot t^m \cdot \frac{b_{n+m}}{a_n}$ лежит в $X \Rightarrow r$ не минимальный. Противоречие.