Семестр I. Комплексные числа, многочлены, матрицы, СЛАУ

18 февраля 2018 г.   21:35

Семестр IV. Специальные разделы

18 февраля 2018 г. 21:36

Содержание

Sunday, May 20, 2018 23:09

35. Взаимно простые идеалы (определение и лемма об их произведении и пересечении).
36. Взаимно простые идеалы (определение и лемма о взаимной простоте с произведением).
37. Китайская теорема об остатках.
38. Неприводимые и ассоциированные элементы кольца (определения для области целостности).
39. Простой идеал и простой элемент (определения).
40. Простые и неприводимые элементы (лемма).
41. Разложение на неприводимые множители в ОГИ.
42. Максимальные идеалы (определение и простота).
43. Факторкольцо по простому и максимальному идеалу.
44. Простые и максимальные идеалы в ОГИ.
45. Евклидово кольцо (определение).
46. Идеалы евклидова кольца. Алгоритм Евклида.
47. Присоединение к полю алгебраического элемента.
48. Классификация конечных полей.
49. Конечные подгруппы мультипликативной группы поля.
50. Строение мультипликативной группы кольца Z/nZ, где n – степень простого числа.
51. Экспонента мультипликативной группы кольца Z/nZ.
52. Тесты Ферма и Эйлера.
53. Псевдопростые числа Ферма и Эйлера.
54. Тест Миллера–Рабина.

Теория групп

4 апреля 2018 г. 16:24

Функция. Отношение

27 февраля 2018 г.   14:45

Функция

Функция f — это тройка (X, Y, Γ), где X, Y — множества, $\Gamma \subseteq X \times Y$; т.е. $\forall x \in X: \exists!\, y \in Y, (x, y) \in \Gamma$

X — **область определения**

Y — **множество значений**

Γ — **график функции**

Вместо $(x, y) \in \Gamma$ обычно пишется $f(x) = y$

Образ функции (образ множества X под действием f) -
$Im\, f = \{f(x) | x \in X\} = \{y \in Y | \exists f(x) = y\}$

Пример: $f(x) = x^2; f: \mathbb{R} \to \mathbb{R}; Im\, f = \mathbb{R}_{\geq 0}$
Для доказательства этого недостаточно сказать, что $f(x) = x^2 \geq 0$. Из этого следует только то, что $Im\, f \subseteq \mathbb{R}_{\geq 0}$. Нужно доказать и обратное включение.

$x^2 = a \geq 0 \Leftarrow x = \sqrt{a};\ \mathbb{R}_{\geq 0} \subseteq Im\, f$ ■

f — **инъективна,** если $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

f — **сюръективна,** если $Im\, f = Y \Leftrightarrow \forall y\ \exists x: f(x) = y$

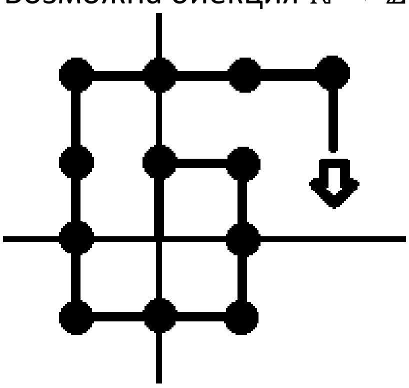
f — **биективна**, если она инъективна и сюръективна

$f(x) = y$

Количество решений	Свойство
≤ 1	Инъективность
≥ 1	Сюръективность
1	Биективность

Два множества, между которыми существует биекция - **равномощны**. Так, равномощны множества $\mathbb{N}$ и $\mathbb{Z}$ — существует биекция: нечетные числа в отрицательные, четные - в положительные.

Возможна биекция $\mathbb{N} \to \mathbb{Z} \times \mathbb{Z}$



Континуум - мощность множества $\mathbb{R}$

Континуум-гипотеза - утверждает, что $\mathbb{R}$ — минимальное несчётное множество.

Недоказуема.

Парадокс Рассела
X – множество всех множеств. Тогда $X \subset X, X \in X$.
Множество R – **рекурсивно**, если $R \in R$, т.е. R содержит самого себя в качестве элемента.
Пусть A – множество всех нерекурсивных множеств.
Если $A \in A \Rightarrow A$ – рекурсивно. Но тогда $\mathrm{A} \notin \mathrm{A}$
Если же $A \notin A$, то A все же содержится в множестве нерекурсивных множеств, т.е. $A \in A$.
Получается, что $A \in A \Leftrightarrow A \notin A$.
Для борьбы с этим парадоксом X считается классом 1-го порядка, и противоречия не возникает.

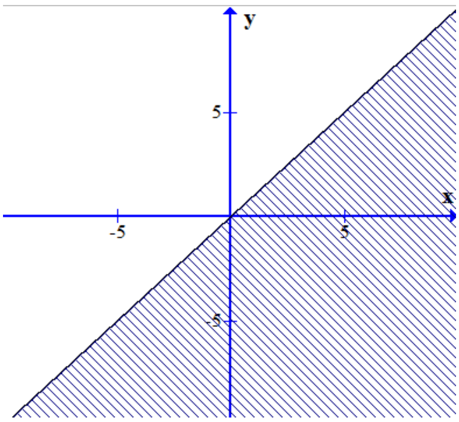
$f: X \to Y$
$g: Y \to Z$
$g \circ f: X \to Z$
$g \circ f(x) = g\big(f(x)\big)$ – **композиция**

$ind_x: X \to X$
$f \circ ind_x = f$
$ind(x) = x$ – **identity**

$f: X \to Y;\ \tilde{f}: Y \to X$
$f, \tilde{f}$ - **взаимно обратны**, если $f \circ \tilde{f} = ind_x$
$\tilde{f} \circ f = ind_y$
$\exists \tilde{f}$: тогда и только тогда, когда f – биективна

Отношение на множестве

Отношение на множестве X – подмножество $X \times X$.
Отношение "$\geq$"



Для отношения R вместо $(x, y) \in R$ пишется xRy.

Отношение " $\sim$ " называется **отношением эквивалентности,** если:
- $x \sim x$
- $x \sim y \Leftrightarrow y \sim x$
- $x \sim y, y \sim z \Rightarrow x \sim z$

Класс эквивалентности x — множество элементов, эквивалентных x.
$[x]_\sim = \{y \in X | y \sim x\}$

Лемма. $[x]_\sim \cap [y]_\sim \neq \emptyset \Rightarrow [x]_\sim = [y]_\sim$
Доказательство: $z \in [x]_\sim \cap [y]_\sim \Rightarrow z \sim x, z \sim y \Rightarrow x \sim y$
$a \in [x]_\sim \Rightarrow \begin{cases} a \sim x \\ a \sim y \end{cases} \Rightarrow a \in [y]_\sim$
Аналогично $a \in [y]_\sim \Rightarrow a \in [x]_\sim$ ■

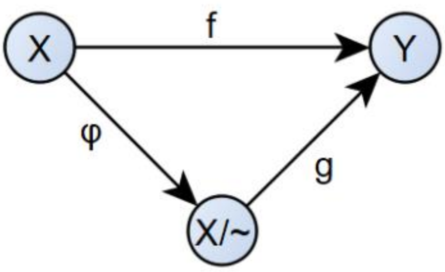
Определение
$\exists A \subseteq X\colon X = \coprod_{x \in A} [x]_\sim$
Множество A состоит из одного элемента для каждого класса эквивалетности.

Если на X задано отношение эквивалетности, то **фактормножество** $x/\sim$ - множество классов эквивалентности.

Пример
" $\equiv_n$ " на $\mathbb{Z}$
$a \equiv_n b \overset{\text{def}}{=} (a - b) \vdots n$

Классы эквивалетности — $\begin{matrix} [\pm 0, \pm n, \pm 2n, \dots] \\ [1, 1 \pm n, 1 \pm 2n, \dots] \\ \dots \\ [n-1, n-1 \pm n, n-1 \pm 2n, \dots] \end{matrix}$
Обычно в качестве представителей в данном случае берутся $0, 1, \dots n - 1$.
$\mathbb{Z}_n/\mathbb{Z} = [0, 1, \dots n - 1]$

Теорема
Рассмотрим множество функций $f\colon X \to Y$ с отношением эквивалентности $\sim$.
$a \sim b \Rightarrow f(a) = f(b)$
В частности, этим свойством обладает функция $\varphi\colon X \to X/\sim$, $\varphi(x) = [x]_\sim$
$a \sim b \Leftrightarrow [a]_\sim = [b]_\sim \Leftrightarrow \varphi(a) = \varphi(b)$



Универсальное свойство функции φ
$\forall f\colon X \to Y, a \sim b \Rightarrow f(a) = f(b)$:
$\exists!\, g\colon X/\sim \to Y, g \circ \varphi = f$

Доказательство
$g([x]_\sim) = f(x)$ по определению
$x \sim y \Rightarrow [x]_\sim = [y]_\sim \Rightarrow g([x]_\sim) = g([y]_\sim) \Rightarrow f(x) = f(y)$ ■

$\mathbb{Z}$

Определение

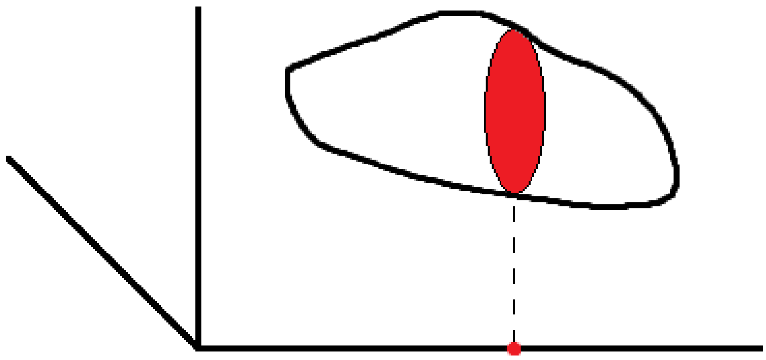
$f^{-1}(y) \coloneqq \{x \in X | f(x) = y\}$ – **полный прообраз точки**

$f^{-1}(Z) \coloneqq \{x \in X | f(x) \in Z\}$ – **полный прообраз множества**

$f^{-1}(g_1) \cap f^{-1}(g_2) = \emptyset$ при $g_1 \neq g_2$

$X = \coprod_{y \in Y} f^{-1}(y)$ - **дизъюнктное объединение** Y

В геометрии полный прообраз называется слоем:



Бинарные операции. Группы. Кольца. Поле

4 апреля 2018 г. 16:35

<u>Бинарные операции</u>

Бинарная операция на множестве X — функция $X * X \to X$
Операция обычно обозначается значком и пишется между операндами, т.е. $a * b$, а не $*(a, b)$

Свойства операции
1. Ассоциативность. $a * (b * c) = (a * b) * c$
2. Нейтральный элемент. $\exists e \in X, \forall x \in X\colon\ e * x = x * e = x$
3. Обратный элемент $\exists a' \in X\ \forall a \in X\colon a * a' = a' * a = \text{e}$
4. Коммутативность. $a * b = b * a$
5. Дистрибутивность (для множества с двумя операциями, например $\cdot$ $, +$)
   $a \cdot (b + c) = a \cdot b + a \cdot c$
   $(a + b) \cdot c = a \cdot c + b \cdot c$

Бинарные операции — Лист

Тип множества	1		2		3		4		5
Полугруппа	+								
Моноид	+		+						
Группа	+		+		+				
Коммутативная полугруппа	+						+		
Коммутативный моноид	+		+				+		
Абелева группа	+		+		+		+		
Операция	**+**	*****	**+**	*****	**+**	*****	**+**	*****	
Кольцо	+	+	+		+		+		+
Кольцо с единицей	+	+	+	+	+		+		+
Коммутативной кольцо	+	+	+		+		+	+	+
Коммутативное кольцо с единицей	+	+	+	+	+		+	+	+
Поле	+	+	+	+	+	+	+	+	+

(1) - **полугруппа**
(1) и (2) - **моноид**
(1), (2) и (3) - **группа**

Если X — моноид
- $\exists!\, e$.
  Пусть e, e' — нейтральные элементы
  $e * e' = e' = e$
- Если $a \in X\ \exists a'\colon a' * a = a' * a = e$, то a' обычно обозначается a^{-1} и называется **обратным** a, а a называется **обратимым**
  Если a', a'' — оба обратные a, то $a'' = ea'' = (a'a)a'' = a'(aa'') = a'e = a'$

Лемма
X — моноид. X^* — множество обратимых элементов моноида.
X^* — всегда группа относительно той же операции
Доказательство

$e * e = e \Rightarrow e \in X^* -$ есть нейтральный элемент
$a \in X^* \Rightarrow a^{-1} \in X^* \Rightarrow$ все элементы обратимы
Ассоциативность очевидным образом следует из того, что $X -$ моноид
Осталось только проверить, что $a, b \in X^* \rightarrow a * b \in X^*$
$(a * b) * (b^{-1} * a^{-1}) = a * e * a^{-1} = a * a^{-1} = e \Rightarrow$
$\Rightarrow (a * b)^{-1} = b^{-1} * a^{-1} \Rightarrow a * b \in X^*$■

(1) и (4) - **коммутативная полугруппа**
(1), (2) и (4) - **коммутативный моноид**
(1), (2), (3) и (4) - **абелева группа**

Если $R, +, *$: $(R, +)$ - абелева группа, $(R,*)$ - полугруппа и имеет место дистрибутивность, то $R -$ **кольцо**

Кольцо - **кольцо с единицей**, если $(R,*)$ - моноид, т.е. если есть нейтральный элемент по "умножению" (Обычно обозначается единицей, 1)

Если умножение коммутативно, то $R -$ **коммутативное кольцо**

Коммутативное кольцо с единицей - кольцо с единицей и коммутативное

Поле - коммутативное кольцо с единицей, в котором $R^* = \mathrm{R} \backslash \{0\}$ - множество обратимых элементов по умножению.

Циклические группы. Гомоморфизм. Перестановки

4 апреля 2018 г. 17:36

<u>Гомоморфизм групп</u>

$(G,*),(H,\#)$ — группы с разными операциями
$f: G \to H$ — **гомоморфизм**
$f(g_1 * g_2) = f(g_1)\#\, f(g_2)$
Инъективный гомоморфизм - **мономорфизм**
Сюръективный гомоморфизм - **эпиморфизм**
Биективный гомоморфизм - **изоморфизм**

Пример
Циклическая группа по умножению - $\{g^n | n \in \mathbb{Z}\}$
$g^n \coloneqq g * g * \cdots * g$ n раз.
$g^{-n} = (g^n)^{-1} = (g^{-1})^n$
Если $g^m \neq g^k$: $m \neq k$, то $g^m g^k = g^{m+k}$
Группа $\{g^n | n \in \mathbb{Z}\}$ с условием $g^m \neq g^k$ при $m \neq k$; $g^m g^k = g^{m+k}$ изоморфна группе целых чисел. Изоморфизм: $f(g^m) = m$.
$f\left(g^m * g^k\right) = f\left(g^{m+k}\right) = m + k = f(g^m) + f(g^k)$
Если $m = k$, то $g^m = g^k \Rightarrow g^{m-k} = g^0 = e$ — нейтральный элемент

Возьмем наименьшее $p \in \mathbb{N}$: $g^p = e$
$\{g^n | n \in \mathbb{Z}\} = \{e, g, \dots, g^{p-1}\} = C_p$
$g^{-1} = g^{p-1}$
$g^m = g^{pq+n} = (g^p)^q * g^n = e^q * g^n = g^n$
Значит, любой элемент группы представляется как $g^n, n \in [0, p]$. Такая подгруппа называется **циклической**
$g^u * g^v = g^{(u+v) mod\ p}$

$\mathbb{Z}_p = \{0, \dots, p-1\}$; $u +_p v \stackrel{\text{def}}{=} (u+v)\ mod\ p$
$\left(\mathbb{Z}_p, +_p\right)$ — группа, изоморфная C_p. Обозначается $\mathbb{Z}_\mathrm{p} \cong C_p$.
Изоморфизм $f(g^m) = m$

Свойства гомоморфизма
$f: G \to H$ — гомоморфизм

1. $f(e_G) = e_H$
   $f(e_G) = f(e_G * e_G) = f(e_G)\ \#\ f(e_G)$
   $e_H = f(e_G)$■
2. $f(g^{-1}) = f(g)^{-1}$
   $f(g^{-1})f(g) = f(g^{-1}g) = f(e) = e \Rightarrow f(g^{-1}) = f(g)$■

Ядро гомоморфизма
$\ker f = \{g \in G | f(g) = e\}$ - т.е. полный прообраз нейтрального элемента

Образ
$Im\, f = \{f(g) | g \in G\}$

Лемма
$f(x) = y$
Тогда $f^{-1}(y) = x * \ker f = \{xy | y \in \ker f\}$
$y \in \ker f \Rightarrow f(xy) = f(x)f(y) = ye = y$
Если $z \in f^{-1}(y)$, т.е. $f(z) = y$
$f(x^{-1}z) = f(x)^{-1} * f(z) = y^{-1}y = e$
$x^{-1}z \in \ker f \Rightarrow z = x(x^{-1}z) \in x * \ker f$ ■

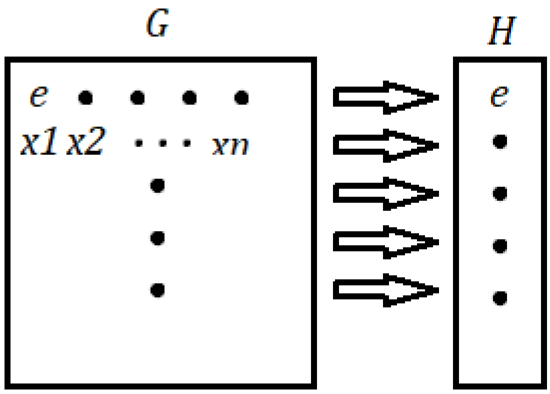
Лемма. Ядро замкнуто относительно умножения
$x, y \in \ker f \Rightarrow x^{-1}, xy \in \ker f$
$f(x, y) = f(x)f(y) = ee = e$
$f(x)^{-1} = f(x)^{-1} = e^{-1} = e$■

Определение
$X \subseteq G$. X – **подгруппа** $(X \leq G)$, если $\forall x, y \in X$: $xy \in X, x^{-1} \in X$
Или $X * X \leq X; X^{-1} \leq X$

Лемма. $X \leq G \Rightarrow X$ является подгруппой относительно той же операции
$X * X \to X$ по определению
Ассоциативность X следует из ассоциативности G.
$x \in X \Rightarrow x^{-1} \in X, xx^{-1} \in X, xx^{-1} = e \in X$■

Лемма. Ядро гомоморфизма является подгруппой.
$f^{-1}(y) = x * \ker F$
$m_x: \ker F \to x * \ker F$ – биекция
$m_x(y) = xy$
$m_x(y) = m_x(h) \Rightarrow xy = xh \Rightarrow y = h$

Лемма. $x * \ker F = \ker F * x$
$\forall y \in \ker F : \exists y' \in \ker F$
$xy = y'x$ и наоборот.
Возьмем $y' = xyx^{-1}$.
$f(y') = f(x)f(y)f(x^{-1}) = e \Rightarrow y' \in \ker F$
Наоборот аналогично■



Пример

$g \in G$

Подгруппа - непустое подмножество H группы G, в котором $ab, a^{-1}, b^{-1} \in H\ \forall a, b \in H$

$< g > = \{g^n | n \in \mathbb{Z}\}$ – **циклическая подгруппа, порожденная** g

В группе $(\mathbb{Z}, +)$: $< 2 > = \{2n | n \in \mathbb{Z}\}$

$< 2 > \cong \mathbb{Z}$

Теорема. Любая циклическая группа изоморфна бесконечной аддитивной группе, если её образующий - элемент бесконечного порядка, и конечной аддитивной группе, если образующий - элемент конечного порядка.

Теорема. Любая ненулевая подгруппа в $\mathbb{Z}$ изоморфна $\mathbb{Z}$

$\{e\}$ – всегда подгруппа.

H – подгруппа $\mathbb{Z}$, $H \neq 0$

Пусть g – наименьший положительный элемент H

$h \in H$

$h = gn + r; 0 \leq r < g$

$gn \in H \Rightarrow r \in H$

Так как g – наименьшей положительный, то $r = 0$. Значит, $H = < g > \cong \mathbb{Z}$

Теорема. Любая подгруппа циклической группы циклическая.

$p: \mathbb{Z} \to \mathbb{Z}_n$ – гомоморфизм

$p(x) = x\, mod\, n$

$p(x + y) = (x + y)\, mod\, n = (x\, mod\, n + y\, mod\, n)\, mod\, n$

$\ker p = < x >$

$p^{-1}(k) = \{k + nz | z \in \mathbb{Z}\} = k + n\mathbb{Z}$

<u>Перестановки</u>

X – множество

S_X – множество биективных функций $X \to X$ с операцией композиии.

Композиция всегда ассоциативна

$ind_x: X \to X$

$ind_x(a) = a_i; \forall a \in X$
Обратный элемент существует, так как функции биективны.
S_n — **симметрическая группа**
Элементы этой группы, т.е. биекции $X \to X$ называются **перестановками**
Запись перестановки:
$\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$
Инверсия перестановки - такая пара индексов i, j, что
$1 \le i \le j \le n \Rightarrow \sigma(i) > \sigma(j)$
Чётность перестановки - количество инверсий
Знакопеременная группа - подгруппа симметрической группы, содержащая только чётные перестановки

Циклическая запись перестановки
$\sigma: (i_1 \dots i_k) \to (i_1 \dots i_k)$
$\sigma(i_1) = i_2; \sigma(i_2) = i_3; \dots; \sigma(i_k) = i_1$
$(i_1 \dots i_k)$ — циклическая запись

Пример
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix}$
$(1\ 2\ 4)(3)(5\ 6)$ — циклическая запись
Получается так: $\sigma(1) = 2; \sigma(2) = 4; \sigma(4) = 1$, т.е. $1 \to 2 \to 4 \to 1$. Это записывается как $(1\ 2\ 4)$. 3 переходит только в себя, поэтому записывается как (3)

Композиция перестановок - применение двух перестановок подряд

$$\begin{pmatrix} 1 & 2 & 3 \\ \boxed{2} & \boxed{1} & \boxed{3} \end{pmatrix} \circ \begin{pmatrix} \boxed{1} & \boxed{2} & \boxed{3} \\ 1 & 3 & 2 \end{pmatrix}$$

Транспозиция - перестановка двух элементов.
Теорема. Любая перестановка записывается в виде произведения транспозиций соседних индексов.
Доказательство.
Индукция по числу инверсий. Для 2 - очевидно.
Если $\sigma \neq e$, то $\exists i: \sigma(i) > \sigma(i+1)$. Тогда в перестановке $\sigma \circ (i\ i+1)$ инверсий на одну меньше, чем в σ.

Теорема. Если перестановка представлена в виде произведения m транспозиций соседних индексов, её четность равна m

Доказательство
Если $\exists i: \sigma(i) > \sigma(i+1)$, то в $\sigma \circ (i\ i+1)$ инверсий на 1 меньше, иначе - на 1 больше.

Произведение групп

5 апреля 2018 г. 19:00

$M_n(R)$ - множество матриц $n \times n$ с элементами из кольца R
$GL_n(R) -$ **General Linear Group** - **полная линейная группа** - множество обратимых матриц $n \times n$ с элементами из кольца R
$GL_n(R) = \{A \in M_n(R) | \exists A^{-1}\}$
$R -$ коммутативное кольцо $\Rightarrow A \in GL_n(R) \Leftrightarrow \det A \in R^*$
$R^* -$ множество обратимых элементов кольца R
$SL_n(R) = \{A \in M_n(R) | \det A = 1\}$ $-$ **Special Linear Group**

Декартово произведение групп
$(G,*), (H,\#) -$ группы
$G \times H = \{(g,h) | g \in G, h \in H\}$ - **декартово произведение**
$(g_1,h_1) \cdot (g_2,h_2) = (g_1 * g_2, h_1 \# h_2)$
$e_{G\times H} = (e_G, e_H) -$ нейтральный элемент
$G \to G \times H$
$g \mapsto (g, e_H)$ - гомоморфизм - **Injection**
$h \mapsto (e_G, h)$
Любой элемент декартового произведения записывается в виде произведения образов единственным способом:
$(g,h) = (g,e_H) \cdot (e_G,h) = (e_G,h) \cdot (g,e_H)$

Пусть $X, Y \leq Z -$ т.е. X, Y - подгруппы Z. Если верно следующее:
1) $\forall z \in Z: \exists!\, x \in X, \exists!\, y \in Y: z = xy$
2) $xy = yx\ \forall x \in X, y \in Y$

То $Z -$ **прямое произведение** X на Y

Предположение. Если выполнены условия 1 и 2, то $Z \cong X \times Y$
Доказательство: $\varphi: X \times Y \to Z$
Отображение можно задать так: $\varphi(x,y) = xy$. Из условия 2 верно:
$\varphi\big((x_1,y_1)\cdot(x_2,y_2)\big) = \varphi(x_1x_2, y_1y_2) = x_1x_2y_1y_2 = x_1y_1x_2y_2$
$= \varphi(x_1,y_1)\varphi(x_2,y_2)$
Из условия 1: $\forall z \in Z: \exists!\, x, y$.
$z = xy = \varphi(x,y) -$ прообраз $\Rightarrow$ гомоморфизм сюръективен.
Так как $\exists!\, x, y$, то $\varphi(x_1,y_1) = \varphi(x_2,y_2) \to (x_1,y_1) = (x_2,y_2) \to x_1 = x_2, y_1 = y_2 \Rightarrow$ это изоморфизм ■

Вместо единственности можно написать $X \cap Y = \{e\}$

$p, q \in \mathbb{Z}; \gcd(p,q) = 1 - p, q$ **взаимно просты**
$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$
$f: \mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$

$f(k) = (k \, mod \, p, k \, mod \, q)$

$f(k) = (0,0) \Rightarrow \begin{matrix} k \vdots p \\ k \vdots q \end{matrix} \Rightarrow k \vdots pq$

Так как p, q - взаимно просты $k = 0 \Rightarrow \ker f = \{0\} \Rightarrow f -$ инъективна ■

В $\mathbb{Z}_{pq}$ рассмотрим подгруппу, порожденную $p - < p > = \{np \mid 0 \le n \le q\}$

Так как в $< p >$ q элементов, то $< p > \cong \mathbb{Z}_q$

Аналогично $< q > \cong \mathbb{Z}_p$

$\forall k \in \mathbb{Z}_{pq} \; \exists x, y : px = qy = k$

$px = qy \Rightarrow x \vdots q \Rightarrow px \vdots pq \Rightarrow px = 0 \; в \; \mathbb{Z}_{pq}$

S_3 - симметрическая группа

$X =< (1,2) >= \{e, (1\ 2)\}$

$Y =< (123) >= \{e, (1\ 2\ 3), (1\ 3\ 2)\}$

В X и Y верны условия 1 и 3:

3 - $X \cap Y = \{e\}$;

1 - $\forall \sigma \in S_3 : \exists \sigma_1 \in X, \sigma_2 \in Y : \sigma = \sigma_1 \sigma_2$

$S_3 \leftarrow X \times Y -$ биекция

$(x_1, y_1)(x_2, y_2)$

$x_1 y_1 x_2 y_2 = x_1 x_2 x_2^{-1} y_1 x_2 y_2;$

$x_1 x_2 \in X; x_2^{-1} y_1 x_2 \in Y$

$(x_1, y_1)(x_2, y_2) := (x_1 x_2)(x_2^{-1} y_1 x_2 y_2)$

- **Полупрямое произведение**

xH **—левый смежный класс**

	$e \; h_1 \dots h_n$	H
x_1	$x_1 \; x_1 h_1 \dots x_1 h_n$	$x_1 H$
x_2	$x_2 \; x_2 h_1 \dots x_2 h_n$	$x_2 H$
…	…	
x_{n-1}		$x_{n-1} H$

$$G = \coprod_{i=0}^{m-1} x_i H$$

$|x_i H| = |H|$

В первой строчке все элементы разные. Домножение в группе - обратимая операция, поэтому во всех остальных группах все элементы тоже разные.

$G -$ **индекс** H в $G =$ количество смежных классов

Теорема Лагранжа

$|G| = |H| \cdot |G : H|$

Лемма 1. $|xH| = |H| \; \forall x \in G$

Доказательство
$f: H \to xH$
$f(h) = xh$
$f^{-1}(y) = x^{-1}y \Rightarrow f -$ биекция, значит $|xH| = |H|$, т.е. во множествах одинаково количество элементов ■.

Лемма 2. $xH \cap yH \neq \emptyset \Rightarrow xH = yH$
Доказательство (для правого смежного класса)
Положим $x \equiv^h y \overset{\text{def}}{=} xy^{-1} \in H$
1) $x \cdot x^{-1} = e \in H \Rightarrow x \equiv^h x$
2) $x \equiv^h y \Rightarrow xy^{-1} \in H \Rightarrow (xy^{-1}) = yx^1 \in H \Rightarrow y \equiv^h x$
3) $x \equiv^h y, y \equiv^h z \Rightarrow xy^{-1} \in H, yz^{-1} \in H \Rightarrow xy^{-1}yz^{-1} \in H \Rightarrow$ $xz^{-1} \in H \Rightarrow x \equiv^h z$

Значит, это отношение эквивалентности
$[x]_{\equiv^h} = \{y \in G \mid y \equiv^h x\} = \{y \in G \mid yx^{-1} \in H\} = \{y \in G \mid y \in H_x\} = H_x$
Таким образом, правые смежные классы - классы эквивалентности.
Поэтому
$$G = \coprod_{i \in I} Hx_i$$
Доказательство для левых смежных классов аналогично
$x \equiv_h y \overset{\text{def}}{=} y^{-1}x \in H$■

Пусть $G = \mathbb{Z}; H = 2\mathbb{Z}$
$|G:H| = 2$

Следствия.
1) $|\mathrm{G}| \vdots |H|$
2) $G =< y >\cong \mathbb{Z}_p$

Доказательство
$g \in G \backslash \{e\}$
$< g >\leq G \Rightarrow p \vdots | < g > | \geq z \Rightarrow< g >= p \Rightarrow< g >= G$

Теорема *(Без доказательства)*
Если m делит $|G|$, то не обязательно существует подгруппа в G порядка m.

Теорема Силова
Пусть $p -$ простое, n наибольшее, удовлетворяющее
$|G| \vdots p^n$
1) $\exists$ подгруппа $H \leq G, |H| = p^n$
2) $\forall S \leq G, |S| = p^n$ $\exists$ Силовская p —подгруппа H, которая содержит S

Факторгруппы. Теорема о гомоморфизме

5 апреля 2018 г. 20:18

$gH = \{gh \mid h \in H\}$ − **смежный класс**

$H \leq G$. H − **нормальная подгруппа**, если верно одно из условий:

1) $g^{-1}Hg \subseteq H \ \forall g \in G \to H \subseteq gHg^{-1}$
2) $g^{-1}Hg = H$
3) $Hg = gH$ − правые и левые смежные классы совпадают
4) $g^{-1}hg \in H \ \forall h \in H, g \in G$

Условия 1 - 4 эквивалентны. Записывается так: $H \trianglelefteq G$

<u>Факторгруппа</u>

Хотим построить сюръективный гомоморфизм $\varphi: G \to F$, такой, что
$\ker \varphi = H$
$H \quad e, \ \ eh_1, \ \ eh_2, \ \ldots \to e$ - ядро
$g_1H \quad g_1, g_1h_1, g_1h_2, \ldots \to (\cdot)$
...
$g_iH \quad g_i, g_ih_1, g_ih_2, \ldots \to (\cdot)$
$\varphi(g_1h) = \varphi(g_1)\varphi(h) = \varphi(g_1)$

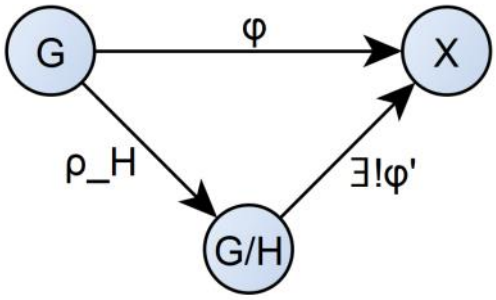
Возьмем в качестве группы F множество, состоящее из смежных классов
$F \coloneqq \{gH \mid g \in G\}$
Возьмем $\varphi(g) = gH$
$(g_1H) \cdot (g_2H) \coloneqq g_1g_2H$
$x_1H = g_1H; x_2H = g_2H$
$(x_1H) \cdot (x_2H) = x_1x_2H$
Вопрос в том, является ли g_1g_2H и x_1x_2H одним и тем же смежным классом
$x_1h_1 = g_1; \ h_1 \in H$
$x_2h_2 = g_2; h_2 \in H$
$g_1g_2H = x_1h_1x_2h_2H = x_1x_2x_2^{-1}h_1x_2h_2H$
$x_2^{-1}h_1x_2 \in H; \ x_2^{-1}h_1x_2h_2 \in H; \ x_2^{-1}h_1x_2h_2H \Rightarrow g_1g_2H \subseteq x_1x_2H$
Осталось показать, что φ − гомоморфизм
$\varphi(g) = gH$
$\varphi(g_1g_2) = (g_1g_2)H = (g_1H)(g_2H) = \varphi(g_1g_2)$. Очевидно, что гоморофизм сюръективен.

F называется **факторгруппой** G по H и обозначается G/H.
$\rho_H : G \to G/H$
$\rho_H(g) = gH = Hg$

Универсальное свойство факторгруппы

$\forall \varphi: G \to X, \ker \varphi \supseteq H$

$\exists \varphi' \colon \mathrm{G/H} \to X$



Т.е. $\varphi' \circ \rho_H = \varphi$.

Доказательство. Построим φ'

$\varphi'(gH) \coloneqq \varphi(g)$

$xH = gH \leftarrow x = gh; h \in H$. Вопрос в том, верно ли следующее: $\varphi'(gH) = \varphi'(xH)$

$\varphi(x) = \varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)e$

$\varphi'(g_1H \cdot g_2H) = \varphi'(g_1g_2H) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \varphi'(g_1H)\varphi'(g_2H)$

Пример

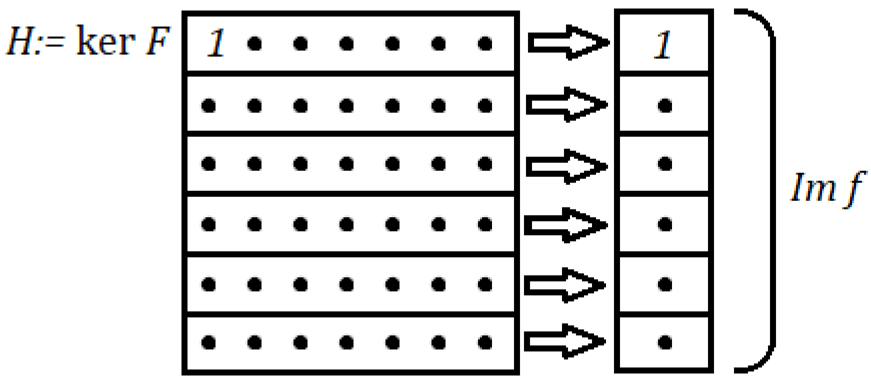
$\mathbb{Z}/\mathrm{n}\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$

$(k + n\mathbb{Z}) + (m + n\mathbb{Z}) = k + m + n\mathbb{Z} = (k + m) \bmod n + n\mathbb{Z}$

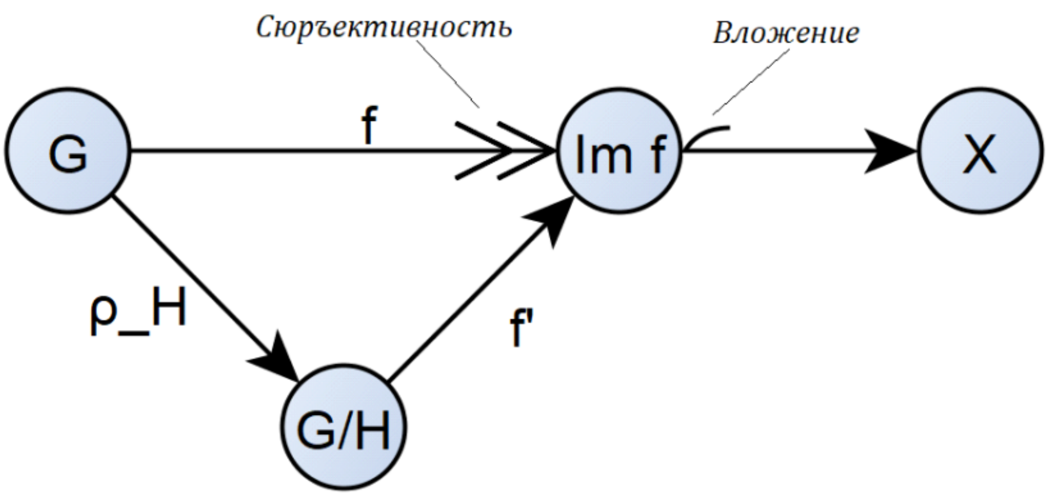
<u>**Теорема о гомоморфизме**</u>

$F \colon G \to X$

$Im\, F \cong \mathrm{G}/\ker F$



Доказательство



$\forall x \in Im\, f \colon \exists g \in G \colon f(g) = x; f'(gH) = x \Rightarrow f$ – сюръективен

$$
\begin{array}{ccc}
f'(g_1H) & = & f'(g_2H) \\
\parallel & & \parallel \\
f(g_1) & = & f(g_2)
\end{array}
$$
$f(g_1)f(g_2) = e$

$g(g_1g_2^{-1}) = e$

$g_1g_2^{-1} \subseteq \ker F = H \Leftrightarrow g_1 \in g_2G \Leftrightarrow g_1H = g_2H -$ инъективность.■

Пусть стоит задача доказать, что G/H≅F

$\varphi: G \to F; \ker\varphi = H$

Пример

$\mathbb{Z}/\mathrm{ab}\mathbb{Z} \cong \mathbb{Z}_A \times \mathbb{Z}_b; \gcd(a, b) = 1$

$\varphi: \mathbb{Z} \to \mathbb{Z}_A \times \mathbb{Z}_b$

$\varphi(n) = (n\ mod\ a, n\ mod\ b)$

Из того, что $(m\ mod\ a + n\ mod\ a) mod\ a = (m + n)\ mod\ a$ и из определения декартового произведения групп верно следующее:

$\varphi(m) + \varphi(n) = (m\ mod\ a, m\ mod\ b) + (n\ mod\ a, n\ mod\ b)$

$= \big((m + n)\ mod\ a, (m + n) mod\ b\big) = \ \varphi(m + n)$

Значит, $\varphi(m) -$ гомоморфизм

Полупрямое произведение

6 апреля 2018 г. 20:43

Полупрямое произведение

$G/N = \{hN | h \in H\}$

H — множество представителей смежных классов

$h_1N \cdot h_2N = (h_1h_2N \cap H)$

Пример

$\mathbb{Z}/\mathbb{Z}_n$

$x + n\mathbb{Z}; x \in \{0, \dots, n-1\}$

$(x_1 + x_2) = (x_1 + x_2) \; mod \; n$

Если H — подгруппа, $G/N \cong H$;

$H \hookrightarrow G \twoheadrightarrow H$

Где $\hookrightarrow$ - **вложение**, $\twoheadrightarrow$ - **проектирование**

$\{h\} = gN \cap h$

$G = H \ltimes N$ — **полупрямое произведение**

Предположение. $G = H \ltimes N$, тогда и только тогда, когда:

Эквивалентные условия:

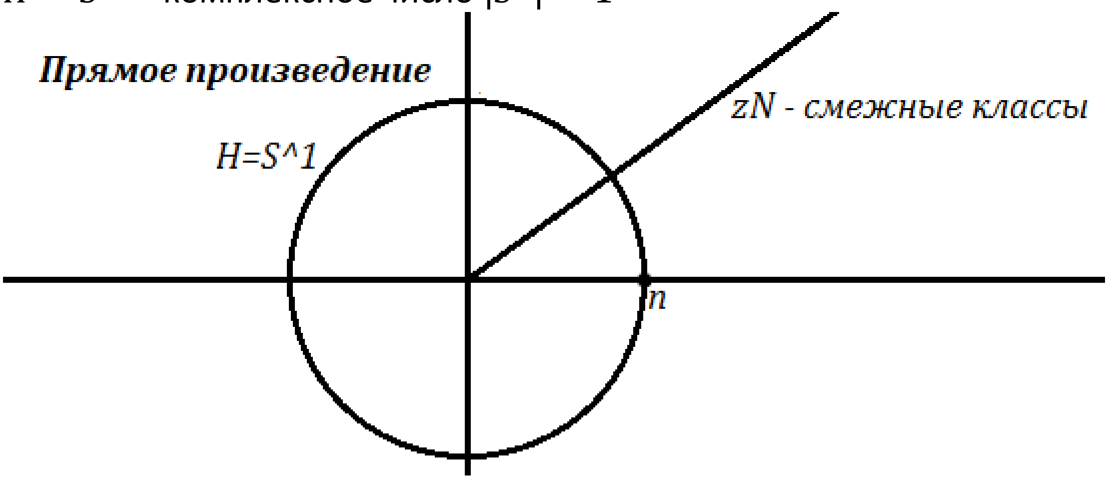
1) $G = H \cdot N$ — любой элемент в G однозначно проектируется в $h \cdot n; h \in H, n \in N$
2) $H \cap N = \{e\}$
3) $N \trianglelefteq G$

Пример

$G = \mathbb{C}^*$

$N = \mathbb{R}^*_{>0}$

$H = S^1$ — комплексное число $|S^1| = 1$



$\{h\} = H \cap z \cdot \mathbb{R}^*_{>0}$

$C^* = R^*_{>0} \times S^1$ — комлексное пространство есть прямое произведение пространства.

$z \cdot S^1 \cap \mathbb{R}^*_{>0} = \{n\}$

Кстати, отсюда значок "\":
$C^*/\mathrm{S}^1 = (\mathbb{R}^*_{>0} \times S^1)/\mathrm{S}^1 = R^*_{>0}$
$\mathbb{R}^*_{>0} \hookrightarrow \mathbb{C}^* \twoheadrightarrow R^*_{>0}$
Проектирование: $z \to |z|$
$S^1 \hookrightarrow \mathbb{C}^* \twoheadrightarrow R^*_{>0}$
$S^1 \hookrightarrow \mathbb{C}^* \twoheadrightarrow S^1\ (?)$
Проектирование $\mathbb{C}^* \to \mathrm{S}^1\ z \to \frac{z}{|z|}$
$\varphi(z) \subseteq S^1$

Действия группы на множестве

Saturday, May 12, 2018 18:55

Действия группы на множестве

G — группа, X — множество.
$G \curvearrowright X$ - G **действует** на X,
если задана функция $G \times X \to X$
$(g, x) \mapsto gx$
И выполнены следующие свойства
1) $g_1(g_2x) = (g_1g_2)x$
2) $1x = x$

Примеры:
1) $N \lhd G$
   $G \curvearrowright N$ - действия сопряжениями
   $(g, n) \mapsto {}^g n \coloneqq gng^{-1}$ - n в левой степени g
   - ${}^{(g_1g_2)}n = {}^{g_1}({}^{g_2}n)$
   - ${}^1 n = n$
2) $S_n \curvearrowright \{1, \dots, n\}$
   $(\sigma, k) \mapsto \sigma(k)$

3) $GL_n(F) \curvearrowright F^n$ — векторное пространство
   $(\mathrm{A}, \mathrm{x}) \mapsto \mathrm{Ax}$

X - множество.
$S_X \curvearrowright X$.
S_X — множество всех биекций из X в X (для конечного множества X - перестановки на множестве).
Если $G \curvearrowright X$, то определен гомоморфизм:
$\Theta: G \to S_x$
$g \mapsto \Theta_g$
$\Theta_g(x) = gx$
$\Theta_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = g_1\left(\theta_{g_2}(x)\right) = \Theta_{g_1}\left(\theta_{g_2}(x)\right)$
$= \theta_{g_1} \circ \theta_{g_2}(x)$
Обратно, если есть гомоморфизм
$\Theta: G \to S_x$
$g \mapsto \Theta_g$,
то можно задать действие $G \curvearrowright X$ по правому $gx = \Theta_g(x)$

$G \curvearrowright X, x \in X, g \in G$:
$\mathrm{St}(\mathrm{g}) = \{g \in G | gx = x\}$ - **стабилизатор**
$g \in G$: $Fix(g) = \{x \in X | gx = x\}$ - **фиксатор** - множество тех точек, которые остаются на месте

$Gx = \{gx | g \in G\} -$ **орбита** элемента x под действием G.

Лемма. Длина орбиты элемента - индекс стабилизатора этого элемента
Доказательство
Индекс подгруппы - количество смежных классов по этой подгруппе.
Зададим функцию
$f: G/St(x) \to Gx$
$f\big(gSt(x)\big) \coloneqq gx$
Сюръективность следует из определения орбиты. Нужно доказать биективность. Пусть $\exists g, h: f\big(gSt(x)\big) = f\big(hSt(x)\big) \Rightarrow gx = hx$
$\Rightarrow h^{-1}gx = x \Rightarrow h^1 g \in St(x) \Rightarrow gSt(x) = hSt(x)$
Значит, f биективно отображает $G/St(x) \to Gx$, а это возможно, только если $|G/St(x)| \to |Gx|$ ■

Действие называется **точным**, если гомоморфизм инъективен
Действие такое, если $\forall g \in G\backslash\{e\}: \exists x \in X: gx \neq x$

Действие называется **свободным**, если $\forall g \in G\backslash\{e\}\ \forall x \in X: gx \neq x$

Лемма Бернсайда
Количество орбит действия группы G на множестве X равно
$$\frac{1}{|G|}\sum_{g\in G} |Fix(g)|$$
Доказательство
$N -$ число орбит. Каждый элемент лежит в орбите Gx, сопоставим ему число $\frac{1}{|Gx|}$. Тогда очевидно, что $N = \sum_{x\in X} \frac{1}{|Gx|}$. По лемме о длине орбиты
$$N = \sum_{x\in X} \frac{1}{|Gx|} = \sum_{x\in X} \frac{|St(x)|}{|G|} = \frac{1}{|G|}\sum_{x\in X} |St(x)|$$
Очевидно, что это же число - количество пар $(g, x) \in G \times X$ - можно посчитать и как $\frac{1}{|G|}\sum_{g\in G}|Fix(x)|$ ■

Кольца

Saturday, May 19, 2018 17:42

Гомоморфизм колец. Идеалы

Saturday, May 19, 2018 17:43

Кольца

Все рассматриваемые далее кольца - коммутативные кольца с единицей.
$\mathbb{Z}$ − кольцо целых чисел
$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ − **гауссовы целые числа**
$F[t]$ − кольцо многочленов над полем F
$\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} | a, b \in \mathbb{Z}\}$

Прямая сумма колец

Кольцо $R = A \oplus B$ − сумма колец A, B, если:
$\forall a_1, a_2 \in A, \forall b_1, b_2 \in B$:
$R = A \times B; (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$
$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$

Гомоморфизм колец

$\varphi: R \to A$ − называется **гомоморфизмом колец** с единицей, если
$\forall r, s \in R$
$\varphi(\mathrm{r} + \mathrm{s}) = \varphi(\mathrm{r}) + \varphi(\mathrm{s})$
$\varphi(r \cdot s) = \varphi(r)\varphi(s)$
$\varphi(1) = 1$

Пример (нет)
$\psi: \mathbb{Z} \to \mathbb{Z}_6$
$\psi(x) = 4x \ mod\ 6$
$\psi(x + y) = 4(x + y)\ mod\ 6 = (4x + 4y)\ mod\ 6 = 4x\ mod\ 6 + 4y\ mod\ 6$
$= \psi(x) + \psi(y)$
$\psi(xy) = 4xy\ mod\ 6 = (4x \cdot 4y) mod\ 6 = \psi(x)\psi(y)$
$\psi(1) = 4 \neq 1 \Rightarrow$ не гомоморфизм

$\mathrm{Ker}\, \varphi = \{r \in R | \varphi(r) = 0\}$ − **ядро гоморфизма колец**
$Im\ \varphi = \{\varphi(r) | r \in R\}$ − **образ**

Идеал

Подмножество I кольца R называется **идеалом**, если
$\forall a, b \in I, r \in R\colon\ (a + b) \in I, ar \in I; -a \in I$
Это аналог нормальной подгруппы в теории групп.
$x \in R; xR = \{xr | r \in R\}$ − **главный идеал** - идеал, порожденный одним элементом

Примеры
$R = F[x, y]: xR + yR = \{xp_1 + yp_2 | p1, p_2 \in R\} = \{p \in R | p(0,0) = 0\}$ − идеал

$R = \mathbb{Z}[\sqrt{5}]$
$(\sqrt{5}+1)(\sqrt{5}-1) = 2 \cdot 2$
$(\sqrt{5}+1)R + 2R -$ не главный идеал

Кольцо главных идеалов - кольцо, в котором все идеалы главные.

Теорема. $\varphi: R \to A; \ker\varphi -$ идеал в R
Доказательство. $\ker\varphi -$ подгруппа в аддитивной группе кольца R.
$a \in \ker\varphi, r \in R. \varphi(ar) = \varphi(a)\varphi(r) = 0\varphi(r) = 0 \Rightarrow ar \in \ker\varphi$ ■

<u>Факторкольцо</u>
Пусть $I -$ идеал.
$\mathrm{R/I} = \{a + I | a \in R\} -$ факторгруппа. Из этого следует, что
$(a+I) + (b+I) = (a+b) + I$
Пусть $(a+I)(b+I) \coloneqq ab + I$
$a' \in a + I; b' \in b + I, \begin{matrix} a' = a + i_1 \\ b' = b + i - 2 \end{matrix}, i_1, i_2 \in I$
$a'b' = (a+i_1)(b+i_2) = ab + i_1 b + i_2 a + i_1 i_2 \in ab + I \Rightarrow$
$\Rightarrow a'b' + I = ab + I -$ смежные классы пересекаются и $\mathrm{R/I} -$ **факторкольцо**

$I = 0 + I -$ нейтральный элемент факторкольца по сложению
$I = 1 + I -$ нейтральный элемент факторкольца по умножению

<u>Теорема о гомоморфизме колец</u>
$\varphi: R \to A -$ гомоморфизм колец. Тогда
$\mathrm{R/\ker\varphi} \cong Im\ \varphi$ - изоморфизм колец.

$\varphi: R \to A$
$\alpha: \mathrm{R}/\ker\mathrm{\varphi} \cong Im\ \varphi$
Нужно доказать, что это - изоморфизм колец.
$\alpha(r + \ker\varphi) \coloneqq \varphi(r)$
$\alpha(r' + \ker\varphi) = \varphi(r') = \varphi(r+k) = \varphi(r) + \varphi(k) = \varphi(r)$
$\alpha\big((r + \ker\varphi)(s + ker\varphi)\big) = \alpha(sr + \ker\varphi) = \varphi(rs)$
$\alpha(r + \ker\varphi) \cdot \alpha(s + \ker\varphi) = \varphi(r)\varphi(s) \Rightarrow \varphi(r)\varphi(s) = \varphi(rs)$

Примеры
$\varphi: \mathbb{Z} \to \mathbb{Z}_n$
$\varphi(x) \coloneqq x\ mod\ n$
$\ker\varphi = n\mathbb{Z}$
$\mathbb{Z}/\mathrm{n}\mathbb{Z} \cong \mathbb{Z}_n$

$\varepsilon: \mathbb{R}[t] \to \mathbb{C}$
$\varepsilon(p) \coloneqq p(i)$
$\ker\varepsilon : \varepsilon(p) = 0 \Leftrightarrow p(i) = 0 \Rightarrow p(-i) = 0 \Leftrightarrow$

$\Leftrightarrow p \vdots (x-i); p \vdots (x+i) \Rightarrow p \vdots (x-i)(x+i) \Rightarrow p \vdots x^2+1$
$p(x) = (x^2+1)g(x) \Rightarrow p(i) = 0 \Leftrightarrow p \in \ker \varepsilon$
$\mathbb{C} \cong \mathbb{R}[t]/(t^2+1)\mathbb{R}[t]$

Китайская теорема об остатках

Saturday, May 19, 2018 18:52

Китайская теорема об остатках для целых чисел

$\mathbb{Z}/\mathrm{ab}\mathbb{Z} \cong \mathbb{Z}/\mathrm{a}\mathbb{Z}\times\mathbb{Z}/\mathrm{b}\mathbb{Z}$, если $a, b -$ взаимно просты
$R, A -$ кольца
$R \times A = \{(r, a) | r \in R, a \in A\}$
$(r_1, a_1)+.(r_2, a_2) = (r_1+.r_2, a_1+.a_2)$

$\varphi\colon \mathbb{Z} \to \mathbb{Z}/\mathrm{a}\mathbb{Z} \times \mathbb{Z}/\mathrm{b}\mathbb{Z}$
$\varphi(x) = (x + a\mathbb{Z}, x + b\mathbb{Z})$
$\ker\varphi : \varphi(x) = 0 = (a\mathbb{Z}, b\mathbb{Z}) \Leftrightarrow x \in a\mathbb{Z} \cap b\mathbb{Z} \Leftrightarrow x \in ab\mathbb{Z}$
$\exists c, d \in \mathbb{Z}$
$ac + bd = 1$
$\varphi(k \cdot bd + m \cdot ac) = (k + a\mathbb{Z}, m + b\mathbb{Z})$
$x + a\mathbb{Z} = kbd + a\mathbb{Z} = k - kac + a\mathbb{Z} = k + a\mathbb{Z}$
$x + b\mathbb{Z} = \cdots = m + b\mathbb{Z}$

Китайская теорема об остатках

Теорема
Если $I, J -$ идеал в R, то $I \cap J -$ идеал в R.
"Доказательство"
$a, b \in I \cap J$
$a + b \in I \cap J$
$na \in I \cap J$■

Наименьший идеал, содержащий I и J одновременно, называется
$I + J = \{a + b | a \in I, b \in J\}$

Пример
$6\mathbb{Z} \cap 9\mathbb{Z} = 18\mathbb{Z}; a\mathbb{R} \cap b\mathbb{R} = c\mathbb{R}; c = lcm\ (a, b)$
$18 = lcm(6,9)$
$\{ar + bg | r, g \in \mathbb{R}\} = d\mathbb{R}$
$d = \gcd(a, b)$

Произведение идеалов - идеал, порожденный элементами ab по всем $a \in A, b \in J$
$I \cdot J = \{\sum_{i=1}^{n} a_i b_i\ | n \in \mathbb{N}; a_i \in I; b_i \in J\}$

$I, J -$ **взаимно простые идеалы,** если их сумма - всё кольцо: $I + J = R$
Лемма. $I + J = R \Rightarrow I \cap J = IJ$
$IJ \subseteq I \cap J -$ очевидно
$x \in I \cap J$
$I + J = R \to \exists a \in I, b \in J: a + b = 1$

$x = xa + xb \in (I \cap J)I + (I \cap J)J \subseteq IJ$■

Лемма. Если $I -$ взаимно прост с каждым из $J_k, k = 1, \dots, n,$ то I взаимно прост с их произведением $J_1 \dots J_n$

Доказательство

Индукция по n

Для $n = 1$ очевидно.

$R = J + I_1 = J + I_1 R = J + I_1(J + I_2) = (J + I_1 J) + I_1 I_2 \subseteq J + I_1 I_2$. Дальше по индукции■

<u>**Китайская теорема об остатках**</u>

$I_1, \dots I_n -$ попарно взаимно простые идеалы

$\mathrm{R}/(\mathrm{I}_1 \cdot \ldots \cdot \mathrm{I}_\mathrm{n}) \cong R/I_1 \times \cdots \times R/I_n$

Доказательство

Для $n = 2$, дальше по индукции

$\mathrm{R}/I_1 I_2 \cong \mathrm{R}/I_1 \times \mathrm{R}/I_2$

$\varphi: R \to \mathrm{R}/I_1 \times \mathrm{R}/I_2$

$\varphi(x) = (x + I_1, x + I_2)$

$\varphi(x + y) = (x + y + I_1, x + y + I_2)$

$= \big((x + I_1) + (y + I_1), (y + I_2) + (x + I_2)\big) = \varphi(x) + \varphi(y)$

Аналогично $\varphi(xy) = \varphi(x)\varphi(y)$

$\varphi(x) = (I_1, I_2) \Leftrightarrow x \in \ker\varphi$

$(\mathrm{x} + \mathrm{I}_1, \mathrm{x} + \mathrm{I}_2) = (I_1, I_2) \Leftrightarrow x \in I_1 \cap I_2 = I_1 I_2 \Rightarrow \ker\varphi = I_1 I_2$

Осталось доказать сюръективность:

$a_1 \in I_1, a_2 \in I_2; a_1 + a_2 = 1$

$\forall (b_1 + I_1, b_2 + I_2) \in \mathrm{R}/I_1 \times \mathrm{R}/I_2$

$\varphi(b_1 a_2 + b_2 a_1) = (b_1 + I, b_2 + J) -$ прообраз■

Теорема

1) В любой области главных идеалов неприводимый элемент порождает простой идеал
2) В любой ОГИ $\neq 0$ любой простой идеал является максимальным
   $M -$ **максимальный**, если $M \subseteq I \Rightarrow I = R$
3) R/M - поле $\Leftrightarrow M -$ максимальный идеал

Евклидовы кольца. Простой идеал

Saturday, May 19, 2018 22:52

<u>**Евклидовы кольца**</u>

$R -$ коммутативное кольцо единицей.

Делители нуля - такие $a, b \in R, a, b \neq 0,$ что $ab = 0$

Область целостности - $ab = 0 \Rightarrow \begin{cases} a = 0 \\ b = 0 \end{cases}$

$\varphi: R \to \mathbb{N}_0 \cup \{\infty\}$ **- евклидова норма**:

1) $\forall r \neq 0: \varphi(0) < \varphi(r)$
2) $\forall a, b \neq 0, a, b \in R\ \exists c, r \in R: a = bc + r; \varphi(r) < \varphi(b)$
   Важно отметить, что однозначность разложения $a = bc + r$ не подразумевается

R - **евклидово кольцо** с евклидовой нормой φ

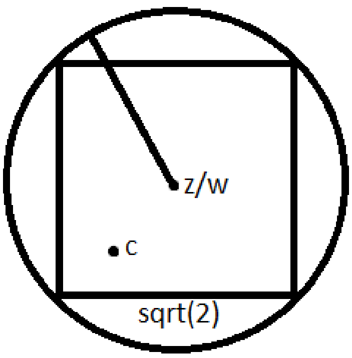
Примеры:

1) $\mathbb{Z}$, евклидова норма - $abs(r)$
2) $F[t]$, норма - $\deg(r)\ \ (\deg 0 = -\infty)$
3) $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$, норма - $abs^2(r)$

$z = w \cdot c + r \mid : w$

$|r| < |w|$

$\frac{z}{w} = c + \frac{r}{w}; \left|\frac{r}{w}\right| < 1$



В отрезке длиной $\sqrt{2}$ найдётся хотя бы одно вещественное или мнимое целое число.

$2 + 3i\ mod\ 1 + 2i$

$\frac{2 + 3i}{1 + 2i} = \frac{(2 + 3i)(1 - 2i)}{(1 + 2i)(1 - 2i)} = \frac{8 - i}{5} = 1 + \frac{3}{5} - \frac{1}{5}i$

$c = 1: 2 + 3i = (1 + 2i) \cdot 1 + (1 + i)$

$|1 + i|^2 < |2 + 3i|^2$

Теорема. Евклидово кольцо - область главных идеалов (любой идеал - главный)

Доказательство:
$R -$ евклидово кольцо, $I -$ идеал.
Выбираем в I элемент с наименьшей евклидовой нормой.
Пусть $\varphi(I\backslash\{0\}) = \{\varphi(a)|a \in I\backslash\{0\}\}$
$k -$ наименьший элемент множества:
$x \in I\backslash\{0\} : \varphi(x) = k\ (xR \subseteq I)$
$y \in I -$ любой элемент идеала
$y = xc + r$
$r = y - xc, \varphi(r) < \varphi(x) \Rightarrow r = 0$
$y = xc \Rightarrow y \in xR$ - любой элемент из идеала делится на x, т.е. $I \subseteq xR$. Так как $y \in I$, то верно и обратное включение

<u>Алгоритм Евклида</u>

Теорема о линейном представлении НОД
$R -$ ОГИ $\Rightarrow \forall \mathrm{a}, \mathrm{b} \in \mathrm{R}: \exists x, y \in R, ax + by = \gcd(a, b)$
Доказательство
$aR + bR -$ минимальный идеал, содержащий a, b - по условию главный.
$aR + bR = dR$, значит, $d = \gcd(a, b)$ по определению НОД ■

Лемма. $\forall a, b, c \in R: \gcd(a, b) = \gcd(a - bc, b)$
Доказательство
$a - bc, b \in aR + bR \Rightarrow (a - bc)R + bR \subseteq aR + bR$
$a = (a - bc) + bc \in (a - bc)R + bR \Rightarrow (a - bc)R + bR \supseteq R + bR$
$\Rightarrow (a - bc)R + bR = aR + bR \Rightarrow$ наименьший главный идеал, содержащий эти идалы, одинаковый ■

Алгоритм Евклида
Пусть $r_0 = a; r_1 = b; i = 1$.
1) $r_{i-1} = r_i g_i + r_{i+1} -$ деление с остатком
2) $r_{i+1} \neq 0 \Rightarrow i \coloneqq i + 1$, назад на 1-й шаг
3) $k \coloneqq i$: $r_{k+1} = 0 \Rightarrow \gcd(a, b) = r_k$

Обратный ход:
$\gcd(a, b) = r_k = r_{k-2}x_{k-2} + r_{k-1}y_{k-2}$, где
$x_{k-2} = 1, y_{k-2} = -q_{k-1}$
Подставляя в это $r_{k-1} = r_{k-3} - r_{k-2}q_{k-2}$, получаем $\gcd(a, b) = r_{k-2}x_{k-2} + (r_{k-3} - r_{k-2}q_{k-2})y_{k-2} = r_{k-3}x_{k-3} + r_{k-2}y_{k-3}$
...
$\gcd(a, b) = r_0x_0 + r_1y_0 = ax_0 + by_0$

<u>Неприводимые и ассоциированные элементы</u>
$R -$ коммутативное кольцо с единицей, $a, b \in R$. a **ассоциировано** с b, если $aR = bR -$ главные идеалы, порождённые ими, равны
$\exists r_1 \in R: a = br_1$
$\exists r_2 \in R: b = ar_2$
$a = ar_2r_1 \Rightarrow a \cdot (1 - r_1r_2) = 0$

(Если $a = 0 \Leftrightarrow aR = 0 \Leftrightarrow bR = 0 \Leftrightarrow b = 0$)
Если R — область целостности, то r_1, r_2 — обратимые

Лемма. Если R — область целостности, то верно следующее:
a ассоциировано с $b \Leftrightarrow a = b\varepsilon; \varepsilon \in R^*$ — множество, где $\exists \varepsilon^{-1}$

$a \in R$ называется **неприводимым**, если $a = bc \Rightarrow a$ асс. b или a асс. c.

Лемма. Если R — область целостности, то: a неприводим $\Leftrightarrow a$ не раскладывается на необратимые множители

<u>Простой идеал и элемент</u>
Идеал I — **простой**, если $bc \in I \Leftrightarrow b \in I$ или $c \in I$. Другими словами, это такой идеал кольца, факторкольцо по которому является областью целостности.
Элемент кольца называется **простым**, если идеал, им порождённый - простой.
Например, $n\mathbb{Z}$ — простой идеал, если n — простое число

Пример
$\mathbb{Z}\left[\sqrt{-3}\right] = \left\{a + b\sqrt{-3} | a, b \in \mathbb{Z}\right\}$
$\left(1 + \sqrt{-3}\right)\left(1 - \sqrt{-3}\right) = 4 = 2 \cdot 2$
Пусть $2 = zw; z, w \in \mathbb{Z}\left[\sqrt{-3}\right]$
$|2|^2 = |z|^2|w|^2$
$\left|a + b\sqrt{-3}\right| = a^2 + 3b^2 \in \mathbb{Z}$
$|2|^2 = |z|^2 \cdot |w|^2$

z^2	w^2
4	1
1	4
2	2

$|z|^2 = 1$
$z \cdot \bar{z} = 1 \Rightarrow z$ — обратим
$|z|^2 = 2$
$a^2 + 3b^2 = 2 \Rightarrow b = 0 \Rightarrow a = \pm\sqrt{2} \notin \mathbb{Z}$ - противоречие
2 не раскладывается на простые множители $\Rightarrow 2$ — неприводим
$\left(1 + \sqrt{-3}\right)\left(1 - \sqrt{3}\right) = u \in 2\mathbb{Z}\left[\sqrt{-3}\right]$
Т.е. произведение лежит в идеале, а сомножители - нет. Значит, 2 — не простой и неприводимый одновременно.

Лемма. Если элемент простой, то он неприводим в коммутативном кольце с единицей
$a \in R$

$a = bc; b, c, \in aR \Rightarrow b \in aR$ или $c \in aR$
Если $b \in aR \Rightarrow bR \subseteq aR$
$a = bc \in bR \Rightarrow aR \subseteq bR \Rightarrow aR = bR$■

Лемма. Если $R -$ ОГИ, то $a \in R -$ неприводимый $\Leftrightarrow a -$ простой
Пусть $bc \in aR$
$aR + bR = dR -$ идеал
$a = dr \Rightarrow$ т.к. $a -$ неприводим, то либо d, либо $r -$ обратим.
Если $d -$ обратим, то $dR -$ все кольцо
$dR = R$
$\exists x, y \in R: ax + by = 1$
$cax + cby = c \Rightarrow a \in aR$
Если $r -$ обратим, $a = dr \Rightarrow aR = dR \Rightarrow aR = aR + bR \Rightarrow bR \subseteq aR$■

<u>Разложение на простые множители</u>
Теорема. Если $R -$ ОГИ, $a = p_1 \dots p_n = q_1 \dots q_m$, где $p_i, q_i -$ простые множители.
Тогда
1) $m = n$
2) $\forall i$: $\exists \sigma \in S_n; p_i$ асс. $q_{\sigma(i)}$

Доказательство
Индукция по n $(m \leq n)$
Для $n = 1$ очевидно
$n > 1$
$a \,\vdots\, p_n \Rightarrow q_i \,\vdots\, p_n$
$q_i = p_n \cdot \alpha$
По определению, неприводимый элемент необратим. Значит, $q_i -$ тоже неприводим.
$\alpha -$ обратим и q_i асс. p_n
$\sigma(n) = i$
$p_1 \dots p_{n-1} = q_1 \dots q_{i-1} \cdot q_{i+1} \dots q_m = a$
По индукционному предположению $n - 1 = m - 1$ и существует биекция: $\sigma\{1, \dots, n-1\} \to \{1, \dots, i-1, i+1, m\}$, такая, что p_i асс. с $q_{\sigma(i)}$■

Макс., пр. идеал. Порядок, экспонента

Sunday, May 20, 2018 21:56

Связь максимального и простого идеала

Лемма 1. $M -$ максимальный идеал $\Leftrightarrow \mathrm{R/M} -$ поле

Лемма 2. $P -$ простой идеал $\Leftrightarrow \mathrm{R/P} -$ область целостности

Следствие. Любой максимальный идеал - простой.

Теорема. $R -$ ОГИ $\Rightarrow I \neq \{0\}$ - простой $\Leftrightarrow \mathrm{I} -$ максимальный

Доказательство 1

$r \in R/\mathrm{M}\ (r + M \neq 0 + M)$

$r + M -$ произвольный элемент $\mathrm{R/M}$

$r + M \in \mathrm{R/M}$

$M + rR$ в кольце R $\mathrm{M} \leq \mathrm{M} + rR$ (т.к. $M + rR,$ но $r \notin M$)

Так как $M -$ максимальный, то $M + rR = R \Rightarrow \exists m \in M, a \in R: m + r = 1$

$(r + M)(a + M) = ra + M = 1 = 1 - m + M = 1 + M -$ любой ненулевой элемент имеет обратный и $\mathrm{R/M} -$ поле ■

Доказательство 2

$$\begin{array}{ccc}
ab \in P & \Leftrightarrow & (a+P)(b+P) = 0 \\
\Updownarrow & & \Updownarrow \\
\left[\begin{array}{l} a \in P \\ b \in P \end{array}\right. & \Leftrightarrow & \left[\begin{array}{l} b + P = 0 + P \\ b + P = 0 + P \end{array}\right.
\end{array}$$

Доказательство теоремы

Пусть $I = \{0\} -$ простой идеал.

$I \subseteq M \subset R$; $\mathrm{M} -$ собственный идеал

$I = aR, M = mR,$ т.к. $R -$ ОГИ.

Если $m \in I$, то $mR \in I \Rightarrow M \leq I$

Если $m \notin I$, то

$\forall r \in R: \exists r': ar = mr' \in I \Leftrightarrow r' \in I \Leftrightarrow r' = ar''$

$ar = mar'' \Rightarrow r = mr'' \in M \Rightarrow M = R$■

Следствие - если $p \neq 0 -$ неприводимый элемент в ОГИ, $\mathrm{R/pR}$ - поле.

Доказательство

$p -$ неприводимый $\Rightarrow p -$ простой $\Rightarrow pR -$ простой идеал $\Rightarrow pR -$ максимальный $\Rightarrow \mathrm{R/pR} -$ поле ■

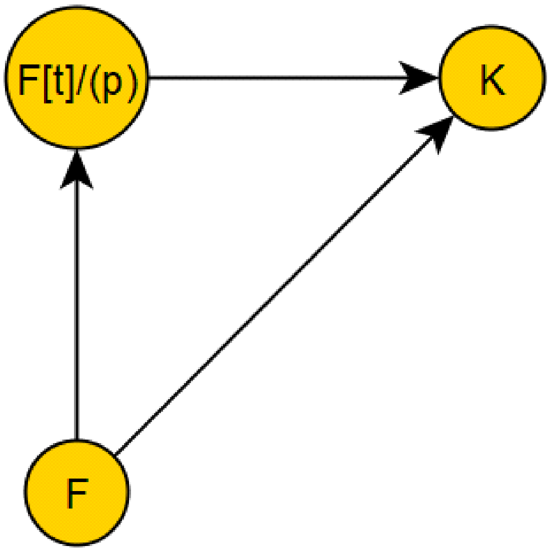
В частности, если $F -$ произвольное поле, $p \in F[t] -$ неприводимый многочлен,

то $F[t]/(\mathrm{p}) -$ поле

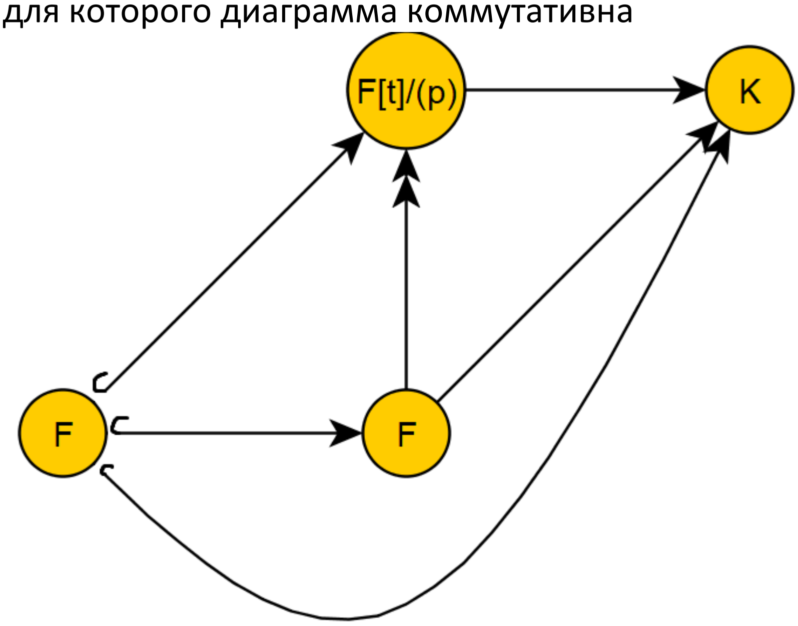
Универсальное свойство *F[t]/(p)*

$\forall$ поля $K \subseteq F$, в котором p имеет корень, $\exists$ гомоморфизм полей.

Следующая диаграмма коммутативна:



Доказательство: α — корень P, $\alpha \in R$
Возьмем отображение $\varphi: F[t] \to k$
$\varphi(g) = g(\alpha)$, т.к. $\varphi(p) = p(\alpha) = 0 \Rightarrow p \in \ker \varphi$
$pF[t] \subseteq \ker \varphi$
$\varphi(1) = 1 \Leftrightarrow \ker \varphi \neq F[t]$
Следовательно, по максимальности $pF[t]$ имеем $pF[t] = \ker \varphi$
По универсальному свойству факторкольца ∃! Отображение $F[t]/(\mathrm{p}) \to K$, для которого диаграмма коммутативна



Пример
$\mathbb{Q}, p(t) = t^3 - 2$
В $\mathbb{C}$ есть 3 корня - $\sqrt[3]{2}, \sqrt[3]{2}\varepsilon, \sqrt[3]{2}\varepsilon^2$

$$\varepsilon = -\frac{1 + \sqrt[3]{2}i}{2} = e^{\frac{i2\pi}{3}}$$

$\varphi: \mathbb{Q}[t]/(p) \to \mathbb{C}$,
$\varphi(p) = p(\omega)$, где ω — любой из 3-х корней

<u>Порядок и экспонента</u>

Порядок $ord\ g = |< g >|$ — наименьший $n \in N: g^n = 1$

Лемма. $a, b \in G \Rightarrow ord(a^{-1}) = ord(a); ord(b) = ord(a^{-1}ba); ord(ab) = ord(ba)$

Доказательство

$\forall k \in \mathbb{Z}: a^k = e \Leftrightarrow a^{(-1)k} = a^{-k} = e$

$a^{-1}b^k a = (a^{-1}ba)^k \Rightarrow b^k = e \Leftrightarrow a^{-1}b^k a = e$

$a^{-1}(ab)a = ba \Rightarrow ord(ab) = ord(ba)$

Теорема. $G = A \times B, a \in A, b \in B. ord(ab) = lcm\big(ord(a), ord(b)\big)$

Очевидно следует из $(a,b)^n = (e,e) \Leftrightarrow a^n = e, b^n = e$

Теорема. Пусть $F -$ поле, $G \leq F^*, |G| < \infty$. Тогда $G -$ циклическая

Пример

$(\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}_7^*$

$< 2> = \{1,2,3\}$

$< 3> = \{1,3,2,6,4,5\}$

Показатель (экспонента) группы - наименьший $e \in \mathbb{N}: \forall g \in G\ g^e = 1$

Лемма. $\exp G = \mathrm{lcm}_{g \in G}(ord\ g)$

Доказательство

$g \in G; e \vdots ord\ g \Leftrightarrow g^e = 1$

$e = k \cdot ord(g) + m$

$g^e = \left(g^{ord(g)}\right)^k \cdot g^m \Rightarrow g^e = k \Leftrightarrow g^m = 1$

т.к. $m < ord(g)$, то $m = 0$ и $g^{ord(g)} = 1$

Т.е. $e = \exp(G) -$ наименьшее натуральное число, которое делится на $ord(g)\ \forall g \in G$ ■

Лемма. Для абелевой группы $G: \exists a \in G: ord(a) = \exp(G)$

Доказательство

$$\exp(G) = \prod_{i=1}^{n} p_i^{k_i}$$

- разложение экспоненты на попарно простые множители p_i

$\forall i\ \exists g_i \in G: ord(g_i) \vdots p_i^{k_i}$

$ord(g_i) = p_i^{k_i \cdot m_i}$

$ord(g^{m_i}) = p_i^{k_i}$

Допустим, что $\prod g_i^{m_i}$ имеет порядок $\prod p_i^{k_i}$. Это следует из следующей леммы:

Лемма. $G -$ абелева группа $x, y \in G: \gcd\big(ord(x), ord(y)\big) = 1 \Rightarrow ord(xy) = ord(x) \cdot ord(y)$

Доказательство

Заметим, что $|< x > \cap < y >| -$ подгруппа и в $< x >$, и в $< y >$

$|< x > \cap < y >| \vdots ord(x)$ и $ord(y) \Rightarrow |< x > \cap < y >| = 1$

Т.е. $x^u = g^v \Rightarrow x^u = g^v = 1$

$(xy)^w = 1 \Leftrightarrow x^w y^w = 1 \Leftrightarrow x^w = y^w = 1$

$x^w = 1 \Rightarrow$ $\begin{cases} w \vdots ord(x) \\ w \vdots ord(y) \end{cases} \Rightarrow w \vdots ord(x) \cdot ord(y)$
$y^w = 1 \Rightarrow$
Т.к. w – наименьшее, то $w = ord(x) \cdot ord(y)$■

Доказательство теоремы
$|G| = n < \infty; G \leq F^*$
$t^n = 1$
$k < n. t^k = 1$ – имеет $\leq k$ корней, значит, все элементы G не могут быть его корнями
$\exists g \in G: g^k \neq 0$
$\exp(G)$ не может быть меньше, чем n. $\exp(G) \geq \mathrm{n}$
Но так как $< g >\vdots |G| = n, \forall g \in G g^n = 1 \Rightarrow \exp(G) = n$
$\exists a \in G: ord\ (g) = \exp(G) = n$
Т.е. $|< a >| = n = |G| \Rightarrow < a > = G$■

Следствие
Конечная абелева группа является циклической тогда и только тогда, когда её экспонента равна её порядку

Группа и кольцо $(\mathbb{Z}/\mathrm{n}\mathbb{Z})^*$

Monday, May 21, 2018 15:12

Присоединение к полю алгебраического элемента

Теорема. Пусть $F \subseteq K -$ поля, а $a \in K -$ алгебраический элемент над F, т.е. $\exists p \in F[t]: p(a) = 0$. Если $p -$ многочлен минимальной степени, обладающий этим свойством, то $F[a] \cong F[t]/pF[t]$, где $F[a] -$ наименьшее подполе в K, содержащее F и a

Теорема (классификация конечных полей)

1) Любое конечное поле состоит из p^n элементов, где $p -$ простое
2) $\forall p -$ простое и $n \in \mathbb{N}$: $\exists!$ Поле из p^n элементов с точностью изоморфизма
3) Если $|k| = p^n; |k| \cong Z_p[t]/(f)$

$(\mathbb{Z}/\mathrm{n}\mathbb{Z})^*$ - в этом кольце обратимые элементы - взаимно простые с n.
Порядок группы - функция Эйлера.
$(\mathbb{Z}/60\mathbb{Z})^*$
$\varphi(60) = \varphi(2^2)\varphi(5)\varphi(3) = 2 \cdot 4 \cdot 2 = 16$
$\exp(\mathbb{Z}/60\mathbb{Z})^* = 4$, т.к. по КТО
$(\mathbb{Z}/60\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$
$\exp(\mathbb{Z}/60\mathbb{Z})^* = lcm(\exp(\mathbb{Z}/4\mathbb{Z})^*, \exp(\mathbb{Z}/5\mathbb{Z})^*, \exp(\mathbb{Z}/3\mathbb{Z})^*) = 4$

Теорема о цикличности конечной подгруппы мультипликативной группы поля

Теорема. Конечная подгруппа мультипликативной группы поля циклическая.

Доказательство. Пусть G – конечная подгруппа мультипликативной группы поля F. Предположим, что G не является циклической и выберем в ней элемент a наибольшего порядка. Обозначим порядок элемента a через n. Поскольку $a^n = 1$, это означает, что a является корнем многочлена $x^n – 1$. Однако элементы $a^2, \ldots, a^{n-1}, a^n = 1$ тоже являются корнями этого многочлена. Поскольку многочлен не может иметь более чем корней, любой элемент, дающий 1 при возведении в степень n, совпадает с некоторой степенью элемента a, т.е. принадлежит подгруппе $\langle a \rangle$. Выберем теперь элемент b из $G \setminus \langle a \rangle$ наименьшего порядка. Порядок элемента b обозначим k. Из сказанного выше следует, что k не делит n. Рассмотрим несколько случаев для k.

1) k имеет два различных простых множителя p и q. Тогда b^p и b^q – элементы, порядки которых равны k / p и k / q соответственно, поэтому ввиду выбора b, они принадлежат подгруппе $\langle a \rangle$, т.е. $b^p = a^i$ и $b^q = a^j$ для некоторых i и j. В силу взаимной простоты p и q найдутся

такие целые u и v, для которых $up + vq = 1$. Тогда $b = b^{up+vq} = (b^p)^u (b^q)^v = (a^i)^u (a^j)^v \in \langle a \rangle$, что противоречит выбору b.

2) $k = p^s$, где p – простое, а $s > 1$. Тогда $b^p \in \langle a \rangle$ в силу выбора b и потому $(b^p)^n = 1$. Это означает, что $k \mid pn$. Поскольку k не делит n, $n = p^{s-1} u$, причём p уже не делит u.

Рассмотрим элемент $a^{-1}b$. Он, конечно, содержится в G, но не принадлежит ни $\langle a \rangle$, ни $\langle b \rangle$, а значит, его порядок m удовлетворяет неравенствам $k < m < n$. Из
$(a^{-1}b)^m = 1$ имеем $b^m = a^m$.
Пусть d = НОД(k, m). Тогда $d = p^t$, а $m = p^t v$,и p не делит v. Заметим, что $t < s$, ибо в противном случае $b^m = 1$, а тогда $a^m = 1$, т.е. $m \mid n$, а это невозможно при $m < n$. Значит, $d \mid n$. Далее, $1 = \mathrm{a}^{\mathrm{n}\frac{\mathrm{m}}{\mathrm{d}}} = \mathrm{a}^{\mathrm{m}\frac{\mathrm{n}}{\mathrm{d}}} = \mathrm{b}^{\mathrm{m}\frac{\mathrm{n}}{\mathrm{d}}} = \mathrm{b}^{\mathrm{vn}}$
Следовательно, $k \mid vn$. Но p не делит v, так что $k \mid n$ – противоречие.

3) $k = p$, где p – простое. Снова рассмотрим элемент $a^{-1}b$. Его порядок m удовлетворяет неравенствам $k < m < n$. Из $(a^{-1}b)^m = 1$ имеем $b^m = a^m$. Следовательно, p не делит m. Значит, найдутся такие целые u и v, для которых $up + vm = 1$. Поэтому $b = b^{up+vm} = (b^p)^u (b^q)^m = (a^m)^v \in \langle a \rangle$, что противоречит выбору b.■

<u>Строение мультипликативной группы кольца Z/nZ</u>

Лемма. $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^* -$ циклическая группа, если p^k не делится на 8
В противном случае для $p = 2$ и $k \geq 3$
$\left(\mathbb{Z}/2^k\mathbb{Z}\right)^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times \left(\mathbb{Z}/2^{k-2}\mathbb{Z}\right)^*$
Доказательство
$2^{2^{k-2}} \equiv 1\, mod\, 2^k$
$2^{2^{k-2}} \not\equiv 1\, mod\, 2^{k+1}$
База: $k = 3$
$25 \equiv 1\, mod\, 8$
$25 \not\equiv 1\, mod\, 16$
Пусть $5^{2^{k-2}} = 1 + z \cdot 2^k$
$z -$ нечётные
$5^{2^{k-1}} = \left(1 + z \cdot 2^k\right)^2 = 1 + z \cdot 2^{k+1} + z^2 2^{2k} = 1 + 2^{k+1}\left(z + z^2 \cdot 2^{k-1}\right)$
$\left(z + z^2 \cdot 2^{k-1}\right) -$ нечетное и не сравнимо с единицей
Для $p \neq 2$:
$\left|\mathbb{Z}/p^k\mathbb{Z}\right| = \varphi\left(p^k\right) = p^k - p^{k-1} = p^{k-1}(p-1)$
$(1+px)(1+py) = 1 + p(\ldots)$
$(1-px)\left(1 + px + (px)^2 + \cdots + (px)^{k-1}\right) = 1 - (px)^k = 1$
Поэтому $\{1 + px \mid x = 0, \ldots, p^{k-1} - 1\} -$ подгруппа в G
$|H| = p^{k-1}$
$g^{p-1} \equiv 1\, mod\, p$ по малой теореме Ферма
$g^{p-1} \in H$
$g^{(p-1)p^m} = 1$

$< g > \cong \mathbb{Z}/(p-1)p^m\mathbb{Z} \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$
g — образующий группы $(\mathbb{Z}/p\mathbb{Z})^*$
Доказательство
База: $\begin{cases} 1 + pz \equiv 1 \, mod \, p \\ 1 + pz \not\equiv 1 \, mod \, p^2 \end{cases}$
Нужно доказать:
$(1 + pz)^{p^{k-1}} \equiv 1 \, mod \, p^k$
$(1 + pz)^{p^{k-1}} \not\equiv 1 \, mod \, p^{k+1}$
$(1 + pz)^p = 1 + p^k w; w \not\vdots \, p$
$(1 + pz)^{p^k} = \left(1 + p^k w\right)^p = \left(1 + C_p^1 p^k w + C_p^2 \left(p^k w\right)^2 + \cdots\right) = 1 +$
$p^{k+1}(w + p \cdot x)$ — сравнимо с единицей по p^{k+1}, но не по p^{k+2}
$ord_H(1 + pz) = p^{k-1} = |H|$
Поэтому H — циклическая группа
Оказывается, если $u \in G; ord \, u = p - 1, ord \, (1 + pz) = p^{k-1}$, то
$ord\big((1 + pz)u\big) = (p - 1)p^{k-1} = |G|$ ∎

Теорема о порядке $(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})^*$
$\exp(\mathbb{Z}/n\mathbb{Z})^* = \lambda(m)$ — **функция Кармайкла**
$n = 2^k \cdot p_1^{k_1} \dots p_n^{k_n}$
p_i — нечетное простое число
$\lambda(n) = lcm\left(2^k, p_i^{k_i} - p_i^{k_{i-1}}\right)$, где $p_k = \begin{cases} 1, k \le 1 \\ 2, k = 2 \\ 2^{k-2}, k \ge 3 \end{cases}$
Иначе
$\lambda(n) = lcm\left(\varphi\left(p_i^{k_i}\right)\right)$ если n не делится на 8
$\lambda(n) = lcm\left(\varphi\left(2^k\right), \varphi\left(p_i^{k_i}\right)\right)$, если делится

Повторение?
$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ — циклическая при $p \ne 2$ или $k \le 2$.
$G = \left(\mathbb{Z}/2^k\mathbb{Z}\right)^* \cong C_2 \times C_{2^{k-2}}$ при $k \ge 3$
$ord(G_5) = 2^{k-2}$
Доказать, что $(1 + 2x)^{2^{k-2}} \equiv 1 mod \, 2^k$. Индукция по k
$(1 + 2x)^2 = 1 + 4x + 4x^2 = 1 + 4x(x + 1) \equiv 1 \, mod \, 8$ - база для 3
Пусть $(1 + 2x)^{2^{k-3}} \equiv 1 \, mod \, 2^{k-1}$
$(1 + 2x)^{k-2} = \left(1 + g \cdot 2^{k-1}\right)^2 = 1 + g2^k + g^2 2^{2k-2}$
$= 1 + 2^k\left(g + g^2 g^{k-2}\right) = 1 \, mod \, 2^k$

Теорема о строении конечных абелевых групп
Любая конечная абелева группа изоморфна произведению циклических групп примарного порядка

$C_{p_1^{k_1}} \times \cdots \times C_{p_m^{k_m}}$

Пример

$|G| = 8$

$G \cong C_2 \times C_2 \times C_2 \; (\exp(G) = 2)$

$G \cong C_2 \times C_4 \; (\exp(g) = 4)$

$G \cong C_8 \; (\exp(g) = 8)$

Вероятностное тестирование

Sunday, May 20, 2018 18:27

Схема вероятностного тестирования на простоту

n — тестируемое число.
$T_n(x)$ — **тест** $T_n: \mathbb{Z}/n\mathbb{Z}\setminus\{0\} \to \mathbb{B}$
$\mathbb{B} \coloneqq \{\text{ИСТИНА}, \text{ЛОЖЬ}\}$
$T_n = \text{И}$ если n — простое
Тест "хороший" в том случае, если n — не простое:
$|\{x|T_n(x) = \text{И}\}| \leq \dfrac{n-1}{2}$

Тест Ферма

$\Phi_n(x) = (x^{n-1} \equiv 1 \; mod \; n)$
Если n — простое, то это - малая теорема Ферма
$f_k: (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$
$f_k(x) = x^k$ — гомоморфизм
$f_k(xy) = x^k y^k$
$\{x|\Phi_n(x)\} = \ker f_{n-1}(x)$
Если $\ker f_{n-1} \neq (\mathbb{Z}/n\mathbb{Z})^*$, то $|\ker f_{n-1}| \leq \frac{n-1}{2}$

n называется **псевдопростым** числом Ферма, если $x^{n-1} \equiv 1 \; mod \; n \; \forall x \in (\mathbb{Z}/n\mathbb{Z})^*$
Самое маленькое - $3 \cdot 11 \cdot 17 = 561$
$\exp(\mathbb{Z}/561\mathbb{Z})^* = \operatorname{lcm}(2,10,16) = 80$
$561 - 1 = 560 \,\vdots\, 80$
Из-за таких чисел тест плохой

Тест Эйлера

Если n — простое, то $\mathbb{Z}/n\mathbb{Z}$ - поле и $x^2 = 1$ имеет решения при $x = \pm 1$
Если n — не простое, то $n = ab, \gcd(ab) = 1$
$\mathbb{Z}/n\mathbb{Z} \equiv \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$
$x^2 = 1 \Rightarrow (x_1^2, x_2^2) = (1,1)$ — уже 4 решения.
Четные числа бессмысленно тестировать на простоту.
Если n — нечетное, то
$\left(x^{\frac{n-1}{2}}\right)^2 = 1$, если n — простое
$E_n(x) = \left(x^{\frac{n-1}{2}} = \pm 1\right)$
Есть и **псевдопростые числа Эйлера**, так что и этот тест плохой

Тест Миллера-Рабина

$n - 1 = 2^k m$, где m — нечётное
$MR_n(x) = \left\{x^m = \pm 1 \text{ или } \exists t = 1, \dots, k-1 : \left(x^{(2^t)^m}\right) = -1\right\}$

Лемма. Если n — простое, то
$MR_n(x) = \text{И}\ \forall x \in (\mathbb{Z}/n\mathbb{Z})$
Доказательство
$x^{n-1} = 1 \Leftrightarrow x^{\frac{n-1}{2}} = \pm 1$
$$x^{\frac{n-1}{2}} = x^{m^{2^{n-1}}} = \left[\begin{array}{c} -1 - \text{тест пройден} \\ 1 \Leftrightarrow x^{m^{2^{k-2}}} \pm 1 \ \left(x^{m^{2^{k-2}}}\right)^2 = 1 \Leftrightarrow x^{m^{2^{k-2}}} = \pm 1 \end{array}\right.$$
Если $x^m = \pm 1$ — тест пройден

Если n — не простое, то $|\{x \in \mathbb{Z}/\mathrm{n}\mathbb{Z}\backslash\{0\} | MR_n(x)\}| \leq \frac{n-1}{4}$