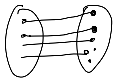
2.5. Пусть $|X| = m$, $|Y| = n$. Найти число:
а) отображении;
б) инъективных отображений;
в) биективных отображений;
г) сюръективных отображений множества X во множество Y.

а) $X \to Y$ n^m

б)  при $m \geqslant n$ и $X \to Y$ число $C_m^n \cdot n!$

n m

2.11. Доказать равенства:

а) $\binom{n}{m} = \binom{n}{n-m}$; б) $\sum\limits_{i=0}^{n} \binom{n}{i} = 2^n$;

в) $\sum\limits_{i=0}^{n} (-1)^i \binom{n}{i} = 0$; г) $\sum\limits_{i=1}^{n} i \binom{n}{i} = n2^{n-1}$;

а) $\binom{n}{m} = \frac{n!}{m!(n-m)!} = \frac{n!}{(n-m)!m!} = \binom{n}{n-m}$

б) $2^n = (1+1)^n = \sum\limits_{i=0}^{n} \binom{n}{i}$

в) $0 = (1-1)^n = \sum\limits_{i=0}^{n} (-1)^i \binom{n}{i}$

Т.1. Преобразование $f : \mathbb{R} \to \mathbb{R}$ задано равенством $f(x) = x^3$. Сколько неподвижных точек имеет f? Является ли множество $[2, +\infty)$ инвариантным относительно f? относительно f^{-1}?

1) $f(x_n) = x_n$

$x_n^3 = x_n \Leftrightarrow$

$\Leftrightarrow x_n = 0$ — 1 н.точка

2) нет т.к. $f([2,+\infty)) = [8,+\infty)$

3) $f^{-1}([2,+\infty)) = [\sqrt[3]{2}, +\infty)$ нет

Т.2. На множестве матриц $\mathbf{M}_{n\times n}$ введем отношение: $A \sim B \Leftrightarrow$ существует обратимая матрица $S \in \mathbf{M}_{n\times n}$ такая, что $B = S^{-1}AS$. Проверьте, что $\sim$ — отношение эквивалентности.

1) $A = S^{-1}AS$, тогда $S = E$

$A = E^{-1}AE = A$

2) $\exists S : B = S^{-1}AS \Rightarrow S^{-1}BS = A \Rightarrow \exists S_1 = S^{-1} : S_1 B S_1^{-1} = A$

3) $\left.\begin{array}{l} \exists S_1 : B = S_1^{-1}AS_1 \\ \exists S_2 : C = S_2^{-1}BS_2 \end{array}\right\} C = S_2^{-1}S_1^{-1}AS_1S_2 = (S_1S_2)^{-1}AS_1S_2 = S_3^{-1}AS_3,\ S_3 = S_1S_2$

Т.3. Проверить, что $(\mathbb{Z}, \circ)$, где $m \circ n = m + n + mn = (1+m)(1+n) - 1$, — коммутативная полугруппа. Что служит ее нейтральным элементом? Найти все обратимые элементы.

1) коммутативность очевидна

3) нейт. эл. — 0

1) коммутативность очевидна

2) $a \circ (b \circ c) = a \circ ((1+b)(1+c)-1) = (1+a)(1+b)(1+c)-1$

$(a \circ b) \circ c = ((1+a)(1+b)-1) \circ c = (1+a)(1+b)(1+c)-1$

3) нейтр. эл. — 0

4) $(1+m)(1+m^{-1})-1=0$

$m^{-1} = \frac{1}{1+m} - 1$

$m=0: m^{-1}=0$

55.1(г, д, е, ж*, з*, м*)

55.1. Какие из указанных числовых множеств с операциями являются группами:

а) $(A, +)$, где A — одно из множеств $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;

б) $(A, \cdot)$, где A — одно из множеств $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;

в) $(A_0, \cdot)$, где A — одно из множеств $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, а $A_0 = A \setminus \{0\}$;

г) $(n\mathbb{Z}, +)$, где n — натуральное число;

д) $(\{-1, 1\}, \cdot)$;

е) множество степеней данного вещественного числа $a \neq 0$ с целыми показателями относительно умножения;

ж) множество всех комплексных корней фиксированной степени n из 1 относительно умножения;

з) множество комплексных корней всех степеней из 1 относительно умножения;

и) множество комплексных чисел с фиксированным модулем r относительно умножения;

к) множество ненулевых комплексных чисел с модулем, не превосходящим фиксированное число r, относительно умножения;

л) множество ненулевых комплексных чисел, расположенных на лучах, выходящих из начала координат и образующих с лучом Ox углы $\varphi_1, \varphi_2, \ldots, \varphi_n$, относительно умножения;

м) множество всех непрерывных отображений φ: $[0, 1] \to [0, 1]$, для которых $\varphi(0) = 0$, $\varphi(1) = 1$, и $x < y \Rightarrow \varphi(x) < \varphi(y)$, относительно суперпозиции?

г) 1) $na, nb, nc \in n\mathbb{Z}$

$na + (nb+nc) = (na+nb)+nc$

2) $na, nb \in n\mathbb{Z}$

$na + nb = n(a+b) \in n\mathbb{Z}$

3) 0 — нейтр. эл. $0 = n \cdot 0 \in \mathbb{Z}$

$na + 0 = na$

4) $(na)^{-1} = -na = n(-a) \in \mathbb{Z}$

$na + (-na) = 0$

$(-na) + na = 0$

это группа.

д) $(\{-1,1\}, \cdot)$ 1) $\left.\begin{array}{l} -1 \cdot 1 = -1 \\ -1 \cdot -1 = 1 \\ 1 \cdot 1 = 1 \end{array}\right\}$ $\cdot$ — бин. операция

2) $-1 \cdot 1 = -1 = 1 \cdot (-1)$

3) 1 — нейтр. элемент: $-1 \cdot 1 = -1 = 1 \cdot (-1)$

$1 \cdot 1 = 1 = (1)(1)$

4) для -1 обрат. -1: $-1 \cdot (-1) = 1$

1 обрат. 1: $1 \cdot 1 = 1$

е) $(\{a^k \mid k \in \mathbb{Z}\}, \cdot)$ 1) $a^m \cdot a^n = a^{m+n} \in Q$

$Q =$

2) $a^m(a^n a^p) = (a^m a^n) a^p$

3) $1 = a^0$ — нейтр. эл.: $a^m a^0 = a^m = a^0 a^m$

4) $(a^m)^{-1} = a^{-m}$: $a^m a^{-m} = a^0 = a^{-m} a^m$

55.6. Какие из указанных множеств квадратных вещественных матриц фиксированного порядка образуют группу:

д) множество матриц с фиксированным определителем d относительно умножения;

нет, т.к. $|A \cdot B| = |A| \cdot |B| = d \cdot d = d^2$ — что не равно d если $d \neq 1$

м) множество верхних унитреугольных матриц относительно умножения;

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} & \ldots & a_{1n} \\ 0 & 1 & a_{23} & \ldots & a_{2n} \\ 0 & 0 & 1 & \ldots & \\ \ldots & & & & 1 \end{pmatrix}$$

1) р-рим $A, B \in G$, $A \cdot B = C$

тогда $c_{ii} = (0 \cdot a_{1i} + 0 \cdot a_{2i} + \ldots + 1 \cdot 1 + 0 \cdot \ldots) = 1$

тогда $c_{ij} (j<i) = 0$ — т.е. $\cdot$ — бин. операция

2) $A, B, C \in G$: $A\cdot(B\cdot C)=(A\cdot B)\cdot C$ из асс. матриц

3) E – нейтр. элем. $A\cdot E=A$

4) $A\in G$, тогда $\exists!\, A^{-1}$ $AA^{-1}=A^{-1}A=E$ т.к. $|A|=1$

Д $^{-1}$. Там очевидно через алг. дополнения что $A^{-1}\in G$

$$A^{-1}=\frac{1}{|A|}\begin{pmatrix} |A_{11}| & \dots & |A_{1n}| \\ - & - & - \\ - & - & - \end{pmatrix}^{T} \quad \begin{matrix} A_{ii}=1 \\ A_{ij}\,(i<j)=0 \end{matrix}$$

н) множество всех ортогональных матриц относительно умножения;

$A\in G$, то $AA^T=A^TA=E$

1) $A, B\in G$ $A\cdot B=C$ тогда $C^T=(AB)^T=B^TA^T$

$CC^T=ABB^TA^T=AA^T=E$

$C^TC=B^TA^TAB=E$ – $C\in G$

2) Ассоциат по умн. матриц.

3) E – нейтр. элем.

4) $\exists A^{-1}$ – орт. тогда $A^{-1}\cdot(A^{-1})^T=A^{-1}\cdot(A^T)^{-1}=\{A^{-1}=A^T\}=A^T(A^T)^{-1}=E \Rightarrow \underline{A^{-1}\in G}$

55.18. Для каких групп G отображение $f\colon G\mapsto G$, определенное правилом:

а) $f(x)=x^2$; б) $f(x)=x^{-1}$,

является гомоморфизмом?

При каком условии эти отображения являются изоморфизмами?

б) 1) $f(x\cdot y)=f(x)\cdot f(y)$

$(xy)^{-1}=x^{-1}\cdot y^{-1}$

$y^{-1}\cdot x^{-1}=x^{-1}\cdot y^{-1}$ – для абелевых групп.

2) $f(x)$ – инъекция т.к. $\nexists\; a, b\in G$, $a\neq b$ т.к. $\exists c\in G$ $ac=e=bc$

$f(x)$ – сюръекция т.к. $\forall a\in G\ \exists a^{-1}$ т.ч. $(a^{-1})^{-1}=a$

$f(x)$ – биекция – т.е. $f(x)$ – изоморфизм.

Т.4. Разбейте на классы попарно изоморфных групп следующие групы: $(\mathbb{Z},+)$, $(n\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{R}_+,\cdot)$.

1) $(\mathbb{Z},+)$, $(n\mathbb{Z},+)$ $f(x)=nx$

2) $(\mathbb{Q},+)$

3) $(\mathbb{R},+)$; $(\mathbb{R}_+,\cdot)$ $f(x)=e^x$

4) $(\mathbb{R}^*,\cdot)$ – это не изоморфно $(\mathbb{R},+)$ т.к.

$f(ab)=f(a)+f(b)$

$f(1\cdot 1)=f(1)+f(1) \Rightarrow f(1)=0$ и $f(-1\cdot -1)=f(1)=0=f(-1)+f(-1)\Rightarrow f(-1)=0$

т.е. $\begin{matrix} f(-1)=0 \\ f(1)=0 \end{matrix}$ – нет инъекции

Т.5*. Изоморфны ли мультипликативные группы $\mathbb{R}^*$ и $\mathbb{C}^*$?

[illegible] $\Rightarrow f(i)=f(1)=1$ – нет инъекции.

Т.5*. Изоморфны ли мультипликативные группы $\mathbb{R}^*$ и $\mathbb{C}^*$?

$1 = f(1) = f(i^4) = f(i)^4 \Rightarrow f(i) = 1 \Rightarrow f(i) = f(1) = 1$ – нет инъекции.

55.21. Найти все изоморфизмы между группами $(\mathbf{Z}_4, +)$ и $(\mathbf{Z}_5^*, \cdot)$.

1) $0 \to 1$ т.к. нейт.

2)

$\mathbb{Z}_4$	$\dot{\mathbb{Z}}_5$
1 – поряд. 4	2 – 4
2 – пор. 2	3 – 4
3 – пор. 4	4 – 2

3) 2 способа: $0 \to 1$, $2 \to 4$, $1 \to 2$, $3 \to 3$; $0 \to 1$, $2 \to 4$, $1 \to 3$, $3 \to 2$

56.7. Доказать, что во всякой группе:
а) элементы x и yxy^{-1} имеют одинаковый порядок;
б) элементы ab и ba имеют одинаковый порядок;
в) элементы xyz и zyx могут иметь разные порядки.

а) $(yxy^{-1})^k = yx^ky^{-1} = yy^{-1} = e \Rightarrow |yxy^{-1}| \le k$

пусть $|yxy^{-1}| = m < k \Rightarrow (yxy^{-1})^m = e$

$yx^my^{-1} = e$

$x^m = y^{-1}ey = e \Rightarrow \underline{|x| = m}$ - противор.

б) $|ab| = k \Rightarrow a\underbrace{bab\ldots a}_{k-1}b = e$

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

$(ba)^{k-1} = (ba)^{-1}$

$(ba)^k = e \Rightarrow |ba| \le k$

Пусть $|ba| = m < k \Rightarrow |ab| \le m \Rightarrow k \le m < k \Rightarrow k < k$ - противор.

56.15. В циклической группе $\langle a \rangle$ порядка n найти все элементы g, удовлетворяющие условию $g^k = e$, и все элементы порядка k при:
а) $n = 24$, $k = 6$; б) $n = 24$, $k = 4$;

а) $a^4, a^8, a^{12}, a^{16}, a^{20}$ б) a^6, a^{12}, a^{18}

60.45. Сколько элементов:
а) порядка 2, 4 и 6 в группе $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_3$;
б) порядка 2, 4 и 5 в группе $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_5$?

а)

$\mathbb{Z}_2$	$\mathbb{Z}_4$	$\mathbb{Z}_3$
0 – пор. 1	0 – п. 1	0 – п. 1
1 – пор. 2	1 – п. 4	1 – п. 3
	2 – п. 2	2 – п. 3
	3 – п. 4	

Порядка 2: $(0,2,0)$; $(1,0,0)$; $(1,2,0)$

Порядка 4: $4 \cdot x = 0$: $x = 0, 1$; $4 \cdot y = 0$: $y = 0,1,2,3$; $4 \cdot z = 0$: $z = 0$ $\Big\}$ $8 - 3 - 1 = 4$

Порядка 3: $3 \cdot x = 0$: $x = 0$; $3 \cdot y = 0$: $y = 0$; $3 \cdot z = 0$: $z = 0,1,2$ $\Big\}$ $3 - 1 = 2$

Порядка 6: $6 \cdot x = 0$: $x = 0,1$; $6 \cdot y = 0$: $y = 0,2$; $6 \cdot z = 0$: $z = 0,1,2$ $\Big\}$ $12 - 3 - 2 - 1 = \underline{6}$

Т.6. В группе порядок любого элемента равен 2. Докажите, что эта группа абелева.

$a^2 = e \Rightarrow a \cdot a = e \Rightarrow ba \cdot ab = b^2 = e$

$ba \cdot ab = e$

$ba \cdot \underbrace{(ab)^2}_{e} = ab$

$ba = ab$

Т.7. Пусть G — группа, $a \in G$ — элемент конечного порядка, $(\operatorname{ord} a,\, n) = 1$. Доказать, что уравнение $x^n = a$ разрешимо в группе G.

$(|a|, n) = 1 \Rightarrow \overset{\exists k, m}{kn} + m|a| = 1 \Rightarrow kn \overset{|a|}{\equiv} 1 \Rightarrow a^{kn} = a \Rightarrow \underline{a^k = x}$

Т.8. Показать, что группа $\mathbb{Z}_7^*$ циклическая. Какие элементы являются ее порождающими?

$2 \to 4 \to 1 \to 2$

$3 \to 2 \to 6 \to 4 \to 5 \to 1 \to 3$

$4 \to 2 \to 1 \to 4$

$5 \to 4 \to 6 \to 2 \to 3 \to 1 \to 5$

$6 \to 1 \to 6$

3.2. Записать в виде произведения независимых циклов перестановки:

б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 6 & 7 & 5 & 2 & 4 \end{pmatrix}$;

$1 \to 3 \to 6 \to 2 \to 1$ $\quad$ $[(1362)(47)5]$

$4 \to 7 \to 4$

$5 \to 5$

3.4. Перемножить перестановки:

а) $[(1\,3\,5)(2\,4\,6\,7)] \cdot [(1\,4\,7)(2\,3\,5\,6)]$; $= [(1542736)]$

1 2 3 4 5 6 7

3 4 5 6 1 7 2 $\to$ $\quad$ $1 \to 5 \to 4 \to 2 \to 7 \to 3 \to 6 \to 1$

5 7 6 2 4 1 3

3.7. Определить четность перестановок:

а) $(1\,2\,3 \ldots k)$;

б) $(i_1\, i_2 \ldots i_k)$;

в) $(1\,4\,7\,3)(6\,7\,2\,4\,8)(3\,2)$;

г) $(i_1\, i_2)(i_3\, i_4)(i_5\, i_6) \ldots (i_{2k-1}\, i_{2k})$;

в) 1 2 3 4 5 6 7 8 $\quad$ $1 \to 4 \to 8 \to 6 \to 3 \to 7 \to 2 \to 1$

1 3 2 4 5 6 7 8 $\quad$ $5 \to 5$

1 3 4 8 5 7 2 6

4 1 7 8 5 3 2 6 $\quad \overset{}{\underset{sgn}{=}} [(1486372)(5)]$ – 14 инверсий $sgn = \underline{1}$

г) Каждый цикл. увел. кол-во инв. на 1

$sgn = (-1)^k$

Т.10. В задаче 3.7(в) найдите порядок данного элемента группы S_n, вычислить его 2023-ю степень.

$\sigma = [(1486372)(5)]$ Порядок равен длине б. цикла +1 т.е. $6+1=\underline{\underline{7}}$

$\sigma^{2023} = \sigma^0 = e$, т.к. $2023 \,\vdots\, 7$

Т.11*. Сколько элементов порядка 6 в группе S_7?

$\operatorname{sgn}\sigma$ = НОК(длин. циклов) = 6 т.е. у σ вида $\underbrace{(\ldots)}_{1}\underbrace{(\ldots\ldots)}_{6}$ и $\underbrace{(\ldots)}_{2}\underbrace{(\ldots\ldots)}_{3}\underbrace{(\,)}_{1}\underbrace{(\,)}_{1}$ и $\underbrace{(\ldots)}_{3}\underbrace{(\ldots)}_{2}\underbrace{(\ldots)}_{2}$

$$\left.\begin{aligned} n_{16} &= C_7^1 \cdot \frac{6!}{6} = 840 \\ n_{23} &= C_7^1 C_6^1 C_5^2 \frac{2!}{2}\cdot\frac{3!}{3} = 7\cdot 6\cdot \frac{5\cdot 4^2}{\cancel{2}}\cdot 2\cdot \cancel{2}\cdot\cancel{8} = 840 \\ n_{322} &= C_7^3 C_5^2 \frac{2!}{2}\cdot\frac{2!}{2}\cdot\frac{3!}{3} = \cancel{2}\cdot\frac{7\cdot 6}{\cancel{2}}\cdot\frac{5\cdot 4}{2} = 7\cdot 6\cdot 5\cdot 2 = 420 \end{aligned}\right\} 2100$$

56.37. Найти смежные классы:

а) аддитивной группы $\mathbb{Z}$ по подгруппе $n\mathbb{Z}$, n — натуральное число;

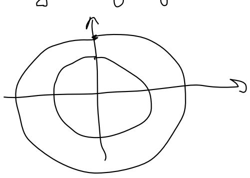
$n\mathbb{Z} \cup n\mathbb{Z}+1 \cup \ldots \cup n\mathbb{Z}+n-1$

в) аддитивной группы $\mathbb{R}$ по подгруппе $\mathbb{Z}$;

$g_1 \sim g_2 \Leftrightarrow g_2 - g_1 \in \mathbb{Z}$ смежные классы — действ. числа с один. др. частью

д) мультипликативной группы $\mathbb{C}^*$ по подгруппе $\mathbf{U}$ чисел с модулем 1;

$g_1 \sim g_2 \Leftrightarrow g_1^{-1}g_2 \in U(1) \Leftrightarrow |g_1^{-1}g_2| = 1 \Rightarrow |g_1| = |g_2|$ — окружности.



56.38. Пусть g — невырожденная матрица из $\mathbf{GL}_n(\mathbb{C})$ и $H = \mathbf{SL}_n(\mathbb{C})$. Доказать, что смежный класс gH состоит из всех матриц $a \in \mathbf{GL}_n(\mathbb{C})$, определитель которых равен определителю матрицы g.

$g_1 \sim g_2 \Leftrightarrow |g_1^{-1}g_2| = 1 \Rightarrow |g_1| = |g_2|$ — т.е. смежные классы — мн-ва матриц с один. опр. g.

56.39. Пусть H — подгруппа в группе G. Доказать, что отображение $xH \mapsto Hx^{-1}$ задает биекцию между множеством левых и множеством правых смежных классов G по H.

1) Инъективность: пусть f не инъектив.: $\exists x_1, x_2$ $f(x_1H) = f(x_2H) \Leftrightarrow Hx_1^{-1} = Hx_2^{-1} \Leftrightarrow x_1^{-1}x_2 \in H \Rightarrow$
$x_1H \neq x_2H$ $\qquad \Rightarrow (x_1^{-1}x_2)^{-1} \in H \Rightarrow$
$x_2^{-1}x_1 \notin H$ $\qquad \Rightarrow x_2^{-1}x_1 \in H$

2) Сюрьективность $\{x^{-1} \mid x \in G\}$ равномощно G, значит $\forall\, Hx^{-1}$ сущ. xH.

63.1. Какие из следующих числовых множеств образуют кольцо относительно обычных операций сложения и умножения:

ж) множество рациональных чисел, в несократимой записи которых знаменатели являются степенями фиксированного простого числа p;

з) множество вещественных чисел вида $x + y\sqrt{2}$, где $x, y \in \mathbb{Q}$;

л) множество комплексных чисел вида $x + yi$, где $x, y \in \mathbb{Z}$;

м) множество комплексных чисел вида $x + yi$, где $x, y \in \mathbb{Q}$;

ж) Пусть $p = 36$: $\frac{1}{36}, \frac{5}{36} \in K$: $\frac{1}{36} + \frac{5}{36} = \frac{1}{6}$ но $6 \neq 36^k$. — + не алг. операция.

3) ⊕ очевидно абелева.
⊙ $(x_1+y_1\sqrt{2})(x_2+y_2\sqrt{2}) = x_1x_2+2y_1y_2+(x_1y_2+y_1x_2)\sqrt{2} \in K$ — да это ~~группа~~ кольцо

л) ⊕ очевидно абелева.
⊙ $(x_1+iy_1)(x_2+iy_2) = x_1x_2-y_1y_2+i(y_2x_2+x_1y_2) \in K$ — кольцо

м) тоже кольцо

з) и м) также явл. полями.

63.2. Какие из указанных множеств матриц образуют кольцо относительно матричного сложения и умножения:

в) множество верхних треугольных матриц порядка $n \geqslant 2$;

⊕ очевидно абелева.

⊙ Ранее док-валось, что умножение треуг. матриц — треуг. матрица.

63.11. Найти все обратимые элементы, все делители нуля и все нильпотентные элементы в кольцах:

а) $\mathbf{Z}_{p^n}$, где p — простое число;

обратимые элементы: $A = \mathbb{Z}_{p^n} \setminus \{p^k, k<n\}$

делители нуля: $Q = \{p^k, k<n\}$

нильпотентные эл-ты: $D = \{p^k, 0<k<n\} \cup \{0\}$

г) верхних треугольных матриц над полем;

обратимые: все a с $\det a \neq 0$

делители нуля: все матрицы с $\det A = 0$

нильпотентные эл-ты: все матрицы с 0 диагональю.

66.20. Решить систему уравнений

$$\overset{(1)}{3x + y + 2z = 1}, \quad \overset{(2)}{x + 2y + 3z = 1}, \quad \overset{(3)}{4x + 3y + 2z = 1}$$

а) в поле $\mathbf{Z}_5$; б) в поле $\mathbf{Z}_7$.

а) $(2)+(3)$: $5x+5y+5z=2 \Leftrightarrow 0=2$ — неверно.

б) $(1)+(2)+(3)$: $8x+6y+7z=3 \Leftrightarrow x-y=3$
$(1)-(3)$: $-x-2y=0 \Leftrightarrow -2y=+x$

$-3y=3 \Rightarrow y=6$
$x=-12=2$
$2z=1-3\cdot 2-6=3 \Rightarrow z=5$

$(2,6,5)$

60.5. Разложить в прямую сумму группы:
а) $\mathbf{Z}_6$; б) $\mathbf{Z}_{12}$; в) $\mathbf{Z}_{60}$.

??

а) $\mathbb{Z}_6 = \mathbb{Z}_2 \oplus \mathbb{Z}_3$
б) $\mathbb{Z}_{12} = \mathbb{Z}_4 \oplus \mathbb{Z}_3$
в) $\mathbb{Z}_{60} = \mathbb{Z}_{15} \oplus \mathbb{Z}_4$

35.10. Пусть V — n-мерное векторное пространство над полем F, состоящим из q элементов. Найти:

а) число векторов в пространстве V;

б) число базисов пространства V;

в) число невырожденных матриц порядка n над полем F;

г) число вырожденных матриц порядка n над полем F;

д) число k-мерных подпространств пространства V;

а) q^n

б) Кол-во всех наборов – $n^{(q^n)}$

Кол-во ЛЗ. в-ров с разм. лин.об. n-1 : $(q^{n-1})^1$

Кол-во ЛЗ. в-ров с разм. лин.об. n-2 : $(q^{n-2})^2$

...

$\Rightarrow$ Кол-во базисов $= \underbrace{n^{q^n} - q^{n-1} - q^{2(n-2)} - \dots - q^n}_{p}$

$p = n^{q^n} - \sum_{k=1}^{n} q^{k(n-k)}$

в) $p = n^{q^n} - \sum_{k=1}^{n} q^{k(n-k)}$ – число ЛНЗ столбцов.

г) $\sum_{k=1}^{n} q^{k(n-k)}$

д) C_p^k, $p = n^{q^n} - \sum_{k=1}^{n} q^{k(n-k)}$

T.12. а) Решите в целых числах уравнение $21x + 76y = 0$.

б) Решите в целых числах уравнение $21x + 76y = 1$. Сколько решений (x_0, y_0) удовлетворяют условию $0 \leq x_0 \leq 75$?

в) В кольце $\mathbb{Z}_{76}$ вычислите 21^{-1}.

а) $21x + 76y = 0$

т.к. НОД$(21, 76) = 1$ то $x = -\frac{76}{21} y$ и $y \vdots 21$ т.е. $y = 21z$, $z \in \mathbb{Z}$
$x = -76z$

б) $21x + 76y = 1$

$x_0 = 29$ $y_0 = -8$ при $0 \leq x_0 \leq 75$ тогда $21x_0 + 76y_0 = 1$

$21(x - x_0) + 76(y - y_0) = 0$

$\left.\begin{array}{l} x - x_0 = -76z \\ y - y_0 = 21z \end{array}\right., z \in \mathbb{Z} \quad \left\}\begin{array}{l} x = 29 - 76z \\ y = -8 + 21z \end{array}\right., z \in \mathbb{Z}$

в) $21x_0 + 76y_0 = 1 \Rightarrow 21x_0 \overset{76}{\equiv} 1 \Rightarrow x_0 \overset{76}{\equiv} 21^{-1}$ т.е. $29 = 21^{-1}$ в $\mathbb{Z}_{76}$

T.13. Докажите, что сопоставление $k \pmod{15} \mapsto (k \pmod 3, k \pmod 5)$ задает изоморфизм колец $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

Докажем, что $f: k_{15} \Rightarrow (k_3, k_5)$ гомоморфизм

$(ab)_{15} = (a_3, a_5) \cdot (b_3, b_5) = (a_3 b_3, a_5 b_5) = ((ab)_3, (ab)_5)$

$\ker f = \{0\}$ – инъекция.

$\forall a \in \mathbb{Z}_3\ \forall b \in \mathbb{Z}_5\ \exists f: \mathbb{Z}_3 \oplus \mathbb{Z}_5 \Rightarrow \mathbb{Z}_{15}$ $f((a, b)) = 5a + b$ – сюрьекция.

25.2. Найти наибольший общий делитель многочленов:

б) $x^6 + 2x^4 - 4x^3 - 3x^2 + 8x - 5$ и $x^5 + x^2 - x + 1$;

$x^6+2x^4-4x^3-3x^2+8x-5 \;\Big|\; x^5+x^2-x+1$

$-\;x^6+x^3-x^2+x \;\Big|\; x$

$2x^4-5x^3-2x^2+7x-5$

$x^5+x^2-x+1 \;\Big|\; 2x^4-5x^3-2x^2+7x-5$

$-\;x^5-\frac{5x^4}{2}-x^3+\frac{7x^2}{2}-\frac{5x}{2} \;\Big|\; \frac{1}{2}x+\frac{5}{4}$

$\frac{5x^4}{2}+x^3-\frac{5x^2}{2}+\frac{3x}{2}+1$

$-\;\frac{5x^4}{2}-\frac{25x^3}{4}-\frac{5x^2}{2}+\frac{35x}{4}-\frac{25}{4}$

$\frac{29x^3}{4}-\frac{29x}{4}+\frac{29}{4}$

$2x^4-5x^3-2x^2+7x-5 \;\Big|\; x^3-x+1 \leftarrow$ НОД.

$2x^4-2x^2+2x \;\Big|\; 2x-5$

$-5x^3+5x-5$

$-5x^3+5x-5$

0

25.7. Найти наибольший общий делитель и его выражение через f и g над полем $\mathbb{F}_2$:

г) $f = x^5 + x^3 + x$, $g = x^4 + x + 1$.

1) $x^5+x^3+x \;\Big|\; x^4+x+1$

$x^5+x^2+x \;\Big|\; x$

x^3-x^2

2) $x^4+x+1 \;\Big|\; x^3-x^2$

$x^4-x^2 \;\Big|\; x$

x^2+x+1

3) $x^3-x^2 \;\Big|\; x^2+x+1$

$x^3+x^2+x \;\Big|\; x-2$

$-2x^2-x$

$-2x^2-2x-2$

$x+2$

4) $x^2+x+1 \;\Big|\; x+2$

$x^2+2x \;\Big|\; x-1$

$-x+1$

$-x-2$

$3 = 1$

5) $x+2 \;\Big|\; 1$

$x+2 \;\Big|\; x+2$

0

НОД $= 1$

$f = xg + r_1 \Rightarrow r_1 = f - gx$

$g = xr_1 + r_2 \Rightarrow g = xf - x^2g + r_2 \Rightarrow r_2 = (x^2+1)g + xf$

$r_1 = (x-2)r_2 + r_3 \Rightarrow r_1 = xr_2 + r_3 \Rightarrow r_3 = f - gx - x(x^2+1)g + x^2f = f(1+x^2) - (x^3-\cancel{x}^{0})g = f(1+x^2) - x^3g$

$r_2 = (x-1)r_3 + 1 \Rightarrow 1 = (x^2+1)g - xf - (x-1)\big(f(x^2+1) - gx^3\big) = f(-x^3-\cancel{x}+x^2+1-\cancel{x}) + g(x^2+1+x^4-x^3) =$

$= f(-x^3+x^2+1) + g(x^4-x^3+x^2+1)$

27.2. Разложить на линейные и квадратные множители над полем вещественных чисел многочлены:

а) $x^6 + 27$; б) $x^4 + 4x^3 + 4x^2 + 1$;

$x^6+27 = (x^2+3)(x^4-3x^2+9) = (x^2+3)(x^4+6x^2+9-9x^2) = (x^2+3)\big((x^2+3)^2-(3x)^2\big) = (x^2+3)(x^2-3x^2+3)(x^2+3x^2+3)$

28.22. Найти:

а) все неприводимые многочлены степени $\leqslant 4$ над полем $\mathbf{Z}_2$;

1: x $x+1$ – непр.

2: привод: x^2+x, x^2, x^2+1 → неприв: x^2+x+1

3: привод: x^3, x^3+x^2, x^3+x^2+x, x^3+1, x^3+x^2+x+1 → неприв: x^3+x^2+1, x^3+x+1

x^3+x^2+x
x^3+1
x^3+x^2+x+1
x^3+x

4: привод: x^4+x^2+1 | $\cancel{x^4+x^2}$ | $\cancel{x^4+x}$ | неприв: $x^4+x^3+x^2+x+1$

x^4+x^3+x | $\cancel{x^4+x^3+x+1}$ | x^4+x^3+x+1

x^4+x^2+x | x^4+1 | x^4+x^3+1

x^4+x^2+x+1 | $\cancel{x^4+x^3+x^2+x}$ | x^4+x+1

$x^4+x^3+x^2+1$

x^4
x^4+x^3
$x^4+x^3+x^2$
x^4+x
$x^4+x^3+x^2+x$
x^4+x^2

Т.14. Дан многочлен $f \in \mathbb{Z}_p[X]$ степенью $n > 1$ (p — данное простое число).
При каких n степень первой разности $f(x+1) - f(x)$ равна $n-1$?

$a_n(x+1)^n - a_n x^n = C_n^1 a_n x^{n-1} + \ldots = n a_n x^{n-1}$ т.е. $n a_n \neq 0$ при $n \neq pk, k \in \mathbb{Z}$

$+\ldots \quad +\ldots$

21.1. Найти тригонометрическую форму числа:

д) $1 + i; = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$

р) $2 + \sqrt{3} + i; = \sqrt{8+4\sqrt{3}}\left(\cos\left(\operatorname{arctg}\left(\frac{1}{2+\sqrt{3}}\right)\right) + i\sin\left(\operatorname{arctg}\left(\frac{1}{2+\sqrt{3}}\right)\right)\right)$

21.2. Вычислить выражения:

$\left(\frac{\sqrt{3}+i}{1-i}\right)^{30}$:

$\frac{\sqrt{3}+i}{1-i} = \frac{(\sqrt{3}+i)(1+i)}{2} = \frac{(\sqrt{3}-1+i(\sqrt{3}+1))}{2} = e^{i\operatorname{arctg}\frac{\sqrt{3}+1}{\sqrt{3}-1}}$

$\left\{ tg\left(\frac{\pi}{4}+\frac{\pi}{6}\right) = \frac{tg\frac{\pi}{4}+tg\frac{\pi}{6}}{-1+tg\frac{\pi}{4}tg\frac{\pi}{6}} = \frac{\sqrt{3}+1}{1-\sqrt{3}} \Rightarrow \right.$

$\left(\frac{\sqrt{3}+i}{1-i}\right)^{30} = e^{i\frac{5\pi}{12}\cdot 30} = e^{i\frac{25\pi}{2}} = e^{\frac{i\pi}{2}} = i$

21.10. Доказать, что если $z + z^{-1} = 2\cos\varphi$, то $z^n + z^{-n} = 2\cos n\varphi$, где $n \in \mathbb{Z}$.

$\left.\begin{array}{l} z = Ae^{i\varphi} \\ z^{-1} = Ae^{-i\varphi} \end{array}\right\}$ $z + z^{-1} = 2A\left(\frac{e^{i\varphi}+e^{-i\varphi}}{2}\right) = 2A\cos\varphi$ т.е. $A = 1 \Rightarrow$ $\left.\begin{array}{l} z^n = e^{in\varphi} \\ z^{-n} = e^{-in\varphi} \end{array}\right\}$ $z^n + z^{-n} =$

$= 2\,\frac{e^{in\varphi}+e^{-in\varphi}}{2} = 2\cos n\varphi$ чтд

22.7. Вычислить:

л) $\sqrt[6]{-27}$; $-27 = 27e^{i\pi}$

$\sqrt[6]{27e^{i\pi}} = \sqrt{3}\, e^{i\left(\frac{\pi}{6}+\frac{\pi n}{3}\right)}$, $n \in 0, 1 \ldots 5$

о) $\sqrt[3]{1+i}$; $1+i = \sqrt{2}\, e^{i\frac{\pi}{4}}$

$\sqrt[3]{\sqrt{2}e^{i\frac{\pi}{4}}} = \sqrt[6]{2}\, e^{i\left(\frac{\pi}{12}+\frac{2\pi n}{3}\right)}$, $n = 0, 1, 2$

23.1. Вычислить суммы:

а) $1 - \binom{n}{2} + \binom{n}{4} - \binom{n}{6} + \ldots;$ $= (\sqrt{2})^n \cos\left(\frac{\pi n}{4}\right)$

$z^n = (1+i)^n = 1 + \binom{n}{1} i - \binom{n}{2} - \binom{n}{3} i + \binom{n}{4}$ $\quad z^n = (\sqrt{2})^n \left(\cos\frac{\pi n}{4} + i \sin\frac{\pi n}{4}\right) \Rightarrow \operatorname{Re} z^n = (\sqrt{2})^n \cos\left(\frac{\pi n}{4}\right)$

тогда $\operatorname{Re} z^n = 1 - \binom{n}{2} + \binom{n}{4} - \ldots$

T.15. Покажите, что множество матриц $\left\{\begin{pmatrix} x & -y \\ y & x \end{pmatrix} | x, y \in \mathbb{R}\right\} \subset \mathrm{Mat}_2(\mathbb{R})$ является полем относительно операций сложения и умножения матриц. Покажите также что отображение $x + iy \mapsto \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$ задает изоморфизм поля $\mathbb{C}$ с полем матриц указанного вида.

Д-жем гомом. по + и ·

$\oplus$: $\begin{pmatrix} x_1+x_2 & -(y_1+y_2) \\ y_1+y_2 & x_1+x_2 \end{pmatrix} = \begin{pmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{pmatrix} + \begin{pmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{pmatrix}$

$f(a_1+a_2) = f(a_1) + f(a_2)$

$\odot$ $\begin{pmatrix} x_1x_2 - y_1y_2 & -(x_1y_2 + y_1x_2) \\ x_1y_2 + y_1x_2 & x_1x_2 - y_1y_2 \end{pmatrix} = \begin{pmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{pmatrix}$

$f(a_1a_2) = f(a_1) \cdot f(a_2)$

Д-жем биекцию f: $x+iy \to \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$ ну я не знаю тут очевидно.

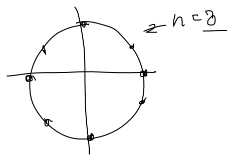
Тогда т.к. есть гомоморф $\odot$ и $\oplus$ и биекция то f – изоморфизм $\Rightarrow$ это поле.

T.16. Проверьте, что отображение $\varphi : \mathbb{R} \to \mathbb{S}^1$, $\varphi(x) = \exp(2\pi i x)$, является сюръективным гомоморфизмом групп. На какую подгруппу в $\mathbb{S}^1$ φ отображает подгруппу $\mathbb{Q} \subset \mathbb{R}$? Найдите ядро $\ker\varphi$. Убедитесь, что φ индуцирует биекцию между $\mathbb{S}^1$ и множеством смежных классов группы $\mathbb{R}$ по подгруппе $\ker\varphi$.

1) $e^{2\pi i x + 2\pi i y} = e^{2\pi i x} e^{2\pi i y}$ – гомоморфизм.

2) рассм $z \in \mathbb{S}^1$ тогда $z = e^{i\ell}$ тогда $x = \frac{\ell}{2\pi}$ – сюрьекция.

3) $e^{2\pi i \frac{m}{n}} = \left\{\begin{array}{l} \text{если } \overline{m} > n \text{ то } m = (\overline{m}, n)\text{-ост} \\ e^{i\frac{2\pi\overline{m}}{n}} = e^{i\frac{2\pi m}{n}} \end{array}\right\} = e^{2\pi i \frac{m}{n}}$ – корни кратности n из 1 для $n \in \mathbb{N}$.



4) $e^{2\pi i x} = 1 \Rightarrow x = m \in \mathbb{Z}$. – ядро

5) Смежные классы $\mathbb{R}$ по $\mathbb{Z}$ – это мн-ва чисел с один. др. частью.

$\varphi(x) = e^{i2\pi(x_ц + x_д)} = \underbrace{e^{i2\pi x_ц}}_{1} \cdot e^{i2\pi x_д} = e^{2\pi i x_д}$ $\quad \left\{\begin{array}{l} x_ц \in \mathbb{Z} \\ x_д \in [0, 1) \end{array}\right.$

т.е. $\varphi(x)$ зависит только от др. части $x \Rightarrow$ есть биекция между $\mathbb{R}\backslash\mathbb{Z}$ и S_1.