ФЕДЕРАЛЬНОЕ АГЕНСТВО ВОЗДУШНОГО ТРАНСПОРТА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
"МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ГРАЖДАНСКОЙ АВИАЦИИ"

Кафедра прикладной математики

М.С. Аль-Натор, Ю.Ф. Касимов, В.Л. Кузнецов

АНАЛИТИЧЕСКАЯ ГЕОМЕТРИЯ И ЛИНЕЙНАЯ АЛГЕБРА ПОСОБИЕ

К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

ДЛЯ СТУДЕНТОВ II КУРСА
СПЕЦИАЛЬНОСТИ 230401
ДНЕВНОГО ОБУЧЕНИЯ

Москва-2007

ББК
К

Р е ц е н з е н т: канд.физ.-мат. наук, доц. В.А. Кокотушкин

Аль-Натор М.С., Касимов Ю.Ф., Кузнецов В.Л.

Аналитическая геометрия и линейная алгебра. Пособие к практическим занятиям. – М.: МГТУ ГА, 2007. – 58 с.

Пособие издается в соответствии с учебным планом для студентов II курса специальности 230401 дневного обучения.

Рассмотрено и одобрено на заседаниях кафедры 8.02.2007 г. и методического совета 8.02.2007 г.

1. Целые числа и модульная арифметика

1. Доказать, что если n целое и $n > 1$, то $\text{НОД}\,(n-1, n^2+n+1) = 1$ или 3.
Prove that if n is an integer with $n > 1$, then $\gcd(n-1, n^2+n+1) = 1$ or 3.

Решение. Разделив n^2+n+1 на $n-1$ с остатком (используя деление многочленов уголком), мы получаем частное $n+2$ и остаток 3:

$$n^2 + n + 1 = (n+2)(n-1) + 3.$$

Отсюда видно, что любой общий делитель для $n-1$ и n^2+n+1 должен быть делителем 3, следовательно, НОД должен быть 1 или 3.

2. Пусть $A = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. Доказать, что если n положительное целое, то $A^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ тогда и только тогда, когда n кратно 4 (т.е. $4 \mid n$).

Let $A = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. Prove that if n is a positive integer, then $A^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ if and only if $4 \mid n$.

Решение. Последовательно вычисляя A^2, $A^3 = AA^2$, $A^4 = AA^3$ и т.д., получим

$$A^2 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

$$A^3 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix},$$

$$A^4 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Таким образом, если n кратно 4, т.е. $n = 4q$, то

$$A^n = A^{4q} = (A^4)^q = I^q = I.$$

Обратно, если $A^n = I$, то, используя алгоритм деления с остатком, получим, $n = 4q + r$, где $0 \leqslant r < 4$. Тогда $A^r = A^{n-4q} = A^n(A^{-4})^q = I \cdot I^q = I$, следовательно, $r = 0$, поскольку A^1, A^2, A^3 не равны I . Отсюда заключаем, что n кратно 4.

3. Доказать по индукции, что каждый член последовательности вида $12, 102, 1002, 10002, \ldots$ является кратным 6.

Give a proof by induction to show that each number in the sequence 12, 102, 1002, $10002, \ldots$, is divisible by 6.

Решение. Мы можем записать элементы последовательности в форме $10^n + 2$, для $n = 1, 2, \ldots$. Таким образом, нам нужно доказать следующее утверждение: *для любого положительного целого n, целое число $10^n + 2$ делится на* 6.

Первый шаг проверяет истинность утверждения при $n = 1$. Действительно, 12 кратно 6. Предположим, что утверждение верно при $n = k$. Покажем, что оно верно и при $n = k + 1$. Начнем с предположения , что $10^k + 2$ кратно 6, т.е. $10^k + 2 = 6q$ для некоторого $q \in \mathbb{Z}$, и затем проверим делимость на 6 числа $10^n + 2$, когда $n = k + 1$. Имеем

$$\begin{aligned} 10^{k+1} + 2 &= (10)(10)^k + 2 = (10)(6q - 2) + 2 \\ &= (10)(6q) - 18 = (6)(10q - 3). \end{aligned}$$

Как мы видим, что если $10^k + 2$ делится на 6, то $10^{k+1} + 2$ так же делится на 6. Утверждение доказано.

4. **a)** Используя алгоритм Евклида, найти $\text{НОД}\,(1776, 1492)$.

b) Используя разложение на простые множители 1492 и 1776, найти $\text{НОД}\,(1776, 1492)$.

a) Use the Euclidean algorithm to find $\gcd(1776, 1492)$.

b) Use the prime factorizations of 1492 and 1776 to to find $\gcd(1776, 1492)$.

Решение. a)

$$\begin{aligned} 1776 &= \underline{1492} \cdot 1 + \underline{284}; \\ 1492 &= \underline{284} \cdot 5 + \underline{72}; \\ 284 &= \underline{72} \cdot 3 + \underline{68}; \\ 72 &= \underline{68} \cdot 1 + \underline{4}; \\ 68 &= 4 \cdot 17 + 0. \end{aligned}$$

Таким образом, $\text{НОД}\,(1776, 1492) = 4$.

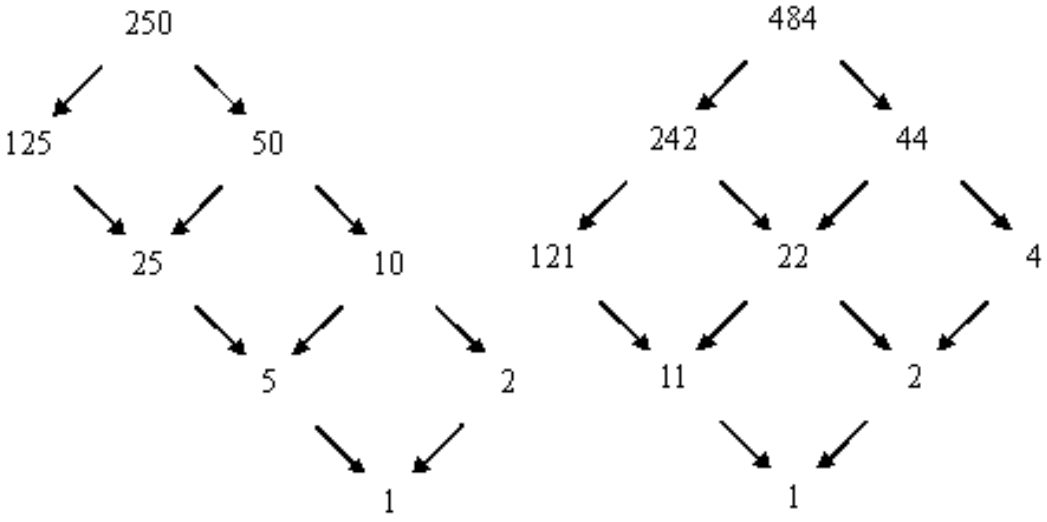
b) Так как $1776 = 2^4 \cdot 3 \cdot 37$ и $1492 = 2^2 \cdot 373$, то

$$\text{НОД}\,(1776, 1492) = 2^{\min(4,2)} \cdot 3^{\min(1,0)} \cdot 373^{\min(1,0)} = 2^2 = 4.$$

5. Построить диаграмму Хассе всех делителей 250. Сделать то же самое для 484.

Give the lattice diagram of all divisors of 250. Do the same for 484.

Решение. Рассмотрим разложение чисел 250 и 484 на простые множители: $250 = 2 \cdot 5^3$, $484 = 2^2 \cdot 11^2$. В каждой диаграмме нам необходимо использовать одну "ось" для каждого простого делителя. Деля (последовательно) исходное число на простые числа, записываем результаты "вдоль соответствующей оси", образуя путь в диаграмме Хассе. К примеру, деление 250 на 5 дает подряд результаты 50, 10 и 2. Эти числа следуют вдоль одной оси диаграммы Хассе.



6. Найти все целочисленные решения уравнения $xy + 2y - 3x = 25$.

Find all integer solutions of the equation $xy + 2y - 3x = 25$.

Решение. Преобразуем это равенство в произведение:

$$xy + 2y - 3x = 25,$$
$$(x + 2)y - 3x - 6 = 25 - 6,$$
$$(x + 2)y - 3(x + 2) = 19,$$
$$(x + 2)(y - 3) = 19.$$

Так как 19 — простое число, то возможны только два способа разложения на множители числа 19: $1 \cdot 19 = 19$ или $(-1) \cdot (-19) = 19$. Поэтому для $x + 2$ возможны 4 варианта: $x + 2 = 1$, $x + 2 = -1$, $x + 2 = 19$ или $x + 2 = -19$. Для каждого из этих значений существует соответствующее значение y, так как второй сомножитель равен $y - 3$. Записывая решение в виде упорядоченной пары (x, y), мы получим четыре решения $(-1, 22)$, $(-3, -16)$, $(17, 4)$ и $(-21, 2)$.

7. Для натуральных a, b доказать, что $\text{НОД}\,(a, b) = 1$, тогда и только тогда, когда $\text{НОД}\,(a^2, b^2) = 1$.

For positive integers a; b, prove that $\gcd(a, b) = 1$ if and only if $\gcd(a^2, b^2) = 1$.

Решение. Напомним, что $\text{НОД}\,(a, bc) = 1$ тогда и только тогда, когда $\text{НОД}\,(a, b) = 1$ и $\text{НОД}\,(a, c) = 1$. В частности, для $c = b$ получим $\text{НОД}\,(a, b^2) = 1$, тогда и только тогда, когда $\text{НОД}\,(a, b) = 1$. Аналогичным образом покажем, что $\text{НОД}\,(a^2, b^2) = 1$, тогда и только тогда, когда $\text{НОД}\,(a, b^2) = 1$.

8. Доказать, что $n - 1$ и $2n - 1$ взамно просты для всех целых $n > 1$. Является ли утверждение истинным для $2n - 1$ и $3n - 1$?

Prove that $n - 1$ and $2n - 1$ are relatively prime, for all integers $n > 1$. Is the same true for $2n - 1$ and $3n - 1$?

Решение. Используя расширенный алгоритм Евклида, находим

$$(1)(2n - 1) + (-2)(n - 1) = 1.$$

Полученное равенство равносильно тому, что $\text{НОД}\,(2n - 1, n - 1) = 1$. Аналогично,

$$(2)(3n - 1) + (-3)(2n - 1) = 1.$$

Таким образом, $\text{НОД}\,(3n - 1, 2n - 1) = 1$.

9. Пусть m и n — положительные целые числа. Доказать, что $\text{НОД}\,(2^m - 1, 2^n - 1) = 1$, тогда и только тогда, когда $\text{НОД}\,(m, n) = 1$.

Let m and n be positive integers. Prove that $\gcd(2^m - 1, 2^n - 1) = 1$ if and only if $\gcd(m, n) = 1$.

Указание. Разобьем доказательство на две части. Сначала докажем, что если $\text{НОД}\,(m, n) = 1$, то $\text{НОД}\,(2^m - 1, 2^n - 1) = 1$. Затем докажем обратное, которое состоит в том, что если $\text{НОД}\,(2^m - 1, 2^n - 1) = 1$, то

$\text{НОД}\,(m,n)=1$. Чтобы доказать это, используем доказательство от противного, предполагая, что $\text{НОД}\,(m,n)\neq 1$ и показывая, что из этого следует, что $\text{НОД}\,(2^m-1,2^n-1)\neq 1$.

Напомним известное тождество

$$x^k-1=(x-1)(x^{k-1}+x^{k-2}+\ldots+x+1). \qquad (*)$$

Решение. Если $\text{НОД}\,(m,n)=1$, то существуют $a,b\in\mathbb{Z}$ такие, что $am+bn=1$. Подставим в $(*)$ $x=2^m$ и $k=a$ и заметим, что 2^m-1 является множителем для $2^{am}-1$, т.е. $2^{am}-1=(2^m-1)(s)$ для некоторого $s\in\mathbb{Z}$. Аналогично можно представить $2^{bn}-1=(2^n-1)(t)$ для некоторого $t\in\mathbb{Z}$. Имеем

$$\begin{aligned}1&=2^1-1\\&=2^{am+bn}-1=2^{bn}(2^{am}-1)+2^{bn}-1\\&=2^{bn}(s)(2^m-1)+(t)(2^n-1)\end{aligned}$$

и так мы имеем линейную комбинацию для 2^m-1 и 2^n-1, равную 1, следовательно, $\text{НОД}\,(2^m-1,2^n-1)=1$.

Если $\text{НОД}\,(m,n)\neq 1$, то $\text{НОД}\,(m,n)=d>1$, следовательно, найдутся такие $p,q\in\mathbb{Z}$, что $m=dq$ и $n=dp$. Как было показано в первой части доказательства, 2^d-1 является общим делителем для $2^{dq}-1$ и $2^{dp}-1$. Следовательно, $\text{НОД}\,(2^m-1,2^n-1)\neq 1$.

10. Доказать, что $\text{НОД}\,(2n^2+6n-4,2n^2+4n-3)=1$ для всех целых $n>1$.

Prove that $\gcd(2n^2+6n-4,2n^2+4n-3)=1$, for all integers $n>1$.

Решение. Воспользуемся алгоритмом Евклида. Деление $2n^2+6n-4$ на $2n^2+4n-3$ дает частное равное 1 и остаток $2n-1$. Следующим шагом является деление $2n^2+4n-3$ на $2n-1$, это дает в частном $n+2$, а в остатке $n-1$. Имеем

$$\begin{aligned}&\text{НОД}\,(2n^2+6n-4,2n^2+4n-3)=\text{НОД}\,(2n^2+4n-3,2n-1)=\\&=\text{НОД}\,(2n-1,n-1)=1,\end{aligned}$$

согласно задаче 8.

11. Найти все идемпотентные элементы в $\mathbb{Z}/(17 \cdot 19) = \mathbb{Z}_{323}$.

Find all idempotent elements in $\mathbb{Z}/(17 \cdot 19) = \mathbb{Z}_{323}$.

Решение. $x \in \mathbb{Z}_{323}$ является идемпотентом, если и только если x удовлетворяет условию $x^2 = x$ в $\mathbb{Z}_{323}$. Это эквивалентно делимости $x^2 - x$ в $\mathbb{Z}$ на $323 = 17 \cdot 19$. Поскольку 17 и 19 взаимно просты это эквивалентно одновременной делимости $x^2 - x$ на 17 и 19, что равносильно выполнению равенств $x^2 = x$ в $\mathbb{Z}_{17}$ и в $\mathbb{Z}_{19}$. Т.к. $\mathbb{Z}_{17}$ и $\mathbb{Z}_{19}$ — поля (17 и 19 являются простыми), то уравнение $x^2 - x = x(x-1) = 0$ имеет в этих полях в точности два корня 0 и 1. Таким образом, элемент x будет идемпотентом в $\mathbb{Z}_{323}$ в одном из четырех случаев:

1) $x = 0$ в $\mathbb{Z}_{17}$ и $\mathbb{Z}_{19}$, т.е. x кратно 17 и 19 одновременно, что равносильно $x = 0$ в $\mathbb{Z}_{323}$.

2) $x = 1$ в $\mathbb{Z}_{17}$ и $\mathbb{Z}_{19}$ т.е. $x - 1$ кратно 17 и 19 одновременно, что равносильно $x - 1 = 0$ в $\mathbb{Z}_{323}$ или $x = 1$ в $\mathbb{Z}_{323}$.

3) $x = 1$ в $\mathbb{Z}_{17}$ и $x = 0$ в $\mathbb{Z}_{19}$. Используя алгоритм Евклида, получаем, что $9 \cdot 17 - 8 \cdot 19 = 1$. Отсюда следует, что $x_1 = -8 \cdot 19 = 171$ удовлетворяет условию 3.

4) $x = 1$ в $\mathbb{Z}_{19}$ и $x = 0$ в $\mathbb{Z}_{17}$. Аналогично предыдущему пункту из равенства $9 \cdot 17 - 8 \cdot 19 = 1$ следует, что $x_2 = 9 \cdot 17 = 153$ удовлетворяет условию 4).

12. Доказать, что в $\mathbb{Z}_{pq}$, где p, q — различные простые числа, нет отличных от нуля нильпотентных элементов.

Show that there are no (non-zero) nilpotent elements in $\mathbb{Z}_{pq}$ for distinct primes p, q.

Решение. Предположим, что x — нильпотентный элемент в $\mathbb{Z}_{pq}$. Тогда для некоторого $n \geq 1$, x^n кратно pq, т.е. x^n делится на pq. Т.к. p, q — простые, это эквивалентно одновременной делимости x^n на p и q. В силу простоты p, q это означает одновременную делимость x на p и q и, значит, делимость x на pq, то есть $x = 0$ в $\mathbb{Z}_{pq}$ и, следовательно, ненулевых нильпотентов в $\mathbb{Z}_{pq}$, нет.

13. Доказать, что нет поля с 35 элементами.

Proof that there is no field with 35 elements.

Решение. Предположим, что $\mathbb{K}$ — поле с pq элементами, где p, q — простые. Применяя теорему Коши к аддитивной группе поля $\mathbb{K}$, получим,

что в $\mathbb{K}$ существует элемент x с аддитивным порядком равным p (т.е. $px = 0$) и элемент y с аддитивным порядком равным q (т.е. $qy = 0$). Конечно, ни x ни y не равны 0, так как аддитивный порядок 0 равен 1.

Пусть $z = xy$. Поскольку $\mathbb{K}$ — поле и $x \neq 0$, $y \neq 0$, то $z \neq 0$. Как обычно, запись nw для целого числа n и $w \in \mathbb{K}$ есть просто сокращение для n-кратного сложения w: $nw = w+w+\ldots+w$. Далее $p(xy) = (px)\cdot y = 0\cdot y = 0$ и $q(xy) = x(qy) = x \cdot 0 = 0$.

Пусть s, t целые числа, такие что $sp + tq = 1$. Тогда

$$xy = 1 \cdot (xy) = (sp + tq) \cdot (xy) = s(px)y + tx(qy) = 0 + 0 = 0,$$

т.е. получили противоречие.

Таким образом, мы доказали, что порядок поля не может делиться на два различных простых числа. Это означает, что порядок любого конечного поля может быть только степенью простого числа.

14. Найти обратные для всех ненулевых элементов из $\mathbb{Z}_7$.

Find the multiplicative inverse of each nonzero element of $\mathbb{Z}_7$.

Решение. Так как $6 \equiv -1 \mod 7$, то вычет $[6]_7$ как $[1]_7$ является обратным для самого себя. Кроме того, из равенств $2\cdot 4 = 8 \equiv 1 \mod 7$ и $3 \cdot 5 = 15 \equiv 1 \mod 7$ следует, что вычеты $[2]_7$ и $[4]_7$; $[3]_7$ и $[5]_7$ — взаимно обратные друг для друга.

15. Найти обратные для всех ненулевых элементов из $\mathbb{Z}_{13}$.

Find the multiplicative inverse of each nonzero element of $\mathbb{Z}_{13}$.

Указание. Если $ab \equiv 1 \mod n$, то $[a]_n$ и $[b]_n$ — взаимно обратные, так же как $[-a]_n$ и $[-b]_n$. Если $ab \equiv -1 \mod n$, то $[a]_n$ и $[-b]_n$, так же как $[-a]_n$ и $[b]_n$ — взаимно обратные друг другу. Таким образом, для нахождения пар взаимно обратных элементов полезно найти целые m, удовлетворяющие условию $m \equiv \pm 1 \mod n$, и рассмотреть их разложение в произведение пары сомножителей.

Решение. Заметим, что числа 14, 27 и 40 дают вычет 1 по модулю 13, а числа 12, 25 и 38 дают вычет -1. Используя разложение $14 = 2\cdot 7$, получаем пару $[2]_{13}$ и $[7]_{13}$ взаимно обратных вычетов. Используя разложение $12 = 3\cdot 4$ и $12 = 2 \cdot 6$, получаем пару $[3]_{13}$ и $[-4]_{13}$, пару $[4]_{13}$ и $[-3]_{13}$ и, наконец, $[6]_{13}$ и $[-2]_{13}$. Используя разложение $40 = 5\cdot 8$, получаем пару $[5]_{13}$ и $[8]_{13}$. В

результате получаем список обратных элементов: $[2]_{13}^{-1} = [7]_{13}$; $[3]_{13}^{-1} = [9]_{13}$; $[4]_{13}^{-1} = [10]_{13}$; $[5]_{13}^{-1} = [8]_{13}$; $[6]_{13}^{-1} = [11]_{13}$; $[12]_{13}^{-1} = [-1]_{13}^{-1} = [-1]_{13} = [12]_{13}$.

16. Найти $[91]_{501}^{-1}$, если он существует в Z_{501}.

Find $[91]_{501}^{-1}$, if possible (in Z_{501}).

Решение. Используя расширенный алгоритм Евклида, получаем

$$\begin{pmatrix} 1 & 0 & 501 \\ 0 & 1 & 91 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -5 & 46 \\ 0 & 1 & 91 \end{pmatrix} \rightsquigarrow$$

$$\begin{pmatrix} 1 & -5 & 46 \\ -1 & 6 & 45 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & -11 & 1 \\ -1 & 6 & 45 \end{pmatrix}.$$

Отсюда получаем $1 = 1 \cdot 501 - 11 \cdot 91$. Таким образом,

$$[91]_{501}^{-1} = [-11]_{501} = [490]_{501}.$$

17. Найти $[3379]_{4061}^{-1}$, если он существует в $\mathbb{Z}_{4061}$.

Find $[3379]_{4061}^{-1}$, if possible (in $\mathbb{Z}_{4061}$).

Решение. Используя расширенный алгоритм Евклида, получаем

$$\begin{pmatrix} 1 & 0 & 4061 \\ 0 & 1 & 3379 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -1 & 682 \\ 0 & 1 & 3379 \end{pmatrix} \rightsquigarrow$$

$$\begin{pmatrix} 1 & -1 & 682 \\ -4 & 5 & 651 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 5 & -6 & 31 \\ -4 & 5 & 651 \end{pmatrix}.$$

Поскольку $31 \mid 651$, то $\text{НОД}\,(4061, 3379) = 31$ и, значит, 4061 и 3379 не взаимно простые, так что $[3379]_{4061}$ необратим в кольце $\mathbb{Z}_{4061}$.

18. Для кольца $\mathbb{Z}_{20}$ найти все обратимые элементы и их обратные, найти все идемпотентные и все нильпотентные элементы.

In $\mathbb{Z}_{20}$ find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.

Указание. Мы знаем, что в кольце $\mathbb{Z}_n$ имеется точно $\varphi(n)$ обратимых элементов, где $\varphi(n)$ — функция Эйлера, равная числу положительных целых чисел меньших n и взаимно простых с ним. Обратимые элементы всегда

парные, т.к. если a — обратимо (т.е. $\text{НОД}(a, n) = 1$), то и $-a$ обратимо (поскольку $\text{НОД}(n - a, n) = 1$).

Решение. Обратимыми элементами в $\mathbb{Z}_{20}$ являются вычеты: 1, 3, 7, 9, 11, 13, 17 и 19. При этом: $[3]_{20}^{-1} = [7]_{20}$, $[9]_{20}^{-1} = [9]_{20}$, $[11]_{20}^{-1} = [11]_{20}$, $[13]_{20}^{-1} = [17]_{20}$ и $[19]_{20}^{-1} = [19]_{20}$.

Идемпотентные элементы в $\mathbb{Z}_{20}$ (т.е. элементы, удовлетворяющие уравнению $x^2 = x$) можно найти методом проб и ошибок. Перебирая последовательно все вычеты от 0 до 19, получим список идемпотентов: $[0]_{20}$, $[1]_{20}$, $[5]_{20}$ и $[16]_{20}$. Более систематический поиск идемпотентных элементов основан на следующем замечании: если $n = bc$ и $\text{НОД}(b, c) = 1$, то вычеты, удовлетворяющие сравнениям $x \equiv 1 \mod b$ и $x \equiv 0 \mod c$, будут идемпотентами по модулю n.

Нильпотентные элементы из $\mathbb{Z}_{20}$ также могут быть найдены перебором. В $\mathbb{Z}_{20}$ их всего 2: $[0]_{20}$ и $[10]_{20}$.

19. Доказать, что $10^{n+1} + 4 \cdot 10^n + 4$ делится на 9 для всех положительных целых n.

Prove that $10^{n+1} + 4 \cdot 10^n + 4$ is divisible by 9, for all positive integers n.

Решение. Это утверждение может быть доказано индукцией по n, но более простое доказательство получается, если заметить, что $10^{n+1} + 4 \cdot 10^n + 4 \equiv 0 \mod 9$, так как $10 \equiv 1 \mod 9$.

20. Доказать, что четвертая степень любого целого числа в качестве числа единиц может иметь только 0, 1, 5 или 6.

Prove that the fourth power of an integer can only have 0, 1, 5, or 6 as its units digit.

Решение. Число единиц целого числа есть наименьший неотрицательный вычет этого числа по модулю 10. Следовательно, необходимо найти $n^4 \mod 10$. Вычисляя последовательно, получим: $0^4 = 0$, $(\pm 1)^4 = 1$, $(\pm 2)^4 = 16 \equiv 6 \mod 10$, $(\pm 3)^4 = 81 \equiv 1 \mod 10$, $(\pm 4)^4 \equiv 6^2 \equiv 6 \mod 10$ и $5^4 \equiv 5^2 \equiv 5 \mod 10$. Это и показывает, что возможными единицами для n^4 являются 0, 1, 5 и 6.

21. Решить уравнение $[x]_{11}^2 + [x]_{11} - [6]_{11} = [0]_{11}$ в $\mathbb{Z}_{11}$.

Solve the equation $[x]_{11}^2 + [x]_{11} - [6]_{11} = [0]_{11}$ in $\mathbb{Z}_{11}$.

Решение. Разлагая на множители, получим $[x]^2 + [x] - [6] = ([x] + [3])([x] - [2])$.

Поскольку $\mathbb{Z}_{11}$ — поле, то в нем нет делителей нуля и, значит, наше уравнение распадается на два линейных: $[x]+[3]=0$ или $[x]-[2]=0$. В итоге получаем решение $[x]=[-3]=[8]$ или $[x]=[2]$.

22. Пусть $n \in \mathbb{N}$ и $a \in \mathbb{Z}$ — взаимно простые. Доказать, что если m — наименьшее положительное целое, для которого $a^m \equiv 1 \mod n$, то $\varphi(n)$ делится на m.

Let n be a positive integer, and let $a \in \mathbb{Z}$ with $\gcd(a,n)=1$ (a and n are relatively prime). Prove that if m is the smallest positive integer for which $a^m \equiv 1 \mod n$, then $\varphi(n)$ is divisible by m.

Решение. Напомним, что $\varphi(n)$ — порядок группы всех обратимых элементов кольца $\mathbb{Z}_n$, он равен числу положительных целых меньших n и взаимно простых с ним (поскольку именно эти и только эти вычеты обратимы по модулю n). Сравнение $a^m \equiv 1 \mod n$ влечет обратимость a, а тот факт, что m наименьшее положительное целое, для которого $a^m \equiv 1 \mod n$, означает, что m — мультипликативный порядок элемента a. По теореме Лагранжа порядок элемента группы является делителем порядка группы. Следовательно, $\varphi(n)$ делится на m.

23. Доказать, что $[a]_n$ — нильпотентный элемент кольца $\mathbb{Z}_n$, тогда и только тогда, когда каждый простой делитель n является делителем a.

Prove that $[a]_n$ is a nilpotent element of $\mathbb{Z}_n$ if and only if each prime divisor of n is a divisor of a.

Решение. Предположим сначала, что каждый простой делитель n является делителем a. Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ — разложение n на простые множители, тогда мы должны иметь $a = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t} d$, где $0 \leqslant \beta_j \leqslant \alpha_j$ для всех j. Если k — наименьшее положительное целое, такое что $k\beta_i \geqslant \alpha_i$ для всех i, то a^k делится на n и, значит, $[a]_n^k = [0]_n$, т.е $[a]_n$ — нильпотентный элемент $\mathbb{Z}_n$.

Обратно, если $[a]_n^k = [0]_n$ для некоторого k, тогда a^k делится на n и, значит, каждый простой делитель n есть делитель a^k, а также делитель a.

24. Решить сравнение $42x \equiv 12 \mod 90$.

Solve the congruence $42x \equiv 12 \mod 90$.

Решение. Т.к. $\text{НОД}\,(42, 90) = 6$ и 12 делится на 6, то существует ровно 6 решений. Данное сравнение эквивалентно уравнению $42x = 12 + 90q$

для целых x и q. Сокращая на 6, получим $7x = 2 + 15q$ или $7x \equiv 2 \mod 15$. Простым перебором найдем 7^{-1} по модулю 15. Числа, дающие в остатке 1 по модулю 15, — это числа $16, 31, 46, 61, \ldots$ и $-14, -29, -34, \ldots$. Среди них на 7 делится -14, т.е. $7^{-1} = -2$ по модулю 15. Умножая обе стороны сравнения $7x \equiv 2 \mod 15$ на -2, получим $-14x \equiv -4 \mod 15$ или $x \equiv 11 \mod 15$. Итак, $x \equiv 11, 26, 41, 56, 71, 86 \mod 90$.

25. a) Найти все решения сравнения $55x \equiv 35 \mod 75$.

Find all solutions to the congruence $55x \equiv 35 \mod 75$.

Решение. Мы имеем $\text{НОД}(55, 75) = 5$, и т.к. 5 является делителем 35, то сравнение имеет 5 решений. Последовательно получаем (делением на 5 и умножением на $11^{-1} = -4$ по модулю 15)

$$\begin{aligned} 55x &\equiv 35 \mod 75; \\ 11x &\equiv 7 \mod 15; \\ -44x &\equiv -28 \mod 15; \\ x &\equiv -13 \mod 15; \\ x &\equiv 2 \mod 15. \end{aligned}$$

Следовательно, $x \equiv 2, 17, 32, 47, 62 \mod 75$.

b) Найти все решения сравнения $55x \equiv 36 \mod 75$.

Find all solutions to the congruence $55x \equiv 36 \mod 75$.

Решение. Это сравнение не имеет решений, т.к. $\text{НОД}(55, 75) = 5$, а 36 не делится на 5.

26. a) Найти какое-нибудь целое решение уравнения $110x + 75y = 45$.

Find one particular integer solution to the equation $110x + 75y = 45$.

Решение. Найдем $\text{НОД}(110, 75)$ в виде линейной комбинации 110 и 75 матричным методом:

$$\begin{pmatrix} 1 & 0 & 110 \\ 0 & 1 & 75 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -1 & 35 \\ 0 & 1 & 75 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -1 & 35 \\ -2 & 3 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 15 & -22 & 0 \\ -2 & 3 & 5 \end{pmatrix}.$$

Таким образом, $-2(110) + 3(75) = 5$. Умножив это равенство на 9, получим решение $x = -18$, $y = 27$.

Комментарий. Матричное вычисление показывает, что

$$110(15) + 75(-22) = 0,$$

так что добавляя любое кратное вектора $(15, -22)$ к решению $(-18, 27)$, получим новое решение.

2-ое решение. Наше уравнение равносильно следующему сравнению $35x \equiv 45 \mod 75$. Деление на 5 приводит к сравнению $7x \equiv 9 \mod 15$, а умножение на -2 дает $x \equiv -3 \mod 15$ или $x = -3 + 15n$. Следовательно, $75y = 45 + 3(110) = 375$, и в результате получаем решение $x = -3$, $y = 5$.

b) Показать, что если $x = m$ и $y = n$ — целочисленное решение уравнения $110x + 75y = 45$, то $x = m + 15q$ и $y = n - 22q$ — тоже решение для любого $q \in \mathbb{Z}$.

Show that if $x = m$ and $y = n$ is an integer solution to the equation $110x + 75y = 45$, then so is $x = m + 15q$ and $y = n - 22q$, for any integer q.

Решение. Если $110m + 75n = 45$, тогда

$$110(m + 15q) + 75(n - 22q) = 45 + 110(15)q + 75(-22)q = 45,$$

т.к. $110(15) - 75(22) = 0$.

27. Решить систему сравнений $x \equiv 2 \mod 9$, $x \equiv 4 \mod 10$.

Solve the system of congruences $x \equiv 2 \mod 9$, $x \equiv 4 \mod 10$.

Решение. Преобразовав второе сравнение в выражение $x = 4 + 10q$, где $q \in \mathbb{Z}$, и подставив в первое, получим $4 + 10q \equiv 2 \mod 9$, что в свою очередь приводится к $q \equiv 7 \mod 9$. Таким образом, $x \equiv 74 \mod 90$ — решение системы.

28. Решить систему сравнений $5x \equiv 14 \mod 17$, $3x \equiv 2 \mod 13$.

Solve the system of congruences $5x \equiv 14 \mod 17$, $3x \equiv 2 \mod 13$.

Решение. Т.к. $7 \cdot 5 \equiv 1 \mod 17$, то, умножая первое сравнение на 7, получим $35x \equiv 98 \mod 17$ и, значит, $x \equiv 13 \mod 17$.

Аналогично, учитывая, что $9 \cdot 3 \equiv 1 \mod 13$, получим из второго сравнения $27x \equiv 18 \mod 13$ или $x \equiv 5 \mod 13$. Полученную упрощенную систему можно решить обычным образом. Переписывая первое сравнение в виде $x = 13 + 17q$ для некоторого $q \in \mathbb{Z}$ и подставляя в левую часть

второго, получим $13 + 17q \equiv 5 \mod 13$. Последнее сравнение приводится к виду $4q \equiv 5 \mod 13$, умножая которое на $10 = 4^{-1}$ по модулю 13, получим $40q \equiv 50 \mod 13$ или $q \equiv 11 \mod 13$. Это приводит в итоге к ответу $x \equiv 13 + 17 \cdot 11 \equiv 200 \mod 221$.

29. Решить систему сравнений $x \equiv 5 \mod 25$, $x \equiv 23 \mod 32$.

Solve the system of congruences $x \equiv 5 \mod 25$, $x \equiv 23 \mod 32$.

Решение. Из второго сравнения получаем $x = 23 + 32q$ для некоторого $q \in \mathbb{Z}$. Подставляя полученное выражение для x в первое сравнение, находим $23 + 32q \equiv 5 \mod 25$, которое приводит к $7q \equiv 7 \mod 25$, так что $q \equiv 1 \mod 15$. Следовательно, $x \equiv 55 \mod 25 \cdot 32$.

30. Найти целые числа a, b, m, n такие, чтобы система

$$x \equiv a \mod m, \quad x \equiv b \mod n$$

не имела решений.

Give integers a, b, m, n to provide an example of a system

$$x \equiv a \mod m, \quad x \equiv b \mod n$$

that has no solution.

Решение. Целые m и n не могут быть взаимно простыми. Это ключ к решению. Положим $m = n = 2$, $a = 1$ и $b = 0$.

31. a) Найти последнюю цифру числа 4^{100} в десятичном представлении.

Compute the last digit in the decimal expansion of 4^{100}.

Решение. Последняя цифра — это остаток деления 4^{100} на 10, т.е. $4^{100} \mod 10$. Имеем $4^2 \equiv 6 \mod 10$ и $6^2 \equiv 6 \mod 10$. Следовательно, $4^{100} = (4^2)^{50} \equiv 6^{50} \equiv 6 \mod 10$.

b) Делится ли число 4^{100} на 3?

Is 4^{100} divisible by 3?

Решение. Нет. В самом деле $4^{100} \equiv 1^{100} \equiv 1 \mod 3$.

Другое решение. $4^{100} = 2^{200}$ — разложение 4^{100} на простые множители. Тогда $\text{НОД}(3, 2^{200}) = 1$ и, значит, число 4^{100} не делится на 3.

32. Найти все целые n, для которых $4(n^2 + 1)$ делится на 13.

Find all integers n for which $13 \mid 4(n^2 + 1)$.

Решение. Задача эквивалентна решению следующего сравнения: $4(n^2+1) \equiv 0 \mod 13$. Поскольку $\text{НОД}(4,13) = 1$, то, сокращая на 4, получим $n^2 \equiv -1 \mod 13$. Далее находим все квадраты вычетов по модулю 13. Имеем $(\pm 1)^2 \equiv 1 \mod 13$, $(\pm 2)^2 \equiv 4 \mod 13$, $(\pm 3)^2 \equiv 9 \mod 13$, $(\pm 4)^2 \equiv 3 \mod 13$, $(\pm 5)^2 \equiv -1 \mod 13$ и $(\pm 6)^2 \equiv -3 \mod 13$. Отсюда получаем ответ: $x \equiv \pm 5 \mod 13$.

33. Найти $\text{НОД}(7605, 5733)$ и выразить его как линейную комбинацию 7605 и 5733.

Find $\gcd(7605, 5733)$, and express it as a linear combination of 7605 and 5733.

Решение. Используя матричную форму алгоритма Евклида, получим

$$\begin{pmatrix} 1 & 0 & 7605 \\ 0 & 1 & 5733 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -1 & 1872 \\ 0 & 1 & 5733 \end{pmatrix} \rightsquigarrow$$

$$\rightsquigarrow \begin{pmatrix} 1 & -1 & 1872 \\ -3 & 4 & 117 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 49 & -65 & 0 \\ -3 & 4 & 117 \end{pmatrix}.$$

Таким образом, $\text{НОД}(7605, 5733) = 117$ и $117 = (-3) \cdot 7605 + 4 \cdot 5733$.

34. Пусть $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Доказать, что $w^n = 1$ для целого n, если и только если n делится на 3.

For $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, prove that $w^n = 1$ if and only if n is divisible by 3.

Решение. Запишем w в тригонометрической форме:

$$w = \cos(2\pi/3) + i\sin(2\pi/3).$$

Используя формулу Муавра, получим

$$w^2 = \cos(4\pi/3) + i\sin(4\pi/3) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i, \quad w^3 = 1.$$

Если $n \in \mathbb{Z}$ и n делится на 3, то $n = 3q$ для некоторого $q \in \mathbb{Z}$. Тогда

$$w^n = w^{3q} = (w^3)^q = 1^q = 1.$$

Обратно, если $n \in \mathbb{Z}$ и $w^n = 1$, то, используя алгоритм деления с остатком, получим $n = q \cdot 3 + r$, где $0 \leqslant r < 3$. Тогда

$$1 = w^n = w^{3q+r} = (w^3)^q w^r = w^r.$$

Т.к. $r = 0, 1, 2$, и $w \neq 1$ и $w^2 \neq 1$, то $r = 0$, и поэтому n делится на 3.

35. Решить сравнение $24x \equiv 168 \mod 200$.

Solve the congruence $24x \equiv 168 \mod 200$.

Решение. Заметим, что $\text{НОД}(24, 200) = 8$. Поскольку 168 делится на 8, сравнение имеет 8 решений. Сокращая на 8 обе части сравнения и модуль 200, получим новое эквивалентное сравнение $3x \equiv 21 \mod 25$. Чтобы решить это сравнение, нужно найти мультипликативный обратный для коэффициента 3 по модулю 25. Перебором устанавливаем, что $3^{-1} \equiv -8 \equiv 17 \mod 25$. Умножая обе части сравнения на -8, получим

$$\begin{aligned} -24x &\equiv -168 \mod 25, \\ x &\equiv 7 \mod 25. \end{aligned}$$

Ответ: $x \equiv 7, 32, 57, 82, 107, 132, 157, 182 \mod 200$.

36. Решить систему сравнений

$$\begin{cases} 2x \equiv 9 \mod 15; \\ x \equiv 8 \mod 11. \end{cases}$$

Solve the system of congruences $\begin{cases} 2x \equiv 9 \mod 15; \\ x \equiv 8 \mod 11. \end{cases}$

Решение. Из второго сравнения представим x в виде $x = 8 + 11q$ для некоторого $q \in \mathbb{Z}$ и подставим это выражение в первое сравнение. Получим сравнение вида $16 + 22q \equiv 9 \mod 15$, упрощая которое находим $7q \equiv -7 \mod 15$ или $q \equiv -1 \mod 15$. Это дает $x \equiv -3 \mod 11 \cdot 15$.

37. Выписать все элементы из $\mathbb{Z}_{15}^*$. Для каждого элемента найти его мультипликативный обратный и найти его мультипликативный порядок.

List the elements of $\mathbb{Z}_{15}^*$. For each element, find its multiplicative inverse, and find its multiplicative order.

Решение. Поскольку $\varphi(15) = 8$, в группе Z_{15}^* должно быть 8 элементов: $[1]$, $[2]$, $[4]$, $[7]$, $[8]$, $[11]$, $[13]$ и $[14]$. Мультипликативный порядок любого неединичного элемента равен 2, 4, или 8. Имеем $[2]^2 = [4]$, $[2]^3 = [8]$ и $[2]^4 = [1]$. Это показывает не только, что мультипликативный порядок $[2]$ равен 4, но и что мультипликативный порядок $[4]$ равен 2. Заметим,

что $[2]^{-1} = [8]$ и $[4]^{-1} = [4]$. Поскольку $[13] = [-2]$, то $[13]$ имеет мультипликативный порядок 4 и $[13]^{-1} = [-2]^{-1} = [-8] = [7]$. Аналогично, $[11]^{-1} = [-4]^{-1} = [-4] = [11]$. Наконец, $[7]^2 = [4]$, $[7]^4 = [4]^2 = [1]$, следовательно, мультипликативный порядок $[7]$ равен 4.

Чтобы вычислить мультипликативный порядок $[8]$, запишем его как $[2]^3$. Ясно, что первое положительное целое k, для которого $([2]^3)^k = [1]$ — это $k = 4$, т.к. $3k$ должно делиться на 4. (Это также можно показать, представив $[8]$ как $[-7]$.) Аналогично, $[11] = [-4]$ имеет мультипликативный порядок 2, и $[13] = [-2]$ имеет мультипликативный порядок 4.

2. Отношения и функции

1. Во множестве всех упорядоченных пар натуральных чисел

$$\mathbb{N} \times \mathbb{N} = \{(a, b) \,|\, a,\, b \in \mathbb{N}\}$$

определим отношение $(a_1, b_1) \sim (a_2, b_2)$, если $a_1 b_2 = a_2 b_1$. Показать, что $\sim$ есть отношение эквивалентности.

On the set $\mathbb{N} \times \mathbb{N} = \{(a, b) \,|\, a,\, b \in \mathbb{N}\}$, of all ordered pairs of natural numbers, define $(a_1, b_1) \sim (a_2, b_2)$ if $a_1 b_2 = a_2 b_1$. Show that this defines an equivalence relation.

Решение. *Рефлексивность* $\sim$. Для произвольной пары (a, b) имеем $ab = ba$ и, таким образом, $(a, b) \sim (a, b)$.

Симметричность $\sim$. Пусть $(a_1, b_1) \sim (a_2, b_2)$, т.е. имеем $a_1 b_2 = a_2 b_1$, тогда $a_2 b_1 = a_1 b_2$, что означает $(a_2, b_2) \sim (a_1, b_1)$.

Транзитивность $\sim$. Пусть $(a_1, b_1) \sim (a_2, b_2)$ и $(a_2, b_2) \sim (a_3, b_3)$, тогда $a_1 b_2 = a_2 b_1$ и $a_2 b_3 = a_3 b_2$. Умножая первое равенство на b_3, а второе на b_1, получим $a_1 b_2 b_3 = a_2 b_1 b_3 = a_3 b_1 b_2$. Поскольку $b_2 \neq 0$, то $a_1 b_3 = a_3 b_1$, что доказывает, что $(a_1, b_1) \sim (a_3, b_3)$.

2. Во множестве $\mathbb{C}$ комплексных чисел определено $z_1 \sim z_2$, если $|z_1| = |z_2|$. Показать, что $\sim$ есть отношение эквивалентности.

On the set $\mathbb{C}$ of complex numbers, define $z_1 \sim z_2$ if $|z_1| = |z_2|$. Show that $\sim$ is an equivalence relation.

Решение. Рефлексивность, симметричность и транзитивность легко проверяются, поскольку $\sim$ определено с помощью равенства, а равенство очевидно является отношением эквивалентности.

3. Пусть $u = (u_1, u_2, u_3)$ — фиксированный вектор из $\mathbb{R}^3$. Предположим, что его длина $|u| = \sqrt{u_1^2 + u_2^2 + u_3^2}$ равна 1. Определим отношение на $\mathbb{R}^3$ следующим образом: для любых двух векторов v и w положим $v \sim w$, если $(v, u) = (w, u)$, где $(\cdot, \cdot)$ обозначает стандартное скалярное произведение. Показать, что $\sim$ есть отношение эквивалентности и дать геометрическое описание классов эквивалентности $\sim$.

Let $u = (u_1, u_2, u_3)$ be a fixed vector in $\mathbb{R}^3$, and assume that u has length 1. For vectors v and w, define $v \sim w$ if $(v, u) = (w, u)$, where $(\cdot, \cdot)$ denotes the standard dot product. Show that $\sim$ is an equivalence relation, and give a geometric description of the equivalence classes of $\sim$.

Решение. Рефлексивность, симметричность и транзитивность отношения $\sim$ легко проверить. Поскольку длина u равна 1, (v, u) представляет длину проекции v на ось, определенную u. Таким образом, два вектора v и w эквивалентны тогда и только тогда, когда они лежат в одной плоскости, перпендикулярной u. Отсюда следует, что классы эквивалентности $\sim$ это плоскости в $\mathbb{R}^3$, перпендикулярные u.

4. Для функции $f : \mathbb{R} \to \mathbb{R}$, где $f(x) = x^2$ описать отношение ядерной эквивалентности на $\mathbb{R}$, определенной функцией f.

For the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$, describe the equivalence relation on $\mathbb{R}$ that is determined by f.

Решение. Ядерная эквивалентность, определенная функцией f, есть отношение эквивалентности вида: $a \sim b$, если $f(a) = f(b)$. В данном случае $a \sim b$ тогда и только тогда, когда $a^2 = b^2$ или $a \sim b$ тогда и только тогда, когда $|a| = |b|$.

5. Для линейного преобразования $L : \mathbb{R}^3 \to \mathbb{R}^3$, определенного соотношением $L(x, y, z) = (x + y + z, x + y + z, x + y + z)$ для всех $(x, y, z) \in \mathbb{R}^3$, дать геометрическое описание классов эквивалентности в $\mathbb{R}^3$, определенных преобразованием L.

For the linear transformation $L : \mathbb{R}^3 \to \mathbb{R}^3$ defined by $L(x, y, z) = (x + y + z, x + y + z, x + y + z)$, for all $(x, y, z) \in \mathbb{R}^3$, give a geometric description of the partition of $\mathbb{R}^3$ that is determined by L.

Решение. Т.к. $(a_1, a_2, a_3) \sim (b_1, b_2, b_3)$ при $L(a_1, a_2, a_3) = L(b_1, b_2, b_3)$, то из определения L следует, что $(a_1, a_2, a_3) \sim (b_1, b_2, b_3)$ тогда и только тогда, когда $a_1+a_2+a_3 = b_1+b_2+b_3$. Например, $\{(x, y, z)|L(x, y, z) = (0, 0, 0)\}$ — плоскость, задаваемая уравнением $x+y+z = 0$ с нормальным вектором $(1, 1, 1)$. Другие классы эквивалентности в $\mathbb{R}^3$ — это плоскости, параллельные этой. Таким образом, фактор-множество ядерной эквивалентности, порожденной преобразованием L, состоит из плоскостей, перпендикулярных вектору $(1, 1, 1)$.

6. Определим отображение $f : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ формулой $f([x]_{12}) = [x]^2_{12}$ для всех $[x]_{12} \in \mathbb{Z}_{12}$. Показать, что формула f определяет функцию. Найти образ f и множество $\mathbb{Z}_{12}/f$ классов эквивалентности, порожденных f.

Define the formula $f : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ by $f([x]_{12}) = [x]^2_{12}$, for all $[x]_{12} \in \mathbb{Z}_{12}$. Show that the formula f defines a function. Find the image of f and the set $\mathbb{Z}_{12}/f$ of equivalence classes

determined by f.

Решение. Функция f корректно определена, т.к. если $[x]_{12} = [y]_{12}$, то $x \equiv y \mod 12$, а тогда $x^2 \equiv y^2 \mod 12$, т.е. $f([x]_{12}) = f([y]_{12})$.

Образ f находим, последовательно возводя в квадрат все вычеты из $\mathbb{Z}_{12}$: $[0]_{12}^2 = [0]_{12}$, $[\pm 1]_{12}^2 = [1]_{12}$, $[\pm 2]_{12}^2 = [4]_{12}$, $[\pm 3]_{12}^2 = [9]_{12}$, $[\pm 4]_{12}^2 = [4]_{12}$, $[\pm 5]_{12}^2 = [1]_{12}$, и $[6]_{12}^2 = [0]_{12}$. Таким образом, $f(\mathbb{Z}_{12}) = \{[0]_{12}, [1]_{12}, [4]_{12}, [9]_{12}\}$. Классы эквивалентности, определенные f $\{[0]_{12}, [6]\}$, $\{[\pm 1]_{12}, [\pm 5]_{12}\}$, $\{[\pm 2]_{12}, [\pm 4]_{12}\}$, $\{[\pm 3]_{12}\}$.

7. Во множестве всех $n \times n$ матриц над $\mathbb{R}$ определим отношение: $A \sim B$, если существует обратимая матрица P, такая что $PAP^{-1} = B$. Проверить, что $\sim$ есть отношение эквивалентности.

On the set of all $n \times n$ matrices over $\mathbb{R}$, define $A \sim B$ if there exists an invertible matrix P such that $PAP^{-1} = B$. Check that $\sim$ defines an equivalence relation.

Решение. *Рефлексивность*. Имеем $A \sim A$, поскольку $IAI^{-1} = A$, где I — это единичная $n \times n$ матрица.

Симметричность. Если $A \sim B$, то $PAP^{-1} = B$ для некоторой обратимой матрицы P, а тогда $A = P^{-1}B(P^{-1})^{-1}$, т.е. $B \sim A$.

Транзитивность. Если $A \sim B$ и $B \sim C$, то $PAP^{-1} = B$ и $QBQ^{-1} = C$ для некоторых обратимых матриц P и Q. Но тогда

$$Q(PAP^{-1})Q^{-1} = (QP)A(QP)^{-1} = C$$

и, следовательно, $A \sim C$.

3. Многочлены над полем

1. Используя алгоритм Евклида, найти $\text{НОД}\,(x^8-1, x^6-1)$ в $\mathbb{Q}[x]$ и записать его в виде линейной комбинации x^8-1 и x^6-1.

Use the Euclidean algorithm to find $\gcd(x^8-1, x^6-1)$ in $\mathbb{Q}[x]$ and write it as a linear combination of x^8-1 and x^6-1.

Решение. Положим $x^8-1=f(x)$ и $x^6-1=g(x)$. Деля с остатком, получим $f(x)=x^2g(x)+(x^2-1)$ и $g(x)=(x^4+x^2+1)(x^2-1)$. Следовательно, $\text{НОД}\,(x^8-1, x^6-1)=x^2-1$ и $x^2-1=f(x)-x^2g(x)$.

2. Используя алгоритм Евклида, показать, что в кольце $\mathbb{Q}[x]$ многочленов с рациональными коэффициентами многочлены $2x^3-2x^2-3x+1$ и $2x^2-x-2$ взаимно простые.

Over the field of rational numbers $\mathbb{Q}$, use the Euclidean algorithm to show that $2x^3-2x^2-3x+1$ and $2x^2-x-2$ are relatively prime.

Решение. Положим $2x^3-2x^2-3x+1=f(x)$ и $2x^2-x-2=g(x)$. Деля с остатком, получим $f(x)=(x-1/2)g(x)-(3/2)x$. Умножая обе части на 2, получим $2f(x)=(2x-1)g(x)-3x$, откуда следует, что $\text{НОД}\,(f,g)=1$.

3. Найти в $\mathbb{Q}[x]$ наибольший общий делитель $x^4+x^3+2x^2+1$ и x^3-1 и записать его в виде линейной комбинации этих многочленов.

Over the field of rational numbers, find the greatest common divisor of $x^4+x^3+2x^2+1$ and x^3-1, and express it as a linear combination of the given polynomials.

Решение. Положим $x^4+x^3+2x^2+1=f(x)$, $x^3-1=g(x)$. Деля с остатком $f(x)$ на $g(x)$, получим $f(x)=(x+1)g(x)+2(x^2+x+1)$, затем деля $g(x)$ на x^2+x+1, получим $g(x)=(x-1)(x^2+x+1)$, откуда

$$\text{НОД}\,(f(x),g(x))=x^2+x+1 \text{ и } x^2+x+1=\tfrac{1}{2}f(x)-\tfrac{1}{2}(x+1)g(x).$$

4. Найти в $\mathbb{Q}[x]$ наибольший общий делитель $2x^4-x^3+x^2+3x+1$ и $2x^3-3x^2+2x+2$ и записать его в виде линейной комбинации этих многочленов.

Over the field of rational numbers, find the greatest common divisor of $2x^4-x^3+x^2+3x+1$ and $2x^3-3x^2+2x+2$, and express it as a linear combination of the given polynomials.

Решение. Положим $2x^4-x^3+x^2+3x+1=f(x)$ и $2x^3-3x^2+2x+2=g(x)$. Используя алгоритм Евклида, последовательно получаем

$f(x) = (x+1)g(x) + (2x^2 - x - 1)$,
$g(x) = (x-1)(2x^2 - x - 1) + (2x+1)$,
$2x^2 - x - 1 = (x-1)(2x+1)$.
Следовательно, $x + 1/2$ — это наибольший общий делитель $f(x)$ и $g(x)$.

Начиная с последнего равенства и двигаясь вверх, получим:

$$\begin{aligned} 2x+1 &= g(x) - (x-1)(2x^2 - x - 1) = \\ &= g(x) - (x-1)[f(x) - (x+1)g(x)] \\ &= g(x) + (x^2-1)g(x) - (x-1)f(x) = x^2 g(x) - (x-1)f(x). \end{aligned}$$

Это дает окончательный ответ:

$$x + \frac{1}{2} = \frac{1}{2}x^2 g(x) + \Big(-\frac{1}{2}\Big)(x-1)f(x).$$

5. Определить, являются ли приводимыми над $\mathbb{Q}$ следующие многочлены:
a) $3x^5 + 18x^2 + 24x + 6$,
b) $7x^3 + 12x^2 + 3x + 45$,
c). $2x^{10} + 25x^3 + 10x^2 - 30$.
Are the following polynomials irreducible over $\mathbb{Q}$?
a) $3x^5 + 18x^2 + 24x + 6$,
b) $7x^3 + 12x^2 + 3x + 45$,
c). $2x^{10} + 25x^3 + 10x^2 - 30$.

Решение. a) Разделив многочлен на 3, мы получим многочлен $x^5 + 6x^2 + 8x + 2$, удовлетворяющий критерию Эйзенштейна для $p = 2$. Следовательно, $3x^5 + 18x^2 + 24x + 6$ неприводим.

b) Преобразуем этот многочлен в многочлен $x^3 + x + 1$ из $\mathbb{Z}_2[x]$, приводя целые коэффициенты к их вычетам по модулю 2. Многочлен $x^3 + x + 1$ неприводим в $\mathbb{Z}_2[x]$, поскольку он не имеет корней. Следовательно, неприводимым будет $7x^3 + 12x^2 + 3x + 45$.

c) Многочлен удовлетворяет критерию Эйзенштейна для $p = 5$.

6. Разложить на множители $f(x) = x^5 - 10x^4 + 24x^3 + 9x^2 + 33x - 12$ в $\mathbb{Q}(x)$.
Factor $f(x) = x^5 - 10x^4 + 24x^3 + 9x^2 + 33x - 12$ over $\mathbb{Q}$.

Решение. Методом проб делителей свободного члена найдем рациональные (целые) корни $f(x)$. Делители 12 есть ± 1, ± 2, ± 3, ± 4, ± 6, ± 12.

Т.к. $f(1) = 21$, то для любого корня z число 21 делится на $(z-1)$. Таким образом, остаются возможности ± 2, 4, -6. Далее $f(2) = 32$, $f(-2) = -294$ и, наконец, $f(4) = 0$. Отделяя этот корень, получим $f(x) = (x-4)(x^4 - 6x^3 + 9x + 3)$.

Второй множитель неприводим в $\mathbb{Q}(x)$, поскольку удовлетворяет критерию Эйзенштейна для $p = 3$.

7. Найти $\text{НОД}\,(x^2 + x + 1, x^4 + x^3 + x + 1)$ в $\mathbb{Z}_2[x]$.

Find the greatest common divisor of $x^2 + x + 1$ and $x^4 + x^3 + x + 1$ in $\mathbb{Z}_2[x]$.

Решение. Для нахождения НОД используем алгоритм Евклида для многочленов. Деля $x^4 + x^3 + x + 1$ на $x^2 + x + 1$ "уголком", получим:

$$\begin{array}{l|l} x^4 + x^3 + x + 1 & \underline{x^2 + x + 1} \\ \underline{x^4 + x^3 + x^2} & x^2 + 1 \\ \quad x^2 + x + 1 & \\ \quad \underline{x^2 + x + 1} & \\ \quad\quad 0 & \end{array}$$

Таким образом, $x^4 + x^3 + x + 1$ делится на $x^2 + x + 1$:

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

и, следовательно, $\text{НОД}\,(x^2 + x + 1, x^4 + x^3 + x + 1) = (x^2 + x + 1)$.

8. Найти $\text{НОД}\ (x^2 + x + 1)$ и $(x^4 + x^3 + x + 1)$ в $\mathbb{Z}_3[x]$.

Find the greatest common divisor of $x^2 + x + 1$ and $x^4 + x^3 + x + 1$ in $\mathbb{Z}_3[x]$.

Решение. Для нахождения НОД используем алгоритм Евклида для многочленов. Деля $x^4 + x^3 + x + 1$ на $x^2 + x + 1$ "уголком", получим

$$\begin{array}{l|l} x^4 + x^3 + x + 1 & \underline{x^2 + x + 1} \\ \underline{x^4 + x^3 + x^2} & x^2 - 1 \\ -x^2 + x + 1 & \\ \underline{-x^2 - x - 1} & \\ -x - 1 & \end{array}$$

Таким образом, получаем

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

Теперь, деля x^2+x+1 на $x+1$, получим

$$\begin{array}{ll} x^2+x+1 & \big|\underline{x+1} \\ \underline{x^2+x} & x \\ 1 & \end{array}$$

Это значит, что $(x^2+x+1)-x(x+1)=1$. Следовательно,

$$\text{НОД}\,(x^2+x+1, x^4+x^3+x+1)=1.$$

Обозначив для краткости $x^4+x^3+x+1=f(x)$ и $x^2+x+1=g(x)$, результаты делений можно записать в виде

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

$$g(x)-x(x+1)=1.$$

Подставляя во второе равенство вместо $-(x+1)$ левую часть первого равенства, получим

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

Приводя подобные члены, получим

$$xf(x)+g(x)(1-x(x^2-1)=1,$$

или

$$xf(x)+(-x^3+x+1)g(x)=1.$$

9. У многочлена $f(x)=x^5+x^3+2x+2$ из $\mathbb{Z}_3[x]$ есть кратный неприводимый множитель. Найти его.

The polynomial $f(x)=x^5+x^3+2x+2$ in $\mathbb{Z}_3[x]$ has a repeated irreducible factor. Find it.

Решение. Производная $f(x)$ есть

$$f'(x)=5x^4+3x^2+2=2x^4+2.$$

Для упрощения дальнейших вычислений можно было бы заменить $f'(x)$ на $2f'(x)=x^4+1$, чтобы сделать старший коэффициент производной равным

1, но мы не будем этого делать, чтобы показать, что это необязательно. Напомним, что в $\mathbb{Z}_3$ имеем $2^{-1} = 2$.

Для нахождения НОД самого многочлена и его производной используем алгоритм Евклида. Опуская (легко восстанавливаемые) деления с остатком последовательно, получаем

$$(x^5 + x^3 + 2x + 2) - (2x)(2x^4 + 2) = x^3 + x + 2,$$
$$(2x^4 + 2) - (2x)(x^3 + x + 2) = x^2 + 2x + 2,$$
$$(x^3 + x + 2) - (x + 1)(x^2 + x + 2) = 0.$$

Таким образом,

$$\text{НОД}\,(f(x), f'(x)) = x^2 + 2x + 2.$$

Докажем неприводимость $x^2 + 2x + 2$. Напомним, что многочлен второй степени над полем $\mathbb{F}$ приводим, тогда и только тогда, когда он имеет корень в $\mathbb{F}$. Проверим существование корней уравнения $x^2+2x+2 = 0$ в $\mathbb{Z}_3$. Имеем

$$0^2 + 2 \cdot 0 + 2 = 2; \quad 1^2 + 2 \cdot 1 + 2 = 2; \quad 2^2 + 2 \cdot 2 + 2 = 1,$$

так что у многочлена $x^2 + 2x + 2$ нет корней в $\mathbb{Z}_3$ и, значит, нет линейных множителей. Поскольку $x^2 + 2x + 2$ является НОД многочлена $f(x)$ и его производной, то его квадрат является делителем $f(x)$. Таким образом, $f(x)$ делится на $(x^2 + 2x + 2)^2$.

10. Пусть u — корень многочлена $x^3 + 3x + 3$. В поле $\mathbb{Q}(u)$ выразить $(u^2 - 2u + 7)^{-1}$ в виде $a + bu + cu^2$.

Let u be a root of the polynomial $x^3 + 3x + 3$. In $\mathbb{Q}(u)$, express $(u^2 - 2u + 7)^{-1}$ in the form $a + bu + cu^2$.

Решение. Деление x^3+3x+3 на x^2-2x+7 дает частное $x+2$ и остаток -11. Так что $u^3 + 3u + 3 = (u + 2)(u^2 - 2u + 7) - 11$ и, следовательно,

$$(u^2 - 2u + 7)^{-1} = \frac{2 + u}{11} = \frac{2}{11} + \frac{1}{11}u.$$

4. Группы

1. Рассмотрим $\mathbb{R}^3$ со стандартным скалярным произведением. Будет ли $\mathbb{R}^3$ группой относительно этой операции?

Use the standard dot product to define a multiplication on $\mathbb{R}^3$. Does this make $\mathbb{R}^3$ into a group?

Решение. Скалярное произведение двух векторов — число, а не вектор. Это означает, что скалярное произведение не является бинарной операцией в $\mathbb{R}^3$.

2. Для векторов $\boldsymbol{a} = (x_1, y_1, z_1)$ и $\boldsymbol{b} = (x_2, y_2, z_2)$ из $\mathbb{R}^3$ векторное произведение определяется как вектор

$$\boldsymbol{a} \times \boldsymbol{b} = (y_1 z_2 - z_1 y_2, z_1 x_2 - x_1 z_2, x_1 y_2 - y_1 x_2).$$

Является ли $\mathbb{R}^3$ группой относительно этой операции?

For vectors $\boldsymbol{a} = (x_1, y_1, z_1)$ and $b = (x_2, y_2, z_2)$ in $\mathbb{R}^3$, the cross product is defined by

$$\boldsymbol{a} \times \boldsymbol{b} = (y_1 z_2 - z_1 y_2, z_1 x_2 - x_1 z_2, x_1 y_2 - y_1 x_2).$$

Is $\mathbb{R}^3$ a group under this multiplication?

Решение. Алгебра $\langle\, \mathbb{R}^3, \times \,\rangle$ не является группой, поскольку векторное произведение обладает следующими свойствами:

Векторное произведение двух ненулевых векторов перпендикулярно каждому из векторов-сомножителей.

Векторное произведение нулевого и любого вектора равно нулевому вектору $\mathbf{0} = (0, 0, 0)$.

В самом деле, если бы $\langle\, \mathbb{R}^3, \times \,\rangle$ было группой, то существовал бы вектор $\boldsymbol{e}$, являющийся нейтральным (единичным) вектором относительно векторного произведения. Это значит, что выполнялось бы равенство $\boldsymbol{a} \times \boldsymbol{e} = \boldsymbol{a}$ для любого $\boldsymbol{a} \in \mathbb{R}^3$. Пусть $\boldsymbol{a} \neq \mathbf{0}$. Если $\boldsymbol{e} \neq \mathbf{0}$, то $\boldsymbol{a} \times \boldsymbol{e}$ перпендикулярно $\boldsymbol{a}$ и, значит, не равно $\boldsymbol{a}$. Если же $\boldsymbol{e} = \mathbf{0}$, то $\boldsymbol{a} \times \boldsymbol{e} = \mathbf{0}$, т.е. снова отлично от $\boldsymbol{a}$. Таким образом, в $\mathbb{R}^3$ нет нейтрального элемента относительно векторного произведения.

Если исключить нулевой вектор, то множество $\mathbb{R}^3 \setminus \{\mathbf{0}\}$ — ненулевых векторов уже не будет замкнутым относительно векторного произведения, т.к. $\boldsymbol{a} \times \boldsymbol{a} = \mathbf{0}$, для любого $\boldsymbol{a} \neq \mathbf{0}$.

3. На множестве $G = \mathbb{Q}^*$ ненулевых рациональных чисел определим новое умножение правилом: $a * b = \frac{ab}{2}$ для всех $a, b \in G$. Докажите, что G — группа относительно этого умножения.

On the set $G = \mathbb{Q}^*$ of nonzero rational numbers, define a new multiplication by $a * b = \frac{ab}{2}$, for all $a, b \in G$. Show that G is a group under this multiplication.

Решение. Если a и b — ненулевые рациональные числа, тогда $\frac{ab}{2}$ также ненулевое рациональное число. Таким образом, множество $G = \mathbb{Q}^*$ замкнуто относительно операции $*$.

Операция $*$ ассоциативна, т.к.

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a\left(\frac{bc}{2}\right)}{2} = \frac{a\,(bc)}{4},$$

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{\left(\frac{ab}{2}\right)c}{2} = \frac{(ab)\,c}{4}.$$

Число 2 является единичным элементом относительно операции $*$:

$$a * 2 = \frac{a \cdot 2}{2} = a, \quad 2 * a = \frac{2 \cdot a}{2} = a.$$

Наконец, если a — ненулевое рациональное число, то число $\frac{4}{a}$ будет обратным элементом для a относительно операции $*$. В самом деле,

$$a * \left(\frac{4}{a}\right) = \frac{a\left(\frac{4}{a}\right)}{2} = 2, \qquad \left(\frac{4}{a}\right) * a = \frac{\left(\frac{4}{a}\right)a}{2} = 2\,.$$

4. Выпишите таблицу Келли для мультипликативной группы $\mathbb{Z}_9^*$.

Write out the multiplication table for $\mathbb{Z}_9^*$.

Решение. $\mathbb{Z}_9^* = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$. Мы будем писать k вместо $[k]_9$.

.	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Комментарий. Записывая элементы в другом порядке, получим другое представление группы

.	1	2	4	8	7	5
1	1	2	4	8	7	5
2	2	4	8	7	5	1
4	4	8	7	5	1	2
8	8	7	5	1	2	4
7	7	5	1	2	4	8
5	5	1	2	4	8	7

Из приведенных таблиц видно, что каждый элемент группы является некоторой степенью 2: $4 = 2^2$, $8 = 2^3$, $7 = 2^4$, $5 = 2^5$, $1 = 2^6$.

5. Выпишите таблицу Келли для мультипликативной группы $\mathbb{Z}_{15}^*$.

Write out the multiplication table for $\mathbb{Z}_{15}^*$.

Решение. $\mathbb{Z}_{15}^* = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}$. Мы будем писать вычеты, как $\{1, 2, 4, 7, -7, -4, -2, -1\}$.

.	1	-1	2	-2	4	-4	7	-7
1	1	-1	2	-2	4	-4	7	-7
-1	-1	1	-2	2	-4	4	-7	7
2	2	-2	4	-4	-7	7	-1	1
-2	-2	2	-4	4	7	-7	1	-1
4	4	-4	-7	7	1	-1	-2	2
-4	-4	4	7	-7	-1	1	2	-2
7	7	-7	-1	1	-2	2	4	-4
-7	-7	7	1	-1	2	-2	-4	4

6. Пусть $G = \{x \in \mathbb{R} \,|\, x > 1\}$ — множество действительных чисел больших 1. Для элементов $x, y \in G$ определим операцию умножения соотношением

$$x * y = xy - x - y + 2.$$

Let $G = \{x \in \mathbb{R} \,|\, x > 1\}$ be the set of all real numbers greater than 1. For $x, y \in G$, define $x * y = xy - x - y + 2$.

a) Показать, что G замкнуто относительно операции умножения $*$.

Show that the operation $*$ is closed on G.

Решение. Если $a, b \in G$, то $a > 1$ и $b > 1$, т.е. $b-1 > 0$ и, следовательно, $a(b-1) > (b-1)$. Отсюда немедленно следует, что $ab - a - b + 2 > 1$.

b) Показать, что операция умножения $*$ ассоциативна в G.

Show that the associative law holds for $*$.

Решение. Для $a, b, c \in G$ имеем

$$\begin{aligned} a * (b * c) &= a * (bc - b - c + 2) = \\ &= a(bc - b - c + 2) - a - (bc - b - c + 2) + 2 = \\ &= abc - ab - ac - bc + a + b + c. \end{aligned}$$

С другой стороны мы имеем

$$\begin{aligned} (a * b) * c &= (ab - a - b + 2) * c = \\ &= (ab - a - b + 2)c - (ab - a - b + 2) - c + 2 = \\ &= abc - ab - ac - bc + a + b + c. \end{aligned}$$

Следовательно, $a * (b * c) = (a * b) * c$.

c) Показать, что 2 — единичный элемент для операции $*$.

Show that 2 is the identity element for the operation $*$.

Решение. Так как введенное выше умножение коммутативно, то достаточно показать, что $2 * y = y$ для всех $y \in G$. Имеем

$$2 * y = 2y - 2 - y + 2 = y.$$

d) Показать, что для каждого элемента $a \in G$ существует обратный элемент $a^{-1} \in G$.

Show that for each element $a \in G$ there exists an inverse $a^{-1} \in G$.

Решение. Обратный элемент y для $a \in G$ удовлетворяет уравнению $a * y = 2$ или $ay - a - y + 2 = 2$, которое имеет единственное решение $y = a/(a-1)$ для любого $a > 1$.

Осталось показать, что $y = a/(a-1) > 1$. Но это следует из очевидного неравенства $a > a - 1$. Далее

$$\begin{aligned} a * (a/a - 1) &= a^2/(a-1) - a - a/(a-1) + 2 = \\ &= (a^2 - a^2 + a - a)/(a-1) + 2 = 2, \end{aligned}$$

так что $y = a/(a-1)$ действительно обратный для a элемент.

7. Найти все циклические подгруппы группы $\mathbb{Z}_{24}^*$.

Find all cyclic subgroups of $\mathbb{Z}_{24}^*$.

Решение. $\mathbb{Z}_{24}^*$ состоит из всех обратимых элементов в $\mathbb{Z}_{24}$. Число таких элементов равно $\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3)\varphi(3) = (2^3 - 2^2) \cdot 2 = 4 \cdot 2 = 8$, а именно $\mathbb{Z}_{24}^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$. Легко проверить, что $x^2 = 1$ для всех элементов группы. Это означает, что каждый отличный от $[1]_{24}$ элемент группы порождает циклическую подгруппу порядка 2, включающую только сам элемент и $[1]_{24}$. Следовательно, имеется $8 - 1 = 7$ различных нетривиальных циклических подгрупп группы $\mathbb{Z}_{24}^*$.

8. В группе $\mathbb{Z}_{20}^*$ найти две подгруппы порядка 4, циклическую и не циклическую.

In $\mathbb{Z}_{20}^*$, find two subgroups of order 4, one that is cyclic and one that is not cyclic.

Решение. Для того, чтобы найти циклическую подгруппу порядка 4 в $\mathbb{Z}_{20}^*$, нужно найти порядки элементов группы $\mathbb{Z}_{20}^* = \{\pm 1, \pm 3, \pm 7, \pm 9\}$. Легко проверить, что $[3]$ имеет порядок 4 и, значит, $G = \langle [3] \rangle$ является циклической подгруппой порядка 4. Элемент $[9] = [3]^2$ имеет, очевидно, порядок 2. Наконец, подмножество $H = \{\pm[1], \pm[9]\}$ замкнуто относительно умножения и, более того, является подгруппой. Кроме того, H не циклическая, так как H не содержит элементов порядка 4.

9. а) Найти циклическую подгруппу в группе S_7 подстановок степени 7, порожденную подстановкой $\sigma = (1, 2, 3)(5, 7)$.

a) Find the cyclic subgroup of S_7 generated by the element $\sigma = (1, 2, 3)(5, 7)$.

Решение. Последовательно вычисляя σ^k, получим

$$\sigma^2 = ((1, 2, 3)(5, 7))^2 = (1, 3, 2),$$

$$\sigma^3 = ((1, 2, 3)(5, 7))^3 = (5, 7),$$

$$\sigma^4 = ((1, 2, 3)(5, 7))^4 = (1, 2, 3),$$

$$\sigma^5 = ((1, 2, 3)(5, 7))^5 = (1, 3, 2)(5, 7),$$

$$\sigma^6 = ((1, 2, 3)(5, 7))^6 = (1).$$

Эти элементы вместе с $(1, 2, 3)(5, 7)$ образуют циклическую подгруппу, порожденную σ.

b) Найти подгруппу в группе S_7, содержащую 12 элементов. Не нужно перечислять все элементы группы. Постарайтесь обосновать, что их в группе 12, и почему они образуют группу.

b) Find a subgroup of S_7 that contains 12 elements. You do not have to list all of the elements if you can explain why there must be 12, and why they must form a subgroup.

Решение. Все, что нам нужно — это найти подстановку порядка 12. Так как порядок произведения независимых циклов (такие циклы коммутируют) равен наименьшему общему кратному порядков сомножителей, то достаточно найти два независимых цикла порядков 3 и 4. Так как цикл длины k имеет порядок k, то достаточно взять два цикла длины 3 и 4. Можно взять, например, циклы $(1,2,3,4)$ и $(5,6,7)$, тогда $(1,2,3,4)(5,6,7)$ порождает циклическую подгруппу порядка 12.

10. Пусть G — абелева группа, и пусть n — фиксированное положительное целое число. Доказать, что $N = \{g \in G \,|\, g = a^n \text{ для некоторого } a \in G\}$ есть подгруппа группы G.

Let G be an abelian group, and let n be a fixed positive integer. Show that $N = \{g \in G \,|\, g = a^n \text{ for some } a \in G\}$ is a subgroup of G.

Решение.

1) Подмножество N не пустое, т.к. единичный элемент e группы G может быть записан в виде $e = e^n$.

2) Предположим, что g_1 и g_2 принадлежат N. Тогда существуют элементы $a_1, a_2 \in G$ такие, что $g_1 = a_1^n$ и $g_2 = a_2^n$. Далее $g_1 g_2 = a_1^n a_2^n = (a_1 a_2)^n$. Последнее равенство выполняется в силу коммутативности G. Таким образом, N замкнуто относительно умножения.

3) Наконец, если $g \in N$, где $g = a^n$, тогда $g^{-1} = (a^n)^{-1} = (a^{-1})^n$ и, значит, g^{-1} принадлежит N. Следовательно, N — подгруппа.

11. Предположим, что p — простое число вида $2^n + 1$.

Suppose that p is a prime number of the form $2^n + 1$.

a) Доказать, что $[2]_p$ имеет в $\mathbb{Z}_p^*$ порядок $2n$.

a) Show that in $\mathbb{Z}_p^*$ the order of $[2]_p$ is $2n$.

Решение. Т.к. $p = 2^n + 1$, то $2^n \equiv -1 \mod p$ и, возводя в квадрат это сравнение, получим $2^{2n} \equiv 1 \mod p$, таким образом, порядок $[2]$ является делителем $2n$. Т.к. для каждого собственного делителя k числа $2n$ имеем

$k \leqslant n$, и $2^k - 1 < 2^n + 1 = p$, то $2^k \not\equiv 1 \mod p$. Это показывает, что порядок $[2]$ равен $2n$.

b) Используя часть a), доказать, что n есть степень 2.

b) Use part a) to prove that n must be a power of 2.

Решение. Порядок $[2]$ является делителем $|\mathbb{Z}_p^*| = p - 1 = 2^n$, тогда из a) следует, что n есть делитель 2^{n-1} и, следовательно, n — степень 2.

12. Найти порядок элемента $A = \begin{pmatrix} i & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -i \end{pmatrix}$ в группе $\mathrm{GL}_3(\mathbb{C})$.

Find the order of the element $A = \begin{pmatrix} i & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -i \end{pmatrix}$ in the group $\mathrm{GL}_3(\mathbb{C})$.

Решение. Для любой диагональной матрицы $A \in \mathrm{GL}_3(\mathbb{C})$ имеем

$$A^n = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}^n = \begin{pmatrix} a^n & 0 & 0 \\ 0 & b^n & 0 \\ 0 & 0 & c^n \end{pmatrix}.$$

Порядок A равен, очевидно, наименьшему общему кратному порядков диагональных элементов i, -1 и $-i$. Таким образом, $\mathrm{ord}(A) = 4$.

13. В мультипликативной группе $\mathbb{C}^*$ ненулевых комплексных чисел найти порядок элементов $-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ и $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$.

In the multiplicative group $\mathbb{C}^*$ of complex numbers,find the order of the elements $-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$ and $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$.

Решение. Самым легким способом решения является преобразование этих чисел из алгебраической формы в тригонометрическую или экспоненциальную. Каждое из этих чисел имеет абсолютную величину, равную 1 и потому их можно записать в тригонометрической форме

$$-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i = \cos(3\pi/4) + i\sin(3\pi/4),$$

$$-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i = \cos(5\pi/4) + i\sin(5\pi/4).$$

Для нахождения степеней этих чисел воспользуемся формулой де Муавра:

$$(\cos(3\pi/4) + i\sin(3\pi/4))^8 = \cos(6\pi) + i\sin(6\pi) = 1.$$

Аналогичным образом получаем, что $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$ также имеет порядок 8.

14. Для группы $G = \mathrm{GL}_2(\mathbb{R})$ обратимых 2×2 матриц с вещественными элементами доказать, что

$$H = \left\{ \left(\begin{array}{cc} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{array} \right) \middle| \, \theta \in \mathbb{R} \right\}$$

— подгруппа в G.

In the group $G = \mathrm{GL}_2(\mathbb{R})$ of invertible 2×2 matrices with real entries, show that

$$H = \left\{ \left(\begin{array}{cc} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{array} \right) \middle| \, \theta \in \mathbb{R} \right\}$$

is a subgroup of G.

Решение. *Замкнутость*. Чтобы доказать, что H замкнуто относительно умножения, следует использовать формулы для синуса и косинуса суммы двух углов. Имеем

$$\left(\begin{array}{cc} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{array} \right) \left(\begin{array}{cc} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{array} \right) =$$

$$= \left(\begin{array}{cc} \cos\theta\cos\phi - \sin\theta\sin\phi & -\cos\theta\sin\phi - \sin\theta\cos\phi \\ \sin\theta\cos\phi + \cos\theta\sin\phi & -\sin\theta\sin\phi + \cos\theta\cos\phi \end{array} \right) =$$

$$= \left(\begin{array}{cc} \cos\theta\cos\phi - \sin\theta\sin\phi & -(\cos\theta\sin\phi + \sin\theta\cos\phi) \\ \sin\theta\cos\phi + \cos\theta\sin\phi & \cos\theta\cos\phi - \sin\theta\sin\phi \end{array} \right) =$$

$$= \left(\begin{array}{cc} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{array} \right) \in H.$$

Существование единицы. Для проверки того, что единичная матрица принадлежит множеству H, положим $\theta = 0$.

Обратимость. $\left(\begin{array}{cc} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{array} \right)^{-1} = \left(\begin{array}{cc} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{array} \right) \in H.$

15. Пусть K — подмножество из $\mathrm{GL}_2(\mathbb{R})$, определяемое как

$$K = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \middle| \, d = a,\ c = -2b,\ ad - bc \neq 0 \right\}.$$

Доказать, что K — подгруппа $\mathrm{GL}_2(\mathbb{R})$.

Let K be the following subset of $\mathrm{GL}_2(\mathbb{R})$

$$K = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| d = a,\ c = -2b,\ ad - bc \neq 0 \right\}.$$

Show that K is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

Решение. *Замкнутость*.

$$\begin{pmatrix} a_1 & b_1 \\ -2b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ -2b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - 2b_1b_2 & a_1b_2 + b_1a_2 \\ -2(a_1b_2 + b_1a_2) & a_1a_2 - 2b_1b_2 \end{pmatrix}.$$

Полученная матрица невырожденна, так как она является результатом произведения двух невырожденных матриц $(\det(AB) = \det(A)\det(B))$.

Единичная матрица принадлежит K и

$$\begin{pmatrix} a & b \\ -2b & a \end{pmatrix}^{-1} = \frac{1}{a^2 + 2b^2} \begin{pmatrix} a & -b \\ -2(-b) & a \end{pmatrix}.$$

Кроме того, обратная матрица невырожденной матрицы также невырожденна $(\det(A^{-1}) = 1/\det(A))$.

Заметим, что определитель любой матрицы из K равен a^2+2b^2 и потому всегда положительный.

16. Найти коммутант матрицы $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ в $G = \mathrm{GL}_2(\mathbb{R})$.

Compute the centralizer in $G = \mathrm{GL}_2(\mathbb{R})$ of the matrix $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$.

Замечание. Согласно определению, коммутант элемента a группы G определяется как подмножество $C(a) = \{x \in G \,|\, xa = ax\}$.

Решение. Пусть $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, и предположим что, $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ принадлежит коммутанту матрицы A в $\mathrm{GL}_2(\mathbb{R})$. Тогда должно выполняться равенство $XA = AX$, или

$$\begin{pmatrix} 2a + b & a + b \\ 2c + d & c + d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 2a + c & 2b + d \\ a + c & b + d \end{pmatrix}.$$

Приравнивая соответствующие элементы, получим систему линейных уравнений

$$\begin{cases} 2a+b=2a+c, \\ a+b=2b+d, \\ 2c+d=a+c, \\ c+d=b+d. \end{cases}$$

Из первого и последнего уравнений следует, что $b=c$. Из второго и третьего уравнений следует, что $a=b+d=c+d$ или $d=a-b$.

С другой стороны любая матрица такого вида коммутирует с A, следовательно, коммутант матрицы $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ в $G=\mathrm{GL}_2(\mathbb{R})$ есть подгруппа вида

$$\left\{ \begin{pmatrix} a & b \\ b & a-b \end{pmatrix} \,\middle|\, a,b\in\mathbb{R},\ ab\neq a^2-b^2 \right\}.$$

17. Пусть G — подгруппа в $G=\mathrm{GL}_2(\mathbb{R})$, определенная как

$$G=\left\{ \begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix} \,\middle|\, m\neq 0 \right\}.$$

Пусть $A=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $B=\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Найти централизаторы $C(A)$ и $C(B)$ матриц A и B и доказать, что $C(A)\cap C(B)=Z(G)$, где $Z(G)$ — центр G.

Let G be the subgroup of $G=\mathrm{GL}_2(\mathbb{R})$ defined by $G=\left\{ \begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix} \,\middle|\, m\neq 0 \right\}$. Let $A=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B=\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Find the centralizers $C(A)$ and $C(B)$, and show that $C(A)\cap C(B)=Z(G)$, where $Z(G)$ is the center of G.

Решение. Согласно определению, централизатор матрицы состоит из всех матриц, перестановочных с этой матрицей, а центр группы — пересечение всех централизаторов. Предположим, что

$$X=\begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix}$$

принадлежит $C(A)$ в G. Тогда должно выполняться условие $XA = AX$, или

$$\begin{pmatrix} m & m+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \\ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} m & b+1 \\ 0 & 1 \end{pmatrix}.$$

Приравнивая соответствующие элементы, получим $m + b = b + 1$, отсюда следует, что $m = 1$. С другой стороны любая матрица такой формы коммутирует с A и, значит,

$$C(A) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| \, b \in \mathbb{R} \right\}.$$

Теперь предположим, что $X = \begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix}$ принадлежит $C(B)$. Тогда должно выполняться условие $XB = BX$ или

$$\begin{pmatrix} -m & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \\ = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -m & -b \\ 0 & 1 \end{pmatrix}.$$

Приравнивая соответствующие элементы, получим $b = 0$ и, значит,

$$C(B) = \left\{ \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \middle| \, 0 \neq m \in \mathbb{R} \right\}.$$

Отсюда следует, что $C(A) \cap C(B) = \{I\}$, где I — единичная матрица, а так как любой элемент центра $Z(G)$ группы G принадлежит $C(A) \cap C(B)$, то $Z(G)$ — тривиальная подгруппа, содержащая только единичную матрицу.

18. Показать, что $\mathbb{Z}_5 \times \mathbb{Z}_3$ — циклическая группа, и найти все образующие для нее.

Show that $\mathbb{Z}_5 \times \mathbb{Z}_3$ is a cyclic group, and list all of the generators for the group.

Решение. Рассмотрим элемент $([a]_5, [b]_3)$ в $\mathbb{Z}_5 \times \mathbb{Z}_3$. Аддитивный порядок этого элемента есть наименьшее общее кратное порядков компонент $[a]_5$ и $[b]_3$. Поскольку $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$ имеют порядок 5 в $\mathbb{Z}_5$, а $[1]_3$, $[2]_3$ —

порядок 3 в $\mathbb{Z}_3$, то элемент $([a]_5, [b]_3)$ будет образующим, если и только если обе компоненты отличны от нуля, т.е. $[a]_5 \neq [0]_5$ и $[b]_5 \neq [0]_5$. Очевидно, что в $\mathbb{Z}_5 \times \mathbb{Z}_3$ есть точно $8 = 4 \cdot 2$ таких элементов.

Комментарий. Остальные 7 элементов группы $\mathbb{Z}_5 \times \mathbb{Z}_3$ будут иметь по крайней мере одну нулевую компоненту. Есть 4 ненулевых элемента порядка 5 (с $[b]_5 = [0]_3$) и 2 ненулевых элемента порядка 3 (с $[a]_5 = [0]_5$). Нулевой элемент $([0]_5, [0]_3)$ завершает список всех 15 элементов $\mathbb{Z}_5 \times \mathbb{Z}_3$.

19. Найти порядок элемента $([9]_{12}, [15]_{18})$ в группе $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$.

Find the order of the element $([9]_{12}, [15]_{18})$ in the group $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$.

Решение. Поскольку $\text{НОД}\,(9, 12) = 3$, то $\operatorname{ord}([9]_{12}) = \operatorname{ord}([3]_{12}) = 4$. Точно так же, из $\text{НОД}\,(15, 18) = 3$ следует, что $\operatorname{ord}([15]_{18}) = \operatorname{ord}([3]_{18}) = 6$. Таким образом, порядок $([9]_{12}, [15]_{18})$ есть $\text{НОК}\,(4, 6) = 12$.

20. Найти 2 группы G_1 и G_2, чье прямое произведение $G_1 \times G_2$ содержит подгруппу, отличную от подгрупп вида $H_1 \times H_2$, для подгрупп $H_1 \subseteq G_1$ и $H_2 \subseteq G_2$.

Find two groups G_1 and G_2 whose direct product $G_1 \times G_2$ has a subgroup that is not of the form $H_1 \times H_2$, for subgroups $H_1 \subseteq G_1$ and $H_2 \subseteq G_2$.

Решение. В $\mathbb{Z}_2 \times \mathbb{Z}_2$ элемент $(1, 1)$ имеет порядок 2, так, что он порождает циклическую подгруппу $\{(0, 0), (1, 1)\}$, не являющуюся произведением подгрупп.

Замечание. Подгруппа вида $H_1 \times H_2$, где $H_1 \subseteq G_1$ и $H_2 \subseteq G_2$ имеет порядок $|H_1| \cdot |H_2|$, равный произведению порядков $|H_1|$, $|H_2|$ подгрупп H_1 и H_2. Если H_1 и H_2 нетривиальны (т.е. H_1 и $H_2 \neq \{e\}$), то $|H_1|$, $|H_2| \geqslant 2$ и, значит, $|H_1| \cdot |H_2| \geqslant 4$.

21. Для группы $G = \mathbb{Z}_{36}^*$ обратимых элементов кольца $\mathbb{Z}_{36}$ положим $H = \{[x] \,|\, x \equiv 1 \mod 4\}$ и $K = \{[y] \,|\, y \equiv 1 \mod 9\}$. Показать, что H и K — подгруппы G и описать подгруппу HK.

In the group $G = \mathbb{Z}_{36}^*$, let $H = \{[x] \,|\, x \equiv 1 \mod 4\}$ and $K = \{[y] \,|\, y \equiv 1 \mod 9\}$. Show that H and K are subgroups of G, and find the subgroup HK.

Решение. Пусть $\varphi_4 : \mathbb{Z}_{36} \to \mathbb{Z}_4$, $\varphi_4(x) = [x]_4$; и $\varphi_9 : \mathbb{Z}_{36} \to \mathbb{Z}_9$, $\varphi_9(x) = [x]_9$ — канонические гомоморфизмы. Из китайской теоремы об остатках следует, что декартово произведение этих гомоморфизмов $\varphi = \varphi_4 \times \varphi_9$:

$\mathbb{Z}_{36} \to \mathbb{Z}_4 \times \mathbb{Z}_9$, $\varphi(x) = ([x]_4, [x]_9)$ есть изоморфизм. Используя этот изоморфизм, легко показать, что произведение $\varphi^* = \varphi_4^* \times \varphi_9^* : \mathbb{Z}_{36}^* \to \mathbb{Z}_4^* \times \mathbb{Z}_9^*$ сужений φ_4^* и φ_9^* гомоморфизмов φ_4 и φ_9 на группы $\mathbb{Z}_4^*$ и $\mathbb{Z}_9^*$ соответственно есть изоморфизм групп. Он совпадает с сужением произведения $\varphi = \varphi_4 \times \varphi_9$ на группу $\mathbb{Z}_{36}^*$. Отсюда следует, что $H = \ker \varphi_4^*$ и $K = \ker \varphi_9^*$, таким образом, K, H — подгруппы группы $\mathbb{Z}_{36}^*$. Короткое вычисление показывает, что $H = \{[1], [5], [13], [17], [25], [29]\}$ и $K = \{[1], [19]\}$. Поскольку $x \cdot [1] \neq x \cdot [19]$ для $x \in G$, то произведение HK должно содержать 12 элементов и, значит, $HK = G$.

22. Показать, что если p — простое число, то порядок полной линейной группы $\mathrm{GL}_n(\mathbb{Z}_p)$ над конечным полем $\mathbb{Z}_p$ равен $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$.

Show that if p is a prime number, then the order of the general linear group $\mathrm{GL}_n(\mathbb{Z}_p)$ is $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$.

Решение. Нужно подсчитать число способов, которыми может быть образована обратимая матрица. Матрица n-го порядка состоит из n столбцов и она будет обратимой тогда и только тогда, когда эти столбцы линейно независимы. Будем последовательно выбирать столбцы обратимой матрицы. Отметим, что число различных столбцов высоты n, составленных из p элементов поля $\mathbb{Z}_p$, равно p^n.

Первый столбец может быть любым ненулевым столбцом из n элементов поля $\mathbb{Z}_p$, так что его можно выбрать $p^n - 1$ способом.

Второй столбец не должен быть коллинеарным первому столбцу. Поскольку в поле $\mathbb{Z}_p$ имеется всего p элементов, то имеется в точности p кратных столбцов и, значит, 2-ой столбец может быть выбран $p^n - p$ способами.

Третий столбец не должен быть равным линейной комбинацией первых двух. Так как имеется в точности p^2 таких комбинаций, то из общего числа p^n столбцов длины n мы должны вычесть p^2, так что остается всего $p^n - p^2$ способов выбора третьего столбца.

Продолжая рассуждения аналогичным образом, можно показать (используя, например, математическую индукцию), что для выбора k-го столбца имеется $p^n - p^{k-1}$ способов, так как он не должен быть линейной комбинацией первых $k-1$ столбцов, а таких комбинаций очевидно p^{k-1}.

23. Пусть даны группа G и ее подгруппа H. Доказать, что если a — про-

извольный элемент из G, то подмножество

$$aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ для некоторого } h \in H\}$$

является подгруппой G, изоморфной H.

Let G be a group, and let H be a subgroup of G. Prove that if a is any element of G, then the subset $aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$ is a subgroup of G that is isomorphic to H.

Решение. Функция $\phi : G \to G$, определяемая как $\phi(x) = axa^{-1}$ для всех $x \in G$, является изоморфизмом группы G на себя, т.е автоморфизмом. При этом $\phi(H) = aHa^{-1}$. Поскольку образ любой подгруппы из G относительно автоморфизма является подгруппой в G, то $\phi(H) = aHa^{-1}$ — подгруппа в G. При этом сужение $\phi|_H = \theta : H \to aHa^{-1}$, $\theta(x) = axa^{-1}$ автоморфизма ϕ на подгруппу H будет, очевидно, изоморфизмом этой подгруппы на подгруппу aHa^{-1}.

24. Даны группы G, G_1, G_2. Доказать, что если G изоморфна произведению групп $G_1 \times G_2$, то существуют подгруппы H и K группы G, такие, что $H \cap K = \{e\}$, $HK = G$ и $hk = kh$ для всех $h \in H$ и $k \in K$.

Let G, G_1, G_2 be groups. Prove that if G is isomorphic to $G_1 \times G_2$, then there are subgroups H and K in G such that $H \cap K = \{e\}$, $HK = G$, and $hk = kh$ for all $h \in H$ and $k \in K$.

Решение. Пусть отображение $\phi : G_1 \times G_2 \to G$ — изоморфизм. Положим

$$H^* = \{(x_1, x_2) \mid x_1 \in G_1,\ x_2 = e_2\},\ \ K^* = \{(x_1, x_2) \mid x_2 \in G_2,\ x_1 = e_1\},$$

где e_1 и e_2 — соответственно единичные элементы групп G_1 и G_2. Подгруппы H^* и K^* группы $G_1 \times G_2$ обладают требуемыми свойствами: $H^* \cap K^* = \{e = (e_1, e_2)\}$, $H^*K^* = G_1 \times G_2$ и $h^*k^* = k^*h^*$ для всех $h^* \in H^*$ и $k^* \in K^*$.

Пусть теперь $H = \phi(H^*)$ и $K = \phi(K^*)$ — образы подгрупп H^* и K^*соответственно. Ясно, что H и K — подгруппы G, так что осталось показать, что $H \cap K = \{e\}$, $HK = G$, и $hk = kh$ для всех $h \in H$ и $k \in K$.

Пусть $y \in G$, $y = \phi(x)$ для $x \in G_1 \times G_2$. Если $y \in H \cap K$, то $y \in H$ и $y \in K$. Но тогда $x \in H^* \cap K^*$ и, значит, $x = (e_1, e_2)$. Таким образом, $y = \phi((e_1, e_2)) = e$ показывает, что $H \cap K = \{e\}$. Так как y — произвольный элемент G, то $x = h^*k^*$ для некоторых $h^* \in H^*$ и $k^* \in K^*$. Отсюда

следует, что $y = \phi(h^*k^*) = \phi(h^*)\phi(k^*)$ и, значит, $G = HK$. Таким образом определенные выше подгруппы H и K удовлетворяют требуемым условиям.

25. Показать, что для любого простого числа p подгруппа диагональных матриц из $\mathrm{GL}_2(\mathbb{Z}_p)$ изоморфна $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$.

Show that for any prime number p, the subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbb{Z}_p)$ is isomorphic to $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$.

Решение. Так как каждая матрица в $\mathrm{GL}_2(\mathbb{Z}_p)$ имеет ненулевой определитель, то отображение $\phi : \mathbb{Z}_p^* \times \mathbb{Z}_p^* \to \mathrm{GL}_2(\mathbb{Z}_p)$, определяемое по правилу

$$\phi(x_1, x_2) = \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}$$

для всех $(x_1, x_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$, биективно отображает $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$ на подгруппу всех диагональных матриц. Это отображение является гомоморфизмом, поскольку сохраняет операции в группах. В самом деле, для $(a_1, a_2), (b_1, b_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ мы имеем

$$\begin{aligned} \phi((a_1, a_2)(b_1, b_2)) &= \phi((a_1b_1, a_2b_2)) = \\ &= \begin{pmatrix} a_1b_1 & 0 \\ 0 & a_2b_2 \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} = \\ &= \phi((a_1, a_2))\phi((b_1, b_2)). \end{aligned}$$

Таким образом, ϕ есть требуемый изоморфизм.

26. a) Для группы $G = \mathrm{GL}_2(\mathbb{R})$ обратимых матриц порядка 2 с вещественными элементами показать, что

$$H = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \,\middle|\, a_{11} = 1, a_{21} = 0, a_{22} = 1 \right\}$$

— подгруппа G.

a) In the group $G = \mathrm{GL}_2(\mathbb{R})$ of invertible 2×2 matrices with real entries, show that

$$H = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \,\middle|\, a_{11} = 1, a_{21} = 0, a_{22} = 1 \right\}$$

is a subgroup of G.

b) Показать, что H изоморфна аддитивной группе $\mathbb{R}$, т.е. группе всех вещественных чисел по сложению.

b) Show that H is isomorphic to the group $\mathbb{R}$ of all real numbers, under addition.

Решение. a) Покажем сначала замкнутость H относительно умножения матриц:

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}.$$

Единичная матрица, очевидно, принадлежит H.

Наконец, обратные матрицы для матриц из H также принадлежат H:

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \in H.$$

Следовательно, H — подгруппа группы G.

b) Определим отображение $\phi : \mathbb{R} \to H$, полагая $\phi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ для всех $x \in \mathbb{R}$. Легко проверить, что ϕ — изоморфизм. Это фактически следует из равенства

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix},$$

которое мы использовали выше для доказательства замкнутости H. В самом деле, в терминах нашего отображения его можно записать как $\phi(ab) = \phi(a)\phi(b)$, а это и означает, что отображение ϕ — гомоморфизм. С другой стороны, биективность отображения ϕ очевидна, так что ϕ — изоморфизм.

27. Пусть G — подгруппа $\mathrm{GL}_2(\mathbb{R})$, определяемая как

$$G = \left\{ \begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix} \;\middle|\; m,\ b \in \mathbb{R},\ m \neq 0 \right\}.$$

Показать, что G не изоморфна прямому произведению $\mathbb{R}^* \times \mathbb{R}$.

Let G be the subgroup of $\mathrm{GL}_2(\mathbb{R})$ defined by $G = \left\{ \begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix} \;\middle|\; m,\ b \in \mathbb{R},\ m \neq 0 \right\}$. Show that G is not isomorphic to the direct product $\mathbb{R}^* \times \mathbb{R}$.

Решение. Для доказательства неизоморфности следует попытаться найти алгебраическое свойство, которое сохраняется при изоморфизмах, но которому удовлетворяют только одна из двух групп. В данном случае это

свойство — коммутативность. Очевидно, что $\mathbb{R}^* \times \mathbb{R}$ — абелева, тогда как G — неабелева, например

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Таким образом, эти две группы не могут быть изоморфными.

28. Показать, что группы $\mathbb{Z}_6$, $\mathbb{Z}_9^*$ и $\mathbb{Z}_{18}^*$ изоморфны друг другу.

Show that the three groups $\mathbb{Z}_6$, $\mathbb{Z}_9^*$ and $\mathbb{Z}_{18}^*$ are isomorphic to each other.

Решение. $|\mathbb{Z}_9^*| = |\mathbb{Z}_{18}^*| = 6$. В $\mathbb{Z}_9^*$ $2^2 = 4$, $2^3 = 8 = -1 \neq 1$ и, значит, $[2]$ должно иметь порядок 6, т.е. $\mathbb{Z}_9^*$ — циклическая группа порядка 6. Отсюда следует, что $\mathbb{Z}_9^* \approx \mathbb{Z}_6$. В $\mathbb{Z}_{18}$ $5^2 = 7$, $5^3 = 17 = -1 \neq 1$ и, значит, $[5]$ должно иметь порядок 6, так что $\mathbb{Z}_{18}$ — циклическая группа порядка 6. Отсюда следует, что $\mathbb{Z}_{18}^* \approx \mathbb{Z}_6$. Таким образом, все три группы изоморфны.

29. Будет ли $\mathbb{Z}_4 \times \mathbb{Z}_{10}$ изоморфна $\mathbb{Z}_2 \times \mathbb{Z}_{20}$?

Is $\mathbb{Z}_4 \times \mathbb{Z}_{10}$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{20}$?

Решение. Согласно китайской теореме об остатках, $\mathbb{Z}_{10} \approx \mathbb{Z}_2 \times \mathbb{Z}_5$ и $\mathbb{Z}_{20} \approx \mathbb{Z}_4 \times \mathbb{Z}_5$. Но тогда $\mathbb{Z}_4 \times \mathbb{Z}_{10} \approx \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5$ и $\mathbb{Z}_2 \times \mathbb{Z}_{20} \approx \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$. Кроме того, очевидно, что $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5$ и $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ изоморфны. Следовательно, $\mathbb{Z}_4 \times \mathbb{Z}_{10} \approx \mathbb{Z}_2 \times \mathbb{Z}_{20}$.

30. Будет ли $\mathbb{Z}_4 \times \mathbb{Z}_{15}$ изоморфна $\mathbb{Z}_6 \times \mathbb{Z}_{10}$?

Is $\mathbb{Z}_4 \times \mathbb{Z}_{15}$ isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_{10}$?

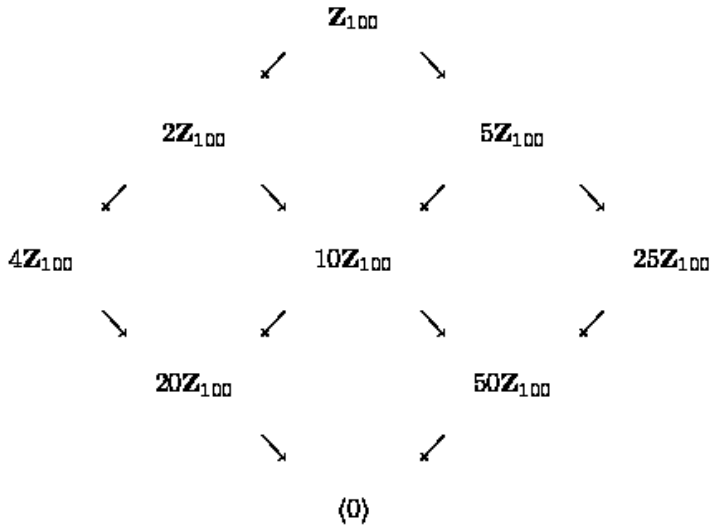
Решение. Т.к. $\mathbb{Z}_4 \times \mathbb{Z}_{15} \approx \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ и $\mathbb{Z}_6 \times \mathbb{Z}_{10} \approx \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_5$, то эти две группы не изоморфны, т. к. первая имеет элемент порядка 4, а вторая не имеет.

31. Описать решетку подгрупп группы $\mathbb{Z}_{100}$.

Give the lattice diagram of subgroups of $\mathbb{Z}_{100}$.

Решение. Решетка подгрупп группы совпадает с решеткой всех делителей порядка группы. Таким образом, в нашем случае она совпадает с частично упорядоченным множеством всех делителей числа 100 по отношению делимости (см. рис. ниже).

Напомним, что для абелевой группы A запись nA означает совокупность всех кратных элементов A: $nA = \{na \mid n \in \mathbb{Z},\ a \in A\}$.



32. Найти все образующие циклической группы $\mathbb{Z}_{28}$.

Find all generators of the cyclic group $\mathbb{Z}_{28}$.

Решение. Образующие (порождающие элементы) циклической группы $\mathbb{Z}_n$ являются меньшими n и взаимно простыми вычетами с порядком n группы $\mathbb{Z}_n$. Число образующих группы $\mathbb{Z}_n$, таким образом, задается функцией Эйлера $\varphi(n)$. В нашем случае

$$\varphi(28) = \varphi(4 \cdot 7) = \varphi(4) \cdot \varphi(7) = 2 \cdot 6 = 12.$$

Таким образом, образующие элементы группы $\mathbb{Z}_{28}$:

$$\{\pm 1, \pm 3, \pm 5, \pm 9, \pm 11, \pm 13\}.$$

33. В $\mathbb{Z}_{30}$ найти порядки циклических подгрупп $\langle [18]_{30} \rangle$ и $\langle [24]_{30} \rangle$, порожденных вычетами $[18]_{30}$ и $[24]_{30}$ соответственно.

In $\mathbb{Z}_{30}$, find the order of the subgroup $\langle [18]_{30} \rangle$; find the order of $\langle [24]_{30} \rangle$.

Решение. Как известно, $\operatorname{ord}([k]_n) = \operatorname{ord}(\text{НОД}([k]_n, n))$. Поскольку $\text{НОД}\,(18, 30) = 6$, то $\langle [18]_{30} \rangle = \langle [6]_{30} \rangle$ и значит, подгруппа имеет $30/6 = 5$ элементов. Аналогично, $\langle [24]_{30} \rangle = \langle [6]_{30} \rangle$, значит, $\langle [24]_{30} \rangle = \langle [18]_{30} \rangle$.

34. Доказать, что если G_1 и G_2 — группы порядка 7 и 11 соответственно, то прямое произведение $G_1 \times G_2$ — циклическая группа.

Prove that if G_1 and G_2 are groups of order 7 and 11, respectively, then the direct product $G_1 \times G_2$ is a cyclic group.

Решение. Т. к. 7 и 11 — простые числа, то группы G_1 и G_2 циклические. Если a имеет порядок 7 в G_1 и b имеет порядок 11 в G_2, то (a, b) имеют порядок $\text{НОК}\,(7, 11) = 77$ в $G_1 \times G_2$. Таким образом, $G_1 \times G_2$ имеет элемент, порядок которого равен порядку группы и, следовательно, $G_1 \times G_2$ — циклическая группа.

35. Найти все гомоморфизмы из $\mathbb{Z}_4$ в $\mathbb{Z}_{10}$.

Find all group homomorphisms from $\mathbb{Z}_4$ into $\mathbb{Z}_{10}$.

Решение. Заметим, что любой гомоморфизм из $\mathbb{Z}_n$ в $\mathbb{Z}_k$ имеет вид $h([x]_n) = [mx]_k$ для всех $[x]_n \in \mathbb{Z}_n$, где $[m]_k = h([1]_n)$. Для любого гомоморфизма $h : \mathbb{Z}_4 \to \mathbb{Z}_{10}$ порядок $[m]_{10} = h([1]_4)$ должен быть делителем 4 и 10, поэтому единственно возможные значения для порядка $h([1]_4)$ это 1 и 2. Имеется всего два таких гомоморфизма: определяемый соотношением $h([1]_4) = [0]_{10}$ — нулевой гомоморфизм, и определяемый соотношением $h([1]_4) = [5]_{10}$, для которого $h([x]_n) = [5x]_{10}$ для всех $[x]_n \in \mathbb{Z}_n$.

36. a) Найти все гомоморфизмы из $\mathbb{Z}_{18}$ в $\mathbb{Z}_{30}$.

b) Выбрать один из ненулевых гомоморфизмов части a) и найти для него ядро и образ, показать как элементы образов соответствуют смежным классам ядра.

a) Find the formulas for all group homomorphisms from $\mathbb{Z}_{18}$ into $\mathbb{Z}_{30}$.

b) Choose one of the nonzero formulas in part a), and for this formula find the kernel and image, and show how elements of the image correspond to cosets of the kernel.

Решение. a) Любой гомоморфизм из $\mathbb{Z}_{18}$ в $\mathbb{Z}_{30}$ имеет вид $h([x]_{18}) = [mx]_{30}$ для всех $[x]_{18} \in \mathbb{Z}_{18}$, где $[m]_{30} = h([1]_{18})$. Порядок $[m]_{30} = h([1]_{18})$ должен быть делителем 18 и 30, Поскольку $\text{НОД}\,(18, 30) = 6$, возможные значения порядка $[m]_{30} = h([1]_{18})$ — 1, 2, 3, 6. Следовательно, имеется в точности 4 гомоморфизма из $\mathbb{Z}_{18}$ в $\mathbb{Z}_{30}$.

b) Выберем, например, $h([x]_{18}) = [5x]_{30}$. Образ h, т.е. множество $h(\mathbb{Z}_{18})$, состоит из всех вычетов кратных 5 в $\mathbb{Z}_{30}$, т.е.

$$h(\mathbb{Z}_{18}) = \{0, 5, 10, 15, 20, 25\}.$$

Ядро $\ker h$ гомоморфизма h состоит из элементов $[x]_{18}$ группы $\mathbb{Z}_{18}$, таких что $h([x]_{18}) = [0]_{30}$. Ясно, что $\ker h = \{0, 6, 12\}$. Смежные классы по ядру состоят из сдвигов $x + \ker h$ ядра на произвольные элементы x группы $\mathbb{Z}_{18}$.

Нетривиальные сдвиги получаются для $x = 1, 2, 3, 4$ и 5 соответственно. Мы имеем следующие соответствия:

$$\{0, 6, 12\} \leftrightarrow h(0) = 0, \quad \{3, 9, 15\} \leftrightarrow h(3) = 15,$$
$$\{1, 7, 13\} \leftrightarrow h(1) = 5, \quad \{4, 10, 16\} \leftrightarrow h(4) = 20,$$
$$\{2, 8, 14\} \leftrightarrow h(2) = 10, \quad \{5, 11, 17\} \leftrightarrow h(5) = 25.$$

37. a) Показать, что $\mathbb{Z}_7^*$ — циклическая группа с порождающим элементом $[3]_7$.

b) Показать, что $\mathbb{Z}_{17}^*$ — циклическая группа с порождающим элементом $[3]_{17}$.

c) Найти все гомоморфизмы из $\mathbb{Z}_{17}^*$ в $\mathbb{Z}_7^*$.

a) Show that $\mathbb{Z}_7^*$ is cyclic, with generator $[3]_7$.

b) Show that $\mathbb{Z}_{17}^*$ is cyclic, with generator $[3]_{17}$.

c) Completely determine all group homomorphisms from $\mathbb{Z}_{17}^*$ into $\mathbb{Z}_7^*$.

Решение. a) Находя последовательно степени 3, получим: $3^2 = 2$ и $3^3 = 6 = -1$. Отсюда следует, что $[3]$ имеет порядок 6.

b) Находя последовательно степени 3, получим: $3^2 = 9$, $3^3 = 27 = 10$, $3^4 = 3 \cdot 10 = 13$, $3^5 = 3 \cdot 13 = 5$, $3^6 = 3 \cdot 5 = 15$, $3^7 = 3 \cdot 15 = 11$, $3^8 = 3 \cdot 11 = 16 = -1 \neq 1$. Таким образом, $[3]_{17}$ имеет порядок $16 = 17 - 1$.

c) Любой гомоморфизм $h : \mathbb{Z}_{17}^* \to \mathbb{Z}_7^*$ циклической группы $\mathbb{Z}_{17}^*$ определяется своим значением $h([3]_{17})$ на образующем элементе $[3]_{17}$ группы $\mathbb{Z}_{17}^*$. Порядок $h([3]_{17})$ должен быть общим делителем 16 и 6. Таким образом, единственные возможные значения для порядка $h([3]_{17})$ — 1 и 2, так что $h([3]_{17}) = [1]_7$ или $h([3]_{17}) = [-1]_7$. В первом случае $h([x]_{17}) = [1]_7$ для всех $[x]_{17} \in \mathbb{Z}_{17}^*$. Во втором случае $h(([3]_{17})^n)) = [-1]_7^n$ для всех $[x]_{17} = ([3]_{17})n \in \mathbb{Z}_{17}^*$.

38. Определим отображение $\phi : \mathbb{Z}_4 \times \mathbb{Z}_6 \to \mathbb{Z}_4 \times \mathbb{Z}_3$ формулой $\phi(x, y) = (x + 2y, y)$.

a) Показать, что ϕ — гомоморфизм групп.

b) Найти ядро и образ отображения ϕ и применить основную теорему о гомоморфизмах.

Define $\phi : \mathbb{Z}_4 \times \mathbb{Z}_6 \to \mathbb{Z}_4 \times \mathbb{Z}_3$ by $\phi(x, y) = (x + 2y, y)$.

a) Show that ϕ is a well-defined group homomorphism.

b) Find the kernel and image of ϕ, and apply the fundamental homomorphism theorem.

Решение. a) Если $y_1 \equiv y_2 \mod 6$, то $2y_1 - 2y_2$ делится без остатка на 12 и $2y_1 \equiv 2y_2 \mod 4$, отсюда немедленно следует, что ϕ корректно определенное отображение. Легко видеть, что отображение ϕ линейно, т.е. является гомоморфизмом аддитивных групп $\mathbb{Z}_4 \times \mathbb{Z}_6$ и $\mathbb{Z}_4 \times \mathbb{Z}_3$.

b) Если $(x, y) \in \ker \phi$, то $y \equiv 0 \mod 3$, т.е. $y = 0$ или $y = 3$. Если $y = 0$, то $x = 0$, а если $y = 3$, то $x = 2$. Таким образом, элементами ядра являются $(0, 0)$ и $(2, 3)$. Отсюда следует, что имеется $24/2 = 12$ классов смежности по этому ядру. Эти классы смежности находятся во взаимно-однозначном соответствии с элементами образа и, следовательно, ϕ отображает $\mathbb{Z}_4 \times \mathbb{Z}_6$ на $\mathbb{Z}_4 \times \mathbb{Z}_3$. Таким образом, $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\{(0, 0), (2, 3)\} \approx \mathbb{Z}_4 \times \mathbb{Z}_3$.

39. Пусть n, m — положительные целые числа и m есть делитель n. Показать, что отображение $\phi : \mathbb{Z}_n^* \to \mathbb{Z}_m^*$, определенное равенством $\phi([x]_n) = [x]_m$ для всех $[x]_n \in \mathbb{Z}_n^*$, есть гомоморфизм.

Let n and m be positive integers, such that m is a divisor of n. Show that $\phi : \mathbb{Z}_n^* \to \mathbb{Z}_m^*$ defined by $\phi([x]_n) = [x]_m$, for all $[x]_n \in \mathbb{Z}_n^*$, is a well-defined group homomorphism.

Решение. Если $[x_1]_n = [x_2]_n$ в $\mathbb{Z}_n^*$ то $(x_1 - x_2)$ делится на n, а т.к. m — делитель n, то $(x_1 - x_2)$ делится на m. Таким образом, из $[x_1]_m = [x_2]_m$ следует $\phi([x_1]_n) = \phi([x_2]_n)$. Следовательно, отображение ϕ корректно определено.

Далее, для всех $[a_n], [b]_n \in \mathbb{Z}_n^*$ имеем
$\phi([a]_n[b]_n) = \phi([ab]_n) = [ab]_m = [a]_m[b]_m = \phi([a]_n)\phi([b]_n)$,
следовательно ϕ — гомоморфизм.

40. Для гомоморфизма групп $\phi : \mathbb{Z}_{36}^* \to \mathbb{Z}_{12}^*$, определенного равенством $\phi([x]_{36}) = [x]_{12}$ для всех $[x]_{36} \in Z_{36}^*$, найти ядро и образ отображения ϕ и применить основную теорему о гомоморфизме.

For the group homomorphism $\phi : \mathbb{Z}_{36}^* \to \mathbb{Z}_{12}^*$ defined by $\phi([x]_{36}) = [x]_{12}$, for all $[x]_{36} \in Z_{36}^*$, find the kernel and image of ϕ, and apply the fundamental homomorphism theorem.

Решение. Предыдущая задача показывает, что ϕ — гомоморфизм групп. Очевидно, что ϕ отображает $\mathbb{Z}_{36}^*$ на $\mathbb{Z}_{12}^*$, поскольку из $\text{НОД}\,(x, 12) = 1$ следует $\text{НОД}\,(x, 36) = 1$. Ядро ϕ состоит из тех элементов в $\mathbb{Z}_{36}^*$, которые сравнимы с 1 по модулю 12, а именно $[1]_{36}$, $[13]_{36}$, $[25]_{36}$. Отсюда следует, что $\mathbb{Z}_{12}^* \approx \mathbb{Z}_{36}^*/\langle [13]_{36} \rangle$.

41. Предположим, что $G = \langle g \rangle$ является циклической группой порядка 144

с образующим элементом g. Каков порядок g^{60}?

Suppose that $G = \langle g \rangle$ is a cyclic group of order 144. What is the order ofg^{60}?

Решение. Нужно найти наименьшее положительное целое число n, такое что $(g^{60})^n = e$.

Поскольку порядок g равен 144, то $g^{60n} = e$ тогда и только тогда, когда $60n \equiv 0 \mod 144$. Т.е. нужно найти наименьшее положительное целое решение уравнения $60x \equiv 0 \mod 144$. Ясно, что для этого необходимо чтобы $60n$ делилось на 144. Наибольший общий делитель чисел 144 и 60 равен 12. Следовательно, $5n$ делится на 12, а это значит (в силу взаимной простоты 5 и 12) что n делится на 12. Таким образом, $n = 12$ — наименьшее решение сравнения $60n \equiv 0 \mod 144$. Следовательно, порядок g^{60} равен 12.

42. Найти все элементы аддитивного порядка 10 из $\mathbb{Z}_{100}$.

Find all elements of order 10 in the additive group $\mathbb{Z}_{100}$.

Решение. 1 является образующим элементом группы $\mathbb{Z}_{100}$. Порядок $n \in \mathbb{Z}_{100}$ по определению есть наименьшее $k > 0$ такое, что $kn \equiv 0 \mod 100$. Как известно, $k = 100/\text{НОД}(n, 100)$. Следовательно, нужно найти все целые n в диапазоне $0, \ldots, 99$ такие, что $10 = \text{НОД}(n, 100)$. Это значит, что число n должно делиться на 10 и $n/10$ должно быть взаимно простым с 2 и 5, т.е. взаимно просто с 10. Пусть $n = 10m$, $0 \leqslant m < 9$. Тогда $n/10 = m$ — взаимно просто с 10. Это значит, что $m \in \{1, 3, 7, 9\}$. Следовательно, $n = 10, 30, 70, 90$ — все вычеты по модулю 100, имеющие аддитивный порядок 10.

43. Пусть p — простое число такое, что $p \equiv 21 \mod 25$. Доказать, что для ненулевой 5-ой степени $b \in \mathbb{Z}_p^*$, $b^{(p+4)/25}$ является корнем 5-ой степени из b по модулю p.

Let p a prime congruent to $21 \mod 25$. Prove that, for any non-zero 5^{th} power $b \in \mathbb{Z}_p^*$, $b^{(p+4)/25}$ is a 5^{th} root of $b \mod p$.

Решение. Возводя в 5-ую степень получим

$$(b^{(p+4)/25})^5 = ((a^5)^{(p+4)/2})^5 = a^{p+4} = a^{p-1} \cdot a^5 = 1 \cdot b = b,$$

где $a^5 = b$. Здесь мы использовали малую теорему Ферма, утверждающую, что $a^{p-1} \equiv 1$ в $\mathbb{Z}_p^*$.

44. Найти примитивный корень из 1 по модулю 17.

Find a primitive root modulo 17.

Решение. Нужно найти вычет $x \in \mathbb{Z}_{17}$, мультипликативный порядок которого равен $16 = 17 - 1$. Таким образом, $x^{16} \equiv 1 \mod 17$, но $x^k \not\equiv 1 \mod 17$ для $0 < k < 16$. Напомним, что ненулевые элементы из $\mathbb{Z}_{17}$ образуют мультипликативную группу. По теореме Лагранжа порядки ненулевых элементов $\mathbb{Z}_{17}$ являются делителями $16 = 17 - 1$. Поэтому непримитивные элементы $\mathbb{Z}_{17}$ имеют порядок $1, 2, 4$ или 8.

Начнем проверку примитивности с 2. Последовательно возводя в степень 2, 4, 8, получим $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^4 = 16 = -1 \neq 1$, и тогда $2^8 = (2^4)^2 = (-1)^2 = 1$. Следовательно, $\mathrm{ord}(2) = 8$ и 2 не является примитивным корнем по модулю 17.

Проверка примитивности для 3:

$$3^1 = 3 \neq 1,\ 3^2 = 9 \neq 1,\ 3^4 = 81 = 13 \neq 1,\ 3^8 = 13^2 = 169 = 16 = -1 \neq 1.$$

Следовательно, $\mathrm{ord}(3) = 16$ и 3 — примитивный корень по модулю 17.

45. Показать, что $f(x) = x^3$ — гомоморфизм $\mathbb{Z}_7^* \to \mathbb{Z}_7^*$. Найти образ и ядро этого гомоморфизма.

Show that $f(x) = x^3$ is a homomorphism $\mathbb{Z}_7^* \to \mathbb{Z}_7^*$. Find the kernel and the image of f.

Решение. Поскольку $\mathbb{Z}_7^*$ — абелева, то

$$f(xy) = (xy)^3 = x^3y^3 = f(x)f(y).$$

Ядро гомоморфизма f:

$$\ker f = \{x \in \mathbb{Z}_7^* : f(x) = 1\} = \{x \in \mathbb{Z}_7^* : x^3 = 1\} = \{1, 2, 4\}.$$

Образ гомоморфизма f:

$$\mathrm{Im} f = f(\mathbb{Z}_7^*) = \{x^3 : x \in \mathbb{Z}_7^*\} = \{1, 6\}.$$

46. Пусть G — группа простого порядка p. Показать, что G — циклическая.

Let G be a group of prime order p. Show that G is cyclic.

Решение. Пусть g — любой элемент, отличный от единичного. Покажем, что g порождает G: $\langle g \rangle = G$. По теореме Лагранжа любая подгруппа

G имеет порядок, являющийся делителем p, поэтому она имеет порядок либо 1, либо p. Подгруппа $\langle g \rangle$ содержит по меньшей мере два различных элемента: единичный e и g (причем $g \neq e$). Таким образом, $|\langle g \rangle| = p$. Следовательно $\langle g \rangle = G$ и G — циклическая группа.

47. Показать, что в коммутативной группе каждая подгруппа является нормальной.

Show that in an abelian group every subgroup is normal.

Решение. Пусть G — коммутативная группа, а N — ее подгруппа. Пусть g принадлежит G. Тогда

$$gNg^{-1} = \{gng^{-1} : n \in N\} = \{gg^{-1}n : n \in N\} = \{n : n \in N\} = N.$$

Таким образом, N является нормальной подгруппой.

48. Показать, что любая коммутативная группа порядка 21, циклическая.

Show that any abelian group of order 21 is cyclic.

Решение. Пусть G — коммутативная группа и $|G| = 21$. По теореме Коши в группе G существуют элементы x, y порядка 3 и 7 соответственно. Покажем, что произведение xy этих элементов имеет порядок 27. Сначала отметим что $\langle x \rangle \cap \langle y \rangle = \{e\}$, так как (по теореме Лагранжа) порядок пересечения должен быть делителем и 3, и 7, а значит, должен быть равным 1. По теореме Лагранжа порядок xy равен одному из делителей порядка группы $|G| = 21$, т.е. 1, 3, 7 или 21.

Если $\mathrm{ord}(xy) = 1$, т.е. $xy = e$, то $x = y^{-1} \in \langle x \rangle \cap \langle y \rangle = \{e\}$. Поэтому $x = y^{-1} = e$, но это невозможно, значит порядок $xy \neq 1$.

Пусть $\mathrm{ord}(xy) = 3$. Тогда $(xy)^3 = e$. Так как группа коммутативная, то $x^3y^3 = e$, и так как $x^3 = e$, то $y^3 = e$. Но $y^7 = e$ по предположению, поэтому если также $y^3 = e$, то $y = y^7 \cdot (y^3)^{-2} = e$, что невозможно, т.к. $y \neq e$. Поэтому порядок $xy \neq 3$. Аналогично можно показать, что $\mathrm{ord}(xy) \neq 7$. Следовательно, $\mathrm{ord}(xy) = 21$, и xy порождает всю группу G, а значит, G является циклической.

49. Пусть h — фиксированный элемент группы G. Определим отображение $f : G \to G$, полагая $f(g) = hgh^{-1}$. Доказать, что f является автоморфизмом группы G.

Fix an element h of a group G. Define $f : G \to G$ by $f(g) = hgh^{-1}$. Prove that f is an automorphism of G.

Решение. Прежде всего покажем, что f — гомоморфизм. В самом деле,

$$f(gg') = h(gg')h^{-1} = (hgh^{-1})(hg'h^{-1}) = f(g)f(g').$$

Таким образом, f — гомоморфизм. Покажем теперь, что f является сюръекцией, т.е. отображением G на G. Для этого нужно показать, что каждый элемент g из G имеет прообраз g', т.е. такой элемент из G, что $f(g') = g$. Согласно определению f для этого нужно показать, что уравнение $g = hg'h^{-1}$ имеет хотя бы одно решение. Из этого уравнения следует, что $g' = h^{-1}gh$. Подставляя это выражение вместо g' в выражение для f, получим $f(g') = h(h^{-1}gh)h^{-1} = g$, что доказывает существование прообраза и, следовательно, сюръективность f.

Наконец, проверим, что f является инъективным отображением. Допустим, что $f(g_1) = f(g_2)$. Тогда $hg_1h^{-1} = hg_2h^{-1}$. Умножая это равенство справа на h и слева на h^{-1}, мы получаем, что $g_1 = g_2$, поэтому f является инъективным отображением. Таким образом, f является изоморфизмом группы G на себя, т.е автоморфизмом.

50. Показать, что любая группа порядка 35 является циклической.

Show that any group of order 35 is cyclic.

Решение. Пусть группа G порядка 35 не является циклической. Тогда в G не существует элемента порядка 35. По Теореме Лагранжа единственные возможные порядки элементов G это 1, 5, 7. При этом каждая подгруппа порядка 5 содержит $4 = 5 - 1$ элементов порядка 5, и две разных подгруппы порядка 5 не имеют общих элементов порядка 5 (опять же по теореме Лагранжа), так как 5 является простым числом. То же самое относится к подгруппам и элементам порядка 7, так как 7 также является простым числом. Согласно теореме Силова, если простое число p является делителем порядка группы, то число подгрупп порядка p имеет вид $pk + 1$ для некоторого целого $k \geqslant 0$. Пусть число подгрупп порядка 5 равно $5x + 1$, а число подгрупп порядка 7 равно $7y + 1$ для некоторых неотрицательных целых чисел x и y. Тогда, подсчитывая элементы G по этим подгруппам, получим:

$$35 = 1 + (5x + 1)(5 - 1) + (7y + 1)(7 - 1).$$

Упрощая, получаем $24 = 20x + 42y$. Так как $42 > 24$, то $y = 0$. Но тогда

$24 = 20x$, а это невозможно, поскольку 20 не делится на 24. Таким образом, в G должен быть элемент порядка 35, поэтому G является циклической.

51. Построить 8 коммутативных групп порядка 900.

List 8 abelian groups of order 900.

Решение. Для решения используем основную теорему о конечнопорожденных абелевых группах. Необходимо найти конечные последовательности целых положительных чисел $d_1, d_2, \ldots, d_n$ больших 1, таких что d_{i+1} делится на d_i, и произведение которых равно 900. Используя теорему Силова, можно решить эту задачу для максимальных степеней простых чисел 2^2, 3^2, 5^2 делящих 900, и тогда объединить результаты. В общем случае для простого числа p существует всего две коммутативных группы порядка p^2: $\mathbb{Z}/p^2\mathbb{Z}$ и $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Таким образом, существует два выбора для $p = 2$, два выбора для $p = 3$ и два выбора для $p = 5$. Таким образом, всего существует $8 = 2^3$ коммутативных групп порядка 900: $\mathbb{Z}_{900}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{450}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_{300}$, $\mathbb{Z}_5 \oplus \mathbb{Z}_{180}$, $\mathbb{Z}_6 \oplus \mathbb{Z}_{150}$, $\mathbb{Z}_{10} \oplus \mathbb{Z}_{90}$, $\mathbb{Z}_{15} \oplus \mathbb{Z}_{60}$, $\mathbb{Z}_{30} \oplus \mathbb{Z}_{30}$.

52. Рассмотрим перестановку

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

Записать σ как произведение независимых циклов. Каков порядок σ? Является ли σ четной перестановкой? Вычислить σ^{-1}.

Consider the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 6 & 9 & 2 & 4 & 8 & 1 & 3 \end{pmatrix}$. Express σ as a product of disjoint cycles. Find the order of σ. Determine whether the permutation σ is even or odd. Find σ^{-1}.

Решение. Имеем $\sigma = (1, 7, 8)(2, 5)(3, 6, 4, 9)$, следовательно, порядок σ равен 12, т.к. $\text{НОК}\,(3, 2, 4) = 12$. Это четная перестановка, т.к. ее декремент равен $2 + 1 + 3 = 6$ — четному числу. Переписывая циклы в обратном порядке, получим $\sigma^{-1} = (1, 8, 7)(2, 5)(3, 9, 4, 6)$.

53. Рассмотрим перестановки

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 1 & 8 & 3 & 6 & 4 & 7 & 9 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 7 & 2 & 6 & 8 & 9 & 3 \end{pmatrix}.$$

Записать каждую из этих перестановок σ, τ , $\sigma\tau$, $\sigma\tau\sigma^{-1}$, σ^{-1}, τ^{-1}, $\tau\sigma$, $\tau\sigma\tau^{-1}$ как произведение независимых циклов.

Consider the permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 1 & 8 & 3 & 6 & 4 & 7 & 9 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 7 & 2 & 6 & 8 & 9 & 3 \end{pmatrix}.$$

Express each of the following permutations σ, τ , $\sigma\tau$, $\sigma\tau\sigma^{-1}$, σ^{-1}, τ^{-1}, $\tau\sigma$, $\tau\sigma\tau^{-1}$ as a product of disjoint cycles.

Решение.

$$\begin{aligned} \sigma &= (1,2,5,3)(4,8,7), \\ \tau &= (2,5)(3,4,7,8,9), \\ \sigma\tau &= (1,2,3,8,9), \\ \sigma\tau\sigma^{-1} &= (1,8,4,7,9)(3,5), \\ \sigma^{-1} &= (1,3,5,2)(4,7,8), \\ \tau^{-1} &= (2,5)(3,9,8,7,4), \\ \tau\sigma &= (1,5,4,9,3), \\ \tau\sigma\tau^{-1} &= (1,5,2,4)(7,9,8). \end{aligned}$$

54. Пусть $\sigma = (2,4,9,7)(6,4,2,5,9)(1,6)(3,8,6) \in S_9$. Записать σ как произведение независимых циклов. Каков порядок σ? Вычислить σ^{-1}.

Let $\sigma = (2,4,9,7)(6,4,2,5,9)(1,6)(3,8,6) \in S_9$. Express σ as a product of disjoint cycles. Find the order of σ. Find σ^{-1}.

Решение. Имеем $\sigma = (1,9,6,3,8)(2,5,7)$, т.о. порядок σ равен $15 = \text{НОК}\,(5,3)$ и $\sigma^{-1} = (1,8,3,6,9)(2,7,5)$.

55. Вычислить порядок

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 2 & 11 & 4 & 6 & 8 & 9 & 10 & 1 & 3 & 5 \end{pmatrix}.$$

Пусть $\sigma = (3,8,7)$. Вычислить порядок $\sigma\tau\sigma^{-1}$.

Calculate the order of $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 2 & 11 & 4 & 6 & 8 & 9 & 10 & 1 & 3 & 5 \end{pmatrix}$. Let $\sigma = (3,8,7)$. Calculate the order of $\sigma\tau\sigma^{-1}$.

Решение. Так как

$$\tau = (1,7,9)(3,11,5,6,8,10),$$

то порядок равен 6. Имеем

$$\sigma\tau\sigma^{-1} = (3,8,7)(1,7,9)(3,11,5,6,8,10)(3,7,8) = (1,3,9)(8,11,5,6,7,10),$$

таким образом, порядок $\sigma\tau\sigma^{-1}$ равен 6.

56. Доказать, что, если $\tau \in S_n$ — перестановка порядка m, то и $\sigma\tau\sigma^{-1}$ имеет тот же порядок m, что и τ, для любой перестановки $\sigma \in S_n$.

Prove that if $\tau \in S_n$ is a permutation of order m then the permutation $\sigma\tau\sigma^{-1}$ has the same order for any $\sigma \in S_n$.

Решение. Предположим, что $\tau \in S_n$ имеет порядок m. Из равенства $(\sigma\tau\sigma^{-1})^k = \sigma\tau^k\sigma^{-1}$ следует, что $(\sigma\tau\sigma^{-1})^m = \sigma\tau^m\sigma^{-1} = \sigma\sigma^{-1} = e$. С другой стороны, порядок $\sigma\tau\sigma^{-1}$ не может быть меньше n. Действительно, если $(\sigma\tau\sigma^{-1})^k = e$, то $\sigma\tau^k\sigma^{-1} = e$ и тогда $\tau^k = \sigma^{-1}\sigma = e$.

57. Перечислить все смежные классы циклической подгруппы $\langle 7\rangle$ из $\mathbb{Z}_{16}^*$. Будет ли фактор-группа $\mathbb{Z}_{16}^*/\langle 7\rangle$ циклической?

List the cosets of $\langle 7\rangle$ in $\mathbb{Z}_{16}^*$. Is the factor group $\mathbb{Z}_{16}^*/\langle 7\rangle$ cyclic?

Решение. Имеем

$$\mathbb{Z}_{16}^* = \{1,3,5,7,9,11,13,15\},\ \langle 7\rangle = \{1,7\}.$$

Классы смежности имеют вид:

$$\langle 7\rangle = \{1,7\},\quad 3\cdot\langle 7\rangle = \{3,5\},\quad 9\cdot\langle 7\rangle = \{9,15\},\quad 11\cdot\langle 7\rangle = \{11,13\}.$$

Т.к. $3^2 \notin \langle 7\rangle$, класс смежности $3\cdot\langle 7\rangle$ имеет порядок $\neq 2$, а именно он должен иметь порядок 4, следовательно, фактор-группа $Z_{16}^*/\langle 7\rangle$ — циклическая.

58. Пусть $G = \mathbb{Z}_6 \times \mathbb{Z}_4$, пусть $H = \{(0,0),(0,2)\}$ и $K = \{(0,0),(3,0)\}$.

a) Перечислить все смежные классы H и смежные классы K.

b) Предположим, что каждая абелева группа порядок 12 изоморфна либо $\mathbb{Z}_{12}$, либо $\mathbb{Z}_6 \times \mathbb{Z}_2$. Какой из этих вариантов верен для G/H? Для G/K?

Let $G = \mathbb{Z}_6 \times \mathbb{Z}_4$, let $H = \{(0,0),(0,2)\}$, and let $K = \{(0,0),(3,0)\}$.

a) List all cosets of H; list all cosets of K.

b) You may assume that any abelian group of order 12 is isomorphic to either $\mathbb{Z}_{12}$ or $\mathbb{Z}_6 \times \mathbb{Z}_2$. Which answer is correct for G/H? For G/K?

Решение. a) Смежные классы $H = \{(0,0),(0,2)\}$:

$$\begin{aligned}
&(0,0)+H=\{(0,0),(0,2)\}, \quad (1,0)+H=\{(1,0),(1,2)\},\\
&(2,0)+H=\{(2,0),(2,2)\}, \quad (3,0)+H=\{(3,0),(3,2)\},\\
&(4,0)+H=\{(4,0),(4,2)\}, \quad (5,0)+H=\{(5,0),(5,2)\},\\
&(0,1)+H=\{(0,1),(0,3)\}, \quad (1,1)+H=\{(1,1),(1,3)\},\\
&(2,1)+H=\{(2,1),(2,3)\}, \quad (3,1)+H=\{(3,1),(3,3)\},\\
&(4,1)+H=\{(4,1),(4,3)\}, \quad (5,1)+H=\{(5,1),(5,3)\}.
\end{aligned}$$

Смежные классы $K = \{(0,0),(3,0)\}$:

$$\begin{aligned}
&(0,0)+K=\{(0,0),(3,0)\}, \quad (0,1)+K=\{(0,1),(3,1)\},\\
&(0,2)+K=\{(0,2),(3,2)\}, \quad (0,3)+K=\{(0,3),(3,3)\},\\
&(1,0)+K=\{(1,0),(4,0)\}, \quad (1,1)+K=\{(1,1),(4,1)\},\\
&(1,2)+K=\{(1,2),(4,2)\}, \quad (1,3)+K=\{(1,3),(4,3)\},\\
&(2,0)+K=\{(2,0),(5,0)\}, \quad (2,1)+K=\{(2,1),(5,1)\},\\
&(2,2)+K=\{(2,2),(5,2)\}, \quad (2,3)+K=\{(2,3),(5,3)\}.
\end{aligned}$$

b) Складывая элементы G с самими собой 6 раз получим 0 в первой компоненте и 0 или 2 — во второй компоненте. Следовательно, порядок элементов G/H самое большее 6 и потому $G/H \approx \mathbb{Z}_6 \times \mathbb{Z}_2$. С другой стороны, $(1,1)+K$ имеет порядок 12 в G/K и, значит, $G/K \approx \mathbb{Z}_{12}$.

59. Пусть G — группа, N и H подгруппы G, причем N — нормальная в G.

a) Доказать, что HN — подгруппа G.

b) Доказать, что N — нормальная подгруппа HN.

c) Доказать, что если $H \cap N = \{e\}$, то HN/N изоморфна H.

Let G be a group, and let N and H be subgroups of G such that N is normal in G.

a) Prove that HN is a subgroup of G.

b) Prove that N is a normal subgroup of HN.

c) Prove that if $H \cap N = \{e\}$, then HN/N is isomorphic to H.

Решение. a) Ясно, что $e = e \cdot e$ принадлежит HN, так что HN непусто. Пусть $x, y \in HN$. Тогда $x = h_1 n_1$ и $y = h_2 n_2$ для некоторых $h_1, h_2 \in H$ и $n_1, n_2 \in N$. Далее

$$xy^{-1} = h_1 n_1 (h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = (h_1 h_2^{-1})(h_2 (n_1 n_2^{-1}) h_2^{-1})$$

и этот элемент принадлежит HN, т.к. из нормальности N получаем, что $h_2(n_1 n_2^{-1})h_2^{-1} \in N$ и, значит $xy^{-1} \in HN$, так что HN — подгруппа G.

b) Т.к. N нормальная в G, она нормальная и в подгруппе HN, которая содержит ее.

c) Определим $\phi : H \to HN/N$, полагая $\phi(x) = xN$ для всех $x \in H$. Тогда $\phi(xy) = xyN = xNyN = \phi(x)\phi(y)$ для всех $x, y \in H$. Каждый класс смежности N в HN имеет вид hnN для некоторых $h \in H$ и $n \in N$. Но тогда $hnN = hN = \phi(h)$, и следовательно, ϕ — сюръекция. Наконец, ϕ — инъекция, т.к. если $h \in H$ принадлежит ядру ϕ, то $hN = \phi(h) = N$, и потому $h \in N$. По предположению $H \cap N = \{e\}$ и следовательно, $h = e$.

Литература

1. *Винберг Э.Б.* Курс алгебры. — М.: Факториал Пресс, 2001.

2. *Кострикин А.И.* Введение в алгебру. Часть I. Основы алгебры. — М.: Физматлит, 2000.

3. *Кострикин А.И.* Введение в алгебру. Часть III. Основные структуры. — М.: Физматлит, 2000.

4. *Курош А.Г.* Курс высшей алгебры. — М.: Наука, 1975.

5. *Проскуряков И.В.* Сборник задач по линейной алгебре. — М.: Наука, 1984.

6. *Фаддеев Д.К.* Лекции по алгебре. — М.: Наука, 1984.

7. *Фаддеев Д.К., Соминский И.С.* Сборник задач по высшей алгебре. — М.: Наука, 1977.

8. *John A. Beachy, William D. Blair.* Abstract Algebra. Waveland Press, Inc., 1996.

СОДЕРЖАНИЕ

1. Целые числа и модульная арифметика 3
2. Отношения и функции 19
3. Многочлены над полем 22
4. Группы 27
Литература 57