МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
КУРГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра алгебры, геометрии и методики преподавания математики

Группы. Кольца. Поля

Методические указания и материалы для практических занятий по алгебре со студентами специальности 010100 - Математика

Курган 2012

Кафедра алгебры, геометрии и методики преподавания математики

Дисциплина: «Алгебра» (специальность 010100 - Математика)

Составитель: доцент О.Н. Шатных

Утверждены на заседании кафедры «06» декабря 2011г.

Рекомендованы методическим
советом университета «12» декабря 2011г.

СОДЕРЖАНИЕ

Введение …….....4
Тема 1. Бинарная алгебраическая операция …….....5
Тема 2. Группы …….....10
Тема 3. Подгруппы……. …….....13
Тема 4. Изоморфизмы и гомоморфизмы групп…….14
Тема 5.Смежные классы по подгруппе……...16
Тема 6.Кольца……20
Тема 7. Подкольца…….23
Тема 8. Гомоморфизмы и изоморфизмы колец……..24
Тема 9. Делимость в кольцах……....26
Тема 10. Идеалы колец……..27
Тема 11. Поля…….29
Тема 12. Упорядоченные поля…….32
Тема 13. Алгебраические числа……. …….....33
Тема 14. Расширения полей…….. …….....38
Список литературы……..…. …42

ВВЕДЕНИЕ

Настоящее пособие составлено в соответствии с программой дисциплины «Алгебра» и предназначено для студентов направления «Математика». Кроме того, пособие будет полезно студентам направления «Педагогическое образование» профиля «Математическое образование», которые также изучают данный раздел алгебры, но в несколько меньшем объеме.

Раздел «Алгебраические системы» изучается в третьем семестре. В данном пособии представлены все темы раздела, которые выносятся на практические занятия. Для каждой темы указаны вопросы для повторения теоретического материала, приведены образцы решения типовых задач и список задач для решения.

Тема 1. Бинарная алгебраическая операция. Свойства бинарной алгебраической операции

Вопросы теории

1. Бинарная алгебраическая операция на множестве. Примеры.
2. N-арная операция на множестве. Примеры.
3. Свойства бинарной алгебраической операции.
4. Нейтральный элемент относительно операции.
5. Симметричный к данному элемент относительно бинарной алгебраической операции.
6. Понятие обратимой операции.
7. Алгебраическая система.
8. Полугруппа, виды полугрупп.

Образцы решения задач

Задача 1. Покажем, что во множестве *M* невырожденных матриц *n-го* порядка $(n \geq 1)$ матричное сложение не является бинарной операцией, а матричное умножение – бинарная операция.

Решение. а) Для доказательства первого утверждения достаточно привести пример двух таких невырожденных матриц, сумма которых является вырожденной матрицей. Возьмем, например, матрицы:

$$A = \begin{pmatrix} 2 & 3 \\ 5 & -2 \end{pmatrix} \text{ и } B = \begin{pmatrix} 2 & -1 \\ -5 & 2 \end{pmatrix}.$$

Поскольку

$$|A| = \begin{vmatrix} 2 & 3 \\ 5 & -2 \end{vmatrix} = -19 \neq 0 \text{ и } |B| = \begin{vmatrix} 2 & -1 \\ -5 & 2 \end{vmatrix} = -1 \neq 0,$$

то матрицы *A* и *B* являются невырожденными. Сумма же их – матрица $C = A + B = \begin{pmatrix} 4 & 2 \\ 0 & 0 \end{pmatrix}$ уже не принадлежит множеству невырожденных матриц, поскольку

$$|C| = 0.$$

б) Пусть *A* и *B* – любые невырожденные матрицы *n-го* порядка:

$$|A| \neq 0, \quad |B| \neq 0.$$

Матрица $A \otimes B = C$ есть снова матрица *n-го* порядка. Нам остается лишь доказать, что матрица *C* является невырожденной.

Поскольку, как известно, определитель произведения двух матриц равен произведению определителей этих матриц, то есть:

$$|C| = |A \otimes B| = |A| \cdot |B|,$$

то с учетом (1) получаем, что $|C| \neq 0.$ Итак, матрица $C = A \otimes B$ является невырожденной, то есть является элементом того же множества, что и матрицы *A* и *B*. По определению бинарной операции умножение во множестве невырожденных матриц *n-го* порядка является бинарной операцией, а само множество невырожденных матриц с операцией умножения, то есть $<M; \otimes>$, является алгебраической системой.

Задача 2. Докажите, что на множестве R бинарная операция, заданная формулой $a \circ b = \frac{a+b}{2}$, коммутативна, но не ассоциативна. Выясните, является ли R полугруппой относительно бинарной операции нахождения среднего арифметического?

Решение. Пусть a, b, c – действительные числа. В силу коммутативности сложения на R получим:

$$a \circ b = \frac{a+b}{2} = \frac{b+a}{2} = b \circ a ,$$

то есть бинарная операция нахождения среднего арифметического на R коммутативна.

Далее:

$$(a \circ b) \circ c = \frac{\frac{a+b}{2} + c}{2} = \frac{a+b+2c}{4} \qquad (1)$$

и

$$a \circ (b \circ c) = \frac{a + \frac{b+c}{2}}{2} = \frac{2a+b+c}{4} . \qquad (2)$$

Из результатов (1) и (2) следует, что при $a \neq c$ равенство $(a \circ b) \circ c = a \circ (b \circ c)$ не является справедливым. Следовательно, заданная операция не ассоциативна на R. В силу вышедоказанного R не является полугруппой относительно бинарной операции нахождения среднего арифметического.

Задача 3. Докажем, что во множестве K, содержащем не менее двух элементов, на котором формулой $a \circ b = b$ задана бинарная операция, не существует нейтрального элемента.

Решение. Допустим, что в K существует нейтральный элемент e, и пусть a – любой элемент из K. По определению нейтрального элемента $a \circ e = a$, а из условия примера следует, что $a \circ e = e$, то есть $a = e$. Это означает, что K состоит из одного элемента. Полученный результат противоречит условию, а потому сделанное допущение ошибочно.

Задача 4. Докажите, что на множестве M матриц вида $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, где x – любое действительное число, бинарная операция матричного умножения обратима.

Решение. Известно, что на множестве квадратных матриц одного и того же порядка операция матричного умножения ассоциативна. Следовательно, рассматриваемая операция ассоциативна на множестве M.

Пусть $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ - любая матрица из M. По правилу умножения матриц получим:

$\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}=A$, и потому матрица $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\in M$ есть нейтральный элемент. Итак, *M* обладает нейтральным элементом.

Так как $|A|=\begin{vmatrix}1 & a\\ 0 & 1\end{vmatrix}=1\neq 0$, то матрица $A=\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$ является невырожденной, и, следовательно, она имеет обратную матрицу. Применяя один из способов нахождения обратных матриц, найдем, что $A^{-1}=\begin{pmatrix}1 & -a\\ 0 & 1\end{pmatrix}$, - $a \in$ R, а потому $A^{-1}\in M$.

Итак, для любого элемента из *M* во множестве *M* существует обратный элемент.

Полученные результаты позволяют сделать вывод, что операция матричного умножения обратима на множестве *M.*

Задачи для решения

1. Какие из арифметических действий (сложение, вычитание, умножение, деление) являются бинарными операциями:
а) на множестве $\{1,0,-1\}$;
б) на множестве **N**;
в) на множестве **Z**?

2. Является ли вычитание бинарной операцией на множестве $A=\{-3,-2,-1,0,1,2,3\}$?

3. Является ли бинарной операцией:
а) умножение на множестве иррациональных чисел;
б) сложение на множестве четных чисел;
в) сложение на множестве нечетных чисел;
г) нахождение десятичных логарифмов на множестве R^+;
д) нахождение среднего геометрического двух чисел на множестве R^+;
е) нахождение наибольшего общего делителя на множестве **N**?

4. Является ли бинарной операцией матричное умножение на множестве:
а) матриц вида $\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}$, где *a* – любое действительное число;
б) треугольных матриц третьего порядка, то есть матриц вида $\begin{pmatrix}a_{1i} & 0 & 0\\ a_{2i} & a_{22} & 0\\ a_{3i} & a_{32} & a_{33}\end{pmatrix}$, где *aij* – любые действительные числа?

5. Является ли алгебраической системой множество чисел вида $a+b\sqrt{5}$, $a,b\in Z$, относительно: а) сложения; б) вычитания; в) умножения?

6. Докажите, что на множестве R^+ бинарная операция $a \circ b = \sqrt{a \cdot b}$ нахождения среднего геометрического коммутативна, но не ассоциативна.

7. Почему действие, выполняемое по правилу $a \circ b = a^2 - b^2$, не является бинарной операцией на множестве **N** и является таковой на множестве **Z**? Выясните, коммутативна ли указанная операция на **Z**; покажите также, что она не является ассоциативной на этом множестве.

8. Покажите, что действие, выполняемое по правилу $a \circ b = a^2 + b^2$, является коммутативной, но не ассоциативной бинарной операцией на множестве **R**.

9. Покажите, что на некотором множестве бинарная операция, заданная формулой $a \circ b = b$, некоммутативна, но ассоциативна.

10. Является ли множество **Z** полугруппой относительно: а) сложения; б) вычитания?

11. Является ли множество **N** полугруппой относительно операции нахождения наибольшего общего делителя?

12. Покажите, что множество $\{1,0,-1\}$ образует полугруппу относительно обычной операции умножения.

13. Покажите, что множество четырехмерных арифметических векторов вида (*a, b, b, 0*), где $a, b \in N$, образует полугруппу относительно операции сложения арифметических векторов.

14. Пусть ***I*** – множество, состоящее из всех подмножеств данного множества *M*. Покажите, что *I* образует полугруппу относительно операции пересечения подмножеств.

15. Почему множество **R** не является полугруппой относительно действия, выполняемого по правилу $a \circ b = a^2 + b^2$ для любых $a, b \in \boldsymbol{R}$?

16. Обладает ли множество чисел вида $a + b\sqrt{5}$, где a и b – любые целые числа, нейтральным элементом относительно обычного умножения? Проверьте, имеются ли в данной алгебраической системе обратные элементы для элементов $2 + \sqrt{5}$ и $5 - 2\sqrt{5}$. Обратима ли на данном множестве операция умножения?

17. Докажите, что бинарная операция матричного умножения на множестве матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где a – любое не равное нулю действительное число,

обратима. Найдите обратные элементы для матриц $A=\begin{pmatrix}-2 & 0\\ 0 & -2\end{pmatrix}$, $B=\begin{pmatrix}\sqrt{2} & 0\\ 0 & \sqrt{2}\end{pmatrix}$, $C=\begin{pmatrix}\frac{1}{3} & 0\\ 0 & \frac{1}{3}\end{pmatrix}$.

18. Докажите, что относительно бинарной операции $a\circ b=\sqrt{a\cdot b}$, множество R^+ не обладает нейтральным элементом. Обратима ли эта операция на множестве R^+?

19. Пусть ***I*** – множество подмножеств некоторого непустого множества *M*. Существует ли в ***I*** нейтральный элемент (если существует, то какой) относительно операции объединения подмножеств на ***I***; пересечения подмножеств? Какие элементы из множества ***I*** имеют обратные? Обратимы ли указанные операции на множестве ***I***?

20. Докажите, что на множестве **Z** действие, выполняемое по правилу $a\circ b=\begin{vmatrix}0 & a\\ b & 0\end{vmatrix}$, является бинарной, коммутативной, ассоциативной, но необратимой операцией. Обладает ли алгебраическая система $<Z;\circ>$ нейтральным элементом, и если обладает, то каким именно?

21. Докажите, что на множестве **Q** действие, выполняемое по правилу $a\circ b=\frac{a\cdot b}{2}$, является бинарной операцией, которая коммутативна, ассоциативна, но не обратима. Каким нейтральным элементом обладает алгебраическая система $<Q;\circ>$? Для элемента $a = 8$ найдите обратный.

22. Являются ли действия, выполняемые по формулам:

а) $a\circ b=(a+b)^2$;

б) $a\circ b=\frac{a+b}{2}$;

в) $a\circ b=\frac{a}{b}$;

г) $a\circ b=a^b$;

д) $a\circ b=a+b-7ab$;

е) $a\circ b=\max(a,b)$;

ж) $U\circ V=U\bigcup V$;

з) $U\circ V=U\bigcap V$;

бинарными операциями на Q, N на множестве вещественных чисел, и если являются, то почему?

23. Какие из нижеприведенных бинарных операций:

а) $a\circ b=a^b$;

б) $a\circ b=c$, с – наибольший общий делитель чисел a и b;

в) $a\circ b=m$, где m – наименьшее общее кратное чисел a и b

коммутативны, ассоциативны на N?

24. Выясните, какими свойствами обладают операции:

а) $a * b = \frac{a}{b} + \frac{b}{a}$ на R/{0};

б) $U * V = U \bigcup V$ на совокупности подмножеств вещественных чисел;

в) $U * V = U / V$ в совокупности подмножеств вещественных чисел;

г) $a * b = a - b$ на R;

д) операция * в множестве учеников класса определяется так, если a и b – два ученика, то $a*b$ – тот из них, кто первым записан на странице классного журнала (если $a = b$, то $a*b = a = b$).

25. Покажите, что действие, выполняемое по правилу $a \circ b = a^2 + b^2$, является коммутативной, но не ассоциативной бинарной операцией на R.

26. Для следующих операций, определенных на множестве R^+, докажите:

а) операция $a*b = ab - ba$ дистрибутивна относительно сложения; умножения;

б) $a*b = \sqrt{ab}$ дистрибутивна относительно операции умножения.

27. Докажите, что относительно бинарной операции $a \circ b = \frac{a+b}{2}$ множество R не содержит нейтрального элемента.

Тема 2. Группы

Вопросы теории

1. Определение группы. Примеры.
2. Виды групп.
3. Подстановки.
4. Симметрическая группа подстановок n-й степени.

Образцы решения задач

Задача 1. Доказать, что множество Z образует группу относительно действия, заданного формулой:

$$a \circ b = \begin{cases} a + b, a - четно, b - целое, \\ a - b, a - нечетно, b - целое. \end{cases}.$$

Доказательство. 1. Рассматриваемое на Z действие сводится к сложению или вычитанию целых чисел, а поскольку как сложение, так и вычитание элементов из Z дает в результате элемент из Z, то на множестве Z рассматриваемое действие является бинарной операцией.

2. Проанализируем возможные случаи:

а) Если a, b – четные числа, а c – любое число из Z, то:

$a \circ (b \circ c) = a + (b + c),$

$(a \circ b) \circ c = (a + b) + c = a + (b + c),$

то есть $a \circ (b \circ c) = (a \circ b) \circ c.$

б) Если a – четное число, b – нечетное число, а c – любое число из Z, то:

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

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

то есть $a \circ (b \circ c) = (a \circ b) \circ c.$

в) Если a – нечетное число, b – четное число, а c – любое число из Z, то $a - b$ нечетно и потому:

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

$(a \circ b) \circ c = (a - b) - c,$

то есть $a \circ (b \circ c) = (a \circ b) \circ c.$

г) Если a, b – нечетные числа, а c – любое число из Z, то $a - b$ четно и потому:

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

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

то есть $a \circ (b \circ c) = (a \circ b) \circ c.$

Итак, во всех возможных случаях заданная на Z бинарная операция является ассоциативной.

3. Так как 0 – четное число, то $0 \circ a = 0 + a = a.$ Кроме того, если a четно, то $a \circ 0 = a + 0 = a$; если же a нечетно, то $a \circ 0 = a - 0 = a$. Итак, $0 \circ a = a \circ 0 = a$, то есть 0 является в Z нейтральным элементом относительно заданной операции.

4. Для любого элемента $a \in Z$ в Z существует обратный элемент: для четного a обратным будет противоположное число $-a$, так как $a \circ (-a) = a + (-a) = 0$; для нечетного a обратным будет само число a, так как $a \circ a = a - a = 0$.

Итак, Z является группой относительно заданной операции.

Однако эта группа не является абелевой, поскольку $4 \circ 5 = 4 + 5 = 9, 5 \circ 4 = 5 - 4 = 1$, то есть $4 \circ 5 \neq 5 \circ 4.$

Задачи для решения

1. Выясните, какие из нижеприведенных множеств являются группами относительно нижеуказанных операций:

а) множество **Z** относительно вычитания;

б) множество четных чисел относительно умножения;

в) множество целых чисел, кратных любому заданному натуральному числу n, относительно сложения;

г) множество Q^+ относительно умножения;

д) множество **Q** относительно умножения;

е) множество **Q** \ {0} относительно умножения;

ж) множество **R** \ {0} относительно умножения;

з) множество квадратных матриц n-го порядка относительно сложения, умножения;

и) множество матриц n-го порядка с определителем, равным 1, относительно умножения матриц, сложения;

к) множество решений любой заданной системы линейных однородных уравнений относительно сложения;

л) множество трехмерных (n-мерных) арифметических векторов относительно сложения;

м) множество чисел вида $a + b\sqrt{2}$ относительно сложения, если a и b – любые рациональные числа;

н) множество параллельных переносов в плоскости относительно операции их последовательного выполнения;

о) множество многочленов одной и той же степени n от одного аргумента относительно сложения;

п) множество многочленов степени не выше n относительно сложения;

р) множество многочленов от одного аргумента относительно сложения;

с) множество матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где $a \in \boldsymbol{R}$ относительно сложения матриц;

т) множество матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где $a \in \boldsymbol{R}$, $a \neq 0$, относительно сложения матриц.

2. Докажите, что множество матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, где a и b –действительные, отличные от нуля числа, составляют группу относительно матричного умножения.

3. Докажите, что множество матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где a и b – любые, не равные одновременно нулю действительные числа, образует группу относительно матричного умножения.

4. Докажите, что множество матриц вида $\begin{pmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, где $aii \neq 0$ (I = 1, 2, 3), является группой относительно матричного умножения.

5. Составьте таблицу умножения элементов симметрической группы $S3$ подстановок 3-й степени, обозначив элементы этой группы буквами. По таблице найдите взаимно обратные элементы этой группы и докажите, что рассматриваемая группа не является коммутативной.

6. Для множества $G1 = \{p_0, p_1, p_2, p_3\}$, состоящего из подстановок $p_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, $p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$, составьте таблицу умножения и с ее помощью убедитесь, что $G1$ – абелева группа.

7. Дано множество $M = \{a_0, a_1, a_2\}$ поворотов (вращений) правильного треугольника в плоскости этого треугольника вокруг его центра против часовой

стрелки соответственно на углы 0º, 120º, 240º. Эти повороты совмещают треугольник с самим собой. Последовательное выполнение двух любых таких поворотов называется *произведением (композицией)* этих двух поворотов. Докажите, что *M* является группой относительно введенной в *M* операции.

8. На множестве **Q** \ {0} определено действие $a \circ b = \frac{a \cdot b}{2}$. Докажите, что относительно указанного действия данное множество является группой.

9.Пусть G – множество всевозможных троек чисел вида $(k_1; k_2; 1)$ и $(k_1; k_2; -1)$ и пусть на G определено действие, выполняемое по правилу $(k_1; k_2; \varepsilon) \circ (l_1; l_2; \delta) = (k_1 + l_1; k_2 + l_2; \varepsilon\delta)$. Докажите, что относительно указанного действия G является группой.

Тема 3. Подгруппы

Вопросы теории

1. Определение подгруппы.
2. Циклическая подгруппа. Циклическая группа.
3. Образующий циклической группы.
4. Порядок элемента группы.
5. Порядок группы.

Образцы решения задач

Задача 1. Доказать, что множество *A* целых чисел, кратных трем, есть подгруппа аддитивной группы **Z.**

Решение. Имеем:

1) $A = \{x | x = 3k, k \in Z\}$, $A \subset$ Z. (1)

2) Пусть *x1*, *x2* – любые элементы из *A*, то есть *x1* = 3*k1*, *x2* = 3*k2*, $k_1, k_2 \in Z$. Так как **Z** есть аддитивная группа, то $k_1 + k_2 \in Z$ и потому
$$x_1 + x_2 = 3k_1 + 3k_2 = 3(k_1 + k_2) \in A. \quad (2)$$

3) Пусть $x = 3k$ есть любой элемент из *A*, следовательно, $k \in Z$; тогда и $-k \in Z$, а потому
$$-x = -3k = 3 \cdot (-k) \in A. \quad (3)$$

Из (1), (2), (3) следует, что *A* есть подгруппа аддитивной группы Z.

Задачи для решения

1. Докажите, что множество четных чисел является подгруппой аддитивной группы **Z** целых чисел. Является ли множество нечетных чисел подгруппой группы **Z**?

2. Пусть *n* – заданное натуральное число. Показать, что множество целых чисел, кратных *n*, является подгруппой аддитивной группы **Z.**

3. Докажите, что множество целых степеней 3 является подгруппой мультипликативной группы **Q** \ {0}. Запишите эту подгруппу символически.

Является ли она циклической? Каков порядок элемента, порождающего эту подгруппу?

4. Найдите порядки элементов $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, $\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ мультипликативной группы невырожденных матриц второго порядка.

5. Найдите порядок каждого элемента симметрической группы S3 третьей степени, а затем выясните, какие циклические подгруппы S3 они порождают. Сколько всего различных подгрупп имеет группа S3? Является ли A3 циклической подгруппой группы S3? Каковы ее образующие? (A3 – знакопеременная группа третьей степени.)

6. Найдите порядок элемента $a = (1243) \in S_4$ и постройте циклическую подгруппу группы S_4, порожденную элементом a.

7. Сколько подгрупп имеет группа $\left\{e=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, a=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, b=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, c=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\right\}$?

8. Элементы группы G всех самосовмещений квадрата представьте подстановками четвертой степени. Составьте для группы G таблицу Кэли. Изоморфно отобразите группу G на одну из подгрупп симметрической группы S8 восьмой степени.

9. Докажите, что симметрическая группа S_n при любом натуральном $n \geq 5$ содержит подгруппу, изоморфную знакопеременной группе A_5.

Тема 4. Гомоморфизм и изоморфизм групп

Вопросы теории

1. Гомоморфизм групп.
2. Свойства гомоморфизма.
3. Ядро гомоморфизма.
4. Биективное отображение.
5. Изоморфизм групп.
6. Свойства изоморфизма.

Образцы решения задач

Задача 1. Доказать, что мультипликативную группу M невырожденных матриц порядка n ($n \geq 1$) можно гомоморфно отобразить на мультипликативную группу $\mathbf{R} \setminus \{0\}$ действительных чисел, отличных от нуля.

Решение. Отобразим группу M в группу $\mathbf{R} \setminus \{0\}$ по правилу φ, которое каждой матрице $A \in M$ ставит в соответствие ее определитель $|A|$ - элемент из $\mathbf{R} \setminus \{0\}$. Так как при этом отображении для любого заданного элемента из $\mathbf{R} \setminus \{0\}$ полный прообраз есть непустое множество (так как существует бесконечно много матриц из M, определитель которых равен заданному действительному числу), то φ является отображением M на $\mathbf{R} \setminus \{0\}$. Более того, такое отображение сохраняет операцию. Действительно, если A, B – любые элементы

из группы M, то и $AB \in M$, и по теореме об определителе произведения матриц получим:

$\varphi(AB) = |AB| = |A| \cdot |B| = \varphi(A)\varphi(B).$

Итак, φ есть отображение группы M на группу **R** \ {0}, сохраняющее операцию, то есть гомоморфное отображение.

Задачи для решения

1. Докажите, что если $\varphi : G \to F$ – гомоморфизм группы G на группу F и при этом группа G коммутативна, то и группа F коммутативна. Верно ли обратное утверждение?
2. Докажите, что если $\varphi_1 : G1 \to G2$ и $\varphi_2 : G2 \to G3$ гомоморфизмы, то и $\varphi_1 \cdot \varphi_2 : G1 \to G3$ – гомоморфизм.
3. Аддитивная группа **Z** гомоморфно отображена на циклическую группу G = (g) $= \{g^0, g, g^2, ..., g^{n-1}\}$. Какие элементы из **Z** отображаются на элемент g^0, какие – на элемент g при этом гомоморфизме? Найдите ядро гомоморфизма.

4. Почему аддитивную группу **Z** можно гомоморфно отобразить на знакопеременную группу $A_3 = \{e = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix},\ a = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix},\ b = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}\}$?
5. Докажите, что симметрическая группа S3 третьей степени является гомоморфным образом симметрической группы S4 четвертой степени.
6. Докажите, что аддитивную группу всех функций вида $ax + b$ $(a \in R, b \in R)$ можно гомоморфно отобразить на аддитивную группу **R**. Каково ядро этого гомоморфизма?
7. Докажите, что аддитивную группу R^2 всех арифметических двумерных векторов с действительными компонентами можно гомоморфно отобразить на аддитивную группу **R**. Единственно ли такое отображение?
8. Докажите, что отображение φ, заданное правилом $x \xrightarrow{\varphi} |x| \in R^+$, является гомоморфизмом группы R \ {0} на R^+ (обе группы – мультипликативные).
9. Докажите, что при гомоморфизме φ группы G1 на группу G2: а) группа G1 некоммутативна, если некоммутативна группа G2; б) группа G1 бесконечна, если бесконечна группа G2; в) элемент $a \in G_1$ такой, что $\varphi(a)$ имеет бесконечный порядок, является элементом, имеющим бесконечный порядок.
10. Докажите, что аддитивная группа **Z**, аддитивная группа черных чисел и мультипликативная группа целых степеней числа 2 изоморфны между собой.
11. Докажите, что аддитивная группа **R** изоморфна группе матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где $a \in \boldsymbol{R}$, относительно матричного сложения.
12. Докажите, что множество двумерных арифметических векторов *(a, b)* и множество матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, где $a, b \in \boldsymbol{R}$, являются изоморфными группами относительных операций сложения в этих множествах.

13.Выясните, изоморфна ли группа Q^+ по умножению группе **Q** по сложению.

Указание. Предположим, что существует изоморфное отображение $\varphi : Q^+ \to$Q. Пусть $\varphi(1) = a$. Тогда $\varphi(n) = a^n$ при любом натуральном n (тем самым $a \neq 1$) и $\varphi\left(\frac{1}{n}\right) = a^{\frac{1}{n}}$. Значит, число $a \in$ Q должно быть таким, что $\sqrt[n]{a} \in Q$ при любом натуральном n. Покажите, что такого числа $a \neq 1$ не существует.

14.Выясните, изоморфна ли группа всех самосовмещений ромба группе всех самосовмещений прямоугольника.

15.Группу самосовмещений правильного треугольника изоморфно отобразите на симметрическую группу S3.

16.Докажите изоморфизм групп $(M,+)$ и $(M',+)$, где $M = \{x \mid x = 3k, k \in Z\}, M' = \{x \mid x = 2k, k \in Z\}$.

17.Докажите, что аддитивная группа целых чисел гомоморфна мультипликативной группе $(\{1, -1\},)$.

18.Какие из следующих отображений являются изоморфными отображениями указанных алгебр:

а) $f : (Z,+) \to (Z,+), f(a) = -a$;

б) $f : (N,+) \to (N,), f(a) = 2^a$;

в) $f : (R^+,) \to (R^+,), f(a) = \frac{1}{a}$;

г) $f : (R^+,) \to (R\ ,+), f(a) = \ln a$;

д) $f : (R\ ,+) \to (R,), f(a) = \sin a$.

Тема 5. Смежные классы по подгруппе. Факторгруппа

Вопросы теории

1. Понятие левого и правого смежных классов группы по подгруппе.
2. Левое и правое разложение группы по подгруппе.
3. Нормальный делитель группы.
4. Факторгруппа группы по ее нормальному делителю.
5. Теорема Лагранжа.

Образцы решения задач

Задача 1. Найти левое и правое разложение симметрической группы S3 $= \{e = (1) = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, a_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, a_2 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, a_3 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, a_4 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, a_5 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\}$ по ее подгруппе $A = \{e, a_1\}$. Совпадают ли они между собой?

Решение. а) Найдем левое разложение группы S3 . В качестве первого левого класса можно взять смежный класс элемента *e*, то есть саму подгруппу $A = \{e, a_1\}$. Возьмем любой элемент из S3, не вошедший в первый класс, например элемент *a2* , и умножим его справа на элементы подгруппы

$A: a_2 e = a_2, a_2 a_1 = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix} = a_4$. Получим второй смежный класс: $a_2 A = \{a_2, a_4\}$. Далее возьмем из группы S3 элемент, который не вошел в два построенных смежных класса, например *a5* . С его помощью получим третий класс: $a_5 A = \{a_3, a_5\}$. В построенные классы вошли все элементы группы S3, то есть $A \cup a_2 A \cup a_5 A = \{e, a_1\} \cup \{a_2, a_4\} \cup \{a_3, a_5\} =$ S3. Эти классы попарно не пересекаются. Следовательно, классы *A,* $a_2 A$, $a_5 A$ составляют искомое левое разложение группы по ее подгруппе *A*.

б) Найдем правое разложение группы S3 по подгруппе *A*. Первый правый класс – сама подгруппа $A = \{e, a_1\}$, второй правый класс - $Aa_2 = \{a_2, a_3\}$. Далее возьмем любой элемент из S3, не вошедший в эти классы, например a_5, и с его помощью получим третий правый класс: $Aa_5 = \{a_4, a_5\}$. Так как эти классы не пересекаются и $A \cup Aa_2 \cup Aa_5 = \{e, a_1, a_2, a_3, a_4, a_5\}$ = S3, то классы $A = \{e, a_1\}$, $Aa_2 = \{a_2, a_3\}$, $Aa_5 = \{a_4, a_5\}$ составляют правое разложение группы S3 по подгруппе *A*.

в) Так как $a_5 A \neq Aa_5$, то левое и правое разложения группы S3 по подгруппе *A* не совпадают.

Задача 2. Построить факторгруппу аддитивной группы ***Z*** по ее подгруппе *B* = (5) = $\{x | x = 5k, k \in Z\}$. Найти сумму смежных классов 3+*B*, 4+ *B* и элемент факторгруппы **Z**/*B*, противоположный элементу 2+*B*.

Решение. Аддитивная группа ***Z*** коммутативна, а потому любая ее подгруппа, в том числе и данная циклическая подгруппа *B*, является нормальным делителем группы ***Z***. Следовательно, оба разложения группы ***Z*** по подгруппе *B* одинаковы – левые и правые классы соответственно совпадут и из них составится одна определенная факторгруппа. Разбиваем группу ***Z*** с помощью ее подгруппы *B* на попарно непересекающиеся классы. За первый смежный класс берем саму подгруппу *B* = (5) ={…, -15, -10, -5, 0, 5, 10, 15, …} = 0+*B* – этот класс состоит из всех тех целых чисел, которые кратны 5; второй смежный класс порождаем с помощью какого-либо целого числа, не вошедшего в первый класс, например с помощью числа 1, непосредственно следующего за 0, путем сложения 1 с элементами подгруппы $B: 1 + B = \{x | x = 1 + 5k, k \in Z\}$ ={…,-14, -9, -4, 1, 6, 11, 16, ….}. В этот класс войдут, как видим, все те целые числа, которые при делении на 5 дают остаток 1. Третий класс образуем из всех тех целых чисел, которые при делении на 5 дают остаток 2; это будет класс $2 + B = \{x | x = 2 + 5k, k \in Z\}$. Аналогично четвертый класс $3 + B = \{x | x = 3 + 5k, k \in Z\}$; пятый класс 4+ *B*. А так как при делении целых чисел на 5 остатки могут быть лишь числа 0, 1, 2, 3, 4, то с помощью подгруппы *B* = (5) никаких других смежных классов, которые были бы отличны от найденных, получить нельзя. Построенные нами смежные классы полностью исчерпывают элементы данной группы ***Z***, то есть $B \cup [1 + B] \cup [2 + B] \cup [3 + B] \cup [4 + B] = Z$. Как легко заметить, полученные классы не имеют общих элементов, то есть попарно не пересекаются. Следовательно, они составляют разбиение множества

Z, то есть разложение группы ***Z*** по нормальному делителю B. Итак, $\mathbf{Z}/B = \{B, 1 + B, 2 + B, 3 + B, 4 + B\}$ есть искомая факторгруппа. Она является также аддитивной группой. По правилу сложения элементов в аддитивной факторгруппе имеем: $(3+B) + (4+B) = (3+4) + B = 7 + B = \{x | x = 7 + 5k = 2 + (5 + 5k) = 2 + 5t, t \in Z\} = 2 + B$;
$(3+B) + B = (3+B) + (0 + B) = (3 + 0) + B = 3 + B$. Аналогично $B + (3 + B) = 3 + B$, поэтому элемент B в группе $\mathbf{Z}/B$ является нулевым. Поскольку $(2 + B) + (3 + B) = (2 + 3) + B = 5 + B = \{x | x = 5 + 5k = 5(1 + k) = 5s, s \in Z\} = B$, элемент $3+B$ является противоположным для элемента $2 + B$.

Задачи для решения

1. Найдите все левые смежные классы группы самосовмещений правильного треугольника: а) по подгруппе M поворотов треугольника; б) по подгруппе $A = \{e, a\}$, где a – одна из симметрий.

2. Известно, что H – любая подгруппа группы G и $x \in H$. Докажите, что $xH = Hx = H$.

3. Докажите, что если элемент y входит в левый смежный класс xH по H, порожденный элементом x, то смежный класс yH совпадает со смежным классом xH.

4. Аддитивную группу $\mathbf{Z}$ гомоморфно отобразите на фактор группу Z / H_3, где $H_3 = (3) = \{x | x = 3k, k \in Z\}$.

5. Постройте левое и правое разложение группы G самосовмещений правильного треугольника: а) по подгруппе M вращений этого треугольника, результаты сравнить; б) по подгруппе $A = \{e, a\}$, где a – одна из симметрий.

6. Постройте левое и правое разложение группы самосовмещений квадрата по подгруппе $A = \{e, a\}$, где a – отражение относительно диагонали.

7. Что представляют собой разложения произвольной группы G по ее единичной подгруппе и по самой G?

8. Группа содержит 4 элемента, из которых лишь один имеет порядок 4. Какой порядок имеют остальные элементы группы, сколько подгрупп имеет эта группа?

9. Сколько подгрупп может иметь группа G, содержащая 17 элементов?

10. Докажите, что если H – подгруппа группы G, а x – некоторый элемент из G, то множество $H_x = xHx^{-1}$ является подгруппой G. В группе G самосовмещений квадрата найдите все подгруппы вида $H_x = xHx^{-1}$, где H – группа поворотов квадрата.

11. Докажите, что если порядок подгруппы в 2 раза меньше порядка самой группы, то эта подгруппа является нормальным делителем группы.

12. Докажите, что подгруппа H группы G является нормальным делителем тогда и только тогда, когда для любого элемента a из H и любого элемента g из G элемент gag^{-1} содержится в H.
Примечание. Элемент gag^{-1} называется сопряженным элементу a.

13. В группе всех самосовмещений квадрата взята подгруппа $H = \{a_0, a\}$, где a_0 - тождественное преобразование, a – отражение относительно одной из диагоналей квадрата. Является ли H нормальным делителем.

14. Найдите все нормальные делители в симметрической группе S3 третьей степени.

15. Докажите, что группа A_5 не содержит нормальных делителей, кроме единичной подгруппы и всей группы.

16. Докажите, что в мультипликативной группе G вещественных невырожденных матриц n-го порядка подмножество H матриц, определитель которых равен 1, является нормальным делителем. Как можно охарактеризовать смежные классы по H?

17. Составьте факторгруппу группы самосовмещений квадрата по ее нормальному делителю $A = \{a_0, a\}$.

18. Докажите, что если группа Является циклической с образующей a, то и факторгруппа этой группы по любому ее нормальному делителю H будет также циклической с образующей aH.

19. Почему подгруппа $A = \{x | x = 3k, k \in Z\}$ аддитивной группы $\boldsymbol{Z}$ является нормальным делителем группы $\boldsymbol{Z}$? Постройте факторгруппу $\boldsymbol{Z} / A$. Будет ли она циклической? Если да, то каков будет ее образующий элемент и как ее элементы могут быть записаны через этот образующий элемент?

Примечание. Если число смежных классов (левых или правых) группы G по ее подгруппе H конечно, то это число называют индексом подгруппы H (в группе G).

20. Постройте факторгруппу $\boldsymbol{Z} / A$, где A =(6) = $\{x|x = 6k, k \in Z\}$. Будет ли она абелевой? Найдите (6 + A) + (9 + A) и (9 + A) + (6 + A).

21. Постройте факторгруппу $\boldsymbol{Z} / A \cap B$, где A = (6), B = (4), и составьте для нее таблицу сложения. Найдите элемент, противоположный элементу 5 + M, где M = A$\cap B$.

22. Будет ли A = $\{x|x = 12k, k \in Z\}$ =(12) подгруппой, нормальным делителем группы M = $\{y|y = 3k, k \in Z\}$ = (3)? Ответ обоснуйте. Постройте факторгруппу M / A и таблицу сложения ее элементов.

23. На множестве G всевозможных троек целых чисел определена бинарная операция $(k_1, k_2, k_3) \circ (s_1, s_2, s_3) = (k_1 + s_1, k_2 + s_2, k_3 + s_3)$. Докажите, что система G = $< G; \circ >$ является группой и что подгруппа $H = \{x|x = (k,0,0), k \in Z$ является нормальным делителем группы G.

Тема 6. Кольца

Вопросы теории

1. Кольцо.
2. Числовые кольца.
3. Виды колец.
4. Делители нуля.
5. Область целостности.

Образцы решения задач

Задача 1. Доказать, что множество M матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где a – любое действительное число, является кольцом относительно матричного сложения и умножения.

Решение. 1) Рассмотрим сумму и произведение двух матриц $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $B = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$ данного множества: $A + B = \begin{pmatrix} a+b & 0 \\ 0 & a+b \end{pmatrix}$, $AB = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix}$.

Мы видим, что $A + B \in M$, $AB \in M$, то есть множество M замкнуто относительно матричного сложения и умножения.

2) Из теории матриц известно, что на множестве квадратных матриц одного и того же порядка, а значит, и на множество M, сложение коммутативно, сложение и умножение ассоциативны и умножение дистрибутивно относительно сложения.

3) Уравнение $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + X = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$ имеет единственное решение $X = \begin{pmatrix} -a+b & 0 \\ 0 & -a+b \end{pmatrix}$, снова принадлежащее множеству M.

Следовательно, множество M является кольцом.

Задачи для решения

1. Выясните, образует ли кольцо относительно обычных сложения и умножения: а) множество ***N***; б) множество ***Z***; в) множество всех нечетных чисел; г) множество всех четных чисел; д) множество чисел вида $a + b\sqrt[3]{5}$, где a, b - любые целые числа. В каких из указанных случаев существует единичный элемент (то есть нейтральный элемент для операции умножения)?

2. Является ли кольцом множество L чисел вида $a + b\sqrt{3} + c\sqrt{5}, a, b, c \in Z$, относительно обычных операций сложения и умножения?

3. Покажите, что множество чисел вида $a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}, a, b, c, d \in Z$, является числовым кольцом, то есть кольцом относительно обычных операций сложения и умножения над числами.

4. Докажите, что в любом кольце для любых его элементов a, b, c имеют место свойства: а) если $a+b = a+c$, то $b=c$; б) $a-b = a+(-b)$; в) $-(a+b) = -a - b$; г) $-(a - b) = b - a$.

5. Запишите левый и правый дистрибутивный законы, если операция $*$ дистрибутивна относительно операции $\circ$. Дистрибутивно ли обычное сложение относительно обычного умножения?

6. Выясните, дистрибутивна ли операция $*$ относительно операции $\circ$, если $*$ является операцией возведения в степень на множестве ***N,*** а $\circ$ - операцией умножения на том же множестве, то есть $a * b = a^b, a \circ b = a \cdot b$, где a, b - любые элементы из ***N***.

7. Справедливы ли формулы сокращенного умножения для элементов некоммутативных колец?

8. Выясните, является ли кольцом относительно матричного сложения и умножения: а) множество всех вещественных матриц одного и того же порядка $n > 1$; б) множество матриц вида $\begin{pmatrix} a & b \\ b & b \end{pmatrix}$ с рациональными компонентами; в) множество вещественных матриц вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$.

9. Докажите, что множество M матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ составляет коммутативное кольцо относительно матричного сложения и умножения. Выделите мультипликативную группу этого кольца.

10. Какие элементы кольца называют делителями нуля? Выясните, имеет ли кольцо M вещественных матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ делители нуля $\Theta = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ этого кольца.

11. Докажите, что множество A чисел вида $2a + 2b\sqrt{3}$ где a, b - любые целые числа, является числовым кольцом.

12. Докажите, что множество $Z\left[\sqrt[3]{2}\right]$ чисел вида $2a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где a, b, c - любые целые числа, является числовым кольцом.

13. Докажите, что если M – коммутативная группа относительно операции сложения, такая, что $ab = 0$ для любых a, b и нулевого элемента 0 группы M, то система $M = < M; +, \bullet >$ является кольцом.

14. Докажите, что если на $\boldsymbol{Z}$ задана операция $a \otimes b = -ab$, то алгебраическая система <Z; +, ⊗> является коммутативным кольцом с единицей. Каков единичный элемент этого кольца?

15. На множестве $A = Q^2$ упорядоченных пар $(a; b)$ рациональных чисел сложение $\oplus$ и умножение $\otimes$ определены следующими правилами: $(a;b) \oplus (c;d) = (a + c; b + d), (a;b) \otimes (c;d) = (ac; bd)$.
Покажите, что $< A; \oplus, \otimes >$ является коммутативным кольцом с единицей и с делителями нуля.

16. Докажите, что если на множестве $Z_n = \{0,1,2,..., n-1\}$, кроме операции сложения $\oplus$ по модулю n, определена еще операция умножения $\otimes$ по модулю n, состоящая в том , что в качестве результата этой операции над двумя числами из Z_n берется остаток от деления на n обычного произведения, то система $Z_n = \langle Z_n; \oplus, \otimes \rangle$ является коммутативным кольцом.
Примечание. Это кольцо называется кольцом вычетов по модулю n.

17. Составьте таблицы сложения и умножения элементов колец ***Z3*** и ***Z8*** , а также выясните, имеются ли в этих кольцах делители нуля.

18. Выясните, является ли $\boldsymbol{I}$ – множество подмножеств некоторого непустого множества – кольцом относительно операций объединения $\cup$ и пересечения $\cap$.

19. Выясните, является ли система <Z; $\oplus, \bullet$ > кольцом относительно обычного умножения и операции сложения $\oplus$, выполняемой по правилу:

$$a \oplus b = \begin{cases} a+b, \text{если a - четное число, b - целое число} \\ a-b, \text{если a - нечетное число, b - целое число.} \end{cases}$$

20. Докажите, что множество $Z[\sqrt{5}]$ чисел вида $a+b\sqrt{5}$, где a,b - любые целые числа, является числовым кольцом. Разрешимы ли в этом кольце уравнения $(1+2\sqrt{5})x = -8+3\sqrt{5}$, $(-8+3\sqrt{5})x = 1+2\sqrt{5}$, $(3+2\sqrt{5})x = 2-3\sqrt{5}$?

Тема 7. Подкольца

Вопросы теории

1. Подкольцо.
2. Критерий подкольца.

Образцы решения задач

Задача 1. Доказать, что множество *A* четных целых чисел есть подкольцо кольца целых чисел *Z***.**

Решение. Имеем:

1) $A = \{x | x = 2k, k \in Z\}$, $A \subset Z$. (1)

2) Пусть *x1*, *x2* – любые элементы из *A*, то есть *x1* = 2*k1*, *x2* = 2*k2*, $k_1, k_2 \in Z$. Так как *Z* есть кольцо, то $k_1 + k_2 \in Z$ и потому:
$$x_1 + x_2 = 2k_1 + 2k_2 = 2(k_1 + k_2) \in A. \quad (2)$$

3) Пусть $x = 2k$ есть любой элемент из *A*, следовательно, $k \in Z$; тогда и $-k \in Z$, а потому:
$$-x = -2k = 2 \cdot (-k) \in A. \quad (3)$$

Из (1), (2), (3) следует, что *A* есть подгруппа аддитивной группы кольца Z.

4) Кроме того, если *x1*, *x2* – любые элементы из *A*, т.е. *x1* = 2*k1*, *x2* = 2*k2*, $k_1, k_2 \in Z$, то $x_1 \cdot x_2 = 2k_1 \cdot 2k_2 = 2(2k_1 \cdot k_2) \in A$, так как $2k_1 \cdot k_2 \in Z$ (*Z* кольцо). Следовательно, А является подкольцом кольца *Z*.

Задачи для решения

1. Докажите, что если непустое подмножество *L* кольца *K* содержит сумму и произведение двух любых своих элементов и для всякого своего элемента содержит противоположный ему элемент, то *L* является подкольцом кольца *K*.

2. Докажите, что если непустое подмножество *L* кольца *K* содержит разность и произведение любых своих элементов, то *L* является подкольцом кольца *K*.

3. Охарактеризуйте все подкольца кольца $< Z;+,\bullet >$ целых чисел.

4. Докажите, что множество *L* матриц вида $\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$, $a,b \in Q$, является подкольцом кольца *M* всех вещественных матриц порядка 2.

5. В кольце M всех вещественных матриц порядка 2 укажите несколько подмножеств, которые являются его подкольцами.

6. Какой вид имеют все подкольца кольца $Z_n =< Z_n;\oplus,\otimes >$ вычетов по модулю n? Сколько их у кольца Z_n?

7. Докажите, что множество диагональных матриц порядка $n \geq 2$, то есть матриц вида $\begin{pmatrix} a_1 & 0 & 0 & \ldots & 0 \\ 0 & a_2 & 0 & \ldots & 0 \\ 0 & 0 & a_3 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & a_n \end{pmatrix}$ с действительными элементами, является подкольцом кольца M всех вещественных матриц порядка n. Будет ли оно коммутативным? Иметь делители нуля?

Тема 8. Гомоморфизмы и изоморфизмы колец

Вопросы теории

1. Гомоморфизм колец.
2. Ядро гомоморфизма.
3. Образ гомоморфизма.
4. Изоморфизм колец.
5. Свойства изоморфизма.
6. Мономорфизмы и эндоморфизмы колец.

Образцы решения задач

Задача 1. Показать, что отображение f: $Q[\sqrt{2}] \to Q[\sqrt{2}]$, определяемое формулой $f(a+b\sqrt{2}) = a - b\sqrt{2}$, где a, $b \in$ Q, есть изоморфное отображение кольца $Q[\sqrt{2}]$ на себя.

Решение. Очевидно, что отображение f является биективным. Покажем, что f сохраняет операции кольца $Q[\sqrt{2}]$. Действительно, для любых $x = a + b\sqrt{2}$ и $y = c + d\sqrt{2} \in Q[\sqrt{2}]$

$$f(xy) = f(ac + 2bd + (ad + bc)\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}) = f(x)f(y);$$

$$f(x + y) = f(a + b\sqrt{2} + c + d\sqrt{2}) = a - b\sqrt{2} + b - d\sqrt{2} = f(x) + f(y);$$

Следовательно, отображение f является изоморфизмом кольца $Q[\sqrt{2}]$.

Задачи для решения

1. а) Докажите, что кольцо чисел вида $a + b\sqrt{5}$ изоморфно кольцу матриц вида $\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$ (в обоих кольцах a, b - любые рациональные числа).

2. Покажите, что кольцо $\boldsymbol{Z}$ можно изоморфно отобразить на кольцо M матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где a – любое целое число.

3. Докажите, что кольцо целых чисел можно гомоморфно отобразить на кольцо вычетов по модулю 2.

4. Докажите, что кольцо целых чисел можно гомоморфно отобразить на кольцо Z_n вычетов по любому модулю n (n – натуральное число).

5. Почему кольцо всех целых чисел нельзя ни изоморфно, ни гомоморфно отобразить на любое подкольцо, отличное от $\{0\}$ и самого кольца?

6. Можно ли некоторое кольцо с единицей гомоморфно отобразить на некоторое кольцо без единицы? Можно ли кольцо без единицы гомоморфно отобразить на кольцо с единицей?

7. Докажите, что изоморфны кольцо матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ и кольцо Q^2 упорядоченных пар ($a;\ b$).

8. Проверьте, является ли отображение $a + b\sqrt[3]{7} + c\sqrt[3]{49} \to a + b\sqrt[3]{49} + c\sqrt[3]{7}$, где $a,\ b \in Z$, изоморфным отображением кольца $Z\left[\sqrt[3]{7}\right]$ на себя.
Примечание. Изоморфное отображение кольца на себя называется *автоморфизмом* этого кольца.

9. Проверьте, что следующие отображения являются гомоморфными отображениями колец:

а) $f : \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in R \right\} \to R, f\begin{pmatrix} a & b \\ b & a \end{pmatrix} = a - b$;

б) $f : \left\{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} \middle| a, b \in Q \right\} \to Q, f\begin{pmatrix} a & a \\ b & b \end{pmatrix} = a + b$

в) $f : R \times R \to R, f(< a, b >) = a$;

г) $f : R \to R \times R, f(a) =< a, a >$;

д) $f : Z \to Z[i], f(a) = a$;

е) $f : Q[\sqrt{2}] \to Q[\sqrt{2}], f(a + b\sqrt{2}) = a - b\sqrt{2}$;

ж) $f : Z[x] \to Z, f(a_0 + a_1 x + ... + a_n x^n) = a_0$;

з) $f : Q[x] \to R, f(a_0 + a_1 x + ... + a_n x^n) = a_0 + a_1\sqrt{2} + ... + a_n(\sqrt{2})^n$.

Для каждого отображения найдите ядро и образ.

Тема 9. Делимость в кольцах

Вопросы теории

1. Понятие делимости в кольце.
2. Обратимые элементы кольца.
3. Свойства делимости.
4. Ассоциированные элементы.
5. Простые и составные элементы кольца.

Образцы решения задач

Задача 1. Делится ли число 23+2*i* на число 2+3*i* в кольце $Z[i]$?

Решение. В самом деле, $\frac{23+2i}{2+3i}=\frac{(23+2i)(2-3i)}{(2+3i)(2-3i)}=\frac{52-65i}{13}=4-5i$, а 4-5*i* $\in Z[i]$.

Следовательно, число 23+2*i* делится на число 2+3*i* в кольце $Z[i]$.

Задача 2. Покажите, что в кольце $Z[\sqrt{3}]$ число 13 является составным.

Решение. Число 13 можно представить в виде 13 = (4 - $\sqrt{3}$)(4 + $\sqrt{3}$), (4 - $\sqrt{3}$) и (4 + $\sqrt{3}$)принадлежат $Z[\sqrt{3}]$. Докажем, что (4 - $\sqrt{3}$) и (4 + $\sqrt{3}$) необратимы.

$\frac{1}{4-\sqrt{3}}=\frac{4+\sqrt{3}}{(4-\sqrt{3})(4+\sqrt{3})}=\frac{4+\sqrt{3}}{16-9}=\frac{4}{7}+\frac{\sqrt{3}}{7}\notin Z[\sqrt{3}]$,

$\frac{1}{4+\sqrt{3}}=\frac{4-\sqrt{3}}{(4+\sqrt{3})(4-\sqrt{3})}=\frac{4-\sqrt{3}}{16-9}=\frac{4}{7}-\frac{\sqrt{3}}{7}\notin Z[\sqrt{3}]$. Так как 13 мы представили в виде произведения необратимых элементов кольца $Z[\sqrt{3}]$, то 13 в этом кольце является составным числом.

Задачи для решения

1. Какие элементы кольца называются обратимыми? Найдите обратимые элементы в кольцах $Z[\sqrt{2}]$ чисел вида $a+b\sqrt{2}$, *a, b* $\in Z$, и $Z[-\sqrt{2}]$.

2. Делится ли число $3-5\sqrt{2}$ на число $2+3\sqrt{2}$ в кольце $Z[\sqrt{2}]$? А число $7+17\sqrt{2}$ на число $3+4\sqrt{2}$?

3. Какие элементы поля Q рациональных чисел делятся на число $\frac{7}{9}$?

4. Делится ли в кольце $Z[\sqrt[3]{3}]$ число $9+3\sqrt[3]{3}+2\sqrt[3]{9}$ на число $2+\sqrt[3]{3}$?

5. Какими дополнительными свойствами обладает отношение делимости в области целостности?

6. Докажите, что если *a* – делитель нуля в кольце R, то все элементы вида *ab*, где *b* $\in R$, тоже являются делителями нуля.

7. Пусть R – область целостности. Является ли областью целостности R^n? (Рассмотрите произведение $(a, 0)\ (0, b)$.)

8. Докажите, что элементы $1+2\sqrt{5}$, $-8+3\sqrt{5}$ кольца $Z[\sqrt{5}]$ ассоциированы.

9. Докажите, что числа 7 и 3 простые в кольце $Z[i]$ и числа 13 и 17 составные в кольце $Z[i]$.
10. Докажите, что 2 разлагается в кольце $Z[i]$ в произведение двух необратимых сомножителей.

Тема 10. Идеалы в кольцах

Вопросы теории

1. Идеал кольца.
2. Свойства идеалов колец.
3. Главные идеалы колец.
4. Свойства главных идеалов.
5. Смежные классы кольца по идеалу.
6. Факторкольцо.

Образцы решения задач

Задача 1. Проверить является ли кольцо $Z[x]$ многочленов с целыми коэффициентами идеалом в кольце $R[x]$.

Например, многочлен $2 + 3x$ принадлежит $Z[x]$, а кратный ему многочлен $(2+3x)\left(\frac{1}{3}-\frac{x}{2}\right)=\frac{2}{3}-\frac{3}{2}x^2$ имеет дробные коэффициенты и потому не принадлежит $Z[x]$. Следовательно, кольцо $Z[x]$ многочленов с целыми коэффициентами идеалом в кольце $R[x]$ не является.

Задача 2. Доказать, что множество I многочленов с нулевым свободным членом является идеалом в кольце $R[x, y]$ многочленов от двух переменных с действительными коэффициентами.

Решение. Если свободные члены многочленов $\varphi(x, y)$ и $\psi(x, y)$ равны нулю, то же самое верно и для многочлена $\varphi - \psi$, а также для любого многочлена вида $f(x, y) \cdot \varphi(x, y)$, где $f(x, y) \in R[x, y]$. Иными словами, если $\varphi \in I$ и $\psi \in I$, то $\varphi - \psi \in I$, а если $\varphi \in I$ и $f \in R[x, y]$, то $f\varphi \in I$. Значит, I – идеал в кольце $R[x, y]$. Этот идеал не является главным. В самом деле, многочлены x и y принадлежат I, но в I нет ни одного многочлена, которому были бы кратны и x и y.

Задачи для решения

1. Являются ли идеалами:

а) Z в $Z[i]$;

б) $\{a+ai|a\in Z\}$ в $Z[i]$;

в) 3Z в Z;

г) $\left\{\begin{pmatrix} a & a \\ a & a \end{pmatrix} |a\in R\right\}$в$\left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} |a,b\in R\right\}$;

д) $\left\{\begin{pmatrix} a & a \\ a & a \end{pmatrix} |a\in Q\right\}$в$\left\{\begin{pmatrix} a & a \\ b & b \end{pmatrix} |a,b\in Q\right\}$;

е) $\{(a,a)|a\in R\}$ в $R\times R$;

ж) $\{2a+bi|a,b\in Z\}$ в $Z[i]$;

з) $\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} |a\in R\right\}$в M (2, R);

и) $\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} |a,b\in R\right\}$в M (2, R);

к) $\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} |a,b\in R\right\}$в M (2, R);

л) $\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} |a,b\in R\right\}$в M (2, R);

м) $\{(a,0)|a\in R\}$ в $R\times R$;

н) $\left\{\frac{m}{n} |m,n\in Z\wedge p\times n\wedge p/m\right\}$ в Qp;

о) Z в $Z[x]$;

п) (nZ) [x] в $Z[x]$;

р) множество всех многочленов на $Z[x]$ с четным старшим коэффициентом в $Z[x]$.

2. Найдите все идеалы в кольцах Z, Z_8, Z_{25}.

3. Пусть A - кольцо, J1, J2 – идеалы A. Обозначим $J_1\cdot J_2$ - множество всех элементов из A, которое можно представить в виде $x_1y_1+...+x_ny_n$, где $x_1,...,x_n\in J_1, y_1,...,y_n\in J_2$. Докажите, что $J_1\cdot J_2$ идеал A и $J_1\cdot J_2\subseteq J_1\cap J_2$.

4. Какие из чисел $3-5i$, $4+6i$, $-15+9i$, $5-3i$ принадлежат идеалу $(3+5i)$ кольца целых гауссовых чисел? Какие из них порождают этот идеал?

5. Найдите идеал (2) в Z; в $Z[i]$; в $Z[x]$; в Q[x].

6. Укажите, какие включения имеют место для следующих идеалов кольца целых чисел: 3Z, 2Z, 4Z, 5Z, 6Z, (-11)Z, 24Z, (-4)Z, 13Z, 33Z, 12Z. Нарисуйте граф и сравните его с графом отношения делимости на множестве {2, 3, 4, 5, 6, 11, 12, 13, 24, 33}.

7. Сколько элементов в факторкольце Z/6Z? Составьте таблицы сложения и умножения для элементов этого факторкольца.

8. Укажите числа, принадлежащие одному смежному классу по идеалу (2) в кольце $Z[i]$: $-3+5i$; $7-8i$; $25+3i$; $47+10i$; -2; $1+i$; $1-i$; $3i$; 1; -1; $2+i$; $-2+3i$.

9. Найдите все элементы факторкольца $Z[i]/(2)$. Составьте таблицы сложения и умножения. Покажите, что это факторкольцо не является областью целостности.

10. Какие из следующих равенств имеют место в факторкольце $Z[i]/(3)$:

а) $1 + 2i + (3) = 1 - 2i + (3)$;
б) $1 + (3) = i + (3)$;
в) $3i + (3) = 3 + (3)$;
г) $3i + (3) = 0 + (3)$;
д) $3 - i + (3) = 3 + i + (3)$?

11. Укажите все элементы кольца $Z[i]/(3)$, составьте таблицы сложения и умножения.

12. Сколько элементов содержит факторкольцо $Z[i]/(5)$?

13. Среди следующих элементов факторкольца $R[x]/(x^2 + x + 1)$ укажите равные нулю:

а) $x^3 + x + 1 + (x^2 + x + 1)$;
б) $x^3 + 1 + (x^2 + x + 1)$;
в) $x^3 - 1 + (x^2 + x + 1)$;
г) $x^3 + x^2 + x + (x^2 + x + 1)$.

Тема 11. Поля

Вопросы теории

1. Поле.
2. Подполе.
3. Характеристика поля.
4. Изоморфизм полей.

Образцы решения задач

Задача 1. Доказать, что множество M матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где a и b – любые действительные числа, является полем относительно матричного сложения и умножения. Найти характеристику этого поля.

Решение. 1) Рассмотрим сумму и произведение двух матриц $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ данного множества: $A + B = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$, $AB = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$.

Мы видим, что $A + B \in M$, $AB \in M$, то есть множество M замкнуто относительно матричного сложения и умножения.

2) Из теории матриц известно, что на множестве квадратных матриц одного и того же порядка, а значит, и на множестве M, сложение коммутативно, сложение и умножение ассоциативны и умножение дистрибутивно относительно сложения.

3) Уравнение $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + X = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ имеет единственное решение:

$X = \begin{pmatrix} -a+c & -b+d \\ b-d & -a+c \end{pmatrix}$, снова принадлежащее множеству M.

4) $BA = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} = AB$, то есть умножение в M коммутативно.

5) Рассмотрим уравнение $AX = B$, где $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$, $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ и, следовательно, $a \neq 0$ или $b \neq 0$. Тогда $|A| = a^2 + b^2 \neq 0$, то есть матрица A является невырожденной, а значит, она имеет обратную матрицу A^{-1}. В таком случае уравнение
$AX = B$ имеет единственное решение $X = A^{-1}B$. Докажем, что это решение принадлежит данному множеству M. Имеем:

$$A^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \in M .$$

Из того, что $A^{-1} \in M$, $B \in M$, имеем в силу первой части доказательства $X = A^{-1}B \in M$. Итак, рассматриваемое уравнение в M разрешимо и имеет единственное решение. Из результатов, найденных в пунктах 1 – 5, следует по определению поля, что M есть поле.
Найдем характеристику поля M. Нулем поля M является матрица $\begin{pmatrix} 0 & 0 \\ -0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Единицей поля M является матрица $\begin{pmatrix} 1 & 0 \\ -0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$. По правилу умножения числа на матрицу получим, что при любом натуральном n $n\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, то есть не существует натурального n такого, чтобы $n\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. А это значит, что характеристика поля M равна нулю.

Задачи для решения

1. Докажите, что алгебраическая система – множество Q рациональных чисел с обычной операцией сложения и операцией $\circ$, выполняемой по правилу $a \circ b = \frac{a \cdot b}{2}$ для любых элементов из Q, - является полем. Каков единичный элемент этого поля?

2. Докажите, что если коммутативное кольцо K состоит из конечного числа n элементов, где $n > 1$, и не содержит делителей нуля, то оно является полем.
Указание. Пусть a – отличный от нуля элемент из K. Покажите, что отображение $x \to ax$ является взаимно однозначным отображением K на себя. Выведите отсюда разрешимость уравнения $ax = b$.

3. Докажите, что множество матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где a – любое рациональное (или действительное) число, является полем относительно матричного сложения и умножения. Будет ли множество матриц данного вида составлять поле, если a – любое целое число?

4. Почему кольцо {0} не является полем?

5. На множестве M = {a, b} сложение $\oplus$ и умножение $\otimes$ определены следующим образом:

$a \oplus a = a, a \oplus b = b \oplus a = b, b \oplus b = a$;

$a \otimes b = b \otimes a = a, a \otimes a = a, b \otimes b = b.$

Выясните, обладает ли это множество нулем и единицей и является ли система $<M; \oplus, \otimes>$ полем относительно заданных бинарных операций.

6. Докажите, что если B – множество пар $(a; b)$ рациональных чисел и на B две бинарные операции - сложение $\oplus$ и умножение $\otimes$ - определены следующим условиями:

$(a;b) \oplus (c;d) = (a + c; b + d),$

$(a;b) \otimes (c;d) = (ac + 2bd; ad + bc)$, то система B = <B; $\oplus$, $\otimes$> является полем, а пары (0; 0) и (1; 0) соответственно нулем и единицей этого поля.

7. Докажите, что кольцо Z_n вычетов по модулю n не является полем, если n – составное число.

8. Убедитесь в том, что поле A = {0, 1} с обычной операцией умножения и операцией сложения $\oplus$, задаваемой равенствами $1 \oplus 1 = 0 \oplus 0 = 0$, $1 \oplus 0 = 0 \oplus 1 = 1$, имеет характеристику, равную двум.

9. Приведите примеры полей, характеристика которых равна нулю.

10. Докажите, что не существует полей характеристикой которых была бы единица или какое-либо составное натуральное число.

11. Докажите, что если непустое подмножество L любого поля P содержит сумму и произведение двух любых своих элементов, а также для любого своего элемента содержит противоположный ему элемент и для любого своего ненулевого элемента содержит обратный ему элемент, то L является подполем поля P.

12. В поле матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где $a, b \in R$, укажите такие его подмножества, которые являются подполями.

13. Докажите, что множество $B = Q[\sqrt{5}]$ чисел вида $a + b\sqrt{5}$, где a,b – любые рациональные числа, является числовым полем.

14. Докажите, что область целостности R, состоящая из конечного числа элементов, является полем.

15. Решите систему уравнений:

$$\begin{cases} x + 2z = 1, \\ y + 2z = 2, \\ 2x + z = 1 \end{cases}$$

над полями: а) Z_3; б) Z_5; в) Z_8.

16.Докажите, что в поле $M = < M;+,\cdot >$, где M – множество всех матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ с действительными a и b, а $+$, $\bullet$ являются операциями над матрицами, существует элемент X, такой, что $X^2 = -E$ (E – единица поля M).

17.Докажите, что изоморфны поле матриц вида $\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$ и поле упорядоченных пар (a; b), в котором сложение $\oplus$ и умножение $\otimes$ определены по следующим правилам:

$(a;b) \oplus (c;d) = (a + c; b + d),$
$(a;b) \otimes (c;d) = (ac + 5bd; ad + bc)$, где a,b – любые рациональные числа.

18.Покажите, что любое поле из двух элементов изоморфно полю Z_2.

19.Докажите, что пересечение любой совокупности подполей поля F есть подполе поля F.

Тема 12. Упорядоченные поля

Вопросы теории

1. Упорядоченное поле.
2. Свойства упорядоченного поля.
3. Примеры упорядоченных полей.

Образцы решения задач

Задача 1. Доказать, что $a > b$ тогда и только тогда когда $a - b > 0$.

Решение.

$a > b.$

Добавим к обеим частям неравенства $-b$. Тогда по свойству монотонности относительно сложения получаем:

$a - b > b - b \Rightarrow a - b > 0.$

Задачи для решения

1. Докажите следующие свойства упорядоченных полей:
   а) если $a < b$ и $c \le d$, то $a + c < b + d$;
   б) если $a < 0$, то $a^{-1} < 0$; если $a > 0$, то $a^{-1} > 0$;
   в) если $0 < a < b$, то $0 < \frac{1}{b} < \frac{1}{a}$;
   г) $a^2 \ge 0$;
   д) если $0 < a < b$ и $0 < c \le d$, то $ac < bd$;
   е) если $a < b < 0$, то $\frac{1}{b} < \frac{1}{a} < 0$;
   ж) если $|a| < b$, то $-b < a < b$$
   з) если $-b < a < b$, то $|a| < b$;
   и) $|ab| = |a| \cdot |b|$;
   к) $|a + b| \le |a| + |b|$;
   л) $|a - b| \ge |a| - |b|$.

2. Докажите, что в упорядоченном поле справедливы следующие неравенства:
   а) $a^2 + b^2 + c^2 + 4 > 2(a + b + c)$;
   б) $(ab + bc + ac)^2 \ge 3abc(a + b + c)$;
   в) $a^4 + b^4 \ge a^3b + ab^3$;
   г) $a^4 + 6a^2b^2 + b^4 \ge 4a^3b + 4ab^3$;
   д) $a^2 + b^2 + c^2 + 4 \ge ab + ac + bc$;
   е) $(a + b + c)^2 \ge 3(ab + ac + bc)$.

3. Докажите, что в упорядоченном поле справедливы следующие неравенства:
   а) $2a^3 + 2a^2 + 1 > a$ при $a \ge 0$
   б) $a^6 + b^6 \ge a^5b + ab^5$ при $a \ge 0$, $b \ge 0$
   в) $(a + b + c)\left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}\right) \ge 9$ при $a>0$, $b>0$, $c>0$;
   г) $a^3 + b^3 + c^3 \ge 3abc$ при $a>0$, $b>0$, $c>0$;
   д) $a^5 + b^5 - a^4b - ab^4 \ge 0$ при $a>0$, $b>0$;
   е) $ab + ac + bc \le 0$ при $a+b+c=0$.

4. Пусть $\langle F,+,-,\cdot,< \rangle$ - упорядоченное поле, $F^+ = \{a \in F \mid a > 0\}$. Докажите, что алгебра $\langle F^+,\cdot,^{-1} \rangle$ является группой.

Тема 13. Алгебраические числа

Вопросы теории

1. Понятие алгебраического числа над полем.

2. Минимальный многочлен алгебраического числа.
3. Степень алгебраического числа.
4. Алгебраическая иррациональность над полем.
5. Алгоритм Евклида.
6. Алгоритм избавления от алгебраической иррациональности в знаменателе дроби.

Образцы решения задач

Задача 1. Доказать непосредственно (исходя из определения алгебраического числа), что каждое из чисел

а) $\sqrt[3]{5}$ 4 б) $2+\sqrt[3]{5}$; в) – 1 +2i; г) – 1 +$i\sqrt[3]{5}$

является алгебраическим, и найти его степень (над Q).

Решение. Число $\alpha \in C$ называется алгебраическим над полем Q (или просто алгебраическим), если оно является корнем некоторого многочлена с коэффициентами из Q.

Многочлен $p(x) \in Q[x]$ наименьшей степени, корнем которого является данное алгебраическое число α, называется минимальным многочленом числа α, степень этого многочлена называется степенью числа α (над Q). Многочлен $p\,(x)$ определен с точностью до числового множителя $a \in Q$. Минимальный многочлен всегда неприводим (над Q); обратно, неприводимый многочлен, имеющий α своим корнем, является минимальным многочленом числа α.

а) Для числа α = $\sqrt[3]{5}$ имеем: $\alpha^3 = 5$, то есть α есть корень многочлена $x^3 - 5$. Следовательно, α - алгебраическое число. Так как многочлен $x^3 - 5$ неприводим над Q, то он является минимальным многочленом числа α; степень α над Q равна 3.

б) Для α = $2+\sqrt[3]{5}$ имеем: $\alpha - 2 = \sqrt[3]{5}$, откуда следует: $(\alpha-2)^3 = 5$. Таким образом, число α является корнем многочлена $p(x) = (x-2)^3 - 5 \in Q[x]$ и, следовательно, алгебраическим числом. Многочлен $p\,(x)$ неприводим над Q, поэтому степень α равна 3.

в) Для α = – 1 +2i имеем: α + 1 = 2i и, следовательно, $(\alpha+1)^2 = -4$. Отсюда видно, что α является корнем многочлена $p(x) = (x+1)^2 + 4 = x^2 + 2x + 5 \in Q[x]$, а значит, алгебраическим числом. Так как $p\,(x)$ неприводим над Q, то степень α равна 2.

г) Для α = – 1 +$i\sqrt[3]{5}$ можем записать: α + 1 = $i\sqrt[3]{5}$ $\Rightarrow (\alpha+1)^6 = -5$.

Следовательно, α – корень многочлена $p(x) = (x+1)^6 + 5 \in Q[x]$. Это означает, что α - алгебраическое число. Так как $p\,(x)$ неприводим над Q (чтобы в этом убедиться, достаточно применить к многочлену $y^6 + 5$ признак Эйзенштейна), то степень α равна 6.

Задача 2. В поле Q (α), где α = $\sqrt[3]{2}$, найти выражение для числа $(1 + 3\alpha + \alpha^2)^{-1}$ в виде $b_0 + b_1\alpha + b_2\alpha^2 (b_0, b_1, b_2 \in Q)$.

Решение. Фактически здесь ставится задача освободиться от корней в знаменателе дроби:

$$\frac{1}{1+3\sqrt[3]{2}+\sqrt[3]{4}},$$

или, как еще говорят, «освободиться от алгебраической иррациональности в знаменателе». Задачу можно решить двумя способами.

Iспособ. Будем искать числа $b_0, b_1, b_2 \in Q$ такие, чтобы $(1+3\sqrt[3]{2}+\sqrt[3]{4})(b_0+b_1\sqrt[3]{2}+b_2\sqrt[3]{4})=1$.

В силу формулы $\gamma = a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-i^{\alpha^{n-1}}}$ неизвестные b_0, b_1, b_2 должны удовлетворять уравнению:

$$(1\cdot b_0 + 2\cdot 3b_2 + 2\cdot 1\cdot b_1) + (1\cdot b_1 + 3\cdot b_0 + 2\cdot 1\times b_2)\sqrt[3]{2} + (1\cdot b_2 + 3\cdot b_1 - 1\cdot b_0)\sqrt[3]{4} = 1$$

или, если учесть, что числа 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$ линейно независимы над Q, системе уравнений:

$$\begin{cases} b_0 + 6b_2 + 2b_1 = 1, \\ b_1 + 3b_0 + 2b_2 = 0, \\ b_2 + 3b_1 - b_0 = 0. \end{cases}$$

Решая эту систему, находим:

$$b_0 = -\frac{5}{41}, b_1 = -\frac{1}{41}, b_2 = \frac{8}{41}.$$

Ответ. $(1+3\sqrt[3]{2}+\sqrt[3]{4})^{-1} = \frac{1}{41}(-5-\sqrt[3]{2}+8\sqrt[3]{4})$.

II способ. Число $1+3\sqrt[3]{2}+\sqrt[3]{4}$ есть значение многочлена $f(x)=1+3x+x^2$ при $x = \alpha = \sqrt[3]{2}$. Этот многочлен взаимно прост с многочленом $p(x) = x^3 - 2$ (минимальным многочленом числа α), так как $p(x)$ неприводим, а $f(x)$ не делится на $p(x)$. Следовательно, существуют многочлены $u(x)$ и $v(x)$ такие, что:

$$u(x)\ f(x) + v(x)\ p(x) = 1.$$

Полагая в этом равенстве $x = \alpha$, будем иметь:

$$u(\alpha)\ f(\alpha) = 1$$

или

$f(\alpha)^{-1} = u(\alpha)$ - искомое представление для числа $f(\alpha)^{-1}$.

Итак, остается лишь найти многочлены $u(x)$ и $v(x)$.

Применим к $f(x)$ и $p(x)$ алгоритм Евклида:

1) $p(x) = f(x)(x-3) + r(x)$, где $r(x) = 8x + 1$;

2) $8f(x) = r(x)\left(x+\frac{23}{8}\right) + r_1$, где $r_1 = \frac{41}{8}$.

Получим:

$$r_1 = 8f(x) - [p(x) - f(x)(x-3)]\left(x+\frac{23}{8}\right) = \left(8+(x-3)\left(x+\frac{23}{8}\right)\right)f(x) - \left(x+\frac{23}{8}\right)p(x).$$

Полагая в последнем равенстве $x = \alpha$, находим:

$$\frac{41}{8} = \left(8+(\alpha-3)\left(\alpha+\frac{23}{8}\right)\right)f(\alpha),$$

или

$$f(\alpha)^{-1} = \frac{8}{41}\left(8 + \alpha^2 - \frac{1}{8}\alpha - \frac{69}{8}\right) = \frac{1}{41}\left(-5 - \alpha + 8\alpha^2\right).$$

Ответ, разумеется, получился тот же самый, что и при I способе решения.

Задача 3. Освободиться от α в знаменателе дроби $\frac{\alpha^2 - 3\alpha + 1}{\alpha^2 + 2\alpha + 1}$, если α – корень уравнения $x^3 + x^2 + 3x + 4 = 0$.

Решение. Положим $p(x) = x^3 + x^2 + 3x + 4$. С помощью известных нам приемов определяем, что многочлен $p(x)$ не имеет рациональных корней; из этого, поскольку степень $p(x)$ равна 3, следует, что $p(x)$ неприводим над Q. Знаменатель данной дроби $\alpha^2 + 2\alpha + 1 = (\alpha + 1)^2$ не равен нулю, так как $\alpha \neq -1$ (число – 1 не является корнем многочлена $p(x)$). Это означает, что многочлен $f(x) = x^2 + 2x + 1$ взаимно прост с $p(x)$ (в противном случае $f(x)$ и $p(x)$ имели бы общий корень – 1, что, как мы видели, невозможно). Пользуясь этим, будем искать многочлены $u(x)$ и $v(x)$ такие, что:

$$u(x)\ f(x) + v(x)\ p(x) = 1.$$

Применяем к $p(x)$ и $f(x)$ алгоритм Евклида. Деля $p(x)$ на $f(x)$ с остатком, получим:

$$p(x) = f(x)\ (x - 1) + r(x),$$

где $r(x) = 4x + 5$. Далее находим:

$$f(x) = \frac{1}{4} r(x)\left(x + \frac{3}{4}\right) + \frac{1}{16}.$$

Отсюда имеем:

$$\frac{1}{16} = f(x) - \frac{1}{4}[p(x) - f(x)(x-1)]\left(x + \frac{3}{4}\right) = f(x)\left(\frac{1}{4}x^2 - \frac{1}{16}x + \frac{13}{16}\right) + p(x)\left(-\frac{1}{4}x - \frac{3}{16}\right).$$

При $x = \alpha$ из последнего равенства получаем:

$$\frac{1}{16} = f(\alpha)\left(\frac{1}{4}\alpha^2 - \frac{1}{16}\alpha + \frac{13}{16}\right),$$

или $\frac{1}{f(\alpha)} = 4\alpha^2 - \alpha + 13$.

Умножая обе части равенства на число $\alpha^2 - 3\alpha - 1$, то есть на числитель данной в задаче дроби, получим:

$$\frac{\alpha^2 - 3\alpha - 1}{\alpha^2 + 2\alpha + 1} = (4\alpha^2 - \alpha + 13)(\alpha^2 - 3\alpha - 1) = 4\alpha^4 - 13\alpha^3 + 12\alpha^2 - 38\alpha - 13.$$

В принципе мы привели дробь к нужному виду. Однако можно еще упростить полученное выражение, воспользовавшись тем, что $p(\alpha) = 0$. Делим с остатком многочлен $g(x) = 4x^4 - 13x^3 + 12x^2 - 38x - 13$ на $p(x) = x^3 + x^2 + 3x + 4$. Получаем:

$$g(x) = p(x)\ (4x - 17) + S(x),$$

где $S(x) = 17x^2 - 3x + 55$. При $x = \alpha$ имеем:

$$g(\alpha) = S(\alpha) = 17\alpha^2 - 3\alpha + 55.$$

Ответ. $\frac{\alpha^2 - 3\alpha - 1}{\alpha^2 + 2\alpha + 1} = 17\alpha^2 - 3\alpha + 55$.

Задачи для решения

1. Доказать непосредственно, что число α является алгебраическим, и найти минимальный многочлен числа α:

а) $\alpha = 1$; б) $\alpha = i$; в) $\alpha = -1 + i\sqrt{3}$; г) $\alpha = 1 - 2\sqrt[3]{4}$;

д) $\alpha = \sqrt{2} + \sqrt{3}$; е) $\alpha = \sqrt{2} + i\sqrt{3}$; ж) $\alpha = \sqrt[4]{1+\sqrt{2}}$;

з) $\alpha = 1 + \sqrt[5]{11}$; и) $\alpha = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$; к) $\alpha = \cos\frac{5\pi}{8} + i\sin\frac{5\pi}{8}$.

2. Доказать непосредственно, что число α является алгебраическим, и найти многочлен над Q (не обязательно минимальной степени), корнем которого является α:

а) $\alpha = \sqrt[5]{2} - \sqrt{2}$; б) $\alpha = \sqrt[5]{2} - \frac{1}{2}i$; в) $\alpha = \sqrt[5]{2} - i\sqrt{2}$.

3. Доказать непосредственно, что если число α алгебраическое, то каждое из чисел $a\alpha + b (a, b \in Q)$, $\frac{1}{\alpha}$ (если $\alpha \neq 0$), α^2 снова алгебраическое.

4. Являются ли алгебраически сопряженными числа: а) $\sqrt{5}$ и $-\sqrt{5}$; б) $\sqrt[3]{5}$ и $-\sqrt[3]{5}$; в) $\sqrt[4]{5}$ и $-\sqrt[4]{5}$; г) $\sqrt{5} + i$ и $\sqrt{5} - i$; д) $\sqrt{5} + i$ и $-\sqrt{5} + i$?

5. Освободиться от иррациональности в знаменателе дроби:

а) $\frac{7}{1 - \sqrt[4]{2} + \sqrt{2}}$; б) $\frac{\sqrt{7}+1}{\sqrt{7} + \sqrt[4]{7} - 1}$.

6. Освободиться от алгебраической иррациональности в знаменателе дроби:

а) $\frac{\alpha}{\alpha^3 + 5}$, где $\alpha^3 - 2\alpha + 2 = 0$;

б) $\frac{\alpha^2}{\alpha^4 + 1}$, где $\alpha^4 + 2\alpha + 2 = 0$;

в) $\frac{1}{\alpha^3 + 3\alpha^2 + 3\alpha + 2}$, где $\alpha^4 + \alpha^3 - 4\alpha^2 - 3\alpha + 2 = 0$.

7. Найти многочлен над Q, корнем которого является число $\alpha + \beta$, если известны минимальные многочлены для α и β:

а) $P_\alpha(x) = x^2 + x + 1, P_\beta(x) = x^2 + 2x + 3$;

б) $P_\alpha(x) = x^3 - 2, P_\beta(x) = x^2 - 5$;

в) $P_\alpha(x) = x^3 + x + 1, P_\beta(x) = x^2 + 2x + 3$.

Тема 14. Расширения полей

Вопросы теории

1. Расширение поля.
2. Простое алгебраическое расширение поля.
3. Составное алгебраическое расширение поля.
4. Размерность расширения.

Образцы решения задач

Задача 1. Поле Q последовательно расширяется – сначала с помощью числа $\sqrt{2}$, затем с помощью $\sqrt[3]{5}$: Q $\subset$ Q1 $\subset$ Q2, где Q1 = Q($\sqrt{2}$),Q2 = Q1 ($\sqrt[3]{5}$). Доказать, что такое расширение может быть достигнуто в один шаг – с помощью числа $\Theta = \sqrt{2}+\sqrt[3]{5}$, то есть что Q($\sqrt{2}$)($\sqrt[3]{5}$)=Q($\sqrt{2}+\sqrt[3]{5}$).

Решение. Согласно теореме о простоте составного расширения любые два последовательно произведенных простых алгебраических расширения поля *P:*

$$P_1 = P(\alpha_1), P_2 = P_1(\alpha_2)$$

(α_1 алгебраично над *P*, а α_2 - над *P*1) могут быть заменены одним, то есть существует такое число θ, алгебраическое над *P*, что:

$$P_2 = P(\theta).$$

Наша задача – показать, что в случае, когда *P* есть поле Q рациональных чисел, а $\alpha_1=\sqrt{2}$ и $\alpha_2=\sqrt[3]{5}$, в качестве θ можно взять $\alpha_1+\alpha_2$.

Достаточно показать, что поле Q ($\alpha_1+\alpha_2$) содержит каждое из чисел α_1 и α_2, так как в этом случае оно будет содержать поле Q1 = Q(α_1) и число α_2, а значит, и поле Q2 = Q1(α_2); тогда из Q ($\alpha_1+\alpha_2$) $\supset$ Q2 и Q ($\alpha_1+\alpha_2$)$\subset$ Q2 (второе включение является очевидным) будет следовать: Q ($\alpha_1+\alpha_2$) = Q2.

На самом деле достаточно показать еще меньше – что поле Q ($\alpha_1+\alpha_2$) содержит α_1, так как α_2 тогда будет принадлежать полю Q ($\alpha_1+\alpha_2$) как разность двух чисел из этого поля (α_2 = ($\alpha_1+\alpha_2$) - α_1).

Для сокращения записей обозначим поле Q ($\alpha_1+\alpha_2$) через *L*. Допустим, рассуждая от противного, что число $\alpha_1=\sqrt{2}$ не принадлежит *L*. Рассмотрим два многочлена над *L*:

$$\varphi(x) = (x-\theta)^3 + 5, \psi(x) = x^2 - 2$$

(напомним, что $\theta = \sqrt{2}+\sqrt[3]{5}$). Каждый из них имеет одним из своих корней число $\sqrt{2}$:

$\varphi(\sqrt{2}) = (\sqrt{2}-(\sqrt{2}+\sqrt[3]{5}))^3 + 5 = 0$; $\psi(\sqrt{2}) = 2-2 = 0$.

Проверим, что других общих корней многочлены $\varphi(x)$ и $\psi(x)$ не имеют. Действительно, корни $\psi(x)$ - это числа $\sqrt{2}$, - $\sqrt{2}$.

Корнями же многочлена $\varphi(x)$ являются корни уравнения $(x-\theta)^3 = 5$, то есть числа:

$$\theta - \sqrt[3]{5}(=\sqrt{2}), \theta - \sqrt[3]{5}\omega, \theta - \sqrt[3]{5}\omega^2,$$

где $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ - корень кубический из 1. Следовательно, мы должны проверить, что ни одно из чисел $\theta - \sqrt[3]{5}\omega, \theta - \sqrt[3]{5}\omega^2$ не равно - $\sqrt{2}$. Но это очевидно, так как числа $\theta - \sqrt[3]{5}\omega, \theta - \sqrt[3]{5}\omega^2$ не являются действительными (коэффициент при *i* отличен от нуля).

Поскольку, таким образом, единственный общий корень многочленов $\varphi(x)$ и $\psi(x)$ в поле *C* есть $\sqrt{2}$, то (нормированный) наибольший общий делитель многочленов $\varphi(x)$ и $\psi(x)$ в кольце *C* [x] есть:

$$D(x) = x - \sqrt{2}.$$

Этот же самый многочлен должен быть (нормированным) НОД многочленов $\varphi(x)$ и $\psi(x)$ также и в кольце *L* [x]. Следовательно, все коэффициенты этого многочлена, в частности

- $\sqrt{2}$, принадлежат полю *L*. Тем самым и число $\sqrt{2}$ принадлежат *L*, что и требовалось показать.

Задача 2. Найти выражение числа $\sqrt{2}$ в виде $\frac{f(\theta)}{g(\theta)}$, где $\theta = \sqrt{2} + \sqrt[3]{5}$, а $f(x)$, $g(x) \in Z$ [x].

Решение. Сам факт принадлежности числа $\sqrt{2}$ полю Q (θ) был установлен в задаче 1. Наша цель теперь – найти «явное» выражение числа $\sqrt{2}$ через θ.

Рассмотрим снова многочлены $\varphi(x)$ и $\psi(x)$ из (1). При решении задачи 1 мы показали, что нормированный НОД этих многочленов есть:

$$D(x) = x - \sqrt{2}.$$

С другой стороны, НОД можно найти, применяя к $\varphi(x)$ и $\psi(x)$ алгоритм Евклида. Для этого делим сначала $\varphi(x)$ на $\psi(x)$ (с остатком):

$$\begin{array}{l} x^3 - 3\theta x^2 + 3\theta^2 x - \theta^3 + 5 \;\big|\; \underline{x^2 - 2} \\ x^3 \qquad\quad - 2x \qquad\quad \big| \; x - 3\theta \end{array}$$

$$\begin{array}{l} -3\theta x^2 + (3\theta^2 + 2)x - \theta^3 + 5 \\ -3\theta x^2 \qquad\qquad + 60 \end{array}$$

$$(3\theta^2 + 2)x - (\theta^2 + 60 - 5)$$

Мы получили в остатке многочлен:

$$r(x) = (3\theta^2 + 2)x - (\theta^3 + 60 - 5)$$

1-й степени. Поскольку ранее уже было доказано, что НОД имеет степень 1, то многочлен $r(x)$ и должен быть как раз НОД многочленов $\varphi(x)$ и $\psi(x)$. Следовательно, многочлены

$D(x)$ и $r(x)$ ассоциированы (отличаются лишь численным множителем):

$$D(x) = \frac{1}{3\theta^2 + 2} r(x),$$

или $$x-\sqrt{2}=x-\frac{\theta^3+60-5}{3\theta^2+2}.$$

Отсюда имеем: $$\sqrt{2}=\frac{\theta^3+60-5}{3\theta^2+2},$$

что и дает искомое выражение для числа $\sqrt{2}$.

Задача 3. Пусть Q ⊂ Q1 ⊂ Q2, где Q1 = Q($\sqrt{2}$),Q2 = Q1 ($\sqrt[3]{5}$). Найти степень поля Q2 относительно Q (то есть размерность Q2 над Q).

Решение. Справедлива теорема: если поле *P1* – конечное расширение поля *P*, а поле *P2* - конечное расширение *P1,* то:

$$\dim_p P_2=\dim_p P_1\cdot\dim_{p_1} P_2 \qquad (1)$$

В нашем случае, очевидно, $\dim_Q Q_1=2$. Покажем, что:

$$\dim_{Q_1} Q_2=3. \qquad (2)$$

Чтобы доказать равенство (2), достаточно проверить, что многочлен $p(x)=x^3-5$ 3-й степени, имеющий число $\sqrt[3]{5}$ своим корнем, неприводим над Q1. Предположим, что это неверно, то есть что $p(x)$ приводим. Тогда один из неприводимых множителей многочлена $p(x)$ должен быть первой степени, и, следовательно, один из корней многочлена $p(x)$ должен принадлежать Q. Таким корнем является, конечно, действительное значение $\sqrt[3]{5}$ (так как все числа из Q1 действительны). Но число $\sqrt[3]{5}$ не может принадлежать Q1, так как его степень над Q равна 3, в то время как степень любого числа из Q1 (над полем Q) не выше 2. Полученное противоречие доказывает (2).

На основании формулы (1) можем теперь записать:

$$\dim_Q Q_2=\dim_Q Q_1\cdot\dim_{Q_1} Q_2=2\cdot 3=6. \qquad (3)$$

Замечание. Сопоставив (3) с тем фактом, что $Q_2=Q(\sqrt{2}+\sqrt[3]{5})$, мы можем вывести заключение, что степень числа $\sqrt{2}+\sqrt[3]{5}$ над полем Q равна 6. Это означает, что многочлен 6-й степени (над полем Q), имеющий своим корнем число $\sqrt{2}+\sqrt[3]{5}$, неприводим.

Задачи для решения

1. Пусть *p* и *q* – натуральные числа, причем $\sqrt{p}$ и $\sqrt[3]{q}$ - не целые. Доказать, что: $Q(\sqrt{p})(\sqrt[3]{q})=Q(\sqrt{p}+\sqrt[3]{q})$.

2. Найти выражение для каждого из чисел $\sqrt{p}$ и $\sqrt[3]{q}$ через $\sqrt{p}+\sqrt[3]{q}$:

а) $p = 3$, $q = 6$; б) $p = 7$, $q = 4$; в) $p = 3$, $q = 3$.

3. Пусть p и q – натуральные числа, причем отношение чисел $\sqrt[3]{p}$ и $\sqrt[3]{q}$ (действительных значений) не является рациональным числом. Доказать, что: $Q(\sqrt[3]{p})(\sqrt[3]{q}) = Q(\sqrt[3]{p} + \sqrt[3]{q})$.

4. Используя условие задачи 3, найти выражение для каждого из чисел $\sqrt[3]{p}$ и $\sqrt[3]{q}$ через $\sqrt[3]{p} + \sqrt[3]{q}$:
а) $p = 3$, $q = 7$; б) $p = 5$, $q = 12$.

Список литературы

1. Кострикин А. И. Введение в алгебру: В 3 кн. Кн. 3: Основные структуры алгебры. – М.: МЦНМО, 2009.
2. Курош А.Г. Курс высшей алгебры. - 17-е изд. - СПб.: Издательский Дом «Лань», 2008.
3. Окунев Л.Я. Высшая алгебра. - 3-е изд. - СПб.: Издательский Дом «Лань», 2009. - 336с.
4. Окунев Л.Я. Сборник задач по высшей алгебре. - 2-е изд. - СПб.: Издательский Дом «Лань», 2009.
5. Фаддеев Д.К., Соминский И.С. Задачи по высшей алгебре. - 17-е изд. - СПб.: Издательский Дом «Лань», 2008. - 288 с.

Шатных Олеся Николаевна

Группы. Кольца. Поля
Методические указания и материалы для практических занятий по алгебре со студентами специальности 010100 - Математика

Редактор Е.А. Устюгова

Подписано к печати	Формат 60x84 1/16	Бумага тип. №1
Печать трафаретная	Усл. печ. л. 2,75	Уч.-изд. л. 2,75
Заказ	Тираж 30	Цена свободная

РИЦ Курганского государственного университета
640669, г. Курган, ул. Гоголя, 25.
Курганский государственный университет