ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)

Кафедра прикладной математики

А.М. Лукацкий

ДОПОЛНИТЕЛЬНЫЕ ГЛАВЫ АЛГЕБРЫ

Учебно-методическое пособие
по изучению дисциплины
и варианты курсовых заданий

для студентов
направления 01.03.04
очной формы обучения

Москва
ИД Академии Жуковского
2020

УДК 512.6
ББК 517
Л84

Рецензент:
Дементьев Ю.И. – канд. физ.-мат. наук

Лукацкий А.М.

Л84 Дополнительные главы алгебры [Текст] : учебно-методическое пособие по изучению дисциплины и варианты курсовых заданий / А.М. Лукацкий. – М.: ИД Академии Жуковского, 2020. – 48 с.

Данное учебно-методическое пособие издается в соответствии с рабочей программой учебной дисциплины «Дополнительные главы алгебры» по учебному плану для студентов направления 01.03.04 очной формы обучения.

Рассмотрено и одобрено на заседаниях кафедры 17.03.2020 г. и методического совета 17.03.2020 г.

УДК 512.6
ББК 517

В авторской редакции

Подписано в печать 02.12.2020 г.
Формат 60x84/16 Печ. л. 3 Усл. печ. л. 2,79
Заказ № 666/0818-УМП21 Тираж 90 экз.

Московский государственный технический университет ГА
125993, Москва, Кронштадтский бульвар, д. 20

Издательский дом Академии имени Н. Е. Жуковского
125167, Москва, 8-го Марта 4-я ул., д. 6А
Тел.: (495) 973-45-68
E-mail: zakaz@itsbook.ru

© Московский государственный технический университет гражданской авиации, 2020

Содержание

Введение

Дополнительные главы алгебры это дисциплина, в которой изучаются алгебраические структуры различных типов, исходя из заданных в каждой структуре наборов операций и системы аксиом. Целью дисциплины является изучение вытекающих из аксиом каждой структуры свойств. Специфика дисциплины состоит в большем, чем в других курсах, количестве определений. Чтобы постоянного обращения читателя к учебникам, все основные определения приводятся в пособии.

В первой части рассматриваются алгебраические структуры с одной операцией (полугруппы, моноиды группы). Вторая часть посвящена структурам с двумя операциями (кольца, поля, алгебры). В третьей части рассматриваются морфизмы алгебраических структур. Изложение построено так, чтобы в единых терминах рассматривать структуры различных типов. В конце излагаются основы теории Галуа. Поскольку ее основные результаты формируются в терминах автоморфизмов полей, она помещена в часть по морфизмам алгебраических структур.

По всем разобранным понятиям строятся примеры. В конце приводятся контрольные задания, каждое из которых получается тиражированием определенной типовой задачи на 20.

Пособие предназначено для студентов 2-го курса, обучающихся по дисциплине дополнительные главы алгебры по направлению подготовки 01.03.04.

Ч А С Т Ь I. Алгебраические структуры с одной бинарной операцией

Исходными для курса алгебры часто являются структуры с одной бинарной операцией. Пусть имеется множеством G, на котором задано соответствие

$$(a,b)\mapsto c=ab, a,b,c\in G. \qquad (1)$$

Если не наложено никаких дополнительных свойств на эту операцию, то G называется группоидом (магмой).

Пример 1.1. Является ли группоидом следующие подмножества $G\subset \mathrm{R}$ множества действительных чисел с операцией умножения:

1) G – положительные числа;

2) G – рациональные числа;

3) G – иррациональные числа.

Решение. Здесь достаточно проверить, является ли числовое множество G замкнутым относительно операции умножения. Это верно для 1 и 2, но неверно для 3.

Более интересными оказываются структуры, в которых операция обладает определенным набором свойств. Они будут рассмотрены ниже.

1.1. Понятия полугруппы, моноида

Определение 1. Группоид G называется полугруппой, если операция (1) ассоциативна:

$$(ab)c=a(bc) \qquad (2)$$

Пример 1.2. Является ли полугруппой множество непрерывных функций на числовой прямой $G=C(\mathrm{R})$ с операцией:

1) $(f*g)(x)=\frac{1}{2}(f(x)+g(x))$;

2) $(f\bullet g)(x)=\max(f(x),g(x))$.

Решение. В случае 1 G замкнуто по операции *, т.к. из непрерывности $f(x), g(x)$ следует непрерывность $\frac{1}{2}(f(x)+g(x))$. Поэтому $G-$ группоид.

Далее имеем

$$((f*g)*h)(x)=\frac{1}{2}\left(\frac{1}{2}(f(x)+g(x))+h(x)\right)=\frac{1}{4}f(x)+\frac{1}{4}g(x)+\frac{1}{2}h(x) \quad ;$$

$$(f*(g*h))(x)=\frac{1}{2}\left(f(x)+\frac{1}{2}(g(x)+h(x))\right)=\frac{1}{2}f(x)+\frac{1}{4}g(x)+\frac{1}{4}h(x) \quad .$$

Таким образом, $((f * g) * h) \neq (f * (h * g))$ и G не является полугруппой по операции *.

В случае 2 G замкнуто по операции $\bullet$, т.к. из непрерывности $f(x), g(x)$ следует непрерывность $\max(f(x), g(x))$. Поэтому G – группоид. Далее заметим, что $\max((a,b),c) = \max(a,(b,c)) = \max(a,b,c)$. Отсюда $((f \bullet g) \bullet h)(x) = (f \bullet (h \bullet g))(x) = \max(f(x), g(x), h(x))$. Значит, G является полугруппой по операции $\bullet$.

Определение 2 . Элемент e полугруппы G называется единицей, если для любого элемента $a \in G$ имеем:

$$ae = ea = a \qquad (3)$$

Полугруппа, обладающая единицей, называется моноидом.

Пример 1.3. Является ли моноидом множество непрерывных функций на числовой прямой $G = C(\mathrm{R})$ с операцией $f \bullet g$ из примера 1.2, 2:

Решение. Согласно примеру 1.2 G является полугруппой. Предположим, что элемент $f \in G$ является ее единицей. Имеем $f \in C(\mathrm{R})$. Фиксируем $x_0 \in \mathrm{R}$. Можно подобрать такую функцию $g \in C(\mathrm{R})$, что $g(x_0) < f(x_0)$. Тогда $(f \bullet g)x_0 = \max(f(x_0), g(x_0)) = f(x_0) \neq g(x_0)$. Таким образом, $f \bullet g \neq g$, значит f не является единицей, а G – моноидом.

Определение 3 . Подмножество H полугруппы (моноида) G называется подполугруппой (подмоноидом), если оно замкнуто относительно операции (1) (и содержит единицу). Тогда H само является полугруппой (моноидом).

Пример 1.4. Является ли подполугруппой в полугруппе непрерывных функций на числовой прямой $G = C(\mathrm{R})$ с операцией $f \bullet g$ из примера 1.2, 2 подмножество $H = C^{+}(\mathrm{R})$, состоящее из неотрицательных функций.

Решение. Если $f, g \in H$, то $\forall x: f(x), g(x) \geq 0$. Но тогда и $\forall x: \max(f(x), g(x)) \geq 0$. Значит $f \bullet g \in H$, откуда H – подполугруппа.

Пример 1.5. Является ли моноидом полугруппа H из предыдущего примера.

Решение. Покажем, что функция $e(x) \equiv 0$ является единицей. Имеем $\mathrm{e} \bullet g\ (x) = \max(0, g(x)) = g(x)$. Поэтому H – имеет единицу и является моноидом.

Определение 4 . Полугруппа (моноид) с коммутативной операцией ($ab = ba$) называется коммутативной.

Пример 1.6. Является ли коммутативной полугруппой (моноидом) множество $Mat(n)$ вещественных матриц $n \times n$ по операции

1) сложения;

2) умножения.

Решение. Т.к. сложение и умножение матриц ассоциативные операции, то по каждой из них $Mat(n)$ является полугруппой. Для операции сложения единицей является нулевая матрица $0=\{a_{i,j} \mid a_{i,j}=0\}$ (все коэффициенты нулевые), для умножения – единичная матрица $\mathrm{Id}=\{a_{i,j} \mid a_{i,j}=0 \text{ при } i\neq j, \text{иначе } 1\}$ (на главной диагонали единицы, остальные – нули). Поэтому по каждой из операций $Mat(n)$ – моноид. Операция сложения матриц коммутативна, а умножения – некоммутативна. Поэтому коммутативным моноидом $Mat(n)$ является только в случае 1.

1.2. Понятия группы

Определение 5. Моноид G называется группой, если по операции (1) каждый элемент имеет обратный:

$$\forall g\in G\,\exists h\in G:\ gh=hg=e. \qquad (4)$$

Обратный элемент обозначается обычно g^{-1}.

Эквивалентным определением является требование разрешимости уравнений

$ax=b$,

$xa=c$.

Если в группе выполняется равенство $gh=gf$, то отсюда следует, что $h=f$, т.к. $g^{-1}(gh)=g^{-1}(gf)=(g^{-1}g)f=ef=f=(g^{-1}g)h=eh=h$. Отсюда следует единственность обратного элемента, т.к. для двух обратных элементов имеем $gh=gf=e$.

Пример 1.7. Является ли группой множество матриц $Mat(n)$ из примера 1.6 с операцией

1) сложения;

2) умножения.

Решение. По каждой из этих операций $Mat(n)$ является моноидом. В случае операции 1 для матрицы $A=\{a_{i,j}\}$ обратной будет матрица $-A=\{-a_{i,j}\}$, т.к. $A+(-A)=\{0\}=0$, поэтому $Mat(n)$ – группа по операции сложения. В случае 2 нулевая матрица не имеет обратной, т.к. $\forall A\in Mat(n): A0=0\neq \mathrm{Id}$. Поэтому по операции умножения $Mat(n)$ не является группой.

Пример 1.8. Являются ли группами следующие подмножества в множестве матриц $Mat(n)$ с операцией умножения

1) $GL(n)=\{A\in Mat(n) \mid \det(A)\neq 0\}$;

2) $SL(n)=\{A\in Mat(n) \mid \det(A)=1\}$.

Решение. Из свойств определителя $\det(AB)=\det(A)\det(B), \det(\mathrm{Id})=1$, поэтому $GL(n), SL(n)$ являются моноидами. Т.к. матрица с ненулевым

определителем имеет обратную по операции умножения, и $\det(A^{-1})=\det(A)^{-1}$, то $\forall A\in GL(n): A^{-1}\in GL(n), \forall B\in SL(n): B^{-1}\in SL(n)$. Поэтому $GL(n), SL(n)$ являются группами.

Определение 6. Группа G называется абелевой, если операция (1) коммутативна.

$$\forall g,h\in G: gh=hg\ . \tag{5}$$

Пример 1.9. Является ли группой, абелевой группой множество вещественных матриц 2×2 с операцией умножения вида:

1) $H=\left\{\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}, n\in \mathrm{Z}\right\}$;

2) $F=\left\{\begin{pmatrix}a & b\\ 0 & a^{-1}\end{pmatrix}, a>0, b\in \mathrm{R}\right\}$.

Решение. Вычислим умножение указанных матриц.

В случае 1 имеем $\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & n+m\\ 0 & 1\end{pmatrix}\in H$. Эта операция коммутативна.

Кроме того, $\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}1 & -n\\ 0 & 1\end{pmatrix}\in H$. Поэтому $H-$ это абелева группа.

В случае 2 имеем $\begin{pmatrix}a & b\\ 0 & a^{-1}\end{pmatrix}\begin{pmatrix}c & d\\ 0 & c^{-1}\end{pmatrix}=\begin{pmatrix}ac & ad+bc^{-1}\\ 0 & (ac)^{-1}\end{pmatrix}\in F$. Эта операция некоммутативна. Например, $\begin{pmatrix}2 & 3\\ 0 & 2^{-1}\end{pmatrix}\begin{pmatrix}3 & 2\\ 0 & 3^{-1}\end{pmatrix}=\begin{pmatrix}6 & 5\\ 0 & 6^{-1}\end{pmatrix}$,

$\begin{pmatrix}3 & 2\\ 0 & 3^{-1}\end{pmatrix}\begin{pmatrix}2 & 3\\ 0 & 2^{-1}\end{pmatrix}=\begin{pmatrix}6 & 10\\ 0 & 6^{-1}\end{pmatrix}$. Также имеем

$\begin{pmatrix}a & b\\ 0 & a^{-1}\end{pmatrix}^{-1}=\begin{pmatrix}a^{-1} & -b\\ 0 & a\end{pmatrix}\in F$. Поэтому $F-$ это группа, но не абелева.

Важным примером группы является группа преобразований конечного множества из *n* элементов (группа подстановок S_n). Элементы этой группы изображаются следующим образом:

$$P=\begin{pmatrix}1 & 2 & \dots & n\\ i_1 & i_2 & \dots & i_n\end{pmatrix} \tag{6}.$$

Закон преобразования этой подстановки имеет вид: $P(k)=i_k$.

Порядок (количество элементов) в группе S_n равен количеству перестановок множества из n элементов $n!$ ($|S_n|=n!$). Простейшим примером подстановки является транспозиция $T_{i,j}$, $i \neq j$, которая переставляет два элемента множества, а остальные не меняет:

$$T_{i,j}(k)=\begin{cases} j, k=i \\ i, k=j \\ k, k\neq i, j \end{cases} \qquad (7).$$

Транспозиция обладает свойством, называемым инволютивностью : $(T_{i,j})^2=\mathrm{Id}$.

Любую подстановку можно разложить в произведение транспозиций. Алгоритм разложения следующий. Заметим, что для подстановки (6) имеем

$$T_{1,i_1}P=\begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & j_2 & \ldots & j_n \end{pmatrix}=Q.$$

Подстановку Q уже можно рассматривать, как преобразование множества из n -1 элементов. Применяем к ней тот же самый прием, и т.д., пока не получим подстановку из двух элементов, которая либо транспозиция, либо тождественное преобразование.

Пример 1.10. Разложить в произведение транспозиций подстановку

$$R=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}.$$

Решение.

Шаг 1.

$$T_{1,5}R=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}=R_1.$$

Шаг 2.

$$T_{2,3}T_{1,5}R=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}=R_2.$$

Шаг 3.

$$T_{3,5}T_{2,3}T_{1,5}R=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}=R_3=T_{4,5}.$$

Отсюда, умножая обе части равенства слева на транспозиции и используя свойство инволютивности, получаем искомое разложение:

$R = T_{1,5}T_{2,3}T_{3,5}T_{4,5}$.

Определение 7. Подмножество H группы G называется

подгруппой, если оно замкнуто относительно операции (1) и вместе с каждым элементом содержит ему обратный, тогда H автоматически содержит единицу и само является группой.

С каждым элементом $g \in G$ можно связать подгруппу $H_g = \{g^k \mid k \in Z\}$, состоящую из целых степеней этого элемента, очевидно, она абелева. Если порядок H_g конечен, то он называется порядком элемента g ($o(g) = |H_g|$). Подгруппа H_g называется циклической. Если группа совпадает со своей циклической подгруппой, она также называется циклической.

Теорема Лагранжа устанавливает, что в конечной группе G порядок ее подгруппы H делит порядок G. В частности, $o(g)$ делит $|G|$.

Если порядок группы – простое число, то у нее не может быть собственных подгрупп, а значит, она является циклической и абелевой.

Пример 1.11. Найти все подгруппы в группе S_3 .

Решение. Имеем $|S_3| = 3! = 6$. Поэтому собственная подгруппа $H \subset S_3$ может состоять из 2-х или 3-х элементов. Существуют 3 подгруппы из 2-х элементов, состоящие из транспозиции и тождественного преобразования.

$H_1 = \{\mathrm{Id}, T_{1,2}\}, H_2 = \{\mathrm{Id}, T_{1,3}\}, H_3 = \{\mathrm{Id}, T_{2,3}\}$.

Кроме того, в S_3 имеется элемент порядка 3. Это подстановка $P = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Имеем $P^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ и $P^3 = \mathrm{Id}$.

Таким образом, элемент P порождает подгруппу из 3-х элементов $H = \{\mathrm{Id}, P, P^2\}$.

Так как

$S_3 = \{\mathrm{Id}, T_{1,2}, T_{1,3}, T_{2,3}, P, P^2\}$,

то других подгрупп нет. Таким образом, S_3 имеет 4 подгруппы:

H_1, H_2, H_3, H .

Пример 1.12. Является ли группа S_3 абелевой.

Решение. Каждая из собственных подгрупп S_3 абелева. Поэтому имеет смысл проверить произведение элементов из разных подгрупп. Имеем :

$T_{2,3}T_{1,2} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $T_{1,2}T_{2,3} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq T_{2,3}T_{1,2}$. Поэтому группа S_3 неабелева.

Если в группе G имеется подгруппа H , то в G можно задать отношение эквивалентности

$$g_1 \approx g_2 \Leftrightarrow g_2 = g_1 h, h \in H \qquad (8)$$

Оно определяет разбиение G на классы эквивалентности, которые называются левыми смежными классами. Если группа G неабелева, можно задать другое отношение эквивалентности

$$g_1 \approx g_2 \Leftrightarrow g_2 = h g_1, h \in H \quad , \qquad (9)$$

которое определяет разбиение G на правые смежные классы.

В общем случае на множестве смежных классах (как левых, так и правых) нельзя задать групповой операции.

Однако, можно выделить класс подгрупп, для которых результат произведения элементов из двух заданных смежных классов попадает в один и тот же смежный, т.е. смежный класс произведения зависит только от смежных классов сомножителей. В таком случае на множестве смежных классов можно задать групповую операции.

Определение 8. Подгруппа H группы G называется нормальным делителем (нормальной подгруппой), если

$$\forall g \in G \; \forall h \in H : g^{-1} h g \in H \quad . \qquad (10)$$

При проверке (10) полезно использовать следующий факт, если оно верно для двух элементов $h_1, h_2 \in H$, то верно и для их произведения $h_1 h_2$, т.к. тогда

$$g^{-1} h_1 h_2 g = g^{-1} h_1 g \; g^{-1} h_2 g \in H . \qquad (11)$$

Для нормальных делителей левые смежные классы совпадают с правыми, и можно ввести групповую операцию на множестве смежных классов.

$$g_1 H * g_2 H = g_1 g_2 H \quad . \qquad (12)$$

Группа с операцией (12) называется факторгруппой и обозначается G / H .

Пример 1.13. Какие из подгрупп группы S_3 являются нормальными делителями. Построить для нормальных подгрупп факторгруппы.

Решение. Рассмотрим сначала подгруппы

$H_1 = \{\mathrm{Id}, T_{1,2}\}, H_2 = \{\mathrm{Id}, T_{1,3}\}, H_3 = \{\mathrm{Id}, T_{2,3}\}.$

Для H_1 имеем

$T_{2,3}{}^{-1} T_{1,2} T_{2,3} = T_{2,3} T_{1,2} T_{2,3} = T_{1,3} \notin H_1$.

Поэтому H_1 не является нормальным делителем. Аналогично это устанавливается для H_2, H_3.

Рассмотрим $H=\{\mathrm{Id}, P, P^2\}$, где $P=\begin{pmatrix}1\ 2 3\\ 2\ 3\ 1\end{pmatrix}$.

Имеем

$$T_{1,2}{}^{-1}PT_{1,2}=T_{1,2}PT_{1,2}=\begin{pmatrix}1\ 2\ 3\\ 3\ 1\ 2\end{pmatrix}=P^2\in H,$$

$$T_{1,3}{}^{-1}PT_{1,3}=T_{1,3}PT_{1,3}=P^2\in H,\ T_{2,3}{}^{-1}PT_{2,3}=T_{2,3}PT_{2,3}=P^2\in H.$$

Для элемента P^2 аналогичную проверку можно не проводить, а использовать (11). Таким образом, H является нормальным делителем. Факторгруппа S_3/H состоит из двух смежных классов $H, T_{1,2}H$, где $H=e-$нейтральный элемент факторгруппы, а $T_{1,2}H=g-$ элемент со свойством $g^2=e$.

Пример 1.14. Является ли описанная в примере 1.8 группа $SL(n)$ нормальным делителем $GL(n)$.

Решение. Возьмем $A\in GL(n), B\in SL(n)$ и покажем, что $A^{-1}BA\in SL(n)$. Имеем $\det(A^{-1}BA)=\det(A^{-1})\det(B)\det(A)=\det(A)^{-1}\det(B)\det(A)=\det(B)=1$. Значит, $A^{-1}BA\in SL(n)$, и $SL(n)-$нормальный делитель.

Определение 9. Коммутатором двух элементов неабелевой группы G называется выражение

$$\{g,h\}=g^{-1}h^{-1}gh\ . \qquad (13)$$

Подгруппа, $\{G,G\}$. порожденная коммутаторами, называется коммутантом, обозначается $\{G,G\}$.

Два элемента группы коммутируют, если их коммутатор равен единице $\{g,h\}=e$.

Пример 1.15. Является ли коммутант группы нормальным делителем, а фактор по нему абелевой группой.

Решение. Возьмем $a,g,h\in G$. Непосредственно проверяется, что $a^{-1}\{g,h\}a=\{a^{-1}ga,\ a^{-1}ha\}\in\{G,G\}$. Отсюда, используя (11), получаем, что $\{G,G\}$ нормальный делитель G. Рассмотрим факторгруппу $G/\{G,G\}$ и возьмем в ней 2 элемента $g\{G,G\}$ и $h\{G,G\}$. Имеем $\{g\{G,G\},h\{G,G\}\}=\{g,h\}\{G,G\}=\{G,G\}$, что соответствует единице факторгруппы. Отсюда факторгруппа $G/\{G,G\}-$абелева.

Ч А С Т Ь II. Алгебраические структуры с двумя операциями

В алгебре весьма распространенными являются структуры с двумя бинарными операциями. Пусть имеется множеством K, на котором заданы соответствия

$$(a,b)\mapsto c=a+b, a,b,c\in K; \qquad (14)$$
$$(a,b)\mapsto c=ab, a,b,c\in K.$$

Условно назовем одну из них сложением (обозначение +), другую умножением. Конкретные алгебраические структуры возникают путем наложения дополнительных свойств на эти операции.

2.1. Понятия почтикольца, кольца

Определение 10. Множество K с операциями (14) называется левым (правым) почтикольцом, если:

1)по операции сложения (+) K является абелевой группой;
2)по операции умножения выполняется свойство левой (правой) дистрибутивности:

$$a(b+c)=ab+ac \quad ((b+c)a=ba+ca) \qquad . \qquad (15)$$

Множество K с операциями (14) называется кольцом, если является и левым и правым почтикольцом.

При дополнительных ограничениях на операцию умножения возникают определенные типы колец:

ассоциативные кольца $a(bc)=(ab)c$;
коммутативные кольца $ab=ba$;
антикоммутативные кольца $ab=-ba$;
кольца с единицей $\exists e\in K:\forall a\in K: ae=ea=a$.

Пример 2.1. Является ли множество $V(\mathrm{R}^3)$ векторов в трехмерном пространстве с операциями сложения векторов ($\vec{u}+\vec{v}$) и векторного произведения ($\vec{u}\times\vec{v}$) кольцом.

Решение. По операции + множество $V(\mathrm{R}^3)$ является абелевой группой, в которой нейтральным элементом является нулевой вектор.

Из свойств векторного произведения имеем

$\vec{u}\times(\vec{v}+\vec{w})=\vec{u}\times\vec{v}+\vec{u}\times\vec{w},\ (\vec{v}+\vec{w})\times\vec{u}=\vec{v}\times\vec{u}+\vec{w}\times\vec{u}$.

Поэтому $V(\mathrm{R}^3)$ кольцо. Из свойств векторного произведения имеем $\vec{u}\times\vec{v}=-\vec{v}\times\vec{u}$, поэтому это кольцо антикоммутативно.

В кольцах возникает новое понятие, – делители нуля.

Определение 11. Ненулевой элемент a кольца K называется левым(правым) делителем нуля, если существует ненулевой элемент b такой, что $ab=0$ ($ba=0$). Элемент, который левый и правый делитель нуля одновременно, называется делителем нуля.

Пример 2.2. В кольце $V(\mathrm{R}^3)$ из примера 2.1 любой ненулевой элемент является делителем нуля, т.к. $\vec{u}\times\vec{u}=-\vec{u}\times\vec{u}=0$.

В кольце без делителей нуля действует закон сокращения: $ab=ac, a\neq 0\Rightarrow b=c\ (ba=ca, a\neq 0\Rightarrow b=c)$.

Определение 12. Коммутативное ассоциативное кольцо K с единицей без делителей нуля называется областью целостности.

Пример 2.3. Является ли кольцом множество матриц $Mat(n)$ из примера 1.7 с операциями сложения и умножения матриц (если да, то какого типа).

Решение. По операции сложения $Mat(n)$ является абелевой группой, по умножению – моноидом. Из свойств умножения матриц $\forall A,B,C\in Mat(n): A(B+C)=AB+AC, (B+C)A=BA+CA$.

Поэтому $Mat(n)-$ассоциативное кольцо с единицей. В общем случае умножение матриц некоммутативно и $Mat(n)$ имеет делители нуля. Например,

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

Пример 2.4. Является ли областью целостности множество Z[N] многочленов с целыми коэффициентами.

Решение. Множество Z[N] замнуто относительно операций сложения и умножения. Из свойств сложения и умножения многочленов это коммутативное, ассоциативное кольцо с единицей. Пусть $p,q\in Z[N]\setminus\{0\}$. Тогда $p=a_0+a_1x+\ldots+a_nx^n, q=b_0+b_1x+\ldots+b_mx^m, a_n\neq 0, b_m\neq 0$. Имеем $pq=a_nb_mx^{n+m}+\ldots\neq 0$. Поэтому $Z[n]$ не имеет делителей нуля и является областью целостности.

Пример 2.5. Является ли областью целостности множество $\mathrm{Gauss}=\{a+bi\,|\,a,b\in\mathrm{Z}\}$ целых гауссовых чисел.

Решение. Множество Gauss замкнуто относительно операций сложения и умножения и содержит единицу ($1=1+0\mathrm{i}$). Из свойств умножения комплексных чисел Gauss коммутативно, ассоциативно. Для пары комплексных чисел $z_1, z_2 \neq 0$ имеем $|z_1 z_2| = |z_1||z_2| > 0$, откуда $z_1 z_2 \neq 0$, значит, Gauss не имеет делителей нуля и является областью целостности.

Для области целостности K через K^* обозначим множество обратимых элементов, т.е. таких элементов, которые имеют обратные по операции умножения ($a \in K^* \Leftrightarrow \exists b \in K : ab = 1$), K^* является группой.

Пример 2.6. Вычислить группу обратимых элементов кольца целых гауссовых чисел Gauss^*.

Решение. Рассмотрим элемент $z = \{a + bi | a, b \in Z\} \in \mathrm{Gauss}^*$. Имеем $|z|^2, |z^{-1}|^2 = (|z|^2)^{-1} \in N$, откуда $|z|^2 = 1$, и получаем $\mathrm{Gauss}^* = \{1, -1, i, -i\}$.

Хотя в областях целостности нет делителей нуля, для них не справедлива теорема о разложении ненулевых элементов на простые множители. Поэтому выделяют более узкий класс колец, называемых евклидовыми кольцами.

Определение 13. Евклидовым кольцом является область целостности K в которой:

1) задана норма, т.е. отображение

$$w : K \mapsto N \cup \{0\}, \forall a, b \in K \setminus \{0\} : w(ab) \geq w(a);$$

2) выполнимо деление с остатком

$$\forall p, q \in K, q \neq 0,$$
$$\exists s, r \in K : p = qs + r,$$
$$w(r) < w(q) \text{ либо } r = 0.$$

Хорошо известные примеры евклидовых колец это кольцо целых чисел, кольцо многочленов с вещественными или комплексными коэффициентами, деление с остатком в которых производится по алгоритму Евклида.

Определение 14. Элемент евклидова кольца $K, p \in K \setminus \{0\}$ называется неприводимым, если из равенства $p = ab$ следует, что $a \in K^*$ или $b \in K^*$.

Пример 2.7. Доказать, что кольцо целых гауссовых чисел Gauss, – евклидово.

Решение. Построим алгоритм деления с остатком. Пусть даны элементы $p,q \in \text{Gauss}, q \neq 0$. Имеем $\frac{p}{q} = a + bi, a, b \in \text{R}$. Возьмем ближайшие к a, b целые числа n, m (при наличии двух таких выберем наименьшее). Тогда $a + bi = n + mi + x + yi$. По построению $|x|, |y| \leq \frac{1}{2}, |x + yi|^2 \leq \frac{1}{2}$. Обозначим $s = n + mi$, $r = (x + yi)q$.

Имеем $p = qs + r$.

Т.к. $p, q, s \in \text{Gauss}$, то $r \in \text{Gauss}$.

Имеем $|r|^2 \leq |q|^2 |x + yi|^2 \leq \frac{1}{2}|q|^2 < |q|^2$, откуда Gauss – евклидово кольцо.

Для евклидовых колец справедлива теорема о существовании разложения на неприводимые множители ненулевого необратимого элемента и единственности такого разложения с точностью до умножения на обратимые элементы.

Пример 2.7. Являются ли неприводимыми элементы кольца целых гауссовых чисел:

1) 2;
2) 3.

Решение. Имеем, элемент $2 = (1 + i)(1 - i)$, – приводим.

Пусть $3 = uv$, где $u, v \in Gauss \setminus Gauss^*$. Тогда $|u|, |v| > 1$, $9 = |u|^2 |v|^2$. Имеем $|u|^2 = 3, |v|^2 = 3$, что невозможно, т.к. $3 \neq a^2 + b^2, a, b \in \text{Z}$. Отсюда 3 – неприводимый элемент в кольце Gauss.

Пример 2.8. Разложить на неприводимые множители элемент кольца целых гауссовых чисел $z = 5 + 7i \in \text{Gauss}$.

Решение. Имеем $|z|^2 = 74$. Если $z = uv, |u|^2 > 1, |v|^2 > 1$, то т.к. $|u|^2 |v|^2 = 74$, и для $|u|^2$ есть две возможности 2 и 37. В случае $|u|^2 = 2$ для элемента u есть две возможности $1 + i, 1 - i$.

Имеем, $\frac{z}{1+i} = \frac{(5+7i)(1-i)}{2} = \frac{12+2i}{2} = 6 + i$.

Отсюда $z = (1 + i)(6 + i)$.

Далее $|1 + i|^2 = 2, |6 + i|^2 = 37$,

поэтому эти элементы неприводимы, т.к. целые числа 2 и 37 не имеют собственных делителей в целых числах. Таким образом, требуемое разложение получено.

2.2. Понятия тела, поля

Определение 15. Ассоциативное кольцо K с единицей e с операциями (14) называется телом, если любой ненулевой элемент имеет обратный по операции умножения:

$$\forall a \in K \setminus \{0\} \exists b \in K : ab = ba = e \ . \qquad (16)$$

Определение 16. Коммутативное тело K называется полем. Конечное поле называется полем Галуа.

Таким образом, полем называется коммутативное ассоциативное кольцо K с единицей e, в котором любой ненулевой элемент имеет обратный по операции умножения (выполнимо(16)). Примерами полей являются:

- множество вещественных чисел R;
- множество рациональных чисел Q;
- множество комплексных чисел C;
- множество вычетов целых чисел по модулю некоторого простого числа p Z_p;

с естественными арифметическими операциями сложения и умножения.
Поля Z_p дают примеры полей Галуа.

Пример 2.9. Является ли полем множество чисел вида $K = \{a + b\sqrt{2} \mid a, b \in \mathrm{Q}\}$.

Решение. Число $a + b\sqrt{2} \mid a, b \in \mathrm{Q}$ однозначно определяется параметрами a, b, т.к. $\sqrt{2}$ – иррациональное число. Из свойств арифметических операций K является областью целостности, где нулем является число 0, а единицей 1. Возьмем $a + b\sqrt{2} \in K \setminus \{0\}$, тогда a или $b \neq 0$. Имеем

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 + 2b^2} = \frac{a}{a^2 + 2b^2} + \frac{(-b)}{a^2 + 2b^2}\sqrt{2} \in K \setminus \{0\}.$$

Поэтому каждый ненулевой элемент имеет обратный по умножению и K является полем.

Определение 17. Подмножество кольца (поля) $L \subset K$ называется подкольцом (подполем), если оно само является кольцом (полем) по операциям сложения и умножения в K.

Пример 2.10. Является ли подкольцом в кольце матриц $Mat(2)$ подмножество $L = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a \in \mathrm{Q}, b \in \mathrm{R} \right\}$.

Решение. L является абелевой группой по операции матричного сложения. Для умножения имеем $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}=\begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix}$, поэтому L замкнуто по операции умножения, откуда L является подкольцом.

Пример 2.11. Может ли подкольцо L в кольце K, не являющимся полем, быть полем.

Решение. Возьмем кольцо многочленов над полем вещественных чисел, $L=\{p\in \mathrm{R}[x] \mid \deg p=0\}$. Тогда элементами L являются многочлены, совпадающие со своими свободными членами, т.е. константы, которые образуют поле R, поэтому подкольцо L является полем.

Если имеется подкольцо L в кольце K, это позволяет построить разбиение K на смежные классы по операции сложения, однако, в общем случае, такое разбиение не будет согласовано с операцией умножения.

Определение 18. Подкольцо кольца $L\subset K$ называется идеалом, если

$$\forall a\in L\,\forall\, b\in K: ab\in L, ba\in L \quad . \qquad (17)$$

Для идеала разбиение K на смежные классы по L как абелевой подгруппе по сложению оказывается согласованным с операцией умножения. Поэтому можно ввести структуру кольца на множестве смежных классов, которое называется факторкольцом и обозначается K/L.

Пусть в кольце K задан ненулевой элемент a. Минимальный идеал, содержащий элемент a, называется главным идеалом L_a. Кольцо, в котором все идеалы главные, называется кольцом главных идеалов.

Если кольцо K – евклидово, а a – неприводимый элемент, то факторкольцо K/L_a является полем. Это дает способ построения новых полей. Если же элемент a – приводим ($a=pq$, где $p,q\notin K^*$), то K/L_a является кольцом с делителями нуля (например, это будут элементы $p+L_a, q+L_a$).

Пример 2.12. Вычислить факторкольцо кольца целых гауссовых чисел Gauss по главному идеалу, порожденному элементом $a=3$.

Решение. Согласно примеру 2.7 элемент 3 – неприводим, поэтому $Q=\mathrm{Gauss}/L_3$ – поле. Смежные классы, образующие Q, имеют в качестве представителей элементы вида $a+bi \mid a,b\in\{0,1,2\}$. Отсюда $||Q|=9$. Таким образом, построено поле из 9-ти элементов, а кольцо целых гауссовых чисел позволяет строить новые примеры полей Галуа. Таблицы операций сложения и умножения в поле Q выглядят следующим образом

Таблица 1. Операция сложения поля Q.

+	0	1	2	i	1+i	2+i	2i	1+2i	2+2i
0	0	1	2	i	1+i	2+i	2i	1+2i	2+2i
1	0	2	0	1+i	2+i	i	1+2i	2+2i	2i
2	2	0	1	2+i	I	1+i	2+2i	2i	1+2i
i	i	1+i	2+i	2i	1+2i	2+2i	0	1	2
1+i	1+i	2+i	i	1+2i	2+2i	2i	1	2	0
2+i	2+i	i	1+i	2+2i	2i	1+2i	2	0	1
2i	2i	1+2i	2+2i	0	1	2	I	1+i	2+i
1+2i	1+2i	2+2i	2i	1	2	0	1+i	2+i	I
2+2i	2+2i	2i	1+2i	2	0	1	2+i	I	1+i

Таблица 2. Операция умножения поля Q .

×	0	1	2	i	1+i	2+i	2i	1+2i	2+2i
0	0	0	0	0	0	0	0	0	0
1	0	1	2	i	1+i	2+i	2i	2+2i	2+2i
2	0	2	1	2i	2+2i	1+2i	I	2+i	1+i
i	0	i	2i	2	2+i	2+2i	1	1+i	1+2i
1+i	0	1+i	2+2i	2+i	2i	1	1+2i	2	I
2+i	0	2+i	1+2i	2+2i	1	i	1+i	2i	2
2i	0	2i	i	1	1+2i	1+i	2	2+2i	2+i
1+2i	0	1+2i	2+i	1+i	2	2i	2+2i	I	1
2+2i	0	2+2i	1+i	1+2i	i	2	2+i	I	2i

Определение 19. Элемент конечного поля $p \in K$ называется примитивным, если его степени исчерпывают мультипликативную группу поля K^*:

$$K^* = \{p^n\} \quad . \qquad (18)$$

Пример 2.13. Найти примитивный элемент поля Q из примера 2.12.

Решение. Имеем, $|Q^*| = 8$. Используем таблицу 2 для вычисления порядков элементов. Получаем $o(2) = 2$. Далее элементы $i, 2i$, квадраты которых равны 2, имеют порядок 4. Элементы $1+i,\ 2+i,\ 2+2i$, квадраты которых равны i или $2i$, имеют порядок 8 и являются примитивными для поля Q .

Пример 2.14. Пусть $q(x)$ многочлен степени 2 или 3 с коэффициентами из поля Q . Если $q(x)$ не имеет корней в поле Q , то это неприводимый элемент кольца многочленов $Q[x]$.

Решение. Предположим, что $q(x)$ – приводим. Тогда $q(x)=s(x)r(x)$, где $\dim s(x)>0, \dim r(x)>0$, кроме того, $\dim q(x)=\dim s(x)+\dim r(x)$. Тогда один из многочленов $s(x), r(x)$ обязан иметь степень 1, значит, $q(x)=s(x)r(x)$ имеет корень.

Пример 2.15. Будут ли неприводимыми следующие многочлены над полем Z_7:

1) $p(x)=x^3+2$;

2) $q(x)=x^3+x+3$.

Решение. Составим таблицу значений многочленов:

x	1	2	3	4	5	6
$p(x)$	3	3	1	3	1	1
$q(x)$	4	5	4	0	6	0

Используя пример 2.14, получаем, что $p(x)$ – неприводим, а $q(x)$ – приводим.

Пример 2.16. Построить конечное поле из 343 элементов.

Решение. Рассмотрим факторкольцо $Z_7[x]/\, p(x)Z_7[x]$, где $p(x)=x^3+2$ взят из примера 2.15. Т.к. $p(x)$ – неприводим, то это поле. Количество элементов в таком факторполе равно $7^{\dim p}=7^3=343$.

Пример 2.17. Показать, что в кольце $\mathrm{R}[x,y]$ многочленов от 2-х переменных с вещественными коэффициентами подмножество $\mathrm{R}_0[x,y]=\{f\in \mathrm{R}[x,y] \mid f(0,0)=0\}$ является идеалом, но не главным.

Решение. Очевидно, $\mathrm{R}_0[x,y]$ – подгруппа по операции +. Возьмем $h\in \mathrm{R}_0[x,y], f\in \mathrm{R}[x,y]$. Тогда $(hf)(0,0)=h(0,0)f(0,0)=0=(fh)(0,0)$. Поэтому $\mathrm{R}_0[x,y]$ – идеал. Предположим, что это главный идеал, а $p[x,y]$ – образующий элемент идеала. Обозначим через $\deg_x p[x,y], \deg_y p[x,y]$ – степени p как многочлена только по x, по y. Т.к. $x,y\in \mathrm{R}_0[x,y]$, то $x=pf, y=pg$. Тогда $\deg_y p\le \deg_y x=0, \deg_x p\le \deg_x, y=0$, откуда $\deg p=0$. Но тогда $p=\mathrm{Const}=0$ и не может быть образующим элементом идеала $\mathrm{R}_0[x,y]$.

Определение 20. Характеристикой поля K ($\mathrm{char}\, K$) называется

1) если оно существует, такое минимальное число $n\in \mathrm{N}$ такое, что

$$\underbrace{1+1+\ldots+1}_{n}=0\ ; \qquad (19)$$

2) если такого $n \in \mathrm{N}$ не существует, то 0.

Минимальное поле заданной характеристики называется простым.
Ненулевая характеристика поля всегда простое число.
Для известных полей имеем:
$\mathrm{char}(\mathrm{Z}_p) = p, \mathrm{char}(\mathrm{Q}) = \mathrm{char}(\mathrm{R}) = \mathrm{char}(\mathrm{C}) = 0.$
Простыми полями являются :
поле рациональных чисел Q;
поля вычетов Z_p, p – простое число. (20)

Пример 2.18. Вычислить характеристику и найти простое подполе для поля из примера 2.12 $Q = \mathrm{Gauss}/L_3$

Решение. Имеем $Q = \{a + bi \mid a, b \in \{0,1,2\}\}$. Отсюда $1+1+1=0$ и $\mathrm{char}(Q)=3$. Простым подполем является $\mathrm{Z}_3 = \{a \mid a \in \{0,1,2\}\}$.

2.3. Понятие алгебры

Определение 21. Алгеброй называется пара из кольца K с операциями (14) и поля Q с дополнительной операцией умножения элементов поля на элементы кольца
$\forall(\lambda, x), \lambda \in Q, x \in K, (\lambda, x) \mapsto \lambda x \in K$:
со свойствами :

1) $(\lambda\mu)x = \lambda(\mu x)$;
2) $1x = x$;
3) $(\lambda + \mu)x = \lambda x + \mu x$;
4) $\lambda(x + y) = \lambda x + \lambda x$;
5) $\lambda(xy) = (\lambda x)y = x(\lambda y)$.

По свойствам (1-4) K с операцией + является векторным пространством над полем Q. Свойство (5) называется билинейностью.

При дополнительных ограничениях на операцию умножения возникают определенные типы алгебр:

ассоциативные алгебры $a(bc) = (ab)c$;
коммутативные алгебры $ab = ba$;
антикоммутативные алгебры $ab = -ba$;
алгебры с единицей $\exists e \in K : \forall a \in K : ae = ea = a$;

алгебры с делением, это алгебры с единицей, в которых $\forall a \in K \setminus \{0\} \forall b \in K$ разрешимы уравнения $ax = b, ya = b$.

Пример 2.19. Является ли алгеброй кольцо $V(\mathrm{R}^3)$ из примера 2.1.

Решение. В качестве поля возьмем $Q = \mathrm{R}$. Т.к. R^3 является векторным пространством над R, то аксиомы алгебры (1-4) выполняются. Из свойств векторного произведения имеем:
$\lambda(u \times v) = (\lambda u) \times v = u \times \lambda v$.
Поэтому $V(\mathrm{R}^3)$ – алгебра. Т.к. векторное произведение антикоммутативно, то это антикоммутативная алгебра.

Определение 22. Подмножество $L \subset K$ алгебры называется подалгеброй, если оно само является алгеброй.

Пример 2.19. Является ли подалгеброй подмножество $L \subset V(\mathrm{R}^3)$, $L = \{\lambda x, x \in R^3 \setminus \{0\}\}$.
Решение. Возьмем два элемента $u = \lambda x, v = \mu x$ из L. Имеем $u + v = (\lambda + \mu)x \in L, u \times v = \lambda x \times \mu x = \lambda \mu\, x \times x = 0 \in L, \alpha u = (\alpha\lambda)x \in L$. Поэтому L является подалгеброй.

Определение 23. Подмножество $L \subset K$ алгебры называется идеалом, если оно является:
1) подалгеброй;
2) $\forall l \in L, k \in K : lk \in L, kl \in L$.

Если алгебра не содержит нетривиальных (отличных от самой алгебры или нуля) идеалов, она называется простой.

Пример 2.20. Имеются ли нетривиальные идеалы в алгебре $V(\mathrm{R}^3)$.

Решение. Пусть L идеал в $V(\mathrm{R}^3)$. Возьмем $x \in L, x \neq 0$. Можно построить такой ортонормированный базис e_1, e_2, e_3 в $V(\mathrm{R}^3)$, что $x = \lambda e_1, \lambda \neq 0$.
Тогда имеем $a = x \times e_2 = \lambda e_1 \times e_2 = \lambda e_3 \in L, b = x \times e_3 = \lambda e_1 \times e_3 = -\lambda e_2 \in L$.

Отсюда $L \supset \{e_1, e_2, e_3\}$ и, значит, $L = V(\mathrm{R}^3)$. Таким образом, алгебра $V(\mathrm{R}^3)$ не имеет нетривиальных идеалов и является простой алгеброй.

Пример 2.21. Обозначим через $M(\mathrm{R})$ множество вещественных ограниченных функций на прямой $(M(\mathrm{R}) = \{f(x) | \max_{x \in \mathrm{R}} |f(x)| < \infty\})$, через $ML(\mathrm{R})$ множество функций, имеющих конечный предел на бесконечности $(ML(\mathrm{R}) = \{f(x) | \exists a \in \mathrm{R} : \lim_{x \to \infty} f(x) = a\})$ и через $ML0(\mathrm{R})$ множество функций, имеющих нулевой предел на бесконечности $(ML0(\mathrm{R}) = \{f(x) | \lim_{x \to \infty} f(x) = 0\})$. Являются ли

1) $M(\mathrm{R})$ алгеброй;

2) $ML(\mathrm{R})$, $ML(\mathrm{R})$ подалгебрами $M(\mathrm{R})$;

3) $ML0(\mathrm{R})$, $ML(\mathrm{R})$ идеалами $M(\mathrm{R})$.

Решение. Пусть $f, g \in M(\mathrm{R}), \lambda \in \mathrm{R}$. Обозначим $\max f = \max_{x\in\mathrm{R}} |f(x)|$. Тогда имеем $\max \lambda f = \max_{x\in\mathrm{R}} |\lambda f(x)| = |\lambda| \max f$, $\max(f+g) \le \max f + \max g$, $\max(fg) \le \max f \max g$, отсюда $M(\mathrm{R})$ – алгебра. Если функция имеет конечный предел на бесконечности, то она ограничена, отсюда $ML(\mathrm{R}) \subset M(\mathrm{R})$, и из свойств пределов это подалгебра. Далее $ML0(\mathrm{R}) \subset ML(\mathrm{R})$, и из свойств пределов это также подалгебра. Если $f \in M(\mathrm{R}), g \in ML0(\mathrm{R})$, то, т.к. произведение ограниченной функции на бесконечно малую является бесконечно малой, то $\lim_{x\to\infty} f(x)g(x) = 0$, поэтому $fg \in ML0(\mathrm{R})$. Таким образом, $ML0(\mathrm{R})$ является идеалом $M(\mathrm{R})$, а, значит, и $ML(\mathrm{R})$. Если $f \in M(\mathrm{R}), g \in ML(\mathrm{R})$, то fg может не иметь предела на бесконечности, например, $f(x) = \sin(x), g(x) \equiv 1$ и $fg \notin ML(\mathrm{R})$. Таким образом, $ML(\mathrm{R})$ не является идеалом $M(\mathrm{R})$.

Ч А С Т Ь III. МОРФИЗМЫ АЛГЕБРАИЧЕСКИХ СТРУКТУР

В алгебре часто требуется устанавливать соответствие между однотипными структурами или же между реализациями одной и той же структуры.

3.1. Понятие гомоморфизма алгебр

Определение 24. Пусть имеются две алгебраические структуры E, F, снабженные одинаковым набором операций. Гомоморфизмом называется отображение $T: E \mapsto F$, сохраняющее эти операции.
Для структур с одной бинарной операцией (1):

$$T(ab)=T(a)T(b) \ ; \tag{21}$$

для структур с двумя бинарными операциями (14):

$$T(a+b)=T(a)+T(b), T(ab)=T(a)T(b); \tag{22}$$

если E, F являются алгебрами над полем Q, то дополнительно требуется $T(\lambda a)=\lambda T(a), \lambda \in Q$.

Пример 3.1. Пусть $E=\mathrm{R}$ множество вещественных чисел с операцией сложения, $F=\mathrm{R}_+^*$ множество положительных чисел с операцией умножения. Будет ли гомомофизмом отображение $T(x)=\exp(\mathrm{x})$.

Решение. Алгебраические структуры E, F являются абелевыми группами. Имеем $T(x+y)=\exp(x+y)=\exp(x)\exp(y)=T(x)T(y)$. Таким образом, $T-$ гомоморфизм групп.

Определение 25. Пусть имеется гомоморфизм $T: E \mapsto F$ двух алгебраических структур E, F. Гомоморфизм называется:

1) мономорфизмом, если отображение $T: E \mapsto F$ взаимно однозначно;

2) эпиморфизмом, если T – отображение на все F $(T(E)=F)$; (23)

3) изоморфизмом, если T мономорфизм и эпиморфизм одновременно;

4) автоморфизмом, если T изоморфизм и $E=F$.

Изоморфные алгебраические структуры можно рассматривать как различные реализации одной и той же структуры.

При изоморфизме групп единица переходит в единицу, колец и полей ноль переходит в ноль.

Пример 3.2. Показать, что при нетривиальном (с ненулевым образом) гомоморфизме областей целостности $T: K \mapsto L$ единица переходит в единицу.

Решение. Возьмем $a \in K, T(a) \neq 0$. Тогда $T(a) = T(a \bullet 1) = T(a) \bullet T(1)$. Отсюда $0 = T(a) \bullet T(1) - T(a) \bullet 1 = T(a) \bullet (1 - T(1))$. Т.к. $T(a) \neq 0$ и в L нет делителей нуля, то $0 = 1 - T(1)$ и $T(1) = 1$.

Пример 3.3. К какому типу относится гомоморфизм из примера 3.1.

Решение. Т.к. функция exp(x) строго монотонна, то отображение $T(x) = \exp(x)$ взаимно однозначно. Возьмем $y \in \mathrm{R}_+^*$ и положим $x = \ln(y) \in \mathrm{R}$, тогда $T(x) = y$, значит, $T(\mathrm{R}) = \mathrm{R}_+^*, T -$ эпиморфизм Таким образом, $T -$ изоморфизм, а группы $\mathrm{R}, \mathrm{R}_+^*$ являются реализациями одной абелевой группы.

Пример 3.4. Является ли изоморфными структурами множества чисел

$$K = \{a + b\sqrt{2} \mid a, b \in \mathrm{Q}\} \text{ и } L = \{a + b\sqrt{3} \mid a, b \in \mathrm{Q}\}$$

со стандартными арифметическими операциями.

Решение. Из примера 2.9 K является полем, по аналогии L – также поле. Пусть существует изоморфизм $T: K \mapsto L$.

Тогда $T(2) = T(1+1) = T(1) + T(1) = 2$.

Обозначим $T(\sqrt{2}) = a + b\sqrt{3}$, имеем

$x^2 = T(\sqrt{2})T(\sqrt{2}) = T(2) = 2$.

Отсюда

$2 = (a + b\sqrt{3})^2 = a^2 + 3b^2 + 2ab\sqrt{3}$.

При $a, b \in \mathrm{Q} \setminus \{0\}$ имеем.

$\sqrt{3} = \dfrac{a^2 + 3b^2 - 2}{2ab} \in \mathrm{Q}$, что невозможно, т.к. $\sqrt{3}$ – иррациональное число.

Если $a = 0 (b = 0)$, имеем $3b^2 = 2 (a^2 = 2)$, что невозможно, т.к. $a, b \in \mathrm{Q}$.

Поэтому поля K, L неизоморфны.

3.2. Понятие ядра и образа гомоморфизма. Вычисление факторов

Определение 26. Пусть имеются гомоморфизмы

1) $T: G \mapsto H$ двух групп G, H;

2) $P: K \mapsto L$ двух колец или алгебр K, L.

Ядром и образом гомоморфизма называется в случаях

1) групп $Ker\, T = \{ g \in G \,|\, T(g) = 1 \}$, $\mathrm{Im} T = \{ T(g) \,|\, g \in G \}$;

2) колец или алгебр $Ker\, P = \{ x \in K \,|\, P(x) = 0 \}$, $\mathrm{Im} P = \{ P(x) \,|\, x \in K \}$. (24)

Пример 3.5. В условиях определения 25 показать, что
1) для групп $Ker\, T$ является нормальным делителем G;
2) для колец $Ker\, P$ является идеалом K.
Решение. Возьмем

1) $h \in Ker\, T, g \in G$.
Имеем $T(g^{-1} h\, g) = T(g^{-1}) T(h) T(g) = T(g)^{-1} T(g) = e$.
Отсюда $g^{-1} h\, g \in Ker T$, и это нормальный делитель.
2) $x \in Ker\, P, y \in K$.
Имеем $P(x\, y) = P(x) P(y) = 0 P(y) = 0$, $P(yx) = P(y) P(x) = P(y) 0 = 0$.
Отсюда $xy, yx \in Ker P$, и это идеал.

Для введенных выше алгебраических структур справедлива теорема о гомоморфизмах:

1) $\mathrm{Im} T \cong G / Ker\, T$;
2) $\mathrm{Im} P \cong P / Ker\, P$. (25)

Пример 3.6. Сформулировать теорему о гомоморфизмах для описанной в примере 1.14 группе $GL(n)$ и отображения $T: GL(n) \mapsto \mathrm{R}^*, T(A) = \det(A)$.
Решение . Имеем
$T(AB) = \det(AB) = \det(A) \det(B) = T(A) T(B)$,
отсюда T –гомоморфизм. Имеем
$Ker T = \{ A \in GL(n) \,|\, \det(A) = 1 \} = SL(n)$.

Покажем, что $\mathrm{Im} T = R^*$, т.е. T –эпиморфизм.
Возьмем $\lambda \in R^*$ и построим матрицу

$A = \{ a_{i,j} \,|\, a_{1,1} = \lambda,\ a_{i,i} = 1 \text{ для } i > 1, a_{i,j} = 0 \text{ для } i \neq j \}$.

Тогда $\det(A)=\lambda$, значит, $\lambda \in \mathrm{Im}T$.

В итоге получаем $GL(n)/SL(n)=\mathrm{R}^*$.

Пример 3.7. В обозначениях примера 2.21 вычислить факторалгебру $ML(\mathrm{R})/ML0(\mathrm{R})$.

Решение. Введем отображение $F:ML(\mathrm{R})\mapsto \mathrm{R}, F(f)=\lim_{x\to\infty} f(x)$. Из свойств пределов это гомоморфизм алгебр. Имеем, $\mathrm{Ker}\, F=\{f=\lim_{x\to\infty} f(x)=0\}=ML0(\mathrm{R}), \mathrm{Im}\, F=\{\lim_{x\to\infty} f(x)\}=\mathrm{R}$, т.е. F – эпиморфизм. Тогда по теореме о гомоморфизмах имеем $ML(\mathrm{R})/ML0(\mathrm{R})\cong\mathrm{R}$.

Ч А С Т Ь IY. ЭЛЕМЕНТЫ ТЕОРИИ ГАЛУА

4.1. Расширения полей

Определение 27. Пусть имеется поле K. Расширением K называется поле $L \supset K$. Расширение называется:

1) конечным, если $\dim_K L < \infty$;

2) алгебраическим, если $\forall l \in L \exists\, p(x) \in K[x] \setminus \{0\} : p(l) = 0$;

3) трансцендентным, если оно не является алгебраическим.

Пример 4.1. Является ли алгебраическим расширение $\mathrm{R} \supset \mathrm{Q}$.

Решение. Возьмем число $\pi \in \mathrm{R}$. Как известно, число π – трансцендентное и не может быть корнем ненулевого многочлена с рациональными коэффициентами, поэтому и расширение $\mathrm{R} \supset \mathrm{Q}$ трансцендентное.

Пример 4.2. Является ли алгебраическим расширение $\mathrm{C} \supset \mathrm{R}$.

Решение. Возьмем $z \in \mathrm{C} \setminus \mathrm{R}$, имеем $z = a + bi, b \neq 0$. Положим $p(x) = x^2 - 2ax + a^2 + b^2$. Тогда $p(z) = 0$ и расширение – алгебраическое.

Пример 4.3. Показать, что любое конечное расширение $L \supset K$ является алгебраическим.

Решение. Пусть $\dim_K L = n$. Возьмем $l \in L$ и рассмотрим элементы $1, l, l^2, \ldots, l^n$. Они являются линейно зависимыми, поэтому существует нетривиальная линейная комбинация

$$c_0 1 + c_1 l + c_2 l^2 + \ldots + c_n l^n = 0.$$

Тогда, если положить $p(x) = c_0 1 + c_1 x + c_2 x^2 + \ldots + c_n x^n$, то $p(l) = 0$.

Определение 28. Пусть имеется расширение поля K (т.е. поле $L \supset K$). Группой $\mathrm{Aut}_K L$ называется группа автоморфизмов поля L, оставляющих неподвижными элементы поля K.

Пример 4.4. Пусть имеется расширение $L \supset K$ и неприводимый многочлен $p(x) \in K[x]$ над полем K, имеющий корень α в поле L, а $F \in \mathrm{Aut}_K L$. Показать, что $p(F(\alpha)) = 0$.

Решение. Имеем $p(x) = c_0 1 + c_1 x + c_2 x^2 + \ldots + c_n x^n, c_i \in K, i = 0,\ldots,n$. Тогда

$$F(p(\alpha)) = F(c_0 1 + c_1 \alpha + c_2 \alpha^2 + \ldots + c_n \alpha^n) =$$

$$= c_0 1 + c_1 F(\alpha) + c_2 F(\alpha)^2 + \ldots + c_n F(\alpha)^n) = p(F(\alpha)) = F(0) = 0 .$$

Определение 29. Пусть имеется конечное расширение $L \supset K$ и неприводимый многочлен $p(x) \in K[x]$ над полем K, имеющий корни в поле L. Многочлен $p(x)$ называется сепарабельным, если он не имеет кратных корней. Конечное расширение поля, получающееся путем добавления корней сепарабельного многочлена, называется сепарабельным расширением.

Если, кроме того, расширение обладает тем свойством, что из наличия хотя бы одного корня в поле L у неприводимого над полем K многочлена $p(x)$ следует, что он разлагается на линейные множители,
то такое расширение называется нормальным, а L – полем разложения многочлена $p(x)$.

Пример 4.5. Вычислить $\mathrm{Aut}_{\mathrm{R}} \mathrm{C}$.

Решение. Возьмем многочлен $p(x) = x^2 + 1$. Пусть $F \in \mathrm{Aut}_{\mathrm{R}} \mathrm{C}$. Многочлен $p(x)$ неприводим над R и имеет корни $i, -i \in \mathrm{C}$. Из примера 3.10 имеем две возможности $1) F(i) = i, 2) F(i) = -i.$ В случае 1 имеем $F(a+bi) = a+bi$ и $F = \mathrm{Id}$. В случае 2 имеем $F(a+bi) = a-bi$ и $F(z) = \bar{z}$. Из свойств операции комплексного сопряжения в случае 2 F – автоморфизм и $F^2 = \mathrm{Id}$. Таким образом, $\mathrm{Aut}_{\mathrm{R}} \mathrm{C} \cong \mathrm{Z}_2$.

Определение 30. Пусть имеется конечное сепарабельное и нормальное расширение $L \supset K$. Тогда $L \supset K$ называется расширением Галуа, а группа $\mathrm{Aut}_K L$ – группой Галуа расширения (обозначается $\mathrm{Gal}_K L$).

Пример 4.6. Является ли расширение $\mathrm{C} \supset \mathrm{R}$ расшрением Галуа, и если да, чему равна группа Галуа расширения.

Решение. Расширение $\mathrm{C} \supset \mathrm{R}$ можно построить при помощи неприводимого над R сепарабельного многочлена $p(x) = x^2 + 1$. По теореме Гаусса любой многочлен над C положительной степени разлагается на линейные множители, поэтому это нормальное расширение, и, следовательно,

является расширением Галуа. Из примера 4.5 группа Галуа расширения $\mathrm{C} \supset \mathrm{R}$ это $\mathrm{Aut}_{\mathrm{R}}\mathrm{C} \cong \mathrm{Z}_2$, она переставляет корни многочлена $p(x)$.

4.2. Понятие разрешимой группы

Определение 31. Пусть дана группа G. Введем центральный ряд группы

$G_1 = \{G, G\}$ (коммутант, см. определение 9),
$G_2 = \{G_1, G_1\}$,
… ,
$G_{n+1} = \{G_n, G_n\}$,
… ,

Группа G называется разрешимой, если ее центральный ряд конечен, т.е. для некоторого номера n имеем $G_n = \{e\}$.

Пример 4.7. Показать, что если группа G разрешима, то подгруппа $H \subset G$ также разрешима.

Решение. Имеем $\{H, H\} \subset \{G, G\}$, т.е. $H_1 \subset G_1$.

Далее $H_2 \subset G_2, \ldots, H_n \subset G_n = \{e\}$. Отсюда H – разрешима.

Пример 4.8. Показать, что группа S_3 из примера 1.13 разрешима.

Решение. Вычислим коммутатор двух транспозиций. Используем то, что обратной к транспозиции является она сама (свойство инволютивности). Тогда в обозначениях 1.13 имеем

$$\{T_{1,2}, T_{1,3}\} = T_{1,2}T_{1,3}T_{1,2}T_{1,3} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P \in H ;$$

$$\{T_{1,2}, T_{2,3}\} = T_{1,2}T_{2,3}T_{1,2}T_{2,3} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = P^2 \in H .$$

$$\{T_{1,3}, T_{2,3}\} = T_{1,3}T_{2,3}T_{1,3}T_{2,3} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P \in H$$

Так как группа S_3 порождается элементами $T_{1,2}, T_{1,3}, T_{2,3}$, то $(S_3)_1 = \{S_3, S_3\} = H$. Далее заметим, что группа H абелева, так как эта группа состоит из 3-х элементов, тогда

$(S_3)_2 = \{(S_3)_1, (S_3)_1\} = \{H, H\} = \{e\}$.

Поэтому группа S_3 разрешима.

4.3. Условие разрешимости в радикалах полиномиального уравнения

Пусть теперь имеется неприводимый многочлен $p(x)$ над полем K и расширение Галуа $L \supset K$, причем L является полем разложения многочлена $p(x)$. Основной результат теории Галуа гласит, что если группа Галуа расширения $\mathrm{Gal}_K L$ – разрешима, то уравнение

$$p(x)=0 \qquad (26)$$

разрешимо в радикалах.

Пример 4.9. Показать, что в условиях выше для многочлена 3-й степени $p(x)$ уравнение (26) разрешимо в радикалах.

Решение. Расширение $L \supset K$ является расширением Галуа. Группа Галуа расширения переставляет корни многочлена $p(x)$, т.е. решения уравнения (26), образующие множество из 3-х элементов. Таким образом, группа Галуа содержится в группе перестановок множества из 3-х элементов S_3, а, значит, разрешима.

Пример 4.10. Вычислить результат операций в непростом поле Галуа $L = Z_2[x] \big/ (x^2+x+1)Z_2[x]$ для выражения $q = x^{33}+1$.

Решение. Возьмем элемент $x \in L$. Имеем $x^2 = x^2+x+1-(x+1) = 0-x-1 = x+1 \in L$.

$x^3 = x(x+1) = x^2+x = x^2+x+1-1 = 0-1 = 1 \in L$

Далее $|L| = 2^2 = 4, |L^*| = |L \setminus \{0\}| = 3$, $\mathrm{Char}\, L = 2$, т.е. это непростое поле Галуа.

Отсюда

L^* – циклическая группа, которая порождается элементом x.

Имеем $L^* = \{x, x^2 = x+1, x^3 = 1\}$.

Тогда $x^{33} = (x^3)^{11} = 1$. Аналогично $x^{3n} = (x^3)^n = (1)^n = 1$.

Таким образом, если в каком-либо расчете возникает элемент x^{3n}, то его можно заменить на 1 и продолжить расчет.

В итоге получаем $q = x^{33}+1 = 1+1 = 0$.

Ч А С Т Ь V. КОНТРОЛЬНЫЕ ЗАДАНИЯ

Контрольная работа № 1

Разложить заданную подстановку в произведение транспозиций.

1. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 3\ 1\ 2\ 6\ 4\ 5 \end{pmatrix}$.
2. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 4\ 1\ 5\ 6\ 3\ 2 \end{pmatrix}$.
3. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 5\ 6\ 2\ 1\ 4\ 3 \end{pmatrix}$.
4. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 6\ 4\ 2\ 3\ 1\ 5 \end{pmatrix}$.
5. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 3\ 1\ 2\ 6\ 4\ 5 \end{pmatrix}$.
6. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 2\ 1\ 6\ 3\ 4\ 5 \end{pmatrix}$.
7. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 2\ 5\ 6\ 3\ 4\ 1 \end{pmatrix}$.
8. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 2\ 3\ 6\ 5\ 4\ 1 \end{pmatrix}$.
9. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 2\ 4\ 5\ 6\ 3\ 1 \end{pmatrix}$.
10. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 2\ 6\ 5\ 1\ 3\ 4 \end{pmatrix}$.
11. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 5\ 4\ 1\ 3\ 6\ 3 \end{pmatrix}$.
12. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 5\ 1\ 4\ 6\ 2\ 3 \end{pmatrix}$.
13. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 3\ 6\ 5\ 1\ 4\ 2 \end{pmatrix}$.
14. $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 3\ 4\ 6\ 2\ 1\ 5 \end{pmatrix}$.

15. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix}$.

16. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 5 & 3 & 2 \end{pmatrix}$.

17. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 1 & 5 \end{pmatrix}$.

18. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 6 & 2 \end{pmatrix}$.

19. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 6 & 2 & 3 \end{pmatrix}$.

20. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 6 & 1 \end{pmatrix}$.

Контрольная работа № 2

Найти при помощи алгоритма Евклида наибольший общий делитель (НОД) d элементов f,g в кольце многочленов над полем действительных чисел $R[x]$ и представить НОД в виде $d = pf+qg$:

1. $f(x)=x^5+1, g(x)=x^3-1$.
2. $f(x)=x^5-1, g(x)=x^3+1$.
3. $f(x)=x^4-16, g(x)=x^2-x-2$.
4. $f(x)=x^4+1, g(x)=x^2+1$.
5. $f(x)=x^5+x-2, g(x)=x^3+2x-3$.
6. $f(x)=x^5-3x-2, g(x)=x^3-5x+4$.
7. $f(x)=x^5+7x-8, g(x)=x^3-1$.
8. $f(x)=x^5-x^4+16, g(x)=x^3-2x-4$.
9. $f(x)=x^5+32, g(x)=x^3+8$.
10. $f(x)=x^7-2x^5+1, g(x)=x^5-1$.
11. $f(x)=x^5+x^2-x-1, g(x)=x^4-1$.
12. $f(x)=x^6-x-2, g(x)=x^5+1$.
13. $f(x)=x^5+243, g(x)=x^3+27$.

14. $f(x)=x^5-20x^2-63,\ g(x)=x^3-27$.
15. $f(x)=x^5-x^4-16, g(x)=x^3+x-10$.
16. $f(x)=x^5-17x^4+16, g(x)=x^3+7x-8$.
17. $f(x)=x^5-2x^4-51, g(x)=x^3-11x+6$.
18. $f(x)=x^5+2x^3-48, g(x)=x^3-17x+26$.
19. $f(x)=x^5-21x^4+20, g(x)=x^3-15x+14$.
20. $f(x)=x^5+2x^3+3, g(x)=x^3+7x+8$.

Контрольная работа № 3

1. Определить, является ли элемент 9 обратимым в кольце вычетов Z_{16} по модулю 16 и, если да, то найти обратный элемент.
2. Определить, является ли элемент 6 обратимым в кольце вычетов Z_{25} по модулю 25 и, если да, то найти обратный элемент.
3. Определить, является ли элемент 14 обратимым в кольце вычетов Z_{27} по модулю 27 и, если да, то найти обратный элемент.
4. Определить, является ли элемент 8 обратимым в кольце вычетов Z_{15} по модулю 15 и, если да, то найти обратный элемент.
5. Определить, является ли элемент 21 обратимым в кольце вычетов Z_{32} по модулю 32 и, если да, то найти обратный элемент.
6. Определить, является ли элемент 24 обратимым в кольце вычетов Z_{35} по модулю 35 и, если да, то найти обратный элемент.
7. Определить, является ли элемент 12 обратимым в кольце вычетов Z_{49} по модулю 49 и, если да, то найти обратный элемент.
8. Определить, является ли элемент 28 обратимым в кольце вычетов Z_{45} по модулю 45 и, если да, то найти обратный элемент.
9. Определить, является ли элемент 9 обратимым в кольце вычетов Z_{16} по модулю 16 и, если да, то найти обратный элемент.
10. Определить, является ли элемент 22 обратимым в кольце вычетов Z_{81} по модулю 81 и, если да, то найти обратный элемент.
11. Определить, ли элемент 15 обратимым в кольце вычетов Z_{46} по модулю 46 и, если да, то найти обратный элемент.
12. Определить, является ли элемент 15 обратимым в кольце вычетов Z_{16} по модулю 16 и, если да, то найти обратный элемент.

13. Определить, является ли элемент 58 обратимым в кольце вычетов Z_{63} по модулю 63 и, если да, то найти обратный элемент.
14. Определить, является ли элемент 39 обратимым в кольце вычетов Z_{34} по модулю 34 и, если да, то найти обратный элемент.
15. Определить, является ли элемент 64 обратимым в кольце вычетов Z_{65} по модулю 65 и, если да, то найти обратный элемент.
16. Определить, является ли элемент 49 обратимым в кольце вычетов Z_{125} по модулю 125 и, если да, то найти обратный элемент.
17. Определить, является ли элемент 48 обратимым в кольце вычетов Z_{55} по модулю 55 и, если да, то найти обратный элемент.
18. Определить, является ли элемент 69 обратимым в кольце вычетов Z_{74} по модулю 74 и, если да, то найти обратный элемент.
19. Определить, является ли элемент 68 обратимым в кольце вычетов Z_{93} по модулю 93 и, если да, то найти обратный элемент.
20. Определить, является ли элемент 75 обратимым в кольце вычетов Z_{82} по модулю 82 и, если да, то найти обратный элемент.

Контрольная работа № 4

Определить, являются ли неприводимыми элементами кольца R[x] многочленов с вещественными коэффициентами (т.е. неразложимиыми в произведение многочленов положительной степени) следующие многочлены $p(x)$?

1. $p(x)=x^2+x+1.$
2. $p(x)=x^2-x+1.$
3. $p(x)=x^2+2x+1.$
4. $p(x)=x^2+2x+2.$
5. $p(x)=x^2+x+10.$
6. $p(x)=x^3+x+1.$
7. $p(x)=x^4+1.$
8. $p(x)=x^2+7x+10.$
9. $p(x)=x^2+8x+64.$
10. $p(x)=x^3-x+10.$

11. $p(x)=x^4+x^2+1.$
12. $p(x)=x^2+10x+100.$
13. $p(x)=x^2+3x+9.$
14. $p(x)=x^2+12x+144.$
15. $p(x)=x^2-2x+2.$
16. $p(x)=x^4+2x^2+4.$
17. $p(x)=x^2-12x+40.$
18. $p(x)=x^2-10x+24.$
19. $p(x)=x^3-23x+132.$
20. $p(x)=x^2+30x+226.$

Контрольная работа № 5

1. Определить, является ли многочлен $p(x)=x^3+x+1$ неприводимым в кольце многочленов $Z_2[x]$ над полем Z_2 .
2. Определить, является ли многочлен $p(x)=x^3+2x+1$ неприводимым в кольце многочленов $Z_3[x]$ над полем Z_3 .
3. Определить, является ли многочлен $p(x)=x^3+3$ неприводимым в кольце многочленов $Z_5[x]$ над полем Z_5 .
4. Определить, является ли многочлен $p(x)=x^3+5$ неприводимым в кольце многочленов $Z_7[x]$ над полем Z_7 .
5. Определить, является ли многочлен $p(x)=x^3+x+4$ неприводимым в кольце многочленов $Z_5[x]$ над полем Z_5 .
6. Определить, является ли многочлен $p(x)=x^3+2x+3$ неприводимым в кольце многочленов $Z_5[x]$ над полем Z_5 .
7. Определить, является ли многочлен $p(x)=x^3+x+3$ неприводимым в кольце многочленов $Z_7[x]$ над полем Z_7 .
8. Определить, является ли многочлен $p(x)=x^3+6x+1$ неприводимым в кольце многочленов $Z_7[x]$ над полем Z_7 .

9. Определить, является ли многочлен $p(x)=x^3+4x+6$ неприводимым в кольце многочленов $Z_7[x]$ над полем Z_7 .
10. Определить, является ли многочлен $p(x)=x^3+x+1$ неприводимым в кольце многочленов $Z_7[x]$ над полем Z_7 .
11. Определить, является ли многочлен $p(x)=x^3+4x+1$ неприводимым в кольце многочленов $Z_5[x]$ над полем Z_5 .
12. Определить, является ли многочлен $p(x)=x^3+3x+3$ неприводимым в кольце многочленов $Z_5[x]$ над полем Z_5 .
13. Определить, является ли многочлен $p(x)=x^3+2$ неприводимым в кольце многочленов $Z_{11}[x]$ над полем Z_{11} .
14. Определить, является ли многочлен $p(x)=x^3+x+7$ неприводимым в кольце многочленов $Z_{11}[x]$ над полем Z_{11} .
15. Определить, является ли многочлен $p(x)=x^3+9$ неприводимым в кольце многочленов $Z_{11}[x]$ над полем Z_{11} .
16. Определить, является ли многочлен $p(x)=x^3+2x+3$ неприводимым в кольце многочленов $Z_{11}[x]$ над полем Z_{11} .
17. Определить, является ли многочлен $p(x)=x^3+5x+2$ неприводимым в кольце многочленов $Z_7[x]$ над полем Z_7 .
18. Определить, является ли многочлен $p(x)=x^3+4x^2+6$ неприводимым в кольце многочленов $Z_7[x]$ над полем Z_7 .
19. Определить, является ли многочлен $p(x)=x^3+6x^2+5$ неприводимым в кольце многочленов $Z_7[x]$ над полем Z_7 .
20. Определить, является ли многочлен $p(x)=x^3+x^2+4$ неприводимым в кольце многочленов $Z_5[x]$ над полем Z_5 .

Контрольная работа № 6

Разложить на простые множители элемент w кольца целых гауссовых чисел.

1. $w=-2i$.
2. $w=13i$.
3. $w=5i$.

4. $w=-2i$.
5. $w=-8$.
6. $w=3+i$.
7. $w=-1-3i$.
8. $w=-29$.
9. $w=5+i$.
10. $w=-1-5i$.
11. $w=-6i$.
12. $w=14i$.
13. $w=-94i$.
14. $w=62i$.
15. $w=-46i$.
16. $w=3+12i$.
17. $w=7-28i$.
18. $w=11-11i$.
19. $w=37+37i$.
20. $w=-82i$.

Контрольная работа № 7

1. Определить порядок элемента 8 в мультипликативной группе поля $\mathbf{Z}_{11}$ вычетов по модулю 11.
2. Определить порядок элемента 7 в мультипликативной группе поля $\mathbf{Z}_{13}$ вычетов по модулю 13.
3. Определить порядок элемента 5 в мультипликативной группе поля $\mathbf{Z}_{7}$ вычетов по модулю 7.
4. Определить порядок элемента 9 в мультипликативной группе поля $\mathbf{Z}_{11}$ вычетов по модулю 11.
5. Определить порядок элемента 11 в мультипликативной группе поля $\mathbf{Z}_{13}$ вычетов по модулю 13.
6. Определить порядок элемента 6 в мультипликативной группе поля $\mathbf{Z}_{17}$ вычетов по модулю 17.
7. Определить порядок элемента 2 в мультипликативной группе поля $\mathbf{Z}_{23}$ вычетов по модулю 23.

8. Определить порядок элемента 4 в мультипликативной группе поля $\mathbf{Z}_{19}$ вычетов по модулю 19.
9. Определить порядок элемента 5 в мультипликативной группе поля $\mathbf{Z}_{13}$ вычетов по модулю 13.
10. Определить порядок элемента 8 в мультипликативной группе поля $\mathbf{Z}_{19}$ вычетов по модулю 7.
11. Определить порядок элемента 2 в мультипликативной группе поля $\mathbf{Z}_{31}$ вычетов по модулю 31.
12. Определить порядок элемента 10 в мультипликативной группе поля $\mathbf{Z}_{11}$ вычетов по модулю 11.
13. Определить порядок элемента 2 в мультипликативной группе поля $\mathbf{Z}_{37}$ вычетов по модулю 37.
14. Определить порядок элемента 4 в мультипликативной группе поля $\mathbf{Z}_{41}$ вычетов по модулю 41.
15. Определить порядок элемента 3 в мультипликативной группе поля $\mathbf{Z}_{31}$ вычетов по модулю 31.
16. Определить порядок элемента 10 в мультипликативной группе поля $\mathbf{Z}_{17}$ вычетов по модулю 17.
17. Определить порядок элемента 12 в мультипликативной группе поля $\mathbf{Z}_{13}$ вычетов по модулю 13.
18. Определить порядок элемента 4 в мультипликативной группе поля $\mathbf{Z}_{23}$ вычетов по модулю 23.
19. Определить порядок элемента 3 в мультипликативной группе поля $\mathbf{Z}_{19}$ вычетов по модулю 19.
20. Определить порядок элемента 16 в мультипликативной группе поля $\mathbf{Z}_{17}$ вычетов по модулю 17.

Контрольная работа № 8

1. Имеются ли делители нуля в кольце матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ с вещественным a с операциями матричного сложения и умножения.
2. Имеются ли делители нуля в кольце многочленов от 2-х переменных $R[\boldsymbol{x},\boldsymbol{y}]$ с вещественными коэффициентами.
3. Найти факторкольцо кольца многочленов от 1-й переменной $R[\boldsymbol{x}]$ с вещественными коэффициентами по главному идеалу многочленов, порожденному $(\boldsymbol{x})$.

4. Можно ли разложить на неприводимые множители элемент 2 в кольце целых гауссовых чисел.
5. Можно ли разложить на неприводимые множители элемент 5 в кольце целых гауссовых чисел.
6. Можно ли разложить на неприводимые множители элемент 7 в кольце целых гауссовых чисел.
7. Приведите примеры делителей нуля в кольце ограниченных функций на отрезке [0,1].
8. Найти факторкольцо кольца целых гауссовых чисел по главному идеалу, порожденному элементом 2 .
9. Описать групповую операцию в мультипликативной группе кольца Z_8 вычетов по модулю 8.
10. Какую алгебраическую структуру образуют матрицы вида $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, где a,b – вещественные числа, с операциями матричного сложения и умножения.
11. Вычислить коммутатор матриц $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ и в группе обратимых вещественных матриц 2-го порядка GL(2,R).
12. Вычислить коммутатор матриц $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ и $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ в группе обратимых вещественных матриц 2-го порядка GL(2,R).
13. Найти собственную подгруппу H в группе G_4 корней 4-й степени из единицы над полем комплексных чисел.
14. Найти собственную подгруппу H в группе G_9 корней 9-й степени из единицы над полем комплексных чисел.
15. Какую алгебраическую структуру образует множество $N[x]$ многочленов с натуральными коэффициентами с операцией умножения многочленов.
16. Найти индекс подгруппы $H=\{1,-1, i, -i\}$ в группе G_{12} корней 12-й степени из 1 над полем комплексных чисел .
17. Какие подгруппы имеются в группе G_{41} корней 41-й степени из 1 над полем комплексных чисел.

18. Образуют ли кольцо множество чисел вида $a + b\sqrt{2}$, где a,b – четные целые числа.
19. Найти собственную подгруппу H в группе G_{10} корней 10-й степени из единицы над полем комплексных чисел.
20. Описать групповую операцию в группе G_8 корней 8-й степени из единицы над полем комплексных чисел.

Контрольная работа № 9

Вычислить результат операций в непростом поле Галуа $L = Z_2[x] / (x^2 + x + 1) Z_2[x]$.

1. $q = x^{34} + x \in L.$
2. $q = x^{99} + 1 \in L.$
3. $q = x^{100} + x \in L.$
4. $q = x^{35} + x + 1 \in L.$
5. $q = x^{35} + x \in L.$
6. $q = x^{60} + 1 \in L.$
7. $q = x^{35} + x^{10} + 1 \in L.$
8. $q = x^{66} + x^{33} \in L.$
9. $q = x^{99} + x^{66} \in L.$
10. $q = x^{28} + 1 \in L.$
11. $q = x^{45} + 1 \in L.$
12. $q = x^{31} + 1 \in L.$
13. $q = x^{32} + x^{31} + 1 \in L.$
14. $q = x^{61} + 1 \in L.$
15. $q = x^{61} + x^{30} \in L.$
16. $q = x^{90} + 1 \in L.$
17. $q = x^{330} + x \in L.$
18. $q = x^{121} + x \in L.$

19. $q = x^{35} + x^{34} + x^{33} \in L.$

20. $q = x^{99} + x^{33} + x^{9} \in L.$

Контрольная работа № 10

1. Найти группу обратимых элементов в кольце матриц вида $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ с операциями матричного сложения и умножения, где a,b целые.
2. Может ли матрица $\begin{pmatrix} 1 & 9 \\ 1 & 8 \end{pmatrix}$ принадлежать коммутанту группы обратимых вещественных матриц 2-го порядка GL(2,R).
3. Показать, что множество матриц $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, где a – вещественное число, с операцией матричного умножения образует группу, изоморфную аддитивной группе вещественных чисел.
4. Какую алгебраическую структуру образуют матрицы с операцией матричного умножения вида $\begin{pmatrix} k & 0 \\ m & n \end{pmatrix}$ с операциями матричного сложения и умножения, где k,n,m –целые числа.
5. Какую алгебраическую структуру образуют матрицы вида $\begin{pmatrix} k & l \\ m & n \end{pmatrix}$ с операциями матричного сложения и умножения, где k,l,n,m- четные целые числа.
6. Какие порядки имеют элементы в группе G_{32} корней 32-й степени из 1 над полем комплексных чисел.
7. Какие порядки имеют элементы в группе G_{37} корней 37-й степени из 1 над полем комплексных чисел.
8. Описать смежные классы подгруппы $H=\{1,-1\}$ в группе G_4 корней 4-й степени из 1 над полем комплексных чисел .
9. Описать смежные классы подгруппы $H=\{1,-1\}$ в группе G_6 корней 6-й степени из 1 над полем комплексных чисел .
10. Найти группу обратимых элементов в кольце многочленов $Z[x]$ с целыми коэффициентами.
11. Образуют ли поле множество чисел вида $a+bi$, где a,b – рациональные числа.

12. Какую структуру образуют матрицы с вида $\begin{pmatrix} 0 & k & l \\ 0 & 0 & m \\ 0 & 0 & 0 \end{pmatrix}$, где k, l, m целые числа, с операциями матричного сложения и умножения.

13. Показать, что в кольце диференцируемых функций на прямой $Diff(\mathrm{R})$ подмножество

$Diff_0(\mathrm{R}) = \{f \in Diff\ (\mathrm{R}), f(0) = 0, f'(0) = 0\}$

образует идеал.

14. Найти факторкольцо кольца многочленов от 1-й переменной $\mathrm{R}[\boldsymbol{x}]$ с вещественными коэффициентами по главному идеалу $(\boldsymbol{x})$.

15. Можно ли разложить на неприводимые множители элемент 11 в кольце целых гауссовых чисел.

16. Можно ли разложить на неприводимые множители элемент 23 в кольце целых гауссовых чисел.

17. Можно ли разложить на неприводимые множители элемент 17 в кольце целых гауссовых чисел.

18. Приведите примеры делителей нуля в кольце дифференцируемых функций на отрезке [0,1].

19. Показать, что матрицы вида $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ с операциями матричного сложения и умножения, где a, b – вещественные числа, образуют структуру, изоморфную полю комплексных чисел.

20. Показать, что множество матриц $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, где λ – ненулевое вещественное число, с операцией матричного умножения образует группу, изоморфную мультипликативной группе вещественных чисел.

Контрольная работа № 11

Для заданных полей K, L $K \subset L$ определить, является ли поле L конечным расширением поля K.

1. $K = \mathrm{R}, -$ поле вещественных чисел, $L = \mathrm{C}, -$ поле комплексных чисел.
2. $K = \mathrm{Q}, -$ поле рациональных чисел, $L = \mathrm{R}, -$ поле вещественных чисел.

3. $K=\mathrm{Q},-$ поле рациональных чисел, $L=\mathrm{C},-$ поле комплексных чисел.
4. $K=\mathrm{Q},-$ поле рациональных чисел, $L=\{p+q\sqrt{2}\mid p,q\in\mathrm{Q}\text{ - рациональные числа}\},-$ поле квадратично иррациональных чисел с иррациональным основанием $\sqrt{2}$.
5. $K=\mathrm{Z}_2,-$ поле вычетов по модулю 2, $L=\mathrm{Z}_2[x]\big/(x^2+x+1)\mathrm{Z}_2[x],-$ фактор кольца многочленов с коэффициентами из Z_2 по идеалу, порожденному неприводимым многочленом (x^2+x+1) .
6. $K=\mathrm{Q},-$ поле рациональных чисел, $L=\{p+q\sqrt{3}\mid p,q\in\mathrm{Q}\text{ - рациональные числа}\},-$ поле квадратично иррациональных чисел с иррациональным основанием $\sqrt{3}$.
7. $K=\mathrm{Q},-$ поле рациональных чисел, $L=\{p+q\mathrm{i}\mid p,q\in\mathrm{Q}\text{ - рациональные числа}\}-$ поле комплексных чисел с рациональными вещественной и мнимой частями.
8. $K=\mathrm{Q},-$ поле рациональных чисел, $L=\{p+q\sqrt{5}\mid p,q\in\mathrm{Q}\text{ - рациональные числа}\},-$ поле квадратично иррациональных чисел с иррациональным основанием $\sqrt{5}$.
9. $K=\mathrm{Z}_2,-$ поле вычетов по модулю 2, $L=\mathrm{Z}_2[x]\big/(x^3+x+1)\mathrm{Z}_2[x],-$ фактор кольца многочленов с коэффициентами из Z_2 по идеалу, порожденному неприводимым многочленом (x^3+x+1) .
10. $K=\mathrm{Q},-$ поле рациональных чисел, $L=\{p+q\sqrt{7}\mid p,q\in\mathrm{Q}\text{ - рациональные числа}\},-$ поле квадратично иррациональных чисел с иррациональным основанием $\sqrt{7}$.
11. $K=\mathrm{Z}_3,-$ поле вычетов по модулю 2, $L=\mathrm{Z}_3[x]\big/(x^2+x+2)\mathrm{Z}_3[x],-$ фактор кольца многочленов с коэффициентами из Z_3 по идеалу, порожденному неприводимым многочленом (x^2+x+2) .

12. $K = \mathrm{Q}$, – поле рациональных чисел, $L = \{p + q\sqrt{11} \mid p, q \in \mathrm{Q}$ - рациональные числа$\}$, – поле квадратично иррациональных чисел с иррациональным основанием $\sqrt{11}$.

13. $K = \mathrm{Z}_3$, – поле вычетов по модулю 2, $L = {}^{\mathrm{Z}_3[x]}\!/_{(x^3+2x+2)\mathrm{Z}_3[x]}$, – фактор кольца многочленов с коэффициентами из Z_3 по идеалу, порожденному неприводимым многочленом (x^2+2x+2) .

14. $K = \mathrm{Q}$, – поле рациональных чисел, $L = \{p + q\sqrt{17} \mid p, q \in \mathrm{Q}$ - рациональные числа$\}$, – поле квадратично иррациональных чисел с иррациональным основанием $\sqrt{17}$.

15. $K = \mathrm{Q}$, – поле рациональных чисел, $L = \{p + q\sqrt{19} \mid p, q \in \mathrm{Q}$ - рациональные числа$\}$, – поле квадратично иррациональных чисел с иррациональным основанием $\sqrt{19}$.

16. $K = \mathrm{Q}$, – поле рациональных чисел, $L = \{p + q\sqrt{23} \mid p, q \in \mathrm{Q}$ - рациональные числа$\}$, – поле квадратично иррациональных чисел с иррациональным основанием $\sqrt{23}$.

17. $K = \mathrm{Q}$, – поле рациональных чисел, $L = \{p + qi \mid p,\ q \in \mathrm{Q}\}$ поле комплексно-рациональных чисел.

18. $K = \mathrm{Q}$, – поле рациональных чисел, $L = \{p + q\sqrt{101} \mid p, q \in \mathrm{Q}$ - рациональные числа$\}$, – поле квадратично иррациональных чисел с иррациональным основанием $\sqrt{101}$.

19. $K = \mathrm{Z}_{11}$, – поле вычетов по модулю 11, $L = {}^{\mathrm{Z}_{11}[x]}\!/_{(x^2+9)\mathrm{Z}_{11}[x]}$, – фактор кольца многочленов с коэффициентами из Z_{11} по идеалу, порожденному неприводимым многочленом (x^2+9) .

20. $K = \mathrm{Q}, -$ поле рациональных

чисел, $L = \{p + q\sqrt{43} \mid p, q \in \mathrm{Q} \text{ - рациональные числа}\}, -$ поле квадратично

иррациональных чисел с иррациональным основанием $\sqrt{43}$.

Контрольная работа № 12

Определить, к какому типу относится заданный гомоморфизм групп $T: G \to H$.

Гомоморфизм;
мономорфизм(ядро тривиальное Ker T = {1});
эпиморфизм(образ вся группа H Im T = H);
изоморфизм (Ker T = {1} и Im T = H)).

1. G=R_+* мультипликативная группа положительных вещественных чисел, H=R аддитивная группа вещественных чисел , $T(x) = \ln x$.
2. G=H=Z аддитивная группа целых чисел, $T(n) = -n$.
3. G=H=Z аддитивная группа целых чисел, $T(n) = 5n$.
4. G=Z аддитивная группа целых чисел,
   H=Z_2 аддитивная группа остатков от деления на 2 целых чисел,
   $T(n) = n \mod 2$ остаток от деления n на 2.
5. G=Z аддитивная группа целых чисел,
   H=Z_4 аддитивная группа остатков от деления на 4 целых чисел,
   $T(n) = n \mod 4$ остаток от деления n на 4.
6. G=H=R аддитивная группа вещественных чисел, $T(x) = 4x$.
7. G=H=R аддитивная группа вещественных чисел, $T(x) = -x$.
8. G=H=R аддитивная группа вещественных чисел, $T(x) = 2x$.
9. G=R* мультипликативная группа ненулевых вещественных чисел,
   H=R_+* мультипликативная группа положительных вещественных чисел
   $T(x) = |x|$.
10. G=H=R* мультипликативная группа ненулевых вещественных чисел,
    $T(x) = \frac{1}{x}$.

11. $G=H=\mathrm{R}_+^*$ мультипликативная группа положительных вещественных чисел, $T(x)=\sqrt{x}$.

12. $G=\mathrm{R}$ мультипликативная группа вещественных чисел, $H=\mathrm{R}_+^*$ мультипликативная группа положительных вещественных чисел , $T(x)=x^2$.

13. $G=H=\mathrm{R}^*$ мультипликативная группа ненулевых вещественных чисел, $T(x)=\sqrt[3]{x}$.

14. $G=\mathrm{R}^*$ мультипликативная группа ненулевых вещественных чисел, $H=\mathrm{R}_+^*$ мультипликативная группа положительных вещественных чисел, $T(x)=\dfrac{1}{x^2}$.

15. $G=\mathrm{R}^*$ мультипликативная группа ненулевых вещественных чисел, $H=\mathrm{R}_+^*$ мультипликативная группа положительных вещественных чисел, $T(x)=\dfrac{1}{|x|}$.

16. $G=\mathrm{R}^*$ мультипликативная группа ненулевых вещественных чисел, $H=\mathrm{R}_+^*$ мультипликативная группа положительных вещественных чисел, $T(x)=|x|^3$.

17. $G=\mathrm{C}^*$ мультипликативная группа ненулевых комплексных чисел, $H=\mathrm{R}_+^*$ мультипликативная группа положительных вещественных чисел, $T(z)=|z|$.

18. $G=\mathrm{C}$ аддитивная группа комплексных чисел, $H=\mathrm{C}$ аддитивная группа комплексных чисел, $T(z)=\bar{z}$ (комплексное сопряжение).

19. $G=\{1,-1,i,-i\}$ мультипликативная группа из 4-х комплексных чисел, $H=\{1,-1\}$ мультипликативная группа из 2-х вещественных чисел, $T(z)=z^2$.

20. $G=\mathrm{Z}_2$ аддитивная группа остатков от деления на 2 целых чисел, $H=\mathrm{Z}_2$ аддитивная группа остатков от деления на 2 целых чисел, $T(n)=n^2$.

БИБЛИОГРАФИЧЕКИЙ СПИСОК

а) основная литература:

1. Ерзакова Н.А.Дополнительные главы алгебры.– тексты лекций. – М.: МГТУ ГА, 2014.
2. Ван дер Ванден Б.Л. Алгебра. – М.: Наука, 1979.
3. Сборник задач по алгебре / под ред. АИ. Кострикина. – М.: Изд-во физ.-мат. литературы, 2001.

б) дополнительная литература:

1. Кострикин А.И. Введение в алгебру. Часть I. Основы алгебры: М. Физматлит, 2001.