Казанский государственный университет

С.Н. Тронин

ВВЕДЕНИЕ В УНИВЕРСАЛЬНУЮ И КАТЕГОРНУЮ АЛГЕБРУ

Часть I

КАЗАНЬ – 2002

Научный редактор:
д. ф.-м. н., проф. М.М. Арсланов

СОДЕРЖАНИЕ

Введение

Данное учебно-методическое пособие представляет собой первую из четырех запланированных частей, предназначенных для ознакомления студентов третьего-пятого курсов механико-математического факультета с одним из направлений современной алгебры (мы называем "универсальной и категорной алгеброй"), где изучаются самые общие и основные алгебраические структуры, частными случаями которых являются группы, кольца, модули и т.п. Первая часть (под названием "Классическая алгебра") имеет, в основном, справочный характер. Материал по группам, кольцам , полям и (отчасти) модулям приводится в пособии с целью повторения, так как во втором семестре второго курса алгебра на мехмате не читается, и к третьему курсу кое-что наверняка забудется. Даны точные определения, формулировки важнейших теорем и основные примеры описываемых алгебраических объектов. Доказательства в большинстве случаев отсутствуют, или приводится основная идея построения или рассуждения. Оправданием этому служит то, что практически все подробности можно найти в приводимом в конце пособия списке литературы. Материал разбросан по множеству разных (и довольно толстых) книг, так что данное пособие предназначено в основном для того, чтобы избавить студентов от чрезмерно большой работы по отысканию необходимого среди массы необязательного.

Вторая часть пособия будет посвящена универсальной алгебре, тождествам и многообразиям, теореме Биркгофа, простейшим понятиям теории категорий и функторов. Часть третья — более детальному введению в теорию категорий. Четвертая часть будет посвящена алгебраической теории операд.

ЧАСТЬ I. КЛАССИЧЕСКАЯ АЛГЕБРА

1. Полугруппы.

Определение 1.1. Полугруппа P есть множество вместе с заданной на нем бинарной операцией , то есть отображением

$$P \times P \longrightarrow P \quad , \quad (x, y) \mapsto xy,$$

(результат применения которого часто называется "умножением"), причем должно быть выполнено следующее тождество ассоциативности: для любых $x, y, z \in P$ имеет место равенство $(xy)z = x(yz)$. Полугруппа называется коммутативной, если для всех $x, y \in P$ имеет место равенство $xy = yx$. Элемент $e \in P$ называется нейтральным элементом полугруппы, если для любого $x \in P$ имеют место равенства $xe = ex = x$. Нейтральный элемент часто называют единицей полугруппы и используют для него соответствующее обозначение: $e = 1$. Полугруппа с единицей называется также моноидом. Легко убедиться, что в полугруппе может быть не более одного нейтрального элемента.

Результат бинарной операции $P \times P \longrightarrow P$, вообще говоря, можно обозначать самым произвольным образом. Запись в виде $(x, y) \mapsto xy$ называют мультипликативной. Кроме нее, часто используется так называемая аддитивная запись $(x, y) \mapsto x + y$ (операция "сложения"), для которой тождество ассоциативности выглядит так : $(x + y) + z = x + (y + z)$, а нейтральный элемент называется нулем, и обозначается соответственно как 0. Чаще всего аддитивные обозначения используются для коммутативных полугрупп, то есть когда $x+y = y+x$. Далее в тексте многие определения и факты формулируются только в мультипликативной записи. Подразумевается, что в случае необходимости читатель сможет сам перейти к другой форме обозначений.

Определение 1.2. Гомоморфизм h из полугруппы P в полугруппу Q — это отображение $h : P \longrightarrow Q$, такое, что для любых $x, y \in P$ имеет место равенство $h(xy) = h(x)h(y)$. Гомоморфизм полугрупп с единицами должен дополнительно удовлетворять условию $h(e) = e$ (или $h(1) = 1$). Если из контекста не будет ясно, к какой полугруппе принадлежит тот или иной нейтральный элемент,то надо использовать обозначения вида 1_P для нейтрального элемента P, и т.п. Таким образом, для гомоморфизма полугрупп с единицей $h(1_P) = 1_Q$.

Если даны два гомоморфизма полугрупп $h : P \to Q$, $f : Q \to W$, то их композиция $fh : P \to W$, определяемая как $(fh)(x) = f(h(x))$, также является гомоморфизмом полугрупп. Тождественное отображение из P в P есть гомоморфизм полугрупп.

Определение 1.3. Подполугруппой P' полугруппы P называется такое подмножество $P' \subseteq P$, для которого из $x, y \in P'$ следует $xy \in P'$. Когда речь идет о подполугруппе полугруппы с единицей, дополнительно предполагается, что $1_P \in P'$, и это — единица полугруппы P'.

Это определение означает, что , если взять ограничение бинарной операции для P на $P' \times P' \subseteq P \times P$, то его можно рассматривать как отображение в P', и относительно этой бинарной операции множество P' само становится полугруппой, причем отображение включения $P' \subseteq P$ есть гомоморфизм полугрупп.

Пусть $h : P \longrightarrow Q$ — гомоморфизм полугрупп. Тогда множество $h(P) = \{\ h(x) \mid x \in P\ \} \subseteq Q$ является подполугруппой полугруппы Q, называемой образом гомоморфизма h. Гомоморфизм h можно представить в виде композиции сюръективного гомоморфизма $P \to h(P)$ и инъективного гомоморфизма (вложения) $h(P) \subseteq Q$.

Нетрудно убедиться, что пересечение любого семейства подполугрупп

снова является подполугруппой.

Пусть X есть подмножество полугруппы P. Существует наименьшая подполугруппа P, содержащая X. Она обозначается через $\langle X \rangle$, и называется подполугруппой, порожденной множеством X. Если же $P' = \langle X \rangle$, то говорят, что X есть множество образующих для P'. Слово "наименьшая" означает, что если $P' \subseteq P$ — подполугруппа, и $X \subseteq P$, то $\langle X \rangle \subseteq P'$. В качестве $\langle X \rangle$ можно взять пересечение непустого семейства всех подполугрупп, содержащих X. Непусто оно потому, что содержит саму P. Более явное построение таково: $\langle X \rangle = \{ x_1 x_2 \dots x_n \mid x_i \in X, 1 \leq i \leq n, n \geq 0 \}$. При $n = 0$ соответствующий элемент есть единица полугруппы P. Таким образом, множество $\langle X \rangle$ состоит из всевозможных произведений компонентов всевозможных конечных (упорядоченных) последовательностей элементов из X. Иногда о них говорят (несколько отклоняясь от строгости) как о словах в алфавите X (см. ниже пример 2.).

Пусть дано произвольное семейство полугрупп $\{ P_i \mid i \in I \}$. Их прямое (или декартово) произведение , обозначаемое $\prod\limits_{i \in I} P_i$, строится следующим образом: это множество семейств элементов $\{ x_i \mid i \in I, x_i \in P_i \}$ (точнее, множество всех функций вида $\varphi : I \to \bigcup\limits_{i \in I} P_i$, таких, что $x_i = \varphi(i) \in P_i$. Произведение семейств $\{ x_i \mid i \in I, x_i \in P_i \}$ и $\{ y_i \mid i \in I, y_i \in P_i \}$ определяется "покомпонентно" — как семейство $\{ x_i y_i \mid i \in I \}$. Семейство единиц всех полугрупп семейства $\{ 1_{P_i} \mid i \in I \}$ есть единица прямого произведения. Отображения проекции

$$\pi_j : \prod_{i \in I} P_i \longrightarrow P_j \quad , \quad \{ x_i \mid i \in I, x_i \in P_i \} \mapsto x_j = \pi_j(\{x_i\})$$

являются гомоморфизмами полугрупп. Если множество $I = \{ 1, 2, \dots, n \}$ конечно, то произведение обозначается так: $P_1 \times P_2 \dots \times P_n$.

Пример 1.1 . Рассмотрим любое множество X, и пусть P есть

множество всех отображений из X в X. Определим на P бинарную операцию как взятие композиции отображений. Точнее, если $f_1, f_2 \in P$, то результат умножения $f_1 f_2$ есть композиция отображений $X \xrightarrow{f_2} X \xrightarrow{f_1} X$. Так как композиция отображений ассоциативна, то P превращается в полугруппу, единицей которой является тождественное отображение 1_X. Если множество X само является полугруппой,то точно таким же образом превращается в полугруппу множество всех гомоморфизмов из X в X.

Пример 1.2. Свободная ассоциативная полугруппа $FP(X)$ с базисом X строится следующим образом. Множество $FP(X)$ есть множество всевозможных конечных последовательностей вида $(x_1, x_2, \ldots, x_n)$, $x_i \in X$, $1 \leq i \leq n$, $n \geq 0$. "Умножение" двух таких последовательностей $a = (x_1, x_2, \ldots, x_n)$ и $b = (y_1, y_2, \ldots, y_m)$ есть приписывание их друг к другу : $ab = (x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$. Ясно, что эта операция ассоциативна. Роль нейтрального элемента (единицы) играет вводимая формально последовательность нулевой длины (пустая), приписывание которой слева или справа к любой другой ничего не меняет. Более традиционная форма записи: $(x_1, x_2, \ldots, x_n) = x_1 x_2 \ldots x_n$, что можно назвать строкой, или словом в алфавите X. Достаточно распространено обозначение $FP(X) = X^*$: множество всех слов в алфавите X. Основное свойство свободных полугрупп: если дано отображение $\varphi : X \to P$ множества X в полугруппу P, то существует, притом только один, гомоморфизм полугрупп $f : FP(X) \to P$, такой, что $f(x) = \varphi(x)$ для всех $x \in X$. Здесь подразумевается, что элементы $x \in X$ являются также и элементами $FP(X)$, как последовательности длины 1. Явный вид гомоморфизма f : $f(x_1 x_2 \ldots x_n) = \varphi(x_1)\varphi(x_2)\ldots\varphi(x_n)$, $f(1) = 1$ по построению. Элементы $FP(X)$ можно мыслить себе как некоммутативные одночлены (мономы) от некоммутирующих переменных из

множества X .

Пример 1.3 . Множество коммутативных мономов (одночленов) от коммутирующих переменных из множества X также образуют полугруппу, которая будет обозначаться $FCP(X)$, и называется свободной коммутативной полугруппой с базисом X . Эта полугруппа коммутативна, но для нее используется мультипликативная запись операции умножения. Основное свойство свободных коммутативных полугрупп: если дано отображение $\varphi : X \to P$ множества X в коммутативную полугруппу P , то существует, притом только один, гомоморфизм полугрупп $f : FCP(X) \to P$, такой, что $f(x) = \varphi(x)$ для всех $x \in X$. Явный вид гомоморфизма f : $f(x_1x_2 \dots x_n) = \varphi(x_1)\varphi(x_2) \dots \varphi(x_n)$, $f(1) = 1$ по построению.

2. Группы.

Определение 2.1. Группа G — это полугруппа с единицей, в которой для каждого $x \in G$ существует (единственный) $y \in G$, такой, что $xy = yx = 1$. Элемент y называется обратным к элементу x , и обозначается x^{-1} . В аддитивной записи обратный элемент обозначается как $-x$, при этом используется также обозначение: $a - b = a + (-b)$. Коммутативные группы часто называются абелевыми. В абелевых группах чаще всего используется аддитивная форма записи операции.

Отметим, что $(x^{-1})^{-1} = x, (xy)^{-1} = y^{-1}x^{-1}$.

Определения, данные выше для полугрупп, превращаются в определения для групп после добавления свойств, связанных с взятием обратных элементов. Так, гомоморфизм групп $h : G \to D$ есть гомоморфизм полугрупп с единицей, такой, что $h(x^{-1}) = h(x)^{-1}$. Заметим, впрочем, что это свойство можно вывести, используя определение группы. Подгруппа G' группы G — это такая подполугруппа, что если $x \in G'$,

то и $x^{-1} \in G'$, так что вложение $G' \subseteq G$ есть гомоморфизм групп. Произведение групп $\prod\limits_{i \in I} G_i$ — это произведение полугрупп, в котором определена операция взятия обратного элемента : $\{ x_i \mid i \in I \}^{-1} = \{ x_i^{-1} \mid i \in I \}$, которая превращает это множество в группу.

Если X есть подмножество группы G, то подгруппа $\langle X \rangle$, порожденная X, есть наименьшая подгруппа в G, содержащая X. Явное построение таково:

$$\langle X \rangle = \{ x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_n}^{\varepsilon_n} \mid x_{i_k} \in X, \varepsilon_k = \pm 1, n \geq 0, 1 \leq k \leq n \}.$$

Как обычно, если $\langle X \rangle = G$, то говорят, что X порождает G, или что X есть множество образующих группы G.

Пример 2.1 . Циклические группы — это группы, у которых существует множество образующих, состоящее из одного элемента. Если $G = \langle x \rangle$, то $G = \{ x^n \mid n = 0, \pm 1, \pm 2, \dots \}$. Возможны два случая. Либо $G \cong \mathbf{Z}$, где $\mathbf{Z}$ — группа всех целых чисел с операцией сложения (аддитивная форма записи). При этом элементу x^n соответствует целое число n. В этом случае G называется бесконечной циклической группой. В ней $x^k = x^m$ тогда и только тогда, если $k = m$. Либо, если циклическая группа конечна и состоит из n элементов, $G \cong \mathbf{U}_n$, где $\mathbf{U}_n = \{ z \in \mathbf{C} \mid z^n = 1 \}$ — группа корней n-й степени из единицы. При этом x соответствует какому-то первообразному корню из единицы. Каждая подгруппа циклической группы — снова циклическая группа.

Пример 2.2 . Симметрическая группа n-й степени S_n (или группа подстановок n-й степени) — это множество всех биективных отображений из множества $[n] = \{ 1, 2, \dots, n \}$ в это же множество. Если $\sigma : [n] \to [n]$, $\sigma \in S_n$, то "табличная" форма записи σ есть $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$. Умножение подстановок — это композиция функций (которая ассоциативна): $(\sigma\tau)(i) = \sigma(\tau(i))$. Обратная подстановка — это обратное к биективному отображению. Единица группы S_n —

это подстановка $\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$, то есть единичная функция. В группе S_n содержится $n!$ элементов.

Пример 2.3. Группа всех обратимых $n \times n$-матриц над кольцом R обозначается через $GL_n(R)$ (или $GL(n, R)$) и называется общей линейной группой степени n над кольцом R. Существует инъективный гомоморфизм $m : S_n \to GL_n(\mathbf{Z})$, который строится следующим образом. Обозначим через E_{ij} матричную единицу n-го порядка, то есть матрицу, у которой ij-я компонента равна единице, а все остальные — нулю. Тогда $E_{ij}E_{kl} = \delta_{jk}E_{il}$, $\sum\limits_{i=1}^{n} E_{ii} = E_n$,где E_n — единичная $n \times n$-матрица. Положим

$$m(\sigma) = \sum_{j=1}^{n} E_{\sigma(j)\, j}.$$

Тогда m — инъективный гомоморфизм групп. Матрица $m(\sigma)$ называется матрицей подстановки σ.

Пусть G — группа, $X, Y \subseteq G$ — подмножества G. Через XY принято обозначать подмножество $\{ xy \mid x \in X, y \in Y \}$. Если дан элемент $x \in G$ и подгруппа $H \subseteq G$, то множество $xH = \{ xh \mid h \in H \}$ называется левым смежным классом G по H с представителем x, а $Hx = \{ hx \mid h \in H \}$ — правым смежным классом G по H с представителем x. Существуют взаимно-однозначные соответствия между множествами H и xH, H и Hx, задаваемые так : $h \to xh$, $y \to x^{-1}y$ для $h \in H$, $y \in xH$, и $h \to hx$, $y \to yx^{-1}$ для $h \in H$, $y \in Hx$. В частности, эти множества равномощны. Мощность множества X будем обозначать через $|X|$. Напомним, что если X конечно, то мощность X — это количество элементов в X. Мощность $|G|$ группы G называется порядком группы.

Теорема 2.1. (1) *Два смежных класса xH и yH либо не пересекаются, либо совпадают. $xH = yH$ тогда и только тогда, если*

$x^{-1}y \in H$. *Если* $a \in xH$, *то* $xH = aH$. $xH = H$ *тогда и только тогда, если* $x \in H$. *Аналогичные утверждения справедливы для правых смежных классов.*

(2) $G = \bigcup\limits_{x \in G} xH$. *В частности, если взять только различные (непересекающиеся) левые смежные классы, и в каждом выбрать по одному представителю* x_i , $i \in I$, *то* G *есть объединение попарно непересекающихся множеств* x_iH , *каждое из которых равномощно* H *(а одно из них есть само множество* H *). Аналогичные утверждения справедливы для правых смежных классов.*

(3) *Число различных левых смежных классов* G *по* H *равно числу различных правых смежных классов* G *по* H *(биекция осуществляется соответствием* $xH \longleftrightarrow Hx^{-1}$ *).*

(4) *Если* G *конечно, то отсюда следует, что* $|G| = |I||H|$. *Число* $|I|$ *различных смежных классов* G *по* H *(левых или правых) обозначается через* $|G : H|$ *и называется индексом подгруппы* H *в группе* G . *Имеет место равенство* ("Теорема Лагранжа")*:*

$$|G| = |G : H||H|$$

В частности, порядок конечной группы нацело делится на порядок любой ее подгруппы.

Если $x \in G$, то порядок циклической подгруппы $\langle x \rangle \subseteq G$, порожденной элементом x , называется порядком элемента x . Если $\langle x \rangle \cong \mathbf{Z}$, то порядок бесконечен, а если он конечен, то равен наименьшему положительному n , такому, что $x^n = 1$. Из теоремы Лагранжа следует, что порядок элемента любой конечной подгруппы нацело делит порядок группы. Отсюда получаем, что если группа G конечна, $m = |G|$, и $x \in G$, то $x^m = 1$.

Определение 2.2. Подгруппа H группы G называется нормальной, если $xH = Hx$ для любого $x \in G$. Это эквивалентно тому, что для любых $x \in G$ и $h \in H$ имеет место включение $xhx^{-1} \in H$, что записывается также в виде $xHx^{-1} \subseteq H$. Элементы a и $b = xax^{-1}$ называются сопряжёнными.

Если группа коммутативна, то любая ее подгруппа будет нормальной.

Определение 2.3. Пусть дан гомоморфизм групп $f : G \longrightarrow W$. Его ядром, обозначаемым как $Ker(f)$, называется множество всех таких $x \in G$, что $f(x) = 1$. Если операция в W записывается аддитивно, то соответственно $Ker(f) = \{ x \in G \mid f(x) = 0 \}$.

Если $f : X \longrightarrow Y$ — любое отображение, и $Z \subseteq Y$, то через $f^{-1}(Z)$ обозначается множество $\{ x \in X \mid f(x) \in Z \}$. Оно называется (полным) прообразом Z относительно f. Отображение f инъективно тогда и только тогда, если прообраз любого элемента $y \in Y$ есть либо пустое множество, либо множество из одного элемента.

Теорема 2.2. *Ядро $H = Ker(f)$ любого гомоморфизма групп $f : G \longrightarrow W$ есть нормальная подгруппа в G. Если $w = f(g)$, $g \in G$, то $f^{-1}(w) = gH = Hg$. Обратно, для любой нормальной подгруппы $H \subseteq G$ найдется группа H и гомоморфизм $f : G \longrightarrow W$, такой, что $H = Ker(f)$.*

Следствие 2.1. *Гомоморфизм групп $f : G \longrightarrow W$ является инъективным тогда и только тогда, когда его ядро состоит из одного элемента, $Ker(f) = \{ 1_G \}$ (или, если запись операций аддитивна, когда $Ker(f) = \{ 0 \}$).*

Явный способ построения W и гомоморфизма f по данной нормальной подгруппе $H \subseteq G$ — конструкция факторгруппы группы G по

нормальной подгруппе H .

Определение 2.4. Факторгруппой группы G по нормальной подгруппе H называется множество G/H всех *различных* смежных классов G по H , со следующими операциями. Умножение: $(xH)(yH) = xyH$. Роль единицы играет класс H . Взятие обратного элемента: $(xH)^{-1} = x^{-1}H$. Для групп с аддитивной записью: $(x+H)+(y+H) = (x+y)+H$, $-(x+H) = (-x)+H$.

Для обоснования корректности определения требуется показать, что результат операции над смежными классами не зависит от выбора представителей классов. Отображение $\pi : G \longrightarrow G/H$, $\pi(x) = Hx = xH$ становится сюръективным гомоморфизмом групп (называемым естественной проекцией на факторгруппу), причем $Ker(\pi) = H$. В случае конечных групп $|G/H| = |G : H|$, $|G| = |G/H||H|$.

Теорема 2.3. (1) ("Теорема о гомоморфизме"). *Пусть дана группа G , ее нормальная подгруппа H , и гомоморфизм групп $f : G \longrightarrow W$, такой, что $H \subseteq Ker(f)$. Тогда существует один и только один гомоморфизм $\varphi : G/H \longrightarrow W$, такой, что $f = \varphi \cdot \pi$, то есть коммутативна диаграмма:*

$$\begin{array}{ccc} G & \xrightarrow{f} & W \\ \downarrow \pi & \nearrow \varphi & \\ G/H & & \end{array}$$

Образ φ совпадает с образом f . Гомоморфизм φ инъективен тогда и только тогда, если $H = Ker(f)$. В этом случае φ осуществляет изоморфизм между G/H и подгруппой $f(G) \subseteq W$.

(2) *В частности, если f — сюръекция , и $H = Ker(f)$, то $G/H \cong W$* ("теорема об изоморфизме").

Явная формула для φ: $\varphi(xH) = f(x)$.

Пример 2.4. Гомоморфизм "знак подстановки" $sgn : S_n \longrightarrow \{+1, -1\}$ строится следующим образом:

$$sgn(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Можно показать, что $sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$, $sgn(1) = 1$, и что если $\sigma = (k, l)$ — транспозиция (то есть $\sigma(k) = l$, $\sigma(l) = k$, $\sigma(i) = i$ при $i \neq k, l$), то $sgn(\sigma) = -1$.

Ядро этого гомоморфизма называется группой четных подстановок n-й степени A_n (или знакопеременной группой n-й степени). Это нормальная подгруппа группы S_n индекса 2. Следовательно, $|A_n| = |S_n|/2 = \frac{1}{2}n!$. Известно, что четные подстановки (то есть элементы A_n) характеризуются тем, что их (и только их) можно записать в виде произведения четного числа транспозиций.

Пример 2.5. Пусть K — коммутативное кольцо, $K^* = U(K)$ — множество его элементов, обладающих обратными по умножению. Это – мультипликативно записываемая группа. Тогда отображение взятия определителя (детерминанта)

$$det : GL_n(K) \longrightarrow K^*$$

есть гомоморфизм групп. Это следует из хорошо известных формул:

$det(AB) = det(A)det(B)$, $det(E_n) = 1$.

Ядро этого гомоморфизма называется специальной линейной группой и обозначается через $SL_n(K)$. Напомним, что для $A = (a_{ij})$

$$det(A) = \sum_{\sigma \in S_n} sgn(\sigma) a_{\sigma(1)\,1} a_{\sigma(2)\,2} \ldots a_{\sigma(n)\,n}$$

Из этой формулы легко вывести, что $det(m(\sigma)) = sgn(\sigma)$.

Пусть G — группа, $X \subseteq G$. Рассмотрим множество $\bar{X} = \{\, gxg^{-1} \mid x \in X, g \in G \,\}$. Подгруппа $\langle \bar{X} \rangle$ будет нормальной подгруппой в G. Такая

подгруппа называется нормальной подгруппой G, порожденной множеством X.

Одно из важнейших приложений этой конструкции — коммутант группы. В качестве X рассмотрим множество всех коммутаторов — элементов вида $[a,b] = aba^{-1}b^{-1}$. Нормальная подгруппа, порожденная множеством всех коммутаторов, обозначается через $[G,G]$, и называется коммутантом группы G. Фактически, так как $c[a,b]c^{-1} = [cac^{-1}, cbc^{-1}]$, коммутант совпадает с просто подгруппой, порожденной всеми коммутаторами. Заметим, что $[a,b] = 1$ тогда и только тогда, если $ab = ba$. Так как $[a,b]^{-1} = [b,a]$, то группа $[G,G]$ состоит из всевозможных произведений коммутаторов.

Теорема 2.4. *Факторгруппа $G/[G,G]$ является коммутативной. Если H — такая нормальная подгруппа G, что G/H коммутативна, то $[G,G] \subseteq H$.*

Пример 2.6 . $[S_n, S_n] = A_n$. При $n \geq 5$ $[A_n, A_n] = A_n$.
$[A_4, A_4] = \{ 1, (12)(34), (13)(24), (14)(23) \}$.

Пример 2.7 . . Если K – поле, то $[GL_n(K), GL_n(K)] = SL_n(K)$.

Рассмотрим цепочку вложений нормальных подгрупп:

$$G \supseteq [G,G] \supseteq [[G,G],[G,G]] \supseteq [[[G,G],[G,G]],[[G,G],[G,G]]] \supseteq \ldots$$

Положим $[G,G] = G^{(1)}$, $[G^{(n-1)}, G^{(n-1)}] = G^{(n)}$.

Определение 2.5. Группа G называется разрешимой, если $G^{(n)} = \{ 1 \}$ для некоторого конечного n.

Теорема 2.5. (Томпсон-Фейт) *Всякая конечная группа нечетного порядка разрешима.*

Доказательство этой теоремы, опубликованное в 1963 году, занимает около 250 страниц журнального формата. В 1970-м году один из авто-

ров, Джон Томпсон, был удостоен Филдсовской премии (высшей награды за достижения в математике).

Группа F называется свободной, если в ней существует подмножество X (базис) , такое, что для любой группы W и любого отображения $\varphi : X \to W$ существует один и только один гомоморфизм $f : F \to W$, такой, что для всех $x \in X$ имеет место равенство $f(x) = \varphi(x)$. Свободная группа с базисом из одного элемента — это бесконечная циклическая группа.

Теорема 2.6. *Свободная группа существует для любого наперед заданного базиса, и определена с точностью до изоморфизма. Любая группа изоморфна факторгруппе некоторой свободной группы.*

Эта теорема есть частный случай более общего факта, который будет доказан в следующей главе. Конкретное же построение F , неформально говоря, таково. F есть множество слов вида $x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_n}^{\varepsilon_n}$, где $x_{i_k} \in X$, $\varepsilon_k = \pm 1$, $n \geq 0$, $1 \leq k \leq n$. Умножение осуществляется путем приписывания одного слова к другому. При этом надо отождествлять все слова xx^{-1} и $x^{-1}x$ с пустым словом, то есть с единицей группы F . Между элементами из X нет никаких соотношений, кроме тех, которые являются следствиями определения группы. Разумеется, на самом деле надо говорить о множестве классов эквивалентных слов.

Пусть группа G изоморфна F/H , где H — нормальная подгруппа F , порожденная (как нормальная подгруппа !) множеством элементов Z , являющихся словами в алфавите X . Тогда говорят, что группа G задана множеством образующих X и соотношений Z . Обозначения:

$$G = \langle\ X \mid Z\ \rangle = \text{гр}(X|Z)$$

Если $z = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_n}^{\varepsilon_n} \in Z$, и образ $x \in X$ в G обозначается снова через x , то это значит, что в G все $x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_n}^{\varepsilon_n}$ равны единице группы

G. Часто вместо самого z пишется $z = 1$, чтобы подчеркнуть это обстоятельство. Если $z = ab^{-1}$, то пишется также $a = b$. Если

$$G = \langle\, x_1, x_2, \ldots, x_n \mid a_1 = b_1, \ldots, a_m = b_m \,\rangle,$$

где $a_j = a_j(x_1, \ldots x_n)$, $b_j = b_j(x_1, \ldots x_n)$ есть слова в алфавите $x_1, \ldots x_n$, и задано отображение $\varphi : \{x_1, \ldots x_n\} \longrightarrow W$ в группу W, такое, что в W выполняются равенства $a_j(\varphi(x_1), \ldots \varphi(x_n)) = b_j(\varphi(x_1), \ldots \varphi(x_n))$, то существует один и только один гомоморфизм групп $f : G \longrightarrow W$, такой, что $f(x_i) = \varphi(x_i)$.

Пример 2.8. Одно из важнейших семейств бесконечных групп — группы кос (группы кос Артина). n-я группа кос ("группа кос с n нитями") обозначается через B_n (или Br_n), и формально определяется как группа с образующими $\sigma_1, \ldots, \sigma_{n-1}$, и следующими соотношениями:

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ при } 1 \le i \le n-2, \qquad \sigma_i\sigma_j = \sigma_j\sigma_i \text{ при } |i-j| \ge 2.$$

Рассмотрим группу подстановок n-й степени S_n. Известно, что она порождается транспозициями $t_i = (i, i+1)$, причем определяющие соотношения выглядят так:

$$t_it_{i+1}t_i = t_{i+1}t_it_{i+1} \text{ при } 1 \le i \le n-2, \qquad t_it_j = t_jt_i \text{ при } |i-j| \ge 2,$$

и, кроме того, $t_i^2 = 1$ при $1 \le i \le n-1$. Ввиду этого существуют гомоморфизмы $\varphi_n : B_n \longrightarrow S_n$, отображающие σ_i в τ_i. Ядра этих гомоморфизмов называются группами крашеных кос Артина.

В теории групп кос важное место занимают представления Бурау (или Бюрау) — гомоморфизмы B_n в группы обратимых матриц, имеющие следующий вид. Зафиксируем комплексное число $t \neq 0$. Неприводимое представление Бурау отображает образующие σ_i группы B_n в матрицы n-го порядка (подразумевается, что в них все пустые

места заняты нулями, а элемент $1-t$ расположен в i-й строке и i-м столбце) :

$$\beta_i = \begin{pmatrix} 1 & \dots & & & & \dots & 0 \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & 1-t & t & & \\ & & & 1 & 0 & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ 0 & \dots & & & & \dots & 1 \end{pmatrix}$$

Другое представление Бурау отображает σ_i в матрицы n-го порядка b_i, устроенные следующим образом (снова предполагается, что пустые места в них заполнены нулями, а на диагоналях — единицами).

$$b_1 = \begin{pmatrix} -t & 0 & & & 0 \\ -1 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} \quad , \qquad b_{n-1} = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & 1 & -t \\ 0 & & & 0 & -t \end{pmatrix}$$

$$b_i = \begin{pmatrix} 1 & \dots & & & & \dots & 0 \\ & \ddots & & & & & \\ & & 1 & -t & 0 & & \\ & & 0 & -t & 0 & & \\ & & 0 & 1 & 1 & & \\ & & & & & \ddots & \\ 0 & \dots & & & & \dots & 1 \end{pmatrix}$$

В матрицах b_i, $2 \le i \le n-2$, элементы $-t$ расположены в i-м столце, в $i-1$-й и в i-й строках.

3. Ассоциативные кольца , алгебры, поля.

Определение 3.1. Кольцом R называется множество с двумя бинарными операциями, сложением и умножением, такими, что относительно сложения R есть абелева группа, и выполняется свойство дистрибутивности (билинейности умножения): для всех $x, y, z \in R$

$$x(y+z) = xy + xz \qquad , \qquad (x+y)z = xz + yz \ .$$

Кольцо называется ассоциативным, если операция умножения в R ассоциативна, то есть для всех $x, y, z \in R$ имеет место равенство $x(yz) = (xy)z$ (значит, R — полугруппа по умножению). Кольцо называется коммутативным, если R — коммутативная полугруппа по умножению, то есть для всех $x, y \in R$ $xy = yx$. Говорят, что R есть кольцо с единицей, если в полугруппе по умножению R есть единица $1 = 1_R$. Ассоциативное коммутативное кольцо с единицей называется телом, если множество ненулевых элементов R есть группа относительно операции умножения. Кольцо R называется полем, если R есть коммутативное тело.

Теорема 3.1. *Каждое конечное тело коммутативно, то есть является полем.*

Говорят, что элемент $x \in R$ является делителем нуля, если $x \neq 0$ и существует $y \neq 0$, такой, что либо $xy = 0$, либо $yx = 0$. Элемент $x \in R$ называется обратимым, если существует $y \in R$, такой, что $xy = 1$ и $yx = 1$. В ассоциативном кольце с единицей множество всех обратимых элементов образует группу по умножению, обозначаемую через $U(R)$ (группу обратимых элементов кольца R). В ассоциативном кольце обратимый элемент не может быть делителем нуля.

В дальнейшем рассматриваются только ассоциативные кольца с единицей, называемые просто кольцами.

Кольцо, в котором каждый ненулевой элемент не является делителем нуля, называется областью целостности (иногда — просто областью). Этот термин чаще всего применяется к коммутативным кольцам.

Определение 3.2. Пусть R, S — кольца. Гомоморфизмом колец (с единицей) называется отображение $f : R \longrightarrow S$, которое является гомоморфизмом аддитивных групп и мультипликативных полугрупп,

и отображают единицу в единицу. Таким образом,

$$f(x \pm y) = f(x) \pm f(y), \quad f(0) = 0,$$
$$f(xy) = f(x)f(y), \qquad f(1) = 1.$$

Ядро гомоморфизма колец: $Ker(f) = \{\, x \in R \mid f(x) = 0 \,\}$.

Определение 3.3. Идеал $\mathfrak{a}$ кольца R — это подмножество $\mathfrak{a} \subseteq R$, являющееся подгруппой аддитивной группы R (то есть группы R по сложению), и такое, что для всех $x \in R$, $a \in \mathfrak{a}$ имеют место включения $xa \in \mathfrak{a}$, $ax \in \mathfrak{a}$.

Идеалы $\{0\}$ и R называются тривиальными. Равенство $\mathfrak{a} = R$ равносильно наличию в $\mathfrak{a}$ хотя бы одного обратимого элемента, или же включению $1 \in \mathfrak{a}$. Таким образом, в телах и в полях нет нетривиальных идеалов. Кольца, в которых нет нетривиальных идеалов, называются простыми.

Ядра гомоморфизмов колец являются идеалами колец. Идеалы являются для колец примерно тем же, чем для групп являются нормальные подгруппы. В частности, имеет место теорема

Теорема 3.2. *Ядро $\mathfrak{a} = Ker(f)$ любого гомоморфизма колец $f : R \longrightarrow S$ есть идеал в R. Если $s = f(r)$, $r \in R$, то $f^{-1}(s) = r + \mathfrak{a}$. Обратно, для любого идеала $\mathfrak{a} \subseteq R$ найдется кольцо S и гомоморфизм $f : R \longrightarrow S$, такой, что $\mathfrak{a} = Ker(f)$.*

Следствие 3.1. *Гомоморфизм колец $f : R \longrightarrow S$ является инъективным тогда и только тогда, когда его ядро — тривиальный, нулевой идеал $Ker(f) = \{\, 0 \,\}$.*

Явный способ построения S и гомоморфизма f по данному идеалу — конструкция факторкольца кольца K по идеалу $\mathfrak{a}$.

Определение 3.4. Факторкольцо кольца R по идеалу $\mathfrak{a}$ — это факторгруппа $R/\mathfrak{a}$ абелевой группы (по сложению) R по ее подгруппе $\mathfrak{a}$ (то есть множество различных смежных классов вида $x+\mathfrak{a}$ с операцией $(x+\mathfrak{a}) \pm (y+\mathfrak{a}) = (x \pm y) + \mathfrak{a}$), на которой дополнительно введена операция умножения

$$(x+\mathfrak{a})(y+\mathfrak{a}) = xy + \mathfrak{a}$$

Роль нуля играет смежный класс $\mathfrak{a}$, роль единицы — класс $1+\mathfrak{a}$.

Отображение $\pi : R \longrightarrow R/\mathfrak{a}$, $\pi(x) = x+\mathfrak{a}$ становится сюръективным гомоморфизмом колец(называемым естественной проекцией на факторкольцо), причем $Ker(\pi) = \mathfrak{a}$.

Теорема 3.3. (1) ("Теорема о гомоморфизме"). *Пусть дано кольцо R, его идеал $\mathfrak{a}$, и гомоморфизм колец $f : R \longrightarrow S$, такой, что $\mathfrak{a} \subseteq Ker(f)$. Тогда существует один и только один гомоморфизм $\varphi : R/\mathfrak{a} \longrightarrow S$, такой, что $f = \varphi \cdot \pi$, то есть коммутативна диаграмма:*

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \downarrow \pi & \nearrow \varphi & \\ R/\mathfrak{a} & & \end{array}$$

Образ φ совпадает с образом f. Гомоморфизм φ инъективен тогда и только тогда, если $\mathfrak{a} = Ker(f)$. В этом случае φ осуществляет изоморфизм между $R/\mathfrak{a}$ и подкольцом $f(R) \subseteq S$.

(2) *В частности, если f — сюръекция, и $\mathfrak{a} = Ker(f)$, то $R/\mathfrak{a} \cong S$* ("теорема об изоморфизме").

Явная формула для φ: $\varphi(x+\mathfrak{a}) = f(x)$.

Пример 3.1. Стандартные обозначения : $\mathbf{Z}$ — кольцо целых чисел, $\mathbf{Q}$ — поле рациональных чисел, $\mathbf{R}$ — поле действительных чисел, $\mathbf{C}$ — поле комплексных чисел.

Пример 3.2 . Пусть R — кольцо. Множество всех квадратных $n \times n$-матриц с компонентами из R образует кольцо относительно обычных операций сложения и умножения матриц. Коммутативность R не обязательна. Кольцо матриц над R обозначается через $M_n(R)$.

Пример 3.3 . Кольцо многочленов $R[x_1, \ldots, x_n]$ с коэффициентами из кольца R: кольцо коэффициентов может не быть коммутативным, переменные x_i коммутируют между собой и со всеми элементами из R.

Определение 3.5. Идеал $\mathfrak{a}$ кольца R называется главным, если существует $r \in R$ (порождающий элемент), такой, что $\mathfrak{a} = \{ a \in R \mid a = \sum\limits_{x,y \in R} xry \}$. Главный идеал, порожденный элементом r, обозначается через (r), или через $\langle r \rangle$. Если R коммутативно, то $(r) = \{ xr = rx \mid x \in R \}$ обозначается через rR или Rr. Кольцо R называется кольцом главных идеалов, если каждый идеал в R является главным. Если R , кроме того — область целостности, то R называется областью главных идеалов.

Теорема 3.4. *Кольца* $\mathbf{Z}$ *и* $K[x]$ *(где* K *— поле) являются областями главных идеалов.*

Таким образом, каждый идеал в $\mathbf{Z}$ имеет вид $n\mathbf{Z}$, где n можно выбрать неотрицательным. Это — множество всех чисел, делящихся на n без остатка.

Теорема 3.5. *Если* $f : R \longrightarrow S$ *— сюръективный гомоморфизм колец, и* R *— кольцо главных идеалов, то* S *— также кольцо главных идеалов.*

Если $\mathfrak{K} \subseteq S$ — идеал в S, то $f^{-1}(\mathfrak{K})$ — идеал в R, который является главным. А образ идеала вида $(r) \subseteq R$ в S есть идеал $(f(r))$.

Говорят, что идеал $\mathfrak{a} \subseteq R$ порожден элементами из множества $\{ r_i \mid i \in I \}$, если $\mathfrak{a}$ есть множество всех элементов вида $\sum\limits_{i \in I} x_i r_i y_i$, где x_i, y_i — всевозможные элементы из R, почти все равные нулю. Говорят, что $\mathfrak{a}$ конечно порожден, если у него существует конечное множество образующих.

Теорема 3.6. ("Теорема Гильберта о базисе"). *Если K — поле, то каждый идеал кольца многочленов $K[x_1, \ldots, x_n]$ конечно порожден.*

Теорема 3.7. (1) *Факторкольцо $\mathbf{Z}/p\mathbf{Z}$ является полем тогда и только тогда, когда p — простое число.*

(2) *Факторкольцо $K[x]/(p)$ (где K — поле, а $p = p(x)$ — многочлен) является полем тогда и только тогда, когда p — неприводимый многочлен.*

Пример 3.4. Факторкольца вида $\mathbf{Z}/n\mathbf{Z}$, состоящие из n элементов

$$\overline{0} = n\mathbf{Z}, \overline{1} = 1 + n\mathbf{Z}, \overline{2} = 2 + n\mathbf{Z}, \ldots, \overline{n-1} = (n-1) + n\mathbf{Z},$$

называются кольцами вычетов по модулю n, а их элементы — классами вычетов по модулю n. Говорят, что числа k и m сравнимы друг с другом по модулю n, если $k + n\mathbf{Z} = m + n\mathbf{Z}$, или, что равносильно, $k - m$ делится нацело на n. Обозначение: $k \equiv m \pmod{n}$.

Прямое произведение колец определяется как прямое произведение соответствующих абелевых групп по сложению, а так как у сомножителей есть еще мультипликативное умножение, делающее их полугруппами, то соответствующее полугрупповое умножение можно определить и на их произведении, которое превращается в результате в ассоциативное кольцо. В случае двух колец R_1 и R_2 это выглядит так. Элементы $R_1 \times R_2$ — всевозможные упорядоченные пары (x_1, x_2), где

$x_1 \in R_1, x_2 \in R_2$. Операции:

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \quad , \quad -(x, y) = (-x, -y),$$
$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2)$$

Нулевой элемент в $R_1 \times R_2$ есть $(0,0)$, единица — $(1,1) = (1_{R_1}, 1_{R_2})$. Отображения $\pi_i : R_1 \times R_2 \to R_i$, $\pi_i(x_1, x_2) = x_i$, $i = 1, 2$, становятся гомоморфизмами колец. Произведение произвольного семейства колец устроено аналогично. Отметим, что если даны два гомоморфизма колец $h_1 : R \to R_1$, $h_2 : R \to R_2$, то отображение

$$h : R \longrightarrow R_1 \times R_2 \qquad , \qquad h(x) = (h_1(x), h_2(x))$$

есть гомоморфизм колец, причем $Ker(h) = Ker(h_1) \cap Ker(h_2)$.

Идеалы $\mathfrak{a}_1, \mathfrak{a}_2$ кольца R называются взаимно простыми (или комаксимальными), если $\mathfrak{a}_1 + \mathfrak{a}_2 = R$. Эквивалентное условие: существуют $a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2$, такие, что $a_1 + a_2 = 1$. Для взаимно простых идеалов $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$, где идеал $\mathfrak{a}_1\mathfrak{a}_2$ определяется как множество всевозможных конечных сумм вида $\sum x_1 x_2$, $x_1 \in \mathfrak{a}_1$, $x_2 \in \mathfrak{a}_2$. Если $R = \mathbf{Z}$, $\mathfrak{a}_1 = n_1\mathbf{Z}$, $\mathfrak{a}_2 = n_2\mathbf{Z}$, то эти идеалы взаимно просты тогда и только тогда, когда взаимно просты числа n_1, n_2 . В этом случае $\mathfrak{a}_1\mathfrak{a}_2 = (n_1 n_2)\mathbf{Z}$.

Теорема 3.8. ("Китайская теорема об остатках"). *Пусть R — коммутативное кольцо, $\mathfrak{a}_1, \mathfrak{a}_2$ — взаимно простые идеалы. Тогда*

$$R/\mathfrak{a}_1\mathfrak{a}_2 \cong R/\mathfrak{a}_1 \times R/\mathfrak{a}_2.$$

Сначала по естественным проекциям $\pi_i : R \to R/\mathfrak{a}_i$ строится гомоморфизм $\pi : R \to R/\mathfrak{a}_1 \times R/\mathfrak{a}_2$, $\pi(x) = (\pi_1(x), \pi_2(x))$ с ядром $\mathfrak{a}_1\mathfrak{a}_2$. Чтобы доказать его сюръективность, надо взять произвольные $x_1, x_2 \in R$, $a_1 \in \mathfrak{a}_1$, $a_2 \in \mathfrak{a}_2$, такие, что $a_1 + a_2 = 1$, и $x = x_1 a_2 + x_2 a_1$. Тогда $\pi(x) = (\pi_1(x_1), \pi_2(x_2))$.

В частности любое кольцо вычетов $\mathbf{Z}/n\mathbf{Z}$ изоморфно прямому произведению

$$\mathbf{Z}/p_1^{k_1}\mathbf{Z} \times \mathbf{Z}/p_2^{k_2}\mathbf{Z} \times \ldots \times \mathbf{Z}/p_m^{k_m}\mathbf{Z},$$

где $n = p_1^{k_1}p_2^{k_2}\ldots p_m^{k_m}$ — разложение числа n в произведение простых сомножителей, p_i — различные простые числа. Кольца вида $\mathbf{Z}/p^k\mathbf{Z}$ уже нельзя разложить в произведение.

Рассмотрим строение групп обратимых элементов колец вычетов.

Лемма 3.1. *Элемент $\overline{m} = m+n\mathbf{Z}$ обратим в $\mathbf{Z}/n\mathbf{Z}$ тогда и только тогда, если m взаимно просто с n.*

Порядок группы обратимых элементов $U(\mathbf{Z}/n\mathbf{Z})$ обозначается через $\varphi(n)$ (φ называется функцией Эйлера). Известно, что $\varphi(p) = p-1$, $\varphi(p^k) = p^k - p^{k-1}$.

Теорема 3.9. (Теорема Эйлера). *$m^{\varphi(n)} \equiv 1 \pmod{n}$ при m взаимно простом с n.*

Теорема 3.10. ("Малая теорема Ферма"). *$m^{p-1} \equiv 1 \pmod{p}$ при простом p и m, не делящемся на p.*

Теорема 3.11. *Группа $U(\mathbf{Z}/p\mathbf{Z})$ при простом p является циклической.*

Лемма 3.2. *$U(R_1 \times R_2) \cong U(R_1) \times U(R_2)$. В частности, $|U(R_1 \times R_2)| = |U(R_1)| \cdot |U(R_2)|$.*

Следствие 3.2. *Функция Эйлера мультипликативна, то есть при взаимно простых n_1, n_2 имеет место равенство: $\varphi(n_1n_2) = \varphi(n_1)\varphi(n_2)$.*

Этот факт позволяет вычислить значение функции Эйлера для любого аргумента.

Определение 3.6. Правым модулем над кольцом R (правым R-модулем) называется абелева группа M (операция — сложение), вместе с заданной операцией "умножения на скаляры"— элементы кольца:

$$M \times R \longrightarrow M \qquad , \qquad (m, r) \mapsto mr \ ,$$

удовлетворяющей следующим свойствам:

$$(m_1 \pm m_2)r = m_1 r \pm m_2 r,$$
$$m(r_1 \pm r_2) = mr_1 \pm mr_2,$$
$$m(r_1 r_2) = (mr_1)r_2,$$
$$0 \cdot r = 0, m \cdot 0 = 0, m \cdot 1 = m.$$

Обозначения вида M_R выражают тот факт, что M есть правый R-модуль.

Гомоморфизм f из правого R-модуля M_1 в правый R-модуль M_2 — это гомоморфизм абелевых групп, такой, что для всех $m \in M_1$, $r \in R$, имеет место равенство $f(mr) = f(m)r$.

Левые модули и их гомоморфизмы определяются совершенно аналогично. Обозначения вида ${}_R M$ выражают тот факт, что M есть левый R- модуль. Если кольцо R коммутативно, то между левыми и правыми модулями нет разницы: правый можно сделать левым, полагая $rm = mr$, и наоборот.

Подмодуль правого R-модуля M — это абелева подгруппа $M' \subseteq M$, такая, что если $x \in M'$, $r \in R$, то $xr \in M'$, и аналогично для левых модулей. Вложение $M' \subseteq M$ в этом случае есть гомоморфизм модулей.

Само кольцо R есть правый R-модуль R_R и левый R-модуль ${}_R R$. Левые подмодули ${}_R R$ называются левыми идеалами кольца R , а правые подмодули R_R называются правыми идеалами R . Если $\mathfrak{a} \subseteq R$ является одновременно и левым, и правым идеалом R , то $\mathfrak{a}$ называет-

ся двухсторонним идеалом R. Это — то же самое, что и идеал кольца в смысле данного выше определения.

Пример 3.5 . Модули над полем — это обычные векторные пространства, гомоморфизмы — обычные линейные отображения.

Пример 3.6 . Модули над $\mathbf{Z}$ — это, в сущности, то же самое, что и (аддитивно записываемые) абелевы группы. Если $x \in M$, $n \in \mathbf{Z}$, то при $n > 0$ элемент nx определяется как сумма n экземпляров x, а при $n < 0$ — как сумма n экземпляров $-x$. Гомоморфизмы модулей над $\mathbf{Z}$ — это гомоморфизмы абелевых групп.

Определение 3.6. Пусть R — кольцо (даже не обязательно ассоциативное или с единицей), K — коммутативное ассоциативное кольцо с единицей. R называется алгеброй над K (или K - алгеброй), если на R определена структура K - модуля (в данном случае неважно, правого или левого), такая, что умножение в R становится K - билинейным отображением. Это означает, что для любых $x, y, z \in R$, $a, b \in K$ имеют место равенства $(ax+by)z = a(xy)+b(xz)$, $x(ay+bz) = a(xy)+b(xz)$.

Подчеркнем, что по определению $ax = xa$ при $x \in R$, $a \in K$, так что $a(xy) = (xa)y = x(ay) = (xy)a$.

Гомоморфизм алгебр — это гомоморфизм колец, одновременно являющийся и гомоморфизмом модулей.

Лемма 3.3. *Если R — ассоциативное кольцо с единицей, то задание на R структуры K - алгебры равносильно заданию гомоморфизма колец с единицей $h : K \longrightarrow R$, такого, что для любых $x \in R$, $a \in K$ имеет место равенство $xh(a) = h(a)x$.*

Если задан гомоморфизм, то структура модуля определяется так : $xa = xh(a)$. Если задана структура алгебры, то гомоморфизм строится так: $h(a) = a \cdot 1_R$. Когда h инъективен, то обычно считают, что это просто

включение, и, таким образом, K есть подкольцо R с дополнительным свойством: все элементы K коммутируют со всеми элементами R. В частности, R есть алгебра над любым своим подкольцом с соответствующим свойством.

Многие рассмотренные примеры колец являются также и примерами алгебр. В частности, $M_n(K)$ и $K[x_1, \ldots, x_n]$ есть алгебры над K. Важный способ описания алгебр дает следующая лемма:

Лемма 3.4. *Пусть R есть свободный модуль над K с базисом $\{ e_i \mid i \in I \}$ (см. определение в следующем разделе). Допустим, что для любых $i, j \in I$ определены выражения $e_i e_j = \sum\limits_{k \in I} e_k c_{ij}^k$, где $c_{ij}^k \in K$ и почти все равны нулю. Тогда на R можно определить структуру K - алгебры, полагая произведение элементов $\sum\limits_{i \in I} e_i a_i$ и $\sum\limits_{j \in I} e_j b_j$ равным $\sum\limits_{i,j \in I} (e_i e_j) a_i b_j$ с последующей подстановкой выражений $e_i e_j$ и приведением подобных членов:*

$$\sum_{k \in I} e_k \Big(\sum_{i,j \in I} c_{ij}^k a_i b_j \Big).$$

Для того, чтобы получившаяся алгебра была ассоциативным кольцом, необходимо и достаточно, чтобы для любых $i, j, k \in I$ имели место равенства $(e_i e_j) e_k = e_i (e_j e_k)$. Для того, чтобы получившаяся алгебра была коммутативным кольцом, необходимо и достаточно, чтобы для любых $i, j \in I$ имели место равенства $e_i e_j = e_j e_i$.

Элементы $c_{ij}^k \in K$ называются структурными константами алгебры R, а о задании выражений $e_i e_j$ будем говорить как о "таблице умножений" алгебры.

Пример 3.7. Тело кватернионов $\mathbf{H}$ — алгебра над $\mathbf{R}$. Рассмотрим векторное пространство над $\mathbf{R}$ с базисом из четырех элементов 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$. Определим "таблицу умножения" следующим образом: $1 \cdot x = x \cdot 1 = x$

для всех x,

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$

$$\mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \mathbf{jk} = \mathbf{i} = -\mathbf{kj}, \mathbf{ki} = \mathbf{j} = -\mathbf{ik}.$$

Нетрудно проверить, что тем самым определена ассоциативная, но не коммутативная алгебра с единицей. Отождествим $\mathbf{R}$ с подкольцом $\mathbf{H}$, состоящим из элементов вида $r \cdot 1$, $r \in \mathbf{R}$. Определим для кватерниона $q = t \cdot 1 + x \cdot \mathbf{i} + y \cdot \mathbf{j} + z \cdot \mathbf{k}$ его сопряженный $\overline{q} = t \cdot 1 - x \cdot \mathbf{i} - y \cdot \mathbf{j} - z \cdot \mathbf{k}$. Тогда $N(q) = q\overline{q} = \overline{q}q = t^2 + x^2 + y^2 + z^2 \in \mathbf{R}$, $N(q) = 0$ тогда и только тогда, если $q = 0$. Теперь для любого $q \neq 0$ можно построить обратный по умножению элемент

$$q^{-1} = \frac{1}{N(q)}\overline{q}.$$

Заметим, что $\mathbf{C}$ также можно считать подкольцом $\mathbf{H}$ (подалгеброй с базисом $1, \mathbf{i}$), но $\mathbf{H}$ не будет алгеброй над $\mathbf{C}$.

Теорема 3.12. (Фробениус). *Пусть K — конечномерная ассоциативная алгебра над полем действительных чисел $\mathbf{R}$ (то есть K — конечномерное векторное пространство над $\mathbf{R}$). Если K является телом (в старых книгах пишут : "алгеброй с делением"), то либо $K = \mathbf{R}$, либо $K \cong \mathbf{C}$, либо $K \cong \mathbf{H}$.*

Пример 3.8. Пусть K — коммутативное кольцо, G — полугруппа с единицей. Как будет показано в следующем разделе, можно построить свободный K-модуль $K[G]$ с базисом G. Его элементы — формальные (конечные) суммы вида $\sum\limits_{x \in G} xc_x$, $c_x \in K$. Умножение в G задает теперь "таблицу умножений" для алгебры $K[G]$. Явный вид умножения элементов таков:

$$(\sum_{x \in G} xa_x)(\sum_{y \in G} yb_y) = \sum_{z \in G} z(\sum_{\substack{x \in G, y \in G \\ xy = z}} a_x b_y)$$

Единица G будет также единицей полугрупповой алгебры $K[G]$. Саму полугруппу G можно считать подмножеством (базисом) $K[G]$.

Если G есть свободная коммутативная полугруппа с базисом X, то $K[G]$ есть не что иное, как кольцо (алгебра) многочленов от переменных X.

Заметим, что если R — алгебра над K, $\mathfrak{a}$ — идеал R, то факторкольцо $R/\mathfrak{a}$ естественным образом также превращается в алгебру над K Достаточно положить для $c \in K$, $x \in R$ $c(x+\mathfrak{a}) = (cx)+\mathfrak{a}$. Соответствующий гомоморфизм $K \longrightarrow R/\mathfrak{a}$ есть композиция гомоморфизмов $K \longrightarrow R$ и $R \longrightarrow R/\mathfrak{a}$. Если K — поле, то все эти гомоморфизмы инъективны, и можно считать K как подкольцом R, так и подкольцои $R/\mathfrak{a}$: $c \in K$ отождествляется с $c \cdot 1_R + \mathfrak{a}$.

Рассмотрим более подробно строение колец вида $K[x]/(f(x))$, где K — поле, $f(x) \in K[x]$. Как уже отмечено, это — алгебры над K.

Теорема 3.13. *Пусть K — поле, $f = f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in K[x]$. Тогда факторалгебра $K[x]/(f(x))$ есть n - мерное векторное пространство над K с базисом*

$$\overline{1} = 1 + (f), \overline{x} = x + (f), \overline{x}^2 = x^2 + (f), \ldots . \overline{x}^{n-1} = x^{n-1} + (f).$$

В частности, если $K = \mathbf{Z}/p\mathbf{Z}$ — конечное поле из p элементов, p — простое число, то множество $K[x]/(f(x))$ состоит из p^n элементов.

Поле $K = \mathbf{Z}/p\mathbf{Z}$ принято обозначать также через $\mathbf{F}_p$ и называть простым конечным полем характеристики p.

Теорема 3.14. (Теорема о строении конечных полей). *Любое конечное поле изоморфно одному из полей вида $\mathbf{F}_p[x]/(f(x))$, где $f(x) \in \mathbf{F}_p[x]$ — некоторый неприводимый многочлен. Простые поля состоят,*

таким образом, из p^n элементов, где p — простое, а $n > 0$ — некоторое целое число. Обратно, для любых p, n существует (и единственно с точностью до изоморфизма) конечное поле из p^n элементов, имеющее вид $\mathbf{F}_p[x]/(f(x))$ (причем f определен неоднозначно). Если K — конечное поле, то группа $U(K)$ является циклической.

Любое поле K (как и любое ассоциативное кольцо с единицей) есть алгебра над $\mathbf{Z}$, и поэтому существует гомоморфизм $h : \mathbf{Z} \longrightarrow K$, такой, что $h(n) = n \cdot 1_K$. Если этот гомоморфизм инъективен, то можно считать, что $\mathbf{Z} \subset K$, а тогда и $\mathbf{Q} \subseteq K$. В этом случае говорят, что поле K имеет нулевую характеристику (или: характеристика K равна нулю, $char(K) = 0$).

Если же $Ker(h) \neq \{0\}$, то $Ker(h) = (p) = p\mathbf{Z}$ для некоторого простого $p > 0$. В этом случае говорят, что характеристика поля K равна p, $char(K) = p > 0$. По теореме о гомоморфизме существует инъективный гомоморфизм $\mathbf{F}_p \to K$, и можно считать, что поля характеристики p — это те поля, которые содержат $\mathbf{F}_p$ в качестве подполя. В полях характеристики $p > 0$ (более того, в алгебрах над такими полями) для любого x имеет место тождество $px = \underbrace{x + \ldots + x}_{p} = 0$, а для любых x, y, таких, что $xy = yx$, выполнено тождество $(x + y)^p = x^p + y^p$.

Теорема 3.15. *Пусть K — поле, $f(x) \in K[x]$ — многочлен степени $n > 0$. Существует поле L, содержащее K в качестве подполя, такое, что $f(x) \in K[x] \subseteq L[x]$ имеет корень в L. Более того, существует даже такое L, что f раскладывается в $L[x]$ на линейные множители.*

Достаточно считать f неприводимым (в $K[x]$), и тогда в качестве поля L можно взять поле $K[x]/(f)$. Поле K можно отождествить с подполем $K[x]/(f)$, и тогда гомоморфизм естественной проекции π :

$K[x] \longrightarrow K[x]/(f)$ становится гомоморфизмом K-алгебр. Если $\pi(x) = x + (f) = \overline{x}$, то это значит, что для любого $g(x) = \sum\limits_{k=0}^{m} a_k x^k$ будет $\pi(g(x)) = \sum\limits_{k=0}^{m} a_k \overline{x}^k = g(\overline{x})$. В частности, для $g = f$ получим $f(\overline{x}) = \pi(f) = 0$.

Пример 3.9. Пусть $f(x) = x^2+1 \in \mathbf{R}[x]$. Тогда $\mathbf{R}[x]/(x^2+1)$ имеет базис над $\mathbf{R}$ из двух элементов — 1 и $\overline{x}$, причем в $\mathbf{R}[x]/(x^2+1)$ будет $\overline{x}^2 + 1 = 0$, то есть $\overline{x}^2 = -1$. Это означает, что $\mathbf{R}[x]/(x^2+1) \cong \mathbf{C}$.

4. Модули и векторные пространства.

Все рассматриваемые модули правые, а гомоморфизмы пишутся слева от аргументов. Случай левых модулей оговаривается особо.

Для модулей определения конструкция фактормодуля по подмодулю вводятся точно также, как выше для (абелевых) групп. Если $M' \subseteq M$ — подмодуль R-модуля M, то структура R-модуля на M/M' определяется следующим образом:

$$(x + M')r = (xr) + M',$$

где $x \in M$, $r \in R$. Для фактормодулей справедливы аналоги всех утверждений о факторгруппах ("теорема об изоморфизме" и т.п.), приводившихся выше.

Определение 4.1. Модуль V над кольцом R называется свободным (свободным R-модулем), если он обладает базисом, то есть таким подмножеством $X \subset V$, которое порождает V, и является линейно независимым над R.

Линейной оболочкой X, или подмодулем, порожденным X (обозначение — $\langle X \rangle$) называется множество всех линейных комбинаций элементов X с коэффициентами из R:

$$\langle X \rangle = \{ \sum_{x \in X} x r_x \mid r_x \in R, \text{ почти все } r_x = 0 \}$$

Таким образом, X порождает V (X есть множество образующих для V), если $V = \langle X \rangle$.

X является линейно независимым, если $\sum_{x \in X} x r_x = 0$ тогда и только тогда, если все $r_x = 0$. В этом случае представление элемента $v \in V$ в виде $v = \sum_{x \in X} x r_x$ однозначно.

Теорема 4.1. *Пусть V есть модуль над телом K (в частности, K может быть полем, и тогда V — векторное пространство).*

(1) *Если в V существует базис X , то любой другой базис Y имеет ту же мощность, что и X . В частности, если существует конечный базис из n элементов, то все базисы содержат ровно n элементов.*

(2) *Если дано линейно независимое подмножество $X \subset V$, и любое порождающее V множество Y , $\langle Y \rangle = V$, то существует подмножество $Z \subseteq Y$, такое, что $X \cap Z = \emptyset$, и $X \cup Z$ есть базис V .*

(3) *В частности, полагая X пустым, получим, что из любого множества образующих V всегда можно выбрать базис. В частности, любой модуль над телом (а значит, и любое векторное пространство над полем) обладает базисом.*

(4) *Другой частный случай пункта (2): любое линейно независимое подмножество содержится в некотором базисе.*

Модули над телами также принято называть векторными пространствами, так как их основные свойства, согласно только что сформу-

лированной теореме, полностью аналогичны свойствам векторных пространств над полями.

Как приложение этих фактов — следующий алгоритм нахождения базиса пересечения двух подпространств векторного пространства:

Теорема 4.2. *Пусть* $U, W \subseteq V$ *— подпространства векторного пространства* V *над* K. *Пусть* $u_1, \ldots, u_n$ *— базис* U, $w_1, \ldots, w_m$ *— базис* W, *и пусть* $u_1, \ldots, u_n, w_1, \ldots, w_k$ *— базис подпространства* $U + W$.*Выразим элементы* $w_{k+1}, \ldots, w_m$ *через этот базис:*

$$w_{k+s} = \sum_{i=1}^{n} u_i a_{i\ k+s} + \sum_{j=1}^{k} w_j b_{j\ k+s} \quad , \quad s = 1, \ldots, m-k.$$

Тогда элементы $v_s = \sum\limits_{i=1}^{n} u_i a_{i\ k+s}$, $s = 1, \ldots, m-k$, *образуют базис* $U \cap W$.

Определение 4.2. Пусть дано семейство модулей $\{ M_i \mid i \in I \}$ над кольцом R. Прямой суммой этого семейства называется модуль M вместе с семейством гомоморфизмов $\{ q_i : M_i \to M \mid i \in I \}$, обладающий следующим свойством. Для любого R-модуля V и любого семейства гомоморфизмов $\{ h_i : M_i \to V \mid i \in I \}$ существует один и только один гомоморфизм R-модулей $f : M \to V$, такой, что для всех $i \in I$ имеют место соотношения $f \cdot q_i = h_i$. Иными словами, коммутативны все диаграммы

$$\begin{array}{ccc} M & \xrightarrow{f} & V \\ \uparrow q_i & \nearrow & h_i \\ M_i & & \end{array}$$

Обозначение : $M = \bigoplus\limits_{i \in I} M_i$, или $M = \sum\limits_{i \in I} \oplus M_i$, или $M = \coprod\limits_{i \in I} M_i$. Если $I = \{1, 2, \ldots, n\}$, то $M = M_1 \oplus M_2 \oplus \ldots \oplus M_n$.

Теорема 4.3. (1) *Прямая сумма модулей существует для любого семейства*

$\{ M_i \mid i \in I \}$.

(2) *Прямая сумма модулей определена однозначно с точностью до изоморфизма.*

(3) *Если дан модуль* M *и семейство его подмодулей* $\{ M_i \subseteq M \mid i \in I \}$, *такое, что* $M = \sum\limits_{i \in I} M_i$, *и для всех* $i \in I$ *имеет место* $M_i \cap (\sum\limits_{j \in I, j \neq i} M_j) = \{0\}$. *Тогда имеет место изоморфизм* $M \cong \sum\limits_{i \in I} \oplus M_i$.

Существование устанавливается следующим образом. Рассмотрим прямое произведение модулей

$$M^* = \prod_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in I \}.$$

с покомпонентно определенными операциями сложения, вычитания и умножения на элементы кольца. В этом модуле рассмотрим подмодуль M, состоящий из всех тех $(m_i)_{i \in I}$, в которых $m_i = 0$ для почти всех $i \in I$. Отображения $q_j : M_j \to M$ определяются так : $q_j(x) = (m_i)$, где $m_j = x$, а при $i \neq j$ $m_i = 0$. Пусть $Im(q_j) = M'_j \cong M_j$. Тогда легко проверить, что каждый элемент $x \in M$ однозначно представляется в виде суммы $x = \sum\limits_{i \in I} x_i$, в которой $x_i \in M'_i$ и $x_i = 0$ для почти всех $i \in I$. Если дано семейство гомоморфизмов $h_i : M_i \to V$, $i \in I$, то гомоморфизм $f : M \to V$, такой, что для всех $i \in I$ имеют место равенства $f \cdot q_i = h_i$, строится следующим образом. Каждый $x \in M$ есть сумма вида $x = \sum\limits_{i \in I} q_i(m_i)$, в которой $m_i \in M_i$ определяются по x однозначно и почти все равны нулю. Положим $f(x) = \sum\limits_{i \in I} h_i(m_i)$. Легко проверить, что это гомоморфизм, удовлетворяющий свойствам $f \cdot q_i = h_i$, и что это единственно возможный гомоморфизм с такими свойствами.

Из построения следует, что если I конечно, например, $I = \{ 1, 2, \ldots, n \}$, то прямая сумма фактически совпадает с прямым произведением, так

что

$$M_1 \oplus M_2 \oplus \ldots \oplus M_n = \{\ (m_1, m_2, \ldots, m_n) \mid m_i \in M_i, 1 \leq i \leq n\ \}.$$

Гомоморфизмы q_i строятся так: если $x \in M_i$, то $q_i(x) = (0, \ldots, x, \ldots, 0)$, где x расположен на i-м месте, а все остальные компоненты строки — нули.

Теорема 4.4. *Эквивалентны следующие утверждения (эквивалентные формы определения прямой суммы).*

(1) $M \cong M_1 \oplus M_2 \oplus \ldots \oplus M_n$ *(в смысле данного выше определения).*

(2) *Существуют гомоморфизмы модулей* $q_i : M_i \to M$, $p_i : M \to M_i$, $1 \leq i \leq n$, *такие, что* $p_i q_i = 1_{M_i}$, $p_i q_j = 0$ *при* $i \neq j$, $q_1 p_1 + q_2 p_2 + \ldots + q_n p_n = 1_M$.

(3) *Существуют гомоморфизмы* $\pi_i : M \to M$, $1 \leq i \leq n$, *такие, что* $\pi_i \pi_i = \pi_i$, $\pi_i \pi_j = 0$ *при* $i \neq j$, $\pi_1 + \pi_2 + \ldots + \pi_n = 1_M$.

Следствие 4.1. *Рассмотрим инъективный гомоморфизм* $q_2 : M_2 \longrightarrow M_1 \oplus M_2$, *и сюръективный гомоморфизм* $p_1 : M_1 \oplus M_2 \longrightarrow M_1$ *из второго способа определения* $M_1 \oplus M_2$. *Тогда* $Ker(p_1) = q_2(M_2)$, *и* $(M_1 \oplus M_2)/q_2(M_2) \cong M_1$. *Отождествляя* $q_2(M_2)$ *с* M_2, *получим* $(M_1 \oplus M_2)/M_2 \cong M_1$.

Следствие 4.2. *Пусть дан модуль* M *над кольцом* R, *его подмодуль* $M_1 \subseteq M$, *и существует гомоморфизм* $\pi : M \to M$, *такой, что* $\pi^2 = \pi\pi = \pi$, *и* $\pi(M) = Im(\pi) = M_1$. *Пусть* $M_2 = Ker(\pi)$. *Тогда* $M = M_1 \oplus M_2$.

Как приложение этого следствия — классическая теорема:

Теорема 4.5. (Машке). *Пусть G — конечная группа , K — поле, характеристика которого не делит порядок группы, M — модуль над $K[G]$, $M_1 \subseteq M$ — его подмодуль. Тогда существует $K[G]$ - подмодуль M_2 модуля M , такой, что $M = M_1 \oplus M_2$.*

Теорема 4.6. *Для модуля F эквивалентны следующие утверждения:*

(1) *F — свободный модуль над кольцом R с базисом $X = \{x_i | i \in I\}$.*

(2) *Существует отображение (не гомоморфизм!) $q : X \to F$, такое, что для любого модуля V и отображения $\varphi : X \to V$ существеует один и только один гомоморфизм $f : F \to V$, такой, что $\varphi = f \cdot q$.*

(3) *$F \cong \bigoplus\limits_{x \in X} xR$, где xR — свободный модуль с базисом $x \in X$, $xR \cong R$ как правые R -модули.*

Множество всех гомоморфизмов из R -модуля M в R -модуль N есть абелева группа относительно операции

$$(f_1 \pm f_2)(x) = f_1(x) \pm f_2(x)$$

Нулевой элемент этой группы — гомоморфизм, отображающий все элементы M в нулевой элемент N . Обозначение: $\mathrm{Hom}_R(M, N)$, или $\mathrm{Hom}(M_R, N_R)$ (группа гомоморфизмов из M в N). Если $M = N$, то эта группа обозначается через $\mathrm{End}_R(M)$, или через $\mathrm{End}(M_R)$. Ее элементы называются эндоморфизмами модуля R . $\mathrm{End}(M_R)$ превращается в ассоциативное кольцо с единицей , если в качестве умножения взять композицию гомоморфизмов:

$$(f_1 f_2)(x) = f_1(f_2(x))$$

Роль единицы играет тождественное отображение $1_M : x \mapsto x$.

Если S — некоторое кольцо,то через S° будет обозначаться так называемое противоположное к S кольцо. Как абелева группа, S° совпадает с S , а операция умножения определяется так: $x \circ y = y \cdot x$, где справа стоит умножение в S . Элементы $\mathrm{End}(M_R)^\circ$ можно представлять как эндоморфизмы M , записываемые *справа* от аргументов: $f : x \mapsto xf$, для которых композиция определяется по правилу $x(f_1 f_2) = (xf_1)f_2$.

Теорема 4.7. *Пусть M — модуль над коммутативным кольцом K , R — алгебра над K . Тогда задание на M структуры правого R -модуля равносильно заданию гомоморфизма K -алгебр $f : R \to \mathrm{End}(M_K)^\circ$. Структура левого R -модуля на M определяется заданием гомоморфизма K -алгебр $f : R \to \mathrm{End}(M_K)$.*

Связь следующая:если $x \in M$, $r \in R$, то $xr = xf(r)$. Для левых модулей соответственно $rx = f(r)(x)$. В случае, когда $R = K[G]$ — полугрупповая алгебра полугруппы с единицей G , то эта теорема допускает следующее уточнение:

Теорема 4.8. *Равносильны следующие комплексы данных:*

(1) *Правое (линейное) действие на K -модуле M полугруппы G , то есть отображение $M \times G \longrightarrow M$, $(x, g) \mapsto xg$, удовлетворяющее свойствам:*

   1) $x(g_1 g_2) = (xg_1)g_2$.

   2) $x \cdot 1 = x$.

   3) $(x_1\lambda_1 + x_2\lambda_2)g = (x_1 g)\lambda_1 + (x_2 g)\lambda_2$

(2) *Структура правого $K[G]$ -модуля на M .*

(3) *Гомоморфизм мультипликативных полугрупп с единицей* $f : G \longrightarrow \mathrm{End}(M_K)^\circ$. *В случае, если* G *— группа, это равносильно заданию гомоморфизма групп* $f : G \longrightarrow \mathrm{Aut}(M_K)$.

Когда K — поле, M — конечномерное векторное пространство, $\dim_K M = n$, то имеет место изоморфизм алгебр $\mathrm{End}(M_K) \cong M_n(K)$, где $M_n(K)$ — алгебра всех $n \times n$-матриц над K . В этом случае $\mathrm{Aut}(M_K) \cong GL_n(K)$, то есть это фактически группа всех обратимых $n \times n$-матриц над K .

Определение 4.3. Гомоморфизмы K-алгебр вида $f : R \longrightarrow M_n(K)$ называются K-линейными представлениями алгебры R . Гомоморфизмы из группы G в группы вида $GL_n(K)$ называются K-линейными представлениями группы G .

5. Решетки.

Определение 5.1. Множество L называется частично упорядоченным, если на нем задано бинарное отношение $\leq$ (то есть подмножество $P \subseteq L \times L$; пишется $x \leq y$, если $(x, y) \in P$), обладающее следующими свойствами :

1. Для каждого $x \in L$ имеет место соотношение $x \leq x$.

2. Для любых $x, y \in L$ из $x \leq y$ и $y \leq x$ следует $x = y$.

3. Для любых $x, y, z \in L$ из $x \leq y$ и $y \leq z$ следует $x \leq z$.

Частично упорядоченное множество L называется линейно упорядоченным, если дополнительно имеет место следующее свойство:

4. Для любых $x, y \in L$ либо $x \leq y$, либо $y \leq x$.

Пример 5.1 . Положим L равным множеству всех подмножеств множества X , $A \leq B$ тогда и только тогда , если $A \subseteq B$. Тогда L - частично упорядоченное множество.

Пример 5.2 . Пусть L есть множество положительных натуральных чисел. У него имеется естественное отношение порядка ("больше-меньше"). Определим новое отношение $\leq$, полагая $n \leq m$ тогда и только тогда, если n нацело делит m, то есть $m = nk$. Легко проверить, что это — также отношение порядка.

Пример 5.3 . По данному частично упорядоченному множеству L всегда можно построить двойственное (дуальное) к нему частично упорядоченное множество L° следующим образом. Как множество , $L^\circ = L$, а $x \leq y$ в L° тогда и только тогда, если $x \geq y$ в L. Заметим, что $(L^\circ)^\circ = L$.

Определение 5.2. Пусть L — частично упорядоченное множество. Элемент $z \in L$ называется точной верхней гранью элементов $x, y \in L$, если $x, y \leq z$, и если $x, y \leq w$, то $z \leq w$. Обозначение: $z = \sup(x, y)$. Элемент $z \in L$ называется точной нижней гранью элементов $x, y \in L$, если $x, y \geq z$, и если $x, y \geq w$, то $z \geq w$. Обозначение: $z = \inf(x, y)$. Совершенно аналогично определяются точные верхние и нижние грани для произвольных подмножеств элементов L.

Точная верхняя грань элементов в L есть их точная нижняя грань в L°, и аналогично для нижней грани.

Определение 5.3. Решеткой (структурой) называется частично упорядоченное множество, в котором для каждой пары элементов x, y существует точная верхняя грань $\sup(x, y)$ и точная нижняя грань $\inf(x, y)$. Подрешеткой решетки L называется подмножество $L' \subseteq L$, такое, что из $x, y \in L'$ следует $\sup(x, y) \in L'$, $\inf(x, y) \in L'$. Наибольший элемент решетки (если он существует) называется единичным элементом решетки (единицей), и будет обозначаться как 1, наименьший элемент решетки (если он существует) называется нулевым элементом решетки (нулем), и будет обозначаться как 0.

Можно показать, что точная верхняя и точная нижняя грани существуют для любых конечных подмножеств. Обозначения: $\sup(x,y) = x \vee y$, $\inf(x,y) = x \wedge y$. В любой конечной решетке существуют нулевой и единичный элементы (как точная нижняя грань и точная верхняя грань всех элементов решетки). Решетка называется полной, если в ней существуют точные верхние и нижние грани для произвольных подмножеств элементов.

Теорема 5.1. *Пусть L — решетка. Тогда для операций $\vee$ и $\wedge$ выполняются следующие тождества :*

(L_1) $x \vee x = x$, $x \wedge x = x$.

(L_2) $x \vee y = y \vee x$, $x \wedge y = y \wedge x$.

(L_3) $(x \vee y) \vee z = x \vee (y \vee z)$, $(x \wedge y) \wedge z = x \wedge (y \wedge z)$.

(L_4) $x \vee (x \wedge y) = x$, $x \wedge (x \vee y) = x$.

Обратно, пусть задано множество L с двумя бинарными операциями $(x,y) \mapsto x \vee y$, $(x,y) \mapsto x \wedge y$, удовлетворяющими тождествам (L_1) , (L_2) , (L_3) , (L_4) при всех $x, y, z \in L$. Тогда можно определить на L отношение частичного порядка равенством

$$x \leq y \Leftrightarrow x \vee y = y \Leftrightarrow x \wedge y = x \qquad (*)$$

При этом оказывается, что $x \vee y = \sup(x,y)$, $x \wedge y = \inf(x,y)$. Если бинарные операции $\vee$ и $\wedge$ сами были первоначально определены, как точные верхние и нижние грани в частично упорядоченном множестве, то определенное с помощью $(*)$ отношение порядка совпадает с исходным.

Таким образом, тождества (L_1) , (L_2) , (L_3) , (L_4) дают другое, равносильное, определение решетки. Отношение порядка выражается через

$\vee$ и $\wedge$ с помощью (*) . Заметим, что обе операции, $\vee$ и $\wedge$, определяют на L структуры коммутативных полугрупп (возможно, без нейтральных элементов). Для нуля и единицы решетки (когда они есть) имеют место соотношения :

$0 \leq x \leq 1$ для любого $x, x \vee 0 = x \wedge 1 = x, x \wedge 0 = 0, x \vee 1 = 1.$

Если L — решетка,то частично упорядоченное множество L° есть решетка, называемая двойственной (дуальной) к данной решетке.

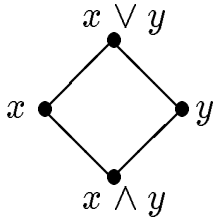
Лемма 5.1. *В любой решетке из* $a_1 \leq b_1$ *и* $a_2 \leq b_2$ *следует* $a_1 \vee a_2 \leq b_1 \vee b_2$, *и* $a_1 \wedge a_2 \leq b_1 \wedge b_2$.

Пример 5.4 . Частично упорядоченное множество подмножеств множества X есть полная решетка. В ней $A \vee B = A \cup B$, $A \wedge B = A \cap B$.

Пример 5.5 . Множество натуральных положительных чисел, упорядоченное так, как описано в примере 2, по делимости, есть решетка. В частности,

$n \vee m = \text{НОК}(n, m)$, $n \wedge m = \text{НОД}(n, m)$.

В некоторых случаях бывает полезно изображать решетку графически, в виде планарного графа, вершины которого — элементы решетки, а ребра (и маршруты) указывают на наличие отношения порядка. Принято изображать больший элемент расположенным выше меньшего элемента. Например, в простейшем случае рисунок выглядит так:



Лемма 5.2. *В любой решетке имеют место неравенства:*

(1) $x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$

(2) $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

(3) $x \leq z \implies x \vee (y \wedge z) \leq (x \vee y) \wedge z$

(4) $x \wedge (y \vee z) \leq x \vee y$

Теорема 5.2. *В решетке L эквивалентны условия:*
(для любых $x, y, z \in L$)

(D_1) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

(D_2) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

Определение 5.4. Решетка L, в которой для любых $x, y, z \in L$ выполняются тождества (D_1) и (D_2), называется дистрибутивной.

Решетка из примера 4 является дистрибутивной. Каждая подрешетка дистрибутивной решетки дистрибутивна.

Пример 5.6 . Любое линейно упорядоченное множество является дистрибутивной решеткой.

Теорема 5.3. *В решетке L равносильна выполнимость следующих условий для любых $x, y, z \in L$:*

(M_1) $x \leq z \Longrightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$

(M_2) $x \vee (y \wedge (x \vee z)) = (x \vee y) \wedge (x \vee z)$

(M_3) $x \wedge (y \vee (x \wedge z)) = (x \wedge y) \vee (x \wedge z)$

(M_4) $(x \vee y) \wedge z = (x \vee (y \wedge (x \vee z))) \wedge z$

(M_5) $(x \wedge y) \vee z = (x \wedge (y \vee (x \wedge z))) \vee z$

(M_6) $(x \vee (y \wedge z)) \wedge (y \vee z) = (x \wedge (y \vee z)) \vee (y \wedge z)$

(M_7) *Из $x \leq z$, $x \vee y = z \vee y$ и $x \wedge y = z \wedge y$ следует $x = z$.*

Определение 5.5. Решетка L, в которой для любых $x, y, z \in L$ выполняются равносильные соотношения из предыдущей теоремы, называется модулярной. Другое (устаревшее) название — дедекиндова структура.

Каждая подрешетка модулярной решетки модулярна.

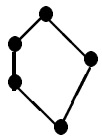
Теорема 5.4. *Каждая дистрибутивная решетка модулярна.*

Пример 5.7 . Пусть L — множество всех подпространств векторного пространства V (или множество всех подмодулей модуля, или множество всех идеалов кольца). Отношение частичного порядка на L определяется так: $A \leq B$ тогда и только тогда, если $A \subseteq B$. Тогда L — решетка, причем $A \vee B = A + B$, $A \wedge B = A \cap B$. Эта решетка модулярна. А именно, справедливо свойство: если $A \subseteq C$, то

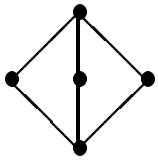
$$A + (B \cap C) = (A + B) \cap C$$

Эта решетка не обязательно дистрибутивна. Контрпример таков. Пусть V — двумерное векторное пространство, A, B, C — различные одномерные подпространства. Тогда $A+B = A+C = B+C = V$, $A \cap B = A \cap C = B \cap C = \{0\}$. Значит, $A \vee (B \wedge C) = A$, $(A \vee B) \wedge (A \vee C) = V$.

Теорема 5.5. *Решетка модулярна тогда и только тогда, если не содержит подрешетки, изоморфной "пентагону" (см. рисунок).*



Теорема 5.6. *Модулярная решетка дистрибутивна тогда и только тогда, если не содержит подрешетки, изоморфной диаманту (ромбу).*



Заметим, что в примере 7 подрешетка из элементов $V \supset A, B, C \supset \{0\}$ — это как раз и есть диамант.

Если дано множество решеток $\{L_i \mid i \in I\}$, то можно определить их прямое произведение $\prod\limits_{i \in I} L_i$ точно так же, как это делается для полугрупп (поскольку операции $\vee$ и $\wedge$ определяют на каждом сомножителе структуру полугруппы). Например, для произведения двух решеток, L_1 и L_2, операции в $L_1 \times L_2$ таковы:

$$(x_1, y_1) \vee (x_2, y_2) = (x_1 \vee x_2, y_1 \vee y_2), (x_1, y_1) \wedge (x_2, y_2) = (x_1 \wedge x_2, y_1 \wedge y_2)$$

В частности, $(x_1, y_1) \leq (x_2, y_2)$ тогда и только тогда, если одновременно $x_1 \leq x_2$ и $y_1 \leq y_2$.

Произведение дистрибутивных решеток есть дистрибутивная решетка, произведение модулярных — модулярная.

Определение 5.6. Пусть L и P - решетки. Отображение $f : L \longrightarrow P$ называется гомоморфизмом решеток, если $f(x \vee y) = f(x) \vee f(y)$, $f(x \wedge y) = f(x) \wedge f(y)$ для любых $x, y \in L$. Изоморфизм решеток — это гомоморфизм, являющийся биективным отображением . Отображение , обратное к изоморфизму, конечно же, гомоморфизизм.

Пример 5.8 . Решетка L целых положительных чисел, упорядоченных отношением делимости (см. примеры 2 и 5) допускает инъективный гомоморфизм в произведение счетного семейства копий решетки $\mathbf{N}$ целых неотрицательных чисел с обычным отношением порядка. Этот порядок линейный, так что $\mathbf{N}$ — дистрибутивная решетка. Таким образом, решетка примера 5, как изоморфная подрешетке прямого произведения дистрибутивных решеток, сама дистрибутивна. Гомоморфизм

строится так. Каждое неотрицательное целое $n \in L$ допускает однозначное разложение вида $n = \prod\limits_{i=1}^{\infty} p_i^{k_i}$, где p_i — все различные простые числа, и почти все k_i равны нулю. Числу n сопоставляется счетная последовательность $(k_1, k_2, \ldots) \in \prod\limits_{i=1}^{\infty} \mathbf{N}$. Если $m = \prod\limits_{i=1}^{\infty} p_i^{l_i}$, то

$$n \vee m = \text{НОК}(n, m) = \prod_{i=1}^{\infty} p_i^{\max(k_i, l_i)}, \quad n \wedge m = \text{НОД}(n, m) = \prod_{i=1}^{\infty} p_i^{\min(k_i, l_i)}$$

По определению произведения решеток,

$$(k_1, k_2, \ldots) \vee (l_1, l_2, \ldots) = (\max(k_1, l_1), \max(k_2, l_2), \ldots),$$
$$(k_1, k_2, \ldots) \wedge (l_1, l_2, \ldots) = (\min(k_1, l_1), \min(k_2, l_2), \ldots).$$

Это означает, что при отображении L в произведение точные верхние грани переходят в точные верхние грани, а точные нижние — в точные нижние. Таким образом, отображение $n \mapsto (k_1, k_2, \ldots)$ — гомоморфизм решеток. Его инъективность следует из однозначности разложения на простые сомножители.

Теорема 5.7. *Дистрибутивность решетки эквивалентна следующему свойству.*

Для любых $x, y, z \in L$ *из* $x \wedge y = z \wedge y$ *и* $x \vee y = z \vee y$ *следует* $x = z$.

Элемент решетки a называется неразложимым, если из $a = b \vee c$ всегда следует $a = b$ или $a = c$. Пусть P — частично упорядоченное множество. Подмножество $Z \subseteq P$ называется наследственным, если из $x \in Z$ и $y \leq x$ следует $y \in Z$.

Теорема 5.8. (Строение конечных дистрибутивных решеток). *Имеют место изоморфизмы*

$$L \cong H(J(L))$$

$$P \cong J(H(P))$$

где L — конечная дистрибутивная решетка, P — конечное частично упорядоченное множество, $J(L)$ — множество неразложимых элементов L (кроме нуля) , которое является частично упорядоченным, $H(P)$ — множество всех наследственных подмножеств P .

Следствие 5.1. *Конечная решетка дистрибутивна тогда и только тогда, если она изоморфна подрешетке решетки всех подмножеств конечного множества.*

6. Булевы и гейтинговы алгебры.

Определение 6.1. Дополнением элемента x в решетке L с нулем и единицей называется такой элемент $y \in L$, что $x \vee y = 1$, $x \wedge y = 0$.

В дистрибутивной решетке дополнение элемента (если оно существует) определено однозначно.

Определение 6.2. Булева алгебра B — это дистрибутивная решетка с нулем и единицей, в которой каждый элемент обладает дополнением.

Дополнение элемента x в булевой алгебре обозначается через x' .

Теорема 6.1. (Свойства операции дополнения). *Для элементов x, y из булевой алгебры B всегда имеют место следующие факты:*

1) $x'' = x$ 2) $(x \wedge y)' = x' \vee y'$

3) $(x \vee y)' = x' \wedge y'$ 4) $x \leq y \quad \Leftrightarrow \quad x' \geq y'$

5) $x \leq y \quad \Leftrightarrow \quad x' \vee y = 1 \quad \Leftrightarrow \quad x \wedge y' = 0$

Примеры булевых алгебр.

Пример 6.1 . Булевой алгеброй является множество всех подмножеств $Pow(X)$ произвольного множества X . Как уже отмечалось выше, это дистрибутивная решетка с нулем $\emptyset$ и единицей X . Дополне-

ние элемента $A \in Pow(X)$ есть теоретико-множественное дополнение $A \subseteq X$, то есть $A' = X \setminus A$.

Пример 6.2 . Рассмотрим множество $X = \{0, 1\}$ и множество B_n всех отображений из X^n в X , где $n \geq 0$ фиксировано. Структура булевой алгебры на B_n определяется следующим образом:

$$(f \vee g)(x_1, \ldots, x_n) = \max(f(x_1, \ldots, x_n), g(x_1, \ldots, x_n)),$$
$$(f \wedge g)(x_1, \ldots, x_n) = \min(f(x_1, \ldots, x_n), g(x_1, \ldots, x_n)),$$
$$f'(x_1, \ldots, x_n) = 1 - f(x_1, \ldots, x_n).$$

Атомом в решетке с нулем L называется такой элемент $a \in L$, для которого из $0 \leq x \leq a$ следует $x = 0$ или $x = a$.

Теорема 6.2. (М.Стоун). *Любая конечная булева алгебра изоморфна булевой алгебре всех подмножеств множества своих атомов.*

Булевым кольцом называется ассоциативное коммутативное кольцо с единицей, в котором для любого элемента x имеют место равенства $x + x = 0$, и $x^2 = x$.Фактически достаточно потребовать , чтобы для каждого x имело место $x^2 = x$. Тогда $x + x = (x + x)^2 = xx + xx + xx + xx = x + x + x + x$, откуда следует $x + x = 0$, то есть $x = -x$. Кроме того, $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$, что влечет $xy + yx = 0$, то есть $xy = -yx = yx$.

Теорема 6.3. *Существует взаимно-однозначное соответствие между булевыми алгебрами и булевыми кольцами, задаваемое следующим образом. Любая булева алгебра превращается в булево кольцо, если определить операцию умножения $x \cdot y = x \wedge y$, и сложения $x + y = (x' \wedge y) \vee (x \wedge y')$. Обратно, любое булево кольцо становится булевой алгеброй, если положить $x \wedge y = x \cdot y$, $x \vee y = x + y + x \cdot y$, $x' = x + 1$.*

В частности, булева алгебра $Pow(X)$ превращается в ассоциативное кольцо с умножением $A \cdot B = A \cap B$, и сложением $A + B = A \triangle B$ (операция симметрической разности множеств).

Определение 6.3. Относительное псевдодополнение элемента a относительно b, обозначаемое $a \to b$, определяется следующим образом: это точная верхняя грань всех тех x, для которых $x \wedge a \leq b$. Иными словами,

$$x \leq (a \to b) \quad \Leftrightarrow \quad x \wedge a \leq b$$

Довольно часто в конкретных примерах существуют точные верхние грани для произвольных семейств элементов, причем

$$(\bigvee_{i \in I} x_i) \wedge y = \bigvee_{i \in I} (x_i \wedge y),$$

и тогда

$$(a \to b) = \bigvee_{x, x \wedge a \leq b} x$$

Определение 6.4. Алгеброй Гейтинга (или гейтинговой алгеброй, или псевдобулевой алгеброй) называется дистрибутивная решетка с нулем и единицей, в которой относительные псевдодополнения $a \to b$ существуют для любых a и b.

Примеры алгебр Гейтинга:

Пример 6.3 . Любая булева алгебра. При этом $(a \to b) = a' \vee b$.

Пример 6.4 . Любая конечная дистрибутивная решетка L. В ней существуют любые точные верхние и нижние грани.

Пример 6.5 . Множество открытых подмножеств топологического пространства X — алгебра Гейтинга. Операции взятия точной верхней и нижней граней — объединение и пересечение множеств, отношение порядка задается включением. Если $Int(A) \subseteq A$ есть внутренность подмножества $A \subseteq X$, то есть наибольшее открытое множество,

содержащееся в A, то $A \to B$ есть $Int((X \backslash A) \cup B)$. При доказательстве этого можно использовать свойства операции взятия внутренности: 1) $Int(X) = X$; 2) $Int(A) \subseteq A$; 3) $A \subseteq B \;\Rightarrow\; Int(A) \subseteq Int(B)$; 4) $Int(A \cap B) = Int(A) \cap Int(B)$; 5) $Int(Int(A)) = Int(A)$. Согласно одной теореме М. Стоуна, любая алгебра Гейтинга изоморфна подалгебре алгебры открытых подмножеств некоторого топологического пространства.

Лемма 6.1. *В любой алгебре Гейтинга выполняются следующие соотношения:*

1) $a \wedge b = (a \to b) \wedge a \leq b \leq (a \to b)$
2) $(\vee_{i \in I}\ x_i) \wedge a = \vee_{i \in I}\,(x_i \wedge a)$
3) $(a \to \wedge_{i \in I}\ b_i) = \wedge_{i \in I}\,(a \to b_i)$
4) $a \leq b \;\Leftrightarrow\; (a \to b) = 1$
5) $(a \to 1) = 1\ ,\ (1 \to b) = b\ ,\ (0 \to a) = 1$
6) $(a \to b) \wedge (b \to c) \leq (a \to c)$
7) $(a \to c) \wedge (b \to c) = (a \vee b \to c)$
8) $a_1 \leq a_2 \;\Rightarrow\; (a_1 \to b) \geq (a_2 \to b)$
9) $b_1 \leq b_2 \;\Rightarrow\; (a \to b_1) \leq (a \to b_2)$
10) $(a \to (b \to c)) = (a \wedge b \to c) = (b \to (a \to c))$

Положим $\neg x = (x \to 0)$. Это можно назвать "отрицанием" или "дополнением" элемента x. В булевой алгебре $\neg x = x'$.

Лемма 6.2. *В любой алгебре Гейтинга выполнены следующие соотношения:*

1) $a \leq b \;\Rightarrow\; \neg a \geq \neg b$
2) $x \wedge \neg x = 0$
3) $x \leq \neg\neg x$
4) $\neg x = \neg\neg\neg x$
5) $\neg a \vee b \leq (a \to b)$
6) $\neg(a \vee b) = (\neg a) \wedge (\neg b)$
7) $(\neg a) \vee (\neg b) \leq \neg(a \wedge b)$

Пример 6.6 . Пример алгебры Гейтинга, не являющейся булевой алгеброй – отрезок $I = [0,1]$, в котором $\sup = \max$, $\inf = \min$. Относительные псевдодополнения существуют и вычисляются так:

$$(x \to y) = \begin{cases} 1 & \text{, если } x \leq y, \\ y & \text{, если } x > y. \end{cases}$$

В частности, $\neg x = 1$ при $x = 0$, а при $x \neq 0$ $\neg x = 0$. Отсюда следует, что $\neg\neg x = x$ только при $x = 0$ или $x = 1$, в остальных же случаях $\neg\neg x = 1$.

Теорема 6.4. (Критерий булевости). *Алгебра Гейтинга H булева тогда и только тогда, если выполнено любое из эквивалентных условий:*

(B_1) $\neg\neg a = a$ *для всех* $a \in H$;

(B_2) $(a \to b) = \neg a \vee b$ *для всех* $a, b \in H$.

Отсюда следует, что алгебра Гейтинга $I = [0,1]$ не является булевой.

ЛИТЕРАТУРА

1. Шафаревич И.Р. Основные понятия алгебры // Современные проблемы математики. Фундаментальные направления. Т. 11. (Итоги науки и техники ВИНИТИ АН СССР). М., 1985. С. 5–288.

2. Ленг С. Алгебра. –М.: Мир,1968.

3. Бахтурин Ю.А. Основные структуры современной алгебры. – М.:Наука,1990.

4. Ван-дер-Варден Б.Л. Алгебра. – М.:Наука, 1976.

5. Кон П. Универсальная алгебра. –М.:Мир, 1968.

6. Курош А.Г. Лекции по общей алгебре. –М.:Наука,1973.

7. Скорняков Л.А. Элементы общей алгебры.– М.:Наука,1983.

8. Скорняков Л.А. Элементы алгебры.– М.:Наука,1986.

9. Кострикин А.И. Введение в алгебру. – М.: Наука, 1977.

10. Фейс К. Алгебра: кольца, модули и категории. Том 1. – М.:Мир,1977.

11. Каш Ф. Модули и кольца. – М.:Мир, 1981.

12. Ламбек И. Кольца и модули. – М.: Мир,1971.

13. Гретцер Г. Общая теория решёток. – М.:Наука,1982.

14. Биркгоф Г. Теория решеток.–М.:Наука,1984.

15. Расёва Е., Сикорский Р. Математика метаматематики. –М.:Наука, 1972.

16. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. – М.: Мир, 1987.

18. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. 3-е изд. – М.: Наука, 1982.

19. Общая алгебра. Том 1. / Под общ. ред. Л.А. Скорнякова. – М.: Наука, 1990. – 592 с.

20. Общая алгебра. Том 2. / Под общ. ред. Л.А. Скорнякова. – М.: Наука, 1991. – 480 с.