Министерство образования и науки России
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Казанский национальный исследовательский
технологический университет»

Л. В. Веселова, О. Е. Тихонов

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Учебное пособие

ISBN 978-5-7882-1636-2

УДК 51(075.8)

Веселова Л.В.

Алгебра и теория чисел: учебное пособие / Л.В. Веселова, О.Е. Тихонов; М-во образ. и науки России, Казан. нац. исслед. технол. ун-т. – Казань : Изд-во КНИТУ, 2014.

ISBN 978-5-7882-1636-2

Изложены основы теории чисел и линейной алгебры. Теоретический материал приведен с доказательствами и иллюстрируется примерами. Даны расчетные задания и вопросы для проверки остаточных знаний по теме «Общая алгебра».

Предназначено для студентов, обучающихся по специальности «Математическое обеспечение и администрирование информационных систем».

Издается по решению редакционно-издательсткого совета Казанского национального исследовательского технологического университета.

Рецензенты: канд. физ.-мат. наук, доцент каф. алгебры и матем. логики К(П)ФУ *Ю.А. Альпин*,
д-р физ.-мат. наук, проф. каф. вычисл. матем. К(П)ФУ, член-кор. АН РТ *И.Б. Бадриев*

Текстовое электронное издание

Минимальные системные требования:
- Windows: процессор Intel 1,3 Гц или аналогичный;
  Microsoft Windows XP Service Pack 2
  128 МБ оперативной памяти
- MacOS: процессор PowerPC G4 или Intel
  MacOS X 10.5
  128 МБ оперативной памяти
- Linux: 32-разрядный процессор Intel Pentium или аналогичный
  SUSE Linux Enterprise Desktop 10 или Ubuntu 7.10; GNOME или KDE Desktop Enviroment

Ответственный за выпуск О.М. Дегтерева

Подписано к использованию 15.10.2014
Объем издания 2,66 Мб «С» 132
Издательство Казанского национального исследовательского технологического университета
420015, Казань, К.Маркса, 68

Оглавление

Введение

Натуральные числа возникли на заре цивилизации в результате счета предметов, в наше время дети знают их уже в дошкольном возрасте. Естественно возникающие операции сложения и умножения не выходят за рамки натуральных чисел, однако обратные операции: вычитание и деление уже заставляют нас вводить новые числа: целые и дробные. С развитием понятия числа стало ясно, что операции над числами имеют общие свойства. Именно эти свойства постулированы в определениях групп, колец и полей. Общая алгебра является скелетом, на котором держится вся математика в целом, связующим звеном между различными математическими дисциплинами.

Данный курс построен так, что через весь курс красной нитью проходят такие понятия общей алгебры, как группы, кольца, поля. Часть линейной алгебры рассматривается над произвольными полями и лишь евклидово пространство – только над полем действительных чисел. Последнее связано с недостаточным количеством часов, отводимых на данный курс в техническом вузе. Также в связи с этим обстоятельством в курсе опущен ряд доказательств, в частности доказательство основной теоремы алгебры. Курс алгебры написан в терминологии конечномерного функционального анализа и может быть использован для обучения студентов математических специальностей университетов.

Теория чисел долгое время считалась чистейшей областью математики – искусством ради искусства. Теория чисел в двадцатом веке считалась настолько бесполезной для народного хозяйства, что в 1970–80 годы курс теории чисел не читался даже на математических специальностях университетов, но оказалось, что эта «ненужная в хозяйстве» теория нашла столько применений, что сейчас этот курс даже входит в программу некоторых специальностей технических университетов. Линейная алгебра, напротив, всегда считалась одной из основных математических дисциплин и применялась как в механике и физике, так и экономике.

Читая курс «Алгебра и теория чисел» студентам первого курса специальности математическое обеспечение и администрирование информационных систем Казанского национального исследовательского университета, автор столкнулся с тем фактом, что немногочисленные имеющиеся учебники по теории чисел предназначены для студентов старших курсов математических специальностей университетов, а следовательно, для более подготовленной аудитории. В связи с этим данное пособие адаптировано для студентов младших курсов технических вузов и претендует более на доступность, чем на полноту изложения. В пособии приведены вопросы по проверке остаточных знаний студентов по теме общая и линейная алгебра. В пособии содержатся все необходимые сведения для ответов на эти вопросы.

§ 1. Основные алгебраические структуры

Вспомним, какие мы знаем числа, как и откуда они появились. Представим себе, что мы находимся в первобытной общине и не умеем считать. Предположим, что охотники нашего племени Острый глаз и Верная рука после удачной охоты на мамонтов решили выяснить кто из них лучший охотник.

Верная рука убил вот столько 0 0 0 0 мамонтов, а
Острый глаз убил вот столько 0 0 0 мамонтов.

Так кто из них сегодня лучший охотник?

Таким образом, вначале возникло не понятие равенства, а понятие сравнения. Но в один прекрасный день они пошли на охоту и принесли одинаковое количество мамонтов (или не мамонтов). Каждому мамонту (или не мамонту) охотника Острый глаз соответствовал мамонт (или не мамонт) охотника Верная рука. Как вы наверное уже поняли, мамонты здесь ни при чем, а при чем взаимно однозначное соответствие между элементами двух множеств. Именно это взаимно однозначное соответствие между элементами множеств и лежит в основе понятия натурального числа. Название натуральные числа показывает происхождение этих чисел из натурального сравнения мамонтов (или не мамонтов). Через $\mathbf{N}=\{1, 2, 3, \ldots\}$ будем обозначать множество натуральных чисел. После того как мы научились считать предметы нам захотелось узнать сколько мамонтов убили оба охотника вместе. Так естественным образом возникла операция сложения натуральных чисел, кстати, обладающая некоторыми очень хорошими свойствами:

1) $a+b=b+a$ – коммутативность,

2) $a+(b+c)=(a+b)+c$ – ассоциативность.

Также нам захотелось сравнить на сколько больше мамонтов (или не мамонтов) убил один охотник по сравнению с другим. Таким образом в противовес операции сложения возникла операция вычитания. Но тут возникла проблема: при вычитании из меньшего числа большего результат уже не является натуральным числом. Это наводит на мысль о расширении множества натуральных чисел с сохранением введенных операций и их свойств. Через $\mathbf{Z}=\{\ldots, -2, -1, 0, 1, 2,\ldots\}$ обозначим множество целых чисел. Отметим особую роль числа 0 относительно операции сложения:

> Для любого натурального числа a имеем: $a + 0 = a$. При этом отрицательное число $-a$ можно рассматривать как обратный элемент к положительному a: $a +(-a)=0$.

На множестве **Z** можно также ввести еще одну операцию – умножение, также обладающую очень хорошими свойствами:

1) $ba= ab$ – коммутативность,

2) $a(bc)=(ab)c$ – ассоциативность,

а также хорошим свойством, связывающим между собой операции сложения и умножения:

3) $a(b+c)=ab+ac$ – дистрибутивность.

Отметим также особую роль числа 1 по отношению к операции умножения: $1\cdot a = a\cdot 1 = a$. Не правда ли, похоже на роль 0 по отношению к операции сложения. Однако, обратный элемент по умножению к целому числу не является целым числом, что ведет нас к введению новых чисел – рациональных дробей. Обозначим:

$\mathbf{Q} = \{\frac{n}{m} : n \in \mathbf{Z},\ m \in \mathbf{N}\}$ – множество рациональных чисел.

Через $\boldsymbol{R}$ обозначим множество всех действительных чисел, которое можно рассматривать как совокупность всевозможных (в том числе бесконечных непериодических) десятичных дробей. Отметим, что во всех введенных множествах сохраняются естественные операции сложения и умножения, а также и их свойства. Теперь введем основные определения, обобщающие рассмотренные примеры.

Определение 1.1. *Группой* называется множество G с одной групповой операцией "$*$", обладающей следующими свойствами:

1) $\forall\, a \in \mathrm{G}, b \in \mathrm{G} \Rightarrow a * b \in \mathrm{G}$,

2) $\forall\, a \in \mathrm{G}, b \in \mathrm{G}, c \in \mathrm{G} \Rightarrow a *(b * c)=(a * b) * c$,

3) $\exists\ 1 \in \mathrm{G} :\ a * 1 = 1 * a = a$ для всех $a \in \mathrm{G}$,

4) $\forall\ a \in G\ \exists\ a^{-1} \in G$: $a * a^{-1} = a^{-1} * a = 1$.

При этом элемент 1 называется *единицей* группы, а элемент a^{-1} называется *обратным элементом* к элементу a по групповой операции "$*$".

Определение 1.2. Группа называется *коммутативной*, если групповая операция коммутативна.

Очевидно, что множество натуральных чисел не является группой ни по сложению, ни по умножению, так как не выполнено свойство 4).

Множество целых чисел является коммутативной группой по сложению, но не является группой по умножению, опять-таки потому, что не выполнено свойство 4). Множества **Q** и **R** являются коммутативными группами по сложению, но не являются группами по умножению, так как для 0 нет обратного элемента по умножению.

Определение 1.3. Множество K называется *кольцом*, если оно является коммутативной группой по сложению со второй операцией – умножением, обладающей следующими свойствами:

1) $\forall\ a \in K, b \in K \Rightarrow ab = ba \in K$,

2) $\forall\ a \in K, b \in K, c \in K \Rightarrow a(bc) = (ab)c$,

3) $\forall\ a \in K, b \in K, c \in K \Rightarrow a(b+c) = ab + ac$.

Определение 1.4. Кольцо называется *кольцом с единицей*, если в нем есть единица по умножению (элемент кольца, умножение на который не меняет других элементов кольца).

Очевидно, что множество целых чисел является кольцом с единицей.

Определение 1.5. Множество P называется *полем*, если оно является кольцом с единицей, умножение в нем коммутативно и для любого ненулевого элемента поля существует обратный элемент по умножению:

$$\forall\ a \in P \setminus \{0\}\ \ \exists\ a^{-1} \in P:\ a \cdot a^{-1} = 1.$$

Определение 1.6. Подмножество G_1 группы G называется *подгруппой* группы G, если G_1 является группой с той же групповой операцией и той же единицей, что и G.

Определение 1.7. Подмножество $K_1 \subset K$ называется *подкольцом* кольца K, если K_1 является кольцом с такими же групповыми операциями и такими же единицей и нулем, что и K.

Определение 1.8. Подмножество $P_1 \subset P$ называется *подполем* поля P, если P_1 вляется полем с такими же групповыми операциями и таки-

ми же единицей и нулем, что и P. В таком случае поле P называется *расширением* поля P_1.

Очевидно, что **Z –** подкольцо **Q**, а **Q –** подполе **R**.

Определение 1.9. Ненулевые элементы *a, b* кольца K называются *делителями нуля*, если $ab=0$.

Теорема 1.1. Если кольцо является полем, то в нем нет делителей нуля.

Доказательство. Доказательство проведем от противного. Предположим, что существуют ненулевые элементы поля P a и b такие, что $ab=0$. Так как P – поле, то $\exists\ a^{-1} \in P$: $aa^{-1} = a^{-1}a = 1$. Тогда

$$a^{-1} \cdot 0 = a^{-1}ab = 1 \cdot b = b = 0,$$

что противоречит нашему предположению.

Задачи.

1. Выяснить обладают ли свойствами ассоциативности и коммутативности операции "$*$" на множестве A, если:

1) A=**N**, $x * y = x+2y$;
2) A=**N**, $x * y = 3xy$;
3) A=**N**, $x * y = x^y$;
4) A=**N**, $x * y = x^2 + y$;
5) A=**Z**, $x * y = x - y$;
6) A=**R**, $x * y = \sin x \cdot \cos y$.

2. Какие из числовых множеств являются группами относительно заданных операций:

1) множество степеней данного вещественного числа с целыми показателями относительно умножения;

2) множество рациональных чисел на интервале (0,1) относительно операции умножения;

3) множество положительных действительных чисел относительно операции умножения;

4) отрезок [0,1] относительно операции умножения;

5) отрезок [0,1] относительно операции $a * b = \{a+b\}$, где $\{a\}$- дробная часть числа a?

3. Доказать, что если в группе G выполнено условие $x * x = 1$ для всех элементов группы G, то группа коммутативна.

4. Доказать, что пересечение двух подгрупп группы будет подгруппой той же группы.

§ 2. Теория делимости

Определение 2.1. Пусть $a, b \in \mathbf{Z}$. Число a делится на число b (b является делителем числа a), если найдется такое число $c \in \mathbf{Z}$, что $a = c\,b$. Запись: $a \vdots b$.

Легко проверить следующее свойство делимости: пусть $a_1 + +a_2 + \ldots + a_n = c_1 + c_2 + \ldots + c_m$ – равенство сумм целых чисел. Если все слагаемые в этом равенстве кроме одного кратны b, то оставшееся слагаемое также кратно b.

Докажем это утверждение для простейшего случая. Пусть $a+b=c$, $a=da_1$, $b=db_1$, тогда $c=d(a_1+b_1)$.

Теорема 2.1. Для данного целого отличного от нуля числа b всякое целое число a единственным образом представимо в виде

$$a = bq + r,$$

где $0 \le r < |b|$. При этом число q называется неполным частным, а число r – остатком от деления a на b.

Доказательство. Приведем доказательство, принадлежащее древним грекам. Без ограничения общности будем считать a и b натуральными числами. Отложим отрезок длины a и уложим на него столько отрезков длины b сколько в него поместится. При этом оставшийся отрезок окажется длиной меньше b.

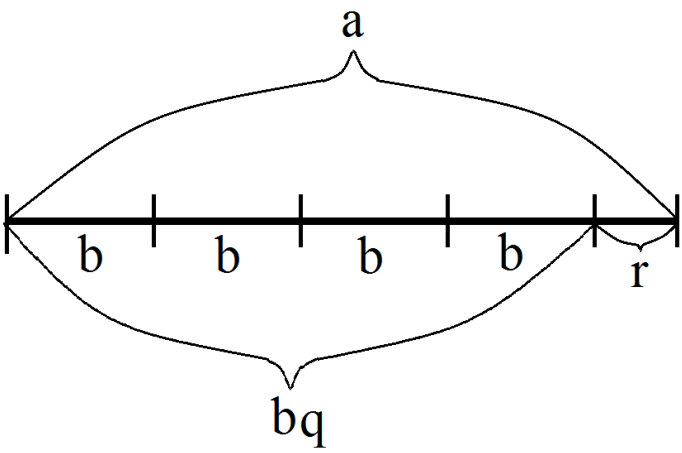

Рис. 1

Определение 2.2. Число $d \in \mathbf{Z}$, делящее одновременно числа $a_1, a_2, \ldots a_k \in \mathbf{Z}$ называется *общим делителем* этих чисел. Наибольшее число d с таким свойством называется *наибольшим общим делителем* чисел $a_1, a_2, \ldots a_k$. Обозначение $d = Н.О.Д.(a_1, \ldots a_k)$.

Определение 2.3. Целые числа a и b называются *взаимно простыми*, если $d = Н.О.Д.(a,b) = 1$.

Определение 2.4. Целые числа $a_1, \ldots a_k$ называются взаимно простыми, если $Н.О.Д.(a_1, \ldots a_k)=1$, попарно взаимно простыми, если для $\forall\, i,j, = \overline{1,k},\ i \neq j,\ Н.О.Д.(a_i, a_j) = 1$.

Например, числа 15, 18, 14 взаимно простые, но не попарно взаимно простые, так как Н.О.Д. (15, 18, 14)=1, но Н.О.Д. (15, 18)=3 и Н.О.Д. (18, 14)=2.

Свойства наибольшего общего делителя.

1. Если Н.О.Д. (*a*,*b*)=1, то Н.О.Д.(*ca*,*b*)=Н.О.Д.(*c*,*b*).
2. Если Н.О.Д. (*a*,*b*)=1, и *ac* делится на *b*, то *c* делится на *b*.
3. Если каждое из чисел $a_1, a_2, \ldots, a_n$ взаимно просто с каждым из чисел $b_1, b_2, \ldots, b_m$, то и произведение $a_1 a_2 \ldots a_n$ взаимно просто с произведением $b_1 b_2 \ldots b_m$.

Задача нахождения наибольшего общего делителя нескольких чисел сводится к нахождению наибольшего общего делителя двух чисел.

Чтобы найти $Н.О.Д.(a_1, \ldots a_n)$ надо найти $d_1 = Н.О.Д.(a_1, a_2)$, $d_2 =$ =Н.О.Д.(d_1,a_3), …, d_n =Н.О.Д. (d_{n-1} ,a_n .) Число d_n и будет наибольшим общим делителем чисел $a_1, \ldots a_n$.

Теорема 2.2. Если Н.О.Д.(*a*,*b*) = *d*, то найдутся такие целые числа *u* и *v*, что $au + bv = d$.

Доказательство. Рассмотрим множество P = {$au + bv \mid u,v \in \mathbf{Z}$ }. Очевидно, что *a*,*b*,0 ∈ P. Пусть *x*,*y* ∈ P и $y \neq 0$. Тогда остаток от деления *x* на *y* содержится в P. Действительно:

$x = yq + r, \quad 0 \leq r < y,$

$r = x - yq = au_1 + bv_1 - (au_2 - bv_2)q = (u_1 - u_2 q)a + (v_1 - v_2 q)b \in$ P.

Пусть *d* – наименьшее положительное число из P. Тогда *a* делится на *d*. Аналогичными рассуждениями получается, что *b* делится на *d*. Значит, *d* – общий делитель *a* и *b*. Для *d* есть представление в виде $d = au_0 + bv_0$. Если d_1 – другой общий делитель *a* и *b*, то d_1 делитель $au_0 + bv_0 = d$. Таким образом, *d* – наибольший общий делитель *a* и *b*.