

С. В. Ларин

# АЛГЕБРА: МНОГОЧЛЕННЫ

УЧЕБНОЕ ПОСОБИЕ  
ДЛЯ АКАДЕМИЧЕСКОГО БАКАЛАВРИАТА

2-е издание, исправленное и дополненное

*Рекомендовано Учебно-методическим отделом  
высшего образования в качестве учебного пособия  
для студентов высших учебных заведений, обучающихся  
по естественнонаучным направлениям*

Книга доступна в электронной библиотечной системе  
**biblio-online.ru**

Москва ■ Юрайт ■ 2019

УДК 511.2(075.8)  
ББК 22.132я73  
Л25

**Автор:**

**Ларин Сергей Васильевич** — кандидат физико-математических наук, профессор кафедры алгебры, геометрии и методики их преподавания Института математики, физики и информатики Красноярского государственного педагогического университета имени В. П. Астафьева.

**Ларин, С. В.**

Л25  
Алгебра: многочлены : учеб. пособие для академического бакалавриата / С. В. Ларин. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2019. — 136 с. — (Серия : Бакалавр. Академический курс).

ISBN 978-5-534-07825-1

В пособии изложен семестровый материал по многочленам в рамках дисциплины предметной подготовки «Алгебра и теория чисел» в соответствии с Федеральным государственным образовательным стандартом высшего образования, а также перечнем профессиональных компетенций, установленных в качестве обязательных. Данный материал обеспечивает выпускнику педагогического вуза способность осуществлять профессиональную деятельность в области преподавания соответствующих разделов алгебры.

В пособии рассмотрены теория делимости многочленов, вопросы, связанные с нахождением корней, многочлены от нескольких переменных, симметрические многочлены, результат и дискриминант. Большое внимание уделяется примерам. Они предваряют введение новых понятий, на них отрабатывается и закрепляется изученный материал.

*Для студентов математических специальностей педагогических вузов.*

УДК 511.2(075.8)  
ББК 22.132я73



*Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав. Правовую поддержку издательства обеспечивает юридическая компания «Дельфи».*

ISBN 978-5-534-07825-1

© Ларин С. В, 2008  
© Ларин С. В, 2018, с изменениями  
© ООО «Издательство Юрайт», 2019

# Оглавление

Предисловие .....	7
<b>Глава 1. Многочлены над областью целостности .....</b>	<b>9</b>
1.1. Основные понятия теории многочленов .....	9
1.1.1. Многочлены, их сложение и умножение .....	9
1.1.2. Уточнение понятия многочлена .....	13
1.1.3. Кольцо многочленов $\mathbb{Z}_p[x]$ .....	14
<i>Контрольные вопросы</i> .....	17
<i>Задачи</i> .....	17
1.2. Деление многочлена на двучлен. Корни многочлена .....	18
1.2.1. Схема Горнера .....	18
1.2.2*. Обобщение схемы Горнера .....	19
1.2.3. Корни многочлена .....	20
1.2.4. Примеры задач, решаемых с помощью схемы Горнера .....	22
1.2.5*. Корни многочленов кольца $\mathbb{Z}_p[x]$ .....	25
1.2.6. Многочлен как функция .....	26
<i>Контрольные вопросы</i> .....	27
<i>Задачи</i> .....	27
<b>Глава 2. Теория делимости многочленов .....</b>	<b>29</b>
2.1. Делимость в кольце многочленов над областью целостности .....	29
2.1.1. Основные понятия теории делимости многочленов .....	29
2.1.2. Наибольший общий делитель двух многочленов .....	30
<i>Контрольные вопросы</i> .....	31
<i>Задачи</i> .....	32
2.2. Делимость многочленов над полем .....	32
2.2.1. Деление с остатком в кольце многочленов над полем ...	32
2.2.2. Алгоритм Евклида .....	35
2.2.3. Взаимно простые многочлены .....	38
<i>Контрольные вопросы</i> .....	39
<i>Задачи</i> .....	40

2.3. Разложение на множители в кольце многочленов	
над полем .....	40
2.3.1. Неприводимые многочлены .....	40
2.3.2. Основные свойства неприводимых над данным полем многочленов .....	41
2.3.3. Разложение многочлена в произведение неприводимых множителей .....	42
2.3.4. Кратные неприводимые множители .....	44
2.3.5. Алгоритм отделения кратных множителей .....	46
2.3.6. Представление отношений многочленов в виде суммы простейших дробей .....	49
2.3.7*. Поле отношений кольца многочленов .....	54
Контрольные вопросы .....	57
Задачи .....	57

### **Глава 3. Многочлены над числовыми кольцами и полями..... 59**

3.1. Многочлены над полем комплексных чисел .....	59
3.1.1. Основная теорема алгебры. Неприводимые многочлены над полем комплексных чисел .....	59
3.1.2. Формулы Виета .....	60
Контрольные вопросы .....	62
Задачи .....	62
3.2. Многочлены над полем действительных чисел .....	63
3.2.1. Неприводимые многочлены над полем действительных чисел .....	63
3.2.2. Границы действительных корней многочлена с действительными коэффициентами .....	65
3.2.3. Отделение действительных корней многочлена методом Штурма .....	66
Контрольные вопросы .....	73
Задачи .....	74
3.3. Кольца многочленов $\mathbb{Q}[x]$ и $\mathbb{Z}[x]$ .....	75
3.3.1. Нахождение рациональных корней многочлена с целыми коэффициентами .....	75
3.3.2. Неприводимые многочлены в кольцах $\mathbb{Q}[x]$ и $\mathbb{Z}[x]$ .....	78
3.3.3. Разложение на множители в кольце $\mathbb{Z}[x]$ .....	81
Контрольные вопросы .....	84
Задачи .....	84
3.4. Общие приемы решения уравнений 3-й и 4-й степеней .....	85
3.4.1. Преобразования общего уравнения третьей степени .....	85
3.4.2. Корни уравнения $x^3 - 1 = 0$ .....	86

3.4.3. Корни уравнения $x^3 - a = 0$ .....	86
3.4.4. Корни уравнения $x^3 + px + q = 0$ .....	86
3.4.5. Корни уравнения $x^3 + px + q = 0$ с действительными коэффициентами .....	88
3.4.6. Решение уравнений четвертой степени методом Феррари.....	91
<i>Контрольные вопросы</i> .....	93
<i>Задачи</i> .....	93
<b>Глава 4. Многочлены от нескольких переменных .....</b>	<b>95</b>
4.1. Основные понятия.....	95
4.1.1. Построение кольца многочленов от нескольких переменных .....	95
4.1.2. Лексикографическое упорядочение многочленов.....	96
<i>Контрольные вопросы</i> .....	98
<i>Задачи</i> .....	98
4.2. Симметрические многочлены .....	99
4.2.1. Элементарные симметрические многочлены.....	99
4.2.2. Леммы о симметрических многочленах .....	100
4.2.3. Основная теорема о симметрических многочленах....	103
<i>Контрольные вопросы</i> .....	106
<i>Задачи</i> .....	106
4.3. Некоторые приложения теории симметрических многочленов .....	107
4.3.1. Симметрические многочлены и формулы Виета .....	107
4.3.2. Степенные суммы и формулы Ньютона .....	108
4.3.3. Решение систем двух симметрических уравнений с двумя неизвестными .....	110
4.3.4. Решение некоторых иррациональных уравнений .....	111
<i>Контрольные вопросы</i> .....	112
<i>Задачи</i> .....	113
4.4. Основная теорема алгебры.....	114
4.4.1. Краткая историческая справка .....	114
4.4.2. Доказательство основной теоремы алгебры.....	115
4.4.3*. Существование поля разложения данного многочлена .....	119
<i>Контрольные вопросы</i> .....	121
<i>Задачи</i> .....	121
4.5. Результант и дискриминант .....	122
4.5.1. Результант двух многочленов .....	122

4.5.2. Исключение неизвестного из системы двух уравнений с двумя неизвестными при помощи результата .....	124
4.5.3. Дискриминант многочлена .....	127
<i>Контрольные вопросы</i> .....	128
<i>Задачи</i> .....	128
<b>Список литературы</b> .....	<b>130</b>
<b>Новые издания по дисциплине «Высшая математика» и смежным дисциплинам</b> .....	<b>132</b>
<b>Предметный указатель</b> .....	<b>135</b>

## Предисловие

Учебное пособие адресовано в первую очередь студентам математических специальностей педагогических вузов и содержит материал семестрового курса по многочленам в рамках дисциплины «Алгебра» («Алгебра и теория чисел»). Вместе с тем изложение имеет целостный, замкнутый характер и может быть использовано всеми желающими для первичного знакомства с многочленами как в плане теории, так и в плане вычислительных приложений.

Многочлены от одной переменной рассматриваются с точки зрения теории делимости и с точки зрения нахождения корней. В теории многочленов от нескольких переменных центральное место занимает теория симметрических многочленов. С использованием основной теоремы о симметрических многочленах приводится «самое алгебраическое» доказательство основной теоремы алгебры, в котором четко указывается момент использования свойства непрерывности системы действительных чисел.

При доказательстве теоремы о делении с остатком рассматривается школьный алгоритм деления «уголком» многочлена на многочлен. Школьный аспект присутствует при освещении разложения многочленов на множители, формул Виета, вопросов нахождения рациональных корней многочленов с целыми коэффициентами, приложений симметрических многочленов. Так что пособие может оказаться полезным школьным учителям математики. Стремясь избежать излишней формализации, мы формальные обоснования отодвигаем на конец изложения соответствующего материала.

Отметим основополагающую роль примеров. Они не только иллюстрируют теоретические положения, но и подготавливают введение новых понятий. Зачастую доказательства теорем повторяют в общем виде те же рассуждения, которые накануне проводились при решении конкретных числовых примеров.

В результате усвоения изложенного материала студент должен приобрести следующие компетенции:

**знать**

- формулировки определений основных понятий и теорем;
- основные операции с многочленами;

**уметь**

- доказывать основные теоремы о многочленах;
- решать задачи, связанные с многочленами;
- находить корни многочлена;
- производить разложение многочлена на множители;

**владеть**

- вычислительными алгоритмами;
- применением теории многочленов к решению вычислительных задач.

В конце каждого из основных пунктов приведены «Контрольные вопросы» и «Задачи», которые призваны проверить и закрепить полученные знания. Контрольные вопросы чаще всего приведены не в тривиальной форме типа «что называется» или «как формулируется», а с некоторой изобретательностью, позволяющей выявить владение знаниями.

В тексте используются значки:  $:$  (делится),  $\Leftrightarrow$  (тогда и только тогда, когда),  $\Rightarrow$  (отсюда следует),  $(\Rightarrow)$  — доказательство необходимости,  $(\Leftarrow)$  — доказательство достаточности. Знаком \* отмечены пункты дополнительного материала.

Автор выражает благодарность доктору физико-математических наук, профессору М. М. Глухову, доктору физико-математических наук, профессору Б. В. Яковлеву, а также рецензентам доктору физико-математических наук, профессору В. М. Левчуку и доктору физико-математических наук, профессору Н. Н. Осипову за ряд ценных советов и замечаний.



# Глава 1

## МНОГОЧЛЕНЫ НАД ОБЛАСТЬЮ ЦЕЛОСТНОСТИ

### 1.1. Основные понятия теории многочленов

#### 1.1.1. Многочлены, их сложение и умножение

Нашей ближайшей целью является уточнение понятия многочлена. На базе школьных знаний приведем примеры многочленов:  $3x^2 - 2x + 5$  — многочлен степени 2 с целыми коэффициентами,  $x^3 + \frac{2}{3}x + 5$  — многочлен степени 3 с рациональными коэффициентами,  $0x^3 + \sqrt{2}x - 7$  — многочлен первой степени с действительными коэффициентами,  $-147$  — многочлен степени 0, наконец,  $0$  — нулевой многочлен. Уточним область значений для коэффициентов многочленов, которые мы будем рассматривать в дальнейшем. Начнем с определения базовых понятий.

**Определение 1.1.** *Кольцом* называется непустое множество  $K$  с определенными на нем бинарными операциями сложения и умножения, которые удовлетворяют следующим условиям:

1) сложение ассоциативно и коммутативно:  $(a + b) + c = a + (b + c)$  и  $a + b = b + a$  для любых  $a, b, c \in K$ ;

2) существует элемент  $0 \in K$ , называемый нулем, такой что  $a + 0 = a$  для любого  $a \in K$ ;

3) для всякого элемента  $a \in K$  существует элемент  $-a \in K$ , называемый противоположным для  $a$ , такой что  $a + (-a) = 0$ ;

4) умножение ассоциативно:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  для любых  $a, b, c \in K$ .

5) умножение дистрибутивно относительно сложения:  $(a + b) \cdot c = a \cdot c + b \cdot c$  и  $c \cdot (a + b) = c \cdot a + c \cdot b$  для любых  $a, b, c \in K$ .

Кольцо  $K$  называется *коммутативным*, если умножение в нем коммутативно:  $a \cdot b = b \cdot a$  для любых  $a, b \in K$ .

Кольцо  $K$  называется *кольцом с единицей*, если существует элемент  $1 \in K$ , называемый единицей, такой что  $a \cdot 1 = 1 \cdot a = a$ .

Элементы  $a, b \in K$  называются *делителями нуля*, если  $a \neq 0$ ,  $b \neq 0$ , но  $a \cdot b = 0$ . Если же в кольце нет таких элементов, то оно называется *кольцом без делителей нуля*.

**Определение 1.2.** *Поле* называется коммутативное кольцо  $P$  с единицей, отличной от нуля, в котором всякий ненулевой элемент имеет обратный, т.е. для любого  $0 \neq a \in P$  существует элемент  $a^{-1} \in P$ , такой что  $a \cdot a^{-1} = 1$ .

Глядя на кольцо целых чисел, введем обобщающее понятие.

**Определение 1.3.** *Область целостности* называется коммутативное кольцо с единицей, отличной от нуля, и без делителей нуля.

Примерами областей целостности являются кольцо целых чисел  $\mathbb{Z}$ , числовые поля  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ . Вообще, всякое поле является областью целостности. Не является областью целостности, например, кольцо четных целых чисел, поскольку не содержит единицы. Но многочлены с четными коэффициентами входят в область многочленов с любыми целыми коэффициентами, так что не выпадают из нашего рассмотрения. Не является областью целостности кольцо квадратных матриц, поскольку оно не коммутативно (хотя в линейной алгебре рассматриваются «значения многочленов от матриц»). Заметим, что нулевое кольцо — это единственное кольцо, в котором нуль равен единице. Оно не является областью целостности.

**Определение 1.4.** *Многочленом над областью целостности  $K$*  называется формальное выражение вида  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  (*стандартная запись многочлена*), где  $a_n, a_{n-1}, \dots, a_1, a_0$  являются элементами из  $K$  и называются *коэффициентами многочлена*, буква  $x$  обозначает *переменную* с областью определения  $K$ . Каждое слагаемое называется *членом многочлена*. Отсюда происходят названия «одночлен», «двучлен», «трехчлен». Слагаемое  $a_0$  называется *свободным членом* (он «свободен» от переменной  $x$ ). Кратко многочлен обозначается  $f(x)$ , а множество всех многочленов над областью целостности  $K$  обозначается  $K[x]$ . Если все коэффициенты многочлена равны нулю, то он называется *нулевым*. Если же в приведенной выше стандартной записи многочлена коэффициент  $a_n \neq 0$ , то он называется *старшим коэффициентом*, соответствующий одночлен  $a_n x^n$  называется *старшим членом многочлена*, а  $n$  называется *степенью многочлена*. Таким образом, нулевой многочлен — единственный многочлен без степени. Многочлен называется *приве-*

денным (или нормированным), если его старший коэффициент равен 1. Считаем, что  $x^0 = 1$ . По обыкновению, коэффициент  $\pm 1$  при переменной не записывают, считая  $\pm 1x^k = \pm x^k$ ,  $k = 1, 2, \dots$ .

Договоримся считать, что многочлен не изменится, если к нему приписать любое количество недостающих одночленов с нулевыми коэффициентами, а также исключить из записи такие одночлены. Таким образом, в записи многочлена  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  по умолчанию считаем, что  $0 = a_{n+1} = a_{n+2} = \dots$ . При этой договоренности можно сказать, что два многочлена равны (алгебраически), если равны их соответствующие коэффициенты.

Определим сложение многочленов:

$$(a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) + (b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0) = \\ = (a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + \dots + (a_1 + b_1) x + (a_0 + b_0).$$

Таким образом, чтобы сложить два многочлена, нужно сложить их соответствующие коэффициенты. В записи суммы двух многочленов слагаемые  $a_i x^i$  и  $b_i x^i$ ,  $i = 0, 1, \dots, n$ , называются подобными, а нахождение их суммы  $a_i x^i + b_i x^i = (a_i + b_i) x^i$  называется приведением подобных. Следовательно, сложение многочленов сводится к приведению подобных.

Заметим, что степень суммы многочленов не превосходит степени каждого из многочленов-слагаемых.

Определим умножение многочленов, положив

$$(a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0) \cdot (b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0) = \\ = c_{m+n} x^{m+n} + c_{m+n-1} x^{m+n-1} + \dots + c_1 x + c_0,$$

где  $c_k = a_k b_0 + a_{k-1} b_1 + \dots + a_1 b_{k-1} + a_0 b_k = \sum_{i+j=k} a_i b_j$  для  $k = 0, 1, \dots$  (на-

помним, что  $0 = a_{m+1} = a_{m+2} = \dots$ ,  $0 = b_{n+1} = b_{n+2} = \dots$ ). Если  $a_m \neq 0$  и  $b_n \neq 0$ , то  $c_{m+n} = a_m b_n \neq 0$ , поскольку в области целостности нет делителей нуля. При этом  $c_{m+n+1} = 0$ ,  $c_{m+n+2} = 0$ ,  $\dots$ . Отсюда делаем вывод, что степень произведения двух многочленов равна сумме степеней перемножаемых многочленов. Таким образом,

$$(a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0) \cdot (b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0) = \\ = a_m b_n x^{m+n} + (a_m b_{n-1} + a_{m-1} b_n) x^{m+n-1} + \dots + (a_1 b_0 + a_0 b_1) x + a_0 b_0.$$

В частности, для одночленов получаем

$$a_i x^i \cdot b_j x^j = a_i b_j x^{i+j}, i, j = 0, 1, \dots$$

Из определения подмечаем правило умножения многочленов: чтобы первый многочлен умножить на второй, нужно каждый член первого многочлена умножить на каждый член второго многочлена, записать сумму полученных одночленов и привести подобные.

**Теорема 1.1.** Множество всех многочленов  $K[x]$  над областью целостности  $K$  относительно сложения и умножения многочленов само является областью целостности.

*Доказательство.* Поскольку при сложении многочленов складываются их соответствующие коэффициенты, то ассоциативность и коммутативность сложения многочленов вытекает из аналогичных свойств сложения элементов области целостности  $K$ . Нулем и единицей в  $K[x]$  будут, соответственно, нулевой многочлен  $0$  и  $1 \in K$ .

Докажем ассоциативность умножения многочленов. Пусть  $f = a_n x^n + \dots + a_1 x + a_0$ ,  $g = b_n x^n + \dots + b_1 x + b_0$ ,  $h = c_n x^n + \dots + c_1 x + c_0$  (здесь мы не предполагаем, что  $a_n \neq 0$  и  $b_n \neq 0$ ). Докажем, что  $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ . Обозначим

$$\begin{aligned} f \cdot g &= p = p_n x^n + \dots + p_1 x + p_0, \\ (f \cdot g) \cdot h &= p \cdot h = u = u_n x^n + \dots + u_1 x + u_0, \\ g \cdot h &= q = q_n x^n + \dots + q_1 x + q_0, \\ f \cdot (g \cdot h) &= f \cdot q = v = v_n x^n + \dots + v_1 x + v_0. \end{aligned}$$

Докажем, что  $u = v$ . Для этого вычислим коэффициенты этих многочленов с номером  $t$ ,  $t = 0, 1, \dots$ :

$$\begin{aligned} u_t &= \sum_{r+k=t} p_r c_k = \sum_{r+k=t} \left( \sum_{i+j=r} a_i b_j \right) c_k = \sum_{i+j+k=t} a_i b_j c_k; \\ v_t &= \sum_{i+s=t} a_i q_s = \sum_{i+s=t} a_i \left( \sum_{j+k=s} b_j c_k \right) = \sum_{i+j+k=t} a_i b_j c_k. \end{aligned}$$

Результаты одинаковы, что и доказывает тождество ассоциативности.

Аналогично доказывается дистрибутивность умножения относительно сложения многочленов. Очевидно, умножение многочленов коммутативно. Таким образом,  $K[x]$  является коммутативным кольцом с единицей, отличной от нуля. Докажем, что это кольцо не имеет делителей нуля. Предположим противное: пусть многочлены  $f(x), g(x) \in K[x]$  являются делителями нуля, т.е.  $f(x) \neq 0$ ,  $g(x) \neq 0$ , но  $f(x) \cdot g(x) = 0$ . Тогда данные многочлены имеют определенные степени, а значит, их

произведение есть многочлен некоторой степени, в то время как 0 есть многочлен без степени. Пришли к противоречию. Теорема доказана.

Кольцо  $K[x]$  называется *кольцом многочленов над областью целостности  $K$* . Если  $K = P$  — поле, то  $P[x]$  называется *кольцом многочленов над полем  $P$* . Например,  $\mathbb{Z}[x]$  есть кольцо многочленов над кольцом целых чисел  $\mathbb{Z}$ , а  $\mathbb{Q}[x]$ ,  $\mathbb{R}[x]$ ,  $\mathbb{C}[x]$  являются кольцами многочленов соответственно над полями  $\mathbb{Q}$ ,  $\mathbb{R}$  и  $\mathbb{C}$ .

В области целостности  $K$ , по определению, есть единица 1, поэтому можно рассматривать *обратимые* элементы области целостности. Напомним, что элемент  $a \in K$  называется *обратимым*, если для него существует элемент  $b \in K$ , называемый *обратным* к  $a$ , такой что  $a \cdot b = 1$ . Множество всех обратимых элементов области целостности  $K$  будем обозначать  $K^*$ . Например, обратимыми в области целостности  $\mathbb{Z}$  являются лишь 1 и  $-1$ . А вот в области целостности  $\mathbb{Q}$ , точнее, в поле  $\mathbb{Q}$  для всякого отличного от нуля числа есть обратное число. Вообще, если  $P$  — поле, то  $P^* = P \setminus \{0\}$ .

**Теорема 1.2.** *В кольце многочленов  $K[x]$  над областью целостности  $K$  обратимыми элементами являются лишь обратимые элементы кольца  $K$ , т.е.  $(K[x])^* = K^*$ .*

*Доказательство.* Пусть многочлен  $d(x) \in K[x]$  является обратимым. Это означает существование многочлена  $q(x) \in K[x]$ , такого что  $d(x) \cdot q(x) = 1$ . Поскольку 1 есть многочлен степени 0, то многочлены  $d(x)$  и  $q(x)$  также должны иметь степень 0, т.е.  $d(x) = d_0 \in K$  и  $q(x) = q_0 \in K$ . Тогда  $d_0 \cdot q_0 = 1$ , т.е.  $d(x) = d_0$  является обратимым элементом кольца  $K$ . Теорема доказана.

Предположим, что  $K = P$  — поле. Вспомним, что в поле всякий ненулевой элемент обратим, поэтому обратимые элементы кольца многочленов  $P[x]$  над полем  $P$  есть в точности ненулевые элементы поля  $P$ . Таким образом,  $(P[x])^* = P^* = P \setminus \{0\}$ . Если же  $K = \mathbb{Z}$ , то  $(\mathbb{Z}[x])^* = \mathbb{Z}^* = \{1, -1\}$ .

### 1.1.2. Уточнение понятия многочлена

Не довольствуясь введением многочлена как «выражения вида»  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , дадим формализованное определение этого понятия.

**Определение 1.5.** *Многочленом над областью целостности  $K$  называется последовательность элементов из  $K$ , записываемая в виде  $(\dots, a_n, a_{n-1}, \dots, a_1, a_0)$ , причем число членов последовательности, отличных от нуля, конечно. Каждый член последовательности называется *коэффициентом* многочлена.*

Если все коэффициенты равны нулю, то многочлен называется *нулевым*. Если же есть коэффициенты, отличные от нуля, то отличный от нуля коэффициент с наибольшим номером называется *старшим коэффициентом*, а его номер называется *степенью многочлена*. Коэффициент  $a_0$  называется *свободным членом*.

**Определение 1.6.** Два многочлена называются *равными*, если равны их соответствующие коэффициенты.

**Определение 1.7.** Сложение и умножение многочленов определим равенствами

$$(\dots, a_n, \dots, a_0) + (\dots, b_n, \dots, b_0) = (\dots, a_n + b_n, \dots, a_0 + b_0);$$

$$(\dots, a_n, \dots, a_0) \cdot (\dots, b_n, \dots, b_0) = (\dots, c_n, \dots, c_0),$$

где  $c_k = a_k b_0 + a_{k-1} b_1 + \dots + a_1 b_{k-1} + a_0 b_k = \sum_{i+j=k} a_i b_j$ ,  $k = 0, 1, \dots$ .

Для получения привычной стандартной записи многочлена степени  $n$  обозначим  $x = (\dots, 0, \dots, 0, 1, 0)$  и  $a = (\dots, 0, \dots, 0, a)$  для любого элемента  $a \in K$ . В частности, нулевой многочлен имеет вид  $0 = (\dots, 0, \dots, 0, 0)$ . Вычислим одночлены, используя правило умножения многочленов:

$$a_0 = (\dots, 0, \dots, 0, a_0);$$

$$a_1 \cdot x = (\dots, 0, \dots, 0, a_1) \cdot (\dots, 0, \dots, 1, 0) = (\dots, 0, \dots, a_1, 0);$$

.....

$$\begin{aligned} a_n \cdot x^n &= (\dots, 0, \dots, 0, a_n) \cdot (\dots, 0, \dots, 0, 1, 0, \dots, 0) = \\ &= (\dots, 0, \dots, 0, a_n, 0, \dots, 0). \end{aligned}$$

В последнем равенстве единица стоит на месте с номером  $n$ , считая справа налево с номера 0. Складывая одночлены, приходим к выводу, что

$$a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \dots + a_1 \cdot x + a_0 = (\dots, a_n, \dots, a_1, a_0).$$

Таким образом, мы осмыслили стандартную запись многочлена, основываясь на новом, формальном его определении.

### 1.1.3. Кольцо многочленов $\mathbb{Z}_p[x]$

Построим кольцо многочленов над конечной областью целостности, которая в частных случаях оказывается полем.

Зафиксируем простое натуральное число  $p$ , скажем  $p = 5$ , и будем называть его модулем. При делении произвольного

целого числа на  $p = 5$  возможны остатки 0, 1, 2, 3, 4, в общем случае получаем остатки 0, 1, ...,  $p - 1$ . Пусть целое число  $a$  при делении на  $p$  дает в остатке  $r$ , т.е.  $a = pq + r$ , где  $0 \leq r < p$ .

Обозначим  $\bar{a} = \{pn + r | n \in \mathbb{Z}\}$ . Таким образом,  $\bar{a}$  есть множество всех целых чисел, которые при делении на  $p$  дают один и тот же остаток  $r$ . Отсюда следует, что  $\bar{a} = \bar{a}_1$  тогда и только тогда, когда  $a - a_1 : p$ . В результате множество целых чисел  $\mathbb{Z}$  распадается на следующие непересекающиеся классы целых чисел:

при $p = 5$	при произвольном простом $p$
$\bar{0} = \{5n   n \in \mathbb{Z}\}$	$\bar{0} = \{pn   n \in \mathbb{Z}\}$
$\bar{1} = \{5n + 1   n \in \mathbb{Z}\}$	$\bar{1} = \{pn + 1   n \in \mathbb{Z}\}$
$\bar{2} = \{5n + 2   n \in \mathbb{Z}\}$	$\bar{2} = \{pn + 2   n \in \mathbb{Z}\}$
$\bar{3} = \{5n + 3   n \in \mathbb{Z}\}$	...
$\bar{4} = \{5n + 4   n \in \mathbb{Z}\}$	$\overline{p-1} = \{pn + p - 1   n \in \mathbb{Z}\}$

При  $p = 5$  получаем  $\bar{5} = \bar{0}$ ,  $\bar{6} = \bar{1}$ ,  $\bar{7} = \bar{2}$  и т.д. Каждый элемент класса называется *вычетом* этого класса, а сам класс называется *классом вычетов по модулю  $p$* . Множество всех классов вычетов по модулю  $p$  обозначается  $\mathbb{Z}_p = \{0, \bar{1}, \dots, \overline{p-1}\}$ .

Определим сложение и умножение классов вычетов по модулю  $p$ , положив  $\bar{a} + \bar{b} = \overline{a + b}$ ,  $\bar{a} \cdot \bar{b} = \overline{ab}$  для любых  $a, b \in \mathbb{Z}$ . Докажем независимость сложения и умножения классов от выбора представителей этих классов. Пусть  $\bar{a} = \bar{a}_1$ ,  $\bar{b} = \bar{b}_1$ . Тогда  $a - a_1 : p$ ,  $b - b_1 : p$ , откуда  $(a + b) - (a_1 + b_1) = (a - a_1) + (b - b_1) : p$ . Но тогда  $a + b = a_1 + b_1$ , откуда  $\bar{a} + \bar{b} = \overline{a + b} = \overline{a_1 + b_1} = \bar{a}_1 + \bar{b}_1$ . Аналогично доказывается, что  $\bar{a} \cdot \bar{b} = \bar{a}_1 \cdot \bar{b}_1$ . Таким образом, результаты сложения и умножения классов вычетов не зависят от выбора представителей этих классов.

Приведем таблицы сложения и умножения классов вычетов по модулю 5:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$