МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
"ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ"

Р.Х. Вахитов, Е.В. Вахитова

ФУНДАМЕНТАЛЬНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА

Часть III

Алгебра многочленов

Учебно-методическое пособие для вузов

Издательско-полиграфический центр
Воронежского государственного университета
2012

Введение

Содержание данного учебно-методического пособия "Фундаментальная и компьютерная алгебра. Часть III. Алгебра многочленов" составляет материал нескольких тем базовой учебной дисциплины профессионального цикла "Фундаментальная и компьютерная алгебра", изучение которой предусмотрено основной образовательной программой подготовки бакалавра по направлению "Математика и компьютерные науки" для студентов факультета компьютерных наук ФГБОУ ВПО "Воронежский государственный университет". Целью учебной дисциплины является формирование представлений о фундаментальной алгебре: структуры алгебры, линейная алгебра, алгебра многочленов и о компьютерной алгебре. Основными задачами учебной дисциплины являются овладение фундаментальными базовыми знаниями в области фундаментальной и компьютерной алгебры, умением формулировать и доказывать теоремы, самостоятельно решать классические задачи фундаментальной алгебры.

Цель учебно-методического пособия состоит в том, чтобы помочь студентам, изучающим учебную дисциплину "Фундаментальная и компьютерная алгебра", формировать представление об алгебре многочленов, приобрести навыки и умения практического использования математических методов при решении задач. В результате изучения учебной дисциплины студент должен знать теоретический материал и уметь формулировать результат, строго доказывать утверждение, грамотно пользоваться языком фундаментальной и компьютерной алгебры.

Учебно-методическое пособие состоит из пяти глав. В конце каждой главы приведены вопросы для самоконтроля и упражнения для самостоятельной работы. Определения, теоремы и их доказательства иллюстрируются численными примерами, цель которых – пояснить общую теорию.

В каждой главе определения, формулы и теоремы имеют независимую нумерацию.

В первой главе рассмотрены следующие вопросы: простое транс-

Если $K_1[\alpha]$ – простое трансцендентное расширение кольца K_1 с помощью элемента α, то $K_1[\alpha]$ называют также кольцом многочленов от α над K_1, а элементы кольца K_1 – многочленами от α над K_1 или многочленами над K_1.

Пример. $K_1 := \mathbf{Z}$, $\alpha = \sqrt{2}$,

$$K_2 := \left\{ m + n\sqrt{2} \,|\, m, n \in \mathbf{Z} \right\}.$$

По определению 2 получим, что $K_2 = K_1[\alpha]$.

Теорема 1. *Для каждого ассоциативного и коммутативного кольца с единицей существует простое трансцендентное расширение кольца с помощью элемента* α.

В дальнейшем для удобства переобозначим многочлен a на f, коэффициенты многочлена γ_0, ..., γ_n на a_0, ..., a_n и элемент α на x и будем записывать

$$f \in K[x], \quad f = a_n x^n + ... + a_1 x + a_0, \quad a_0, a_1, ..., a_n \in K.$$

§ 2. Степень многочлена

Пусть K – ненулевое ассоциативное и коммутативное кольцо, $K[x]$ – простое трансцендентное расширение кольца K с помощью элемента x, то есть кольцо многочленов от x над K. Из определения простого трансцендентного расширения кольца с помощью элемента следует, что всякий элемент из $K[x]$ можно единственным образом представить в виде суммы степеней x с коэффициентами из K (это можно доказать от противного): если

$$(\gamma_0, \gamma_1, ..., \gamma_n) \neq (\beta_0, \beta_1, ...\beta_n),$$

то из равенства

$$\gamma_n x^n + \gamma_{n-1} x^{n-1} + ... + \gamma_0 = \beta_n x^n + \beta_{n-1} x^{n-1} + ... + \beta_0$$

получим, что $\gamma_n = \beta_n, \gamma_{n-1} = \beta_{n-1}, ..., \gamma_0 = \beta_0$.

Определение 3. *Число n называется степенью многочлена f, если $f = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$, где $a_n \neq 0$, а n – натуральное число или 0.*

Элементы a_n, a_{n-1}, ..., a_0 называются коэффициентами многочлена f, a_n – старший коэффициент.

Если $a_n = 1$, где 1 – единица кольца K, то многочлен f называется нормированным многочленом.

Обозначение степени многочлена: $n = deg\, f$. Если $f = a_0$, $a_0 \neq 0$, то $deg\, f = 0$. Если $f = a_0, a_0 = 0$, то степень многочлена не определена. Итак, будем считать, что степень нулевого многочлена не определена.

Отметим некоторые свойства степеней многочленов. Пусть f и g – ненулевые многочлены, а K – ассоциативное и коммутативное кольцо.

1) $deg\,(f+g) \leq max\,(deg\, f,\ deg\, g)$;

2) $deg\,(f \cdot g) \leq deg\, f + deg\, g$;

3) Если кольцо K – область целостности, то

$$deg\,(f \cdot g) = deg\, f + deg\, g.$$

§ 3. Деление многочлена на двучлен x – c

Пусть K – ненулевое ассоциативное и коммутативное кольцо, $K[x]$ – простое трансцендентное расширение кольца K с помощью элемента x, то есть кольцо многочленов от x над K.

$$f \in K[x],\ f = a_n x^n + a_{n-1}x^{n-1} + ... + a_0,$$

$$a_n,\ a_{n-1},\ ...,\ a_0 \in K.$$

Для $c \in K$ значением многочлена f от аргумента x будет

$$f(c) = a_n\, c^n + a_{n-1}\, c^{n-1} + \,\dots\, + a_0.$$

Теорема 2 (Безу). *Остаток от деления многочлена f из $K[x]$, где K – ассоциативное и коммутативное кольцо, на двучлен $x - c$, где $c \in K$, равен $f(c)$, то есть*

$$\Big(\exists q \in K[x]\Big)\Big(f = (x-c)\cdot q + f(c)\Big).$$

Доказательство. Рассмотрим отдельно два случая.

$$1)\ f = 0, \quad 2)\ f \neq 0.$$

1) $f = 0$. Тогда $f(c) = 0$, $f = (x-c)\cdot 0 + 0$, следовательно, в этом случае $q = 0$, $f(c) = 0$.

2) $f \neq 0$. $f = a_n c^n + a_{n-1} c^{n-1} + \dots + a_0$. Для $c \in K$ имеем

$$f(c) = a_n\, c^n + a_{n-1}\, c^{n-1} + \,\dots\, + a_0.$$

Тогда

$$f - f(c) = a_n(x^n - c^n) + a_{n-1}(x^{n-1} - c^{n-1}) + \dots + a_1(x - c).$$

Применим теперь тождество:

$$a^n - b^n = (a-b)(a^{n-1} + b\,a^{n-2} + \dots + b^{n-2}\,a + b^{n-1}), \quad n \in \mathbf{N}.$$

Тогда получим, что

$$f - f(c) = a_n(x-c)(x^{n-1} + c\,x^{n-2} + \dots + c^{n-2}\,x + c^{n-1}) + \dots$$

$$\dots + a_2(x-c)(x+c) + a_1(x-c),$$

следовательно,

$$f - f(c) = (x-c)\cdot q, \quad q \in K, \quad deg\, q = n - 1.$$

Таким образом, получим, что $f = (x-c)\cdot q, + f(c)$.

Теорема 2 доказана.