ФГБОУ ВПО «Воронежский государственный
технический университет»

Кафедра высшей математики и физико-математического
моделирования

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для организации самостоятельной работы
по дисциплине «Алгебра и геометрия»
для студентов специальностей
10.05.02 «Информационная безопасность
телекоммуникационных систем»,
10.05.03 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Воронеж 2015

Составители: канд. физ.-мат. наук С.П. Майорова,
канд. физ.-мат. наук М.Г. Завгородний

УДК 512.8

Методические указания для организации самостоятельной работы по дисциплине «Алгебра и геометрия» для студентов специальностей 10.05.02 «Информационная безопасность телекоммуникационных систем», 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. С.П. Майорова, М.Г. Завгородний. Воронеж, 2015. 44 с.

Методические указания содержат краткие теоретические сведения по разделу «Кольцо многочленов», примеры решения типовых задач, задачи для самостоятельного решения и тестовые задания для заключительного контроля.

Методические указания подготовлены в электронном виде в текстовом редакторе MS Word 2003 и содержатся в файле Мет_АлГео.pdf.

Библиогр.: 5 назв.

Рецензент канд. техн. наук, доц. Н.А. Ююкин

Ответственный за выпуск зав. кафедрой
д-р физ.-мат. наук, проф. И.Л. Батаронов

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

ВВЕДЕНИЕ

Система университетского образования предполагает рациональное сочетание таких видов учебной деятельности, как лекции, практические занятия, самостоятельная работа студентов, а также контроль полученных знаний.

Лекции представляют собой систематическое, последовательное изложение учебного материала.

Практические занятия позволяют научиться применять теоретические знания, полученные на лекциях при решении конкретных задач.

Самостоятельная работа студентов способствует глубокому усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие:

- работа с текстами: учебниками, справочниками, дополнительной методической литературой, а также проработка конспектов лекций;
- выполнение домашних заданий и типовых расчетов;
- работа над темами для самостоятельного изучения;
- подготовка к зачетам и экзаменам.

Данные методические указания содержат материал по разделу «Кольцо многочленов» и направлены на систематизацию и закрепление лекционного материала, а так же на получение практических умений и навыков студентов по этому разделу. Кроме того, в методических указаниях рассмотрены темы, выносимые на самостоятельное изучение: «Интерполяционный многочлен Лагранжа», «Критерий Батлера неприводимости многочлена над конечным полем», что поможет студентам в усвоении соответствующего материала.

Для эффективной подготовки к текущему контролю по данному разделу дисциплины в настоящих методических указаниях приведены вопросы для самоконтроля, тестовые задания, образец контрольной работы.

1. ПОСТРОЕНИЕ КОЛЬЦА МНОГОЧЛЕНОВ. ДЕЛЕНИЕ С ОСТАТКОМ. СХЕМА ГОРНЕРА

Основные теоретические сведения

Пусть K - коммутативное кольцо с единицей, не содержащее делителей нуля (т.е. K - область целостности).

Определение. *Многочленом от одного переменного x над кольцом K* называется формальное выражение вида $a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$, где n - целое неотрицательное число, и элементы $a_0, a_1, a_2, ..., a_n \in K$.

Обозначать многочлены будем $a(x)$, $b(x)$, $f(x)$ и т.п.

Элементы $a_0, a_1, a_2, ..., a_n$ называют *коэффициентами* многочлена, a_0 - *свободным членом*. Если $a_n \neq 0$, то число n называется *степенью многочлена*, а элемент a_n - *старшим коэффициентом*. Степень многочлена $a(x)$ обозначается символом $\deg a(x)$. Многочлен со старшим коэффициентом, равным единице, называется *унитарным*.

Если все коэффициенты многочлена $a(x)$ равны нулю, то $a(x)$ называют нулевым многочленом и обозначают $a(x) = 0$. Степень нулевого многочлена считают равной $-\infty$.

В качестве K обычно рассматриваются следующие алгебраические структуры: $\mathbb{R}$ - поле действительных чисел, $\mathbb{C}$ - поле комплексных чисел, $\mathbb{Q}$ - поле рациональных чисел, $\mathbb{Z}$ - кольцо целых чисел, $\mathbb{Z}_p$ - поле вычетов по простому модулю p.

Множество всех многочленов над кольцом K обозначим $K[x]$. Зададим на множестве $K[x]$ две операции - сложение и умножение. Пусть

$$a(x) = a_0 + a_1 x + ... + a_n x^n, \quad b(x) = b_0 + b_1 x + ... + b_m x^m \quad (n \geq m).$$

Определение. *Суммой многочленов $a(x)$ и $b(x)$* назо-

вем многочлен вида $a(x)+b(x)=\sum_{i=0}^{n} c_i x^i$, где $c_i = a_i + b_i$, $i = \overline{0,m}$, и $c_i = a_i$, $i = \overline{m+1,n}$.

Определение. *Произведением многочленов* $a(x)$ и $b(x)$ назовем многочлен вида $a(x)\cdot b(x) = d_0 + d_1 x + ... + d_{n+m} x^{n+m}$, где $d_k = \sum_{i+j=k} a_i b_j = a_0 b_k + a_1 b_{k-1} + ... + a_k b_0$, $k = \overline{0, n+m}$.

Здесь свободный член $d_0 = a_0 b_0$ и старший коэффициент $d_{n+m} = a_n b_m$.

Из введенных определений суммы и произведения многочленов вытекает:

1) $\deg\big(a(x)+b(x)\big) \le \max\{\deg a(x), \deg b(x)\}$;

2) $\deg(a(x)\cdot b(x)) = \deg a(x) + \deg b(x)$.

Ометим, что свойство 2 верно в силу того, что в кольце K нет делителей нуля.

Теорема. *Множество* $K[x]$ *с введенными операциями сложения и умножения является коммутативным кольцом с единицей.*

Зафиксируем произвольное поле P, и рассмотрим кольцо многочленов над полем P.

Определение. Пусть $a(x), b(x) \in P[x]$. Говорят, что $a(x)$ *делится с остатком* на $b(x)$, если существуют многочлены $q(x),\ r(x) \in P[x]$ такие, что выполняются условия:

1) $a(x) = b(x)q(x) + r(x)$, 2) $\deg r(x) < \deg b(x)$.

При этом $q(x)$ называют *неполным частным*, а $r(x)$ *остатком* от деления $a(x)$ на $b(x)$.

Теорема (о делении с остатком). *Если* $a(x), b(x) \in P[x]$ *и* $b(x) \neq 0$, *то* $a(x)$ *можно разделить с остатком на* $b(x)$, *причем неполное частное и остаток находятся однозначно.*

Заключение теоремы становится неверным, если P - кольцо, а не поле. Например, в кольце многочленов $\mathbb{Z}[x]$ с целыми коэффициентами многочлен $a(x) = x^2 + 1$ *нельзя* разделить с остатком на $b(x) = 3x$, так как коэффициенты частного и остатка не являются целыми числами.

При доказательстве этой теоремы предлагается практический способ нахождения неполного частного и остатка. Этот способ совпадает с известным из средней школы делением многочлена на многочлен "уголком".

Особо выделяется случай деления многочлена $f(x)$ на двучлен вида $(x - c)$. В этом случае можно использовать *схему Горнера*, которая позволяет найти неполное частное и остаток, **не** производя деление многочленов "уголком". Пусть требуется разделить с остатком многочлен

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

на двучлен $(x - c)$. Тогда в силу теоремы о делении с остатком получим $f(x) = (x - c)q(x) + r$, где $q(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \ldots + b_1 x + b_0$ - частное и r - остаток от деления. Коэффициенты b_i частного и остаток r находят из таблицы:

	a_n	a_{n-1}	a_{n-2}	...	a_1	a_0
c	$b_{n-1} =$ $= a_n$	$b_{n-2} =$ $= cb_{n-1} + a_{n-1}$	$b_{n-3} =$ $= cb_{n-2} + a_{n-2}$	...	$b_0 =$ $= cb_1 + a_1$	$r =$ $= cb_0 + a_0$

Здесь первая строка – это *все* коэффициенты многочлена f (по убывающим степеням), и каждый коэффициент b_k вычисляется путем умножения предыдущего коэффициента b_{k+1} на c и добавления числа a_{k+1}, стоящего над ним. Остаток вычисляется по тому же правилу.

Из теоремы о делении с остатком вытекает следующий факт.

Теорема (Безу). *Остаток от деления многочлена* $f(x) \in K[x]$ *на двучлен* $x - c \in K[x]$ *равен* $f(c)$.

В силу этой теоремы $f(c) = r$, поэтому схема Горнера может быть использована для быстрого вычисления значения многочлена в точке c, и для отыскания корней многочлена.

Вопросы для самоконтроля

1) Что называется многочленом над кольцом?
2) Что такое степень многочлена?
3) Какой многочлен называется унитарным?
4) Как определяется сумма и произведение двух многочленов?
5) Что можно сказать о степенях многочленов $a(x) + b(x)$ и $a(x) \cdot b(x)$?
6) Может ли кольцо многочленов быть полем? Докажите.
7) Что значит «разделить с остатком многочлен $a(x)$ на $b(x)$»? Какому условию должен удовлетворять остаток?
8) Сформулируйте теорему о делении с остатком.
9) Как выполнить деление с остатком многочлена на двучлен при помощи схемы Горнера?
10) Сформулируйте теорему Безу.

Примеры решения задач

Задача 1. Выполнить деление с остатком многочлена $f(x) = 2x^4 + x^3 + x^2 - x - 3$ на многочлен $g(x) = x^3 + 2x^2 - 1$ в кольцах $\mathbb{R}[x]$ и $\mathbb{Z}_7[x]$.

Решение. Воспользуемся схемой деления многочленов "уголком". Имеем:

$$\begin{array}{r|l} 2x^4 + x^3 + x^2 - x - 3 & x^3 + 2x^2 - 1 \\ \underline{-\,(2x^4 + 4x^3 - 2x)} & \\ -3x^3 + x^2 + x - 3 & 2x - 3 \\ \underline{-\,(-3x^3 - 6x^2 + 3)} & \\ 7x^2 + x - 6 & \end{array}$$

Итак, в кольце $\mathbb{R}[x]$ частное $q(x)=2x-3$, остаток $r(x)=7x^2+x-6$. Для получения результата в кольце $\mathbb{Z}_7[x]$ преобразуем коэффициенты полученного частного и остатка. По модулю 7 имеем: $-3\equiv 4$, $7\equiv 0$, $-6\equiv 1$. Окончательно в кольце $\mathbb{Z}_7[x]$ получаем: $q(x)=2x+4$, $r(x)=x+1$.

Задача 2. Пользуясь схемой Горнера, разделить с остатком многочлен $f(x)=2x^5-3x^3-6x^2-7x+6$ на двучлен $(x-3)$ в кольцах $\mathbb{R}[x]$ и $\mathbb{Z}_7[x]$.

Решение. Применим схему Горнера. Все коэффициенты многочлена $f(x)$, в том числе и нулевые, запишем в верхней строке таблицы, а в нижней строке получим коэффициенты частного $q(x)$ и остаток r.

Старший коэффициент $a_n=2$ сразу запишем во вторую строку. Каждый следующий коэффициент частного будем вычислять по формуле $b_k=cb_{k+1}+a_{k+1}$, где $c=3$; при этом в последней клетке таблицы получим остаток. Имеем:

	2	0	–3	–6	–7	6
3	2	$3\cdot 2+0=6$	$3\cdot 6-3=15$	$3\cdot 15-6=39$	$3\cdot 39-7=110$	$3\cdot 110+6=336$

Таким образом, в кольце многочленов $\mathbb{R}[x]$ верно

$$q(x)=2x^4+6x^3+15x^2+39x+110,\quad r=336.$$

В кольце многочленов $\mathbb{Z}_7[x]$ преобразуем коэффициенты частного и остаток (по модулю 7): $15\equiv 1$, $39\equiv 4$, $110\equiv 5$, $336\equiv 0$; тогда $q(x)=2x^4+6x^3+x^2+4x+5$, $r=0$.

Отсюда видно, что $x=3$ не является корнем многочлена $f(x)\in\mathbb{R}[x]$, но является корнем в случае $f(x)\in\mathbb{Z}_7[x]$.

Задачи и упражнения для самостоятельного решения

1) Выполните деление с остатком в кольце $\mathbb{R}[x]$:

а) $2x^4-3x^3+4x^2-5x+6$ на x^2-3x+1;

б) x^3-3x^2-x-1 на $3x^2-2x+1$.

2) В кольце $\mathbb{Z}_5[x]$ выполните деление с остатком

$2x^4+3x^3+x+4$ на x^2+2.

3) Пользуясь схемой Горнера, разделите в кольце $K[x]$ многочлен $f(x)$ на двучлен $(x-c)$:

а) $K=\mathbb{Z}$, $f(x)=x^4-3x^3+x-1$, $c=2$;

б) $K=\mathbb{Z}$, $f(x)=9x^3+8x^2-10x$, $c=-3$;

в) $K=\mathbb{Z}_7$, $f(x)=3x^3+6x^2-2$, $c=2$;

г) $K=\mathbb{Z}_{11}$, $f(x)=7x^4-9x^3+8x^2+10x-6$, $c=-3$.

4) Пользуясь схемой Горнера, найдите значение многочлена $f(x)$ в точке c: а) $f(x)=x^4+5x^3-3x+6\in\mathbb{Z}[x]$, $c=2$;

б) $f(x)=x^4+3x^3-3x+2\in\mathbb{Z}_7[x]$, $c=4$.

5) Пользуясь схемой Горнера, найдите кратность корня x_0 многочлена $f(x)$:

а) $f(x)=x^5-5x^4+7x^3-2x^2+4x-8\in\mathbb{Z}[x]$, $x_0=2$;

б) $f(x)=x^5-2x^3+x^2-2\in\mathbb{Z}_3[x]$, $x_0=2$.

6) Пользуясь схемой Горнера, составьте таблицу всех значений многочлена $f(x)\in\mathbb{Z}_p[x]$:

а) $f(x)=x^4-2x^3+x^2+2$, $p=5$;

б) $f(x)=3x^5+x^3-2x+1$, $p=7$.

7) Найдите все корни и их кратности для многочлена $f(x)\in\mathbb{Z}_5[x]$: $f(x)=x^7-3x^6+x^5-x^3+4x^2-4x+2$.

8) Найдите сумму коэффициентов многочлена

$$f(x)=(3x^5-4x^3+2x^2-x-1)^{20}$$

2. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ МНОГОЧЛЕНОВ. АЛГОРИТМ ЕВКЛИДА

Основные теоретические сведения

Пусть $f_1(x), f_2(x),..., f_n(x)$ - многочлены над полем P.

Определение. *Наибольшим общим делителем* многочленов $f_1(x), f_2(x),..., f_n(x)$ называется любой многочлен $d(x) \in P[x]$, который удовлетворяет двум условиям:

1) $d(x)$ является общим делителем многочленов $f_1(x)$, $f_2(x)$, ... , $f_n(x)$;
2) $d(x)$ делится на любой другой общий делитель этих многочленов.

Обозначение: $НОД\left(f_1(x), f_2(x),..., f_n(x)\right) = d(x)$.

НОД двух многочленов находят с помощью *алгоритма Евклида*. Алгоритм Евклида для нахождения НОД многочленов $a(x)$ и $b(x)$ при $b(x) \neq 0$ состоит в следующем.

Выполним цепочку последовательных делений. Сначала делим с остатком $a(x)$ на $b(x)$. Затем $b(x)$ делим на остаток $r_1(x)$, потом $r_1(x)$ делим на $r_2(x)$, и так далее, пока не получим остаток, равный нулю. Этот процесс можно записать следующим образом:

$a:b$	$a(x) = b(x)q_1(x) + r_1(x)$,	$\deg r_1 < \deg b$;
$b:r_1$	$b(x) = r_1(x)q_2(x) + r_2(x)$,	$\deg r_2 < \deg r_1$;
$r_1:r_2$	$r_1(x) = r_2(x)q_3(x) + r_3(x)$,	$\deg r_3 < \deg r_2$;
… …	… … … … …	
$r_{k-2}:r_{k-1}$	$r_{k-2}(x) = r_{k-1}(x)q_k(x) + r_k(x)$,	$\deg r_k < \deg r_{k-1}$;
$r_{k-1}:r_k$	$r_{k-1}(x) = r_k(x)q_{k+1}(x)$.	

Тогда НОД$(a(x),b(x))=r_k(x)$. Таким образом, *последний ненулевой остаток* $r_k(x)$ *в алгоритме Евклида является наибольшим общим делителем многочленов* $a(x)$ *и* $b(x)$.

Справедлива теорема о линейном представлении НОД.

Теорема. *Если* $a(x), b(x) \in P[x]$ *и* $d(x) = НОД(a(x), b(x))$, *то существуют многочлены* $u(x), v(x) \in P[x]$ *такие, что* $d(x) = a(x)u(x) + b(x)v(x)$.

Нахождение НОД *нескольких многочленов* сводится к нахождению НОД двух многочленов. Так, для трех многочленов имеем: $\text{НОД}(f_1, f_2, f_3) = \text{НОД}\big(\text{НОД}(f_1, f_2), f_3\big)$.

Аналогично для четырех многочленов: $\text{НОД}(f_1, f_2, f_3, f_4) =$

$= \text{НОД}\big(\text{НОД}(f_1, f_2), f_3, f_4\big) = \text{НОД}\big(\text{НОД}\big(\text{НОД}(f_1, f_2), f_3\big), f_4\big)$.

Как видно из приведенных формул, при вычислении НОД нескольких многочленов можно заменять любую пару многочленов на их наибольший общий делитель.

Вопросы для самоконтроля

1) Что называют наибольшим общим делителем многочленов?
2) Как найти наибольший общий делитель двух многочленов? Опишите алгоритм Евклида.
3) Как найти наибольший общий делитель трех многочленов?
4) Сформулируйте теорему о линейном представлении наибольшего общего делителя.
5) Какие многочлены называются взаимно простыми? Приведите примеры.

Примеры решения задач

Задача 1. Найти НОД многочленов $f(x) = x^3 + x^2 + 2x + 2$ и $g(x) = x^2 + x + 1$ в кольцах $\mathbb{Q}[x]$ и $\mathbb{Z}_3[x]$.

Решение. Применяя алгоритм Евклида, получим:

$$f : g \quad \begin{array}{r|l} x^3 + x^2 + 2x + 2 & x^2 + x + 1 \\ \underline{x^3 + x^2 + x} & x \\ x + 2 = r_1 & \end{array}$$

$g : r_1$

$$\begin{array}{r|l} x^2+x+1 & x+2 \\ \underline{x^2+2x} & \hline x-1 \\ -x+1 & \\ \underline{-x-2} & \\ 3=r_2 & \end{array}$$

$r_1 : r_2$

$$\begin{array}{r|l} x+2 & 3 \\ \underline{x} & \hline \frac{1}{3}x+\frac{2}{3} \\ 2 & \\ \underline{2} & \\ 0 & \end{array}$$

Итак, в кольце $\mathbb{Q}[x]$ последний ненулевой остаток – это r_2, поэтому $НОД(f,g)=3$, или переходя к унитарному многочлену, имеем $НОД(f,g)=1$.

В кольце $\mathbb{Z}_3[x]$ остаток $r_2=3\equiv 0(\mathrm{mod}\,3)$, поэтому последним ненулевым остатком в этом кольце многочленов является r_1, а значит $НОД(f,g)=x+2$.

Задача 2. В кольце $\mathbb{Q}[x]$ найти НОД многочленов

$f(x)=x^5+2x^4+x^3+7x^2+x+6$ и $g(x)=x^4+4x^3+4x^2+3x+14$.

Решение. Выполняя цепочку последовательных делений алгоритма Евклида, имеем:

$f : g$

$$\begin{array}{r|l} x^5+2x^4+x^3+7x^2+x+6 & x^4+4x^3+4x^2+3x+14 \\ \underline{x^5+4x^4+4x^3+3x^2+14x} & \hline x-2 \\ -2x^4-3x^3+4x^2-13x+6 & \\ \underline{-2x^4-8x^3-8x^2-6x-28} & \\ 5x^3+12x^2-7x+34(=r_1) & \end{array}$$

Для удобства дальнейших вычислений умножим $g(x)$ на 5. Это не повлияет на окончательный ответ, так как 5 - обратимый элемент кольца $\mathbb{Q}[x]$. Чтобы избежать дробных коэффициентов, один из промежуточных остатков также умножим на 5. Получим:

$$5g : r_1 \qquad \begin{array}{r|l} 5x^4+20x^3+20x^2+15x+70 & 5x^3+12x^2-7x+34 \\ \underline{5x^4+12x^3-7x^2+34x} & x\,//+8 \end{array}$$

$$\underline{\underline{8x^3+27x^2-19x+70 \quad (\times 5)}}$$

$$\underline{40x^3+135x^2-95x+350}$$

$$\underline{40x^3+96x^2-56x+272}$$

$$39x^2-39x+78 (= r_2)$$

В этой схеме знак // разделяет различные частные. Разделим теперь r_1 на r_2, или для удобства дальнейших вычислений – на $\frac{1}{39}r_2$. Имеем:

$$r_1 : (\frac{1}{39}r_2) \qquad \begin{array}{r|l} 5x^3+12x^2-7x+34 & x^2-x+2 \\ \underline{5x^3-5x^2+10x} & 5x+17 \end{array}$$

$$\underline{17x^2-17x+34}$$

$$\underline{17x^2-17x+34}$$

$$0$$

Итак, в кольце $\mathbb{Q}[x]$ последний ненулевой остаток - это r_2, тогда переходя к унитарному многочлену, получим

$$НОД(f,g) = \frac{1}{39}r_2 = x^2 - x + 2.$$

Отметим, что домножение промежуточного остатка на число возможно лишь в случае, когда не ставится задача об отыскании линейного представления НОД, поскольку при таком домножении изменяется частное.

Задача 3. В кольце $\mathbb{Z}_3[x]$ найти НОД многочленов

$$f(x) = x^5 + 2x^4 + 2x^3 + x^2 + x + 2, \qquad g(x) = x^5 + x^3 + x$$

и получить линейное представление НОД.

Решение. Выполним цепочку последовательных делений, сразу преобразуя коэффициенты (напомним, что кольцо $\mathbb{Z}_3$ состоит из трех элементов - это 0, 1, 2):

$f : g$

$$\begin{array}{r|l} x^5+2x^4+2x^3+x^2+x+2 & x^5+x^3+x \\ \underline{-\,x^5\qquad\quad +x^3\qquad +x} & \\ 2x^4+x^3+x^2+2\,(=r_1) & 1 \end{array}$$

$g : r_1$

$$\begin{array}{r|l} x^5\qquad +\ x^3+x & 2x^4+x^3+x^2+2 \\ \underline{-\,x^5+2x^4+2x^3+x} & \\ -\,x^4+2x^3 & \\ \underline{x^4+2x^3+2x^2+1} & \\ x^2+2\,(=r_2) & 2x+2 \end{array}$$

$r_1 : r_2$

$$\begin{array}{r|l} 2x^4+x^3+x^2+2 & x^2+2 \\ \underline{-\,2x^4\qquad +x^2} & \\ -\,x^3\qquad +2 & \\ \underline{x^3+2x} & \\ x+2\,(=r_3) & 2x^2+x \end{array}$$

$r_2 : r_3$

$$\begin{array}{r|l} x^2+2 & x+2 \\ \underline{-\,x^2+2x} & \\ -\,x+2 & \\ \underline{x+2} & \\ 0\,(=r_4) & x+1 \end{array}$$

Итак, $НОД(f,g)=r_3(x)=x+2$.

Для получения линейного представления НОД найдем многочлены $u(x),v(x)\in\mathbb{Z}_3[x]$ такие, что $НОД(f,g)=u(x)f(x)+v(x)g(x)$. Запишем алгоритм Евклида в сокращенной форме:

$$f(x)=g(x)\cdot 1+r_1(x),$$
$$g(x)=r_1(x)\cdot(2x+2)+r_2(x),$$
$$r_1(x)=r_2(x)\cdot(2x^2+x)+r_3(x).$$

Из этих равенств выразим остатки, начиная с последнего:

$$r_3(x)=r_1(x)-r_2(x)\cdot(2x^2+x),$$
$$r_2(x)=g(x)-r_1(x)\cdot(2x+2),$$
$$r_1(x)=f(x)-g(x).$$

Будем последовательно исключать остатки из выражений для r_3 и r_2. Для остатка $r_3(x) = НОД(f, g)$ получим:

$$r_3(x) = r_1(x) - \boxed{r_2(x)} \cdot (2x^2 + x) =$$

$$= r_1(x) - (g(x) - r_1(x) \cdot (2x + 2)) \cdot (2x^2 + x) =$$

$$= -g(x) \cdot (2x^2 + x) + \boxed{r_1(x)} \cdot (x^3 + 2x + 1) =$$

$$= -g(x) \cdot (2x^2 + x) + (f(x) - g(x)) \cdot (x^3 + 2x + 1) =$$

$$= f(x) \cdot (x^3 + 2x + 1) - g(x) \cdot (x^3 + 2x^2 + 1) =$$

$$= f(x) \cdot (x^3 + 2x + 1) + g(x) \cdot (2x^3 + x^2 + 2).$$

Таким образом, линейное представление НОД найдено, а именно: $НОД(f, g) = (x^3 + 2x + 1) \cdot f(x) + (2x^3 + x^2 + 2) \cdot g(x)$.

Задачи и упражнения для самостоятельного решения

1) Найдите наибольший общий делитель многочленов $f, g \in \mathbb{R}[x]$, если:

   а) $f(x) = x^4 + x^3 - 3x^2 - 4x - 1$, $g(x) = x^3 + x^2 - x - 1$;

   б) $f(x) = 2x^6 + 2x^4 - 4x^3 - 3x^2 + 8x - 5$, $g(x) = x^5 + x^2 - x + 1$;

   в) $f(x) = x^3 - 7x + 7$, $g(x) = 3x^2 - 7$.

2) Для многочленов $f(x)$, $g(x)$ над данным полем P найдите НОД и его линейное представление:

   а) $f(x) = 3x^3 - 2x^2 + x + 2$, $g(x) = x^2 - x + 1$, $P = \mathbb{R}$;

   б) $f(x) = x^4 + 1$, $g(x) = x^3 + x + 1$, $P = \mathbb{Z}_3$;

   в) $f(x) = x^4 - 2x^2 + x + 4$, $g(x) = x^4 + 6x^2 + 2$, $P = \mathbb{Z}_7$.

3) Выясните, являются ли взаимно простыми многочлены $f, g \in \mathbb{R}[x]$, если: а) $f(x) = x^3 - 3x^2 + 2x + 1$, $g(x) = 2x^2 - x - 1$;

   б) $f(x) = 2x^3 - 3x^2 - x + 2$, $g(x) = x^4 - 2x^2 - 3x + 4$.

3. НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ НАД ПОЛЕМ. КАНОНИЧЕСКОЕ РАЗЛОЖЕНИЕ МНОГОЧЛЕНА

Основные теоретические сведения

Определение. Многочлен $f(x) \in P[x]$ степени $n \geq 1$ называется *неприводимым* над полем P, если не существует многочленов $f_1(x),\ f_2(x) \in P[x]$ таких, что

$$f(x) = f_1(x) \cdot f_2(x), \quad \text{где} \quad 0 < \deg f_i < n, \quad i = 1, 2.$$

В противном случае многочлен называется *приводимым* над полем P. Многочлены нулевой степени и нулевой многочлен не относят ни к приводимым, ни к неприводимым многочленам.

Другими словами, многочлен *неприводим* над полем, если он не может быть разложен в произведение двух многочленов меньшей степени.

Понятие неприводимого многочлена существенно привязано к полю, над которым этот многочлен рассматривается. Например, многочлен $f(x) = x^2 - 3$ можно рассматривать и над полем $\mathbb{Q}$ рациональных чисел, и над полем $\mathbb{R}$ действительных чисел. Над полем $\mathbb{Q}$ он неприводим, так как не имеет рациональных корней; но над полем $\mathbb{R}$ многочлен $f(x)$ уже приводим, так как верно разложение $f(x) = (x - \sqrt{3})(x + \sqrt{3})$.

Отметим, что многочлен первой степени, т.е. многочлен вида $ax + b$, $a \neq 0$, является неприводимым над любым полем.

Роль неприводимых многочленов раскрывается следующей теоремой.

Теорема. *Любой многочлен $f(x) \in P[x]$ степени $n \geq 1$ разлагается в произведение неприводимых над полем P многочленов, и такое разложение единственно с точностью до перестановки сомножителей и множителей нулевой степени.*

Следствие. *Любой многочлен* $f(x) \in P[x]$ *степени* $n \geq 1$ *над полем* P *представляется в виде*

$$f(x) = a\varphi_1^{k_1}(x)\varphi_2^{k_2}(x)...\varphi_m^{k_m}(x),$$

где $a \in P \setminus \{0\}$; $\varphi_1(x)$, $\varphi_2(x)$, ... , $\varphi_m(x)$ - *различные унитарные неприводимые над полем* P *многочлены;* k_1, k_2, ... , k_m - *натуральные числа.*

Такое представление многочлена $f(x)$ называется его *каноническим разложением* над полем P.

Заметим, что каноническое разложение многочлена на неприводимые множители существенно зависит от того поля, над которым этот многочлен рассматривается. Так, например, многочлен $f(x) = x^4 - 4$ можно рассматривать над любым из полей $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, и над каждым из них $f(x)$ разлагается в произведение неприводимых множителей. Однако разложения эти различны, а именно:

над полем $\mathbb{Q}$ $\quad f(x) = (x^2 - 2)(x^2 + 2)$,

над полем $\mathbb{R}$ $\quad f(x) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2)$,

над полем $\mathbb{C}$ $\quad f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - i\sqrt{2})(x + i\sqrt{2})$.

Вопросы для самоконтроля

1) Какой многочлен называется неприводимым?
2) Докажите, что многочлен третьей степени, не имеющий корней в данном поле, неприводим.
3) Приведите пример приводимого многочлена четвертой степени в кольце $\mathbb{R}[x]$, не имеющего действительных корней.
4) Что такое каноническое разложение многочлена?
5) Докажите, что многочлен второй или третьей степени приводим над полем P тогда и только тогда, когда он имеет корни в поле P. Покажите, что уже для многочленов четвертой степени этот факт неверен.

6) Как найти НОД нескольких многочленов, если известно каноническое разложение каждого из них?
7) Как найти НОД нескольких многочленов, если известно разложение одного из них на неприводимые множители?

Примеры решения задач

Пример. Пусть $P=\mathbb{Z}_2$. Тогда в $P[x]$ неприводимы многочлены x^2+x+1, x^3+x+1, x^3+x^2+1, так как они не имеют корней в поле $P=\mathbb{Z}_2$. Многочлен x^4+x^2+1 также не имеет корней в данном поле P, но он приводим, так его можно разложить на множители: $x^4+x^2+1=(x^2+x+1)^2$.

Задачи и упражнения для самостоятельного решения

1) Даны многочлены x^2-1, x^2-2, x^2+1, x^4-25. Выясните, будут ли эти многочлены приводимы над полями $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$? В случае положительного ответа запишите соответствующее каноническое разложение многочлена.
2) В кольце $\mathbb{Q}[x]$ найдите наибольший общий делитель многочленов: а) $x^3(x^3-2)^2(x^2-3)$ и $x(x^2+1)^2(x^3-2)$;
   б) $(x^4-4)(x^2-2)$ и $(x^2+2)^2(x^4+4)$;
   в) $(x-1)^{125}(x+2)^{107}(x-3)^{92}$ и
   $x^9+x^8-5x^7+x^6+11x^5-13x^4-7x^3+15x^2-4$.
3) Пусть A - множество корней многочлена f и B - множество корней многочлена g. Справедливы ли следующие утверждения:
   а) Если $A\cap B=\varnothing$, то наибольший общий делитель многочленов f и g равен 1.
   б) Если наибольший общий делитель многочленов f и g равен 1, то $A\cap B=\varnothing$?

4. НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ НАД ПОЛЕМ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

Основные теоретические сведения

Рассмотрим сначала многочлены с комплексными коэффициентами. Описание неприводимых многочленов над полем $\mathbb{C}$ дает следующая теорема.

Теорема. *Над полем $\mathbb{C}$ комплексных чисел неприводимы все многочлены первой степени, и только они.*

Следствие. *Каноническое разложение многочлена*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{C}[x]$$

над полем $\mathbb{C}$ имеет вид $f(x) = a_n (x - c_1)^{k_1} (x - c_2)^{k_2} \ldots (x - c_s)^{k_s}$,

где $c_1, c_2, \ldots, c_s$ *- различные комплексные корни многочлена;* $k_1 + k_2 + \ldots + k_s = n$.

Рассмотрим теперь $\mathbb{R}[x]$ - кольцо многочленов над полем действительных чисел. С помощью последней теоремы можно описать все неприводимые многочлены над полем $\mathbb{R}$. Напомним, что дискриминантом многочлена $ax^2 + bx + c \in \mathbb{R}[x]$, $a \neq 0$, называется число $D = b^2 - 4ac$, и многочлен не имеет корней в поле $\mathbb{R}$ тогда и только тогда, когда $D < 0$.

Теорема. *Над полем $\mathbb{R}$ действительных чисел неприводимыми являются все многочлены первой степени и многочлены второй степени с отрицательными дискриминантами, и только они.*

Следствие 1. *Каноническое разложение многочлена*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{R}[x]$$

над полем $\mathbb{R}$ имеет вид

$$f(x) = a_n (x - c_1)^{k_1} \ldots (x - c_s)^{k_s} (x^2 + p_1 x + q_1)^{m_1} \ldots (x^2 + p_l x + q_l)^{m_r},$$

где $p_i^2 - 4q_i < 0 \quad (i = \overline{1, r})$; $\quad k_1 + \ldots + k_s + 2m_1 + \ldots + 2m_r = n$;

c_1, c_2, ... , c_s *- различные действительные корни* $f(x)$.

Следствие 2. *Любой многочлен нечетной степени над полем* $\mathbb{R}$ *имеет действительные корни.*

Укажем некоторые свойства корней многочленов с действительными коэффициентами.

Теорема. *Если комплексное число* $z = a + bi$ *является корнем многочлена* $f(x)$ *с действительными коэффициентами, то сопряженное с ним число* $\overline{z} = a - bi$ *также будет корнем этого многочлена.*

Вопросы для самоконтроля

1) Какие многочлены неприводимы над полем комплексных чисел?
2) Какой вид имеет каноническое разложение многочлена n-й степени над полем комплексных чисел?
3) Какие многочлены неприводимы над полем действительных чисел?
4) Какой вид имеет каноническое разложение многочлена n-й степени над полем действительных чисел?
5) Докажите, что в кольце $\mathbb{R}[x]$ нет неприводимых многочленов нечетной степени.
6) Приведите пример многочлена четвертой степени над полем действительных чисел, не имеющего корней в этом поле.
7) Покажите, что кольцо $\mathbb{R}[x]$ многочленов с действительными коэффициентами не является полем.

Примеры решения задач

Задача 1. Найти многочлен наименьшей степени с действительными коэффициентами, который имеет следующие корни: $2+i$, 3 - простые корни, $1+i$ - корень кратности 2.

Решение. Искомый многочлен обозначим через $f(x)$. Так как $f(x) \in \mathbb{R}[x]$, то вместе с корнем $2+i$ комплексно сопряженное число $2-i$ также является корнем этого многочлена. Поэтому $f(x) \vdots g(x)$, где

$$g(x)=(x-(2+i))(x-(2-i))=x^2-4x+5.$$

Кроме того, по условию $1+i$ - корень кратности 2; следовательно, число $1-i$ также является корнем кратности 2. Тогда $f(x)\vdots h(x)$, где $h(x)=\left(x-(1+i)\right)^2\left(x-(1-i)\right)^2=(x^2-2x+2)^2$.

По условию число 3 также является корнем $f(x)$, значит $f(x)\vdots(x-3)$. Таким образом, искомый многочлен $f(x)$ имеет вид $f(x)=(x-3)(x^2-4x+5)(x^2-2x+2)^2$.

Задача 2. Зная, что многочлен $f(x)=x^4+3x^3+2x^2-x+5$ имеет корень $-2+i$, найти его остальные корни.

Решение. Так как $f(x)$ - многочлен с действительными коэффициентами, то вместе с корнем $-2+i$ он обязан иметь корень $-2-i$. Следовательно, многочлен $f(x)$ делится на многочлен $(x+2-i)(x+2+i)=x^2+4x+5$. Разделив $f(x)$ на этот многочлен, получим $f(x)=(x^2+4x+5)(x^2-x+1)$. Отсюда видно, что остальные корни $f(x)$ являются корнями уравнения $x^2-x+1=0$, т.е. равны числам $\frac{1}{2}\pm\frac{i\sqrt{3}}{2}$. Итак, многочлен $f(x)$ имеет 4 корня: $-2+i$, $-2-i$, $\frac{1}{2}\pm\frac{i\sqrt{3}}{2}$.

Задачи и упражнения для самостоятельного решения

1) Разложите на неприводимые множители в кольце $\mathbb{C}[x]$ многочлен x^4+4.
2) Известно, что многочлен $x^4+3x^3+2x^2-x+5$ имеет комплексный корень $x_0=-2+i$. Какое число обязано быть корнем этого многочлена? Разложите многочлен на неприводимые множители над полем действительных чисел.
3) Постройте многочлен наименьшей степени с действительными коэффициентами, имеющий данные корни:

а) корень 1 кратности 2 и простой корень $2+i$;

б) корень $1-i$ кратности 2 и простой корень -3;

в) корень $2+i$ кратности 2 и простой корень $1-i$.

4) Выясните, над каким из полей $\mathbb{Q}$, $\mathbb{R}$ или $\mathbb{C}$ приводимы следующие многочлены: а) $x^2-10x+21$; б) x^2+2x-1; в) $2x^2-3x-5$; г) $3x^2+x+3$.

5. НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ НАД ПОЛЕМ РАЦИОНАЛЬНЫХ ЧИСЕЛ

Основные теоретические сведения

Как следует из предыдущих пунктов, в кольцах $\mathbb{C}[x]$ и $\mathbb{R}[x]$ удается явно описать все неприводимые многочлены. В кольце $\mathbb{Q}[x]$ полного описания неприводимых многочленов не существует, и можно дать лишь некоторые достаточные условия неприводимости.

Отметим следующее. Изучение свойств многочленов с рациональными коэффициентами удается свести к изучению многочленов с целыми коэффициентами. А именно, если $f(x)\in\mathbb{Q}[x]$, то умножив $f(x)$ на наименьшее общее кратное знаменателей его коэффициентов, получим многочлен с целыми коэффициентами, имеющий те же корни, что и $f(x)$. Поэтому достаточно научиться находить рациональные корни многочленов с целыми коэффициентами.

Теорема (о рациональных корнях многочлена). *Если несократимая дробь* m/q *является корнем многочлена* $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ *с целыми коэффициентами, то число* m *является делителем свободного члена* a_0*; число* q *является делителем старшего коэффициента* a_n*. Причем* $f(k)\vdots(m-kq)$ *для любого* $k\in\mathbb{Z}$*; в частности* $f(1)\vdots(m-q)$, $f(-1)\vdots(m+q)$.

Следствие. *Если целое число* m *является корнем многочлена с целыми коэффициентами, то* m *является делителем свободного члена.*

Сформулированная теорема дает способ нахождения всех рациональных корней многочлена с целыми коэффициентами:

1) сначала надо найти все делители m свободного члена a_0;
2) затем найти все делители q старшего коэффициента a_n;
3) составить всевозможные дроби вида m/q. Тогда все рациональные корни многочлена будут находиться среди таких дробей.
4) вычислить значения $f(m/q)$ для каждой дроби. В случае $f(m/q)=0$ получаем корень многочлена $x=m/q$. Вычисление $f(m/q)$ можно выполнять по схеме Горнера.

Приведем достаточное условие неприводимости многочленов над полем $\mathbb{Q}$.

Теорема (признак неприводимости Эйзенштейна). *Пусть* $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0$ *- многочлен с целыми коэффициентами. Если существует такое простое число p, что: 1) старший коэффициент* a_n *не делится на p;*

2) все остальные коэффициенты a_i *делятся на* p*;*

3) свободный член a_0 *не делится на* p^2*;*

тогда $f(x)$ *неприводим над полем* $\mathbb{Q}$ *рациональных чисел.*

Следствие. *Над полем* $\mathbb{Q}$ *существуют неприводимые многочлены любой натуральной степени.*

Важное значение этой теоремы состоит не только в том, что она позволяет легко доказывать неприводимость некоторых многочленов, но и в том, что она дает возможность строить такие многочлены. Например, для любого простого числа p многочлен x^n-p неприводим над $\mathbb{Q}$.

Вопросы для самоконтроля

1) Какие многочлены неприводимы над полем $\mathbb{Q}$ рациональных чисел?
2) В каком случае многочлен может быть разложен на линейные множители над полем $\mathbb{Q}$?
3) Как находятся рациональные корни многочлена с целыми коэффициентами?
4) Как найти целые корни многочлена?
5) Приведите пример многочлена третьей степени над полем рациональных чисел, имеющего ровно один корень в этом поле.
6) Сформулируйте признак неприводимости Эйзенштейна.
7) Пользуясь признаком Эйзенштейна, постройте несколько неприводимых многочленов шестой степени над полем рациональных чисел.

Примеры решения задач

Задача 1. Выясните, приводимы ли над полем $\mathbb{Q}$ данные многочлены. В случае приводимости разложите их на неприводимые множители: а) $4x^2-12x+5$; б) x^2-3x-5; в) $x^3+6x^2-15x+2$; г) x^3-2x+1.

Решение. а) Многочлен $4x^2-12x+5$ имеет рациональные корни $x_1=5/2$, $x_2=1/2$. Поэтому он приводим над $\mathbb{Q}$:

$$4x^2-12x+5=4(x-\frac{5}{2})(x-\frac{1}{2}).$$

б) Корнями многочлена x^2-3x-5 являются числа $x_{1,2}=\frac{3\pm\sqrt{29}}{2}$. Таким образом, данный многочлен *не имеет* рациональных корней, и поэтому он неприводим над $\mathbb{Q}$.

в) Найдем рациональные корни многочлена $f(x)=x^3+6x^2-15x+2$. Так как старший коэффициент ра-

вен единице, то все рациональные корни должны быть целыми и их следует искать среди делителей свободного члена $a_0 = 2$, т.е. среди чисел ± 1, ± 2. Имеем: $f(1) = -6 \neq 0$, $f(-1) = 22 \neq 0$, $f(2) = 4 \neq 0$, $f(-2) = 48 \neq 0$, поэтому целых корней нет. Итак, $f(x)$ не имеет рациональных корней, причем $\deg f(x) = 3$; следовательно, $f(x)$ - неприводим над $\mathbb{Q}$.

г) Для многочлена $f(x) = x^3 - 2x + 1$ имеем $f(1) = 0$; следовательно, $f(x)$ - приводим над $\mathbb{Q}$. Производя деление на $(x-1)$, получим $f(x) = (x-1)(x^2 + x - 1)$. Здесь многочлен $x^2 + x - 1$ неприводим над $\mathbb{Q}$, так как его корни $\frac{-1 \pm \sqrt{5}}{2}$ иррациональны.

Задача 2. Пользуясь признаком Эйзенштейна, докажите, что многочлен $5x^5 + 6x^4 - 144x^3 + 18x^2 - 42x + 12$ неприводим над полем $\mathbb{Q}$.

Решение. Замечаем, что все коэффициенты данного многочлена, кроме старшего $a_n = 5$, делятся на простое число $p = 3$, причем свободный член $a_0 = 12$ не делится на $p^2 = 9$. Следовательно, условия признака Эйзенштейна выполнены, и многочлен – неприводим.

Отметим, что признак Эйзенштейна неприменим к данному многочлену при $p = 2$. Действительно, старший коэффициент не делится на 2, а все остальные коэффициенты на 2 делятся; однако, свободный член делится на $p^2 = 4$.

Задача 3. Найдите все рациональные корни многочлена $f(x) = x^4 + 3x^3 + 4x^2 + 18x + 18$ и разложите его на неприводимые над полем $\mathbb{Q}$ множители.

Решение. Старший коэффициент многочлена $f(x)$ равен единице, поэтому многочлен может иметь только целые

корни. В силу следствия из теоремы о рациональных корнях многочлена такие корни содержатся среди делителей свободного члена. В нашем случае делителями свободного члена $a_0 = 18$ являются следующие числа: $\pm1, \pm2, \pm3, \pm6, \pm9, \pm18$. Заметим, что все коэффициенты многочлена $f(x)$ положительны, поэтому он может иметь только отрицательные корни. Итак, возможные корни $f(x)$ - это числа -1, -2, -3, -6, -9, -18. Проверим каждое из этих чисел по схеме Горнера:

	1	3	4	18	18
-1	1	2	2	16	$2 \neq 0$
-2	1	1	2	14	$-10 \neq 0$
-3	1	0	4	6	0

Число -3 является корнем многочлена $f(x)$. Остальные корни $f(x)$ являются корнями многочлена $q(x) = x^3 + 4x + 6$. Применив к $q(x)$ признак Эйзенштейна при $p = 2$, получим, что $q(x)$ - неприводим. Поэтому $q(x)$ рациональных корней иметь не может. Итак, многочлен $f(x)$ имеет единствееый рациональный корень -3, и разложение $f(x)$ на неприводимые множители имеет вид: $f(x) = (x+3)(x^3 + 4x + 6)$.

Задача 4. Найдите все рациональные корни многочлена $f(x) = 6x^5 + 7x^4 + 5x^3 + 5x^2 - x - 2$ и разложите его на неприводимые над полем $\mathbb{Q}$ множители.

Решение. Старший коэффициент данного многочлена отличен от единицы. Поэтому многочлен может иметь как целые, так и дробные корни. Для их отыскания воспользуемся теоремой о рациональных корнях многочлена. Корни данного многочлена $f(x)$ будем искать в виде $\frac{m}{q}$, где m - делители свободного члена $a_0 = -2$ и q - делители старшего ко-

эффициента $a_n = 6$, причем можно рассматривать только положительные значения q:

$$m \in d(-2) = \{\pm 1, \pm 2\}; \qquad q \in d(2) = \{1, 2, 3, 6\}.$$

Затем составим всевозможные дроби вида m/q. Далее каждое из этих чисел надо проверить по схеме Горнера. Для отсеивания чисел, которые *не могут* быть корнями, используем тот факт, что если дробь $\frac{m}{q}$ является корнем многочлена $f(x)$, то $\frac{f(1)}{m-q}$ - целое число. Проверим это условие, учитывая, что $f(1) = 20$. Результаты запишем в таблицу: вверху – строка возможных числителей дробей $\frac{m}{q}$, слева – столбец возможных знаменателей; знак + означает, что условие $\frac{f(1)}{m-q} \in \mathbb{Z}$ выполняется.

$q \backslash m$	1	-1	2	-2
1	–	+	+	–
2	+	–	–	+
3	+	+	+	+
6	+	–	+	–

Таким образом, рациональные корни многочлена $f(x)$ находятся среди чисел -1, 2, $\frac{1}{2}$, $\pm\frac{1}{3}$, $\pm\frac{2}{3}$, $\frac{1}{6}$. Проверим каждое из этих чисел по схеме Горнера. Начинаем с числа -1:

	6	7	5	5	-1	-2
-1	6	1	4	1	-2	0

Так как остаток от деления $f(x)$ на $(x+1)$ оказался равным нулю, то -1 корень $f(x)$, т.е. $f(x) = (x+1)q(x)$, где

$q(x) = 6x^4 + x^3 + 4x^2 + x - 2$. Проверим, не является ли -1 двукратным корнем, для чего полученное от деления частное $q(x)$ снова разделим на $(x+1)$:

	6	1	4	1	-2
-1	6	-5	9	-8	$6 \neq 0$

Здесь остаток равен $6 \neq 0$; следовательно, число -1 является простым корнем $f(x)$. Теперь проверим число 2. Здесь можно на $(x-2)$ делить не $f(x)$, а $q(x)$:

	6	1	4	1	-2
2	6	13	30	61	$120 \neq 0$

Из таблицы видно, что $q(2) = 120 \neq 0$. Следовательно, число 2 не является корнем $q(x)$, а значит, и $f(x)$. Проверим следующее число $1/2$. Вновь используем коэффициенты частного $q(x)$:

	6	1	4	1	-2
$1/2$	6	4	6	4	0

Здесь остаток равен нулю. Поэтому число $1/2$ является корнем $q(x)$, а значит, и $f(x)$. Запишем соответствующее разложение на множители для $f(x)$:

$$f(x) = (x+1)(x-\frac{1}{2})(6x^3 + 4x^2 + 6x + 4).$$

Заметим, что многочлен $6x^3 + 4x^2 + 6x + 4$ может иметь только отрицательные корни. Поэтому осталось проверить лишь числа $-\frac{1}{3}$ и $-\frac{2}{3}$. Запишем схему Горнера для коэффициентов многочлена $6x^3 + 4x^2 + 6x + 4$. Для числа $-2/3$ имеем:

	6	4	6	4
$-2/3$	6	0	6	0

Из таблицы видно, что $-2/3$ является корнем. Следовательно, разложение на множители для данного многочлена $f(x)$ имеет вид: $f(x)=(x+1)(x-\frac{1}{2})(x+\frac{2}{3})(6x^2+6)$. Причем многочлен $6x^2+6=6(x^2+1)$ рациональных корней не имеет.

Окончательно получаем, что исходный многочлен $f(x)$ имеет три рациональных корня: -1, $1/2$, $-2/3$; и его разложение на неприводимые над полем $\mathbb{Q}$ множители имеет вид: $f(x)=6(x+1)(x-\frac{1}{2})(x+\frac{2}{3})(x^2+1)$.

Задачи и упражнения для самостоятельного решения

1) Пользуясь признаком Эйзенштейна, докажите неприводимость над полем $\mathbb{Q}$ следующих многочленов:

   а) $2x^5-15x^3+21x-24$; б) $3x^6-20x^4+30x^2-20x+20$;

   в) $4x^7-21x^5+28x^4-14x^2-35$; г) $2x^8+14x^3-35x^2-56x+63$.

2) Найдите все рациональные корни данных многочленов:

   а) $x^3-11x^2+38x-40$; б) $3x^4+\frac{1}{2}x^3+x^2-2x+\frac{1}{2}$;

   в) $3x^4-2x^3+4x^2-x+2$; г) $8x^5-14x^4-77x^3+128x^2+45x-18$.

3) Выясните, какие из данных многочленов 2-й и 3-й степени приводимы над полем $\mathbb{Q}$ рациональных чисел. В случае приводимости разложите их на множители, неприводимые над $\mathbb{Q}$: а) $3x^2-2x-1$; б) $2x^2-3x+4$; в) $x^2-x+\frac{1}{4}$;

   г) $3x^3+4x^2+4x+4$; д) $3x^3+5x^2+5x+2$; е) $2x^3+3x^2+6x-24$;

   ж) $2x^3+12x^2+17x-2$; з) x^3+x^2-x-1.

4) Разложите многочлены на неприводимые над полем $\mathbb{Q}$ множители: а) $x^4+4x^3-2x^2-12x+9$;

   б) $x^5+x^4-6x^3-14x^2-11x-3$; в) $6x^4+19x^3-7x^2-26x+12$;

г) $24x^5+10x^4-x^3-19x^2-5x+6$.

Ответы: 2) а) $2;\ 4;\ 5$; б) $1/2;\ 1/3$; в) нет рациональных корней; г) $2;\ 3;\ 3;\ 1/4;-1/2$. **3)** а) приводим, $3(x-1)(x+1/3)$; б) неприводим, т.к. $D<0$; в) приводим, $(x-1/2)^2$; г) неприводим, т.к. нет рациональных корней; д) приводим, $3(x+2/3)(x^2+x+1)$; е) неприводим по признаку Эйзенштейна при $p=3$; ж) неприводим, т.к. нет рациональных корней; з) приводим, $(x-1)(x+1)^2$. **4)** а) $(x-1)^2(x+3)^2$; б) $(x+1)^4(x-3)$; в) $(x+3)(x-1/2)(6x^2+4x-8)$; г) $24(x-1/2)(x+2/3)(x-3/4)(x^2+x+1)$

6. ИНТЕРПОЛЯЦИОННЫЙ МНОГОЧЛЕН ЛАГРАНЖА

Основные теоретические сведения

Пусть известно значение многочлена в нескольких точках. Как восстановить в явном виде сам многочлен? Это задача «интерполяции».

Рассмотрим следующую задачу: по данной таблице

$$\begin{array}{c|c|c|c|c} x & b_1 & b_2 & \dots & b_{n+1} \\ \hline f(x) & c_1 & c_2 & \dots & c_{n+1} \end{array}$$

найти многочлен $f(x)$, принимающий в данных точках b_i заданные значения c_i, т.е. $f(b_i)=c_i$, $i=\overline{1,n+1}$, и имеющий степень n.

Теорема. *Существует единственный многочлен* $f(x)$ *степени* $\le n$ *такой, что* $f(b_i)=c_i$, $i=\overline{1,n+1}$. *Этот многочлен определяется формулой*

$$f(x)=\sum_{i=1}^{n+1} c_i \frac{(x-b_1)\dots(x-b_{i-1})(x-b_{i+1})\dots(x-b_{n+1})}{(b_i-b_1)\dots(b_i-b_{i-1})(b_i-b_{i+1})\dots(b_i-b_{n+1})}.$$

В правой части этой формулы имеется $n+1$ слагаемое, каждое из которых представляет собой многочлен n-й степени, поскольку содержит n линейных множителей.

Сформулированная теорема дает формулу, которая называется *интерполяционной формулой Лагранжа*, и позволяет по значению многочлена в $n+1$ данной точке вычислять его значения во всех других данных точках.

Вопросы для самоконтроля

1) Для чего используется интерполяционный многочлен Лагранжа?
2) Как построить интерполяционный многочлен Лагранжа? Какую степень он имеет?

Примеры решения задач

Задача 1. Найдите многочлен по данной таблице его значений

$$\begin{array}{c|c|c|c|c} x & -1 & 0 & 2 & 3 \\ \hline f(x) & 3 & -2 & 0 & 1 \end{array}.$$

Решение. Известно значение многочлена в четырех точках, поэтому его степень ≤ 3. С помощью интерполяционной формулы Лагранжа получаем:

$$f(x)=\sum_{i=1}^{4} c_i f_i(x) = 3\cdot f_1(x) - 2\cdot f_2(x) + 0\cdot f_3(x) + 1\cdot f_4(x) =$$

$$= \frac{3(x-0)(x-2)(x-3)}{(-1-0)(-1-2)(-1-3)} - \frac{2(x+1)(x-2)(x-3)}{(0+1)(0-2)(0-3)} + \frac{(x+1)(x-0)(x-2)}{(3+1)(3-0)(3-2)}.$$

После раскрытия скобок и приведения подобных членов получим:

$$f(x) = -\frac{1}{2}(x-2)(x^2-3x-2) = -\frac{1}{2}(x^3-5x^2+4x+4).$$

Для проверки результата достаточно найти значения $f(b_i)=c_i$, $i=1,2,3,4$.

Используя полученный вид $f(x)$, можно найти значение $f(x)$ в любой точке, например, $f(5)$, хотя таблица задает значения многочлена лишь в точках -1, 0, 2 и 3.

Задачи и упражнения для самостоятельного решения

1) Используя интерполяционную формулу Лагранжа, постройте многочлен $f(x) \in \mathbb{R}[x]$ такой, что:
   $f(1) = 2$, $f(2) = 1$, $f(3) = 4$, $f(4) = 3$.
2) Используя интерполяционную формулу Лагранжа, постройте многочлен $f(x) \in \mathbb{Z}_{11}[x]$ такой, что $f(1) = 8$, $f(3) = 1$, $f(7) = 4$.

7. ИСПОЛЬЗОВАНИЕ МНОГОЧЛЕНОВ ДЛЯ ПОСТРОЕНИЯ КОНЕЧНЫХ КОЛЕЦ И ПОЛЕЙ

Основные теоретические сведения

Аналогично тому, как мы построили серию конечных колец и полей $\mathbb{Z}_m$ из кольца целых чисел $\mathbb{Z}$, можно построить новую серию колец и полей из кольца многочленов $P[x]$ над любым заданным полем P. С этой целью введем отношение сравнимости многочленов.

Пусть $f(x) \in P[x]$ - унитарный многочлен, $\deg f(x) \geq 1$.

Определение. Многочлены $a(x), b(x) \in P[x]$ называются *сравнимыми по модулю данного многочлена* $f(x)$, если они дают одинаковые остатки при делении на $f(x)$.

Обозначение: $a(x) \equiv b(x) \pmod{f(x)}$.

Для сравнений многочленов имеют место все свойства, справедливые для сравнений целых чисел по модулю. В частности, сравнения многочленов можно почленно складывать, вычитать, умножать.

Отношение сравнимости по $\bmod f(x)$ является отношением эквивалентности на множестве $P[x]$. Следовательно, множество $P[x]$ можно разбить на непересекающиеся классы. К одному классу отнесем все многочлены, дающие при делении на $f(x)$ один и тот же остаток. Класс, содер-

жащий многочлен $a(x)$, обозначим $[a(x)]_f$, а множество всех классов – через $P[x]/f$. На множестве $P[x]/f$ зададим две операции - сложение и умножение, положив:

$$[a(x)]_f + [b(x)]_f = [a(x)+b(x)]_f, \quad [a(x)]_f \cdot [b(x)]_f = [a(x)\cdot b(x)]_f.$$

Теорема. *Множество классов вычетов $P[x]/f$ с определенными выше операциями сложения и умножения является коммутативным кольцом с единицей.*

Нулевым элементом этого кольца является класс $[0]_f$, единицей является класс $[1]_f$, где 1 - единица поля P. Причем нулевой класс состоит из всех таких многочленов, которые делятся на $f(x)$ без остатка. В частности, $[f(x)]_f = [0]_f$.

Теорема. *Кольцо $P[x]/f$ является полем тогда и только тогда, когда многочлен f(x) неприводим над полем P.*

Приступим к построению конечных полей.

Рассмотрим поле $P[x]/f$. В качестве P возьмем поле вычетов $\mathbb{Z}_p$, где p - простое число. В качестве $f(x)$ возьмем унитарный, неприводимый над полем $\mathbb{Z}_p$ многочлен степени n: $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$, где $a_i \in \mathbb{Z}_p$. Тогда получим конечное поле $\mathbb{Z}_p[x]/f$. Найдем число элементов этого поля.

Каждому классу $[a(x)]_f \in \mathbb{Z}_p[x]/f$ поставим в соответствие тот многочлен, который является остатком от деления всех многочленов этого класса на $f(x)$. Так как $\deg f(x) = n$, то выбранный остаток имеет вид $r(x) = c_{n-1}x^{n-1} + ... + c_1x + c_0$, где $c_i \in \mathbb{Z}_p$. Тогда поле $\mathbb{Z}_p[x]/f$ содержит столько классов, сколько разных остатков мы можем получить от деления на $f(x)$. Найдем коли-

чество таких остатков. Остаток $r(x)$ имеет n коэффициентов, причем каждый коэффициент $c_i \in \mathbb{Z}_p$, т.е. может принимать p разных значений. Тогда мы получим p^n различных наборов из n коэффициентов, и соответственно, p^n разных остатков. Следовательно, поле $\mathbb{Z}_p[x]/f$ состоит из p^n элементов.

Из проведенных рассуждений видно, что мы получили способ построения новых полей. Достаточно взять неприводимый многочлен $f(x) \in \mathbb{Z}_p[x]$ степени n, рассмотреть множество классов вычетов $\mathbb{Z}_p[x]/f$, задать в этом множестве операции сложения и умножения классов, и мы получим поле из p^n элементов.

В заключение отметим, что конечное поле из q элементов существует тогда и только тогда, когда q является простым числом или степенью простого числа: $q = p^n$, где p - простое число, n - натуральное число.

Любое конечное поле называют *полем Галуа* и обозначают $GF(q)$, где q - число элементов этого поля.

Вопросы для самоконтроля

1) Какие многочлены называются сравнимыми?
2) Перечислите свойства сравнений по модулю данного многочлена.
3) Что называется классом вычетов по модулю данного многочлена? Как определяются операции сложения и умножения классов?
4) В каком случае кольцо классов вычетов по модулю данного многочлена является полем?
5) Существует ли поле из 6, 9, 10, 16, 91, 121 элементов?
6) Как построить поле из 8 элементов?

Примеры решения задач

Задача 1. В поле $\mathbb{Z}_3[x]/f$ найдите сумму, произведение классов $[a(x)]_f$, $[b(x)]_f$ и элемент, обратный к классу $[a(x)]_f$, если $a(x)=x^2+2x+2$, $b(x)=x^2+1$, $f(x)=x^3+2x+2$.

Решение. В силу определения операций сложения и умножения классов имеем:

$$[a(x)]_f+[b(x)]_f=[2x^2+2x+3]_f=[2x^2+2x]_f,$$

$$[a(x)]_f\cdot[b(x)]_f=[(x^2+2x+2)\cdot(x^2+1)]_f=$$

$$=[x^4+2x^3+3x^2+2x+2]_f=[x^4+2x^3+2x+2]_f.$$

Упростим результат для произведения классов. Для этого многочлен x^4+2x^3+2x+2 заменим остатком от деления на модуль $f(x)=x^3+2x+2$. В процессе вычислений будем сразу преобразовывать коэффициенты многочленов по модулю 3. Имеем:

$$\begin{array}{r|l} x^4+2x^3+2x+2 & x^3+2x+2 \\ \underline{-\,x^4+2x^2+2x} & \hline x+2 \\ 2x^3+x^2+2 & \\ \underline{-\,2x^3+x+1} & \\ x^2+2x+1 & \end{array}$$

Отсюда получаем: $[a(x)]_f\cdot[b(x)]_f=[x^2+2x+1]_f$.

Найдем теперь элемент $[a(x)]_f^{-1}$. Для этого сначала найдем унитарный НОД многочленов $a(x)$ и $f(x)$, а затем получим его линейное представление.

Выполним цепочку последовательных делений алгоритма Евклида, сразу преобразуя коэффициенты:

$f(x):a(x)$

$$\begin{array}{r|l} x^3+2x^2+2 & x^2+2x+2 \\ \underline{x^3+2x^2+2x} & \overline{x+1} \\ x^2+2 & \\ \underline{x^2+2x+2} & \\ x\,(=r_1) & \end{array}$$

$a(x):r_1(x)$

$$\begin{array}{r|l} x^2+2x+2 & x \\ \underline{x^2} & \overline{x+2} \\ 2x+2 & \\ \underline{2x} & \\ 2\,(=r_2) & \end{array}$$

На последнем шаге алгоритма Евклида при делении $r_1(x)=x$ на $r_2(x)=2$ получим нулевой остаток. Тогда, $НОД(a,f)=r_2(x)=2$. Линейное представление НОД имеет вид (проверьте!):

$$2=f(x)\cdot(2x+1)+a(x)\cdot x^2.$$

Разделив последнее равенство на 2, получим:

$$1=f(x)\cdot(x+2)+a(x)\cdot 2x^2.$$

Тогда

$$[1]_f=[f(x)\cdot(x+2)]_f+[a(x)\cdot 2x^2]_f.$$

Отсюда, учитывая равенство $[f(x)\cdot(x+2)]_f=[0]_f$, имеем:

$$[a(x)]_f\cdot[2x^2]_f=[1]_f.$$

Последнее равенство означает, что элемент, обратный к классу $[a(x)]_f$, имеет вид:

$$[a(x)]_f^{-1}=[2x^2]_f.$$

Задача 2. Построить поле из восьми элементов.

Решение. Так как $8=2^3$, то в качестве поля P можно взять $\mathbb{Z}_2=\{0,1\}$, а в качестве модуля $f(x)$ - неприводимый многочлен степени $n=3$, например, $f(x)=x^3+x+1\in\mathbb{Z}_2[x]$. Тогда искомое поле – это $\mathbb{Z}_2[x]/f$.

Выпишем все элементы этого поля. Для этого рассмотрим всевозможные остатки, которые получаются от деления на $f(x)$ - это многочлены из $\mathbb{Z}_2[x]$, степень которых <3, т.е. многочлены вида ax^2+bx+c, где $a,b,c\in\mathbb{Z}_2=\{0;1\}$: $0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1$. Тогда поле $\mathbb{Z}_2[x]/f$ состоит из классов, которые порождаются этими остатками:

$$\mathbb{Z}_2[x]/f(x)=\{[0],\ [1],\ [x],\ [x+1],\ [x^2],\ [x^2+1],\ [x^2+x],\ [x^2+x+1]\}$$

Составим таблицы сложения и умножения для элементов этого поля. Сначала, для примера, найдем сумму и произведение классов $[x^2]$ и $[x^2+x]$. Для суммы имеем:

$$[x^2]+[x^2+x]=[2x^2+x]=[x],$$

здесь мы сначала сложили два данных многочлена, а затем преобразовали полученные коэффициенты, учитывая, что $2\equiv 0(\mathrm{mod}\,2)$.

Теперь найдем произведение классов, для этого сначала перемножим два данных многочлена:

$$[x^2]\cdot[x^2+x]=[x^4+x^3],$$

а затем упростим результат; для этого найдем остаток от деления x^4+x^3 на модуль $f(x)=x^3+x+1$. Имеем:

$$
\begin{array}{r|l}
x^4+x^3 & x^3+x+1 \\
\cline{2-2}
x^4 \quad +x^2+x & x+1 \\
\cline{1-1}
x^3+x^2+x & \\
\cline{1-1}
x^3 \quad +x+1 & \\
\cline{1-1}
x^2+1 &
\end{array}
$$

Окончательно получаем: $[x^2]\cdot[x^2+x]=[x^4+x^3]=[x^2+1]$.

Аналогично находятся сумма и произведение для всех остальных классов. Таблицы сложения и умножения для поля $\mathbb{Z}_2[x]/f$ выглядят следующим образом (проверьте!):

$\oplus$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

$\otimes$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Тем самым, поле из восьми элементов построено.

Задачи и упражнения для самостоятельного решения

1) Сколько элементов содержится в кольце классов вычетов $\mathbb{Z}_3[x]/(x^2-1)$. Обратим ли в этом кольце элемент $[2x+1]$?
2) Покажите, что кольцо $\mathbb{Z}_2[x]/f$, где $f(x)=x^4+x^3+x+1$, не является полем. Найдите число его элементов, укажите все обратимые элементы и найдите обратные к ним.
3) Покажите, что многочлен $f(x)=x^4+x^3+x^2+3$ неприводим над полем $\mathbb{Z}_7$. В поле $\mathbb{Z}_7[x]/f$ найдите элемент, обратный для класса $[x^2+x+3]_f$. *Ответ:* $[6x^3+2x+5]_f$
4) Найдите неприводимый многочлен над полем $\mathbb{Z}_3$, и с его помощью постройте поле из 9 элементов. Составьте таблицы для операций сложения и умножения в этом поле. Для каждого элемента этого поля укажите обратный.

8. КРИТЕРИЙ БАТЛЕРА НЕПРИВОДИМОСТИ МНОГОЧЛЕНА НАД КОНЕЧНЫМ ПОЛЕМ

Основные теоретические сведения

Если поле P конечно, то над ним существуют неприводимые многочлены любой степени. Этот факт значительно усложняет решение вопроса о неприводимости многочлена над данным полем. Приведем критерий неприводимости многочлена над конечным полем, установленный М.Батлером в 1954 году.

Теорема (критерий Батлера). *Многочлен* $f(x)\in P[x]$ *степени* n *неприводим над полем* $P=GF(q)$ *тогда и только тогда, когда выполнены условия:*

1) унитарный $НОД(f,f')=1$;

2) уравнение $z^q-z=0$ *имеет в кольце* $P[x]/f(x)$ *ровно* q *решений.*

Из этой теоремы вытекает практически удобный способ распознавания приводимости или неприводимости многочлена $f(x)$ над полем $GF(q)$. А именно:

1) Если $НОД(f, f') \neq 1$, то по теореме многочлен $f(x)$ приводим над $GF(q)$.

2) Пусть $НОД(f, f') = 1$. Тогда проверим, выполняется ли условие 2 теоремы.

Построим многочлены $\alpha_i(x) \equiv x^{iq} - x^i (\mathrm{mod}\, f)$, $i = \overline{1, n-1}$, такие, что $\alpha_i(x) = \alpha_{0i} + \alpha_{1i}x + ... + \alpha_{n-1,i}x^{n-1}$, т.е. многочлен $\alpha_i(x)$ выполняет роль остатка от деления $x^{iq} - x^i$ на $f(x)$.

Из коэффициентов многочленов $\alpha_i(x)$ составим матрицу A, при этом коэффициенты запишем в матрицу столбцами, где первый столбец – всегда нулевой:

$$A = \begin{pmatrix} 0 & \alpha_{01} & ... & \alpha_{0,n-1} \\ 0 & \alpha_{11} & ... & \alpha_{1,n-1} \\ . & . & ... & . \\ 0 & \alpha_{n-1,1} & ... & \alpha_{n-1,n-1} \end{pmatrix}.$$

Заметим, что сначала выписываются коэффициенты при меньших степенях x. В силу критерия Батлера многочлен $f(x)$ неприводим над $GF(q)$ тогда и только тогда, когда $\mathrm{rang}\, A = n-1$. В противном случае $f(x)$ - приводим.

Вопросы для самоконтроля

1) Какую степень могут иметь непрводимые многочлены над конечными полями?
2) Приведите примеры многочленов второй, третьей, четвертой степени, неприводимых над полем $\mathbb{Z}_3$.
3) Сформулируйте критерий Батлера.
4) Как проверить условия критерия Батлера?

Примеры решения задач

Задача 1. Пользуясь критерием Батлера, определите, приводим или нет над полем $GF(3)$ многочлен $f(x) = x^4 - 2$.

Решение. Сначала найдем унитарный $НОД(f, f')$. С помощью алгоритма Евклида получаем (проверьте!):

$$НОД(f, f') = НОД(x^4 - 1, x^3) = 1.$$

Так как условие 1 выполнено, то переходим к проверке условия 2. Построим многочлены $\alpha_i(x) \equiv x^{iq} - x^i \pmod f$, $i = 1,2,3$, выполняющие роль остатка от деления $x^{iq} - x^i$ на f. По условию $q = 3$ и степень многочлена $f(x)$ равна четырем. Поэтому $\alpha_i(x) \equiv x^{3i} - x^i \pmod f$, и многочлены $\alpha_i(x)$ должны иметь степень ≤ 3.

1) При $i = 1$ получаем $\alpha_1(x) \equiv x^3 - x \pmod f$.

Так как должно выполняться неравенство $\deg \alpha_1(x) \le 3$, то можно считать $\alpha_1(x) = x^3 - x$. Откуда, учитывая равенство $-1 \equiv 2 (\mathrm{mod}\, 3)$, находим

$$\alpha_1(x) = x^3 - x = x^3 + 2x = 0 + 2x + 0 \cdot x^2 + 1 \cdot x^3.$$

2) При $i = 2$ получаем $\alpha_2(x) \equiv x^6 - x^2 \pmod f$.

Здесь многочлен $\alpha_2(x)$ - это остаток от деления многочлена $x^6 - x^2$ на $f(x) = x^4 - 2$. Выполняя деление уголком, находим остаток x^2. Значит,

$$\alpha_2(x) = x^2 = 0 + 0 \cdot x + 1 \cdot x^2 + 0 \cdot x^3.$$

3) При $i = 3$ получаем $\alpha_3(x) \equiv x^9 - x^3 \pmod f$.

Выполняя деление уголком многочлена $x^9 - x^3$ на $f(x) = x^4 - 2$, находим остаток $2x^3 + x$. Значит,

$$\alpha_3(x) = 2x^3 + x = 0 + 1 \cdot x + 0 \cdot x^2 + 2x^3 .$$

Многочлены $\alpha_i(x) \equiv x^{iq} - x^i \pmod f$, $i = 1,2,3$, построены.

Теперь составим матрицу A, записав в ее первый столбец нули, а в остальные столбцы – коэффициенты построенных многочленов $\alpha_i(x)$ по убывающим степеням x. Получим:

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix}.$$

Вычислим ранг этой матрицы и сравним его с числом $n-1$, где $n = 4$ - это степень данного многочлена $f(x)$. Имеем:

$$\operatorname{rang} A = 2 < n - 1 = 3 \quad \text{(Проверьте!)}$$

Следовательно, в силу критерия Батлера многочлен $f(x) = x^4 - 2$ приводим над $GF(3)$. Нетрудно показать, что разложение $f(x)$ на неприводимые множители над $GF(3)$ имеет вид $f(x) = (x^2 + 2x + 2)(x^2 + x + 2)$.

Задачи и упражнения для самостоятельного решения

1) Пользуясь критерием Батлера, определите, приводимы или нет над полем $GF(2)$ многочлены $x^2 + 1$ и $x^3 + x + 1$.
2) Пользуясь критерием Батлера, определите, приводимы или нет над полем $GF(3)$ многочлены $x^3 + x^2 + 1$ и $x^4 + x^3 + x + 2$. В случае приводимости - разложите на неприводимые множители.

ТЕСТОВЫЕ ЗАДАНИЯ

1. Многочлен $f(x)=a_nx^n+\ldots+a_1x+a_0$ с целыми коэффициентами неприводим над полем рациональных чисел, если существует простое число p такое, что:

1) $a_n\not\vdots p$, $a_i\vdots p(i=\overline{0,n-1})$, $a_0\not\vdots p^2$;

2) $a_n\not\vdots p^2$, $a_i\vdots p(i=\overline{1,n})$, $a_0\not\vdots p$;

3) $a_n\not\vdots p^2$, $a_i\vdots p(i=\overline{0,n})$, $a_0\not\vdots p^2$;

4) $a_i\vdots p(i=\overline{0,n})$, $a_0\not\vdots p^2$.

2. Наибольший общий делитель многочленов $f,g\in\mathbb{Q}[x]$, где $f(x)=x^5+3x^4+x^3+x^2+3x+1$, $g(x)=x^4+2x^3+x+2$, имеет вид: 1) $x+1$; 2) x^3+1; 3) $x+2$; 4) 1.

3. Укажите, какие из данных многочленов неприводимы над полем $\mathbb{Q}$ рациональных чисел: а) x^4+5x^2+3;

б) $3x^{25}+4x^8+2$; в) $x^{94}-2x^2+1$; г) x^6+2x^3-8.

4. Разложение многочлена $f(x)=x^5-7x^3-12x^2+6x+36$ на неприводимые множители над полем $\mathbb{Q}$ рациональных чисел имеет вид:

1) $(x-2)(x-3)(x^3+x^2-6)$; 2) $(x+2)(x-3)(x^3+x^2+6)$;

3) $(x+2)(x^4-9x^3+6x^2-6x+18)$; 4) $(x+2)(x-3)(x^3+x^2-6)$.

5. Найдите кратность корня $x_0=-2$ для многочлена $x^5+7x^4+16x^3+8x^2-16x-16\in\mathbb{Q}[x]$: 1) 4; 2) 3; 3) 2; 4) 1.

6. Какова наибольшая степень многочленов $f(x)\in\mathbb{R}[x]$, неприводимых над полем $\mathbb{R}$ действительных чисел?

1) 1; 2) 2; 3) 4, 4) наибольшей степени нет

7. Какое наибольшее число различных целых корней может иметь многочлен $a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0\in\mathbb{Z}[x]$, если $a_n=3$, $a_0=9$? 1) 8; 2) 4; 3) 6, 4) 3

8. Известно, что многочлен $x^4+x^3+x^2-4x+10$ имеет корень $x_0=1+i$. Укажите, какое из следующих чисел обязано быть корнем этого многочлена:

1) i; 2) $-1-i$; 3) $-1+i$; 4) $1-i$

9. Число α является k-кратным корнем многочлена $f(x)$, если: 1) $f(\alpha)=0$; 2) $f(\alpha^k)=0$;

3) $f(x)=(x-\alpha)^k q(x)$ для некоторого $q(x)$;

4) $f(x)=(x-\alpha)^k q(x)$, где $q(\alpha)\neq 0$.

10. Кратность корня $x_0=2$ многочлена $x^2(x-2)^3(x^2+7)$ над полем $\mathbb{Z}_{11}$ равна: 1) 2; 2) 3; 3) 4; 4) 0.

11. Разложение многочлена $x^4-3x^3+2x^2-4x-11$ на неприводимые множители над полем $\mathbb{Z}_5$ имеет вид:

1) $(x+1)(x+2)(x^2+x-2)$; 2) $(x-1)(x^3+3x^2+1)$;

3) $(x-1)^2(x-2)^2$; 4) $(x+4)^2(x+2)^2$.

12. В поле $\mathbb{Z}_3[x]/f$ найдите произведение классов $[a(x)]_f$ и $[b(x)]_f$, если $a(x)=2x+2$, $b(x)=x^2+x+2$, $f(x)=x^3+x^2+2$.

1) $2x^2$; 2) $2x^3+x^2+1$; 3) x^2+x+2; 4) $2x^2+1$.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Глухов, М. М. Алгебра [Текст] : учебник. В 2-х т. Т. 1. / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. – М. : Гелиос АРВ, 2003. – 336 с. – ISBN 8-85438-071-4.

2. Глухов, М. М. Алгебра [Текст] : учебник. В 2-х т. Т. 2. / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. – М. : Гелиос АРВ, 2003. – 416 с. – ISBN 8-85438-072-2.

3. Глухов, М. М. Алгебра и аналитическая геометрия [Текст] : учеб. пособие / М. М. Глухов. – М. : Гелиос АРВ, 2005. – 392 с. – ISBN 5-85438-054-4.

4. Солодовников, А. С. Задачник-практикум по алгебре [Текст] : учеб. пособие / А. С. Солодовников, М. А. Родина. – М. : Просвещение, 1985. – Ч. 4. – 127 с.

5. Майорова, С. П. Алгебра : Курс лекций [Текст] : учеб. пособие [Электронный ресурс] / С. П. Майорова, М. Г. Завгородний. – Воронеж : ГОУ ВПО "Воронежский государственный технический университет", 2010. – Ч. 2. – электрон. опт. диск.

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для организации самостоятельной работы
по дисциплине «Алгебра и геометрия»
для студентов специальностей
10.05.02 «Информационная безопасность
телекоммуникационных систем»,
10.05.03 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Составители:
Майорова Светлана Павловна
Завгородний Михаил Григорьевич

В авторской редакции

Компьютерный набор С.П. Майоровой

Подписано к изданию 20.05.2015.
Уч.- изд. л. 2,7.

ФГБОУ ВПО «Воронежский государственный
технический университет»
394026 Воронеж, Московский просп., 14