МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ОСНОВЫ ВЫСШЕЙ АЛГЕБРЫ

Учебное пособие

ПЕНЗА 2005

УДК 517.

Рассматриваются такие разделы высшей алгебры, как основы теории чисел; основные алгебраические структуры; теория многочленов. Приведены основные теоретические сведения и примеры с подробным решением. Составлено достаточное количество задач для упражнений.

Учебное пособие подготовлено на кафедре «Высшая и прикладная математика» и предназначено для студентов различных технических специальностей при изучении курса «Высшая математика».

Библиогр. 8 назван.

Составитель: *Кудряшова Н.Ю.*

Рецензенты:

А.М. Данилов, д.т.н., профессор, заведующий кафедрой «Высшая математика» Пензенского государственного университета архитектуры и строительства;

В.И. Паньженский, профессор, декан физико-математического факультета Пензенского государственного педагогического университета.

Введение

Высшая алгебра представляет собой естественное обобщение основного школьного курса элементарной алгебры.

Учебное пособие предназначено для студентов технических специальностей и состоит из трех частей.

В первой части учебного пособия освещаются такие вопросы, как теория делимости, основные функции теории чисел и сравнения.

Во второй части изучению подвергаются немногие, наиболее важные типы алгебраических систем, т е. множеств, составленных из элементов какой-либо природы, для которых определены некоторые алгебраические операции. Таковы, в частности, поля, кольца и группы. Теория полей оказалась естественной областью для дальнейшего развития теории уравнений, а ее основные ветви — теория полей алгебраических чисел и теория полей алгебраических функций — связали ее соответственно с теорией чисел и теорией функций комплексного переменного. Более широким, чем понятие поля, является понятие кольца. Простейшими примерами колец служат совокупность всех целых чисел (включая и отрицательные), система многочленов от одного неизвестного и система действительных функций действительного переменного. Теория колец включает в себя такие старые ветви алгебры, как теория гиперкомплексных систем и теория идеалов, она связана с рядом математических наук, в частности с функциональным анализом, и уже нашла некоторые выходы в физику. Еще большую область применений имеет теория групп. Группы играли большую роль уже в теории Галуа, в вопросе о разрешимости уравнений в радикалах, сейчас же они являются важным орудием в теории полей, во многих разделах геометрии, в топологии, а также и в кристаллографии, в теоретической физике. Вообще, по широте области приложений теория групп занимает среди всех ветвей алгебры следующее после линейной алгебры место.

Третья часть учебного пособия посвящена изучению уравнений от одного неизвестного произвольной степени. Учитывая существование формулы для решения квадратных уравнений, естественно было искать аналогичные формулы для уравнений более высоких степеней. Исторически этот отдел алгебры так и развивался, причем формулы для решения уравнений третьей и четвертой степени были найдены еще в XVI веке. После этого начались безуспешные поиски формул, которые выражали бы корни уравнений пятой и более высоких степеней через коэффициенты этих уравнений при помощи радикалов. Эти поиски продолжались до начала XIX века, когда было, наконец, доказано, что такие формулы не могут быть найдены и что для всех степеней, начиная с пятой, существуют даже конкретные примеры уравнений с целочисленными коэффициентами, корни которых не могут быть записаны при помощи радикалов.

Отсутствие формул для решения уравнений высоких степеней не следует считать очень печальным обстоятельством — даже в случае уравнений третьей и четвертой степени, где такие формулы существуют, они очень громоздки и практически почти бесполезны. С другой стороны, коэффициенты тех уравнений, которые приходится решать физикам или инженерам, являются обычно величинами, полученными в результате измерений, т. е. известны лишь приближенно, а поэтому и корни нужно знать лишь приближенно, с заданной точностью. Это привело к разработке различных методов приближенного решения уравнений.

Часть 1. Основы теории чисел

1. Теория делимости

Теория чисел занимается изучением свойств целых чисел. Целыми мы будем называть не только числа натурального ряда 1, 2, 3, … (положительные целые), но также нуль и отрицательные целые —1, —2, —3, …

Сумма, разность и произведение двух целых *a* и b будут также целыми, но частное от деления *a* на b (если b не равно нулю) может быть как целым, так и не целым.

В случае, когда частное от деления *a* на *b* — целое, обозначая его буквою *q,* имеем *a=bq,* т. е. *a равно произведению b на целое.* Мы говорим тогда, что *a делится* на *b* или что *b делит a*. При этом *a* называем *кратным* числа *b и b — делителем* числа *a.* То обстоятельство, что *b* делит *a*, записывается так; *b\a*.

Имеют место две следующие теоремы.

Теорема 1.1.1 *Если a кратно m,m кратно b, то a кратно b.*

Действительно, из $a = a_1 m$, $m = m_1 b$ следует $a = a_1 m_1 b$, где $a_1 m_1$ — целое. А это и доказывает теорему.

Теорема 1.1.2 *Если в равенстве вида* $k+l+\ldots+n=p+q+\ldots+s$ *относительно всех членов, кроме какого-либо одного, известно, что они кратны b, то и этот один член кратен b.*

В общем случае, включающем, как частный, и случай, когда *a* делится на *b,* имеем теорему:

Теорема 1.1.3 *Всякое целое a представляется единственным способом через положительное целое b* в виде

$a = bq + r;\ 0 \le r < b.$

Число *q* называется *неполным частным,* а число *r* – остатком от деления *a* на *b.*

Пример1.1.1. Пусть *b*= 14. Имеем

$$177 = 14 \cdot 12 + 9; \qquad 0 < 9 < 14,$$
$$-64 = 14 \cdot (-5) + 6; \quad 0 < 6 < 14,$$
$$154 = 14 \cdot 11 + 0; \qquad 0 = 0 < 14.$$

1.1 Наибольший общий делитель

Всякое целое, делящее одновременно целые *a, b, …, l*, называется их *общим делителем.* Наибольший из общих делителей называется *общим наибольшим делителем* и обозначается символом *(a, b, …,l).* Ввиду конечности числа общих делителей существование общего наибольшего делителя очевидно. Если *(a, b, …, l)* = 1, то *a, b,…,l* называются *взаимно простыми.* Если каждое из чисел *a, b,…,l* взаимно просто с каждым другим из них, то *a, b,…,l* называются *попарно простыми.* Очевидно, числа попарно простые всегда и взаимно простые; в случае же двух чисел понятия «попарно простые» и «взаимно простые» совпадают.

Пример 1.1.2. Числа 6, 10, 15 ввиду (6, 10, 15) = 1 — взаимно простые. Числа 8, 13, 21 ввиду (8, 13) =(8, 21) = (13, 21) = 1—попарно простые.

Теорема 1.1.4. *Если a кратно b, то совокупность общих делителей чисел a и b совпадает с совокупностью делителей одного b; в частности, (a, b) = b.*

Действительно, всякий общий делитель чисел *a* и *b* является делителем и одного *b.* Обратно, раз *a* кратно *b,* то всякий делитель числа *b* является также делителем числа a, т. е. он будет общим делителем чисел *b* и a. Таким образом, совокупность общих делителей чисел *a и. b* совпадает с совокупностью делителей одного *b.* А так как наибольший делитель числа *b* есть само *b,* то (*a, b) = b.*

Теорема 1.1.5 *Если a = bq +c, то совокупность общих делителей чисел a и b совпадает с совокупностью общих делителей чисел b и c; в частности, (a, b)=(b, c).*

Для разыскания общего наибольшего делителя, а также для вывода его важнейших свойств применяется ***алгоритм Евклида***. Последний состоит в следующем. Пусть a и b — положительные целые. Находим ряд равенств:

$$\begin{aligned} a &= bq_1 + r_2, \qquad 0 < r_2 < b, \\ b &= r_2 q_2 + r_3, \qquad 0 < r_3 < r_2, \\ r_2 &= r_3 q_3 + r_4, \qquad 0 < r_4 < r_3, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, \; 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n, \end{aligned} \tag{1.1.1}$$

заканчивающийся, когда получаем некоторое $r_{n+1} = 0$. Последнее неизбежно, так как ряд b, r_2, r_3, … как ряд убывающих целых не может содержать более чем b положительных.

Рассматривая равенства (1.1.1), идя сверху вниз, убеждаемся, что общие делители чисел a и b одинаковы с общими делителями чисел b и r_2, далее одинаковы с общими делителями чисел r_2 и r_3, чисел r_3 и r_4,…, чисел r_{n-1} и r_n, наконец, с делителями одного числа r_n. Одновременно с этим имеем

$$(a,b) = (b,r_2) = (r_2,r_3) = \ldots = (r_{n-1},r_n) = r_n.$$

Мы приходим к следующим результатам.

1. *Совокупность общих делителей чисел a и b совпадает с совокупностью делителей их общего наибольшего делителя.*

2. Этот общий наибольший делитель равен r_n, т.е. последнему не равному нулю остатку алгоритма Евклида.

Пример 1.1.3. Применим алгоритм Евклида к отысканию (525,231). Находим

$$
\begin{array}{r|l}
525 & 231 \\
\underline{462} & 2 \\
\end{array}
$$

$$
\begin{array}{r|l}
231 & 63 \\
\underline{189} & 3 \\
\end{array}
$$

$$
\begin{array}{r|l}
63 & 42 \\
\underline{42} & 1 \\
\end{array}
$$

$$
\begin{array}{r|l}
42 & 21 \\
\underline{42} & 2 \\
\end{array}
$$

""

$$525 = 231 \cdot 2 + 63,$$
$$231 = 63 \cdot 3 + 42,$$
$$63 = 42 \cdot 1 + 21,$$
$$42 = 21 \cdot 2.$$

Здесь последний положительный остаток есть r_4=21. Значит, (525, 231) =21.

Свойства наибольшего общего делителя (НОД)

1 Обозначая буквой *m* любое положительное целое, имеем (*am, bm*) = (*a,b*)*m.*

2 Обозначим буквой δ любой общий делитель чисел *a* и *b,* имеем $\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a,b)}{\delta}$; в частности, имеем $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$- т.е- частные от деления двух чисел на их общий наибольший делитель суть числа взаимно простые.

3 Если *(a,b)*=1, то *(ac,b)=(c,b).*

4 Если *(a,b)*=1 и *ac* делится на *b,* то *c* делится на *b.*

5 Если каждое $a_1, a_2, ..., a_m$ взаимно просто с каждым $b_1, b_2, ..., b_n$, то и произведение $a_1 a_2 \cdots a_m$ взаимно просто с произведением $b_1 b_2 \cdots b_n$.

Задача отыскания общего наибольшего делителя более чем двух чисел сводится к таковой для двух чисел. Именно, чтобы найти общий наибольший делитель чисел $a_1, a_2, ..., a_m$, составляем ряд чисел:

$$(a_1, a_2) = d_2, \quad (d_2, a_3) = d_3, \quad (d_3, a_4) = d_4, \quad \ldots, (d_{n-1}, a_n) = d_n.$$

Число d_n и будет общим наибольшим делителем всех данных чисел.

1.2 Общее наименьшее кратное

Всякое целое, кратное всех данных чисел, называется их *общим, кратным.* Наименьшее положительное общее кратное называется *общим наименьшим кратным.* Найдем общее кратное двух чисел *a* и *b.* Пусть $(a,b)=d$, $a=a_1d$, $b=b_1d$ и, следовательно, $(a_1,b_1)=1$. Пусть *M* — какое-либо общее кратное *a* и *b.* Так как *M* кратно *a*, то $M = ak$, где *k* — целое. Но *M* кратно и *b.* Поэтому

$$\frac{ak}{b}=\frac{a_1k}{b_1}$$

должно быть целым и, следовательно, *k* должно делиться на b_1. Поэтому $k = b_1t = \frac{b}{d}t$, где *t*—целое, причем для *M* получаем формулу

$$M = \frac{ab}{d}t \qquad (1.1.2)$$

Обратно, очевидно, что *M,* представляемое формулой (1.1.2), при любом целом *t* будет общим кратным *a* и *b,* и, таким образом, формула (1.1.2) дает общий вид всех общих кратных чисел *а к b.*

Наименьшее положительное из этих общих кратных, т. е. общее наименьшее кратное, получим при $t=1$. Оно будет

$$m = \frac{ab}{d} \qquad (1.1.3)$$

Теперь формулу (1) можно переписать так:

$$M = mt \qquad (1.1.4)$$

Формулы (1.1.3) и (1.1.4) приводят к теоремам:

Теорема 1.1.6. *Совокупность общих кратных двух чисел совпадает с совокупностью кратных их общего наименьшего кратного.*

Теорема 1.1.7. *Это общее наименьшее кратное двух чисел равно их произведению, деленному на их общий наибольший делитель.*

Пусть требуется найти общее наименьшее кратное более чем двух чисел $a_1, a_2, ..., a_n$. Обозначая вообще символом *[a, b]* общее наименьшее кратное чисел *a* и *b*, составим ряд чисел:

$$[a_1, a_2] = m_2, \quad [m_2, a_3] = m_3, \quad \ldots, [m_{n-1}, a_n] = m_n.$$

Полученное таким путем m_n и будет общим наименьшим кратным всех данных чисел.

Справедлива следующая теорема:

Теорема 1.1.8 *Общее наименьшее кратное попарно простых чисел равно их произведению.*

1.3 Разложение чисел в непрерывные дроби

Пусть α — любое вещественное число. Обозначим буквой q_1 наибольшее целое, не превосходящее α. При нецелом α имеем

$$\alpha = q_1 + \frac{1}{\alpha_2}; \alpha_2 > 1.$$

Точно так же при нецелых $a_2, \ \ldots, \ a_{s-1}$ имеем

$$\alpha_2 = q_2 + \frac{1}{\alpha_3}; \alpha_3 > 1;$$

……

$$\alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s}; \alpha_s > 1,$$

ввиду чего получаем следующее *разложение α в непрерывную дробь:*

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}}} \qquad (1.1.5)$$

Если α иррациональное, то и всякое α_s иррациональное и указанный процесс может быть неограниченно продолжен.

Если же α рациональное и, следовательно, может быть представлено рациональной несократимой дробью с положительным знаменателем: $\alpha = \frac{a}{b}$,

то указанный процесс будет конечен и может быть выполнен с помощью алгоритма Евклида. Действительно, имеем:

$$a = bq_1 + r_2; \qquad \frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_2}},$$

$$b = r_2 q_2 + r_3; \qquad \frac{b}{r_2} = q_2 + \frac{1}{\frac{r_2}{r_3}},$$

……

$$r_{n-2} = r_{n-1} q_{n-1} + r_n; \qquad \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},$$

$$r_{n-1} = r_n q_n; \qquad \frac{r_{n-1}}{r_n} = q_n,$$

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}}}.$$

Числа q_1 q_2, ..., участвующие в разложении числа α в непрерывную дробь, называются *неполными частными (*в случае рационального α это будут неполные частные последовательных делений алгоритма Евклида), дроби же

$$\delta_1 = q_1, \quad \delta_2 = q_1 + \frac{1}{q_2}, \quad \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}, \quad \ldots$$

называются *подходящими дробями.*

Пример 1.1.4 Разложим в непрерывную дробь число $\frac{105}{38}$.

$$
\begin{array}{r|l}
105 & 38 \\
\underline{76} & 2 \\
\cline{1-2}
38 & 29 \\
\underline{29} & 1 \\
\cline{1-2}
29 & 9 \\
\underline{27} & 3 \\
\cline{1-2}
9 & 2 \\
\underline{8} & 4 \\
\cline{1-2}
2 & 1 \\
\underline{2} & 2 \\
\cline{1-2}
\end{array}
$$

""

$$\frac{105}{38} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}}.$$

1.4 Каноническое разложение числа

Число 1 имеет только один положительный делитель, именно 1. В этом отношении число 1 в ряде натуральных чисел стоит особо.

Всякое целое, большее 1, имеет не менее двух делителей, именно 1 и самого себя; если этими делителями исчерпываются все положительные делители целого числа, то оно называется *простым*. Целое > 1, имеющее кроме 1 и самого себя другие положительные делители, называется *составным.*

Всякое целое a или взаимно просто с данным простым p, или же делится на p.

Если произведение нескольких сомножителей делится на p, то, по крайней мере, один из сомножителей делится на p.

Теорема 1.1.9 *Всякое целое, большее единицы, разлагается на произведение простых сомножителей и притом единственным способом, если отвлечься от порядка следования сомножителей.*

В разложении числа *a* на простые сомножители некоторые из них могут повторяться. Обозначая буквами $p_1, p_2, ..., p_k$ различные из них и буквами $\alpha_1, \alpha_2, ..., \alpha_k$ кратность их вхождения в *a,* получим так называемое *каноническое разложение числа a на сомножители:*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Пример 1.1.5 Каноническое разложение числа 588000 будет: $588000 = 2^5 \cdot 3 \cdot 5^3 \cdot 7^2$

Пусть $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *— каноническое разложение числа a. Тогда все делители a суть все числа вида*

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k};\ 0 \le \beta_1 \le \alpha_1,\quad 0 \le \beta_2 \le \alpha_2, \ldots, 0 \le \beta_k \le \alpha_k. \qquad (1.1.6)$$

Пример 1.1.6 Все делители числа 720 = $2^4 \cdot 3^2 \cdot 5$ получим, если в выражении $2^{\beta_1} 3^{\beta_2} 5^{\beta_3}$ заставим $\beta_1, \beta_2, \beta_3$ независимо друг от друга пробегать значения β_1=0, 1, 2, 3, 4; β_2=0, 1, 2; β_3=0, 1. Поэтому указанные делители будут: 1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144, 5, 10, 20, 40, 80, 15, 30, 60, 120, 240, 45, 90, 180, 360, 720.

2. Функции теории чисел.

2.1 Функция [*x*] определяется для всех вещественных *x* и представляет собою наибольшее целое, не превосходящее *x.* Эта функция называется *целой частью от x.*

Пример 1.2.1 [7]=7; [2,6] = 2; [-4,75] =-5.

2.2 Функция { *x* } = x — $[x]$ называется *дробной частью от x.*

Пример 1.2.2.

{7}=0; {2,6}= 0,6; {-4,75} =0,25.

Функция $\theta(a)$ называется *мультипликативной,* если выполнены следующие условия.

1. *Функция* $\theta(a)$ *определена для всех целых положительных a и не обращается в нуль хотя бы при одном таком a.*

2. *Для любых положительных взаимно простых* a_1 *и* a_2 *имеем*

$$\theta(a_1 a_2) = \theta(a_1)\theta(a_2)$$

Пример 1.2.3 Нетрудно видеть, что мультипликативной будет

функция $\theta(a) = a^s$, где *s* — любое вещественное или комплексное число.

Пусть $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ - каноническое разложение числа а.

Рассмотрим функцию, которая представляет собой сумму делителей *S(a)* числа *a.* Справедлива формула

$$S(a) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

Пример 1.2.4.

$$\text{S(720)=S}(2^4 \cdot 3^2 \cdot 5) = \frac{2^{4+1} - 1}{2 - 1} \cdot \frac{3^{2+1} - 1}{3 - 1} \cdot \frac{5^{1+1} - 1}{5 - 1} = 2418.$$

Функция $\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_k + 1)$ представляет число делителей числа *a.*

Пример 1.2.5.

$$\tau(720) = (4+1)(2+1)(1+1) = 30.$$

2.3 ***Функция Мёбиуса*** $\mu(a)$ определяется для всех целых положительных *a.* Она задается равенствами: $\mu(a)$=0, если *a* делится на квадрат, отличный от единицы; $\mu(a) = (-1)^k$, если *a* не делится на квадрат, отличный от единицы, при этом *k* обозначает число простых делителей числа *a;* в частности, при $a = 1$ считаем *k=0,* поэтому принимаем $\mu(1) = 1$.

Пример 1.2.6.

$$\begin{aligned}
&\mu(1) = 1, \quad &&\mu(5) = -1, \quad &&\mu(9) = 0,\\
&\mu(2) = -1, \quad &&\mu(6) = 1, \quad &&\mu(10) = 1,\\
&\mu(3) = -1, \quad &&\mu(7) = -1, \quad &&\mu(11) = -1,\\
&\mu(4) = 0, \quad &&\mu(8) = 0, \quad &&\mu(12) = 0.
\end{aligned}$$

2.4 Функция Эйлера $\varphi(a)$ определяется для всех целых положительных *a* и представляет собою число чисел ряда 0, 1, …, а-1, взаимно простых с *a.*

Пример 1.2.7.

$$\begin{aligned}
&\varphi(1) = 1, \quad \varphi(4) = 2,\\
&\varphi(2) = 1, \quad \varphi(5) = 4,\\
&\varphi(3) = 2, \quad \varphi(6) = 2.
\end{aligned}$$

Пусть $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ — *каноническое разложение числа a.* Тогда

$$\varphi(a) = a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

или также

$$\varphi(a) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1})\ldots(p_k^{\alpha_k} - p_k^{\alpha_k-1})$$

в частности,

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}, \quad \varphi(p) = p-1.$$

3 Сравнения

Будем рассматривать целые числа в связи с остатками от деления их на данное целое положительное m, которое назовем *модулем.*

Каждому целому числу отвечает определенный остаток от деления его на m; если двум целым a и b отвечает один и тот же остаток r, то они называются *равноостаточными* по модулю m или *сравнимыми* по модулю m.

Сравнимость чисел a и b по модулю m записывается так:

$$a \equiv b (\mathrm{mod}\ m),$$

что читается: a сравнимо с b по модулю m.

Сравнимость чисел a и b по модулю m равносильна:

1. *Возможности представить a в виде a=b+mt, где t — целое.*
2. *Делимости a—b на m.*

3.1. Свойства сравнений.

1. *Два числа, сравнимые с третьим, сравнимы между собою.*
2. *Сравнения можно почленно складывать.*

Действительно, пусть

$$a_1 \equiv b_1 (\mathrm{mod}\ m), \quad a_2 \equiv b_2 (\mathrm{mod}\ m), \quad ..., a_k \equiv b_k (\mathrm{mod}\ m). \qquad (1.3.1)$$

Тогда

$$a_1 = b_1 + mt_1, \quad a_2 = b_2 + mt_2 \quad a_k = b_k + mt_k, \qquad (1.3.2)$$

откуда

$$a_1 + a_2 + \ldots + a_k = b_1 + b_2 + \ldots + b_k + m(t_1 + t_2 + \ldots + t_k),$$

или

$$a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \pmod{m}.. \qquad (1.3.3)$$

Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, переменив знак на обратный.

К. каждой части сравнения можно прибавить любое число, кратное модуля.

3 Сравнения можно почленно перемножать.

Рассмотрим сравнения (1.3.1) и вытекающие из них равенства (1.3.2). Тогда

$$a_1 a_2 \cdots a_k \equiv b_1 b_2 \cdots b_k \pmod{m}. \qquad (1.3.4)$$

Обе части сравнения можно возвести в одну и ту же степень.

Обе части сравнения можно умножить на одно и то же целое.

Свойства 2 и 3 можно обобщить следующей теоремой.

Теорема 1.3.1. *Если в выражении многочлена с целыми коэффициентами* $S = \sum A_{\alpha_1,\ldots\alpha_k} x_1^{\alpha_1} \cdots x_k^{\alpha_k}$ *заменим* $A_{\alpha_1,\ldots,\alpha_k}$, $x_1,\ldots x_k$ *числами* $B_{\alpha_1,\ldots\alpha_k}$, $y_1,\ldots y_k$, *сравнимыми с прежними по модулю m, то новое выражение S будет сравнимо с прежним по модулю m.*

Действительно, из

$$A_{\alpha_1,\ldots,\alpha_k} \equiv B_{\alpha_1,\ldots,\alpha_k} \pmod{m},$$

$$x_1 \equiv y_1 \pmod{m}, \quad \ldots, x_k \equiv y_k \pmod{m}$$

находим

$$x_1^{\alpha_1} \equiv y_1^{\alpha_1} \pmod{m}, \quad \ldots, x_k^{\alpha_k} \equiv y_k^{\alpha_k} \pmod{m},$$

$$A_{\alpha_1,\ldots\alpha_k} x_1^{\alpha_1} \cdots x_k^{\alpha_k} \equiv B_{\alpha_1,\ldots\alpha_k} y_1^{\alpha_1} \cdots y_k^{\alpha_k} \pmod{m},$$

откуда, суммируя, получим

$$\sum A_{\alpha_1,\ldots\alpha_k} x_1^{\alpha_1} \cdots x_k^{\alpha_k} \equiv \sum B_{\alpha_1,\ldots\alpha_k} y_1^{\alpha_1} \cdots y_k^{\alpha_k} \pmod{m}.$$

Если $a \equiv b(\mathrm{mod}\, m), \quad a_1 \equiv b_1(\mathrm{mod}\, m), \quad ..., a_n \equiv b_n(\mathrm{mod}\, m), \quad x \equiv x_1(\mathrm{mod}\, m)$,

то

$$ax^n + a_1x^{n-1} + ... + a_n \equiv bx^n + b_1x^{n-1} + ... + b_n(\mathrm{mod}\, m).$$

4 Обе части сравнения можно разделить на их, общий делитель, если последний взаимно прост с модулем.

5 Обе части сравнения и модуль можно умножить на одно и то же целое.

Действительно, из $a \equiv b(\mathrm{mod}\, m)$ следует

$$a=b+mt,\ ak=bk+mkt$$

и, следовательно, $ak \equiv bk(\mathrm{mod}\, mk)$.

6 Обе части сравнения и модуль можно разделить на любой их общий делитель.

7 Если сравнение $a \equiv b$ *имеет место по нескольким модулям, то оно имеет место и по модулю, равному общему наименьшему кратному этих модулей.*

8 Если сравнение имеет место по модулю m, то оно имеет место и по модулю d, равному любому делителю числа m.

9 Если одна часть сравнения и модуль делятся на какое-либо число, то и другая часть сравнения должна делиться на то же число.

Пример 1.3.1 Найдем остаток от деления $\left(5^{100}+55\right)^{100}$ на 24.

Имеем $5^2 \equiv 1(\mathrm{mod}\ 24)$, поэтому $5^{100} \equiv 1(\mathrm{mod}\ 24)$. Прибавляя к обеим частям сравнения по 55, получаем:

$$5^{100}+55 \equiv 56 \equiv 8(\mathrm{mod}\ 24).$$

Имеем: $8^2 \equiv (-8)(\mathrm{mod}\ 24)$, поэтому $8^{2k} \equiv (-8)(\mathrm{mod}\ 24)$ при любом $k \in N^+$. Следовательно,

$$\left(5^{100}+55\right)^{100} \equiv (-8)(\mathrm{mod}\, 24).$$

Поскольку $(-8) \equiv 16(\mathrm{mod}\ 24)$, искомым остатком является 16.

3.2 Система вычетов

Числа равноостаточные, или, что то же самое, сравнимые по модулю m, образуют *класс чисел по модулю m.*

Из такого определения следует, что всем числам класса отвечает один и тот же остаток r, и мы получим все числа класса, если в форме $mq+r$ заставим q пробегать все целые числа.

Соответственно да различным значениям r имеем m классов чисел по модулю m

Любое число класса называется *вычетом по модулю m* по отношению ко всем числам того же класса. Вычет, получаемый при q=0, равный самому остатку r, называется *наименьшим неотрицательным вычетом.*

Вычет ρ, самый малый по абсолютной величине, называется *абсолютно наименьшим вычетом.*

Очевидно, при $r < \frac{m}{2}$ имеем $\rho = r$; при $r > \frac{m}{2}$ имеем $\rho = r - m$; наконец, если m четное и $r = \frac{m}{2}$ то за ρ можно принять любое из двух чисел $\frac{m}{2}$ и $\frac{m}{2} - m = -\frac{m}{2}$.

Взяв от каждого класса по одному вычету, получим *полную систему вычетов по модулю m.* Чаще всего в качестве полной системы вычетов употребляют наименьшие неотрицательные вычеты 0, 1, … , m—1 или также абсолютно наименьшие вычеты; последние, как это следует из вышеизложенного, в случае нечетного m представляются рядом

$$-\frac{m-1}{2}, \quad ...,-1, 0, 1, \quad ..., \frac{m-1}{2},$$

а в случае четного m каким-либо из двух рядов

$$-\frac{m}{2}+1, \quad ...,-1, 0, 1, ..., \frac{m}{2},$$

$$-\frac{m}{2},\quad ...,-1,0,1,...,\frac{m}{2}-1.$$

Любые m чисел, попарно несравнимые по модулю m, образуют полную систему вычетов по этому модулю.

Действительно, будучи несравнимы, эти числа тем самым принадлежат к различным классам, а так как их *m,* т. е.

Если (a,m) = 1 и x пробегает полную систему вычетов по модулю m, то ax+b, где b—любое целое, тоже пробегает полную систему вычетов по модулю m.

Числа одного и того же класса по модулю *m* имеют с модулем один и тот же общий наибольший делитель. Особенно важны классы, для которых этот делитель равен единице, т.е. классы, содержащие числа, взаимно простые с модулем.

Взяв от каждого такого класса по одному вычету, получим *приведенную систему вычетов по модулю m.* Приведенную систему вычетов, следовательно, можно составить из чисел полной системы, взаимно простых с модулем. Обыкновенно приведенную систему вычетов выделяют из системы наименьших неотрицательных вычетов: 0, 1, …, *m*—1. Так как среди этих чисел число взаимно простых с *m* есть $\varphi(m)$, то число чисел приведенной системы, равно как и число классов, содержащих числа, взаимно простые с модулем, есть $\varphi(m)$.

Пример. 1.3.2 Приведенная система вычетов по модулю 42 будет 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.

Любые $\varphi(m)$ чисел, попарно несравнимые по модулю m и взаимно простые с модулем образуют приведенную систему вычетов по модулю m.

Если (a, m) = 1 и x пробегает приведенную систему вычетов по модулю m, то ax тоже пробегает приведенную систему вычетов по модулю m.

3.3. Теоремы Эйлера и Ферма

Теорема Эйлера *При m > 1 и (a,m)=1 имеем* $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m)$.

Действительно, если *x* пробегает приведенную систему вычетов

$$x = r_1, r_2, ..., r_c; \quad c = \varphi(m),$$

составленную из наименьших неотрицательных вычетов, то наименьшие неотрицательные вычеты $\rho_1, \rho_2, ..., \rho_c$ чисел ax будут пробегать ту же систему, но расположенную, вообще говоря, в ином порядке. Перемножая почленно сравнения

$$ar_1 \equiv \rho_1 (\mathrm{mod}\ m), \quad ar_2 \equiv \rho_2 (\mathrm{mod}\ m), \quad ..., ar_c \equiv \rho_c (\mathrm{mod}\ m),$$

получим

$$a^c r_1 r_2 \cdots r_c \equiv \rho_1 \rho_2 \cdots \rho_c (\mathrm{mod}\ m),$$

откуда, деля обе части на произведение $r_1 r_2 \cdots r_c \equiv \rho_1 \rho_2 \cdots \rho_c$, получим

$$a^c \equiv 1 \ (\mathrm{mod}\ m).$$

Теорема Ферма *При p простом и a, не делящемся на p, имеем*

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p) \text{ или } a^p \equiv a (\mathrm{mod}\ p).$$

3.4 Сравнения первой степени

Будем изучать сравнения такого общего вида:

$$f(x) \equiv 0 (\mathrm{mod}\ m); \quad f(x) = ax^n + a_1 x^{n-1} + ... + a_n. \qquad (1.3.5)$$

Если *a* не делится на *m,* то *n* называется *степенью сравнения.*

Решить сравнение — значит найти все значения *x*, ему удовлетворяющие. Два сравнения, которым удовлетворяют одни и те же значения *x,* называются *равносильными.*

Если сравнению (1.3.5) удовлетворяет какое-либо $x=x_1$, то тому же сравнению будут удовлетворять и все числа, сравнимые с x_1 по модулю *m:* $x = x_1 (\mathrm{mod}\ m)$. Весь этот класс чисел считается за *одно решение.* При таком соглашении *сравнение* (1.3.5) *будет иметь столько решений, сколько вычетов полной системы ему удовлетворяет.*

Пример 1.3.3. Сравнению

$$x^5 + x + 1 \equiv 0 (\mathrm{mod}\ 7)$$

среди чисел 0, 1, 2, 3, 4, 5, 6 полной системы вычетов по модулю 7 удовлетворяют два числа: $x = 2$ и $x = 4$. Поэтому указанное сравнение имеет два решения: $x \equiv 2(\mathrm{mod}\ 7)$, $x \equiv 4(\mathrm{mod}\ 7)$.

Сравнение первой степени перенесением свободною члена (с обратным знаком) в правую часть можно привести к виду

$$ax \equiv b(\mathrm{mod}\ m) \qquad (1.3.6)$$

Наложим условие $(a,m)=1$.

Сравнение имеет столько решений, сколько вычетов полной системы ему удовлетворяет. Но когда x пробегает полную систему вычетов по модулю m, то ax пробегает полную систему вычетов**.** Следовательно, при одном и только одном значении x, взятом из полной системы, ax будет сравнимо с b. Итак, при $(a, m) = 1$ сравнение (1.3.6) имеет одно решение.

Пусть теперь $(a, m) = d > 1$. Тогда, чтобы сравнение (3.6) имело решения, необходимо**,** чтобы b делилось на d, иначе сравнение (3.6) невозможно ни при каком целом x. Предполагая поэтому b кратным d, положим $a = a_1 d$, $b=b_1 d$, $m=m_1 d$. Тогда сравнение (3.6) будет равносильно такому (по сокращении на d): $a_1 x \equiv b_1(\mathrm{mod}\ m_1)$, в котором уже $(a_1, m_1) = 1$, и потому оно будет иметь одно решение по модулю m_1. Пусть x_1 — наименьший неотрицательный вычет этого решения по модулю m_1, тогда все числа x, образующие это решение, найдутся в виде

$$x \equiv x_1(\mathrm{mod}\ m_1). \qquad (1.3.7)$$

По модулю же m числа (1.3.7) образуют не одно решение, а больше, именно столько решений, сколько чисел (1.3.7) найдется в ряде 0, 1, 2, …, m—1 наименьших неотрицательных вычетов по модулю m. Но сюда попадут следующие числа (1.3.7):

$$x_1, x_1 + m_1, x_1 + 2m_1, ..., x_1 + (d-1)m_1, ,$$

т.е. всего d чисел (1.3.7); следовательно, сравнение (1.3.6) имеет d решений.

Справедлива следующая

Теорема 1.3.2 *Пусть (a, m) = d. Сравнение* $ax \equiv b \pmod m$ *невозможно, если b не делится на d. При b, кратном d, сравнение имеет d решений.*

Укажем способ решения сравнения (1.3.6), основанный на теории непрерывных дробей, причем достаточно ограничиться лишь случаем $(a,m)=1$.

Разлагая в непрерывную дробь отношение *m:a,*

$$\frac{m}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}}}$$

и рассматривая две последние подходящие дроби:

$$\frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n} = \frac{m}{a},$$

согласно свойствам непрерывных дробей имеем

$$mQ_{n-1} - aP_{n-1} = (-1)^n,$$
$$aP_{n-1} \equiv (-1)^{n-1} (\mathrm{mod}\ m),$$
$$a(-1)^{n-1} P_{n-1} b \equiv b (\mathrm{mod}\ m).$$

Тогда наше сравнение имеет решение

$$x \equiv (-1)^{n-1} P_{n-1} b (\mathrm{mod}\ m),$$

для разыскания которого достаточно вычислить P_{n-1} по формулам

$$P_i = q_i P_{i-1} + P_{i-2}.$$

Пример 1.3.4. Решим сравнение

$$111x \equiv 75 (\mathrm{mod}\, 321). \qquad (1.3.8)$$

Здесь (111, 321) = 3, причем 75 кратно 3. Поэтому сравнение имеет три решения.

Деля обе части сравнения и модуль на 3, получим сравнение

$$37x \equiv 25 (\mathrm{mod}\, 107), \qquad (1.3.9)$$

которое нам следует сначала решить. Имеем

$$
\begin{array}{r|l}
107 & 37 \\
\underline{74} & 2 \\
\end{array}
$$

$$
\begin{array}{r|l}
37 & 33 \\
\underline{33} & 1 \\
\end{array}
$$

$$
\begin{array}{r|l}
33 & 4 \\
\underline{32} & 8 \\
\end{array}
$$

$$
\begin{array}{r|l}
4 & 1 \\
\underline{4} & 4 \\
\end{array}
$$

""

q_i		2	1	8	4
P_i	1	2	3	26	107

Значит, в данном случае $n = 4$, $P_{n-1} = 26$, $b = 25$, и мы имеем решение сравнения (1.3.9) в виде

$$x \equiv -26 \cdot 25 \equiv 99 \pmod{107}.$$

Отсюда решения сравнения (3.8) представляются так:

$$x \equiv 99; \quad 99 + 107; \quad 99 + 2 \cdot 107 (\mathrm{mod}\, 321),$$

т. е.

$$x \equiv 99; \quad 206; \quad 313 \pmod{321}.$$

Задачи к части 1

1.1 Применяя алгоритм Евклида, найти наибольший общий делитель

1) (6188, 4709),

2) (321, 843),

3) (23521, 75217),

4) (6787, 7194),

5) (42598, 2014),

6) (2961, 13959),

7) (171124, 116887),

8) (416455, 42957),

9) (12994, 20114),

10) (8613, 10962),

11) (91476, 3960, 3360),

12) (5713, 6989, 3509),

13) (81719, 52003, 33649, 30107).

1.2 Найти наименьшее общее кратное чисел

1) [1573,273],

2) [2093,1633],

3) [2365, 5060],

4) [3813,1066],

5) [1395, 403],

6) [615, 1770],

7) [2465, 476, 1921],

8) [969, 1615, 1919],

9) [1751, 1649, 1054, 833],

10) [767, 7139, 6726, 2537].

3 Разложить в непрерывную дробь число

1) $\frac{145}{13}$, 2) $\frac{119}{29}$, 3) $\frac{31}{49}$, 4) $\frac{61}{111}$ 5) $\frac{23}{117}$.

1.3 Найти каноническое разложение чисел

1) 1440, 2) 1575, 3) 111111, 4) 82798848,

5) 81057226635000

1.4 Построить графики функций *[x], {x}.*

1.5 Найти значения функций

1) $\tau(10^6)$, 2) $S(360)$, 3) $\tau(5600)$, 4) $S(5600)$,

5) $\tau(116424)$, 6) $S(116424)$, 7) $\varphi(5040)$, 8) $\varphi(1294700)$,

9) $\mu(56)$, 10) $\mu(70)$, 11) $\mu(100)$.

1.6 Найти остаток от деления $\left(12371^{56}+34\right)^{28}$ на 111.

1.7 Найти остаток от деления $\left(6^{50}+71\right)^{144}$ на 35

1.8 Представляя целое число в обычной десятичной системе исчисления, вывести признаки делимости на 3, 9, 11.

1.9 Представляя целое число в системе исчисления с основанием 100, вывести признаки делимости на 101.

1.10 Представляя целое число в системе исчисления с основанием 1000, вывести признаки делимости на 37, 7, 11, 13.

1.11 Решить сравнения

1) $2x+1 \equiv 0 \pmod{13}$,

2) $5x \equiv 7 \pmod{21}$,

3) $10x \equiv 3 \pmod{49}$

4) $256x \equiv 179 \pmod{337}$,

5) $1215x \equiv 560 \pmod{2755}$,

6) $1296x \equiv 1105 \pmod{2413}$.

Часть 2. Основные алгебраические структуры

1. Группы

1.1 Определение и примеры

Пусть G — какое-то множество элементов (например, множество чисел, или функций, или каких-нибудь объектов геометрической природы и т. д.). Говорят, что в множестве G определена *алгебраическая операция,* если каждым двум элементам a, b из G, взятым в определенном порядке, однозначным образом поставлен в соответствие некоторый третий элемент c из G.

Примеры алгебраических операций: сложение целых чисел (каждым двум целым числам ставится в соответствие их сумма), их вычитание; сложение векторов на плоскости; сложение или умножение квадратных матриц n-го порядка; векторное умножение векторов трехмерного пространства.

Алгебраическая операция, определенная в множестве $G,$ обычно называется или *умножением,* или *сложением.* В первом случае, если элементам $a, b \in G$ поставлен в соответствие элемент $c \in G,$ пишут $c = ab,$ во втором случае пишут $c = a + b.$

Множество G с определенной в нем алгебраической операцией является *группой,* если выполнены следующие условия:

1) для любых трех элементов $a, b, c \in G$

$$a(bc) = (ab)c$$

(*ассоциативность* умножения);

2) в множестве G существует такой элемент $e,$ что для любого $a \in G$

$$ae = ea = a;$$

3) для любого $a \in G$ существует такое $a' \in G,$ что

$$aa' = a'a = e.$$

Элемент e называется *единицей* группы, элемент a' называется элементом, *обратным* a, и обозначается обычно через a^{-1}. Если операция, определенная в группе, называется сложением, то вместо единицы группы говорят о *нуле* группы (это элемент, обозначаемый символом 0 и обладающий свойством $a+0 = 0+a = a$ для любого $a \in G$), а вместо элемента a^{-1}, обратного элементу a, говорят об элементе — a, *противоположном* a ($a+(-a)=0$).

Множество X с заданной на нем ассоциативной алгебраической операцией называется *полугруппой*. Полугруппу с единичным (нейтральным) элементом называют *моноидом*.

Пример 2.1.1 Группами являются:

1) множество всех целых чисел относительно операции сложения (так называемая *аддитивная группа* всех целых чисел);

2) множество всех четных чисел относительно операции сложения (аддитивная группа всех четных чисел);

3) множество всех отличных от нуля рациональных чисел относительно операции умножения *Мультипликативная группа* отличных от нуля рациональных чисел);

4) множество всех векторов на плоскости относительно обычного сложения векторов;

5) множество всех невырожденных квадратных матриц n-го порядка с действительными элементами относительно операции умножения матриц.

Целые числа относительно операции умножения группы не образуют, так как для целого числа, отличного от ± 1, не существует обратного ему целого числа. По той же причине не образуют группы относительно умножения все квадратные матрицы n-го порядка. Не является группой и множество всех векторов трехмерного пространства относительно векторного умножения векторов, так как эта операция не ассоциативна.

Если операция, определенная в группе, *коммутативна* (т.е. для любых элементов *a, b* группы *ab = ba),* то сама группа называется *коммутативной* или *абелевой.* Группы приведенных выше примеров 1, 2, 3, 4 абелевы, группа примера 5 не абелева. Еще пример не абелевой группы — множество всех вращений трехмерного пространства вокруг начала координат, где произведением двух вращений называется их последовательное выполнение.

Если группа *G* состоит из конечного числа элементов, то она называется *конечной группой,* а число элементов в ней называется *порядком группы.*

Пример 2.1.2. Произведением двух подстановок *n*-й степени называется результат их последовательного выполнения (например, если $n=4$ и $a=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$, $b=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$, то $ab=\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}$, так как, например, число 1 при подстановке *a* переходит в 2, а число 2 при подстановке *b* переходит в 4, т.е. в итоге 1 переходит в 4, и т. д.). Это— алгебраическая операция, относительно которой множество всех подстановок *n*-й степени является группой. Единицей группы служит тождественная подстановка, $\begin{pmatrix}1&2&\dots&n\\1&2&\dots&n\end{pmatrix}$, элементом, обратным к подстановке $\begin{pmatrix}1&2&\dots&n\\i_1&i_2&\dots&i_n\end{pmatrix}$ является подстановка $\begin{pmatrix}i_1&i_2&\dots&i_n\\1&2&\dots&n\end{pmatrix}$. Эта группа называется *симметрической группой n-й степени* и обычно обозначается через S_n.

1.2. Изоморфизм групп. Говорят, что между элементами множеств (см. введение) *M* и *N* установлено *взаимно однозначное соответствие,* если каждому элементу множества *M* поставлен в соответствие некоторый вполне определенный элемент множества *N*, причем

различным элементам из M соответствуют различные элементы в N и всякий элемент из N соответствует некоторому элементу из M.

Две группы G и H называются *изоморфными,* если между их элементами можно установить взаимно однозначное соответствие, при котором для любых элементов $a,\ b \in G$ и соответствующих им элементов $a', b' \in H$ элементу $ab = c$ будет соответствовать элемент $c'=a'b'$.

Пример 2.1.3 Аддитивная группа G всех целых чисел изоморфна аддитивной группе H всех четных чисел (для установления изоморфизма между ними можно каждому числу $k \in G$ поставить в соответствие число $2k \in H$).

Пример 2.1.4. Мультипликативная группа всех положительных действительных чисел изоморфна аддитивной группе всех действительных чисел (изоморфизм: $a \to \lg a$).

Изоморфное отображение группы на себя называется *автоморфизмом* этой группы.

Пример 2.1.5. Одним из автоморфизмов аддитивной группы всех целых чисел является отображение, при котором каждому целому числу a ставится в соответствие число $-a$.

1.3. Гомоморфизм. Пусть каждому элементу группы G соответствует однозначно определенный элемент группы H, причем если элементам $a, b \in$ G соответствуют элементы $a', b' \in H$, то элементу $ab = c$ соответствует элемент $c'=a'b'$. Такое отображение $G \to H$ называется *гомоморфизмом;* говорят, что *группа G гомоморфно отображена в группу H.* Если при этом на каждый элемент группы H отображается хотя бы один элемент группы G, то говорят о *гомоморфном отображении* группы G *на* группу H; гомоморфизм в этом случае называется *эпиморфизмом.*

Вообще говоря, при гомоморфизме в данный элемент группы H могут переходить различные элементы *группы* G , а также может не переходить ни одного.

Пример 2.1.6. Если каждому четному числу поставить в соответствие число 1, а каждому нечетному поставить в соответствие число —1, то получится гомоморфное отображение аддитивной группы всех целых чисел в мультипликативную группу всех отличных от нуля рациональных чисел. Это отображение будет также гомоморфным отображением аддитивной группы всех целых чисел на мультипликативную группу, состоящую из чисел —1, 1.

Пример 2.1.7. Если каждой невырожденной квадратной матрице n-го порядка с действительными элементами поставить в соответствие определитель этой матрицы, то получится гомоморфное отображение группы (по умножению) всех действительных невырожденных квадратных матриц n-го порядка на мультипликативную группу всех отличных от нуля действительных чисел.

При всяком гомоморфном отображении группы G в группу H единица группы G (или нуль, если групповая операция — сложение) переходит в единицу (в нуль) группы H. Совокупность всех элементов группы G, переходящих в единицу (в нуль) группы H, называется *ядром* данного гомоморфизма. В приведенном выше примере 2.1.6 ядро гомоморфизма составляют все четные числа, в примере 2.1.7 — все матрицы с определителем, равным 1.

Гомоморфное отображение группы в себя называется *эндоморфизмом* этой группы. Примером эндоморфизма может служить отображение, при котором каждому элементу группы ставится в соответствие единица этой группы.

Если группа G гомоморфно отображена на какое-то множество M, в котором определена алгебраическая операция, то относительно этой

алгебраической операции множество M само необходимо является группой.

1.4. Подгруппы. Циклические группы. Подмножество A группы G называется *подгруппой* этой группы, если вместе с каждым элементом a оно содержит также обратный ему элемент a^{-1} и вместе с каждыми двумя элементами $a,\ b$ оно содержит и их произведение ab. Эти два требования можно заменить одним: для любых элементов a, $b \in A$ элемент ab^{-1} должен лежать в A.

Всякая подгруппа данной группы G сама является группой относительно той операции, которая определена в G.

Пример 2.1.8. Аддитивная группа всех четных чисел является подгруппой аддитивной группы всех целых чисел, которая сама является подгруппой аддитивной группы всех комплексных чисел.

Пример 2.1.9. Множество всех четных подстановок n элементов является подгруппой в группе всех подстановок n элементов. Эта подгруппа называется *знакопеременной группой, n-й степени* и обычно обозначается через A_n.

В любой группе подмножество, состоящее только из единичного элемента группы, является подгруппой. Эта подгруппа называется *единичной подгруппой* данной группы и обычно обозначается символом E. Сама группа также всегда является своей подгруппой. Всякая подгруппа, отличная от всей группы, называется *истинной подгруппой* этой группы.

Если в группе G взять какой-нибудь элемент g и все степени этого элемента (или все его кратные, если операция в группе — сложение), то также получится подгруппа группы G. Эта подгруппа называется *циклической подгруппой, порожденной элементом g,* и обозначается через $\{g\}$. Если подгруппа $\{g\}$ совпадает со всей группой G, то сама группа G называется *циклической группой.*

Пусть G – произвольная группа, a – еенекоторый элемент. Имеются две возможности.

1) Все степени элемента a различны, т.е. $m \neq n \Rightarrow a^m \neq a^n$. В этом случае говорят, что элемент $a \in G$ имеет *бесконечный порядок.*

2) Имеются совпадения $a^m = a^n$ при $m \neq n$. Если, например, $m>n$, то существуют положительные степени элемента $a \in G$, равные единичному элементу. Пусть q – наименьший положительный показатель, для которого $a^q = e$. Тогда говорят, что a – элемент *конечного порядка q.*

В конечной группе все элементы будут конечного порядка.

Пример 2.1.10. Аддитивная группа всех целых чисел есть бесконечная циклическая группа (она состоит из всех кратных числа 1).

Пример 2.1.11. Все значения корня n-й степени из 1 образуют (относительно умножения) циклическую группу порядка n, порожденную любым из первообразных корней n-й степени из 1.

1.5. Смежные классы. Разложение группы по подгруппе.

Если A — подгруппа, g—произвольный элемент группы G то через gA обозначается множество всех элементов группы G, получающихся при умножении элемента g на всевозможные элементы из подгруппы A (т.е, множество всех элементов вида ga, где $a \in A$). Это множество называется *левым смежным классом группы G по подгруппе A, определяемым элементом g.* Аналогично *правым смежным классом* Ag группы G по подгруппе A, определяемым элементом g, называется множество всех элементов вида ag, где $a \in A$. Если групповая операция — сложение, то левые и правые смежные классы обозначаются соответственно через $g+A$ и $A+g$.

Пример 2.1.12. В группе всех подстановок третьей степени возьмем подгруппу A, состоящую из подстановок $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ и $a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, и возьмем элемент $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Тогда левый смежный класс gA будет

состоять из подстановок $ge=g=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ и $ga=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$, а правый смежный класс Ag—из подстановок $eg = g=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ и $ag=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$.

Каждый левый смежный класс определяется любым из входящих в него элементов, т. е. если $g_1 \in gA$, то $g_1A=gA$.

Два любых левых смежных класса группы G по подгруппе A или совпадают, или не имеют ни одного общего элемента. Одним из левых смежных классов группы G по подгруппе A является сама подгруппа $A(A=eA,$ где e — единица группы G); все остальные левые смежные классы по подгруппе A подгруппами группы G не являются.

Эти же утверждения верны для правых смежных классов.

Число всех различных левых смежных классов группы G по подгруппе A всегда равно числу всех различных правых смежных классов группы G по этой же подгруппе (в бесконечном случае это означает, что мощность множества всех различных левых смежных классов группы G по подгруппе A совпадает с мощностью множества правых смежных классов). Это число (в бесконечном случае—мощность) называется *индексом* подгруппы A в группе G. Если группа G конечна, то ее порядок равен произведению порядка любой ее подгруппы A на индекс этой подгруппы в группе G *(теорема Лагранжа).* Отсюда следует, что порядок всякой подгруппы конечной группы является делителем порядка группы. Также порядок любого элемента конечной группы является делителем порядка этой группы. Обратно, если порядок конечной группы G делится на простое число $p,$ то G обладает элементами порядка p *(теорема Коши).*

Если в произвольной группе G выбрана какая-то подгруппа $A,$ то все элементы группы G можно разбить на непересекающиеся классы, объединяя вместе те элементы, которые лежат в одном и том же левом

смежном классе группы G по подгруппе A. Такое разбиение называется *левосторонним разложением группы G по подгруппе A*. Если вместо левых смежных классов взять правые смежные классы по подгруппе A, то получится *правостороннее разложение группы G по подгруппе A*.

Пример 2.1.13. В симметрической группе 3-й степени S_3, элементы которой $a_1 = e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $a_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $a_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $a_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $a_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $a_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, возьмем подгруппу A, состоящую из элементов e и a_6. Тогда при левостороннем разложении группы S_3 по подгруппе A множество ее элементов разобьется на классы: 1) e, a_6 (смежный класс $eA = A$), 2) a_2, a_5, (смежный класс a_2A), 3) a_3, a_4 (смежный класс a_3A), а при правостороннем разложении получатся классы: 1) e, a_6 (смежный класс $Ae = A$), 2) a_2, a_4 (смежный класс Aa_2), 3) a_3, a_5 (смежный класс Aa_3). Индекс подгруппы A в группе S_3 равен 3.

1.6. Нормальный делитель группы. Если при левостороннем и при правостороннем разложении группы G по некоторой ее подгруппе H классы, на которые распадаются элементы группы G, получаются одинаковыми, то подгруппа H называется *нормальным делителем* группы G (или *инвариантной подгруппой.)*

Пример 2.1.14. В примере 1.13 подгруппа A группы S_3 не является нормальным делителем этой группы.

Подгруппа H тогда и только тогда является нормальным делителем группы G, когда для любого элемента g группы G

$$gH = Hg.$$

Это равенство означает, что для всякого элемента h из H можно найти в H такие элементы h' и h'', что

$$gh = h'g, \qquad hg = gh''. \tag{2.1.1}$$

Пример 2.1.15. Если группа G абелева, то всякая ее подгруппа H является нормальным делителем.

1.7. Фактор-группа. Если в множестве всех смежных классов группы G по нормальному делителю H ввести операцию по правилу $(g_1H)(g_2H) = (g_1g_2)H$ (при аддитивной записи $(g_1+H)+(g_2+H) =(g_1+g_2)+H$, то это будет алгебраическая операция, относительно которой множество всех смежных классов группы G по нормальному делителю H само окажется группой. Эта группа называется *фактор-группой группы G по нормальному делителю H* и обозначается через *G/H*. Единицей фактор-группы *G/H* является смежный класс *H*. Элементом, обратным элементу фактор-группы gH, является смежный класс $g^{-1}H$. Порядок фактор-группы *G/H* равен индексу *H* в *G*..

1.8. Группы подстановок. *Группы подстановок* — это подгруппы симметрических групп. При их изучении обычно для удобства пользуются записью подстановок в виде произведений циклов. *Циклом* или *циклической подстановкой* называется такая подстановка чисел 1,2,..., n, которая одно из этих чисел i_1 переводит в число i_2, i_2 переводит в i_3 и т.д., i_{k-1} переводит в i_k $(k \le n)$ i_k переводит в i_1 а все остальные числа оставляет на месте. Эта подстановка обозначается через $(i_1\ i_2,..., i_k)$. Циклы $(i_1\ i_2,..., i_k)$ и, например, $(i_2,\ldots,i_k, i_1)$ равны между собой. Число k называется *длиной* цикла. Цикл длины 1 — это тождественная подстановка. Чтобы представить произвольную подстановку чисел 1, 2,..., n в виде произведения циклов, нужно взять любое из этих чисел (например, 1), затем число, в которое оно переводится данной подстановкой (пусть это число—j_2), затем число, в которое j_2 переходит при этой подстановке, и т.д. до числа j_l, переводящегося данной подстановкой в первое из взятых чисел (в нашем случае в 1), и выписать цикл $(1, j_2, \ldots, j_l)$, после этого нужно взять какое-нибудь из чисел 1,2,..., n, которое пока еще не встречалось (если такое число существует), и, начиная с него, сделать то же самое и т.д., пока не будут использованы все числа 1, 2,..., n. Тогда мы получим несколько циклов, не имеющих общих действительно перемещаемых ими чисел, произведению которых

(в любом порядке) и будет равна данная подстановка. Циклы, не содержащие общих действительно перемещаемых ими чисел, называются *независимыми.* Те циклы, входящие в произведение, длина которых равна 1, обычно не пишут. При этом условии всякая подстановка разлагается в произведение независимых циклов единственным образом.

Пример 2.1.16. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 1 & 5 & 7 & 4 & 6 & 3 \end{pmatrix} = (183)\,(4576).$

2. Кольца

2.1. Определения, примеры Множество R с двумя определенными в нем алгебраическими операциями, сложением и умножением, называется *кольцом,* если относительно операции сложения оно является абелевой группой, а операция умножения связана с операцией сложения законами *дистрибутивности,* т. е. для любых трех элементов $a, b, c \in R$

$$a\,(b + c) = ab + ac \text{ и } (b+c)\,a = ba + ca. \qquad (2.2.1)$$

Умножение, определенное в кольце, не обязано быть ни ассоциативным, ни коммутативным. Если умножение, определенное в кольце $R,$ ассоциативно (т. е. для любых трех элементов $a,\ b,\ c \in R$ $a(bc)=(ab)c$), то кольцо R называется *ассоциативным кольцом.* Если, кроме того, умножение, определенное в $R,$ коммутативно, то R называется *коммутативным кольцом.* В коммутативном кольце второе из равенств (2.2.1) является следствием первого.

Если в кольце R для любого элемента a выполнено условие $a^2 = 0$ и для любых трех элементов a, b, c

$$a\,(bc)+b\,(ca)+ c\,(ab) = 0$$

(тождество Якоби), то R называется *кольцом Ли.*

Пример 2.1.1. Все целые числа относительно обычных операций сложения и умножения чисел образуют коммутативное кольцо.

Пример 2.2.2. Все рациональные числа, все действительные числа, все комплексные числа относительно обычных операций сложения и умножения образуют коммутативные кольца.

Пример 2.2.3. Вес многочлены от одного переменного с произвольными числовыми коэффициентами относительно обычных операций сложения и умножения многочленов образуют коммутативное кольцо.

Пример 2.2.4. Ассоциативное, но не коммутативное, кольцо образуют все квадратные матрицы n-го порядка с произвольными числовыми элементами.

Пример 2.2.5. Множество всех векторов трехмерного пространства, где векторы складываются обычным образом, а произведением двух векторов называется их векторное произведение, является неассоциативным кольцом. Это кольцо есть кольцо Ли.

Абелева группа, которая получится, если в кольце рассматривать только одну операцию сложения, называется *аддитивной группой* кольца. Нулевой элемент этой группы называется *нулем кольца*. Произведение любого элемента a кольца на нуль равно нулю кольца: $a \cdot 0 = 0$.

Если для элементов a, b некоторого кольца $ab = 0$, но $a \neq 0$ и $b \neq 0$, то a и b называются *делителями нуля* (a — левый делитель нуля, b — правый). Если в кольце R делителей нуля нет, то R называется *кольцом без делителей нуля.* Коммутативное кольцо без делителей нуля называется *областью целостности.*

Пример 2.2.6. Всякое кольцо, в котором элементы — числа, а операции — обычное сложение и умножение чисел, является областью целостности.

Пример 2.2.7. Все функции, определенные и непрерывные на отрезке [—1,1], относительно обычных операций сложения и умножения функций образуют кольцо с делителями нуля (например, произведение функций

$$f_1(x)=\begin{cases}0 & при \quad -1\le x\le 0,\\ x & при \quad 0<x\le 1\end{cases};\qquad f_2(x)=\begin{cases}x & при \quad -1\le x\le 0,\\ 0 & при \quad 0<x\le 1\end{cases};$$

ни одна из которых не равна нулю кольца, является нулем).

Если для элементов a, b_1, b_2 кольца выполнено равенство $ab_1=ab_2$ (или $b_1a = b_2a$), причем $a\neq 0$ не есть левый (соответственно — правый) делитель нуля, то $b_1 = b_2$, т. е. на отличные от нуля элементы, не являющиеся делителями нуля, равенства можно сокращать. Производить сокращение на элемент, являющийся делителем нуля, нельзя.

Пример 2.2.8. В кольце всех квадратных матриц 2-го порядка (пример 2.2.4) для матриц

$$A=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix},\quad B_1=\begin{pmatrix}1 & 2\\ 3 & 6\end{pmatrix},\quad B_2=\begin{pmatrix}1 & 2\\ 4 & 0\end{pmatrix}$$

справедливо равенство $AB_1=AB_2$, хотя $B_1 \neq B_2$. Здесь A— левый делитель нуля: например, $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 0\\ 1 & 3\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$.

Элемент e кольца R называется *единицей* этого кольца, если для любого элемента $a\in R$ $ae = ea = a$. Единицы в кольце может и не быть. Если в кольце R единица есть, то R называется *кольцом с единицей.*

Пример 2.2.9. Кольцо всех целых чисел есть кольцо с единицей.

Пример 2.2.10. Все четные числа образуют кольцо без единицы.

В кольце с единицей e для элемента $a\neq 0$ может существовать *обратный* ему элемент a^{-1} со свойством $aa^{-1} = a^{-1}a = e$ (но может такого элемента и не быть). Элементы кольца с единицей, для которых в этом кольце обратный элемент существует, называются *делителями единицы.*

Пример 2.2.11. В кольце всех квадратных матриц *n-го* порядка единицей является единичная матрица. Обратный элемент существует для всякой невырожденной матрицы; для вырожденных матриц обратных им элементов не существует.

2.2 Изоморфизм. Гомоморфизм. Кольца R и Q называются *изоморфными,* если между их элементами можно установить такое взаимно однозначное соответствие, что если элементам a_1 $a_2 \in R$, соответствуют элементы b_1 $b_2 \in$ Q, то элементу $a_1 + a_2$ соответствует элемент $b_1 + b_2$ и элементу $a_1 a_2$— элемент $b_1 b_2$.

Пример 2.2.12. Кольцо всех квадратных матриц n-го порядка с действительными элементами изоморфно кольцу всех линейных преобразований, действующих в действительном n-мерном линейном векторном пространстве

Говорят, что кольцо R *гомоморфно отображено* в кольцо Q, если каждому элементу кольца R поставлен в соответствие однозначно определенный элемент кольца Q, причем если элементам a_1, a_2 кольца R соответствуют элементы $b_1, b_2 \in Q$, то элементу $a_1 + a_2$ соответствует $b_1 + b_2$, элементу $a_1 a_2$ соответствует $b_1 b_2$. Если при этом на каждый элемент кольца Q отображается по крайней мере один элемент кольца R, то говорят о гомоморфном отображении кольца R на кольцо Q; гомоморфизм в этом случае называется *эпиморфизмом.*

2.3. Подкольца. Идеалы. Подгруппа A аддитивной группы кольца R называется *подкольцом* этого кольца, если она вместе с каждыми двумя элементами a_1, a_2 содержит также их произведение $a_1 a_2$. Подкольцо A кольца R называется *левым* (соответственно *правым) идеалом* этого кольца, если оно вместе с каждым элементом a содержит также все элементы вида ra (вида ar), где r — произвольный элемент кольца R,. В коммутативных кольцах понятия левого и правого идеала совпадают. Если подкольцо A произвольного кольца одновременно является и левым, и правым идеалом, то оно называется *двусторонним идеалом* этого кольца.

Пример 2.2.13 В кольце всех целых чисел числа, кратные некоторому фиксированному числу n, составляют двусторонний идеал.

Пример 2.2.14 В кольце всех квадратных матриц *n-го* порядка множество всех матриц, у которых последний столбец состоит из нулей, является левым идеалом, а множество всех матриц, у которых последняя строка состоит из нулей, является правым идеалом

В любом кольце элемент 0 и само кольцо являются двусторонними идеалами. Если других двусторонних идеалов в кольце нет, оно называется *простым кольцом.*

Пример 2.2.15 Простым кольцом служит кольцо всех квадратных матриц *n*-го порядка с любыми комплексными (или с любыми действительными) элементами

Пример 2.2.16. Всякое поле является простым кольцом.

Если в кольце R дано некоторое множество элементов N, то наименьший (левый, правый или двусторонний) идеал кольца R, содержащий все элементы из N, называется (соответственно левым, правым или двусторонним) *идеалом, порожденным множеством N;* этот идеал является пересечением всех (соответственно левых, правых или двусторонних) идеалов кольца R, содержащих множество N. Идеал, порожденный одним элементом a, называется *главным идеалом (обозначение:* $(a)_l$, $(a)_r$ или (a), в зависимости от того, идеал левый, правый или двусторонний). Если R — коммутативное кольцо, то главный идеал (a), порожденный элементом a этого кольца, состоит из всех элементов вида $ra+na$, где $r \in R$, n — целое число. Если R — коммутативное кольцо с единицей, то (a) состоит просто из всех элементов вида ra, где $r \in R$.

3. Поля. Тела

3.1. Поля. *Полем* называется коммутативное кольцо, состоящее не только из нуля, в котором для любого элемента $a \neq 0$ и любого элемента b существует ровно один такой элемент x, что $ax = b$. Элемент x

называется *частным* от деления элемента b на элемент a (обозначение: $x=\frac{b}{a}$).

Примерами полей служат: кольцо всех рациональных чисел, кольцо всех действительных чисел, кольцо всех комплексных чисел. Все комплексные числа, являющиеся корнями многочленов с рациональными коэффициентами, также образуют поле, называемое *полем алгебраических чисел.* Кольцо всех целых чисел полем не является

Всякое поле обладает единицей. Для любого отличного от нуля элемента поля существует обратный ему элемент. Множество всех отличных от нуля элементов поля образует относительно умножения, определенного в поле, абелеву группу *(мультипликативную группу поля).* Никакое поле не содержит делителей нуля. Единственными идеалами поля являются нулевой идеал и само поле.

Множество с двумя алгебраическими операциями, изоморфное полю, само является полем. Всякое гомоморфное отображение одного поля в другое является или изоморфизмом, или отображением, переводящим все элементы поля в нуль.

Если некоторое целое положительное кратное единичного элемента e поля P $ne=e+e+...+e$ (n слагаемых) равно нулю, то наименьшее целое положительное число p со свойством $pe = 0$ называется *характеристикой поля P; p* всегда является простым числом. Если никакое целое положительное кратное единичного элемента поля P нулю не равно, то P называется полем *характеристики нуль.* Пример поля характеристики p — поле классов вычетов по модулю p, пример поля характеристики нуль — любое числовое поле (например, поле всех действительных чисел).

Множество P' элементов поля P называется *подполем* этого поля, если оно само является полем по отношению к тем операциям, которые определены в P; P' тогда и только тогда является подполем поля P, когда

оно вместе с любыми двумя элементами a,b содержит также $a+b$, ab, $a-b$ и $\frac{a}{b}$ (если $b\neq 0$). Если P' — подполе поля P, то P называется *расширением* поля P'. Поле, не имеющее никаких подполей, кроме него самого, называется *простым полем*. Примеры простых полей — поле классов вычетов по модулю p, поле всех рациональных чисел.

Всякое поле характеристики p содержит подполе, изоморфное полю классов вычетов по модулю p, а всякое поле характеристики нуль содержит подполе, изоморфное полю всех рациональных чисел.

Если в поле P даны подполе P' и множество элементов N, то наименьшее подполе P'' поля P, содержащее P' и N, называется полем, полученным *присоединением* к полю P' множества N (обозначение: $P''=P'(\mathrm{N})$). Поле $P'(N)$ состоит из всех элементов, получающихся из элементов поля P' и множества N путем сложения, вычитания, умножения и деления, и является пересечением всех подполей поля P, содержащих P' и N. Если множество N состоит из одного элемента α, то P'' называется *простым расширением* поля P'. Если при этом α является корнем некоторого многочлена $f(x)$ с коэффициентами из поля P', то $P'' = P'(\alpha)$ называется *простым алгебраическим расширением* поля P', а элемент α называется *алгебраическим относительно P';* если же не существует многочлена $f(x)$ с коэффициентами из P', корнем которого был бы элемент α, то $P'' = P'(\alpha)$ называется *простым трансцендентным расширением* поля P', а элемент α называется *трансцендентным относительно P'*

Пример 2.3.1. Простое алгебраическое расширение поля рациональных чисел, полученное присоединением к нему числа $\alpha=\sqrt[3]{2}$, состоит из всех чисел вида $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, где a, b, c — рациональные числа.

Пример 2.3.2 Поле всех комплексных чисел является простым алгебраическим расширением поля всех действительных чисел, полученным из него присоединением корня i многочлена x^2+1.

3.2. Тела. *Телом* называется ассоциативное кольцо, состоящее не только из нуля, в котором для любого элемента $a \neq 0$ и любого элемента b существуют такой элемент x и такой элемент y, что $ax = b$, $ya = b$. Отличие тела от поля состоит в том, что умножение в теле не обязано быть коммутативным.

3.4. Алгебры. Кольцо A называется *алгеброй* над полем P, если его аддитивная группа есть векторное пространство над полем P и если умножение в A связано с умножением на элементы из P формулой $\alpha(ab)=(\alpha a)b=a(\alpha b)$ $(a,b\in A, \alpha\in P)$.

Если векторное пространство, которое служит аддитивной группой алгебры A, является n-мерным, то число n называется *рангом* алгебры A. Алгебры конечного ранга называются также *гиперкомплексными системами.* Если алгебра A является кольцом Ли, то она называется *алгеброй Ли*. Если какая-то алгебра является не только кольцом, но даже телом, она называется *алгеброй с делением.*

Пример 2.3.3. Множество всех векторов трехмерного пространства, в котором векторы складываются и умножаются на числа обычным образом, а произведением двух векторов является их векторное произведение, есть алгебра Ли над полем действительных чисел.

Пример 2.3.4. Множество всех квадратных матриц n-го порядка с комплексными элементами, в котором обычным образом определены операции сложения и умножения матриц и операция умножения матрицы на комплексное число, является алгеброй ранга n^2 над полем комплексных чисел.

Пример 2.3.5. Все комплексные числа относительно обычных операций сложения и умножения комплексных чисел и обычной

операции умножения комплексных чисел на действительные числа образуют алгебру с делением ранга 2 над полем действительных чисел.

Задачи к части 2

2.1 Ассоциативна ли операция * на множестве M, если

1) $M=N,\ x*y=x^y$,

2) $M=N,\ x*y=(x,y)$ – наименьший общий делитель

3) $M=N,\ x*y=2xy$,

4) $M=Z,\ x*y=x-y$,

5) $M=Z,\ x*y=x^2+y^2$,

6) $M=R,\ x*y=\sin x\cdot\sin y$,

2.2 Пусть S- полугруппа матриц $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$, где $x,\ y\in R$ с операцией умножения. Найти в этой полугруппе левые и правые нейтральные элементы, элементы, обратимые слева и справа относительно этих нейтральных.

2.3 Какие из указанных числовых множеств с операциями являются группами:

1) $(A, +)$, где A — одно из множеств N, Z, Q, M, C;

2) $(A, \bullet)$, где A — одно из множеств N, Z, Q, R, C;

3) $(A_0, \bullet)$, где A — одно из множеств N, Z, Q, R, C, а $A_0 = A \setminus \{0\}$;

4 $(nZ, +)$, где n — натуральное число;

5) $(\{-1, 1\},\cdot)$;

6) множество степеней данного вещественного числа $a \neq 0$ с целыми показателями относительно умножения;

7) множество всех комплексных корней фиксированной степени n из 1 относительно умножения;

8) множество комплексных корней всех степеней из 1 относительно умножения;

9) множество комплексных чисел с фиксированным модулем r относительно умножения;

10) множество ненулевых комплексных чисел с модулем, не превосходящим фиксированное число r, относительно умножения;

11) множество ненулевых комплексных чисел, расположенных на лучах, выходящих из начала координат и образующих с лучом Ox углы $\varphi_1, \varphi_2, \ldots, \varphi_n$ относительно умножения;

2.4 Какие из указанных множеств квадратных вещественных матриц фиксированного порядка образуют группу:

1) множество симметрических матриц относительно сложения;

2) множество симметрических матриц относительно умножения;

3) множество невырожденных матриц относительно сложения;

4) множество невырожденных матриц относительно умножения;

5) множество матриц с фиксированным определителем d относительно умножения;

6) множество диагональных матриц относительно сложения;

7) множество диагональных матриц относительно умножения;

8) множество диагональных матриц, все элементы диагоналей которых отличны от 0, относительно умножения;

9) множество верхних треугольных матриц относительно умножения.

2.5 Перемножить перестановки в указанном и обратном порядках

1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \times \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$,

2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix}$,

3) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} \times \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$,

4) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 2 & 4 \end{pmatrix} \times \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix}$.

2.6 Составить таблицу умножения перестановок порядка 3, порядка 4.

2.7 Записать в виде произведения независимых циклов перестановки

1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 1 & 7 & 3 & 6 & 2 \end{pmatrix}$,

2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 6 & 7 & 5 & 2 & 4 \end{pmatrix}$,

3) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 6 & 5 & 1 & 2 & 4 \end{pmatrix}$,

4) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 6 & 7 & 1 & 5 & 2 \end{pmatrix}$,

5) $\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & 2n-1 & 2n \\ 2 & 1 & 4 & 3 & \dots & 2n & 2n-1 \end{pmatrix}$.

2.8 Какие из отображений групп $f : C \mapsto R$ являются гомоморфизмами

1) $f(z) = |z|$, 2) $f(z) = 2|z|$, 3) $f(z) = \frac{1}{|z|}$, 4) $f(z) = 1 + |z|$,

5) $f(z) = |z|^2$, 6) $f(z) = 1$.

2.9 Найти порядок элемента группы

1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in S_5$, 2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix} \in S_6$,

3) $\frac{-\sqrt{3}}{2} + \frac{1}{2} i \in C$, 4) $\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} i \in C$.

2.10 Найти смежные классы

1) аддитивной группы Z по подгруппе nZ (множество чисел, кратных n), n – натуральное число,

2) аддитивной группы R по подгруппе Z,

3) аддитивной группы C по подгруппе R,

4) мультипликативной группы C по подгруппе U чисел с модулем 1,

5) мультипликативной группы C по подгруппе R,

6) мультипликативной группы C по подгруппе положительных вещественных чисел,

7) аддитивной группы всех многочленов степени не выше 5 с комплексными коэффициентами по подгруппе многочленов степени не выше 3.

2.11 Какие из следующих числовых множеств образуют кольцо относительно обычных операций сложения и умножения:

1) множество Z;

2) множество чисел кратных n, nZ ($n > 1$);

3) множество неотрицательных целых чисел;

4) множество Q;

5) множество рациональных чисел, в несократимой записи которых знаменатели делят фиксированное число $n \in N$;

6) множество рациональных чисел, в несократимой записи которых знаменатели не делятся на фиксированное простое число p,

7) множество рациональных чисел, в несократимой записи которых знаменатели являются степенями фиксированного простого числа p;

8) множество вещественных чисел вида $x + y\sqrt{2}$, где $x,y \in Q$;

9) множество вещественных чисел вида $x + y\sqrt[3]{2}$, где $x,y \in Q$;

10) множество вещественных чисел вида $x + y\sqrt[3]{2} + z\sqrt[3]{4}$, где $x,y,z \in Q$;

11) множество комплексных чисел вида $x + yi$, где $x,y \in Z$;

12) множество комплексных чисел вида $x + yi$, где $x, y \in \mathrm{Q}$;

2.12. Какие из указанных множеств матриц образуют кольцо относительно матричного сложения и умножения:

1) множество вещественных симметрических матриц порядка n;

2) множество верхних треугольных матриц порядка $n \geq 2$;

3) множество матриц порядка $n \geq 2$, у которых две последние строки нулевые;

4) множество матриц вида $\begin{pmatrix} x & y \\ Dy & x \end{pmatrix}$, где D – фиксированное целое число, $x,y \in Z$;

2.13 Какие из следующих множеств функций образуют кольцо относительно обычных операций сложения и умножения функций:

1) множество функций вещественного переменного, непрерывных на отрезке [*a, b*];

2) множество функций, имеющих вторую производную на интервале (*a, b*);

3) множество целых рациональных функций вещественного переменного;

4) множество рациональных функций вещественного переменного;

5) множество функций вещественного переменного, обращающихся в 0 на некотором подмножестве $D \subseteq R$;

6) множество тригонометрических многочленов

$$a_0 + \sum_{k=1}^{n} (a_k \cos kx + b_k \sin kx)$$

с вещественными коэффициентами, где n — произвольное натуральное число;

7) все степенные ряды от одной или нескольких переменных;

8) все лорановские степенные ряды от одной переменной ?

2.14 Какие из колец в задачах 11, 12, 13 являются полями?

2.15 Какие из следующих множеств матриц образуют поле относительно обычных матричных операций

1) $\left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix}; \quad x, y \in Q \right\}$, где n – фиксированное целое число;

2) $\left\{\begin{pmatrix} x & y \\ ny & x \end{pmatrix};\quad x, y \in R\right\}$, где n – фиксированное целое число;

3) $\left\{\begin{pmatrix} x & y \\ ny & x \end{pmatrix};\quad x, y \in Z\right\}$, где n – фиксированное целое число;

Часть 3 Теория многочленов

1. Кольцо многочленов

Понятие многочлена, или целой рациональной функции, от неизвестного x возникло в связи с задачей решения алгебраических уравнений первой и выше первой степени с одним неизвестным, задачей, которой занимались уже в глубокой древности. Еще за 2000 лет до нашей эры в древнем Вавилоне умели решать задачи, сводящиеся к квадратным уравнениям, а при помощи таблиц решали некоторые задачи, приводящие даже к уравнениям третьей степени.

Обратимся к алгебраическому уравнению *n-й* степени *(n* — целое положительное число):

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0,$$

где $a_0, a_1, \ldots, a_n$ — комплексные (в частности, действительные) числа. Его левая часть $a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ и называется многочленом n-й степени от неизвестного x.

Пусть P — некоторое числовое поле. Элементы поля P мы будем обозначать начальными буквами *a, b, c, ...* латинского алфавита. *Многочленом от x над полем P мы назовем выражение вида:*

$$a_1 x^{k_1} + a_2 x^{k_2} + \ldots + a_s x^{k_s}, \ (s \geq 1), \qquad (3.1.1)$$

где $a_1, a_2, \ldots, a_s$ — *числа из P,* $k_1 < k_2 < \ldots < k_s$ — *целые неотрицательные числа.*

Очевидно, что, складывая или перемножая два каких-нибудь многочлена от неизвестного x с коэффициентами из P, мы всегда получаем однозначно многочлен от x *с* коэффициентами из того же поля P.

Обозначим теперь через $P[x]$ это множество многочленов. Действия сложения и умножения подчиняются основным алгебраическим законам.

Множество многочленов *P [x]* мы будем коротко называть *кольцом многочленов от x над P.*

Назовем *степенью* многочлена наибольшую из степеней его членов, у которых коэффициенты не равны нулю.

Пример 3.1.2,

$$f(x) = 1 + 2x — 7x^2 + 0•x^3 + 5x^4 + 0•x^5$$

есть многочлен четвертой степени над полем рациональных чисел.

Для многочленов, как и для целых чисел, существует алгоритм деления с остатком. Рассмотрим кольцо многочленов над полем комплексных чисел. Справедлива следующая

Теорема 3.1.1. *Для любых двух многочленов f(x) и g(x) можно найти такие многочлены q(x) и r(x), что*

$$f(x)=g(x)q(x) + r(x), \qquad (3.1.1)$$

причем степень r(x) меньше степени g(x) или же r(x) = 0. Многочлены q (x) и r(x), удовлетворяющие этому условию, определяются однозначно.

Заметим, что многочлен *q(x)* называется *частным от* деления *f(x)* на *g(x),* а *r(x)— остатком* от этого деления.

2 Наибольший общий делитель многочленов.

Пусть даны ненулевые многочлены *f(x)* и *φ(x)* с комплексными коэффициентами. Если остаток от деления *f(x)* на *φ(x)* равен нулю, т. е., как говорят, *f(x) делится* (или *нацело делится)* на *φ(x),* то многочлен *φ(x)* называется *делителем* многочлена *f(x).*

Многочлен φ(x) тогда и только тогда будет делителем многочлена f(x), если существует многочлен ψ(x), удовлетворяющий равенству

$$f(x) = \varphi(x)\psi(x). \qquad (3.2.1)$$

В самом деле, если *φ(x)* является делителем для *f(x),* то в качестве *ψ(x)* следует взять частное от деления *f(x)* на *φ(x).* Обратно, пусть многочлен *ψ(x),* удовлетворяющий равенству (3.2.1), существует.

Из единственности многочленов $q(x)$ и $r(x)$, удовлетворяющих равенству

$$f(x) = \varphi(x)q(x) + r(x)$$

и условию, что степень $r(x)$ меньше степени $\varphi(x)$, в нашем случае следует, что частное от деления $f(x)$ на $\varphi(x)$ равно $\psi(x)$, а остаток равен нулю.

Пусть даны произвольные многочлены $f(x)$ и $g(x)$. Многочлен $\varphi(x)$ будет называться *общим делителем* для $f(x)$ и $g(x)$, если он служит делителем для каждого из многочленов. Если других общих делителей эти два многочлена не имеют, то они называются *взаимно простыми.*

В общем же случае многочлены $f(x)$ и $g(x)$ могут обладать делителями, зависящими от x. Введем понятие *наибольшего* общего делителя этих многочленов.

Наибольшим общим делителем отличных от нуля многочленов $f(x)$ и $g(x)$ называется такой многочлен $d(x)$, который является их общим делителем и, вместе с тем, сам делится на любой другой общий делитель этих многочленов. Обозначается наибольший общий делитель многочленов $f(x)$ и $g(x)$ символом $(f(x), g(x))$.

Для целых чисел существует, *алгоритмом последовательного деления* или *алгоритм Евклида;* этот способ вполне применим и к многочленам.

Пример. 3.2.1 Найти наибольший общий делитель многочленов $f(x)=x^4+3x^3-x^2-4x-3$, $g(x)=3x^3+10x^2+2x-3$.

Применяя алгоритм Евклида к многочленам с целыми коэффициентами, мы можем, чтобы избежать дробных коэффициентов, умножить делимое или сократить делитель на любое не равное нулю число, причем не только начиная какое-либо из последовательных делений, но и в процессе самого этою деления. Это будет приводить, понятно, к искажению частного, но интересущие нас остатки будут

приобретать лишь некоторый множитель нулевой и пени, что, как мы знаем, при разыскании наибольшего общего делителя допускается.

Делим $f(x)$ на $g(x)$, предварительно умножив $f(x)$ на 3:

$$\begin{array}{l|l} 3x^4+9x^3-3x^2-12x-9 & 3x^3+10x^2+2x-3 \\ \underline{3x^4+10x^3+2x^2-3x} & \overline{x+1} \\ -x^3-5x^2-9x-9 & \end{array}$$

умножаем на -3

$$\begin{array}{r} 3x^3+15x^2+27x+27 \\ \underline{3x^3+10x^2+2x\quad -\ 3} \\ 5x^2+25x+30. \end{array}$$

Таким образом, первый остаток, после сокращения на 5, будет $r_1(x)=x^2+5x+6$. Делим на него многочлен $g(x)$:

$$\begin{array}{l|l} 3x^3+10x^2+2x-3 & x^2+5x+6 \\ \underline{3x^3+15x^2+18x} & \overline{3x-5} \\ -5x^2-16x-3 & \\ \underline{-5x^2-25x-30} & \\ 9x+27. & \end{array}$$

Вторым остатком, после сокращения на 9, будет, следовательно, $r_2(x)=x+3$. Так как

$$r_1(x)=r_2(x)(x+2),$$

то $r_2(x)$ будет тем последним остатком, на который нацело делится предшествующий остаток. Он будет, таким образом, искомым наибольшим общим делителем:

$$(f(x),\ g(x))=x+3.$$

Справедлива следующая

Теорема 3.2.1. *Если $d(x)$ есть наибольший общий делитель многочленов $f(x)$ и $g(x)$, то можно найти такие многочлены $u(x)$ и $v(x)$, что*

$$f(x)u(x)+g(x)v(x)=d(x). \qquad (3.2.3)$$

Можно считать при этом, если степени многочленов $f(x)$ и $g(x)$ больше нуля, что степень $u(x)$ меньше степени $g(x)$, а степень $v(x)$ меньше степени $f(x)$.

Доказательство основано на равенствах (3.2.2). Если мы учтем, что $r_k(x) = d(x)$, и положим $u_1(x) = 1$, $v_1(x) = —q_k(x)$, то предпоследнее из равенств (3.2.2) даст:

$$d(x) = r_{k-2}(x)\, u_1(x) + r_{k-1}(x)\, v_1(x).$$

Подставляя сюда выражение $r_{k-1}(x)$ через $r_{k-2}(x)$ и $r_{k-2}(x)$ из предшествующего равенства (3.2.2), мы получим:

$$d(x) = r_{k-3}(x)\, u_2(x) + r_{k-2}(x)\, v_2(x),$$

где, очевидно, $u_2(x)=v_1(x)$, $v_2(x) = u_1(x)—v_1(x)q_{k-1}(x)$. Продолжая подниматься вверх по равенствам (3.2.2), мы придем, наконец, к доказываемому равенству (3.2.3).

Для доказательства второго утверждения теоремы предположим, что многочлены $u(x)$ и $v(x)$, удовлетворяющие равенству (3.2.3), уже найдены, но, например, степень $u(x)$ больше или равна степени $g(x)$. Делим $u(x)$ на $g(x)$:

$$u(x)=g(x)q(x) + r(x),$$

где степень $r(x)$ меньше степени $g(x)$, и подставляем это выражение в (3.2.3). Мы получим равенство

$$f(x)\, r(x) + g(x)\, [v(x) + f(x)\, q(x)] = d(x).$$

Степень множителя, стоящего при $f(x)$, уже меньше степени $g(x)$. Степень многочлена, стоящего в квадратных скобках, будет в свою очередь меньше степени $f(x)$, так как в противном случае степень второго слагаемого левой части была бы не меньше степени произведения $g(x)f(x)$, а так как степень первого слагаемого меньше степени этого произведения, то вся левая часть имела бы степень, большую или равную степени $g(x)f(x)$, тогда как многочлен $d(x)$ заведомо имеет, при наших предположениях, меньшую степень. Теорема доказана.

Одновременно мы получаем, что если многочлены *f(x)* и *g(x)* имеют рациональные или действительные коэффициенты, то и многочлены *u(x)* и *v(x),* удовлетворяющие равенству (3.2.3), можно подобрать так, что их коэффициенты будут рациональными или, соответственно, действительными.

Пример 3.2.2. Найдем многочлены *u(x) и v(x),* удовлетворяющие равенству (3.2.3) при

$$f(x)=x^3-x^2+3x-10,\ g(x)=x^3+6x^2-9x-14.$$

Применим к этим многочленам алгоритм Евклида, причем теперь при выполнении делений уже нельзя допускать искажения частных, так как эти частные используются при разыскании многочленов *u(x)* и *v(x).* Мы получим такую систему равенств:

$$f(x)=g(x)+(-7x^2+12x+4);$$

$$g(x)=(-7x^2+12x+4)\left(-\frac{1}{7}x-\frac{54}{49}\right)+\frac{235}{49}(x-2);$$

$$-7x^2+12x+4=(x-2)(-7x-2).$$

Отсюда следует, что $(f(x),\ g(x))=x-2$ и что

$$u(x)=\frac{7}{235}x+\frac{54}{235},\quad v(x)=-\frac{7}{235}x-\frac{5}{235}.$$

Применяя доказанную сейчас теорему к взаимно простым многочленам, мы получаем такой результат:

Многочлены f(x) и g(x) тогда и. только тогда взаимно просты, если можно найти многочлены. u(x) и v (x), удовлетворяющие равенству

$$f(x)u(x)+g(x)v(x)=1. \qquad (3.2.4)$$

Опираясь на этот результат, можно доказать несколько простых, но важных теорем о взаимно простых многочленах.

Теорема 3.2.2. *Если многочлен f(x) взаимно прост с каждым из многочленов $\varphi(x)$ и $\psi(x)$, то он взаимно прост и с их произведением.*

Теорема 3.2.3. *Если произведение многочленов $f(x)$ и $g(x)$ делится на $\varphi(x)$, но $f(x)$ и $\varphi(x)$ взаимно просты, то $g(x)$ делится на $\varphi(x)$.*

Теорема 3.2.4. *Если многочлен $f(x)$ делится на каждый из многочленов $\varphi(x)$ и $\psi(x)$, которые между собой взаимно просты, то $f(x)$ делится и на их произведение.*

Определение наибольшего общего делителя может быть распространено на случай любой конечной системы многочленов: *наибольшим общим делителем* многочленов $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ называется такой общий делитель этих многочленов, который делится на любой другой общий делитель этих многочленов. Существование наибольшего общего делителя для любой конечной системы многочленов вытекает из следующей теоремы, дающей также способ его вычисления.

Теорема 3.2.5. *Наибольший общий делитель многочленов $f(x)$, $f_2(x)$, ..., $f_s(x)$ равен наибольшему общему делителю многочлена $f_s(x)$ и наибольшего общего делителя многочленов $f_1(x)$, $f_2(x)$, ..., $f_{s-1}(x)$.*

В частности, система многочленов $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ называется *взаимно простой,* если общими делителями этих многочленов являются лишь многочлены нулевой степени, т. е. если их наибольший общий делитель равен 1. Если $s>2$, то попарно эти многочлены могут и не быть взаимно простыми.

3 Корни многочленов.

Если

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \qquad (3.3.1)$$

есть некоторый многочлен, а c — некоторое число, то число

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

полученное заменой в выражении (3.3.1) для $f(x)$ неизвестного x; числом c и последующим выполнением всех указанных операций, называется *значением многочлена $f(x)$ при $x = c$.* Если $f(c)=0$, т. е. многочлен $f(x)$

обращается в нуль при подстановке в него числа с вместо неизвестного, то *с* называется *корнем* многочлена *f(x)* (или уравнения *f(x)=0).*

Если мы будем делить многочлен *f(x)* на произвольный многочлен первой степени (или, как будем говорить дальше, на *линейный многочлен),* то остаток будет либо некоторым многочленом нулевой степени, либо нулем, т. е. во всяком случае некоторым числом *r*. Следующая теорема позволяет найти этот остаток, не выполняя деления, в случае, когда производится деление на многочлен вида *x—c.*

Пример 3.3.1 Разделить $f(x) = 2x^5 - x^4 - 3x^3 + x - 3$ на $x - 3$.

Составим таблицу, в которой над чертой расположены коэффициенты многочлена *f(x),* под чертой — соответствующие коэффициенты частного и остаток, последовательно вычисляемые, а слева сбоку — значение *с* в данном примере:

	2	−1	−3	0	1	−3
3	2,	$3\cdot 2-1=5$,	$3\cdot 5-3=12$,	$3\cdot 12+0=36$,	$3\cdot 36+1=109$,	$3\cdot 109-3=324$

Таким образом, искомое частное будет

$$q(x) = 2x^4 + 5x^3 + 12x^2 + 36x + 109,$$

а остаток $r=f(3)=324$.

Если *с* — корень многочлена *f(x),* т, е. $f(c)=0$, то *f(x)* делится на *x—c*. Может оказаться, что многочлен *f(x)* делится не только на первую степень линейного двучлена *x—c,* но и на более высокие его степени. Во всяком случае найдется такое натуральное число *k,* что *f(x)* нацело делится на $(x-c)^k$, но не делится на $(x-c)^{k+1}$. Поэтому

$$f(x)=(x-c)^k \varphi(x),$$

где многочлен $\varphi(x)$ на $x - c$ уже не делится, т. е. число *с* своим корнем не имеет. Число *k* называется *кратностью* корня *с в* многочлене *f(x),* а сам корень *с — k-кратным корнем* этого многочлена. Если $k=1$, то говорят, что корень *с — простой.*

Пусть дан многочлен *n*-й степени

$$f(x) = a_0x^n + a_1x^{n-1}+...+a_{n-1}x + a_n$$

с любыми комплексными коэффициентами. Его *производной* (или *первой производной)* называется многочлен *(n*—1)-й степени

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + ... + 2a_{n-2}x + a_{n-1}.$$

Теорема 3.3.1. *Если число c является k-кратным корнем многочлена f(x), то при k*>1 *оно будет (k*—1*)-кратным корнем первой производной этого многочлена; если же k*=1*, то c не будет служить корнем для f'(x).*

*k-кратный корень многочлена f(x) будет (k — s)-кратным в s-*й *производной этого многочлена (k*≤*s)) и не будет служить корнем для k-й производной от f(x).*

4 Основная теорема алгебры

Основная теорема. *Всякий многочлен с любыми числовыми коэффициентами, степень которого не меньше единицы, имеет хотя бы один корень, в общем случае комплексный.*

Пусть дан многочлен *n-й* степени, *n*≥1,

$$f(x) = a_0x^n + a_1x^{n-1}+...+a_{n-1}x + a_n \qquad (3.4.1)$$

с любыми комплексными коэффициентами. Основная теорема о существовании корня позволяет утверждать существование для *f(x)* корня α_1 комплексного или действительного. Поэтому многочлен *f(x)* обладает разложением

$$f(x) = (x — \alpha_1)\varphi(x).$$

Коэффициенты многочлена $\varphi(x)$ снова являются действительными или комплексными числами, и поэтому $\varphi(x)$ обладает корнем α_2, откуда

$$f(x) = (x — \alpha_1)(x — \alpha_2)\psi(x).$$

Продолжая так далее, мы придем после конечного числа шагов к разложению многочлена *n-й* степени *f(x) в* произведение *n* линейных множителей,

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n) \qquad (3.4.2)$$

Коэффициент a_0 появился по следующей причине: если бы справа в выражении (3.4.2) стоял некоторый коэффициент b, то после раскрытия скобок старший член многочлена $f(x)$ имел бы вид bx^n, хотя на самом деле, ввиду (3.4.1), им является член a_0x^n. Поэтому $b=a_0$.

Разложение (3.4.2) *является для многочлена f(x) единственным с точностью до порядка сомножителей разложением такого типа.*

Объединяя вместе одинаковые множители, разложение (3.4.2) можно переписать в виде

$$f(x) = a_0(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\ldots(x-\alpha_l)^{k_l}, \qquad (3.4.3)$$

где

$$k_1 + k_2 + \ldots + k_l = n.$$

При этом предполагается, что среди корней $\alpha_1,\alpha_2,\ldots,\alpha_l$ уже нет равных.

Число k_i из (3.4.3), $i = 1, 2, \ldots, l$, *является кратностью корня α_i- в многочлене f(x).*

Всякий многочлен f(x) степени n, $n\geq 1$, с любыми числовыми коэффициентами имеет n корней, если каждый из корней считать столько раз, какова его кратность.

5 Неприводимые многочлены над полем комплексных чисел

Многочлен f(x) из P[x] называется приводимым над полем P, если он может быть разложен в произведение двух многочленов меньшей степени из того же кольца P[x].

Многочлен p(x) выше нулевой степени из P[x] называется неприводимым над полем P, если p(x) не может быть разложен в произведение двух многочленов меньшей степени из того же кольца P[x].

Согласно этому определению многочлен нулевой степени нельзя считать приводимым, а также нельзя считать неприводимым многочленом.

Пример. 3.5.1 Многочлен $f(x) = x^4 - 5x^2 + 6$ можно разложить на множители: $f(x) = (x^2 - 2)(x^2 - 3)$, причем $x^2 - 2$ и $x^2 - 3$ имеют степень меньшую, чем $f(x)$, и являются многочленами над тем же полем рациональных чисел, что $f(x)$. Следовательно, рассматриваемый многочлен $f(x)$ приводим над полем рациональных чисел.

Пример 3.5.2. Многочлен первой степени $p(x) = x + 1$ неприводим над любым числовым полем P.

Действительно, если $g(x)$ и $h(x)$ —произвольные, многочлены выше нулевой степени, то их произведение будет иметь по меньшей мере вторую, а не первую степень.

Пример 3.5.3.Многочлен $p(x) = x^2 - 2$ неприводим над полем рациональных чисел.

Однако этот же многочлен будет уже приводимым над полем действительных чисел, так как в поле действительных чисел мы считаем допустимым разложение и на множители с иррациональными коэффициентами:

$$p(x) = (x-\sqrt{2})(x+\sqrt{2}).$$

Для многочленов кольца $P[x]$ имеет место теорема, аналогичная теореме о разложении целого числа на простые множители.

Основная теорема теории делимости многочленов. *Всякий многочлен из $P[x]$ выше нулевой степени разлагается в произведение неприводимых многочленов:*

$$f(x) = p_1(x)\, p_2(x) \ldots p_k(x),$$

($p_i(x)$ — неприводимый многочлен над полем P), и это разложение является единственным с точностью до порядка следования и множителей нулевой степени.

Рассмотрим несколько свойств неприводимых многочленов, сходных со свойствами простых чисел.

I. *Если $p_1(x)$ и $p_2(x)$ — неприводимые многочлены над полем P и $p_1(x)$ делится на $p_2(x)$, то справедливо $p_1(x)=cp_2(x)$, где $c\neq 0$.*

II. *Многочлен $f(x)$ из $P[x]$ тогда и только тогда не делится на многочлен $p(x)$, неприводимый над полем P, когда $f(x)$ и $p(x)$ взаимно просты.*

III. Если произведение $f(x)\ g(x)$ двух многочленов $f(x)$ и $g(x)$ из $P[x]$ делится на многочлен $p(x)$, неприводимый над P, то на $p(x)$ делится по меньшей мере один из сомножителей $f(x)$, $g(x)$.

Теорема 3.5.1. *Над полем всех комплексных чисел неприводимыми являются только полиномы первой степени,*

Доказательство. Что полиномы первой степени неприводимы, мы уже знаем. Пусть степень полинома $f(x)$ над полем всех комплексных чисел больше единицы. Тогда полином $f(x)$ должен иметь корень. Обозначим его через α. $f(x)$ будет делиться на полином первой степени $x-\alpha$. Поэтому $f(x)$ будет приводимым над полем комплексных чисел.

6 Неприводимые полиномы над полем всех вещественных чисел

Обозначим через P поле всех вещественных чисел. Для произвольного комплексного числа $z\in Z$ определим полином $\psi_z(x)$, который будет играть вспомогательную роль в дальнейших построениях:

$$\psi_z(x)=\begin{cases} x-z, & \text{если } z\in R,\\ (x-z)(x-\overline{z}), & \text{если } \overline{z}\notin R.\end{cases}$$

(здесь z означает комплексное число, сопряженное с числом z в смысле общей теории комплексных чисел).

Сразу отметим, что z является корнем полинома $\psi_z(x)$.

В обоих случаях $\psi_z(x)$ есть полином над R.

В первом случае это непосредственно очевидно. Во втором имеем:

$$\psi_z(x) = (x - z)(x - \bar{z}) = x^2 - (z + \bar{z})x + z\bar{z}..$$

Коэффициенты оказываются вещественными, так как и сумма и произведение сопряженных комплексных чисел вещественны.

Теорема 3.6.1. *Полином f (x) над R имеет своим корнем число z тогда и только тогда, когда f (x) делится на полином* $\psi_z(x)$.

Доказательство. 1) Пусть $f(x)$ делится на $\psi_z(x)$

$$f(x) = \psi_z(x)s(x).$$

Имеем: $f(z) = \psi_z(z)\, s(z) = 0$, поскольку z—корень для $\psi_z(x)$.

2) Пусть $f(z) = 0$. Тогда по следствию из теоремы Безу $f(x)$ делится на x. В случае $z \notin R$ совершаем деление с остатком $f(x)$ на $\psi_z(x)$:

$$f(x) = \psi_z(x)s(x) + Ax + B.$$

Поскольку степень $\psi_z(x)$ равна двум, степень остатка $Ax + B$ не может превосходить 1. Так как $f(x)$ и $\psi_z(x)$ *оба* являются полиномами над R, то и остаток есть полином над R, т. е. $A, B \in R$.

Положив в этом равенстве $x = z$, получаем:

$$f(z) = \psi_z(z)s(z) + Az + B,$$

$$0 = 0 + Az + B.$$

При $A \neq 0$ мы получили бы $z = -\frac{B}{A} \in R$, что в рассматриваемом случае не так.

Следовательно, $A = 0$. Но тогда из последнего равенства получаем также и $B = 0$.

То, что $A = B = 0$, означает, что $f(x)$ делится на $\psi_z(x)$.

Пример 3.6.1. Для числа 5 имеем $\psi_5(x) = x - 5$.

Для $1 + i$ имеем $\psi_{1+i}(x) = [x-(1+i)][x-(1-i)]$. Раскрывая скобки, получаем $= \psi_{1+i}(x) = x^2 - 2x + 2$.

Теорема 3.6.2. *Если комплексное число* $z = a + bi$ *является корнем полинома* $f(x)$ *надR, то и сопряженное с ним число* $z=a — bi$ *будет корнем этого полинома.*

Доказательство. Так как z есть корень $f(x)$, то $f(x)$ делится на $\psi_z(x)$. Из самого вида $\psi_z(x)$ следует, что и число $\bar{z}$ является корнем $\psi_z(x)$. (в случае $z \in R$ имеем $z = \bar{z}$). Но тогда $\bar{z}$ будет корнем и для $f(x)$.

Теорема 3.6.3. *Над полем всех вещественных чисел, кроме полиномов первой степени, неприводимыми являются только такие полиномы второй степени*

$$ax^2 + bx + c,$$

у которых

$$b^2 — 4ac < 0.$$

Следствие оразложении намножители полиномов над R. *Полином степени n над полем всех вещественнных чисел может быть единственным образом представлен в виде следующего произведения полиномов первой и второй степени над R:*

$$f(x) = a(x-\alpha_1)...(x-\alpha_k)(x^2 + p_1x + q_1)...(x^2 + p_lx + q_l),$$

где

$$a \neq 0,\ p_i^2 - 4q_i < 0\ (i = 1,\ 2,\ \ldots,\ l),\ k + 2l = n.$$

7 Неприводимые полиномы над полем всех рациональных чисел

Перейдем к третьему основному числовому полю — полю всех рациональных чисел. Как непосредственно следует из определения неприводимых полиномов, чем «меньше» поле, тем многочисленнее и разнообразнее неприводимые над данным полем полиномы. В самом «большом» поле — поле всех комплексных чисел — неприводимыми оказывались лишь полиномы первой степени. В поле всех вещественных чисел наравне с полиномами первой степени неприводимыми оказались уже и некоторые полиномы второй степени. В «минимальном поле» — поле всех

рациональных чисел Q — встречаются неприводимые полиномы любой степени. При этом они столь разнообразны, что описать их всех каким-нибудь удобным способом нам не удастся.

Среди полиномов над Q особого внимания заслуживают целочисленные полиномы, т. е. полиномы, коэффициентами которых являются целые числа. В дальнейшем нам понадобится следующее свойство целочисленных полиномов.

Лемма.3.7.1. *Пусть простое число p таково, что у полиномов с целыми коэффициентами*

$$f_1(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n,$$

$$f_2(x)=b_0x^m+b_1x^{m-1}+\ldots+b_{m-1}x+b_m$$

не все коэффициенты $a_0, a_1, a_2. \ldots, a_{n-1}, a_n$ *делятся на p и не все коэффициенты* $b_0, b_1, b_2, \ldots, b_{m-1}, b_m$ *делятся на p. Если у произведения этих полиномов*

$$f_1(x)f_2(x)=c_0x^{n+m}+c_1x^{n+m-1}+\ldots+c_{n+m-1}x+c_{n+m}$$

коэффициенты $c_1, c_2, \ldots, c_{n+m-1}, c_{n+m}$ *делятся на p, то у исходных полиномов должны делиться на p коэффициенты* $a_1, a_2, \ldots, a_{n-1}, a_n, b_1, b_2, \ldots, b_{m-1}, b_m$.

Теорема о приводимости целочисленных полиномов*. Полином с целыми коэффициентами, приводимый над полем всех рациональных чисел, разлагается на произведение полиномов ненулевой степени с целыми коэффициентами.*

Доказательство. Если полином с целыми коэффициентами $f(x)$ приводим над полем всех рациональных чисел, то он может быть разложен на произведение двух полиномов ненулевой степени, коэффициенты которых — рациональные числа. Умножим $f(x)$ на такое натуральное число n, чтобы указанное разложение превратилось в разложение полинома $nf(x)$ на произведение двух полиномов ненулевой степени, коэффициенты которых будут уже целыми числами:

$$nf(x) = f_1(x)\, f_2\,(x).$$

Пусть n есть наименьшее из натуральных чисел, таких, что $nf(x)$ разлагается на произведение полиномов ненулевой степени с целыми коэффициентами. Для доказательства нашей теоремы надо показать, что $n = 1$. Допустим противное: пусть $n > 1$. Обозначим через p какое-либо простое число, являющееся делителем n. Если бы все коэффициенты $f_1(x)$ делились на p, то можно было бы в нашем равенстве произвести сокращение на p, разделив слева n *на* p и справа все коэффициенты $f_1(x)$ на p. После этого мы получили бы опять требуемое разложение, но с первым множителем $\frac{n}{p}$, меньшим n, что противоречит определению числа n. Следовательно, не все коэффициенты полинома $f_1(x)$ делятся на p. Совершенно аналогично убеждаемся, что не все коэффициенты $f_2(x)$ делятся на p. Что касается коэффициентов полинома $nf(x)$, то они все делятся на p, *так* как n делится на p. Значит, к нашему разложению применима лемма 3.1.1. Согласно этой лемме все коэффициенты $f_1(x)$ и $f_2(x)$, кроме старших, делятся на p. Старшие же коэффициенты не могут делиться на p, так как среди коэффициентов $f_1(x)$ и $f_2(x)$ должны иметься не делящиеся на p. Однако это противоречит тому, что произведение старших коэффициентов $f_1(x)$ и $f_2(x)$ равно старшему коэффициенту полинома $nf(x)$, делящемуся на p.

В качестве примера использования доказанных выше леммы и теоремы приведем одно следствие, дающее достаточное (но отнюдь не необходимое) условие неприводимости целочисленного полинома над полем всех рациональных чисел.

С л е д с т в и е . (***Признак неприводимости Эйзенштейна)*** *Если все коэффициенты полинома*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

целые числа, причем a_0 не делится на некоторое простое число p, тогда как все остальные коэффициенты делятся на p, причем, однако, a_n не делится на p^2, то f(x) неприводим над полем всех рациональных чисел.

Доказательство. Если бы *f(x)* был приводим над полем всех рациональных чисел, то он разлагался бы на множители ненулевой степени, имеющие коэффициентами целые числа. Старшие коэффициенты каждого из этих множителей не делятся на p, так как a_0 не делится на p. Поэтому можно применить лемму 3.7.1, согласно которой все прочие коэффициенты множителей, в том числе и свободные члены, должны делиться на p. Но отсюда следовало бы, что a_n равное произведению этих свободных членов, делилось бы на p^2.

Пример 3.7.1 Полином

$$5x^5 + 6x^4 - 144x^3 + 18x^2 - 42x + 12$$

неприводим над полем всех рациональных чисел. Действительно, все его коэффициенты, кроме старшего, делятся на 3, причем свободный член не делится на 9.

Вопрос о рациональных корнях полиномов над *Q,* очевидно, непосредственно сводится к нахождению рациональных корней полиномов с целыми коэффициентами. Для решения последней задачи существует алгоритм, очень просто выводимый и вполне пригодный для применения в тех или иных конкретных случаях.

Теорема 3.7.1. *Если рациональное число $\frac{p}{q}$ (где p и q — взаимно простые целые числа) является корнем полинома с целыми коэффициентами f(x), то p является делителем свободного члена, а q — делителем старшего коэффициента.*

Теорема 3.7.1 дает способ нахождения всех рациональных корней полинома с целыми коэффициентами. Для этого надо сперва найти всевозможные делители старшего коэффициента и всевозможные делители свободного члена. Этих делителей конечное число, и

нахождение их обычно не представляет труда. Затем надо составить всевозможные дроби $\frac{p}{q}$, где p — делитель свободного члена, а q — делитель старшего коэффициента, причем p и q взаимно просты. Не обязательно все получившиеся числа $\frac{p}{q}$ будут корнями нашего полинома, но все рациональные корни будут находиться среди этих чисел. Поэтому, вычисляя значения $f\left(\frac{p}{q}\right)$ для всех этих чисел, узнаем, какие из них действительно являются корнями, а какие нет. Вычисление $f\left(\frac{p}{q}\right)$ можно вести путем деления с остатком на $x-\frac{p}{q}$. В этом случае, повторяя деление частного, мы одновременно узнаем и кратность каждого корня.

Вычисления, связанные с изложенным выше способом, могут быть значительно сокращены, если воспользоваться еще одним необходимым (но опять-таки не достаточным) условием того, чтобы заданное рациональное число являлось корнем данного полинома с целыми коэффициентами.

Теорема 3.7.2. *Пусть рациональное число* $\frac{p}{q}$, *где p и q — взаимно простые целые числа, является корнем полинома с целыми коэффициентами f(x). Тогда при всяком целом числе m целое число f(m) будет делиться на (p — qm).*

Пример 3.7.2. Найдем все рациональные корни полинома:

$$f(x) = 12x^5 — 41x:^4 + x^3 + 47^2 — 4x — 12.$$

Если $\frac{p}{q}$, где p и q — взаимно простые целые числа, есть корень $f(x)$, то p и q могут принимать следующие значения:

$$p \mid \pm 1, \pm 2, \pm 3, \pm 4, +6, \pm 12$$

q | 1, 2, 3, 4, 6, 12

Различных, подлежащих проверке комбинаций $\frac{p}{q}$ оказывается несколько десятков. Поэтому воспользуемся теоремой 3.7.2. Без труда вычисляется значение *f(x)* при $x = 1$:

$$f(1) = 3.$$

Согласно теореме 3.7.2, p — q должно быть делителем 3, т. е. p — q может равняться или ±1, или ±3.

Благодаря этому некоторые из первоначальных возможностей отпадают (например, $3 = \frac{3}{1}$, поскольку в этом случае $p = 3$, $q = 1$, т. е. p — $q = 2$), Очевидно, остаются лишь следующие возможности:

$$\frac{p}{q} = \frac{1}{2},\ \frac{1}{4},\ \frac{2}{1},\ \frac{2}{3},\ \frac{3}{2},\ \frac{3}{4},\ \frac{4}{1},\ \frac{4}{3},\ -\frac{1}{2},\ -\frac{2}{1}.$$

Теперь вычислим значение *f(x)* при $x = —1$:

$$f(-1) = -15.$$

Согласно теореме 3.8.2 отсюда следует, что $p + q$ может равняться лишь ±1, ±3, ±5 ±15. Благодаря этому отпадают числа $\frac{3}{4}$ и $\frac{4}{3}$.

Вычислим $f(2)$:

$$f(2) = -96.$$

Отсюда следует, что p — $2q$ есть делитель —96. Но для всех наших чисел $\frac{p}{q}$ число p — $2q$ по абсолютной величине не превосходит 7. Следовательно, $p—2q$ может равняться лишь ±1, ±2, ±3, ±4, ±6. Этому условию удовлетворяют лишь следующие числа:

$$\frac{p}{q} = \frac{1}{2},\ \frac{2}{3},\ \frac{3}{2},\ \frac{4}{1},\ -\frac{2}{1}.$$

Осталось лишь пять чисел, относительно которых существует сомнение, не являются ли некоторые из них корнями нашего полинома.

Непосредственной проверкой (для чего удобно привлечь схему Горнера) убеждаемся, что числа $\frac{1}{2}, \frac{3}{2}, 4, -2$ не являются корнями полинома *f(x), а* $\frac{2}{3}$ есть корень.

8 Рациональные дроби

В курсе математического анализа изучаются, помимо целых рациональных функций, названных нами многочленами, также *дробно-рациональные функции;* это будут частные $\frac{f(x)}{g(x)}$ двух целых рациональных функций, где $g(x) \neq 0$. Над этими функциями производятся алгебраические операции по таким же законам, как над рациональными числами, т. е. как над дробями с целыми числителями и знаменателями. Равенство двух дробно-рациональных функций или, *рациональных дробей* также понимается и том же смысле, что и равенство дробей в элементарной арифметике. Для определенности будем рассматривать рациональные дроби с действительными коэффициентами; нетрудно заметить, что все, ниже изложенное может быть почти дословно перенесено на случай рациональных дробей с комплексными коэффициентами.

Рациональная дробь называется *несократимой,* если ее числитель взимно прост со знаменателем.

Всякая рациональная дробь равна некоторой несократимой дроби, определяемой однозначно с точностью до множителя нулевой степени, общего для числителя и знаменателя.

Рациональная дробь называется *правильной,* если степень числителя меньше степени знаменателя. Если к числу правильных дробей условимся причислять многочлен 0, то справедлива следующая

Теорема 3.8.1. *Всякая рациональная дробь представила, притом единственным способом, в виде суммы многочлена и правильной дроби.*

Правильная рациональная дробь $\frac{f(x)}{g(x)}$ называется *простейшей,* если ее знаменатель $g(x)$ является степенью неприводимого многочлена $p(x)$,

$$g(x) = p^k(x),\ k \geq 1,$$

а степень числителя $f(x)$ меньше степени $p(x)$.

Справедлива следующая

Теорема 3.8.2. *Всякая правильная рациональная дробь разлагается в сумму простейших дробей.*

Пример.3.8.1 Разложить в сумму простейших дробей действительную правильную дробь $\frac{f(x)}{g(x)}$, где

$$f(x) = 2x^4 - 10x^3 + 7x^2 + 4x + 3,$$
$$g(x) = x^5 - 2x^3 + 2x^2 - 3x + 2.$$

Легко проверяется, что

$$g(x) = (x+2)(x-1)^2(x^2+1),$$

причем каждый из многочленов $x+2$, $x-1$, x^2+1 неприводим. Искомое разложение должно иметь вид

$$\frac{f(x)}{g(x)} = \frac{A}{x+2} + \frac{B}{(x-1)^2} + \frac{C}{x-1} + \frac{Dx+E}{x^2+1}, \qquad (3.8.1)$$

где числа A, B, C, D и E еще должны быть разысканы. Из (3.9.3) вытекает равенство

$$f(x) = A(x-1)^2(x^2+1) + B(x+2)(x^2+1) + C(x+2)(x-1)(x^2+1) + D x(x+2)(x-1)^2 + E(x+2)(x-1)^2 . \qquad (3.8.2)$$

Приравнивая коэффициенты при одинаковых степенях неизвестного x из обеих частей равенства (3.8.2), мы получили бы систему пяти линейных уравнений относительно пяти неизвестных A, B, C, D, E, причем, эта

система обладает решением и притом единственым. Мы пойдем, однако, иным путем.

Полагая в равенстве (3.8.2) x = — 2, мы придем к равенству 45A=135, откуда

$$A=3. \tag{3.8.3}$$

Полагая, далее, в (3.8.2) x=1, мы получим $6B = 6$, т. е.

$$B = 1. \tag{3.8.4}$$

После этого положим в равенстве (3.8.2) последовательно $x = 0$ и x=—1. Используя (3.8.3) и (3.8.4), мы получим уравнения

$$\begin{cases} -2C + 2E = -2, \\ -4C - 4D + 4E = -8 \end{cases} \tag{3.8.5}$$

Отсюда

$$D = 1. \tag{3.8.6}$$

Положим, наконец, в равенстве (3.8.2) $x = 2$. Используя (3.8.3), (3.8.4) и (3.8.5), мы придем к уравнению

$$20C + 4E = —52,$$

которое вместе с первым из уравнений (3.9.7) дает

$$C = —2,\ E = — 3.$$

Таким образом,

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

9. Сравнения с одним неизвестным

Среди алгебраических уравнений особое место занимают уравнения, в которые входят полиномы с целыми коэффициентами.

С точки зрения теории чисел представляют интерес такие решения этих уравнений, которые являются целыми числами. Ввиду той роли, которую играют в теории чисел сравнения целых чисел по какому-нибудь модулю, полезным и интересным является

рассмотрение соотношений родственного вида, в которых вместо равенства имеет место сравнимость по заданному модулю. Такие соотношения с точки зрения понятия уравнения в широком смысле можно считать некоторым специальным видом уравнений.

Пусть заданы полиномы с целыми коэффициентами

$$f(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} + c_n x^n,$$

$$g(x) = d_0 + d_1 x + d_2 x^2 + \ldots + d_{k-1} x^{k-1} + d_k x^k$$

и натуральное число $m > 1$. *Условие того, что целые числа, являющиеся значениями этих полиномов при некоторых целых числах x, сравнимы по модулю m, называется сравнением с неизвестным x по модулю m и обозначается:*

$$f(x) = g(x) \pmod{m}.$$

Значения неизвестного x, являющиеся целыми числами, при которых значения f(x) и g(x) сравнимы по модулю m, называются решением данного сравнения. Говорят также, что эти значения неизвестного *удовлетворяют данному сравнению.*

При указанной записи сравнения с неизвестным полином $f(x)$ называют его *левой частью, а* $g(x)$ *— правой частью.*

Сравнение с неизвестным, обладающее решениями, называется *разрешимым,* а не обладающее решениями — *неразрешимым.*

Решить сравнение с неизвестным — это значит найти в явном виде все его решения.

Если все числа некоторого класса чисел по модулю m' являются решениями сравнения с неизвестным по модулю m, то такой класс будем называть *классом решений по модулю* m' этого сравнения. Особого внимания заслуживает случай, когда $m' = m$.

Пусть целое число и является решением сравнения

$$f(x) = g(x) \pmod{m},$$

где

$$f(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} + c_n x^n,$$

$$g(x) = d_0 + d_1x + d_2x^2 + \ldots + d_{k-1}x^{k-1} + d_kx^k$$

Тогда и всякое число из класса чисел по модулю m, содержащего u, является решением данного сравнения.

Действительно, если $v \equiv u \pmod m$, то имеем:

$$c_0 + c_1v + c_2v^2 + \ldots + c_{n-1}v^{n-1} + c_nv^n \equiv c_0 + c_1u + c_2u^2 + \ldots + c_{n-1}u^{n-1} + c_nu^n \pmod m$$

$$d_0 + d_1v + d_2v^2 + \ldots + d_{k-1}v^{k-1} + d_kv^k \equiv d_0 + d_1u + d_2u^2 + \ldots + d_{k-1}u^{k-1} + d_ku^k \pmod m$$

и следовательно, $f(v) \equiv g(v) \pmod m$, т. е. v оказывается также решением рассматриваемого сравнения.

Следовательно, для всякого класса чисел по модулю m имеет место одно из двух: или все числа этого класса суть решения данного сравнения с неизвестным по модулю m (и значит, мы имеем класс решений по модулю m данного сравнения), или ни одно из чисел этого класса не является решением данного сравнения. Поэтому *множество решений сравнения с неизвестным по модулю m разбивается на несколько классов решений по модулю m.*

Всякое разрешимое сравнение с неизвестным по модулю m благодаря доказанному выше имеет бесконечное множество решений. Однако количество классов его решений по модулю m конечно и не превосходит m.

Ввиду сказанного для произвольного сравнения с неизвестным по модулю m важной характеристикой является количество классов его решений по модулю m.

Нахождение всех решений сравнения с неизвестным по модулю m, *или* нахождение всех классов решений по модулю m этого сравнения, может быть произведено с использованием какой-нибудь полной системы вычетов по модулю m, т.е. совокупности чисел, взятых по одному из классов чисел по модулю m.

Возьмем какую-нибудь полную систему вычетов по модулю m и в ней выберем все числа, являющиеся решениями данного сравнения с неизвестным по модулю m. Пусть это будут k_1 k_2, …,k_r $(r \le m)$.

Полученная совокупность характеризуется тем, что каждое из ее чисел есть решение данного сравнения, эти числа попарно не сравнимы по модулю m и всякое решение рассматриваемого сравнения сравнимо по модулю m *с* одним из k_i. Такую совокупность естественно было бы назвать приведенной системой решений данного сравнения. При помощи такой совокупности можно удобным и полезным образом задать все решения сравнения.

При всяком $i=1, 2, \ldots, r$ множество целых чисел $x = k_i \pmod m$ является для данного сравнения классом его решений по модулю m. Множество всех решений сравнения есть объединение этих классов. Тем самым данное сравнение имеет в точности r классов решений по модулю m. Поэтому совокупность всех решений данного сравнения может быть записана в виде:

$$x \equiv k_1 \pmod m,\ x \equiv k_2 \pmod m,\ \ldots,\ x \equiv k_r \pmod m,$$

Пример 3.9.1. Для того чтобы решить сравнение

$$x^3 + 2x + 2 = 0 \pmod 5,$$

возьмем полную систему наименьших по абсолютной величине вычетов по модулю 5: 0, 1, —1, 2, —2. Из этих чисел данному сравнению удовлетворяют лишь 1 и —2. Значит, все решения сравнения составляют два класса решений по модулю 5:

$$x \equiv \pmod 5,\ x \equiv -2 \pmod 5.$$

Можно рассматривать и системы нескольких сравненийс одним неизвестным. Решением такой системы называется всякое целое число, являющееся решением каждого сравнения системы. Можно также говорить и о классах решений системы по тому или иному модулю.

Отметим следующее свойство.

Пусть для натуральных чисел m, $m_1 > 1$ *имеет место делимость* m *на* m_1 *:*

$$m = m_1 d.$$

Тогда всякий класс чисел K по модулю m_1 разбивается на d классов чисел по модулю m. При этом для любого $u \in K$ числа

$$u,\ u+m_1,\ u+2m_1,\ldots,\ u+(d-1)m_1$$

являются вычетами указанных классов чисел по модулю m, на которые разбивается K.

Два сравнения с одними тем же неизвестным называются *эквивалентными* или *равносильными,* если всякое решение каждого из них является решением другого. Другими словами, множество решений одного из них совпадает с множеством решений другого.

Из свойств числовых сравнения очевидным образом вытекает справедливость следующих свойств, устанавливающих эквивалентность сравнений с неизвестным.

1) *При любом полиноме h(x) с целыми коэффициентами сравнение*

$$f(x) \equiv g(x) \pmod{m}$$

эквивалентно сравнению

$$f(x) + h(x) \equiv g(x) + h(x) \pmod{m}.$$

2) *При любом натуральном числе k сравнение*

$$f(x) = g(x) \pmod{m}$$

эквивалентно сравнению

$$kf(x) = kg(x) \pmod{km}.$$

3) *При любом целом числе a, взаимно простом с модулем m, сравнение*

$$f(x) \equiv g(x) \pmod{m}$$

эквивалентно сравнению

$$af(x) == ag(x) \pmod{m}.$$

4) *Если в сравнении*

$$c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} + c_n x^n \equiv$$
$$\equiv d_0 + d_1 x + d_2 x^2 + \ldots + d_{k-1} x^{k-1} + d_k x^k \pmod{m}$$

коэффициенты c_i и d_j *заменить сравнимыми с ними по модулю m числами*

$$c_i' \equiv c_l \pmod m, \quad d_j' \equiv d \pmod m$$

(i = 0 1,2, ..., *n;* j =0, 1,2, ..., *k), то полученное сравнение*

$$c_0' + c_1'x + c_2'x^2 + \ldots + c_{n-1}'x^{n-1} + c_n'x^n \equiv$$

$$\equiv d_0' + d_1'x + d_2'x^2 + \ldots + d_{k-1}'x^{k-1} + d_k'x^k \pmod m$$

эквивалентно исходному.

Благодаря свойству 1) всякое сравнение $f(x) = g(x) \pmod m$ может быть заменено эквивалентным ему сравнением

$$f(x) - g(x) = 0 \pmod m.$$

Пример 3.9.2. Решим сравнение

$$117x^4 + 72x^2 + 51 \equiv 0 \pmod{24}.$$

Заменяем коэффициенты их остатками при делении с остатком на 24:

$$21x^4 + 3 \equiv 0 \pmod{24}.$$

Делим коэффициенты и модуль на 3:

$$7x^4 + 1 = 0 \pmod 8,$$

или

$$7x^4 - 7 \equiv 0 \pmod 8.$$

Коэффициенты делим на число 7, взаимно простое с модулем 8:

$$x^4 - 1 \equiv 0 \pmod 8.$$

Полученное сравнение эквивалентно исходному. Решаем его. Из полной системы наименьших по абсолютной величине вычетов по модулю 8 решениями полученного сравнения являются лишь 1, —1, 3, —3. Поэтому полученное сравнение, а значит, и исходное имеют четыре класса решений по модулю 8:

$x \equiv 1 \pmod 8$, $x \equiv -1 \pmod 8$, $x \equiv 3 \pmod 8$, $x \equiv -3 \pmod 8$.

Каждый из этих классов можно разбить на три класса чисел по модулю 24.

Класс чисел $x \equiv 1 (\text{mod } 8)$ разбивается на классы чисел по модулю 24, вычетами которых являются числа 1, 1 + 8=9, 1 + 2 • 8 = 17:

$$x \equiv= 1 \ (\text{mod } 24), \quad x \equiv 9 \ (\text{mod } 24), \quad x \equiv 17 \ (\text{mod } 24).$$

Рассуждая аналогично для других классов, получаем:

$$x \equiv —1 \ (\text{mod } 24), \ x \equiv 7 \ (\text{mod } 24), \ x \equiv 15 \ (\text{mod } 24),$$

$$x \equiv 3 \ (\text{mod } 24), \ x \equiv 11 \ (\text{mod } 24), \ \text{x} \equiv 19 \ (\text{mod } 24),$$

$$x \equiv — 3 \ (\text{mod } 24), \ x \equiv 5 \ (\text{mod } 24), \ x \equiv 13 \ (\text{mod } 24).$$

Таким образом, исходное сравнение имеет двенадцать классов решений по модулю 24.

Если в сравнении

$$c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n \equiv 0 \ (\text{mod } m)$$

какой-нибудь коэффициент c_i делится на m, то согласно свойству 4) он может быть заменен нулем и, значит, соответствующее слагаемое может быть опущено. Если коэффициент c_n при наибольшей степени x не делится на m, то n называется *степенью сравнения.* Сравнение нулевой степени, очевидно, не имеет решений.

Рассмотрим сравнения с неизвестным первой степени. Очевидно, их всегда можно представить в виде

$$ax \equiv b \ (\text{mod } m),$$

где $a \neq 0 \ (\text{mod } m)$.

Теорема 3.9.1. *Сравнение с неизвестным первой степени* $ax \equiv b (\text{mod } m)$ *разрешимо тогда и только тогда, когда* b *делится на наименьший общий делитель* $d = (a, m)$. *В этом случае количество классов его решений по модулю* m *равно* d.

Доказательство. Разрешимость данного сравнения, очевидно, означает разрешимость в целых числах уравнения

$$ax — my = b.$$

При этом целое число u будет решением сравнения тогда и только тогда, когда найдется целое число u, такое, что пара u, v оказывается решением полученного уравнения.

Разрешимость исходного сравнения означает делимость числа b на d.

Пусть u — какое-нибудь целое число, удовлетворяющее нашему сравнению. Тогда все целые числа, удовлетворяющие сравнению, — это числа

$$x = u + \frac{m}{d}t \qquad (t \in N).$$

Они составляют один класс чисел по модулю $\frac{m}{d}$:

$$x \equiv u \left(\bmod \frac{m}{d} \right).$$

Этот класс чисел разбивается на d классов чисел по модулю m, вычетами которых являются числа:

$$u, u + \frac{m}{d}, u + 2\frac{m}{d}, ..., u + (d-1)\frac{m}{d}.$$

В связи с теоремой 3.9.1 отметим, что сравнение с неизвестным первой степени

$$ax \equiv b \pmod{m}$$

в случае, когда оно разрешимо (т. е. $b \vdots d = (a, m)$), эквивалентно, благодаря свойству (2), сравнению

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\bmod \frac{m}{d} \right).$$

Здесь числа $\frac{a}{d}$ и $\frac{m}{d}$ взаимно просты. Последнее сравнение имеет один класс решений по модулю $\frac{m}{d}$. Он разбивается на d классов решений по модулю m.

Для нахождения всех решений сравнения нам достаточно найти какое-нибудь одно его решение u, поскольку благодаря сказанному выше все решения данного сравнения составляют один класс чисел

$$x \equiv u\left(\bmod \frac{m}{d}\right).$$

Этот класс ввиду теоремы 3.9.1 разбивается на d классов решений по модулю m исходного сравнения, вычетами которых служат числа:

$$u_0 = u, u_1 = u + \frac{m}{d}, u_2 = u + 2\frac{m}{d}, ..., u_{d-1} = u + (d-1)\frac{m}{d}.$$

Поэтому все решения исходного сравнения могут быть также записаны с помощью классов решений по модулю m в виде:

$x \equiv u_0 \pmod m$, $x \equiv u_1 \pmod m$, $x \equiv u_2 \pmod m$, ..., $x \equiv u_{d-1} \pmod m$.

Нахождение какого-нибудь одного решения сравнения с неизвестным первой степени

$$ax \equiv b \pmod m$$

очевидным образом можно свести к нахождению какого-нибудь целочисленного решения уравнения

$$ax - my = b.$$

Укажем непосредственную формулу для нахождения одного из решений рассматриваемого сравнения. Данное сравнение эквивалентно сравнению

$$a_1 \equiv b_1 \pmod{m_1},$$

где

$$a_1 = \frac{a}{d},\ b_1 = \frac{b}{d},\ m_1 = \frac{m}{d}, d = (a, m)$$

Благодаря взаимной простоте чисел a_1 и m_1 мы на основании свойства функции Эйлера имеем $a_1^{\varphi(m_1)} \equiv 1 \pmod{m_1}$. Отсюда вытекает, что число

$$u = a_1^{\varphi(m_1)-1} \cdot b_1 \qquad (3.9.1)$$

является решением рассматриваемого сравнения:

$$a_1 \cdot u = a_1^{\varphi(m_1)} \cdot b_1 \equiv b_1 (\text{mod } m_1).$$

Пример 3.9.3 Сравнение $6x \equiv 10 \pmod{45}$ неразрешимо, поскольку 10 не делится на (6,45) = 3.

Пример 3.9.4 Сравнение $6x \equiv 15 \pmod{45}$ разрешимо, поскольку 15 делится на (6,45) = 3. Оно имеет три класса решений по модулю 45. Данное сравнение эквивалентно сравнению $2x \equiv 5 \pmod{15}$, которое имеет один класс решений по модулю 15. По формуле (3.9.1), находим одно из решений заданного сравнения:

$$u = 2^{\varphi(15)-1} \cdot 5 = 2^7 \cdot 5 = 640$$

Имеем: $640 = 10 \pmod{15}$.

Все решения нашего сравнения составляют один класс чисел

$$x = 10 \pmod{15}.$$

Он разбивается на три класса решений по модулю 45:

$$x \equiv 10 \pmod{45},\ x \equiv 25 \pmod{45},\ x \equiv 40 \pmod{45}.$$

Задачи к части 3

3.1 Выполнить деление с остатком

1) $2x^4 - 3x^3 + 4x^2 - 5x + 6$ на $x^2 - 3x + 1$,

2) $x^3 - 3x^2 - x - 1$ на $3x^2 - 2x + 1$,

3) $x^4 - 2x^3 + 4x^2 - 6x + 8$ на $x - 1$,

4) $2x^5 - 5x^3 - 8x$ на $x + 3$,

5) $4x^3 + x^2$ на $x + 1 + i$,

6) $x^3 - x^2 - x$ на $x - 1 + 2i$.

3.2 Найти наибольший общий делитель многочленов

1) $x^4 + x^3 - 3x^2 - 4x - 1$ и $x^3 + x^2 - x - 1$,

2) $x^6 + 2x^4 - 4x^3 - 3x^2 + 8x - 5$ и $x^5 + x^2 - x + 1$,

3) $x^5 + 3x^2 - 2x + 2$ и $x^6 + x^5 + x^4 - 3x^2 + 2x - 6$,

4) $x^4 + x^3 - 4x + 5$ и $2x^3 - x^2 - 2x + 2$,

5) $x^5+x^4-x^3-2x-1$ и $3x^4+2x^3+x^2+2x-2$,

6) $x^6-7x^4+8x^3-7x+7$ и $3x^5-7x^3+3x^2-7$,

7) $x^5-2x^4+x^3+7x^2-12x+10$ и $3x^4-64x^3+5x^2+2x-2$,

8) $x^5+3x^4-12x^3-52x^2-52x-12$ и $x^4+3x^3-6x^2-22x-12$,

9) $x^5+x^4-x^3-3x^2-3x-1$ и $x^4-2x^3-x^2-2x+1$,

10) x^4-4x^3+1 и x^3-3x^2+1,

11) $x^6+2x^4-4x^3-3x^2+8x-5$ и x^5+x^2-x+1,

12) $2x^6-5x^5-14x^4+36x^3+86x^2+12x-31$ и $2x^5-9x^4+2x^3+37x^2+10x-14$,

13) $3x^6-x^5-9x^4-14x^3-11x^2-3x-1$ и $3x^5+8x^4+9x^3+15x^2+10x+9$.

3.3 Пользуясь алгоритмом Евклида, подобрать такие многочлены *u(x), v(x),* что $f(x)u(x)+g(x)v(x)=1$

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

2) $f(x)=x^4-x^3-4x^2+4x+1,\quad g(x)=x^2-x-1$,

3) $f(x)=x^5-5x^4-2x^3+12x^2-2x+12,\quad g(x)=x^3-5x^2-3x+17$,

4) $f(x)=2x^4+3x^3-3x^2-5x+2,\quad g(x)=2x^3+x^2-x-1$,

5) $f(x)=3x^4-5x^3+4x^2-2x+1,\quad g(x)=3x^3-2x^2+x-1$,

6) $f(x)=x^5+5x^4+9x^3+7x^2+5x+3,\quad g(x)=x^4+2x^3+2x^2+x+1$.

3.4 Методом неопределенных коэффициентов подобрать такие многочлены *u(x), v(x),* что $f(x)u(x)+g(x)v(x)=1$

1) $f(x)=x^4-4x^3+1,\quad g(x)=x^3-3x^2+1$,

2) $f(x)=x^3,\quad g(x)=(1-x)^2$,

3) $f(x)=x^4,\quad g(x)=(1-x)^4$.

3.5 Разделить многочлен $f(x)$ с остатком на $x-x_0$ и вычислить значение $f(x_0)$

1) $f(x)=x^4-2x^3+4x^2-6x+8,\quad x_0=1$,

2) $f(x)=2x^5-5x^3-8x,\quad x_0=-3,$

3) $f(x)=3x^5+x^4-19x^2-13x-10,\quad x_0=2,$

4) $f(x)=x^4-3x^3-10x^2+2x+5,\quad x_0=-2,$

5) $f(x)=x^5,\quad x_0=1,$

6) $f(x)=x^4+2x^3-3x^2-4x+1,\quad x_0=-1,$

7) $f(x)=x^4-8x^3+24x^2-50x+90,\quad x_0=2,$

8) $f(x)=x^4+2ix^3-(1+i)x^2-3x+7+i,\quad x_0=-i,$

9) $f(x)=x^4+(3-8i)x^3-(21+18i)x^2-(33-20i)x+7+18i,\quad x_0=-1+2i$

3.6 Пользуясь схемой Горнера, вычислить $f(x_0)$

1) $f(x)=x^4-3x^3+6x^2-10x+16,\quad x_0=4,$

2) $f(x)=x^5+(1+2i)x^4-(1+3i)x^2+7,\quad x_0=-2-i.$

3.7 Найти значения полинома $f(x)$ и его производных при $x=x_0$

1) $f(x)=x^5-4x^3+6x^2-8x+10,\quad x_0=2,$

2) $f(x)=x^4-3ix^3-4x^2+5ix-1,\quad x_0=1+2i.$

3.8 Чему равен показатель кратности корня

1) 2 для полинома $x^5-5x^4+7x^3-2x^2+4x-8,$

2) -2 для полинома $x^5+7x^4+16x^3+8x^2-16x-16,$

3) -1 для полинома $3x^5+2x^4+x^3-10x-8,$

4) 3 для полинома $x^5-6x^4+2x^3+36x^2-27x-54.$

3.9 Разложить многочлен $f(x)$ по степеням $x-x_0$ и найти значения его производных в точке x_0

1) $f(x)=x^5-4x^3+6x^2-8x+10,\quad x_0=2,$

2) $f(x)=x_4-3ix^3-4x^2+5ix-1,\quad x_0=1+2i,$

3) $f(x)=x^4+4x^3+6x^2+10x+20,\quad x_0=-2.$

3.10 Разложить на линейные множители над полем комплексных чисел многочлены

1) $x^3 - 6x^2 + 11x - 6$,

2) $x^4 + 4$,

3) $x^6 + 27$,

4) $x^4 + 4x^3 + 4x^2 + 1$,

5) $x^4 - 10x^2 + 1$.

3.11 Построить полиномы наименьшей степени с комплексными коэффициентами по данным корням

1) двойной корень 1, простые 2, 3 и $1+i$;

2) тройной корень -1, простые 3 и 4;

3) двойной корень i, простой $-1-i$.

3.12 Разложить на неприводимые множители над полем вещественных чисел многочлены

1) $x^6 + 27$,

2) $x^4 + 4x^3 + 4x^2 + 1$,

3) $x^4 - ax^2 + 1, |a| < 2$,

4) $x^{2n} + x^n + 1$,

5) $x^6 - x^3 + 1$,

6) $x^{12} + x^8 + x^4 + 1$.

3.13 Найти все рациональные корни многочленов

1) $x^3 - 6x^2 + 15x - 14$,

2) $x^4 - 2x^3 - 8x^2 + 13x - 24$,

3) $6x^4 + 19x^3 - 7x^2 - 26x + 12$,

4) $24x^4 - 42x^3 - 77x^2 + 56x + 60$,

5) $24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6$,

6) $10x^4 - 13x^3 + 15x^2 - 18x - 24$,

7) $4x^4 - 7x^2 - 5x - 1$,

8) $2x^3 + 3x^2 + 6x - 4$,

9) $x^4 + 2x^3 - 13x^2 - 38x - 24$,

10) $x^4+4x^3-2x^2-12x+9$.

3.14 Пользуясь признаком Эйзенштейна, доказать неприводимость над полем рациональных чисел многочленов

1) $x^4-8x^3+12x^2-6x+2$,

2) $x^5-12x^3+36x-12$,

3) x^4-x^3+2x+1.

3.15 Представить рациональную дробь в виде суммы простейших дробей над полем комплексных чисел

1) $\dfrac{x^2}{(x-1)(x+2)(x+3)}$, 2) $\dfrac{1}{x^4+4}$, 3) $\dfrac{x}{\left(x^2-1\right)^2}$, 4) $\dfrac{5x^2+6x-23}{(x-1)^3(x+1)^2(x-2)}$,

5) $\dfrac{x+3}{(x-1)\left(x^2+1\right)}$, 6) $\dfrac{x^2}{x^4-1}$, 7) $\dfrac{1}{x^3-1}$, 8) $\dfrac{1}{\left(x^2-1\right)^2}$.

3.16 Разложить на простейшие дроби над полем вещественных чисел

1) $\dfrac{x}{(x+1)^2(x^2+1)^2}$, 2) $\dfrac{2x-1}{x(x+1)^2(x^2+x+1)^2}$, 3) $\dfrac{1}{(x^4-1)^2}$.

3.17 Решить сравнения

1) $x^2\equiv -1(\mathrm{mod}\,13)$, 2) $x^2\equiv -1(\mathrm{mod}\,11)$, 3) $x^2\equiv 2(\mathrm{mod}\,31)$,

4) $x^2+2x+14\equiv 0(\mathrm{mod}\,17)$, 5) $x^2+3x+10\equiv 0(\mathrm{mod}\,19)$,

6) $9x^2+29x+62\equiv 0(\mathrm{mod}\,64)$, 7) $x^3-3x+1\equiv 0(\mathrm{mod}\,19)$,

8) $x^3\equiv 5(\mathrm{mod}\,11)$, 9) $x^3\equiv 10(\mathrm{mod}\,37)$, 10) $x^3+2x+2\equiv 0(\mathrm{mod}\,125)$,

11) $x^4+4x^3+2x^2+2x+12\equiv 0(\mathrm{mod}\,625)$,

12) $6x^3+27x^2+17x+20\equiv 0(\mathrm{mod}\,30)$,

13) $31x^4+57x^3+96x+191\equiv 0(\mathrm{mod}\,225)$

Литература

1 Курош А.Г. Курс высшей алгебры. Москва, Наука, 1968.

2 Ляпин Е.С., Евсеев А.Е. Алгебра и теория чисел. Т 1, 2. Москва, Просвещение, 1978.

3 Окунев Л.Я. Высшая алгебра. Москва, Просвещение, 1966.

4 Мишина А.П., Проскуряков И.В. Высшая алгебра. Линейная алгебра, многочлены, общая алгебра. Москва, Наука, 1965.

5 Виноградов И.М. Основы теории чисел. Москва, Наука, 1972.

6 Кострикин А.И. Введение в алгебру. Т. 1, 2. Москва, Физматлит, 2001.

7 Сборник задач по алгебре под ред. Кострикина А.И. Москва, Физматлит, 2001.

8 Фаддеев Д.К., Соминский И.С. Сборник задач по высшей алгебре. Москва, Наука, 1977.