помощью такой возможности, как произвольное расширение возможностей учебных моделей и конструктивной среды, эта программа может использоваться также на уроках информатики, в том числе, при обучении компьютерному моделированию.

Данная программа поможет так же для создания факультативного курса по математике. Внеурочная деятельность по «МК» в курсе математики для обучающихся предназначена на изменение традиционного подхода к преподаванию математики в средней школе в рамках внедрения информационных и коммуникационных технологий, в которых большое значение придается развитию у учащихся способности максимально использовать современные компьютерные технологии. преимущества для личного интеллектуального развития.

Исходя из вышеизложенного, можно сделать вывод, что «МК» является незаменимой программой для составления факультативного курса по геометрии в средней школе.

Список литературы :

Математический конструктор [Электронный ресурс]. – Режим доступа: http://obr.1c.ru/educational/Uchenikam/mathkit/ свободный доступ;

Электронные ресурсы: https://studbooks.net/2036541/pedagogika/interaktivnaya_tvorcheskaya_sreda_matematicheskiy_konstruktor свободный доступ;

Электронные ресурсы: https://mat.1sept.ru/view_article.php?id=200901306 свободный доступ;

Далингер В.А. Интерактивная динамичная геометрия с «математическим конструктором» // Международный журнал экспериментального образования. – 2016. – № 8. – С. 90-90;

Дубровский В.Н., Лебедева Н.А., Белайчук О.А. 1С:Математический конструктор - новая программа динамической геометрии // Компьютерные инструменты в образовании. - СПб.: Изд-во ЦПО"Информатизация образования", 2007. №3. - С. 47-56.

UDC 512.62

THE POLYNOMIALS AND THEIR CONGRUENCE

Author: Fazyl Z. G., KOSTANAY STATE PEDAGOGICAL UNIVERSITY named after U. Sultangazin
Scientific adviser: Alimbaev A.A., KOSTANAY STATE PEDAGOGICAL UNIVERSITY named after U. Sultangazin
Kostanay, Kazakhstan

Аннотация: Полиномы играют важную роль в математике, в программировании, в прикладной физике и во многих науках. Это не было полностью изучено как ветвь алгебры, и есть много вопросов относительно этого раздела. В этой научной статье я попытался объяснить простыми словами понятие «полином» и какими свойствами он обладает, а также какие действия и операции мы можем выполнять с ними.

Ключевые слова: кольцо полиномов, конгруэнция, сложение полиномов, умножение полиномов, по модулю.

Annotation**:** Polynomials play an important role in mathematics, in programming, in applied physics, and in many sciences. It has not been fully studied as a branch of algebra,

and there are many questions regarding this section. In this scientific article I tried to explain in simple words the concept of a “polynomial” and what properties it possesses, as well as what actions and operations we can perform with them.

Keywords**:** the polynomials ring, congruence, polynomial addition, polynomial multiplication, modulo.

Аннотация: Полиномдар математикада, физикада, компьютерлық ғылымдарда және көптеген ғылымдарда маңызды рөл атқарады. Ол алгебраның бір саласы ретінде толық зерттелмеген, осы бөлімге қатысты көптеген сұрақтар туындауы мүмкін. Осы ғылыми мақалада мен «полином» ұғымын және оның қандай қасиеттерге ие екендігін, сондай-ақ олармен қандай әрекеттер мен операцияларды жүргізуге болатындығын қарапайым сөздермен түсіндіруге тырыстым.

Түйін сөздер: көпмүшелер сақинасы, конгруэнция, көпмүшелерді(полиномдарды) қосу, көпмүшелерді(полиномдарды), модуль.

Introduction

Before starting, I want to say that this article is written for readers who already have basic knowledge of algebra, who already know such concepts as field, rings, integral domain, etc.

Where does algebra start? With some approximation, we can say that the origins of algebra lie in the art of adding, multiplying and raising to the power integers. A formal, but far from obvious and ambiguous substitution of numbers by letters allows one to act according to similar rules within much more general algebraic systems. Consequently, an attempt to answer in an exhaustive manner the question posed would lead us away only centuries ago, into the secrets of the origin of mathematical thought. The more difficult part of the answer would be related to the description of the basic structures of the algebra of our days: groups, rings, modules, etc. In this case, it is with the theory of polynomials rings. Many questions arise regarding the ring of polynomials, which we will consider.

The polynomials ring

What is a polynomial? What properties does it possess? What does the word "polynomial" mean? The main task of classical algebra was to solve equations. By an equation, we mean what happens when a certain expression - in which known and unknown quantities can be present, as well as their sum, difference and product - is 0. When solving the equation, various transformations of this expression were made. That is why, even before solving the equation, it is advisable to see what transformations and actions can be performed with this expression. To begin with, we will consider only those expressions in which there is only one unknown. Since the discussion so far will not be about equations, the unknown should not be considered as a number, but only as an indefinite quantity, over which it is possible to perform actions in the same way as over numbers. If in one expression there is only one unknown, then the expression can be written as the sum of the degrees of the unknown multiplied by some coefficients. To solve the equation, it is also important to know which numbers are present in the equation, and what number is the solution of the equation itself, that is, are they, for example, rational, real or complex numbers. Based on these considerations, we give the following definition:

Definition. Let R be any ring. A *polynomial with coefficients* in R is an expression of the form $a_0 + a_1x + a_2x^2 + ... + a_nx^n$, where n is a nonnegative integer and $a_i \in R$.

The main idea here is to define a *“polynomial”* in a way that is an obvious extension polynomials with real number coefficients.

But even this definition is not enough, because there are many questions. What is x? What properties does it have? Is x an element of R? What does it mean to multiply x by a

ring element? To find out the answers to these questions, note that an expression of the form $a_0 + a_1x + a_2x^2 + ... + a_nx^n$ makes sense, provided that the a_i and x are all elements of some larger ring. I will give you an example. The number π is not an integer, but an expression such as $5 + 2\pi - 3\pi^2 - 12\pi^3$ and $3\pi^2 - 4\pi^3$ make sense in the real numbers. So we shall think of polynomials with coefficients in a ring R in much the same way, as elements of a larger ring that contains both R and a special element x that is not in R. The following theorem closes all questions regarding the definition of a *polynomial*.

Theorem 2.1.

If R is a ring, then there exists a ring T containing an element x that is not in R and has these properties:

1)R is a subring of T.

2) $x \cdot a = a \cdot x$ for every $a \in R$.

3) The set $R[x]$ of elements of T of the form

$a_0 + a_1x + a_2x^2 + ... + a_nx^n$ (where $n \geq 0$ and $ai \in R$) is a subring of T that contains R.

4)The representation of elements $R[x]$ is unique: if $n \leq m$ and $a_0 + a_1x + a_2x^2 + ... + a_nx^n = b_0 + b_1x + b_2x^2 + ... + b_mx^m$, then $a_i = b_i$ for $i = 1, 2, ..., n$ and $b_i = 0$ for each $i > n$.

5)$a_0 + a_1x + a_2x^2 + ... + a_nx^n = 0$ if and only if $a_i = 0$ for every i.

The elements of the ring $R[x]$ in this theorem are called *polynomials with coefficients* in R and the elements a_i are called *coefficients*. The special element x is sometimes called an *indeterminate.*

*Example 1***.** Let D be the ring of odd integers. Then $3 - x + 5x^3 \in D[x]$. However the polynomial x is not in $D[x]$, because it cannot be written with odd coefficients.

The rules for addition and multiplication of polynomials directly follow from the fact that $R[x]$ is a ring.

Example 2. Let $f(x) = 2 + 3x + 4x^2 - 6x^3$ and $g(x) = 1 + 5x + 2x^2 + 7x^3$, then the associative, commutative and distributive laws show that

$f(x) + g(x) = (2 + 3x + 4x^2 - 6x^3) + (1 + 5x + 2x^2 + 7x^3) = (2 + 1) + (3x + 5x) + (4x^2 + 2x^2) + (-6x^3 + 7x^3) = (2 + 1) + (3 + 5)x + (4 + 2) \cdot x^2 + (-6 + 7) \cdot x^3 = 3 + 8x + 6x^2 + 1x^3$

The product of polynomials follows from the distributive law:

$$(2 + x^2)(x + x^3) = 2 \cdot (x + x^3) + x^2 \cdot (x + x^3)$$
$$= 2 \cdot (x) + 2 \cdot (x^3) + x^2 \cdot (x) + x^2 \cdot (x^3) = 2x + 2x^3 + x^3 + x^5$$
$$= 2x + 3x^3 + x^5$$

The *polynomial addition* is given by the rule:

$$(a_0 + a_1x + a_2x^2 + ... + a_nx^n) + (b_0 + b_1x + b_2x^2 + ... + b_nx^n)$$
$$= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ...+ (a_n + b_n)x^n$$

and *polynomial multiplication* is given by the rule:

$(a_0 + a_1x + a_2x^2 + ... + a_nx^n)(b_0 + b_1x + b_2x^2 + ... + b_nx^n) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + a_nb_mx^{n+m}$.

For each $k \geq 0$, the coefficient of x^k the product is

$a_0b_k + a_1b_{k-1} + a_2b_{k-2} + ... + a_{k-2}b_2 + a_{k-1}b_1 + a_kb_0 = \sum_{i=0}^{k} a_i\, b_{k-i}$, where $a_i = 0$ if $i > n$ and $b_j = 0$ if $j > m$. It follows readily from this description of multiplication in $R[x]$ that if R is commutative, then so is $R[x]$. Furthermore, if R has a multiplicative identity *1*, then 1 is also the multiplicative identity of $R[x]$.

Definition**.** Let $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ be a polynomial in $R[x]$ with an $a_n \neq 0$.Then a_n is called the *leading coefficient* of $f(x)$. The degree of $f(x)$ is the

integer n; it is denoted "deg $f(x)$". In other words, deg $f(x)$ is the largest exponent of x that appears with a nonzero coefficient, and this coefficient is the leading coefficient. The ring R that we start with is a subring of the polynomial ring $R[x]$. The elements of R, considered as polynomials in $R[x]$, are called constant polynomials. The polynomials of degree 0 in $R[x]$ are precisely the nonzero constant polynomials. Note that

the constant polynomial 0 does not have a degree (because no power of *x* appears with nonzero coefficient).

Theorem 2.2.

If R is an *integral domain* and $f(x)$, $g(x)$ are nonzero polynomials in $R[x]$, then deg$[f(x) \cdot g(x)]$ = deg $f(x)$ + deg $g(x)$.

Corollary 2.3.

Let R be a ring. If $f(x)$, $g(x)$, and $f(x) \cdot g(x)$ are nonzero in $R[x]$, then deg $[f(x) \cdot g(x)] \leq$ deg $f(x)$ + deg $g(x)$.

Example 3. Let $f(x) = 3x^3$ and $g(x) = 5x^2$ in $Z_9[x]$. Then $f(x) \cdot g(x) = (3x^3) \cdot (5x^2) = 6x^5$. However, if $g(x) = 1 + 3x^4$, then $f(x) \cdot g(x) = (3x^3) \cdot (1 + 3x^4) = 3x^3 + 0x^7 = 3x^3$.

You have familiarized yourself with the basic concepts regarding the topic of polynomial rings, except for one. Division of polynomials. As in the field of integers, division in a system of polynomials is not feasible at all. For integers, division to some extent managed to replace division with the remainder. Division with remainder can also be determined for polynomials. When dividing integers, the remainder always turned out to be less than the divisor. However, in the system of polynomials it cannot be said that one polynomial is smaller than the other. Here, this function is performed by degrees of polynomials. It is easy to show that in a system of polynomials one can perform division with a remainder in such a way that the degree of the remainder is less than the divisor.

Let $f(x)$ – an arbitrary polynomial and $g(x)$ – a nonzero polynomial, then there are exist the polynomials $q(x)$ and $r(x)$, that $f(x) = q(x) \cdot g(x) + r(x)$, where deg $r(x) <$ deg $g(x)$ or $r(x) = 0$.

Example 4.

$x^3 + 2x^2 + 3x - 6 = (x - 1)(x^2 + 3x - 4) + (10x - 10)$ or $x^2 + 5x - 6 = (x - 1)(x + 6)$.

In the second expression $r(x) = 0$.

And now, knowing all the basic definitions and terms, we can proceed to the next chapter, called "Congruence of polynomials".

The congruence of polynomials

The concept of congruence of integers depends only on some basic facts about divisibility in Z. If F is a field, then the ring of polynomials $F[x]$ has the same properties as Z. The properties can be almost literally transferred to $F[x]$. Based on these considerations, we have given you the following definition.

Let F be a field and $f(x), g(x), p(x) \in F[x]$ with $p(x)$ nonzero. *Then $f(x)$ is congruent to $g(x)$ modulo $p(x)$* - written $f(x) \equiv g(x) \pmod{p(x)}$ - provided that $p(x)$ divides $f(x) - g(x)$.

Example 5. In $Q[x]$, $x^2 + 2x + 3 \equiv x + 4 \pmod{x + 1}$ because $(x^2 + 2x + 3) - (2x + 4) = x^2 - 1 = (x - 1)(x + 1)$

Theorem 3.1.

Let F be a field and $p(x)$ a nonzero polynomial in $F[x]$. Then the relation of congruence modulo $p(x)$ is

(1) *reflexive*: $f(x) \equiv f(x) \pmod{p(x)}$ for all *f*(*x*) ∈ *F*[*x*];

(2) *symmetric*: if $f(x) \equiv g(x) \pmod{p(x)}$, then $g(x) \equiv f(x) \pmod{p(x)}$;
(3) *transitive*: if $f(x) \equiv g(x) \pmod{p(x)}$ and $g(x) \equiv h(x) \pmod{p(x)}$, then $f(x) \equiv h(x) \pmod{p(x)}$.

Theorem 3.2.

Let F be a field and $p(x)$ a nonzero polynomial in $F[x]$. If $f(x) \equiv g(x) \pmod{p(x)}$ and $h(x) \equiv k(x) \pmod{p(x)}$, then

(1) $f(x) + h(x) \equiv g(x) + k(x) \pmod{p(x)}$,
(2) $f(x) \cdot h(x) \equiv g(x) \cdot k(x) \pmod{p(x)}$.

Definition. Let F be a field and $f(x)$, $p(x) \in F[x]$ with $p(x)$ nonzero. The congruence class (or residue class) of $f(x)$ modulo $p(x)$ is denoted $[f(x)]$ and consists of all polynomials in $F[x]$ that are congruent to $f(x)$ modulo $p(x)$, that is,

$$[f(x)] = \{g(x) \mid g(x) \in F[x] \text{ and } g(x) \equiv f(x) \pmod{p(x)}\}.$$

Since $g(x) = f(x) \pmod{p(x)}$ means that $g(x) - f(x) = k(x) \cdot p(x)$ for some $k(x) \in F[x]$ or, equivalently, that $g(x) = f(x) + k(x) \cdot p(x)$, we see that

$$[f(x)] = \{g(x) \mid g(x) \equiv f(x) \pmod{p(x)}\} = \{f(x) + k(x) \cdot p(x) \mid (x) \in F[x]\}.$$

Example 6.

Consider a comparison modulo $5x^2 + 2$ in $R[x]$. The congruence class $3x + 4$ is the set $\{(3x + 4) + k(x) \cdot (5x^2 + 2) \mid k(x) \in R[x]\}$.

The division algorithm shows that the elements of this set are polynomials from $R[x]$, which leave the remainder $3x + 4$ when divided by $5x^2 + 2$.

Example 7.

Consider congruence modulo $x^2 + x + 2$ in $Z_3[x]$. The possible remainders on division by $x^2 + x + 2$ are the polynomials of the form $ax + b$ with $a, b \in Z_3$. Thus there are only nine possible remainders: 0, 1, 2, x, $x+1$, $x+2$, $2x$, $2x+1$ and $2x+2$. Therefore, $Z_3[x]/(x^2 + x + 2)$ consists of nine congruence classes: $[0]$, $[1]$, $[2]$, $[x]$, $[x+1]$, $[x+2]$, $[2x]$, $[2x+1]$ and $[2x+2]$.

Statement 3.1.

If $p(x)$ is a nonzero constant polynomial in $F[x]$, then any two polynomials in $F[x]$ are congruent modulo $p(x)$.

Proof:

Let $p(x) = c$ for some nonzero $c \in F$. For any $f(x) \in F[x]$ we have $f(x) \vdots c$ (since $f(x) = c(c^{-1}f(x))$). Also for any $g(x) \in F[x]$ we have $g(x) \vdots c$ (since $g(x) = c(c^{-1}g(x))$) Therefore $f(x) \equiv g(x) \pmod{p(x)}$, because

$$f(x) - g(x) = c(c^{-1}f(x)) - c(c^{-1}g(x)) = c(c^{-1}f(x) - c^{-1}g(x)) \vdots c$$

Exercise 3.1.

How many distinct congruence classes are there modulo $x^3 + x + 1$ in $Z_2[x]$? List them.

Solution:

There are 15 polynomials less or equal $x^3 + x + 1$ in $Z_2[x]$:

$1, x, x^2, x^3, x+1, x^2+x, x^3+x, x^2+1, x^3+1, x^3+x^2, x^3+x^2+x, x^3+x^2+1, x^3+x+1, x^2+x+1$ and x^3+x^2+x+1.

It is easy to find the reminder by the division algorithm.

$x^3 + x + 1 = (x^3 + x + 1) \cdot 1 + 0$ $\quad x^3 + x + 1 = 1 \cdot (x^3 + x) + 1$

$x^3 + x + 1 = (x^2) \cdot (x) + (x + 1)$ $\quad x^3 + x + 1 = 1(x^3 + x^2 + x) + (x^2 + 1)$

$x^3 + x + 1 = (x) \cdot (x^2) + (x + 1)$ $\quad x^3 + x + 1 = 1 \cdot (x^3 + 1) + x$

$x^3 + x + 1 = 1 \cdot (x^3) + (x + 1)$ $\quad x^3 + x + 1 = 1(x^3 + x^2) + (x^2 + x + 1)$

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

There are 8 classes. $[0]$, $[1]$, $[x]$, $[x + 1]$, $[x^2]$, $[x^2 + 1]$, $[x^2 + x]$, $[x^2 + x + 1]$.

Statement 3.2.

There are infinitely many distinct congruence classes modulo $x^2 - 2$ in $Q[x]$. Describe them.

Proof.

The classes are uniquely represented by the elements $ax + b$ for $a, b \in Q$. There are an infinite number of different choices.

Exercise 3.2.

Describe the congruence classes in $F[x]$ modulo the polynomial x.

Solution.

$f(x) \equiv g(x) \pmod{x}$ if and only if $f(x) - g(x)$ is divisible by x. This happens if and only if $f(x) - g(x)$ has a zero constant term. So $f(x) \equiv g(x) \pmod{x}$ whenever the constant terms in f and g are the same, so that there is one congruence class for each possible constant.

Conclusion

Polynomials make up the old and well-studied section of traditional algebra. It plays a large role not only in mathematics itself, but in the information sciences, in physics, in engineering, etc. It would seem that polynomial rings have been fully studied, but actually not. There are many unresolved issues. And the deeper we dig, the more questions we get. Many questions arise when it comes to polynomials from two or more unknowns, whether it preserves its structure as a single variable, whether the laws of arithmetic are respected, and how they are divided into classes. And I set myself the goal of learning polynomials from several unknowns.

List of used literature

Abstract Algebra: An Introduction, Third Edition Thomas H. Huneerford. Brooks/Cole 20 Channel Center Street Boston, MA 02210 USA, 2014

Л. Я. Куликов, Алгебра и теория чисел/ Москва «Высшая школа», 1979 – 559 с.

А. И. Кострикин, Введение в алгебру/ Издательство «Наука», 1977 – 496 с.

Э. Фрид, И. Пастор, П. Ревес, И. Рейман, И. Ружа, Малая математическая энциклопедия/ Издательство академии наук Венгрии, Будапешт 1976 – 693 с.

МАТЕМАТИЧЕСКОЕ НАСЛЕДИЕ АЛЬ-ФАРАБИ

Фишер М.Д.
Костанайский Государственный Педагогический Университет
им.У.Султангазина, г.Костанай

Научный руководитель: Телегина О.С.
Костанайский Государственный Педагогический Университет
им.У.Султангазина, г.Костанай