ЛЕКЦИЯ №1

Тема: Кольцо многочленов от одного неизвестного. Свойства делимости многочленов

Понятие многочлена, или целой рациональной функции, от неизвестного *x* возникло в связи с задачей решения алгебраических равнений различных степеней еще в глубокой древности. В древнем Вавилон, например, умели решать задачи, сводившиеся к квадратным и кубическим уравнениям.

Рассмотрим алгебраическое уравнение n- степени

$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$ (1)

Его левую часть мы назовем многочленом n –й степени. Многочлен n-степени мы можем рассматривать как функцию переменной x – это прерогатива математического анализа. Возможен и алгебраический подход. Оказывается, этот подход дает массу результатов. Наиболее же прагматичный и результативный - это сочетание алгебры и математического анализа при изучении многочленов.

Дадим алгебраическое определение многочлена от одной неизвестной.

Определение 1. *Пусть P – некоторое числовое поле. Многочленом от x над полем P назовем выражение вида*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0 x^0, \text{ где } n \gg 1, \qquad (2)$$

$a_n, a_{n-1}, \ldots, a_0$ *-числа из поля P, 1, …. , n – положительные числа, выражения* $a_i x^i, x, x^2, \ldots, x^n$*- чисто символьные выражения, также как и символ +.*

Символ x – назовем неизвестным, числа $a_n, \ldots, a_0$ *назовем коэффициентами, выражения* $a_i x^i$ *- членами многочлена. В частности,* $a_n x^n$ *- старший член многочлена (соответственно,* a_n*- старший коэффициент многочлена),* $a_{n-1} x^{n-1}$*- второй член многочлена(соответственно,* a_{n-1} *- второй коэффициент многочлена),* $a_1 x^1$ *- линейный член многочлена,* $a_0 x^0$*-*

свободный член многочлена (соответственно, a_0- свободный коэффициент многочлена).Обозначим a_1x^1 как a_1x, a_0x^0 как a_0.

Введем теперь понятия равенства двух многочленов, суммы двух многочленов и произведения двух многочленов.

Определение 2. *Пусть f(x) и g(x) – два многочлена над полем P . Назовем их равными (тождественно равными), если они состоят из одних и тех же членов.*

Пример. $x^2 - 3 \neq x + x^2 - 3$.

Тогда многочлен тождественно равен нулю, если все его коэффициенты равны нулю. То есть многочлен отличен от нуля если хотя бы один его коэффициент отличен от нуля.

Определение 3. *Пусть*

$$f(x)= a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$
$$g(x)= b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0.$$

Тогда их суммой назовем многочлен

$$f(x)+g(x) = h(x)= c_kx^k + c_{k-1}x^{k-1} + \cdots + c_1x + c_0,$$

где k- это наибольшее из чисел m и n, $c_i = a_i + b_i$. Если m> n, то полагаем, что $a_m = \cdots = a_{n+1} = 0$. Если же n> m, то полагаем, что $b_n = \cdots = b_{m+1} = 0$.

Пример. $(x^2 - 3) + (x + x^2 - 3) = 2x^2 + x - 6$

Определение 4. *Пусть*

$$f(x)= a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$
$$g(x)= b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0.$$

Тогда их произведением назовем многочлен

$$f(x)\cdot g(x) = c_{m+n}x^{m+n} + \cdots + c_1x + c_0 = (a_n \cdot b_m)\, x^{m+n} + (a_n \cdot b_{m-1} + a_{n-1} \cdot b_m)x^{m+n-1} + \cdots (a_i \cdot b_0 + a_{i-1} \cdot b_1 + \cdots + a_0 \cdot b_i)x^i + \cdots + (a_1 \cdot b_0 + b_1 \cdot a_0)x + a_0 \cdot b_0,$$

где $a_i = 0$ при $i > n$; $b_i = 0$ при $i > m$.

Примечание. *а) Очевидно, что умножая или складывая два многочлена от неизвестного x с коэффициентами из поля P , мы всегда, согласно*

определений 3-4, получим многочлен от x, однозначно определенный, с коэффициентами из того же поля P.

б) *При умножении любого многочлена на нулевой многочлен получается всегда нулевой многочлен.*

Теорема 1. *Пусть* $P[x]$ *- это множество многочленов над полем P. Тогда операции сложения многочленов и умножения многочленов, согласно определений 3-4, удовлетворяют следующим законам:*

1^0. *Законам коммутативности:*

$$f(x) + g(x) = g(x) + f(x)$$

$$f(x)\cdot g(x) = g(x)\cdot f(x)$$

2^0. *Законам ассоциативности:*

$$\big(f(x) + g(x)\big) + h(x) = f(x)+(g(x)+h(x))$$

$$(f(x)\cdot g(x))\cdot h(x) = f(x)\cdot(g(x)\cdot h(x))$$

3^0. *Существования нулевого многочлена: существует нулевой многочлен такой,*

$$0(x)+f(x)=f(x)+0(x)=f(x)$$

4^0. *Существования противоположного многочлена: для каждого многочлена f(x) существует единственный многочлен h(x) , такой, что f(x)+h(x)=0(x). Этот многочлен h(x) называется противоположным многочленом.*

5^0. *Существования единичного многочлена: существует единичный многочлен 1(x) , такой, что при умножении любого многочлена на единичный получается сам многочлен.*

6^0. *Дистрибутивному закону умножения относительно сложения:*

$$f(x)\cdot\big(g(x) + h(x)\big) = f(x)\cdot g(x) + f(x)\cdot h(x).$$

□. Нулевой многочлен мы уже определили.

Единичный многочлен $1(x)\equiv 1$.

Для получения противоположного многочлена, достаточно изменить знаки всех коэффициентов на противоположный.

Далее доказательство проверить самостоятельно, - оно тривиальное. ■

Примечание. *Таким образом, множество многочленов над полем P относительно операций сложения и умножения многочленов образует* ***коммутативное кольцо с единицей.***

Определение 5. *Сумма и произведение нескольких многочленов строится индуктивно:*

$$f_1(x) + f_2(x) + \cdots + f_k(x) = \big(f_1(x) + f_2(x) + \cdots + f_{k-1}(x)\big) + f_k(x)$$

$$f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_k(x) = \big(f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_{k-1}(x)\big) \cdot f_k(x)$$

Методом математической индукции можно легко доказать следующие две теоремы:

Теорема 2. *Во всякой сумме многочленов из $P[x]$ скобки можно расставлять произвольно.*

Теорема 3. *Во всяком произведении многочленов из $P[x]$ скобки можно расставлять произвольно.*

Примечание. *Из приведенных закономерностей следует, что*

а) многочлен

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

можно рассматривать как сумму его членов $a_i x^i$. При этом члены многочлена можно записывать в любом порядке;

б) символы x^i можно рассматривать как степени переменной x;

в) наибольшую из степеней членов многочлена назовем степенью самого многочлена.

Теорема 4. *Если $f(x)$ и $g(x)$ – многочлены из $P[x]$, отличные от нуля, то их произведение $f(x) \cdot g(x)$ также отлично от нуля.*

□. *По условию теоремы существуют коэффициенты $a_k \neq 0$ и $b_s \neq 0$, здесь k и s – это степени многочленов. Тогда в произведение $f(x) \cdot g(x)$ коэффициент $c_{k+s} \neq 0$ – старший коэффициент отличен от нуля.* ■

Примечание. *Таким образом, в кольце $P[x]$ нет делителей нуля.*

Определение 6. *Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ - это произвольный многочлен из $P[x]$. Если вместо переменной x подставить в формулу какую-нибудь константу c, то произведя все операции, заданные по*

формуле, получим некоторую константу f(c), которую назовем значением многочлена при x=c.

Теорема 5. *Если f(x)≡g(x), то f(c)=g(c) для любого числа c из поля P.*

□. Доказательство очевидно. ■

Определение 7. *Скажем, что многочлен f(x) делится на многочлен g(x) в кольце $P[x]$, если в этом кольце найдется многочлен h(x) такой, что*

$$f(x)=g(x)\cdot h(x).$$

Тогда g(x) называется делителем многочлена f(x), а h(x) – частное при делении f(x) на g(x).

Примечание. *Заметим, что не всегда можно разделить многочлен на многочлен, например, невозможно разделить на многочлен большей степени, так как по правилам умножения многочлен h(x) тогда должен иметь отрицательную степень.*

Простейшие свойства делимости многочленов:

1) *Всякий многочлен $f(x)$ из $P[x]$ делится на самого себя.*

2) *Если $f(x)$ и g(x) – многочлены из $P[x]$, и f(x) делится на g(x), а g(x) делится на f(x), то $f(x)$ и g(x) отличаются друг от друга на множитель нулевой степени, т. е. f(x)=c· $g(x)$. Тогда их называют совпадающими с точностью до множителя нулевой степени.*

3) *Если два многочлена и $f(x)$ и g(x) из $P[x]$ делятся на один и тот же многочлен h(x) из $P[x]$, то их сумма и разность делятся на h(x).*

4) *Если многочлены $f_1(x)$, … , $f_n(x)$ из $P[x]$ делятся на один и тот же многочлен h(x) из $P[x]$, то их линейная комбинация* $c_1 f_1(x) + \dots + c_т f_n(x)$ *так делится на h(x).*

5) *Если многочлены $f_1(x)$, … , $f_n(x)$ из $P[x]$, и $f_1(x)$делится на многочлен h(x) из $P[x]$,то произведение $f_1(x)\cdot \dots \cdot f_n(x)$ делится на многочлен h(x).*

6) *Если многочлены $f(x)$, g(x)и h(x) из $P[x]$, и f(x) делится на g(x), а g(x) делится на h(x), то $f(x)$ делится на h(x).*

7) *Многочлены нулевой степени из $P[x]$ являются делителями любого многочлена из $P[x]$.*

***Теорема 6* (О делении с остатком).** *Для любого многочлена f(x) из $P[x]$и многочлена g(x) , не равного нулю, из $P[x]$ существует такая пара многочленов q(x) и r(x) из того же кольца $P[x]$, что*

$$f(x)=g(x)\cdot q(x)+r(x) \qquad (3)$$

*При этом **q(x)называют неполным частным**, **r(x)- остатком при делении** многочлена f(x) на многочлен g(x).*

□. *Пусть*

$f(x)= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ - *многочлен степени n,*

$g(x)= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$- *многочлен степени m.*

Если $f(x)\equiv 0$ *или* $n < m$, *то равенство (3) справедливо при q(x)=0 и r(x)=f(x). Если* $n \gg m$, *то алгоритм действия следующий. Вычитаем из f(x) многочлен g(x), умноженный на* $\frac{a_n}{b_m}x^{n-m}$, *получим многочлен* $f_1(x)$*:*

$$f(x)- g(x)\cdot \frac{a_n}{b_m}x^{n-m} = f_1(x).$$

В результате старший член многочлена f(x) будет уничтожен, т. е. исчезнет, и

$$f_1(x)=a'_{n-1}x^{n-1} + a'_{n-2}x^{n-2} + \cdots + a'_0.$$

Если $n-1 \gg m$, *то повторим процесс уничтожения старшего члена* $f_1(x)$*:*

$$f_1(x)- g(x)\cdot \frac{a'_{n-1}}{b_m}x^{n-m-1} = f_2(x)$$

и т.д. ……

$$f_k(x)- g(x)\cdot \frac{a^{(k)}_{n-k}}{b_m}x^{n-m-1} = r(x)$$

Очевидно, что через конечное число шагов алгоритма получим многочлен r(x), равный нулю или имеющий степень ниже степени g(x).

Сложим все полученные равенства и упростим:

$f(x)- (\frac{a_n}{b_m}x^{n-m} + \frac{a'_{n-1}}{b_m}x^{n-m-1} + \cdots + \frac{a^{(k)}_{n-k}}{b_m}x^{n-m-1})\cdot g(x) = r(x)$ *или*

$f(x)=g(x)\cdot q(x)+r(x)$, *где* $q(x)= \frac{a_n}{b_m}x^{n-m} + \frac{a'_{n-1}}{b_m}x^{n-m-1} + \cdots + \frac{a^{(k)}_{n-k}}{b_m}x^{n-m-1}$. ■

Теорема 7 (О единственности деления с остатком). *Независимо от процесса их получения частное и остаток при делении многочлена f(x) из* $P[x]$ *на многочлен* $g(x) \neq 0$ *также из* $P[x]$ *определяются единственным образом.*

□. *Доказательство проведем от противного. Пусть*

$f(x)=g(x)\cdot q(x)+r(x)$ *и*

$f(x)=g(x)\cdot q_1(x)+r_1(x)$*,т. е. существуют по меньшей мере два частных, два остатка.*

Вычтем два равенства друг из друга:

$g(x)\cdot q(x)+r(x)= g(x)\cdot q_1(x)+r_1(x)$ *или*

$g(x)\cdot\big(q(x)-q_1(x)\big)=r(x)-r_1(x).$

Если $q(x) \neq q_1(x)$*, то и* $q(x)-q_1(x)\neq 0$*. Тогда степень* $r(x)$-$r_1(x)$*не ниже степени g(x), что противоречит методу получения остатка.*

Следовательно, предположение, что $q(x) \neq q_1(x)$*,неверное. То есть* $q(x)= q_1(x)$*,откуда и* $r(x)=r_1(x)$. ■

Очевидной является тогда теорема:

Теорема 8. *Многочлен f(x) из* $P[x]$ *делится на многочлен g(x) из* $P[x]$ *тогда и только тогда, когда остаток при делении f(x) на g(x) равен нулю.*

Примечание. *Согласно этой теореме, получается, что делимость многочлена на многочлен не зависит от того, над каким полем рассматриваются многочлены f(x) и g(x), т. е. и при расширении поля P мы получим одни и те же частные и остаток.*

Образец деления многочлена на многочлен:

Пример. *Разделить с остатком многочлен* $f(x) = 3x^3+4x^2-7$ *на многочлен* $g(x) = 2x-3$

Решение. Произведем деление столбиком, как обычно делим числа друг на друга (эта процедура так и называется – деление многочлена на многочлен столбиком). Делим до тех пор, пока не получим константу, т. е. многочлен нулевой степени: Степень остатка должна быть ниже степени делителя, т. е. меньше 1, т. е. равно нулю.

$$
\begin{array}{l|l}
3x^3+4x^2-7 & 2x-3 \\
3x^3-\frac{9}{2}x^2 & \hline \\
\hline
\frac{17}{2}x^2-7 & \frac{3}{2}x^2+\frac{17}{4}x+\frac{51}{4} \\
\frac{17}{2}x^2-\frac{51}{2}x & \\
\hline
\frac{51}{2}x-7 & \\
\frac{51}{2}x-\frac{153}{4} & \\
\hline
\frac{125}{4} &
\end{array}
$$

Остаток нулевой степени, как и положено: $<$ степень $g(x)$

Итого, мы получили: $\frac{3x^3+4x^2-7}{2x-3}=\frac{3}{2}x^2+\frac{17}{4}x+\frac{51}{4}+\frac{\frac{125}{4}}{2x-3}$

Или: $3x^3+4x^2-7=(2x-3)\cdot\left(\frac{3}{2}x^2+\frac{17}{4}x+\frac{51}{4}\right)+\frac{125}{4}$,

т. е $q(x)=\frac{3}{2}x^2+\frac{17}{4}x+\frac{51}{4}$; $r(x)=\frac{125}{4}$.

Проверка: *Умножим и сложим то, что в правой части, - все верно.*

Ответ: $3x^3+4x^2-7=(2x-3)\cdot\left(\frac{3}{2}x^2+\frac{17}{4}x+\frac{51}{4}\right)+\frac{125}{4}$.