Многочлены от нескольких переменных

Пусть K - коммутативное, ассоциативное кольцо с единицей.

Опр: 1. Кольцо многочленов от n переменных с коэффициентами из кольца K это ассоциативное, коммутативное кольцо с единицей, удовлетворяющее следующим свойствам:

1) $K \subset K[x_1, \ldots, x_n]$;
2) $x_1, \ldots, x_n \in K[x_1, \ldots, x_n]$, $x_1, \ldots, x_n \notin K$;
3) $\forall f \in K[x_1, \ldots, x_n]$, $\exists!$ представление:

$$f = \sum_{k_1, \ldots, k_n \geq 0} a_{k_1 \ldots k_n} \cdot x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$$

С точностью до добавления нулевых слагаемых;

Обозначение: $K[x_1, \ldots, k_n]$.

Опр: 2. Элементы $x_1, \ldots, x_n \in K[x_1, \ldots, x_n]$ называются переменными.

Опр: 3. Элементы $a_{k_1 \ldots k_n} \in K$ в представлении $f \in K[x_1, \ldots, x_n]$ называются коэффициентами.

Опр: 4. Элементы $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ в представлении $f \in K[x_1, \ldots, x_n]$ называются одночленами.

Теорема 1. $K[x_1, \ldots, x_n]$ - существует и единственно с точностью до изоморфизма.

□

Существование: Проведём индукцией по числу переменных.

База индукции: При $n = 1$ - ранее доказали.

Шаг индукции: При $n > 1$ определим кольцо так:

$$K[x_1, \ldots, x_n] = (K[x_1, \ldots, x_{n-1}])[x_n]$$

То есть рассматриваем кольцо многочленов от одной переменной x_n с кольцом коэффициентов равным кольцу многочленов от $n-1$ переменной, построенное по индукции. Надо проверить, что новое кольцо будет удовлетворять свойствам из определения:

1) $K \subset K[x_1, \ldots, x_{n-1}] \subset (K[x_1, \ldots, x_{n-1}])[x_n]$;
2) $x_1, \ldots, x_{n-1} \in K[x_1, \ldots, x_{n-1}] \Rightarrow x_1, \ldots, x_{n-1} \in (K[x_1, \ldots, x_{n-1}])[x_n]$, $x_n \in (K[x_1, \ldots, x_{n-1}])[x_n]$;
3) Поскольку мы строим кольцо многочленов от одной переменной, то каждый элемент из построенного кольца единственным образом представляется единственным образом в виде многочлена от переменной x_n с коэффициентами из $K[x_1, \ldots, x_{n-1}]$:

$$\forall f \in (K[x_1, \ldots, x_{n-1}])[x_n],\ \exists! \text{ представление}\colon\ f = \sum_{k \geq 0} f_k \cdot x_n^k,\ f_k \in K[x_1, \ldots, x_{n-1}]$$

где f_k также имеют единственное представление по предположению индукции:

$$\forall k,\ \exists! \text{ представление}\colon\ f_k = \sum_{k_1, \ldots, k_{n-1} \geq 0} a_{k_1 \ldots k_{n-1} k} \cdot x_1^{k_1} \cdot \ldots \cdot x_{n-1}^{k_{n-1}} \Rightarrow$$

$$\Rightarrow f = \sum_{k_1,\ldots,k_{n-1},k\geq 0} a_{k_1\ldots k_{n-1}k}\cdot x_1^{k_1}\cdot\ldots\cdot x_{n-1}^{k_{n-1}}\cdot x_n^k$$

Если существует другое представление f, то:

$$f = \sum_{k_1,\ldots,k_{n-1},k\geq 0} b_{k_1\ldots k_{n-1}k}\cdot x_1^{k_1}\cdot\ldots\cdot x_{n-1}^{k_{n-1}}\cdot x_n^k = \sum_{k\geq 0}\left(\sum_{k_1,\ldots,k_{n-1}\geq 0} b_{k_1\ldots k_{n-1}k}\cdot x_1^{k_1}\cdot\ldots\cdot x_{n-1}^{k_{n-1}}\right)\cdot x_n^k \Rightarrow$$

$$\Rightarrow \sum_{k_1,\ldots,k_{n-1}\geq 0} b_{k_1\ldots k_{n-1}k}\cdot x_1^{k_1}\cdot\ldots\cdot x_{n-1}^{k_{n-1}} = f_k$$

где последнее равенство верно в силу единственности представления в кольце многочленов от x_n. Поскольку в кольце многочленов от $n-1$ переменной каждый многочлен единственным способом представляется в виде многочлена от одночленов, то:

$$\forall k_1,\ldots,k_{n-1},k,\ a_{k_1\ldots k_{n-1}k} = b_{k_1\ldots k_{n-1}k}$$

Единственность: доказывается как для $n = 1$: операции над многочленами не зависят существенным образом от переменных. В самом деле, пусть есть два многочлена:

$$f = \sum a_{k1\ldots k_n}\cdot x_1^{k_1}\cdot\ldots\cdot x_n^{k_n}, \quad g = \sum b_{l_1\ldots l_n}\cdot x_1^{l_1}\cdot\ldots\cdot x_n^{l_n} \Rightarrow$$

$$\Rightarrow f+g = \sum_{m_1,\ldots,m_n\geq 0}(a_{m_1\ldots m_n}+b_{m_1\ldots m_n})\cdot x_1^{m_1}\cdot\ldots\cdot x_n^{m_n}$$

$$\Rightarrow f\cdot g = \sum_{\substack{k_1,\ldots,k_n\geq 0\\ l_1,\ldots,l_n\geq 0}} a_{k_1\ldots k_n}\cdot b_{l_1\ldots l_n}\cdot x_1^{k_1+l_1}\cdot\ldots\cdot x_n^{k_n+l_n} = \sum_{m_1,\ldots,m_n\geq 0}\left(\sum_{\substack{k_1,\ldots,k_n\geq 0\\ l_1,\ldots,l_n\geq 0\\ k_i+l_i=m_i}} a_{k_1\ldots k_n}\cdot b_{l_1\ldots l_n}\right)\cdot x_1^{m_1}\cdot\ldots\cdot x_n^{m_n}$$

Таким образом, коэффициенты суммы и произведения определяются только по коэффициентам исходных многочленов, независимо от переменных $\Rightarrow$ мы можем построить изоморфизм между двумя кольцами многочленов от n переменных:

$$\varphi K[x_1,\ldots,x_n] \underset{\sim}{\rightarrow} K[y_1,\ldots,y_n], \quad f\mapsto\varphi(f) = \sum_{k_1,\ldots,k_{n-1},k\geq 0} a_{k1\ldots k_n}\cdot y_1^{k_1}\cdot\ldots\cdot y_n^{k_n}$$

Такое соответствие взаимнооднозначно, поскольку каждый многочлен единственным способом представляется в виде линейной комбинации одночленов, то есть он определяется последовательностью своих коэффициентов. Это соответствие также согласовано с операциями сложения/умножения, поскольку результат операций зависит только от исходных коэффициентов многочленов. ■

Свойства кольца многочленов от многих переменных

Опр: 5. Функция многих аргументов $f\colon K^n \to K$ называется полиномиальной функцией.

Каждый многочлен $f \in K[x_1, \ldots, x_n]$ задаёт полиномиальную функцию $f\colon K^n \to K$:

$$\forall c_1, \ldots, c_n \in K,\ f(c_1, \ldots, c_n) = \sum_{k_1, \ldots, k_n \geq 0} a_{k_1 \ldots k_n} \cdot c_1^{k_1} \cdot \ldots \cdot c_n^{k_n}$$

Мы можем доказать утверждение, аналогичное утверждению для кольца многочленов от одной переменной про эквивалентность формального равенства функциональному.

Утв. 1. Пусть K - бесконечное поле, тогда функциональное равенство двух многочленов от многих переменных над этим полем равносильно формальному равенству:

$$\forall f, g,\ K[x_1, \ldots, x_n],\ f = g \Leftrightarrow \forall c_1, \ldots, c_n \in K,\ f(c_1, \ldots, c_n) = g(c_1, \ldots, c_n)$$

$\square$

($\Rightarrow$) Очевидно, поскольку если многочлены равны покоэффициентно, то подставляя вместо $x_1, \ldots, x_n$ любые значения, мы получим равенство значений.

($\Leftarrow$) Воспользуемся индукцией по числу переменных:

База индукции: При $n = 1$ - ранее доказали.

Шаг индукции: Пусть у нас есть два многочлена $f, g \in K[x_1, \ldots, x_n]$, которые равны функционально:

$$f = \sum_k f_k \cdot x_n^k, \quad g = \sum_k g_k \cdot x_n^k, \quad f_k, g_k \in K[x_1, \ldots, x_{n-1}]$$

$$\forall c_1, \ldots, c_n \in K,\ f(c_1, \ldots, c_n) = g(c_1, \ldots, c_n) \Rightarrow \sum_k f_k(c_1, \ldots, c_{n-1}) \cdot c_n^k = \sum_k g_k(c_1, \ldots, c_{n-1}) \cdot c_n^k$$

Зафиксируем $c_1, \ldots, c_{n-1}$ и будем менять только c_n, тогда мы получим равенство двух полиномиальных функций только от одной переменной. Используя случай $n = 1$, в $K[x_n]$ будет верно:

$$\psi(x_n) = \sum_k f_k(c_1, \ldots, c_{n-1}) \cdot x_n^k = \sum_k g_k(c_1, \ldots, c_{n-1}) \cdot x_n^k = \varphi(x_n),\ \psi(x_n), \varphi(x_n) \in K[x_n]$$

Равенство двух многочленов это равенство их соответствующих коэффициентов, тогда:

$$\forall k,\ \forall c_1, \ldots, c_{n-1} \in K,\ f_k(c_1, \ldots, c_{n-1}) = g_k(c_1, \ldots, c_{n-1})$$

По предположению индукции, равенство полиномиальных функций от $n - 1$ переменной влечет их формальное равенство, тогда: $f_k = g_k,\ f_k, g_k \in K[x_1, \ldots, x_{n-1}] \Rightarrow f = g$. $\blacksquare$

Опр: 6. Степенью одночлена $u = x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ от n переменных по переменной x_i называется число:

$$\deg_{x_i}(u) = \deg_{x_i}\left(x_1^{k_1} \cdot \ldots \cdot x_i^{k_i} \cdot \ldots \cdot x_n^{k_n}\right) = k_i$$

Опр: 7. Полной степенью одночлена $u = x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ от n переменных называется число:

$$\deg(u) = \deg\left(x_1^{k_1} \cdot \ldots \cdot x_i^{k_i} \cdot \ldots \cdot x_n^{k_n}\right) = k_1 + \ldots + k_i + \ldots + k_n$$

Опр: 8. Степенью многочлена $f \in K[x_1, \ldots, x_n]$ по переменной x_i называется максимальная степень одночленов по переменной x_i, входящих в него с ненулевым коэффициентом:

$$\deg_{x_i}(f) = \deg_{x_i}\left(\sum_{k_1,\ldots,k_n \geq 0} a_{k_1\ldots k_n} \cdot x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}\right) = \max_{i\colon a_{k_1\ldots k_n} \neq 0} \deg_{x_i}(x_1^{k_1} \cdot \ldots \cdot x_n^{k_n})$$

Опр: 9. Степенью многочлена $f \in K[x_1, \ldots, x_n]$ называется максимальная полная степень одночленов, входящих в него с ненулевым коэффициентом:

$$\deg(f) = \deg\left(\sum_{k_1,\ldots,k_n \geq 0} a_{k_1\ldots k_n} \cdot x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}\right) = \max_{a_{k_1\ldots k_n} \neq 0} \deg(x_1^{k_1} \cdot \ldots \cdot x_n^{k_n})$$

Опр: 10. Многочлен $f \in K[x_1, \ldots, x_n]$ называется однородным, если полная степень всех одночленов входящих в f с ненулевыми коэффициентами - одинакова.

Отметим следующее полезное утверждение.

Утв. 2. Любой многочлен от n переменных можно разложить на сумму однородных многочленов, причем единственным образом:

$$\forall f \in K[x_1, \ldots, x_n],\ f \neq 0,\ \deg(f) = d,\ \exists!\,\text{разложение}\colon\ f = f_0 + f_1 + \ldots + f_d$$

где все многочлены f_k - однородны, степени $\deg(f_k) = k$.

□ Если у f есть одночлены разных степеней в него входящие, то все одночлены одной и той же фиксированной степени k сгруппируем в одну подсумму большой суммы $\Rightarrow$ получим f_k. Единственность очевидно следует из определения кольца многочленов от n переменных. ■

Опр: 11. Однородные многочлены $f_0, f_1, \ldots, f_d$ называются однородными компонентами f.

Лексикографиечский порядок

В случае одной переменной все одночлены можно различать и упорядочивать по их степеням: у двух разных одночленов разные степени и их можно сравнивать по степеням. В случае одночленов от нескольких переменных их уже нельзя сравнивать по степени, поскольку бывают разные одночлены одной и той же степени. При этом, их хочется как-то сравнивать и упорядочивать между собой.

Опр: 12. Лексикографический порядок на одночленах устроен следующим образом:

$$u = x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \succ v = x_1^{l_1} \cdot \ldots \cdot x_n^{l_n}$$

Одночлен u старше, чем одночлен v, если:

$$\exists\, i\colon k_i > l_i,\ \forall j < i,\ k_j = l_j$$

Rm: 1. Лексикографический означает - словарный. Похожим образом, например, сравниваются слова в словаре.

Пример: Рассмотрим два одночлена: $x_1^2x_2x_3^3x_4^2x_5$ и $x_1^2x_2x_3^2x_4^3x_5^4$. Первый одночлен старше:

$$x_1\colon 2 = 2,\ x_2\colon 1 = 1,\ x^3\colon 3 > 2 \Rightarrow x_1^2x_2x_3^3x_4^2x_5 \succ x_1^2x_2x_3^2x_4^3x_5^4$$

При этом: $\deg(x_1^2x_2x_3^2x_4^3x_5^4) = 2+1+2+3+4 = 12 > \deg(x_1^2x_2x_3^3x_4^2x_5) = 2+1+3+2+1 = 9$.

Rm: 2. Заметим, что лексикографический порядок, вообще говоря, не согласован с полной степенью. Можно модифицировать определение лексикографического порядка - сначала упорядочивая члены по степени, а уже одночлены одинаковых степеней упорядочивать лексикографически. Такой порядок будет называться однородным лексикографическим порядком.

Утв. 3. (**Свойства лексикографического порядка**):

1) Для любых двух одночленов u и v верно одно из трёх: $u \succ v$, $u \prec v$, $u = v$;
2) **Транзитивность**: $u \succ v \succ w \Rightarrow u \succ w$;
3) Если $u \succ v$, то $u{\cdot}w \succ v{\cdot}w$;
4) Если $u_1 \succ v_1$, $u_2 \succ v_2$, то $u_1{\cdot}u_2 \succ v_1{\cdot}v_2$;

□

1) Очевидно, поскольку по порядку степени переменных в одночленах либо равны, либо больше или меньше друг друга;
2) Пусть $u = x_1^{k_1}\cdot\ldots\cdot x_n^{k_n}$, $v = x_1^{l_1}\cdot\ldots\cdot x_n^{l_n}$, $w = x_1^{m_1}\cdot\ldots\cdot x_n^{m_n}$, будем их сравнивать:

$$\begin{matrix} k_1 & k_2 & \ldots & k_i & \ldots & k_j & \ldots & k_n \\ \shortparallel & \shortparallel & \ldots & \vee & \ldots & ? & \ldots & ? \\ l_1 & l_2 & \ldots & l_i & \ldots & l_j & \ldots & l_n \\ \shortparallel & \shortparallel & \ldots & \shortparallel & \ldots & \vee & \ldots & ? \\ m_1 & m_2 & \ldots & m_i & \ldots & m_j & \ldots & m_n \end{matrix} \Rightarrow \begin{cases} k_i > l_i,\ k_p = l_p, & p < i \\ l_j > m_j,\ l_s = m_s, & s < j \end{cases}$$

Сравним теперь u и w:

$$r = \min(i,j) \Rightarrow \forall t < r,\ k_t = l_t = m_t,\ k_r \geq l_r \geq m_r$$

Причем в последнем неравенстве одно из них будет строгим $\Rightarrow k_r > m_r \Rightarrow u \succ w$;

3) Пусть, например: $u \succ v$ и $w = x_1^{m_1}\cdot\ldots\cdot x_n^{m_n}$, тогда:

$$\exists\, i\colon k_i > l_i,\ \forall j < i,\ k_j = l_j \Rightarrow k_i + m_i > l_i + m_i,\ \forall j < i,\ k_j + m_j = l_j + m_j \Rightarrow u{\cdot}w \succ v{\cdot}w$$

4) Воспользуемся свойством 3) и 2):

$$u_1 \succ v_1,\ u_2 \succ v_2 \underset{3)}{\Rightarrow} u_1{\cdot}u_2 \succ v_1{\cdot}u_2,\ v_1{\cdot}u_2 \succ v_1{\cdot}v_2 \underset{2)}{\Rightarrow} u_1{\cdot}u_2 \succ v_1{\cdot}v_2$$

■

Опр: 13. Старший член многочлена $f \in K[x_1,\ldots,x_n]$, $f \neq 0$ это самый старший из одночленов, входящих в f с ненулевым коэффициентом.

Обозначение: $\widehat{f}$.

Утв. 4. Пусть K это область целостности (коммутативное, ассоциативное кольцо с единицей без делителей нуля). Тогда если $f, g \in K[x_1, \ldots, x_n]$, $f, g \neq 0$, то $f \cdot g \neq 0$ и $\widehat{fg} = \widehat{f} \cdot \widehat{g}$.

□ Пусть многочлены имеют вид:

$$f = a_0 u_0 + a_1 u_1 + \ldots + a_k u_k, \quad g = b_0 v_0 + b_1 v_1 + \ldots + b_l v_l$$

где u_i, v_j это одночлены, $a_i, b_j \in K$, $a_i, b_j \neq 0$. Пусть также будет верен лексикографический порядок:

$$u_0 \succ u_1 \succ \ldots \succ u_k,\ \widehat{f} = u_0 \quad v_0 \succ v_1 \succ \ldots \succ v_k,\ \widehat{g} = v_0 \Rightarrow$$

$$\Rightarrow f \cdot g = \underbrace{a_0 \cdot b_0}_{\neq 0} \cdot u_0 \cdot v_0 + \sum_{i,j:\ i>0 \vee j>0} a_i \cdot b_j \cdot u_i \cdot v_j$$

где $a_0 \cdot b_0 \neq 0$ поскольку мы находимся в целостном кольце и произведение ненулевых элементов также дает ненулевой элемент. Рассмотрим одночлен $u_0 \cdot v_0$:

$$\widehat{f} = u_0 \Rightarrow \forall i > 0,\ u_0 v_0 \succ u_i v_0,\ \widehat{g} = v_0 \Rightarrow \forall j,\ u_i v_0 \succeq u_i v_j \Rightarrow \forall i > 0,\ u_0 v_0 \succ u_i v_j$$

$$\widehat{g} = v_0 \Rightarrow \forall j > 0,\ u_0 v_0 \succ u_0 v_j,\ \widehat{u} = u_0 \Rightarrow \forall i,\ u_0 v_j \succeq u_i v_j \Rightarrow \forall j > 0,\ u_0 v_0 \succ u_i v_j$$

Таким образом, мы получаем: $\forall i, j > 0,\ u_0 v_0 \succ u_i v_j \Rightarrow$ первое слагаемое ни с кем не сокращается $\Rightarrow f \cdot g \neq 0$ и вместе с этим: $\widehat{f \cdot g} = u_0 \cdot v_0 = \widehat{f} \cdot \widehat{g}$. ■

Следствие 1. Если K это область целостности, то $K[x_1, \ldots, x_n]$ тоже будет областью целостности.

□ Произведение ненулевых элементов не равно нулю $\Rightarrow$ нет делителей нуля $\Rightarrow$ получим область целостности. Коммутативность, ассоциативность, наличие единицы всегда будет иметь место. ■

Упр. 1. Если K это область целостности, $f, g \in K[x_1, \ldots, x_n]$, $f, g \neq 0$, то тогда:

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

В том числе это будет верно для степеней по переменным.

Факториальность кольца многочленов от многих переменных

В случае многочленов от одной переменной кольцо многочленов с коэффициентами из поля - евклидово, а всякое евклидово кольцо факториально: есть однозначное разложение на простые множители. Оказывается, что $K[x_1, \ldots, x_n]$ уже не евклидово при $n > 1$, тем не менее оно факториально.

Упр. 2. Доказать, что $K[x_1, \ldots, x_n]$ над полем K - не евклидово.

Теорема 2. Если A это факториальное кольцо, то тогда $A[x]$ тоже факториально.

Следствие 2. $\mathbb{Z}[x]$ - факториально.

□ $\mathbb{Z}$ это факториальное кольцо $\Rightarrow$ применяя теорему получаем требуемое. ■

Следствие 3. $K[x_1, \ldots, x_n]$ - факториально, если K - это поле (или факториальное кольцо).

□ Индукцией по n.

База индукции: При $n = 1$: кольцо многочленов над полем евклидово $\Rightarrow$ факториально. Кольцо многочленов над произвольным факториальным кольцом, то это следует из теоремы.

Шаг индукции: Представим наше кольцо многочленов следующим образом:

$$K[x_1, \dots, x_n] = (K[x_1, \dots, x_{n-1}])\,[x_n]$$

По предположению индукции $K[x_1, \dots, x_{n-1}]$ будет факториальным $\Rightarrow$ кольцо многочленов над этим кольцом также будет факториальным по теореме. ■

Докажем теорему 2. Обозначим $K = Q(A)$ - поле дробей факториального кольца A. Вспомним:

Опр: 14. Целостное кольцо A называется факториальным, если $\forall a \in A$, $a \neq 0$, $a \notin A^\times$ можно разложить в произведение простых множителей единственным образом, с точностью до перестановки множителей и их замены на ассоциированные элементы.

Опр: 15. Многочлен $g = a_0 + a_1x + \ldots + a_nx^n \in A[x]$ называется примитивным, если все его коэффициенты $a_0, a_1, \dots, a_n \in A$ взаимно просты в совокупности: $(a_0, a_1, \dots, a_n) = 1$.

Rm: 3. Взаимная простота коэффициентов в совокупности $\Leftrightarrow$ у них нет общего необратимого делителя.

Лемма 1.

1) $f \in K[x] \Rightarrow f = \lambda \cdot g$, $\lambda \in K^\times$, $g \in A[x]$ - примитивен;
2) $f \in A[x] \Rightarrow \lambda \in A$;

□

1) Пусть многочлен $f \in K[x]$ имеет вид:

$$f = c_0 + c_1x + \ldots + c_nx^n,\ c_0, c_1, \dots, c_n \in K$$

Поскольку $K = Q(A)$, то каждый из коэффициентов представляется в виде дроби с числителем и знаменателем из A, причем их можно привести к общему знаменателю:

$$\forall i = \overline{0, n},\ c_i = \frac{b_i}{c},\ b_i, c \in A$$

Так как мы находимся в факториальном кольце, то у любого набора элементов есть НОД, он вычисляется по разложению на простые множители (смотри лекцию 17 этого семестра). Положим НОД: $b = (b_0, b_1, \dots, b_n) \in A$, тогда:

$$\forall i = \overline{0, n},\ b_i = b \cdot a_i,\ a_i \in A \colon (a_0, a_1, \dots, a_n) = 1 \Rightarrow$$

$$\forall i = \overline{0, n},\ c_i = \frac{b}{c} \cdot a_i,\ \lambda = \frac{b}{c} \Rightarrow f = \lambda(a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n)$$

где многочлен $g = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n$ будет примитивным с коэффициентами из A;

2) Воспользуемся 1) и представим $f \in A[x]$ в виде: $f = \lambda \cdot g$, где g - примитивный и $\lambda = \frac{b}{c}$. Можем считать, что $(b, c) = 1$ в кольце A, сократив их на НОД, тогда:

$$f \in A[x] \Rightarrow \forall i = \overline{0, n},\ c_i = \frac{ba_i}{c} \in A \Rightarrow ba_i = c_ic \Rightarrow ba_i \,\vdots\, c$$

где последнее верно по определению делимости. Предположим противное: пусть $\lambda = \frac{b}{c} \notin A$, тогда:

$$\exists\,\text{простое}\ p \in A\colon p \mid c,\ p \nmid b \Rightarrow \forall i = \overline{0,n},\ b{\cdot}a_i \vdots p \Rightarrow \forall i = \overline{0,n},\ a_i \vdots p$$

Последнее следует из того факта, что если произведение двух множителей делится на какой-то простой элемент, то один из множителей должен на него делится, в силу единственности разложения на простые множители.

Получили противоречие с примитивностью многочлена, так как все его коэффициенты делятся на p, хотя их НОД $(a_0, a_1, \ldots, a_n) = 1 \Rightarrow \lambda \in A$;

■

Лемма 2. (**Гаусс**) Произведение примитивных многочленов - примитивный многочлен.

□ Пусть $f = a_0 + a_1x + \ldots + a_nx^n$ и $g = b_0 + b_1x + \ldots + b_mx_m$ - два примитивных многочлена. Рассмотрим их произведение:

$$f{\cdot}g = c_0 + c_1x + \ldots + c_{n+m}x^{n+m},\ c_k = \sum_{i+j=k} a_ib_j$$

Предположим противное: пусть $f{\cdot}g$ - не примитивен, тогда

$$\exists\,\text{простой}\ p \in A\colon \forall k = \overline{0, n+m},\ c_k \vdots p$$

Поскольку многочлены f, g были примитивными, то: $\exists\, i, j\colon a_i, b_j \not\vdots\ p$. Возьмем наименьшие i, j с этими свойствами и рассмотрим коэффициент $c_k = c_{i+j}$:

$$c_k = a_0b_k + \ldots + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + \ldots + a_kb_0$$

$$\forall k < i,\ a_k \vdots p \Rightarrow a_0, \ldots, a_{i-1} \vdots p \Rightarrow a_0b_k, \ldots, a_{i-1}b_{j+1} \vdots p$$

$$\forall k < j,\ b_k \vdots p \Rightarrow b_{j-1}, \ldots, b_0 \vdots p \Rightarrow a_{i+1}b_{j-1}, \ldots, a_kb_0 \vdots p$$

Получаем противоречие, поскольку c_k делится на p и все члены кроме a_ib_j тоже делятся на p. ■

□ (**Доказательство теоремы** 2)

1) Описание простых элементов в $A[x]$:

   (1) deg $= 0$: Простые элементы $p \in A$: если многочлен степени 0 мог бы разлагаться на два множителя нулевой степени, то он не мог бы быть простым элементом в $A \Rightarrow$ он простой в A;

   (2) deg > 0: Многочлены примитивные в $A[x]$ и неприводимые в $K[x]$: такой многочлен мог бы разлагаться на следующие множители:

      a) На два множителя меньшей степени (тоже положительной) $\Rightarrow$ по определению был бы приводимым многочленом $\Rightarrow$ не разлагается на такие множители;

      b) На два множителя нулевой и первончальной степеней $\Rightarrow$ из коэффициентов исходного многочлена можно было бы вынести общую константу $\Rightarrow$ он не был бы примитивным $\Rightarrow$ не разлагается на такие множители;

   Других простых нет, поскольку каждый многочлен из $A[x]$ может быть разложен в произведение многочленов нулевой и положительной степени (вытекает из следующего пункта);

2) Разложение многочленов в $A[x]$:

$$\forall f \in A[x],\ \exists \text{ разложение}\colon f = p_1 \cdot \ldots \cdot p_m \cdot g_1 \cdot \ldots \cdot g_n$$

где $p_1, \ldots, p_m$ - простые в A, а $g_1, \ldots, g_n$ - примитивные многочлены, неприводимые над K. В самом деле, кольцо многочленов над полем K факториально (поскольку оно евклидово) $\Rightarrow$ каждый многочлен разлагается в произведение неприводимых, тогда:

$$\forall f \in A[x] \Rightarrow f \in K[x] \Rightarrow f = f_1 \cdot \ldots \cdot f_n,\ \forall i = \overline{1, n},\ f_i \text{ - неприводимые в } K[x]$$

По лемме 1 многочлены f_i в f можно представить в следующем виде:

$$f = f_1 \cdot \ldots \cdot f_n = (\lambda_1 g_1) \cdot \ldots \cdot (\lambda_n g_n),\ \forall i = \overline{1, n},\ \lambda_i \in K^\times,\ g_i \text{ - примитивные},\ g_i \in A[x]$$

Соберём все константы $\lambda_1, \ldots, \lambda_n$ в одну λ, тогда:

$$f = \lambda \cdot \underbrace{g_1 \cdot \ldots \cdot g_n}_{\text{примитивно}},\ \lambda \in K^\times,\ \forall i = \overline{1, n},\ g_i \in A[x]$$

Заметим, что произведение $g_1 \cdot \ldots \cdot g_n$ примитивно по лемме 2. Вместе с этим g_i ещё и неприводимы, поскольку пропорциональны неприводимым многочленам над K. Так как произведение примитивного многочлена на λ даёт многочлен с коэффициентами из A, то по лемме 1 пункту 2), коэффициент $\lambda \in A \Rightarrow$ его можно разложить в произведение простых элементов:

$$\lambda = p_1 \cdot \ldots \cdot p_m,\ \forall i = \overline{1, m},\ p_i \text{ - простые},\ p_i \in A$$

Следовательно, мы получили требуемое разложение;

3) Единственность разложения $f \in A[x]$:

Пусть $f \in A[x]$ разлагается двумя способами:

$$f = p_1 \cdot \ldots \cdot p_m \cdot g_1 \cdot \ldots \cdot g_n = q_1 \cdot \ldots \cdot q_k \cdot h_1 \cdot \ldots \cdot h_l$$

где p_i, q_j - простые в A, а g_i, h_j - примитивные многочлены из $A[x]$, неприводимые над K. Поскольку кольцо многочленов $K[x]$ факториально $\Rightarrow$ разложение на неприводимые многочлены над K единственно $\Rightarrow$ количество неприводимых множителей в обоих способах одинаковое: $n = l$ и после перенумерации будет верно:

$$\forall i = \overline{1, n},\ h_i = \alpha_i \cdot g_i,\ \alpha_i \in K^\times,\ h_i, g_i \in A[x]$$

Но поскольку h_i и g_i примитивны, то по лемме 1 будет верно: $\alpha_i \in A$ и более того, у h_i не может быть необратимого общего делителя его коэффициентов $\Rightarrow$ он обратим $\Rightarrow$ $\alpha_i \in A^\times$. Таким образом, если мы заменим h_i на $\alpha_i g_i$, то получим равенство констант:

$$p_1 \cdot \ldots \cdot p_m = \underbrace{\alpha_1 \cdot \ldots \cdot \alpha_n}_{\in A^\times} \cdot q_1 \cdot \ldots \cdot q_k$$

В результате, мы имеем два разложения на простые множители уже для константы из кольца A, но поскольку кольцо A факториально, то такое разложение единственно $\Rightarrow$ $m = k$ и после упорядочивания получим ассоциированные элементы:

$$\forall i = \overline{1, m},\ p_i \sim q_i$$

Следовательно, разложения совпадают с точностью до перестановки множителей и их ассоциированности. Таким образом, мы доказали единственность разложения на простые элементы $A[x]$;

Поскольку разложение любого многочлена $A[x]$ на простые элементы единственно с точностью до перестановки и ассоциированности множителей, то $A[x]$ - факториально. ■