Полиноми на една променлива. Алгоритъм за деление с остатък.

Ако F е някакво поле, то знаем, че полином на една променлива с коефициенти от F е израз от вида

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

за естествено число $n \in \mathbb{N}$ и $a_i \in F$ за $i = 0, 1, \ldots, n$.

Сега ще дадем по-формална и обобщена дефиниция на понятието полином,която същевременно разглежда множеството от полиномите на една променлива като алгебричната структура пръстен.

Нека A е комутативен пръстен с единица. Разглеждаме наредени редици от вида $(a_0, a_1, a_2, \ldots)$, където $a_i \in A$ за $i = 0, 1, 2, \ldots$, в които само краен брой елементи a_i са различни от 0_A. Такива редици ще наричаме *финитни*. Означаваме с B множеството от всички финитни редици и в него дефинираме операции $+$ и $\cdot$ по следните правила: ако $a = (a_0, a_1, a_2, \ldots), b = (b_0, b_1, b_2, \ldots) \in B$, то $a + b = (a_0 + b_0, a_1 + b_1, \ldots)$ и $ab = (c_0, c_1, c_2, \ldots)$, където $c_0 = a_0b_0, c_1 = a_0b_1 + a_1b_0, c_2 = a_0b_2 + a_1b_1 + a_2b_0, \ldots, c_i = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0, \ldots$ за $i = 0, 1, 2, \ldots$. Очевидно редиците $a + b$ и ab също са финитни и принадлежат на множеството B. И така, относно тези операции B се превръща в комутативен пръстен с единица. Нулевият елемент на B е редицата $(0_A, 0_A, \ldots)$, асоциативността и комутативността на операцията $+$ са очевидни, а асоциативността и комутативността на операцията $\cdot$ се проверяват директно, единичният елемент на пръстена е редицата $(1_A, 0_A, 0_A, \ldots)$.

Подмножеството

$$B_0 = \{(a, 0_A, 0_A, \ldots) \mid a \in A\}$$

е подпръстен на B, а изображението, което извършва съпоставянето $(a, 0_A, 0_A, \dots) \mapsto a$ е изоморфизъм на пръстените B_0 и A (т.е. $B_0 \cong A$). По този начин може да отъждествим елементът $(a, 0_A, 0_A, \dots) =$ и да считаме, че A е подпръстен на B. Въвеждаме специални означения за някои от елементите на B, а именно $x = (0_A, 1_A, 0_A, 0_A, \dots), x^2 = x.x = (0_A, 0_A, 1_A, 0_A, 0_A, \dots)$ и така нататък $x^k = (\underbrace{0_A, 0_A, \dots, 0_A}_{k}, 1_A, 0_A, \dots)$. Нека $a \in A$. Тогава имаме $ax^k = (a, 0_A, 0_A, \dots) \cdot (\underbrace{0_A, 0_A, \dots, 0_A}_{k}, 1_A, 0_A, \dots) = (\underbrace{0_A, 0_A, \dots, 0_A}_{k}, a, 0_A, \dots)$.

Нека $f \in B$ е такъв, че $f \neq 0_B = (0_A, 0_A, \dots)$. Тогава съществува поне един елемент от редицата $f = (f_0, f_1, \dots, f_n, \dots)$, който е ненулев. Нека n е най-голямото число, за което $f_n \neq 0_A$. Ясно е, че n е цяло неотрицателно число. Съгласно операциите $+$ и $\cdot$ и означенията, които въведохме, можем да запишем $f = (f_0, 0_A, 0_A, \dots) + (0_A, f_1, 0_A, \dots) + \dots + (\underbrace{0_A + \dots + 0_A}_{n}, f_n, 0_A, \dots) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n$. По този начин получаваме еднозначен запис за всеки от елементите на B.

Така полученият пръстен B се нарича *пръстен на полиномите на една променлива x с коефициенти от A* и се означава с $A[x]$. Елементите $f = f(x) \in B$ се наричат *полиноми с коефициенти от A* или още *полиноми над A*. Както видяхме, всеки полином $f(x) \in A[x], f(x) \neq 0_B$ се записва еднозначно като $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n$, където $f_i \in A$ за $i = 1, 2, \dots, n$, $f_n \neq 0_A$ и n е цяло неотрицателно число.

Оттук нататък стандартният начин за записване на полином ще бъде

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

където $a_i \in A$ за $i = 0, 1, \dots, n$, $a_0 \neq 0_A$ и n е цяло неотрицателно число. Елементът a_0 се нарича *старши коефициент на полинома f*, а елементът a_n се нарича *свободен член на полинома f*. Числото n се нарича *степен на полинома f* и се бележи $\deg f = n$. В случай, че $f = 0_{A[x]}$ е нулевият полином, то дефинираме $\deg f = -\infty$.

Отсега нататък ще считаме, че пръстенът A ще бъде известен и ще записваме 0 вместо 0_A. По същият начин ще записваме и нулевият полином на $A[x]$, а именно 0 вместо $0_{A[x]}$. Разлика е лесно да се направи според контекста.

Нека $f = a_0x^n + \cdots + a_n, a_0 \neq 0$ и $g = b_0x^m + \cdots + b_m, b_0 \neq 0$ са два полинома. На базата на въведените операции за събиране и умножение на полиноми е лесно да се съобрази, че $\deg(f+g) = \max\{n, m\}$. Полиномът fg има старши едночлен $a_0b_0x^{m+n}$ и следователно $\deg(fg) \leq m+n$. Ако пръстенът A е област, то $a_0b_0 \neq 0$ и тогава $\deg(fg) = m+n = \deg f + \deg g$.

Нека $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in A[x]$, а $\alpha \in A$. Елементът $f(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n \in A$ ще наричаме *стойност на полинома f при $x = \alpha$*. По този начин всеки полином $f(x) \in A[x]$ определя функция

$$f : A \longrightarrow A.$$

Ако $f(x) = g(x)$, то е ясно, че $f(\alpha) = g(\alpha)$ за $\forall\alpha \in A$ и в такъв случай функциите $f : A \longrightarrow A$ и $g : A \longrightarrow A$ съвпадат. Обратното обаче не е вярно. Например в пръстена $A = \mathbb{Z}_p$, където p е просто число разглеждаме полиномите $f(x) = x^p$ и $g(x) = x$. За всеки елемент $\overline{k} \in \mathbb{Z}_p$ е изпълнено, че $f(\overline{k}) = \overline{k}^p = \overline{k}$ според теоремата на Ферма и също $g(\overline{k}) = \overline{k}$. По този начин $f : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ и $g : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ съвпадат като функции, но $f(x) \neq g(x)$.

Ако A е област и $f(x), g(x) \in A[x]$ са два полинома със степени, ненадминаващи n и ако $f(a)i) = g(a_i)$ за $n+1$ различни елемента $a_1, a_2, \ldots, a_{n+1} \in A$, то $f(x) = g(x)$. Оттук следва, че ако A е безкрайна област и $f : A \longrightarrow A$ и $g : A \longrightarrow A$ съвпадат като функции, то обезателно $f(x) = g(x)$.

Предстои да докажем теоремата за деление с частно и остатък на полиноми, която е аналог на теоремата за деление с частно и остатък на цели числа.

Теорема. *Нека F е поле. За всеки два полинома $f(x), g(x) \in F[x]$, $g(x) \neq 0$ съществуват единствени полиноми $q(x) \in F[x]$, наречен частно и $r(x) \in F[x]$, наречен остатък, такива че е изпълнено*

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

и $\deg r < \deg g$.

Доказателство. Съществуване: нека $f(x) = a_ox^n + \cdots + a_n$, $g(x) = b_0x^m + \cdots + b_m$. Ако $\deg f < \deg g$, то $f = 0 \cdot g + f$, т.е. $r(x) = f(x)$ и $q(x) = 0$ и всичко е изпълнено. Нека сега $\deg f \geq \deg g$. За определеност $\deg f = n, \deg g = m$ (т.е. $a_0 \neq 0, b_0 \neq 0$) и $n \geq m$. Ще проведем индукция по степента на полинома f. Основа на индукцията – $n = 0$. Т.к. $n \geq m$, то тогава и $m = 0$ и имаме, че $f(x) = a_0$, $g(x) = b_0$. Тогава полагаме $q(x) =$

$\frac{a_0}{b_0}$ и $r(x) = 0$ и получаваме, че $f = q \cdot g + r$. При това $\deg r = -\infty < 0 = \deg g$. Индукционното предположение е, че това твърдение е изпълнено за всички естествени числа по-малки от n. Индукционна стъпка – ще докажем, че то е вярно и за n. Разглеждаме полинома $a_0 b_0^{-1} x^{n-m} \cdot g$. Той има старши едночлен $a_0 b_0^{-1} x^{n-m} b_0 x^m = a_0 x^n$, който съвпада със старшия едночлен на $f(x)$. Разглеждаме полинома $f_1 = f - a_0 b_0^{-1} x^{n-m} \cdot g$. Ясно е, че $f_1 \in F[x]$, а от казаното по-горе следва, че $\deg f_1 < n$. От индукционото предположение, приложено за f_1 и g следва, че съществуват полиноми $q_1, r_1 \in F[x]$, такива че $f_1 = q_1 \cdot g + r_1$ и $\deg r_1 < \deg g$. Сега $f = f_1 + a_0 b_0^{-1} x^{n-m} \cdot g = q_1 \cdot g + r_1 + a_0 b_0^{-1} x^{n-m} \cdot g = (q_1 + a_0 b_0^{-1} x^{n-m}) \cdot g + r_1$. Означаваме $q = q_1 + a_0 b_0^{-1} x^{n-m}$ и $r = r_1$ и тогава е изпълнено, че $f = q \cdot g + r$ с $\deg r < \deg g$. Принципът на математическата индукция доказва твърдението.

Единственост: нека $q, r \in F[x]$ са такива, че $f = q \cdot g + r$ и $\deg r < \deg g$. Нека предположим, че $q', r' \in F[x]$ също са такива, че $f = q' \cdot g + r'$ и $\deg r' < \deg g$. Това ни дава, че

$$qg + r = q'g + r',$$

$$(q - q')g = r' - r.$$

Ако допуснем, че $q \neq q'$, то това би означавало, че $q - q' \neq 0$, т.е. $\deg(q - q') \geq 0$ и $\deg[g(q - q')] = \deg g + \deg(q - q') \geq \deg g$. От друга страна обаче $\deg r < \deg g$ и $\deg r' < \deg g$ дават, че $\deg(r' - r) < \deg g$. Сега горните равенства водят до противоречието

$$\deg g \leq \deg[(q - q')g] = \deg(r' - r) < \deg g,$$

т.е. $\deg g < \deg g$. Тогава остава да е вярно, че $q' = q$ и $r - r' = (q' - q)g = 0g = 0$, което означава, че и $r' = r$. Така единствеността е доказана. □

Забележка: от доказателството следва, че теоремата е в сила и ако вместо поле F се вземе област A (т.е. $f, g \in A[x]$) и $b_0 \neq 0_A$ е обратим елемент. Например при $A = \mathbb{Z}$ и $b_0 = \pm 1$ теоремата е в сила и получаваме, че $q, r \in \mathbb{Z}[x]$.

Твърдение 1. *Ако F е поле, в пръстена $F[x]$ всеки идеал е главен.*

Доказателство. Нека $I \trianglelefteq F[x]$. Ако $I = \{0\}$, то просто $I = (0)$. Нека $I \neq \{0\}$ и нека $d \in I$ е такъв, че е ненулев и от най-ниска степен в

I. Щом $d \in I$ и $I \trianglelefteq F[x]$, то $(g) = \{hd \mid h \in F[x]\} \subseteq I$. Да вземем произволен полином $f \in I$. При деление на f на d с частно q и остатък r, такива че $q, r \in F[x], \deg r < \deg d$, получаваме, че $f = qd + r$. Но $f \in I$ и $qd \in (d) \subseteq I$ дават, че трябва и $r \in I$. По този начинполучихме, че $r \in I$ и $\deg r < \deg d$. Ако допуснем, че $r \neq 0$, то веднага получаваме противоречие с минималността на d. Следователно $r = 0$ и $f = qd$. Но това означава, че $f \in (d)$ за произволен полином $f \in I$ т.е. $I \subseteq (d)$. Така достигаме до факта, че $I = (d)$, което означава, че I е главен идеал с пораждащ d. $\square$