Финитна редица (дефиниция)

Нека A е комутативен пръстен с единица.

Безкрайната редица $f = f_0, f_1, f_2, \ldots$ $(f_i \in A,\ i \in \mathbb{N} \cup \{0\})$ наричаме *финитна* ако само краен брой нейни елементи са различни от нула.
Т.е. $\exists\, n:\ f_{n+t} = 0,\ \forall t \in \mathbb{N}$[1]

Теорема

Ако A е комутативен пръстен с единица.
$\Longrightarrow B = \{f \,|\, f$ - финитна редица с елементи от $A\}$
с операциите *събиране* и *умножение* на финитни редици е комутативен пръстен с единица.

Това всъщност наричат **Пръстенът на полиномите над A (с една променлива)**
Отбелязваме: $B = A[x]$

Доказателство на теоремата:

Първо нека си дефинираме операциите събиране и умножение на финитни редици:

Нека $f = f_0, f_1, \ldots$ и $g = g_0, g_1, \ldots\ \in B$

- *Събиране на финитни редици*: $f + g = d = f_0 + g_0, f_1 + g_1, f_2 + g_2, \ldots$, т.е. $d_i = f_i + g_i$
- *Умножение*: $f.g = h = h_0, h_1, h_2, \ldots$, където $h_k = f_0 g_k + f_1 g_{k-1} + \cdots + f_k g_0 = \sum_{i=0}^{k} f_i g_{k-i}$

f - финитна $\Longrightarrow \exists n:\ f_{n+t} = 0$
g - финитна $\Longrightarrow \exists m:\ g_{m+t} = 0$

Ако вземем $k = \max\{n, m\}$, то $d_{k+t} = f_{k+t} + g_{k+t} = 0 + 0 = 0 \Longrightarrow d$ е финитна и $f + g \in B$
Т.е. операцията *събиране на финитни редици* е бинарна. ;)

Нека сега $t = m + n$
Тогава $h_{t+s} = \sum_{i=0}^{t+s} f_i g_{t+s-i} = 0 \Longrightarrow h$ е финитна и $f.g \in B$
Т.е. *умножението на финитни редици* е също бинарна операция

За $\forall f, g, h \in B$, са налице следните очевидни свойства:

1. $f+g=g+f$
2. $(f+g)+h=f+(g+h)$
3. $\exists\ 0=0,0,0,\cdots\in B:\ f+0=0+f=f$
4. $-f=-f_0,-f_1,-f_2,\cdots\in B$

$\Longrightarrow B$ **е Абелева група относно** ***събирането на финитни редици***

Ето и другата партида очевидни свойства ;)
Шегувам се, разбира се. Ако всичко беше толкова очевидно, нямаше да пиша лекции.

Всъщност, за да докажем тоеремата, трябва да покажем *асоциативността, комутативността и двата дистрибутивни закона* за

умножението, както и *съществуването на единичен елемент*.

1. ***Асоциативност на умножението***:
Нека $fg=h,\ gt=u, ht=l, fu=v$

Имаме, че $(fg)t=f(gt)\iff ht=fu\iff l=v$

$$l=ht\Longrightarrow l_s=\sum_{i=0}^{s}h_it_{s-i}=\sum_{i=0}^{s}\left(\sum_{j=0}^{i}f_jg_{i-j}\right)t_{s-i}=\sum_{i=0}^{s}\sum_{j=0}^{i}f_jg_{i-j}t_{s-i} \tag{1}$$

$$v=fu\Longrightarrow v_s=\sum_{i=0}^{s}f_iu_{s-i}=\sum_{i=0}^{s}f_i\left(\sum_{j=0}^{s-i}g_jt_{s-j-i}\right)=\sum_{i=0}^{s}\sum_{j=0}^{s-i}f_ig_jt_{s-j-i} \tag{2}$$

$\Longrightarrow l=v\Longrightarrow (fg)t=f(gt)$
За тези, които са се занимавали с математика извън рамките на учебниците в гимназията, последното ще им се стори очевидно.
За останалите - с удоволствие бих го обяснила на всеки.

2. ***Дистрибутивни закони***:

Нека $g+t=h, fh=l$

$$=f(g+t)\Longrightarrow l_s=\sum_{i=0}^{s}f_ih_{s-i}=\sum_{i=0}^{s}f_i(g_{s-i}+t_{s-i})=\sum_{i=0}^{s}[f_ig_{s-i}+f_it_{s-i}]=\sum_{i=0}^{s}f_ig_{s-i}+\sum_{i=0}^{s}f_it_{s-i}=fg+ft \tag{3}$$

Аналогично и за другия дистрибутивен закон: $(f+g)t=ft+gt$

3. ***Комутативност на умножението***:
Нека $fg=v,\ gf=l$

$$fg=v\Longrightarrow v_s=\sum_{i=0}^{s}f_ig_{s-i} \tag{4}$$

$$gf=l\Longrightarrow l_s=\sum_{i=0}^{s}g_if_{s-i} \tag{5}$$

$\Longrightarrow l=v\Longrightarrow fg=gf$

4. ***Съществуване на единичен елемент***:
За единичен елемент на пръстена B си избираме финитната редица $e=1,0,0,\ldots$
От дефиницията за умножение на финитни редици следва, че $fe=ef=f,\ \forall f\in B$

От всички манийки, казани дотук, можем да твърдим, че B е комутативен пръстен с единица,… с което теоремата е доказана. □

Общ вид на полином

Следва да покажем връзката между понятието *полином*, което всички знаем от детството си и *манийките*, които учим

сега.

В следващите определения с B означаме множеството от всички финитни редици с елементи от даден комутативен пръстен с единица A.
...или пръстенът на полиномите над A (от предната теорема)

Нека $x = 0, 1, 0, 0, \dots$
Лесно (или не чак толкова лесно) се вижда, че $x^2 = x.x = 0, 0, 1, 0, 0, \dots$
Аналогично $x^3 = 0, 0, 0, 1, 0, 0, \dots$

По индукция се доказва, че
$x^n = \underbrace{0, 0, \dots, 0}_{n}, 1, 0, 0, \dots$

Това ще ни трябва след малко.

Определяме си следното множество:
$A_1 = \{a, 0, 0, 0, \dots \mid a \in A\}$

Очевидно $A_1 \subset B$

Сега си дефинираме следното изображение:
$\varphi : A \to A_1$

$\varphi(a) = a, 0, 0, \dots$

Забелязваме, че:
$\varphi(a + b) = a + b, 0, 0, \cdots = (a, 0, 0, \dots) + (b, 0, 0, \dots) = \varphi(a) + \varphi(b)$
и
$\varphi(ab) = ab, 0, 0, \cdots = (a, 0, 0, \dots).(b, 0, 0, \dots) = \varphi(a).\varphi(b)$

$\Longrightarrow \varphi$ е хомоморфизъм. Освен това е ясно, че φ е биекция

$\Longrightarrow \varphi$ е изоморфизъм $\Longrightarrow A \cong A_1 \subset B$

Т.е. можем накратно да означим
$A_1 \ni \alpha = a, 0, 0, \cdots = a \in A$

Сега, ако вземем един елемент $a \in A(A_1)$ (мислим за a като за финитна редица) и $f \in B$, то
$af = h \Longrightarrow h_s = \sum_{i=0}^{s} a_i f_{s-i}$, но $a_i = 0,\ \forall i > 0$

$\Longrightarrow h_s = af_s \Longrightarrow af = af_0, af_1, af_2, \dots$

$f \in B \Longrightarrow f$ е финитна $\Longrightarrow \exists n : f_{n+i} = 0$

$$= f_0, f_1, f_2, \cdots = (f_0, 0, 0, \dots) + (0, f_1, 0, 0, \dots) + \cdots + (0, 0, \dots, 0, f_n, 0, 0, \dots) = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n \quad (6)$$

Воала!
Вече знаем, че **всяка финитна редица е всъщност полином** (такъв, какъвто си го знаем)

Припомням:
f_0 - *свободен член*
$f_i x^i$ - *едночлен от i -та степен* (все пак има само един ненулев елемент в съответната финитна редица)

Интересното е, че B също е комутативен пръстен с единица, т.е. за него можем да направим същата процедура, както в

теоремата по-горе.
Така ще получим пръстен на полиномите на две променливи $A[x, y]$ и т.н.

$A \subset A[x] \subset A[x][y] \dots$

Степен на полином (дефиниция)

Нека $f \in B = A[x], \quad f = f_0, f_1, f_2, \dots$
Числото n наричаме **степен на полинома**, ако $f_n \neq 0$ и $f_{n+i} = 0,\ \forall i \in \mathbb{N}$

Означаваме:
$n = \deg f$

За тоталност на дефиницията означаваме $\deg 0 = -\infty$

Свойства на степените на полиномите

Нека $f, g \in B = A[x]$
Тогава:

1. $\deg (f+g) \leq \max\{\deg f, \deg g\}$
2. $\deg (f.g) \leq \deg f + \deg g$

Първото свойство е ясно. Ако събираме полиноми съответно от *m*-та и *n*-та степен. не можем да получим полином със степен,

по-голяма от по-голямата от двете степени.
Но пък ако *m* = *n* и коефициентите пред най-високата степен са противоположни елементи, съответно ще получим по-малка степен

на резултата.

Скрий

$f = 7x^5 + 102x^4 + 2x - 13$
$g = -7x^5 + 3$
$f + g = 102x^4 + 2x - 10$, т.е $\deg (f+g) = 4 < 5 = \max\{\deg f, \deg g\}$

Второто свойство не е чак толкова очевидно (даже хич)
Свикнали сме, степента на произведението на два полинома да е сума от степените им.

Скрий

$f = 3x^2 + 4$
$g = x^3$
$f.g = 3x^5 + 4x^3$, т.е. $\deg(f.g) = 5 = 3 + 2 = \deg f + \deg g$

Причината за "По-малко или равно" е, че в A можем да имаме делители на нулата, които да прецакат нещата.
Ето...
Скрий нагледния пример

Набелязваме си Z_6 - комутативен пръстен с единица.

$f = \bar{2}x + 1 \in Z_6[x]$
$g = \bar{3}x \in Z_6[x]$
$fg = \bar{2}.\bar{3}x^2 + \bar{3}x = \bar{6}x^2 + \bar{3}x = \bar{3}x$

$\deg fg = 1 < 2 = \deg f + \deg g$

Теорема за деление с частно и остатък на полиноми

Нека F е *поле* и $f,\ g \in F[x],\ g \neq 0$

Тогава $\exists!\ q, r \in F[x] :\ f = q.g + r,\ \deg r < \deg g$

Доказателство:

1. Съществуване

Провеждаме индукция по $n = \deg f$

I.
1. Ако $f = 0$, т.е това е случаят $n = -\infty$, то тогава $f = 0 = 0g + 0$
Тук имаме, че $q = 0,\ r = 0$

2. Ако $\deg f < \deg g$, то тогава $f = 0g + f$
т.е. $q = 0,\ r = f$

3. Ако $\deg f = 0 = \deg g$, тогава $f = g(fg^{-1}) + 0$
и $q = fg^{-1},\ r = 0$

Базата е доказана/показана.

II. Нека е доказано за всички полиноми $f:\ \deg f < n$

III. Нека $\deg f = n$
1. Ако $\deg f < \deg g$... виж I. 2.
2. Ако $\deg f \geq \deg g$

$f = f_0 + f_1 x + \cdots + f_n x^n$
$g = g_0 + g_1 x + \cdots + g_k x^k, \quad n \geq k$

Тук си харесваме следния полином:

$h = f_n {g_k}^{-1} x^{n-k} g$

Не е чак толкова неочивидно, понеже
като заместим g в записа на h получаваме следното:

$$h = f_n {g_k}^{-1} x^{n-k} g_0 + f_n {g_k}^{-1} x^{n-k} g_1 x + \cdots + \underbrace{f_n {g_k}^{-1} x^{n-k} g_k x^k}_{f_n x^n} \tag{7}$$

Т.е степента на h е n и, освен това, старшият коефициент е f_n
Затова логично е да си образуваме разликата:

$$s = f - h = f - f_n {g_k}^{-1} x^{n-k} g \tag{8}$$

Тъй като коефициентите пред най-високите степени на f и на h са противоположни елементи на полето F,
следва, че $\deg s < \deg f = n$

От индукционното допускане (II.), следва че

$\exists\, q_1,\ r_1:\ s = q_1 g + r_1,\ \deg r_1 < \deg g$

$$s = f - h = f - f_n {g_k}^{-1} x^{n-k} g = q_1 g + r_1 \implies f = \underbrace{(f_n {g_k}^{-1} x^{n-k} + q_1)}_{q(x)} g + \underbrace{r_1}_{r(x)},\ \deg r_1 < \deg g \tag{9}$$

Т.е получихме, че наистина съществуват полиноми $q,\ r$, такива, че $f = qg + r$ и $\deg r < \deg g$

2. Единственост

Допускаме, че
$f = gq_1 + r_1,\ \deg r_1 < \deg g$
$f = gq_2 + r_2,\ \deg r_2 < \deg g$

Като извадим двете равенства получаваме логичното:

$0 = g(q_1 - q_2) + r_1 - r_2 \iff g(q_1 - q_2) = r_2 - r_1$

Extra close brace or missing open brace ?

Ако $q_1 - q_2 \neq 0 \implies \deg\left(g(q_1 - q_2)\right) = \deg g + \deg\left(q_1 - q_2\right) \geq \deg g$

Надявам се всички видяхте *противоречието*.
Не може от двете страни на знака $=$ да има полиноми от различни степени.

$\implies q_1 - q_2 = 0 \iff q_1 = q_2 \implies r_1 = r_2$

Т.е. частното и остатъкът са единствени. □

Скрий примера

to be written

Обобщение на теоремата за деление с частно и остатък

Нека A е комутативен пръстен с единица.

$f,\ g \in A[x]$ и $\deg g = k$
т.е. $g = g_0, g_1, \ldots, g_k, 0, 0, \cdots = g_0 + g_1 x + \ldots g_k x^k$

и ако g_k е обратим елемент

$\Longrightarrow \exists!\ q, r \in A[x] : f = qg + r,\ \deg r < \deg g$

/* Няма да прилагам доказателство, понеже е същото както в частния случай (когато A е поле) */

Твърдение

Нека F е поле.

Нека $I \blacktriangleleft F[x]$ (I е идеал на пръстена на полиномите над полето F)

Тогава $\exists f \in F[x] :\ I = (f(x))$ (съществува елемент, който поражда идеала).

Или иначе: всеки идеал на пръстена на полиномите над дадено поле е главен.

Доказателство:

I. $I = \{0\} \Longrightarrow I = (0) \Longrightarrow ok!$

II. $I \neq \{0\}$
Нека $0 \neq d(x) \in I$ е полиномът с най-ниска степен.

Нека $f(x) \in I$ - произволен.
Разделяме $f(x)$ с частно и остатък на $d(x)$

$f(x) = q(x)d(x) + r(x),\ \deg r < \deg d$

$\Longrightarrow r(x) = \underbrace{f(x)}_{\in I} - \underbrace{d(x)q(x)}_{\in I} \Longrightarrow r(x) \in I$

Тъй като $d(x)$ е с минимална степен, а $\deg r < \deg d$ и $r \in I$, то $r(x) = 0$

$\Longrightarrow f(x) = q(x)d(x) \Longrightarrow f(x) \in (d(x)) \Longrightarrow I \subset (d(x))$
Очевидно е, че щом $d(x) \in I$, то $(d(x)) \subset I$

$\Longrightarrow I = (d(x))\ \square$

Забележка:
Ако F не е поле, твърдението **не** е вярно!

Скрий примера

Нека вземем *не*полето $\mathbb{Z}$ и нека $I \blacktriangleleft \mathbb{Z}[x]$

$I = (2) + (x) = \{f_0 + f_1 x + \cdots + f_n x^n \mid f_0 \equiv 0 \pmod 2\}$

Допускаме, че $I = (d)$
$\Longrightarrow d|2 \Longrightarrow \deg d = 0 \Longrightarrow d = 1\ or\ d = 2$

$d|x,\ 2 \nmid x \Longrightarrow d = 1$, но $(1) = \mathbb{Z}$, което е противоречие.

Принцип за сравняване на коефициентите

Нека F е поле.
Нека $f(x),\ g(x) \in F[x],\ \deg f \leq n,\ \deg g \leq n$

Ако $a_1, a_2, \ldots, a_n, a_{n+1} \in F$ са две по две различни помежду си (т.е $a_i = a_j \iff i = j$)) и такива, че:

$f(a_i) = g(a_i),\ 1 \leq i \leq n+1$, то $f(x) = g(x)$

Или, иначе казано, ако за два полинома със степени не по-големи от дадено фиксирано число **n** (най-често **n** е по-голямата от двете степени), намерим **n + 1** числа, такива, че стойностите на полиномите са равни, то те изцяло съвпадат.

Или, иначе казано, полином от степен **n** се дефинира от **n+1** точки

Доказателство:

Дефинираме си полинома $h(x) = f(x) - g(x)$
Очевидно $\deg h \leq n$

Освен това,
$h(a_i) = f(a_i) - g(a_i) = 0 \Longrightarrow (x - a_i) | h,\ i = 1, 2, \ldots, n+1$

Сега забелязваме, че $(x - a_i, x - a_j) = 1,\ a_i \neq a_j$

Скрий

Нека $(x - a_i, x - a_j) = d(x)$
$\Longrightarrow d | x - a_i \Longrightarrow d = c(x - a_i)$ или $d = c,\ c$ е константа.

Но, $d | x - a_j$ и $x - a_i \nmid x - a_j \Longrightarrow d = c$

Т.е най-големият общ делител на $x - a_i$ и $x - a_j$ е всяка константа.

За удобство си мислим, че $d(x) = 1$ - константата 1.

$$\Longrightarrow \underbrace{(x - a_1)(x - a_2) \ldots (x - a_{n+1})}_{\deg = n+1} | \underbrace{h(x)}_{\deg \leq n}$$

$$\Longrightarrow \underbrace{h(x)}_{\deg \leq n} = \underbrace{t(x)(x - a_1)(x - a_2) \ldots (x - a_{n+1})}_{\deg \geq n+1}$$

$$\Longrightarrow t(x) = 0 \Longrightarrow h(x) = 0$$

От дефиницията за $h(x)$ следва, че $f(x) = g(x)$. $\square$

Footnotes

1. цитирам Гугъл: Няма резултати за "финитна редица". За "крайна редица", обаче има доста :)

page revision: 14, last edited: 29 Jun 2011, 13:38 (738 days ago)