Делител на нулата (дефиниция)

Нека A е пръстен. Елементът $a \in A,\ a \neq 0$ наричаме *делител на нулата*, ако $\exists b \in A,\ b \neq 0 :\ ab = 0$

Област на цялост (дефиниция)

Нека A е комутативен пръстен с единица.

Ако A няма делители на нулата, казваме, че A е *област (на цялост)*.[1]

Примери:

Пример 1:
Множеството от целите числа $\mathbb{Z}$ е област на цялост.

Ако $a,\ b \in \mathbb{Z}$, знаем, че $ab = 0 \iff a = 0$ или $b = 0$, т.е. $\mathbb{Z}$ действително няма делители на нулата.
И също така знаем, че пръстенът на целите числа е комутативен пръстен.
$(a.b = b.a,\ \forall a,\ b \in \mathbb{Z})$

И, следователно, $\mathbb{Z}$ е област на цялост.

Пример 2:

Пръстенът с елементи множествата остатъци по модул 6, Z_6, **не** е област на цялост.

Това е така, тъй като, например, $\bar{2} \neq \bar{0}$ и $\bar{3} \neq \bar{0}$, но $\bar{2}.\bar{3} = \bar{6} = \bar{0}$.

Демек Z_6 има делители на нулата и, следователно, не е област.

Дефиниция (влагане)

Нека A е област на цялост и B е поле. Ако съществува изображение:

$$\varphi : A \to B \tag{1}$$

където φ е инекция и хомоморфизъм, то казваме, че областта на цялост A се влага в полето B.

Теорема

Нека $A \neq \varnothing$ е ненулева област на цялост.
Тогава съществува *поле*, в което A се влага.

Доказателство:

0. ***Идея***: Доказателството на теоремата е изключително дълго и глупаво. В смисъл, че се доказват много очевидни неща. Ключовото в такива доказателства е да разберете **основните стъпки** през които се минава. Веднъж запомните ли самите стъпки (мислете си го като междинните градове докато пътувате от София за Варна) можете сами да ги направите. Например стъпка от сорта - трябва да се докаже, че X е поле е тривиална - или ще използваме дефинициите за поле (това трябва да го знаем) или теоремката за подполе (т.е да докажем, че X е подполе на нещо друго). Проверката на самата дефиниция или необходимите условия за теоремата са сами по себе си тривиални - всеки може да ги направи по всяко време, не е нужно да се зубри ред по ред.
Та това доказателство ще протече в следните стъпки:

1. Ще си построим полето B. Всъщност това поле много прилича на полето $\mathbb{Q}$ - елементи имащи числител и знаменател, които обаче не са цели числа, а са от произволна обляст на цялост A. За да направим това трябва:
    1. да си построим 'всички дроби' (ще наричаме базово множество) - B_0
    2. да въведем еквивалентност между тях - т.е да дефинираме някак че $\frac{1}{2}$ и $\frac{2}{4}$ са едно и също нещо
    3. да построим множество B от *класовете на еквивалентност* на горната релация, и да въведем подходящи обратими операции за събиране и умножение
    4. да докажем, че така построеното множество с така въведените операции е поле
2. Ще докажем, че A се влага в B:
    1. ще си построим изображение $\varphi : A \to B$, ще докажем че е коректно
    2. ще докажем инекция (т.е на различни елементи съпоставяме различни)
    3. ще докажем хомоморфизъм (запазва операцията)

1. ***Построяване на поле*** B:
1.1 ***Построяване на базовото множество*** B_0:
Нека $\tilde{A} = A \setminus \{0\}$. Ще използваме $\tilde{A}$ за множеството, от което ще избираме *знаменатели* на нашите дроби (както знаете - знаменателите не могат да бъдат 0). Дефинираме си B_0 като скаларно произведение на A и $\tilde{A}$ (или по друг начин казано - множ. от наредени двойки с първи елемент от A и втори елемент от $\tilde{A}$):

$$\mathcal{Z}_0 = A \times \tilde{A} = \{(x,y) \mid x \in A,\ y \in \tilde{A}\} = \{(x,y) \mid x,y \in A,\ y \neq 0\} \tag{2}$$

1.2 ***Въвеждаме релация на еквивалентност в*** B_0:

1.2.0 **Дефиниция на релацията**

Нека (x,y) и (x_1,y_1) са произволни елементи от B_0. Казваме, че те са *еквивалентни*, ако $xy_1 = x_1y$. (За да се сещате по-лесно си мислете за дроби, и кога те са еднакви). Отбелязваме:

$$(x,y) \sim (x_1,y_1) \iff xy_1 = x_1y \tag{3}$$

1.2.1 **Доказателство, че е релация на еквивалентност**:

Ние хубаво я въведохме, но трябва да покажем, че $\sim$ наистина е *релация на еквивалентност*. Както добре знаем от курса по дискретна математика, релация на еквивалентност е просто една рефлексивна, симетрична и транзитивна релация. Ще докажем трите подред:

1.2.1.1 **Рефлексивност**:

Очевидно $(x,y) \sim (x,y)$, защото $xy = xy$.

1.2.1.2 **Симетричност**:

Ако $(x,y) \sim (x_1,y_1)$, тогава $xy_1 = x_1y$, следователно и $(x_1,y_1) \sim (x,y)$. (т.е от $(x,y) \sim (x_1,y_1) \Rightarrow (x_1,y_1) \Rightarrow (x,y)$).

1.2.1.3 **Транзитивност**:

Сега ще покажем, че ако $(x,y) \sim (x_1,y_1)$ и $(x_1,y_1) \sim (x_2,y_2)$, то $(x,y) \sim (x_2,y_2)$.

Имаме, че $xy_1 = x_1y$ и $x_1y_2 = x_2y_1$ (използвайки дефиницията и даденото). Умножаваме първото уравнение с $y_2 \neq 0$, а второто - с $y \neq 0$. Така получаваме, че $xy_1y_2 = x_1yy_2$ и $x_1y_2y = x_2y_1y$.

Тъй като A е комутативен пръстен $\Longrightarrow x_1yy_2 = x_1y_2y$ (просто разместваме буквите). Следователно и другите страни на равенството са еднакви: $xy_1y_2 = x_2y_1y$ или записано по друг начин $xy_1y_2 - x_2y_1y = 0$. Изнасяме y_1 пред скоби: $y_1xy_2 - y_1x_2y = y_1(xy_2 - x_2y) = 0$. И понеже, $y_1 \neq 0$ и в A няма делители на нулата, следователно $xy_2 - x_2y = 0$, т.е $xy_2 = x_2y$. Сега според дефиницията $(x,y) \sim (x_2,y_2)$, с което доказахме, че релацията е транзитивна.

От 1.2.1[1-3] следва, че $\sim$ е *релация на еквивалентност*.

1.3 ***Разбиване на класове на еквивалентност и въвеждане на подходящи операции***:

1.3.1 **Разбиване на класове**:

Пак от теорията за релации на еквивалентност имаме, че множество с такава релация се разбива на *класове на еквивалентност*, т.е елементите се разбиват на групички, като във всяка група елементите са еднакви помежду си (т.е елементите са в релацията $\sim$ помежду си). Ще бележим класовете на еквивалентност с квадратни скоби:

$$[x,y] = \{(a,b) \mid (a,b) \sim (x,y)\} \tag{4}$$

Време е да построим и множеството от самите класове на еквивалентност, т.е множество, в което всеки клас е елемент (нали не забравяте, че класовете са някаква съвкупност от еднакви елементи):

$$B = \{[x,y] \mid x,y \in A,\ y \neq 0\} \tag{5}$$

1.3.2 **Въвеждане на операции в B**:
Тъй като в следващата точка ще доказваме, че B е поле, първо ще трябва да дефинираме подходящи операции между елементите му:
1.3.2.1 **Събиране**:

$$[x,y] + [z,t] = [xt + zy, yt] \tag{6}$$

1.3.2.2 **Умножение**:

$$[x,y].[z,t] = [xz, yt] \tag{7}$$

1.3.3 **Бинарност и Коректност на операциите**:
Дефиницията на една операция, сама по себе си не ни дава нищо - трябва да докажем поне че е *бинарна* и *коректна*.
1.3.3.1 **Бинарност на операциите**: Ще докажем, че резултата от операциите винаги е от множеството B.
1.3.3.1.1 **Бинарност на събирането**: Не е трудно да се провери, че $xt + zy \in A$, ако $x,y,z,t \in A$, както и че $yt \neq 0$, защото имаме произведение на ненулеви елементи в област на цялост, следователно $xy + zt \in A \& yt \in \tilde{A}$, т.е $[xt + zy, yt] \in B$.
1.3.3.1.2 **Бинарност на умножението**: Аналогично $xz \in A$ и $yt \in \tilde{A}$, следователно $[xz, yt] \in B$.
1.3.3.2 **Коректност на операциите**:
Тъй като в случая имаме класове на еквивалентност, които бележим с произволен представител - т.е класа $[x,y]$, може да е абсолютно еднакъв с класа $[x_1, y_1]$, стига $(x,y) \sim (x_1, y_1)$ и точно за това трябва да покажем, че независимо от избора на представител за изобразяване на класа, горните две операции връщат един и същи резултат (т.е няма да се окаже, че $\frac{1}{2} + \frac{1}{2} = 1$, а пък $\frac{1}{2} + \frac{2}{4} = \frac{3}{8}$ примерно).
Ами нека да си изберем представителите (x_1, y_1) и (x_2, y_2) от класа $[x,y]$, както и $(z_1, t_1), (z_2, t_2)$ от класа $[z,t]$.
1.3.3.2.1 **Коректност на събирането**: Сега да пресметнем $[x,y] + [z,t]$ като използваме първо първите представители, после вторите:

(8)

$$[x_1,y_1]+[z_1,t_1]=[x_1t_1+z_1y_1,y_1t_1]$$
$$[x_2,y_2]+[z_2,t_2]=[x_2t_2+z_2y_2,y_2t_2]$$

Сега ще докажем, че $[x_1t_1+z_1y_1,y_1t_1]=[x_2t_2+z_2y_2,y_2t_2]$. Това е еквивалентно на $(x_1t_1+z_1y_1)(y_2t_2)=(x_2t_2+z_2y_2)(y_1t_1)$.

$$\begin{aligned}(x_1t_1+z_1y_1)(y_2t_2)&=(x_2t_2+z_2y_2)(y_1t_1)\iff\\ x_1t_1y_2t_2+z_1y_1y_2t_2&=x_2t_2y_1t_1+z_2y_2y_1t_1\iff\\ (x_1y_2-x_2y_1)t_1t_2&+(z_1t_2-z_2t_1)y_1y_2=0\impliedby\\ x_1y_2=x_2y_1&\quad z_1t_2=z_2t_1\iff\\ (x_1,y_1)\sim(x_2,y_2)&\quad(z_1,t_1)\sim(z_2,t_2)\end{aligned}\tag{9}$$

Обърнете внимание на предпоследния ред:стрелката следователно(не еквивалентно!!) е на обратно,за да имаме вярно твърдение.
Както виждате, ако вземем различни представители на един и същи клас получаваме, че сумата им също попада в един и същи клас. Следователно дефиницията на събирането е коректна.

1.3.3.2.2 **Коректност на умножението**:

$$\begin{aligned}[x_1,y_1].[z_1,t_1]&=[x_1z_1,y_1t_1]\\ [x_2,y_2].[z_2,t_2]&=[x_2z_2,y_2t_2]\end{aligned}\tag{10}$$

$$\begin{aligned}[x_1z_1,y_1t_1]&=[x_2z_2,y_2t_2]\iff\\ x_1z_1y_2t_2&=x_2z_2y_1t_1\iff\\ (x_1y_2)(z_1t_2)&=(x_2y_1)(z_2t_1)\impliedby\\ (x_1,y_1)\sim(x_2,y_2)&\quad(z_1,t_1)\sim(z_2,t_2)\end{aligned}\tag{11}$$

С това доказахме, че операциите събиране и умножение са бинарни (резултата е в B) и коректно дефинирани (при едни и същи аргументи връщат едни и същи резултати).

1.4 ***Доказателство, че B с така дефинираните операции е поле***:
Ще използваме дефиницията на поле, защото няма подходящо 'надполе', което да използваме (т.е да докажем някак си че сме му подполе).

скрии животното

Нека $[x,y],[z,t],[k,l]\in B$ - произволни три елемента.
1.4.1 **Операция събиране**: Ще докажем, че е асоциативна, комутативна, обратима, с неутрален елемент:
1.4.1.1 **Асоциативност**:

$$
\begin{aligned}
([x,y]+[z,t])+[k,l] &= [xt+zy,yt]+[k,l] \\
&= [(xt+zy)l+k(yt),ytl] \\
&= [xtl+zyl+kyt,ytl] \\
&= [x(tl)+(zl+kt)y,y(tl)] \\
&= [x,y]+[zl+kt,tl] \\
&= [x,y]+([z,t]+[k,l])
\end{aligned} \tag{12}
$$

1.4.1.2 **Комутативност**:

$$
\begin{aligned}
[x,y]+[z,t] &= [xt+zy,yt] \\
&= [zy+xt,ty] \\
&= [z,t]+[x,y]
\end{aligned} \tag{13}
$$

1.4.1.3 **Неутрален елемент**: Дефинираме си неутрален елемент да бъде класа на еквивалентност $[0,1]$. (проста проверка показва, че в него влизат всички представители от вида $(0,y)$, където $y \in \tilde{A}$). Сега да проверим, че изпълнява нужните изисквания за неутрален елемент:

$$
[x,y]+[0,1]=[x.1+0.y,y.1]=[x,y] \quad [0,1]+[x,y]=[0.y+x.1,1.y]=[x,y] \tag{14}
$$

1.4.1.4 **Противоположен елемент**: Ще докажем, че на произволен елемент $[x,y]$, противоположния му е $[-x,y]$ (където разбира се $-x$ е противоположния на x в областта на цялост A):

$$
\begin{aligned}
[x,y]+[-x,y]=[xy+(-x)y,yy]=[0,yy]=[0,1] \\
[-x,y]+[x,y]=[(-x)y+xy,yy]=[0,yy]=[0,1]
\end{aligned} \tag{15}
$$

1.4.2 **Операция умножение**: Ще докажем, че е асоциативна, комутативна, с неутрален елемент, с обратен елемент
1.4.2.1 **Асоциативност**:

$$
\begin{aligned}
([x,y].[z,t]).[k,l] &= [xz,yt].[k,l] \\
&= [(xz)k,(yt)l] \\
&= [x(zk),y(tl)] \\
&= [x,y].[zk,tl] \\
&= [x,y].([z,t].[k,l])
\end{aligned} \tag{16}
$$

1.4.2.2 **Комутативност**:

$$\begin{aligned}[x,y].[z,t] &= [xz,yt] \\ &= [zx,ty] \\ &= [z,t].[x,y]\end{aligned} \tag{17}$$

1.4.2.3 **Неутрален елемент**: Избираме си за неутрален елемент $[1,1]$. Разбира се този клас е същият като $[x,x]$, за произволно $x \in \tilde{A}$.

$$\begin{aligned}[x,y].[1,1] = [x.1, y.1] = [x,y] \\ [1,1].[x,y] = [1.x, 1.y] = [x,y]\end{aligned} \tag{18}$$

1.4.2.4 **Обратен елемент**: Ще докажем, че за произволен ненулев елемент $[x,y]$ (т.е $x \neq 0$), елемента $[y,x]$ му е обратен. Първо трябва да се уверим, че $[y,x] \in B$, но това е очевидно, защото $x,y \in \tilde{A}$:

$$\begin{aligned}[x,y].[y,x] = [xy,yx] = [1,1] \\ [y,x].[x,y] = [yx,xy] = [1,1]\end{aligned} \tag{19}$$

1.4.3 **Дистрибутивни закони**:

$$\begin{aligned}[x,y].([z,t]+[k,l]) &= [x,y].[zl+kt,tl] \\ &= [x(zl+kt),ytl] \\ &= [xzl+xkt,ytl] \\ &= [xzl,ytl]+[xkt,ytl] \\ &= [xz,yt]+[xk,yl] \\ &= [x,y].[z,t]+[x,y].[k,l] \\ ([z,t]+[k,l]).[x,y] &= [zl+kt,tl].[x,y] \\ &= [(zl+kt)x,tly] \\ &= [zlx+ktx,tly] \\ &= [zlx,tly]+[ktx,tly] \\ &= [zx,ty]+[kx,ly] \\ &= [z,t].[x,y]+[k,l].[x,y]\end{aligned} \tag{20}$$

С това доказахме (само чрез дефиниции), че B е поле. Ето защо е по-добре да се използват теоремите за подполе когато е възможно :)

2. ***Доказателство, че A се влага в B***:
Както се вижда ясно от дефиницията, нужно ни е инективно изображение от A към B, което е хомоморфизъм.
2.1 ***Дефиниране на изображението***:
Нека да си дефинираме изображението φ по следния начин:

$$\begin{aligned} \varphi &: A \to B \\ \varphi(a) &= [a, 1] \end{aligned} \tag{21}$$

На елемент от A съпоставяме елемент от B по следния начин:

$$\varphi(a) = [ax, x],\ x \in A \tag{22}$$

2.1.0 **Коректност на дефиницията**:

$$\begin{aligned} \varphi(a_1) = \varphi(a_2) &\iff \\ [a_1, 1] = [a_2, 1] &\iff \\ a_1.1 = a_2.1 &\iff \\ a_1 = a_2 &\iff \end{aligned} \tag{23}$$

2.2 **Инекция**: Трябва да докажем, че $a_1 \neq a_2 \iff \varphi(a_1) \neq \varphi(a_2)$. Това е абсолютно равносилно на $a_1 = a_2 \iff \varphi(a_1) = \varphi(a_2)$, което доказахме в 2.1.0 *коректност*.

2.3 **Хомоморфизъм**:

2.3.1 **Хомоморфизъм на събирането**:

$$\begin{aligned} \varphi(a_1 + a_2) &= [a_1 + a_2, 1] \\ &= [a_1.1 + a_2.1, 1.1] \\ &= [a_1, 1] + [a_2, 1] \\ &= \varphi(a_1) + \varphi(a_2) \end{aligned} \tag{24}$$

2.3.2 **Хомоморфизъм на умножението**:

$$\begin{aligned} \varphi(a_1 . a_2) &= [a_1 . a_2, 1] \\ &= [a_1 . a_2, 1.1] \\ &= [a_1, 1] . [a_2, 1] \\ &= \varphi(a_1) . \varphi(a_2) \end{aligned} \tag{25}$$

С това доказахме, че A се влага в B.

Footnotes

1. Искрен - област на цяло е комутативен пръстен **с** единица. Вижте в официалната уикипедиа (не че до сега нямаше примери за различия между Великова <-> wikipedia.org) и все пак :). Ползва се и във финалната стъпка от доказателството на огромната теорема.

page revision: 10, last edited: 29 Jun 2009, 12:35 (1468 days ago)