Характеристика

Дефиниция: Нека F е поле и e е произволен елемент от него, а k е естествено число. Тогава казваме, че:

$$\underbrace{e+e+\cdots+e}_{k}=ke \tag{1}$$

е *k-кратно на елемента e*.

Дефиниция (Характеристика)

Нека F е поле и $e \in F$ е произволен елемент в него. *Характеристика на поле* наричаме минималния брой пъти k които трябва да прибавим e със себе си така че да се получи 0 (минималното k, за което k-кратното на e е равно на 0).

$$ke=\underbrace{e+e+\cdots+e}_{k}=0 \tag{2}$$

Бележим $\operatorname{char} F = k$. Ако такова k не съществува (т.е колкото и пъти да прибавяме e със себе си винаги получаваме различно от 0), тогава казваме, че

характеристиката му е 0.

Забележка: По принцип характеристика се дефинира за *пръстен*. И елементът е не кой да е - а точно единицата на пръстена. Разбира се в нашите дефиниции пръстенът си няма единица. Според уикипедиа това въобще не е пръстен (Ring) ами е Rng (без *identity element*, *i*). Но както и да е :) Ако пръстенът има единица все пак тривиално се вижда (заради дистрибутивния закон), че горната дефиниция е еквивалентна на дефиницията, при която вместо e се използва именно единицата.

Теорема

Нека F е поле с ненулева характеристика : $\operatorname{char} F = k \neq 0$. Тогава k е просто число.

Доказателство: Ами да допуснем, че числото не е просто. Тогава съществува разлагане $k = m.s$ където $1 < m, s < k$. Тогава:

$$0 = k1 = \underbrace{1+1+\cdots+1}_{m.s} = \underbrace{(1+1+\cdots+1)}_{m}\underbrace{(1+1+\cdots+1)}_{s} = (m1).(s1) \qquad (3)$$

Т.е получихме, че $0 = (m1).(s1)$, при това $m1$ и $s1$ са различни от 0, защото k е най-малкото такова. Т.е получихме, че $m1$ и $s1$ са делители на 0, което очевидно е невъзможно в поле (или си обратим, или си делител на нулата - такива са законите на джунглата - в полетата няма място за делители на нулата :)).

Забележка 2: Много работи трябва да се забелязват тук - k-кратно на елемент е абсолютната помия, особено ако има и операция умножение наоколо. Като цяло ще гледаме да пишем точка, когато имаме умножение и без точка, когато имаме k-кратно. Например $m1$ е елемент от полето, защото сумираме краен брой пъти елементи, и сумата на 2 елемента е в полето (а не защото произведението на 2 елемента е в полето - просто тука няма произведение).

Просто поле

Дефиниция (Просто поле)

Просто поле ще наричаме поле, което няма собствени подполета.

Теорема

Всяко поле съдържа единствено просто подполе.
Доказателство: Нека F е поле, а $U = \{\mathbb{U}_1, \mathbb{U}_2, \mathbb{U}_3, \dots\}$ (U може да е безкрайно, ако F е поле с безкрайна характеристика) е множество, образувано от всички подполета на F. Да образуваме сечението на $\mathbb{U}_i$ (за - $i \in \{1, 2, 3, \dots\}$) да го обозначим с V (т.е $\cap\mathbb{U}_i = V$ - това са всички елементи, които участват едновременно във всички подполета на F). Ще докажем, че V е подполе:

$$a,b \in V \Rightarrow \begin{cases} a-b \in V & \forall a,b \in V \\ a^{-1} \in V & \forall a \neq 0 \\ ab \in V & \forall a,b \in V \end{cases} \tag{4}$$

Горните 3 твърдения следват непосредствено от доказаните в миналата глава свойства за поле (тук). Ако разсъждаваме за произволно подполе $X \in U$, тогава примерно $a-b \in X$ от твърдението приложено за полето X. Това е вярно за всяко подполе от U, следователно $a-b$ всъщност принадлени на сечението им - т.е на V.
Сега прилагаме в обратната посока същото твърдение за V и получаваме, че V е подполе на F.

Сега ако допуснем, че V не е просто подполе, ще излезе че съществува подполе на V - нека го наречем V', и разбира се $V' \subseteq V$. Но V' е подполе и на F, следователно $V' \in U$. Т.е получихме, че $\cap \mathbb{U}_i = V \subseteq V'$. Окончателно получаваме, че $V' = V$, т.е V няма същинско подполе, следователно V е просто подполе. Job done.

Теорема (класификация на простите полета)

Нека F е просто поле.

1. ако $\mathrm{char}\, F = 0$, следователно $F \cong \mathbb{Q}$
2. ако $\mathrm{char}\, F = p$, следователно $F \cong \mathbb{Z}_p$

Доказателство:
Само искам да вметна - тука яко се объркват умножението със k-кратното. Моля всеки читател да чете **внимателно** - ще пиша какво се опитваме да правим - ако някой не разбира може да пробва да си го разпише сам (стига разбира се да знае какво се опитваме да докажем).

1. $\mathrm{char}\, F = 0 \Longrightarrow F \cong Q$
Щом ще доказваме изоморфизъм на две полета се нуждаем от **функция** (още - изображение) между 2^те^ множества, която е едновременно **биекция** и **хомоморфизъм**.
1.1 ***Функцията***
Нека $\varphi : \mathbb{Q} \to F$ е такава, че:

$$\varphi\left(\frac{m}{n}\right) = (m1).(n1)^{-1} \tag{5}$$

1.1.1 ***Коректност на функцията***
Ние хубаво я дефинирахме, ама сега трябва да докажем, че дефиницията е коректна - т.е че $\varphi(a) = \varphi(b)$, когато $a = b$ (т.е ако подаваме еднакви аргументи на функцията очакваме да получим еднакви резултати). Тук става интересно, защото

едно рационално число $\frac{m}{n}$ може да бъде записано по няколко начина - примерно $\frac{1}{2} = \frac{2}{4}$. Трябва да докажем именно, че различни записи на числото биха дали еднакви стойности на функцията (защото очевидно функцията зависи от това кой запис е избран (или поне така изглежда на пръв поглед)).
Да проверим кога две функционални стойности съвпадат. Нека

$$\begin{aligned} \varphi\left(\frac{m}{n}\right) &= (m1).(n1)^{-1} \\ \varphi\left(\frac{a}{b}\right) &= (a1).(b1)^{-1} \\ (m1).(n1)^{-1} &\stackrel{?}{=} (a1).(b1)^{-1} \end{aligned} \tag{6}$$

Ще запишем с поредица от еквивалентности:

$$\begin{aligned} (m1).(n1)^{-1} = (a1).(b1)^{-1} &\iff \\ (m1).(b1) = (a1).(n1) &\iff \\ ((m.b)1) = ((a.n)1) &\iff \\ (m.b - a.n)1 = 0 &\iff \\ m.b - a.n = 0 &\iff \\ m.b = a.n \end{aligned} \tag{7}$$

Тук използвахме комутативността на полето (първи ред) и още някои очевидни неща свързани с кратност на елемент.
Сега вече не е трудно да се види, че

$$\frac{m}{n} = \frac{a}{b} \iff m.b = a.n \iff \varphi\left(\frac{m}{n}\right) = \varphi\left(\frac{a}{b}\right) \tag{8}$$

С това доказахме коректността на функцията. Ако още спите - доказахме и че е **инективна** (използваме горната връзка в обратната посока).
1.2 ***Хомоморфизъм***
Всъщност трябва да докажем следните работи:

$$\begin{aligned} \varphi(x+y) &= \varphi(x) + \varphi(y) \\ \varphi(xy) &= \varphi(x)\varphi(y) \end{aligned} \tag{9}$$

за произволни $x, y \in \mathbb{Q}$. Ще караме подред, без паника
1.2.1 ***Хомоморфизъм на събирането***:
Ще разпишем $\varphi\left(\frac{m}{n} + \frac{a}{b}\right)$, като целта ще бъде да го добутаме до $\varphi\left(\frac{m}{n}\right) + \varphi\left(\frac{a}{b}\right)$.

Затегнете колани:

$$\begin{aligned}\varphi\left(\frac{m}{n}+\frac{a}{b}\right) &= \varphi\left(\frac{m.b+a.n}{n.b}\right) \\ &= ((m.b+a.n)1).((n.b)1)^{-1} \\ &= [((m.b)1)+((a.n)1)][(n1).(b1)]^{-1} \\ &= [(m1).(b1)+(a1).(n1)][(b1)^{-1}.(n1)^{-1}] \\ &= (m1).(b1).(b1)^{-1}.(n1)^{-1}+(a1).(n1).(b1)^{-1}.(n1)^{-1} \\ &= (m1).(n1)^{-1}+(a1).(b1)^{-1} \\ &= \varphi\left(\frac{m}{n}\right)+\varphi\left(\frac{a}{b}\right)\end{aligned} \tag{10}$$

Не случайно ни наричат ФМИ - Факултет по Магичните Изкуства ;-)

1.2.2 ***Хомоморфизъм на умножението***:

Сега пък ще разпишем $\varphi\left(\frac{m}{n}.\frac{a}{b}\right)$, като целта ще бъде да го добутаме до $\varphi\left(\frac{m}{n}\right).\varphi\left(\frac{a}{b}\right)$. Ще го разпишем ама друг път! Я сядай и си го разписвай сам!

1.3 ***Биекция***

1.3.1 ***Инекция***

Доказателството на инекция е същото, като доказателството за коректност (или поне в доказателството за коректност правим и доказателство за инекция :)) - виж 1.1.1

1.3.2 ***Сюрекция***

Тук ще играем малко нечестно. Ще докажем, че $\operatorname{Im}\varphi = F_1 \equiv F$. Ами от хомоморфизма и очевидната биекция между $\mathbb{Q}$ и F_1, заключваме, че $\mathbb{Q} \cong F_1$, следователно F_1 е поле. Освен това, от $\operatorname{Im}\varphi \subseteq F$ имаме, и че F_1 е подмножество на F. Т.е получихме, че F_1 е подполе на F. Е да, ама F няма същински подполета, следователно $F_1 \equiv F$.[1]

С това изоморфизмът между F и $\mathbb{Q}$ е доказан.

2 . $\operatorname{char} F = p \neq 0 \Longrightarrow F \cong \mathbb{Z}_p$

Тук доказателството ще въврви по подобен начин на горното. Ще създадем функция, между 2^ге полета и ще докажем **биекция** и **хомоморфизъм**:

2.1 ***Функцията***

Дефинираме функцията ψ по следния начин:

$$\psi : \mathbb{Z}_p \to F \quad \psi(\bar{a}) = \underbrace{1+1+\cdots+1}_{a} = a1 \tag{11}$$

2.1.1 ***Коректност на функцията***

Разбира се трябва да докажем, че функцията е дефинирана коректно. Поради

естеството на доказателството парчето текст(/код :)) което пише тук ще се използва и при доказателството за ***инективност***. Да разпишем с еквивалентности $\psi(\bar{a}) = \psi(\bar{b})$:

$$\begin{aligned} \psi(\bar{a}) = \psi(\bar{b}) &\iff \\ a1 = b1 &\iff \\ |a-b|1 = 0 &\iff \\ p \ / \ a-b & \\ a \equiv b \pmod{p} &\iff \\ \bar{a} = \bar{b} & \end{aligned} \tag{12}$$

в правата посока ($\Rightarrow$) това е доказателство за инекция, в обратната посока ($\Leftarrow$) това е доказателство за коректност на функцията.

2.2 ***Хомоморфизъм***

Сега ще докажем, че функцията ψ всъщност е хомоморфизъм (запазва операциите), което ще е ключовото и при доказателството на сюрективност (ще видиш по-долу).

2.2.1 ***Хомоморфизъм на събирането***

Сега трябва да добутаме $\psi(\bar{a} + \bar{b})$ до $\psi(\bar{a}) + \psi(\bar{b})$:

$$\begin{aligned} \psi(\bar{a} + \bar{b}) &= \psi(\overline{a+b}) \\ &= (a+b)1 \\ &= a1 + b1 \\ &= \psi(\bar{a}) + \psi(\bar{b}) \end{aligned} \tag{13}$$

Тук просто използвахме очевидно свойство на k-кратното.

2.2.2 ***Хомоморфизъм на умножението***

Сега пък блъскаме $\psi(\bar{a}.\bar{b})$ докато не заприлича на $\psi(\bar{a}).\psi(\bar{b})$:

$$\begin{aligned} \psi(\bar{a}.\bar{b}) &= \psi(\overline{a.b}) \\ &= (a.b)1 \\ &= (a1).(b1) \\ &= \psi(\bar{a}).\psi(\bar{b}) \end{aligned} \tag{14}$$

както виждате пак използваме тривиално свойство на k-кратното.

2.3 ***Биекция***

2.3.1 ***Инекция***

Виж 2.1.1

2.3.2 ***Сюрекция***

Да разгледаме функцията върху $H = \operatorname{Im}\psi : \psi : \mathbb{Z}_p \to \operatorname{Im}\psi$. Очевидно всичко доказано до сега важи за нея, освен това е и сюрективна. Сега ще докажем, че H е поле.

Достатъчно е да проверим, че $a+(-b) \in H$, $a^{-1} \in H$ и $a.b \in H$ при $a,b \in H$ произволни. Разбира се операциите събиране, умножение взимане на обратен и противоположен, са същите, дефинирани в F. Ами щом $a,b \in H = \operatorname{Im} \psi$, то съществуват първообрази a', b', такива че $\psi(a') = a$ и $\psi(b') = b$. Тогава:

1. $a+(-b) = \psi(a') - \psi(b') = \psi(a'-b') \in \operatorname{Im} \psi = H$ - използваме хомоморфизма
2. $a^{-1} = \psi(a')^{-1} = \psi(a'^{-1}) \in H$ - отново хомоморфизъм
3. $a.b = \psi(a').\psi(b') = \psi(a'.b') \in H$ - от теоремата на Моор и законите за междупланетен свръхсветлинен превоз с понита.

Както виждате необходимите и достатъчни условия за подгрупа са изпълнени, и следователно $H < F$. Е да ама F е просто поле (не е ходило в университет) следователно $E \equiv F$. Така показахме, че ψ е сюрективна.

That's all folks!

Footnotes

1. бе тука го правим малко по-кратко от доказателството дадено на лекции. Подполе сме дефинирали като поле със същите операции. Е мисля че може да го докараме, като използваме хомоморфизма до дупка - но като цяло даже на мен ми е малко мъгла (някой да го преработи тоя параграф че съвсем заспах)

page revision: 8, last edited: 27 Jun 2012, 20:43 (374 days ago)