Характеристика на поле. Прости полета.

Разглеждаме произволно (не непременно числово) поле F с единичен елемент 1_F. Възможни са следните два случая:

1. Ако $m, n \in \mathbb{Z}$ са такива числа, че $m \neq n$, то да имаме $m.1_F \neq n.1$, където $m.1_F$ означава просто $\underbrace{1_F + 1_F + \cdots + 1_F}_{m \text{ пъти}}$. В такъв случай казваме, че полето F има *характеристика* 0 и пишем $\operatorname{char} F = 0$.

2. Ако съществуват $m, n \in \mathbb{Z}$, такива че $m \neq n$, но $m.1_F = n.1_F$. Ако без ограничение смятаме, че $m > n$, то последното равенство ни дава $(m-n).1_F = 0_F$ и $m - n \in \mathbb{N}$. Нека p е най-малкото естествено число, за което $p.1_F = 0_F$. Тогава казваме, че полето F има *характеристика* p и пишем $\operatorname{char} F = p$.

Примери:

1. За числовите полета $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ равенството $m.1 = n.1$ за $m, n \in \mathbb{Z}$ е изпълнено единствено при $m = n$ и следователно $\operatorname{char} F = 0$.

2. Нека $p \in \mathbb{N}$ е просто число. Тогава пръстенът от класовете остатъци

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$$

е поле, в което е изпълнено $p.\overline{1} = \overline{p} = \overline{0}$, а за $k : 1 \leq k \leq p-1$ имаме, че $k.\overline{1} = \overline{k} \neq \overline{0}$, т.к. $p \nmid k$. Оттук виждаме, че $\operatorname{char} \mathbb{Z}_p = p$.

Твърдение 1. *Нека F е произволно поле с характеристика* $\operatorname{char} F = p$. *Тогава p е просто число.*

Доказателство. $\operatorname{char} F = p$ означава, че p е най-малкото естествено число, за което $p.1_F = 0_F$. Да допуснем, че p е съставно. Това означава, че

съществуват числа $m, n \in \mathbb{N}$, такива че $m < p, n < p$ и $p = mn$. Тогава имаме, че $mn.1_F = 0_F$ или $(m.1_F)(n.1_F) = 0_F$. Тъй като F е поле, в него няма делители на нулата и следователно или $m.1_F = 0_F$, или $n.1_F = 0_F$. Но $m < p$ и $n < p$ и това би противоречало на минималността на избора на p. Следователно остава да е вярно, че числото p е просто. □

Нека F е поле с характеристика $\operatorname{char} F = p$. Ако $a \in F$ и числото $n \in \mathbb{Z}$ е такова, че $p \mid n$, то $n.a = 0_F$. Наистина, $p \mid n$ означава, че $\exists m \in \mathbb{Z}$, такива че $n = pm$. Тогава $n.a = pm.a = mp.1_F.a = m.(p.1_F).a = m.0_F.a = 0_F$. По-общо, нека $a \in F$ е ненулев елемент, т.е. $a \neq 0_F$, и $n \in \mathbb{Z}$. Тогава,

(1) ако $\operatorname{char} F = 0$, то $n.a = 0_F \Leftrightarrow n = 0$;

(2) ако $\operatorname{char} F = 0$, то $n.a = 0_F \Leftrightarrow p \mid n$.

Твърдение 2. *Нека F е поле с характеристика $\operatorname{char} F = p \neq 0$. Тогава за всеки два елемента $a, b \in F$ е изпълнено*

$$(a + b)^p = a^p + b^p$$

или по-общо

$$(a + n)^{p^m} = a^{p^m} + b^{p^m}$$

за всяко естествено число $m \in \mathbb{N}$.

Доказателство. Вече видяхме, че ако $c \in F$, а $n \in \mathbb{Z}$ е такова, че $p \mid n$, то $n.c = 0_F$. По формулата за нютонов бином имаме, че

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \cdots + \binom{p}{p-1} ab^{p-1} + b^p.$$

Понеже $\binom{p}{i} = \dfrac{p!}{i!(p-i)!} = \dfrac{p(p-1)\ldots(p-i+1)}{i!}$ за $i = 1, 2, \ldots, p-1$, то всеки един от биномните коефициенти в горното равенство се дели на p и оттам $\binom{p}{i} a^{p-i}b^i = 0_F$ за $i = 1, 2, \ldots, p-1$. По този начин остана

$$(a + b)^p = a^p + b^p.$$

Останалата част от твърдението се доказва лесно с индукция по m, чиято основа току-що установихме. □

Нека F е поле, а $K \subset F$ е неово подмножество, такова че $|K| \geq 2$. Казваме, че K е *подполе* на F, ако за $\forall a, b \in K$ е изпълнено, че $a+b, a-b, ab$ и $ab^{-1} = \frac{a}{b}$ за $b \neq 0_F$ също принадлежат на K. От тази дефиниция лесно следва, че $0_F \in K, 1_F \in K$ и че разглеждано само по себе си K също е поле спрямо операциите, наследени от F. Означаваме $K \leq F$. Друг начин да изкажем същия факт е да заявим, че полето F е *разширение* на полето K и да запишем $F \geq K$. Ако $K \leq F$, то $\operatorname{char} K = \operatorname{char} F$.

Нека F е поризволно поле. Ще казваме, че полето F е *просто*, ако F няма никакви подполета освен себе си. (За да няма объркване ще отбележим, че подпръстена $\{0_F\}$ на пръстена F няма как да образува подполе, т.к. се състои само от един елемент.)

Твърдение 3. *Полетата $\mathbb{Q}$ и $\mathbb{Z}_p$, където p е просто число, са прости полета.*

Доказателство. Относно $\mathbb{Q}$: Нека $K \leq \mathbb{Q}$е подполе на $\mathbb{Q}$. По дефиниция трябва $|K| \geq 2$ и тогава съществува елемент $a \in K$, който е ненулев. Тогава $a - a = 0 \in K$ и $\frac{a}{a} = 1 \in K$. Освен това за $\forall n \in \mathbb{N}$ имаме, че $\underbrace{1+1+\cdots+1}_{n \text{ пъти}} = n \in K$ и $0 - n = -n \in K$. По този начин всъщност се оказва, че $\mathbb{Z} \subseteq K$. Нека $r \in \mathbb{Q}$. Тогава r се записва като $\frac{m}{n}$ за $m, n \in \mathbb{Z}, n \neq 0$. Но това означава, че $m, n \in K$, а оттам и $\frac{1}{n} \in K$. Следователно $m \cdot \frac{1}{n} = \frac{m}{n} \in K$, т.е. $r \in K$, което всъщност показва, че $\mathbb{Q} \subseteq K$. Но така $K = \mathbb{Q}$, откъдето следва, че полето $\mathbb{Q}$ е просто, защото съдържа само себе си като подполе.

Относно $\mathbb{Z}_p$: Нека K е подполе на $\mathbb{Z}_p$. Тогава $\overline{0}, \overline{1} \in K$. Също така за $\forall k \in \mathbb{N}, 1 \leq k \leq p-1$ имаме, че $\underbrace{\overline{1}+\overline{1}+\cdots+\overline{1}}_{k \text{ пъти}} = \overline{k} \in K$. Но това означава всъщност, че $\mathbb{Z}_p \subseteq K$ и така $K = \mathbb{Z}_p$. По този начин се вижда, че $\mathbb{Z}_p$ е просто поле. □

Твърдение 4. *Всяко поле F съдържа, при това едно единствено просто подполе F_0.*

Доказателство. Ясно е, че всяко поле F, съдържа подполе K, например при $K = F$ имаме тривиалното подполе $F \leq F$. Тогава можем да образуваме F_0 като сечението на всички подполета на F, т.е. $F_0 = \bigcap_{K \leq F} K$.

Тогава F_0 също е подполе на F. Да видим, че F_0 е просто поле. Наистина, ако L е подполе на F_0, то $L \leq F_0 \leq F$ е подполе и на F и следователно участва в сечението на всички подполета на F, т.е. $F_0 \subseteq L$. Но последното означава, че $F_0 = L$, което доказва, че полето F_0 е просто и като такова е поросто подполе на F. Ще докажем, че F_0 е единственото просто подполе. Нека F_1 е просто подполе на F. Тогава то участва в сечението на всички подполета и следователно $F_1 \supseteq F_0$. Така F_0 е подполе на F_1, но по предположение то е просто и остава $F_0 = F_1$. Така F_1 е единствено. $\square$

Нека R и R' са пръстени. Казваме, че изображението

$$\varphi : R \longrightarrow R'$$

е *хомоморфизъм на пръстени*, ако е изпълнено $\varphi(x + y) = \varphi(x) + \varphi(y)$ и $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

Свойства:
1. $\varphi(0_R) = 0_{R'}$.
2. $\varphi(-a) = -\varphi(a)$ за $\forall a \in R$.
3. Нека R е пръстен с единица 1_R и φ не е нулевото изображение. Тогава $\varphi(1_R) = 1_{R'}$ и за обратим елемент $a \in R$ е в сила, че $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

Ако хомоморфизмът на пръстени φ е и биекция на R върху R', то φ е *изоморфизъм на пръстени*, а R и R' са изоморфни пръстени и пишем $R \cong R'$.

Да отбележим, че ако R е област, то за $a, b, c \in R, c \neq 0_R$ е изпълнено $ac = bc \Leftrightarrow a = b$. Наистина, $ac = bc \Leftrightarrow (a - b)c = 0_R$. Т.к. R е област и $c \neq 0_R$, то остава $a - b = 0_R$, което означава, че $a = b$.

Следващата теорема класифицира простите полета.

Теорема. *Нека F е просто поле. Ако* $\operatorname{char} F = 0$, *то $F \cong \mathbb{Q}$. Ако* $\operatorname{char} F = p \neq 0$, *то $F \cong \mathbb{Z}_p$.*

Доказателство. Нека F е просто поле с $\operatorname{char} F = 0$. Знаем, че

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid n, m \in \mathbb{Z}, n \neq 0 \right\}.$$

Ако $n \in \mathbb{Z}, n \neq 0$, то $n.1_F \neq 0_F$. Разглеждаме подмножеството

$$F_0 = \{(m.1_F)(n.1_F)^{-1} \mid m, n \in \mathbb{Z}, n \neq 0\} \subseteq F.$$

То притежава следните свойства:

1. $(m.1_F)(n.1_F)^{-1} = (k.1_F)(l.1_F)^{-1}$ за $k, l \in \mathbb{Z}, l \neq 0 \Leftrightarrow ml = kn$. Наистина, умножаваме двете страни на равенството с $(n.1_F)(l.1_F) \neq 0_F$ и получаваме $(m.1_F)(l.1_F) = (k.1_F)(n.1F)$, т.е. $(ml).1_F = (kn).1_F$. Сега, т.к. $\operatorname{char} F = 0$ имаме, че просто $ml = kn$.

2. $(m.1_F)(n.1)F)^{-1} \pm (k.1_F)(l.1_F) = [(ml \pm kn).1_F][(nl).1_F]^{-1}$.

3. $(m.1_F)(n.1_F)^{-1} \cdot (k.1_F)(l.1_F)^{-1} = [(mk).1_F][(nl).1_F]^{-1}$.

4. Ако $m \neq 0$, то $[(m.1_F)(n.1_F)^{-1}]^{-1} = (n.1_F)(m.1_F)^{-1}$. Наистина, т.к. $m \neq 0$, то $m.1_F \neq 0_F$ и следователно $\exists (m.1_F)^{-1}$. Сега свойството следва от директната проверка, че $(m.1_F)(n.1_F)^{-1} \cdot (n.1_F)(m.1_F)^{-1} = 1_F$.

Свойства 2, 3 и 4 ни дават, че за всеки два елемента$a, b \in F_0$ елементите $a + b, a - b, ab$ и a^{-1} при $a \neq 0_F$ също принадлежат на F_0. По този начин F_0 е подполе на F, но т.к. F е просто, то $F = F_0$.

Да разгледаме изображението

$$\varphi : F \longrightarrow \mathbb{Q},$$

дефинирано с $\varphi[(m.1_F)(n.1_F)^{-1}] = \dfrac{m}{n}$. То е коректно зададено, защото ако $(k.1_F)(l.1_F)^{-1} = (m.1_F)(n.1_F)^{-1}$, то свойство 1 ни дава, че $kn = lm$ или $\dfrac{k}{l} = \dfrac{m}{n}$. Така $\varphi[(k.1_F)(l.1_F)^{-1}] = \dfrac{k}{l} = \dfrac{m}{n} = \varphi[(m.1_F)(n.1_F)^{-1}]$, т.е. на всеки елемент $a \in F$ е съпоставен единствен елемент $\varphi(a) \in \mathbb{Q}$.

Свойства 2 и 3 ни дават, че за $\forall a, b \in F$е изпълнено $\varphi(a + b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$, т.е. φе хомоморфизъм на пръстени.

Освен това φ е биекция на F върху $\mathbb{Q}$. Наистина, за всяко число $\dfrac{m}{n} \in \mathbb{Q}$ съществува елемент $(m.1_F)(n.1_F)^{-1} \in F$, такъв че $\dfrac{m}{n} = \varphi[(m.1_F)(n.1)F)^{-1}]$; ако $\varphi[(m.1_F)(n.1_F)^{-1}] = \varphi[(k.1_F)(l.1_F)^{-1}]$, то $\dfrac{m}{n} = \dfrac{k}{l}$, т.е. $lm = kn$ и според свойство 1 получаваме, че $(m.1_F)(n.1_F)^{-1} = (k.1_F)(l.1_F)^{-1}$.

Така φ е изоморфизъм на пръстени и $F \cong \mathbb{Q}$.

Нека сега F е просто поле с характеристика $\operatorname{char} F = p \neq 0$. Тогава числото p е просто и имаме полето от остатъци

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}.$$

Разглеждаме подмножеството

$$F_0 = \{0, 1_F, 2.1_F, \ldots, (p-1).1_F\} \subseteq F.$$

Нека $n \in \mathbb{Z}$ е произволно число. Тогава $n = pt + r$ за $t, r \in \mathbb{Z}$ и $0 \leq r \leq p-1$ според теоремата за деление с частно исотатък. Сега $n.1_F = t(p.1_F) + r.1_F = t.0_F + r.1_F = r.1_F \in F_0$ (понеже $0 \leq r \leq p-1$). По този начин $n.1_F \in F_0$ за $\forall n \in \mathbb{Z}$ и сега следва, че $\forall a, b \in F_0$ е изпълнено $a+b, a-b, ab \in F_0$. Нека $\overline{k} \neq \overline{0}$, т.е. $1 \leq k \leq p-1$ i razgledame $k.1_F \in F_0$. Имаме, че $(k,p) = 1$ и тъждеството на Безу ни дава, че съществуват числа $u, v \in \mathbb{Z}$, такива че $uk + vp = 1$. Следователно в F имаме, че $(uk + pv).1_F = 1_F$ и разписвайки лявата страна получаваме последователно $(u.1_F)(k.1_F) + (v.1_F)(p.1_F) = (u.1_F)(k.1_F) + 0_F = (u.1_F)(k.1_F) = 1_F$ или с други думи $(k.1_F)^{-1} = (u.1_F) \in F_0$, защото $u \in \mathbb{Z}$. По този начин доказахме, че за всеки ненулев елемент $a \in F_0$ е изпълнено $a^{-1} \in F_0$ и F_0 се оказва подполе на F. Простотата на F обаче води до $F = F_0$.

Да разгледаме изображението

$$\varphi : F \longrightarrow \mathbb{Z}_p,$$

дефинирано с $\varphi(k.1_F) = \overline{k}$. Очевдино е, че φ е хомоморфизъм на пръстени, а и биекция на F върху $\mathbb{Z}_p$. Така φ е изоморфизъм на пръстени и $F \cong \mathbb{Z}_p$. □

Следствие 1. *Всяко поле F има, при това единствено просто подполе F_0, такова че $F_0 \cong \mathbb{Q}$, ако* $\operatorname{char} F = 0$ *или $F_0 \cong \mathbb{Z}_p$, ако* $\operatorname{char} F = p \neq 0$.