Характеристика на поле и поле от частни

Сайт: learn.fmi.uni-sofia.bg
Курс: Алгебра 2, поток 1, летен семестър 2021/2022
Книга: Характеристика на поле и поле от частни

Разпечатано от: Мартин Попов
Дата: Saturday, 16 April 2022, 13:47

Съдържание

1. Характеристика

За да се дефинира характеристика на поле е необходимо да разгледаме понятието кратност на елементи от полето.

Нека F е поле, $a \in F$ и $k \in \mathbb{Z}$, тогава k кратно на елемента a се записва ka и се дефинира по следния начин

$$ka = \begin{cases} \underbrace{a + \ldots + a}_{k}, & \forall k \geq 1 \\ 0, & k = 0 \\ \underbrace{(-a) + \ldots + (-a)}_{|k|}, & k < 0 \end{cases}$$

Въпреки, че записът ka напомня за произведение на два елемента, да не забравяме, че ka не е умножението в полето, първият елемент в този запис е цяло число, а вторият е елемент на полето. Когато има опасност от объркване при това записване, може да означим k кратно на елемента a като $k(a)$.
Например, в полето $\mathbb{Z}_5$ е изпълнено следното:

$$\begin{aligned} 3(\bar{1}) &= \bar{1} + \bar{1} + \bar{1} = \bar{3}, \\ 55(\bar{1}) &= \underbrace{\bar{1} + \ldots + \bar{1}}_{55} = \bar{0}, \\ -43(\bar{1}) &= \underbrace{\bar{4} + \ldots + \bar{4}}_{43} = \bar{2}. \end{aligned}$$

От свойствата на степените, които в случая на елементи на адитивната група на полето са свойства на кратните елементи, знаем че е изпълнено $(k+s)a = ka + sa$ и $k(s(a)) = (k.\, s)a$.

1.1. Определение

Определение:
Казваме, че полето F има характеристика k, ако k е минималното естествено число, за което единичния елемент на полето $1 \in F$ изпълнява равенството

$$k1 = k(1) = \underbrace{1 + \ldots + 1}_{k} = 0.$$

записваме този факт с $\mathtt{char}(F) = k$.
Ако за всяко естествено число k е изпълнено

$$k1 = k(1) = \underbrace{1 + \ldots + 1}_{k} \neq 0,$$

тогава казваме, че полето F има характеристика 0 и записваме $\mathtt{char}(F) = 0$.

Примери:
За реалното число 1 е изпълнено $k1 = k \neq 0, \forall k \in \mathbb{N}$ и поради тази причина е изпълнено, че характеристиката на полето на реалните числа е равна на $0 = \mathtt{char}(\mathbb{R})$.

Известно е, че $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ е поле точно когато p е просто число и от $p(\overline{1}) = \underbrace{\overline{1} + \ldots + \overline{1}}_{p} = \overline{0}$, установяваме, че p е минималното естествено число, за което $p(\overline{1}) = \overline{0}$, затова характеристиката на това поле е равна на $p = \mathtt{char}(\mathbb{Z}_p)$.

Забележка:
Ако L и F са полета и $L < F$ е подполе на F, тогава 1 е общ елемент за двете полета и затова характеристиките на тези полета са равни $\mathtt{char}(L) = \mathtt{char}(F)$.

1.2. Свойства -1

Твърдение:
Нека F е поле с ненулева характеристика $k = \mathtt{char}(F) \neq 0,$ тогава характеристиката на F е просто число.
Доказателство:
Допускаме, че $k = \mathtt{char}(F)$ е съставно число и $k = m.\,s,\ \ 1 < m < k,\ \ 1 < s < k.$ В полето F е изпълнено равенството

$$\begin{aligned} 0 = k1 &= \underbrace{1 + \cdots + 1}_{m.s} = \underbrace{(\underbrace{1 + \cdots + 1}_{m}) + \ldots + (\underbrace{1 + \cdots + 1}_{m})}_{s} = \\ &= \underbrace{m1 + \cdots + m1}_{s} = (m1).(\underbrace{1 + \cdots + 1}_{s}) = \\ &= (m1).(s1) \end{aligned}$$

Числото k е характеристиката на полето и е минималното естествено число със свойството $k1 = 0.$ Следователно $m1 \neq 0$ и $s1 \neq 0$, и от написаното равенство, получаваме че $(m1).(s1) = 0$ р т.е. $m1$ и $s1$ са делители на нулата. Това е в противоречие с твърдението, че в полетата няма делители на нулата.
По този начин се получи, че характеристиката k на полето трябва да бъде просто число.

□

От написания пример виждаме, че за всяко p полето $\mathbb{Z}_p$ има p, така че характеристиките на полетата са точно числата 0 и всички прости числа.

Твърдение:
Нека F е поле с ненулева характеристика $p = \mathtt{char}(F) \neq 0,$ тогава е изпълнено $pa = 0$, за всяко $a \in F.$
Доказателство:

$$pa = \underbrace{a + \ldots + a}_{p} = \underbrace{a.1 + \ldots + a.1}_{p} = a(\underbrace{1 + \ldots + 1}_{p}) = a.0 = 0$$

□

Забележка:

Характеристиката на полето се явява точно реда на единичния елемент, разглеждан като елемент на адитивната група на полето. От последното твърдение следва, че ако полето е с ненулева характеристика p тогава всички ненулеви елементи на полето имат адитивен ред равен на p.

Въпрос: Използвайки факта, доказан в последното твърдение, да се изясни колко елемента е възможно да има в едно поле с краен брой елементи (крайно поле).

1.3. Свойства - 2

Теорема:
Нека F е поле и $\mathtt{char}(F) = p$, където p е просто число, тогава за произволни елементи $a, b \in F$ е изпълнено

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

Доказателство:

Първо ще докажем следното свойство за биномните коефициенти - ако p е просто число, тогава $p \;\Big|\; \binom{p}{k}$ за всяко k, за което $1 \leq k \leq p-1$. Използваме, че простото число p е взаимно просто с всички естествени числа, по-малки от p и затова е изпълнено

$$\binom{p}{k} = \frac{p!}{(p-k)!k!} \;\Rightarrow\; \left\{ \begin{array}{l} p \mid p! \\ p \nmid (p-k)!k! \end{array} \right\} \;\Rightarrow\; p \;\Big|\; \binom{p}{k}$$

За да докажем основното равенство прилагаме формулата за Нютонов бином към $(a+b)^p$. Всички формули за съкратено умножение, които са ни известни от училище, са следствие от комутативен, асоциативен и дистрибутивен закон и затова, тяхното доказателство е едно и също при произволен комутативен пръстен. Поради тази причина, можем да използваме формулата за Нютонов бином във произволно поле.

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

Биномният коефициент $\binom{p}{k}$ пред $a^{p-k}b^k$ означава кратността с която елемента $a^{p-k}b^k$ участва във формулата. Но характеристика на полето е простото число p и доказахме, че p кратното на всеки елемент е 0. По този начин, за всяко $1 \leq k \leq p-1$, се получава:

$$p \;\Big|\; \binom{p}{k} \Rightarrow \binom{p}{k} a^{p-k}b^k = \underbrace{a^{p-k}b^k + \ldots + a^{p-k}b^k}_{\binom{p}{k}} = 0$$

Затова е изпълнено, че

$$(a+b)^p = a^p + \underbrace{\binom{p}{1} a^{p-1}b}_{=0} + \ldots + \underbrace{\binom{p}{p-1} ab^{p-1}}_{=0} + b^p = a^p + b^p$$

□

Пример:
Нека $a, b \in \mathbb{Z}_{11}$, тогава е изпълнено:

$$(a+b)^{121} = ((a+b)^{11})^{11} = (a^{11} + b^{11})^{11} = (a+b)^{11} = a+b$$

В това равенство също е използвана и Теоремата на Ферма, от която имаме, че $x^{11} \equiv x (\mathtt{mod} 11)$.

1.4. Просто поле

Определение:
Поле K се нарича просто поле, ако K няма собствени подполета.

Пример:
Полето $\mathbb{Z}_5$ е просто поле, защото ако L е подполе на $\mathbb{Z}_5$, известно ни е, че $\bar{0}, \bar{1} \in L < \mathbb{Z}_5$, откъдето получаваме

$$\left.\begin{array}{ll} \bar{1}+\bar{1}=\bar{2} & \in L \\ \bar{1}+\bar{2}=\bar{3} & \in L \\ \bar{1}+\bar{3}=\bar{4} & \in L \end{array}\right\} \Rightarrow \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} \subset L \Rightarrow L = \mathbb{Z}_5.$$

По аналогичен начин се получава, също и че полето $\mathbb{Z}_p$ е просто поле, за всяко просто число p.

Твърдение:
Всяко поле F съдържа единствено просто подполе, което е сечение на всички подполета на F.

Доказателство:
Нека T е сечението на всички подполета на полето F.

$$T = \bigcap_{L<F} L$$

Ще докажем, че T е единственото просто подполе на F:

- За да поверим, че T е поле, вземаме два произволни елемента $a, b \in T \cap L$, и $a, b \in L$, където L е произволно подполе на F.
  - L е подполе и затова е изпълнено $a - b \in L$, $a.b \in L$ и $a^{-1} \in L$, когато $a \neq 0$.
  - Понеже $T = \cap L$, където L е произволно подполе, следва, че $a - b \in T$, $a.b \in T$ и също $a^{-1} \in T$, за $a \neq 0$. Така, установихме, че T е подполе на F.
- За да докажем, че T е просто поле, да допуснем, че $U \subset T$ е подполе на T, тогава от $U < T < F$ ще се получи, че U също е подполе на F, откъдето следва, че U е едно от полетата, участващо в сечението $\bigcap L = T$ и следователно $T \subset U$. По този начин установихме, че $T = U$ и следователно T няма собствени подполета и затова T е просто поле.
- За да установим, че T е единственото просто подполе на F, да допуснем, че и подполето P също е просто поле. Тогава, виждаме че $T \cap P$ е подполе и $T \cap P < T$, както и $T \cap P < P$. Но T и P са прости полета и нямат собствени подполета, затова $T \cap P = P = T$, откъдето установявихме, че простото поле T е единственото просто подполе на F.

□

2. Основна теорема за характеристика

Основната Теорема за характеристиката на полетата дава пълно описание на всички възможни прости полета, като изброява кои са "минималните" полета, съдържащи се във всяко поле.

Теорема (*Основна теорема за характеристика на поле*)
Нека F е поле и F_0 е простото му подполе. Изпълнено е, че:

1. ако $\mathtt{char}(F) = p$, където p е просто число, тогава $\mathbb{Z}_p \cong F_0 < F$.
2. ако $\mathtt{char}(F) = 0$, тогава $\mathbb{Q} \cong F_0 < F$.

2.1. Деф. изоморфизъм

Основната Теорема за характеристика на поле описва простите полета с точност до изоморфизъм и затова тук е приложено определението и основните свойства на изоморфизмите. Свойствата ще бъдат по-подробно разгледани в темата за хомоморфизмите при пръстени.

Определение:
Нека K, M са пръстени. Изображението $\varphi : K \to M$ се нарича хомоморфизъм, ако е изпълнено

- $\varphi(a+b) = \varphi(a) + \varphi(b)$;
- $\varphi(a.b) = \varphi(a).\varphi(b)$.

Ако хомоморфизмът φ е биекция, тогава той се нарича изоморфизъм и казваме че пръстените са изоморфни, което са записва по следния начин $K \cong M$.

От дефиницията е видно, че хомоморфизмът на пръстени $\varphi : K \to M$ е също и хомоморфизъм на адитивните групи на пръстените, при който има съгласуване и на операцията произведение.

Свойства:
Ако $\varphi : K \to M$ е хомоморфизъм на пръстени, тогава е изпълнено:

- $\varphi(0_K) = 0_M$,
- $\varphi(a-b) = \varphi(a) - \varphi(b)$,
- $\varphi(-b) = -\varphi(b)$.

Ако освен това K, M са полета и изображението φ не е нулевото (т.е. има поне един елемент, чийто образ е различен от 0), тогава

- $\varphi(e_K) = e_M$, където e_K и e_M са единичните елементи на съответните полетата,
- $\varphi(b^{-1}) = (\varphi(b))^{-1}, b \neq 0$.

2.2. Док-во при char(F)=p

Доказателство случай 1.

Нека характеристиката на полето е $\mathtt{char}(F) = p$, където p е просто число. Разглеждаме изображението $\varphi : \mathbb{Z}_p \to F$, което действа по следния начин $\varphi(\bar{k}) = \underbrace{1 + \ldots + 1}_{k} = k1 \in F$. Ще докажем, че φ е търсения изоморфизъм между $\mathbb{Z}_p$ и F_0.

- Знаем, че елементите на $\mathbb{Z}_p$ са класове от цели числа, които дават равни остатъци при делене с p, затова е необходимо да се покаже, че φ е дефинирано коректно. Като се използва, че p кратното на единичния елемент в полето F е равно на 0, непосредствено се получава коректността на дефинираното изображение

$$\left.\begin{array}{r} \bar{s} = \bar{k} \in \mathbb{Z}_p \Leftrightarrow s = k + lp \in \mathbb{Z}, \;\; l \in \mathbb{Z} \\ s1 = (k+lp)1 = k1 + \underbrace{(lp)1}_{=0} = k1 \in F \end{array}\right\} \Rightarrow \varphi(\bar{s}) = \varphi(\bar{k})$$

- За да проверим, че изображението φ е хомоморфизъм, да вземем произволни числа $k, s \in \mathbb{Z}$ и да разделим тяхната сума и произведението им с частно и остатък на p

$$k + s = q_1 p + r_1, \quad k.\,s = q_2 p + r_2, \quad 0 \le r_1, r_2 < p$$

Използвайки, че редът на единичния елемент $1 \in F$ като част от адитивната група е p, получаваме за сумата

$$\left.\begin{array}{r} \varphi(\bar{k}) + \varphi(\bar{s}) = k1 + s1 = \underbrace{(q_1 p)1}_{=0} + r_1 1 = r_1 1 \\ \varphi(\bar{k} + \bar{s}) = \varphi(\overline{k+s}) = \varphi(\overline{r_1}) = r_1 1 \end{array}\right\} \Rightarrow \varphi(\bar{k}) + \varphi(\bar{s}) = \varphi(\bar{k} + \bar{s})$$

и за произведението

$$\left.\begin{array}{r} \varphi(\bar{k}).\,\varphi(\bar{s}) = (k1).\,(s1) = \underbrace{(q_2 p)1}_{=0} + r_2 1 = r_2 1 \\ \varphi(\bar{k}.\,\bar{s}) = \varphi(\overline{k.\,s}) = \varphi(\overline{r_2}) = r_2 1 \end{array}\right\} \Rightarrow \varphi(\bar{k}).\,\varphi(\bar{s}) = \varphi(\bar{k}.\,\bar{s})$$

Получи се, че изображението φ е хомоморфизъм на пръстени.

- Ще проверим, че образът при това изображение $T_0 = \mathtt{Im}(\varphi)$ е поле. Знаем, че $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ и затова нека

$$T_0 = \mathtt{Im}(\varphi) = \{\varphi(\bar{k}) \mid k \in \mathbb{Z},\; 0 \le k < p\} = \{k1 \mid 0 \le k < p\},$$

което представлява точно подгрупата на адитивната група, породена от елемента $1 \in F$, който има адитивен ред p, т.е. $T_0 =< 1 >$.

  - разлика на два произволни елементи от T_0 също е елемент от T_0, защото образа на изображението е подгрупата на адитивната група .
  - Нека $k1, s1 \in T_0,\; 0 \le k, s < p$ са произволни елементи, делим $k.\,s$ с частно и остатък $k.\,s = q_2 p + r_2$ и получаваме

$$(k1).\,(s1) = (ks)1 = \underbrace{(q_2 p)1}_{=0} + r_2 1 = r_2 1 \in T_0$$

По този начин се получава, че T_0 **е пръстен.**

- Нека $k1$ е произволен ненулев елемент от пръстена T_0, което означава, че кратността принадлежи на интервала $1 \le k \le p-1$. Тогава тази кратност е взаимно-просто число с характеристиката на полето $\text{НОД}(k, p) = 1$ и от тъждеството на Безу, знаем че съществуват цели числа $u, v \in \mathbb{Z}$, за които е изпълнено $ku + pv = 1$. Коефициентите от тъждеството на Безу не са единствени и лесно се проверява, че тъждеството е изпълнено и при други случаи:

$$ku + pv = 1 \implies k(u + t.\,p) + p(v - t.\,k) = 1, \;\; \forall t \in \mathbb{Z}.$$

Поради тази причина можем да изберем такива множители u_1, v_1, за които $0 < u_1 < p$ и $ku_1 + pv_1 = 1$. Това равенство прилагаме като кратности на единичния елемент на полето и получаваме

$$(k1)(u_1 1) = (1 - v_1 p)1 = 1 \in F \implies u_1 1 = (k1)^{-1}$$

Получихме, че всеки ненулев елемент $k1$ от пръстена T_0 е обратим и поради тази причина T_0 **е поле.**

- Всички елементи от полето T_0 се получават като кратни на $1 \in F$, следователно елементите на T_0 се съдържат във всяко подполе на полето F, откъдето непосредствено се получава, че T_0 **е просто поле** .

- Да разгледаме изображението $\widetilde{\varphi} : \mathbb{Z}_p \to T_0$ което действа по същия начин както изображението $\varphi : \mathbb{Z}_p \to F$, а именно $\widetilde{\varphi}(\overline{k}) = k1$ и $\widetilde{\varphi}$ е хомоморфизъм.
  - Проверяваме, че $\widetilde{\varphi}$ е инекция

$$\widetilde{\varphi}(\overline{k}) = \widetilde{\varphi}(\overline{s}) \Leftrightarrow k1 = s1 \Leftrightarrow (k-s)1 = 0 \Leftrightarrow p|(k-s) \Leftrightarrow \overline{k} = \overline{s}$$

  - От друга страна имаме, че $\mathtt{Im}(\varphi) = \mathtt{Im}(\widetilde{\varphi}) = T_0$ и затова хомоморфизмът $\widetilde{\varphi}$ е сюрекция.

Окончателно получихме, че $\widetilde{\varphi}$ е изоморфизъм, откъдето $F_0 = T_0 \cong \mathbb{Z}_p$, следователно простото поле $\mathbb{Z}_p$ е изоморфно на простото подполе $F_0 = T_0$ на полето F. }

2.3. Д-во - при char(F)=0 (част 1)

Доказателство Случай 2.

Нека характеристиката на полето е $\mathtt{char}(F) = 0$.

Първо ще се опитаме да идентифицираме простото подполе на полето F. Да обърнем внимание на факта, че когато характеристиката на полето е p просто число, тогава се оказа, че адитивната циклична група породена от единичния елемент на полето представлява точно простото подполе на F.
В случай на характеристика 0, единичния елемент на полето е от безкраен адитивен ред и адитивната циклична група, породена от него е

$$M =< 1 >= \{k1 \mid k \in \mathbb{Z}\} \subset F, \text{ и е изпълнено } k1 \neq s1 \Leftrightarrow k \neq s.$$

Лесно се установява, че освен че е адитивна група, множеството M е подпръстен на полето F и освен това, ако $T < F$ е произволно подполе на F, тогава T съдържа не само единичния елемент на полето, но и всички негови кратни елементи, т.е. $M \subset T$.
За да получим поле, се налага да разширим множеството M и да разгледаме множеството:

$$L = \{(k1).(s1)^{-1} \mid k, s \in \mathbb{Z},\ s \neq 0\}$$

Ще докажем, че L е поле и за целта да разгледаме два произволни елемента $(k1)(s1)^{-1} \in L$ и $(m1)(t1)^{-1} \in L$ и да проверим, че тяхната разлика принадлежи също на L:

$$\begin{aligned}(k1)(s1)^{-1} - (m1)(t1)^{-1} &= (k1)(t1)^{-1}(t1)(s1)^{-1} - (m1)(t1)^{-1}(s1)(s1)^{-1} = \\ &= [(k1)(t1) - (m1)(s1)].[(t1)(s1)]^{-1} = \\ &= [(\underbrace{kt - ms}_{\in\mathbb{Z}})1][(\underbrace{ts}_{\in\mathbb{Z}})1]^{-1} \in L\end{aligned}$$

.

Аналогично се проверява и за произведението

$$(k1)(s1)^{-1}.(m1)(t1)^{-1} = (km1)(st1)^{-1} \in L$$

Съобразяваме, че обратния елемент на произволен ненулев елемент от L е също елемент на L:

$$\begin{gathered}\text{Ако } (k1)(s1)^{-1} \neq 0 \Leftrightarrow (k1) \neq 0 \in L \Leftrightarrow k \neq 0 \in \mathbb{Z} \\ \Downarrow \\ [(k1)(s1)^{-1}].[(s1)(k1)^{-1}] = 1 \\ \Downarrow \\ [(k1)(s1)^{-1}]^{-1} = (s1)(k1)^{-1} \in L\end{gathered}$$

Следователно L е подполе на F, и нещо повече е изпълнено, че ако $T < F$ е подполе на F, тогава $M \subset T$, но елементите на L са само от вида частно на два елемента на множеството M, затова всеки елемент на полето L се съдържа в T -произволно подполе - и имаме $M \subset L \subset T$. Поради тази причина L няма собствени подполета и $L = F_0$ е простото подполе на F.

2.4. Д-во –char(F)=0- (част 2)

Да разгледаме следното изображение:

$$\varphi : \mathbb{Q} \to F, \quad \varphi\left(\frac{k}{s}\right) = (k1)(s1)^{-1} \in F, \text{ където } \frac{k}{s} \in \mathbb{Q}$$

Използвайки това изображение ще докажем изоморфизма от теоремата.

- Първо трябва да докажем, че изображението е коректно, защото още от училище знаем, че едно рационално число може да се запише по много начини като обикновена дроб - числител върху знаменател (например $\frac{1}{2} = \frac{3}{6} = \frac{-5}{-10}$) .

$$\begin{aligned} \frac{k}{s} = \frac{m}{t} \in \mathbb{Q} \quad &\Leftrightarrow \quad kt = ms \in \mathbb{Z} \Rightarrow \\ &\Rightarrow \quad (kt)1 = (ms)1 = (k1)(t1) = (m1)(s1) \in F \Rightarrow \\ &\Rightarrow \quad (k1)(s1)^{-1} = (m1)(t1)^{-1} \in F \Rightarrow \\ &\Rightarrow \quad \varphi\left(\frac{k}{s}\right) = \varphi\left(\frac{m}{t}\right) \end{aligned}$$

- За да проверим, че изображението φ е хомоморфизъм, да вземем произволни рационални числа $\frac{k}{s}, \ \frac{m}{t} \ \in \mathbb{Q}$ и да пресметнем какъв е образът на сумата на тези две дроби

$$\begin{aligned} \varphi\left(\frac{k}{s}\right) + \varphi\left(\frac{m}{t}\right) \quad &= \quad (k1).(s1)^{-1} + (m1).(t1)^{-1} = \\ &= \quad (k1)(t1)^{-1}(t1).(s1)^{-1} + (m1).(s1)^{-1}(s1).(t1)^{-1} = \\ &= \quad [(kt+ms)1].[(ts)1]^{-1} = \\ &= \quad \varphi\left(\frac{kt+ms}{ts}\right) = \varphi\left(\frac{k}{s} + \frac{m}{t}\right) \end{aligned}$$

  Аналогично се получава за образа на произведението

$$\begin{aligned} \varphi\left(\frac{k}{s}\right).\varphi\left(\frac{m}{t}\right) \quad &= \quad (k1).(s1)^{-1}.(m1).(t1)^{-1} = \\ &= \quad [(km)1][(st)1]^{-1} = \\ &= \quad \varphi\left(\frac{km}{ts}\right) = \varphi\left(\frac{k}{s}.\frac{m}{t}\right) \end{aligned}$$

  Получи се, че изображението φ е хомоморфизъм на пръстени.
- Да разгледаме изображението $\widetilde{\varphi} : \mathbb{Q} \to L$ което действа по същия начин както изображението $\varphi : \mathbb{Q} \to F,$ а именно $\widetilde{\varphi}\left(\frac{k}{s}\right) = (k1)(s1)^{-1} \in L.$ Проверяваме, че това изображение, за което знаем, че е хомоморфизъм, също е и биекция:

$$\widetilde{\varphi}\left(\frac{k}{s}\right) = \widetilde{\varphi}\left(\frac{m}{t}\right) \quad \Leftrightarrow \quad (k1)(s1)^{-1} = (m1)(t1)^{-1}$$

$$\Updownarrow$$

$$\frac{k}{s} = \frac{m}{t} \ \Leftrightarrow \ kt = ms \quad \Leftrightarrow \qquad (k1)(t1) = (m1)(s1)$$

  Получи се, че $\widetilde{\varphi}$ е инекция. От друга страна имаме, че $\mathtt{Im}(\varphi) = \mathtt{Im}(\widetilde{\varphi}) = L$ и затова $\widetilde{\varphi}$ е сюрекция.

Следователно $\widetilde{\varphi}$ е изоморфизъм, откъдето се получава $F_0 = L \cong \mathbb{Q}$.

3. Поле от частни

Оказва се, че от всяка област на цялост може да се състави поле, което се нарича поле от частни за областта. Конструкцията е идентична с тази, която се използва за построяване на рационалните числа, изхождайки от множеството на целите числа.

Този универсален начин за получаване на полета, когато се стартира от произволен комутативен пръстен без делители на нулата е разгледан подробно в този въпрос. Този начин, като обобщение на метода по който се формират обикновените дроби от целите числа, е добре познат от училище. Показвайки как се прилага при произволен пръстен, ще стане ясна причината, поради която се извършват някои от действията и преобразуванията при дроби, както и да се осъзнае в дълбочина цялата процедура по съставяне на рационалние числа.

3.1. област на цялост

Определение:
Комутативен пръстен без делители на нулата се нарича *област на цялост*.

Примери:

- При дефиниране на пръстени доказахме, че в полетата няма делители на нулата, затова всички полета F са области на цялост.
- Пръстенът на целите числа $\mathbb{Z}$, както и пръстенът на целите Гаусови числа $\mathbb{Z}[i]$ са области на цялост, защото са подпръстени на полето на комплексните числа $\mathbb{C}$. Поради същата причина пръстенът $5\mathbb{Z}$ също е област на цялост, въпреки че е пръстен без единица.
- Ако F е поле, тогава пръстенът на полиномите $F[x]$ с коефициенти от това поле също е област на цялост.
- От примерите при пръстени, видяхме, че когато n е съставно число в пръстенстена $\mathbb{Z}_n$ има делители на нулата и $\overline{a}$ е делител на нулата, когато най-големият общ делител $(a, n) > 1$. Получава се, че
  - при n просто число, $\mathbb{Z}_n$ е област на цялост и поле,
  - при n съставно число, $\mathbb{Z}_n$ не е област на цялост.

Твърдение (*Правило за съкращаване в област на цялост*)
Нека A е област на цялост. Ако за елементите $a, x, y \in A,\ a \neq 0,$ е изпълнено $ax = ay$, тогава следва че $x = y$.
Доказателство:
В пръстена A няма делители на нулата е затова се получава

$$ax = ay \implies a(x - y) = 0,\ a \neq 0 \implies x - y = 0, \text{ т.е. } x = y$$

□

Прилагайки, правилото за съкращаване в крайна област на цялост, може да се реши следната хубава задача.
Задача:
Да се докаже, че всяка крайна област на цялост, която има поне два елемента е поле.

3.2. релация в AxA и класове на еквивиалентност

Знаем, че всяко рационално число може да се представи във вида $\frac{a}{b},\ a,b\in\mathbb{Z},\ a\neq 0.$ Известно е правилото кога две дроби съвпадат $\frac{a}{b}=\frac{c}{d}\ \Leftrightarrow\ ad=bc.$

Поради тази причина е удачно да се разгледа множеството от наредени двойки от елементи от една област на цялост.

Твърдение:
Нека A е област на цялост и

$$B=\{(a,b)\mid a,b\in A,\ b\neq 0\}\subset A\times A.$$

В множеството B разглеждаме релацията $(a,b)\ \sim\ (c,d)$, когато $ad=bc$. Тогава "$\sim$" е релация на еквивалентност в множеството B.

Доказателство:

Проверяваме, че

- релацията е рефлексивна, $(a,b)\ \sim\ (a,b)$, защото $ab=ba$;
- релацията е симетрична, защото ако $(a,b)\ \sim\ (c,d)$, тогава $(c,d)\ \sim\ (a,b).$, защото от $ad=bc$ следва $cb=da$;
- транзитивна, защото ако $(a,b)\ \sim\ (c,d)$ и $(c,d)\ \sim\ (f,g)$, тогава $(a,b)\ \sim\ (f,g)$. Изпълнено е, защото

$$\begin{array}{rcl}(c,d) & \sim & (f,g)\\ & \Downarrow & \\ cg=df & \Rightarrow & acg=adf\\ & \Downarrow & \text{от } (a,b)\ \sim\ (c,d)\\ acg & = & bcf\\ (\text{ когато } c\neq 0)\ ag=bf & \Downarrow & a=c=f=0\ (\text{ когато } c=0)\\ (a,b) & \sim & (f,g)\end{array}$$

Получихме, че " $\sim$" е релация на еквивалентност.

Релацията на еквивалентност, разбива множеството B на класове на еквивалентност по следния начин:

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

Свойство: ([Правило за съкращаване)
Изпълнено е $[a,b]=[ka,kb],$ когато $k\neq 0.$

Доказателство:

$$akb=bka\ \Rightarrow\ (a,b)\ \sim\ (ka,kb)\ \Rightarrow\ [a,b]=[ka,kb]$$

3.3. действия с класовете

Известно е, че всяко рационално число може да се запише по множество различни начини, а именно като се умножат числителя и знаменателя с еднакви множители, т.е. всяко рационално число може да се утъждествi с множество от двойки цели числа, които дават еднакво частно. За де се извърши събиране с рационални числа се налага да се разширяват дробите, като се променят числителя и знаменателя на събираемите по подходящ начин. Следвайки тази идея може да се получи поле, използвайки наредените двойки елементи от произволна област на цялост.
Множеството на различните начини, по които може да се запише едно рационално число

$$\{\frac{ka}{kb} \mid k \in \mathbb{Z}\}$$

при нашето разглеждане ще съответства на класа на еквивалентност на който принадлежи (a, b):

$$[a, b] = \{(x, y) \mid x, y \in A, y \neq 0, ay = bx\}$$

Теорема:
Нека A е област на цялост и нека $[a, b] = \{(x, y) \mid x, y \in A,\ y \neq 0,\ ay = bx\}$ са класовете на еквивалентност при разглежданата релация на еквивалентност. Множеството от всички класове на еквивалентност

$$P = \{[a, b] | a, b \in A, b \neq 0\},$$

разглеждано спрямо операциите

$$[a, b] + [c, d] = [ad + cb, bd], \quad [a, b].\,[c, d] = [ac, bd]$$

е поле, което се нарича поле от частни на областта A.

Доказателство:
В множество, което съставихме, въведохме две нови операции и затова трябва да се проверят всички аксиоми за пръстен. Елементите на множеството P са подмножества, а резултатът от операциите зависи само от един конкретен представител, чрез който сме описали всяко едно подмножество $[a, b]$ и поради тази причина първо трябва да се провери коректно ли е така да бъдат дефинирани операции.

- *Коректно ли са дефинирани операциите ?* Произволно множество $[a, b] = \{(x, y) \mid x, y \in A,\ y \neq 0,\ ay = bx\} \in P$ може да бъде описано, чрез всеки един от своите елементи и затова, нека да разгледаме случая, когато $[a, b] = [a_1, b_1]$ и $[c, d] = [c_1, d_1]$. Това означава, че е изпълнено $(a_1, b_1) \in [a, b]$ и $ab_1 = a_1 b$ и съответно $(c_1, d_1) \in [c, d]$ и $cd_1 = c_1 d$. Пресмятаме, като прилагаме тези равенства:

$$\begin{array}{rcl} (ad + bc)b_1 d_1 & = & \underline{ab_1} dd_1 + bb_1 \underline{cd_1} = \\ & = & a_1 bdd_1 + bb_1 c_1 d = \\ & = & (a_1 d_1 + b_1 c_1)bd \\ & \Downarrow & \\ [ad + cb, bd] & = & [a_1 .\, d_1 + c_1 .\, b_1\ ,\ b_1 .\, d_1] \end{array}$$

Следователно събирането е коректно дефинирано и е бинарна операция за P. За умножението имаме

$$\begin{array}{c} (ac)(b_1 d_1) = (ab_1)(cd_1) = (a_1 b)(c_1 d) = (a_1 c_1)(bd) \\ \Downarrow \\ [ac, bd] = [a_1 c_1,\ b_1 .\, d_1] \end{array} .$$

Следователно и умножението е коректно дефинирано и е бинарна операция за P.

- *Комутативност.* Нека $[a, b]$ и $[c, d]$ са поизволни елементи на P. Изпълнено е

$$\begin{array}{rcl} [a, b] + [c, d] & = & [ad + cb, bd] \\ & & \| \\ [c, d] + [a, b] & = & [cb + ad, db] \end{array} \quad \Rightarrow \quad \begin{array}{c} "+" \text{ е} \\ \text{комутативно} \end{array}$$

$$\begin{array}{rcl} [a,b]\,.\,[c,d] & = & [ac,bd] \\ & & \| \\ [c,d]\,.\,[a,b] & = & [ca,db] \end{array} \Rightarrow \underset{\text{комутативно}}{\text{"}.\text{" е}}$$

- За да докажем асоциативност, проверяваме за произволни елементи $[a,b],\ [c,d]$ и $[f,g]$ (*равенствата са написани едно под друго*). Виждаме, че преобразуванията, извършени в лявата колона и в дясната колона водят до един и същи резултат, откъдето се получава, че при двата начина на разполагане на скобите при три множителя се получава еднаква стойност.

$$\begin{array}{c|c} ([a,b]+[c,d])+[f,g] & [a,b]+([c,d]+[f,g]) \\ \| & \| \\ [ad+cb,bd]+[f,g] & [a,b]+[cg+fd,dg] \\ \| & \| \\ [\,adg+cbg+fbd\,,\ bdg\,] & [\,adg+cgb+fdb\,,\ bdg\,] \end{array}$$

Аналогично се установява и асоциативност при умножението :

$$\begin{array}{ccc|ccc} \Downarrow & ([a,b]\,.\,[c,d]).\,[f,g] & & [a,b]\,.\,([c,d]\,.\,[f,g]) & \Downarrow \\ & \| & & \| & \\ \Downarrow & [ac,bd]\,.\,[f,g] & & [a,b]\,.\,[cf,dg] & \Downarrow \\ & \| & & \| & \\ & [\,acf\,,\ bdg\,] & = & [\,acf\,,\ bdg\,] & \end{array}$$

- За произволни елементи $[a,b],\ [c,d]$ и $[f,g]$ пресмятаме

$$([a,b]+[c,d]).\,[f,g] = [\,ad+cb,bd\,].\,[f,g] = [\,adf+cbf,bdg\,]\,;$$

$$\begin{array}{rcl} [a,b].\,[f,g]+[c,d].\,[f,g] & = & [\,af,bg\,]+[\,cf,dg\,] = \\ & = & [\,afdg+cfbg\,,\ bgdg\,] = \\ & = & [\,afd+cfb,bdg\,] \end{array}$$

Във второто пресмятане сме приложили правилото за съкращаване и получихме, че е изпълнен дистрибутивния закон

$$([a,b]+[c,d]).\,[f,g] = [a,b].\,[f,g]+[c,d].\,[f,g].$$

- Нека $c \neq 0$ е елемент на пръстена A. Като използваме правилото за съкращаване, получаваме

$$\begin{array}{rcl} [a,b]+[0,c] & = & [\,ac+0b,bc\,] = \\ & = & [\,ac\,,\ bc\,] = \\ & = & [\,a,b\,] \end{array}$$

  По този начин се установява, че $\vartheta = [0,c]$ е нулев елемент. Вижда се, че $\vartheta = [0,c] = \{(0,b) \mid b \in A, b \neq 0\}$,затова в зависимост от необходимостта при пресмятанията нулевия елемент може да се запише по произволен начин $\vartheta = [0,b]$, като елемента $b \neq 0$ може да се променя.

- Противоположния на един елемент намираме лесно, по следния начин:

$$[a,b]+[-a,b]=[ab-ab\ ,\ b^2]=[0,b^2]=\vartheta.$$

Следователно $-[a,b]=[-a,b]$.

- В множеството P има единичен елемент, дори и когато в изходния пръстен A няма такъв, защото ако $c\neq 0$ е произволен елемент от A е изпълнено

$$[a,b].[c,c]=[\ ac\ ,\ bc\ ]=[a,b]$$

Получихме, че $[c,c]=e_P$ е единичния елемент и

$$e_P=[c,c]=\{(a,a)\mid a\in A, a\neq 0\}.$$

- Ако $[a,b]\neq\vartheta$, което означава $a\neq 0$, тогава съществува $[b,a]$ и е изпълнено

$$[a,b].[b,a]=[ab,ab]=e_P$$

По този начин се получи, че елементът $[a,b]\neq\vartheta$ е обратим и $[a,b]^{-1}=[b,a]$.

Чрез директна проверка установихме, че множеството P от класовете на еквивалентност е поле спрямо така дефинираните бинарни операции събиране и умножение.

□

3.4. А се съдържа в полето от частни

След като съставихме полето от частни, по подобен начин по който се съставя полето от рационални числа е необходимо да се уверим, че изходния пръстен A е част от това поле P. Ясно е, че елементите на двете множества имат съвсем различно естество -елементите на P са множества от наредени двойки, които са съставени от елементи на A. Но въпреки това, не е трудно да се направи това влагане по аналогичен начин, по който се установява, че целите числа са част от рационалните числа - на всяко цяло число се съпоставя съответното дробно число, което има знаменател 1:

$$\forall z \in \mathbb{Z} \ \rightarrow \frac{z}{1} = \frac{zk}{k} \in \mathbb{Q}, \ \forall k \in \mathbb{Z}, k \neq 0$$

Теорема:
Ако A е област на цялост и P е полето от частни на областта A, съществува подпръстен $A_1 < P$, който е изоморфен на областта $A \cong A_1 < P$

Доказателство:
Нека да фиксираме един произволен елемент $0 \neq c \in A$. Разглеждаме изображението

$$\varphi : A \rightarrow P, \quad \varphi(x) = [xc, c] \in P$$

Проверяваме, че φ е хомоморфизъм,, като използваме правилото за съкращаване, когато е необходимо :

$$\left.\begin{array}{rcc} \varphi(x) + \varphi(y) = [xc, c] + [yc, c] & = & \left[xc^2 + yc^2, c^2\right] \\ & & \| \\ \varphi(x + y) = [(x + y)c, c] & = & [xc + yc, c] \end{array}\right\} \Rightarrow \begin{array}{c} \varphi(x) + \varphi(y) = \\ = \varphi(x + y) \end{array}$$

$$\left.\begin{array}{rcc} \varphi(x).\varphi(y) = [xc, c].[yc, c] & = & \left[xyc^2, c^2\right] \\ & & \| \\ \varphi(x.y) & = & [xyc, c] \end{array}\right\} \Rightarrow \begin{array}{c} \varphi(x).\varphi(y) = \\ = \varphi(x.y) \end{array}$$

Да обърнем внимание, че този хомоморфизъм не зависи от избрания елемент c, защото е изпълнено

$$xcd = cxd \ \Rightarrow \ [xc, c] = [xd, d].$$

За да покажем, че A е изоморфно на подпръстен на полето от частни, трябва да докажем, че изображението φ е инективно и затова проверяваме кога образите на два елемента съвпадат, като в пресмятанията пак се налага да използваме правилото за съкращаване

$$\begin{array}{rcc} \varphi(x) = \varphi(y) & \Longleftrightarrow & [xc, c] = [yc, c] \\ & & \Updownarrow \\ x = y & \Longleftrightarrow & xc.c = c.yc \end{array}$$

Получихме, че φ е инекция и хомоморфизъм, което понякога накратко се нарича хомоморфно влагане.
Тогава, ако $A_1 = \mathtt{Im}(\varphi)$ е образа на изображението, тогава φ разгледано само като изображение от A към $A_1 = \mathtt{Im}(\varphi)$ е биекция и затова $A \cong A_1 < P$. Поради тази причина, като утъждествяваме областта A с нейния образ A_1, можем да считаме че пръстенът A \textbf{се влага} в областта P.

□

3.5. примери

На практика елементите на полето от частни, които представляват множества от наредени двойки елементи от A не се записват, както в доказателството във вида $[a, b]$, а често се записват по начина по който се записват рационалните числа - във вида на обикновена дроб $\frac{a}{b}$. Като ги запишем така ще видим, че полето от частни на пръстена на целите числа е точно полето на рационалните числа.

Пример:
Ясно е, че всяко рационално число може да се представи във вид на дроб, в който и числителя и знаменателя се делят на фиксирано цяло число (например 5) $\frac{a}{b} = \frac{5a}{5b}$. Виждаме, че събирането и умножението се извършват точно по тези правила, които бяха описани в теоремата

$$\frac{5a}{5b} + \frac{5c}{5d} = \frac{25ad + 25bc}{25bd}, \quad \frac{5a}{5b}.\frac{5c}{5d} = \frac{25ac}{25bd}$$

По този начин се получава, че полето от частни за областта $5\mathbb{Z}$ също е полето на рационалните числа $\mathbb{Q}$.

По аналогичен начин установяваме, че полето от частни за пръстена от полиномите $\mathbb{R}[x]$ е полето от рационалните функции

$$\mathbb{Z}(x) = \left\{ \frac{f(x)}{g(x)} \middle| \ f(x), g(x) \in \mathbb{R}[x], \ g \neq 0 \right\}.$$

3.6. Минималното поле, съдържащо A

В следващата теорема ще докажем, че полето от частни се съдържа във всички полета, на които областта A е подпръстен, и от такава гледна точка, можем да възприемаме полето от частни като минималното поле, което съдържа A.

Теорема:
Ако A е област на цялост, която се съдържа в поле F, тогава съществува подполе $P_1 < F$, за което е изпълнено: $A \subset P_1$ и $P_1 \cong P$, където P е полето от частни за областта A.

Доказателство:
Нека $P = \{[a,b] | a,b \in A, b \neq 0\}$ е полето от частни за A. Разглеждаме изображението $\psi : P \to F$, за което $\psi([a,b]) = ab^{-1}$. Проверяваме:

- ψ е коректно дефинирано изображение, защото:

$$[a,b] = [c,d] \Rightarrow ad = bc \Rightarrow ab^{-1} = cd^{-1} \Rightarrow \psi([a,b]) = \psi([c,d])$$

- ψ е хмоморфизъм, защото

$$\begin{aligned} \psi([a,b] + [c,d]) &= \psi([ad+bc, bd]) = \\ &= (ad+bc).(bd)^{-1} = ab^{-1} + cd^{-1} \\ &= \psi([a,b]) + \psi([c,d]) \end{aligned}$$

$$\begin{aligned} \psi([a,b].[c,d]) &= \psi([ac,bd]) = (ac).(bd)^{-1} = \\ &= (ab^{-1}).(cd^{-1}) = \\ &= \psi([a,b]).\psi([c,d]) \end{aligned}$$

- ψ е инективно изображение

$$\begin{array}{ccc} \psi([a,b]) = \psi([c,d]) & \Longrightarrow & ab^{-1} = cd^{-1} \\ & & \Downarrow \\ [a,b] = [c,d] & \Longleftarrow & ad = bc \end{array}$$

Следователно полето от частни P е изоморфно на образа P_1 на ψ, което е подполе на полето F, т.е. $P \cong P_1 < F$.

Виждаме, че $A \subset P_1$, защото ако $a \in A$ то е образ на елемент от P, защото $\psi([ac,c] = ac.c^{-1} = a)$. Следователно $A \subset P_1$.

□

Пример:
Знаем, че всяко поле F е област на цялост, и можем да приложим последната теорема. Виждаме, че областта F е подпръстен на полето F и за това полето от частни за F е изоморфно на подполе P_1 на полето F, като P_1 съдържа областта F. По този начин получаваме, че $P_1 = F$, т.е. полето от частни на поле е изоморфно на самото поле.