Количнички прстен и коначна поља

Теорема

Ако је I идеал комутативног прстена R, онда се Абелова група R/I може „надоградити" као комутативни прстен, тако да је природни хомоморфизам $\pi : R \to R/I$, $\pi(a) = a + I$, $a \in R$, заправо епиморфизам.

скица доказа

- операција $+$ се наслеђује из фактор групе
- операцију $\cdot$ дефинишемо као
  $$(a+I)(b+I) := ab + I$$

задатак: доказати да је $\cdot$ добро дефинисана.

Дефиниција

Комутативни прстен R/I за дати прстен R и његов идеал I се назива количнички прстен и означава $R \bmod I$.

Пример

Нека је R прстен цијелих бројева $\mathbb{Z}$, а $I = m\mathbb{Z} = (m)$.

Онда је $R/I = \mathbb{Z}/(m\mathbb{Z}) \cong \mathbb{Z}_m$.

- Два теорема о изоморфизму прстена

$f: R \to A$ (хомоморфизам прстена)

$R / \mathrm{Ker}\, f \cong \mathrm{Im}\, f$

- поље (појам)
- потпоље (појам)
- просто поље $\equiv$ оно поље које нема нетривијалних потпоља

<u>задатак:</u> Нека је S фамилија свих потпоља датог поља k. Онда је

$$\bigcap_{F \in S} F$$

просто потпоље поља k.

<u>Лема</u> Нека је k поље. Онда је његово просто потпоље изоморфно $\mathbb{Q}$ или $\mathbb{F}_p$ за неки прост број p.
($\mathbb{F}_p$ је ознака за $\mathbb{Z}_p$).

<u>доказ</u>
Успоставимо $\chi: \mathbb{Z} \to k$ хомоморфизам прстена дефинисан са $\chi(n) = n \cdot 1$, где је 1 јединица у пољу k.
Онда је $\mathrm{Ker}\, \chi$ главни идеал у $\mathbb{Z}$ облика $m\mathbb{Z}$.
Ако је $m = 0$, онда је χ инјективно, па постоји изоморфна копија $\mathbb{Z}$ унутар k.
Међутим, у том случају, мора постојати и изоморфна копија $\mathbb{Q}$ у k и имамо да $\mathrm{Im}\, \chi \subseteq \mathbb{Q} \subseteq k$.
задатак: доказати да $\mathbb{Q}$ нема нетривијалних

Задатак: доказати да ...
потпоља.

Дакле, $\mathbb{Q}$ је просто потпоље поља k.

Ако је $m \neq 0$, онда

$$\mathbb{Z}_m \cong \operatorname{Im} \chi \subseteq k.$$

Пошто се $\operatorname{Im} \chi$ налази унутар поља, онда $\operatorname{Im} \chi$ нема нетривијалних дјелитеља нуле, па што значи да је $\operatorname{Im} \chi$ домен.

С друге стране $\mathbb{Z}_m$ је домен ако и само ако је m прост број.

Значи, m мора бити прост број p.

Закључујемо да је $\operatorname{Im} \chi = \{0, 1, 2, \dots, p-1\}$, па је $\operatorname{Im} \chi \cong \mathbb{F}_p$.

Поље $\mathbb{F}_p$ нема правих потпоља, па је оно просто потпоље поља k.

- $\operatorname{char}(k)$ се може схватити као ред јединичног елемента поља k. Заправо

$$\operatorname{char}(k) = \begin{cases} 0, & \text{ако је } \mathbb{Q} \text{ просто потпоље поља } k \\ p, & \text{ако је } \mathbb{F}_p \text{ просто потпоље поља } k \end{cases}$$

Задатак:
Нека је $\operatorname{char}(k) = p$, p прост број.
Доказати $p \cdot a = 0$, за свако $a \in k$.

Лема Ако је k коначно поље, онда је $|k| = p^n$, за неки прост број p и $n \in \mathbb{N}$.

<u>доказ:</u>

Како је k коначно поље, онда је његово просто потпоље $\mathbb{F}_p$, за неки прост број p.
Значи, k можемо представити као в. простор над пољем $\mathbb{F}_p$.
Пошто је k коначно поље, онда $\dim_k^{\mathbb{F}_p} = n$, $n \in \mathbb{N}$.
Дакле, сваки елемент „векторског простора" k је облика

$$c_1 v_1 + \dots + c_n v_n, \quad v_i \in k, \; c_i \in \mathbb{F}_p,$$

$i = 1, \dots, n$.
То значи $\left| \{ c_1 v_1 + \dots + c_n v_n \mid v_i \in k, \, c_i \in \mathbb{F}_p, \, i = 1, \dots, n \} \right| = p^n$, па је $|k| = p^n$.

<u>Напомена</u>: Претходни доказ можемо извести помоћу теорије група.
Претпоставимо да је коначан број $|k|$ дјељив са два различита броја p и q, p и q прости.
На основу Кошијеве теореме, постоје елементи a и $b \in k$, тако да

$\operatorname{ord}(a) = p$, $\operatorname{ord}(b) = q$, при чему су $a \neq 0$, $b \neq 0$.

Онда $p \cdot a = 0$, па је $(p \cdot 1) \cdot a = 0 \Rightarrow p \cdot 1 = 0$.
Слично закључујемо $q \cdot 1 = 0$.
Пошто је НЗД$(p, q) = 1$, онда

$s p + t \cdot q = 1$ за $s, t \in \mathbb{Z}$.

$sp+tq=1$ за $s,t \in$ ...

$$(sp+tq)\cdot 1_k = 1\cdot 1_k = 0 \Rightarrow 0=1 \text{ у пољу } k,$$

што је контрадикција.

Лема

Ако је k поље и $I=(p(x))$, гдје је $p(x)\in k[x]$, $p(x)\neq 0$, онда је $k[x]/I$ поље ако и само ако је $p(x)$ иредуцибилан.

доказ:

Нека је $p(x)$ иредуцибилан полином. Примијетимо да је $I=(p(x))$ прави идеал, јер $p(x)\neq 0$ и $p(x)\notin k$, зато што је $p(x)$ иредуцибилан (не може бити инвертибилан).

То значи да $1\notin I$, па је $1+I$ ненулти елемент $k[x]/I$.

Ако $f(x)\notin I \Rightarrow p(x)\nmid f(x)$.

Онда $НЗД(f(x),p(x))=1 \Rightarrow$ постоје $s(x),t(x)\in k[x]$,

$s(x)f(x)+t(x)p(x)=1$, односно

$$(s(x)+I)(f(x)+I)+\underbrace{(t(x)+I)(p(x)+I)}_{I}=1+I$$

$$\Rightarrow (s(x)+I)(f(x)+I)=1+I.$$

Значи, доказали смо постојање инверзног елемента за ненулти елемент $f(x)+I$.

Даље, уважавајући да је $k[x]/I$ Абелова група, као и подгрупа у односу на мултипликативну операцију, претходним смо доказали да сваки ненулти елемент из $k[x]/I$ има свој мултипликативни инверз, па је $k[x]/I$ поље.

Задатак: Доказати тврђење у супротном смеру.

k поље, $p(x) \in k[x]$, I идеал у $k[x]$.

$p(x) = c_0 + c_1 x + \dots + c_m x^m$, $c_i \in k$.

Нека је $K = k[x]/I$

$\tilde{p}(x) \in K[x]$,

$$\tilde{p}(x) = (c_0+I) + (c_1+I)\cdot x + \dots + (c_m+I)\cdot x^m$$

$$\tilde{p}(x+I) = (c_0+I) + (c_1+I)(x+I) + \dots + (c_m+I)(x+I)^m$$

$$= c_0 + I + c_1 x + I + \dots + c_m x^m + I$$

$$= p(x) + I.$$

Лема

Нека је k поље и $p(x) \in k[x]$ монични иредуцибилни полином степена m, $K = k[x]/I$, $I = (p(x))$, а $z = x + I \in K$.

(1) K је поље и $k' = \{a + I \mid a \in k\}$ је потпоље поља K изоморфно са k.
Дакле, суштински k је потпоље поља K.

(2) z је нула полинома $\tilde{p}(x)$ у K.
$\left(\tilde{p}(x) = \sum_{i=0}^{m} (c_i + I)x^i,\ p(x) = \sum_{i=0}^{m} c_i x^i\right)$

$\tilde{p}(\zeta) = \tilde{p}(x+I) = I$.

(3) Нека је $g(x) \in k[x]$. Ако је $\tilde{g}(x+I) = I$, онда $p(x) \mid g(x)$ у $k[x]$.

(4) $p(x)$ је јединствен моничан, иредуцибилан полином у $k[x]$, тако да је његов „аналогон" $\tilde{p}(x)$ такав да $\tilde{p}(\zeta) = I$, односно $\tilde{p}(x)$ има нулу у ζ.

(5) Вектори $1, \zeta, \zeta^2, \dots, \zeta^{m-1}$ су база векторског простора K над пољем k, $[K:k] = m$.

<u>Доказ:</u>

(1) тривијално.

(2) $\tilde{p}(x) = (c_0+I) + (c_1+I)x + \dots + (c_m+I)x^m$

$\zeta = x + I$

$$\tilde{p}(x+I) = (c_0+I) + (c_1+I)\cdot(x+I) + \dots + (c_m+I)(x+I)^m$$

$$= c_0 + I + c_1x + I + \dots + c_m x^m + I$$

$$= p(x) + I = I.$$

Дакле, $\tilde{p}(x)$ има нулу у „тачки" $\zeta = x + I$.

(3) Нека је $g(x) = b_0 + b_1x + \dots + b_nx^n$

$\tilde{g}(x) = (b_0+I) + (b_1+I)x + \dots + (b_n+I)x^n$

$\tilde{g}(\zeta) = \tilde{g}(x+I) = I$ (*)

$\tilde{g}(x+I) = (b_0+I) + (b_1+x)(x+I) + \dots + (b_m+I)(x+I)^n$

$\tilde g(x+I) = \ldots$

$= g(x) + I$

Међутим, из $(*)$

$\tilde g(x+I) = I \Rightarrow g(x)+I = I \Rightarrow g(x) \in I$

С друге стране, $I = (p(x))$, одакле је

$p(x) \mid g(x)$.

(4) Претпоставимо да је $h(x) \in k[x]$ такав да $\tilde h(\zeta) = I$, $h(x)$ моничан, иредуцибилан полином.

Из (3) имемо да $p(x) \mid h(x)$, али како је $h(x)$ моничан и иредуцибилан, онда $p(x) = h(x)$.

(5) Сви елементи из K су облика

$f(x)+I$, $f(x) \in k[x]$.

На основу алгоритма дијељења,

$$f(x) = p(x)\cdot q(x) + r(x), \quad q(x), r(x) \in k[x]$$

$r(x) = 0$ или $\deg(r(x)) < \deg(p(x)) = m$.

$p(x)\cdot q(x) \in I$.

Онда је $f(x)+I = r(x)+I$.

$r(x)+I = a_0 + a_1 x + \ldots + a_{m-1}x^{m-1} + I$,

гдје су $a_i \in k$, $i = 0, \ldots, m-1$.

$$a_0 + a_1\underbrace{(x+I)}_{\zeta} + \ldots + a_{m-1}\underbrace{(x+I)^{m-1}}_{\zeta^{m-1}}$$

$= r(x) + I$

Дакле $1, \zeta, \ldots, \zeta^{m-1}$ су генератори скуп за простор K.

вјежба: доказати да је $1, 3, \ldots, 3^{m-1}$ линеарно независан скуп.

Дакле, $[K:k] = \dim_k K = m$.

<u>Дефиниција</u> Ако поље K садржи k као потпоље, онда кажемо да је K проширење поља k, а означавамо са $K \mid k$.

Проширење $K \mid k$ је <u>коначно</u>, ако је $\dim_k K$ коначна (димензија в. простора K над пољем k).

Димензија $\dim_k K$, коју означавамо и $[K:k]$ називамо степен проширења $K \mid k$.

<u>пример</u>

Полином $x^2+1 \in \mathbb{R}[x]$ је монтичан, нерастављиван, па је $K = \mathbb{R}[x] / (x^2+1)$ проширење поља $\mathbb{R}$ степена 2.

За корјен полинома x^2+1 у $K[x]$, који означавамо са i, кажемо да је то имагинарна јединица.

На основу претходне леме, база в. простора K над $\mathbb{R}$ је $1, i$.

То значи да је

$$K = \{ a_0 + a_1 i \mid a_0, a_1 \in \mathbb{R} \},$$

што је заправо поље комплексних бројева.

<u>Дефиниција</u>

Нека је $K|k$ проширење поља. Елемент $\alpha \in K$ је <u>алгебарски</u> над k, ако постоји ненулти полином $f(x) \in k[x]$ чији је корјен α.
У супротном, за α кажемо да је <u>трансцендентан</u>.
Проширење $K|k$ је <u>алгебарско</u> ако је сваки $\alpha \in K$ алгебарски над k.

<u>Лема</u>

Ако је $K|k$ коначно проширење, онда је оно и алгебарско.

<u>доказ:</u>

Нека је $[K:k]=n$, $n \in \mathbb{N}$.
За произвољно $\alpha \in K$, јасно је да је $1, \alpha, \alpha^2, \dots, \alpha^n$ линеарно зависан систем в. простора K над пољем k.
То значи да постоје $c_i \in k$, $i=0,\dots,n$, од којих је бар један различит од нуле, тако да

$$\sum_{i=0}^{n} c_i \alpha^i = 0$$

Другим ријечима, $f(x) = \sum_{i=0}^{n} c_i x^i \in k[x]$, је ненулти полином чија је нула α.
Дакле, α је алгебарски над k.

<u>Дефиниција</u>

Нека је $K|k$ проширење, а $A \subseteq K$ произвољан подскуп.
$k(A)$ означавамо минимално потпоље

са $k(A)$ ...
поља K које садржи k и A.

Уколико је $A = \{z_1, \dots, z_n\}$

онда $k(A)$ означавамо са $k(z_1, \dots, z_n)$,

$n \in \mathbb{N}$.

За $\alpha \in K$, поље $k(\alpha)$ називамо <u>простим</u> проширењем поља k, чији је α <u>примитивни</u> <u>елемент</u>.

<u>Примјер</u>

Нека је $K \mid k$ проширење, а $\alpha \in K$.

$k(\alpha) = ?$

$k(\alpha)$ мора да садржи све елементе облика

$$\underbrace{a_0 + a_1\alpha + \dots + a_m\alpha^m}_{p(\alpha)}, \quad a_i \in k, \quad m \in \mathbb{N}.$$

$$p(x) = \sum_{i=0}^{m} a_i x^i$$

Међутим, $k(\alpha)$ мора да садржи и $\frac{1}{p(\alpha)}$,

за $p(x) \in k[x]$, $p(\alpha) \neq 0$.

Тако долазимо до закључка да

$k(\alpha)$ мора да садржи

скуп $\mathcal{K} = \left\{ \frac{p(\alpha)}{q(\alpha)} \mid p(x), q(x) \in k[x], q(\alpha) \neq 0 \right\}$

Треба показати да је $\mathcal{K}$ поље.

Из тог се закључује да је

$$\mathcal{K} = k(\alpha) = \left\{ \frac{p(\alpha)}{q(\alpha)} \mid p(x), q(x) \in k[x], q(\alpha) \neq 0 \right\}$$

... поље $k(\alpha)$ је заправо поље разломака

Обично као $k[x]$,

прстена $k[\alpha]$,

$$k[\alpha] = \{ p(\alpha) \mid p(x) \in k[x] \}.$$

Следећа теорема ће се позабавити питањем да ли је у одређеним случајевима $k[\alpha] = k(\alpha)$.

Теорема

(1) Нека је K/k проширење и $\alpha \in K$ алгебарски елемент над k.
Онда постоји монични, иредуцибилни полином $p(x) \in k[x]$ чији је корјен α.
Посебно, за $I = (p(x))$ вриједи

$$k[x]/I \cong k(\alpha).$$

(2) Ако је $\alpha' \in K$ неки други корјен $p(x) \in k[x]$ онда постоји изоморфизам

$$\theta : k(\alpha) \to k(\alpha')$$

тако да је $\theta|_k \equiv \mathrm{id}$, $\theta(\alpha) = \alpha'$.

доказ:

Посматрајмо хомоморфизам (прстена)

$$\varphi : k[x] \to K$$

$$\varphi(f(x)) := f(\alpha).$$

$$\operatorname{Ker} \varphi = \{ f(x) \in k[x] \mid f(\alpha) = 0 \}.$$

$\operatorname{Im} \varphi = k[\alpha]$.

$\operatorname{Ker} \varphi \neq 0$, јер α алгебарски над k.

$\operatorname{Ker} \varphi$ је идеал домена г. идеала $k[x]$, па је $\operatorname{Ker} \varphi$ главни идеал, односно

$\operatorname{Ker} \varphi = (p(x))$, $p(x) \in k[x]$.

Знамо

$$k[x] / \operatorname{Ker} \varphi \cong \operatorname{Im} \varphi.$$

Међутим, $\operatorname{Im} \varphi = k[\alpha]$ је подпрстен K, па је домен.

Закључујемо да $p(x)$ мора бити иреду-цибилан полином.

Без умањења општости можемо подразуми-јевати да је $p(x)$ и моничан.

У том случају, $k[x] / (p(x))$ је поље, што значи да је и $k[\alpha]$ поље.

Закључујемо да је онда $k(\alpha) = k[\alpha]$.

(2) Постоје изоморфизми:

$$\varphi : k[x] / I \to k(\alpha)$$

$$\psi : k[x] / I \to k(\alpha')$$

$\theta = \varphi^{-1} \psi$ је тражени изоморфизам.

<u>Дефиниција</u>

Нека је $K | k$ проширење поља и $\alpha \in K$ алгебарски над k. Јединствени, монични, нерастављиви полином $p(x) \in k[x]$ који има α као коријен, назива се <u>минимални полином</u> од α над k и означава са

$$p(x) = \operatorname{irr}(\alpha, k)$$

Минимални полином $\operatorname{irr}(\alpha, k)$ неравно зависи од k.

На примјер

$$\operatorname{irr}(i, \mathbb{R}) = x^2+1, \quad \operatorname{irr}(i, \mathbb{C}) = x-i.$$

<u>Теорема</u>

Нека су $k \subseteq E \subseteq K$ поља, при чему је E коначно проширење поља k, а K коначно проширење поља E.

Онда је K коначно проширење поља k и

$$[K:k] = [K:E]\cdot[E:k].$$

<u>доказ:</u>

Директно из особина в. простора.

$A = \{a_1, \dots, a_n\}$ база E над k

$B = \{b_1, \dots, b_m\}$ база K над E.

Показати да је

$$\{a_i b_j \mid i=1,\dots,n;\ j=1,\dots,m\}$$

база в. простора K над k.

<u>Теорема</u> (Кронекер)

Ако је k поље и $f(x) \in k[x]$, онда постоји поље K, $k \subseteq K$, тако да се $f(x)$ може разложити на линеарне факторе у $K[x]$.

Доказ:

Тврђење доказујемо индукцијом по $\deg(f(x))$.

За $\deg(f(x)) = 1$, онда $f(x) = ax + b$, $a, b \in k$, што значи $K = k$.

Ако је $\deg(f) > 1$, онда постоји разлагање $f(x) = p(x) \cdot g(x)$, гдје је $p(x)$ иредуцибилан.

Доказали смо у једној од претходних лема да постоји поље F које садржи k и неки коријен z полинома $p(x)$.

Дакле, у $F[x]$ имамо разлагање

$$p(x) = (x - z) \cdot h(x),$$

што значи да је

$$f(x) = (x - z) \cdot h(x) \cdot g(x). \quad (\text{посматрамо у } F[x])$$

Јасно је $\deg(h(x) \cdot g(x)) < \deg(f(x))$.

По индуктивној претпоставци, постоји поље K које садржи F (а тиме и k) у ком полином $h(x) \cdot g(x)$ можемо разложити на линеарне факторе.

Дакле, $f(x)$ се потпуно разлаже на линеарне факторе у $K[x]$.