Комутативни прстени

- дефиниција прстена
- комутативни прстен

примјер

1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

2) $\mathbb{Z}_m$ - прстен цјелобројних остатака по модулу m

3) $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$

Гаусов цјелобројни прстен или прстен Гаусових цијелих

задатак

Испитати да ли је скуп

$$S = \{a + b\omega \mid a, b \in \mathbb{Z}, \ \omega = \sqrt[3]{2}\}$$

прстен у односу на стандардно сабирање и множење.

- подпрстен
- дјелитељ нуле у прстену R

$c \in R$, $c \neq 0$, постоји $d \in R$, $d \neq 0$

$c \cdot d = 0$.

[illegible] c називамо дјелитељем нуле.

Онда c називамо дјелитељ [illegible]

у $\mathbb{Z}_6$, 2 и 3 су дјелитељи нуле, јер $2 \cdot 3 \equiv 0 \pmod 6$

Дефиниција

Домен (интегрални домен) је комутативни прстен који има сљедеће особине

(1) $1 \neq 0$

(2) Из $ca = cb$ и $c \neq 0$ слиједи $a = b$.

Примјери комутативних прстена који су и домени су $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_7$, ... док нула прстен није домен.

Лема Комутативни прстен R, $R \neq \{0\}$, је домен ако и само ако је производ два ненулта елемента ненулти.

Лема Комутативни прстен $\mathbb{Z}_m$ је домен ако и само ако је m прост број.

– Елемент $c \in R$ дијели $d \in R$, ако

постоји $b \in R$ тако да $d = c \cdot b$.
Означавамо са $c \mid d$.

- Елемент $a \in R$ је јединичан (инвертибилан) ако
  $a \mid 1$, односно постоји $a' \in R$
  $a \cdot a' = 1$.
  Елемент a' називамо <u>инверзом</u> елемента $a \in R$.

<u>Лема</u> Нека је R домен, $a, b \in R$ ненулти елементи. Онда $a \mid b$ и $b \mid a$ ако и само ако $b = u \cdot a$, при чему је u инвертибилан елемент.

<u>доказ</u>: $b = u \cdot a$, $a = v \cdot b$,

$$b = (u \cdot v) \cdot b \Rightarrow u \cdot v = 1.$$

<u>задатак</u> Који су инвертибилни елементи у $\mathbb{Z}_m$, $m \in \mathbb{N}$?

$$a \in \mathbb{Z}_m, \quad НЗД(a, m) = 1$$

$$1 = a \cdot a' + m \cdot m'$$

$a \cdot a' = 1$)

<u>Последица</u> Ако је p прост број, онда је сваки $a \in \mathbb{Z}_p$, $a \neq 0$ инвертибилан.

Нека је R комутативан прстен.
Са $U(R)$ означавамо скуп свих јединичних елемената у R.

$$U(R) = \{u \in R \mid u \text{ је инвертибилан у } R\}.$$

Лако закључујемо да је $U(R)$ у односу на множење група.

Посебно,

$$U(\mathbb{Z}_m) = \mathbb{I}_m = \{a \in \mathbb{Z}_m \mid НЗД(a,m)=1\}$$

– дефиниција <u>поља</u>.

<u>Поље $\mathbb{F}$</u> је комутативни прстен, $1 \neq 0$, и сваки ненула елемент $a \in F$ је инвертибилан.

Комутативни прстен R је поље ако и само ако $U(R) = R^* = R \setminus \{0\}$.

<u>Лема</u> Свако поље је домен.

Лема Комутативни прстен $\mathbb{Z}_m$ је поље ако и само ако је m прост број.

- Сваки потпрстен домена је домен.
- сваки потпрстен поља је домен.

Теорема Ако је R домен, онда постоји поље F које садржи R као потпрстен. Посебно, F можемо изабрати тако да за сваки $f \in F$, постоје $a, b \in R$, $b \neq 0$, тако да је $f = a \cdot b^{-1}$.

скица доказа

Нека је $X = \{(a,b) \in R \times R : b \neq 0\}$

$$\frac{a_1}{b_1} = \frac{a_2}{b_2}$$

$$a_1 b_2 = a_2 b_1$$

$$[a_1, b_1] \equiv [a_2, b_2] \iff a_1 b_2 = a_2 b_1$$

Дефинишимо релацију $\equiv$ на X тако да

$$(a,b) \equiv (c,d) \iff ad = bc$$

Докажимо да је $\equiv$ релација еквиваленције.

Означимо са $[a,b]$ класу еквиваленције којој припада (a,b).

Претпостављајући да је $[a,b]$ заправо репрезентација разломка $\frac{a}{b}$, онда

$$F = \{ [a,b] \mid a \in R,\ b \neq 0 \},$$

можемо „опремити" стандардним операцијама

$$[a,b] + [c,d] = [ad+bc,\ bd]$$
$$[a,b] \cdot [c,d] = [ac,\ bd]$$

$b \neq 0$, $d \neq 0$, $bd \neq 0$.

провјерити да ли су операције добро дефинисане.

Лако се показује да је F комутативни прстен.

$[0,1]$ је нула у F.

$[1,1]$ је јединица у F.

Адитивни инверз за $[a,b]$ је $[-a,b]$.

Показати да је

$$R' = \{ [a,1] : a \in R \}$$

потпрстен од F и $R' \cong R$.

Нека је $[a,b] \neq [0,1]$ $\quad [\, a \cdot 1 = b \cdot 0,\ a = 0 \,]$

онда $a \neq 0$.

Дакле, $[b,a] \in F$ и

$$[a,b]\cdot[b,a] = [ab, ba] = [1,1].$$

F је, дакле, поље.

Коначно, ако $b \neq 0$, онда

$[1,b] = [b,1]^{-1}$ па

$$[a,b] = [a,1]\cdot[b,1]^{-1}.$$

__Дефиниција__

Поље F конструисано у претходној теореми домена R назива се __поље разломака__ од R и означава са $\mathrm{Frac}(R)$.

Елемент $[a,b] \in \mathrm{Frac}(R)$ често означавамо са $\frac{a}{b}$, а посебно $[a,1] \in \mathrm{Frac}(R)$ означавамо само са a.

Приметимо да је $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

– потпоље.

Полиноми – дијељење полинома

- Обновити основне дефиниције и појмове.
- полиноми у више промјенљивих
- алгоритам дијељења полинома

<u>Дефиниција</u> Ако су $f(x), g(x) \in K[x]$, гдје је K поље, онда се полиноми $q(x), r(x) \in K[x]$, такви да

$$f(x) = g(x)\cdot q(x) + r(x)$$

$$\deg(r(x)) < \deg(g(x)),$$

називају <u>количник</u> и <u>остатак</u> приликом дијељења $f(x)$ са $g(x)$.

<u>Последица</u> Нека је R комутативан прстен и $f(x) \in R[x]$ монични полином. Ако је $g(x) \in R[x]$, онда постоје $q(x)$ и $r(x) \in R[x]$ тако да

$$g(x) = q(x) f(x) + r(x)$$

гдје је $r(x) = 0$ или $\deg(r) < \deg(f)$.

Дефиниција

Ако је $f(x) \in K[x]$, гдје је K поље, онда елемент $a \in K$, такав да

$$f(a) = 0,$$

називамо <u>коријен</u> $f(x)$ или <u>нула</u> полинома $f(x)$.

Лема

Нека је $f(x) \in K[x]$, K поље и $u \in K$. Онда постоји $q(x) \in K[x]$ тако да

$$f(x) = q(x)(x-u) + f(u).$$

доказ:

$f(x) \in K[x]$, $x - u \in K[x]$.

Алгоритам дијељења обезбјеђује постојање $q(x) \in K[x]$ тако да

$$f(x) = (x-u) \cdot q(x) + r(x)$$

при чему $r(x) = 0$ или $\deg(r) < \underbrace{\deg(x-u)}_{=1}$

$$f(u) = \underbrace{r}_{\text{мора бити константа због } *.}$$

Посљедица

Ако је $f(x) \in K[x]$, K поље, онда је a корјен $f(x)$ у K акко $x-a \mid f(x)$ у $K[x]$.

Теорема

Нека је K поље и $f(x) \in K[x]$, $f(x) \neq 0$. Ако $f(x)$ има степен n, онда $f(x)$ има највише n корјена у K.

доказ

Индукцијом по n.

Ако је $n=0$, онда је $f(x)$ ненулта константа па има 0 корјена.

Нека је $n>0$.

Ако $f(x)$ нема корјена у K, онда је доказ завршен.

У супротном постоји $a \in K$ такво да

У супротном, постоји $a \in K$ т.д.

$$f(x) = q(x)(x-a)$$

Јасно, $\deg(q) = n-1$.

Ако је $b \in K$ коријен $f(x)$,

$$f(b) = 0$$

$$q(b)(b-a) = 0.$$

Подразумијевајући да је $b \neq a$, закључујемо да је $q(b) = 0$.

Међутим, q је степена $n-1$, па по индуктивној претпоставци q може имати највише $n-1$ коријена.

Дакле, f може имати највише n коријена.

Примјер

Претходна теорема не важи у општем случају, односно у окружењу $R[x]$, кад је R комутативни прстен.

На примјер, $R = \mathbb{Z}_8$.

За $x^2 - 1 \in R[x]$ имамо 4 коријена

[1], [3], [5], [7].

Последица

Сви комплексни корјени полинома $X^n - 1$ су $e^{\frac{2\pi i k}{n}} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$

$k = 0, 1, \ldots, n-1$.

Последица

Нека је k бесконачно поље, $f(x), g(x) \in k[x]$. Ако су $f(x)$ и $g(x)$ такви да $f(a) = g(a)$, $a \in k$, онда $f(x) = g(x)$.

доказ

Ако је $f(x) \neq g(x)$, онда $h(x) = f(x) - g(x)$ је полином степена n.

С друге стране сваки $a \in k$ је корјен полинома $h(x)$, а k је бесконачно.

Закључујемо да $h(x) \equiv 0$.

Последица Нека је k поље. Ако су $f(x), g(x)$ $\in k[x]$ такви да $\deg(f) \leq \deg(g) \leq n$,

те ако је $f(a)=g(a)$ за бар $n+1$ $a\in k$,
онда $f(x)=g(x)$.

Теорема

Нека је G коначна подгрупа мултипликативне групе k^*, поља k. $\lceil k^* = k\setminus\{0\}\rfloor$
Тада је G циклична. Посебно, ако је k коначно поље, онда је k^* циклична група.

Доказ

Нека је d дјелитељ $|G|$.
Претпоставимо да постоје двије подгрупе S и T реда d, $S\neq T$.

$$|S\cup T| > d.$$

Међутим, за $a\in S\cup T$ вриједи $a^d=1$.
С друге стране, полином

$$x^d-1\in k[x]$$

може имати највише d нула.
Контрадикција.
Не постоје двије различите подгрупе реда

d.

Дакле, за сваки дјелитељ d, $d \mid |G|$, постоји највише једна подгрупа реда d, а на основу претходно доказане теореме, G мора бити циклична.

<u>Дефиниција</u> Ако је k коначно поље, онда генератор цикличне групе k^* називамо <u>примитивни (генератори)</u> елемент k.

<u>Последица</u> Ако је $n \in \mathbb{N}$, онда скуп свих n-тих коријена јединице неког поља k чини мултипликативну, цикличну групу.