Лема

Нека је R комутативан прстен са јединичним елементом. Нека постоји природан број $n \in \mathbb{N}$, тако да $n \cdot 1 = 0$, а нека је $p \in \mathbb{N}$ најмањи природан број са тим својством.

Онда је

1) $p \cdot R = 0$
2) Ако R нема нетривијалних дјелитеља нуле, онда је p прост број.
3) $mx = 0 \iff p \mid m$ или $x = 0$

Доказ

1) $p \cdot 1 = 0 \implies p \cdot r = p \cdot (1 \cdot r) = (p \cdot 1) \cdot r = 0.$

2) Нека је p сложен број

$$p = r \cdot s$$

$$(r \cdot 1) \cdot (s \cdot 1) = \underbrace{(1 + 1 + \dots + 1)}_{r \text{ пута}} \cdot \underbrace{(1 + 1 + \dots + 1)}_{s \text{ пута}}$$

$$= \underbrace{1^2 + 1^2 + \dots + 1^2}_{r \cdot s \text{ пута}} = p \cdot 1 = 0$$

Слиједи да је $r \cdot 1 = 0$ или $s \cdot 1 = 0$, а што је у контрадикцији са избором броја p.

3) вјежба.

Дефиниција

Домен R је главно-идеалски домен (ГИД)

... R главни.

ако је сваки идеал у R главни.

<u>Примјер</u>

(1) Прстен $\mathbb{Z}$ цијелих бројева је ГИД.

...

$$\underbrace{x}_{\in I} = \underbrace{m \cdot q}_{\in I} + r \qquad 0 \le r < m$$

(2) Свако поље k је ГИД

$a \in I$, $a \neq 0$, постоји $a^{-1} \in k$,

$a \cdot a^{-1} = 1 \in I \Rightarrow I = k$.

<u>Теорема</u>

Ако је k поље, онда је сваки идеал у $k[x]$ главни.
Посебно, ако је $I \neq \{0\}$, онда постоји монични полином који генерише I.

<u>доказ</u>

Парафраза доказа за прстен $\mathbb{Z}$.

<u>примјер</u>

Нека је $R = \mathbb{Z}[x]$, а I скуп свих полинома чији је слободан члан дјељив са 2.

Покажујемо да I јесте идеал, али није главни.

Доказ да је I идеал је тривијалан.

Претпоставимо да је $I = (d(x))$.

Како је $2 \in I$, онда постоји $f(x) \in \mathbb{Z}[x]$, такав да $2 = d(x) f(x)$.

Јасно је да $\deg(d) = \deg(f) = 0$, одакле да су $d(x)$ и $f(x)$ заправо цијели бројеви.

Закључујемо, $d(x)=\pm 1$ или $d(x)=\pm 2$

Нека је $d(x)=\pm 2$. Како је $h(x)=x \in I$, онда постоји $g(x)\in \mathbb{Z}[x]$ тако да

$$x = d(x)\cdot g(x) \Rightarrow x = \pm 2g(x) \quad (*)$$

Сви коефицијенти полинома $\pm 2g(x)$ су парни, док је коефицијент уз x полинома $h(x)$ једнак 1.

Дакле, $d(x)=\pm 1$.

Међутим, у овом случају $I=(d(x))=\mathbb{Z}[x]$.

Контрадикција.

<u>Напомена</u>

Нека је R ГИД, а $\pi, \alpha \in R$, тако да је π иредуцибилан.

$$\text{НЗД}(\pi,\alpha) = \begin{cases} 1, & \text{ако } \pi \nmid \alpha \\ \pi, & \text{ако } \pi \mid \alpha \end{cases}$$

<u>Теорема</u>

Нека је R ГИД

(1) За елементе $\alpha, \beta \in R$ постоји $\delta = \text{НЗД}(\alpha,\beta)$ и
$$\delta = \sigma\alpha + \tau\beta,$$
где је $\sigma, \tau \in R$.

(2) Ако је π иредуцибилни елемент и $\pi \mid \alpha\beta$, онда $\pi\mid\alpha$ или $\pi\mid\beta$.

<u>доказ</u>

(1) Подразумијевамо да је бар један, α или β ненулти елемент из R (у супротном НЗД је нула и резултат је очигледан)

Нека је I задат на следећи начин
$$I = \{ r_1\alpha + r_2\beta : r_1, r_2 \in R \}$$
Очигледно, α и β су у I. Такође, I је идеал у R.
Пошто је R ГИД, онда $I = (\delta)$.
Дакле, $\delta \mid \alpha$ и $\delta \mid \beta$.
Такође, $\delta = \sigma \cdot \alpha + \tau\beta$ (*)
Нека је γ заједнички дјелитељ за α и β.
Онда је $\alpha = \gamma \cdot \alpha'$, $\beta = \gamma \cdot \beta'$, па из (*)
$$\delta = \gamma(\sigma\alpha' + \tau\beta') \Rightarrow \gamma \mid \delta.$$
Дакле $\delta = НЗД(\alpha, \beta)$.

(2) Ако $\pi \mid \alpha$, онда је тврђење доказано.
Ако $\pi \nmid \alpha$, онда $НЗД(\pi, \alpha) = 1$, а из (1)
слиједи $1 = \sigma\pi + \tau\alpha$
$$\Rightarrow \beta = \sigma\pi\beta + \tau\alpha\beta$$
Како $\pi \mid \alpha\beta \Rightarrow \pi \mid (\sigma\pi\beta + \tau\alpha\beta) \Rightarrow \pi \mid \beta$.

<u>Задатак</u>
Ако су I и J идеали у R, онда је $I \cap J$ идеал у R.

<u>Еуклидови прстени</u>
Идеја за Е. прстене потиче од погледе генерализације алгоритма дијељења.

<u>Дефиниција</u>
Еуклидски прстен је домен R на коме постоји функција

[illegible]

$$\delta : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

коју називамо <u>функција степена</u> са особинама:

(1) $\delta(f) \leq \delta(f \cdot g)$ за $f, g \in R \setminus \{0\}$.

(2) За $f, g \in R$, $f \neq 0$, постоје $q, r \in R$

такво да $\quad g = qf + r$

за које вриједи $r = 0$ или $\delta(r) < \delta(f)$.

У случају да је $\delta \equiv 0$, онда из (2) $\Rightarrow$ да је $r = 0$.
Ако за g одаберемо 1, онда је произвољно f инвертибилно, па је R поље.

<u>примјер</u>

(1) За домен $\mathbb{Z}$, функција степена

$$\delta : \mathbb{Z} \setminus \{0\} \to \mathbb{N} \cup \{0\} \text{ је}$$

$$\delta(z) = |z|.$$

(2) Ако је k поље, онда је

$$\delta : k[x] \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

$$\delta(p(x)) = \deg(p(x)).$$

<u>Теорема</u>

Сваки Е. прстен је ГИД.

<u>Рекапитулација</u>: Основи линеарне алгебре