ДА Касиярян ~~16. 04~~
1 г

1 г. 04 Конституция ХФ 601
18 04 Диференц ХФ 604 13-15 г сам →
упр ДА 1 поп 13-15 526 ФМИ
22 04 - 13 г контролно ХФ 604

Пръстени и подпръстени - опр
примери основни св-ва
Нер $Q \neq 0$ е пръстен ако са операции
$R \times R \to R(\cdot, \cdot) \to z+s$ и $Z \times R \to R(\cdot, \cdot) \to zs$
т. Z
1) R_+ е абелева гр
2) $(R, \cdot)$ е асоц
3) Дистр зак-ни $(a+b)c = ac+bc$
$a(b+c) = ab+ac$. $0_R \in R$, $0_R + z = z$, за $\forall z \in R$ $\exists -z \in R$
с $z + (-z) = 0_R$

Нер
Пръстенът R е комутативен ако
$z.s = s.z$ за $\forall z, s \in R$

Примери
// и числовите полета F са комутативни
За $n \in \mathbb{N}$ $n \geq 2$ матриците $M_{n \times n}(F)$
образуват некомутативен пръстен.
~~Т. a, b~~ Т. $A, B \in M_{n \times n}(F)$ сбс $AB + BA$

$$A = \begin{pmatrix} \frac{1}{3} & \frac{2}{4} & 0 \\ 0 & 0 & 0 \end{pmatrix}_{n-2}^{2} \qquad B = \begin{pmatrix} \frac{5}{7} & \frac{6}{8} & 0 \\ 0 & 0 & 0 \end{pmatrix}_{n-2}^{2}$$

~~AB~~ $= \begin{pmatrix} 19 & \\ \hline & T \end{pmatrix}$

Блочно разлагане

$$\begin{pmatrix} \frac{5}{7} & \frac{6}{8} & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{3} & \frac{2}{4} & 0 \\ 0 & 0 & 0 \end{pmatrix} = BA = \begin{pmatrix} 23 & & 0 \\ \hline & & \\ 0 & & 0 \end{pmatrix}$$

Деф Делител на нулата

Елементът $a \in R \setminus \{0_R\}$ е делител на нулата в R ако $\exists\, s \in R \setminus \{0_R\}$ с $as = 0_R$ или $sa = 0_R$

Примери

$\mathbb{Z}$ и числовите полета F нямат делители на нулата

Матриците $M_{n\times n}(F)$ за $n \geq 2$ имат

Например

$$2\begin{pmatrix} \begin{matrix} 2 & 0 \\ \pm 1 & 0 \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \end{matrix} & \begin{matrix} 0 \end{matrix} \end{pmatrix} \; 2\begin{pmatrix} \begin{matrix} 0 & 2 \\ \pm 1 & 0 \end{matrix} & \\ & \end{pmatrix} = \begin{pmatrix} \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \end{matrix} & \begin{matrix} 0 \end{matrix} \end{pmatrix} = 0_{n\times n}$$

$n-2$

Деф

Пръстен R без делители на нулата се нарича област

Деф

Пръстенът R е тяло ако има единица и $\forall$ ненулев елемент $a \in R \setminus \{0_R\}$ е обратим относно умножението, т.е. $R^* = R \setminus \{0_R\}$

Деф

Комутативно тяло се нарича поле

Примери

$\mathbb{Z}$ Не е поле т.к. $\mathbb{Z}^* = \{\pm 1\}$ (Ако $z \in \mathbb{Z}^*$, $\exists\, b \in \mathbb{Z}$ с $zb = 1 \Rightarrow z = b = \pm 1$)

комутативен но не е поле

$\forall$ числово поле F е поле т.к $F^* = F \setminus \{0\}$

R^* - мултипликативна група

За $n \geq 2$ $M_{n\times n}(F)$ не образува поле т.к $M_{n\times n}(F)^* = GL(n,F) = \{A \in M_{n\times n} / \det A \neq 0\}$ Това множество се сбърка с $\forall C \in M_{n\times n}(F)$ с $\det C = 0$ не е обратима. Напри

$$C = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ c_{n1} & \dots & c_{nn} \\ 0 & \dots & 0 \end{pmatrix} \in M_{n\times n}(F) \setminus \{0_F\}$$ не е обратима $M_{n\times n}(F)$ сбс $c_{ij} \neq 0$

Следствия от аксиомите

1) Ако R е пръстен то $(R,+)$ е група така че нулата на R е единствена, като неутрален елемент на адитивната група $(R,+)$. Всеки елемент $\in R$ има единствен противоположен $(-\varepsilon) \in R$

2) Ако R е пръстен сбс единица то множеството R^* на обратимите относно умножението елементи на R е група $(R^*, \cdot)$ относно умножението. Отгук $\Rightarrow$ че единицата на R е единствена и всеки $\varepsilon \in R^*$ има единствен обратен $\varepsilon^{-1} \in R^*$ относно умножението т.е $\varepsilon\varepsilon^{-1} = \varepsilon^{-1}\varepsilon = 1_R$

3) Ако R е пръстен, $a \in R$ то $a0_R = 0_R$ и $0_R a = 0_R$

Док

За $\forall b \in R$ е в сила $a0_R + ab \overset{\text{дистр}}{=} a(0_R + b) = ab$

Прибавяне $-(ab) \in R$ към 2-те страни и получаване

$$a0_R = a0_R + 0_R = a0_R + [ab + (-(ab))] = (a0_R + ab) + [-(ab)] = ab + [-(ab)] = 0_R$$

Zom 17

Сл 4) Ако R е пръстен $a, b \in R$ то $-(a+b) = (-a)+(-b)$.

Док
адитивната гр
$(R,+)$ елементът $-(a+b)$ е единственото решение на $x+(a+b)=0_R$. Но $(-a)+(-b)$ е също решение на това уравнение защото $[(-a)+(-b)]+(a+b) = [(-a)+(-b)]+(b+a)$ комутативно

$(-a)+[(-b)+b]+a = (-a)+0_R+a = (-a)+a = 0_R$

откъдето $(-a)+(-b) = -(a+b)$ □

Сл 5) Ако $a, b \in R$ за пръстен R то $-(ab) = (-a)b = a(-b)$

Док

Знаем че $-(ab) \in R$ е единственото решение на $ab+x=0_R$. От $ab+(-a)b = [a+(-a)]b = 0_R b \overset{сл3}{=} 0_R$ и $ab+a(-b) = a[b+(-b)] = a0_R \overset{сл3}{=} 0_R$ следва че $(-a)b$ и $a(-b)$ са решения на това ур-е откъдето $\Rightarrow -(ab) = (-a)b = a(-b)$ □

Сл 6) Ако R е пръстен $a, b, c \in R$ то $(a-b)c = ac-bc$ и $a(b-c) = ab-ac$

По определение $ac-bc$ е единственото решение на $x+bc=ac$. От $(a-b)c+bc = [(a-b)+b]c = ac$ следва че $(a-b)c$ е също решение на $x+bc=ac$ откъдето единственото решение $ac-bc = (a-b)c$ □

Сл 8) Ако R е пръстен със единица $e \in R^*$, то e не е делител на нулата

Док.

Допускаме противното. Ако $\varepsilon s = 0_R$ за $s \in R \setminus \{0_R\}$ то лявото почленно умножение със ε^{-1} дава

$s = 1_R s = (\varepsilon^{-1}\varepsilon)s = \varepsilon^{-1}\varepsilon s = \varepsilon^{-1} 0_R = 0_R \to s = 0_R$

Противоречието доказва че обратимите елементи не делят нулата (аналогично от $s\varepsilon = 0_R$ с $\varepsilon \in R^*$ отдясно

$0_R = 0_R \varepsilon^{-1} = \varepsilon s \varepsilon^{-1} = s(\varepsilon\varepsilon^{-1}) = s 1_R = s$ - противоречие $\square$

Сл 8)

Ако R е тяло или поле то R е област

Док Сл 6

Зад. Е-ва области които не са тела или полета

Например простият $\mathbb{Z}$ на целите числа е област но не е поле.

Сл 9) Ако R е крайна област със единица 1_R то R е тяло. (всеки ненулев е е обратим)

Док

За произволно $x \in R \setminus \{0_R\}$ разглеждаме лявото умножение $L_x : R \setminus \{0_R\} \to R \setminus \{0_R\}$, $L_x(\varepsilon) = x\varepsilon$ със x. Ако $x\varepsilon = L_x(\varepsilon) = L_x(s) = xs$ то $0_R = x\varepsilon - xs = x(\varepsilon - s)$ с $x \neq 0_R$. В областта R оттук следва че $\varepsilon - s = 0_R$ или $\varepsilon = s$

Следователно броят на елементите

разл $|L_x(R \setminus \{0_R\})| = |R \setminus \{0_R\}|$ инжекция

следователно от $L_x(R \setminus \{0_R\}) \subseteq R \setminus \{0_R\}$ следва съвпадение на $L_x(R \setminus \{0_R\}) = R \setminus \{0_R\}$ оттук $1_R \in R \setminus \{0_R\} = L_x(R \setminus \{0_R\})$ или $\exists\, y \in R \setminus \{0_R\}$ със

$xy = L_x(y) = 1_R$ с други думи $\exists$

десен обратен у на x. Аналогично
$R_x : R\setminus\{0_R\} \to R\setminus\{0_R\}$ което на
$R_x(\varepsilon) = \varepsilon x$ е взаимно еднозначно с образа си
тъй като $R_x(R\setminus\{0_R\}) \subseteq R\setminus\{0_R\}$, $|R_x(R\setminus\{0_R\})| =$
$|R\setminus\{0_R\}|$ и $R_x(R\setminus\{0_R\}) = R\setminus\{0_R\}$. Сега 1_R
е ненулев елемент а оттам
$1_R \in R\setminus\{0_R\} = R_x(R\setminus\{0_R\})$ т.е $\exists z \in R\setminus\{0_R\}$
с $1_R = R_x(z) = zx$. елементът z е
ляв обратен на x. В резултат
$$y = 1_R y = (zx)y = z(xy) = z1_R = z$$
т.е $y = z = x^{-1}$ е обратен на $x \in R\setminus\{0_R\}$ и
$R^* = R\setminus\{0_R\}$. По определение R е тяло □

Деф
Непразното подмножество S на пръстен R се
подпръстен ако за $\forall a,b \in S$ е в сила
$a+b, a-b, ab \in S \iff S$ за е подгрупа
$(S,+) \leq (R,+)$ и за $\forall a,b \in S$ е в сила $ab \in S$ и
за $\forall ab \in S$ е в сила $a-b, ab \in S$

Деф
Ако F е поле то подмножеството $E \neq \emptyset \subseteq F$
е подполе ако за $\forall a,b \in E$ е в сила $a+b, a-b$ и
$ab^{-1} \in E$ (при $b \neq 0_F$) $\iff$ за $\forall ab \in E$ е в сила
$a-b, ab^{-1}$ (при $b \neq 0_F$) $\in E \iff (E,+) \leq (F,+)$ и $(E\setminus\{0_F\}, \cdot) \leq$
$F^* = (F\setminus\{0_F\}, \cdot)$

Например $\forall$ числово поле F е поле
Ако F е поле то $\forall$ подполе E на F е
подпръстен. $\exists$ пръстени на
полета които не са полета. Например
$\mathbb{Z}$ е подпръстен на полетата $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ но не е
подполе

Заб Ако S е подпръстен на пръстен R то $(S,+) \leq (R,+)$, т.е. $0_R \in S$ и така $0_R = 0_S$
Освен това за $\forall s \in S \Rightarrow -s \in S$. Аналогично
Ако E е подполе на поле F, то $(E\setminus\{0_E\},\cdot) \leq (F^*=F\setminus\{0_F\},\cdot)$
т.е. $1_F \in E$ и така $1_E = 1_F$. За $\forall e \in E\setminus\{0\}$ е в сила $e^{-1} \in E$

Лема (i)
Ако $\{R_\alpha\}_{\alpha\in A}$ е фамилия от подпръстени на пръстен R то $\bigcap_{\alpha\in A} R_\alpha$ е подпръстен на R

(ii) Ако $\{E_\alpha\}_{\alpha\in A}$ са подполета на поле F, то $\bigcap_{\alpha\in A} E_\alpha$ е подполе на F.

Док(i)
Ако $a,b \in \bigcap_{\alpha\in A} R_\alpha$ то $a,b \in R_\alpha$ за $\forall \alpha \in A$. Оттук $a-b, a\cdot b \in R_\alpha$ за $\forall \alpha \in A$. тк R_α е подпръстен на R
С други думи $a-b, a\cdot b \in \bigcap_{\alpha\in A} R_\alpha$ и $\bigcap_{\alpha\in A} R_\alpha$ е подпръстен на R

Док(ii)
Ако $x,y \in \bigcap_{\alpha\in A} E_\alpha$ то $x,y \in E_\alpha$ за $\forall \alpha \in A$. Понеже
E_α е подполе на $F \Rightarrow x-y, x\cdot y^{-1} \in E_\alpha$ за $\forall \alpha \in A$
Следователно $x-y, x\cdot y^{-1} \in \bigcap E_\alpha$ и $\bigcap_{\alpha\in A} E_\alpha$ е подполе на F □