6/3/08
(1)

הרצאה 12 ~~אלגברה~~ אלגברה לינארית

הגדרנו $\mathbb{Z}_n = \mathbb{Z}/\sim$

$x \sim y \Leftrightarrow (x-y) \vdots n$

$\mathbb{Z}_n = \{[0],[1],\dots,[n-1]\}$

נכון שאלה כל האיברים בקבוצה הנ"ל: $[x]$

$x = an+k$

$0 \le k < n$

$x-k \vdots n \Rightarrow [x]=[k]$

נגדיר פעולות חיבור וכפל בקבוצה $\mathbb{Z}_n$:

$[x]+[y]=[x+y]$

$[x]\cdot[y]=[xy]$

$[x+y] \stackrel{?}{=} [x'+y'] \Leftarrow \begin{array}{l}[x]=[x'] \\ [y]=[y']\end{array}$

דוגמה $\underline{n=2}$ $\{[0],[1]\}=\mathbb{Z}_2$

$[1]+[1]=[0]$

נוכיח: $\begin{cases} x-x'=n\cdot a \Leftarrow [x]=[x'] \\ y-y'=n\cdot b \Leftarrow [y]=[y'] \end{cases}$

$\begin{cases} x=x'+na \\ y=y'+nb \end{cases}$

$x+y=(x'+y')+n(a+b)$

חיבור ב-$\mathbb{Z}_n$ מוגדר היטב $\Leftarrow [x+y]=[x'+y'] \Leftarrow (x+y)-(x'+y') \vdots n$

נבדוק את הכפל:

$[x\cdot y] \stackrel{?}{=} [x'\cdot y'] \stackrel{?}{\Leftarrow} \begin{array}{l}[x]=[x'] \\ [y]=[y']\end{array}$

$\begin{cases} x'=x+na \\ y'=y+nb \end{cases}$ $a,b\in\mathbb{Z}$

$x'\cdot y'=(x+na)(y+nb)=xy+xnb+nay+n^2ab = xy+n\underbrace{(xb+ay+nab)}_{c\in\mathbb{Z}}$

לכן $x'y'-xy \vdots n$ ומכאן שגם הכפל מוגדר היטב. מש"ל

האיבר הניטרלי ביחס לחיבור ב- $\mathbb{Z}_n$ הוא $[0]$.

האיבר הניטרלי ביחס לכפל ב- $\mathbb{Z}_n$ הוא $[1]$.

נבדוק שהאיבר הניטרלי הוא אכן $[0]$:

$$[x]+[0] \stackrel{?}{=} [x]$$

$$[x]=[x+0] \quad \text{(לפי הגדרת החיבור)}$$

$$[x]\cdot[1]=[x\cdot 1]=[x]$$

<u>טענה</u>: כפל וחיבור הם קומוטטיביים, אסוציאטיביים וגם הדיסטריבוטיביות מתקיימת. לכל איבר ב- $\mathbb{Z}_n$ יש איבר נגדי.

<u>הוכחה</u>: *נוכיח דיסטריבוטיביות: $[a]\cdot([b]+[c])=[a][b]+[a][c]$

$$[a]\cdot[b+c]=[a(b+c)]=[ab+ac]=[ab]+[ac]=[a][b]+[a][c]$$

(אסוציאטיביות וקומוטטיביות מוכחות באותה צורה)

* $-[x]=[-x]$

$$[x]+[-x]\stackrel{?}{=}[0]$$

$$=[x+(-x)]$$

<u>מש"ל</u>

<u>משפט</u>: $\mathbb{Z}_n$ שדה $\iff$ n ראשוני.

<u>הוכחה</u>: נניח ש- n לא ראשוני ונוכיח ש- $\mathbb{Z}_n$ לא שדה.

נראה שהתכונה שאין מחלקי אפס: $\underset{\neq 0\ \neq 0}{\alpha,\beta}\in F \Rightarrow \alpha\beta\neq 0$ לא מתקיימת.

(כי n לא ראשוני) $\to n=n_1\cdot n_2$ כאשר $n_1,n_2\in\mathbb{N}$, $n_1,n_2\neq 1$

$1<n_1,n_2<n \Rightarrow [n_1]\neq 0$, $[n_2]\neq 0$

$[n_1]\cdot[n_2]=[n]=[0] \Rightarrow$ לא שדה $\mathbb{Z}_n$

נניח ש- n ראשוני ונוכיח ש- $\mathbb{Z}_n$ שדה.

יהי $[0]\neq\alpha\in\mathbb{Z}_n$. נתבונן בפונקציה $f:\mathbb{Z}_n\to\mathbb{Z}_n$ שמוגדרת ע"י $f(t)=\alpha\cdot t$ לכל $t\in\mathbb{Z}_n$. מספיק להוכיח ש- f היא על

($\Leftarrow$ קיים t כך ש $f(t)=1$)

$$\alpha t=1$$

אנו יודעים ש- $\mathbb{Z}_n$ קבוצה סופית, לכן מספיק להוכיח כי f חח"ע.

$$f([x])=f([y])$$

$$\alpha[x]=\alpha[y]$$

$[ax]=[ay]$ $\qquad$ $\underset{\mathbb{Z}_n}{\alpha=[a]}$ (a נציג של α) $\quad a\in\mathbb{Z}$

$ax-ay \vdots n$

$a(x-y)\vdots n$

עובדה: אם מספר ראשוני n מחלק מכפלה של שני מספרים שלמים אז הוא מחלק לפחות אחד מהם.

n מחלק את המכפלה $a\cdot(x-y)$ לכן אחד הגורמים חייב להתחלק ב-n כלומר $n \mid a$ או $n \mid (x-y)$

$$\alpha \overset{!!}{=} [a] = [0]$$

זו סתירה! (כי הנחנו $\alpha \neq 0$) לכן $n \mid x-y \Rightarrow [x]=[y]$

כלומר f חח"ע. מש"ל

$[$ $f: X \to X$, $|X|<\infty$ (סופית) אז f על $\iff$ f חח"ע $]$

הערות: (1) $Z_2=\{[0],[1]\}$ (זה השדה שהכרנו בשיעור שעבר)

(2) $Z_3=\{[0],[1],[2]\}$

$$-[1]=[2]$$
$$-[2]=[1]$$

(3) Z_4 לא שדה כי $[2][2]=[0]$

מציין של שדה (characteristic)

יהי F שדה

הגדרה: אם לכל מספר טבעי n $\underbrace{1+1+\dots+1}_{n \text{ פעמים}} \neq 0$ נגיד שמציין של F=0. אחרת, מציין של F זה המספר הטבעי המינימלי של n שמקיים

$$\underbrace{1+1+\dots+1}_{n}=0$$

סימון: $\operatorname{char} F$

דוגמאות

(1) $\operatorname{char} \mathbb{R}=0$

(2) $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{C} = 0$

(3) יהי p ראשוני. נחשב $p = \operatorname{char} Z_p$

$$\underbrace{[1]+\dots+[1]}_{p} = [\overbrace{1+\dots+1}^{p}] = [p] = [0]$$

$$\underbrace{[1]+\dots+[1]}_{k<p} = [k] \neq [0] \quad 1 \le k < p$$

משפט: $\operatorname{char} F$ תמיד או 0 או מספר ראשוני.

הוכחה: נניח $n=\operatorname{char} F \neq 0$. נניח בשלילה כי $n=n_1 n_2$, $1<n_1,n_2<n$

נסמן $0 \neq x = \underbrace{1+\dots+1}_{n_1}$.

נתבונן בסכום $\underbrace{x+\dots+x}_{n_2} = x\underbrace{(1+\dots+1)}_{n_2}$

נסמן $0 \neq y = \underbrace{1+\dots+1}_{n_2}$

$$\underbrace{x+\dots+x}_{n_2} = x \cdot y \neq 0$$

$$\underbrace{\underbrace{(1+\dots+1)}_{n_1}+\dots+\underbrace{(1+\dots+1)}_{n_1}}_{n_2} = \underbrace{1+\dots+1}_{n} = \underline{0}$$

סתירה

מש"ל

תרגיל $\mathrm{char}F = p \neq 0$

(א) לכל $x\in F$ $\underbrace{x+\dots+x}_{p} = 0$

(ב) אם $n\in\mathbb{N}$ שמקיים $\underbrace{1+\dots+1}_{n}=0$ אזי $n \vdots p$.

משפט: אם F שדה סופי אזי $|F| = p^r$ כאשר p ראשוני, $\in\mathbb{N}$

ו- $p = \mathrm{char}F$

תרגיל: אם F שדה סופי אזי $\mathrm{char}F \neq 0$

יהי V מ"ו מעל שדה F

דוגמה: $F^n = \{(x_1,x_2,\dots,x_n) | x_i\in F\}$

סכום של שני מרחבים

הגדרה: יהיו $M,N\subset V$ תתי מרחבים. הסכום שלהם הוא:

$$M+N = \mathrm{span}\{M\cup N\}$$

טענה: $M+N = \underbrace{\{a+b \mid a\in M \,,\, b\in N\}}_{\text{נסמן ב-}T}$

הוכחה:

ברור ש- $T\subset M+N$. נוכיח הכלה בכיוון השני.

יהי $x\in M+N$ ו- $x = \underbrace{\sum_i \lambda_i a_i}_{\in M} + \underbrace{\sum_j \mu_j b_j}_{\in N}$ כאשר $a_i\in M$ ו- $b_j \in N$,

(M ו- N תתי מרחבים לכן אם a שייך ל- M כל צירוף לינארי שלו שייך ל- M)

$a\in M$, $b\in N$ <= $x=a+b\in T$ לכן $M+N\subset T$

הגדרה: יהיו $M_1,\dots,M_s\subset V$ תתי-מרחבים.

נגדיר $M_1+\dots+M_s = \mathrm{span}(M_1\cup\dots\cup M_s)$

טענה: $M_1+\dots+M_s=\{a_1+\dots+a_s \mid a_i\in M_i$ לכל $i=1,\dots,s\}$

(ההוכחה מושארת כתרגיל - אפשר באינדוקציה)

משפט: יהיו $M,N\subset V$ תת-מרחב ב-V ונניח M,N ממימד סופי. אזי $M+N$ ממימד סופי ו-$\dim(M+N)=\dim M+\dim N-\dim(M\cap N)$

הוכחה: $M\cap N\subset M$ $\Leftarrow$ $M\cap N$ ממימד סופי.

$k=\dim(M\cap N)$. יהי $c_1,\dots,c_k$ בסיס כלשהו ב-$M\cap N$

$M\cap N\subset M$ לכן כל סדרה בת"ל ב-M ניתן להשלים עד לבסיס של M:

$c_1,\dots,c_k,a_1,\dots,a_{m-k}$ כאשר $m=\dim M$

באופן דומה נשלים את c_i-ים עד לבסיס של N:

$c_1,\dots,c_k,b_1,\dots,b_{m-k}$ כאשר $n=\dim N$.

אנו טוענים שהסדרה $c_1,\dots,c_k,a_1,\dots,a_{m-k},b_1,\dots,b_{n-k}$ (*) בסיס של $M+N$.

$$\dim(M+N)=k+(m-k)+(n-k)=m+n-k=\dim M+\dim N-\dim(M\cap N)$$

נוכיח קודם כי שהסדרה (*) פורשת את $M+N$. יהי $z\in M+N$

$$z=x+y,\quad x\in M,\ y\in N$$

$$x=\sum_i\lambda_ic_i+\sum_j\mu_ja_j$$

$$y=\sum_i\lambda_i'c_i+\sum_l\nu_lb_l$$

נחבר את שתי המשוואות:

$$z=x+y=\sum_i(\lambda_i+\lambda_i')c_i+\sum_j\mu_ja_j+\sum_l\nu_lb_l$$

לכן (*) פורשת את $M+N$.

נוכיח ש-(*) בת"ל. נניח $\underbrace{\sum_i\lambda_ic_i+\sum_j\mu_ja_j}_{x\in M}+\underbrace{\sum_l\nu_lb_l}_{y\in N}=0$

$$M\ni x=-y\in N$$

$$\boxed{x\in M\cap N}$$

לכן $x=\sum_i\lambda_i'c_i$ ומכאן ש

$$\sum_i\lambda_ic_i+\sum\mu_ja_j=\sum_i\lambda_i'c_i$$

$$\sum_i(\lambda_i-\lambda_i')c_i+\sum\mu_ja_j=0$$

אבל $c_1,\dots,c_k,a_1,\dots,a_{m-k}$ בת"ל $\Leftarrow$ $\lambda_i-\lambda_i'=0$ וגם $\boxed{\mu_j=0}$ לכל j

אבל $\sum_i\lambda_ic_i+\sum_l\nu_lb_l=0$ אבל $c_1,\dots,c_k,b_1,\dots,b_{n-k}$ לכן

$\lambda_i=0$ לכל i

$\nu_l=0$ לכל l

מש"ל