הרצאה 25

תזכורת: שדה F, הערכה על F הינה פונקציה.

$|\cdot|: F \to \mathbb{R}_{\geq 0}$ שמקיימת:

א) $|a| = 0 \iff a = 0_F$

ב) $|ab| = |a| \cdot |b|$ לכל $a,b \in F$.

ג) $|a+b| \leq |a| + |b|$ לכל $a,b \in F$.

אם נגדיר $d(a,b) = |a-b|$, אזי F מקבל מבנה של מרחב מטרי ובפרט של מרחב טופולוגי.

הגדרה: ההערכה $|\cdot|$ נקראת לא-ארכימדית אם

$$|a+b| \leq \max\{|a|, |b|\}$$

ההשלמה של F עבור ההערכה $|\cdot|$ הינה $\hat{F} = R/I$ כאשר

$R = \{ \{a_n\}_{a_n \in F}$ סדרות קושי $\}$

$I = \{$ סדרות האפסיות $\} \triangleleft R$

הנורמות ה-p-אדיות. יהי p ראשוני: אזי $F=\mathbb{Q}$,

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$$

$$|a|_p = \begin{cases} 0, & a=0 \\ \dfrac{1}{p^c} & a = \dfrac{m}{n} = p^c \dfrac{m'}{n'} \end{cases}$$

$p \nmid m'$
$p \nmid n'$

דוגמא $p=3$

$$a = \frac{117}{5}$$

$$a = \frac{3^2 \cdot 13}{3^0 \cdot 5} = 3^2 \cdot \frac{13}{5}$$

$$|a|_3 = \frac{1}{9}$$

משפט (אוסטרובסקי) תהי $|\cdot|$ הנורמה לא-טריוויאלית על $F=\mathbb{Q}$. אזי $|\cdot|$ שקולה או ל-$|\cdot|_p$ עבור p ראשוני, או ל-$|\cdot|_\infty$ (הערך המוחלט הרגיל).

שתי הנורמות נקראות שקולות אם יש להן אותה טופולוגיה מטרית.

<u>הוכחה</u> תהי $|\cdot|$ הנורמה על $\mathbb{Q}$, לא-טריוויאלית עובדה: אם $|\cdot|$ ארכימדית, אזי $|\cdot|$ שקולה ל-$|\cdot|_\infty$.

אם תהי $|\cdot|$ לא-ארכימדית. אזי $|n|\le 1$ לכל $n\in\mathbb{Z}$. אכן $|1|=1$

$$|2|=|1+1|\le\max\{|1|,|1|\}=1$$
$$|3|=|2+1|\le\max\{|1|,|2|\}=1$$
$$\vdots$$

באינדוקציה, $|n|\le 1$ לכל $n\in\mathbb{N}$.

$$|-1|^2=|1|=1 \Rightarrow |-1|=1$$

לכן $|n|=|-n|$.

נגדיר בקבוצה $I=\{n\in\mathbb{Z} : |n|<1\}$.

אזי $I\neq(0)$, כי $|\cdot|$ לא-טריוויאלית לפי הנחה.

ברור כי $I\lhd\mathbb{Z}$ אידאל אמיתי. $(1\notin I)$

$a,b\in I$, אזי $|a+b|\le\max\{|a|,|b|\}<1 \Rightarrow a+b\in I$.

$a\in I$, $n\in\mathbb{Z}$, $|an|=\underbrace{|a|}_{<1}\cdot\underbrace{|n|}_{\le 1}<1 \Rightarrow an\in I$.

יתר מזה, I הינו אידיאל ראשוני, כי

$n,m\in\mathbb{Z}$, $nm\in I \Rightarrow |n|\cdot|m|<1$. אך $|n|\le 1$, $|m|\le 1$

ולכן $|n|<1$ או $|m|<1$.
$n\in I$ $\quad$ $m\in I$

לכן קיים מספר ראשוני p יחיד כך ש- $I=p\mathbb{Z}$.

עכשיו, יהי $0\neq a\in\mathbb{Q}$, $\;p\nmid m'$, $p\nmid n'$, $\;a=p^c\frac{m'}{n'}$.

אז $m'\in\mathbb{Z}\setminus I \Rightarrow |m'|=1$

$n'\in\mathbb{Z}\setminus I \Rightarrow |n'|=1$ $\;\Rightarrow |a|=|p|^c\cdot\frac{1}{1}=|p|^c$.

$s=-\log_p|p|$

$s\in\mathbb{R}$

ידוע לנו כי $p\in I \Rightarrow |p|<1 \Rightarrow$ קיים $s>0$

כך ש- $|p|=\frac{1}{p^s}$

לכן, $|a|=|p|^c=\frac{1}{p^{cs}}=|a|_p^s$ לכל $0\neq a$.

קיבלנו: $|a|=|a|_p^s$ לכל $a\in\mathbb{Q}$. לכן להערכות

$|\cdot|_p$, $|\cdot|$ יש אותו אוסף של כדורים פתוחים,

לכן אותה טופולוגיה מטרית, לכן $|\cdot|_p, |\cdot|$ שקולות.

הגדרה תהי $\mathbb{Q}_p$ ההשלמה של $\mathbb{Q}$ עבור הנורמה ה-p-אדית.

תוצאה של אוסטרובסקי כל ההשלמות של $\mathbb{Q}$ הן:

$\mathbb{Q}_p$, p ראשוני

$\mathbb{Q}_\infty = \mathbb{R}$, הממשיים

תזכורת יהי $\alpha \in \mathbb{Q}_p$ $\qquad \alpha = [\{a_n\}]$

$\mathbb{Q}_p = R/I$

$a_n \in \mathbb{Q}$

$\{a_n\}$ סדרת קושי

עבור $|\cdot|_p$.

ראינו בשיעור הקודם שאפשר להגדיר $|\cdot|$ הנורמה

על $\mathbb{Q}_p$ ע"י $|\alpha| = \lim_{n\to\infty} \underbrace{|a_n|_p}_{\in\mathbb{R}}$.

נשים לב כי לכל $a \in \mathbb{Q}$,

$$|a|_p \in \{0, 1, p, p^2, p^3, \dots, p^{-1}, p^{-2}, p^{-3}, \dots\}$$

בקבוצה הנ"ל יש רק נקודת אוסף אחת, כלומר 0.

לכן, אם $\{a_n\}$ הינה סדרת קושי לא אפסית,
אזי הסדרה $|a_n|_p$ מתייצבת, כלומר קיים $N\in\mathbb{N}$
וקיים $m\in\mathbb{Z}$ כך ש- $|a_n|_p=p^{-m}$ לכל $n\geq N$.

<u>הגדרה</u> יהי $\mathbb{Z}_p$ חוג ההערכה של $\mathbb{Q}_p$

$$\mathbb{Z}_p=\mathcal{O}=\{a\in\mathbb{Q}_p:|a|\leq 1\}$$

זה חוג מקומי (הוכחנו בשיעור הקודם) עם אידיאל מקסימלי יחיד $I=\{a\in\mathbb{Q}_p:|a|<1\}$.

<u>טענה</u> יהי $0\neq\alpha\in\mathbb{Q}_p$. אזי קיים $m\in\mathbb{Z}$ כך
ש- $\alpha=p^m u$, כאשר $u\in\mathbb{Z}_p$ הפיך ($\Leftrightarrow |u|=1$)

<u>הוכחה</u> יהי $0\neq\alpha\in\mathbb{Q}_p$. תהי $\{a_n\}$ סדרת קושי
של רציונליים במחלקה α. זה אומר כי $\{a_n\}$
לא אפסית (כי $\alpha\neq 0$). לכן הסדרה $|a_n|_p$ מתייצבת.
אזי $|a_n|_p=p^{-m}$ לכל $n\geq N$.

אזי, לכל $n \geq N$, $\left|\frac{a_n}{p^m}\right|_p = \frac{|a_n|_p}{|p^m|_p} = \frac{p^{-m}}{p^{-m}} = 1$. לכן,

$$\lim_{n\to\infty} \left|\frac{a_n}{p^m}\right|_p = 1,$$ (כמובן $\left\{\frac{a_n}{p^m}\right\}_n$ סדרת קושי)

לכן, $\alpha = p^m u$

כאשר $u = \left[\left\{\frac{a_n}{p^m}\right\}\right]$.

<u>טענה</u> יהי $0 \neq J \triangleleft \mathbb{Z}_p$ אידיאל אמיתי, לא אפסי. אזי קיים $m \in \mathbb{N}$ יחיד כך ש- $J = (p^m)$.

<u>הוכחה</u> יהי $0 \neq J \triangleleft \mathbb{Z}_p$ אידיאל אמיתי. ידוע לנו כי לכל $0 \neq \alpha \in \mathbb{Z}_p$,

$$|\alpha| = \lim_{n\to\infty} |a_n|_p \in \left\{1, \frac{1}{p}, \frac{1}{p^2}, \frac{1}{p^3}, \ldots\right\}$$

נבחר $\beta \in J$ עם הנורמה מקסימלית. תהי $|\beta| = p^{-m}$.

$p^m \in \mathbb{Q}_p$
"$[\{p^m, p^m, \dots\}]$"

אזי נוכיח כי $J=(p^m)$.

$J \subseteq (p^m)$ נשים לב כי $|p^m| = |p^m|_p = p^{-m}$
$= |\beta|$

לכן $\left|\frac{\beta}{p^m}\right| = 1 \Leftarrow u = \frac{\beta}{p^m} \in \mathbb{Z}_p$ הפיך. לכן, p^m, β חברים.

לכן $J \subseteq (p^m) = (\beta)$ כי $\beta \in J$.

$J \subseteq (p^m)$ יהי $\gamma \in J$. אזי $|\gamma| \le |\beta| = |p^m|$ בגלל המקסימליות של $|\beta|$. אזי $\left|\frac{\gamma}{p^m}\right| \le 1 \Leftarrow \frac{\gamma}{p^m} \in \mathbb{Z}_p$,

לכן $\gamma \in (p^m)$.

$$\gamma = p^m \cdot \underbrace{\frac{\gamma}{p^m}}_{\in \mathbb{Z}_p}$$

מסקנה לחוג $\mathbb{Z}_p$ יש מבנה אידיאלים פשוט במיוחד

$(p) \supsetneq (p^2) \supsetneq (p^3) \supsetneq \dots \supsetneq (0)$.

בפרט, האידיאל המקסימלי היחיד של $\mathbb{Z}_p$ הינו (p).

<u>מדוע זה נוצר?</u>

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p$$
$$n \longmapsto [\{n, n, n, \dots\}]$$

<u>הרעיון</u> כשעוברים מ-$\mathbb{Z}$ ל-$\mathbb{Z}_p$ לא מפסידים מידע.
אך הרבה יותר נוח לעבוד עם $\mathbb{Z}_p$ מאשר עם $\mathbb{Z}$.

איך לדמיין את האיברים של $\mathbb{Z}_p$?

<u>טענה</u> $\mathbb{Z}_p$ הינו הסגור של $\mathbb{Z}$ במרחב הטופולוגי $\mathbb{Q}_p$.

<u>הוכחה</u>

<u>$\overline{\mathbb{Z}} \subseteq \mathbb{Z}_p$</u> תהי $\{a_n\}$ סדרת קושי, $a_n \in \mathbb{Z}$. הגבול הינו $[\{a_n\}] \in \mathbb{Q}_p$. הוכחנו בתחילת השיעור כי $|a_n|_p \le 1$ (כי $a_n \in \mathbb{Z}$) ולכן

$$\|[\{a_n\}]\| = \lim_{n\to\infty} |a_n|_p \le 1$$

ולכן $[\{a_n\}] \in \mathbb{Z}_p$.

<u>$\mathbb{Z}_p \subseteq \overline{\mathbb{Z}}$</u> יהי $\alpha \in \mathbb{Z}_p$. צריך להוכיח שבמחלקה α

יש סדרת קושי $\{a_n\}$ כך ש- $a_n \in \mathbb{Z}$. נניח $\alpha \neq 0$.

אך $|\alpha| \le 1$. תהי $\{d_n\}$ סדרת קושי כלשהי במחלקה

α. אזי $|d_n|_p = |\alpha| \le 1$ לכל n מספיק גדול

(בלי הגבלת הכלליות, לכל n). אזי $\mathbb{Q} \ni d_n = \frac{b_n}{\underbrace{c_n}_{\text{שבר מצומצם}}}$

כלומר $p \nmid c_n$.

בפרט, $\gcd(c_n, p^n) = 1$. לכן קיימים x_n, y_n כך ש:

$$x_n c_n + y_n p^n = 1$$

$$x_n b_n c_n + y_n b_n p^n = b_n$$

נגדיר $a_n = x_n b_n \in \mathbb{Z}$. אזי $a_n c_n \equiv b_n \mod p^n$, כלומר

$$\left|a_n - \frac{b_n}{c_n}\right|_p = \left|\frac{1}{c_n}\left(\text{מספר שמתחלק ב-}p^n\right)\right|_p \le \frac{1}{p^n}$$

לכן הסדרה $\{a_n - d_n\}$ אפיסה, לכן $\{a_n\}$ מתכנסת אל המחלקה α.

<u>תרגיל</u> לכל $m \in \mathbb{N}$, $\mathbb{Z}/p^m\mathbb{Z} \cong \mathbb{Z}_p/(p^m)$.

<u>פתרון חלקי</u> נגדיר הומומורפיזם

$$\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_p/(p^m)$$
$$n \longmapsto [\{n,n,n,\dots\}]$$

ברור כי $\ker\varphi = \mathbb{Z} \cap p^m\mathbb{Z}_p = p^m\mathbb{Z}$, צריך להוכיח כי φ על. זה נובע מן הטענה הקודמת.

<u>מסקנה</u> יהי $\alpha \in \mathbb{Z}_p$. אזי קיימת סדרה יחידה $\{b_n\}$ כך ש- $b_n \in \{0,1,\dots,p-1\}$ וכך ש-

$$\alpha = \sum_{n=0}^{\infty} b_n p^n$$