מבוא לחוגים ומודולים - תרגול 14

הערכות

הגדרה:

יהי F שדה. **הערכה** (valuation) על F היא פונקציה $|\cdot|:F\to\mathbb{R}_{\geq 0}$ שמקיימת:

א. $|a|=0 \iff a=0$.

ב. $|ab|=|a|\cdot|b|$.

ג. $|a+b|\leq|a|+|b|$.

כל הערכה מגדירה מטריקה $d(a,b)=|a-b|$.

דוגמאות:

א. $\mathbb{Q},\mathbb{R},\mathbb{C}$ עם הערך המוחלט הרגיל.

ב. לכל שדה יש הערכה טריוויאלית $|a|=\begin{cases}1, & a\neq 0\\ 0, & a=0\end{cases}$.

ג. ההערכה ה-p-אדית על $\mathbb{Q}$: ניקח מספר ראשוני p.

לכל $m\in\mathbb{Z}$ נגדיר $V_p(m)=\max\{k \mid p^k|m\}$. לכל $\frac{m}{n}\neq 0$,

$$\left|\frac{m}{n}\right|_p=\left(\frac{1}{p}\right)^{V_p(m)-V_p(n)}$$

ד. יהי F שדה. אפשר להגדיר הערכה על $F((x))$:

$$\left|\sum_{n=n_0}^{\infty}a_nx^n\right|=c^{\min\{n \mid a_n\neq 0\}}$$

c קבוע, $0<c<1$.

הגדרה:

אומרים שהערכה היא **לא ארכימדית** אם היא מקיימת את אי-שוויון המשולש החזק:
$|a+b| \le \max\{|a|,|b|\}$.

אומרים שהערכה היא **ארכימדית** אם היא לא לא ארכימדית.

[תכונת הארכימדיות של $\mathbb{N}$ ב-$\mathbb{R}$ באופן 1:
לכל $x\in\mathbb{R}$ קיים $n\in\mathbb{N}$ כך ש- $|x|\le|n|$ (עם הערך המוחלט הרגיל)]

בהערכה לא ארכימדית: לכל $n\in\mathbb{Z}$, $|n|\le|1|$.

דוגמאות:

ההערכה הטריוויאלית, ההערכות ה-p-אדיות וההערכה על $F((x))$ הן לא ארכימדיות.

הערך המוחלט הרגיל על $\mathbb{Q}$, $\mathbb{R}$ ו-$\mathbb{C}$ הוא כן ארכימדי.

תרגיל:

יהי F שדה עם הערכה לא ארכימדית $|\cdot|$. אם $|a|\ne|b|$, אז
$|a+b| = \max\{|a|,|b|\}$.

הוכחה:

נניח בה"כ $|a|>|b|$.

לפי אי-שוויון המשולש החזק, $|a+b| \le \max\{|a|,|b|\} = |a|$.

מהצד השני,

$$\underset{3}{|a|} = |(a+b)-b| \le \max\{|a+b|,|-b|\} = \max\{|a+b|,\overset{2}{|b|}\} = |a+b|$$

$\overset{3}{|a|} > \overset{2}{|b|}$, לכן לא יכול להיות שנקבל בסוף $|b|$

לכן נקבל $|a+b| = |a| = \max\{|a|,|b|\}$.

$\square$

הערה:

לכל הערכה, $|1|=|-1|=1$.

למה?

$$|1|=|1^2|=|1|\cdot|1|=|1|^2 \xRightarrow[|1|\neq 0]{} |1|=1$$

$$1=|1|=|(-1)^2|=|-1|^2 \xRightarrow[|-1|\geq 0]{} |-1|=1$$

תרגיל:

יהי F שדה עם הערכה לא ארכימדית $|\cdot|$. הראו שכל משולש ב-F הוא שווה שוקיים.

פתרון:

יהי $a,b,c\in F$. אם $|a-b|=|b-c|$, סיימנו.

אחרת, $|a-b|\neq|b-c|$, ומהתרגיל הקודם

$$|a-c|=|(a-b)+(b-c)|=\max\{|a-b|,|b-c|\}$$

לכן זה משולש שווה שוקיים. $\square$

תרגיל:

יהי F שדה עם הערכה לא ארכימדית $|\cdot|$, ויהי $B(a,r)$ כדור פתוח ב-F.

$$B(a,r)=\{x\in F \mid |x-a|<r\}$$

הראו שלכל $x\in B(a,r)$, $B(a,r)=B(x,r)$.

[אולטרה-מטריקה: מטריקה + $d(x,z)\leq\max\{d(x,y),d(y,z)\}$]

הוכחה:

נניח $y\in B(x,r)$. לכן $|y-x|<r$. אז

$$|y-a|=|(y-x)+(x-a)|\leq\max\{|y-x|,|x-a|\}<r$$

לכן $y\in B(a,r)$. ההכלה השנייה – באופן דומה. $\square$

הגדרה:

יהי F שדה עם הערכה $|\cdot|$. ההשלמה של F ביחס ל-$|\cdot|$ מוגדרת באופן הבא:

$$\hat{F} = \{\text{סדרות קושי ב-}F\} \Big/ \{\text{סדרות אפסות ב-}F\}$$

מקבלים שדה עם טופולוגיה שמושרית מ-F, והוא שלם ביחס לטופולוגיה הזו. (אפשר להרחיב את ההערכה מ-F ל-$\hat{F}$)

דוגמאות:

א. $\mathbb{Q}$ עם הערך המוחלט הרגיל $\Leftarrow$ $\hat{\mathbb{Q}} = \mathbb{R}$.

ב. $F((x))$ שדה שלם ביחס להערכה שהגדרנו עליו.

ג. ההשלמה של $\mathbb{Q}$ ביחס ל-$|\cdot|_p$ = $\mathbb{Q}_p$.

משפט: (משפט אוסטרובסקי)

כל ההשלמות הלא טריוויאליות של $\mathbb{Q}$ שקולות לאחת מהבאות:

- המקרה הארכימדי - הערך המוחלט האוקלידי.
- המקרה הלא ארכימדי - הערכה p-אדית ל-p כלשהו.

תחומי הערכה

הגדרה:

יהי R תחום שלמות, ויהי F שדה השברים שלו. אומרים ש-R הוא תחום הערכה, אם לכל $a\in F^{\times}$ מתקיים $a\in R$ או $a^{-1}\in R$.

האיברים ההפיכים של F = $F\setminus\{0\}$

טענה:

התנאים הבאים שקולים:

א. R תחום הערכה.

ב. לכל $I,J \lhd R$ מתקיים $I\subseteq J$ או $J\subseteq I$.

ג. לכל $I,J\lhd R$ ראשיים מתקיים $I\subseteq J$ או $J\subseteq I$.

מסקנה:

כל תחום הערכה הוא חוג מקומי.

דוגמה:

יהי F שדה עם הערכה לא ארכימדית $|\cdot|$. אז

$$R=\{x\in F \mid |x|\le 1\}$$

הוא תחום הערכה, עם האידאל המקסימלי היחיד

$$I=\{x\in F \mid |x|<1\}.$$

למנה R/I (שהוא שדה) קוראים גם <u>שדה השארית (residue field)</u> של F.

דוגמה לדוגמה:

ניקח $F((x))$ עם ההערכה שראינו.

$$R=\{x\in F \mid |x|\le 1\}=F[[x]]$$

והאידאל המקסימלי היחיד הוא

$$I=\{x\in F \mid |x|<1\}=xF[[x]].$$

שדה השארית פה הוא $F[[x]]/xF[[x]]\cong F$.

תרגיל: (מועד ממבחן)

יהי R תחום שלמות. הוכיחו שכל אידאל נוצר סופית של R הוא ראשי.

הוכחה:

ניקח אידאל $I \trianglelefteq R$ נוצר סופית. נכתוב $I=\langle a_1,\dots,a_n\rangle$ עבור n מינימלי.

נניח בשלילה ש- $n>1$. נתבונן באידאלים $\langle a_1\rangle, \langle a_2\rangle$.

כיוון ש- R תחום שלמות, אחד האידאלים מוכל בשני. בה"כ $\langle a_1\rangle\subseteq\langle a_2\rangle$.

לכן

$$I=\langle a_1,a_2,\dots,a_n\rangle=\langle a_2,a_3,\dots,a_n\rangle$$

בסתירה למינימליות של n. $\square$

תרגיל:

יהי R תחום שלמות. הוכיחו כי R סגור בשלמות בשדה השברים שלו.

הוכחה:

נסמן $F=\mathrm{Frac}(R)$. יהי $a\in F$ שלם מעל R. אם $a\in R$ סיימנו.

אחרת, כיוון ש- R תחום שלמות, $a^{-1}\in R$.

a שלם מעל R, לכן קיימים $\alpha_{n-1},\dots,\alpha_0\in R$ שעבורם

$$a^n+\alpha_{n-1}a^{n-1}+\dots+\alpha_1 a+\alpha_0=0 \quad \Big|\cdot(a^{-1})^{n-1}$$

$$a=-\underset{\in R}{\alpha_{n-1}}-\underset{\in R}{\alpha_{n-2}}\,\underset{\in R}{a^{-1}}-\dots-\underset{\in R}{\alpha_1}\,\underset{\in R}{a^{-(n-2)}}-\underset{\in R}{\alpha_0}\,\underset{\in R}{a^{-(n-1)}}\in R$$

לכן $a\in R$, כנדרש. $\square$

המספרים ה-p-אדיים

p - מספר ראשוני קבוע.

הגדרה:

ההשלמה של $\mathbb{Q}$ ביחס להערכה ה-p-אדית $|\cdot|_p$ נקראת שדה **המספרים ה-p-אדיים**, ומסומנת $\mathbb{Q}_p$. בהתאמה, **השלמים ה-p-אדיים** $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$.

טענה:

תהי $\{a_n\}$ סדרה ב-$\mathbb{Q}_p$. אז $\sum_{n=1}^{\infty} a_n$ מתכנס $\Longleftrightarrow$ $a_n \xrightarrow[n\to\infty]{} 0$.

דוגמה:

ניקח $a_n = p^n$, $|a_n|_p = \left(\frac{1}{p}\right)^n \xrightarrow[n\to\infty]{} 0$, לכן $\sum_{n=0}^{\infty} p^n$ מתכנס.

$$\sum_{n=0}^{\infty} p^n = \frac{1}{1-p}$$

איך אפשר לתאר את $\mathbb{Q}_p$? כל איבר של $\mathbb{Q}_p$ אפשר לכתוב בצורה יחידה

$$x = \sum_{n=n_0}^{\infty} a_n p^n$$

כאשר $n_0 \in \mathbb{Z}$, $0 \leq a_n \leq p-1$.

(למה הטור מתכנס ב-$\mathbb{Q}_p$? $|a_n p^n|_p = \left(\frac{1}{p}\right)^n \xrightarrow[n\to\infty]{} 0$)

שים לב: בהצגה הזו יש רק מספר סופי של חזקות שליליות, ואולי אינסוף חיוביות. בהצגה העשרונית הרגילה זה הפוך.

דוגמה:

$p=2$,
$$-1=\sum_{n=0}^{\infty}2^n=\dots111_2=\bar{1}_2$$

ייצוג באינסוף p מבזים — סימון מקוצר

$p=5$,
$$175=1200_5=1\cdot5^3+2\cdot5^2+0\cdot5^1+0\cdot5^0$$

$p=7$,
$$\frac{194}{7}=36.5_7=3\cdot7^1+6\cdot7^0+5\cdot7^{-1}$$

איך מוצאים את ההצגה ה-p-אדית של $x\in\mathbb{Q}$?

למספר טבעי – ההצגה בבסיס p. למספרים רציונליים:

למה:

יהי $x\in\mathbb{Z}_p$ עם הצגה p-אדית $x=\sum_{n=0}^{\infty}a_np^n$. אז לכל $m\geq1$,
$$x\equiv\sum_{n=0}^{m-1}a_np^n \pmod{p^m}$$

דוגמה:

ניקח $p=5$, $x=\frac{4}{3}$. נחשב את ההצגה ה-5-אדית של $\frac{4}{3}$.
$$\left|\frac{4}{3}\right|_5=1$$

[למה? אם a,b לא מתחלקים ב-p, $\left|p^k\cdot\frac{a}{b}\right|_p=\left(\frac{1}{p}\right)^k$]

נחפש הצגה $\frac{4}{3}=\sum_{n=0}^{\infty}a_n5^n$.

מודולו 5:
$$a_0\equiv\frac{4}{3}\pmod 5=4\cdot\left(3^{-1}\pmod 5\right)\pmod 5=$$
$$=4\cdot2\pmod 5=3$$

מצאנו את a_0.

מה לגבי a_1?

<u>מודולו 25:</u>

$$a_1\cdot 5 + a_0 \equiv \frac{4}{3} \pmod{25} = 4\cdot 3^{-1} \pmod{25} =$$
$$= (4\cdot 17) \pmod{25} = 68 \pmod{25} = 18$$

$$a_1\cdot 5 + 3 \equiv 18 \pmod{25}$$
$$5a_1 \equiv 15 \pmod{25}$$
$$a_1 = 3$$

דרך אחרת: אם $x=\sum_{n=0}^{\infty} a_n p^n$, אז

$$\frac{x-a_0}{p} = \sum_{n=1}^{\infty} a_n p^{n-1} = a_1 + a_2 p + a_3 p^2 + \cdots$$

ואז אפשר לעבוד מודולו p על $\frac{x-a_0}{p}$ במקום מודולו p^2 על x.

אם נמשיך נקבל

$$\frac{4}{3} = \overline{13}3_5 = 3\cdot 5^0 + 3\cdot 5^1 + 1\cdot 5^2 + 3\cdot 5^3 + 1\cdot 5^4 + \cdots.$$

<u>תרגיל:</u>
הוכיחו
$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

<u>הוכחה:</u>

נגדיר $\varphi:\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ לפי $\varphi\left(\sum_{m=0}^{\infty} a_m p^m\right) = \sum_{m=0}^{n-1} a_m p^m$.

φ הומומורפיזם – ישיר. ברור ש-φ על.

$$\ker\varphi = \left\{\sum_{m=0}^{\infty} a_m p^m \,\middle|\, a_0 = \cdots = a_{n-1} = 0\right\} = p^n\mathbb{Z}_p.$$

$\square$

הערה:

$$\mathbb{Z} \subseteq \mathbb{Z}_{\langle p\rangle} \subseteq \mathbb{Z}_p$$

"

המיקום של $\mathbb{Z}$

ב- $\langle p\rangle$

$$\mathbb{Z}_{\langle p\rangle} = \left\{ \frac{a}{b} \,\middle|\, p\nmid b \right\}$$

שני החוגים האלו דומים:

א. $\mathbb{Z}_p$, $\mathbb{Z}_{\langle p\rangle}$ מקומיים, האידאלים המקסימליים הם $p\mathbb{Z}_p$, $p\mathbb{Z}_{\langle p\rangle}$.

ב. $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}_{\langle p\rangle}/p^n\mathbb{Z}_{\langle p\rangle} \cong \mathbb{Z}/p^n\mathbb{Z}$

ג. "$\mathbb{Z}_{\langle p\rangle} = \mathbb{Z}_p \cap \mathbb{Q}$"

ד. $\mathbb{Z}_p\left[\frac{1}{p}\right] = \mathbb{Q}_p$, $\mathbb{Z}_{\langle p\rangle}\left[\frac{1}{p}\right] = \mathbb{Q}$.

הוכחת ד':

למה $\mathbb{Z}_p\left[\frac{1}{p}\right] = \mathbb{Q}_p$? $\boxed{\subseteq}$ ✓

$\boxed{\supseteq}$ יהי $x \in \mathbb{Q}_p$. נסמן $|x|_p = \left(\frac{1}{p}\right)^n$.

אז $|x\cdot p^{-n}|_p = \left(\frac{1}{p}\right)^0 = 1 \Rightarrow x\cdot p^{-n} \in \mathbb{Z}_p$

$$x = \underbrace{x\cdot p^{-n}}_{\in\, \mathbb{Z}_p} \cdot p^n$$

אם $n \geq 0$ - $x \in \mathbb{Z}_p$. אחרת $p^n = \left(\frac{1}{p}\right)^{-n} \in \mathbb{Z}_p\left[\frac{1}{p}\right]$.

הלמה של הנזל:

יהי p מספר ראשוני, ויהי $f(x) \in \mathbb{Z}[x]$. אם $0 \leq r \leq p-1$ הוא שורש של $f(r) \equiv 0 \pmod{p}$, וגם $f'(r) \not\equiv 0 \pmod{p}$, אז לכל $k \geq 2$ קיים $0 \leq x \leq p^k - 1$ יחיד כך ש- $x \equiv r \pmod{p}$ ו- $f(x) \equiv 0 \pmod{p^k}$. ובפרט, לפולינום f יש שורש של $\mathbb{Q}_p$.

הפרקים בגדול:

א. מושגים בסיסיים בחוגים

ב. אידאלים ראשוניים ומקסימליים

ג. תחומי שלמות + מיקום

ד. חוגי פולינומים - אי-פריקות + תכונות (כמו נותריות)

ה. מודולים

ו. שלמות, תחומי דדקינד

ז. חוגים מקומיים, הערכות, תחומי הערכה