הרצאה 2

<u>הגדרה</u> חוג A נקרא תחום דדקינד אם הוא מקיים את התנאים הבאים:

1) A תחום שלמות.
2) A נותרי.
3) A סגור בשלמות
4) $\dim A = 1$ (כל אידיאל ראשוני לא אפסי הינו מקסימלי).

<u>תרגיל</u> כל תחום ראשי הינו תחום דדקינד.

<u>טענה</u> יהי K שדה מספרים. אזי חוג השלמים $\mathcal{O}_K$ הינו תחום דדקינד.

<u>הוכחה</u> 1) $\mathcal{O}_K$ מוכל בשדה, לכן תחום שלמות.

2) הוכחנו $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n$, אך $\mathbb{Z}$ נותרי, לכן כל אידיאל $I \trianglelefteq \mathcal{O}_K$ נוצר סופית כ-$\mathbb{Z}$-מודול, לכן גם כ-$\mathcal{O}_K$-מודול. לכן $\mathcal{O}_K$ נותרי.

3) $\mathcal{O}_K$ הינו הסגור השלם של $\mathbb{Z}$ ב-K, לכן $\mathcal{O}_K$ סגור בשלמות.

4) יהי $0 \neq P \trianglelefteq \mathcal{O}_K$ אידיאל ראשוני. אזי $P \cap \mathbb{Z} = p\mathbb{Z}$ כאשר p מספר ראשוני. אכן, יהי $0 \neq y \in P$, אזי y שלם מעל $\mathbb{Z}$ לכן

$$y^m + a_{m-1}y^{m-1} + \dots + a_1 y + a_0 = 0$$

כאשר $a_i \in \mathbb{Z}$, $a_0 \neq 0$. אזי

$$a_0 = -y\left(y^{m-1} + a_{m-1}y^{m-2} + \dots + a_1\right) \in P \cap \mathbb{Z}$$

ולכן $P \cap \mathbb{Z} \neq (0)$ וברור שזה אידיאל ראשוני של $\mathbb{Z}$.

יש ל- $\mathcal{O}_K/p$ מבנה טבעי של $\mathbb{Z}/p\mathbb{Z}$-מודול. יהי

$\alpha_1, \dots, \alpha_n$ בסיס שלם:

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n$$

$$\mathcal{O}_K/p = \mathbb{Z}/p\mathbb{Z} \cdot \bar{\alpha}_1 + \dots + \mathbb{Z}/p\mathbb{Z} \cdot \bar{\alpha}_n, \qquad \bar{\alpha}_i = \alpha_i + P \in \mathcal{O}_K/p$$

לכן, $\mathcal{O}_K/p$ תחום שלמות (כי P ראשוני) סופי. לכן

$\mathcal{O}_K/p$ שדה $\Leftrightarrow$ P מקסימלי.

<u>הערה</u> תחום דדקינד אינו בהכרח תחום פריקות יחידה:

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

<u>הגדרה</u> A חוג (חילופי), $I, J \trianglelefteq A$ אידיאלים.

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : \ a_i \in I, \ b_i \in J, \ n \in \mathbb{N} \right\}$$

נגדיר כך גם מכפלה של תת-A-מודולים של $K = \mathrm{Frac}\, A$.

<u>למה 1</u> יהי A חוג נתרי. יהי $0 \neq I \trianglelefteq A$ אידיאל. אזי

$$P_1 P_2 \cdots P_r \subseteq I$$

כאשר $P_1, \dots, P_r$ ראשוניים לא אפסיים.

<u>הוכחה</u> תהי $\mathcal{S} = \{ I \trianglelefteq A :$ I לא מכיל מכפלה של אידיאלים ראשוניים $\}$

נניח בשלילה כי $\mathcal{S} \neq \emptyset$. כיוון ש-$A$ נתרי, כל שרשרת של איברים של $\mathcal{S}$ חסומה מלעיל, לכן לפי הלמה של צורן יש איבר מקסימלי $I \in \mathcal{S}$. ברור כי I לא ראשוני (כי אחרת היה מכיל מכפלה של ראשוניים). לכן קיימים $x, y \notin I$ אך $xy \in I$. לפי המקסימליות של I,

$$P_1P_2\cdots P_r \subseteq I + A_x$$
$$Q_1\cdots Q_s \subseteq I + A_y$$

לכן $P_1P_2\cdots P_rQ_1\cdots Q_s \subseteq (I+A_x)(I+A_y) \subseteq I$
סגירה.

<u>הגדרה</u> יהי A תחום דדקינד. יהי $0\neq P\triangleleft A$ אידיאל ראשוני.
נגדיר $P^{-1} = \{x\in K : xP\subseteq A\}$
$= \{x\in K :$ לכל $y\in P$ מתקיים $xy\in A\}$

ברור כי $A\subseteq P^{-1}$. ברור כי P^{-1} הינו A-תת-מודול של K.

<u>למה 2</u> יהי A תחום דדקינד, $0\neq P\triangleleft A$ ראשוני. אזי $A\subsetneq P^{-1}$.

<u>הוכחה</u> מספיק להוכיח $A\neq P^{-1}$. נבחר $0\neq y\in P$
לפי הלמה 1, $P_1P_2\cdots P_r \subseteq I = yA \subseteq P$, נבחר מכפלה כנ"ל
עם r מינימלי.

אבל P אידיאל ראשוני, לכן $P_i\subseteq P$ עבור איזשהו $1\le i\le r$,
נניח $P_r\subseteq P$. אבל $\dim A = 1 \Leftarrow P, P_r$ מקסימליים
$\Leftarrow P_r = P$. לפי המינימליות של r,
$P_1P_2\cdots P_{r-1}\not\subseteq yA$. יהי

$z\in P_1\cdots P_{r-1}\setminus yA$.

מצד אחד, $z\notin yA \Leftrightarrow \frac{z}{y}\notin A$.

מצד שני $zP \subseteq (zA)P \subseteq P_1P_2\cdots P_{r-1}P =$
$P_1P_2\cdots P_{r-1}P_r \subseteq yA$

זה אומר שלכל $x \in P$, $zx \in yA$

$\frac{z}{y} x \in A$

זה אומר $\frac{z}{y} \in P^{-1}$. לכן $P^{-1} \neq A$.

<u>למה 3</u> יהי A תחום נתרייני, יהי $0 \neq P \trianglelefteq A$ אידיאל ראשוני, יהי $0 \neq I \trianglelefteq A$ אידיאל. אזי $I \subsetneqq IP^{-1}$.

<u>הוכחה</u> A נתרי $\Leftarrow$ $I = Aa_1 + Aa_2 + \dots + Aa_m$. יהי $x \in P^{-1}$, נניח בשלילה כי $I = IP^{-1}$. לכן, לכל $1 \le i \le m$,

$$xa_i \in IP^{-1} = I \implies xa_i = \sum_{j=1}^{m} c_{ij} a_j, \quad c_{ij} \in A.$$

$$C = (c_{ij})$$

$$(xI_m - C)\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

נכפיל במטריצה המצורפת של $(xI_m - C) \in M_m(K)$

$$\det(xI_m - C) = 0$$

$$\det\begin{pmatrix} x-c_{11} & \cdots & -c_{1m} \\ \vdots & \ddots & \\ -c_{m1} & & x-c_{mm} \end{pmatrix}$$

נקבל: x הינו שורש של פולינום מתוקן ממעלה m ועם מקדמים ב-A $\Leftarrow$ x שלם מעל A.

A סגור בשלמות $\Leftarrow$ $x \in A$. $\Leftarrow$ $P^{-1} \subseteq A$ בסתירה ללמה 2.

<u>למה 4</u> יהי A תחום נתרייני, $0 \neq P \trianglelefteq A$ אידיאל ראשוני. אזי $PP^{-1} = A$.

הוכחה $P \underset{\text{למה 3}}{\subsetneqq} PP^{-1} \subseteq A$

אבל P מקסימלי, לכן $PP^{-1}=A$.

<u>משפט</u> יהי A תחום דדקינד. יהי $0\neq I\triangleleft A$ אידיאל.
לא בהכרח ראשוני

אזי $I=P_1\cdots P_r$, כאשר P_i ראשוניים.

יתר מזה, הפירוק יחיד עד כדי שינוי סדר הגורמים:

אם $I=P_1\cdots P_r=Q_1\cdots Q_s$

אזי $r=s$ ויש תמורה $\sigma\in S_r$ כך ש- $Q_i=P_{\sigma(i)}$
לכל $1\le i\le r$.

(אם $I=A$, אזי I שווה למכפלה הריקה)

<u>הוכחה</u> קיום: יהי

$\mathcal{S}=\{I\triangleleft A: \text{ראשוניים}\ \text{של}\ \text{מכפלה}\ \text{אינו}\ I\}$

נניח בשלילה כי $\mathcal{S}\neq\emptyset$. אזי לפי הלמה של צורן

יש איבר מקסימלי $I\in\mathcal{S}$ (כי A נתרי).

קיים $P\triangleleft A$ מקסימלי כך ש- $I\subsetneq P$.

לפי למה 1, $IP^{-1}\subseteq PP^{-1}=A$, לכן $IP^{-1}\triangleleft A$ אידיאל.

לפי למה 3, $I\subsetneq IP^{-1}$, לכן $IP^{-1}\notin\mathcal{S}$. לכן

$$IP^{-1}=P_1\cdots P_r$$

$$I=IA=IP^{-1}P=P_1\cdots P_rP$$

לכן $I\in\mathcal{S}$ בסתירה.

<u>יחידות</u>. נניח שיש שני פירוקים שונים

$$I=P_1P_2\cdots P_r=Q_1\cdots Q_s$$

אינדוקציה על r:

$r=0$, $I=A$, בשני האגפים מכפלה ריקה. ✓

נניח שהטענה ידועה עבור $r-1$.

$$I=P_1P_2\cdots P_r=Q_1\cdots Q_s\subseteq P_r$$

אך P_r ראשוני, לכן $Q_i\subseteq P_r$ עבור $1\le i\le s$ מסוים.

לכן $Q_i=P_r$. עד כדי שינוי בסדר ה-Q-ים, נניח $s=i$:

לכן $$IP_r^{-1}=IQ_s^{-1}=P_1\cdots P_{r-1}=Q_1\cdots Q_{s-1}$$

וסיימנו באינדוקציה.

<u>הגדרה</u> יהי A תחום דדקינד. אידאל שברי של A הינו תת-A-מודול שונה-מאפס נוצר סופית של $K=\mathrm{Frac}\,A$.

אידאל של A ייקרא גם אידאל <u>שלם</u>.

<u>טענה</u> הקבוצה J_A של כל האידאלים השבריים של A הינה חבורה אבלית תחת כפל מודולים.

<u>הוכחה</u> $O=A$. החלק הלא-טריוויאלי היחיד זה להוכיח כי לכל אידאל שברי יש הפיך.

אכן, אם $I=P$ אידאל ראשוני, אזי P^{-1} הינו הפיך, כי $PP^{-1}=A$ לפי למה 4.

אם $I\trianglelefteq A$ אידאל שלם, אזי $I=P_1\cdots P_r$,

לכן $I^{-1}=P_1^{-1}P_2^{-1}\cdots P_r^{-1}$.

נניח $\underline{a}\in J_A$ אידאל שברי. אזי הוא נוצר סופית

כי A-נותרי: $\quad x_i \in \underline{a} \subseteq K \quad , \quad \underline{a} = Ax_1 + \dots + Ax_m$

תהי y המכפלה של המכנים של כל ה-x_i-ים.

אזי
$$\underline{a}(yA) = Ax_1y + \dots + Ax_my = I \triangleleft A$$

לכן,
$$\underline{a} = I(yA)^{-1}$$

אזי
$$\underline{a}^{-1} = I^{-1}(yA).$$

<u>טענה</u> יהי $\underline{a} \in J_A$ אידאל שברי. אזי ניתן לרשום אותו באופן יחיד בצורה
$$\underline{a} = \prod_{\substack{P \triangleleft A \\ \text{ראשוניים}}} P^{e_p}$$

כאשר $e_p \in \mathbb{Z}$ וכאשר רק מספר סופי של e_p-ים שונים מאפס. ($\underline{a}$ אידאל שלם $\iff$ $0 \leq e_p$ לכל p).

תהי $P_A \subseteq J_A$ תת-חבורה של אידאלים שברים ראשיים ($\underline{a} \in P_A \iff \underline{a} = Ax$ לאיזשהו $x \in K^*$). תהי
$$Cl_A = J_A / P_A$$
חבורת המחלקות של A.

<u>טענה</u> A תחום ראשי $\iff$ Cl_A טריוויאלית.

<u>משפט</u> (Claborn, 1960's) תהי G חבורה אבלית. אזי קיים תחום דדקינד A כך ש- $Cl_A \simeq G$.

טענה יהי A תחום דדקינד. אזי A תחום ראשי אם ורק אם A תחום פריקות יחידה.

הוכחה $\Rightarrow$) נכון לכל חוג.

$\Leftarrow$) יהי A תחום דדקינד ופ"י. יהי $0 \neq P \triangleleft A$ אידיאל ראשוני, ויהי $0 \neq y \in P$. אזי

$y = p_1 p_2 \cdots p_r \in P$ כאשר $p_i \in A$ איברים אי-פריקים.

אך P ראשוני, לכן $p_i \in P$ $\Leftarrow$ $(p_i) \subseteq P$
ראשוני

$\dim A = 1$ $\Leftarrow$ (p_i) מקסימלי $\Leftarrow$ $P = (p_i)$.

לכן כל אידיאל ראשוני הינו ראשי. אך כל אידאל הינו מכפלה של ראשוניים, לכן גם ראשי.

המטרה הבאה: יהי K שדה מספרים. אזי $Cl_{\mathcal{O}_K} = Cl_K$ הינה סופית.

סריגים

הגדרה יהי V מרחב וקטורי סוף-מימדי מעל $\mathbb{R}$. סריג הינו תת-קבוצה מן הצורה

$$\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m \subseteq V$$

כאשר $\{v_1, \dots, v_m\}$ בלתי תלויים לינארית.

ברור כי Γ הינו תת-חבורה של V.

Γ נקרא סריג שלם (complete lattice) אם $m = \dim V$ $\Longleftrightarrow$ Γ פורש את V מעל $\mathbb{R}$.

__הגדרה__ תת-חבורה $\Gamma \subseteq V$ נקראת דיסקרטית אם
טופולוגית התת-קבוצה של Γ הינה דיסקרטית $\Longleftrightarrow$
לכל $\gamma \in \Gamma$ קיימת $U \subseteq V$ פתוחה כך ש- $U \cap \Gamma = \{\gamma\}$.

__משפט__ תהי $\Gamma \subseteq V$ תת-חבורה. אזי Γ דיסקרטית $\Longleftrightarrow$ Γ סריג.

__הוכחה__ $(\Leftarrow)$ יהי $\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$.
נשלים את $\{v_1, \dots, v_m\}$ לבסיס $\{v_1, \dots, v_n\}$ של V, כאשר $n = \dim V$. יהי $\gamma = \sum_{i=1}^{n} a_i v_i \in \Gamma$
$a_i \in \mathbb{Z}$

ניקח $U = \{ \sum_{i=1}^{n} b_i v_i \in V \mid |b_i - a_i| < \frac{1}{2} \}$ פתוחה ב- V.
$U \cap \Gamma = \{\gamma\}$.

$(\Rightarrow)$ תהי $\Gamma \subseteq V$ דיסקרטית.
__שלב 1__ נוכיח כי Γ סגורה.
__הוכחה__ תהי $U \subseteq V$ פתוחה כך ש- $\Gamma \cap U = \{0\}$.
תהי $\{\gamma_k\}$ סדרה מתכנסת של איברים של Γ
לכל סביבה פתוחה U של 0 קיים N כך שלכל $N < k, l$ מתקיים $\gamma_k - \gamma_l \in U$, אך $\gamma_k - \gamma_l \in \Gamma \cap U$
לכן הסדרה $\{\gamma_k\}$ מתייצבת, לכן הגבול מוכל ב- Γ.
__שלב 2__ יהי $V_0 \subseteq V$ התת-מרחב הנפרש על ידי Γ.
יהי $\{u_1, \dots, u_m\} \subseteq \Gamma$ בסיס של V_0.

יהי $\Gamma_0 = \mathbb{Z}u_1 + \dots + \mathbb{Z}u_m$. ברור כי $\Gamma_0 \le \Gamma$.

נוכיח $[\Gamma:\Gamma_0] < \infty$ (Γ_0 תת-חבורה של Γ מאינדקס סופי).

<u>הוכחה</u> נגדיר $\Phi_0 = \{a_1u_1+\dots+a_mu_m : 0 \le a_i < 1\}$

אזי $V_0 = \bigcup_{\delta\in\Gamma_0} (\Phi_0 + \delta)$ (האיחוד הינו זר)

יהי $\{\gamma_i\}_{i\in I}$ קבוצה של נציגים של המחלקות Γ/Γ_0.

אז $\gamma_i \in V_0$, לכן ניתן להציג באופן יחיד

$$\gamma_i = \varphi_i + \delta_i, \quad \varphi_i \in \Phi_0, \ \delta_i \in \Gamma_0$$

$$\varphi_i = \gamma_i - \delta_i \in \underbrace{\Gamma \cap \overline{\Phi_0}}$$

קומפקטי ודיסקרטי, לכן סופית.

זה אומר שיש רק מספר סופי של אפשרויות ל-φ_i

אך $\gamma_i \equiv \varphi_i \mod \Gamma_0$ ⇐ יש רק מספר סופי של γ_i-ים.

<u>שלב 3</u> Γ סריג.

<u>הוכחה</u> יהי $d=[\Gamma:\Gamma_0]$ אזי

$$d\Gamma \le \Gamma_0 \le \Gamma$$

$$\Gamma \le \mathbb{Z}\cdot\frac{u_1}{d}+\dots+\mathbb{Z}\cdot\frac{u_m}{d}$$

לפי המיון של חבורות אבליות נוצרות סופית, $\Gamma \simeq \mathbb{Z}^r$,

כמובן $r\le m$. מצד שני Γ פורש את V_0 ⇐ $r \ge m$. לכן $r=m$, $\Gamma = \mathbb{Z}v_1+\dots+\mathbb{Z}v_m$.

טענה יהי $\Gamma \leq V$ שריג הוא שלם אם ורק אם קיימת קבוצה חסומה $\Phi \leq V$ כך ש-

$$V = \bigcup_{\gamma \in \Gamma} (\Phi + \gamma)$$

הגדרה יהי $\Gamma \leq V$ שריג שלם.

$$\Gamma = \mathbb{Z} v_1 + \dots + \mathbb{Z} v_n$$

יהי

$$vol(\Gamma) = vol(\underbrace{\{\sum a_i v_i \mid 0 \leq a_i < 1\}}_{\Phi}) = \left| \det \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \right|$$

נפ' מקבילון היסוד.

משפט (מינקובסקי) תהי $\Gamma \leq \mathbb{R}^n$ שריג שלם.

תהי $\emptyset \neq X \subseteq \mathbb{R}^n$ תת-קבוצה סימטרית ($-x \in X \Leftarrow x \in X$) וקמורה ($tx + (1-t)y \in X \Leftarrow x, y \in X$ לכל $t \in [0,1]$).

נניח $vol(X) > 2^n vol(\Gamma)$

אזי $X \cap \Gamma \neq \{0\}$

הוכחה מספיק למצוא $\gamma_1 \neq \gamma_2 \in \Gamma$ כך ש-

$$\left(\tfrac{1}{2}X + \gamma_1\right) \cap \left(\tfrac{1}{2}X + \gamma_2\right) \neq \emptyset$$

אכן, יש נקודה בחיתוך

$$\tfrac{1}{2}x_1 + \gamma_1 = \tfrac{1}{2}x_2 + \gamma_2 \qquad x_1, x_2 \in X$$

$$\Gamma \ni \gamma_1 - \gamma_2 = \tfrac{1}{2}x_2 - \tfrac{1}{2}x_1 \in X \cap \Gamma$$

$$\gamma_1 - \gamma_2 \neq 0.$$

נניח בשלילה כי $\frac{1}{2}X+\gamma$, $\gamma\in\Gamma$ כולם זרים.

אזי $\Phi\cap(\frac{1}{2}X+\gamma)$ כולם זרים.

$$\mathrm{vol}(\Phi)\geq\sum_{\gamma\in\Gamma}\mathrm{vol}\left(\Phi\cap\left(\tfrac{1}{2}X+\gamma\right)\right)=$$

$$\sum_{\gamma\in\Gamma}\mathrm{vol}\Big(\underbrace{(\Phi-\gamma)\cap\tfrac{1}{2}X}_{\text{כולם זרים}}\Big)\geq\mathrm{vol}\left(\tfrac{1}{2}X\right)=\frac{1}{2^n}\mathrm{vol}(X$$

כי $\Phi-\gamma$ כולם זרים

מכסים את $\frac{1}{2}X$

בסתירה להנחה $\mathrm{vol}(X)<2^n\,\mathrm{vol}(\Gamma)$.