7.6.2010

שיעור 13

f - תבנית ריבועית לא מנוונת ב-n משתנים מעל $\mathbb{Q}$.
f_v מייצגת אפס, מעל $\mathbb{Q}_v$, לכל v.
המטרה היא להוכיח כי f מייצגת אפס מעל $\mathbb{Q}$.

אפשר להניח כי f אלכסונית ומנורמלת בצורה הבאה:

$$f = x_1^2 + a_2x_2^2 + \dots + a_nx_n^2 \qquad (a_i = 0).$$

<u>$n=2$</u>: הוכחנו.

<u>$n=3$</u>: נבחר: $f = x^2 - ay^2 - bz^2$ $\quad 0 \neq a,b \in \mathbb{Q}$.

אפשר להניח כי $a,b \in \mathbb{Z}$ (למשל אם $a = \frac{m}{r}$, r ו-m שלמים,

$$ay^2 = \frac{m}{r}y^2 = mr\left(\frac{y}{r}\right)^2 = mr(y')^2)$$

כמו כן אפשר להניח כי a,b חופשיים מריבועים.

לבסוף אפשר להניח כי $1 \le |a| \le |b|$.

נסמן $m = |a| + |b|$, ההוכחה היא באינדוקציה על m.

<u>$m=2$</u>: $\Leftarrow$ $|a| = |b| = 1$, $a,b = \pm 1$, $f = z^2 \pm y^2 \pm x^2$. כיוון ש-f_∞ מייצגת אפס (מעל $\mathbb{R}$) ברור כי $f \neq z^2 + y^2 + x^2$. ($(a,b) \neq (-1,-1)$)
לכן התבנית מייצגת אפס: $f = z^2 - y^2 \pm x^2$ ואז $x=0$, $z=y=1$.

<u>$m>2$</u>: $\Leftarrow$ $|b| \ge 2$. נכתוב $b = \pm p_1p_2\cdots p_r$ מכפלת ראשוניים שונים.

יהי p אחד הראשוניים הנ"ל. נוכיח כי a הוא ריבוע מודולו p.
אם $a \equiv 0 \pmod p$ אז אין מה להוכיח.
נניח $a \not\equiv 0 \pmod p$. f מייצגת אפס מעל $\mathbb{Q}_p$, לכן יש פתרון פרימיטיבי מעל $\mathbb{Z}_p$ למשוואה $x^2 - ay^2 - bz^2 = 0$.
כיוון ש-$b \equiv 0 \pmod p$ נובע כי אחד מ-x,y צריך להיות ב-$\mathbb{Z}_p^*$.
נקבל $x^2 \equiv ay^2 \pmod p$. כיוון ש-$a \in \mathbb{Z}_p^*$, נקבל כי $x,y \in \mathbb{Z}_p^*$.
לכן a הוא ריבוע של איבר ב-$\mathbb{Z}_p^*$.

$$\mathbb{Z}_p/p\mathbb{Z}_p \xrightarrow[\text{של חוגים}]{\sim} \mathbb{Z}/p\mathbb{Z}$$

$$a + p\mathbb{Z}_p \mapsto \underset{\substack{\| \\ \varepsilon_1(a)}}{a} + p\mathbb{Z}$$

לכן a הוא ריבוע ב-$\mathbb{Z}/p\mathbb{Z}$ (כלומר $\left(\frac{a}{p}\right) = 1$)

$$\mathbb{Z}/b\mathbb{Z} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \dots \times \mathbb{Z}/p_n\mathbb{Z}$$

$$a+b\mathbb{Z} \longmapsto (a+p_1\mathbb{Z},\ a+p_2\mathbb{Z},\ \dots,\ a+p_n\mathbb{Z})$$

כיוון ש $a+p_i\mathbb{Z}$ ריבוע ב- $\mathbb{Z}/p_i\mathbb{Z}$ לכל i, נקבל ש $a+b\mathbb{Z}$ ריבוע במודולו $\mathbb{Z}/b\mathbb{Z}$. לכן יש שלמים t, b' כך ש $a=t^2+bb'$,
אפשר לבחור t כך ש $|t|\le\frac{|b|}{2}$ (אחרת אפשר להחליף את t ב- $b-t$)

$$bb' = t^2-a = N(t+\sqrt{a}) \quad (\mathbb{Q}(\sqrt{a}))$$

מכאן $b'\in N(\mathbb{Q}(\sqrt{a})) \iff b\in N(\mathbb{Q}(\sqrt{a}))$.
(אפשר להניח כי a אינו ריבוע, כלומר $a\neq 1$, אחרת $f=x^2-y^2-bz^2$ מייצגת אפס.)
לכן $f=x^2-ay^2-bz^2$ מייצגת אפס $\iff$ $f'=x^2-ay^2-b'z^2$ מייצגת אפס מעל $\mathbb{Q}$.

באותו אופן מראים שאם $a\notin(\mathbb{Q}_v^*)^2$ וכיוון ש $N_{\mathbb{Q}_v(\sqrt{a})}(t+\sqrt{a})=bb'=t^2-a$.
$f_v=x^2-ay^2-bz^2$ מייצגת אפס מעל $\mathbb{Q}_v$ $\iff$ $f_v'=x^2-ay^2-b'z^2$ מייצגת אפס מעל $\mathbb{Q}_v$.
נתון. לכן f_v' מייצגת אפס מעל $\mathbb{Q}_v$.
אם $a\in(\mathbb{Q}_v^*)^2$, אז $f'\sim x^2-y^2-bz^2$ מייצגת אפס ($(1,1,0)$)
לכן f_v' מייצגת אפס מעל $\mathbb{Q}_v$ לכל v.

$$|a|+|b'| = |a| + \frac{|t^2-a|}{|b|} \le |a| + \frac{|t|^2}{|b|} + \frac{|a|}{|b|} \le |a| + \underbrace{\tfrac{1}{4}|b|+1}_{\overset{\wedge}{|b|}\ \leftarrow\ |b|\ge 2} < |a|+|b| = m$$

ע"י שינוי משתנים ב- f', אפשר ~~את~~ להחליף את b' ב- b''
"החלק החופשי מריבועים" של b'; $|a|+|b''|\le|a|+|b'|<m$.
$f'\sim f''=z^2-ay^2-b''x^2$ (שקילות מעל $\mathbb{Q}$ ולכן גם מעל $\mathbb{Q}_v$)
לכן f_v'' מייצגת אפס מעל $\mathbb{Q}_v$ לכל v. באינדוקציה, f'' מייצגת אפס מעל $\mathbb{Q}$ ולכן f' מייצגת אפס מעל $\mathbb{Q}$, ומכאן f מייצגת אפס מעל $\mathbb{Q}$.

$\underline{n=4}$: נסמן $f=a_1x_1^2+a_2x_2^2-a_3x_3^2-a_4x_4^2 =: f_1\ominus f_2$.
כיוון ש- f_v מייצגת אפס מעל $\mathbb{Q}_v$, יש ~~[illegible]~~ $b_v\in\mathbb{Q}_v^*$ המיוצג
ע"י $f_{1,v}$ וגם ע"י $f_{2,v}$. לפי מה שלמדנו זה אומר $(b_v,-a_1a_2)_v=(a_1,a_2)_v$
$(b_v,-a_3a_4)_v=(a_3,a_4)_v$
מהמשפט בדבר המשוואות הגלובליות של סמל הילברט, יש $b\in\mathbb{Q}^*$ כך ש:

$$\begin{cases}(b,-a_1a_2)_v=(a_1,a_2)_v\\(b,-a_3a_4)_v=(a_3,a_4)_v\end{cases} \quad \text{לכל } v.$$

זה אומר ש $f_{2,v}$, $f_{2,v}$ מייצגות את לכל v. כלומר

ו־ $f_1 \ominus bz^2$, $f_2 \ominus bz^2$ מייצגות אפס מעל $\mathbb{Q}_v$ לכל v.

מהמקרה $n=3$, $f_1 \ominus bz^2$, $f_2 \ominus bz^2$ מייצגות אפס מעל $\mathbb{Q}$

כלומר f_1, f_2 מייצגות את b מעל $\mathbb{Q}$. לכן $f = f_1 \ominus f_2$ מייצגת אפס מעל $\mathbb{Q}$.

<u>$n \geq 5$:</u> נסמן

$$f = \underbrace{a_1x_1^2 + a_2x_2^2}_{f_1} \ominus \underbrace{- a_3x_3^2 - \dots - a_nx_n^2}_{f_2}$$

כיוון ש־f_v מייצגת אפס ב־$\mathbb{Q}_v$, יש $b_v \in \mathbb{Q}_v^*$ המיוצג ע"י $f_{1,v}$ וגם $f_{2,v}$.

נסמן $S = \{ p \text{ ראשוני} \mid p \mid a_i,\ \exists\, 3 \leq i \leq n \} \cup \{2, \infty\}$

נחשוב על $f_{1,v}$ בתור פונקציה $f_{1,v} : \mathbb{Q}_v \times \mathbb{Q}_v \to \mathbb{Q}_v$ והיא כמובן רציפה, ונתבונן בקבוצה הפתוחה הבאה $\prod_{v \in S} \mathbb{Q}_v$, $\prod_{v \in S} b_v(\mathbb{Q}_v^*)^2$ פתוחה (כי כזכור $(\mathbb{Q}_v^*)^2$ פתוחה ב־$\mathbb{Q}_v$ לכל v).

נתבונן בפונקציה: $f_{1,S} : \prod_{v \in S} \mathbb{Q}_v \times \prod_{v \in S} \mathbb{Q}_v \to \prod_{v \in S} \mathbb{Q}_v$

$$f_{1,S}\left(\prod_{v \in S} x_{1,v}, \prod_{v \in S} x_{2,v}\right) = \prod_{v \in S} f_{1,v}(x_{1,v}, x_{2,v})$$

גם היא, כמובן, פונקציה רציפה, ולכן התמונה ההפוכה של $\prod_{v \in S} b_v(\mathbb{Q}_v^*)^2$ (נסמנה R) תחת $f_{1,S}$ היא פתוחה. זה אומר שאם

$f_{1,v}(\alpha_v, \beta_v) \in b_v(\mathbb{Q}_v^*)^2 \Leftarrow (\alpha, \beta) \in R$ הם כך ש $\alpha = \prod_{v \in S} \alpha_v$, $\beta = \prod_{v \in S} \beta_v$

ממשפט הקירוב, יש $x_1, x_2 \in \mathbb{Q}$ כך שהוקטור שנוצר מהשיכון האלכסוני של x_1, x_2 בתוך $\prod_{v \in S} \mathbb{Q}_v \times \prod_{v \in S} \mathbb{Q}_v$, שייך ל־$R$.

כלומר, לכל $v \in S$ $a_1x_1^2 + a_2x_2^2 = f_{1,v}(x_1, x_2) \in b_v(\mathbb{Q}_v^*)^2$

נסמן $a_1x_1^2 + a_2x_2^2 = a$. לכן a מיוצג ע"י f_1 מעל $\mathbb{Q}$ ומקיים:

$a \equiv b_v \pmod{(\mathbb{Q}_v^*)^2}$ לכל $v \in S$.

נראה כי f_2 מייצגת את a מעל $\mathbb{Q}$.

לשם כך, נראה כי $f_{2,v} \ominus az^2$ מייצגת אפס מעל $\mathbb{Q}_v$ לכל v, ואז נסיק מאינדוקציה.

אם $v \in S$, כיוון ש־$a \in b_v(\mathbb{Q}_v^*)^2$! $f_{2,v}$ מייצגת את b_v, אז $f_{2,v}$ מייצגת את a מעל $\mathbb{Q}_v$.

נניח כי $v \notin S$ $\quad d(f_{2,v}) = a_3 \cdots a_n \in \mathbb{Z}_v^*$

כי $\forall_{3 \leq i}\ a_i \in \mathbb{Z}_v^* \Leftarrow \varepsilon(f_{2,v}) = \prod_{3 \leq i < j \leq n} (a_i, a_j)_v = 1$

ראינו כי $f_{2,v}$ מייצגת את a מעל $\mathbb{Q}_v$ אם $n-2\geq 4$

או $n-2=3$ וגם $a\not\equiv -d(f_{2,v})$ או
$$\begin{cases} a\equiv -d(f_{2,v}) \\ \underbrace{(-1,-d(f_{2,v}))_v}_{=1} = \underbrace{\varepsilon(f_{2,v})}_{=1} \end{cases}$$
$\hat{Z}_v^*$

באינדוקציה $f_2\oplus az^2$ מייצגת אפס מעל $\mathbb{Q}$, כלומר f_2 מייצגת a מעל $\mathbb{Q}$ ולכן $f=f_1\oplus f_2$ מייצגת אפס מעל $\mathbb{Q}$.

<u>משפט</u>: יהי $0\neq a\in\mathbb{Q}$, אז ל-a יש שורש ריבועי רציונלי אם״ם יש ל-a שורש ריבועי ב-$\mathbb{Q}_v$ כמעט לכל v.

<u>הוכחה</u>: נניח כי כמעט לכל v: $a\in(\mathbb{Q}_v^*)^2$. לכן כמעט לכל p ראשוני זר ל-a $a\in(\mathbb{Q}_p^*)^2$ ולכן התבנית x^2-ay^2 מייצגת אפס מעל $\mathbb{Q}_p$.
לכן יש פתרון פרימיטיבי מעל $\mathbb{Z}_p$ ל-$x^2-ay^2=0$: וכמו קודם בהכרח $x,y\in\mathbb{Z}_p^*$ ($a\in\mathbb{Z}_p^*$). ולכן a הוא ריבוע ב-$\mathbb{Z}_p^*$. נסיק שהוא שארית ריבועית מודולו p. (כמו קודם אפשר להניח כי $a\in\mathbb{Z}$).
לכן כמעט לכל p ראשוני $\left(\frac{a}{p}\right)=1$.
אם a אינו ריבוע שלם ראינו כי הצפיפות של $\{p \text{ ראשוני} \mid \left(\frac{a}{p}\right)=1\}$ היא ½, ולכן השוויון $\left(\frac{a}{p}\right)=1$ אינו יכול להתקיים כמעט לכל p ראשוני.
<u>מסקנה: a ריבוע שלם.</u>

<u>משפט</u>: תהיינה f,f' שתי תבניות ריבועיות לא מנוונות, באותו מספר משתנים מעל $\mathbb{Q}$, אז $f\sim f'$ מעל $\mathbb{Q}$ $\Leftrightarrow$ $f_v\sim f'_v$ לכל v.

<u>הוכחה</u>: $\Rightarrow$ יהי $0\neq a\in\mathbb{Q}$ המיוצג ע״י f, אז a מיוצג גם ע״י f' (מעל $\mathbb{Q}$), כי a מיוצג ע״י f'_v מעל v, ולכן a מיוצג ע״י f'.
לכן אפשר לרשום $f\sim f_1\oplus az^2$, $f'\sim f_1'\oplus az^2$ (f_1',f_1 תבניות ריבועיות לא מנוונות כי זה משפט מעל $\mathbb{Q}$)
כיוון ש $f_v\sim f'_v \Rightarrow f_{1,v}\oplus az^2\sim f'_{1,v}\oplus az^2 \Rightarrow f'_{1,v}\sim f_{1,v}$ $\forall v$
באינדוקציה f_1 שקולה ל-f_1' (המקרה n=1 טריוויאלי).
ולכן $f\sim f_1\oplus az^2\sim f_1'\oplus az^2\sim f'$.

משפט: תהיינה f, f' שתי תבניות ריבועיות לא מנוונות, ב-n משתנים,
מעל $\mathbb{Q}$, אז $f\sim f' \Leftrightarrow$

1) לכל p ראשוני $\varepsilon_p(f)=\varepsilon_p(f')$
2) כמעט לכל p ראשוני $d_p(f)\equiv d_p(f')$
3) ל-f_∞ ול-f'_∞ יש אותה סיגנטורה.

הערה ②: $\overset{\text{רציונלי}}{\frac{d(f)}{d(f')}}\in(\mathbb{Q}_p^*)^2$ כמעט לכל p.

$\Leftarrow \frac{d(f)}{d(f')}\in(\mathbb{Q}^*)^2$ ולכן $d(f)\equiv d(f') \pmod{(\mathbb{Q}^*)^2}$.

לתבנית f מעל $\mathbb{Q}$, לא מנוונת, ב-n משתנים
סיגנטורה, $\underline{d, \{\varepsilon_v\}_{v\in V}}$ מקיימים:

1) $\varepsilon_v=1$, כמעט לכל v, וגם $\prod_{v\in V}\varepsilon_v=1$
2) כאשר $n=1$, $\varepsilon_v=1$, לכל v
וכאשר $n=2$, אם $d_v\equiv -1$ אז $\varepsilon_v=1$
($f=a_1x_1^2+a_2x_2^2$, $\varepsilon_v=(a_1,a_2)_v=(a_1,-a_1a_2)=(a_1,-d_v)_v$)
3) נסמן את הסיגנטורה של f_∞ ב-(r,s), $r+s=n$.
4) $\varepsilon_\infty=(-1)^{\frac{s(s-1)}{2}}$, $d_\infty=(-1)^s$

משפט: נתונים n טבעי, $d\in\mathbb{Q}^*$, סדרה $\{\varepsilon_v=\pm1\}_{v\in V}$ וזוג שלמים אי שליליים (r,s) המקיימים ①-⑤ (כאשר d_v היא התמונה של d ב-$\mathbb{Q}_v^*/(\mathbb{Q}_v^*)^2$)
אז יש תבנית ריבועית לא מנוונת f ב-n משתנים מעל $\mathbb{Q}$
כך ש-$d(f)\equiv d \pmod{(\mathbb{Q}^*)^2}$, $\varepsilon_v(f)=\varepsilon_v\ \forall v$, $(r,s)=$ סיגנטורה של f

הוכחה: $n=1$: קח $f=dx^2$
$n=2$: לכל v יש $b_v\in\mathbb{Q}_v^*$ כך ש: $(b_v,-d_v)_v=\varepsilon_v$
אם $-d_v\not\equiv 1$, אז מיון שסמל הילברט מעל $\mathbb{Q}_v$ מנוון יש b כזה.
אם $-d_v\equiv 1$, אז לפי (2) $\varepsilon_v=1$, ואז אפשר לבחור b כלשהו.
לפי קודם, יש $b\in\mathbb{Q}^*$, כך ש: $(b,-d)_v=\varepsilon_v$ לכל v.
נגדיר $f=bx^2+dby^2$. $d(f)=b^2d\equiv d$, $\varepsilon_v(f)=(b,bd)_v=(b,-d)_v=\varepsilon_v$.
מיון ש-$n=2$, d_∞, ε_∞ קובעים את s ולכן את הסיגנטורה של f_∞.

n=3: נסמן $S=\{v \mid (-1,-d)_v = -\varepsilon_v\}$ זוהי קבוצה סופית.

כי $(-1,-d)_v = 1 = \varepsilon_v$ כמעט לכל v.

לכל $v\in S$, נבחר $c_v \in \mathbb{Q}_v^*$ כך ש: $c_v \not\equiv -d_v \pmod{(\mathbb{Q}_v^*)^2}$

כמו קודם יש $c\in\mathbb{Q}^*$ כך ש $c\in c_v(\mathbb{Q}_v^*)^2 \quad \forall v\in S$

נגדיר $\tilde{d} = cd$, $\tilde{\varepsilon}_v = (c,-d)_v\varepsilon_v$,

$\{\tilde{\varepsilon}_v\}$, $\tilde{d}$ מגדירים תבנית g בשני משתנים מעל $\mathbb{Q}$.

אם $\tilde{d}_v \equiv -1$, אז $c_v d_v \equiv -1$ כלומר $-cd$ הוא ריבוע ב $\mathbb{Q}_v$,..

$\tilde{\varepsilon}_v = (c,-d)_v\varepsilon_v = (-d,d)_v\varepsilon_v = (-d,-1)_v\varepsilon_v$

לכן $v\notin S$ (מהגדרת S).

לכן צריך לבדוק עבור $v\notin S$ ($(-1,-d)_v=\varepsilon_v$) ואז $\tilde{\varepsilon}_v = \varepsilon_v^2 = 1$.

תהי g בשני משתנים כנ"ל ($\varepsilon_v(g)=\tilde{\varepsilon}_v$, $d(g)=\tilde{d}$). נגדיר $f = cx^2 \oplus g$.

$d(f) = cd(g) = ccd \equiv d$, $\varepsilon_v(f) = (c,d(g))_v\varepsilon_v(g) =$

$= (c,cd)_v(c,-d)_v\varepsilon_v = (c,-d)_v(c,-d)_v\varepsilon_v = \varepsilon_v$

כיוון ש $n=3$, $\varepsilon_\infty, d_\infty$ קובעים את s לכן את הסיגנטורה.

n≥4: נניח $r\geq 1$. באינדוקציה, יש תבנית f_1 ב-$n-1$ משתנים, לא מנוונת, מעל $\mathbb{Q}$ כך ש: $d(f_1)=d$, $\varepsilon_v(f_1)=\varepsilon_v$ וסיגנטורה $(r-1,s)$

נגדיר $f = x^2\oplus f_1$ ואז f כנדרש.

נניח $r=0$; $\underbrace{\tilde{d} = -d \,,\ \tilde{\varepsilon}_v = (-1,-d)_v\varepsilon_v \,,\ \tilde{s} = s-1}_{\text{מקיימים את ①-⑤ בשביל } n-1 \text{ משתנים}}$.

$\tilde{d}_\infty = -d_\infty = -(-1)^s = (-1)^{s-1} = (-1)^{\tilde{s}}$.

$\tilde{\varepsilon}_\infty = (-1,(-1)^{n-1})_{\mathbb{R}}(-1)^{s(s-1)/2} = (-1)^{n-1+\frac{n(n-1)}{2}} = (-1)^{(n-1)(1+\frac{n}{2})} =$

$= (-1)^{\frac{s}{2}(n-1)(n-2)} = (-1)^{\tilde{s}\frac{(\tilde{s}-1)}{2}}$

באינדוקציה יש תבנית ריבועית לא מנוונת ב $n-1$ משתנים, f_1, מעל $\mathbb{Q}$

כך ש: $d(f_1) \equiv \tilde{d}$, $\varepsilon_v(f_1)=\tilde{\varepsilon}_v$, סיגנטורה $=(0,n-1)$.

נגדיר $f=-x^2\oplus f_1$. $d(f) = -d(f_1) = -\tilde{d} = d$

$\varepsilon_v(f) = (-1,d(f_1))_v\varepsilon_v(f_1) = (-1,-d)_v(-1,-d)_v\varepsilon_v = \varepsilon_v$