הרצאה 26

<u>תזכורת</u> (מתמורות). תהי G חבורה שפועלת על קבוצה A.

תהי S_A חבורת התמורות של A.

אזי פעולה (משמאל) של G על A $\leftrightarrow$ הומ' $f: G \to S_A$

$$G \times A \to A \quad \longleftarrow \quad f(g) = \{a \mapsto ga\}$$

$$f: G \to S_A \quad \longmapsto \quad g \cdot a = (f(g))(a) \qquad f(g): A \to A$$

<u>הגדרה</u> תהי G חבורה. הצגה של G על מרחב וקטורי V (מעל שדה F) היינו הומ' $\rho: G \to Aut_F(V)$

$$Aut_F(V) = \{ f: V \to V \quad F\text{-ליניארי חח״ע ועל} \} \leq S_V$$

אם V n-מימדי ואם נבחר בסיס של V, אזי נקבל

$$Aut_F(V) \simeq GL_n(F)$$

<u>דוגמאות</u> 1) $G = GL_n(F)$ ו- $V = F$ מרחב וקטורי 1-מימדי

$$\rho: G \to Aut_F(V) \simeq F^* = F \setminus \{0\} = GL_1(F)$$

$$g \mapsto \det g$$

2) $G = GL_2(F)$. ויהי $d \in \mathbb{N}$

$$V = \left\{ \begin{array}{r} P \in F[x,y] \quad \text{פולינומים} \\ d \quad \text{הומוגניים ממעלה} \end{array} \right\} = \left\{ \sum_{i=0}^{d} a_i x^i y^{d-i} : a_i \in F \right\}$$

מ"ו $(d+1)$-מימדי מעל F.

$$\rho : G \longrightarrow Aut_V(F) \qquad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$$

$$\overbrace{\rho(g)(P)}^{gP} \in V$$

$$(\rho(g)(P))(x,y) = P(ax+cy,\, bx+dy)$$

$$d = 2$$

$$P(x,y) = x^2 + 2xy$$

$$g = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$$

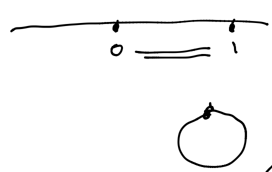
$$\rho(g)P = (x+0y)^2 + 2(x+0y)(6x+y) =$$

$$x^2 + 2x(6x+y) = 13x^2 + 2xy$$

3) $G = \mathbb{R}/\mathbb{Z}$ $\qquad V = \mathbb{R}^2$

$$\rho : G \longrightarrow GL_2(\mathbb{R}) = Aut_{\mathbb{R}}(V)$$

$$x \longmapsto \begin{pmatrix} \cos 2\pi x & -\sin 2\pi x \\ \sin 2\pi x & \cos 2\pi x \end{pmatrix}$$



מעגל
עם
היקף 1

$x \longmapsto$ {סיבוב בזוית $2\pi x$}

חח"ע $\rho : G \hookrightarrow GL_2(\mathbb{R})$

4) $G = D_n$

$= \langle r, s : r^2 = s^n = e,\ rs = s^{-1} r \rangle$

$\rho : D_n \hookrightarrow GL_2(\mathbb{R})$

$$\rho(r) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\rho(s) = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}$$

5) $G = S_n$ $\quad V = F^n = \langle e_1, e_2, \dots, e_n \rangle$

$\sigma \in S_n$

$$\rho(\sigma) : \underbrace{(e_i \longmapsto e_{\sigma(i)})}$$

מטריצה של אפסים ו-1-ים

בכל שורה ובכל עמודה יש בדיוק 1 יחיד

6) סגור אלגברי של $\mathbb{Q}$ $= \overline{\mathbb{Q}} = \{ z \in \mathbb{C} :$ z שורש של פולינום עם מקדמים ב-$\mathbb{Q}$ $\} \subseteq \mathbb{C}$

$G = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$

$\overline{\mathbb{Q}} = \{$ הסגור האלגברי של $\mathbb{Q}$ ב-$\mathbb{C}$ $\}$

$G = \{ \sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}} :$ σ אוטומורפיזם של שדות $\}$

כן החבורה מסובכת ביותר. משימה נואשת לעבוד איתה
ישירות, רוצים למצוא הצגות.

קודם כל, נראה פעולות של G על יריעות.

תהי U יריעה אלגברית מעל $\mathbb{Q}$:

$$U=\{(a_1,\dots,a_n)\in\bar{\mathbb{Q}}^n : f_1(\underline{a})=f_2(\underline{a})=\dots=f_m(\underline{a})=0\}$$
$$f_i\in\mathbb{Q}[x_1,\dots,x_n]$$

יש פעולה של G על $\bar{\mathbb{Q}}^n$:

$$\sigma(a_1,\dots,a_n)\longmapsto(\sigma(a_1),\dots,\sigma(a_n))$$

והפעולה הנ״ל שומרת את U. אכן, יהי

$$f_i(x_1,\dots,x_n)=\sum b_{i_1,\dots,i_n}x_1^{i_1}\cdots x_n^{i_n},\quad b_{i_1,\dots,i_n}\in\mathbb{Q}$$

$$f_i(\underline{a})=\sum b_{i_1,\dots,i_n}a_1^{i_1}\cdots a_n^{i_n}=0 \quad\Leftarrow \underline{a}\in U$$

$\sigma(1)=1$
$\sigma(n)=n$ לכל $n\in\mathbb{Z}$
$\sigma(\frac{m}{n})=\frac{m}{n}$ לכל $\frac{m}{n}\in\mathbb{Q}$.

$$\sum\sigma(b_{i_1,\dots,i_n})\sigma(a_1)^{i_1}\cdots\sigma(a_n)^{i_n}=$$
$$\sum b_{i_1,\dots,i_n}\sigma(a_1)^{i_1}\cdots\sigma(a_n)^{i_n}$$

לכן $f_i(\sigma(\underline{a}))=0$. לכן $\sigma:U\to U$

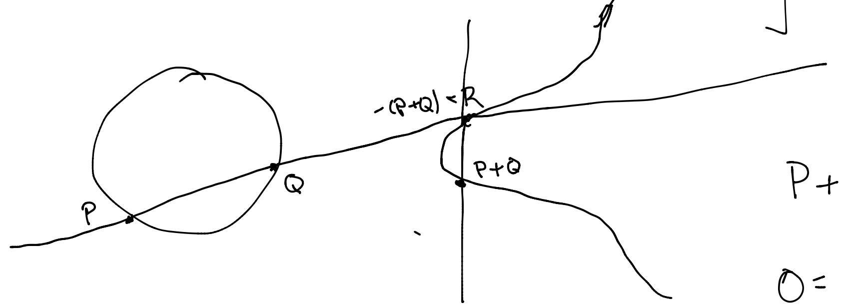
כל הפעולות האלה בגרון כלל לא הלקוה, כי לקבוצה U אין מבנה של מ"ו.

E עקום אליפטי מעל $\mathbb{Q}$

יריעה אלגברית. $E: \{ y^2 = x^3 + bx + c, \quad b, c \in \mathbb{Q} \}$

<u>עובדה</u> לקבוצה $E(\overline{\mathbb{Q}}) = \{ (x,y) \in \overline{\mathbb{Q}}^2 : y^2 = x^3 + bx + c \} \cup \{\infty\}$

יש מבנה של חבורה אבלית.



$P + Q + R = O$

כאשר $O = \infty$

הנקודה באינסוף

יהי $n \in \mathbb{N}$, נגדיר ה-n-פיתול

$$E[n] : \{ P = (x,y) \in E(\overline{\mathbb{Q}}) : \underbrace{P + P + \cdots + P}_{n \text{ פעמים}} = O \} \underset{\text{חבורה}}{\le} E(\overline{\mathbb{Q}})$$

נשים לב כי $E[n]$ גם יריעה, מוגדרת על ידי אפסים פולינומים.

<u>עובדה</u> $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

נניח $n=p$ ראשוני. אזי $E[p]\simeq \mathbb{F}_p^2$ מ"ו דו-מימדי מעל $\mathbb{F}_p$.

$G=Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ פועלת על נק', כי נק' $E[p]$ יריעה אלגברית מעל $\mathbb{Q}$.

<u>תזכורת</u> יהי G חבורה, F שדה. הגדרנו חוג של חבורה

$$F[G]=\left\{\sum_{g\in G} a_g\cdot g \ : \ \begin{array}{c} a_g\in F \\ \text{רק מספר} \\ \text{סופי של} \\ a_g\text{-ים שונים} \\ \text{מאפס} \end{array}\right\}$$

$$(a_g\cdot g)(b_h\cdot h)= a_g b_h\cdot gh$$

<u>טענה</u> הצגה של G על מ"ו V $\longleftrightarrow$ מבנה של $F[G]$-מודול על V.

אכן, בהינתן הצגה $\rho: G\to Aut_F(V)$, נגדיר

$v\in V$

$$\left(\sum a_g\cdot g\right)v = \sum a_g\,(\rho(g))(v)$$

כך ניתן מבנה של $F[G]$-מודול על V.

אם נתון מבנה של $F[G]$-מודול על V, נקבל הצגה

$$(\rho(g))(v)= (1_F\cdot g)v$$

הגדרה תהי $\rho : G \to Aut_F(V)$ הצגה. תת-הצגה הינה תת-מרחב $W \subseteq V$ שנשמר תחת הפעולה, כלומר $(\rho(g))(w) \in W$ לכל $g \in G$, $w \in W$.

משפט (משפט משקה) (Maschke) תהי G חבורה סופית. נניח כי $\operatorname{char} F = 0$ או $(\operatorname{char} F) \nmid |G|$. תהי $\rho : G \to Aut_F(V)$ הצגה, תהי $W \subseteq V$ תת-הצגה. אזי קיימת תת-הצגה אחרת $W' \subseteq V$ כך ש- $V \simeq W \times W'$.

הוכחה תהי $W \subseteq V$ תת-הצגה. תהי $\pi : V \to W$ הטלה F-לינארית על W, כלומר $\pi(w) = w$ לכל $w \in W$.

נגדיר $\varphi : V \to W$

$$\varphi(v) = \frac{1}{|G|} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot v) \in W$$

$\varphi(w) = w$ לכל $w \in W$.

$\left(g \cdot v = (\rho(g))(v) \right)$

אני טוען כי $\varphi : V \to W$ הינו הומ' של $F[G]$-מודולים.
יהי $W' = \ker \varphi$, לכן W' הינו $F[G]$-תת-מודול של V, כלומר תת-הצגה. אני טוען כי $V \simeq W \times W'$.