22.3.10

שיעור 5

נניח כי $F \subseteq k$ שדות. נאמר ש- k הרחבה אלגברית של F, אם כל איבר של k הוא אלגברי מעל F. איבר $a \in k$ הוא אלגברי מעל F, אם יש פולינום $f(x) \in F[x]$ כך ש: $f(a) = 0$.

למשל אם $\dim_F k = n < \infty$, אז k היא הרחבה אלגברית. כי לכל $a \in k$, הקבוצה $\{1, a, \dots, a^n\}$ תלויה לינארית מעל F.

הגדרה: שדה k יקרא סגור אלגברית, אם לכל פולינום ב- $k[x]$ יש שורש ב- k.

משפט: לכל שדה F, יש שדה סגור אלגברית k, ושיכון של F בשדה $k \xrightarrow{\sigma} F$, כך שלכל שדה סגור אלגברית Σ ושיכון $\eta : F \to \Sigma$ אז יש שיכון יחיד $\alpha : k \to \Sigma$, כך ש: $\eta = \sigma \circ \alpha$.

נשתמש כי k הוא **סגור** האלגברי של F.

k מכיל כל הרחבה אלגברית של F. כלומר, אם $L \supseteq F$ הרחבה אלגברית, אז אפשר להרחיב את σ לשיכון $\sigma : L \to k$.

סימון מקובל: $\bar{F} = k \supseteq F$

משפט: יהי k שדה סגור אלגברית מהמציין p (ראשוני). אז לכל n טבעי, k מכיל שדה חלקי יחיד בעל p^n איברים. שדה זה נתון ע"י: $\{0 = t^q - t \mid t \in k\}$ $(q = p^n)$.

הוכחה: ראינו כי ההעתקה $\sigma : k \to k$ המוגדרת $\sigma(a) = a^p$, היא הומומורפיזם חח"ע של שדות. σ זה נקרא, כי k סגור אלגברית, לכל k אפשר לפולינום $x^p - a = 0$ יש שורש ב- k. מכאן $a = f(a)^p$ הוא הומומורפיזם של k על עצמו.

תת-חבורה של k^+ היא $F = \{t \in k \mid f(t) = t\}$

F סגור תחת חיבור, כלומר:

$$f(t_1 + t_2) = t_1 + t_2 = f(t_1) + f(t_2)$$

$$1 \in F \iff f(1) = 1^q = 1$$

$$0 \in F \iff f(0) = 0^q = 0$$

$$t \neq 0 \quad f(t^{-1}) = t^{-q} \quad \exists t^{-1} \in F \iff$$

לכן F שדה עליו k.

~~[illegible]~~ $|F| \geq \deg(x^q - x) = q$

אבל לפולינום $x^q - x$ לא שורשים מרובים, כי נגזרתו

היא: $f' = 1 - 0 \cdot x^{q-1} = 1 \neq 0$.

כיוון ש-k סגור אלגברית, $x^q - x$ מתפרק למכפלת

גורמים לינאריים שונים מעל k. מכאן: $|F| = q$.

יחידות: נניח כי $|L| = q$ הוא שדה עליו, בעל q איברים.

$L^* = L \setminus \{0\}$, היא חבורה ביחס לכפל (ב k) בעל

$q-1$ איברים.

בפרט: $\forall a \neq 0 \quad a^{q-1} = 1$ לכן $\forall a \in L$.

לכן $a^q = a$ לכל $a \in L$.

כלומר $F \subseteq L$ ומשום ש $|F| = q = |L|$, $F = L$.

משפט: לכל שני שדות סופיים בעלי אותו מספר איברים יש

איזומורפיזם.

הוכחה: נניח כי F_1, F_2 הם שדות סופיים בעלי $q = p^n$

איברים (p ראשוני). לכן יש שיכון $\alpha_i : \mathbb{Z}_p \hookrightarrow F_i$.

נקבע סגור אלגברי $\overline{\mathbb{Z}}_p \supseteq \mathbb{Z}_p$.

כמו שציינו קודם, יש שיכון $\eta_i : F_i \hookrightarrow \overline{\mathbb{Z}}_p$

$$\eta_i \circ \alpha_i = \alpha \quad \text{כך ש} \quad \overline{\mathbb{Z}}_p \supseteq \mathbb{Z}_p \xrightarrow{\alpha} F_i \xrightarrow{\eta_i} \overline{\mathbb{Z}}_p$$

מתכונת היקודים: $\eta_2(F_2) = \eta_1(F_1)$ מכאן $\eta_2^{-1} \circ \eta_1 : F_1 \to F_2$

הוא איזומורפיזם בין F_1 ל F_2.

למה: תהי G חבורה סופית מסדר n, נניח כי לכל מחלק d של n, קבוצת $\{g \in G \mid g^d = 1\}$ מכילה לכל היותר d איברים. אז G ציקלית.

הוכחה: נניח כי n. יש $a \in G$ מסדר d. נראה כי קיים $g \in G$ מסדר d. נשים לב כי $\langle a \rangle$ היא בעלת d איברים, ולכולם מקיימים $g^d = 1$.

$$\langle a \rangle = \{g \in G \mid g^d = 1\}$$

נסמן: בנוסף לכך איבר מסדר d הוא יוצר ציקלי של $\langle a \rangle$, ו $\psi(d)$ כאלה.

נשים לב ש n או 0 איברים מסדר d, או $\phi(d)$ איברים מסדר d.

נניח כי $d_1, \ldots, d_k$ הם כל המחלקים הטבעיים של n שעבורם ב-G יש איבר מסדר d_i. מכיוון שלכל איבר ב-G יש סדר המחלק את n נקבל: $n = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_k)$.

נוסחת ϕ מקיימת $n = \sum_{d \mid n} \phi(d)$.

נסיים כי $\{d \mid n \geq 1\} = \{d_1, \ldots, d_k\}$

מכאן יש ב-G איבר מסדר n. ולכן G ציקלית.

מסקנה: יהי F שדה, אז כל תת חבורה סופית של F^* היא ציקלית.

הוכחה: נניח כי $G \leq F^*$ היא תת חבורה בגודל n. יהי $d \mid n$:

בעלת d איברים $\longleftarrow$ $\{$שורשי הפולינום $x^d - 1$ בשדה $F\} \supseteq \{g \in G \mid g^d = 1\}$

מסקנה: $F_q^* = F_q \setminus \{0\}$ ציקלית.

משפט Chevalley

יהי F שדה סופי. משתנים מעל $F[x_1,\dots x_n]$ $f_1,\dots f_l$.
כך ש: $\sum_{i=1}^{l}\deg f_i < n$ נסמן:
$V=\{(t_1,\dots,t_n)\in F^n \mid \forall i\le l \; f_i(t_1,\dots t_n)=0\}$
ונניח $q=p^m=|F|$ (חזקה של p). אז: $|V|\equiv 0 \pmod p$.

הוכחה: נגדיר:

$$g(x_1,\dots x_n)=\prod_{i=1}^{l}\left(1-[f_i(x_1,\dots x_n)]^{q-1}\right)\in F[x_1,\dots x_n]$$

נשים לב כי $g(x_1,\dots x_n)$, כפונקציה מ-F^n לתוך עצמו, מקבלת את הערך 1 בכל נקודה $v\in V$, שכן $f_i(v)=0$ לכל i, ולכן $1-f_i(v)^{q-1}=1$ לכל i, ומכאן $g(v)=1$.
אם $v\in F^n\setminus V$, אז קיים $1\le j\le l$ כך ש-$f_j(v)\neq 0$. כיוון ש-F^* היא חבורה סופית מסדר $q-1$, מתקיים $f_j(v)^{q-1}=1$, ולכן $1-f_j(v)^{q-1}=0$, כלומר $g(v)=0$.
לכן $S(g)\equiv\sum_{u\in F^n} g(u)=|V|\cdot 1_F$ (סכום ב-F).
נראה כי $S(g)=0$, ומכאן $|V|\cdot 1_F=0$, כלומר $p\mid |V|$.

$$g=\sum_{1\le i_1<i_2<\dots<i_s\le l}\alpha_{i_1,\dots i_s} f_{i_1}^{q-1}\cdot\dots\cdot f_{i_s}^{q-1}$$

$$\Rightarrow \deg g(x_1,\dots x_n)\le \max\{\deg(f_{i_1}^{q-1}\cdot\dots\cdot f_{i_s}^{q-1})\}=$$
$$=(q-1)\sum_{i=1}^{l}\deg f_i < n(q-1)$$

יהי $M=x_1^{k_1}\cdot\dots\cdot x_n^{k_n}$ מונום השונה מ-$g(x_1,\dots x_n)$.
נראה כי $S(M)=0$.

$$S(M)=\sum_{t_1,\dots t_n\in F} t_1^{k_1}\cdots t_n^{k_n}=\prod_{i=1}^{n}\left(\sum_{t_i\in F} t_i^{k_i}\right)$$

נשים לב כי אם קיים i כך ש-$k_i=0$, אז הסכום שווה 0 (כשכל $t^0=1$).

$$\sum_{t_j \in F} t_j^{k_j} = \sum_{t_j \in F} 1_F = |F| \cdot 1_F = q \cdot 1_F = 0$$

$$\sum_{t_1, \ldots, t_{j-1}, t_{j+1}, \ldots, t_n \in F} \sum_{t_j \in F} t_1^{k_1} \cdot \ldots \cdot t_{j-1}^{k_{j-1}} \cdot t_{j+1}^{k_{j+1}} \cdot \ldots \cdot t_n^{k_n} =$$

$$= \sum q \cdot t_1^{k_1} \cdot \ldots \cdot t_{j-1}^{k_{j-1}} \cdot t_{j+1}^{k_{j+1}} \cdot \ldots \cdot t_n^{k_n} = 0$$

k_j לפחות אחד j כך ש- $k_i \neq 0$ נניח כי $q-1$ לא מחלק את k_j.
($k_j \geq 1$ ו- $q-1$ לא מחלק את k_j משום ש- $\sum_{i=1}^{n} k_i \geq n(q-1)$).
נרשום כי $\sum_{t \in F} t^{k_j} = 0$.

יהי $a \in F^*$ יוצר של החבורה הכפלית F^*. מכיוון ש- $q-1$ לא מחלק את k_j,
$a^{k_j} \neq 1$.

$$\sum_{t \in F} t^{k_j} = \sum_{t \in F^*} t^{k_j}$$

$$a^{k_j} \left(\sum_{t \in F^*} t^{k_j} \right) = \sum_{t \in F^*} (at)^{k_j} \underset{t \mapsto at}{=} \sum_{t \in F^*} t^{k_j}$$

$$\Rightarrow (a^{k_j} - 1) \left(\sum_{t \in F^*} t^{k_j} \right) = 0 \Rightarrow \sum_{t \in F^*} t^{k_j} = 0$$
$\neq 0$

משפט: יהי F שדה סופי, ונניח כי $f_1, \ldots, f_l \in F[x_1, \ldots, x_n]$.
כך ש: $f_i(0, \ldots, 0) = 0$ (כלומר ללא איבר חופשי).
ונניח כי $n > \sum_{i=1}^{l} \deg f_i$.
אזי קיים $0 \neq v \in F^n$ כך ש $f_i(v) = 0$ לכל $i \leq l$.

הוכחה: באינדוקציה מקוננת על $V \ni (0, \ldots, 0)$, לכן $1 \leq |V|$.
יהי d כך ש $|V| \leq d$, ונניח ש $V \ni v \neq 0$. אז

משפט: יהי F שדה סופי, כל תבנית ריבועית בשדה מספרים
ומעלה מ-2 משתנים מעל F.

$$f(x_1, \ldots, x_n) = (x_1 \ldots x_n) A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \qquad A = A^t \in M_n(F)$$

$$= \sum_{i=1}^{n} a_{ii} x_i^2 + 2 \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j$$

(משפט שאנחנו נוכיח מאוחר יותר) קיים $t \in F^n$ כך ש $f(t)=0$ אבל $t \neq 0$.

כלומר $n \geq 3$, $\deg f = 2$, $n \geq 3 > 2$, $l=1$.

טענה 3: שדה המספרים ה- p-אדיים (p ראשוני)

המרחב $\mathbb{Z}_p$ (הוא נקרא גם ה-p-אדיים) ($\mathbb{Z}_p$ ו).

נשתמש בחוגים $A_n = \mathbb{Z}/p^n\mathbb{Z}$ לכל $n \geq 1$ ובהומומורפיזמים:

$$\phi_n : A_n \to A_{n-1} \qquad \phi_n(a+p^n\mathbb{Z}) = a+p^{n-1}\mathbb{Z}$$

$$\ker \phi_n = \{ p^{n-1}\alpha + p^n\mathbb{Z} \mid \alpha \in \mathbb{Z} \} = p^{n-1}A_n$$

$$\cdots \to A_{n+1} \xrightarrow{\phi_{n+1}} A_n \xrightarrow{\phi_n} A_{n-1} \to \cdots \to A_3 \xrightarrow{\phi_3} A_2 \xrightarrow{\phi_2} A_1$$

נגדיר: $Z_p = \left\{ \{x_k\}_{k=1}^{\infty} \mid x_n \in A_n \ \ \phi_n(x_n) = x_{n-1} \ \forall n \right\}$

$Z_p \subseteq \prod_{n=1}^{\infty} A_n$.

$Z_p \neq \phi$ (נראה בקרוב), כי לכל $a \in \mathbb{Z}$, נגדיר $i(a) = \{a+p^n\mathbb{Z}\}_{n=1}^{\infty}$?
ברור כי $\phi_n(a+p^n\mathbb{Z}) = a+p^{n-1}\mathbb{Z}$ לכל $n \geq 2$.
$\Rightarrow i(a) \in Z_p$

Z_p הוא חוג כיוון שניתן לחבר ולכפול סדרות לפי הקואורדינטות.

$$\{x_n\}_{n=1}^{\infty} + \{y_n\}_{n=1}^{\infty} = \{x_n+y_n\}_{n=1}^{\infty}$$

$$\phi(x_n+y_n) = \phi(x_n)+\phi(y_n) = x_{n-1}+y_{n-1}$$

ובכך ו לכל n.

$\hat{i}(1) = \{1 + p^n\mathbb{Z}\}_{n=1}^{\infty}$: מוגדר הומומורפיזם

$\hat{i}(0) = \{0 + p^n\mathbb{Z}\}_{n=1}^{\infty}$: מוגדר הומומורפיזם

טענה: $i : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ הוא הומומורפיזם חח"ע שאינו על.

הומומורפיזם: ברור.

חח"ע: אם $a \in \ker i$ אז לכל n מתקיים $p^n \mid a$.

לכן ישנם רק אחד $a = 0$.

הגדרה: $\varepsilon_n : \mathbb{Z}_p \longrightarrow A_n$, $\varepsilon_n(\{x_k\}_{k=1}^{\infty}) = x_n$.

ε_n הוא הומומורפיזם על שאינו.

לכל m שלם נגדיר $l_m : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$, $l_m(x) = mx$.

$l_m(x) = \underbrace{x + x + \cdots + x}_{m} = x \cdot i(m) = \{mx_k\}_{k=1}^{\infty}$

כלומר הומומורפיזם על המבוי המבוי.

$l_m(x+y) = m(x+y) = m(x) + m(y)$.

משפט: הסדרה הבאה היא מדויקת:

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{l_{p^n}} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \longrightarrow 0$$

כלומר: ε_n על, l_{p^n} חח"ע, $\operatorname{Im}(l_{p^n}) = \ker(\varepsilon_n)$

חח"ע l_{p^n}: כיוון ש-l_{p^n} היא הכפלה על p^n אשר שונה מאפס,

כי $\mathbb{Z}_p$ תחום שלמות. נראה כי $\ker l_{p^n} = 0$.

נניח כי $x \in \mathbb{Z}_p$ הוא כזה כך ש- $p^n x = 0$.

נפתוח $x = \{x_n\}_{n=1}^{\infty} = \{a_n + p^n\mathbb{Z}\}_{n=1}^{\infty}$ אז

$p^n x = p^n a_n + p^n\mathbb{Z} = p^n\mathbb{Z}$ כלומר $p^n a_n \in p^n\mathbb{Z}$ $\forall n$.

לכן $p^n \mid a_n$ $\forall n$

$\Leftarrow$ $p^n \mid a_{n+1}$ $\forall n$

מ-$\phi_{n+1}(a_{n+1} + p^{n+1}\mathbb{Z}) = a_n + p^n\mathbb{Z}$ נקבל ($x \in \mathbb{Z}_p$ כי)

לכן $a_{n+1} \equiv a_n \pmod{p^n}$

כיוון ש-$p^n \mid a_{n+1}$ נקבל כי $p^n \mid a_n$ לכל $n \geq 1$ לכן

$x_n = a_n + p^n\mathbb{Z} = 0$ לכל $n \geq 1$. $\Leftarrow$ $x = 0$.

$$\varepsilon_n(\ell_{p^n}(x)) = \varepsilon_n(\lambda_{p^n}(\{x_k\}_{k=1}^\infty)) = \varepsilon_n(\{p^n x_k\}_{k=1}^\infty) = p^n x_n = 0$$

$\underline{\mathrm{Im}(\ell_{p^n}) \subseteq \ker \varepsilon_n}$

$x = \{x_k\}_{k=1}^\infty = \{a_k + p^k\mathbb{Z}\}_{k=1}^\infty$ נניח כי $\varepsilon_n(x) = 0$ ולכן

$$a_n + p^n\mathbb{Z} = p^n\mathbb{Z} \Rightarrow p^n \mid a_n$$

נשים לב כי, $1 \le k \le n$ לכל k, אם $p^n \mid a_n$ אז

$$a_n \equiv a_{n-1} \pmod{p^{n-1}} \Rightarrow p^{n-1} \mid a_{n-1}$$

$$\vdots$$

$$a_2 \equiv a_1 \pmod{p} \Rightarrow p \mid a_1$$

$n \ge k$ לכל $x_k = 0$ מתקיים

$k \ge n+1$ לכל k מתקיים

$$a_{n+1} \equiv a_n \pmod{p^n}$$

$$a_{n+2} \equiv a_{n+1} \pmod{p^n}$$

$$\vdots \Rightarrow p^n \mid a_k \quad \forall k > n$$

כלומר $a_k = p^n v_k$, $v_k \in \mathbb{Z}$, $b_k = v_k + p^k\mathbb{Z} \in A_k$.

$$x_k = p^n v_k + p^k\mathbb{Z} = p^n b_k$$

$\underline{\text{בכיוון}}$: $y = \{\ldots, v_{n+k} + p^k\mathbb{Z}, \ldots, v_{n+1} + p\mathbb{Z}\}$

$y_k = v_{n+k} + p^k\mathbb{Z}$.

$\ell_{p^n}(y) = x$ כך ש

$y \in \mathbb{Z}_p$ כך ש $\exists$ מתקיים

$$\phi_{n+k+1}(x_{n+k+1}) = x_{n+k}$$

$$\phi_{n+k+1}(p^n v_{n+k+1} + p^{n+k+1}\mathbb{Z}) = p^n v_{n+k+1} + p^{n+k}\mathbb{Z} = p^n v_{n+k} + p^{n+k}\mathbb{Z}$$

$$\iff p^n v_{n+k+1} \equiv p^n v_{n+k} \pmod{p^{n+k}}$$

$$\iff v_{n+k+1} \equiv v_{n+k} \pmod{p^k}$$

$$\iff \phi_{k+1}(v_{n+k+1} + p^{k-1}\mathbb{Z}) = v_{n+k} + p^k\mathbb{Z}$$

$$\forall k \ge 1 \quad \phi_{k+1}(y_{k+1}) = y_k$$

$\exists$ שנוכיח כי $\ell_{p^n}(y) = x$. כלומר $\exists$ כך ש $k \le n$ מתקיים $p^n y_k = x_k$.

$k > n$ כי $p^n(v_{n+k} + p^k\mathbb{Z}) = \underbrace{p^n v_k}_{a_k} + p^k\mathbb{Z}$ $\exists$ כך ש

(כי A_k חבורה אבלית סופית).

$$p^n v_{n+k} + p^k\mathbb{Z} = p^n v_k + p^k\mathbb{Z}$$

$n < k$ לכל $v_{n+k} \equiv v_k \pmod{p^{k-n}}$

$$v_{n+k} - v_k = (v_{n+k} - v_{n+k-1}) + (v_{n+k-1} - v_{n+k-2}) + \cdots + (v_{k+1} - v_k) \in p^{k-n}\mathbb{Z}$$

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{l_{p^n}} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \longrightarrow 0$$

$$\mathbb{Z}_p / \ker \varepsilon_n \cong \mathrm{Im}(\varepsilon_n)$$

$$\mathbb{Z}_p / \mathrm{Im}(l_{p^n}) \cong A_n$$

$$\mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z} / p^n \mathbb{Z}$$

$x_1 \neq 0$ $\Leftrightarrow$ כנ"ל $x = \{x_n\}_{n=1}^{\infty} \in \mathbb{Z}_p$

$x \notin p\,\mathbb{Z}_p$ $\Leftrightarrow$ $\varepsilon_1(x) \neq 0$ $\Leftrightarrow$

"$p \nmid x$" $\Leftrightarrow$