אלגברה ב – פולינום מינימאלי

נושאים:
1. תזכורת: משפט קיילי המילטון
2. חוגים ואידיאליים
3. פולינום מינימאלי

תזכורת: משפט קיילי המילטון

- יהי V מ"ו מעל F ממימד n, יהי $T:V\to V$ אופרטור. בהינתן בסיס B_V של V, הגדרנו את הפולינום האופייני של $[T]_{B_V}$ בתור $det(\lambda I-[T]_{B_V})$.
- אם נבחר בסיס אחר C_V של V, נקבל מטריצה מייצגת אחרת $[T]_{C_V}$. ראינו כי במקרה זה יש P הפיכה המקיימת $P^{-1}[T]_{B_V}P=[T]_{C_V}$ (P היא מטריצת מעבר הבסיסים). כמו כן, אנו יודעים במקרה זה ש – $det(\lambda I-[T]_{B_V})=det(\lambda I-[T]_{C_V})$, לכן ניתן להגדיר את הפולינום האופייני של האופרטור T (בתור $det(\lambda I-[T]_{B_V})$ לבסיס כלשהו B_V של V).
- ניזכר גם, שאם $p(x)$ פולינום עם מקדמים ב – F, אזי $p(T)$ הוא אופרטור על V.
- תזכורת – פולינום $p(x)=a_n x^n+...+a_1 x+a_0$ מדרגה n נקרא מתוקן אם $a_n=1$.

<u>משפט (קיילי המילטון):</u> האופרטור T מאפס את הפולינום האופייני שלו.

- ברור כי קיימים פולינומים נוספים אותם T מאפס (חוץ מהפולינום האופייני). איך ניתן לאפיין את כל הפולינומים אותם T מאפס?

חוגים ואידיאליים

<u>הגדרה:</u> $(R,+,\cdot)$ נקרא חוג (עם יחידה) אם מקיים:
1. $(R,+)$ חבורה קומוטטיבית (ז"א יש סגירות, אסוציאטיביות, אבר אדיש לחיבור ולכל איבר יש הפיך).
2. יש סגירות לכפל (ז"א לכל $a,b\in R$ מתקיים $a\cdot b\in R$).
3. הכפל אסוציאטיבי (ז"א לכל $a,b,c\in R$ מתקיים $(a\cdot b)\cdot c=a\cdot(b\cdot c)$).
4. קיים איבר ניטראלי לכפל (ז"א יש $1\in R$ כך ש – $a\cdot 1=1\cdot a=a$ לכל $a\in R$).
5. מתקיימים חוגי פילוג וקיבוץ (ז"א $a\cdot(b+c)=a\cdot b+a\cdot c$ לכל $a,b,c\in R$).

דוגמאות:
1. כל שדה הוא בפרט חוג קומוטטיבי.
2. הקבוצה Z (המספרים השלמים), עם חיבור וכפל רגיל הוא חוג קומוטטיבי.
3. עבור שדה F, הקבוצה $F[x]$ (כל הפולינומים מכל הדרגות) עם חיבור וכפל פולינומים רגיל היא חוג קומוטטיבי.
4. $M_{nxn}(F)$ חוג (עם חיבור וכפל מטריצות).

<u>הגדרה:</u> 1. חוג R נקרא קומוטטיבי אם הכפל בו קומוטטיבי (ז"א $ab=ba$ לכל $a,b\in R$)
2. חוג R נקרא "ללא מחלקי אפס" אם לכל $a,b\in R$ מתקיים $ab=0\to a=0\vee b=0$.
3. חוג R נקרא חוג חילוק אם לכל $0\neq a\in R$ קיים $b\in R$ כך ש – $a\cdot b=b\cdot a=1$.

<u>הגדרה:</u> יהי R חוג. I < R נקרא אידיאל דו צדדי אם I מקיים:
1. לכל $a,b\in I$ מתקיים $a+b\in I$.
2. לכל $a\in I, r\in R$ מתקיים $r\cdot a\in I, a\cdot r\in I$.

<u>הגדרה:</u> יהי R חוג קומוטטיבי, $x_1,...,x_n\in R$. הקבוצה $I=\{r_1 x_1+...+r_n x_n | r_i\in R\}$ נקרא

"האידיאל הנוצר ע"י $x_{1,} \dots, x_n$". אידיאל זה מסומן $(x_{1,} \dots, x_n)$

דוגמאות:

1. ל – $n \in Z$, קבוצת כל הכפולות שלמות של n הם אידיאל (הנוצר ע"י n).
2. יהי V מ"ו מעל F ממימד n, יהי T אופרטור על V. נסמן $I_T = \{ p(x) \in F[x] \| p(T) = 0 \}$, אז I_T אידיאל ב - $F[x]$.
<u>הוכחה:</u> עבור $p_{1,} p_2 \in I_T$ *מתקיים* $(p_1 + p_2)(T) = p_1(T) + p_2(T) = 0$ *לכן* $p_1 + p_2 \in I_T$ *. כמו כן, עבור* $p \in I_T, q \in F[x]$ *מתקיים* $(qp)(T) = q(T) p(T) = 0$ *לכן* $qp \in I_T$.

<u>טענה:</u> יהי $R = F[x]$ חוג הפולינומים, I < R אידיאל שונה מאפס, אזי קיים פולינום מתוקן יחיד $d \in R$ כך ש – $I = (d)$.
<u>הוכחה:</u> I שונה מאפס, לכן קיים $p \in I$ *כלשהו. נבחר פולינום ב – I מדרגה מינימלית. ע"י כפל בסקלר, ניתן לבחור את הפולינום הנ"ל שיהיה מתוקן. נסמן פולינום זה ב – d. יהי* $f \in I$ *, מבחירת d מתקיים* $deg(f) \geq deg(d)$ *, לכן ניתן לכתוב* $f = qd + r$ *ל –* $q, r \in R$ *כך ש –* $r = 0$ *או* $deg(r) < deg(d)$ *(חלוקת הפולינום f בפולינום d). עבור q ו – r מתקיים* $qd \in I$ *ו –* $r = f - qd \in I$ *(כי I אידיאל). מההנחה ש – d מדרגה מינימלית, לא יכול להיות ש –* $deg(r) < deg(d)$ *, לכן* $r = 0$ *, ז"א* $f = qd$ *ולכן* $I = (d)$.
נניח קיים $g \in R$ *מתוקן אחר כך ש –* $(g) = I$ *, אז קיימים p,q כך ש –* $g = pd,\ d = qg$ *, לכן* $d = qpd$ *, ומתקיים* $deg(d) = deg(d) + deg(p) + deg(q)$ *לכן* $deg(p) = deg(q) = 0$ *, ז"א p,q סקלרים. כיוון שהנחנו ש – d,g מתוקנים, בפרט* $q = p = 1$.

<u>הפולינום המינימלי</u>

<u>הגדרה:</u> יהי V מ"ו מעל F, יהי T אופרטור על V. יהי $m_T \in F[x]$ הפולינום המקיים $I_T = (m_T)$, אז m_T נקרא "הפולינום המינימלי של T".

<u>הערה:</u> באופן דומה מוגדר כמובן הפולינום המינימלי של מטריצה.

<u>משפט:</u> יהי V מ"ו מעל F, יהי T אופרטור על V. לפולינום האופייני של T ולפולינום המינימלי של T יש את אותם שורשים (עד כדי ריבוי אלגברי).
<u>הוכחה</u>: נסמן את הפולינום האופייני של T כ - p_T *. נניח כי c שורש של* m_T *, אזי ניתן לרשום* $m_T = (x - c) q$ *ל-* $q \in F[x]$ *המקיים* $deg(q) < deg(m_T)$ *, לכן בהכרח* $q(T) \neq 0$ *(מהגדרת הפולינום המינימלי), ז"א קיים וקטור v כך ש –* $u = q(T) v \neq 0$ *. נקבל אם כן:* $0 = m_T(T) v = (T - cI) q(T) v = T(u) - cu$ *לכן u ו"ע של T עם ע"ע c, (לכן* $p_T(c) = 0$ *).*
מצד שני, נניח c שורש של p_T *(ז"א ערך עצמי), עם וקטור עצמי v, אזי* $m_T(T) v = m_T(c) v$ *אבל* $m_T(T) = 0$ *בעוד* $v \neq 0$ *, לכן* $m_T(c) = 0$.

<u>מסקנה:</u> יהי T אופרטור לכסין, אז הדרגה של הפולינום המינימלי של אופרטור שווה למספר ערכיו העצמיים.

<u>הערה:</u> נשים לב כי בפולינום האופייני של אופרטור על מ"ו ממשי יכול להיות גורם אי פריק מדרגה 2 (למשל $x^2 + 1$). במקרה זה גורם זה יהיה גם גורם בפולינום המינימלי. זו אינה מסקנה מיידית מהמשפט, אבל נובע ממה שלמדנו על מרכוב – ז"א הפולינום האופייני והמינימלי של המרכוב של T הוא בדיוק אותו פולינום כמו של T עצמו, ואז לאופרטור המרוכב הפולינום מתפרק לגורמים ליניארים, ונובע מהמסקנה למעלה.