הרצאה 8

תכונות של חוג הפולינומים

בהרצאה זו נניח ש- F שדה.

הגדרה 1. שני פולינומים $f(x),g(x)\in F[x]$ נקראים פרופורציונאליים (סימון, $f(x)\sim g(x)$) אם קיים $a\in F\setminus\{0\}$ כך ש-$f(x)=ag(x)$.

הגדרה 2. הפולינום $f(x)\in F[x]$ מחלק את הפולינום $g(x)\in F[x]$ (סימון, $f(x)\,|\,g(x)$) אם קיים $h(x)\in F[x]$ כך ש-$g(x)=f(x)\cdot h(x)$.

טענה 1. אם $f(x),g(x)\in F[x]$ שני פולינומים שונים מפולינום-האפס, אז $f(x)\sim g(x)\Leftrightarrow \left(f(x)\,|\,g(x)\right)\wedge\left(g(x)\,|\,f(x)\right)$.

הוכחה.

$\Rightarrow$

מהגדרת ההתחלקות נובע שקיימים $a(x),b(x)\in F[x]$ כך ש-
$f(x)=a(x)\cdot g(x), g(x)=b(x)\cdot f(x)$. מכאן נובע ש-$a(x)\cdot b(x)=1$ ולכן
$0=\deg(a(x)\cdot b(x))=\deg(a(x))+\deg(b(x))$. לפי הנתון $\deg(a(x))\geq 0,\deg(b(x))\geq 0$.
לכן $\deg(a(x))=0,\deg(b(x))=0$, כלומר $a(x)=a_0x^0, b(x)=b_0x^0$ כאשר
$a_0\neq 0, b_0\neq 0$.

$\Leftarrow$

מ-$f(x)\sim g(x)$ נובע שקיים $a\in F\setminus\{0\}$ כך ש-$f(x)=ag(x)$. אז $f(x)=ax^0\cdot g(x)$
וגם $g(x)=a^{-1}x^0\cdot f(x)$. מ.ש.ל.

טענה 2. (התחלקות עם שארית).

אם $f(x),g(x)\in F[x]$ שני פולינומים כלשהם , $g(x)\neq 0(x)$, אז קיימים שני פולינומים $q(x),r(x)\in F[x]$ כך ש :

$$\boxed{\begin{aligned} f(x)&=q(x)\cdot g(x)+r(x)\\ \deg(r(x))&<\deg(g(x))\end{aligned}\qquad (8.1)}$$

הערה: הפולינום $r(x)$ נקרא השארית והפולינום $q(x)$ נקרא המנה החלקית של החילוק $f(x)$ ב- $g(x)$.

הוכחה.

נקבע את $g(x)$ ונוכיח את הטענה באינדוקציה על $\deg(f(x))$.

בדיקה: $\deg(f(x))=-\infty$.

מהשוויון $\deg(f(x))=-\infty$ נובע ש-$f(x)=0(x)$. לכן $q(x):=0, r(x):=f(x)$ מקיימים את (8.1).

צעד האינדוקציה:

נניח שכל פולינום ממעלה $<n$ ניתן לחלק ב- $g(x)$ עם שארית. ניקח פולינום $f(x)$ ממעלה n ונוכיח שגם אותו ניתן לחלק ב- $g(x)$.

אם $\deg(f(x))<\deg(g(x))$ אז $q(x)=0, r(x)=f(x)$ מקיימים (8.1).

נניח עכשיו ש- $\deg(f(x)) \ge \deg(g(x))$. נסמן $m := \deg(g(x))$. מפני ש- $n \ge m \ge 0$, כל אחד מהפולינומים $f(x), g(x)$ ניתן לכתוב בצורה הבאה:

$$(8.2)\quad f(x) = f_n x^n + \sum_{i=0}^{n-1} f_i x^i,\; g(x) = g_m x^m + \sum_{i=0}^{m-1} g_i x^i$$

כאשר $f_n \ne 0, g_m \ne 0$. נביט בפולינום $h(x) := f(x) - \left(f_n g_m^{-1} x^{n-m}\right) \cdot g(x)$. מ-(8.2) נובע ש- $\deg(h(x)) < n$. לפי הנחת האינדוקציה קיימים $q(x) \in F[x], r(x) \in F[x]$ כך ש: $h(x) = q(x) \cdot g(x) + r(x), \deg(r(x)) < \deg(g(x))$. לכן $f(x) = \left(q(x) + \left(f_n g_m^{-1} x^{n-m}\right) \cdot g(x)\right) \cdot g(x) + r(x)$. זה מוכיח את צעד האינדוקציה, כי $\deg(r(x)) < \deg(g(x))$. מ.ש.ל.

<u>אלגוריתם של חילוק $f(x) \in F[x]$ ב- $g(x) \in F[x]$ עם שארית ($g(x) \ne 0(x)$)</u>

1. $q(x) := 0(x), r(x) := 0(x)$.
2. If $\deg(g(x)) < \deg(f(x))$, then $r(x) := f(x)$ and goto 4
3. $f(x) := f(x) - \left(f_n g_m^{-1} x^{n-m}\right) \cdot g(x); q(x) := q(x) + f_n g_m^{-1} x^{n-m}$ and goto 2.
4. Stop and print $q(x), r(x)$

<u>דוגמא 1.</u> נחלק את $x^4 + x + 1 \in \mathbf{Z}_2[x]$ ב- $x^2 + 1 \in \mathbf{Z}_2[x]$ עם שארית.

$$\begin{array}{l} x^2 + 1 \\ \hline x^4 + x + 1 \mid x^2 + 1 \\ \underline{x^4 + x^2} \\ \quad x^2 + x + 1 \\ \quad \underline{x^2 + 1} \\ \qquad x \end{array}$$

מקבלים ש- $q(x) = x^2 + 1, r(x) = x$.

טענה 3. שארית החילוק של הפולינום $f(x) \in F[x]$ בפולניום $x - a, a \in F$ שווה ל- $f(a)$.

<u>הוכחה.</u>
נחלק $f(x)$ ב- $x - a$ עם שארית: $f(x) = (x-a)q(x) + r(x)$. מהאי-שוויון $\deg(r(x)) < \deg(x-a) = 1$ נובע ש- $r(x) = r_0 x^0$. לכן $f(x) = (x-a)q(x) + r_0 x^0$. נציב a במקום x לשני הצדדים. אז נקבל $f(a) = r_0$. מ.ש.ל.

טענה 4. (משפט Bezout).
לכל פולינום $f(x) \in F[x]$ ולכל סקלר $a \in F$ התנאים הבאים שקולים:
א. a שורש של $f(x)$ (כלומר $f(a) = 0$).
ב. $f(x)$ מתחלק ב- $x - a$ ללא שארית.

הוכחה.

א' $\Leftarrow$ב'.

מטענה 3 נובע ש- $f(x)=(x-a)q(x)+f(a)x^0$. אם a שורש של $f(x)$ אז $f(a)=0$ ו $f(x)=(x-a)q(x)$.

ב' $\Leftarrow$ א'.

אם $(x-a)\,|\,f(x)$ אז קיים $q(x)\in F[x]$ כך ש- $f(x)=(x-a)q(x)$. אחרי ההצבה $x\leftarrow a$ נקבל $f(a)=0$. מ.ש.ל.

בעיה 1.

א. הוכח ש-~ יחס שקילות על הקבוצה $F[x]$.

ב. הוכח שלכל פולינום $f(x)\in F[x]$ קיים פולינום מתוקן אחד ויחיד $f_0(x)\in F[x]$ כך ש- $f_0(x)\sim f(x)$.

ג. תהי $F_0[x]$ קבוצה של כל הפולינומים המתוקנים מעל שדה F . הוכח שיחס ההתחלקות מעל $F_0[x]$ הוא יחס סדר חלקי.

בעיה 2.

הוכח שאם $g(x)\sim f(x), a(x)\sim b(x)$ אז $f(x)\,|\,b(x) \Leftrightarrow a(x)\,|\,g(x)$.

בעיה 3.

הוכח ששארית החילוק של $f(x)$ ב- $g(x)\neq 0(x)$ מוגדרת באופן יחיד.