אלגברה - שעור 3 (גשר) 15/05/03

<u>תזכורת</u>: אם $\emptyset \neq S \subset F[x]$, אז $g=\gcd(S)$ הוא הפולינום המתוקן היחיד כך ש-q מחלק את $g \iff q$ מחלק את כל איברי S $(\forall q\in F[x])$ (בפרט g מחלק את כל איברי S), וראינו שיש $s_1,\dots,s_n\in S$, $f_1,\dots,f_n\in F[x]$ כך ש: $g=f_1s_1+\dots+f_ns_n$.

אלגוריתם אוקלידס ל-$\gcd(f_1,f_2)$:

א. אם $f_2=0$ אז: $\gcd(f_1,0)=\gcd(f_1)=$ הפולינום המתוקן של f_1.

ב. נניח $f_2\neq 0$ ונחלק f_1 ב-f_2:

(*) $\deg f_3<\deg f_2$ $\quad f_1=r_1f_2+f_3$

מתקיים $\gcd(f_1,f_2)=\gcd(f_2,f_3)$

אם $f_3=0$ עוברים ל(א), ואם $f_3\neq 0$ ממשיכים,

(התהליך חייב לעצור (לאור (*)).

לגבי מספר פולינומים: $\gcd(f_1,\dots,f_n)=\gcd(\gcd(f_1,\dots,f_{n-1}),f_n)$

תאור פולינומים זרים בעזרת משוואה:

<u>הגדרה</u>: יהיו $q_1,\dots,q_k\in F[x]$ $(k\ge 2)$

$q_1,\dots,q_k$ זרים אם מתקיים התנאי הבא:

אם $q\in F[x]$ מחלק את $q_1,\dots,q_k$ אז הוא הפיך.

<u>משפט</u>: יהיו $q_1,\dots,q_k\in F[x]$, התנאים הבאים שקולים:

(א) $q_1,\dots,q_k$ זרים. (ב) $q\in F[x]$ מחלק את $q_1,\dots,q_k \iff q$ הפיך.

(ג) $g=\gcd(q_1,\dots,q_k)=1$ (ד) קיימים פולינומים $f_1,\dots,f_k$ כך ש: $1=f_1q_1+\dots+f_kq_k$.

הוכחה: (א) $\iff$ (ב) לפי הגדרה,

(ב) $\to$ (ג) כי g מתוקן ומחלק את $q_1,\dots,q_k$

(ג) $\to$ (ד) נובע מתכונות $\gcd$. (ד) $\to$ (א) ברור.

15.5.08

אלגברה לינארית 2 - שיעור 3 (המשך)

פולינומים אי-פריקים ופולינומים ראשוניים

הגדרה: יהי $p\in F[x]$ עם $\deg p\geq 1$.

① p אי-פריק אם: $p=p_1p_2$ ← p_1 הפיך (ואז p דומה ל-p_2).
p_2 " (" " " p_1).

② p ראשוני אם לכל $f,g\in F[x]$ מתקיים:
p מחלק את fg ← p מחלק את f או את g.

הערה: אם p ראשוני אז p אי-פריק, כי אם $p=p_1p_2$ אז בפרט, p מחלק את p_1p_2 ולכן p מחלק את p_1 או את p_2.
ואם למשל, p מחלק את p_1 אז p ו-p_1 דומים.

משפט: יהי $p\in F[x]$ עם $\deg p\geq 1$, אז p ראשוני אם ורק אם p אי-פריק.

הוכחה: נניח p אי-פריק (כיוון שני הוכחנו), צ"ל p ראשוני.
נניח p מחלק את fg, צ"ל p מחלק את f או את g.
אם p מחלק את f סיימנו.
נניח ש-p לא מחלק את f.
מאחר ש-p אי-פריק נובע ש-p ו-f זרים. (כי אם q מחלק את p ו-f אז q לא דומה ל-p ולכן q הפיך).
לכן יש $h,k\in F[x]$ כך ש- $1=hf+kp$.
נכפיל ב-g: $g=hfg+kpg$.
נתון ש-p מחלק את fg ← p מחלק צד ימין ← p מחלק את g.

פירוק פולינומים

משפט: יהי F שדה ו- $0\neq f\in F[x]$.
אז קיימים טבעי k ו- $n_1,\dots,n_k\geq 1$, ופולינומים אי-פריקים מתוקנים $p_1,\dots,p_k$ שונים זה מזה כך ש: $f=ap_1^{n_1}\cdots p_k^{n_k}$ כאשר $0\neq a\in F$.
והפירוק זה יחיד עד כדי סדר הגורמים ו-a= המקדם הראשי של f.

הערה: $p_1,\dots,p_k$ הם הגורמים האי-פריקים של f.

15.5.08

אלגברה לינארית 2 - שיעור 3 (עשר)

הוכחה: קיום: ההוכחה באינדוקציה על $n=\deg f$, $n=0$ ברור $(k=0)$.
אם f אי-פריק, ו-a המקדם הראשי של f, אז $f=a\cdot(\frac{f}{a})$ ו- $p_1=\frac{f}{a}$,
אי-פריק מתוקן.
אם f פריק, יש פירוק $f=f_1 f_2$ עם $\deg f_1, f_2 < \deg f$.
באינדוקציה יש פירוק ל-f_1 ופירוק ל-f_2, ומתקבל פירוק ל-f.
יחידות: $p_1,\dots,p_k$ מתוקנים $\leftarrow$ $a=$ המקדם הראשי של f.
נניח שיש שני פירוקים: $a p_1^{n_1}\cdots p_k^{n_k} = f = b q_1^{m_1}\cdots q_h^{m_h}$
(עם התכונות כמו במשפט), אז $a=b=$ מקדם ראשי של f.
q_1 מחלק את צד ימין $\leftarrow$ q_1 מחלק את צד שמאל
$\leftarrow q_1$ מחלק לפחות אחד מבין $p_1,\dots,p_k$ (כי q_1 ראשוני).
עד כדי שינוי סדר אפשר להניח ש-q_1 מחלק את p_1 ולכן $p_1=q_1$ כי
הם אי-פריקים מתוקנים. נצמצם את השוויון ונקבל: $a p_1^{n_1-1}\cdots p_k^{n_k} = b q_1^{m_1-1}\cdots q_h^{m_h}$
ולכן היחידות נובעת באינדוקציה.

ריבוי של גורם אי-פריק:

הגדרה: יהי $0\neq f\in F[x]$ ו-$p\in F[x]$ אי פריק.
אם p לא מחלק את f נסמן $v(f,p)=0$
ואם p מחלק את f נסמן $v(f,p)=\max\{n : f \text{ מחלק את } p^n\}$.
אז $v(f,p)\geq 0$ נקרא הריבוי של p ב-f.

הערות:
1. $v(f,p)=0 \iff$ p לא מחלק את f.
$v(f,p)>0 \iff$ p מחלק את f.
2. בסימוני המשפט $v(f,p_i)=n_i$ $(i=1,\dots,k)$
3. תנאי התחלקות: g מחלק את f $\iff$ $v(f,p)\geq v(g,p)$ (לכל p אי-פריק).

דוגמא: לתאר את המחלקים של $x^2(x-1)$:
$a, ax, ax^2, a(x-1), ax(x-1), ax^2(x-1)$
4. $g_1,\dots,g_n$ זרים $\iff$ ל-$g_1,\dots,g_n$ אין גורם אי-פריק משותף.

15.5.08

אלגברה לינארית 2 - שיעור 3 (המשך)

5. נניח $p=x-\lambda$, זהו פולינום אי-פריק.
נסמן $k=\nu(f, x-\lambda)$. אז יש הפירוק $f(x)=(x-\lambda)^k g(x)$ ו- $g(x)$ לא מתחלק ב- $(x-\lambda)$. לכן λ אינו שורש של g.
אם $k\geq 1$, אז k נקרא הריבוי של שורש λ של f.
בכיוון הפוך, אם $f(x)=(x-\lambda)^k g(x)$ $(k\geq 1)$ עם $g(\lambda)\neq 0$, אז k הוא הריבוי של השורש λ ב-f.
אם $k=1$ אז λ נקרא שורש פשוט של f.

פולינומים מתפצלים (מעל F)

(1) בכל שדה F: $x-\lambda$ $(\lambda\in F)$ אי-פריק ומתוקן.
וכמו כן, כל פולינום ממעלה 1 דומה לפולינום מסוג זה:

$$ax+b= a\Big(x-\underbrace{\left(\tfrac{-b}{a}\right)}_{\lambda}\Big) \qquad (a\neq 0)$$

(2) הגדרה: $0\neq f(x)\in F[x]$ מתפצל (מעל F) אם כל הגורמים האי-פריקים שלו הם ממעלה 1.
דוגמא: x^2+1 לא מתפצל מעל $\mathbb{R}$.
$x^2+1=(x-i)(x+i)$ כן מתפצל מעל $\mathbb{C}$.

(3) יהי $f(x)=a_nx^n+\dots+a_0\in F[x]$, $a_n\neq 0$, $0\leq n=\deg f$.
אז f מתפצל מעל F אם"ם הפירוק של f ב-$F[x]$ הוא מהצורה הבאה:

$$f(x)=a_n(x-\lambda_1)^{n_1}\cdots(x-\lambda_k)^{n_k}$$

כאשר $\lambda_1,\dots,\lambda_k\in F$ שונים זה מזה ו- $n_i\geq 1$ $(i=1,\dots,k)$
והפירוק זה יחיד עד כדי סדר הגורמים. במקרה זה:
(א) $\lambda_1,\dots,\lambda_k$ הם השורשים השונים של f ו- $n_i=$ הריבוי של λ_i $(\forall i)$.
(ב) משיקולי מעלה: $n_1+\dots+n_k=n=\deg f$. לכן אומרים שלפולינום מתפצל ממעלה n, יש n שורשים כולל ריבויים.
(ג) f מתפצל עם שורשים פשוטים $\Leftrightarrow$ $f=a_n(x-\lambda_1)\cdots(x-\lambda_n)$, $\lambda_1,\dots,\lambda_n$ שונים זה מזה.

15.5.08

אלגברה לינארית 2 - שיעור 3

$\mathbb{C}$: יש משפט האומר שכל פולינום ב-$\mathbb{C}[x]$ ממעלה ≥ 1, יש שורש.
אם נסמן שורש זה ב-λ, אז הפולינום מתחלק ב-$(x-\lambda)$.
מסקנה: רשימת כל הפולינומים האי-פריקים המתוקנים ב-$\mathbb{C}[x]$ היא: $\{x-\lambda : \lambda \in \mathbb{C}\}$.
מסקנה: כל פולינום $\neq 0$ ב-$\mathbb{C}[x]$ מתפרק.

$\mathbb{R}[x]$:

(א) אם $f(x)=a_nx^n+\dots+a_1x+a_0 \in \mathbb{R}[x]$ (כלומר $a_0,\dots,a_n$ ממשיים)
ואם $\lambda \in \mathbb{C}$ (λ ממשי או מרוכב) שורש של f, אזי $\bar{\lambda}$ שורש של f כי:
$$0=a_n\lambda^n+\dots+a_1\lambda+a_0=a_n\bar{\lambda}^n \dots + a_1\bar{\lambda}+a_0$$

(ב) **מסקנה:** אם $f(x)\in\mathbb{R}[x]$ ו- $\deg f \geq 3$ אז f פריק.
הוכחה: יש ל-f שורש $\lambda\in\mathbb{C}$, ולכן יש פירוק $f(x)=(x-\lambda)g(x)$ (ב-$\mathbb{C}[x]$).
g היא תוצאת החילוק של f ב-$(x-\lambda)$.
אם λ ממשי, אז נובע מאלגוריתם החילוק שגם g ממשי, ולכן $f(x)=(x-\lambda)g(x)$ הוא פירוק מעל $\mathbb{R}$, ($1\leq \deg g$) ולכן f פריק ב-$\mathbb{R}[x]$.
נניח ש-λ אינו ממשי, אז $\lambda\neq\bar{\lambda}$, ו-$\bar{\lambda}$ שורש של f. לכן $\bar{\lambda}$ שורש של g. מכאן נובע שיש פירוק $g(x)=(x-\bar{\lambda})h(x)$ ב-$\mathbb{C}[x]$ (ובחלוקה).
קיבלנו:
$$f(x)=(x-\lambda)g(x)=(x-\lambda)(x-\bar{\lambda})h(x)=$$
$$=(x^2-(\lambda+\bar{\lambda})x+|\lambda|^2)h(x)$$
אם נסמן $\lambda=\alpha+i\beta$ (α,β ממשיים) אז $\bar{\lambda}=\alpha-i\beta$
$\lambda+\bar{\lambda}=2\alpha$, $|\lambda|^2=\alpha^2+\beta^2$: $x^2-(\lambda+\bar{\lambda})x+|\lambda|^2=\underbrace{x^2-2\alpha x+(\alpha^2+\beta^2)}$. פולינום ממשי.
לכן, h גם ממשי (כי $h=$ תוצאת החילוק של f ב-).
וקיבלנו פירוק של f ב-$\mathbb{R}[x]$ עם שני גורמים ממעלה ≥ 1.

(ג) רשימת הפולינומים האי-פריקים המתוקנים ב-$\mathbb{R}[x]$ היא: $x-\lambda$, λ ממשי.
x^2+bx+c ללא שורשים ממשיים, כלומר עם התנאי $b^2-4c<0$.
לפולינום מסוג זה יש שני שורשים מרוכבים $\lambda,\bar{\lambda}\in\mathbb{C}-\mathbb{R}$.
ומתקיים $x^2+bx+c=(x-\lambda)(x-\bar{\lambda})=x^2-(\lambda+\bar{\lambda})x+|\lambda|^2$
ונוכל להציג לפי זה את b ו-c.