פולינומים
צחי אבנור

Zachi Evenor
Email: z-evenor@lycos.com
Home Page: http://www.tau.ac.il/~bahatgal

פולינומים (סוכם ע"י צחי אבנור ; מרצה: פרופ' אשר בן-ארצי)

1. הגדרות ומושגי יסוד

הגדרה: פולינום מעל שדה F הוא ביטוי $p(x)=a_0+a_1x+a_2x^2+...+a_nx^n$ כך ש $\forall i.a_i\in F$.

הגדרה: פולינום האפס $0(x)=0+0\cdot x+0\cdot x^2+...=0$.

הגדרה: מעלה/דרגה של פולינום היא $\deg p(x)=\max\{n\mid a_n\neq 0\}$. כמו כן $\deg 0(x)=-\infty$.

הגדרה: פולינום קבוע $p(x)=c+0\cdot x+0\cdot x^2+...=c$ כאשר $c\neq 0$ ו $\deg c=0$.

2. חוג הפולינומים

הגדרה: תהי R קבוצה שמעליה פעולות "חיבור" ו"כפל". כדי ש R תיקרא חוג Ring נדרוש שהיא תקיים את התכונות הבאות, לכל $p,q,r\in R$: (1) היא חבורה קומוטטיבית ביחס לחיבור (כלומר, היא מקיימת את $p+0=0$, $p+(-p)=0$, $(p+q)+r=p+(q+r)$, $p+q=q+p$). (2) $p\cdot 1=p$ (כאשר 1 הוא הפולינום הקבוע 1). (3) $(pq)r=p(qr)$. (4) $pq=qp$. (5) פילוגיות: $p(q+r)=pq+pr$.

משפט: קבוצת כל הפולינומים מעל שדה כלשהו F מהווה "חוג" ונקראת "חוג הפולינומים" ותסומן $F[x]$.

משפט: קבוצת הפולינומים $\{1,x,x^2,...,x^n\}$ היא בלתי תלויה ליניארית.

משפט: לכל $p(x),q(x)\in F[x]$: (1) $\deg(p+q)\le\max\{\deg p,\deg q\}$. (2) $\deg(pq)=\deg p+\deg q$.

מסקנה: אם $p\neq 0$, $q\neq 0$ אזי $pq\neq 0$. לחוג המקיים תכונה זו קוראים "חוג שלמות".

כלל הצמצום: אם $pq=pr$ ו $p\neq 0$ אזי $q=r$.

הוכחה: $pq=pr\Leftrightarrow p(q-r)=0$ ומאחר ש $p\neq 0$ לפי מסקנה קודמת $q-r=0$ ולכן $q=r$. ∎

הגדרה: פולינום p נקרא הפיך אם קיים $q\in F[x]$ כך ש $pq=1$ (כלומר, $p(x)q(x)=1(x)$).

משפט: פולינום הפיך אם ורק אם הוא פולינום קבוע (השונה מאפס), כלומר $\deg p=0\Leftrightarrow p(x)=c\neq 0\Leftrightarrow$.

טענה: יהי $p\neq 0$. אזי $\deg(pq)<\deg p\Leftrightarrow q=0$ וכן $\deg(pq)=\deg p$ $\Leftrightarrow\deg q=0$.

3. חילוק פולינומים, פולינומים מתוקנים ושקילות של פולינומים

שיטה לחשב מנת פולינומים: באמצעות חילוק ארוך.

משפט החלוקה: יהיו $f,g\in F[x]$ פולינומים, אז קיימים זוג פולינומים יחיד: $r\in F[x]$ שארית $s\in F[x]$ מנה כך שמתקיים: $f=g\cdot s+r$. יתרה מזו, בהכרח מתקיים הקשר הבא: $\deg r<\deg g$ (דרגת השארית קטנה מדרגת המחלק).

הוכחה: הקיום נובע מאלגוריתם החילוק הארוך. נוכיח יחידות: נניח בשלילה שקיימים $s',r'\in F[x]$ כך ש $f=g\cdot s'+r'$ ו $\deg r'<\deg g$. אזי $gs+r=gs'+r'\Rightarrow g(s-s')=r'-r$. אם $g=0$ אזי יש יחידות כאשר $r=f=r'$. לכן, נניח $g\neq 0$ ואז, מאחר ש $\deg(r'-r)<\deg g\le\deg(q(s-s'))$ לפי טענה אחרונה בסעיף 2 $s-s'=0$ ולכן גם $r'-r=0$ ובסה"כ $s=s'$, $r=r'$ ויש יחידות. ∎

הגדרה: יהיו $f,g\in F[x]$ פולינומים, נאמר ש g מחלק את f ונסמן $g\mid f$ (או $\frac{f}{g}$) אם קיים פולינום $s\in F[x]$ כך ש $f=g\cdot s$. ל s נקרא המנה של חלוקת f ב g.

תכונות: (1) 0 מחלק רק את 0. (2) כל פולינום מחלק את 0. (3) כל פולינום הפיך מחלק כל פולינום ובפרט 1 מחלק כל פולינום. (4) פולינום מחלק את 1 אם ורק אם הוא הפיך.

קשר עם חילוק: g מחלק את f אם ורק אם השארית בביצוע החלוקה של f ב g היא 0.

משפט: אם $g \mid f_k$, ... , $g \mid f_2$, $g \mid f_1$ אזי לכל $h_1, h_2, ..., h_k \in F[x]$ מתקיים $g \mid \sum_{i=1}^{k} h_i f_i$.

טענה: אם $g \mid f$ ו $f \mid p$ אזי $g \mid p$.

הגדרה: יהיו $f, g \in F[x]$ פולינומים, נאמר ש f ו g שקולים אם $g \mid f$ וגם $f \mid g$.

מסקנה: אם f ו g שקולים אזי $f = c \cdot g$ כאשר c פולינום קבוע שונה מאפס.

הגדרה: יהי $f \in F[x]$ פולינום. אם $f(x) = 0$ או אם $f(x) \neq 0$ וגם המקדם הראשי שלו שווה ל 1 (כלומר: $a_{\deg f} = 1$) אזי נאמר שהפולינום f הוא פולינום מתוקן.

תכונות: (1) כל פולינום f שקול לפולינום מתוקן יחיד שיקרא "הפולינום המתוקן של f". (2) אם f ו g שקולים ומתוקנים, אזי f=g.

הגדרה: יהיו $q_1, q_2 \in F[x]$ פולינומים. נאמר שהם זרים אם כל פולינום p שמחלק את שניהם (כלומר, הוא מקיים $p \mid q_1 \wedge p \mid q_2$) הוא בהכרח הפיך (הווה אומר $\deg p = 0$).

4. הצבות ושורשים

הגדרה: יהי F שדה ויהי $p(x) = a_0 + a_1 x + ... + a_n x^n$ פולינום. לכל $\gamma \in F$ נתאים איבר ב F ע"י $p(\gamma) = a_0 + a_1 \gamma + ... + a_n \gamma^n$ ו $p(\gamma)$ נקרא תוצאת הצבה $x = \gamma$ ב p.

טענה: עבור פולינום האפס, $\forall \gamma \in F. 0(\gamma) = 0$. עבור פולינום קבוע, $\forall \gamma \in F. c(\gamma) = c$.

משפט: ההצבה שומרת על הפעולות. (1) $(p+q)(\gamma) = p(\gamma) + q(\gamma)$. (2) $(pq)(\gamma) = p(\gamma)q(\gamma)$.

הגדרה: $\gamma \in F$ יקרא שורש של $p(x) \in F[x]$ אם $p(\gamma) = 0$.

משפט – קשר בין שורשים ויחס חלוקה: יהי $p(x)$ פולינום. γ שורש של p אם ורק אם $(x-\gamma)$ מחלק את p. הווה אומר: $p(\gamma) = 0 \Leftrightarrow (x-\gamma) \mid p(x)$.

הוכחה: ($\Leftarrow$) נניח ש γ שורש של p. אזי, ממשפט החלוקה קיימים s, r כך ש $p(x) = (x-\gamma)s(x) + r(x)$. כעת, נציב את γ ונקבל: $p(\gamma) = 0 = (\gamma - \gamma)s + r$ ומכאן $r = 0$ ולכן $(x-\gamma) \mid p$. ($\Rightarrow$) נניח ש p, $(x-\gamma) \mid p$ ואז $p(x) = (x-\gamma)s(x)$ וברור מכאן ש $p(\gamma) = 0$. ∎

מסקנה: לכל $p(x) \in F[x]$, $\gamma \in F$ מתקיים השוויון הבא: $p(x) = (x-\gamma)s(x) + p(\gamma)$.

5. המחלק המשותף הגדול ביותר

האלגוריתם האוקלידי
GCD

$f_0 = g_1 f_1 + f_2$
$f_1 = g_2 f_2 + f_3$
$f_2 = g_3 f_3 + f_4$
⋮ ⋮ ⋮
$f_{k-3} = g_{k-2} f_{k-2} + f_{k-1}$
$f_{k-2} = g_{k-1} f_{k-1} + f_k$
$f_{k-1} = g_k \cdot \boxed{f_k} + 0$

האלגוריתם של אוקלידס: יהיו f_0, f_1 פולינומים. כדי למצוא את המחלק המשותף הגדול ביותר gcd נרשום את השוויונות הבאים (מימין). נחלק את f_0 ב f_1 ונרשום את השארית והמנה. אז נחלק את המחלק f_1 בשארית הקודמת f_2 ונרשום את השארית והמנה. ושוב, נחלק את המחלק (הפעם זו השארית הקודמת-קודמת) f_2 בשארית של השלב השני f_3 וכו.

התהליך ייעצר כאשר נקבל שארית 0 ואז ה gcd הוא המחלק שגרם להתאפסות השארית.

בהתאם לסימונים שבתרשים שמימין, $\gcd(f_0, f_1) = f_k$.

תכונות ה gcd: נסמן $f_k = \gcd(f_0, f_1)$. אזי: (1) כל פולינום שמחלק את f_0 וגם את f_1 מחלק את f_k. (2) טריוויאלי אבל $f_k \mid f_1 \wedge f_k \mid f_0$. (3) קיימים $h_0, h_1 \in F[x]$ כך ש $h_0 f_0 + h_1 f_1 = f_k$.

משפט קיום ויחידות ה gcd: יהיו f_0, f_1 פולינומים. אזי קיים פולינום מתוקן יחיד f המקיים את התכונות הבאות: (1) הפולינום f מחלק את f_0, f_1, כלומר: $f \mid f_1 \wedge f \mid f_0$. (2) כל פולינום שמחלק את f_0 וגם את f_1 מחלק את f. (3) קיימים $h_0, h_1 \in F[x]$ כך ש $h_0 f_0 + h_1 f_1 = f_k$. אזי נסמן אותו $f = \gcd(f_0, f_1)$.
הוכחה: אם אחד מהם שונה מאפס הקיום נובע מהאלגוריתם האוקלידי, ובייחוד תכונה 3. אם שניהם אפס אזי פולינום האפס מקיים עבורם את תכונות 1-3. נוכיח יחידות: נניח שקיים $f' \in F[x]$ מתוקן המקיים את תכונות 1-3. הוא מקיים את תכונה 1 ולכן $f' \mid f$, כמו כן, מתכונה 2 $f \mid f'$ וכאן שהם שקולים. מאחר שהם שקולים ומתוקנים נובע ש $f = f'$. ∎

משפט – קריטריונים לפולינומים זרים: יהיו f_0, f_1 פולינומים. אזי התנאים הבאים שקולים:
(1) הפולינומים f_0 ו f_1 זרים. (2) $\gcd(f_0, f_1) = 1$. (3) קיימים $h_0, h_1 \in F[x]$ כך ש $h_0 f_0 + h_1 f_1 = 1$.
הוכחה: (1) $\Leftarrow$ (2) מכך שהם זרים, כל פולינום שמחלק את שניהם בהכרח הפיך ובפרט ה gcd הפיך ובגלל שהוא מתוקן הוא שווה ל 1. (2) $\Leftarrow$ (3) נובע מהמשפט הקודם. (3) $\Leftarrow$ (1) נניח ש $\exists h_0, h_1 \in F[x]$ כך ש $h_0 f_0 + h_1 f_1 = 1$. אזי כל פולינומים שמחלק את f_0 ו f_1 בהכרח מחלק את 1 ולכן הפיך. מכאן הזרות. ∎

6. פירוק פולינומים

הגדרה: יהי $p \in F[x]$ פולינום כך ש $\deg p \geq 1$. אזי רק אחת מבין שתי האפשרויות הבאות מתקיימת:
(1) קיים פירוק לא-טריוויאלי $p = p_1 p_2$ כך ש $1 \leq \deg p_1, \deg p_2 < \deg p$ ואז נמר ש p פריק.
(2) לא קיים פירוק לא-טריוויאלי. כלומר, בכל פירוק אחד הפולינומים הפיך והשני שקול ל p. במקרה זה אומרים ש p הוא אי-פריק irreducible.
משפט: (1) אם $\deg p = 1$ אזי הוא בהכרח אי-פריק. (2) אם $\deg p = 2$ או $\deg p = 3$ אזי p אי-פריק אם ורק אם אין לו שורשים מעל F. (3) אם $\deg p \geq 2$ ויש ל p שורש ב F אזי הוא פריק.
טענה I – קיום פירוק לפולינומים אי-פריקים: יהי $p \in F[x]$ פולינום כך ש $\deg p \geq 1$. אזי קיים פירוק מהצורה $p = c \cdot q_1 ... q_k$ כך ש $q_1, ..., q_k$ אי-פריקים מתוקנים ו c פולינום הפיך (קבוע).
הוכחה: באינדוקציה. עבור פולינום ממעלה 1 זה נכון באופן טריוויאלי כי הוא אי-פריק. נניח שזה נכון עבור פולינומים ממעלה n-1 ונוכיח עבור n. אם p ממעלה n אי-פריק אז סיימנו, אחרת, קיים פירוק לא-טריוויאלי $p = p_1 p_2$ כך ש $1 \leq \deg p_1, \deg p_2 < \deg p$ ולפי הנחת האינדוקציה ל p_1, p_2 קיימים פירוקים לפולינומים אי-פריקים $p_1 = c_1 q_1 ... q_t$, $p_2 = c_2 q_{t+1} ... q_k$ ולכן $p = (c_1 c_2) q_1 ... q_t q_{t+1} ... q_k$ כנדרש. ∎
הגדרה: פולינום $p \in F[x]$ נקרא ראשוני אם p איננו הפיך ומתקיים התנאי הבא: לכל זוג פולינומים $f, g \in F[x]$, אם $p \mid fg$ אזי או ש $p \mid f$ או ש $p \mid g$ (כלומר, הוא מחלק לפחות אחד מהם).
מסקנה: אם p ראשוני ו $p \mid f_1 ... f_k$ אזי קיים $1 \leq i \leq k$ כך ש $p \mid f_i$.
משפט: אם $p \neq 0$ ו p ראשוני, אזי p אי-פריק.
הוכחה: מאחר ש p ראשוני שונה מאפס, $\deg p \geq 1$ ולכן קיים פירוק $p = q_1 q_2$ כאשר $\deg q_1, q_2 \leq \deg p$. נראה שהפירוק בהכרח טריוויאלי. $p \mid q_1 q_2$ (כי הוא ראשוני) ולכן בהכרח $p \mid q_1$ או $p \mid q_2$. ב.ה.כ נניח $p \mid q_1$ וכמו כן ברור ש $q_1 \mid p$. לכן הם שקולים ומכאן $\deg q_1 = \deg p$ ומתכונות הכפל $\deg q_2 = 1$, כלומר, הוא פולינום הפיך. מכאן, לפי ההגדרה, p אי-פריק. ∎
טענה II – יחידות הפירוק לגורמים ראשוניים: אם לפולינום $f(x) \neq 0$ יש שני פירוקים $f = c \cdot p_1 ... p_k$ ו $f = c' \cdot q_1 ... q_{k'}$ כאשר $c, c' \in F$ ו $p_1, ..., p_k, q_1, ..., q_{k'}$ אזי $k = k'$, $c = c'$ והסדרות $q_1, ..., q_k$ $p_1, ..., p_k$ זהות עד כדי סדר. במילים אחרות: יש תמורה בה $\forall i = 1, ..., k \,.\, p_i = q_i$.

הוכחה: נניח את שני הפירוקים הנ"ל. $c=c'$ ברור, כי זה קובע את המקדם הראשי של f. כעת, $q_i \mid f$ ולכן $q_j \mid p_1 \cdots p_k$ ומאחר ש q_i ראשוני, בהכרח קיים $1 \le j \le k$ כך ש $q_i \mid p_j$. מאחר ש $p_j \neq 0$ ראשוני הוא אי-פריק ולכן שקול ל q_i, מכך שהם מתוקנים נובע השוויון $q_i = p_j$. באותו אופן (אפשר באינדוקציה ממשיכים עבור כל ה q-ים וה p-ים וכך מסיקים על שוויון בין איברי הסדרות ועל כך ש $k=k'$ (כי מצאנו התאמה חח"ע ועל בין שתי הסדרות). בכך הוכחנו את יחידות הפירוק. ■

טענה III – שקילות בין ראשוניות לאי-פריקות: יהי $0 \neq p(x) \in F[x]$ פולינום שונה מאפס (כלומר, $\deg p \ge 1$). אזי p ראשוני אם ורק אם p אי-פריק.

הוכחה: ($\Leftarrow$) כבר הוכחנו (לפני טענה II). ($\Rightarrow$) נניח ש p אי-פריק ונוכיח שהוא ראשוני. כלומר, יהיו $f,g \in F[x]$, ונראה שאם $p \mid fg$ אזי או ש $p \mid f$ או ש $p \mid g$. אם $p \mid f$ המשפט נכון, לכן נניח ש $p \nmid f$ ונראה ש $p \mid g$. יהי $q = \gcd(f,p)$, מאחר ש q מחלק את p ו p אי-פריק נובע ש q שקול ל p או ש q הפיך (כי הפירוק $p = qq'$ טריוויאלי). אם $q = p$ אזי היינו מחלקים ש $p \mid f$ בסתירה להנחה ומכאן בהכרח ש q הפיך ולכן $q = \gcd(f,p) = 1$. מכך ש $1 = h_1 f + h_2 p$ כך ש $h_1, h_2 \in F[x]$. נכפיל ב g ונקבל $h_1(fg) + (h_2 g)p = g$ ומאחר ש $p \mid p$ ו $p \mid fg$ נובע ש $p \mid g$. כלומר $p \mid h_1(fg) + (h_2 g)p = g$, מכאן ש p ראשוני. ■

משפט הפירוק (מסקנה מטענות I, II ו III): יהי $0 \neq f(x) \in F[x]$ פולינום שונה מאפס. אזי קיים פירוק יחיד $f(x) = c \cdot p_1(x) \cdot \ldots \cdot p_k(x)$ כך ש $c \in F$ ו $p_1, \ldots, p_k$ פולינומים אי-פריקים (כלומר, ראשוניים) מתוקנים. כל פירוק אחר יכול להיבדל מהפירוק הנ"ל רק בסדר האיברים. הפירוק הזה, שהמשפט מבטיח את קיומו ואת יחידותו, נקרא "פירוק של f למרכיבים אי-פריקים" או "פירוק לגורמים ראשוניים".

7. פירוק פרימרי

הגדרה: בפירוק של סעיף 6 יתכן שיהיו פולינומים ראשוניים שחוזרים על עצמם, כלומר $p_i = p_j$. במקרה זה, פשוט נקבץ אותם לגורם אחד, כאשר כל גורם שחוזר על עצמו יתרום 1+ לחזקה. נקבל פירוק מהצורה הבאה: $f(x) = c \cdot \left(p_1(x)\right)^{R_1} \cdot \ldots \cdot \left(p_m(x)\right)^{R_m}$ כאשר $c \in F$ ו $p_1, \ldots, p_k$ פולינומים אי-פריקים (כלומר, ראשוניים) מתוקנים ו $\forall 1 \le i \le m.\ R_i \ge 1$. הפירוק הנ"ל יקרא הפירוק הפרימרי של f.

משפט: g מחלק את f אם ורק אם כל גורם ראשוני של g הוא גם גורם ראשוני של f וכמו כן, החזקה שלו ב g קטנה או שווה מהחזקה שלו ב f. כלומר: $g = c' \cdot p_1^{\mu_1} \cdot \ldots \cdot p_k^{\mu_k}$ כאשר $\forall i.\ 0 \le \mu_i \le R_i$.

משפט: יהיו $f(x), g(x) \in F[x]$ פולינומים, אזי $\gcd(f,g) = \prod_{p_i \in f \cap g} p_i^{\min\{R_i^{(f)}, R_i^{(g)}\}}$.

משפט: פולינומים f ו g זרים אם ורק אם אין להם מחלקים ראשוניים משותפים.

מסקנה: אם $h_1 \mid f$ .... $h_l \mid f$ ו h_i זרים בזוגות אזי $h_1 \cdots h_l \mid f$.

7. ריבוי של שורש ופולינומים מתפצלים

הגדרה: יהי $0 \neq f(x) \in F[x]$ פולינום ויהי $\lambda \in F$ שורש שלו. אזי $(x-\lambda) \mid f$ וכמו כן הפולינום $x-\lambda$ הוא אי-פריק ולכן מחלק ראשוני של f. החזקה של המחלק הראשוני $x-\lambda$ נקראת הריבוי של השורש $x=\lambda$. הריבוי של כל שורש הוא לפחות 1.

משפט: R הוא הריבוי של השורש λ אם ורק אם $(x-\lambda)^R \mid f \wedge (x-\lambda)^{R+1} \nmid f$.

מינוח: שורש שהריבוי שלו 1 נקרא שורש פשוט.

משפט: כל פולינום (פריק) $f(x)$ שמעלתו n , $\deg f = n$, שיש לו שורשים ניתן לפירוק כך:
$f(x) = c \cdot (x-\lambda_1)^{R_1} \cdot \ldots \cdot (x-\lambda_t)^{R_t} \cdot q_{t+1}^{R_{t+1}} \cdot \ldots \cdot q_k^{R_k}$ כאשר $\lambda_1,\ldots,\lambda_t \in F$ הם שורשי הפולינום מעל F ו $q_{t+1},\ldots,q_k$ הם פולינומים ראשוניים אי-פריקים שמעלתם גדולה ממש מ 1 ואין להם שורש.

מסקנות: (1) $n = \deg f \geq \sum_{i=1}^{t} R_i$. (2) לפולינום שונה מאפס ממעלה n יש לכל היותר n שורשים שונים.

הגדרה: פולינום שהפירוק הפרימרי שלו הוא מהצורה $f(x) = c(x-\lambda_1)^{R_1} \cdot \ldots \cdot (x-\lambda_k)^{R_k}$ יקרא פולינום מתפצל ו $\lambda_1,\ldots,\lambda_k \in F$ הם שורשי הפולינום.

משפט: פולינום f מתפצל אם ורק אם סכום ריבויי השורשים שווה לדרגתו, כלומר: $\sum_{i=1}^{k} R_i = \deg f$.

הוכחה: ($\Leftarrow$) ברור. ($\Rightarrow$) ברור שאת f ניתן להציג כך: $f(x) = q(x)\prod_{i=1}^{k}(x-\lambda_i)^{R_i}$, אבל מאחר ש $\deg\prod_{i=1}^{k}(x-\lambda_i)^{R_i} = \sum_{i=1}^{k}\deg(x-\lambda_i)^{R_i} = \sum_{i=1}^{k} R_i = \deg f$ נובע בהכרח ש $\deg q = 0$ ולכן הוא הפיך. ∎

הגדרה: נאמר ש f מתפצל עם שורשים פשוטים (או מתפצל פשוט) אם ורק אם f ניתן להצגה כך:
$f(x) = (x-\lambda_1)(x-\lambda_2)\ldots(x-\lambda_n)$ כאשר $\deg f = n$ (כלומר, ל f יש n שורשים שונים).
הערה: עניין הפיצול תלוי בשדה.

8. פירוק מעל שדה המרוכבים ומשפט הסגירות האלגברית

משפט הסגירות האלגברית: השדה $\mathbb{C}$ סגור אלגברית, כלומר: לכל פולינום $p(z)$ ממעלה ≥ 1 יש לפחות שורש מרוכב אחד.

למה: יהי $p(z) = 1 + a_1 z + \ldots + a_n z^n$ כך ש $\deg p \geq 1$ ונוכיח שהפונקציה $|p(z)|$ $\lambda z \in \mathbb{C}$. אינה מקבלת מינימום.

הוכחה: ראשית $|p(0)| = 1$. כעת, יהי a_k האיבר הראשון ששונה מאפס, אזי $p(z) = 1 + a_k z^k + \ldots + a_n z^n$

ויהי $\gamma \in \mathbb{C}$ כך ש $\gamma^k = \frac{-1}{a_k}$. נראה שקיים $0 < t < 1$ כך ש $|p(0)| = 1 > |p(t\gamma)|$. ואכן, אם $0 < t < 1$ אזי

$$|p(t\gamma)| \leq |1 + a_k t^k \gamma^k| + |a_{k+1}(t\gamma)^{k+1}| + \ldots + |a_n(t\gamma)^n| \leq |1 - t^k| + \left(\sum_{j=k+1}^{n} |a_j \gamma^j|\right) t^{k+1} = |1 - t^k| + Mt^{k+1}$$

כאשר $M = \sum_{j=k+1}^{n} |a_j \gamma^j|$. מאחר ש $1 - t^k > 0$ אפשר לוותר על הערך המוחלט ונקבל:

$|p(t\gamma)| = 1 - t^k + Mt^{k+1} = 1 - t^k(1 - tM) < 1$ כנדרש. כלומר, ב $z = 0$ אין מינימום. ∎

מסקנה 1: אם $p(z) = a_0 + a_1 z + \ldots + a_n z^n$ ואם הפונקציה $|p(z)|$ $\lambda z \in \mathbb{C}$. מקבלת את המינימום ב $z = 0$ אזי חייב להתקיים $a_0 = 0$ ומכאן $z = 0$ הוא שורש של p והמינימום הוא אפס.

הוכחה: אם $a_0 \neq 0$ נתקן את p (נכפול את כולו ב a_0^{-1}) ואז נקבל סתירה ללמה. ∎

מסקנה 2: ע"י ההזזה $z \to z + z_0$ מקבלים: אם $p(z)$ פולינום מעל $\mathbb{C}$ ו $1 \leq \deg p$ ואם $|p(z)|$ $\lambda z \in \mathbb{C}$. מקבלת את המינימום בנקודה z_0 אזי z_0 שורש של p.

הוכחת משפט הסגירות האלגברית: יהי $p(z)=a_0+a_1z+...+a_nz^n$ כך ש $1\le \deg p$. נשים לב שלכל $z\neq 0$ מתקיים $p(z)=\left(a_n+\frac{a_{n-1}}{z}+...+\frac{a_0}{z^n}\right)z^n$. לכן, אם $\{z_n\}_{n=1}^{\infty}$ סדרת מספרים מרוכבים כך ש $\lim_{n\to\infty}|z_n|=\infty$ מתקיים גם $\lim_{n\to\infty}|p(z_n)|=\infty$. כעת נסמן $\mu=\inf_{z\in\mathbb{C}}|p(z)|$. אזי יש סדרה $\{z_n\}_{n=1}^{\infty}$ כך ש $\lim_{n\to\infty}|p(z_n)|=\mu$. כמו כן, ברור שהיא חסומה ולכן לפי משפט בולצאנו-ויירשטרס קיימת תת-סדרה $\{z_{n_k}\}_{k=1}^{\infty}$ שמתכנסת למספר מרוכב ב $\mathbb{C}$, כלומר $\lim_{k\to\infty}z_{n_k}=z_0$. מאחר שפולינום היא פונקציה רציפה מתקיים $\mu=\lim_{n\to\infty}|p(z_n)|=|p(z_0)|$ ומכאן שהמינימום מתקבל ב z_0 ולפי מסקנה 2, $z_0\in\mathbb{C}$ הוא שורש של הפולינום. בכך הוכחנו את משפט הסגירות האלגברית. ■

משפט: הפולינום האי-פריקים מעל $\mathbb{C}$ הם כל (ורק) הפולינומים מהצורה $x-\lambda$ כך ש $\lambda\in\mathbb{C}$.

מסקנה: כל פולינום מתפצל מעל $\mathbb{C}$. כלומר, מעל $\mathbb{C}$ תמיד קיימת ההצגה $f(x)=c(x-\lambda_1)^{R_1}\cdot...\cdot(x-\lambda_k)^{R_k}$.

הגדרה: הצמדת פולינום $f(x)=\sum_{i=0}^{n}a_ix^i$ היא הפעולה הבאה: $\overline{f}(x)=\sum_{i=0}^{n}\overline{a}_ix^i$.

תכונות: (1) $\overline{f+g}=\overline{f}+\overline{g}$ (2) $\overline{f\cdot g}=\overline{f}\cdot\overline{g}$ (3) $\overline{f(\lambda)}=\overline{f}(\overline{\lambda})$.

משפט: $\lambda\in\mathbb{C}$ שורש של f אם ורק אם $\overline{\lambda}\in\mathbb{C}$ שורש של $\overline{f}$, ובמקרה זה – הריבוי שלהם זהה.

9. פירוק מעל שדה הממשיים (נניח שכל המקדמים הם ממשיים)

משפט (מציאת שורשים רציונליים): יהי $f(x)=a_0+a_1x+...+a_nx^n$ פולינום עם מקדמים שלמים. כעת נניח ש $\frac{p}{q}\in\mathbb{Q}$ כאשר p ו q זרים הוא שורש של f. אזי $q\mid a_n$ ו $p\mid a_0$, כלומר $\frac{a_n}{q},\frac{a_0}{p}\in\mathbb{Z}$.

הוכחה: נציב $x=p/q$. אזי $0=a_0+a_1\left(\frac{p}{q}\right)+...+a_n\left(\frac{p}{q}\right)^n$, נכפיל ב q^n ונקבל $0=a_0q^n+a_1pq^{n-1}+a_2p^2q^{n-2}+...+a_np^n$ ולכן $a_0q^n=p\cdot(-a_1q^{n-1}-a_2pq^{n-2}-...-a_np^{n-1})$. מאחר ש p מחלק את אגף ימין הוא מחלק גם את אגף שמאל ומאחר ש p ו q זרים, בהכרח $p\mid a_0$. באותו אופן, $p^na_n=q(-a_0q^n-...-a_{n-1}qp^{n-1})$ ולכן $q\mid a_n$. ■

מסקנה: אם $f(x)=a_0+a_1x+...+x^n$ פולינום מתוקן, אזי כל שורש רציונלי שלו הוא מספר שלם המתחלק במקדם החופשי a_0. באמצעות שיטה זו אפשר לנחש שורשים של הפולינום. אחרי שניחשנו שורש יש להציב אותו ולוודא שהוא אכן שורש של הפולינום.

משפט: יהא $f(x)\in\mathbb{R}[x]$ פולינום שכל מקדמים ממשיים. אזי אם $\lambda\in\mathbb{C}$ שורש, גם $\overline{\lambda}$ שורש.

מסקנה 1: ל $f(x)$ יש מספר זוגי של שורשים מרוכבים שאינם ממשיים ($z=a+bi\mid b\neq 0$).

מסקנה 2: לפולינום ממשי ממעלה אי-זוגית יש לפחות שורש ממשי אחד.

משפט: יהא $f\in\mathbb{R}[x]$ פולינום שכל מקדמיו ממשיים, אזי $\overline{f}(x)=f(x)$.

מסקנה: אם $\lambda=a+bi$ כך ש $b\neq 0$ שורש של f אזי גם $\overline{\lambda}=a-bi$ שורש של f באותו ריבוי.

משפט: כל המקדמים של f ממשיים אם ורק אם ניתן לפרקו כך:

$f(x)=\left(\prod_{i=1}^{s}(x-\mu_i)^{R_i}\right)\left(\prod_{j=s+1}^{t}(x-\lambda_j)^{R_j}(x-\overline{\lambda}_j)^{R_j}\right)$ כאשר $\mu_1,...,\mu_s\in\mathbb{R}$ שונים זה מזה ו $\lambda_{s+1},...,\lambda_t\in\mathbb{C}-\mathbb{R}$ שונים זה מזה ושונים מ $\overline{\lambda}_{s+1},...,\overline{\lambda}_t$.

הערה: $(x-\lambda)^R(x-\overline{\lambda})^R=\left[(x-\lambda)(x-\overline{\lambda})\right]^R=\left[x^2-(\lambda+\overline{\lambda})x+\lambda\overline{\lambda}\right]^R=\left(x^2-2\operatorname{Re}\lambda+|\lambda|^2\right)^R$.

מסקנה: הפולינום האי-פריקים מעל $\mathbb{R}$ הם הפולינומים הליניאריים או הפולינומים מהצורה $p(x)=ax^2+bx+c$ כך ש $b^2-4ac<0$.

הוכחת נוסחת השורשים: $0=x^2+bx+c=(x+\frac{b}{2})^2-\frac{b^2-4c}{4}\Leftrightarrow x+\frac{b}{2}=\pm\sqrt{\frac{b^2-4c}{4}}\Leftrightarrow x=\frac{-b\pm\sqrt{b^2-4c}}{2}$. ■

מסקנה: מעל $\mathbb{R}$, כל פולינום שמעלתו גדולה מ 2 הוא פריק.

10. אידיאלים (ויישומם לגבי פולינומים ו gcd והגדרת זרות על קבוצת פולינומים)

הגדרה: קבוצה לא ריקה I של פולינומים ב $F[x]$ נקראת אידיאל אם היא סגורה תחת חיבור (כלומר: $f\in I,g\in I\Rightarrow f+g\in I$) וכן אם $p\in I,f\in F[x]\Rightarrow p\cdot f\in I$.

משפט: כל אידיאל של חוג הוא חוג.

מסקנה מתכונות האידיאל: אם $p_1,...,p_n\in I$ ו $f_1,...,f_n\in F[x]$ אזי $\sum_{i=1}^{n}f_ip_i\in I$.

הגדרה: יהי $p(x)\in F[x]$ פולינום. אזי אוסף כל הפולינום המתחלקים ב p מהווים אידיאל ונקראים האידיאל הנוצר ע"י p שמסומן $(p)=p\cdot F[x]$. אומרים ש p הוא היוצר של האידיאל. אידיאל מסוג זה הוא אידיאל ראשי. אם p_0 הוא הפולינום המתוקן של p אזי $(p_0)=p_0\cdot F[x]=p\cdot F[x]=(p)$.

משפט: לכל אידיאל ראשי קיים יוצר מתוקן יחיד שנקרא היוצר המתוקן של האידיאל.

משפט: כל אידיאל $I\subseteq F[x]$ הוא אידיאל ראשי, כלומר, לכל אידיאל קיים פולינום מתוקן p כך ש $I=p\cdot F[x]$, כלומר, p יוצר את האידיאל I שאפשר לפרשו כאוסף כל הפולינומים שמתחלקים ב p.

הוכחה: אם קיים יוצר מתוקן, היחידות היא טריוויאלית. לכן, נוכיח קיום. אם $I=\{0\}$ אז ניקח $p=0$ וגמרנו. לכן, נניח $I\neq\{0\}$ ויהי $p\in I$ מתוקן כך שמעלת p היא מינימלית מבין הפול' ב I השונים מאפס. נראה כי p יותר את I. מאחר ש $p\in I$ כל פולינום מהצורה $fp\,|\,f\in F[x]$ שייך ל I. בכיוון השני, אם $g\in I$ אזי נחלק ונרשום $g=ps+r$ ו $\deg r<\deg p$ ואז מאחר ש $sp\in I$, f גם $r=f-ps\in I$ ומאחר ש $\deg p$ מינימלית מבין הפולינומים השונים מאפס נובע $r=0$ ולכן $p\,|\,g$. ■

מסקנה: אם $\{0\}\neq I\subseteq F[x]$ אידיאל, אזי היוצר המתוקן שלו הוא הפולינום המתוקן שמעלתו מינימלית מבין הפולינומים השונים מאפס.

הגדרה: תהי $\Omega\subset F[x]$ קבוצה לא ריקה של פולינומים ונגדיר את האידיאל הבא:

$I_\Omega=\left\{\sum_{i=1}^{n}\omega_if_i\;\middle|\;\omega_1,...,\omega_n\in\Omega\ ,\ f_1,...,f_n\in F[x]\right\}$. אידיאל זה נקרא האידיאל שנוצר ע"י Ω.

הגדרה: היוצר המתוקן (היחיד) של I_Ω נקרא המחלק המשותף הגדול ביותר של Ω ומסומן ב $\gcd(\Omega)$.

משפט – תכונות ה gcd: נסמן $p=\gcd(\Omega)$. אזי: (1) p מחלק את כל איברי Ω. (2) אם קיים פולינום q שמחלק את כל איברי Ω אזי q מחלק גם את p. (3) הפולינום p מתוקן. (4) קיימים $h_1,...,h_n\in F[x]$ כך ש $\gcd(\Omega)=p=\sum_{i=1}^{n}h_i\omega_i$. (5) $\gcd(\Omega)=0\Leftrightarrow I_\Omega=\{0\}\Leftrightarrow\Omega=\{0\}$.

טענה: תכונות 1-3 במשפט הקודם קובעות את p באופן יחיד.

משפט: $p=\gcd(\Omega)$ הוא הפולינום היחיד שמקיים את התכונה הבאה: אם $q\mid p$ אזי q מחלק את כל איברי Ω, כלומר: $q\mid\omega_1$, ... , $q\mid\omega_n$.

משפט: $\gcd(f_1,f_2,f_3)=\gcd(f_1,\gcd(f_2,f_3))$.

הוכחה: נסמן $p=\gcd(f_1,\gcd(f_2,f_3))$. אזי לכל $q\in F[x]$ מתקיים:

$$q\mid\gcd(f_1,f_2,f_3)\Leftrightarrow q\mid f_1\wedge q\mid f_2\wedge q\mid f_3\Leftrightarrow q\mid f_1\wedge(q\mid f_2\wedge q\mid f_3)\Leftrightarrow q\mid f_1\wedge q\mid\gcd(f_2,f_3)\Leftrightarrow q\mid p$$

כל המעברים לעיל מבוססים על המשפט הקודם. כעת, הראנו שכל q מחלק את שני האגפים ומאחר שהם מתוקנים נובע השוויון ביניהם. ■

מסקנה: $\gcd(f_1,...,f_n)=\gcd(f_1,\gcd(f_2,...,\gcd(f_{n-1},f_n)))$.

הגדרה: תהי $\Psi\subset F[x]$ קבוצה לא ריקה של פולינומים ויהי J אוסף כל הפולינומים המחלקים את $p(x)$ כאשר $p(x)$ מתחלק בכל אברי Ψ. אזי J אידיאל והיוצר של J נקרא הכפולה המשותפת הקטנה ביותר ומסומן $p=lcm(\Psi)$.

תכונות ה lcm: אם $p=lcm(\Psi)$ אזי: (1) p מתחלק בכל איברי Ψ. (2) אם h פולינום שמתחלק בכל איברי Ψ אזי h מתחלק ב p. (3) p מתוקן.

משפט: $lcm(f_0,f_1)=\frac{f_0\cdot f_1}{\gcd(f_0,f_1)}$.

משפט: $lcm(f_1,...,f_n)=lcm(f_1,lcm(f_2,...,lcm(f_{n-1},f_n)))$ ובפרט $lcm(f_1,f_2,f_3)=lcm(f_1,lcm(f_2,f_3))$.

משפט: שלושת התנאים הבאים שקולים: (1) $\gcd(f_1,...,f_n)=1$ (2) קיימים פולינומים $h_1,...,h_n$ כך ש $\sum_{i=1}^{n}h_if_i=1$. (3) אין אף פולינום אי-פריק p שמחלק את כל הפולינומים $f_1,...,f_n$.

הוכחה: $(1\Leftrightarrow 2)$ מתכונות ה gcd. $(2\Leftarrow 3)$ אכן, אם היה קיים p אי-פריק שמחלק את $f_1,...,f_n$ אזי בפרט הוא היה מחלק את $\sum_{i=1}^{n}h_if_i=1$ ולכן בהכרח $p\mid 1$ וזו סתירה. $(1\Leftarrow 3)$ מאחר ו $\gcd(f_1,...,f_n)$ מחלק את $f_1,...,f_n$ אז בפרט הוא מחלק את 1 ומכיוון שהם מתוקנים נובע ש $\gcd(f_1,...,f_n)=1$. ■

הגדרה: יהיו $f_1,...,f_k$ פולינומים שונים זה מזה, נאמר שהם זרים בזוגות אם לכל $i\neq j$, f_i ו f_j זרים.

משפט: כל התנאים להלן שקולים: (1) $f_1,...,f_k$ זרים בזוגות. (2) אין אף פולינום אי-פריק המחלק שני פולינומים, f_i ו f_j, מתוך $f_1,...,f_k$ כאשר $i\neq j$. (3) אין אף פולינום אי-פריק המחלק את כל הפולינומים הבאים: $g_i=\prod_{i\neq j=1}^{k}f_j=f_1...f_{i-1}f_{i+1}...f_k$. $i=1,...,k$ (4) $\gcd(g_1,...,g_k)=1$.

מסקנה: יהיו $f_1,...,f_k$ פולינומים שונים, אזי הם זרים בזוגות אם ורק אם קיימים $h_1,...,h_k\in F[x]$ כך ש

$$\sum_{i=1}^{k}h_i\left(\prod_{i\neq j=1}^{k}f_j\right)=\sum_{i=1}^{k}h_i\left(f_1...f_{i-1}f_{i+1}...f_k\right)=1$$