על פולינומים

אלגברה ליניארית (1) - 80134

מרצה: ערן נבו

מתרגלים: איתמר ישראלי ושני שלומי

סמסטר ב' תשפ"ב, האוניברסיטה העברית

-

אלגברה ליניארית (2) - 80135

מרצה: איתמר צביק

מתרגלים: גיל לבנה ויואב כהן

סמסטר א' תשפ"ג, האוניברסיטה העברית

-

סוכם ע"י שריה אנסבכר

תוכן העניינים

בליניארית 1 למדנו רק את הפרק הראשון והפרק הרביעי, שני הפרקים האחרים שייכים לליניארית 2.
בחרתי להביא את נושא הפולינומים רק בליניארית 2 מפני שבליניארית אחת לא עוסקים במה שמייחד את מרחב הפולינומים ממרחבים וקטוריים אחרים ולעומת זאת בליניארית 2 הפולינומים מהווים חלק מהותי מהקורס.

* * *

תודתי נתונה לגלעד שרם על סיכומיו המצוינים שהיו לי לעזר רב עד כדי כך שניתן לומר שהסיכום הזה מבוסס על סיכומיו.

סיכומי קורס זה מוקדשים לאהרון כהן;
אהרון, הידיעה שתקרא את הסיכומים הללו דרבנה אותי לאורך כל הדרך.
בהצלחה!

* * *

סביר להניח שהסיכומים שלי מכילים טעויות רבות - אני מוצא כאלה כל יום (רשימת טעויות נפוצות),
אני מפציר בכם לעדכן אותי בכל טעות שאתם מוצאים (ממש כל טעות ללא יוצא מן הכלל);
אתם מוזמנים להגיב על המסמכים ב-Google Drive, לשלוח לי דוא"ל או למלא פנייה באתר.

לסיכומים נוספים היכנסו לאתר:
אקסיומת השלמות - סיכומי הרצאות במתמטיקה
https://srayaa.wixsite.com/math

1 התחלה

יהי $\mathbb{F}$ שדה.

הגדרה 1.1. פולינום מעל $\mathbb{F}$ הוא ביטוי מהצורה $a_0+a_1x+a_2x^2+...+a_nx^n$ כאשר $a_k\in\mathbb{F}$ לכל $n\geq k\in\mathbb{N}$.
המקדם של החזקה הגדולה ביותר (a_n) נקרא המקדם המוביל והמקדם של החזקה ה-0 (a_0) נקרא המקדם החופשי.
נסמן את קבוצת הפולינומים מעל $\mathbb{F}$ ב-$\mathbb{F}[x]$.

- ♣ מונום הוא פולינום בעל איבר יחיד, כלומר כל פולינום הוא חיבור של מונומים.

- ♣ מבחינה פורמלית פולינומים הם פשוט מחרוזות תווים, כדאי לזכור זאת בהמשך מבלי לאבד את האינטואיציה המזהה פולינום כפונקציה פולינומיאלית.
דוגמה הממחישה את העניין: הפולינומים 1, x^2+x+1 ו-x^3+x+1 הם פולינומים שונים מעל $\mathbb{F}_2$ למרות שכפונקציות הם שווים:

$$1^3+1+1=1=1^2+1+1$$
$$0^3+0+1=1=0^2+0+1$$

- ♣ ה-x בסימון $\mathbb{F}[x]$ הוא משתנה סרק, באותה מידה היה יכול להופיע שם כל קשקוש עקבי אחר, יתרה מזאת - לפעמים משתמשים בסימון זה כאשר במקום x כותבים מספר כלשהו ואז פירוש הסימון הוא קבוצת כל הביטויים הפולינומיאליים כשמציבים בהם את אותו מספר, לדוגמה (חוג השלמים של גאוס):

$$\begin{aligned}\mathbb{Z}[i] &:= \left\{\sum_{k=0}^{n}a_k\cdot i^k \;\middle|\; a_0,a_1,\ldots,a_n\in\mathbb{Z}\right\}\\ &= \{a+bi \mid a,b\in\mathbb{Z}\}\end{aligned}$$

- ♣ כל מה שנראה בקובץ זה נכון גם עבור קבוצת הפולינומים מעל חוג (שאינו בהכרח שדה), למעט נקודה אחת שעליה נעיר במפורש.

הגדרה 1.2. שוויון בין פולינומים
יהיו $P,G\in\mathbb{F}[x]$ ויהיו $a_0,a_1,\ldots,a_n,b_0,b_1,\ldots,b_m$ כך שמתקיים:

$$P(x)=\sum_{k=0}^{n}a_k\cdot x^k$$
$$G(x)=\sum_{k=0}^{m}b_k\cdot x^k$$

נאמר ש-$P=G$ אם $a_k=b_k$ לכל $\min\{n,m\}\geq k\in\mathbb{N}_0$ ובנוסף מתקיים: $n\geq m$ ו-$a_k=0$ לכל $m<k\in\mathbb{N}$ ו/או $n\leq m$ ו-$b_k=0$ לכל $n<k\in\mathbb{N}$.
כלומר אם ממקום מסוים ואילך המקדמים של פולינום הם אפסים, אז מקדמים אלו (אך לא אלו שלפניהם) אינם משפיעים על זהות הפולינום.

הגדרה 1.3. הדרגה או המעלה של פולינום $0 \neq P \in \mathbb{F}[x]$[1] (מסומנת ב-$\deg P$) היא החזקה הגדולה ביותר של הפולינום שהמקדם שלה אינו 0.[2]

נסמן גם $\deg 0 := -\infty$ ונכתוב $\deg 0 < \deg P$ לכל $0 \neq P \in \mathbb{F}[x]$.

♣ באותה מידה היה אפשר להגדיר $\deg 0 := -1$ (או כל מספר שלילי אחר) ואז אפילו לא היינו צריכים להסכים ש-$\deg 0 < \deg P$.

♣ נזהה פולינום עם סדרת המקדמים האינסופית שלו, כלומר עם סדרה כזו: $(a_0, a_1, a_2, ..., a_n, 0, 0, 0, ...)$[3], כך שהפולינום $1+x$ והפולינום $1+x+0\cdot x^2$ (לדוגמה) יזוהו כאותו פולינום.

♣ פולינומים מדרגה 0 נקראים פולינומים קבועים משום שכפונקציות הם מהווים פונקציות קבועות.

הגדרה 1.4. יהיו $P, G \in \mathbb{F}[x]$ ויהיו $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m$ כך שמתקיים:

$$P(x) = \sum_{k=0}^{n} a_k \cdot x^k$$
$$G(x) = \sum_{k=0}^{m} b_k \cdot x^k$$

- חיבור פולינומים יוגדר ע"י[4]:

$$(P+G)(x) := \sum_{k=0}^{\max\{n,m\}} (a_k + b_k) \cdot x^k = \left(\sum_{k=0}^{n} a_k \cdot x^k\right) + \left(\sum_{k=0}^{m} b_k \cdot x^k\right)$$

- כפל פולינומים יוגדר ע"י:

$$\begin{aligned}(P \cdot G)(x) &:= \left(\sum_{i=0}^{n} a_i \cdot x^i\right) \cdot \left(\sum_{j=0}^{m} b_j \cdot x^j\right) := \sum_{i=0}^{n} \left(a_i \cdot x^i \cdot \left(\sum_{j=0}^{m} b_j \cdot x^j\right)\right) \\ &:= \sum_{i=0}^{n} \left(\sum_{j=0}^{m} \left(a_i \cdot x^i\right) \cdot \left(b_j \cdot x^j\right)\right) := \sum_{i=0}^{n} \left(\sum_{j=0}^{m} a_i \cdot b_j \cdot \left(x^i \cdot x^j\right)\right) \\ &:= \sum_{i=0}^{n} \left(\sum_{j=0}^{m} a_i \cdot b_j \cdot x^{i+j}\right) = \sum_{k=0}^{n+m} \left(\left(\sum_{i=0}^{k} a_i \cdot b_{k-i}\right) \cdot x^k\right)\end{aligned}$$

- כפל פולינום בסקלר יוגדר ע"י (לכל $c \in \mathbb{F}$):

$$(c \cdot P) := \sum_{k=0}^{n} (c \cdot a_k) \cdot x^k$$

♣ כפל בסקלר הוא בעצם כפל בפולינום הקבוע המתאים.

טענה 1.5. $\mathbb{F}[x]$ הוא חוג חילופי[5] ביחס לפעולות החיבור והכפל הנ"ל.

---

[1] מדובר בפולינום האפס וכך גם בהמשך הקובץ.

[2] כלומר אם $P(x) = \sum_{k=0}^{n} a_k \cdot x^k$ אז $\deg P := \max\{k \in \mathbb{N}_0 \mid a_k \neq 0\}$.

[3] סדרות כאלה (שהחל ממקום מסוים כל איבריהן אפסים) נקראות סדרות נתמכות סופית.

[4] אם $n < m$ אז נגדיר $a_k := 0$ לכל $k \in \mathbb{N}$ כך ש-$n < k \leq m$ ואם $m < n$ אז נגדיר $b_k := 0$ לכל $k \in \mathbb{N}$ כך ש-$m < k \leq n$.

[5] חוג חילופי (קומוטטיבי) הוא קבוצה שעליה מוגדרות פעולות חיבור וכפל המקיימת את כל אקסיומות השדה מלבד קיום הופכי.

הגדרה 1.6 יהיו $P,G\in\mathbb{F}[x]$, נאמר ש-G מחלק את P (או ש-P הוא כפולה של G) אם קיים $Q\in\mathbb{F}[x]$ כך ש-$P=Q\cdot G$[6] ובמקרה כזה נסמן $G\mid P$.

טענה 1.7 יהיו $A,B,C\in\mathbb{F}[x]$, מתקיימים שלושת הפסוקים הבאים:

1. אם $A\mid B$ אז $A\mid Q\cdot B$ לכל $Q\in\mathbb{F}[x]$.
2. אם $A\mid B$ וגם $A\mid C$ אז $A\mid P\cdot B+G\cdot C$ לכל $P,G\in\mathbb{F}[x]$.
3. יחס החלוקה הוא טרנזיטיבי, כלומר אם $A\mid B$ ו-$B\mid C$ אז $A\mid C$.

משפט 1.8 לכל שני פולינומים $P,G\in\mathbb{F}[x]$ מתקיים:

1. $\deg(P+G)\leq\max\{\deg P,\deg,G\}$[7].
2. $\deg(P\cdot G)=\deg P+\deg G$[8].

מסקנה 1.9 יהיו $0\neq P,Q\in\mathbb{F}[x]$, אם $P\mid Q$ אז $\deg Q\leq\deg P$.

מסקנה 1.10 אם לפולינום $P\in\mathbb{F}[x]$ יש פולינום הופכי (כלומר קיים $G\in\mathbb{F}[x]$ כך ש-$P\cdot G=1$), אז P הוא פולינום קבוע.

♣ כלומר קבוצת האיברים ההפיכים בחוג פולינומים מעל שדה[9] היא קבוצת הפולינומים הקבועים.

מסקנה 1.11 יהיו $P,G\in\mathbb{F}[x]$, P ו-G מחלקים זה את זה אם"ם קיים $0\neq c\in\mathbb{F}$ כך ש-$P=c\cdot G$, אותו c הוא המנה של חלוקת המקדם המוביל של P במקדם המוביל של G.

מסקנה 1.12 יהיו $P,G\in\mathbb{F}[x]$ שני פולינומים המחלקים זה את זה ובעלי מקדמים זהים, מתקיים $P=G$.

משפט 1.13. חילוק פולינומים עם שארית
לכל שני פולינומים $P,G\in\mathbb{F}[x]$ כך ש-$G\neq 0$ קיימים שני פולינומים $Q,R\in\mathbb{F}[x]$ יחידים כך ש-$P=Q\cdot G+R$ ו-$\deg R<\deg G$.

♣ R זה נקרא השארית של חלוקת P ב-G ו-Q נקרא המנה של חלוקה זו.

♣ בעמוד הבא מופיע אלגוריתם לחילוק פולינומים עם שארית (דוגמאות לפעולת האלגוריתם ניתן למצוא בוויקיפדיה וב-MathWorld), האלגוריתם מוכיח את קיומם של פולינום המנה ופולינום השארית, והיחידות נובעת מהשוויון $P-Q\cdot G=R$ ומהעובדה ש-$\deg R<\deg G$[10].

♣ זהו אלגוריתם דומה מאד לאלגוריתם "חילוק ארוך" שלמדנו בבית הספר היסודי[11].

---

[6] כלומר שארית החלוקה של P ב-G היא פולינום האפס.
[7] בד"כ מתקיים שוויון אך אם $\deg P=\deg Q$ וגם המקדמים המובילים נגדיים זה לזה (סכומם הוא $0_{\mathbb{F}}$) אז יתקיים א"ש חזק.
[8] אם אחד הפולינומים הוא פולינום האפס, נגיד P, אז $\deg(P\cdot G)=\deg(0)=-\infty:=-\infty+\deg G$.
[9] מעל חוג (בניגוד לשדה) קבוצת הפולינומים ההפיכים תהיה קבוצת הפולינומים הקבועים כך שהקבוע המתאים להם הוא איבר הפיך בחוג.
[10] שני הנתונים מחייבים ש-$\deg P=\deg(Q\cdot G)$ ושהמקדם המוביל ב-$Q\cdot G$ הוא הנגדי של המקדם המתאים ב-P, כלומר הדרגה של Q והמקדם המוביל שלו נקבעים ביחידות ע"י P ו-G, לאחר מכן המקדם הזה קובע ביחידות את המקדם הבא בתור וכן הלאה (ממש כפי שעובד האלגוריתם).
[11] למעשה אלגוריתם "חילוק ארוך" הוא מקרה פרטי של חילוק פולינומים כאשר מציבים במשתנה את 10 (או, אם תרצו, זהו חילוק פולינומים ב-$\mathbb{R}[10]$).

אלגוריתם 1 חילוק פולינומים עם שארית

יהיו $P,G\in\mathbb{F}[x]$ כך ש-$G\neq 0$, נרצה למצוא שני פולינומים $Q,R\in\mathbb{F}[x]$ כך ש-$P=Q\cdot G+R$ ו-$\deg R<\deg G$.
נסמן $R_0:=P$ ו-$Q_0=0$, א"כ מתקיים $P=Q_0\cdot G+R_0$.
נסמן $n:=\deg G$ ויהיו $a_0,a_1,\ldots,a_n\in\mathbb{F}$ כך שמתקיים:

$$G(x)=\sum_{k=0}^{n}a_k\cdot x^k$$

נסמן $i:=0$ וכל עוד $\deg R_i\geq\deg G$:

- נסמן $r:=\deg R_i$ ויהיו $b_0,b_1,\ldots,b_m\in\mathbb{F}$ כך שמתקיים:

$$R_i(x)=\sum_{j=0}^{r}b_j\cdot x^j$$

- נגדיר (מהגדרה $a_n\neq 0$):

$$\begin{aligned}q_{r-n}&:=\frac{b_r}{a_n}\\ Q_{i+1}(x)&:=Q_i(x)+q_{r-n}\cdot x^{r-n}\\ R_{i+1}(x)&:=R_i(x)-q_{r-n}\cdot x^{r-n}\cdot G(x)\end{aligned}$$

נשים לב לשני דברים:

1.

$$\begin{aligned}P(x)&=Q_i(x)\cdot G(x)+R_i(x)\\ &=Q_i(x)\cdot G(x)+q_{r-n}\cdot x^{r-n}\cdot G(x)+R_{i+1}(x)\\ &=Q_{i+1}(x)\cdot G(x)+R_{i+1}(x)\end{aligned}$$

2. המקדם המוביל של $q_{r-n}\cdot x^{r-n}\cdot G(x)$ הוא b_r ו-$\deg(q_{r-n}\cdot x^{r-n}\cdot G(x))=(r-n)+\deg G=r=\deg R_i$, ומשכאן ש-$\deg R_{i+1}<\deg R_i$.

טענה 1.14. יהיו $P,G\in\mathbb{F}[x]$ כך ש-$G\neq 0$, $G\mid P$ אם"ם השארית של חלוקת P ב-G היא פולינום האפס.

טענה 1.15. יהיו $P,G\in\mathbb{F}[x]$, לכל $0\neq F\in\mathbb{F}[x]$ מתקיים $G\mid P$ אם"ם $F\cdot G\mid F\cdot P$.

הוכחה. יהי $0\neq F\in\mathbb{F}[x]$, ההוכחה שאם $G\mid P$ אז $F\cdot G\mid F\cdot P$ היא טריוויאלית, נוכיח את הכיוון השני.
נניח ש-$F\cdot G\mid F\cdot P$ ונחלק את G ב-P עם שארית: יהיו $Q,R\in\mathbb{F}[x]$ כך ש-$G=Q\cdot P+R$ ו-$\deg R<\deg P$, מכאן שמתקיים $F\cdot G=Q\cdot F\cdot P+F\cdot R$ ו-$\deg(F\cdot R)<\deg(F\cdot P)$.
מיחידות השארית נובע ש-$F\cdot R$ היא השארית של חלוקת $F\cdot G$ ב-$F\cdot P$, א"כ $F\cdot R=0$ ומכיוון ש-$F\neq 0$ נדע ש-$R=0$ ולכן $P\mid G$. ■

2 מחלק משותף מקסימלי וכפולה משותפת מינימלית

יהי $\mathbb{F}$ שדה.

הגדרה 2.1. פולינום $P\in\mathbb{F}[x]$ יקרא פולינום מתוקן אם המקדם המוביל שלו הוא 1, פולינום האפס אינו נחשב מתוקן.

משפט 2.2. יהיו $P_1,P_2,\ldots,P_r\in\mathbb{F}[x]$, מתקיימים שני הפסוקים הבאים:

- אם קיים $r\geq i\in\mathbb{N}$ כך ש-$P_i\neq 0$ אז קיים פולינום מתוקן $D\in\mathbb{F}[x]$ יחיד כך ש-$D\mid P_i$ לכל $r\geq i\in\mathbb{N}$ ובנוסף לכל $Q\in\mathbb{F}[x]$ המחלק את כולם ($Q\mid P_i$ לכל $r\geq i\in\mathbb{N}$) מתקיים $Q\mid D$.
- אם $P_i\neq 0$ לכל $r\geq i\in\mathbb{N}$ אז קיים פולינום מתוקן $L\in\mathbb{F}[x]$ כך ש-$P_i\mid L$ לכל $r\geq i\in\mathbb{N}$ ובנוסף לכל $M\in\mathbb{F}[x]$ המתחלק בכולם ($P_i\mid M$ לכל $r\geq i\in\mathbb{N}$) מתקיים $L\mid M$.

הגדרה 2.3. מחלק משותף מקסימלי וכפולה משותפת מינימלית

יהיו $P_1,P_2,\ldots,P_r\in\mathbb{F}[x]$,

- אם קיים $r\geq i\in\mathbb{N}$ כך ש-$P_i\neq 0$ אז נסמן ב-$\gcd(P_1,P_2,\ldots,P_r)$ את אותו D יחיד שמקיים את התנאים במשפט שלעיל, ונקרא לו המחלק המשותף המקסימלי של $P_1,P_2,\ldots,P_r$.
- אם $P_i\neq 0$ לכל $r\geq i\in\mathbb{N}$ אז נסמן ב-$\operatorname{lcm}(P_1,P_2,\ldots,P_r)$ את אותו M יחיד שמקיים את התנאים במשפט שלעיל ונקרא לו הכפולה המשותפת המינימלית של $P_1,P_2,\ldots,P_r$.

♣ הגדרות שקולות ל-gcd ול-lcm הן:

- המחלק המשותף המקסימלי הוא הפולינום המתוקן המחלק את $P_1,P_2,\ldots,P_r$ שדרגתו היא הגבוהה ביותר מבין אלה שמחלקים את כולם.
- הכפולה המשותפת המינימלית היא הפולינום המתוקן המתחלק ב-$P_1,P_2,\ldots,P_r$ שדרגתו היא הנמוכה ביותר מבין אלה שמתחלקים בכולם.

משפט 2.4. יהיו $P,G\in\mathbb{F}[x]$.

יהיו $Q_1,Q_2,\ldots,Q_r\in\mathbb{F}[x]$, $n_1,n_2,\ldots,n_r,m_1,m_2,\ldots,m_r\in\mathbb{N}_0$ ו-$a,b\in\mathbb{F}$ כך שהפירוקים של P ו-Q לגורמים אי-פריקים הם[12]:

$$P=\prod_{i=1}^{r}(Q_i)^{n_i}$$
$$G=\prod_{i=1}^{r}(Q_i)^{m_i}$$

מתקיים:

$$\gcd(P,G)=\prod_{i=1}^{r}(Q_i)^{\min\{n_i,m_i\}}$$
$$\operatorname{lcm}(P,G)=\prod_{i=1}^{r}(Q_i)^{\max\{n_i,m_i\}}$$

מסקנה 2.5. יהיו $P,G\in\mathbb{F}[x]$, מתקיים:

$$\operatorname{lcm}(P,G)=\frac{P\cdot G}{\gcd(P,G)}$$

[12] אם Q_i הוא גורם של P אך אינו גורם של G אז $m_i=0$, ולהיפך, אם Q_i הוא גורם של G אך לא של P אז $n_i=0$.

טענה 2.6. יהיו $P,G,Q,R\in\mathbb{F}[x]$ כך ש-$P=Q\cdot G+R$, מתקיים $\gcd(P,G)=\gcd(G,R)$.

טענה 2.7. יהיו $P,G\in\mathbb{F}[x]$.

1. $\gcd(F,G)=\gcd(G,F)$.
2. לכל $Q\in\mathbb{F}[x]$ מתקיים $Q\cdot\gcd(F,G)=\gcd(Q\cdot F,Q\cdot G)$.
3. אם קיים $Q\in\mathbb{F}[x]$ כך ש-$Q\mid F\cdot G$ וגם $\gcd(G,Q)=1$ אז $Q\mid F$.

הגדרה 2.8. פולינומים זרים

נאמר ששני פולינומים $P,G\in\mathbb{F}[x]$ <u>זרים זה לזה</u> אם $\gcd(P,G)=1$, כלומר אין להם מחלק שאינו טריוויאלי.

הגדרה 2.9. פולינומים ידידים

נאמר ששני פולינומים $P,G\in\mathbb{F}[x]$ הם <u>פולינומים ידידים</u> אם $G\mid P$ וגם $P\mid G$.

♣ מהגדרה אם $P,G\in\mathbb{F}[x]$ הם פולינומים ידידים אז קיים $c\in\mathbb{F}[x]$ כך ש-$P=c\cdot G$ ולכן בהכרח $\deg P=\deg G$, אותו c הוא המנה בין שני המקדמים המובילים ולכן אם נתון בנוסף ששניהם מתוקנים אז הם שווים.

הגדרה 2.10. אידיאל

קבוצה $I\subseteq\mathbb{F}[x]$ תקרא <u>אידיאל</u> אם מתקיימים שלושת התנאים הבאים:

1. $0\in I$.
2. לכל $P,G\in I$ מתקיים $P+G\in I$.
3. לכל $P\in I$ ולכל $Q\in\mathbb{F}[x]$ מתקיים $Q\cdot P\in I$.

♣ למעשה זהו מקרה פרטי, בכל חוג חילופי קיימים אידאלים וזוהי ההגדרה שלהם.

משפט 2.11. יהי $I\subseteq\mathbb{F}[x]$ אידיאל, מתקיימת אחת משתי האפשרויות הבאות: $I=\{0\}$ או שקיים פולינום מתוקן יחיד $P\in\mathbb{F}[x]$ כך שמתקיים $I=\{Q\cdot P\mid Q\in\mathbb{F}[x]\}$.

הוכחה. נניח ש-$I\neq\{0\}$, יהי $P\in I$ פולינום מתוקן מדרגה מינימלית, כלומר לכל $0\neq G\in I$ מתקיים $\deg P\leq\deg G$.
יהי $G\in I$ פולינום ויהיו $Q,R\in\mathbb{F}[x]$ כך ש-$G=Q\cdot P+R$ ו-$\deg R<\deg P$, מהגדרת האידיאל נובע ש-$R\in I$ ולכן מהגדרת P נובע ש-$R=0$ ומכאן ש-$G=Q\cdot P$.
היחידות נובעת מהעובדה שאם G מתוקן ו-$\deg G=\deg P$ אז $Q=1$. ■

טענה 2.12. יהיו $P,G\in\mathbb{F}[x]$ שני פולינומים, הקבוצה $I:=\{A\cdot P+B\cdot G\mid A,B\in\mathbb{F}[x]\}$ היא אידיאל ומתקיים $I=\{0\}$ או $I=\{Q\cdot\gcd\{P,G\}\mid Q\in\mathbb{F}[x]\}$, בפרט אם $P\neq 0$ ו/או $G\neq 0$ אז קיימים $A,B\in\mathbb{F}[x]$ כך ש-$\gcd(P,G)=A\cdot P+B\cdot G$.

♣ נשים לב למספר נקודות דמיון בין $\mathbb{F}[x]$ לבין $\mathbb{Z}$:

1. שניהם חוגים חילופיים, כלומר החיבור והכפל שלהם מקיימים את כל אקסיומות השדה מלבד קיום הופכי.
2. בשניהם קיים חילוק עם שארית.
3. בשניהם קיים יחס חלוקה ("a מחלק את b" או $a\mid b$).
4. בשניהם לכל איבר יש הצגה יחידה כמכפלה של אי-פריקים (ב-$\mathbb{Z}$ האי-פריקים נקראים גם המספרים הראשוניים).
5. בשניהם ניתן להגדיר מחלק משותף מקסימלי וכפולה משותפת מינימלית באותה צורה (ע"י יחס החלוקה הנ"ל), כמו כן, שני מספרים שלמים נקראים זרים אם המחלק המשותף המקסימלי שלהם הוא 1.
6. כל ההגדרות והטענות בפרק זה תקפות באותה צורה גם בחוג השלמים.

♣ בקורס "תורת המספרים האלמנטרית" מופיע סיכום מקביל על המספרים השלמים תחת הכותרת "התחלקות".

2.1 אלגוריתם אוקלידס

יהיו $P,G\in\mathbb{F}[x]$ כך שלפחות אחד מהם שונה מפולינום האפס, נרצה למצוא את $\gcd(P,G)$.

נגדיר $R_0=P$ ו-$R_1=G$[13] ונמצא את $\gcd(R_0,R_1)$.

לאלגוריתם ישנן שתי גרסאות: האלגוריתם הבסיסי והאלגוריתם המורחב, להלן הפירוט של שניהם בפסאודו-קוד.

אלגוריתם 2 אלגוריתם אוקלידס הבסיסי

נגדיר $i:=0$.

כל עוד R_{i+1} אינו פולינום האפס:

- נחלק את R_i ב-R_{i+1} עם שארית, נסמן ב-Q_i את המנה וב-R_{i+2} את השארית (כלומר יהיו $Q_i,R_{i+2}\in\mathbb{F}[x]$ כך ש-$\deg R_{i+2}<\deg R_{i+1}$ וגם $R_i=R_{i+1}\cdot Q_i+R_{i+2}$).
- נגדיר את i להיות $i+1$ ונעבור לשלב הבא בלולאה.

כעת מתקיים $R_{i+1}=0$ ו-$R_i=\gcd(R_0,R_1)$.

אלגוריתם 3 אלגוריתם אוקלידס המורחב

נגדיר $i:=0$.

נגדיר $A_{-1}:=0$ ו-$B_{-1}:=1$ ומכאן שמתקיים:

$$R_1=A_{-1}\cdot R_0+B_{-1}\cdot R_1$$

כל עוד $R_{i+1}\neq 0$:

- נחלק את R_i ב-R_{i+1} עם שארית, נסמן ב-Q_i את המנה וב-R_{i+2} את השארית.
- נחלק למקרים:
  - אם $i=0$ אז נגדיר $A_0:=1$ ו-$B_0:=-Q_0$.
  - אחרת, נגדיר $A_i=A_{i-2}-Q_i\cdot A_{i-1}$ ו-$B_i:=B_{i-2}-Q_i\cdot B_{i-1}$.
- נגדיר את i להיות $i+1$ ונעבור לשלב הבא בלולאה.

כעת מתקיים $R_{i+1}=0$ וגם:

$$\gcd(R_0,R_1)=R_i=A_{i-2}\cdot P+A_{i-2}\cdot G$$

בעמוד הבא נוכיח את הנכונות של האלגוריתם המורחב וממילא נקבל את הנכונות של האלגוריתם הבסיסי.

[13] כדאי להגדיר את R_0 להיות בעל הדרגה הגדולה יותר מבין השניים משום שבשלב הראשון של האלגוריתם נחלק את R_0 ב-R_1 עם שארית.

נגדיר $i:=0$.

נגדיר $A_{-1}:=0$ ו-$B_{-1}:=1$ ומכאן שמתקיים:

$$R_1 = A_{-1}\cdot R_0 + B_{-1}\cdot R_1$$

כל עוד $R_{i+1}\neq 0$:

- נחלק את R_i ב-R_{i+1} עם שארית, נסמן ב-Q_i את המנה וב-R_{i+2} את השארית.

$$\Rightarrow R_{i+2} = R_i - R_{i+1}\cdot Q_i$$

מטענה 2.6 נובע שבכל שלב מתקיים $\gcd\left(R_{i+2},R_{i+1}\right)=\gcd\left(R_{i+1},R_i\right)=\ldots=\gcd\left(R_0,R_1\right)$, וגם $\deg R_{i+2}<\deg R_{i+1}$ (לכן האלגוריתם מוכרח להיעצר בשלב כלשהו שהרי מדובר במספרים שלמים).

- יהיו $A_i,B_i\in\mathbb{F}\left[x\right]$ כך שמתקיים:

$$R_{i+2} = A_i\cdot R_0 + B_i\cdot R_{i+1}$$

נסביר כיצד למצוא A_i ו-B_i כאלה:

  - אם $i=0$ אז נגדיר $A_0:=1$ ו-$B_0:=-Q_0$ ואכן מתקיים $R_2=1\cdot R_0-Q_0\cdot R_1$.
  - אחרת, נזכור ש-$R_{i+1}=A_{i-1}\cdot R_0+B_{i-1}\cdot R_1$ וגם $R_i=A_{i-2}\cdot R_0+B_{i-2}\cdot R_1$, ומכיוון ש-$R_{i+2}=R_i-Q_i\cdot R_{i+1}$ ניתן להציג את R_{i+2} כך:

$$\begin{aligned}R_{i+2} &= R_i - R_{i+1}\cdot Q_i = \left(A_{i-2}\cdot R_0+B_{i-2}\cdot R_1\right)-\left(A_{i-1}\cdot R_0+B_{i-1}\cdot R_1\right)\cdot Q_i\\ &= \left(A_{i-2}-Q_i\cdot A_{i-1}\right)\cdot R_0+\left(B_{i-2}-Q_i\cdot B_{i-1}\right)\cdot R_1\end{aligned}$$

ולכן נגדיר $A_i=A_{i-2}-Q_i\cdot A_{i-1}$ ו-$B_i:=B_{i-2}-Q_i\cdot B_{i-1}$.

- נגדיר את i להיות $i+1$ ונעבור לשלב הבא בלולאה.

כעת מתקיים $R_{i+1}=0$, כלומר:

$$0 = R_{i+1} = R_{i-1} - R_i\cdot Q_{i-1}$$

וממילא:

$$R_i = \gcd\left(R_{i+1},R_i\right)=\gcd\left(R_i,R_{i-1}\right)=\ldots=\gcd\left(R_0,R_1\right)$$

בנוסף מתקיים:

$$\gcd\left(R_0,R_1\right)=R_i=A_{i-2}\cdot P+B_{i-2}\cdot G$$

ולכן נחזיר את R_i,A_{i-2},B_{i-2} ונסיים.

3 שורשים ופריקות

3.1 מעל שדה כללי

יהי $\mathbb{F}$ שדה.

הגדרה 3.1. נאמר שפולינום לא קבוע $P \in \mathbb{F}[x]$ הוא אי-פריק אם לא קיים פולינום $G \in \mathbb{F}[x]$ כך ש-$G \mid P$ וגם $0 < \deg G < \deg P$.[14]

הגדרה 3.2. סקלר $\lambda \in \mathbb{F}$ יקרא שורש של פולינום $P \in \mathbb{F}[x]$ אם מתקיים $P(\lambda) = 0_{\mathbb{F}}$.[15]

♣ לכל פולינום מדרגה 1 יש שורש יחיד.

טענה 3.3. לכל $P \in \mathbb{F}[x]$ ולכל $a \in \mathbb{F}$ מתקיים $x - a \mid P(x) - P(a)$ ובאופן שקול השארית של חלוקת P ב-$x - a$ היא $P(a)$.

הוכחה. נחלק את $P(x) - P(a)$ ב-$x - a$ עם שארית: יהיו $Q, R \in \mathbb{F}[x]$ כך ש-$P(x) - P(a) = Q(x) \cdot (x - a) + R(x)$ ו-$\deg R < \deg(x - a)$.
מהגדרה $\deg(x - a) = 1$ ולכן $\deg R = 0$ ש-R הוא פולינום האפס, בכל מקרה R הוא פולינום קבוע.
נציב a בשני האגפים ונקבל:

$$0 = P(a) - P(a) = Q(a) \cdot (a - a) + R(a) = Q(a) \cdot 0 + R(a) = R(a)$$

א"כ $R(a) = 0$ ומהיות של R פולינום קבוע נובע ש-$R(x) = 0$ לכל $x \in \mathbb{F}$, כלומר R הוא פולינום האפס ומכאן ש-$x - a \mid$ $P(x) - P(a)$. ■

מסקנה 3.4. סקלר $\lambda \in \mathbb{F}$ הוא שורש של פולינום $P \in \mathbb{F}[x]$ אם"ם $x - \lambda \mid P(x)$.

מסקנה 3.5. יהי $P \in \mathbb{F}[x]$ ונסמן $n := \deg P$, ל-P יש לכל היותר n שורשים שונים ב-$\mathbb{F}$.

מסקנה 3.6. אם לפולינום מדרגה גדולה מ-1 יש שורש אז הוא פריק.

הגדרה 3.7. ריבוי שורש של פולינום
יהי $P \in \mathbb{F}[x]$ ונניח כי $\lambda \in \mathbb{F}$ הוא שורש של P, ראינו שמתקיים $x - \lambda \mid P(x)$.
יהיו $Q \in \mathbb{F}[x]$ ו-$k \in \mathbb{N}$ כך ש-$P(x) = (x - \lambda)^k \cdot Q(x)$ ו-λ אינו שורש של Q,[16] k יקרא הריבוי האלגברי של λ (ביחס ל-P).

למה 3.8. אם $\lambda \in \mathbb{F}$ הוא שורש של פולינום $P \in \mathbb{F}[x]$ אז λ הוא שורש של $P \cdot Q$ לכל $Q \in \mathbb{F}[x]$.

טענה 3.9. אם לפולינום מדרגה 2 או 3 אין שורש אז הוא אי-פריק.

הוכחה. אם הוא היה פריק אז אחד הגורמים שלו היה מוכרח להיות מדרגה 1 וכפי שראינו זה אומר שיש לו שורש. ■

משפט 3.10. פולינום $P \in \mathbb{F}[x]$ הוא אי-פריק אם"ם לכל $F, G \in \mathbb{F}[x]$ כך ש-$P \mid F \cdot G$ מתקיים $P \mid F$ ו/או $P \mid G$.

♣ לתכונה הנ"ל קוראים ראשוניות, כלומר פולינום הוא אי-פריק אם"ם הוא ראשוני.

הוכחה. יהי $P \in \mathbb{F}[x]$.

- $\Leftarrow$
  נניח ש-P אי-פריק ויהיו $F, G \in \mathbb{F}[x]$ כך ש-$P \mid F \cdot G$.
  נסמן $D := \gcd(F, P)$, מהגדרה $D \mid P$ ולכן מהעובדה ש-P אי-פריק נובע ש-$D = 1$ או ש-$D = c \cdot P$ עבור $0 \neq c \in \mathbb{F}$ כלשהו.
  אם $D = 1$ אז D ו-F זרים ולכן מסעיף 3 בטענה 2.7 נובע ש-$P \mid G$, ואם $D = c \cdot P$ אז מהגדרת ה-gcd P מחלק את F.

---
[14] דרישות אלו נצרכות בגלל שבהכרח מתקיים $P \mid P$ ו-$1 \mid P$.
[15] כאן אנו מתייחסים ל-P כפונקציה מ-$\mathbb{F}$ ל-$\mathbb{F}$.
[16] כלומר k הוא החזקה המקסימלית המקיימת $(x - \lambda)^k \mid P(x)$.

- $\Rightarrow$

נניח שלכל $F,G\in\mathbb{F}[x]$ כך ש-$P\mid F\cdot G$ מתקיים $P\mid F$ ו/או $P\mid G$, ויהי $G\in\mathbb{F}[x]$ כך ש-$P\mid G$.
יהי $Q\in\mathbb{F}[x]$ כך ש-$P=G\cdot Q$, א"כ מתקיים $P\mid G\cdot Q$ ולכן מההנחה נובע ש-$P\mid G$ או ש-$P\mid Q$.
אם $G\mid P$ אז P ו-G הם פולינומים ידידים ולכן קיים $c\in\mathbb{F}$ כך ש-$P=c\cdot G$ ואם $Q\mid P$ אז קיים $c\in\mathbb{F}$ כך ש-$P=c\cdot Q$, א"כ מתקיים $\deg G=\deg P$ או $\deg Q=\deg P$, כלומר $\deg G=\deg P$ או $\deg G=\deg 0$ ולכן מהגדרה P אי-פריק.

■

למה 3.11. יהי $P\in\mathbb{F}[x]$ פולינום אי-פריק ויהיו $G_1,G_2,\ldots,G_n\in\mathbb{F}[x]$ כך ש-$P\mid G_1\cdot G_2\cdot\ldots\cdot G_n$, קיים $n\geq i\in\mathbb{N}$ כך ש-$P\mid G_i$.

למה 3.12. יהי $P\in\mathbb{F}[x]$ פולינום אי-פריק מתוקן ויהיו $G_1,G_2,\ldots,G_n\in\mathbb{F}[x]$ פולינומים אי-פריקים מתוקנים כך ש-$P\mid G_1\cdot G_2\cdot\ldots\cdot G_n$, קיים $n\geq i\in\mathbb{N}$ כך ש-$P=G_i$.

משפט 3.13. פירוק לגורמים אי-פריקים
יהי $G\in\mathbb{F}[x]$ פולינום. קיימים פולינומים מתוקנים $P_1,P_2,\ldots,P_r\in\mathbb{F}[x]$ שונים זה מזה, מספרים טבעיים $n_1,n_2,\ldots,n_r\in\mathbb{N}$ וסקלר $c\in\mathbb{F}$ יחידים[17] כך שמתקיים:

$$G=c\cdot\prod_{i=1}^{r}(P_i)^{n_i}$$

הצגה זו נקראת הפירוק של P לגורמים אי-פריקים.

הוכחה. ניתן להוכיח באינדוקציה שניתן להציג כל פולינום כמכפלה של פולינומים אי-פריקים מתוקנים וסקלר[18].
יהיו $P_1,P_2,\ldots P_r,Q_1,Q_2,\ldots Q_s\in\mathbb{F}[x]$ כך ש-$P_i\neq P_j$ אם $i\neq j$ (לכל $r\geq i,j\in\mathbb{N}$) וכמו כן $Q_i\neq Q_j$ אם $i\neq j$ (לכל $s\geq i,j\in\mathbb{N}$), $n_1,n_2,\ldots,n_r,m_1,m_2,\ldots,m_s\in\mathbb{N}$ ו-$c,c'\in\mathbb{F}$ כך שמתקיים:

$$c\cdot\prod_{i=1}^{r}(P_i)^{n_i}=G=c'\cdot\prod_{j=1}^{s}(Q_j)^{m_i}$$

ראשית נשים לב לכך ש-c ו-c' מוכרחים להיות שווים למקדם המוביל של G משום שכל הפולינומים במכפלה מתוקנים.
נגדיר פונקציה $f:\{i\in\mathbb{N}\mid i\leq r\}\to\{i\in\mathbb{N}\mid i\leq s\}$ באופן אינדוקטיבי.
נסמן $i:=1$

- לכל $r\geq i\in\mathbb{N}$:
  - מהלמה האחרונה (3.12) נובע שקיים $s\geq j\in\mathbb{N}$ כך ש-$Q_j=P_i$ ובנוסף $n_i=m_j$, יהי j כנ"ל ונסמן $f(i):=j$.
  - כעת נסיר מהמכפלה באגף שמאל את $(P_i)^{n_i}$ ומאגף ימין נסיר את $(Q_j)^{m_j}$ ושוב נקבל שוויון כך ש-$(Q_j)^{m_j}$ כבר אינו מופיע מופיע במכפלה הימנית ומכאן שהפונקציה שנגדיר תהיה חח"ע.
  - נעבור לשלב הבא בלולאה.
- כעת אגף שמאל הוא המכפלה הריקה השווה ל-1 ולכן גם אגף ימין שווה ל-1, כלומר $s=r$ ומכאן ש-f על ומכיוון שהיא חח"ע הרי שהיא הפיכה.

■

[17] עד כדי שינוי סדר ושינוי סימן.
[18] מפרקים לגורמים עד שכבר א"א לחלק מפני שכל הגורמים אי-פריקים.

3.2 מעל שדה המרוכבים

משפט 3.14. המשפט היסודי של האלגברה
לכל $P\in\mathbb{C}\left[x\right]$ יש שורש מרוכב.

- ♣ לא הוכחנו את המשפט בכיתה, זהו חומר מתקדם יותר.
- ♣ שדה שלכל פולינום מעליו יש שורש בשדה נקרא סגור אלגברית.

מסקנה 3.15. יהי $P\in\mathbb{C}\left[x\right]$ פולינום מתוקן ונסמן $n:=\deg P$, קיימים $\lambda_{1},\lambda_{2},\ldots,\lambda_{n}\in\mathbb{C}$ (לאו דווקא שונים) כך שמתקיים:

$$P\left(x\right)=\prod_{i=1}^{n}\left(x-\lambda_{i}\right)$$

מסקנה 3.16. כל פולינום אי-פריק מעל $\mathbb{C}$ הוא מדרגה 1.

טענה 3.17. לכל $P\in\mathbb{R}\left[x\right]\subseteq\mathbb{C}\left[x\right]$ ולכל $\lambda\in\mathbb{C}$ מתקיים $P\left(\overline{\lambda}\right)=\overline{P\left(\lambda\right)}$.

- ♣ הטענה נובעת מהעובדה שהצמדה היא כפלית וחיבורית (כלומר לכל $z,w\in\mathbb{C}$ מתקיים $\overline{z+w}=\overline{z}+\overline{w}$ ו-$\overline{z\cdot w}=\overline{z}\cdot\overline{w}$), הטענה נכונה דווקא בפולינום בעל מקדמים ממשיים משום שרק אז המקדמים צמודים לעצמם.

מסקנה 3.18. יהי $P\in\mathbb{R}\left[x\right]\subseteq\mathbb{C}\left[x\right]$ ויהי $\lambda\in\mathbb{C}$ שורש של P, גם $\overline{\lambda}$ הוא שורש של P.

מסקנה 3.19. לכל פולינום מדרגה אי-זוגית מעל $\mathbb{R}$ יש שורש ממשי.

מסקנה 3.20. כל פולינום אי-פריק מעל $\mathbb{R}$ הוא פולינום מדרגה 1 או פולינום מדרגה 2 חסר שורשים.

- ♣ כלומר הפולינומים האי-פריקים מעל $\mathbb{R}$ הם פולינומים ליניאריים ופולינומים ריבועיים שהדיסקרימיננטה שלהם שלילית.

4 הפולינומים כמרחב וקטורי

יהי $n\in\mathbb{N}_{0}$ ויהא $\mathbb{F}$ שדה.

הגדרה 4.1. תהא $\left(a_{n}\right)_{n=1}^{\infty}$ סדרה שכל איבריה ב-$\mathbb{F}$, נאמר ש-$\left(a_{n}\right)_{n=1}^{\infty}$ היא סדרה נתמכת סופית אם קיים $N\in\mathbb{N}$ כך שלכל $N<n\in\mathbb{N}$ מתקיים $a_{n}=0$.

מסקנה 4.2. קבוצת הסדרות הנתמכות סופית היא תמ"ו של קבוצת הסדרות ($\mathbb{F}^{\mathbb{N}}$), וכמרחב וקטורי היא אינה נוצרת סופית.

סימון: $\mathbb{F}_{n}\left[x\right]:=\mathbb{F}_{\leq n}\left[x\right]:=\left\{ P\in\mathbb{F}\left[x\right]\mid\deg P\leq n\right\}$

משפט 4.3. $\mathbb{F}\left[x\right]$ הוא מרחב וקטורי מעל $\mathbb{F}$ ביחס לפעולת החיבור והכפל בסקלר שהוגדרו בפרק הראשון, ו-$\mathbb{F}_{n}\left[x\right]$ הוא תמ"ו שלו.

- ♣ נשים לב שישנו איזומורפיזם פשוט בין $\mathbb{F}_{n}\left[x\right]$ ל-$\mathbb{F}^{n+1}$ ובין $\mathbb{F}\left[x\right]$ לקבוצת הסדרות הנתמכות סופית מעל $\mathbb{F}$: נעתיק כל פולינום לסדרת המקדמים שלו.

מסקנה 4.4. $\mathbb{F}\left[x\right]$ הוא מרחב וקטורי שאינו נוצר סופית אך $\dim\mathbb{F}_{n}\left[x\right]=n+1$.

הגדרה 4.5. הבסיס הסטנדרטי של $\mathbb{F}_{n}\left[x\right]$ הוא $\left(1,x,x^{2},\ldots,x^{n}\right)$.