אלגברה לינארית 2א

ⓒ ארזים

17 במרץ 2013

ניזכר בהגדרות שנתנו בסוף השיעור שעבר.

הגדרה 0.1 אידאל $I \lhd R$ הוא תת קבוצה המקיימת:

1. $0 \in I$
2. $\forall i_1, i_2 \in I . i_1 + i_2 \in I$
3. $\forall r \in R, \forall i \in I . r \cdot i \in I$

הגדרה 0.2 אידאל ראשי הוא אידאל שנוצר על ידי איבר יחיד, כלומר עבור $a \in R$ כלשהו

$$I = (a) = \{ra \mid r \in R\}$$

<u>דוגמא לאידאל לא־ראשי:</u>

$$\begin{aligned} R &= R[x, y] \\ I &= \{p \in R \mid p(0,0) = 0\} \end{aligned}$$

משפט 0.3 בתחום $R = F[x]$, כל אידאל הוא אידאל ראשי.

הוכחה: יהי $I \lhd R$ אידאל. נניח שהוא לא אידאל האפס (שהוא ראשי ־ נוצר על ידי אפס). מתוך כל איברי I שאינם אפס ניקח פולינום ממעלה מינימלית. נסמנו $p(x)$.
עתה יהי $f(x) \in I$. נרצה להראות שמתקיים $p \mid f$. אכן, אם הדבר לא מתקיים, נבצע חילוק עם שארית:

$$f(x) = h(x) \cdot p(x) + r(x)$$

עבור $r(x)$ כלשהו שמקיים $\deg r < \deg p$. משום שהאיבר $p(x)$ באידאל גם האיבר $h(x) \cdot p(x)$, ומשום שהאיבר $f(x)$ באידאל גם האיבר $r(x)$, שמעלתו נמוכה משל p ־ בסתירה למינימליות. ■

הוכחה אנלוגית עובדת בשביל $\mathbb{Z}$ ־ גם שם כל אידאל הוא ראשי.

הערה 0.4 היחידות בחילוק עם שארית לא שיחקה תפקיד בהוכחה - רק הקיום.

הגדרה 0.5 תחום שלמות שבו כל אידאל הוא אידאל ראשי נקרא <u>תחום ראשי</u>.

משפט 0.6 יהי R תחום ראשי, ויהיו $a,b \in R$. אזי קיים $c \in R$ יחיד עד כדי כפל בהפיך המקיים את התכונה הבאה: $c \mid a$, $c \mid b$ וכן

$$d \mid a, d \mid b \Rightarrow d \mid c$$

c כזה מסומן $c = \gcd(a,b)$. כמו כן מתקיים שקיימים $r,s \in R$ כך שמתקיים

$$c = ra + sb$$

הוכחה: נסמן

$$I = \{ra + sb\}$$

ברור שזהו אידאל. R תחום ראשי, לכן I אידאל ראשי, כלומר קיים c כך שמתקיים $I = (c)$.
מבניית c ברור שקיימים r_0, s_0 כך שמתקיים $c = r_0 a + s_0 b$.
מתקיים $a \in I$ (עבור $r = 1, s = 0$), ולכן $c \mid a$, מהגדרת אידאל ראשי. אותו טיעון תקף גם לגבי b (עבור $r = 0, s = 1$).
נראה עתה שאם $d \mid a, d \mid b \Rightarrow d \mid c$. אכן, $c = r_0 a + s_0 b$, ולכן d מחלק כל אחד מהמחוברים באגף ימין, לכן הוא מחלק את כולו, ולכן הוא מחלק גם את אגף שמאל.
נשאר רק להראות את יחידות c (עד כדי חברות - כפל בהופכי). אכן, אם לאיבר d יש את אותה תכונה, אזי

$$c \mid d, d \mid c \Rightarrow d \sim c$$

■

משפט 0.7 אם R תחום ראשי, אזי $p \in R$ אי פריק $\Leftarrow$ p ראשוני (את הכיוון ההפוך הוכחנו לכל תחום שלמות, לאו דווקא ראשי).

הוכחה: יהי p אי־פריק. נניח $p \mid ab$. יש להוכיח $p \mid a$ או $p \mid b$. נגדיר $c = \gcd(p,a)$. מהגדרת gcd, אנחנו יודעים שמתקיים $c \mid p$. p אי פריק, לכן $c \sim p$ או c הפיך.

1. אם $c \sim p$ אזי כיוון שמתקיים גם $c \mid a$, נובע גם $p \mid a$.
2. אם c הוא הפיך, כיוון שהוא gcd, קיימים r,s כך שמתקיים

$$rp + sa = c$$

כעת, c הפיך, לכן נכפול בהופכי שלו ונקבל

$$r'p + s'a = 1, r' = rc^{-1}, s' = sc^{-1}$$

כעת נכפול את שני אגפי השוויון פי b:

$$r'pb + s'ab = b$$

כעת, p מחלק את שני המחוברים באגף שמאל, לכן גם את סכומם, ולכן גם את אגף ימין - כלומר $p \mid b$.

■

משפט 0.8 יהי R תחום ראשי, $a \in R$. בתרגיל הבית נראה כי קיים פירוק שלו למכפלת אי פריקים. כעת נניח שקיימים שני פירוקים כאלה:

$$a = \prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_i$$

אזי $n = m$, ולאחר סידור מחדש של אחד מהם, לכל $1 \leq i \leq n$ מתקיים $p_i \sim q_i$.

הוכחה: נוכיח באינדוקציה על n. אם $n = 1$, אזי מתקיים $p \mid \prod q_j$, ומשום שהאיבר p אי פריק הוא ראשוני, ולכן מחלק את אחד הגורמים. בלי הגבלת הכלליות, $p \mid q_1$, שגם הוא אי פריק, לכן $p \sim q_1$, וכעת לא ייתכן שמתקיים $m > 1$.
נניח שהטענה נכונה עבור n ונוכיח עבור $n + 1$.
כעת,

$$\prod_{i=1}^{n+1} p_i = \prod_{j=1}^{m} q_j$$

כעת, p_1 מחלק את אגף שמאל ולכן גם את אגף ימין. לכן מראשוניות, נובע $p \mid q_j$ כלשהו. כיוון שכולם אי פריקים, נובע, אחרי שינוי סדר, $p_1 \sim q_1$. על ידי העברת האיבר ההפיך שמבדיל ביניהם אל הגורם הבא, נוכל להניח שמתקיים $p_1 = q_1$. לכן מתקבל

$$p_1 \prod_{i=2}^{n+1} p_i = p_1 \prod_{j=2}^{m} q_j$$

לכן, מכלל הצמצום נקבל

$$\prod_{i=2}^{n+1} p_i = \prod_{j=2}^{m} q_j$$

כעת נפעיל את הנחת האינדוקציה ונקבל את הנדרש. ■

הערה 0.9 בחוגים $F[x], \mathbb{Z}$ קיים לכל איבר פירוק יחיד למכפלת אי-פריקים, עד כדי סדר וחברות.

הוכחה: קיום: בפולינומים, מפרקים כל עוד אפשר, המעלה תמיד יורדת, ולכן באינדוקציה מוכיחים את הטענה. בשלמים, אותה שיטה עובדת, כאשר האינדוקציה היא על גודל השלם.
■

מכאן אפשר להסיק תוצאות שהשתמנו בהן בעבר לגבי $F[x]$.
למשל, אם f מתפרק למכפלת גרומים לינאריים, וכן $f = h \cdot g$, אז גם h, g מתפרקים למכפלת גורמים לינאריים גם כן - שכן הגורמים הלינאריים הם אי פריקים, ואם נפרק את h, g למכפלת אי פריקים, נקבל שמכפלת הפירוקים היא הפירוק של f - שמתפרק לגורמים לינאריים. מיחידות הפירוק נובעת הטענה.
טענה אחרת - סכום הריבויים האלגבריים של השורשים קטן או שווה למעלת הפולינום - נשאיר כתרגיל (קל).

איך ניתן לחשב את $\gcd(a,b)$ דרך הפירוק למכפלת אי פריקים? נכתוב:

$$\begin{aligned} a &= \prod_{i=1}^{k} p_i^{n_i} \\ b &= \prod_{i=1}^{k} p_i^{m_i} \end{aligned}$$

כאשר $m_i, n_i \geq 0$ לכל i. כעת

$$c = \gcd(a,b) = \prod_{i=1}^{k} p_i^{\min(n_i, m_i)}$$

באופן אנלוגי למושג של $\gcd(a,b)$, ניתן להגדיר $\mathrm{lcm}(a,b)$ - זהו איבר l שמקיים $a \mid l, b \mid l$ וכן לכל איבר m שמקיים $a \mid m, b \mid m$ מקיים גם $l \mid m$.
במונחים של הפירוק לראשוניים שראינו למעלה,

$$l = \mathrm{lcm}(a,b) = \prod_{i=1}^{k} p_i^{\max(n_i, m_i)}$$

<u>שימוש:</u> נשתמש בתורה זו כדי לבנות שדות הרחבה $F \subseteq K$ שבהם מוצאים שורשים לפולינומים מעל F.
בדומה לבנייה של השדה הסופי שבו p איברים, נוכל לבנות שדות שמכילים את השדה F באופן הבא:
ניקח פולינום אי פריק $p(x)$ ונגדיר על $F[x]$ פעולות של חיבור וכפל מודולו $p(x)$. כדי להיות קונקרטיים, אם $\deg p = n$ אזי בגלל משפט חילוק עם שארית, את כל שאריות החלוקה בפולינום $p(x)$ ניתן להתאים באופן חח"ע לכל הפולינומים ממעלה לכל היותר $n-1$.
בדיוק כמו בחלוקה בראשוני p בשלמים, מגדירים חיבור וכפל של פולינומים מודולו $p(x)$, וקל לראות שמתקיימות כל אקסיומות השדה - למעט קיום איבר הופכי, שאת זאת יש לבדוק. כל האקסיומות מתקיימות כי הן מתרחשות בתוך $F[x]$.
מדוע קיים איבר הופכי לכל $f(x)$ שאינו 0 בחוג זה? **הוכחה:** יהי $f \neq 0$, כלומר f אינו מתחלק בפולינום $p(x)$ שאיתו אנחנו עובדים. לכן f, p זרים (כלומר $\gcd(f,p) = 1$), ולכן

קיימים r, s שעבורם

$$\begin{aligned} r(x) \cdot f(x) + s(x) \cdot p(x) &= 1 \\ r(x) \cdot f(x) &= 1 \ (\mod p(x)) \end{aligned}$$

ולכן $r(x)$ הוא ההופכי של f מודולו $p(x)$. ■

זהו שדה שמכיל את F - שכן איברי F הם הפולינומים הקבועים.