תרגיל בית 3 אינפי II

הגדרה: יהי R תח"ע קומוטטיבי עם איבר יחידה. יהיו $a,b\in R$ שאינם שניהם 0. איבר $d\neq 0$. אנו אומרים ש- $d\in R$ הוא $\gcd(a,b)$ אם מתקיים:

(1) $d\mid a$, $d\mid b$

(2) $x\mid a, x\mid b \Rightarrow x\mid d$.

משפט: ב- $\mathbb{Z}[x]$, $\mathbb{F}[x]$ $\gcd$ תמיד קיים.

הערה: כאן ש- $\gcd(a,b)$ מוגדר עד כדי כפל באבר ההפיך.

מסקנה (הזהות של בזו): יהיו $a,b\in\mathbb{Z}[x]$ שאינם שניהם 0, $d=\gcd(a,b)$.
אזי קיימים $u,v\in\mathbb{Z}[x]$ כך ש- $d=au+bv$.

הגדרה: יהי R תח"ת קומוטטיבי. $a\in R$ נקרא **אי פריק** אם: a אינו הפיך (a לא ניתן להצגה כמכפלה $a=b\cdot c$ כאשר b,c אינם הפיכים).

דוגמא: $R=\mathbb{Z}$. $a\in\mathbb{Z}$ אי פריק $\Leftrightarrow$ כאשר $a=\pm p$.

משפט: יהי $f\in\mathbb{Z}[x]$ אי הפיך. אזי: הדרגה של f שווה ל- $\deg f$ אם f אי פריק.

ההפך הכי חיובי שאפשר שהתנאי הראשון וכפי שיהיה אי פריק השני.

תרגיל: ב- R. (1) $a=\gcd(a,b)\Leftrightarrow a\mid b$

(2) $a=\gcd(a,b)$ כאשר $a\neq 0$

(3) $\gcd(ta,tb)=t\gcd(a,b)$ (→ אז כל הכי אבר הפיך..)

(4) $\gcd(\gcd(a,b),c)=\gcd(a,\gcd(b,c))=\gcd(a,b,c)$

הוכחה: (1) $\Rightarrow$ $a\mid b$ כן $a=aq$, $a\mid a$. ע"י $a\mid x, a\mid x$ בל"כ: $a\mid x\Rightarrow$ קורה.

$\Leftarrow$ $a=\gcd(a,b)\Rightarrow a\mid b$ ראינו $\gcd$.

(2) קורה $a\mid a, a\mid b$. ע"י $a\mid x, a\mid x\Rightarrow a\mid x$.

(3) $d=\gcd(a,b)$ $\Rightarrow d\mid a, d\mid b$ $\Rightarrow td\mid ta, td\mid tb$ $\Rightarrow td\mid D$ (הגדרת $\gcd$).
$D=\gcd(ta,tb)$

כן $c\cdot td=D$. $\begin{cases} ta=D\cdot u \\ tb=D\cdot v \end{cases}$ $\Rightarrow$ $\begin{cases} ta=td\cdot cu \\ tb=td\cdot cv \end{cases}$

$\Rightarrow$ ניתן לצמצם כי אין מתקיים אפס וקיבלנו $a=dcu$ כלומר $d\mid a$, $d\mid b$
$b=dcv$

$\Rightarrow$ מהגדרת $\gcd$: $d\mid d$, $cc\cdot d=d\Rightarrow cc=1$ כן c הפיך ($c\cdot td=D$) כמבוקש!

(4) $d_1=\gcd(\gcd(a,b),c)$, $d_2=\gcd(a,\gcd(b,c))$. $\gcd$ הוכיחו:

$d_1 \mid a$, $d_1 \mid b$ (מהגדרה) $\Rightarrow d_1 \mid \gcd(a,b)$ $\Rightarrow d_1 \mid \gcd(\gcd(a,b),c)$

$d_1 \mid \gcd(b,c)$ $\Rightarrow d_1 \mid d_2$

■ $d_1=d_2\cdot c$ כך ש- c קיים $\Leftarrow d_2 \mid d_1$ באופן סימטרי

טענה: יהיו $a,b,c \in F[x]$ (ראינו ב-$\mathbb{Z}$)

(1) אם $\gcd(a,b)=1$ וגם $\gcd(a,c)=1$ אז $\gcd(a,bc)=1$.

(2) אם $a \mid bc$ ו- $\gcd(a,b)=1$ אז $a \mid c$.

(3) אם $b \mid a$, $c \mid a$ וגם $\gcd(b,c)=1$ אז $bc \mid a$

הוכחה:

(1) נסמן $\begin{cases} au_1+bv_1=1 \\ au_2+bv_2=1 \end{cases}$ כפי שראינו

$$1=(au_1+bv_1)(au_2+bv_2)=a^2u_1u_2+$$
$$=a^2u_1u_2+au_1cv_2+au_2bv_1+bc\cdot v_1v_2=$$
$$=a(\underbrace{au_1u_2+u_1cv_2+u_2bv_1}_{u})+bc\cdot\underbrace{v_1v_2}_{v}$$

כלומר $au+(bc)v=1$ ולכן $\gcd(a,bc)=1$ ✓

(2) $au+bv=1$ כפי שראינו, נכפול ב-c: $acu+bcv=c$ $\Leftarrow a \mid c$ ✓

(3) $b \mid a \Leftarrow a=bx$

$c \mid a \Leftarrow c \mid bx$, $\gcd(b,c)=1 \Leftarrow c \mid x$, $x=cy$ כפי שראינו

$a=bcy \Leftarrow bc \mid a$ ✓ ■

⚠ **הערה:** ① $p \in F[x]$ אי פריק. $f \mid p$. אז f הפיך $\Leftarrow h$ הפיך $\Leftarrow f=p\cdot h^{-1}$ (הפיך)

$p=f\cdot h$

② $\gcd(p,g)$ $\begin{cases} p \\ 1 \end{cases}$

הוכחת הטענה הקודמת (ה"ז אי פריקות):

(1) נוכיח ע"י אינדוקציה על $n=\deg f$. $n=1 \Rightarrow f$ אי פריק.

$n \to n$. אם h אי פריק אז סיימנו. אחרת $f=g\cdot h$ כאשר $\deg g, \deg f<n$

$f=g\cdot h=p_1\cdots p_s q_1\cdots q_t \Leftarrow$ אי פריקים p_i, q_j , $h=q_1\cdots q_t$, $g=p_1\cdots p_s$ לפי הנ"ל

(2) יחידות: $f=p_1\cdots p_s=p'_1\cdots p'_t$ אי יחידות כך ש- s:

$s=1$: $p_1=p'_1\cdots p'_t$ נפסיק $(p'_2\cdots p'_t)$ אי $p_1 \mid p'_1$. אי $\gcd(p_1,p'_1)=1 \Leftarrow p_1 \nmid p'_1$.

תרגיל מחלקה 3:

המשך ההוכחה:

נניח ש $p_1, p_2, \dots, p_s$ ו $p'_1, p'_2, \dots, p'_t$ ראשוניים כך ש $p_1 \cdot \dots \cdot p_s = p'_1 \cdot \dots \cdot p'_t$.

נוכיח באינדוקציה על s.

בסיס: $s=1$. אז $p_1 = p'_1 \cdot \dots \cdot p'_t$. אם $t=1$ אז $p_1 = p'_1$ ואנחנו סיימנו. אחרת, $t>1$ ו p_1 מחלק מכפלה של t ראשוניים, ולכן $p_1 = p'_i$ עבור i כלשהו. אבל אז $p_1 \mid p'_1 \cdot \dots \cdot p'_t$ ולכן $p_1 = p'_1$ (כי p_1 ראשוני). אבל אז $p_1 = p'_1 \cdot \dots \cdot p'_t$ ולכן $t=1$.

צעד: נניח שהטענה נכונה עבור $s-1$. אז $p_1 \mid p'_1 \cdot \dots \cdot p'_t$ ולכן $p_1 \mid p'_i$ עבור i כלשהו. אבל אז $p_1 = p'_i$ (כי p_1 ראשוני). נסדר מחדש כך ש $p_1 = p'_1$.

אחרי הסידור שעשינו מתקיים $p_2 \cdot \dots \cdot p_s = p'_2 \cdot \dots \cdot p'_t$. לפי הנחת האינדוקציה $s-1 = t-1$ ולכן $s=t$.

$s \Rightarrow s+1$: נניח ש $p_1 \cdot \dots \cdot p_s \cdot p_{s+1} = p'_1 \cdot \dots \cdot p'_t$. כמו קודם, $p_{s+1} \mid p'_1 \cdot \dots \cdot p'_t$ ולכן $p_{s+1} = p'_i$ עבור i כלשהו. אחרי הסידור שעשינו מתקיים $p_s = p'_t$.

$p_1 \cdot \dots \cdot p_{s-1} \cdot p_s = p'_1 \cdot \dots \cdot p'_{t-1} \cdot p_s$

לפי הנ"ל קיבלנו את הנדרש.