משפט - יהיו $f,g\in F[x]$, כך שלפחות אחד מהם $\neq 0$.
אזי, קיים $d=\gcd(f,g)$. יתרה מזאת, קיימים $u,v\in F[x]\ (\mathbb{Z})$
כך ש- $d=fu+gv$

הוכחה - נתבונן בקבוצה: $X=\{h \mid h=fu+gv,\ h\neq 0\}$ * $X\neq\phi$
כי אז f שייך ל-X או $g\in X$.
יהי $d\in X$ מדרגה הכי נמוכה (בערך מוחלט הכי קטן), נוכיח
$d=\gcd(f,g)$.

$$d=fu_0+gv_0$$

תנאי (2) בהגדרה: נניח $c|f,\ c|g \Longrightarrow c|(fu+gv)$
לכל u,v. בפרט, $c|d$.
תנאי (1) נוכיח $d|f$. נחלק את f ב-d עם שארית:

$$f=q\cdot d+r$$

כאשר או $r=0$, או $\deg d>\deg r$
אם $r\neq 0$, אזי:

$$r=f-qd=f-q(fu_0+gv_0)=$$
$$=f(\underbrace{1-qu_0}_{\in F[x](\mathbb{Z})})+g(\underbrace{-qv_0}_{\in F[x](\mathbb{Z})})\in X$$

$\deg r<\deg d \rightarrow$ סתירה לבחירה של d.

לכן, $r=0 \rightarrow d|f$, באופן דומה $d|g$. $\Longleftarrow d=\gcd(f,g)$.
מש"ל.

משפט 2: $a,b,c\in F[x](\mathbb{Z})$:
(1) אם $\gcd(a,b)=1$ וגם $\gcd(a,c)=1$, אזי, $\gcd(a,bc)=1$
(2) אם $a|(bc)$ וגם $\gcd(a,b)=1$, אזי $a|c$
(3) אם $b|a$, וגם $c|a$, וגם $\gcd(b,c)=1$, אזי $(bc)|a$

הוכחה:

(1)

$$\begin{cases} au_1+bv_1=1 \\ au_2+cv_2=1 \end{cases} \rightarrow \text{נכפיל}$$

$$(au_1+bv_1)(au_2+cv_2)=1$$

$$a^2u_1u_2+au_1cv_2+bv_1au_2+bv_1cv_2$$

$$a\underbrace{(au_1u_2+cu_1v_2+bv_1u_2)}_{u_3}+(bv_1cv_2)=1$$

$$bv_1cv_2 = bc\underbrace{(v_1v_2)}_{v_3}$$

$$au_3+bcv_3=1$$

$$t=\gcd(a,bc)$$

$$t|a,\ t|(bc) \rightarrow t|(au_3+(bc)v_3)$$

$$t|1$$

$t \cdot s=1 \rightarrow t$ הפיך

$$\Downarrow$$

לכן, $\gcd(a,bc)=1$

(2) $au+bv=1$, נכפיל ב-c

$$auc+(bc)v=c$$

auc מתחלק ב-a.

$(bc)v$ מתחלק ב-a לפי הנתון.

לכן, $a|c$.

(3) $c|a=b\cdot f$

$$c|(b\cdot f) \rightarrow \gcd(c,b)=1 \xrightarrow{(2)} c|f.$$

$$f=c\cdot g$$

$$a=b\cdot c\cdot g$$

$$\Downarrow$$

$(bc)|a$ מש"ל.