Tétel. *Legyen $f \in \mathbb{Z}[x]$ egy tetszőleges n-edfokú polinom ($n \geq 1$). Ekkor az alábbi két állítás ekvivalens:*

(1) $\exists u, v \in \mathbb{Z}[x] : f = u \cdot v$ *és* $0 < \deg u, \deg v < n$;
(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ *és* $0 < \deg g, \deg h < n$.

Biz. Az világos, hogy (1) $\implies$ (2). A másik irány bizonyításához

(a) tegyük fel, hogy (2) teljesül, azaz $f = g \cdot h$, ahol $g, h \in \mathbb{Q}[x]$ és

(b) $0 < \deg g, \deg h < n$.

(c) Léteznek olyan $g^*, h^* \in \mathbb{Z}[x]$ polinomok és $r, s \in \mathbb{Q}$, amelyekre $g = r \cdot g^*,\ h = s \cdot h^*$,

(d) és g^*, h^* primitív polinomok. ..... □

(e) Legyen $rs = \frac{p}{q}$, ahol $p \in \mathbb{Z}, q \in \mathbb{N}$, és

(f) $\text{lnko}(p, q) = 1$.

(g) Az $f = gh$ egyenlőségbe behelyettesítve a fentieket kapjuk, hogy $q \cdot f = p \cdot g^* h^*$.

(h) Meg fogjuk mutatni, hogy $q = 1$.

(i) Legyen $g^* h^* = \sum_{i=0}^{n} a_i x^i$; erről a polinomról tudjuk, hogy primitív. ..... □

(j) Minden $i \in \{0, \ldots, n\}$ esetén $q \mid p \cdot a_i$, ... □

(k) és ebből következik, hogy $q \mid a_i$ minden i-re. ..... □

(l) Ezért csak $q = 1$ lehetséges, ... □

(m) tehát $f = pg^* \cdot h^*$.

(n) Ebben a felbontásban mindkét polinom egész együtthatós, ... □

(o) és $0 < \deg pg^*, \deg h^* < n$. ..... □

(p) Tehát az $u = pg^*$, $v = h^*$ polinomok mutatják, hogy (1) teljesül, és épp ezt kellett bizonyítanunk.

□