Megoldás. Ha p és q is felcserélhető f-fel, akkor $p \circ q$ is felcserélhető f-fel, ugyanis

$$\big((p \circ q) \circ f\big)(x) = p\big(q\big(f(x)\big)\big) = p\big(f\big(q(x)\big)\big) = f\big(p\big(q(x)\big)\big) = \big(f \circ (p \circ q)\big)(x)$$

teljesül minden x-re, amiből következik, hogy a $(p \circ q) \circ f$ polinom azonos az $f \circ (p \circ q)$ polinommal. Ugyanez igaz természetesen a $q \circ p$ polinomra is. Vegyük észre, hogy ha a $p(x)$ polinom foka n, a $q(x)$-é pedig m, akkor mind a $p \circ q$, mind a $q \circ p$ polinom foka nm. Elegendő tehát belátni a következő állítást: tetszőleges k pozitív egészhez legfeljebb egy olyan $r(x)$ k-ad fokú polinom van, amely f-fel felcserélhető.

Állításunk igazolásához keressük az r polinomot

$$r(x) = r_k x^k + r_{k-1} x^{k-1} + \ldots + r_1 x + r_0$$

alakban, ahol $r_k \neq 0$. Legyen $f(x) = ax^2 + bx + c$, ahol $a \neq 0$. Az r polinom pontosan akkor felcserélhető f-fel, ha

$$\begin{aligned} a(r_k x^k + r_{k-1} x^{k-1} + \ldots + r_0)^2 + b(r_k x^k + r_{k-1} x^{k-1} + \ldots + r_0) + c = \\ = r_k (ax^2 + bx + c)^k + r_{k-1} (ax^2 + bx + c)^{k-1} + \ldots + r_0. \end{aligned}$$

Mindkét oldalon egy $2k$-ad fokú polinom áll. A két polinomban x^{2k} együtthatóját összehasonlítva az $ar_k^2 = r_k a^k$ összefüggésre jutunk, ahonnan $r_k = a^{k-1}$. Ha valamilyen $0 \leq i < k$ esetén az $r_k, r_{k-1}, \ldots, r_{k-i}$ együtthatókat már meghatároztuk, akkor r_{k-i-1} is egyértelműen meghatározható, ha a két polinomban összehasonlítjuk x^{2k-i-1} együtthatóját. Valóban, a második polinomban ez az együttható, t_{2k-i-1} kifejezhető az a, b, c számok és a már meghatározott r_{k-j} $(j \leq i)$ együtthatók segítségével, azok valamilyen többváltozós polinomjaként, míg az első polinomban a megfelelő együttható az a, b, c és r_{k-j} $(j \leq i+1)$ együtthatók $s_{2k-i-1} + 2ar_k r_{k-i-1}$ polinomjaként írható fel, ahol s_{2k-i-1}-ben is csak már eddig meghatározott együtthatók szerepelnek. Így a

$$t_{2k-i-1} = s_{2k-i-1} + ar_k r_{k-i-1}$$

összefüggés alapján r_{k-i-1} valóban meghatározható. Ilyen módon az $r(x)$ polinom valamennyi együtthatóját meghatározhatjuk, melyeknek még k további összefüggést is ki kell elégíteniük. Ezért az $r(x)$ polinom vagy egyértelműen meghatározható, vagy pedig nem létezik, és éppen ezt akartuk igazolni.