Endliche Körper.

Vorbemerkung: Ist k ein Körper der Charakteristik p, so ist die durch $x \mapsto x^p$ definierte Abbildung $k \to k$ ein Ring-Homomorphismus, insbesondere injektiv (da ja k ein Körper ist). Man nennt diese Abbildung den *Frobenius-Homomorphismus.*

Satz. *Ist k ein Körper der Charakteristik p und ist der Frobenius-Homomorphismus surjektiv, so ist jedes irreduzible Polynom $f \in k[X]$ separabel.*

Beweis. Angenommen, es gibt ein irreduzibles Polynom $f \in k[X]$, das nicht separabel ist. Sei $n = \operatorname{grad} f$. Da f nicht sepearabel ist, haben f und die formale Ableitung f' eine gemeinsame Nullstelle (im algebraischen Abschluss von k). Ist h der größte gemeinsame Teiler von f, f', so ist demnach $\operatorname{grad} h \geq 1$. Da f irreduzibel und h ein Teiler von f ist, folgt $f = h$. Nun ist aber $\operatorname{grad} f' \leq n - 1$. Da h ein Teiler von f' ist, folgt $f' = 0$. Schreiben wir $f(X) = \sum_{i=0}^{n} c_i X^i$, so ist $f'(X) = \sum_{i=1}^{n} i c_i X^{i-1}$, also sehen wir: $ic_i = 0$ für $1 \leq i \leq n$. Demnach gilt: Ist p kein Teiler von i, so ist $c_i = 0$.

Wir setzen

$$g(X) = \sum\nolimits_{j=0}^{n/p} d_j X^j, \quad \text{mit} \quad {d_j}^p = c_{jp},$$

(hier verwenden wir die Surjektivität des Frobenius-Homomorphismus, um aus c_{jp} eine p-te Wurzel zu ziehen). Es ist

$$g(X)^p = (\sum\nolimits_j d_j X^j)^p = \sum\nolimits_j {d_j}^p X^{jp} = \sum\nolimits_j c_{jp} X^{jp} = f(X).$$

Wir erhalten einen Widerspruch zur Irruduzibilität von f.

Folgerung. *Ist k ein endlicher Körper, so ist jedes irreduzible Polynom $f \in k[X]$ separabel.*

Beweis: Als endlicher Körper hat k Charakteristik $p > 0$. Der entsprechende Frobenius-Homomorphismus ist eine injektive Abbildung einer endlichen Menge in sich, also surjektiv.