Exkurs: Zur Irreduzibilität der Polynome $x^n - a$

Sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Die Irreduzibilität des Polynoms $x^n - a \in K[x]$ lässt sich einfach charakterisieren:

Satz. *Sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Dann sind folgende Aussagen (1) und (2) äquivalent:*

(1) *$x^n - a \in K[x]$ ist irreduzibel.*
(2) *Für alle Primteiler p von n ist $a \notin K^p$ und zusätzlich $a \notin (-4) \cdot K^4$ im Fall $4 \mid n$. (Dabei ist $K^p = \{c^p : c \in K\}$ und $(-4) \cdot K^4 = \{-4c^4 : c \in K\}$.)*

Die Beweisrichtung (2) $\Longrightarrow$ (1) braucht einige Vorbereitungen.

Lemma (Ap). *Sei K ein Körper, p eine ungerade Primzahl, $a \in \overline{K}$ mit*

$$a \notin K(a)^p.$$

Sei $b \in \overline{K}$ mit $b^p = a$. Dann gilt:

(1) $K(a) \subseteq K(b)$.
(2) $[K(b) : K(a)] = p$.
(3) $\mathrm{N}_{K(b)|K(a)}(b) = a$.
(4) $b \notin K(b)^p$.

Beweis:

(1) Wegen $a = b^p$ gilt $a \in K(b)$, und damit $K(a) \subseteq K(b)$.
(2) Sei $d = [K(b) : K(a)]$. Da b Nullstelle des Polynoms $x^p - a \in K(a)[x]$ ist, gilt $d \le p$. Aus $b^p = a$ folgt durch Normbildung
$$\mathrm{N}_{K(b)|K(a)}(b)^p = a^d.$$
Wäre $d < p$, so wäre $\mathrm{ggT}(p, d) = 1$, es gäbe also $u, v \in \mathbb{Z}$ mit $up + vd = 1$. Dies würde
$$a = a^{up+vd} = (a^u)^p \cdot (a^d)^v = (a^u)^p \cdot (\mathrm{N}_{K(b)|K(a)}(b)^p)^v = \left(a^u \cdot \mathrm{N}_{K(b)|K(a)}(b)^v\right)^p$$
implizieren, also $a \in K(a)^p$, im Widerspruch zur Voraussetzung. Also ist $d = p$, wie behauptet.
(3) Wegen $b^p = a$ und $[K(b) : K(a)] = p$ ist $x^p - a \in K(a)[x]$ das Minimalpolynom von b über $K(a)$. Es stimmt mit dem charakteristischen Polynom von b über $K(a)$ überein. Das charakteristische Polynom ist
$$\begin{aligned} \chi_{b,K(a)}(x) &= x^p - \mathrm{Sp}_{K(b)|K(a)}(b)x^{p-1} + \cdots + (-1)^p \mathrm{N}_{K(b)|K(a)}(b) \overset{p \text{ ungerade}}{=} \\ &= x^p - \mathrm{Sp}_{K(b)|K(a)}(b) + \cdots - \mathrm{N}_{K(b)|K(a)}(b). \end{aligned}$$
Aus $x^p - a = \chi_{b,K(a)}(x)$ folgt sofort $\mathrm{N}_{K(b)|K(a)}(b) = a$.
(4) Wäre $b \in K(b)^p$, so gäbe es ein $c \in K(b)$ mit $b = c^p$. Mit (3) folgt
$$a = \mathrm{N}_{K(b)|K(a)}(b) = \mathrm{N}_{K(b)|K(a)}(c)^p, \quad \text{also} \quad a \in K(a)^p,$$
ein Widerspruch zur Voraussetzung. Also gilt $b \notin K(b)^p$, wie behauptet. ■

Im Fall $p = 2$ stimmen die Aussagen (3) und (4) vor Lemmas Ap im Allgemeinen nicht. Daher muss das Lemma etwas modifiziert werden.

Lemma (A2). *Sei K ein Körper, $a \in \overline{K}$ mit*

$$a \notin K(a)^2 \quad \textit{und} \quad a \notin (-4) \cdot K(a)^4.$$

Sei $b \in \overline{K}$ mit $b^2 = a$. Dann gilt:

(1) $K(a) \subseteq K(b)$.
(2) $[K(b) : K(a)] = 2$.
(3) $\mathrm{N}_{K(b)|K(a)}(b) = -a$.
(4) $b \notin K(b)^2$.

---

(5) $b \notin (-4) \cdot K(b)^4$.

Beweis:

(1) Wegen $b^2 = a$ gilt $a \in K(b)$ und damit $K(a) \subseteq K(b)$.

(2) Da a kein Quadrat in $K(a)$ ist, besitzt das Polynom $x^2 - a \in K(a)[x]$ keine Nullstelle, ist also irreduzibel. Nun ist b eine Nullstelle des Polynoms. Daher ist das Polynom das Minimalpolynom von b über $K(a)$, woraus sofort
$$[K(b) : K(a)] = 2$$
folgt.

(3) $1, b$ ist eine $K(a)$-Basis von $K(b)$. Wegen
$$b \cdot \begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} b \\ b^2 \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \begin{pmatrix} 1 \\ b \end{pmatrix}$$
ist
$$\mathrm{N}_{K(b)|K(a)}(b) = \det \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} = -a.$$

(4) *Annahme:* Es ist $b \in K(b)^2$. Wegen $[K(b) : K(a)] = 2$ ist $1, b$ eine $K(a)$-Basis von $K(b)$, es gibt also $u, v \in K(a)$ mit
$$b = (u + vb)^2.$$
Multipliziert man den Ausdruck aus, so ergibt sich
$$b = (u^2 + v^2 a) + 2uvb,$$
sodass Koeffizientenvergleich die Gleichungen
$$1 = 2uv \quad \text{und} \quad u^2 + v^2 a = 0$$
liefert. Die erste Gleichung liefert $v = \frac{1}{2u}$, die zweite damit
$$a = -\frac{u^2}{v^2} = -u^2 \cdot (\frac{1}{v})^2 = -u^2 \cdot (2u)^2 = -4u^4.$$
Dies widerspricht aber der Voraussetzung $a \notin (-4) \cdot K(a)^4$. Die Annahme war also falsch, es gilt also $b \notin K(b)^2$, wie behauptet.

(5) *Annahme:* $b \in (-4) \cdot K(b)^4$. Dann gibt es ein $c \in K(b)$ mit $b = -4c^4$. Normbildung liefert mit $\mathrm{N}_{K(b)|K(a)}(b) = -a$
$$-a = \mathrm{N}_{K(b)|K(a)}(b) = \mathrm{N}_{K(b)|K(a)}(-4c^4) = 16\mathrm{N}_{K(b)|K(a)}(c)^4,$$
damit
$$-1 = \frac{16\mathrm{N}_{K(b)|K(a)}(c)^4}{a},$$
also (mit $a = b^2$)
$$b = -4c^4 = \frac{16\mathrm{N}_{K(b)|K(a)}(c)^4}{a} \cdot 4c^4 = \left(\frac{8\mathrm{N}_{K(b)|K(a)}(c)^2 \cdot c^2}{b} \right)^2.$$
Dies steht aber im Widerspruch zur Aussage, die wir gerade in (4) gezeigt haben. Die Annahme war also falsch, es gilt daher $b \notin (-4) \cdot K(b)^4$, wie behauptet. ■

Lemma (B). *Sei K ein Körper, $a \in K$ und p eine Primzahl. Wir setzen voraus:*

- *$a \notin K^p$ im Fall $p > 2$,*
- *$a \notin K^2$ und $a \notin (-4) \cdot K^4$ im Fall $p = 2$.*

Wir definieren rekursiv eine Folge $(a_i)_{i \geq 0}$ mit $a_i \in \overline{K}$ wie folgt: Es sei $a_0 = a$. Ist a_i bereits definiert, so wählen wir ein Element $a_{i+1} \in \overline{K}$ mit $a_{i+1}^p = a_i$. Zusammengefasst:
$$a_0 = a, \quad a_{i+1}^p = a_i \text{ für } i \geq 0.$$
(Die Folge $(a_i)_{i \geq 0}$ ist dadurch nicht eindeutig bestimmt.) Dann gilt:

(1) • *$a_i \notin K(a_i)^p$ im Fall $p > 2$,*

- $a_i \notin K(a_i)^2$ *und* $a_i \notin (-4) \cdot K(a_i)^4$ *im Fall* $p = 2$.

(2) $[K(a_{i+1}) : K(a_i)] = p$.
(3) $[K(a_i) : K] = p^i$.
(4) *Das Polynom* $x^{p^i} - a \in K[x]$ *ist irreduzibel für alle* $i \in \mathbb{N}$.

Beweis:

(1) Wir beweisen die Aussage durch Induktion.
- *Induktionsanfang:* Dies ist genau die Voraussetzung, die wir für $a_0 = a$ gefordert haben.
- *Induktionsvoraussetzung:* Wir setzen nun voraus, dass für i die Aussage stimmt, d.h.
$$a_i \notin K(a_i)^p \text{ und zusätzlich } a_i \notin (-4) \cdot K(a_i)^4 \text{ im Fall } p = 2.$$
- *Induktionsschluss:* Aus den Lemmas Ap und A2 folgt dann sofort
$$a_{i+1} \notin K(a_{i+1})^p \text{ und zusätzlich } a_{i+1} \notin (-4) \cdot K(a_{i+1})^4 \text{ im Fall } p = 2.$$

Damit ist die Behauptung durch Induktion bewiesen.

(2) Dies steht in den Lemmas Ap und A2.
(3) Dies folgt sofort aus (2):
$$[K(a_i) : K] = [K(a_i) : K(a_{i-1})] \cdot [K(a_{i-1}) : K(a_{i-2})] \cdot \dots \cdot [K(a_1) : K(a_0)] = p^i.$$
(4) a_i ist Nullstelle des Polynoms $x^{p^i} - a$. Da a_i nach (3) Grad p^i hat, hat das Minimalpolynom von a_i über K Grad p^i. Daher ist $x^{p^i} - a$ das Minimalpolynom von a_i über K. Da Minimalpolynome irreduzibel sind, ist $x^{p^i} - a \in K[x]$ irreduzibel. ■

Wir können nun die Richtung (2) $\Longrightarrow$ (1) unseres Satzes beweisen. Wir schreiben die Aussage nochmals auf:

Satz ((2) $\Longrightarrow$ (1)). *Sei* K *ein Körper,* $a \in K$ *und* $n \in \mathbb{N}$ *mit der Eigenschaft*
$$a \notin K^p \text{ für alle Primteiler } p \text{ von } n$$
und zusätzlich
$$a \notin (-4) \cdot K^4 \text{ im Fall } 4 \mid n.$$
Dann ist $x^n - a \in K[x]$ *irreduzibel.*

Beweis: Sei
$$n = p_1^{e_1} \dots p_r^{e_r}$$
die Primfaktorzerlegung von n. Sei $\alpha \in \overline{K}$ eine Nullstelle des Polynoms $x^n - a$. Dann ist $\alpha^n = a$, und damit für alle $i \in \{1, \dots, r\}$
$$\left(\alpha^{\frac{n}{p_i^{e_i}}}\right)^{p_i^{e_i}} = a.$$
Das Element $\alpha^{\frac{n}{p_i^{e_i}}}$ ist also Nullstelle des Polynoms $x^{p_i^{e_i}} - a \in K[x]$.

- In den Fällen $p_i > 2$ und $p_i = 2, e_2 \geq 2$ ist das Polynom $x^{p_i^{e_i}} - a$ irreduzibel nach dem letzten Lemma.
- Im Fall $p_i = 2, e_i = 1$ ist das Polynom $x^2 - a$ irreduzibel wegen $a \notin K^2$. (Hierfür braucht man die Voraussetzung $a \notin (-4) \cdot K^4$ nicht.)

Daher ist $x^{p_i^{e_i}} - a$ das Minimalpolynom von $\alpha^{\frac{n}{p_i^{e_i}}}$ über K, sodass
$$[K(\alpha^{\frac{n}{p_i^{e_i}}}) : K] = p_i^{e_i}$$
folgt.
Da die Grade $[K(\alpha^{\frac{n}{p_i^{e_i}}}) : K] = p_i^{e_i}$ paarweise teilerfremd sind, gilt
$$K(\alpha^{\frac{n}{p_1^{e_1}}}, \dots, \alpha^{\frac{n}{p_r^{e_r}}}) : K] = p_1^{e_1} \dots p_r^{e_r} = n.$$
Wegen $K(\alpha^{\frac{n}{p_1^{e_1}}}, \dots, \alpha^{\frac{n}{p_i^{e_r}}}) \subseteq K(\alpha)$ folgt
$$[K(\alpha) : K] \geq n.$$

Da aber α Nullstelle von $x^n - a$ ist, gilt natürlich auch $[K(\alpha) : K] \leq n$. Zusammen ergibt sich

$$[K(\alpha) : K] = n.$$

Dann ist aber $x^n - a$ das Minimalpolynom von α über K, also irreduzibel. ■

Die Umkehrung des Satzes ist einfacher:

Satz ((1) $\Longrightarrow$ (2) bzw. nicht (2) impliziert nicht (1)). *Sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$.*

(1) *Ist p ein Primteiler von n und $a \in K^p$, d.h. $a = c^p$ für ein $c \in K$, so ist $x^{\frac{n}{p}} - c$ ein Teiler von $x^n - a$, insbesondere ist $x^n - a$ reduzibel.*

(2) *Im Fall $4 \mid n$ und $a \in (-4) \cdot K^4$, d.h. $a = -4c^4$ für ein $c \in K$, gilt*

$$x^n - a = (x^{\frac{n}{2}} + 2cx^{\frac{n}{4}} + 2c^2)(x^{\frac{n}{2}} - 2cx^{\frac{n}{4}} + 2c^2),$$

insbesondere ist $x^n - a$ reduzibel.

Beweis:

(1) Wir schreiben $n = pm$ und $a = c^p$. Setzen wir in die Zerlegung

$$y^p - z^p = (y - z)(y^{p-1} + y^{p-2}z + \cdots + yz^{p-2} + z^{p-1})$$

$y = x^m$ und $z = c$ ein, so erhalten wir

$$(x^m)^p - c^p = (x^m - c)((x^m)^{p-1} + \cdots + c^{p-1}),$$

also

$$x^n - a = (x^{\frac{n}{p}} - c)(x^{m(p-1)} + \cdots + c^{p-1}),$$

was die Behauptung beweist.

(2) Wir schreiben $n = 4m$ und $a = -4c^4$. Es gilt

$$y^4 + 4c^4 = (y^2 + 2cy + 2c^2)(y^2 - 2cy + 2c^2).$$

Setzen wir $y = x^m$ und $a = -4c^4$ ein, so ergibt sich

$$x^n - a = (x^{2m} + 2cx^m + 2c^2)(x^{2m} - 2cx^m + 2c^2),$$

also

$$x^n - a = (x^{\frac{n}{2}} + 2cx^{\frac{n}{4}} + 2c^2)(x^{\frac{n}{2}} - 2cx^{\frac{n}{4}} + 2c^2),$$

wie behauptet. ■

Damit ist der zu Beginn angegebene Satz bewiesen.