zu (c) und (d): zu zeigen ist nur (d), (c) folgt aus $n = \mathrm{grad}(f)$.

(i) $1, a^1, \dots, a^{n-1}$ erzeugen $K(a) = K[a]$:

- Sei $r \in K(a) = K[a]$. Dann ex. $p \in K[X]$ mit $r = p(a)$. Mit eukl. Alg. ex. $q, r_1 \in K[X]$ mit $\mathrm{grad}(r_1) < \mathrm{grad}(f)$ und $p = q \cdot f + r_1$.
- Also gilt: $r = p(a) = q(a) \cdot \underbrace{f(a)}_{=0} + r_1(a) = r_1(a)$.

D.h. $r = r_1(a) = \lambda_0 + \lambda_1 \cdot a + \dots + \lambda_m a^m$

mit $m = \mathrm{grad}(r_1) < \mathrm{grad}(f) = n$; insbes. $m \leq n-1$.

(ii) $1, a^1, \dots, a^{n-1}$ sind lin. unabh.:

- Sei $\lambda_0 + \lambda_1 a^1 + \dots + \lambda_{n-1} a^{n-1} = 0$ mit $\lambda_i \in K$.
- Für $p = \lambda_0 + \lambda_1 X + \dots + \lambda_{n-1} X^{n-1} \in K[X]$ ist dann $p(a) = 0$. D.h. $p \in \ker(\varphi_a) = (f) = \{g \cdot f : g \in K[X]\}$.
- Ist $p \neq 0$, so ist $\mathrm{grad}(p) \geq \mathrm{grad}(f) = n$.
- Weil aber $\mathrm{grad}(p) = n-1 < n$ gilt $p = 0$, d.h. $\lambda_i = 0$ (für $0 \leq i \leq n-1$) und $1, a^1, \dots, a^{n-1}$ sind lin. unabh. $\dashv$

<u>Satz 14.4</u> Seien K, K' Körper und $\varphi: K \to K'$ ein Körperisomorphismus. Seien $L : K$, $L' : K'$ Körpererweiterungen, $a \in L$, $a' \in L'$, wobei gilt:

entweder (a) a ist transzendent über K und

a' ———— " ———— K',

oder (b) es ex. ein irred. Polynom $f \in K[X]$ mit $f(a) = 0$ und $(\varphi f)(a') = 0$.

Dann gilt: Es ex. ein Isom. $\tilde{\varphi} : K(a) \xrightarrow{\sim} K'(a')$ mit $\tilde{\varphi}(a) = a'$ und $\tilde{\varphi}|_K = \varphi$.

<u>Beweis:</u> Der Isom. $\varphi: K \xrightarrow{\sim} K'$ lässt sich erweitern zu einem Isom. $\varphi: K[X] \xrightarrow{\sim} K'[X]$, dieser lässt sich heben zu $\varphi: K(X) \xrightarrow{\sim} K'(X)$.

zu (a): Mit Satz 14.2 ist $K(a) \cong K(X)$, $K'(a') \cong K'(X)$,
also $K(a) \cong K(X) \xrightarrow{\sim} K'(X) \cong K'(a')$.

zu (b): OBdA sei f normiert, also Minimalpolynom von a.
- Dann ist auch φf normiert und irred., also ist φf Minimalpolynom von a'.

$K \xrightarrow[\varphi]{\sim} K' \hookrightarrow K'[a'] = K'(a')$ lässt sich heben zu
$K[X] \xrightarrow[\bar\varphi]{} K'[a']$ mit $\bar\varphi|_K = \varphi$ und $\bar\varphi(X) = a'$.
[universelle Eigenschaft 12.3]

- $\ker(\bar\varphi) = \{p \in K[X] : (\varphi p)(a') = 0\} = (f)$
da $(\varphi f)(a') = 0$.
- Somit gilt:

$$\begin{tikzcd} K(a) \arrow[r, "\cong", "\text{Satz 14.3}"'] \arrow[rr, bend right, "\tilde\varphi"'] & K[X]/(f) \arrow[r, "\sim"] & K'(a') \end{tikzcd}$$

$\dashv$

<u>Folgerung 14.5</u> Sind $L:K$ und $M:K$ Körpererweiterungen, $a \in L$, $b \in M$ beide alg. über K, dann gilt:
a, b besitzen dasselbe Minimalpolynom $\Longleftrightarrow$ es ex. Isom. $\varphi: K(a) \xrightarrow{\sim} K(b)$ mit $\varphi(a) = b$ und $\varphi|_K = \mathrm{id}$.

<u>Beweis:</u> ($\Rightarrow$) klar; folgt direkt aus Satz 14.4.

($\Leftarrow$) $\varphi: K(a) \to K(b)$ mit $\varphi(a) = b$ und $\varphi|_K = \mathrm{id}$.
- Sei f Minimalpolynom von a, g Minimalpol. von b.
- $f = a_0 + a_1 X + \ldots + X^n \in K[X]$

$0 = a_0 + a_1 \cdot a + \ldots + a^n \in K(a)$

$0 = \varphi(0) = \varphi(f(a)) = \varphi(a_0 + a_1 \cdot a + \ldots + a^n) = a_0 + a_1 \cdot b + \ldots + b^n$

$\Rightarrow f(b) = 0 \Rightarrow f \in (g) \Rightarrow g \mid f \Rightarrow g = f$
weil f irreduzibel ist.

$\dashv$

Satz 14.6 Sei K ein Körper und $f \in K[X]$ mit $\operatorname{grad}(f) = n \geq 1$. Dann ex. eine einfache Erweiterung $L = K(a)$ von K mit:

(a) a ist Nullstelle von f.

(b) $[K(a):K] \leq n$; $[K(a):K] = n$ gdw. f ist irred.

(c) Ist f irred., so ist L eindeutig bis auf Isomorphien welche eingeschränkt auf K die Identität sind.

Beweis: (c) folgt aus Folgerung 14.5.

Fall I f ist irreduzibel.

- Dann ist (f) max. Ideal und $K[X]/(f)$ ist ein Körper.
- Sei $\pi : K[X] \longrightarrow K[X]/(f) =: L$

$$X \longmapsto \bar{X} =: a$$ (Adjunktion einer symbolischen Nullstelle)

- $\bar{X} = X + (f)$ nach Definition.

$a_n \bar{X}^n = a_n (X + (f))^n = a_n X^n + (f)$, und somit ist für $f = a_0 + a_1 X + \ldots + a_n X^n$: $f(\bar{X}) = a_0 + a_1 \bar{X} + \ldots + a_n \bar{X}^n =$

$$a_0 + a_1 X + (f) + \ldots + a_n X^n + (f) =$$

$$\underbrace{a_0 + a_1 X + \ldots + a_n X^n}_{=f} + (f) = (f) = 0 \in L.$$

D.h. $f(\bar{X}) = f(a) = 0$.

- $K \cong \pi[K] \subseteq L$ und a ist alg. über K.
- Ist nun, ohne Einschränkung, f normiert, so ist f Minimalpolynom von a über K.
- Also ist $[K(a):K] = n$ $(= \operatorname{grad} f)$.

Fall II Ist f zerlegbar, so ist $f = \varepsilon \cdot f_1 \cdot \ldots \cdot f_r$ mit $\varepsilon \in K$ und f_i irred. über K.

- Mit Fall I ex. einfache Erweiterung $K(a)$ von K mit $f_1(a) = 0$ und $[K(a):K] = \operatorname{grad}(f_1) < \operatorname{grad}(f) = n$. $\dashv$