Definition der Radikalerweiterungen

Definition (24.3)

Eine Radikalerweiterung ist eine endliche Körpererweiterung $L|K$ mit folgenden Eigenschaften: Es gibt ein $r \in \mathbb{N}_0$, eine Kette von Zwischenkörpern

$$K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = L \ ,$$

natürliche Zahlen $n_1, \ldots, n_r$ und für $1 \leq i \leq r$ Elemente $\gamma_i \in L_i$, so dass jeweils $L_i = L_{i-1}(\gamma_i)$ und $\gamma_i^{n_i} \in L_{i-1}$ erfüllt ist.

Auflösbarkeit eines Polynoms durch Radikale

Definition (24.4)

Man sagt, ein nicht-konstantes Polynom $f \in K[x]$ ist durch Radikale auflösbar, wenn eine Radikalerweiterung $L|K$ existiert, so dass f über L in Linearfaktoren zerfällt.

Hinreichendes Kriterium für die Auflösbarkeit

Satz (24.5)

Sei $f \in K[x]$ ein nicht-konstantes Polynom mit auflösbarer Galoisgruppe $G = \mathrm{Gal}(f|K)$. Dann ist f durch Radikale auflösbar.

Das Kompositum normaler Erweiterungen

Lemma (24.6)

Seien $L_1|K$ und $L_2|K$ zwei normale Erweiterungen desselben Körpers K.

- Dann ist auch die Erweiterung $L_1 \cap L_2|K$ normal.
- Sind L_1 und L_2 in einem gemeinsamen Erweiterungskörper M enthalten, dann ist auch $L_1 \cdot L_2|K$ eine normale Erweiterung, wobei $L_1 \cdot L_2$ das Kompositum von L_1 und L_2 in M bezeichnet.

Eigenschaften von Radikalerweiterungen

Proposition (24.7)

(i) Sei $L|K$ eine Radikalerweiterung, $\tilde{K}$ ein algebraischer Abschluss von K und $\sigma : L \to \tilde{K}$ ein K-Homomorphismus. Dann ist auch $\sigma(L)|K$ eine Radikalerweiterung.

(ii) Ein Kompositum zweier Radikalerweiterungen ist eine Radikalerweiterung.

(iii) Ist $L|K$ eine separable Radikalerweiterung, so gibt es einen Erweiterungskörper M von L mit der Eigenschaft, dass $M|K$ eine Galois-Erweiterung und zugleich eine Radikalerweiterung ist.

„Radikalerweiterung $\Rightarrow$ auflösbare Gruppe“

Proposition (24.8)

Ist $L|K$ eine galoissche Radikalerweiterung, dann ist $G = \mathrm{Gal}(L|K)$ eine auflösbare Gruppe.

Satz (24.9)

Sei $f \in K[x]$ ein nicht-konstantes, durch Radikale auflösbares Polynom. Dann ist $\mathrm{Gal}(f|K)$ eine auflösbare Gruppe.

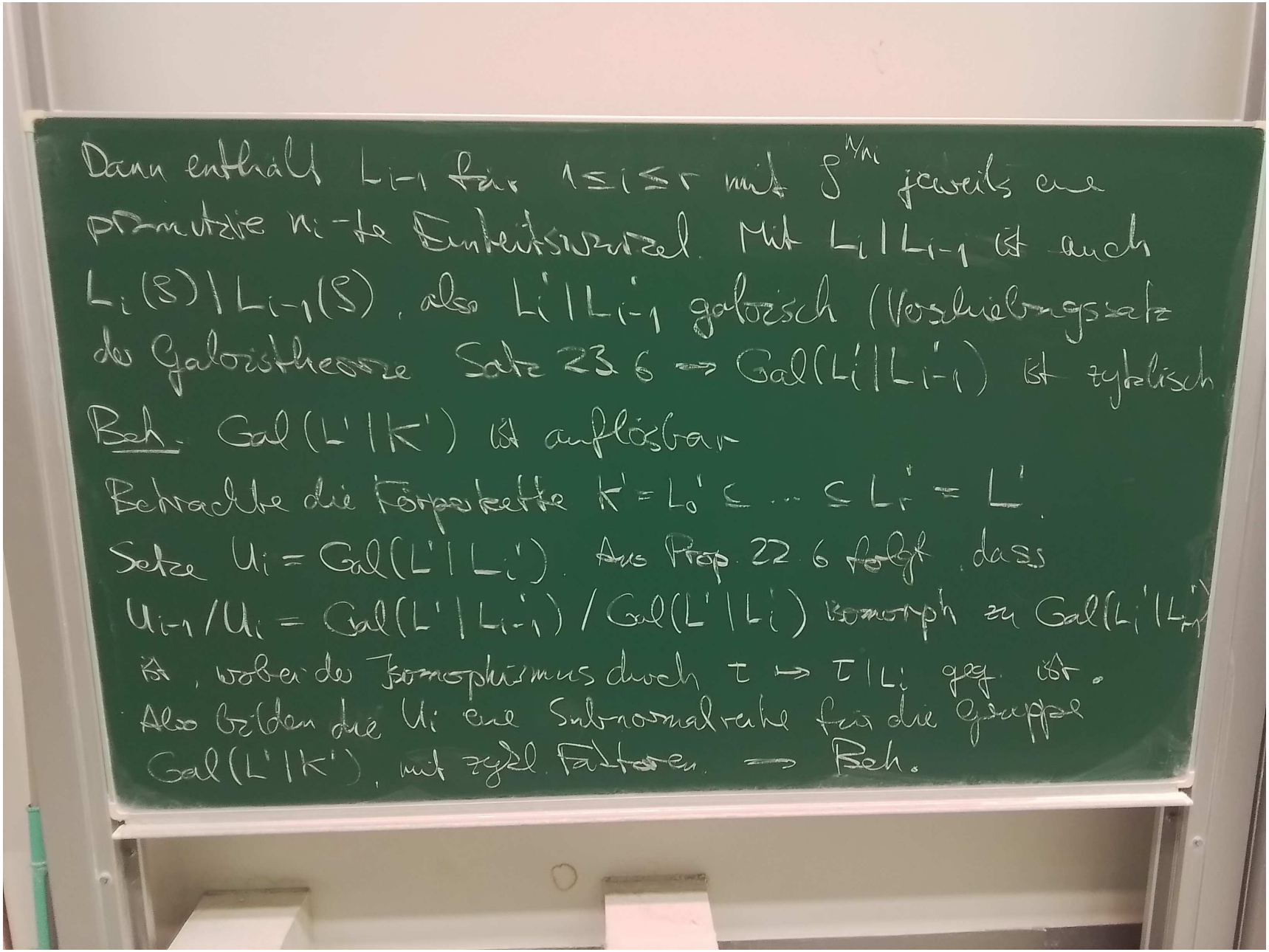
Beweis von Prop. 24.8:

geg.: eine galois'sche Radikalerweiterung $L|K$

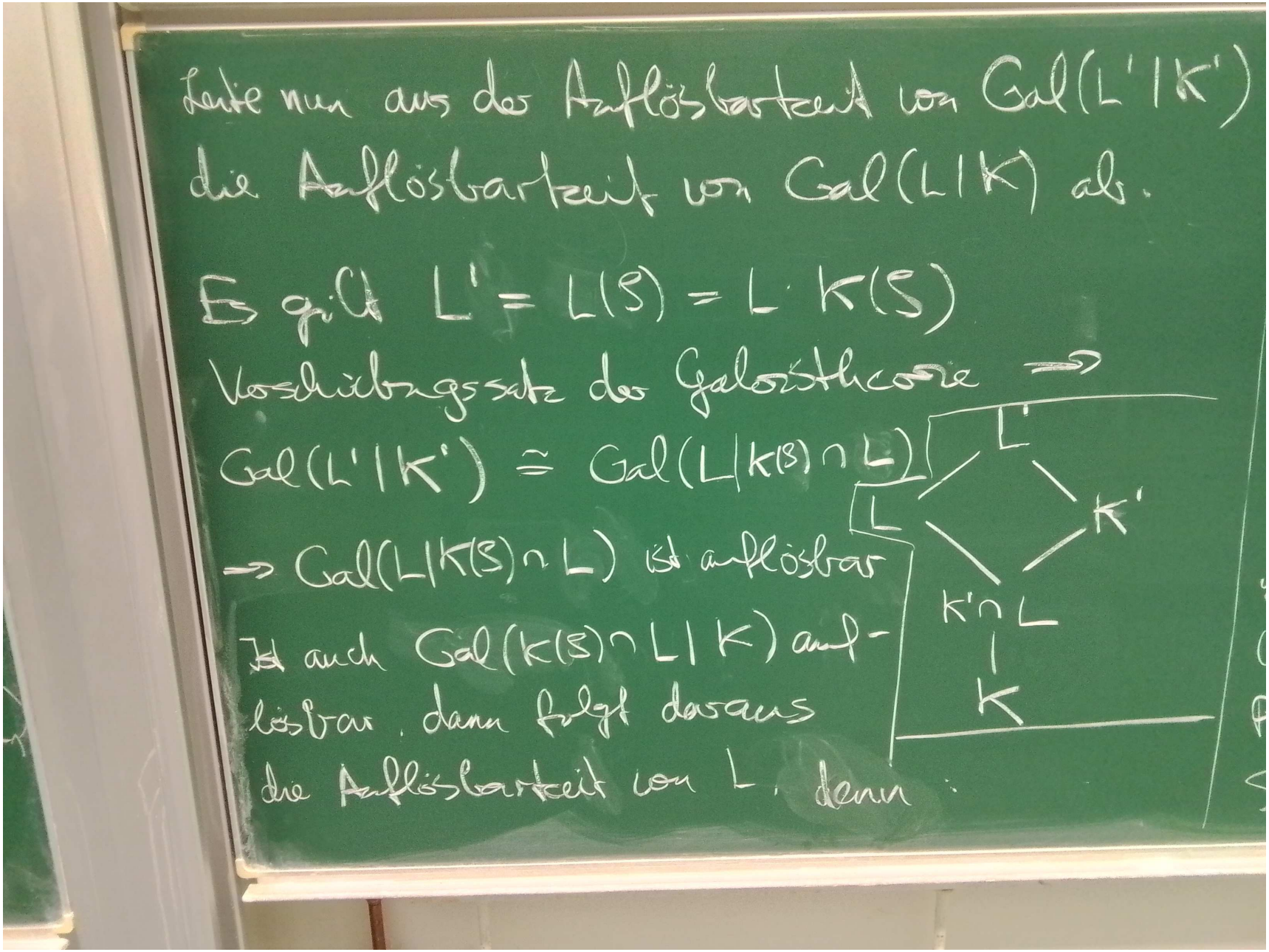
z.zg.: $G = \mathrm{Gal}(L|K)$ ist auflösbar

Vor $\Rightarrow$ Es gibt eine Körperkette $K = L_0 \subseteq \dots \subseteq L_r = L$, Elemente $\gamma_1, \dots, \gamma_r \in L$ und Zahlen $n_1, \dots, n_r \in \mathbb{N}_0$, so dass $L_i = L_{i-1}(\gamma_i)$ und $\gamma_i^{n_i} \in L_{i-1}$ für $1 \leq i \leq r$ erfüllt ist.

Sei $n = \mathrm{kgV}(n_1, \dots, n_r)$, $\tilde{L}$ ein alg. Abschluss von L und $\zeta \in \tilde{L}$ eine primitive n-te Einheitswurzel. Setze $K' = K(\zeta)$, $L' = L(\zeta)$, $L_i' = L_i(\zeta)$ für $0 \leq i \leq r$.



Korrektur erste Zeile: Dann enthält L_i' für $1 \leq i \leq r$...



Korrektur letzte Zeile: ersetze L durch G

Es ist $G = \mathrm{Gal}(L|K)$, setze

$N = \mathrm{Gal}(L|L \cap K(S))$

$K(S)|K$ ist Kreisteilungserweiterung und somit galoisch.

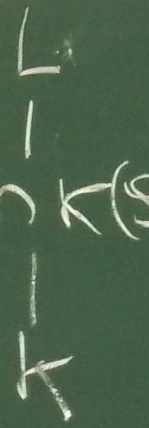
$L|K$, $K(S)|K$ galoisch $\Rightarrow L \cap K(S)|K$ gal.

$\Rightarrow N \trianglelefteq G$ außerdem: $G/N =$

$\mathrm{Gal}(L|K) / \mathrm{Gal}(L|L \cap K(S)) \cong \mathrm{Gal}(L \cap K(S)|K)$

nach Prop 22.6

$K(S)|K$ ist Kreisteilungserw. $\Rightarrow \mathrm{Gal}(K(S)|K)$ abelsch. Als ~~Faktor~~gruppe davon ist auch $\mathrm{Gal}(L \cap K(S)|K)$ abelsch, insbesondere auflösbar.



$\Rightarrow G/N$ ist auflösbar

siehe oben $\Rightarrow N$ ist auflösbar

G/N, N auflösbar $\Rightarrow G$ ist auflösbar. $\square$

Beweis von Satz 24.9:

geg: $f \in K[x]$, durch Radikale auflösbar

z.Zg.: $G = \mathrm{Gal}(f|K)$ ist auflösbar

Vor. $\Rightarrow$ Es gibt eine Radikalerweiterung $M|K$, über der f in Linearfaktoren zerfällt.

Nach Prop. 24.7 können wir $M|K$ durch eine galoissche Radikalerweiterung ersetzen (über der f immer noch zerfällt).

Prop. 24.8 $\Rightarrow$ $\mathrm{Gal}(M|K)$ ist auflösbar.

Sei L der Zerfällungskörper von f über K in M.

Dann gilt nach Def. $\mathrm{Gal}(f|K) = \mathrm{Gal}(L|K)$.

Kap. 22.6 $\Rightarrow \mathrm{Gal}(L|K) \cong \mathrm{Gal}(M|K) / \mathrm{Gal}(L|M)$

(beachte: $\mathrm{Gal}(L|M) \trianglelefteq \mathrm{Gal}(M|K)$, da $L|K$ galoisch)

Da $\mathrm{Gal}(L|K)$ isomorph zu einer Faktorgruppe der auflösbaren Gruppe $\mathrm{Gal}(M|K)$ ist, ist auch $\mathrm{Gal}(L|K)$ auflösbar. $\square$

Auflösbarkeit der Polynome vom Grad ≤ 4

Satz (24.10)

Jedes Polynom über einem Körper der Charakteristik 0 vom Grad ≤ 4 ist durch Radikale auflösbar.

Erzeugendensysteme von S_5

Proposition (25.1)

Jede zweielementige Menge $\{\sigma, \tau\}$ bestehend aus dem 5-Zykel $\sigma = (1\ 2\ 3\ 4\ 5)$ und einer beliebigen Transposition τ ist ein Erzeugendensystem von S_5.

Beweis von Prop. 24.1

geg: $\sigma = (1\,2\,3\,4\,5)$, τ bel Transposition

$U = \langle \sigma, \tau \rangle$

Beh.: $U = S_5$

Betrachte $\sigma' = \tau \sigma \tau^{-1} = (\tau(1)\,\tau(2)\,\tau(3)\,\tau(4)\,\tau(5))$

insb. ist σ' wieder ein 5-Zyklel. Bew.:

σ' stimmt mit keinem Element aus $\langle \sigma \rangle$ überein.

(Elemente von $\langle \sigma \rangle$: $\sigma^0 = id$, $\sigma^1 = \sigma$, $\sigma^2 = (1\,3\,5\,2\,4)$,

$\sigma^3 = (1\,4\,2\,5\,3)$, $\sigma^4 = (1\,5\,4\,3\,2)$)

$\Rightarrow$ U besitzt mindestens zwei 5-Sylowgruppen, ebenso

die Untergr. $V = \langle a, a' \rangle$ von U

Lagrange $\Rightarrow |U|$ teilt $|S_5| = 5 \cdot 24 \Rightarrow |U| = 5m$

wobei m Teiler von 24, d.h. $m \in \{1, 2, 4, 8, 3, 6, 12, 24\}$

3 Sylowsatz $\Rightarrow$ Für die Anzahl r_5 der 5-Sylowgr. von U gilt $r_5 \mid m$, somit auch $r_5 \mid 24$, außerdem $r_5 \equiv 1 \bmod 5$

$\Rightarrow r_5 = 6$ (wegen $r_5 \geq 2$). Dasselbe gilt auch für die Anzahl der 5-Sylowgr. von V. $\Rightarrow U, V$ haben als Ordn. ein Vielfaches von 30

a, a' sind 5-Zykel, liegen also in $A_5 \Rightarrow V = \langle a, a' \rangle \subseteq A_5$ Ang. $V = 30$. $\overset{|A_5|=6}{\Rightarrow} (A_5 : V) = 2 \Rightarrow V \trianglelefteq A_5$

$\lightning$ da A_5 einfach $\Rightarrow V = A_5 \overset{U \geq V}{\Rightarrow} U = A_5$ oder $U = S_5$

τ Transp. $\Rightarrow \operatorname{sgn} \tau \neq A_5 \overset{\tau \in U}{\Rightarrow} U = S_5$ $\square$

Nicht-Auflösbarkeit von Polynomen fünften Grades

Satz (25.2)

Sei $f \in \mathbb{Q}[x]$ ein normiertes, irreduzibles Polynom vom Grad 5 mit genau drei reellen Nullstellen. Dann ist $\mathrm{Gal}(f|\mathbb{Q})$ isomorph zu S_5.

Satz (24.3)

Es gibt Polynome in $\mathbb{Q}[x]$ vom Grad 5, die nicht durch Radikale auflösbar sind.

Angabe eines irreduziblen Polynoms vom Grad 5 in $\mathbb{Q}[x]$ mit genau drei reellen Nullstellen

Betrachte $g = x(x^2-2)(x^2+2)$

$= x^5 - 4x$

g hat genau drei reelle Nullst.: $0, \pm\sqrt{2}$

Kurvendiskussion $\Rightarrow$ Graph von g hat

Hochpunkt in $\approx (-0{,}950;\ 3{,}026)$,

Tiefpunkt in $\approx (0{,}950;\ -3{,}026)$

$\Rightarrow$ Auch $f = g + 2 = x^5 - 4x + 2$ hat genau drei reelle Nullstellen (da weiterhin der Hochpunkt über und der Tiefpunkt unter der x-Achse liegt)

außerdem: f ist irreduzibel auf Grund des Eisenstein-Kriteriums