Freie und vollständig freie Elemente in endlichen, abelschen Erweiterungen

Diplomarbeit

von
Petra Meyer

Fachbereich Mathematik
Universität Kaiserslautern

März 1992

Einleitung

Aus der Körpertheorie ist der Satz von der Normalbasis bekannt (siehe z.B. [9, §12. Satz 3]), der besagt, daß es zu jeder endlichen Galoiserweiterung L/K ein Element in L gibt, dessen Konjugierte unter der Galoisgruppe von L/K eine K-Basis von L bilden. Ein solches Element wird als regulär in L/K bezeichnet, die zugehörige K-Basis von L heißt Normalbasis. Für einen Zwischenkörper M einer Galoiserweiterung L/K ist nach dem Hauptsatz der Galoistheorie auch L/M galoissch und besitzt infolgedessen eine Normalbasis. Ist ein reguläres Element von L/K auch regulär in L/M für alle Zwischenkörper M von L/K, so wird es vollständig regulär in L/K genannt. Dies wirft die Frage auf, ob es in jeder Galoiserweiterung ein vollständig reguläres Element gibt. Wie sich zeigt, kann diese Frage für alle endlichen Galoiserweiterungen bejaht werden.

Ein reguläres Element x einer Galoiserweiterung L/K ist durch zwei Eigenschaften gekennzeichnet: zum einen wird L von x über K erzeugt und zum anderen sind die Konjugierten von x unter der Galoisgruppe von L/K linear unabhängig über K. Letzteres besagt gerade, daß die Nullstellen des Minimalpolynoms von x über K linear unabhängig über K sind. Hat x diese zweite Eigenschaft, so heißt x frei über K. Ist x ein Element aus einer algebraische Hülle A von K, so wird x vollständig frei über K genannt, wenn für jeden Zwischenkörper M von A/K die Nullstellen des Minimalpolynoms von x über M linear unabhängig über M sind.

Es läßt sich zeigen, daß ein $x \in A$ genau dann vollständig frei über K ist, wenn x frei über allen Zwischenkörpern M von N/K ist, wobei N den Zerfällungskörper des Minimalpolynoms von x über K bezeichnet. Daß es in jeder endlichen Galoiserweiterung L/K ein vollständig reguläres Element gibt, ist daher ein Spezialfall der Aussage, daß es in jeder endlichen, separablen Körpererweiterung L/K ein über K vollständig freies Element gibt, welches L erzeugt.

Das erste Ziel dieser Arbeit ist deshalb der Beweis, daß jede endliche, separable Körpererweiterung L/K von einem über K vollständig freien Element erzeugt wird. Ist K ein Körper mit unendlich vielen Elementen, so ist der Beweis eine Verallgemeinerung des Beweises von E. Artin [1] zur Existenz von Normalbasen in Galoiserweiterungen.

Weitaus schwieriger ist der Fall, wenn K ein endlicher Körper ist. Dann ist L/K stets eine Galoiserweiterung und die über K vollständig freien Elemente, die L über K erzeugen, sind genau diejenigen, die in L/K vollständig regulär sind. Ist G die Galoisgruppe von L/K, so läßt sich L zu einem KG-Modul machen, der als solcher wegen des Satzes von der Normalbasis sogar isomorph zu KG ist. Ein Element aus L ist genau dann regulär in L/K, wenn es in keinem echten KG-Teilmodul von L liegt. Entsprechendes gilt natürlich auch für alle Zwischenkörper M von L/K. Das heißt, ein Element aus L ist genau dann vollständig regulär in L/K, falls es für keinen Zwischenkörper

M von L/K in einem echten MU-Teilmodul von L liegt; hierbei bezeichnet U die Galoisgruppe von L/M. In Abschnitt 2 wird gezeigt, daß der Beweis auf den Fall, daß G eine zyklische Gruppe von Primzahlpotenzordnung ist, reduziert werden kann. Durch nähere Betrachtung der MU-Teilmoduln von L für diese Situation, wobei bereits allgemeiner K und L nicht als endlich vorausgesetzt werden, läßt sich dann zeigen, daß es stets ein Element in L gibt, das vollständig regulär in L/K ist.

Die Tatsache, daß es in jeder Galoiserweiterung L/K ein vollständig reguläres Element gibt, läßt natürlich nicht darauf schließen, daß jedes reguläre Element in L/K auch schon vollständig regulär in L/K ist. Dies leitet über zu der von C. C. Faith [6] gestellten Frage, wann in einer endlichen, abelschen Galoiserweiterung jedes reguläre Element schon vollständig regulär ist; eine solche Galoiserweiterung heißt dann vollständig regulär. Im letzten Abschnitt wird diese Frage für Galoiserweiterungen L/K mit zyklischer Galoisgruppe G von Primzahlpotenzordnung beantwortet. Ist $|G| = q^n$ mit einer Primzahl q, so gibt es zwei Möglichkeiten: entweder q ist gleich oder q ist ungleich der Charakteristik von K. Im ersten Fall läßt sich relativ einfach zeigen, daß L/K stets vollständig regulär ist, selbst wenn G nur als abelsche q-Gruppe vorausgesetzt wird.

Ist hingegen q ungleich der Charakteristik von K, so ist weit mehr Aufwand erforderlich. Die Untersuchung der Strukturen von L als MU-Modul für die verschiedenen Zwischenkörper M von L/K, — hierbei ist U wieder die Galoisgruppe von L/M —, die schon beim Existenzbeweis von vollständig regulären Elementen durchgeführt wird, ist dabei das entscheidende Hilfsmittel. Unter den gemachten Voraussetzungen ergibt sich dann folgende Charakterisierung einer vollständig regulären Erweiterung: L/K ist genau dann vollständig regulär, wenn $L \cap K[\zeta^q] = K$ gilt, wobei ζ eine primitive q^n-te Einheitswurzel ist. Wird K zusätzlich als endlich angenommen, so läßt sich dieses notwendige und hinreichende Kriterium sogar recht einfach überprüfen.

Die vorliegende Arbeit stützt sich im wesentlichen auf die Artikel [2], [3] und [4] von D. Blessenohl und K. Johnson.

Abschließend möchte ich mich noch bei Herrn Lüneburg für die vielen, guten Ratschläge bedanken. Ein herzliches Dankeschön sei auch an die Dr. Sthamer/Marquard-Stiftung für die finanzielle Unterstützung und an Silvia Christmann, die mir ihren Drucker zum Drucken dieser Arbeit geliehen hat, gerichtet.

1 Freie und vollständig freie Elemente

Das erste Ziel ist der Beweis des folgenden Satzes.

Satz 1.1 *Ist L/K eine endliche separable Körpererweiterung, so wird L von einem über K vollständig freien Element erzeugt.*

Um diesen Satz beweisen zu können, müssen zunächst ein paar Bezeichnungen eingeführt werden. Dazu seien K ein Körper, A die algebraische Hülle von K und $A[X]$ der Polynomring über A in der Unbestimmten X. Entsprechend sei $K[X]$ der Polynomring in der Unbestimmten X über K.

Definition 1.2 *Es sei $f \in K[X]$.*

1. *Der von den Nullstellen von f erzeugte K-Teilraum $W_K(f)$ von A heißt der* Wurzelraum von f über K.
2. *Es ist* $\dim_K f := \dim_K W_K(f)$ *die* Dimension von f über K.

Es gilt dann sicherlich $\dim_K f \leq \operatorname{grad} f$. Für die nächsten Sätze brauchen wir noch

Definition 1.3 *Ein Polynom $f \in K[X]$ wird als* frei über K *bezeichnet, falls* $\dim_K f = \operatorname{grad} f$ *ist.*

Aus den Definitionen folgt sofort, daß $f = \prod_{i=1}^{n}(X - a_i)$ mit $a_1, \ldots, a_n \in A$ genau dann frei über K ist, wenn $a_1, \ldots, a_n$ linear unabhängig über K ist.

Satz 1.4 *Ein über K freies Polynom f ist separabel und irreduzibel.*

Beweis: Sei f ein freies Polynom über K, wobei wir annehmen können, daß der Leitkoeffizient von f gleich 1 ist. Dann kann f keine mehrfachen Nullstellen haben, da sonst $\dim_K f < \operatorname{grad} f$ wäre. Damit ist f separabel. Angenommen f ist reduzibel in $K[X]$ und $f = g \cdot h$ ist eine echte Zerlegung von f in $K[X]$, wobei die Leitkoeffizienten von g und h gleich 1 sind. Sei weiter $Y := \{y_1, \ldots, y_m\}$ die Menge der Nullstellen von g und $Z := \{z_1, \ldots, z_l\}$ die Menge der Nullstellen von h in A. Dann gilt sicherlich: $Y, Z \neq \emptyset$, da weder g noch h ein konstantes Polynom ist, und $Y \cap Z = \emptyset$, da f keine mehrfache Nullstelle hat. Außerdem ist $Y \cup Z$ die Menge der Nullstellen von f.

Da f frei über K ist, sind $y_1, \ldots, y_m$ linear unabhängig über K, ebenso $z_1, \ldots, z_l$. Deshalb ist sowohl y als auch z, definiert als $y := y_1 + \cdots + y_m$ bzw. $z := z_1 + \cdots + z_l$, ungleich Null. Für g gilt:

$$\begin{aligned} g(X) &= \prod_{i=1}^{m}(X - y_i) \\ &= X^m - X^{m-1}(y_1 + \cdots + y_m) + \text{ Terme kleineren Grades.} \end{aligned}$$

Weil g in $K[X]$ liegt, ist daher $y \in K$. Eine analoge Überlegung ergibt, daß auch z in K liegt. Weiter gilt:

$$\begin{aligned} 0 &= yz - zy \\ &= y_1 z + \cdots + y_m z - z_1 y - \cdots - z_l y. \end{aligned}$$

Das widerspricht aber der linearen Unabhängigkeit der Nullstellen von f, welche genau die Menge $\{y_1, \ldots, y_m, z_1, \ldots, z_l\}$ bilden. Damit folgt die Behauptung. $\square$

Definition 1.5 *Es sei $z \in A$.*

1. *Das Minimalpolynom von z über K wird mit $m_{K,z}$ bezeichnet. Die Nullstellen von $m_{K,z}$ heißen die* Konjugierten von z über K.
2. *z heißt* frei über K, *falls $m_{K,z}$ frei über K ist.*
3. *Ist L/K eine Galoiserweiterung, so ist* $\mathrm{Gal}(L/K)$ *die zugehörige Galoisgruppe.*

Also ist $z \in A$ genau dann frei über K, wenn die Konjugierten von z linear unabhängig über K sind. Wie wir gesehen haben, ist ein freies Element separabel. Der folgende Satz gibt eine hinreichende Bedingung dafür, daß ein separables Element frei ist.

Hilfssatz 1.6 *Es sei $z \in A$ separabel.*

1. *Ist N/K eine endliche, galoissche Erweiterung mit $z \in N \subseteq A$ und sind $g_1, \ldots, g_m$ Elemente von* $\mathrm{Gal}(N/K)$ *mit* $\det(z^{g_i g_j^{-1}}) \neq 0$, *so ist $\{z^{g_1}, \ldots, z^{g_m}\}$ linear unabhängig über K.*
2. *Ist $M := K[z]$ und $N \subseteq A$ der Zerfällungskörper von $m_{K,z}$, sowie $G :=$* $\mathrm{Gal}(N/K)$, *$U :=$* $\mathrm{Gal}(N/M)$ *und schließlich $R = \{g_1, \ldots, g_m\}$ ein Repräsentantensystem für die Rechtsrestklassen von U in G mit* $\det(z^{g_i g_j^{-1}}) \neq 0$, *so ist z frei über K.*

Beweis: 1) Seien $c_1, \ldots, c_m \in K$ mit $\sum_{i=1}^m c_i z^{g_i} = 0$. Da $g_j^{-1} \in \mathrm{Gal}(N/K)$ ist, folgt für $j = 1, \ldots, m$:

$$0 = \left(\sum_{i=1}^m c_i z^{g_i} \right)^{g_j^{-1}} = \sum_{i=1}^m c_i^{g_j^{-1}} z^{g_i g_j^{-1}} = \sum_{i=1}^m c_i z^{g_i g_j^{-1}}.$$

Es ist aber $\det(z^{g_i g_j^{-1}}) \neq 0$ vorausgesetzt worden, also ist $c_1 = \cdots = c_m = 0$, was gerade die lineare Unabhängigkeit von $z^{g_1}, \ldots, z^{g_m}$ besagt.

2) Weil N ein Zerfällungskörper eines separablen Polynoms aus $K[X]$ ist, ist N/K eine Galoiserweiterung. Insbesondere ist daher auch der Zwischenkörper M über K separabel und es gilt:

$$\text{Anzahl der Nullstellen von } m_{K,z} = \operatorname{grad} m_{K,z} = M : K.$$

Weiter ist

$$M : K = \frac{N : K}{N : M} = \frac{|G|}{|U|} = |G : U| = m.$$

Also hat $m_{K,z}$ genau m verschiedene Nullstellen, zu denen offensichtlich $z^{g_1}, \dots, z^{g_m}$ gehören. Wäre $z^{g_i} = z^{g_j}$ für $g_i, g_j \in R$, so würde $z = z^{g_i g_j^{-1}}$ und damit $g_i g_j^{-1} \in U$ folgen. Also wäre $g_i = g_j$, da g_i, g_j Repräsentanten der Rechtsrestklassen von U in G sind. Für $i \neq j$ sind damit z^{g_i} und z^{g_j} verschieden, d.h. die Konjugierten von z sind genau $z^{g_1}, \dots, z^{g_m}$. Nach Voraussetzung ist $\det(z^{g_i g_j^{-1}}) \neq 0$, womit sich jetzt 1) anwenden läßt, was zeigt, daß $z^{g_1}, \dots, z^{g_m}$ linear unabhängig über K sind. Daraus folgt die Behauptung. □

Definition 1.7 *Sei Ω eine Erweiterung des Körpers K und E, F zwei Erweiterungen von K, die in Ω liegen. E und F heißen* linear disjunkt über K, *falls eine der beiden folgenden, äquivalenten Bedingungen erfüllt ist.*

- *Ist (a_α) eine Familie von Elementen aus E, die linear unabhängig über K sind, so sind diese auch linear unabhängig über F.*

- *Sind (a_α) und (b_β) zwei über K linear unabhängige Familien aus E bzw. F, so ist die Familie $(a_\alpha b_\beta)$ linear unabhängig über K.*

Hilfssatz 1.8 *Es sei $z \in A$ frei über K und $N \subseteq A$ der Zerfällungskörper von $m_{K,z}$. Ferner sei L ein Teilkörper von A mit $N \cap L = K$. Dann ist z frei über L.*

Beweis: Wegen $K \subseteq L$ liegt $m_{K,z}$ auch in $L[X]$. Sei nun $m_{K,z} = f \cdot g$ mit $f, g \in L[X]$. Die Leitkoeffizienten von g und f seien außerdem gleich 1. Nach Voraussetzung zerfällt $m_{K,z}$ in $N[X]$, weshalb f und g in $N[X]$ liegen. Daher gilt:

$$g, f \in L[X] \cap N[X] = K[X].$$

Weil $m_{K,z}$ irreduzibel in $K[X]$ ist, kann $f \cdot g$ keine echte Zerlegung von $m_{K,z}$ sein, d.h. $m_{K,z}$ ist auch in $L[X]$ irreduzibel.

Weil N ein Zerfällungskörper von $m_{K,z}$ ist, ist N/K eine Galoiserweiterung. Daher folgt aus [5, V.10.4.Théorème 1], daß N und L linear disjunkt über K sind. Das bedeutet gemäß Definition 1.7: Ist eine Familie von Elementen aus N linear unabhängig über K, so ist sie auch linear unabhängig über L.

Nach Voraussetzung sind die Nullstellen von $m_{K,z}$ linear unabhängig über K und liegen in N, also sind sie auch linear unabhängig über L. Wegen $m_{K,z} = m_{L,z}$ folgt die Behauptung. □

Definition 1.9 *Ein Element $z \in A$ heißt* vollständig frei über K, *wenn z frei ist über allen Zwischenkörpern M von A/K.*

Um zu testen, ob $z \in A$ vollständig frei über K ist, genügt es zu überprüfen, ob z frei über allen Zwischenkörpern von N/K ist, wobei N den Zerfällungskörper von $m_{K,z}$ bezeichnet. Diese Tatsache, die durch den folgenden Satz zum Ausdruck kommt, wird den Beweis von 1.1 wesentlich vereinfachen.

Satz 1.10 *Es sei wieder $z \in A$ und $N \subseteq A$ der Zerfällungskörper von $m_{K,z}$. Dann sind äquivalent:*

1. *z ist vollständig frei über K,*
2. *z ist frei über allen Zwischenkörpern von N/K.*

Beweis: „1) $\Rightarrow$ 2):“ Das ist trivial.
„2) $\Rightarrow$ 1):“ Sei L ein Zwischenkörper von A/K. Sei weiter $M := N \cap L$. Dann ist M ein Zwischenkörper von N/K und nach Voraussetzung ist z frei über M. Ferner ist N auch der Zerfällungskörper von $m_{K,z}$. Nach 1.8 ist z also frei über L und damit vollständig frei über K. $\square$

Jetzt läßt sich folgendes Zwischenergebnis beweisen:

Satz 1.11 *Ist L/K eine endliche, separable Körpererweiterung und K ein Körper mit unendlich vielen Elementen, so wird L von einem über K vollständig freien Element z erzeugt.*

Beweis: Dieser Beweis ist eine Verallgemeinerung des Beweises von E. Artin zur Existenz von Normalbasen im Fall unendlicher Körper aus [1].

Sei o.B.d.A. $L \subseteq A$. Ferner sei $N \subseteq A$ die normale Hülle von L/K. Weiter sei $G := \mathrm{Gal}(N/K)$ und $U := \mathrm{Gal}(N/L)$, sowie $R := \{g_1, \ldots, g_m\}$ ein Repräsentantensystem der Rechtsrestklassen von U in G mit $g_1 = 1$. Da L/K separabel und N die normale Hülle von L ist, ist N/K galoissch.

$g_1|_L, \ldots, g_m|_L$ sind die K-Isomorphismen von L in A. Diese sind, weil L unendlich viele Elemente hat, nach [8, I.Theorem 16] algebraisch unabhängig über N, was folgendes bedeutet: Ist $F \in N[X_1, \ldots, X_m]$ mit $F(z^{g_1}, \ldots, z^{g_m}) = 0$ für alle $z \in L$, so ist $F = 0$.

Sei nun M ein Zwischenkörper von N/K und $V := \mathrm{Gal}(N/M)$, dann läßt sich wegen $U \cap V \subseteq V$ ein Repräsentantensystem $S := \{y_1, \ldots, y_s\}$ mit $y_1 = 1$ für die Rechtsrestklassen von $U \cap V$ in V wählen. Für $g \in G$ werde mit $\rho(g)$ das Element aus R bezeichnet, für das $Ug = U\rho(g)$ gilt. Weiter sei $X_{g_i} := X_i$ für $i \in \{1, \ldots, m\}$, wobei $X_1, \ldots X_m$ Unbekannte über N sind. Ferner sei

$$D_M(X_1, \ldots, X_m) := \det(Y) \ \in N[X_1, \ldots, X_m],$$

wobei Y eine $(s \times s)$-Matrix mit $Y_{ij} = X_{\rho(y_i y_j^{-1})}$ ist. Schließlich sei noch

$$D := \prod_{K \subseteq M \subseteq N} D_M \quad \in N[X_1, \ldots, X_m].$$

Genau dann ist $X_{\rho(y_i y_j^{-1})} = X_1$ für $i, j \in \{1, \dots, s\}$, wenn $i = j$ ist. Denn:

$$\begin{aligned} X_1 = X_{\rho(y_i y_j^{-1})} &\iff U y_i y_j^{-1} = U \\ &\iff y_i y_j^{-1} \in U \\ &\iff y_i y_j^{-1} \in U \cap V \\ &\iff i = j \text{ (nach Definition von } y_i \text{ und } y_j). \end{aligned}$$

Daher ergibt sich für $X_1 := 1$ und $X_i := 0$ mit $i \in \{2, \dots, m\}$ folgendes:

$$\begin{aligned} D_M(X_1, \dots, X_m) &= D_M(1, 0, \dots, 0) \\ &= \det(E_s) \quad (E_s \text{ ist die } (s \times s)\text{-Einheitsmatrix}) \\ &= 1, \text{ für alle } K \subseteq M \subseteq N. \end{aligned}$$

Also ist $D(1, 0, \dots, 0) = 1$, und D ist sicherlich nicht das Nullpolynom von $N[X_1, \dots, X_m]$. Nun sind aber $g_1, \dots, g_m$ algebraisch unabhängig über N, somit gibt es ein $z \in L$ mit

$$D(z^{g_1}, \dots, z^{g_m}) = \prod_{K \subseteq M \subseteq N} D_M(z^{g_1}, \dots, z^{g_m}) \neq 0.$$

Für dieses z gilt dann sicherlich auch:

$$0 \neq D_M(z^{g_1}, \dots, z^{g_m}) = \det(z^{\rho(y_i y_j^{-1})})$$

für alle M mit $K \subseteq M \subseteq N$. Nach Definition ist $U\rho(y_i y_j^{-1}) = U y_i y_j^{-1}$, deshalb läßt sich ein $u \in U$ finden mit $\rho(y_i y_j^{-1}) = u y_i y_j^{-1}$. Dann ist

$$z^{\rho(y_i y_j^{-1})} = z^{u y_i y_j^{-1}} = z^{y_i y_j^{-1}}$$

und damit

$$\det(z^{y_i y_j^{-1}}) \neq 0 \qquad (i, j \in \{1, \dots, s\}).$$

Für $M = K$ können wir insbesondere $S = R$ wählen und erhalten:

$$\det(z^{g_i g_j^{-1}}) \neq 0.$$

Sei $T := \{z^{g_1}, \dots, z^{g_m}\}$. Da N/K galoissch ist und $g_1, \dots, g_m \in \mathrm{Gal}(N/K)$ sind, folgt mit 1.6.1, daß die Elemente von T linear unabhängig über K sind. G operiert offensichtlich transitiv auf T, da $z \in L$ ist. Da G die Galoisgruppe von N/K ist und z insbesondere auch in N liegt, ist T damit genau die Menge der Konjugierten von z über K. Es folgt:

$$m_{K,z} = \prod_{i=1}^{m} (X - z^{g_i}).$$

Das bedeutet:

$$L : K = m = \text{grad } m_{K,z} = K[z] : K.$$

Wegen $L \supseteq K[z] \supseteq K$ ist also $K[z] = L$ und es gilt:

$$\mathrm{Gal}(N/M[z]) = \mathrm{Gal}(N/K[z]) \cap \mathrm{Gal}(N/M) = U \cap V.$$

Es ist N ein Zerfällungskörper von $m_{M,z}$. Aus $U \cap V = \mathrm{Gal}(N/M[z])$, sowie den Definitionen von U, V und S folgt nun wegen $\det(z^{y_i y_j^{-1}}) \neq 0$ mit 1.6.2, daß z frei über M ist. Nach 1.10 ist z dann vollständig frei über K, was schließlich die Behauptung ergibt. $\square$

2 Vollständig reguläre Elemente

In diesem Abschnitt wird gezeigt, daß es zum Beweis von 1.1 für endliche Körper genügt, sich auf den Fall zu beschränken, daß L/K eine zyklische Galoisgruppe von Primzahlpotenzordnung hat. Wird unter dieser Voraussetzung zusätzlich noch angenommen, daß die Charakteristik von K die Ordnung der Galoisgruppe teilt, so kann 1.1 für diesen Spezialfall gezeigt werden, was am Schluß dieses Abschnittes geschieht.

Sei zunächst allgemeiner L/K eine beliebige endliche Galoiserweiterung mit Galoisgruppe G. Dann wird L zu einem KG-Modul vermöge

$$\sum_{g\in G} k_g g \cdot l = \sum_{g\in G} k_g g(l)$$

für $\sum_{g\in G} k_g g \in KG$ und $l \in L$.

Definition 2.1 *Das Element $x \in L$ heißt* regulär *in L/K, wenn $\{g(x)|g \in G\}$ eine Basis von L über K ist. Basen dieser Art werden* Normalbasen *genannt.*

Weil L/K endlich galoissch ist, gibt es nach dem Satz von der Normalbasis ein reguläres Element $x_0 \in L$. Für dieses Element gilt:

$$L = \left\{ \sum_{g\in G} k_g g(x_0) \,\middle|\, \sum_{g\in G} k_g g \in KG \right\} = KG \cdot x_0.$$

Also ist L als KG-Modul zyklisch. Sei ψ die durch

$$\psi\left(\sum_{g\in G} k_g g \right) := \sum_{g\in G} k_g g(x_0)$$

definierte Abbildung von KG auf L. Dann ist ψ ein KG-Epimorphismus. Außerdem ist ψ injektiv, denn:

$$0 = \sum_{g\in G} k_g g(x_0) \qquad \Longleftrightarrow \qquad k_g = 0 \text{ für alle } g \in G,$$

da $\{g(x_0)|g \in G\}$ eine K-Basis von L ist. Also sind L und KG als KG-Moduln zueinander isomorph.

Bemerkung 2.2 *Sei $x \in L$. Dann ist x in L/K genau dann regulär, wenn x in keinem echten KG-Teilmodul von L enthalten ist.*

Für $x \in L$ ist $\{g(x)|g \in G\}$ die Menge der Nullstellen von $m_{K,x}$. Daher sind die regulären Elemente von L/K genau die Elemente, die L über K erzeugen und frei über K sind. Genau dann gilt $\dim_K m_{K,x} = L : K$, wenn x in L/K regulär ist.

Sei nun M ein Zwischenkörper von L/K. Dann ist L/M ebenfalls endlich galoissch, die Galoisgruppe von L über M sei U. Insbesondere ist L auch MU-isomorph zu MU.

Definition 2.3 *Das Element $x \in L$ heißt* vollständig regulär in L/K, *wenn x regulär in L/M für alle Zwischenkörper M von L/K ist.*

Wegen 2.2 ist $x \in L$ genau dann vollständig regulär in L/K, wenn x für alle Zwischenkörper M von L/K in keinem echten MU-Teilmodul von L enthalten ist. Das ist genau dann der Fall, wenn $L = MU \cdot x$ für alle Zwischenkörper M von L/K gilt. Nach 1.10 ist ein vollständig reguläres Element von L/K auch vollständig frei über K. Also ist x in L/K genau dann vollständig regulär, wenn L von x über K erzeugt wird und x vollständig frei über K ist. Für eine endliche Galoiserweiterung ist 1.1 daher äquivalent zu

Satz 2.4 *Ist L/K endlich und galoissch, so gibt es ein vollständig reguläres Element in L/K.*

Wegen 1.11 ist dieser Satz ebenso wie 1.1 für unendliche Körper schon gezeigt. Wenn bewiesen ist, daß dieser Satz auch für endliche Körper gilt, ist damit auch 1.1 gänzlich bewiesen; denn für einen endlichen Körper K ist jede endliche Erweiterung L/K auch schon galoissch. Um den Satz für endliche Körper zeigen zu können, bedarf es jedoch noch weiterer Vorbereitung.

Definition 2.5 *Sind E und F zwei Körper, die in einem gemeinsamen Oberkörper enthalten sind, so bezeichnet EF das Kompositum von E und F.*

Satz 2.6 *Sei L/K galoissch mit Galoisgruppe G. Ferner sei $G = G_1 \times G_2$, wobei $|G_1|$ und $|G_2|$ teilerfremd sind. Schließlich seien M_1 und M_2 die zu G_1 bzw. G_2 gehörenden Fixkörper. Ist dann x_i vollständig regulär in M_i/K für $i \in \{1, 2\}$, so ist x_1x_2 vollständig regulär in L/K.*

Beweis: Es ist

$$\{1\} = G_1 \cap G_2 = \mathrm{Gal}(L/M_1M_2)$$

und

$$G = G_1G_2 = \mathrm{Gal}(L/M_1 \cap M_2).$$

Daraus folgt $L = M_1M_2$ und $M_1 \cap M_2 = K$. Sei jetzt M ein Zwischenkörper von L/K und $i \in \{1, 2\}$, dann ist $M \cap M_i$ ein Zwischenkörper von M_i/K und x_i ist nach Voraussetzung regulär in $M_i/M \cap M_i$. Damit ist M_i Zerfällungskörper des Minimalpolynoms $m_{M\cap M_i,x_i}$. In 1.8 wurde gezeigt, daß x_i dann frei über M ist. Außerdem wird M_i von x_i über $M \cap M_i$ erzeugt, so daß sich

$$M_i = (M_i \cap M)[x_i] \subseteq M[x_i]$$

ergibt. Daraus folgt:

$$MM_i \subseteq MM[x_i] = M[x_i].$$

Wegen $x_i \in M_i$ gilt aber $M[x_i] \subseteq MM_i$, woraus sich die Gleichheit von $M[x_i]$ und MM_i ergibt. Damit ist x_i regulär in MM_i/M.

Sei jetzt $H := \mathrm{Gal}(L/M)$, $h \in H$ sowie $h = h_1 \cdot h_2$ mit $h_1 \in G_1$ und $h_2 \in G_2$. Der Kommutator von h_1 und h_2 ist gleich 1. Weil Teilerfremdheit von $|G_1|$ und $|G_2|$ gefordert wurde, gibt es l_1 und l_2 in $\mathbb{Z}$ mit

$$1 = l_1|G_1| + l_2|G_2|,$$

was äquivalent ist zu

$$1 - l_1|G_1| = l_2|G_2|.$$

Daraus ergibt sich:

$$\begin{aligned} h^{l_2|G_2|} &= (h_1h_2)^{l_2|G_2|} \\ &= h_1^{l_2|G_2|}h_2^{l_2|G_2|} \\ &= h_1^{1-l_1|G_1|}h_2^{l_2|G_2|} = h_1. \end{aligned}$$

Also ist $h_1 \in H$. Ebenso läßt sich $h_2 \in H$ zeigen, woraus

$$H \subseteq (H \cap G_1) \times (H \cap G_2)$$

folgt. Die andere Inklusion ist trivial und wir erhalten

$$H = (H \cap G_1) \times (H \cap G_2).$$

Daraus folgt, weil $H \cap G_i = \mathrm{Gal}(L/MM_i)$ ist:

$$\begin{aligned} H &= (H \cap G_1) \cdot (H \cap G_2) \\ &= \mathrm{Gal}(L/MM_1) \cdot \mathrm{Gal}(L/MM_2) \\ &= \mathrm{Gal}(L/MM_1 \cap MM_2). \end{aligned}$$

Also ist $M = MM_1 \cap MM_2$. Durch Anwendung von [5, V.10.4.Théorème 1] zeigt sich, daß MM_1 und MM_2 linear disjunkt sind. Außerdem gilt:

$$\{(x_1x_2)^h | h \in H\} = \{x_1^{h_2}x_2^{h_1} | h_1 \in H \cap G_1, h_2 \in H \cap G_2\}.$$

Es läßt sich wieder [5, V.10.4.Théorème 1] anwenden, und wir erhalten

$$\begin{aligned} \mathrm{Gal}(L/MM_2) &= \mathrm{Gal}((MM_1)(MM_2)/MM_2) \\ &\cong \mathrm{Gal}(MM_1/MM_1 \cap MM_2) = \mathrm{Gal}(MM_1/M) \end{aligned}$$

sowie $\mathrm{Gal}(L/MM_1) \cong \mathrm{Gal}(MM_2/M)$. Außerdem besteht $\mathrm{Gal}(MM_1/M)$ genau aus den Einschränkungen der Elemente von $\mathrm{Gal}(L/MM_2)$ auf MM_1, sowie $\mathrm{Gal}(MM_2/M)$ aus den Einschränkungen der Elemente von $\mathrm{Gal}(L/MM_1)$ auf MM_2. Damit ergibt sich, weil $x_1 \in MM_1$ und $x_2 \in MM_2$ ist, folgendes:

$$\begin{aligned} \{(x_1x_2)^h | h \in H\} &= \{x_1^{h_2}x_2^{h_1} | h_1 \in \mathrm{Gal}(L/MM_1), h_2 \in \mathrm{Gal}(L/MM_2)\} \\ &= \{x_1^{h_1}x_2^{h_2} | h_1 \in \mathrm{Gal}(MM_1/M), h_2 \in \mathrm{Gal}(MM_2/M)\}. \end{aligned}$$

Für $i \in \{1,2\}$ ist aber x_i regulär in MM_i/M, was besagt, daß $\{x_i^h | h \in \mathrm{Gal}(MM_i/M)\}$ eine M-Basis von MM_i ist. MM_1 und MM_2 sind außerdem linear disjunkt über M, woraus jetzt folgt, daß $\{(x_1x_2)^h | h \in H\}$ linear unabhängig über M ist. Seien nun $h_1, g_1 \in \mathrm{Gal}(MM_1/M)$ und $h_2, g_2 \in \mathrm{Gal}(MM_2/M)$ und es gelte

$$x_1^{h_1} x_2^{h_2} = x_1^{g_1} x_2^{g_2}.$$

Weil x_1 und x_2 nicht Null sind, folgt daraus

$$x_1^{h_1}(x_1^{g_1})^{-1} = x_2^{g_2}(x_2^{h_2})^{-1}.$$

Also sind $x_1^{h_1}(x_1^{g_1})^{-1}$ und $x_2^{g_2}(x_2^{h_2})^{-1}$ Elemente von $MM_1 \cap MM_2 = M$. Wegen

$$x_1^{h_1} = (x_1^{h_1}(x_1^{g_1})^{-1}) \cdot x_1^{g_1} \qquad \text{bzw.} \qquad x_2^{g_2} = (x_2^{g_2}(x_2^{h_2})^{-1}) \cdot x_2^{h_2}$$

sind $x_1^{h_1}$ und $x_1^{g_1}$ bzw. $x_2^{g_2}$ und $x_2^{h_2}$ linear abhängig über M. Deshalb ist $h_1 = g_1$ und $h_2 = g_2$. Daraus folgt:

$$\begin{aligned} |\{(x_1x_2)^h | h \in H\}| &= |\mathrm{Gal}(MM_1/M)| \cdot |\mathrm{Gal}(MM_2/M)| \\ &= |\mathrm{Gal}(L/MM_2)| \cdot |\mathrm{Gal}(L/MM_1)| \\ &= |G_2 \cap H| \cdot |G_1 \cap H| = |H|. \end{aligned}$$

Wegen $\dim_M L = |H|$ ist die Menge $\{(x_1x_2)^h | h \in H\}$ daher eine M-Basis von L. Dies besagt, x_1x_2 ist regulär in L/M für alle Zwischenkörper M von L/K. Also ist x_1x_2 vollständig regulär in L/K. $\square$

Definition 2.7 *Eine endliche Galoiserweiterung L/K heißt* vollständig regulär*, wenn jedes in L/K reguläre Element schon vollständig regulär in L/K ist.*

Sind K und L endliche Körper, dann ist $G = \mathrm{Gal}(L/K)$ zyklisch und direktes Produkt von zyklischen Gruppen, deren Ordnungen zueinander teilerfremde Primzahlpotenzen sind. Wegen 2.6 können wir deshalb zum Beweis von 2.4 für endliche Körper annehmen, daß $|G| = q^n$ gilt, wobei q eine Primzahl und $n \in \mathbb{N}$ ist. Ist char $K = p$, dann lassen sich die Fälle $p = q$ und $p \neq q$ unterscheiden. Der erste Fall wird durch den folgenden Satz, der allgemeiner für beliebige Körper und abelsche p-Gruppen formuliert ist, bewiesen. Zugleich wird gezeigt, daß eine solche Erweiterung stets vollständig regulär ist.

Satz 2.8 *Sei K ein Körper der Charakteristik p und L/K eine endliche Galoiserweiterung. Weiter sei* $\mathrm{Gal}(L/K)$ *eine abelsche p-Gruppe. Dann gibt es ein vollständig reguläres Element in L/K, und L/K ist sogar vollständig regulär.*

Beweis: Sei M ein Zwischenkörper von L/K und $U := \mathrm{Gal}(L/M)$. Nach Voraussetzung ist U eine p-Gruppe. Mit $J(A)$ werde das Jacobson-Radikal der Algebra A bezeichnet. Mit [7, V.5.16] läßt sich folgendes über $J(MU)$ sagen:

$$J(MU) = \left\{ \sum_{u\in U} m_u u \,\middle|\, \sum_{u\in U} m_u = 0 \right\},$$

sowie $\dim_M J(MU) = |U| - 1$. Da $J(MU)$ der Schnitt über alle maximalen MU-Teilmoduln von MU ist, gelten für einen maximalen MU-Teilmodul W die Inklusionen $J(MU) \subseteq W \subset MU$. Wegen

$$\dim_M J(MU) = |U| - 1 \leq \dim_M W < \dim_M MU = |U|$$

ist damit $\dim_M W = |U| - 1$ und $W = J(MU)$. Also ist $J(MU)$ der einzige maximale MU-Teilmodul von MU. Das gilt natürlich insbesondere auch, wenn $M = K$ ist.

$J(MU)$ ist der Annullator von $\sum_{u\in U} u$. Denn ist $\sum_{u\in U} m_u u \in MU$, so gilt

$$\begin{aligned}
\left(\sum_{u\in U} m_u u\right)\left(\sum_{u\in U} u\right) = 0 \quad &\iff \quad \sum_{v\in U}\left(\sum_{u\in U} m_u\right) v = 0 \\
&\iff \quad \sum_{u\in U} m_u = 0 \\
&\iff \quad \sum_{u\in U} m_u u \in J(MU).
\end{aligned}$$

Sei weiter

$$J_{MU} := \left\{ x \in L \,\middle|\, \sum_{u\in U} u(x) = 0 \right\}.$$

Weil L und MU als MU-Moduln isomorph sind, gibt es einen MU-Isomorphismus ϱ von MU auf L. Es gilt

$$\begin{aligned}
x \in J(MU) \quad &\iff \quad x \cdot \sum_{u\in U} u = 0 \\
&\iff \quad \varrho\left(x \cdot \sum_{u\in U} u\right) = 0 \\
&\iff \quad \sum_{u\in U} u \cdot \varrho(x) = 0 \\
&\iff \quad \sum_{u\in U} u(\varrho(x)) = 0 \\
&\iff \quad \varrho(x) \in J_{MU},
\end{aligned}$$

d.h. J_{MU} ist das Bild von $J(MU)$ und daher der einzige maximale MU-Teilmodul von L. Für $g \in G$ und $x \in J_{MU}$ gilt, weil G abelsch ist, folgendes:

$$\sum_{u\in U} u(g(x)) = \sum_{u\in U} g(u(x)) = g\left(\sum_{u\in U} u(x)\right) = g(0) = 0.$$

Also ist $g(J_{MU}) \subseteq J_{MU}$. Damit läßt sich aus J_{MU} sogar einen KG-Teilmodul machen, der als solcher in dem einzigen maximalen KG-Teilmodul J_{KG} von L liegt. Sei jetzt x regulär in L/K — und ein solches x gibt es nach dem Satz von der Normalbasis —, dann liegt x nach 2.2 in keinem echten KG-Teilmodul von L. Damit ist $x \notin J_{KG}$ und insbesondere auch $x \notin J_{MU}$. Da aber alle echten MU-Teilmoduln von L in J_{MU} enthalten sind, liegt x in keinem echten MU-Teilmodul von L. Nach 2.2 ist x regulär in L/M, also vollständig regulär in L/K. Außerdem ist gezeigt, daß alle regulären Elemente von L/K schon vollständig regulär sind, was den Satz beweist. $\square$

Damit sind 1.1 und 2.4 nun auch für den Fall bewiesen, daß L/K eine Erweiterung endlicher Körper mit zyklischer Galoisgruppe von Primzahlpotenzordnung ist, wobei die Charakteristik der Körper die Ordnung der Galoisgruppe teilt.

3 Ein Satz über Körper der q^m-ten Einheitswurzeln

Um 1.1 und 2.4 für den noch verbleibenden Fall zeigen zu können, werden in diesem und dem nächsten Abschnitt die dazu nötigen Hilfsmittel bereitgestellt. Wir betrachten dabei jedoch beliebige Körper, was später in einem anderen Zusammenhang noch von Nutzen sein wird.

Satz 3.1 *Sei K ein Körper, q eine von der Charakteristik von K verschiedene Primzahl, $m \in \mathbb{N}$ und θ eine primitive q^m-te Einheitswurzel. Ferner seien $c \in \mathbb{N}_0$ und $s \in \mathbb{N}$ so gewählt, daß $K[\theta] : K = q^c s$ und $s|(q-1)$ gilt.*

1. *Ist $c \geq 1$, so gilt genau eine der folgenden beiden Aussagen:*
   - *(a) $K[\theta] : K[\theta^q] = q$;*
   - *(b) $q = 2,\ m \geq 3,\ K[\theta] : K = 2$ und $K[\theta] = K[\theta^2]$.*
2. *$K[\theta] : K[\theta^{q^i}] = q^i$ für $0 \leq i \leq c-1$.*
3. *Genau eine der beiden folgenden Aussagen ist wahr:*
   - *(a) $K[\theta] : K[\theta^{q^c}] = q^c$;*
   - *(b) $q = 2$ und $K[\theta^{2^{c-1}}] = K[\theta^{2^c}]$.*
4. *Ist $\mathrm{Gal}(K[\theta]/K)$ nicht zyklisch, so ist $q = 2$ und $m \geq 3$. Ferner ist dann $\mathrm{Gal}(K[\theta]/K[\theta^{2^i}])$ zyklisch für $0 \leq i \leq c-1$.*

Beweis: Sei $H := \mathrm{Gal}(K[\theta]/K)$. Ist $\alpha \in H$, so gibt es bekanntlich ein $a \in \mathbb{N}$ mit $\alpha(\theta) = \theta^a$, und die durch $\sigma(\alpha) := a + q^m\mathbb{Z}$ definierte Abbildung σ ist ein Monomorphismus von H in die Gruppe der Einheiten $(\mathbb{Z}/q^m\mathbb{Z})^*$ von $\mathbb{Z}/q^m\mathbb{Z}$, welche jetzt mit E bezeichnet wird. Es existiert also eine Untergruppe $\tilde{H} \subseteq E$, die isomorph zu H ist.

1) Wir betrachten zunächst den Fall, daß $q \neq 2$ ist. Dann gilt b) offensichtlich nicht. Nach Voraussetzung ist $K[\theta] : K = q^c s$ mit $c \geq 1$, d.h. q teilt $|H|$. Weiter ist E für ungerade Primzahlen bekanntermaßen zyklisch, damit ist auch $\tilde{H}$ zyklisch und besitzt wegen der Isomorphie zu H eine Untergruppe der Ordnung q. Wie man leicht sieht, wird diese durch $(1 + q^{m-1}) + q^m\mathbb{Z}$ erzeugt. Des weiteren werde mit U die Untergruppe der Ordnung q von H bezeichnet. Dann gilt $U = \langle\alpha\rangle$, wobei α das Urbild von $(1 + q^{m-1}) + q^m\mathbb{Z}$ unter σ ist, d.h. α ist bestimmt durch

$$\alpha(\theta) = \theta^{1+q^{m-1}}.$$

Daraus ergibt sich:

$$\alpha(\theta^q) = (\alpha(\theta))^q = \theta^{q+q^m} = \theta^q.$$

Also liegt θ^q im Fixkörper von U und es ist $U \subseteq \mathrm{Gal}(K[\theta]/K[\theta^q])$. Aus $K[\theta] : K[\theta^q] \geq |U| = q$ und $K[\theta] : K[\theta^q] \leq q$ ergibt sich nun die Aussage a).

Sei jetzt $q = 2$ und $m \geq 2$. Wir setzen $j := (1+2^{m-1})+2^m\mathbb{Z}$. Wenn $j \in \tilde{H}$ gilt, dann können wir wie im ersten Fall folgern, daß a) richtig ist. Dies ist insbesondere für $m = 2$ der Fall. Also können wir annehmen, daß $m \geq 3$ ist. Wegen

$$(1 + 2^{m-1})^2 = 1 + 2^m(1 + 2^{m-2})$$

und

$$1 + 2^m(1 + 2^{m-2}) \equiv 1 \bmod 2^m$$

ist j eine Involution. Weiter seien

$$j_1 := (-1 + 2^{m-1}) + 2^m\mathbb{Z} \qquad \text{und} \qquad j_2 := -1 + 2^m\mathbb{Z}.$$

Einfache Rechnungen zeigen, daß auch j_1, j_2 Involutionen sind, deren Produkt gerade j ist. Durch vollständige Induktion läßt sich beweisen, daß

$$1 + 2^{m-1} \equiv 5^{2^{m-3}} \bmod 2^m$$

für $m \geq 3$ ist. Wegen $q = 2$ und $m \geq 3$ hat E folgende Gestalt:

$$E = \langle j_2 \rangle \times \langle z \rangle,$$

wobei z durch $z := 5 + 2^m\mathbb{Z}$ definiert ist. Es gilt dann $\mathrm{ord}(z) = 2^{m-2}$ und $j = z^{2^{m-3}}$. Daher ist $\langle j \rangle$ die minimale Untergruppe von $\langle z \rangle$ und liegt in allen nicht-trivialen Untergruppen von $\langle z \rangle$. Jedes Element x von E läßt sich auf eindeutige Weise schreiben als

$$x = j_2^k \cdot z^l \text{ mit } k \in \{0,1\} \text{ und } l \in \{0,\ldots,2^{m-2}-1\}.$$

Ist jetzt V eine Untergruppe von E, dann ergeben sich folgende Fälle:

Fall 1. Es gibt ein $v \in V$ mit $v = j_2^k \cdot z^l$, wobei $k \in \{0,1\}$ und $l \in \{1,\ldots,2^{m-2}-1\} \backslash \{2^{m-3}\}$ ist. Wegen der Wertebereiche von l und k ist dann:

$$v^2 = j_2^{2k} \cdot z^{2l} = z^{2l} \neq 1.$$

Also ist $\langle v^2 \rangle$ eine nicht-triviale Untergruppe von $\langle z \rangle$, die auch $\langle j \rangle$ enthält. Womit gezeigt ist, daß $j \in V$ ist.

Fall 2. Für V gilt:

$$\begin{aligned} V &\subseteq \{j_2^k \cdot z^l | k \in \{0,1\} \text{ und } l \in \{0, 2^{m-3}\}\} \\ &= \{1, z^{2^{m-3}}, j_2, j_2 z^{2^{m-3}}\} \\ &= \{1, j, j_2, j_1\}. \end{aligned}$$

Ist V nicht trivial und liegt j nicht in V, dann bleibt nur noch die Möglichkeit, daß $V = \langle j_1 \rangle$ oder $V = \langle j_2 \rangle$ ist.

Beide Fälle zusammengefaßt ergeben, daß die beiden Gruppen $\langle j_1 \rangle$ und $\langle j_2 \rangle$ die einzigen nicht-trivialen Untergruppen von E sind, die j nicht enthalten.

Gilt nun a) nicht, so darf $\tilde{H}$, wie wir erst gesehen haben, j nicht enthalten, und muß deshalb eine dieser beiden Gruppen sein. Wegen der Isomorphie zu H ergibt sich sofort:

$$K[\theta] : K = 2.$$

Weiter ist jetzt klar, daß H von einem Element erzeugt wird. Dieses heiße α. Ist $\tilde{H} = \langle j_1 \rangle$, dann ergibt sich

$$\alpha(\theta) = \theta^{-1+2^{m-1}},$$

woraus folgt:

$$\alpha(\theta^2) = \theta^{-2+2^m} = \theta^{-2}.$$

Andernfalls ist

$$\alpha(\theta^2) = \theta^{-2}.$$

Da $m \geq 3$ ist, muß $\theta^4 \neq 1$ sein, weshalb $\alpha(\theta^2) \neq \theta^2$ gilt. Weil aber alle Elemente aus K unter α fest bleiben, kann θ^2 nicht in K liegen, also ist

$$K[\theta] = K[\theta^2] \qquad \text{und} \qquad K[\theta^2] : K = 2,$$

was gerade b) besagt. Die Fallunterscheidung ist damit vollständig, da für $q = 2$ und $m = 1$ die Voraussetzungen des Satzes nicht erfüllt sind.

2) Der Beweis erfolgt mittels vollständiger Induktion über i. Für $i = 0$ ist die Aussage sicher richtig. Sei also $0 < i \leq c - 1$ und die Behauptung für $i - 1$ schon bewiesen. Dann gilt:

$$K[\theta] : K[\theta^{q^{i-1}}] = q^{i-1}.$$

Daraus folgt:

$$K[\theta^{q^{i-1}}] : K = q^{c-i+1}s.$$

Wegen $i \leq c - 1$ ist q^2 ein Teiler von $(K[\theta^{q^{i-1}}] : K)$. Weiter ist $\theta^{q^{i-1}}$ eine primitive q^{c-i+1}-te Einheitswurzel. Mit Teil 1) erhalten wir

$$K[\theta^{q^{i-1}}] : K[\theta^{q^i}] = q.$$

Also ist $K[\theta] : K[\theta^{q^i}] = q^{i-1} \cdot q = q^i$.

3) Wegen Teil 2) gilt $K[\theta] : K[\theta^{q^{c-1}}] = q^{c-1}$. Also ist

$$K[\theta^{q^{c-1}}] : K = \frac{K[\theta] : K}{K[\theta] : K[\theta^{q^{c-1}}]} = \frac{q^c \cdot s}{q^{c-1}} = qs.$$

Da $\theta^{q^{c-1}}$ eine primitive q^{m-c+1}-te Einheitswurzel ist, liefert Teil 1), daß entweder $K[\theta^{q^{c-1}}] : K[\theta^{q^c}] = q$ gilt, woraus $K[\theta] : K[\theta^{q^c}] = q^{c-1} \cdot q = q^c$ folgt, oder $q = 2,\ c \leq m - 2$ und $K[\theta^{2^{c-1}}] = K[\theta^{2^c}]$ richtig ist.

4) Es sei $H_i := \mathrm{Gal}(K[\theta]/K[\theta^{q^i}])$. Nach Voraussetzung ist H nicht zyklisch, also ist $\tilde{H}$ nicht zyklisch und damit E auch nicht. Es ist bekannt, daß E genau dann nicht zyklisch ist, falls $q = 2$ und $m \geq 3$ ist. Deshalb ist $|H_i| = 2^i$ für $0 \leq i \leq c-1$ nach 2). Weil $|H| = K[\theta] : K = 2^c$ gilt, ergibt sich für die Ordnung von E folgendes:

$$|E| = |(\mathbb{Z}/2^m\mathbb{Z})^*| = 2^{m-1}.$$

Also ist

$$|E : \tilde{H}| = \frac{|E|}{|\tilde{H}|} = \frac{|E|}{|H|} = 2^{m-1-c}.$$

Es ist weiter bekannt, daß $E = \langle -1+2^m\mathbb{Z}\rangle \times \langle 5+2^m\mathbb{Z}\rangle$ mit $|\langle 5+2^m\mathbb{Z}\rangle| = 2^{m-2}$ ist. Aus $5 + 2^m\mathbb{Z} \in E$, folgt $(5 + 2^m\mathbb{Z})\tilde{H} \in E/\tilde{H}$. Also ergibt sich:

$$((5 + 2^m\mathbb{Z})\tilde{H})^{|E/\tilde{H}|} = 1_{E/\tilde{H}} = \tilde{H}.$$

Das bedeutet, daß $(5 + 2^m\mathbb{Z})^{2^{m-1-c}} = (5^{2^{m-1-c}} + 2^m\mathbb{Z})$ in $\tilde{H}$ liegt und es ein Urbild $\beta \in H$ gibt mit

$$\beta(\theta) = \theta^{5^{2^{m-1-c}}}.$$

Sei jetzt $0 \leq i \leq c-1$. Wegen $|\langle 5 + 2^m\mathbb{Z}\rangle| = 2^{m-2}$ folgt:

$$(*) \qquad |\langle 5^{2^{m-2-i}} + 2^m\mathbb{Z}\rangle| = \frac{2^{m-2}}{2^{m-2-i}} = 2^i.$$

Sei $\alpha := \beta^{2^{c-1-i}}$, so liegt α insbesondere in H, und es ist

$$\alpha(\theta) = \theta^{(5^{2^{m-1-c}})^{2^{c-1-i}}} = \theta^{5^{2^{m-2-i}}}.$$

Zusammen mit $(*)$ ergibt sich $|\langle\alpha\rangle| = 2^i$. Also ist

$$\alpha(\theta^{2^i}) = (\theta^{2^i})^{5^{2^{m-2-i}}} = \theta^{2^i \cdot 5^{2^{m-2-i}}}.$$

Wegen $0 \leq i \leq c-1 \leq m-1-1 = m-2$ ist $m-i \geq 2$. Man kann leicht durch Induktion über $m-i$ zeigen, daß die Kongruenz $5^{2^{m-2-i}} \equiv 1 \bmod 2^{m-i}$ für alle $0 \leq i \leq c-1$ richtig ist. Also gibt es ein $x \in \mathbb{Z}$ mit $2^{m-i} \cdot x = 5^{2^{m-2-i}} - 1$, woraus $2^m \cdot x = 2^i \cdot 5^{2^{m-2-i}} - 2^i$ folgt. Dadurch erhalten wir

$$2^i \cdot 5^{2^{m-2-i}} \equiv 2^i \bmod 2^m.$$

Weil θ eine 2^m-te Einheitswurzel ist, ergibt sich nun

$$\alpha(\theta^{2^i}) = \theta^{2^i \cdot 5^{2^{m-2-i}}} = \theta^{2^i}.$$

Damit liegt θ^{2^i} im Fixkörper von α, also auch $K[\theta^{2^i}]$, und es muß $\langle\alpha\rangle \subseteq H_i$ sein. Da andrerseits aber $|\langle\alpha\rangle| = |H_i| = 2^i$ ist, ist $\langle\alpha\rangle = H_i$ und H_i zyklisch für alle $0 \leq i \leq c-1$. $\square$

4 Beschreibung der Gruppenalgebra einer endlichen abelschen Gruppe

Sei G eine endliche abelsche Gruppe, K ein Körper, dessen Charakteristik die Ordnung von G nicht teilt, und KG die Gruppenalgebra von G über K. Nach einem Satz von Maschke ist KG halbeinfach und läßt sich nach einem Satz von Wedderburn zerlegen als

$$KG = B_1 \oplus \cdots \oplus B_b.$$

$B_1, \ldots, B_b$ sind dabei die homogenen Komponenten von KG. Da G abelsch ist, ist KG kommutativ, damit sind $B_1, \ldots, B_b$ Körper und außerdem sämtliche verschiedenen, irreduziblen KG-Teilmoduln von KG. Insbesondere sind B_i und B_j für $i, j \in \{1, \ldots, b\}$ genau dann KG-isomorph, wenn $i = j$ gilt. Es kann aber durchaus sein, daß B_i und B_j mit $i \neq j$ als Körper isomorph sind. Weiter ist jeder irreduzible KG-Modul zu einem B_i isomorph.

Sei jetzt $e := \exp(G)$ der Exponent von G und $F := \mathrm{Zerf}_K(X^e - 1)$ der Zerfällungskörper von $X^e - 1$ über K. Weiter sei $\tilde{G}$ die Menge der e-ten Einheitswurzeln von F. Dann ist $\tilde{G}$ zyklisch und $|\tilde{G}| = e$. Mit G^* werde die Menge aller Homomorphismen von G in $\tilde{G}$ bezeichnet. Sei nun $\lambda \in G^*$ und $\hat{\lambda}$ die K-lineare Fortsetzung von λ auf KG. Dann ist $\hat{\lambda}$ ein K-Algebra-Homomorphismus von KG in $F = K[\tilde{G}]$; denn $\hat{\lambda}$ ist nach Konstruktion K-linear und für $\sum_{g \in G} k_g g, \sum_{g \in G} l_g g \in KG$ gilt:

$$\begin{aligned}
\hat{\lambda}\Big(\sum_{g \in G} k_g g\Big) \cdot \hat{\lambda}\Big(\sum_{g \in G} l_g g\Big) &= \Big(\sum_{g \in G} k_g \lambda(g)\Big) \cdot \Big(\sum_{g \in G} l_g \lambda(g)\Big) \\
&= \sum_{g \in G} \Big(\sum_{h \in G} k_h l_{h^{-1}g}\Big) \lambda(g) \\
&= \hat{\lambda}\Big(\sum_{g \in G} \Big(\sum_{h \in G} k_h l_{h^{-1}g}\Big) g\Big) \\
&= \hat{\lambda}\Big(\Big(\sum_{g \in G} k_g g\Big) \cdot \Big(\sum_{g \in G} l_g g\Big)\Big).
\end{aligned}$$

Sei $G^\lambda := \mathrm{Bild}\lambda$, dann ist $\mathrm{Bild}\hat{\lambda} = K[G^\lambda]$ und insbesondere ein Teilkörper von F. Denn wegen $G^\lambda \subseteq \tilde{G}$ gilt $K[G^\lambda] \subseteq K[\tilde{G}] = F$; außerdem ist F eine endliche und daher algebraische Erweiterung von K, weshalb $K[G^\lambda]$ ein Körper ist. $\hat{\lambda}$ ist ein Ringepimorphismus von KG auf $K[G^\lambda]$ und

$$\mathrm{Bild}\hat{\lambda} \cong KG / \ker \hat{\lambda}.$$

Nun ist aber $\mathrm{Bild}\hat{\lambda}$ ein Körper, also ist $\ker \hat{\lambda}$ ein maximales Ideal von KG. Die maximalen Ideale von KG sind aber genau die paarweise verschiedenen Ideale

$$W_i := B_1 \oplus \cdots \oplus B_{i-1} \oplus B_{i+1} \oplus \cdots \oplus B_b$$

für $i \in \{1, \ldots, b\}$. Also gibt es genau ein $i \in \{1, \ldots, b\}$ mit $\ker \hat{\lambda} = W_i$. Es gilt dann

$$\mathrm{Bild}\hat{\lambda} \cong KG/W_i \cong B_i.$$

Insbesondere sind Bild$\hat{\lambda}$ und B_i als Körper isomorph.

Wir wollen nun umgekehrt zeigen, daß es zu jedem B_i ein $\lambda \in G^*$ gibt mit Bild$\hat{\lambda} = B_i$. Dazu sei e_i das Einselement von B_i für $i \in \{1, \ldots, b\}$. Die Abbildung von K auf Ke_i, bei der k in $k \cdot e_i$ übergeht, ist wegen $e_i^2 = e_i$ ein Körperisomorphismus von K auf Ke_i. Sei weiter $H := \{ge_i | g \in G\}$. Weil B_i ein irreduzibler KG-Modul ist, ist $B_i = KGe_i$. Also liegen H und Ke_i in B_i und $Ke_i[H]$ ist ein Zwischenkörper der Körpererweiterung B_i/Ke_i. Für ein $x \in B_i$, das sich ja als $x = \sum_{g \in G} k_g g \cdot e_i$, wobei $\sum_{g \in G} k_g g \in KG$ ist, darstellen läßt, folgt dann

$$x = \sum_{g \in G} k_g g e_i^2 = \sum_{g \in G} k_g e_i g e_i,$$

also ist $x \in Ke_i[H]$ und damit $B_i = Ke_i[H]$. Wegen $(ge_i)^{|G|} = g^{|G|} e_i^{|G|} = e_i$ für alle $g \in G$, enthält H nur $|G|$-te Einheitswurzeln (von e_i). Es gibt daher einen Zwischenkörper von F/K, der zu B_i isomorph ist. Sei τ ein Isomorphismus von B_i auf diesen Zwischenkörper, sei weiter σ der Isomorphismus von KG/M_i auf B_i und schließlich κ der kanonische Epimorphismus von KG auf KG/M_i. Dann ist die Abbildung $\mu := \tau \circ \sigma \circ \kappa$ ein Epimorphismus von KG auf einen Zwischenkörper von F/K, der isomorph zu B_i ist. Bezeichnet λ die Einschränkung von μ auf G, so ist λ wegen $g^{|G|} = 1$ ein Homomorphismus von G in $\tilde{G}$. Dann ist $\lambda \in G^*$ und $\hat{\lambda} = \mu$. Damit gibt es zu jedem B_i ein $\lambda \in G^*$, so daß Bild$\hat{\lambda} \cong B_i$ gilt.

Sei jetzt $\lambda \in G^*$ und $x \in K[G^\lambda]$, sowie $r \in KG$, dann wird $K[G^\lambda]$ durch die Festlegung $r \cdot x = \hat{\lambda}(r) \cdot x$ zu einem KG-Modul, welcher mit M_λ bezeichnet wird. Wegen $s \cdot \hat{\lambda}(r) = \hat{\lambda}(s) \cdot \hat{\lambda}(r) = \hat{\lambda}(r \cdot s)$ für $r, s \in KG$ ist $\hat{\lambda}$ dann sogar ein KG-Epimorphismus von KG auf M_λ. Weiter gibt es, wie schon gesehen, genau ein $i \in \{1, \ldots, b\}$, so daß $\ker \hat{\lambda} = M_i$ ist. Das heißt, es gibt zu jedem M_λ ein $i \in \{1, \ldots, b\}$, so daß M_λ und B_i als KG-Moduln isomorph sind. Dieses i ist eindeutig, da B_i und B_j für $i \neq j$ nicht KG-isomorph sind.

Hilfssatz 4.1 *Seien $\lambda, \mu \in G^*$. Dann sind äquivalent:*

1. *M_λ und M_μ sind KG-isomorph.*

2. *Es gibt ein $\alpha \in \mathrm{Gal}(F/K)$ mit $\alpha \circ \lambda = \mu$.*

Beweis: „1) $\Rightarrow$ 2)“: Seien $\lambda, \mu \in G^*$ und $M_\lambda \cong M_\mu$ als KG-Moduln. Dann sind, wie schon gesehen, $\hat{\lambda}$ bzw. $\hat{\mu}$ zwei KG-Epimorphismen von KG auf M_λ bzw. M_μ, und es gibt genau ein i und ein j aus $\{1, \ldots, b\}$ mit $M_\lambda \cong B_i$ und $M_\mu \cong B_j$ als KG-Moduln. Weil M_λ und M_μ als KG-Moduln isomorph sind, muß $i = j$ sein. Also ist

$$\ker \hat{\lambda} = B_1 \oplus \cdots \oplus B_{i-1} \oplus B_{i+1} \oplus \cdots \oplus B_b = \ker \hat{\mu}$$

und damit $B_i^{\hat\lambda} = \mathrm{Bild}\hat\lambda$ sowie $B_i^{\hat\mu} = \mathrm{Bild}\hat\mu$. Insbesondere ist $\hat\lambda|_{B_i}$ bzw. $\hat\mu|_{B_i}$ ein K-Isomorphismus von B_i auf $\mathrm{Bild}\hat\lambda$ bzw. $\mathrm{Bild}\hat\mu$. Damit ist $(\hat\lambda|_{B_i})^{-1}$ eine wohldefinierte Abbildung von $B_i^{\hat\lambda}$ auf B_i, und wir können den K-Isomorphismus α_0 von $\mathrm{Bild}\hat\lambda$ auf $\mathrm{Bild}\hat\mu$ durch

$$\alpha_0 := \hat\mu \circ (\hat\lambda|_{B_i})^{-1}$$

definieren. α_0 ist also ein K-Isomorphismus von $K[G^\lambda]$ auf $K[G^\mu]$, welche beide Zwischenkörper von F/K sind. Da F/K galoissch ist, läßt sich α_0 zu einem K-Automorphismus α von F fortsetzen, welcher offensichtlich ein Element von $\mathrm{Gal}(F/K)$ ist. Sei nun $g \in G$. Dann gilt:

$$\begin{aligned}
(\alpha\circ\lambda)(g) &= \alpha(\lambda(g)) \\
&= \alpha_0(\lambda(g)), \text{ da } \lambda(g) \in \mathrm{Bild}\hat\lambda \\
&= (\hat\mu \circ (\hat\lambda|_{B_i})^{-1} \circ \lambda)(g) \\
&= \hat\mu(g) \\
&= \mu(g).
\end{aligned}$$

Also ist $\alpha\circ\lambda = \mu$.

„2) $\Rightarrow$ 1)“: Seien nun $\lambda, \mu \in G^*$ und $\alpha \in \mathrm{Gal}(F/K)$ mit $\alpha\circ\lambda = \mu$. Dann zeigt eine einfache Rechnung, daß $\alpha \circ \hat\lambda = \hat\mu$ ist. Wir setzen $\alpha_0 := \alpha|_{\mathrm{Bild}\hat\lambda}$. Dann ist $\alpha_0 \circ \hat\lambda = \hat\mu$ und deshalb α_0 ein Körperisomorphismus von $\mathrm{Bild}\hat\lambda$ auf $\mathrm{Bild}\hat\mu$. Für $x \in \mathrm{Bild}\hat\lambda$ und $\sum_{g\in G} k_g g \in KG$ gilt:

$$\begin{aligned}
\alpha_0\left(\left(\sum_{g\in G} k_g g\right)\cdot x\right) &= \alpha_0\left(\hat\lambda\left(\sum_{g\in G} k_g g\right)\cdot x\right) \\
&= (\alpha_0\circ\hat\lambda)\left(\sum_{g\in G} k_g g\right)\cdot \alpha_0(x) \\
&= \hat\mu\left(\sum_{g\in G} k_g g\right)\cdot \alpha_0(x) \\
&= \left(\sum_{g\in G} k_g g\right)\cdot \alpha_0(x).
\end{aligned}$$

Damit ist α_0 sogar KG-linear, was beweist, daß M_λ und M_μ als KG-Moduln isomorph sind. $\square$

Es läßt sich jetzt eine detailliertere Beschreibung der Zerlegung von KG finden. Die Abbildung φ von $\mathbb{N}$ in $\mathbb{N}$ bezeichnet von nun an immer die Eulersche Totienten-Funktion. Ferner sei F_l der Zerfällungskörper von $X^l - 1$ über K in F.

Satz 4.2 *Es ist*

$$KG \cong \bigoplus_{\substack{U \leq G \\ G/U \text{zyklisch}}} F_{|G/U|} \oplus \cdots \oplus F_{|G/U|}$$

als K-Algebra, wobei die Anzahl der Summanden jeweils gleich

$$\frac{\varphi(|G/U|)}{F_{|G/U|} : K}$$

ist. Diejenigen irreduziblen Teilmoduln von KG, deren Zentralisator in G gerade U ist, sind dabei zu $F_{|G/U|}$ als K-Algebra isomorph.

Beweis: Für $\lambda \in G^*$ und $\alpha \in \mathrm{Gal}(F/K)$ ist $\alpha \circ \lambda$ offensichtlich ein Homomorphismus von G in $\tilde{G}$. Daher operiert $\mathrm{Gal}(F/K)$ auf G^* via $\lambda^\alpha \longrightarrow \alpha \circ \lambda$. Weiter ist $\ker \lambda = \ker(\alpha \circ \lambda)$, denn:

Sei $x \in \ker \lambda$, dann ist $\lambda(x) = 1_F$ und deshalb

$$(\alpha \circ \lambda)(x) = \alpha(1_F) = 1_F.$$

Ist andrerseits $x \in \ker(\alpha \circ \lambda)$, so folgt $(\alpha \circ \lambda)(x) = 1_F$ und damit

$$\lambda(x) = (\alpha^{-1} \circ \alpha \circ \lambda)(x) = \alpha^{-1}(1_F) = 1_F.$$

Für $\lambda \in G^*$ ist $\mathrm{Bild}\lambda \cong G/\ker \lambda$ zyklisch, da $\mathrm{Bild}\lambda$ eine Untergruppe der zyklischen Gruppe $\tilde{G}$ ist. Wir wollen jetzt zeigen, daß es für jede Untergruppe $U \subseteq G$, für die G/U zyklisch ist, genau $\varphi(|G/U|)$ Elemente in G^* gibt, deren Kern gerade U ist. Sei jetzt also U eine Untergruppe von G, für die G/U zyklisch ist. Dann gilt:

G/U ist isomorph zu genau einer Untergruppe $\tilde{U}$ von $\tilde{G}$.

Nach Definition ist $e = \exp(G) = |\tilde{G}|$. Da G/U zyklisch ist, folgt $\exp(G/U) = |G/U|$. Ist nun $gU \in G/U$, so gilt $(gU)^e = g^eU = U$, also wird e von $\exp(G/U)$ geteilt. Daraus folgt, daß $|G/U|$ ein Teiler von e ist, d.h. $|G/U|$ ist ein Teiler von $|\tilde{G}|$. Deshalb hat $\tilde{G}$ genau eine zyklische Untergruppe $\tilde{U}$ der Ordnung $|G/U|$ und diese ist zu G/U isomorph.

Es gibt ein $\mu \in G^*$ mit $\ker \mu = U$ und $\mathrm{Bild}\mu = \tilde{U}$.

Dazu wählen wir $\mu := \psi \circ \kappa$, wobei κ der kanonische Epimorphismus von G auf G/U und ψ ein Isomorphismus von G/U auf $\tilde{U}$ ist. μ ist dann sicher ein Homomorphismus von G in $\tilde{G}$ mit $\ker \mu = U$ und $\mathrm{Bild}\mu = \tilde{U}$.

Sei jetzt $G^*(U) := \{\lambda \in G^* | \ker \lambda = U\}$. Dann ist $G^*(U) = \{\alpha \circ \mu | \alpha \in \mathrm{Aut}(\tilde{U})\}$.

„$\supseteq$“: Weil $K[\tilde{U}]/K$ eine Galoiserweiterung ist, die in F enthalten ist, induziert jedes $\alpha \in \mathrm{Aut}(\tilde{U})$ einen K-Automorphismus auf $K[\tilde{U}]$, der zu einem K-Automorphismus α' auf F fortgesetzt werden kann. Da $\mathrm{Bild}\mu = \tilde{U}$ ist, folgt dann die Behauptung:

$$\ker(\alpha \circ \mu) = \ker(\alpha'|_{\tilde{U}} \circ \mu) = \ker(\alpha' \circ \mu) = \ker \mu = U.$$

„$\subseteq$": Sei $\lambda \in G^*(U)$. Da es genau eine Untergruppe $\tilde{U}$ von $\tilde{G}$ gibt, die zu G/U isomorph ist, gilt: $\text{Bild}\mu = \text{Bild}\lambda = \tilde{U}$. Also gibt es ein $\alpha \in \text{Aut}(\tilde{U})$ mit $\alpha \circ \mu = \lambda$.

Offenbar gilt $\alpha \circ \mu = \beta \circ \mu$ für $\alpha, \beta \in \text{Aut}(\tilde{U})$ genau dann, wenn $\alpha = \beta$ ist. Da G/U zyklisch ist, ergibt sich

$$|G^*(U)| = |\text{Aut}(\tilde{U})| = |\text{Aut}(G/U)| = \varphi(|G/U|).$$

Sei jetzt $\lambda \in G^*(U)$. Wegen $|G^\lambda| = |G/U|$ und $G^\lambda \subseteq \tilde{G}$ ist dann G^λ die Gruppe der $|G/U|$-ten Einheitswurzeln. Damit ist $\text{Bild}\hat{\lambda} = K[G^\lambda]$ der Zerfällungskörper von $X^{|G/U|} - 1$ über K in F, der $F_{|G/U|}$ heißt. Sei weiter $0 \neq x \in M_\lambda$ und $g \in G$, dann gilt:

$$\begin{aligned} g \cdot x = x \quad &\iff \quad \lambda(g) \cdot x = x \\ &\iff \quad g \in U, \text{ da } \ker\lambda = U \text{ ist.} \end{aligned}$$

Also ist der Zentralisator von M_λ in G gerade U.

Trivialerweise gilt für $\lambda \in G^*$ und $\alpha \in \text{Gal}(F/K)$ folgendes:

$$\alpha \circ \lambda = \lambda \iff \alpha|_{G^\lambda} = \text{id}|_{G^\lambda} \iff \alpha|_{K[G^\lambda]} = \text{id}|_{K[G^\lambda]}.$$

Insbesondere gilt für $\lambda \in G^*(U)$:

$$\alpha \circ \lambda = \lambda \iff \alpha \in \text{Gal}(F_{|G/U|}/K).$$

Damit zerfällt $G^*(U)$ unter $\text{Gal}(F/K)$ in

$$\frac{|G^*(U)|}{|\text{Gal}(F_{|G/U|}/K)|} = \frac{\varphi(|G/U|)}{F_{|G/U|} : K}$$

Bahnen. Als nächstes soll gezeigt werden:

Sind $\lambda, \mu \in G^*$, so sind M_λ und M_μ genau dann KG-isomorph, wenn es eine Untergruppe U von G gibt, so daß G/U zyklisch ist, sowie $\lambda, \mu \in G^*(U)$ gilt, und λ, μ in derselben Bahn von $G^*(U)$ unter $\text{Gal}(F/K)$ liegen.

„$\Rightarrow$": Wegen $M_\lambda \cong M_\mu$ ist sicherlich $\ker\lambda = \ker\mu$. Nun wurde aber bereits erwähnt, daß $G/\ker\lambda$ zyklisch ist, also gilt $\lambda, \mu \in G^*(\ker\lambda)$. Aus 4.1 folgt, daß es ein $\alpha \in \text{Gal}(F/K)$ gibt mit $\alpha \circ \lambda = \mu$. Also liegen λ und μ in derselben Bahn von $G^*(\ker\lambda)$ unter $\text{Gal}(F/K)$.

„$\Leftarrow$": Seien nun $\lambda, \mu \in G^*(U)$. Da λ und μ in derselben Bahn unter $\text{Gal}(F/K)$ liegen, gibt es ein $\alpha \in \text{Gal}(F/K)$ mit $\alpha \circ \lambda = \mu$. Nach 4.1 sind dann M_λ und M_μ als KG-Moduln isomorph.

Das bedeutet, für $\lambda, \mu \in G^*$ sind M_λ und M_μ genau dann nicht KG-isomorph, wenn entweder $\ker\lambda \neq \ker\mu$ ist oder $\lambda, \mu \in G^*(\ker\lambda)$ gilt und λ, μ in verschiedenen Bahnen von $G^*(\ker\lambda)$ unter $\text{Gal}(F/K)$ liegen.

Da es zu jedem M_λ genau ein $i \in \{1, \ldots, b\}$ gibt, so daß M_λ und B_i als KG-Moduln isomorph sind, und man umgekehrt zu jedem B_i ein KG-isomorphes M_λ finden kann, ist KG als KG-Modul isomorph zur direkten

Summe über alle paarweise nicht KG-isomorphen M_λ mit $\lambda \in G^*$. Weil eine Untergruppe U von G genau dann Kern eines Homomorphismus $\lambda \in G^*$ ist, wenn G/U zyklisch ist, folgt mit dem oben gezeigten:

$$KG \cong \bigoplus_{\substack{U \leq G \\ G/U zyklisch}} M_{\lambda_1}^{(U)} \oplus \cdots \oplus M_{\lambda_{\varphi(|G/U|)/(F_{|G/U|}:K)}}^{(U)}$$

als KG-Moduln, wobei $M_{\lambda_i}^{(U)}$ Repräsentanten der Bahnen von $G^*(U)$ unter $\mathrm{Gal}(F/K)$ sind. Wie wir gesehen haben gilt $M_{\lambda_i}^{(U)} \cong F_{|G/U|}$ als K-Algebren für alle $i = 1, \ldots, \varphi(|G/U|)/(F_{|G/U|} : K)$. Daraus folgt die Behauptung. $\square$

5 Der Schluß des Beweises zur Existenz vollständig freier Elemente in endlich separablen Körpererweiterungen

Sei nun L/K eine endliche Galoiserweiterung, sowie $G := \mathrm{Gal}(L/K)$ eine zyklische q-Gruppe mit $|G| = q^n$ und q ungleich der Charakteristik von K. Dann hat G genau $n+1$ Untergruppen $G_0, \ldots, G_n$, die sich so numerieren lassen, daß

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

gilt. Dabei ist $|G_i| = q^{n-i}$ für $0 \leq i \leq n$. Da die Erweiterung galoissch ist, gibt es eine entsprechende Kette aller Zwischenkörper K_i von L/K mit

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L,$$

wobei $G_i = \mathrm{Gal}(L/K_i)$ ist. Offenbar gilt dann $K_{i+1} : K_i = q$ für alle $0 \leq i \leq n-1$.

Als $L(i)$ sei nun der K_iG_i-Modul L bezeichnet. Weil L/K_i galoissch ist, sind dann, wie schon gezeigt, $L(i)$ und K_iG_i als K_iG_i-Moduln isomorph. Außerdem ist $L(i)$ halbeinfach, da die Charakteristik von K kein Teiler von $|G|$ ist.

Jeder Teilmodul von $L(i)$ ist offensichtlich auch ein G_i-Modul und als solcher genau dann treu, wenn id_L das einzige Element von G_i ist, das auf diesem Teilmodul trivial operiert.

Weiter bezeichne $T(i)$ die Summe aller irreduziblen G_i-treuen Teilmoduln von $L(i)$, sowie $U(i)$ die Summe aller irreduziblen G_i-untreuen Teilmoduln von $L(i)$ für $0 \leq i \leq n$. Im Spezialfall $i = n$ ist $L(n)$ wegen $G_n = \{\mathrm{id}_L\}$ ein L-Vektorraum. Dieser ist sicherlich G_n-treu und wegen $\dim_L L(n) = 1$ auch irreduzibel. Daher ist $T(n) = L$, und es ist sinnvoll, $U(n) := \{0\}$ zu setzen. Weil $L(i)$ als halbeinfacher Modul die Summe seiner irreduziblen Teilmoduln ist, folgt

$$L(i) = U(i) \oplus T(i) \qquad \text{für } 0 \leq i \leq n.$$

Definition 5.1 *Die Abbildung* $\mathrm{Tr}_{L/K_{n-1}}$ *von* L *auf* K_{n-1}*, die durch*

$$\mathrm{Tr}_{L/K_{n-1}}(l) = \sum_{g \in G_{n-1}} g(l)$$

definiert ist, heißt die Spur von L auf K_{n-1}.

Es ist bekannt, daß $\mathrm{Tr}_{L/K_{n-1}}$ ein K_{n-1}-Epimorphismus ist. Weiter gilt:

$$K_{n-1} \cap \ker(\mathrm{Tr}_{L/K_{n-1}}) = \{0\}.$$

Denn für $k \in K_{n-1}^*$ folgt $\mathrm{Tr}_{L/K_{n-1}}(k) = \sum_{g \in G_{n-1}} g(k) = |G_{n-1}| \cdot k \neq 0$, da die Charakteristik von K kein Teiler von $|G_{n-1}|$ ist.

Es ist $L = K_{n-1} + \ker(\mathrm{Tr}_{L/K_{n-1}})$.

Denn: Für $l \in L$ sei

$$k := \frac{\mathrm{Tr}_{L/K_{n-1}}(l)}{|G_{n-1}|},$$

wobei $|G_{n-1}|$ als $\sum_{i=1}^{|G_{n-1}|} 1_{K_{n-1}}$ zu verstehen ist. Dann ist k wohldefiniert, weil char $K \not| \, |G_{n-1}|$ gilt, und liegt außerdem in K_{n-1}. Jetzt läßt sich l schreiben als $l = l - k + k$. Es gilt:

$$\begin{aligned} \mathrm{Tr}_{L/K_{n-1}}(l-k) &= \mathrm{Tr}_{L/K_{n-1}}(l) - \mathrm{Tr}_{L/K_{n-1}}(k) \\ &= \mathrm{Tr}_{L/K_{n-1}}(l) - k \cdot \mathrm{Tr}_{L/K_{n-1}}(1) \\ &= \mathrm{Tr}_{L/K_{n-1}}(l) - \frac{\mathrm{Tr}_{L/K_{n-1}}(l)}{|G_{n-1}|} \cdot |G_{n-1}| = 0. \end{aligned}$$

Also ist $(l-k) \in \ker(\mathrm{Tr}_{L/K_{n-1}})$ und es folgt die Behauptung.

Zusammengefaßt ergibt sich

$$L = K_{n-1} \oplus \ker(\mathrm{Tr}_{L/K_{n-1}}).$$

Da G_{n-1} ein Normalteiler von G ist, folgt $g(K_{n-1}) \subseteq K_{n-1}$ für alle $g \in G$. Man kann daher aus K_{n-1} einen K_iG_i-Modul für $0 \leq i \leq n-1$ machen, der jetzt $K_{n-1}(i)$ genannt wird. Sei nun $0 \leq i \leq n-1$ und V ein Teilmodul von $K_{n-1}(i)$. Wegen $\{\mathrm{id}_L\} \neq G_{n-1} \subseteq G_i$ gibt es ein von id_L verschiedenes Element in G_{n-1}, welches also auch in G_i liegt, das trivial auf K_{n-1} und damit auch trivial auf V operiert. Daher ist $K_{n-1} \subseteq U(i)$ für $0 \leq i \leq n-1$.

Sei wieder $0 \leq i \leq n-1$. Ferner sei V ein Teilmodul von $L(i)$, der als G_i-Modul nicht treu ist. Das bedeutet, es gibt ein Element g in $G_i \backslash \{\mathrm{id}_L\}$, das trivial auf V operiert. Dann operiert auch $\langle g \rangle$ trivial auf V. Weil G_{n-1} in jeder von $\{\mathrm{id}_L\}$ verschiedenen Untergruppe von G enthalten ist, bleibt jedes Element aus V insbesondere unter allen Elementen von G_{n-1} fest. Also ist V eine Teilmenge von K_{n-1}, d.h. $U(i) \subseteq K_{n-1}$ für $0 \leq i \leq n-1$. Zusammengefaßt ergibt sich damit

$$K_{n-1} = U(i) \qquad \text{für } 0 \leq i \leq n-1.$$

Wegen der Eindeutigkeit der Komplemente folgt daraus:

$$T(i) = \ker(\mathrm{Tr}_{L/K_{n-1}}) \qquad \text{für } 0 \leq i \leq n-1.$$

Wir setzen jetzt $T := \ker(\mathrm{Tr}_{L/K_{n-1}})$. Weiter sei $z_i := \{T_1(i), \ldots, T_{r(i)}(i)\}$ die Menge der G_i-treuen irreduziblen Teilmoduln von $L(i)$ für $0 \leq i \leq n$. Dann ist z_i für $0 \leq i \leq n-1$ sicherlich eine direkte Zerlegung von T. Für $0 \leq i \leq n-1$ ist K_iG_{i+1} ein Teilring von K_iG_i. Mit $Z_i := \{H_1(i), \ldots, H_{s(i)}(i)\}$ wird die Menge der homogenen Komponenten von T als K_iG_{i+1}-Modul bezeichnet, Z_i ist dann eine direkte Zerlegung von T.

Um z_i und Z_i miteinander in Beziehung setzen zu können, benötigen wir die beiden nächsten Sätze und die darauf folgende Definition.

Satz 5.2 *Sei L/K galoissch mit Galoisgruppe G, ferner M ein Zwischenkörper von L/K, sowie $H := \mathrm{Gal}(L/M)$. Ist dann W ein KH-Teilmodul von L, so ist für alle $m \in M$ mit $m \neq 0$ auch mW ein KH-Teilmodul von L, der KH-isomorph zu W ist. Ist insbesondere L als KH-Modul halbeinfach, so sind die homogenen KH-Komponenten von L auch MH-Teilmoduln.*

Beweis: Sei W ein KH-Teilmodul von L und $m \in M\backslash\{0\}$. Weiter werde die Abbildung $\tau_m : L \longrightarrow L$ durch $\tau_m(l) := ml$ definiert. Dann ist τ_m sicherlich bijektiv und additiv. Außerdem gilt für $\sum_{h\in H} k_h h \in KH$:

$$\begin{aligned}
\tau_m\Bigg(\Bigg(\sum_{h\in H} k_h h\Bigg) l\Bigg) &= m\Bigg(\sum_{h\in H} k_h h(l)\Bigg) \\
&= \sum_{h\in H} k_h h(ml) \\
&= \Bigg(\sum_{h\in H} k_h h\Bigg)\tau_m(l).
\end{aligned}$$

Also ist τ_m ein KH-Automorphismus von L. Daraus folgt, daß W und mW als KH-Moduln isomorph sind.

Ist nun L als KH-Modul halbeinfach und V eine homogene KH-Komponente von L, dann gilt insbesondere $V \cong mV$ für alle $m \in M\backslash\{0\}$. Da V eine homogene Komponente ist, gilt sogar $V = mV$. Deshalb ergibt sich für alle $\sum_{h\in H} m_h h \in MH$ und alle $v \in V$:

$$\sum_{h\in H} m_h h \cdot v = \sum_{h\in H} m_h h(v) \quad \in mV = V.$$

Also ist V auch ein MH-Teilmodul von L. $\Box$

Satz 5.3 (Clifford) *Es sei K ein Körper, G eine Gruppe und H ein Normalteiler von G. Ist M ein irreduzibler KG-Modul, dann ist M ein vollständig reduzibler und homogener KH-Modul [7, V.17.3].*

Definition 5.4 *Seien $X = \{M_1, \ldots, M_r\}$ und $Y = \{N_1, \ldots, N_s\}$ zwei direkte Zerlegungen einer Gruppe M. Dann heißt X* feiner *als Y (geschrieben als $X \geq Y$), falls jedes M_j in einem N_i enthalten ist, bzw.* gröber *($X \leq Y$), falls jedes N_i in einem M_j enthalten ist.*

Ist $X \geq Y$ und $r > s$, so heißt X echt feiner *als Y (geschrieben als $X > Y$). Analog wird X* echt gröber *Y definiert. Ein Element m aus M heißt* X-regulär, *wenn sämtliche Komponenten von m bzgl. der direkten Zerlegung X von Null verschieden sind.*

Bemerkung 5.5 *Sei M eine Gruppe und X, Y zwei Zerlegungen von M. Wenn X feiner als Y ist, ist jedes X-reguläre Element aus M schon Y-regulär. Ist X echt feiner als Y, dann gibt es ein Y-reguläres Element, das nicht X-regulär ist.*

Bemerkung 5.6 *Sei X_i die Menge aller irreduziblen K_iG_i-Teilmoduln von $L(i)$, d.h. X_i ist insbesondere eine direkte Zerlegung von L. Dann ist ein Element x in L/K_i genau dann regulär, wenn es X_i-regulär ist.*

Beweis: Sei $x \in L$ in L/K_i regulär. Nach 2.2 ist x dann in keinem echten Teilmodul von $L(i)$ enthalten. Sei weiter $X_i := \{M_1, \ldots, M_t\}$ und $x := x_1 + \cdots + x_t$, wobei $x_j \in M_j$ ist. Gäbe es nun ein $k \in \{1, \ldots, t\}$, so daß $x_k = 0$ ist, dann wäre x ein Element von $M_1 \oplus \cdots \oplus M_{k-1} \oplus M_k \oplus \cdots \oplus M_t$. Das ist aber ein echter K_iG_i-Teilmodul von $L(i)$. Also ist x doch X_i-regulär.

Sei jetzt x ein X_i-reguläres Element aus L. Wir nehmen nun an, es gäbe einen echten K_iG_i-Teilmodul V von L, in dem x liegt. Dann hätte V auch ein Komplement W in $L(i)$ und $Y = \{V, W\}$ wäre eine direkte Zerlegung von L, die gröber als X_i wäre. Nach 5.5 wäre x auch Y-regulär. Das ergäbe aber einen Widerspruch, da $x \in V$ ist. Also ist x in keinem echten Teilmodul von $L(i)$ enthalten und nach 2.2 damit regulär in L/K_i. □

Sei $\bar{L}$ eine algebraische Hülle von L und $\zeta \in \bar{L}$ eine primitive q^n-te Einheitswurzel. Es ist bekannt, daß dann $K[\zeta] : K = q^l s$ mit einem geeignetem $l \in \{0, \ldots, n-1\}$ und einem s, das $(q-1)$ teilt, ist. Wegen $K \subseteq K[\zeta] \cap L \subseteq L$ und weil G zyklisch ist, gibt es ein $a \in \{0, \ldots, n\}$, so daß $K_a = K[\zeta] \cap L$ ist. Da K_a in $K[\zeta]$ enthalten ist, ist $K_a : K$ ein Teiler von $K[\zeta] : K$, also wird $q^l s$ von q^a geteilt, und es ist $a \leq l$.

Hilfssatz 5.7 *Für $0 \leq i \leq a$ ist $K_i[\zeta] = K[\zeta]$. Außerdem gilt:*

$$K_i[\zeta] : K_i = \begin{cases} q^{l-i}s & \text{für } 0 \leq i \leq a \\ q^{l-a}s & \text{für } a \leq i \leq n. \end{cases}$$

Für $0 \leq i \leq n$ ergibt sich also

$$K_i[\zeta] : K_i = q^{l-\min\{i,a\}}s.$$

Beweis: Sei $0 \leq i \leq a$. Dann ist $K_i \subseteq K_a \subseteq K[\zeta]$ und damit $K_i[\zeta] \subseteq K[\zeta]$. Trivialerweise gilt aber auch $K[\zeta] \subseteq K_i[\zeta]$, also ist $K_i[\zeta] = K[\zeta]$. Daraus folgt:

$$K_i[\zeta] : K_i = \frac{K_i[\zeta] : K}{K_i : K} = \frac{K[\zeta] : K}{K_i : K} = \frac{q^l s}{q^i} = q^{l-i}s.$$

Sei nun $a \leq i \leq n$. Dann ist $K_a \subseteq K_i \cap K[\zeta]$. Andrerseits gilt

$$K_i \cap K[\zeta] \subseteq L \cap K[\zeta] = K_a.$$

Daraus folgt $K_a = K_i \cap K[\zeta]$. Sei nun $m_{K_i,\zeta}$ das Minimalpolynom von ζ über K_i und $f := X^{q^n} - 1$. Offensichtlich ist dann $f(\zeta) = 0$ und, weil f in $K_i[X]$ liegt, muß $m_{K_i,\zeta}$ ein Teiler von f in $K_i[X]$ sein. Da f in $K[\zeta][X]$ zerfällt, zerfällt $m_{K_i,\zeta}$ erst recht in $K[\zeta][X]$. Daher ergibt sich:

$$m_{K_i,\zeta} \in K_i[X] \cap K[\zeta][X] = K_a[X].$$

Weil $m_{K_i,\zeta}$ als Minimalpolynom irreduzibel in $K_i[X]$ ist, ist es auch irreduzibel in $K_a[X]$, d.h. $m_{K_i,\zeta}$ ist das Minimalpolynom von ζ über K_a. Daraus folgt: $K_i[\zeta] : K_i = K_a[\zeta] : K_a = q^{l-a}s$. $\square$

Wir benötigen jetzt noch folgende Bezeichnungen. Der Fall $q = 2, n \geq 3$ und $K_1 = K[\zeta] = K[\zeta^2]$ heißt der *Ausnahmefall*. Im Ausnahmefall gilt $l = 1 = a$.

$$\lambda(L/K) := \begin{cases} 1, & \text{im Ausnahmefall} \\ \frac{l-2}{2}, & \text{falls } q = 2, 2|l, 0 \leq \frac{l}{2} \leq a, K_{l/2} \neq K_{l/2-1}[\zeta^{2^{l/2}}] \\ \min\{a, \frac{l-1}{2}\}, & \text{sonst,} \end{cases}$$

$$\mu(L/K) := \begin{cases} \max\left\{l-a-2, \frac{l-2}{2}\right\}, & \text{falls } q = 2 \text{ und } \zeta^{2^{l-a}} \notin L \\ \max\left\{l-a-1, \frac{l-1}{2}\right\}, & \text{sonst.} \end{cases}$$

Falls $\zeta \notin L$ ist, sei $\nu(L/K) \in \mathbb{N}_0$ folgendermaßen definiert:

$$\zeta^{q^{\nu(L/K)}} \notin L \text{ und } \zeta^{q^{\nu(L/K)+1}} \in L.$$

Es gilt dann $0 \leq \nu(L/K) \leq n-1$. Für $x \in \mathbb{R}$ sei:

$$\lfloor x \rfloor := \max\{z | x \geq z \in \mathbb{Z}\}, \quad \lceil x \rceil := \min\{z | x \leq z \in \mathbb{Z}\}.$$

Mit dem folgenden Satz kann der Beweis zur Existenz vollständig regulärer Elemente in endlichen Galoiserweiterungen (2.4) und damit auch der Beweis zur Existenz vollständig freier Elemente in endlichen, separablen Erweiterungen (1.1) beendet werden. Der folgende Satz ist jedoch allgemeiner formuliert, weil er später noch für einen anderen Zweck verwendet wird.

Satz 5.8 *Sei L/K eine endliche, galoissche Erweiterung mit Galoisgruppe G. Sei weiter G zyklisch und $|G| = q^n$, wobei q eine Primzahl ungleich der Charakteristik von K ist. Ferner seien $\lambda := \lambda(L/K)$,$\mu := \mu(L/K)$ und $\nu := \nu(L/K)$.*

1. *Liegt nicht der Ausnahmefall vor, so ist $\lceil \lambda \rceil \leq \lfloor \mu \rfloor + 1$ und es gilt:*

$$z_0 < z_1 < \cdots < z_{\lceil \lambda \rceil} = \cdots = z_{\lfloor \mu \rfloor + 1}.$$

Weiter ist entweder

$$z_{\lfloor \mu \rfloor + 1} > z_{\lfloor \mu \rfloor + 2} > \cdots > z_{n-1}$$

oder es ist $q = 2, \zeta^{2^{l-a}} \notin L, \lfloor \mu \rfloor + 1 \leq \nu < n-1$ und

$$z_{\lfloor \mu \rfloor + 1} > \cdots > z_\nu = z_{\nu+1} > \cdots > z_{n-1}.$$

2. *Liegt der Ausnahmefall vor, so ist $z_1 > z_2 > \cdots > z_{n-1}$, ferner ist $r(0) = r(1)$, sowie*

$$\dim_K T_i(0) = \dim_K T_j(1) = 2 \qquad \text{und} \qquad T_i(0) \cap T_j(1) = \{0\}$$

für alle $i, j \in \{1, \ldots, r(0)\}$. Außerdem ist jede homogene K_0G_1-Komponente $H_k(0)$ von T Summe von genau zwei Elementen aus z_0 und von genau zwei Elementen aus z_1.

Beweis: Wir zeigen zunächst:

(1) $Z_i \leq z_i$ für $0 \leq i \leq n-1$

(1′) $Z_i \leq z_{i+1}$ für $0 \leq i \leq n-2$.

Für $0 \leq j \leq r(i)$ und $0 \leq i \leq n-1$ ist G_{i+1} ein Normalteiler von G_i und $T_j(i)$ ein irreduzibler K_iG_i-Modul. Aus 5.3 folgt, daß $T_j(i)$ ein homogener K_iG_{i+1}-Modul ist. Also gilt (1). Sei jetzt $0 \leq j \leq s(i)$ und $0 \leq i \leq n-2$. Da L als K_iG_{i+1}- Modul halbeinfach ist, folgt mit 5.2, daß $H_j(i)$ ein $K_{i+1}G_{i+1}$-Teilmodul von L und als solcher Summe von irreduziblen $K_{i+1}G_{i+1}$-Moduln ist. Das zeigt (1′).

(2) $$r(i) = \frac{\varphi(|G_i|)}{K_i[\zeta^{q^i}] : K_i} \text{ für } 0 \leq i \leq n-1.$$

Nach 4.2 enthält K_iG_i genau $\varphi(|G_i|)/(\mathrm{Zerf}_{K_i}(X^{q^{n-i}}-1) : K_i)$ irreduzible K_iG_i-Teilmoduln, deren Zentralisator in G_i gerade id_L ist. Wegen $\mathrm{Zerf}_{K_i}(X^{q^{n-i}}-1) = K_i[\zeta^{q^i}]$ folgt (2).

(3) $$s(i) = \frac{\varphi(|G_{i+1}|)}{K_i[\zeta^{q^{i+1}}] : K_i} \text{ für } 0 \leq i \leq n-1.$$

(3′) Jede homogene Komponente von T ist Summe von genau q irreduziblen, G_{i+1}-treuen K_iG_{i+1}-Teilmoduln für $0 \leq i \leq n-2$.

Sei $0 \leq i \leq n-2$. Nach dem Satz von der Normalbasis gibt es ein reguläres Element x in L/K_i. Das bedeutet $L = K_iG_i \cdot x$. Sei $G_i = \langle g \rangle$, dann ist $G_{i+1} = \langle g^q \rangle$ und die Menge $\{x, g(x), \ldots, g^{|G_i|-1}(x)\}$ eine K_i-Basis von L. Offensichtlich gilt dann:

$$L = K_iG_{i+1} \cdot x \oplus K_iG_{i+1} \cdot g(x) \oplus \cdots \oplus K_iG_{i+1} \cdot g^{q-1}(x).$$

Es sei $\gamma := |G_{i+1}|$ und weiter $t \in \{0, \ldots, q-1\}$, sowie die Abbildung ψ_t von K_iG_{i+1} auf $K_iG_{i+1} \cdot g^t(x)$ definiert durch

$$\psi_t\Big(\sum_{j=0}^{\gamma-1} k_j g^{qj}\Big) := \sum_{j=0}^{\gamma-1} k_j g^{qj+t}(x).$$

Dann ist ψ_t offenbar ein K_iG_{i+1}-Epimorphismus. Sei nun $\sum_{j=0}^{\gamma-1} k_j g^{qj} \in \ker \psi_t$, das heißt, es ist $\sum_{j=0}^{\gamma-1} k_j g^{qj+t}(x) = 0$, dann folgt $k_0 = \cdots = k_{\gamma-1} = 0$, da $\{g^t(x), \ldots, g^{q(\gamma-1)+t}(x)\}$ eine Teilmenge der K_i-Basis $\{x, g(x), \ldots, g^{q\gamma-1}(x)\}$ von L ist. Also ist ψ_t sogar ein K_iG_{i+1}-Isomorphismus und

$$W_t := K_iG_{i+1} \cdot g^t(x)$$

ist als K_iG_{i+1}-Modul isomorph zu K_iG_{i+1}. Es ergibt sich

$$L = W_0 \oplus \cdots \oplus W_{q-1}.$$

Sei jetzt H eine homogene K_iG_{i+1}-Komponente von L mit

$$H = V_1 \oplus \cdots \oplus V_m,$$

wobei $V_1, \ldots V_m$ zueinander isomorphe, irreduzible K_iG_{i+1}-Teilmoduln von L sind.

Sei $j \in \{1, \ldots, m\}$, dann gibt es ein $t_j \in \{0, \ldots, q-1\}$, so daß $V_j \subseteq W_{t_j}$ ist; denn andernfalls gäbe es ein $t' \in \{0, \ldots, q-1\}$ mit $\{0\} \neq W_{t'} \cap V_j \subset V_j$, und V_j wäre nicht irreduzibel. Außerdem ist t_j eindeutig; denn gäbe es ein $t' \neq t_j$ mit $V_j \subseteq W_{t'}$, so würde sich der Widerspruch $\{0\} \neq V_j \subseteq W_{t_j} \cap W_{t'} = \{0\}$ ergeben. Da V_1 in W_{t_1} enthalten ist und alle W_t mit $t \in \{0, \ldots, q-1\}$ K_iG_{i+1}-isomorph zu W_{t_1} sind, enthalten alle W_t jeweils einen Teilmodul, der K_iG_{i+1}-isomorph zu V_1 ist. Das bedeutet $m \geq q$.

Sei nun $t \in \{0, \ldots, q-1\}$, dann ist W_t ja K_iG_{i+1}-isomorph zu K_iG_{i+1}, das bedeutet die irreduziblen K_iG_{i+1}-Teilmoduln von W_t sind schon die homogenen Komponenten von W_t. Also kann es höchstens ein $j \in \{1, \ldots, m\}$ geben mit $V_j \subseteq W_t$, damit ist $q \geq m$, und es folgt $q = m$.

Nach 4.2 wissen wir, daß jedes W_t für $t \in \{0, \ldots, q-1\}$ wegen der Isomorphie zu K_iG_{i+1} genau $\varphi(|G_{i+1}|)/(K_i[\zeta^{q^{i+1}}] : K_i)$ irreduzible, G_{i+1}-treue K_iG_{i+1}-Teilmoduln enthält. Weil $L = W_0 \oplus \cdots \oplus W_{q-1}$ ist, enthält L genau $q \cdot \varphi(|G_{i+1}|)/(K_i[\zeta^{q^{i+1}}] : K_i)$ irreduzible, G_{i+1}-treue K_iG_{i+1}-Teilmoduln. Deren Summe ist genau T, — das rechnet man genauso nach, wie die Tatsache, daß T die Summe der G_i-treuen K_iG_i-Teilmoduln von L ist. Weil jede homogene K_iG_{i+1}-Komponente von T auch homogene K_iG_{i+1}-Komponente von L ist, ist jede eine direkte Summe von genau q irreduziblen, G_{i+1}-treuen K_iG_{i+1}-Teilmoduln von T. Also ist

$$s(i) = \frac{\varphi(|G_{i+1}|)}{K_i[\zeta^{q^{i+1}}] : K_i},$$

für $0 \leq i \leq n-2$. Das zeigt (3′) und (3) für $0 \leq i \leq n-2$.

Für $i = n-1$ ist $K_iG_{i+1} = K_{n-1}G_n$. Weil $G_n = \{\mathrm{id}_L\}$ ist, kann $K_{n-1}G_n$ mit K_{n-1} identifiziert werden. Die irreduziblen $K_{n-1}G_n$-Teilmoduln von T sind dann die 1-dimensionalen K_{n-1}-Unterräumen von T. Diese sind alle zueinander isomorph. Also hat T als $K_{n-1}G_n$-Modul nur eine homogene Komponente. Andrerseits gilt:

$$\frac{\varphi(|G_n|)}{K_{n-1}[\zeta^{q^n}] : K_{n-1}} = 1.$$

Damit ist (3) bewiesen.

Einfache Umformungen ergeben für alle $x \in \mathbb{R}$:

$$(4) \qquad a < l - a - x \iff a < \frac{l-x}{2} \iff \frac{l-x}{2} < l - a - x.$$

Jetzt läßt sich zeigen, daß $\lceil \lambda \rceil \leq \lfloor \mu \rfloor + 1$ gilt, falls nicht der Ausnahmefall vorliegt:

Fall 1. Es ist $\lambda = \frac{l-2}{2}$. Dann ist

$$\lambda \leq \max\left\{l-a-2, \frac{l-2}{2}\right\} \leq \max\left\{l-a-1, \frac{l-1}{2}\right\}.$$

Also ist $\lambda \leq \mu$ und es folgt die Behauptung.

Fall 2. Es ist $\lambda = \min\{a, \frac{l-1}{2}\}$.

Fall 2.1. Es gilt $a < \frac{l-1}{2}$, also $\lambda = a$. Weil a eine natürliche Zahl ist, ist dann $a \leq \frac{l-2}{2}$, woraus sich

$$a \leq \max\left\{l-a-2, \frac{l-2}{2}\right\} \leq \max\left\{l-a-1, \frac{l-1}{2}\right\}$$

ergibt. Also ist $\lambda \leq \mu$ und es folgt die Behauptung.

Fall 2.2. Es gilt $\frac{l-1}{2} \leq a$, also $\lambda = \frac{l-1}{2}$. Dann ist

$$\lambda = \frac{l-1}{2} \leq \max\left\{l-a-1, \frac{l-1}{2}\right\}.$$

Weiter ist $\frac{l-2}{2} < a$, woraus mit (4) folgt, daß $\frac{l-2}{2} > l-a-2$ ist; d.h.

$$\max\left\{l-a-2, \frac{l-2}{2}\right\} = \frac{l-2}{2}.$$

Daraus ergibt sich

$$\lceil\lambda\rceil = \left\lfloor\frac{l-2}{2}\right\rfloor + 1 = \left\lfloor\max\left\{l-a-2, \frac{l-2}{2}\right\}\right\rfloor + 1.$$

Damit gilt auch in diesem Fall $\lceil\lambda\rceil \leq \lfloor\mu\rfloor + 1$.

(5) Für zwei $i, j \in \{0, \ldots, n-1\}$ gelte $K_{i+1} \subseteq K_i[\zeta^{q^j}] = K_i[\zeta^{q^{j+1}}]$, dann ist $q = 2, i = 0$ und $K_1 = K_0[\zeta^{2^j}]$.

Beweis von (5). Wegen $K_i \subseteq K_{i+1} \subseteq K_i[\zeta^{q^j}]$ wird $(K_i[\zeta^{q^j}] : K_i)$ von q geteilt. Außerdem ist ζ^{q^j} eine primitive q^{n-j}-te Einheitswurzel, so daß sich 3.1.1 anwenden läßt. Es folgt wegen $K_i[\zeta^{q^j}] : K_i[\zeta^{q^{j+1}}] = 1 \neq q$, daß 3.1.1.a gilt, das heißt:

$$q = 2,\ K_i[\zeta^{2^j}] : K_i = 2 \quad \text{und} \quad K_i[\zeta^{2^j}] = K_i[\zeta^{2^{j+1}}].$$

Wegen $K_{i+1} \subseteq K_i[\zeta^{2^j}]$ und $K_{i+1} : K_i = 2$ ist deshalb $K_{i+1} = K_i[\zeta^{2^j}]$. Wir nehmen nun an, daß $i-1 \geq 0$ ist. Dann ergibt sich:

$$K_{i-1} \subseteq K_{i-1}[\zeta^{2^{j+1}}] \subseteq K_i[\zeta^{2^{j+1}}] = K_{i+1}.$$

Aus $K_i[\zeta^{2^{j+1}}] : K_i = K_{i+1} : K_i = 2$ folgt nun weiter $(K_{i-1}[\zeta^{2^{j+1}}] : K_{i-1}) \geq 2$. Da die Galoisgruppe von K_{i+1} über K_{i-1} zyklisch der Ordnung 4 ist, ergibt sich:

$$K_i = K_{i-1}[\zeta^{2^{j+1}}] \quad \text{oder} \quad K_{i+1} = K_{i-1}[\zeta^{2^{j+1}}].$$

Auf jeden Fall gilt:

$$K_i \subseteq K_{i-1}[\zeta^{2^{j+1}}] \subseteq K_{i+1}.$$

Wegen $\zeta^{2^{j+1}} \notin K_i$, denn es ist $K_i[\zeta^{2^{j+1}}] : K_i = 2$, muß $K_{i-1}[\zeta^{2^{j+1}}] = K_{i+1}$ sein. Daraus ergibt sich:

$$K_{i+1} = K_{i-1}[\zeta^{2^{j+1}}] \subseteq K_{i-1}[\zeta^{2^j}] \subseteq K_i[\zeta^{2^j}] = K_{i+1}.$$

Das bedeutet $K_{i-1}[\zeta^{2^{j+1}}] = K_{i-1}[\zeta^{2^j}]$ und

$$K_{i-1}[\zeta^{2^j}] : K_{i-1} = K_{i+1} : K_{i-1} = 4.$$

Daraus folgt mit 3.1.1 der Widerspruch $K_{i-1}[\zeta^{2^j}] : K_{i-1}[\zeta^{2^{j+1}}] = 2$. Also ist $i = 0$ und es gilt (5).

(6) $\quad r(i+1) = s(i)$ für $\lambda \leq i \leq n-2$.

Nach (2) und (3) gilt:

$$\begin{aligned} r(i+1) &= \frac{\varphi(|G_{i+1}|)}{K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1}} \\ s(i) &= \frac{\varphi(|G_{i+1}|)}{K_i[\zeta^{q^{i+1}}] : K_i}. \end{aligned}$$

Damit ist (6) äquivalent zu $K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1} = K_i[\zeta^{q^{i+1}}] : K_i$ für $\lambda \leq i \leq n-2$.

(6′) $\quad K_{i+1} \not\subseteq K_i[\zeta^{q^{i+1}}]$ für $\lambda \leq i \leq n-2$.

Wir zeigen zunächst, daß (6) und (6′) äquivalent sind. Es gelte (6) und wir nehmen an, daß (6′) falsch ist, also $K_{i+1} \subseteq K_i[\zeta^{q^{i+1}}]$ richtig ist. Dann folgt $K_{i+1}[\zeta^{q^{i+1}}] = K_i[\zeta^{q^{i+1}}]$, und damit ergibt sich der Widerspruch

$$\begin{aligned} K_i[\zeta^{q^{i+1}}] : K_i &= K_{i+1}[\zeta^{q^{i+1}}] : K_i \\ &= (K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1}) \cdot (K_{i+1} : K_i) \\ &= (K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1}) \cdot q \\ &> K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1}. \end{aligned}$$

Sei jetzt (6′) richtig. Wegen $K_i \subseteq K_{i+1} \cap K_i[\zeta^{q^{i+1}}] \subseteq K_{i+1}$ und $K_{i+1} \not\subseteq K_i[\zeta^{q^{i+1}}]$ ist

$$K_{i+1} \cap K_i[\zeta^{q^{i+1}}] = K_i.$$

Aus $K_{i+1}K_i[\zeta^{q^{i+1}}] = K_{i+1}[\zeta^{q^{i+1}}]$ folgt mit [5, V.10.4.Théorème 1], daß

$$K_{i+1} : K_i = K_{i+1}[\zeta^{q^{i+1}}] : K_i[\zeta^{q^{i+1}}]$$

ist. Das ergibt

$$\begin{aligned} K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1} &= \frac{(K_{i+1}[\zeta^{q^{i+1}}] : K_i[\zeta^{q^{i+1}}]) \cdot (K_i[\zeta^{q^{i+1}}] : K_i)}{K_{i+1} : K_i} \\ &= K_i[\zeta^{q^{i+1}}] : K_i. \end{aligned}$$

Also gilt (6).

BEWEIS VON (6′). Sei $i \geq a$. Dann ist $K_i[\zeta] \cap L = K_i$, weil einerseits $K_i \subseteq K_i[\zeta] \cap L$ richtig ist und andrerseits aus $K_j \subseteq K_i[\zeta] \cap L$ mit $j > i$ ein Widerspruch folgen würde; denn es wäre $K_j \subseteq K_i[\zeta]$, also $K_i[\zeta] = K_j[\zeta]$ und daraus würde sich

$$K_i[\zeta] : K_i = K_j[\zeta] : K_i = (K_j[\zeta] : K_j) \cdot (K_j : K_i)$$

ergeben, was nach 5.7 zu dem Widerspruch $q^{l-a}s \geq q^{l-a}s \cdot q$ führen würde. Also ist

$$K_i[\zeta^{q^{i+1}}] \cap K_{i+1} \subseteq K_i[\zeta] \cap L = K_i.$$

Daraus folgt $K_{i+1} \not\subseteq K_i[\zeta^{q^{i+1}}]$, da sonst $K_{i+1} \subseteq K_i$ wäre, d.h. es gilt (6′) für $i \geq a$.

Im Ausnahmefall ist $i \geq a = 1 = \lambda$. Mit dem eben gezeigten können wir den Ausnahmefall jetzt also ausschließen, sowie $\lambda \leq i < a$ voraussetzen. Nach Defintion ist daher $\lambda \in \{\frac{l-1}{2}, \frac{l-2}{2}\}$. Wegen $a \leq l$ ist außerdem $l \neq 0$.

FALL 1. Es sei $\frac{l-1}{2} \leq i < a$. Dann ergibt sich $i + 1 \geq l - i$ mit (4). Nach 5.7 ist $K_i[\zeta] : K_i = q^{l-i}s$. Es ist daher auf Grund von 3.1.3 entweder

$$(*) \qquad K_i[\zeta] : K_i[\zeta^{q^{l-i}}] = q^{l-i}$$

oder

$$(**) \qquad K_i[\zeta^{q^{l-i}}] = K_i[\zeta^{q^{l-i-1}}] \text{ und } q = 2.$$

FALL 1.1. Es gelte $(*)$. Wegen $i+1 \geq l-i$ folgt $K_i[\zeta^{q^{i+1}}] \subseteq K_i[\zeta^{q^{l-i}}]$ und es ergibt sich:

$$\underbrace{K_i[\zeta] : K_i}_{=q^{l-i}s} = \underbrace{(K_i[\zeta] : K_i[\zeta^{q^{l-i}}])}_{=q^{l-i}} \cdot (K_i[\zeta^{q^{l-i}}] : K_i[\zeta^{q^{i+1}}]) \cdot (K_i[\zeta^{q^{i+1}}] : K_i).$$

Damit ist q kein Teiler von $K_i[\zeta^{q^{i+1}}] : K_i$. Deshalb muß $K_{i+1} \not\subseteq K_i[\zeta^{q^{i+1}}]$ gelten, weil sonst

$$K_i[\zeta^{q^{i+1}}] : K_i = (K_i[\zeta^{q^{i+1}}] : K_{i+1}) \cdot (K_{i+1} : K_i) = (K_i[\zeta^{q^{i+1}}] : K_{i+1}) \cdot q$$

wäre. Also gilt (6′).

FALL 1.2. Es gelte $(**)$. Wir nehmen an, daß (6′) falsch ist. Wegen $i+1 \geq l-i$ und $(**)$ folgt dann, daß $q = 2$ und

$$K_{i+1} \subseteq K_i[\zeta^{2^{i+1}}] \subseteq K_i[\zeta^{2^{l-i}}] = K_i[\zeta^{2^{l-i-1}}]$$

ist. Daraus folgt mit (5) weiter, daß $i = 0$ und $K_1 = K_0[\zeta^{2^{l-1}}]$ ist. Wegen $i \geq \frac{l-1}{2}$ ist damit $0 \geq \frac{l-1}{2}$, d.h. $l \leq 1$. Weil $l \neq 0$ ist, muß $l = 1$ gelten. Also ergibt sich:

$$K_1 = K_0[\zeta] = K_0[\zeta^2].$$

Das ist aber der Ausnahmefall, der ausgeschlossen wurde. Daher ist (6′) doch richtig.

Fall 2. Es sei $i = \frac{l-2}{2}$. Dann ist insbesondere $\lambda = \frac{l-2}{2}$. Aus der Definition von λ ergibt sich, daß $q = 2$ und $K_{i+1} \neq K_i[\zeta^{2^{i+1}}]$ ist. Wegen $a > i$ und $l - i = i + 2$ folgt mit 5.7:

$$K_i[\zeta] : K_i = 2^{l-i} = 2^{i+2}.$$

Mit 3.1.2 folgt daraus weiter

$$K_i[\zeta] : K_i[\zeta^{2^{i+1}}] = 2^{i+1}.$$

Also ist

$$K_i[\zeta^{2^{i+1}}] : K_i = \frac{K_i[\zeta] : K_i}{K_i[\zeta] : K_i[\zeta^{2^{i+1}}]} = \frac{2^{i+2}}{2^{i+1}} = 2.$$

Wäre nun $K_{i+1} \subseteq K_i[\zeta^{2^{i+1}}]$, so würde sich

$$2 = K_i[\zeta^{2^{i+1}}] : K_i = (K_i[\zeta^{2^{i+1}}] : K_{i+1}) \cdot \underbrace{(K_{i+1} : K_i)}_{=2}$$

ergeben. Wegen $K_{i+1} \neq K_i[\zeta^{2^{i+1}}]$ kann das aber nicht sein. Also gilt doch $K_{i+1} \nsubseteq K_i[\zeta^{2^{i+1}}]$.

(7) $r(i) = s(i)$ für $1 \leq i \leq \mu$,
$r(0) = s(0)$ falls nicht der Ausnahmefall vorliegt,
$r(\nu) = s(\nu)$ für $q = 2$ und $\zeta \notin L$.

Nach (2) und (3) gilt für $0 \leq i \leq n-1$ folgendes

$$\begin{aligned} r(i) = s(i) \quad &\Longleftrightarrow \quad \frac{\varphi(q^{n-i})}{K_i[\zeta^{q^i}] : K_i} = \frac{\varphi(q^{n-i-1})}{K_i[\zeta^{q^{i+1}}] : K_i} \\ &\Longleftrightarrow \quad \frac{K_i[\zeta^{q^i}] : K_i}{K_i[\zeta^{q^{i+1}}] : K_i} = q. \end{aligned}$$

Also ist (7) äquivalent zu

(7′) Es ist $K_i[\zeta^{q^i}] : K_i[\zeta^{q^{i+1}}] = q$ für $1 \leq i \leq \mu$, für $i = 0$, falls nicht der Ausnahmefall vorliegt und für $i = \nu$, falls $q = 2$ und $\zeta \notin L$ ist.

Beweis von (7′). Es sei $q = 2$ und $\zeta \notin L$. Nach Definition von ν ist dann $\zeta^{2^\nu} \notin L$ und $\zeta^{2^{\nu+1}} \in L$. Also gilt insbesondere $K_\nu[\zeta^{2^{\nu+1}}] \subseteq L$ und ζ^{2^ν} kann kein Element von $K_\nu[\zeta^{2^{\nu+1}}]$ sein. Damit ist (7′) für diesen Fall gezeigt. Sei nun $0 \leq i \leq \mu$.

Fall 1. Es sei $\mu = \max\{l - a - 2, \frac{l-2}{2}\}$. Dann sind nach (4) zwei Fälle möglich:

$$l - a - 2 > \frac{l-2}{2} > a \qquad \text{oder} \qquad l - a - 2 \leq \frac{l-2}{2} \leq a.$$

Also ist $i \leq \min\{a, \frac{l-2}{2}\}$ oder $a < i \leq l-a-2$. Daher ist entweder $i \leq \frac{l-2}{2}$, woraus mit (4) folgt $i+2 \leq l-i$, oder es ist $i+2 \leq l-a$. Insgesamt ergibt sich $i+2 \leq l - \min\{i,a\}$. Nach 5.7 ist $K_i[\zeta] : K_i = q^{l-\min\{i,a\}}s$, womit die Voraussetzungen von 3.1.2 für i und $i+1$ erfüllt sind. Es ergibt sich:

$$K_i[\zeta] : K_i[\zeta^{q^i}] = q^i \qquad \text{und} \qquad K_i[\zeta] : K_i[\zeta^{q^{i+1}}] = q^{i+1}.$$

Daraus folgt nun $(7')$; denn es ist

$$K_i[\zeta^{q^i}] : K_i[\zeta^{q^{i+1}}] = \frac{K_i[\zeta] : K_i[\zeta^{q^{i+1}}]}{K_i[\zeta] : K_i[\zeta^{q^i}]} = q.$$

Fall 2. Es sei $\mu = \max\{l-a-1, \frac{l-1}{2}\}$. Analog zu Fall 1 ergibt sich hier $i+1 \leq l - \min\{i,a\}$. Wir haben also einerseits $0 \leq i \leq l - \min\{i,a\} - 1$ und andrerseits $K_i[\zeta] : K_i = q^{l-\min\{i,a\}}s$ nach 5.7. Mit 3.1.2 folgt daraus

$$K_i[\zeta] : K_i[\zeta^{q^i}] = q^i \quad \text{für } 0 \leq i \leq l - \min\{i,a\} - 1 \quad (*),$$

$$K_i[\zeta] : K_i[\zeta^{q^{i+1}}] = q^{i+1} \quad \text{für } 0 \leq i+1 \leq l - \min\{i,a\} - 1.$$

Also gilt $(7')$ für $0 \leq i \leq l - \min\{i,a\} - 2$.

Es bleibt noch der Fall $i = l - \min\{i,a\} - 1$ übrig. Sei daher nun $i+1 = l - \min\{i,a\}$. Ist $q \neq 2$, so folgt weiter mit 3.1.3, daß $K_i[\zeta] : K_i[\zeta^{q^{i+1}}] = q^{i+1}$ ist. Zusammen mit $(*)$ ergibt das $(7')$.

Ist $q = 2$, so ist $\zeta^{2^{l-a}} \in L$ auf Grund der Definition von μ. Wegen $i+1 = l - \min\{i,a\} \geq l-a$ ist dann auch $\zeta^{2^{i+1}} \in L$. Außerdem ist $K_i[\zeta] : K_i = 2^{l-\min\{i,a\}}$, mit 3.1.2 folgt deshalb $K_i[\zeta] : K_i[\zeta^{2^i}] = 2^i$. Daraus ergibt sich

$$K_i[\zeta^{2^i}] : K_i = \frac{K_i[\zeta] : K_i}{K_i[\zeta] : K_i[\zeta^{2^i}]} = \frac{2^{i+1}}{2^i} = 2.$$

Wäre nun $K_i[\zeta^{2^i}] : K_i[\zeta^{2^{i+1}}] = 1$, so wäre $K_i[\zeta^{2^i}] = K_i[\zeta^{2^{i+1}}] = K_{i+1}$; denn es wäre ja $\zeta^{2^{i+1}} \in L$ und $K_i[\zeta^{2^{i+1}}] : K_i = 2$. Nach (5) würde dann aber $i = 0$ folgen, und es läge der ausgeschlossene Ausnahmefall vor. Also gilt $(7')$.

(8) Es ist $r(i+1) = q \cdot s(i)$ für $0 \leq i < \lambda$.

Nach (2) und (3) ist

$$\begin{aligned} r(i+1) &= \frac{\varphi(|G_{i+1}|)}{K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1}} \\ q \cdot s(i) &= q \cdot \frac{\varphi(|G_{i+1}|)}{K_i[\zeta^{q^{i+1}}] : K_i}. \end{aligned}$$

Damit ist $r(i+1) = q \cdot s(i)$ äquivalent zu

$$K_i[\zeta^{q^{i+1}}] : K_i = q \cdot (K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1}).$$

(8′) Es ist $K_{i+1} \subseteq K_i[\zeta^{q^{i+1}}]$ für $0 \leq i < \lambda$.

Zunächst zeigen wir, daß (8) und (8′) äquivalent sind. Es gelte nun (8), d.h. $K_i[\zeta^{q^{i+1}}] : K_i = q \cdot (K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1})$. Dann folgt:

$$\begin{aligned} K_{i+1}[\zeta^{q^{i+1}}] : K_i[\zeta^{q^{i+1}}] &= \frac{(K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1}) \cdot (K_{i+1} : K_i)}{K_i[\zeta^{q^{i+1}}] : K_i} \\ &= \frac{q \cdot (K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1})}{q \cdot (K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1})} = 1. \end{aligned}$$

Also ist $K_i[\zeta^{q^{i+1}}] = K_{i+1}[\zeta^{q^{i+1}}] \supseteq K_{i+1}$ und es gilt (8′).

Sei jetzt (8′) richtig. Wegen $K_{i+1} \subseteq K_i[\zeta^{q^{i+1}}]$ ist $K_{i+1}[\zeta^{q^{i+1}}] = K_i[\zeta^{q^{i+1}}]$ und es ergibt sich

$$\begin{aligned} K_i[\zeta^{q^{i+1}}] : K_i &= (K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1}) \cdot (K_{i+1} : K_i) \\ &= (K_{i+1}[\zeta^{q^{i+1}}] : K_{i+1}) \cdot q. \end{aligned}$$

Damit gilt (8).

Beweis von (8′). Sei $0 \leq i < \lambda$. Liegt der Ausnahmefall vor, so ist $i = 0, \ , q = 2, \ \lambda = 1$ und $K_1 = K[\zeta^2]$. Also gilt $K_{i+1} \subseteq K_i[\zeta^{q^{i+1}}]$.

Wir können deshalb jetzt annehmen, daß der Ausnahmefall nicht vorliegt. Aus der Definition von λ folgt $i < \lambda \leq a$, also $i + 1 \leq a$. Daher gilt

$$K_{i+1} \subseteq K_a \subseteq K[\zeta] \subseteq K_i[\zeta].$$

Aus der Definition von λ folgt weiter $i < \lambda \leq \frac{l-1}{2}$. Nach (4) gilt dann $i+1 < l - i$, was äquivalent zu $0 < l - 2i - 1$ ist. Nach 5.7 ist $K_i[\zeta] : K_i = q^{l-i}s$, weshalb mit 3.1.2 folgt, daß $K_i[\zeta] : K_i[\zeta^{q^{i+1}}] = q^{i+1}$ ist. Daraus ergibt sich:

$$K_i[\zeta^{q^{i+1}}] : K_i = \frac{K_i[\zeta] : K_i}{K_i[\zeta] : K_i[\zeta^{q^{i+1}}]} = q^{l-2i-1}s.$$

Fall 1. Es sei $H := \mathrm{Gal}(K_i[\zeta]/K_i)$ zyklisch. Dann ist K_{i+1} ein Teilkörper von $K_i[\zeta^{q^{i+1}}]$; denn $K_i[\zeta^{q^{i+1}}]$ und K_{i+1} sind Zwischenkörper von $K_i[\zeta]/K_i$ und $K_{i+1} : K_i = q$ ist ein Teiler von $K_i[\zeta^{q^{i+1}}] : K_i$.

Fall 2. Es sei H nicht zyklisch. Dann folgt mit 3.1.4, daß $q = 2$ und außerdem $U := \mathrm{Gal}(K_i[\zeta]/K_i[\zeta^{2^{l-i-1}}])$ eine zyklische 2-Gruppe ist. Mit 3.1.2 ergibt sich

$$K_i[\zeta] : K_i[\zeta^{2^{l-i-1}}] = 2^{l-i-1}.$$

Fall 2.1. Es sei $i + 1 < l - i - 1$. Dann gilt:

$$K_i[\zeta^{2^{l-i-1}}] : K_i = \frac{K_i[\zeta] : K_i}{K_i[\zeta] : K_i[\zeta^{2^{l-i-1}}]} = \frac{2^{l-i}}{2^{l-i-1}} = 2.$$

Wegen $0 < l - 2i - 2$ ist deshalb

$$K_i[\zeta^{2^{i+1}}] : K_i[\zeta^{2^{l-i-1}}] = \frac{K_i[\zeta^{2^{i+1}}] : K_i}{K_i[\zeta^{2^{l-i-1}}] : K_i} = \frac{2^{l-2i-1}}{2} = 2^{l-2i-2} \neq 1.$$

Daher folgt:

$$K_i[\zeta] \supseteq K_i[\zeta^{2^{i+1}}] \supset K_i[\zeta^{2^{l-i-1}}].$$

Weil $K_i[\zeta^{2^{l-i-1}}] : K_i = 2$ ist, muß außerdem $(K_{i+1}[\zeta^{2^{l-i-1}}] : K_{i+1}) \leq 2$ sein. Also ergibt sich

$$\begin{aligned} K_{i+1}[\zeta^{2^{l-i-1}}] : K_i[\zeta^{2^{l-i-1}}] &= \frac{(K_{i+1}[\zeta^{2^{l-i-1}}] : K_{i+1}) \cdot (K_{i+1} : K_i)}{K_i[\zeta^{2^{l-i-1}}] : K_i} \\ &= (K_{i+1}[\zeta^{2^{l-i-1}}] : K_{i+1}) \quad \in \{1, 2\}. \end{aligned}$$

Da $K_{i+1}[\zeta] = K_i[\zeta]$ nach 5.7 gilt und U zyklisch ist, liegt $K_{i+1}[\zeta^{2^{l-i-1}}]$ im minimalen Zwischenkörper von $K_i[\zeta]/K_i[\zeta^{2^{l-i-1}}]$. Wegen $K_i[\zeta^{2^{i+1}}] \supset K_i[\zeta^{2^{l-i-1}}]$ liegt dieser minimale Zwischenkörper in $K_i[\zeta^{2^{i+1}}]$. Damit folgt (8′); denn wir erhalten

$$K_i[\zeta^{2^{i+1}}] \supseteq K_{i+1}[\zeta^{2^{l-i-1}}] \supseteq K_{i+1}.$$

Fall 2.2. Es sei $i+1 = l-i-1$, das heißt $i = \frac{l-2}{2}$. Da nach Voraussetzung $i < \lambda$ ist, kann λ nicht gleich $\frac{l-2}{2}$ sein. Weiter ist $l = 2i+2$, das bedeutet l wird von 2 geteilt. Außerdem ist $l > 0$ und nach Voraussetzung $i = \frac{l-2}{2} < a$. Aus der Definition von λ folgt daher $K_{l/2} = K_{l/2-1}[\zeta^{2^{l/2}}]$, da sonst $\lambda = \frac{l-2}{2}$ wäre. Wegen $\frac{l}{2} = i+1$ und $\frac{l}{2} - 1 = i$ ergibt sich damit $K_{i+1} = K_i[\zeta^{2^{i+1}}]$. Also gilt auch in diesem Fall (8′).

(9) Es ist $r(i) = q \cdot s(i)$ für $\mu < i \leq n-2$ außer für $i = \nu$, falls $q = 2$ und $\zeta \notin L$ ist.

Für $0 \leq i \leq n-1$ gilt nach (2) und (3) folgendes:

$$\begin{aligned} r(i) &= \frac{\varphi(|G_i|)}{K_i[\zeta^{q^i}] : K_i} \\ q \cdot s(i) &= q \cdot \frac{\varphi(|G_{i+1}|)}{K_i[\zeta^{q^{i+1}}] : K_i} = \frac{\varphi(|G_i|)}{K_i[\zeta^{q^{i+1}}] : K_i}. \end{aligned}$$

Da $K_i[\zeta^{q^{i+1}}]$ in $K_i[\zeta^{q^i}]$ enthalten ist, ist (9) äquivalent zu

(9′) $K_i[\zeta^{q^i}] = K_i[\zeta^{q^{i+1}}]$ für $\mu < i \leq n-2$ außer für $i = \nu$, falls $q = 2$ und $\zeta \notin L$ ist.

Beweis von (9′). Sei $\mu < i \leq n-2$, dann ist insbesondere $i+1 \leq n-1$. Also ist die primitive q-te Einheitswurzel $\zeta^{q^{n-1}}$ ein Element von $K_i[\zeta^{q^{i+1}}]$. Zunächst zeigen wir, daß folgendes gilt:

$$(K_i[\zeta^{q^i}] : K_i[\zeta^{q^{i+1}}]) \in \{1, q\}.$$

Ist $\zeta^{q^i} \in K_i[\zeta^{q^{i+1}}]$, so folgt $K_i[\zeta^{q^i}] : K_i[\zeta^{q^{i+1}}] = 1$. Sei also $\zeta^{q^i} \notin K_i[\zeta^{q^{i+1}}]$. Die q-ten Wurzeln von $\zeta^{q^{i+1}}$ sind $\zeta^{q^i}(\zeta^{q^{n-1}})^j$ mit $j = 0, \ldots, q-1$. Diese liegen wegen $\zeta^{q^i} \notin K_i[\zeta^{q^{i+1}}]$ und $(\zeta^{q^{n-1}})^j \in K_i[\zeta^{q^{i+1}}]$ allesamt nicht in $K_i[\zeta^{q^{i+1}}]$. Sei $f(X) := X^q - \zeta^{q^{i+1}}$. Dann ist ζ^{q^i} eine Nullstelle von f und es gilt $f \in$

$K_i[\zeta^{q^{i+1}}]$. Die Nullstellen von f sind die q-ten Wurzeln aus $\zeta^{q^{i+1}}$, also läßt sich f folgendermaßen schreiben:

$$f(X) = \prod_{j=0}^{q-1} (X - \zeta^{q^i}(\zeta^{q^{n-1}})^j).$$

Angenommen, f ist reduzibel in $K_i[\zeta^{q^{i+1}}][X]$ und $f = g \cdot h$ ist eine echte Zerlegung in $K_i[\zeta^{q^{i+1}}][X]$, wobei die Leitkoeffizienten von g und h gleich 1 sind. Dann gibt es eine Menge $M \subset \{0, \dots, q-1\}$ mit $1 \le |M| \le q-1$, so daß gilt:

$$g(X) = \prod_{j \in M} (X - \zeta^{q^i}(\zeta^{q^{n-1}})^j).$$

Daraus folgt, daß $\zeta^{|M|q^i} \prod_{j \in M} (\zeta^{q^{n-1}})^j \in K_i[\zeta^{q^{i+1}}]$ ist. Wegen $\zeta^{q^{n-1}} \in K_i[\zeta^{q^{i+1}}]$ ist dann auch $\zeta^{|M|q^i} \in K_i[\zeta^{q^{i+1}}]$. Aus $1 \le |M| \le q-1$ folgt die Teilerfremdheit von $|M|$ und q^n. Also gibt es $\alpha, \beta \in \mathbb{Z}$ mit $1 = \alpha|M| + \beta q^n$, und es ist $\alpha|M| \equiv 1 \bmod q^n$. Deshalb ergibt sich:

$$(\zeta^{|M|q^i})^\alpha = (\zeta^{\alpha|M|})^{q^i} = \zeta^{q^i}.$$

Das ist aber ein Widerspruch, denn einerseits ist $(\zeta^{|M|q^i})^\alpha \in K_i[\zeta^{q^{i+1}}]$ und andrerseits gilt $\zeta^{q^i} \notin K_i[\zeta^{q^{i+1}}]$. Also ist f das Minimalpolynom von ζ^{q^i} über $K_i[\zeta^{q^{i+1}}]$ und es gilt $K_i[\zeta^{q^i}] : K_i[\zeta^{q^{i+1}}] = q$.

Sei jetzt $q \neq 2$. Aus der Definition von μ folgt dann $i > \mu \ge l - a - 1$ und $i > \mu \ge \frac{l-1}{2}$, mit (4) folgt weiter $i + 1 > l - a$ und $i + 1 > l - i$. Zusammengefaßt heißt das $i + 1 > l - \min\{a, i\}$ und es ergibt sich

$$K_i[\zeta^{q^{l-\min\{a,i\}}}] \supseteq K_i[\zeta^{q^i}] \supseteq K_i[\zeta^{q^{i+1}}] \supseteq K_i \quad (*).$$

Mit 3.1.3 folgt, weil $q \neq 2$ vorausgesetzt ist, daß $K_i[\zeta] : K_i[\zeta^{q^{l-\min\{i,a\}}}] = q^{l-\min\{i,a\}}$ ist. Da $K_i[\zeta] : K_i = q^{l-\min\{i,a\}}s$ nach 5.7 richtig ist, folgt $K_i[\zeta^{q^{l-\min\{i,a\}}}] : K_i = s$. Wegen $(*)$ ist $K_i[\zeta^{q^i}] : K_i[\zeta^{q^{i+1}}]$ ein Teiler von s und kann deshalb nicht gleich q sein. Also gilt $K_i[\zeta^{q^i}] : K_i[\zeta^{q^{i+1}}] = 1$ nach dem vorher Bewiesenen. Damit ist $(9')$ für $q \neq 2$ gezeigt.

Sei nun $q = 2$. Wir nehmen an, das $K_i[\zeta^{2^i}] : K_i[\zeta^{2^{i+1}}] = 2$ ist. Weiter sei angenommen, daß $\zeta^{2^{i+1}} \notin K_i$ ist. Dann ist 2 ein Teiler von $K_i[\zeta^{2^{i+1}}] : K_i$ und wegen

$$K_i[\zeta^{2^i}] : K_i = (K_i[\zeta^{2^i}] : K_i[\zeta^{2^{i+1}}]) \cdot (K_i[\zeta^{2^{i+1}}] : K_i)$$

wird $K_i[\zeta^{2^i}] : K_i$ von 4 geteilt. Deshalb muß $i < l - \min\{i, a\} - 1$ sein; denn andernfalls würde aus 3.1.2 folgen

$$K_i[\zeta^{2^{l-\min\{i,a\}-1}}] : K_i = \frac{K_i[\zeta] : K_i}{K_i[\zeta] : K_i[\zeta^{2^{l-\min\{i,a\}-1}}]} = \frac{2^{l-\min\{i,a\}}}{2^{l-\min\{i,a\}-1}} = 2,$$

was wegen $K_i[\zeta^{2^i}] \subseteq K_i[\zeta^{2^{l-\min\{i,a\}-1}}]$ hieße, daß $K_i[\zeta^{2^i}] : K_i$ nicht von 4 geteilt wird. Also ist $i < l-a-1$ oder $i < l-i-1$, wobei letzteres nach (4) äquivalent zu $i < \frac{l-1}{2}$ ist. Damit ist $i < \max\{l-a-1, \frac{l-1}{2}\}$. Ist dann $l-a-1 > \frac{l-1}{2}$, so folgt $l-a-1 > i > \mu \geq l-a-2$, was ein Widerspruch ist. Ist hingegen $l-a-1 \leq \frac{l-1}{2}$, so folgt $\frac{l-1}{2} > i > \mu \geq \frac{l-2}{2}$, was ebenfalls ein Widerspruch ist. Also ist doch $\zeta^{2^{i+1}} \in K_i$.

Deshalb ergibt sich nun:

$$K_i[\zeta^{2^i}] : K_i = K_i[\zeta^{2^i}] : K_i[\zeta^{2^{i+1}}] = 2.$$

Ist $\zeta \in L$, dann ist trivialer Weise auch $\zeta^{2^i} \in L$. Ist $\zeta \notin L$, so muß nach Voraussetzung $i \neq \nu$ sein; wegen $\zeta^{2^{i+1}} \in L$ und der Definition von ν gilt dann ebenfalls $\zeta^{2^i} \in L$. Insbesondere erhalten wir $K_i \subseteq K_i[\zeta^{2^i}] \subseteq L$. Da $\mathrm{Gal}(L/K_i)$ zyklisch und $K_i[\zeta^{2^i}] : K_i = 2$ ist, folgt $K_i[\zeta^{2^i}] = K_{i+1}$. Wegen $K_i[\zeta^{2^i}] \subseteq L \cap K_i[\zeta] = K_a$ ist $i+1 \leq a$ oder anders gesagt $i < a$. Zusammen mit 3.1.2 folgt weiter:

$$K_i[\zeta^{2^{l-i-1}}] : K_i = \frac{K_i[\zeta] : K_i}{K_i[\zeta] : K_i[\zeta^{2^{l-i-1}}]} = \frac{2^{l-i}}{2^{l-i-1}} = 2.$$

Daraus ergibt sich

$$K_i[\zeta^{2^{l-i-1}}] = K_i[\zeta^{2^i}] = K_{i+1}.$$

Wegen $i > \mu \geq \frac{l-2}{2}$ ist $i \geq \frac{l-1}{2}$ und wegen (4) ist das äquivalent zu $i \geq l-i-1$.

Sei zunächst $i > l-i-1$. Dann erhalten wir

$$K_i[\zeta^{2^{l-i-1}}] \supseteq K_i[\zeta^{2^{l-i}}] \supseteq K_i[\zeta^{2^i}] = K_i[\zeta^{2^{l-i-1}}].$$

Das bedeutet, es ist

$$K_i[\zeta^{2^{l-i-1}}] = K_i[\zeta^{2^{l-i}}] = K_i[\zeta^{2^i}] = K_{i+1}.$$

Wegen (5) muß deshalb $i = 0$ und $K_1 = K[\zeta]$ sein. Während aus $i = 0$ folgt, daß $l = 0$ ist, ergibt sich aus $K_1 = K[\zeta]$, daß $l = 1$ ist. Das ist sicher ein Widerspruch und es gilt doch $K_i[\zeta^{2^i}] = K_i[\zeta^{2^{i+1}}]$.

Es bleibt noch der Fall $i = l-i-1$ übrig. Dann ist nach Voraussetzung $\frac{l-1}{2} = i > \mu$. Aus der Definition von μ folgt, daß $\zeta^{2^{l-a}} \notin L$ ist. Wegen $i < a$ gilt nach 5.7 folgendes

$$K_a[\zeta] = K_{a-1}[\zeta] = K_i[\zeta] = K[\zeta].$$

Außerdem ist $K[\zeta] : K_i = 2^{l-i}$. Nach 3.1.4 muß daher $\mathrm{Gal}(K[\zeta]/K_i[\zeta^{2^{l-i-1}}])$ zyklisch sein. Wegen $K_i[\zeta^{2^{l-i-1}}] = K_{i+1}$ ist $\mathrm{Gal}(K[\zeta]/K_{i+1})$ zyklisch. Nach 5.7 ist ferner ist $K[\zeta] : K_a = 2^{l-a}$, sowie $K[\zeta] : K_{a-1} = 2^{l-a+1}$. Mit 3.1.2 folgt weiter $K[\zeta] : K_{a-1}[\zeta^{2^{l-a}}] = 2^{l-a}$. Ist nun $i+1 < a$, so sind $K_{a-1}[\zeta^{2^{l-a}}]$ und K_a Zwischenkörper der zyklischen Erweiterung $K[\zeta]/K_{i+1}$. Das bedeutet $K_a = K_{a-1}[\zeta^{2^{l-a}}]$, was ein Widerspruch zu $\zeta^{2^{l-a}} \notin L$ ist. Ist $i+1 = a$, so folgt $\zeta^{2^{l-a}} = \zeta^{2^{l-i-1}} \in K_{i+1}$, also auch ein Widerspruch. Damit ist die Annahme endgültig widerlegt und es gilt $(9')$.

Hier ist eine kurze Zusammenfassung der wichtigsten Zwischenergebnisse:

(1) $\quad Z_i \leq z_i \quad$ für $0 \leq i \leq n-1$,

(1′) $\quad Z_i \leq z_{i+1} \quad$ für $0 \leq i \leq n-2$,

(6) $\quad r(i+1) = s(i) \quad$ für $\lambda \leq i \leq n-2$,

(7) $\quad r(i) = s(i) \quad$ für $1 \leq i \leq \mu$,
$r(0) = s(0)$ falls nicht der Ausnahmefall vorliegt,
$r(\nu) = s(\nu)$ für $q = 2$ und $\zeta \notin L$,

(8) $\quad r(i+1) = qs(i) \quad$ für $0 \leq i < \lambda$,

(9) $\quad r(i) = qs(i) \quad$ für $\mu < i \leq n-2$ außer für $i = \nu$,
falls $q = 2$ und $\zeta \notin L$ ist.

Wegen $Z_i = \{H_1(i), \dots, H_{s(i)}(i)\}$ und $z_i = \{T_1(i), \dots, T_{r(i)}(i)\}$ ergibt sich mit (1), (1′), (6), (7), (8) und (9) folgendes:

(10) $\quad z_{i+1} = Z_i \leq z_i \quad$ für $\lambda \leq i \leq n-2$,

(11) $\quad z_i = Z_i \leq z_{i+1} \quad$ für $1 \leq i \leq \mu$,
$z_0 = Z_0 \leq z_1$ falls nicht der Ausnahmefall vorliegt,
$z_\nu = Z_\nu \leq z_{\nu+1}$ für $q = 2$ und $\zeta \notin L$,

(12) $\quad z_{i+1} > Z_i \quad$ für $0 \leq i < \lambda$,

(13) $\quad z_i > Z_i \quad$ für $\mu < i \leq n-2$ außer für $i = \nu$,
falls $q = 2$ und $\zeta \notin L$ ist.

Im Ausnahmefall ist $\lambda = 1$, also folgt aus (10) und (11)

(14) $\quad z_i = z_{i+1} \quad$ für $\lambda \leq i \leq \mu$,
$z_\nu = z_{\nu+1}$ für $q = 2$, falls $\zeta \notin L$ und $\nu \geq \lambda$ ist.

Für $i \in \mathbb{Z}$ gelten die Äquivalenzen:

$$(+) \qquad i < \lambda \iff i \leq \lceil \lambda \rceil - 1 \qquad \text{und} \qquad i > \mu \iff i \geq \lfloor \mu \rfloor + 1.$$

Aus (11), (12) und (+) folgt dann

(15) $\quad z_i < z_{i+1} \quad$ für $0 \leq i \leq \min\{\mu, \lceil \lambda \rceil - 1\}$,
falls nicht der Ausnahmefall vorliegt.

Aus (10), (13) und (+) folgt

(16) $\quad z_i > z_{i+1} \quad$ für $\max\{\lambda, \lfloor \mu \rfloor - 1\} \leq i \leq n-2$,
außer für $i = \nu$, falls $q = 2$ und $\zeta \notin L$ ist.

(17) Ist $q = 2$, sowie $\zeta \notin L$ und $\nu \geq \lfloor \mu \rfloor + 1$, so ist $\zeta^{2^{l-a}} \notin L$.

Denn wäre $\zeta^{2^{l-a}} \in L$, so wäre $\nu > \mu \geq l - a - 1$, also $\nu \geq l - a$, und aus der Definition von ν würde der Widerspruch $\zeta^{2^{l-a}} \notin L$ folgen.

Sei jetzt nicht der Ausnahmefall. Es ist bereits gezeigt worden, daß dann $\lceil \lambda \rceil \leq \lfloor \mu \rfloor + 1$ ist. Daraus ergibt sich:

$$(++) \qquad \lambda \leq \lceil \lambda \rceil \leq \lfloor \mu \rfloor + 1 \text{ und } \lceil \lambda \rceil - 1 \leq \lfloor \mu \rfloor \leq \mu.$$

Aus (14), (15) und (++) folgt jetzt

$$z_0 < z_1 < \cdots < z_{\lceil \lambda \rceil} = \cdots = z_{\lfloor \mu \rfloor + 1}.$$

Weiter folgt aus (16), (17) und (++) sowohl

$$z_{\lfloor \mu \rfloor + 1} > z_{\lfloor \mu \rfloor + 2} > \cdots > z_{n-1},$$

falls nicht $q = 2, \zeta^{2^{l-a}} \notin L$ und $\lfloor \mu \rfloor + 1 \leq \nu < n - 1$ ist, als auch

$$z_{\lfloor \mu \rfloor + 1} > \cdots > z_\nu = z_{\nu+1} > \cdots > z_{n-1},$$

wenn $q = 2, \zeta^{2^{l-a}} \notin L$ und $\lfloor \mu \rfloor + 1 \leq \nu < n - 1$ ist. Damit ist Teil 1) bewiesen.

Um Teil 2) zu zeigen, setzen wir jetzt den Ausnahmefall voraus. Das heißt, es ist $q = 2$, $n \geq 3$ und $K_1 = K_0[\zeta] = K_0[\zeta^2]$. Dann ist $\lambda = 1$ und $l = 1 = a$. Also ist $\zeta^{2^{l-a}} \in L$ und für μ gilt:

$$\mu = \max\left\{ l - a - 1, \frac{l-1}{2} \right\} = \max\{-1, 0\} = 0.$$

Aus (16) folgt deshalb $z_1 > \cdots > z_{n-1}$. Durch (2) und (3) erhalten wir außerdem

$$\begin{aligned} r(0) &= \frac{\varphi(|G_0|)}{K_0[\zeta] : K_0} = \frac{\varphi(q^n)}{q} = q^{n-2}(q-1) \\ r(1) &= \frac{\varphi(|G_1|)}{K_1[\zeta^2] : K_1} = \varphi(q^{n-1}) = q^{n-2}(q-1). \end{aligned}$$

Also ist $r(0) = r(1)$. Nach 4.2 sind die G_0-treuen, irreduziblen K_0G_0-Teilmoduln von L als K_0-Algebra isomorph zum Zerfällungskörper von $X^{q^n} - 1$ über K_0, also zu $K_0[\zeta]$. Für $i \in \{1, \ldots, r(0)\}$ folgt daraus

$$\dim_{K_0} T_i(0) = \dim_{K_0} K_0[\zeta] = \dim_{K_0} K_1 = 2.$$

Aus analogen Überlegungen ergibt sich $\dim_{K_0} T_i(1) = \dim_{K_0} K_1[\zeta^2] = 2$ für $i \in \{1, \ldots, r(0)\}$ und, daß jeder G_1-treue, irreduzible K_0G_1-Teilmodul von L die Dimension $K_0[\zeta^2] : K_0 = 2$ über K_0 hat. Da K_0G_1 ein Unterring sowohl von K_0G_0 als auch von K_1G_1 ist, sind $T_i(0)$ und $T_j(1)$ für alle $i, j \in$

$\{1, \ldots, r(0)\}$ auch K_0G_1-Moduln, die wegen $G_1 \subseteq G_0$ auch G_1-treu und aus Dimensionsgründen als K_0G_1-Moduln sogar irreduzibel sind. Nach (3′) ist jede homogene Komponente $H_k(0)$ von T eine direkte Summe von zwei G_1-treuen, irreduziblen K_0G_1-Moduln. Also ist jedes $H_k(0)$ wegen $Z_0 \leq z_0$ bzw. $Z_0 \leq z_1$ Summe von genau zwei Elementen aus z_0 bzw. aus z_1.

Weil $T_i(0)$ und $T_j(1)$ als K_0G_1-Moduln irreduzibel sind, ist entweder $T_i(0) \cap T_j(1) = \{0\}$ oder $T_i(0) = T_j(1)$. Wir nehmen nun an, daß es $\alpha, \beta \in \{1, \ldots, r(0)\}$ gibt mit $T_\alpha(0) = T_\beta(1)$. Weiter sei $V := T_\alpha(0)$. Jedes $k \in K_1$ induziert eine Abbildung $v \to kv$ von V in V. Weil V insbesondere auch ein K_1G_1-Modul ist, sind alle diese Abbildungen offenbar K_0G_1-Endomorphismen von V; deshalb kann K_1 als Teilmenge von $\mathrm{End}_{K_0G_1}(V)$ aufgefaßt werden. Da V als K_0G_1-Modul irreduzibel ist, folgt mit dem Lemma von Schur, daß $\mathrm{End}_{K_0G_1}(V)$ ein Schiefkörper und V ein $\mathrm{End}_{K_0G_1}(V)$-Vektorraum ist. Aus $\dim_{K_1} V = 1$ und der Tatsache, daß K_1 ein Teilkörper von $\mathrm{End}_{K_0G_1}(V)$ ist, ergibt sich daher $K_1 = \mathrm{End}_{K_0G_1}(V)$.

Sei nun $G_0 = \langle g \rangle$. Weil V auch ein K_0G_0-Modul ist, ist g ein K_0G_1-Endomorphismus von V. Wegen $K_1 = \mathrm{End}_{K_0G_1}(V)$ gibt es dann ein $k \in K_1$ mit $g(v) = kv$ für alle $v \in V$. Aus $|G_0| = 2^n$ folgt $g^{2^n}(v) = v \neq g^{2^{n-1}}(v)$ und damit auch $k^{2^n}v = v \neq k^{2^{n-1}}v$ für alle $v \in V$. Also ist k eine primitive 2^n-te Einheitswurzel, woraus $K_1 = K_0[\zeta] = K_0[k]$ folgt, weil der Ausnahmefall vorliegt. Andrerseits ergibt sich

$$k(kv) = g(kv) = g(k)g(v) = g(k)kv$$

für alle $v \in V$. Deshalb ist $g(k) = k$ und aus $g \in G_0 = \mathrm{Gal}(L/K_0)$ folgt $k \in K_0$. Das bedeutet aber $K_1 = K_0[k] = K_0$, was ein Widerspruch ist. Also gilt doch $T_i(0) \cap T_j(1) = \{0\}$ für alle $i, j \in \{1, \ldots, r(0)\}$, womit alles gezeigt ist. □

Schluß des Beweises von 1.1 und 2.4:
Es bleibt noch die Existenz eines vollständig regulären Elements in L/K für den Fall, daß K endlich, $L : K = q^n$ eine Primzahlpotenz und q ungleich der Charakteristik von K ist, nachzuweisen. Dies soll nun mittels vollständiger Induktion über n geschehen.

Für $n = 0$ ist nichts zu zeigen, für $n = 1$ ist sicher jedes reguläre Element vollständig regulär und nach dem Satz von der Normalbasis gibt es ein reguläres Element in K_1/K. Sei also $n > 1$ und die Behauptung für $n-1$ schon gezeigt. Nach Induktionsannahme gibt es dann ein $x \in K_{n-1}$, das vollständig regulär in K_{n-1}/K ist. Für $0 \leq i \leq n-1$ sei $\hat{G}_i := \mathrm{Gal}(K_{n-1}/K_i)$. Dann ist x nach 2.2 in keinem echten $K_i\hat{G}_i$-Teilmodul von K_{n-1} enthalten für alle $0 \leq i \leq n-1$. Sei außerdem $\hat{X}_i$ die Menge der irreduziblen $K_i\hat{G}_i$-Teilmoduln von K_{n-1}. Wegen 5.6 ist x dann $\hat{X}_i$-regulär für alle $0 \leq i \leq n-1$. Weil $\hat{G}_i$ genau aus den Restriktionen der Elemente von G_i auf K_{n-1} besteht, wird $\hat{X}_i$ von den irreduziblen K_iG_i-Teilmoduln von $K_{n-1} = U(i)$ gebildet. Also sind die Komponenten von x bzgl. der direkten Zerlegung von $U(i)$ in irreduzible Teilmoduln allesamt von Null verschieden für $0 \leq i \leq n-1$. Wenn es ein

$y \in T$ gäbe, so daß für $0 \leq i \leq n-1$ die Komponenten von y bezüglich der direkten Zerlegung von $T = T(i)$ in irreduzible Teilmoduln auch alle von Null verschieden wären, so würde wegen $L = U(i) \oplus T(i)$ das Element $x + y \in L$ in keinem echten K_iG_i-Teilmodul von $L = L(i)$ für $0 \leq i \leq n-1$ enthalten sein. Offensichtlich wäre weder x noch y gleich Null. Weil $K_{n-1} \cap T = \{0\}$ ist, würde $x+y$ auch von Null verschieden sein. Wie wir gesehen haben, hat $L(n)$ nur $\{0\}$ als echten Teilmodul. Daher wäre $x + y$ auch für $i = n$ in keinem echten Teilmodul von $L(i)$ enthalten. Nach 2.2 wäre $x+y$ vollständig regulär in L/K und die Behauptung gezeigt. Wir müssen also nur noch nachweisen, daß es ein $y \in T$ gibt, welches z_i-regulär ist für alle $0 \leq i \leq n-1$. Das soll nun geschehen.

Liegt nicht der Ausnahmefall vor, so ist nach 5.8.1 und 5.5 jedes $z_{\lfloor\lambda\rfloor}$-reguläre Element auch z_i-regulär für $0 \leq i \leq n-1$. Da es sicherlich ein $z_{\lfloor\lambda\rfloor}$-reguläres Element gibt, ist die Behauptung für diesen Fall gezeigt.

Sei jetzt der Ausnahmefall, dann ist nach 5.8.2 jedes z_1-reguläre Element wegen 5.5 auch z_i-regulär für $1 \leq i \leq n-1$. Es bleibt also noch zu zeigen, daß es ein z_0-reguläres Element gibt, welches z_1- regulär ist. Sei dazu $H_j(0)$ eine homogene K_0G_1-Komponente von T. Dann hat $H_j(0)$ nach 5.8.2 die beiden Zerlegungen $X := \{T_\alpha(0), T_\beta(0)\}$ und $Y := \{T_\gamma(1), T_\delta(1)\}$ mit geeigneten $\alpha, \beta, \gamma, \delta \in \{1, \ldots, r(0)\}$. Sei weiter $R_{j,0}$ bzw. $R_{j,1}$ die Menge der X-regulären bzw. Y-regulären Elemente von $H_j(0)$. Dann ist $x \in H_j(0)$ genau dann X-regulär, wenn x weder in $T_\alpha(0)$ noch in $T_\beta(0)$ liegt, d.h.

$$R_{j,0} = H_j(0) \backslash (T_\alpha(0) \cup T_\beta(0)).$$

Eine analoge Überlegung ergibt:

$$R_{j,1} = H_j(0) \backslash (T_\gamma(1) \cup T_\delta(1)).$$

Daraus folgt:

$$R_{j,0} \cap R_{j,1} = H_j(0) \backslash (T_\alpha(0) \cup T_\beta(0) \cup T_\gamma(1) \cup T_\delta(1)).$$

Durch 5.8.2 wissen wir außerdem, daß

$$\dim_K T_\alpha(0) = \dim_K T_\beta(0) = \dim_K T_\gamma(1) = \dim_K T_\delta(1) = 2$$

ist. Das bedeutet

$$|T_\alpha(0)| = |T_\beta(0)| = |T_\gamma(1)| = |T_\delta(1)| = |K|^2$$

und wegen $H_j(0) = T_\alpha(0) \oplus T_\beta(0)$ ist $|H_j(0)| = |K|^4$. Es gilt also

$$|R_{j,0} \cap R_{j,1}| \geq |K|^4 - 4|K|^2.$$

Weil der Ausnahmefall vorliegt ist $q = 2$. Wegen $q \neq \operatorname{char} K$ ist die Charakteristik von K mindestens 3, also $|K| \geq 3$. Daraus folgt $|K|^2 > 4$ und weiter $|K|^4 > 4|K|^2$. Wir erhalten also

$$|R_{j,0} \cap R_{j,1}| > 0$$

und $R_{j,0} \cap R_{j,1} \neq \emptyset$. Wir können jetzt für jedes $j \in \{1, \ldots, s(0)\}$ ein y_j aus $R_{j,0} \cap R_{j,1}$ wählen und $y := \sum_{j=1}^{s(0)} y_j$ setzen. Offenbar ist y sowohl z_0-regulär als auch z_1-regulär. Damit sind 1.1 und 2.4 gezeigt. $\square$

6 Bestimmung vollständig regulärer Erweiterungen, deren Galoisgruppen zyklisch von Primzahlpotenzordnung sind

Wir wollen jetzt der Frage nachgehen, wann eine endliche, galoissche Erweiterung mit zyklischer Galoisgruppe von Primzahlpotenzordnung vollständig regulär ist. Dabei genügt es, sich auf den Fall zu beschränken, daß die Charakteristik der Körper kein Teiler der Ordnung der Galoisgruppe ist. Denn, teilt die Charakteristik der Körper die Ordnung der Galoisgruppe, so haben wir bereits in 2.8 gesehen, daß die Galoiserweiterung dann stets vollständig regulär ist.

Hilfssatz 6.1 *Im Ausnahmefall gibt es ein z_0-reguläres Element in T, das nicht z_1-regulär ist, und umgekehrt.*

Beweis: Nach 5.8.2 ist jede homogene Komponente $H_k(0)$ von T die direkte Summe von genau zwei Elemente aus z_0 und genau zwei Elementen aus z_1. Sei jetzt o.B.d.A. (Umnumerierung)

$$H_1(0) = T_1(0) \oplus T_2(0) = T_1(1) \oplus T_2(1).$$

Dann sind $X := \{T_1(0), T_2(0)\}$ und $Y := \{T_1(1), T_2(1)\}$ zwei Zerlegungen von $H_1(0)$. Ist nun $y_1 \neq 0$ ein Element von $T_1(1)$, so ist y_1 nicht Y-regulär in $H_1(0)$. Aus 5.8.2 folgt ferner

$$T_1(1) \cap T_1(0) = \{0\} = T_1(1) \cap T_2(0).$$

Also liegt y_1 weder in $T_1(0)$ noch in $T_2(0)$, d.h. y_1 ist X-regulär in $H_1(0)$. Für $3 \leq i \leq r(0)$ wählen wir jeweils ein y_i aus $T_i(0)\backslash\{0\}$ und setzen

$$w := y_1 + y_3 + y_4 + \cdots + y_{r(0)}.$$

Dann ist w offenbar z_0-regulär aber nicht z_1-regulär. Analog kann man ein Element konstruieren, das zwar z_1-regulär aber nicht z_0-regulär in T ist. □

Mit X_i wird jetzt die Menge aller irreduziblen Teilmoduln von $L(i)$ bezeichnet; dann ist X_i eine direkte Zerlegung von L, und es gilt folgender Satz.

Satz 6.2 *Es sei L/K eine endliche Galoiserweiterung und die zugehörige Galoisgruppe sei zyklisch der Ordnung q^n, wobei q eine Primzahl ungleich der Charakteristik von K ist. Dann sind die drei folgenden Aussagen äquivalent:*

1. *L/K ist vollständig regulär,*

2. *$\lambda(L/K) \leq 0$,*

3. *$X_0 \geq X_1 \geq \cdots \geq X_n$.*

Ferner ist K_i/K für $0 \le i \le n$ vollständig regulär, falls L/K vollständig regulär ist.

Beweis: Es sei wieder $\lambda = \lambda(L/K)$. Wir betrachten zunächst den Fall $n \in \{0,1\}$. Dann ist L/K trivialerweise vollständig regulär, d.h. es gilt 1). Außerdem folgt $l = a = 0$. Insbesondere kann der Ausnahmefall nicht eintreten, und es ist $\lambda = \min\{0, -\frac{1}{2}\} < 0$, d.h. es gilt 2). Ist $n = 0$, so ist 3) trivial. Für ein beliebiges n ist, wie wir schon gesehen haben, $L(n)$ irreduzibel, was $X_n = \{L\}$ bedeutet. Jede andere Zerlegung ist also feiner als X_n. Für $n = 1$ ist damit $X_0 \ge X_1$ richtig und es folgt 3). Für $n \in \{0,1\}$ gelten also stets die Aussagen 1) – 3), insbesondere ist die Äquivalenz von 1) – 3) richtig.

Sei jetzt $n \ge 2$ und z_i' für $0 \le i \le n$ die Menge der irreduziblen K_iG_i-Teilmoduln von $L(i)$, die als G_i-Moduln untreu sind. Dann ist $z_n' = \emptyset$, weil $U(n) = \{0\}$ ist. Für $0 \le i \le n-1$ ist z_i' wegen $U(i) = K_{n-1}$ eine direkte Zerlegung von K_{n-1}.

Offensichtlich ist $X_i = z_i \cup z_i'$ für $0 \le i \le n-1$. Sei weiter R_i bzw. R_i' bzw. S_i die Menge der z_i-regulären bzw. der z_i'-regulären bzw. X_i-regulären Elemente von T bzw. K_{n-1} bzw. L. Dann gilt

$$S_i = R_i + R_i' = \{r_i + r_i' | r_i \in R_i, r_i' \in R_i'\}$$

für alle $0 \le i \le n-1$. Jedes Element aus L^* ist sicherlich regulär in L/K_n. Wegen 5.6 ist ein Element aus L genau dann vollständig regulär in L/K, wenn es X_i-regulär ist für alle $0 \le i \le n$. Wird mit V die Menge der vollständig regulären Elemente von L/K bezeichnet, so folgt:

$$V = \bigcap_{i=0}^{n-1} S_i \cap L^* = \bigcap_{i=0}^{n-1} S_i,$$

da $S_i \subseteq L^*$ für $0 \le i \le n-1$ ist. Nach Definition und 5.6 ist S_0 genau die Menge der regulären Elemente von L/K. Das ergibt folgende Äquivalenzen:

$$\begin{array}{lcl}
L/K \text{ ist vollständig regulär} & \Longleftrightarrow & S_0 \subseteq V = \bigcap_{i=0}^{n-1} S_i \\
 & \Longleftrightarrow & S_0 \subseteq S_i \text{ für alle } 1 \le i \le n-1 \\
 & \Longleftrightarrow & R_0 + R_0' \subseteq R_i + R_i' \\
(*) & & \quad \text{für alle } 1 \le i \le n-1 \\
 & \Longleftrightarrow & R_0 \subseteq R_i \text{ und } R_0 \subseteq R_i' \\
 & & \quad \text{für alle } 1 \le i \le n-1.
\end{array}$$

„3) $\Rightarrow$ 1)“: Es gelte $X_0 \ge X_1 \ge \cdots \ge X_n$. Nach 5.5 ist deshalb jedes X_i-reguläre Element schon X_{i+1}-regulär für $0 \le i \le n-1$. Mit den obigen Bezeichnungen ausgedrückt, heißt das

$$S_0 \subseteq S_1 \subseteq \cdots \subseteq S_n.$$

Aus $(*)$ folgt, daß L/K vollständig regulär ist, also gilt 1).

„1) $\Rightarrow$ 2)“: Sei L/K vollständig regulär. Der Ausnahmefall kann nicht eintreten. Denn nach 6.1 gibt es im Ausnahmefall ein z_0-reguläres Element, das nicht z_1-regulär ist, also $R_0 \not\subseteq R_1$ gilt. Wegen $(*)$ kann dann L/K nicht vollständig regulär sein.

Wir nehmen jetzt an, es ist $\lceil\lambda\rceil > 0$. Dann folgt mit 5.8.1

$$z_0 < z_1 < \cdots < z_{\lceil\lambda\rceil}.$$

Nach 5.5 gilt dann für die Mengen der z_i- regulären Elemente:

$$R_{\lceil\lambda\rceil} \subset R_{\lceil\lambda\rceil-1} \subset \cdots \subset R_0.$$

Aus $(*)$ folgt der Widerspruch

$$R_{\lceil\lambda\rceil} \supseteq R_{\lceil\lambda\rceil-1} \supseteq \cdots \supseteq R_0.$$

Das ist ein Widerspruch, also muß $\lceil\lambda\rceil \leq 0$ und damit $\lambda \leq 0$ sein. Das zeigt 2).

„2) $\Rightarrow$ 3)“: Sei $\lambda \leq 0$, also $\lceil\lambda\rceil \leq 0$. Dann ist insbesondere $\lambda \neq 1$ und es liegt nicht der Ausnahmefall vor. Weiter gilt mit 5.8.1 folgendes

$$(**) \qquad z_0 \geq z_1 \geq \cdots \geq z_{n-1}.$$

Für die Erweiterung K_{n-1}/K wollen wir l', s', a' und λ' analog zu l, s, a und λ definieren. Da ζ^q eine primitive q^{n-1}-te Einheitswurzel ist, gibt es ein $l' \in \{0, \ldots, n-2\}$ und ein $s' \in \mathbb{N}$, welches $q-1$ teilt, so daß $K[\zeta^q] : K = q^{l'}s'$ gilt. Weiter sei $K_{a'} := K[\zeta^q] \cap K_{n-1}$ und $\lambda' := \lambda(K_{n-1}/K)$, das heißt

$$\lambda' = \begin{cases} 1, & \text{falls } q = 2,\ n-1 \geq 3 \text{ und } K_1 = K[\zeta^2] = K[\zeta^4] \\ \frac{l'-2}{2}, & \text{falls } q = 2,\ 2|l',\ 0 < \frac{l'}{2} \leq a' \\ & \text{und } K_{l'/2} \neq K_{l'/2-1}[\zeta^{2^{l'/2+1}}] \\ \min\left\{a', \frac{l'-1}{2}\right\}, & \text{sonst.} \end{cases}$$

Da $K[\zeta^q] : K = q^{l'}s'$ ein Teiler von $K[\zeta] : K = q^l s$ ist, folgt $l' \leq l$. Außerdem ist $K_{a'} = K[\zeta^q] \cap K_{n-1} \subseteq K[\zeta] \cap L = K_a$, d.h. $a' \leq a$. Wir wollen jetzt zeigen, daß $\lambda' \leq 0$ gilt.

Zunächst nehmen an, es wäre $q = 2$, $n-1 \geq 3$ und $K_1 = K[\zeta^2] = K[\zeta^4]$. Weil nicht der Ausnahmefall vorliegt, müßte dann $K[\zeta] \neq K[\zeta^2]$ sein. Daraus würde folgen

$$K[\zeta] : K = (K[\zeta] : K[\zeta^2]) \cdot (K[\zeta^2] : K) = 2 \cdot 2 = 4.$$

Also wäre dann $l = 2$ und $a \in \{1, 2\}$. Wegen $\lambda \leq 0$ wäre ferner

$$\min\left\{a, \frac{l-1}{2}\right\} = \min\left\{a, \frac{1}{2}\right\} = \frac{1}{2} \neq \lambda.$$

Nach der Definition von λ müßte dann aber $K_{l/2} \neq K_{l/2-1}[\zeta^{2^{l/2}}]$ gelten. Das ist aber wegen $l = 2$ ein Widerspruch zu $K_1 = K[\zeta^2]$. Also kann der angenommen Fall nicht eintreten.

Es sei nun $q = 2$, $0 < l$ gerade und $\lambda = \frac{l-2}{2}$. Wegen $\lambda \leq 0$ muß $l = 2$ sein. Mit 3.1.1 folgt, daß $K[\zeta] : K[\zeta^2] = 2$ ist. Also gilt

$$K[\zeta^2] : K = \frac{K[\zeta] : K}{K[\zeta] : K[\zeta^2]} = \frac{2^2}{2} = 2.$$

Das heißt $l' = 1$. Aus der Definition von λ' ergibt sich das gewünschte Resultat:

$$\lambda' = \min\left\{a', \frac{l'-1}{2}\right\} = \min\{a', 0\} \leq 0.$$

Es sei schließlich $\lambda = \min\{a, \frac{l-1}{2}\}$. Wegen $\lambda \leq 0$ ist dann entweder $l \leq 1$ oder $a = 0$. Ist $l \leq 1$, so folgt $l' \leq l \leq 1$, also ergibt sich

$$\lambda' = \min\left\{a', \frac{l'-1}{2}\right\} \leq \min\{a', 0\} \leq 0.$$

Ist $l \geq 2$, so muß $a = 0$ sein. Dann ist aber der Fall $0 < \frac{l'}{2} \leq a'$ wegen $a' \leq a = 0$ nicht möglich. Also ist

$$\lambda' = \min\left\{a', \frac{l'-1}{2}\right\} \leq \min\left\{0, \frac{l'-1}{2}\right\} \leq 0.$$

Damit ist bewiesen, daß $\lambda' \leq 0$ ist. Wir haben also folgendes gezeigt:

(+) Für alle $n \in \mathbb{N}$ folgt $\lambda(K_{n-1}/K) \leq 0$, aus $\lambda(K_n/K) \leq 0$ ist.

Wir zeigen jetzt:

$$z'_0 \geq \cdots \geq z'_{n-1}.$$

Der Beweis soll durch vollständige Induktion über n geschehen. Für $n = 1$ ist die Behauptung trivial. Sei also $n \geq 2$ und die Behauptung für K_{n-1}/K schon bewiesen. Mit $\hat{G}_i$ werde die Galoisgruppe von K_{n-1} über K_i für $0 \leq i \leq n-1$ bezeichnet. K_{n-1} läßt sich dann zu einem $K_i\hat{G}_i$-Modul machen und alle weiteren Überlegungen, die wir über L/K geführt haben, lassen sich hier entsprechend machen. Für K_{n-1}/K seien daher $\hat{U}(i), \hat{T}(i), \hat{z}_i$ und $\hat{z}'_i$ analog zu $U(i), T(i), z_i$ und z'_i definiert. Nach Induktionsvoraussetzung folgt dann

$$\hat{z}'_0 \geq \hat{z}'_1 \geq \cdots \geq \hat{z}'_{n-2}.$$

Weil $\lambda' \leq 0$ ist, gilt mit 5.8.1

$$\hat{z}_0 \geq \hat{z}_1 \geq \cdots \geq \hat{z}_{n-2}.$$

Zusammengefaßt ergibt das

$$\hat{z}'_0 \cup \hat{z}_0 \geq \hat{z}'_1 \cup \hat{z}_1 \geq \cdots \geq \hat{z}'_{n-2} \cup \hat{z}_{n-2}.$$

Für K_{n-1} gilt analog zu L :

$$U(i) = K_{n-1} = \hat{T}(i) \oplus \hat{U}(i).$$

Wegen $\hat{G}_{n-1} = \{\mathrm{id}_{K_{n-1}}\}$ ist K_{n-1} als $K_{n-1}\hat{G}_{n-1}$-Modul ein K_{n-1}-Vektorraum, der als $\hat{G}_{n-1}$-Modul treu ist. Deshalb ist $\hat{z}_{n-1} = \{K_{n-1}\}$ und $\hat{z}'_{n-1} = \emptyset$. Nach dem Hauptsatz der Galoistheorie ist

$$\hat{G}_i = \{g|_{K_{n-1}} \text{ mit } g \in G_i\} \quad \text{für } 0 \leq i \leq n-1.$$

Demnach ist eine Teilmenge von K_{n-1} genau dann ein $K_i\hat{G}_i$-Modul, wenn sie ein K_iG_i-Modul ist. Die irreduziblen $K_i\hat{G}_i$-Teilmoduln von K_{n-1} sind also genau die irreduziblen K_iG_i-Teilmoduln von K_{n-1}. Da einerseits die irreduziblen $K_i\hat{G}_i$-Teilmoduln von K_{n-1} die Menge $\hat{z}_i \cup \hat{z}'_i$ bilden und andrerseits die irreduziblen K_iG_i-Teilmoduln von K_{n-1} genau diejenigen sind, die als G_i-Moduln nicht treu sind, gilt

$$\hat{z}_i \cup \hat{z}'_i = z'_i \text{ für } 0 \leq i \leq n-1.$$

Damit folgt jetzt wegen

$$\hat{z}_0 \cup \hat{z}'_0 \geq \cdots \geq \hat{z}_{n-2} \cup \hat{z}'_{n-2} \geq \{K_{n-1}\} = \hat{z}_{n-1} \cup \hat{z}'_{n-1},$$

daß $z'_0 \geq \cdots \geq z'_{n-1}$ gilt. Das zeigt die Behauptung.

Wir haben also nach $(**)$ einerseits

$$z_0 \geq \cdots \geq z_{n-1}$$

und nach dem eben Bewiesenen andrerseits

$$z'_0 \geq \cdots \geq z'_{n-1}.$$

Weil $X_i = z_i \cup z'_i$ für $0 \leq i \leq n-1$ und $X_n = \{L\}$ ist, folgt damit

$$X_0 \geq \cdots \geq X_{n-1} \geq \{L\} = X_n.$$

Das heißt, es gilt 3). Die Äquivalenz der drei Aussagen ist damit gezeigt.

Sei jetzt L/K vollständig regulär, dann ist $\lambda(K_n/K) \leq 0$ nach dem vorher Bewiesenen. Aus $(+)$ folgt mit vollständiger Induktion, daß auch $\lambda(K_i/K) \leq 0$ für $0 \leq i \leq n$ gilt, was äquivalent dazu ist, daß K_i/K für $0 \leq i \leq n$ vollständig regulär ist. Damit ist alles gezeigt. □

Sind die Voraussetzungen des soeben gezeigten Satzes erfüllt und ist $n \leq 2$, so ist L/K vollständig regulär. Denn der Ausnahmefall kann nicht vorliegen, weil $n < 3$ ist; außerdem ist $l \leq n-1 \leq 1$, womit aus der Definition von λ sofort $\lambda \leq 0$ und mit 6.2 die Behauptung folgt.

Durch nähere Betrachtung der Definition von λ erhalten wir folgendes Korollar:

Korollar 6.3 *Sei L/K eine Galoiserweiterung mit zyklischer Galoisgruppe G der Ordnung q^n, wobei q eine Primzahl ungleich der Charakteristik von K ist. Genau dann ist L/K vollständig regulär, wenn einer der folgenden Fälle vorliegt:*

1. $L \cap K[\zeta] = K$,
2. $q \neq 2,\ K[\zeta] : K = q \cdot s,\ s|(q-1)$ *und* $K_1 \subseteq K[\zeta]$,
3. $q = 2,\ K_1 = K[\zeta]$ *und* $\zeta^2 \in K$,
4. $q = 2,\ K[\zeta] : K = 4,\ K[\zeta^2] \neq K_1 \subseteq K[\zeta]$ *und* $K[\zeta^2] : K = 2$.

Beweis: Die Bedingung

$$q = 2 \ \wedge \ 2|l \ \wedge \ 0 < \frac{l}{2} \leq a \ \wedge \ K_{l/2} \neq K_{l/2-1}[\zeta^{2^{l/2}}]$$

sei durch $(\star)$ abgekürzt. Ferner ist wieder $\lambda := \lambda(L/K)$.

„⇒“: Sei L/K vollständig regulär. Nach 6.2 ist dann $\lambda \leq 0$. Insbesondere liegt nicht der Ausnahmefall vor.

Fall 1. Es sei die Bedingung $(\star)$ erfüllt. Nach der Definition von λ muß dann $\frac{l-2}{2} \leq 0$ sein, das heißt $l \in \{0, 1, 2\}$. Wegen $(\star)$ ist l durch 2 teilbar und es gilt $0 < \frac{l}{2} \leq a$. Daraus folgt $l = 2$ und $a \geq 1$. Insbesondere ist dann $K_1 \neq K[\zeta^2]$ und $K_1 \subseteq K_a \subseteq K[\zeta]$. Aus $l = 2$ folgt außerdem $K[\zeta] : K = 4$, woraus sich mit 3.1.1 weiter $K[\zeta] : K[\zeta^2] = 2$ ergibt. Damit erhalten wir

$$K[\zeta^2] : K = \frac{K[\zeta] : K}{K[\zeta] : K[\zeta^2]} = \frac{4}{2} = 2,$$

und es gilt 4).

Fall 2. Es gelte nicht $(\star)$. Nach der Definition von λ ist dann $\min\{a, \frac{l-1}{2}\} \leq 0$, also ist entweder $a = 0$ oder $a = l = 1$. Wenn $a = 0$ ist, dann gilt $L \cap K[\zeta] = K$ nach der Definition von a. Also ist 1) richtig.

Sei jetzt $a = l = 1$. Ist $q \neq 2$, dann folgt sofort Aussage 2). Sei nun $q = 2$. Dann ist $K[\zeta] : K = 2$ und $K_1 \subseteq K[\zeta]$. Daraus ergibt sich $K[\zeta] = K_1$. Ist $n \leq 2$, so ist trivialerweise $\zeta^2 \in K$, d.h. es gilt 3). Ist $n \geq 3$, dann ist $K[\zeta] \neq K[\zeta^2]$, weil ja nicht der Ausnahmefall vorliegen kann. Wegen $K[\zeta] : K = 2$ muß aber $K[\zeta^2] = K$ sein, also ist wiederum $\zeta^2 \in K$ und es gilt 3).

„⇐“: Es sei eine der Aussagen 1) – 4) richtig.

Fall 1. Es gelte Aussage 1), d.h. es ist $L \cap K[\zeta] = K$. Dann ist $a = 0$, und es kann insbesondere nicht der Ausnahmefall vorliegen. Weiter ist die Bedingung $(\star)$ nicht erfüllt, weil dort $0 < a$ gefordert ist. Also ist $\lambda = \min\{0, \frac{l-1}{2}\} \leq 0$.

Fall 2. Es gelte 2). Aus der Definition von l folgt, daß $l = 1$ ist. Wegen $q \neq 2$ liegt weder der Ausnahmefall vor noch ist $(\star)$ erfüllt. Also ist $\lambda = \min\{a, 0\} \leq 0$.

Fall 3. Es gelte 3). Dann ist $K[\zeta^2] = K \neq K_1 = K[\zeta]$, also liegt nicht der Ausnahmefall vor. Außerdem ist

$$K[\zeta] : K = K_1 : K = 2,$$

das bedeutet $l = 1$. Insbesondere ist l ungerade, weshalb $(\star)$ nicht erfüllt ist. Damit ist $\lambda = \min\{a, 0\} \leq 0$.

Fall 4. Es gelte 4). Wegen $K[\zeta^2] \neq K_1$ liegt nicht der Ausnahmefall vor. Weiter folgt aus $K[\zeta] : K = 4$, daß $l = 2$ und insbesondere gerade ist. Wegen $K_1 \subseteq K[\zeta]$ ist außerdem $a \geq 1$, so daß $0 < \frac{l}{2} \leq a$ gilt. Schließlich ist noch

$$K_{l/2-1}[\zeta^{2^{l/2}}] = K[\zeta^2] \neq K_1 = K_{l/2}.$$

Also ist $(\star)$ erfüllt und es ergibt sich $\lambda = \frac{l-2}{2} = 0$.

In allen vier Fällen ist $\lambda \leq 0$. Daraus folgt mit 6.2, daß L/K vollständig regulär ist. $\square$

Der folgende Satz liefert nun die gewünschte notwendige und hinreichende Bedingung für vollständig reguläre Körpererweiterungen.

Satz 6.4 *Die Voraussetzungen seien die gleichen wie in 6.3. Dann ist L/K genau dann vollständig regulär, wenn $K[\zeta^q] \cap L = K$ gilt.*

Beweis: „$\Rightarrow$“: Sei L/K vollständig regulär. Nach 6.3 lassen sich vier Fälle unterscheiden.

Fall 1. Es gelte 6.3.1, das heißt, es ist $L \cap K[\zeta] = K$. Weil $K[\zeta^q]$ in $K[\zeta]$ enthalten ist, folgt $L \cap K[\zeta^q] = K$.

Fall 2. Es gelte 6.3.2. Es ist also $K[\zeta] : K = q \cdot s$ mit $s|(q-1)$ und $q \neq 2$. Nach 3.1.1 ist dann $K[\zeta] : K[\zeta^q] = q$. Wir nehmen an, K_1 läge in $K[\zeta^q]$. Dann würde folgen

$$\begin{aligned} K[\zeta] : K &= (K[\zeta] : K[\zeta^q]) \cdot (K[\zeta^q] : K_1) \cdot (K_1 : K) \\ &= q^2 \cdot (K[\zeta^q] : K_1). \end{aligned}$$

Also wäre q^2 ein Teiler von $q \cdot s$. Das ist sicher ein Widerspruch. Damit ist $K_1 \not\subseteq K[\zeta^q]$ und $L \cap K[\zeta^q] = K$.

Fall 3. Es gelte 6.3.3. Dann ist $q = 2$ und $\zeta^2 \in K$, also ist $L \cap K[\zeta^2] = L \cap K = K$.

Fall 4. Es gelte 6.3.4. Dann ist $q = 2$, $K[\zeta^2] : K = 2$ und $K_1 \neq K[\zeta^2]$. Wäre $K_1 \subseteq K[\zeta^2]$, so müßte $K = K_1$ sein, was ein Widerspruch ist. Also ist $K_1 \not\subseteq K[\zeta^2]$, und es folgt $L \cap K[\zeta^2] = K$.

„$\Leftarrow$“: Es sei nun $K[\zeta^q] \cap L = K$. Ist $L \cap K[\zeta] = K$, so liegt 6.3.1 vor, und L/K ist vollständig regulär. Sei also $L \cap K[\zeta] \neq K$; dann liegt K_1 in $L \cap K[\zeta]$ und damit auch in $K[\zeta]$. Insbesondere ist $l \geq 1$ und $K_1[\zeta] = K[\zeta]$. Auf Grund der Voraussetzung $K[\zeta^q] \cap L = K$ ist ferner $K_1 \not\subseteq K[\zeta^q]$.

Ist $l = 1$ und $q \neq 2$, so erhalten wir 6.3.2, und L/K ist vollständig regulär. Ist $l = 1$ und $q = 2$, dann ist $K[\zeta] : K = 2$. Zusammen mit $K_1 \subseteq K[\zeta]$ folgt daraus $K_1 = K[\zeta]$. Weil K_1 nicht in $K[\zeta^2]$ enthalten ist, folgt weiter $K = K[\zeta^2]$, also ist $\zeta^2 \in K$, und mit 6.3.3 ergibt sich ebenfalls die Behauptung.

Wir können deshalb annehmen, daß $l > 1$ ist. Nach 3.1.1 muß dann $K[\zeta] : K[\zeta^q] = q$ sein; denn andernfalls wäre $q = 2$ und $K[\zeta] = K[\zeta^2]$, woraus sich der Widerspruch $K_1 \subseteq K[\zeta] = K[\zeta^2]$ ergeben würde. Nach 5.7 gilt $K[\zeta] : K_1 = K_1[\zeta] : K_1 = q^{l-1}s$, wobei $l - 1 \geq 1$ ist. Mit 3.1.1 ergeben sich nun zwei Möglichkeiten:

$$K[\zeta] : K_1[\zeta^q] = q$$

oder

$$q = 2,\ K[\zeta] : K_1 = 2 \text{ und } K[\zeta] = K_1[\zeta^2].$$

Würde der erste Fall vorliegen, so wäre

$$K_1[\zeta^q] : K[\zeta^q] = \frac{K[\zeta] : K[\zeta^q]}{K[\zeta] : K_1[\zeta^q]} = \frac{q}{q} = 1,$$

was ein Widerspruch ist, da $K_1 \not\subseteq K[\zeta^q]$ gilt. Also liegt der zweite Fall vor, und wir erhalten

$$K[\zeta] : K = (K[\zeta] : K_1) \cdot (K_1 : K) = 2 \cdot 2 = 4,$$

sowie

$$K[\zeta^2] : K = \frac{K[\zeta] : K}{K[\zeta] : K[\zeta^2]} = \frac{4}{2} = 2.$$

Das ist die Situation von 6.3.4, und L/K ist auch in diesem Fall vollständig regulär, womit alles gezeigt ist. □

Mit 6.4 lassen sich jetzt Beispiele für vollständig reguläre Körpererweiterungen finden:

- Sei L/K eine endliche, zyklische Galoiserweiterung mit $L : K = q^n$, wobei q eine Primzahl ungleich der Charakteristik von K ist. Enthält K eine primitive q^{n-1}-te Einheitswurzel, so ist L/K nach 6.4 vollständig regulär. Das ist insbesondere der Fall, wenn K eine primitive q^n-te Einheitswurzel enthält.

- Sei $L/\mathbb{Q}$ eine endliche, zyklische Galoiserweiterung über dem Körper der rationalen Zahlen mit $L : \mathbb{Q} = q^n$, wobei q wieder eine Primzahl ist. Weil die Galoisgruppe von $L/\mathbb{Q}$ insbesondere abelsch ist, gibt es nach einem Satz von Kronecker-Weber eine natürliche Zahl m, so daß L im m-ten Kreisteilungskörper liegt, dieser heiße $\mathbb{Q}_{(m)}$. Bezeichnet ζ eine primitive q^n-te Einheitswurzel, so ist ζ^q eine primitive q^{n-1}-te Einheitswurzel. Ist m teilerfremd zu q^{n-1}, dann gilt $\mathbb{Q}_{(m)} \cap \mathbb{Q}[\zeta^q] = \mathbb{Q}$

nach [10, 12.8]. Wegen 6.4 ist $L/\mathbb{Q}$ dann vollständig regulär. Hierzu ein Beispiel:

Sei $m = 487$ und $\mathbb{Q}_{(487)}$ der 487-te Kreisteilungskörper. Weil m eine Primzahl ist, ist $\Delta := \mathrm{Gal}(\mathbb{Q}_{(487)}/\mathbb{Q}) \cong (\mathbb{Z}/487\mathbb{Z})^*$ eine zyklische Gruppe der Ordung $486 = 2 \cdot 3^5$. Also besitzt Δ einen Normalteiler der Ordnung 2, dessen zugehöriger Fixkörper L heiße. $L/\mathbb{Q}$ ist dann eine zyklische Galoiserweiterung mit $L : \mathbb{Q} = 3^5$. Ist θ eine primitive 3^4-te Einheitswurzel, so folgt $\mathbb{Q}[\theta] \cap \mathbb{Q}_{(487)} = \mathbb{Q}$, weil 3^4 und 487 zueinander teilerfremd sind. Also ist $L/\mathbb{Q}$ nach 6.4 vollständig regulär.

Sind k und m zwei teilerfremde natürliche Zahlen, so wird mit $\mathrm{ord}_k(m)$ die Ordnung von $m + k\mathbb{Z}$ in der Einheitengruppe $(\mathbb{Z}/k\mathbb{Z})^*$ bezeichnet. Für endliche Körper läßt sich dann folgendes Korollar formulieren.

Korollar 6.5 *Sei L/K eine Erweiterung endlicher Körper vom Grad q^n und $|K| = p^m$, wobei p und q zwei verschiedene Primzahlen und $n, m \in \mathbb{N}$ sind. Genau dann ist L/K vollständig regulär, wenn q kein Teiler von $\mathrm{ord}_{q^{n-1}}(p^m)$ ist.*

Beweis: Weil L und K endlich sind, ist L/K eine zyklische Galoiserweiterung. Die Charakteristik von K ist p. Da p und q teilerfremd sind, sind alle Voraussetzungen von 6.4 erfüllt, ferner ist $\mathrm{ord}_{q^{n-1}}(p^m)$ wohldefiniert.

Nach Voraussetzung ist $|K| = p^m$, außerdem ist ζ^q eine primitive q^{n-1}-te Einheitswurzel. Bekanntlich ist dann

$$K[\zeta^q] : K = \mathrm{ord}_{q^{n-1}}(p^m).$$

Weil K endlich ist, ist $K_1[\zeta^q]/K$ zyklisch mit K_1 und $K[\zeta^q]$ als Zwischenkörpern. Also ist K_1 genau dann in $K[\zeta^q]$ enthalten, wenn $K_1 : K = q$ ein Teiler von $K[\zeta^q] : K$ ist. Andrerseits ist genau dann $L \cap K[\zeta^q] = K$, wenn $K_1 \not\subseteq K[\zeta^q]$ gilt. Mit 6.4 folgt jetzt die Behauptung. □

Hierzu ein Beispiel : Seien $q := 2,\ n := 9,\ p := 257$ und $m := 1$. Dann ist $\mathrm{ord}_{2^8}(257) = 1$, weil $257 \equiv 1 \bmod 256$ ist. Also ist $\mathrm{GF}(257^{512})/\mathrm{GF}(257)$ eine vollständig reguläre Erweiterung.

Literatur

[1] E. Artin: „Galoissche Theorie," Harri Deutsch Verlag, Zürich/Frankfurt, 1973

[2] D. Blessenohl und K. Johnsen: „Eine Verschärfung des Satzes von der Normalbasis," J.Algebra 103, 141–159 (1986)

[3] D. Blessenohl: „Abelsche Erweiterungen, in denen jedes reguläre Element vollständig regulär ist," Arch.Math., Vol.54, 146–156 (1990)

[4] D. Blessenohl: Supplement zu „Eine Verschärfung des Satzes von der Normalbasis," J.Algebra 132, 154–159 (1990)

[5] N. Bourbaki: „Éléments de mathématique," Livre III, „Algèbre," Chap.5, Corps commutatifs, Paris, 1959

[6] C. C. Faith: „Extensions of normal bases and completely basic fields," Trans. Amer. Math. Soc. 85, 406–427 (1957)

[7] B. Huppert: „Endliche Gruppen I," Springer-Verlag, Berlin/Heidelberg/New York, 1967

[8] N. Jacobson: „Lectures in Abstract Algebra," Vol.III, „Theory of Fields," Van Nostrand, New York/London/Toronto/Melbourne, 1964

[9] F. Lorenz: „Einführung in die Algebra I," Bibl. Inst. Mannheim, 1987

[10] H. Lüneburg: „Galoisfelder, Kreisteilungskörper und Schieberegisterfolgen," Bibl. Inst. Mannheim, 1979

Index