Norbert Klingen

Arithmetische Ähnlichkeiten

Vorlesung (4-stdg.)

Universität zu Köln WS 1987/88

Inhaltsverzeichnis

§1 Zahlentheoretische Grundlagen

a. Ganzheitsringe

(1.1) Definition: a) Ein *algebraischer Zahlkörper* ist eine endliche Körpererweiterung K von $\mathbb{Q}$.
b) Sein *Ganzheitsbereich* Z_K besteht aus allen Elementen $a \in K$, deren Minimalpolynome $f_{a,\mathbb{Q}}$ Koeffizienten in $\mathbb{Z}$ haben.

(1.2) Satz: *Sei K ein algebraischer Zahlkörper, $a \in K$. Dann sind äquivalent:*

i) $a \in Z_K$

ii) *a ist ganz über $\mathbb{Z}$, d. h. es gibt ein normiertes(!) Polynom $f \in \mathbb{Z}[X]$ mit $f(a) = 0$.*

iii) *$\mathbb{Z}[a]$, der von a über $\mathbb{Z}$ erzeugte Unterring von K, ist ein endlich-erzeugter $\mathbb{Z}$-Modul, d. h. es gibt $a_1, \ldots, a_n$ mit*

$$\mathbb{Z}[a] = \langle a_1, \ldots, a_n \rangle_{\mathbb{Z}} = \Big\{ \sum_{i=1}^{r} n_i a_i \mid r \in \mathbb{N}, n_i \in \mathbb{Z} \Big\}.$$

iv) *Es gibt einen endlich-erzeugten $\mathbb{Z}$-Untermodul M von K mit $M \neq (0)$ und $aM \subseteq M$.*

Beweis: i) $\Rightarrow$ ii) ist klar. ii) $\Rightarrow$ iii): Es gilt $a^n = -\sum_{i=0}^{n-1} c_i a^i$ mit den Koeffizienten $c_i \in \mathbb{Z}$ $(i=0,\ldots,n-1)$ des gemäß ii) gegebenen Polynoms f. Damit ist jede $\mathbb{Z}$-Linearkombination von beliebigen Potenzen a^j $(j \in \mathbb{N})$ von a bereits als Linearkombination der a^i $(i = 0, \ldots, n-1)$ darstellbar, d. h.

$$\mathbb{Z}[a] = \langle a^i \mid i = 0, \ldots, n-1 \rangle_{\mathbb{Z}}$$

ist endlich erzeugt über $\mathbb{Z}$.
iii) $\Rightarrow$ iv) ist klar mit $M = \mathbb{Z}[a]$.
iv) $\Rightarrow$ ii): Sei $w_1, \ldots, w_n$ ein $\mathbb{Z}$-Erzeugendensystem von M. Dann existieren $m_{ij} \in \mathbb{Z}$ $(i, j = 1, \ldots, n)$ mit

$$aw_i = \sum_{j=1}^{n} m_{ij} w_j \quad \text{für alle } i.$$

Da $M \neq (0)$ ist, verschwinden nicht alle w_j, so daß $a \in K$ ein Eigenwert der Matrix $B := (m_{ij}) \in M_n(\mathbb{Z})$, also eine Nullstelle des charakteristischen Polynoms f von B ist. Da die Matrix B nur Einträge aus $\mathbb{Z}$ hat, ist gemäß Definition f ein normiertes Polynom vom Grad n mit Koeffizienten in $\mathbb{Z}$, und ii) ist bewiesen. Die noch fehlende Implikation ii) $\Rightarrow$ i) beweisen wir erst nach dem folgenden Korollar, das sich bereits aus der Äquivalenz der Aussagen ii) - iv) ergibt.

Der Beweis von Satz (1.2) zeigt, daß die Äquivalenz dieser Aussagen ii) - iv) für jeden unitären Unterring $R \subseteq K$ statt $\mathbb{Z}$ gilt. Dies werden wir im folgenden auch benutzen.

(1.3) Korollar: *Sei K ein Zahlkörper und R ein unitärer Teilring. Dann bilden die über R ganzen Elemente von K einen Ring.*

Beweis: Seien $a, b \in K$ ganz über R. Es ist zu zeigen: $a \pm b$ sind ganz über R. Da a, b ganz über R sind, sind die Ringe $R[a]$ und $R[b]$ endlich-erzeugte R-Moduln. Dann ist aber auch der Ring $R[a, b]$ als R-Modul endlich erzeugt, also ist gemäß Satz (1.2), iv) $\Rightarrow$ ii) jedes Element von $R[a, b]$ ganz über R und die Behauptung gezeigt.

Induktiv ergibt sich so für jeden Unterring R von K und $a_i \in K$:

$$\left| \begin{array}{lll} a_1, \ldots, a_n & \text{ganz über } R & \iff R[a_1, \ldots, a_n] \text{ endlich-erzeugter } R\text{-Modul} \\ & & \iff \text{Alle } \; b \in R[a_1, \ldots, a_n] \text{ sind ganz über } R. \end{array} \right.$$

Beweisschluß von Satz (1.2): ii) $\Rightarrow$ i): Sei $f \in \mathbb{Z}[X]$ gemäß ii) und $f_{a,\mathbb{Q}}$ das Minimalpolynom von a über $\mathbb{Q}$. Dann ist $f_{a,\mathbb{Q}}$ ein Teiler von f in $\mathbb{Q}[X]$, also ist jede Nullstelle von $f_{a,\mathbb{Q}}$ im Zerfällungskörper von $f_{a,\mathbb{Q}}$ auch Nullstelle von f und daher ganz. Die Koeffizienten von $f_{a,\mathbb{Q}}$ berechnen sich als die elementar-symmetrischen Polynome in den Wurzeln von $f_{a,\mathbb{Q}}$, sind also selbst ganz über $\mathbb{Z}$ (Korollar (1.3),a)). Da die Koeffizienten von $f_{a,\mathbb{Q}}$ natürlich in $\mathbb{Q}$ liegen, genügt es zu zeigen:

(1.4) Bemerkung: $Z_{\mathbb{Q}} = \mathbb{Z}$, m.a.W. die über $\mathbb{Z}$ ganzen Elemente von $\mathbb{Q}$ liegen bereits in $\mathbb{Z}$. Man sagt auch: $\mathbb{Z}$ ist (in seinem Quotientenkörper) *ganz-abgeschlossen.*

Dies folgert man aus der ZPE-Eigenschaft von $\mathbb{Z}$; übung.

(1.5) Korollar: *a) Z_K ist ein Ring.*
b) Ist $K|k$ eine Zahlkörpererweiterung, so gilt:

$$Z_K = \{\, a \in K \mid a \text{ ganz über } Z_k \,\}.$$

Beweis: a) ist in (1.3) bewiesen worden.
Ad b): Diese Behauptung beruht auf der Transitivität der Ganzheit:

$$a \text{ ganz über } R \quad \text{und} \quad \text{alle } b \in R \text{ ganz über } R_0 \quad \Longrightarrow \; a \text{ ganz über } R_0.$$

Ist a ganz über R, so auch über dem Unterring $S := R_0[c_0, \ldots, c_{s-1}]$, erzeugt von den Koeffizienten $c_i \in R$ einer 'ganzen Gleichung' für a über R. Gemäß den Bemerkungen im Beweis von (1.3) ist S ein endlich-erzeugter R_0-Modul:

$$S = \langle r_1, \ldots, r_m \rangle_{R_0},$$

und gemäß Satz (1.2) ist $S[a]$ ein endlich-erzeugter S-Modul:

$$S[a] = \langle b_1, \ldots, b_n \rangle_S.$$

Dann ist natürlich $S[a]$ endlich erzeugt über R_0, nämlich

$$S[a] = \langle r_i b_j \mid i = 1, \ldots, m\,,\, j = 1, \ldots, n \rangle_{R_0}\,,$$

und folglich a ganz über R_0.

(1.6) Satz: *Sei K ein algebraischer Zahlkörper. Dann ist der Ganzheitsring Z_K ein freier $\mathbb{Z}$-Modul vom Rang $n = (K\!:\!\mathbb{Q})$, d. h. es existieren $a_1, \ldots, a_n \in Z_K$, so daß sich jedes Element $b \in Z_K$ eindeutig als $\mathbb{Z}$-Linearkombination der a_i darstellen läßt. Solch eine $\mathbb{Z}$-Basis von Z_K nennt man auch eine* **Ganzheitsbasis** *von K.*

Beweis: 1) Argumentation auf der Basis des Elementarteilersatzes bzw. des Hauptsatzes über endlich-erzeugte abelsche Gruppen:
Daß der Rang von Z_K höchstens $n = \dim_{\mathbb{Q}} K$ sein kann, ist klar, denn eine $\mathbb{Z}$-Basis von Z_K ist natürlich $\mathbb{Q}$-linear-unabhängig. Andererseits kann der Rang auch nicht kleiner sein, da Z_K eine $\mathbb{Q}$-Basis von K enthält. Dies folgt aus

$(*)$ Jedes Element von $a \in K$ ist darstellbar als $\frac{c}{m}$ mit $c \in Z_K$ und $m \in \mathbb{N}_+$.

Wähle dazu g als Minimalpolynom von a über $\mathbb{Q}$, und m als Hauptnenner der Koeffizienten von g. Durch Multiplikation der Gleichung $0 = g(a)$ mit m^d, $d = \deg g$, erhält man eine ganze Gleichung für $ma =: c$.

Nun ist Z_K als Unterring von K ein torsionsfreier $\mathbb{Z}$-Modul, d. h. eine abelsche Gruppe ohne Elemente endlicher Ordnung. Ist nun Z_K endlich erzeugt, so folgt aus dem Hauptsatz über endlich-erzeugte abelsche Gruppen, daß Z_K $\mathbb{Z}$-frei ist. (Damit ist Z_K natürlich über jedem Unterring R als Modul endlich erzeugt, aber i. a. nicht frei!) Man konstruiert nun einen endlich

erzeugten $\mathbb{Z}$-Modul, der Z_K enthält (siehe unten 2)). Dann ist Z_K selbst auch endlich erzeugt. Dieser Schluß gilt allgemein für Noethersche Ringe R statt $\mathbb{Z}$ (siehe etwa S.Lang: Algebra, p.143f). Man kann es für $\mathbb{Z}$ aber ebenfalls aus dem Elementarteilersatz entnehmen, auf dem der Hauptsatz über endlich erzeugte abelsche Gruppen beruht: Untermoduln endlich erzeugter $\mathbb{Z}$-Moduln sind Quotienten von Untermoduln in freien $\mathbb{Z}$-Moduln endlichen Ranges, die gemäß des Elementarteilersatzes selbst endlich erzeugt – und frei – sind.

Die Konstruktion eines endlich-erzeugten $\mathbb{Z}$-Modul, der Z_K enthält, geschieht mit Hilfe der Spur.
2) Die Spurform:
Ist $K|k$ eine Zahlkörpererweiterung, so definiert man für $a \in K$ die **Spur** durch

$$\mathrm{Sp}_{K|k}(a) := \sum_{\sigma: K \to \tilde{K}} \sigma(a),$$

wobei σ alle k-Monomorphismen $\sigma\colon K \to \tilde{K}$ von K in eine algebraisch-abgeschlossene Hülle $\tilde{K}$ von K durchläuft. [Übung: Die Spur ganzer Elemente ist ganz.]
Nun gilt: $\mathrm{Sp}_{K|k}$ ist ein k-Vektorraumhomomorphismus $\neq 0$ mit Werten in k.
Begründung: Wegen $\mathrm{char}\, k = 0$ sind alle algebraischen Erweiterungen von k separabel, so daß man mittels Galoistheorie folgern kann, daß die Werte der Spurabbildung tatsächlich im Grundkörper k liegen, da sie unter allen Galoisautomorphismen invariant sind. (Man berechnet übrigens die Spur von a als zweithöchsten Koeffizienten des Minimalpolynoms von a über k multipliziert mit $-(K\colon k(a))$.) Nun ist die Spur der 1 gerade der Körpergrad $(K\colon k)$, also verschieden von 0, wieder wegen $\mathrm{char}\, k = 0$. Damit erhält man

$(**)$ eine symmetrische, nicht-entartete k-Bilinearform $\langle\ ,\ \rangle$ auf K durch die Festsetzung:

$$\langle a, b\rangle := \mathrm{Sp}_{K|k}(a \cdot b)\,.$$

Die k-Bilinearität ist klar. Sei nun $a \perp K$ bzgl. $\langle\ ,\ \rangle$, d. h. $\langle a, b\rangle = 0$ für alle $b \in K$. Wäre $a \neq 0$, so wäre

$$0 = \langle a, a^{-1}b\rangle = \mathrm{Sp}_{K|k}(b) \quad \text{für alle } b \in K,$$

im Widerspruch zu $\mathrm{Sp}_{K|k} \neq 0$. Also ist $a = 0$ und $\langle\ ,\ \rangle$ nicht ausgeartet. Dies bedeutet, daß der k-Vektorraumhomomorphismus

$$f : K \to K^*\,, a \mapsto \langle \ldots, a\rangle$$

von K in seinen Dualraum $K^* := \mathrm{Hom}_k(K, k)$ injektiv, also wegen der Dimensionsgleichheit ein Isomorphismus ist. Darauf beruht die aus der linearen Algebra wohlvertraute Konstruktion der Dualbasis zu einer gegebenen Basis, die wir nun benutzen wollen für den Beweis, daß Z_K in einem endlich erzeugten $\mathbb{Z}$-Modul enthalten ist:

Sei $a_1, \ldots, a_n$ eine $\mathbb{Q}$-Basis von K mit $a_i \in Z_K$ (möglich nach $(*)$) und $a_1', \ldots, a_n' \in K$ die Dualbasis dazu bzgl. $\langle\ ,\ \rangle$, d. h.

$$\langle a_i, a_j'\rangle = \delta_{ij} \quad \text{(Kroneckersymbol)}.$$

Dann ist Z_K enthalten in $\overset{n}{\underset{i=1}{\oplus}} \mathbb{Z}a_i'$. Ist nämlich

$$a = \sum_{i=1}^{n} r_i a_i' \quad (r_i \in \mathbb{Q})$$

ein beliebiges Element in Z_K, so folgt

$$r_i = \langle a, a_i\rangle = \mathrm{Sp}_{K|\mathbb{Q}}(a \cdot a_i) \in \mathbb{Z},$$

weil a, a_i, und also auch die Spur ihres Produktes ganz ist. Damit ist Z_K Untermodul eines endlich erzeugten $\mathbb{Z}$-Modul.

3) Beweis von Satz (1.6) ohne explizite Verwendung des Hauptsatzes über endlich erzeugte abelsche Gruppen und zugleich Einführung des wichtigen Begriffs der Diskriminante.

Für eine $\mathbb{Q}$-Basis a_i $(i=1,\ldots,n)$ von K sei die *Diskriminante* definiert als

$$D(a_1,\ldots,a_n) := (\det(\sigma_i(a_j)))^2 = \det(\langle a_i, a_j\rangle) \in \mathbb{Q}$$

mit den verschiedenen $\mathbb{Q}$-Monomorphismen $\sigma_i : K \to \tilde{K}$ $(i=1,\ldots,n)$.

Beweis der 2. Gleichung: Sei $M = (\sigma_i(a_j))_{ij} \in M_n(K)$. Dann hat M^tM als (i,k)-ten Koeffizienten

$$\sum_{j=1}^{n} \sigma_j(a_i)\sigma_j(a_k) = \mathrm{Sp}_{K|Q}(a_i a_k) = \langle a_i, a_k\rangle$$

und die Behauptung folgt.

Die zweite Beschreibung zeigt, daß die Diskriminante in $\mathbb{Q}$ liegt.

Ist $T = (t_{ij}) \in GL_n(\mathbb{Q})$ die Übergangsmatrix von einer $\mathbb{Q}$-Basis $(a_1,\ldots,a_n)$ von K zu einer anderen Basis $(b_1 \ldots, b_n)$, d. h.

$$b_i = \sum_{j=1}^{n} t_{ij} a_j, \quad (i=1,\ldots,n),$$

so folgt unmittelbar

$$D(b_1,\ldots,b_n) = (\det T)^2 \cdot D(a_1,\ldots,a_n),$$

d. h. die Diskriminanten unterscheiden sich um das Determinantenquadrat der Übergangsmatrix T. Betrachtet man speziell ein primitives Element a für $K|\mathbb{Q}$, so bilden die Potenzen a^i $(i = 0,\ldots,n-1)$ von a eine $\mathbb{Q}$-Basis von K und man berechnet die Diskriminante $D(1,a,\ldots,a^{n-1})$ als Quadrat der Vandermonde-Determinante der $\sigma_i(a)$ $(i=1,\ldots,n)$:

$$D(1,a,\ldots,a^{n-1}) = \prod_{i<j} (\sigma_i(a) - \sigma_j(a))^2.$$

Da a die Körpererweiterung $K|k$ erzeugt, sind die $\sigma_i(a)$ verschieden und folglich ist diese, und damit jede Diskriminante einer $\mathbb{Q}$-Basis von K ungleich 0. Wir betrachten nun nur $\mathbb{Q}$-Basen $a_1,\ldots,a_n$ von K, die in Z_K liegen. Diese existieren gemäß $(*)$ und ihre Diskriminante $D(a_1,\ldots,a_n) = \det(\langle a_i, a_j\rangle)$ ist dann eine ganze Zahl $\neq 0$.

Es existiert somit unter allen $\mathbb{Q}$-Basen von K aus ganzen Elementen eine, deren Diskriminante minimalen Betrag hat. Jede solche Basis $a_1,\ldots,a_n$ bildet ein $\mathbb{Z}$-Erzeugendensystem von Z_K.

Beweis: Sei $a \in Z_K$ mit der Basisdarstellung

$$a = \sum_{i=1}^{n} q_i a_i \quad (q_i \in \mathbb{Q})$$

bezüglich der $\mathbb{Q}$-Basis a_i $(i=1,\ldots,n)$ von K. Wäre $q_1 \notin \mathbb{Z}$, also

$$q_1 = c_1 + r_1 \quad \text{mit} \quad c_1 \in \mathbb{Z}\,,\ r_1 \in \mathbb{Q}\,, 0 < r_1 < 1,$$

so betrachtet man folgende neue $\mathbb{Q}$-Basis $b_1,\ldots,b_n$ von K:

$$\begin{aligned} b_1 &:= a - c_1 a_1 = r_1 a_1 + \textstyle\sum_{i=2}^{n} q_i a_i, \\ b_i &:= a_i \qquad \text{für } i \neq 1. \end{aligned}$$

Die b_i sind ebenfalls ganz, und sie bilden eine $\mathbb{Q}$-Basis von K, da die übergangsmatrix

$$T = \begin{pmatrix} r_1 & q_2 & \ldots & q_n \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$

von der alten zur neuen Basis offenbar die Determinante $r_1 \neq 0$ hat. Damit berechnet sich die Diskriminante gerade als

$$D(b_1, \ldots, b_n) = r_1^2 \cdot D(a_1, \ldots, a_n).$$

Wegen $r_1 < 1$ steht dies im Widerspruch zur Minimalität von $|D(a_1, \ldots, a_n)|$.

Es folgt also, daß alle q_i in $\mathbb{Z}$ liegen und somit die a_i ein $\mathbb{Z}$-Erzeugendensystem von Z_K bilden. Als $\mathbb{Q}$-Basis von K sind die a_i natürlich $\mathbb{Z}$-linear-unabhängig und bilden so eine $\mathbb{Z}$-Basis von Z_K.

b. Idealtheorie

Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Hauptidealring und daher auch ZPE-Ring. Diese Eigenschaften gelten nun i. a. nicht für die Ganzheitsringe Z_K in beliebigen algebraischen Zahlkörpern. Jedoch gibt es in diesen Ringen einen Ersatz für die eindeutige Primelementzerlegung, nämlich die *eindeutige Primidealzerlegung.*

(1.7) Proposition: *Sei K ein algebraischer Zahlkörper vom Grad n über $\mathbb{Q}$, Z_K sein Ganzheitsring und $\mathfrak{a}$ ein Ideal $\neq (0)$ in Z_K. Dann gilt:*

a) $\mathfrak{a} \cap \mathbb{Z} \neq (0)$.

b) $\mathfrak{a}$ *ist ein freier $\mathbb{Z}$-Modul vom Rang n.*

c) Jedes Ideal von Z_K ist endlich erzeugt, d. h. der Ring Z_K ist Noethersch.

d) Jedes Primideal $\mathfrak{p} \neq (0)$ von Z_K ist maximal.

e) Jedes Ideal $\mathfrak{a} \neq (0)$ von Z_K enthält ein Produkt von maximalen Idealen.

Beweis: a) Sei $a \in \mathfrak{a}$, $a \neq 0$. Ist

$$f_{a,\mathbb{Q}} = \sum_{i=0}^{m} c_i X^i$$

das Minimalpolynom von a über $\mathbb{Q}$, so sind alle $c_i \in \mathbb{Z} \subseteq Z_K$, $c_0 \neq 0$ wegen der Irreduzibilität von $f_{a,\mathbb{Q}}$, und

$$c_0 = -\sum_{i=1}^{m} c_i a^i \in \mathfrak{a}.$$

b) Wähle $c \in \mathfrak{a} \cap \mathbb{Z}$ mit $c \neq 0$ gemäß a). Ist dann $a_1, \ldots, a_n \in Z_K$ eine $\mathbb{Q}$-Basis von K, so bilden die Elemente ca_i ebenfalls eine $\mathbb{Q}$-Basis von K, die außerdem in $\mathfrak{a}$ liegt. Damit enthält jedes von (0) verschiedene Ideal von Z_K eine $\mathbb{Q}$-Basis von K. Wie im Beweis von Satz (1.6) wählt man unter allen solchen Basen eine mit minimalem Betrag der Diskriminante und folgert, daß diese eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ ist.
c) Jedes Ideal $\mathfrak{a} \neq (0)$ von Z_K ist bereits als $\mathbb{Z}$-Modul endlich erzeugt.
d) Sei $\mathfrak{p} \neq (0)$ ein Primideal von Z_K und $\mathfrak{p}'$ ein maximales Ideal von Z_K mit $\mathfrak{p} \subseteq \mathfrak{p}'$. Zu zeigen: $\mathfrak{p}' \subseteq \mathfrak{p}$.
Es ist $\mathfrak{p} \cap \mathbb{Z}$ ein Primideal $\neq (0)$ von $\mathbb{Z}$, also $\mathfrak{p} \cap \mathbb{Z} = p \cdot \mathbb{Z}$ maximales Ideal von $\mathbb{Z}$ (p eine Primzahl). Wegen $\mathfrak{p}' \cap \mathbb{Z} \supseteq \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ ist dann auch $\mathfrak{p}' \cap \mathbb{Z} = p\mathbb{Z}$. (Da $\mathfrak{p}'$ die 1 nicht enthält, ist auch $\mathfrak{p}' \cap \mathbb{Z}$ ein echtes Ideal von Z.) Sei nun $a \in \mathfrak{p}'$ beliebig und

$$0 = c_0 + a \sum_{i=1}^{m} c_i a^{i-1}$$

die minimale Gleichung für a über $\mathbb{Q}$. Deren Koeffizienten sind ganz, da a ganz ist. Das Ideal $\mathfrak{p}'$ enthält a, also auch $c_0 = -a \sum_{i=1}^{m} c_i a^{i-1}$. Dann folgt aber

$$-a \sum_{i=1}^{m} c_i a^{i-1} = c_0 \in \mathfrak{p}' \cap \mathbb{Z} = \mathfrak{p} \cap \mathbb{Z} \subseteq \mathfrak{p}.$$

Wäre nun a nicht in $\mathfrak{p}$, so folgte aus der Primidealeigenschaft von $\mathfrak{p}$

$$\sum_{i=1}^{m} c_i a^{i-1} \in \mathfrak{p}.$$

Induktiv schließt man nun weiter, daß alle c_i zu $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ gehören. Aber $c_m = 1$, ein Widerspruch. Folglich gehört jedes $a \in \mathfrak{p}'$ auch zu $\mathfrak{p}$, d. h. $\mathfrak{p} = \mathfrak{p}'$, und $\mathfrak{p}$ ist maximal.
e) Da Z_K Noethersch ist, besitzt jede nicht-leere Menge von Idealen von Z_K ein maximales Element (Lemma von Zorn; siehe S.Lang: Algebra, l.c.). Gälte also die Behauptung e) nicht, so gäbe es ein Ideal $\mathfrak{a} \neq (0)$ maximal mit der Eigenschaft:

$$\mathfrak{a} \text{ enthält kein Produkt von Primidealen} \neq (0)\,.$$

Insbesondere ist $\mathfrak{a}$ dann selbst kein Primideal, so daß $b, c \in Z_K$ existieren mit

$$bc \in \mathfrak{a}, \quad \text{aber} \quad b, c \notin \mathfrak{a}\,.$$

Damit sind die Ideale $\mathfrak{b} = \mathfrak{a} + b \cdot Z_K$ und $\mathfrak{c} = \mathfrak{a} + c \cdot Z_K$ echte Oberideale von $\mathfrak{a}$ und enthalten aufgrund der Maximalität von $\mathfrak{a}$ jeweils Produkte von maximalen Idealen. Dann enthält natürlich auch $\mathfrak{b} \cdot \mathfrak{c}$ ein Produkt von maximalen Idealen im Widerspruch zu $\mathfrak{b} \cdot \mathfrak{c} \subseteq \mathfrak{a}$.

(1.8) Definition/Bemerkung: Sei K ein Zahlkörper.

a) Ein *gebrochenes Ideal* von K ist ein Z_K-Untermodul $\mathfrak{a} \neq (0)$ von K, für den ein $c \in K^\times$ existiert mit $c\mathfrak{a} \subseteq Z_K$. $c\mathfrak{a}$ ist dann ein gewöhnliches Ideal in Z_K (ein *ganzes* Ideal von K) und also $\mathfrak{a}$ von der Form

$$\mathfrak{a} = \frac{1}{c} \cdot \mathfrak{b} \quad \text{mit einem Ideal } \mathfrak{b} \lhd Z_K\,.$$

Gebrochene Ideale sind also gemäß (1.7), b) freie $\mathbb{Z}$-Moduln vom Rang $n = (K\colon \mathbb{Q})$; wegen $(*)$ (siehe im Beweis von (1.6)) genügt dann bereits eine natürliche Zahl $c \in \mathbb{N}_+$, um ein gebrochenes Ideal $\mathfrak{a}$ nach Z_K zu 'transportieren'.

b) Gebrochene Ideale kann man multiplizieren, indem man für zwei Z_K-Untermoduln $\mathfrak{a}$, $\mathfrak{a}'$ von K das *Idealprodukt* $\mathfrak{a} \cdot \mathfrak{a}'$ definiert als den von allen*Produkten* aa' ($a \in \mathfrak{a}$, $a' \in \mathfrak{a}'$) *erzeugten* Z_K-Untermodul von K, und bemerkt, daß $\mathfrak{a} \cdot \mathfrak{a}'$ wieder ein gebrochenes Ideal ist.

c) Jedes $a \in K^\times$ bestimmt ein gebrochenes Ideal $aZ_K = \langle a \rangle$, das sog. gebrochene *Hauptideal* zu a. (Man beachte dazu, daß wegen $(*)$ K der Quotientenkörper von Z_K ist.) Die Zuordnung $a \mapsto aZ_K$ ist ein Homomorphismus von der Multiplikationsgruppe $K^\times$ von K in die Halbgruppe $\mathcal{I}_K$ der gebrochenen Ideale von K, deren Bild die Gruppe $\mathcal{H}_K$ der gebrochenen Hauptideale von K ist. Die Halbgruppe $\mathcal{I}_K$ hat ein neutrales Element, nämlich $\langle 1 \rangle = Z_K$.

d) Ein gebrochenes Ideal $\mathfrak{a}$ heißt *invertierbar,* wenn es in $\mathcal{I}_K$ ein Inverses besitzt.

Ziel der nun folgenden Überlegungen ist der Beweis der Tatsache, daß alle gebrochenen Ideale invertierbar sind, d. h. daß $\mathcal{I}_K$ eine Gruppe ist. Diese Eigenschaft charakterisiert den Ring Z_K als sog. *Dedekindring.* Man muß also für ein gebrochenes Ideal $\mathfrak{a}$ von K ein Inverses finden, d. h. ein gebrochenes Ideal $\mathfrak{a}^*$ mit

$$\mathfrak{a} \cdot \mathfrak{a}^* = Z_K.$$

Es gibt dafür nur einen Kandidaten, nämlich den sog. em Transporteur

$$[Z_K\colon \mathfrak{a}] := \{\, x \in K \mid x \cdot \mathfrak{a} \subseteq Z_K \,\}\,.$$

Sei nämlich $\mathfrak{a}^*$ ein solches Inverses. Offensichtlich ist dann $\mathfrak{a}^*$ in $[Z_K\colon \mathfrak{a}]$ enthalten. Umgekehrt folgt aus $x \cdot \mathfrak{a} \subseteq Z_K$ durch Multiplikation mit $\mathfrak{a}^*$ sofort $x \cdot Z_K \subseteq \mathfrak{a}^*$. überdies ist dieser 'Kandidat'

auch ein gebrochenes Ideal, denn allgemein ist für zwei gebrochene Ideale $\mathfrak{a}$, $\mathfrak{b}$ der Transporteur $[\mathfrak{b}\colon\mathfrak{a}]$ wieder ein gebrochenes Ideal: Offenbar ist nämlich $[\mathfrak{b}\colon\mathfrak{a}]$ ein Z_K-Modul und aus

$$c\cdot\mathfrak{a}\subseteq Z_K,\quad d\cdot\mathfrak{b}\subseteq Z_K,\quad a\in\mathfrak{a},\ b\in\mathfrak{b}\quad\text{für geeignete } a,b,c,d\in K^\times$$

folgt

$$0\neq b\cdot c\in[\mathfrak{b}\colon\mathfrak{a}]\quad\text{und}\quad da\cdot[\mathfrak{b}\colon\mathfrak{a}]\subseteq Z_K\quad\text{mit } da\neq 0\,.$$

(1.9) Proposition: *Sei K ein algebraischer Zahlkörper mit Ganzheitsring Z_K. Dann gilt: Jedes maximale Ideal $\mathfrak{p}$ von Z_K ist invertierbar; das Inverse $\mathfrak{p}^{-1}$ ist der Transporteur $[Z_K\colon\mathfrak{p}]$.*

Beweis: Sei $\mathfrak{p}$ ein maximales Ideal in Z_K und $\mathfrak{p}'$ der oben definierte Transporteur $[Z_K\colon\mathfrak{p}]$. Dann gilt per definitionem $\mathfrak{p}\cdot\mathfrak{p}'\subseteq Z_K$ und wegen $\mathfrak{p}\subseteq Z_K$, also $1\in\mathfrak{p}'$, folgt

$$\mathfrak{p}\subseteq\mathfrak{p}\mathfrak{p}'\subseteq Z_K.$$

Da $\mathfrak{p}$ maximal ist, muß entweder $\mathfrak{p}=\mathfrak{p}\mathfrak{p}'$ oder $\mathfrak{p}\mathfrak{p}'=Z_K$ gelten.
Annahme: $\mathfrak{p}=\mathfrak{p}\mathfrak{p}'$.
Dann gilt für jedes $c\in\mathfrak{p}'$: $\quad c\cdot\mathfrak{p}\subseteq\mathfrak{p}$.
Da $\mathfrak{p}$ ein endlich erzeugter $\mathbb{Z}$-Modul ist, muß c gemäß Satz (1.2) zu Z_K gehören, d. h. $\mathfrak{p}'\subseteq Z_K$. Wegen $\mathfrak{p}\subseteq Z_K$ gilt $\mathfrak{p}'\supseteq Z_K$, und damit $\mathfrak{p}'=Z_K$. Dies führen wir nun zum Widerspruch, und es folgt dann $\mathfrak{p}\cdot\mathfrak{p}'=Z_K$, die Behauptung.

Sei $a\in\mathfrak{p}$ und (gemäß (1.7), e)) $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ maximale Ideale von Z_K mit

$$\mathfrak{p}_1\cdot\ldots\cdot\mathfrak{p}_r\subseteq a\cdot Z_K\subseteq\mathfrak{p}\,.$$

O.E. sei r minimal gewählt. Es ist $r\geq 1$, da sonst $Z_K\subseteq a\cdot Z_K\subseteq\mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist, muß es eines der Ideale $\mathfrak{p}_i$ umfassen, und dann wegen der Maximalität der $\mathfrak{p}_i$ mit diesem übereinstimmen. Sei o.E. $\mathfrak{p}_1=\mathfrak{p}$. Wegen der Minimalität von r gilt

$$\mathfrak{p}_2\cdot\ldots\cdot\mathfrak{p}_r\not\subseteq a\cdot Z_K\,.$$

Wählt man nun

$$b\in\mathfrak{p}_2\cdot\ldots\cdot\mathfrak{p}_r,\quad b\notin a\cdot Z_K\,,$$

so ist

$$b\cdot\mathfrak{p}=b\cdot\mathfrak{p}_1\subseteq\mathfrak{p}_1\cdot\mathfrak{p}_2\cdot\ldots\cdot\mathfrak{p}_r\subseteq a\cdot Z_K\,,$$

und damit $ba^{-1}\in\mathfrak{p}'\setminus Z_K$, im Widerspruch zu $\mathfrak{p}'\subseteq Z_K$.

(1.10) Satz: *Sei K ein algebraischer Zahlkörper mit Ganzheitsring Z_K. Dann gilt:*

a) *Die gebrochenen Ideale von K bilden eine Gruppe $\mathcal{I}_K$.*

b) *Jedes gebrochene Ideal $\mathfrak{a}$ von K ist eindeutig darstellbar als Potenzprodukt von maximalen Idealen von Z_K:*

$$\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^{w_{\mathfrak{p}}(\mathfrak{a})}$$

mit eindeutig bestimmten $w_{\mathfrak{p}}(\mathfrak{a})\in\mathbb{Z}$, $w_{\mathfrak{p}}(\mathfrak{a})=0$ für fast alle $\mathfrak{p}$.

c) *Ein solches Potenzprodukt ist genau dann ein ganzes Ideal, wenn alle Exponenten ≥ 0 sind.*

Beweis: a) Es genügt b) zu beweisen, da nach (1.9) alle maximalen Ideale invertierbar sind. b) Es genügt die Existenz einer solchen Darstellung zu beweisen, da die Eindeutigkeit dann wieder aus (1.9) folgt:

$$\mathfrak{p}_1\cdot\ldots\cdot\mathfrak{p}_r=\mathfrak{q}_1\cdot\ldots\cdot\mathfrak{q}_s\implies\mathfrak{p}_1\supseteq\mathfrak{q}_i\implies\mathfrak{p}_1=\mathfrak{q}_i.$$

Gemäß (1.9) kann man nun kürzen und dann induktiv weiterschließen.
Man kann weiter o.E. annehmen, daß $\mathfrak{a}$ ein ganzes Ideal ist, denn im allgemeinen Fall wählt man zu $\mathfrak{a}$ ein $c \in Z_K$ mit $c \cdot \mathfrak{a} \subseteq Z_K$ und leitet aus Produktdarstellungen für $c \cdot Z_K$ und $c \cdot \mathfrak{a}$ die gewünschte Produktdarstellung für $\mathfrak{a} = (c\mathfrak{a}) \cdot (cZ_K)^{-1}$ her.

Wir beweisen nun b) für ganze Ideale $\mathfrak{a}$ mit Exponenten $w_\mathfrak{p}(\mathfrak{a}) \geq 0$.
Angenommen, dies wäre falsch. Dann betrachten wir, ähnlich wie im Beweis von (1.7),e), ein ganzes Ideal $\mathfrak{a}$, das maximal ist mit der Eigenschaft

$$\mathfrak{a} \text{ ist nicht als Produkt von Primidealen darstellbar.}$$

Insbesondere ist $\mathfrak{a} \neq Z_K$ und selbst kein Primideal, also echt enthalten in einem maximalen Ideal $\mathfrak{p}$: $\mathfrak{a} \subsetneq \mathfrak{p}$. Wegen der Invertierbarkeit von $\mathfrak{p}$ folgt $\mathfrak{a} \cdot \mathfrak{p}^{-1} \subsetneq Z_K$. Wäre nun $\mathfrak{a} = \mathfrak{a} \cdot \mathfrak{p}^{-1}$, so wäre wieder jedes Element von $\mathfrak{p}^{-1}$ ganz (siehe Satz (1.2), $\mathfrak{a}$ ist ein endlich erzeugter $\mathbb{Z}$-Modul, invariant unter allen $c \in \mathfrak{p}^{-1}$). Damit ergäbe sich der Widerspruch $\mathfrak{p}^{-1} \subseteq Z_K$. Also muß $\mathfrak{a}$ echt in $\mathfrak{a} \cdot \mathfrak{p}^{-1}$ enthalten sein. Aufgrund der Maximalität von $\mathfrak{a}$ ist $\mathfrak{a} \cdot \mathfrak{p}^{-1}$ nun als Produkt von maximalen Idealen darstellbar, dann aber auch $\mathfrak{a} = (\mathfrak{a}\mathfrak{p}^{-1}) \cdot \mathfrak{p}$. Es kann also kein solches $\mathfrak{a}$ geben, d. h. jedes ganze Ideal ist Produkt von maximalen Idealen.
c) Sind alle Exponenten ≥ 0, so ist das Potenzprodukt natürlich ein ganzes Ideal. Ist umgekehrt ein Potenzprodukt $\mathfrak{a}$ mit den Exponenten $m_\mathfrak{p} \in \mathbb{Z}$ vorgegeben und ist $\mathfrak{a}$ ganz, so besitzt $\mathfrak{a}$ nach dem Beweis von b) eine Darstellung als Potenzprodukt mit nicht-negativen Exponenten $w_\mathfrak{p}(\mathfrak{a})$. Aufgrund der Eindeutigkeit der Darstellung müssen also die Exponenten $m_\mathfrak{p} \geq 0$ sein.

Anmerkung: Die Faktorgruppe $\mathcal{C}_K = \mathcal{I}_K/\mathcal{H}_K$ der gebrochenen Ideale nach den gebrochenen Hauptidealen nennt man die *Klassengruppe* von K. Einer der zentralen Endlichkeitssätze der algebraischen Zahlentheorie besagt, daß die Klassengruppe endlich ist; ihre Ordnung ist die sog. *Klassenzahl* h_K von K.

Wie für Elemente in einem Ring definiert man auch für ganze Ideale den Begriff der Teilbarkeit:

$$\mathfrak{a} \text{ teilt } \mathfrak{b} \text{ (in Zeichen } \mathfrak{a}|\mathfrak{b}) \iff \text{es gibt ein ganzes Ideal } \mathfrak{c} \text{ mit } \mathfrak{a} \cdot \mathfrak{c} = \mathfrak{b}.$$

Für Zahlringe Z_K kann man dies aufgrund von Satz (1.10) wie folgt umformulieren:

$$\mathfrak{a} \text{ teilt } \mathfrak{b} \iff \mathfrak{b} \cdot \mathfrak{a}^{-1} \text{ ist ganz} \iff \mathfrak{b} \cdot \mathfrak{a}^{-1} \subseteq Z_K \iff \mathfrak{b} \subseteq \mathfrak{a}.$$

Dies hat nun zur Folge, daß für Ideale $\mathfrak{a}, \mathfrak{b}$ in $R = Z_K$ (de facto in beliebigen Dedekindringen R) gilt:

$$\mathfrak{a}, \mathfrak{b} \text{ teilerfremd} \iff \mathfrak{a}, \mathfrak{b} \text{ coprim} :\iff \mathfrak{a} + \mathfrak{b} = R$$
$$\mathrm{ggT}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b} \quad \text{und} \quad \mathrm{kgV}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$$

ggT und kgV lassen sich natürlich aus der Primidealzerlegung unmittelbar ablesen.

Schließlich wird der bekannte chinesische Restsatz, der in beliebigen Ringen (kommutativ, unitär) die Lösbarkeit simultaner Kongruenzen sichert, wenn die Moduln paarweise coprim sind (siehe S. Lang, Algebra, p. 63 f.), für beliebige teilerfremde Moduln anwendbar, also z. B. für Potenzen verschiedener Primideale. Dies wollen wir nun benutzen zum Beweis des folgenden

(1.11) Satz: *Sei $R = Z_K$ Ganzheitsring[1] eines algebraischen Zahlkörpers K. Dann gilt:*

a) Jedes Ideal $\mathfrak{a} \lhd R$ ist von 2 Elementen erzeugbar; genauer:

$$a \in \mathfrak{a} \setminus \{0\} \text{ beliebig} \implies \mathfrak{a} = \langle a, b \rangle_R = aR + bR \quad \text{für ein geeignetes } b \in \mathfrak{a}\,.$$

b) Jeder echte Faktorring $\bar{R} = R/\mathfrak{a}$ mit $(0) \neq \mathfrak{a} \lhd R$ ist ein Hauptidealring.

[1] Der Satz gilt allgemein für beliebige Dedekindringe.

Beweis: a) Sei

$$aR = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i} \quad (n_i \geq 1)$$

die Primzerlegung von aR im Dedekindring R. Wegen $a \in \mathfrak{a}$, also $\mathfrak{a} | aR$, hat $\mathfrak{a}$ als Primzerlegung

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{m_i} \quad \text{mit } 0 \leq m_i \leq n_i \,.$$

Wähle nun Elemente

$$b_i \in \mathfrak{p}_i^{m_i} \setminus \mathfrak{p}_i^{m_i+1}.$$

(Dies ist möglich wegen der Eindeutigkeit der Primidealzerlegung.) Nach dem chinesischen Restsatz existiert dann ein einziges Element b, das diese Eigenschaft für alle i hat (als Lösung der simultanen Kongruenzen $b \equiv b_i \bmod \mathfrak{p}_i^{m_i+1}$). Damit ergibt sich für bR folgende Primzerlegung:

$$bR = \prod_{i=1}^{r} \mathfrak{p}_i^{m_i} \cdot \prod_{j=1}^{s} \mathfrak{q}_j^{k_j}$$

mit Primidealen $\mathfrak{q}_j \neq \mathfrak{p}_i$ und $k_j \geq 1$. Man berechnet nun leicht

$$aR + bR = \mathrm{ggT}(aR, bR) = \prod \mathfrak{p}^{\min(\ldots)} = \prod_{i=1}^{r} \mathfrak{p}_i^{m_i} = \mathfrak{a} \,.$$

b) Ist $\overline{\mathfrak{b}}$ ein Ideal von $R/\mathfrak{a}$ mit vollem Urbild $\mathfrak{b}$ unter der natürlichen Abbildung $R \to R/\mathfrak{a}$, so ist $\mathfrak{b}$ ein Oberideal von $\mathfrak{a}$. Ergänzt man nun ein beliebig gewähltes Element $a \in \mathfrak{a} \setminus \{0\}$ zu einem Erzeugendensystem a, b von $\mathfrak{b}$, so wird $\overline{\mathfrak{b}}$ von $\overline{b}$ erzeugt.

c. Primzerlegung in Zahlkörpererweiterungen

Gemäß Satz (1.10) wird die Idealgruppe von $R := Z_K$ durch die Primideale $\neq (0)$ von Z_K bestimmt. Diese sind, wie schon erwähnt, genau die maximalen Ideale von Z_K. Eine erste übersicht über diese maximalen Ideale erhält man durch die Tatsache, daß $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ ist mit einer Primzahl p. Dabei ist p charakterisiert als *die* Primzahl, die in $\mathfrak{p}$ liegt. Zugleich folgt aus $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$, daß die Inklusion $\mathbb{Z} \hookrightarrow R = Z_K$ einen Körpermonomorphismus der Restklassenringe $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow R/\mathfrak{p}$ induziert, wodurch p charakterisiert ist als die Charakteristik des Restklassenkörpers von $R = Z_K$ nach dem maximalen Ideal $\mathfrak{p}$.

Nach dieser ersten groben Unterteilung aller maximalen Ideale von Z_K entsprechend dem *'darunter liegenden'* maximalen Ideal von $\mathbb{Z}$ hat man sich nun also einen Überblick über alle maximalen Ideale $\mathfrak{p}$ zu verschaffen mit $\mathfrak{p} \supseteq p\mathbb{Z}$ für eine feste Primzahl p. Nun besagt $\mathfrak{p} \supseteq p\mathbb{Z}$ nichts anderes als $\mathfrak{p} \supseteq pZ_K$ bzw. $\mathfrak{p}$ teilt pZ_K. Hier gibt nun Satz (1.10) eine erste Antwort: Das ganze Ideal pZ_K ist Potenzprodukt von maximalen Idealen von Z_K:

$$pZ_K = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p}|\,p)}$$

mit natürlichen Zahlen $e(\mathfrak{p}|\,p)$, fast alle 0.
Dabei sind die in diesem Produkt tatsächlich auftretenden Primideale (d. h. die $\mathfrak{p}$ mit $e(\mathfrak{p}|\,p) \geq 1$) genau die maximalen Ideale von Z_K *'über p'*, insbesondere gibt es nur endlich viele davon.

Für $\mathfrak{p}$ über p (in Zeichen $\mathfrak{p}|\,p$) ist $e(\mathfrak{p}|\,p)$ eine natürliche Zahl ≥ 1 und wird *Verzweigungsexponent* von $\mathfrak{p}$ über p genannt. Daneben haben wir für $\mathfrak{p}|\,p$ noch eine weitere wichtige Größe, den sog. *Restklassengrad* $f(\mathfrak{p}|\,p)$ von $\mathfrak{p}$ über p. Dieser ist wie folgt definiert:

Wegen $\mathfrak{p}|\,p$ ist der *Restklassenkörper* $\bar{K}_\mathfrak{p} := Z_K/\mathfrak{p}$ von $\mathfrak{p}$ ein Erweiterungskörper von $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ (vermöge der schon oben erwähnten natürlichen Einbettung $\mathbb{Z}/p\mathbb{Z} \hookrightarrow R/\mathfrak{p}$). Der Restklassengrad $f(\mathfrak{p}|\,p)$ ist dann der Körpergrad dieser Erweiterung:

$$f(\mathfrak{p}|\,p) = (R/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}) \in \mathbb{N}_+ \cup \{\infty\}.$$

[Wir werden sehen, daß $f(\mathfrak{p}|\,p)$ eine natürliche Zahl ist.]

Da das zugrundeliegende Primideal $p\mathbb{Z}$ bereits durch $\mathfrak{p}$ und den Grundkörper $\mathbb{Q}$ bestimmt ist: $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$, können $e(\mathfrak{p}|\,p)$ bzw. $f(\mathfrak{p}|\,p)$ auch mit $e_{K|Q}(\mathfrak{p})$ bzw. $f_{K|Q}(\mathfrak{p})$ bezeichnet werden. Schließlich lassen sich beide Größen offenbar auch über einem beliebigen Grundkörper $k \subseteq K$) definieren und werden dann entsprechend mit $e_{K|k}(\mathfrak{p})$, $f_{K|k}(\mathfrak{p})$ bezeichnet.

(1.12) Satz: *Sei $K|k$ eine Zahlkörpererweiterung und $\mathfrak{p}$ ein Primideal von k. Dann gilt die fundamentale Beziehung*

$$\sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}|\mathfrak{p}) \cdot f(\mathfrak{P}|\mathfrak{p}) = (K\colon k),$$

wobei sich die Summation über alle Primteiler $\mathfrak{P}$ von $\mathfrak{p}$ in K erstreckt.

Beweis: Es seien $S = Z_K$, $R = Z_k$ die Ganzheitsringe,

$$\mathfrak{p}S = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

die Primzerlegung von $\mathfrak{p}S$ mit $e_i \geq 1$, und $f_i := f(\mathfrak{P}_i|\mathfrak{p})$.

Der Beweis beruht auf der Berechnung der $R/\mathfrak{p}$-Dimension von $S/\mathfrak{p}S$ auf 2 verschiedene Weisen:

$$\sum_{i=1}^{r} e_i f_i \underset{(1)}{=} \dim_{R/\mathfrak{p}}(S/\mathfrak{p}S) \underset{(2)}{=} (K\colon k)\,.$$

Ad (1): Aus dem chinesischen Restsatz folgt

$$S/\mathfrak{p}S = S \Big/ \prod_{i=1}^{r} \mathfrak{P}_i^{e_i} \;\; \backsimeq \;\; \prod_{i=1}^{r} S/\mathfrak{P}_i^{e_i}.$$

Es genügt nun zu zeigen ($\mathfrak{P} := \mathfrak{P}_i$, $e := e_i$, $f := f_i$): $S/\mathfrak{P}^e$ ist ein $R/\mathfrak{p}$-Vektorraum der Dimension $e \cdot f$.
Wegen $\mathfrak{p} \subseteq \mathfrak{P}^e$ ist $S/\mathfrak{P}^e$ ein $R/\mathfrak{p}$-Vektorraum. Betrachte nun im S-Modul $S/\mathfrak{P}^e$ die Kette von Untermoduln

$$S/\mathfrak{P}^e \supset \mathfrak{P}/\mathfrak{P}^e \supset \ldots \supset \mathfrak{P}^{e-1}/\mathfrak{P}^e.$$

Diese sind als $S/\mathfrak{P}^e$-Moduln von einem Element erzeugt (Satz (1.11), b)), also auch die Quotienten

$$\mathfrak{P}^{i-1}/\mathfrak{P}^e \Big/ \mathfrak{P}^i/\mathfrak{P}^e \;\simeq\; \mathfrak{P}^{i-1}/\mathfrak{P}^i.$$

Diese Quotienten sind in natürlicher Weise $S/\mathfrak{P}$-Vektorräume, offenbar von der Dimension 1, da sie von einem Element erzeugt werden. Definitionsgemäß hat $S/\mathfrak{P}$ über $R/\mathfrak{p}$ den Körpergrad f, also hat $\mathfrak{P}^{i-1}/\mathfrak{P}^i$ über $R/\mathfrak{p}$ die Dimension f. Für den $R/\mathfrak{p}$-Vektorraum $S/\mathfrak{P}^e$ ergibt sich insgesamt die $R/\mathfrak{p}$-Dimension $e \cdot f$.

Ad (2): Dieser Teil soll hier nur für den Grundkörper $\mathbb{Q}$ bewiesen werden.
Es ist dann $\mathfrak{p} = p\mathbb{Z}$ für eine Primzahl p und $\mathfrak{p}S = pS$. über dem Grundring $\mathbb{Z}$ ist der Ganzheitsring S gemäß Satz (1.6) ein *freier* $\mathbb{Z}$-Modul vom Rang $n = (K\colon k) = (K\colon \mathbb{Q})$, also

$$S = \bigoplus_{i=1}^{n} \mathbb{Z}a_i, \qquad pS = \bigoplus_{i=1}^{n} p\mathbb{Z}a_i,$$

und folglich

$$S/pS = \bigoplus_{i=1}^{n} \mathbb{Z}/p\mathbb{Z} \cdot a_i$$

als $\mathbb{Z}/p\mathbb{Z}$-Vektorraum ebenfalls von der Dimension n.

[Für beliebigen Grundkörper k statt $\mathbb{Q}$ ist Z_k i. a. kein Hauptidealring und Z_K kein freier Z_k-Modul. Man geht dann von $R = Z_k$ über zum sogenannten *lokalen Ring* $R_{(\mathfrak{p})} = (R \setminus \mathfrak{p})^{-1}R$

und der Erweiterung $S_{(\mathfrak{p})} = (R \setminus \mathfrak{p})^{-1}S$. Der Ring $R_{(\mathfrak{p})}$ ist als diskreter Bewertungsring ein Hauptidealring und $S_{(\mathfrak{p})}$ ein freier $R_{(\mathfrak{p})}$-Modul von Rang n; man muß dann schließlich noch zeigen, daß die Beziehung (1) für $S_{(\mathfrak{p})}$, $R_{(\mathfrak{p})}$ statt S, R gültig bleibt.]

Satz (1.12) beinhaltet natürlich eine Reihe von Endlichkeitsaussagen, die hier noch einmal explizit formuliert werden sollen:
Für eine Zahlkörpererweiterung $K|k$ vom Grad n gilt:
1) Über einem Primideal $\mathfrak{p}$ von k liegen in K höchstens n Primideale $\mathfrak{P}$.
2) Restklassengrad $f(\mathfrak{P}|\mathfrak{p})$ und Verzweigungsexponent $e(\mathfrak{P}|\mathfrak{p})$ sind ebenfalls durch n beschränkt.
3) Der Restklassenkörper $\bar{K}_{\mathfrak{P}}$ eines Primideals $\mathfrak{P}$ von K ist ein endlicher Körper. Seine Mächtigkeit $\mathcal{N}(\mathfrak{P}) := (Z_K : \mathfrak{P})$, die sog. *Absolutnorm* von $\mathfrak{P}$, ist $q = p^{f(\mathfrak{P}|\,p)}$ mit der in $\mathfrak{P}$ liegenden Primzahl $p \in \mathbb{Z}$ und dem absoluten Restklassengrad $f(\mathfrak{P}|\,p) = f_{K|\mathbb{Q}}(\mathfrak{P}) \leq (K : \mathbb{Q})$.

Weitergehende Information über die *Zerlegungsdaten* eines Primideals von k in einer Zahlkörpererweiterung K, über die Anzahl der Primteiler und die entsprechenden Verzweigungsexponenten und Restklassengrade, werden wir im folgenden Paragraphen mit Hilfe der Galoisschen Theorie gewinnen.

§2 Primzerlegung und Gruppentheorie

a. Hilbertsche Theorie

Gegenstand der Hilbertschen Theorie ist die Untersuchung der Zerlegungsdaten eines Primideals $\mathfrak{p}$ eines Zahlkörpers k in einem *galoisschen* Erweiterungskörper N, insbesondere der Zusammenhang zwischen den Zerlegungsdaten und der Struktur der Galoisgruppe. Fundamental für alle nachfolgenden Überlegungen ist

(2.1) Proposition: *Sei $N|k$ eine galoissche Zahlkörpererweiterung mit Galoisgruppe $G = G(N|k)$. Es sei $\mathfrak{p}$ ein Primideal von k. Dann gilt:*
Die Gruppe G operiert in natürlicher Weise auf den Primteilern von $\mathfrak{p}$ in N, und diese Operation ist transitiv. Dies bedeutet explizit: Sind $\mathfrak{P}$ und $\mathfrak{P}'$ zwei Primideale von N über demselben Primideal $\mathfrak{p}$ von k, so existiert ein k-Automorphismus $\sigma \in G(N|k)$ mit $\sigma\mathfrak{P} = \mathfrak{P}'$.

Beweis: Der Ganzheitsring Z_N besteht aus den über Z_k ganzen Elementen von N. Jeder Galoisautomorphismus $\sigma \in G(N|k)$ führt daher Z_N in sich über, also ist für ein maximales Ideal $\mathfrak{P}$ von Z_N auch $\sigma\mathfrak{P}$ maximal. Da σ den Grundkörper k elementweise festläßt, liegen $\mathfrak{P}$ und $\sigma\mathfrak{P}$ über demselben Primideal $\mathfrak{p}$ von k. Also operiert die Galoisgruppe G auf der (endlichen) Menge

$$\{\mathfrak{P} \mid \mathfrak{P} \text{ Primideal von } N\,, \mathfrak{P} \text{ liegt über } \mathfrak{p}\}$$

aller Primteiler von $\mathfrak{p}$. Wir müssen nun zu zwei beliebigen maximalen Idealen $\mathfrak{P}$, $\mathfrak{P}'$ in dieser Menge einen Galoisautomorphismus $\sigma \in G(N|k)$ konstruieren mit $\sigma\mathfrak{P} = \mathfrak{P}'$. Annahme: Für alle $\sigma \in G$ ist $\mathfrak{P}' \neq \sigma\mathfrak{P}$. Dann gilt natürlich auch $\sigma\mathfrak{P} \neq \sigma'\mathfrak{P}'$ für alle $\sigma, \sigma' \in G$ (betrachte $\sigma'^{-1}\sigma \in G$). Nach dem chinesischen Restsatz existiert dann ein Element $a \in Z_N$, für das die simultanen Kongruenzen

$$\left.\begin{array}{l} a \equiv 0 \bmod \sigma\mathfrak{P} \\ a \equiv 1 \bmod \sigma\mathfrak{P}' \end{array}\right\} \quad \text{für alle } \sigma \in G$$

erfüllt sind und daher auch

$$\left.\begin{array}{l} \sigma^{-1}a \equiv 0 \bmod \mathfrak{P} \\ \sigma^{-1}a \equiv 1 \bmod \mathfrak{P}' \end{array}\right\} \quad \text{für alle} sigma \in G$$

gilt. Betrachtet man nun die *Norm*

$$\mathcal{N}_{N|k}(a) := \prod_{\sigma \in G} \sigma(a)\,,$$

so folgt:

$$\mathcal{N}_{N|k}(a) \equiv \begin{cases} 0 \mod \mathfrak{P}, \\ 1 \mod \mathfrak{P}'. \end{cases}$$

Da $N|k$ galoissch ist, besteht G aus allen k-Monomorphismen von N in eine algebraisch abgeschlossene Hülle $\tilde{N}$ von N, so daß die Norm das multiplikative Analogon der Spur ist. Wie diese liegt dann natürlich auch die Norm eines Elementes $a \in Z_N$ in Z_k, also folgt

$$\mathcal{N}_{N|k}(a) \begin{cases} \in \mathfrak{P} \cap Z_k, \\ \notin \mathfrak{P}' \cap Z_k, \end{cases}$$

im Widerspruch zu $\mathfrak{P} \cap Z_k = \mathfrak{p} = \mathfrak{P}' \cap Z_k$.

Bevor wir nun eine Reihe wichtiger Folgerungen ziehen, definieren wir für eine Galoiserweiterung $N|k$ von Zahlkörpern und ein maximales Ideal $\mathfrak{P}$ von N die *Zerlegungsgruppe* $\mathcal{Z}(\mathfrak{P}|\mathfrak{p}) = \mathcal{Z}_{N|k}(\mathfrak{P})$ von $\mathfrak{P}$ über k als die Fixgruppe von $\mathfrak{P}$ in G, d.h.

$$\mathcal{Z}_{N|k}(\mathfrak{P}) := \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Mit $r_{N|k}(\mathfrak{p})$ sei die Zahl der Primteiler von $\mathfrak{p}$ in N bezeichnet. Dann gilt folgendes

(2.2) Korollar: *Sei $N|k$ eine galoissche Erweiterung von Zahlkörpern und $\mathfrak{p}$ ein Primideal von k. Dann gilt:*

a) *Die Verzweigungsexponenten $e(\mathfrak{P}|\mathfrak{p})$ der verschiedenen Primteiler $\mathfrak{P}$ von $\mathfrak{p}$ in N stimmen überein; dasselbe gilt für die Restklassengrade $f(\mathfrak{P}|\mathfrak{p})$. Sie können deshalb auch als $e_{N|k}(\mathfrak{p})$ bzw. $f_{N|k}(\mathfrak{p})$ bezeichnet werden.*

b) *Es gilt*
$$r_{N|k}(\mathfrak{p}) \cdot e_{N|k}(\mathfrak{p}) \cdot f_{N|k}(\mathfrak{p}) = (N\colon k).$$

c) *Die Zerlegungsgruppen $\mathcal{Z}(\mathfrak{P}|\mathfrak{p})$ zu verschiedenen Primteilern $\mathfrak{P}$ von $\mathfrak{p}$ sind untereinander konjugiert in G; ihre Ordnung ist $e_{N|k}(\mathfrak{p}) \cdot f_{N|k}(\mathfrak{p})$, ihr Index in G ist gerade die Anzahl $r_{N|k}(\mathfrak{p})$ der Primteiler von $\mathfrak{p}$ in N.*

d) *Ist L der Fixkörper der Zerlegungsgruppe $\mathcal{Z}_{N|k}(\mathfrak{P})$ von $\mathfrak{P}$ in N, der sog.* **Zerlegungskörper** *von $\mathfrak{P}$ über k, und ist $\mathfrak{P}_L := \mathfrak{P} \cap L$ das unter $\mathfrak{P}$ liegende Primideal von L, so gilt:*
$$e(\mathfrak{P}_L|\mathfrak{p}) = f(\mathfrak{P}_L|\mathfrak{p}) = 1,$$
insbesondere stimmen also die Restklassenkörper $\bar{L}_{\mathfrak{P}_L} = \bar{k}_{\mathfrak{p}}$ überein.

Beweis: a) Da jedes $\sigma \in G$ den Grundkörper k und somit auch $\mathfrak{p}$ festläßt, folgt mit $S := Z_N$

$$\mathfrak{p}S = \sigma(\mathfrak{p}S) = \prod_{\mathfrak{P}|\mathfrak{p}} (\sigma\mathfrak{P})^{e(\mathfrak{P}|\mathfrak{p})},$$

und wegen der Eindeutigkeit der Primidealzerlegung in S dann

$$e(\sigma\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}).$$

Für den Restklassengrad f beachtet man, daß ein Galoisautomorphismus σ mit $\sigma\mathfrak{P} = \mathfrak{P}'$ in natürlicher Weise einen $Z_k/\mathfrak{p}$-Isomorphismus

$$\bar{\sigma} : Z_N/\mathfrak{P} \xrightarrow{\sim} Z_N/\mathfrak{P}'$$

induziert, so daß die Restklassengrade $f(\sigma\mathfrak{P}|\mathfrak{p})$ und $f(\mathfrak{P}|\mathfrak{p})$ übereinstimmen. Wegen (2.1) ist damit a) bewiesen.
b) folgt wegen a) aus Satz (1.12).

Ad c): Konjugiertheit und Indexaussage sind klar, da bei einer transitiven Gruppenoperation die Fixgruppen stets konjugiert sind und ihr Index gerade die Bahnlänge ist. Explizit:
1) $\mathrm{Fix}_G(\sigma\mathfrak{P}) = \sigma \cdot \mathrm{Fix}_G(\mathfrak{P}) \cdot \sigma^{-1}$ für $\sigma \in G$.
2) Die natürliche Abbildung

$$G \to \{\mathfrak{P}' \mid \mathfrak{P}' \text{ Primideal von } N \text{ über } \mathfrak{p}\},\ \sigma \mapsto \sigma\mathfrak{P}$$

($\mathfrak{P}$ ein festes Primideal über $\mathfrak{p}$ in N) ist nach (2.1) surjektiv und induziert so eine Bijektion zwischen den Rechtsnebenklassen σH der Zerlegungsgruppe $H = \mathcal{Z}(\mathfrak{P}|\mathfrak{p})$ und den Primteilern von $\mathfrak{p}$ in N.

Der Rest von c) folgt aus b), da die Ordnung der Galoisgruppe ja gerade der Körpergrad $(N\colon k)$ ist.

d) Offenbar gilt gemäß Definition der Zerlegungsgruppe

$$\mathcal{Z}_{N|L}(\mathfrak{P}) \subseteq \mathcal{Z}_{N|k}(\mathfrak{P})\,,$$

und nach Definition von L die umgekehrte Inklusion, also die Gleichheit. Nach c) bedeutet dies:

$$\begin{aligned} e_{N|L}(\mathfrak{P}) \cdot f_{N|L}(\mathfrak{P}) &= e_{N|k}(\mathfrak{P}) \cdot f_{N|k}(\mathfrak{P}) \\ &= e_{L|k}(\mathfrak{P}_L) e_{N|L}(\mathfrak{P}) \cdot f_{L|k}(\mathfrak{P}_L) f_{N|L}(\mathfrak{P}) \end{aligned}$$

Da alle Faktoren natürliche Zahlen sind, folgt durch Kürzen die Behauptung.

Im folgenden soll nun die Struktur der Zerlegungsgruppe und der Zusammenhang mit den Größen e und f noch ein wenig genauer aufgeklärt werden.

(2.3) Satz: *Sei $N|k$ eine galoissche Zahlkörpererweiterung, $\mathfrak{P}$ ein Primideal von N mit Restklassenkörper $\bar{N} := \bar{N}_{\mathfrak{P}}$. $\bar{k} := \bar{k}_{\mathfrak{p}}$ sei der Restklassenkörper des darunter liegenden Primideals $\mathfrak{p} = \mathfrak{P} \cap k$ von k. Dann gilt:*

*a) Die Restklassenabbildung induziert einen Gruppen***epi***morphismus*

$$\mathcal{Z}_{N|k}(\mathfrak{P}) \twoheadrightarrow G(\bar{N}|\bar{k}),\ \sigma \mapsto \bar{\sigma}$$

der Zerlegungsgruppe von $\mathfrak{P}$ auf die Galoisgruppe der Restklassenkörpererweiterung $\bar{N}|\bar{k}$. Letztere ist zyklisch von der Ordnung $f_{N|k}(\mathfrak{P})$.

b) Der Kern dieses Epimorphismus ist die Trägheitsgruppe

$$\mathcal{T}_{N|k}(\mathfrak{P}) := \{\sigma \in G(N|k) \mid \sigma(a) \equiv a \bmod \mathfrak{P} \text{ für alle } a \in Z_N\}$$

von $\mathfrak{P}$. Diese hat die Ordnung $e_{N|k}(\mathfrak{P})$; sie ist ein Normalteiler in der Zerlegungsgruppe $\mathcal{Z}_{N|k}(\mathfrak{P})$ mit zyklischer Faktorgruppe $\mathcal{Z}_{N|k}(\mathfrak{P})/\mathcal{T}_{N|k}(\mathfrak{P})$ von der Ordnung $f_{N|k}(\mathfrak{P})$.

Beweis: a) Die Restklassenerweiterung ist eine Erweiterung endlicher Körper, per definitionem vom Grad $f = f_{N|k}(\mathfrak{P})$. Aus der Galoistheorie ist bekannt, daß diese Erweiterungen zyklisch sind: $G(\mathbb{F}|\mathbb{F}_q)$ wird erzeugt vom sog. *Frobeniusautomorphismus* $\sigma_q : x \mapsto x^q$; dessen Ordnung in $G(\mathbb{F}|\mathbb{F}_q)$ ist die Zahl f mit $\#\mathbb{F} = q^f$, also der Grad $(\mathbb{F}\colon \mathbb{F}_q)$ der Erweiterung $\mathbb{F}|\mathbb{F}_q$. Für $\sigma \in \mathcal{Z}_{N|k}(\mathfrak{P})$, d.h. $\sigma \in G(N|k)$ mit $\sigma\mathfrak{P} = \mathfrak{P}$, ist die induzierte Abbildung $a + \mathfrak{P} \mapsto \sigma(a) + \mathfrak{P}$ ($a \in Z_N$) ein Automorphismus $\bar{\sigma} \in G(\bar{N}|\bar{k})$. Die Zuordnung $\sigma \mapsto \bar{\sigma}$ ist dann offenbar ein Gruppenhomomorphismus

$$\mathcal{Z}_{N|k}(\mathfrak{P}) \to G(\bar{N}|\bar{k}).$$

Zum Beweis der entscheidenden Surjektivität wählen wir ein primitives Element $\bar{a}$ der Erweiterung $\bar{N}|\bar{k}$: $\bar{N} = \bar{k}(\bar{a})$ mit $a \in Z_N$. Dann hat das Minimalpolynom $f := f_{a,L}$ von a über

dem Zerlegungskörper L von $\mathfrak{P}$ Koeffizienten in Z_L. Das Restklassenpolynom $\bar{f}$ liegt dann in $\bar{L}[X] = \bar{k}[X]$ (Korollar (2.2),d)) und hat $\bar{a}$ als Nullstelle. Daher ist das Minimalpolynom $\varphi = f_{\bar{a},\bar{k}}$ ein Teiler von $\bar{f}$.

Ist nun $\sigma \in G(\bar{N}|\bar{k})$ beliebig, so ist $\sigma(\bar{a})$ Nullstelle von φ, also von $\bar{f}$. Es muß daher eine Nullstelle b von f in N existieren mit $\bar{b} = \sigma(\bar{a})$. Da $f \in L[X]$ irreduzibel ist, existiert ein $\tau \in G(N|L) = \mathcal{Z}_{N|k}(\mathcal{P})$ mit $\tau(a) = b$, also

$$\bar{\tau}(\bar{a}) = \overline{\tau(a)} = \bar{b} = \sigma(\bar{a}).$$

Da $\bar{a}$ die Erweiterung $\bar{N}|\bar{k}$ erzeugt, folgt $\bar{\tau} = \sigma$. b) ist dann klar.

b. Verzweigung und Frobeniusautomorphismus

Von besonderer Bedeutung ist die Spezialisierung des letzten Satzes für die sogenannten *unverzweigten* Primideale. Dabei heißt in einer Erweiterung $N|k$ ein Primideal $\mathfrak{P}$ von N *verzweigt,* wenn $e_{N|k}(\mathfrak{P}) > 1$ gilt. Entsprechend nennt man ein Primideal $\mathfrak{p}$ von k in N verzweigt, wenn in N ein Primideal $\mathfrak{P}|\mathfrak{p}$ existiert mit $e(\mathfrak{P}|\mathfrak{p}) > 1$.

Die Beweismethoden von Satz (2.3) können nun benutzt werden, um zu zeigen, daß *fast alle* Primideale unverzweigt sind:

(2.4) Satz: *Sei $K|k$ eine Zahlkörpererweiterung. Dann gilt:*

a) *In $K|k$ verzweigen nur endliche viele Primideale (von K bzw. von k).*

b) *Ist $N|k$ galoissch mit primitivem Element $a \in Z_N$ und $D := D(1, a, .., a^{n-1})$ die Diskriminante der k-Basis $1, a, \ldots, a^{n-1}$ von N, so ist jedes in N verzweigte Primideal $\mathfrak{p}$ von k ein Teiler von D.*

Beweis: a) folgt aus b): Man geht von der vorgegebenen Erweiterung $K|k$ zur galoisschen Hülle $N|k$ über und kann dann b) anwenden. Da die Diskriminante D von 0 verschieden ist, hat DZ_k nur endlich viele Primteiler, und nur diese können in N verzweigen. Wegen der Multiplikativität des Verzweigungsexponenten gilt dann die Behauptung erst recht für $K|k$.

Ad b): Seien a und D wie in der Formulierung des Satzes. Weiter sei $\mathfrak{P}$ ein Primideal von N über $\mathfrak{p}$ mit Restklassenkörper $\bar{N}$. Wir zeigen nun:
Ist $\mathfrak{p}$ kein Teiler von D, so ist der Epimorphismus

$$\mathcal{Z}_{N|k}(\mathfrak{P}) \to G(\bar{N}|\bar{k})$$

injektiv, also gemäß Satz (2.3),b) $e_{N|k}(\mathfrak{P}) = 1$.

Das Minimalpolynom $f = f_{a,k}$ von a über k zerfällt über N in Linearfaktoren

$$f = \prod_{i=1}^{n}(X - a_i)$$

mit verschiedenen Wurzeln $a_1 = a, \ldots, a_n \in Z_N$. Ist nun $\sigma \in \mathcal{Z}_{N|k}(\mathfrak{P})$ mit $\bar{\sigma} = id_{\bar{N}}$, so folgt $\bar{a}_1 = \bar{a}_i$ für das $i \in \{1, \ldots, n\}$ mit $a_i = \sigma(a_1)$. Nun bedeutet die Voraussetzung $\mathfrak{p} \not| D \in Z_k$ nichts anderes als $\bar{D} \neq 0 \in \bar{k}$, also gemäß der Berechnung der Diskriminante im Beweis von (1.6)

$$\prod_{i<j}(\bar{a}_i - \bar{a}_j) \neq 0\,.$$

Damit sind auch die n Restklassen $\bar{a}_i$ $(i = 1, \ldots, n)$ verschieden und aus $\bar{a}_1 = \bar{a}_i$ folgt daher $i = 1$. So ergibt sich $\sigma(a) = a_i = a$, und σ ist die Identität auf $N = k(a)$.

Es sei angemerkt, daß schärfer als Satz (2.4) folgendes gilt: Ein Primideal von k ist *genau* dann in K verzweigt, wenn es die *Diskriminante* $\mathfrak{d}_{K|k}$ von $K|k$ teilt. Diese ist für $k = \mathbb{Q}$ definiert

als die Diskriminante einer Ganzheitsbasis von Z_K. Im allgemeinen Fall ist sie ein ganzes Ideal von k.

Aufgrund von Satz (2.4) werden wir uns bei den nachfolgenden Untersuchungen im wesentlichen auf unverzweigte Primideale konzentrieren. Daher formulieren wir zunächst Satz (2.3) für den Spezialfall unverzweigter Primideale:

(2.5) Bemerkung: Sei $N|k$ eine galoissche Zahlkörpererweiterung und $\mathfrak{P}$ ein über k unverzweigtes Primideal von N. Dann gilt:

a) Die Reduktion $\bmod \mathfrak{P}$ induziert einen **Iso**morphismus der Zerlegungsgruppe $\mathcal{Z}_{N|k}(\mathfrak{P})$ auf die Galoisgruppe $G(\bar{N}_{\mathfrak{P}}|\bar{k})$ der Restklassenkörpererweiterung:

$$\mathcal{Z}_{N|k}(\mathfrak{P}) \backsimeq G(\bar{N}|\bar{k}).$$

b) Der eindeutig bestimmte Automorphismus $F_{N|k}(\mathfrak{P}) \in \mathcal{Z}_{N|k}(\mathfrak{P})$, der auf $\bar{N}$ die Potenzierung mit $q = \#\bar{k}$ induziert, wird *Frobeniusautomorphismus* von $\mathfrak{P}$ über k genannt. Explizit ist der Frobeniusautomorphismus $F_{N|k}(\mathfrak{P})$ charakterisiert als der eindeutig bestimmte Automorphismus $\sigma \in G(N|k)$ mit

$$\sigma(a) \equiv a^q \bmod \mathfrak{P} \quad \text{für alle } a \in Z_N,$$

wobei $q = \#\bar{k}$ ist.

c) Der Frobeniusautomorphismus $F_{N|k}(\mathfrak{P})$ hat die Ordnung $f_{N|k}(\mathfrak{P})$ und erzeugt die Zerlegungsgruppe $\mathcal{Z}_{N|k}$ von $\mathfrak{P}$ über k.

Man beachte bei b) lediglich, daß aus $\sigma(a) \equiv a^q \bmod \mathfrak{P}$ natürlich $\sigma\mathfrak{P} = \mathfrak{P}$, also $\sigma \in \mathcal{Z}_{K|k}(\mathfrak{P})$ folgt.

Für spätere Zwecke sollen hier nun noch einige Eigenschaften des Frobeniusautomorphismus zusammengestellt werden:

(2.6) Bemerkung: Sei $N|k$ eine galoissche Zahlkörpererweiterung mit Gruppe G, K ein Zwischenkörper. Weiter sei $\mathfrak{P}$ ein über k unverzweigtes Primideal von N, $\mathfrak{P}_K := \mathfrak{P} \cap K$, $\mathfrak{p} := \mathfrak{P} \cap k$ und $\sigma \in G$. Dann gilt:

a) $F_{N|k}(\sigma\mathfrak{P}) = \sigma F_{N|k}(\mathfrak{P})\sigma^{-1}$.

b) $(F_{N|k}(\mathfrak{P}))^{f(\mathfrak{P}_K|\mathfrak{p})} = F_{N|K}(\mathfrak{P})$.

c) $F_{N|\sigma K}(\sigma\mathfrak{P}) = \sigma F_{N|K}(\mathfrak{P})\sigma^{-1}$.

Zum *Beweis* benutzt man die in (2.5),b) angegebene Charakterisierung. Es sei $F = F_{N|k}(\mathfrak{P})$ und $q = \#\bar{k}$.
a) Wir zeigen, daß $\sigma F_{N|k}(\mathfrak{P})\sigma^{-1}$ die $F_{N|k}(\sigma\mathfrak{P})$ charakterisierende Eigenschaft hat:

$$\begin{aligned} \textstyle\bigwedge_{a\in Z_N} F(a) \equiv a^q \bmod \mathfrak{P} &\implies \textstyle\bigwedge_{a\in Z_N} F(\sigma^{-1}(a)) - (\sigma^{-1}(a))^q \in \mathfrak{P} \\ &\implies \textstyle\bigwedge_{a\in Z_N} \sigma F\sigma^{-1}(a) - a^q \in \sigma\mathfrak{P} \end{aligned}$$

b) Es ist

$$q' := \#\bar{K}_{\mathfrak{P}'} = q^{f'} \quad \text{mit } \mathfrak{P}' := \mathfrak{P}_K\,,\ f' := f(\mathfrak{P}'|\mathfrak{p}).$$

Dann gilt:

$$F(a) \equiv a^q \bmod \mathfrak{P} \implies F^{f'}(a) \equiv a^{q^{f'}} = a^{q'} \bmod \mathfrak{P}\,.$$

c) Es gilt

$$f_{\sigma K|k}(\sigma\mathfrak{P} \cap \sigma K) = f_{\sigma K|k}(\sigma(\mathfrak{P} \cap K)) = f_{K|k}(\mathfrak{P} \cap K) = f',$$

also haben $\mathfrak{P} \cap K$ und $\sigma\mathfrak{P} \cap \sigma K$ dieselbe Absolutnorm. Schließlich ist

$$F' := \sigma F_{N|K}(\mathfrak{P})\sigma^{-1} \in \sigma G(N|K)\sigma^{-1} = G(N|\sigma K)$$

und aus

$$F_{N|K}(\mathfrak{P})(b) \equiv b^{q'} \bmod \mathfrak{P} \quad \text{für alle } b \in Z_N$$

folgt

$$F'(a) \equiv a^{q'} \bmod \sigma\mathfrak{P} \quad \text{für alle } a \in Z_N\,,$$

womit c) bewiesen ist. [a) ist natürlich ein Spezialfall von c).]

c. Primzerlegung und Permutationsgruppen

Wir wollen nun aus den bisherigen Ergebnissen über die Primzerlegung in galoisschen Erweiterungen gruppentheoretische Kriterien für die Zerlegung unverzweigter Primideale in beliebigen Erweiterungen ableiten. Um den angestrebten Satz befriedigend formulieren zu können, sollen hier zunächst einige Bemerkungen über Permutationsgruppen vorangestellt werden.

Eine *Operation* ('von links') einer Gruppe G auf einer Menge M ist eine Abbildung

$$G \times M \to M,\ (s, m) \mapsto s.m$$

mit den Eigenschaften:

$$(st).m = s.(t.m) \quad \text{und} \quad 1.m = m \quad \text{für alle } s, t \in G, m \in M.$$

Als *Bahn* (oder *Orbit)* von $m \in M$ unter der Operation von G bezeichnet man die Menge $G.m = \{g.m \mid g \in G\}$. Die Bahnen bilden eine Klasseneinteilung von M. Die Abbildung $G \to G.m, g \mapsto g.m$ induziert eine Bijektion der Rechtsnebenklassen der *Fixgruppe* $\mathrm{Fix}_G(m) = G_m$ auf die Bahn von m unter G vermöge $gG_m \mapsto g.m$.

Als Standardbeispiel haben wir: Die symmetrische Gruppe $\mathcal{S}_n$ (und damit jede Untergruppe) operiert auf $\{1, \ldots, n\}$. Ist $\sigma \in \mathcal{S}_n$ eine beliebige Permutation, so sind die Bahnen der zyklischen Gruppe $\langle\sigma\rangle$ nichts anderes als die Zyklen in der Zyklenzerlegung von σ. Die Bahnen von $\langle\sigma\rangle$ wollen wir auch kurz *Bahnen von* σ nennen.

Eine Operation von G auf M kann man auch beschreiben durch den Gruppenhomomorphismus $P\colon G \to \mathcal{S}(M),\ \sigma \mapsto (m \mapsto \sigma.m)$, eine em Permutationsdarstellung von G. Dann sind die Bahnen von G nichts anderes als die Bahnen der Permutationsgruppe $P(G)$; insbesondere sind die Bahnen von σ dasselbe wie die Zyklen von $P(\sigma) \in \mathcal{S}(M)$. Hat die Operation von G auf M nur eine Bahn (nämlich M), so ist die Operation *transitiv,* d. h. zu je zwei Elementen $m, m' \in M$ existiert ein $\sigma \in G$ mit $m' = \sigma.m$. Transitive Operationen sind bereits durch die Fixgruppe eines Elementes festgelegt:

$$U = G_m \implies M = G.m \cong G/U \quad \text{und} \quad m \mapsto \sigma U \implies \sigma'.m \mapsto \sigma'\sigma U\,.$$

Umgekehrt bestimmt jede Untergruppe U von G vom Index n eine transitive Operation von G auf der n-elementigen Menge aller Rechtsnebenklassen. Gleiches gilt auch für die Linksnebenklassen, wobei man jedoch Operationen 'von rechts' betrachtet.

Im folgenden betrachten wir Untergruppen U vom Index n in G; es bezeichne dann $P_U : G \to \mathcal{S}_n$ die transitive Operation von G auf den n Linksnebenklassen $U\sigma$. In Bezug auf P_U machen dann Begriffe wie Zyklenzerlegung, Zyklenlänge, etc. für die Elemente von G Sinn. Wir kommen nun zum angestrebten

(2.7) Satz: *Es sei $K|k$ eine Zahlkörpererweiterung, $N|k$ eine galoissche Erweiterung mit $N \supseteq K$ und $U := G(N|K) \subseteq G := G(N|k)$. Sei $\mathfrak{p}$ ein maximales Ideal von k, unverzweigt in N und $\mathfrak{P}$ ein beliebiger Primteiler von $\mathfrak{p}$ in N. Weiter sei $F := F_{N|k}(\mathfrak{P})$ der Frobeniusautomorphismus von $\mathfrak{P}$. Dann sind äquivalent:*

i) $\mathfrak{p}$ *besitzt in* K *genau* r *Primteiler mit den Restklassengraden* $f_1, \ldots, f_r$ *über* k.
Kurz: Der Zerlegungstyp von $\mathfrak{p}$ *in* K *ist* $(f_1, \ldots, f_r)$.

ii) F *operiert auf den Nebenklassen von* U *als Produkt von* r *Zyklen der Längen* $f_1, \ldots, f_r$.
Kurz: Der Zyklentyp von $P_U(F)$ *ist* $(f_1, \ldots, f_r)$.

Beweis: Sämtliche maximalen Ideale von K über $\mathfrak{p}$ erhält man, indem man die maximalen Ideale von N über $\mathfrak{p}$ auf K einschränkt. Gemäß Proposition (2.1) sind dies gerade die Ideale $\mathfrak{Q}_\sigma := \sigma\mathfrak{P} \cap K$ ($\sigma \in G$). Um ihre Anzahl festzustellen, muß man also untersuchen, wann Q_σ und $Q_{\sigma'}$ übereinstimmen. Nun gilt nach den Resultaten aus Abschnitt b.

$$\begin{aligned}
Q_\sigma = Q_{\sigma'} &\iff \sigma\mathfrak{P} \cap K = \sigma'\mathfrak{P} \cap K \\
&\iff \sigma\mathfrak{P} \text{ und } \sigma'\mathfrak{P} \text{ liegen über demselben maximalen Ideal von } K \\
&\iff \sigma\mathfrak{P} = \tau\sigma'\mathfrak{P} \quad \text{für ein } \tau \in G(N|K) = U \\
&\iff \sigma^{-1}\tau\sigma' \in \mathcal{Z}_{N|k}(\mathfrak{P}) = \langle F \rangle \text{ für ein } \tau \in U \\
&\iff \tau\sigma' = \sigma F^m \text{ für geeignete } m \in \mathbb{Z} \text{und } \tau \in U \\
&\iff U\sigma' = U\sigma F^m \text{ für geeignetes } m \in \mathbb{Z} \\
&\qquad [\iff \text{Doppelnebenklassen } U\sigma'\mathcal{Z}_{N|k}(\mathfrak{P}) = U\sigma\mathcal{Z}_{N|k}(\mathfrak{P})] \\
&\iff \text{DieLinksnebenklassen } U\sigma' \,,\ U\sigma \text{ liegen in derselben Bahn unter } F \,.
\end{aligned}$$

Damit ist gezeigt, daß die Anzahl der Primteiler von $\mathfrak{p}$ in K gerade die Anzahl der Bahnen des Frobeniusautomorphismus $F = F_{N|k}(\mathfrak{P})$ bei der Operation auf den Linksnebenklassen von U, d. h. die Anzahl der Zyklen in der Zyklendarstellung von $P_U(F)$ ist.
Man muß nun noch für ein solches $\mathfrak{Q}_\sigma$ den Restklassengrad $f_\sigma := f_{K|k}(\mathfrak{Q}_\sigma)$ bestimmen. Es gilt:

f_σ ist die Bahnlänge von $U\sigma$ unter F, d.h. die Länge des Zyklus von F, zu dem $U\sigma$ gehört.

Zum Beweis: Diese Zyklenlänge ist die kleinste Zahl $m \in \mathbb{N}_+$ mit $U\sigma F^m = U\sigma$. Wir fixieren $\sigma \in G$ und setzen $F_\sigma := F_{N|k}(\sigma\mathfrak{P})$. Dann gilt:

$$\begin{aligned}
U\sigma F^m = U\sigma &\iff \sigma F^m \sigma^{-1} \in U \\
&\iff F_\sigma^m \in U && \text{[gemäß (2.6),a)]} \\
&\iff F_\sigma^m \in U \cap \mathcal{Z}_{N|k}(\sigma\mathfrak{P}) = \mathcal{Z}_{N|K}(\sigma\mathfrak{P}) \\
&\iff F_\sigma^m \in \langle F_{N|K}(\sigma\mathfrak{P}) \rangle \\
&\iff F_\sigma^m \in \langle F_\sigma^{f_\sigma} \rangle && \text{[gemäß (2.6),b)]}
\end{aligned}$$

Nun ist f_σ ein Teiler von $f_{N|k}(\sigma\mathfrak{P}) = ord(F_\sigma)$, also ist offenbar f_σ die kleinste Zahl m mit dieser Eigenschaft.

§3 Primzerlegung und Zetafunktionen

a. Die Dedekindsche Zetafunktion

Spricht man über Zetafunktionen, so muß man notwendig mit der *Riemannschen Zetafunktion* beginnen, die (zunächst) für komplexes Argument $s \in \mathbb{C}$ mit $\mathrm{Re}\,(s) > 1$ definiert ist als die formal (!) einfachste *Dirichletreihe*

$$\zeta(s) := \sum_{n \in \mathbb{N}_+} \frac{1}{n^s}.$$

Diese Reihe konvergiert für $\mathrm{Re}\,(s) \geq \sigma\ (> 1)$ absolut gleichmäßig, da für $\sigma > 1$

$$\sum_{n=1}^{\infty} \frac{1}{n^\sigma}$$

offenbar eine konvergente Majorante ist. Die Konvergenz dieser Majorante ergibt sich aus dem Integralkriterium:

$$\frac{1}{\sigma-1} = \int_1^\infty \frac{1}{x^\sigma}\,dx \le 1 + \sum_{n=2}^{\infty} \frac{1}{n^\sigma} \le 1 + \int_1^\infty \frac{1}{x^\sigma}\,dx = 1 + \frac{1}{\sigma-1} \tag{1}$$

Wegen der gleichmäßigen Konvergenz stellt die Dirichletreihe im Bereich $\mathrm{Re}\,(s) > 1$ eine holomorphe Funktion dar. Wie Riemann selbst schreibt, war für ihn die (für $s \in \mathbb{N}$ von Euler) stammende Beziehung

$$\sum_{n\in\mathbb{N}_+} \frac{1}{n^s} = \prod_{p \text{ Primzahl}} \frac{1}{1-\frac{1}{p^s}}$$

Ausgangspunkt seiner Überlegungen. Diese *Eulerproduktdarstellung* ist die analytische Formulierung der ZPE-Eigenschaft des Ringes $\mathbb{Z}$. Durch sie ist die Zetafunktion aufs Engste mit den Primzahlen und deren Verteilung verbunden. An diesem Eulerprodukt kann man auch erkennen, daß $\zeta(s) \neq 0$ ist für $\mathrm{Re}\,(s) > 1$; genauer gilt folgende Abschätzung für den (Hauptwert des) Logarithmus der Zetafunktion:

$$|\log \zeta(s)| \;\le\; \log\,\zeta(\sigma) \;\le\; 2\zeta(\sigma)$$

für $\sigma = \mathrm{Re}\,(s) > 1$. Wegen des Eulerproduktes gilt

$$\log \zeta(s) = -\sum_{p \text{ Primzahl}} \log(1-p^{-s}) = \sum_{p,n\ge 1} \frac{1}{np^{ns}},$$

also

$$|\log \zeta(s)| \le \sum_{p,n\ge 1} \frac{1}{np^{n\sigma}} \le \sum_{p,n\ge 1} \frac{1}{p^{n\sigma}} = \sum_p \frac{p^{-\sigma}}{1-p^{-\sigma}} \le 2\cdot \sum_p p^{-\sigma}, \tag{2}$$

denn für $\sigma > 1$ ist $p^{-\sigma} < \frac{1}{2}$, also $\frac{1}{1-p^{-\sigma}} < 2$.

Dies zeigt, daß $\log \zeta(s)$ betraglich beschränkt bleibt, also $\zeta(s)$ im Bereich $\mathrm{Re}\,(s) > 1$ keine Nullstelle haben kann. Damit ist $\log \zeta(s)$ auf dem einfach-zusammenhängenden Gebiet $\{s \in \mathbb{C} \mid \mathrm{Re}\,(s) > 1\}$ eine holomorphe Funktion. Während Euler die obige Beziehung für $s \in \mathbb{N}$ mehr formal verstanden hatte, hatte bereits Dirichlet (einer von Riemanns Lehrern) sie für reelle Argumente s bewiesen. Aber erst Riemann tat den wesentlichen Schritt; er betrachtete ζ als Funktion auf ganz $\mathbb{C}$: Riemann "... leitete eine überall gültige Beschreibung für $\zeta(s)$ her!" In heutiger Sprechweise: Riemann bewies die *analytische Fortsetzbarkeit* der Zetafunktion zu einer meromorphen Funktion auf ganz $\mathbb{C}$. Dies beinhaltete den Beweis einer *Funktionalgleichung* für die Zetafunktion ζ beim Übergang $s \to 1-s$. (Auf den interessanten funktionentheoretischen Beweis kann hier leider nicht eingegangen werden.)

Die obige Abschätzung (1) $1 \le (\sigma-1)\zeta(\sigma) \le \sigma$ für $\sigma \in \mathbb{R}, \sigma > 1$ ergibt für die Zetafunktion:

$\zeta(s)$ hat bei $s = 1$ einen Pol erster Ordnung mit Residuum 1 .

Für uns hier ist nun die folgende Verallgemeinerung der Riemannschen Zetafunktion von besonderer Bedeutung: Ist K ein beliebiger Zahlkörper, so definiert man seine *Dedekindsche Zetafunktion* $\zeta_K(s)$ als Dirichletreihe

$$\zeta_K(s) := \sum_{\substack{\mathfrak{A}\lhd Z_K \\ \mathfrak{A}\neq 0}} \frac{1}{\mathcal{N}\mathfrak{A}^s}$$

wobei $\mathcal{N}\mathfrak{A}$ die Absolutnorm $(Z_K\colon\mathfrak{A})$ von $\mathfrak{A}$ bezeichnet. Für $K = \mathbb{Q}$ ergibt sich offensichtlich die Riemannsche Zetafunktion. Aufgrund der eindeutigen Primidealzerlegung in Z_K erhält man auch für die Dedekindsche Zetafunktion eine *Eulerproduktdarstellung*

$$\zeta_K(s) = \prod_{\mathfrak{P}} \frac{1}{1 - \mathcal{N}\mathfrak{P}^{-s}}.$$

[Das Produkt erstreckt sich über alle maximalen Ideale $\mathfrak{P}$ von K.]
Diese Darstellung gilt im (übereinstimmenden) Konvergenzbereich beider Seiten. Dieser Konvergenzbereich ist - wie bei der Riemannschen Zetafunktion - der Bereich $\sigma := \mathrm{Re}\,(s) > 1$: Zum Beweis logarithmiert man zunächst das Eulerprodukt und erhält:

$$\log \prod_{\mathfrak{P}} \frac{1}{1 - \mathcal{N}\mathfrak{P}^{-s}} = -\sum_{\mathfrak{P}} \log(1 - \mathcal{N}\mathfrak{P}^{-s}) = \sum_{\mathfrak{P},m\geq 1} \frac{1}{m\mathcal{N}\mathfrak{P}^{ms}} \tag{3}$$

Von diesen zunächst rein formal durchgeführten Umformungen ist die letzte bei festem $\mathfrak{P}$ gültig für $|\mathcal{N}\mathfrak{P}^{-s}| = \mathcal{N}\mathfrak{P}^{-\sigma} < 1$, also wegen $\mathcal{N}\mathfrak{P} \geq 1$ für $\sigma = \mathrm{Re}\,(s) > 0$. Die letzte Reihe

$$\sum_{\mathfrak{P}}(\ldots) = \sum_{p}(\sum_{\mathfrak{P}|p}\ldots)$$

wird majorisiert durch $(K\colon\mathbb{Q}) \cdot \log\zeta(\sigma)$, da natürlich $m\mathcal{N}\mathfrak{P}^m = mp^{fm} \geq mp^m$ für alle $\mathfrak{P}|p$ gilt und $(K\colon\mathbb{Q})$ eine Schranke für die Anzahl der maximalen Ideale $\mathfrak{P}$ von K über einer festen Primzahl p ist. Sie konvergiert also (siehe (2)) für $\sigma > 1$, so daß die gesamte Umformung für $\mathrm{Re}\,(s) > 1$ gilt und die Dedekindsche Zetafunktion in diesem Bereich wohldefiniert ist.

Außerdem ist damit zugleich für $\sigma = \mathrm{Re}\,(s) > 1$ gezeigt:

$$|\log\zeta_K(s)| \leq \log\zeta_K(\sigma) \leq (K\colon\mathbb{Q}) \cdot \log\zeta(\sigma) \leq 2(K\colon\mathbb{Q}) \cdot \zeta(\sigma). \tag{4}$$

Analog zu (2) gilt natürlich auch

$$|\log\zeta_K(s)| \leq 2\zeta_K(\sigma) \tag{2_K}$$

für $\sigma = \mathrm{Re}\,(s) > 1$. Zugleich zeigen diese Überlegungen, daß in obiger Reihe für $\log\zeta_K(s)$ die $m > 1$, aber auch die maximalen Ideale $\mathfrak{P}$ von K mit absolutem Restklassengrad $f_{K|\mathbb{Q}}(\mathfrak{P}) = f(\mathfrak{P}) > 1$ einen Beitrag liefern, der für $\mathrm{Re}\,(s) > \frac{1}{2}$ konvergiert, und folglich gilt:

$$\left|\begin{array}{l} \log\zeta_K(s)\ ,\ Z(s) := \displaystyle\sum_{\mathfrak{P}} \frac{1}{\mathcal{N}\mathfrak{P}^s} \ \text{ und } \ Z_1(s) := \sum_{\mathfrak{P},f(\mathfrak{P})=1} \frac{1}{\mathcal{N}\mathfrak{P}^s} \\ \\ \text{unterscheiden sich um eine für } \mathrm{Re}\,s > \frac{1}{2} \text{ holomorphe Funktion.} \end{array}\right. \tag{5}$$

Beweis: Wie beim Beweis von (2) schätzt man für $\sigma = Re(s) > \frac{1}{2}$ ab:

$$\begin{aligned} |\log\zeta_K(s) - Z(s)| &\leq \sum_{\mathfrak{P},m\geq 2} \frac{1}{m\mathcal{N}\mathfrak{P}^{m\sigma}} \leq \sum_{\mathfrak{P},m\geq 2} \mathcal{N}\mathfrak{P}^{-m\sigma} \\ &\leq \sum_{\mathfrak{P}} \mathcal{N}\mathfrak{P}^{-2\sigma} \frac{1}{1 - \mathcal{N}\mathfrak{P}^{-\sigma}} \\ &\leq c_\sigma \cdot \sum_{\mathfrak{P}} \mathcal{N}\mathfrak{P}^{-2\sigma} \leq c_\sigma \cdot \zeta_K(2\sigma) \end{aligned}$$

mit

$$c_\sigma := \max_{\mathfrak{P}} \frac{1}{1 - \mathcal{N}\mathfrak{P}^{-\sigma}} \leq \frac{1}{1 - 2^{-\sigma}}\,.$$

Damit ist eine für $2\sigma > 1$, d.h. für $\sigma > \frac{1}{2}$ konvergente Majorante gefunden und $\log \zeta_K(s) - Z(s)$ im Bereich $\operatorname{Re} s > \frac{1}{2}$ holomorph. Genauso zeigt man

$$|Z(s) - Z_1(s)| \leq \sum_{\mathfrak{P}, f(\mathfrak{P}) \geq 2} \mathcal{N}\mathfrak{P}^{-\sigma} \leq \sum_{p \text{ Primzahl}} \sum_{\mathfrak{P}|p} p^{-2\sigma} \leq (K\colon \mathbb{Q}) \cdot \zeta(2\sigma)$$

und folgert die zweite Behauptung.

Auch die Dedekindsche Zetafunktion ist *analytisch em* fortsetzbar auf ganz $\mathbb{C}$ mit einem einzigen Pol bei $s = 1$ und einer Funktionalgleichung für $s \to 1 - s$. Der Beweis ist für beliebige Zahlkörper K statt $\mathbb{Q}$ aber funktionentheoretisch erheblich aufwendiger. Er wurde nach großen Anstrengungen berühmter Mathematiker im Anfang dieses Jahrhunderts 1918/20 von E. Hecke geführt. Mit einfacheren Mitteln kann man die analytische Fortsetzung in den Bereich $\operatorname{Re}(s) > 1 - \frac{1}{(K:\mathbb{Q})}$ und die Residuumsformel beweisen (siehe S.Lang, Algebraic Number Theory, VIII,§2).

Wir formulieren (ohne Beweis des entscheidenden Teils b)) den folgenden wichtigen

(3.1) Satz: *Sei K ein algebraischer Zahlkörper. Dann gilt:*

a) *Die Dirichletreihe*

$$\sum_{\substack{\mathfrak{A} \lhd Z_K \\ \mathfrak{A} \neq 0}} \frac{1}{\mathcal{N}\mathfrak{A}^s}$$

definiert eine in der Halbebene $\operatorname{Re} s > 1$ holomorphe Funktion.

b) *Diese ist fortsetzbar zu einer meromorphen Funktion auf ganz $\mathbb{C}$, der Dedekindschen Zetafunktion ζ_K, mit einer Funktionalgleichung für $s \to 1 - s$. ζ_K hat genau einen Pol, und zwar bei $s = 1$ von erster Ordnung mit dem Residuum*

$$\frac{2^{r(K)}(2\pi)^{s(K)} h_K R_K}{w_K \sqrt{d_K}}.$$

Hierbei bezeichnen $r(K) = r_1$ die Zahl der reellen und $2s(K) = 2r_2$ die der komplexen Konjugierten von K, h_K die Klassenzahl, R_K den Regulator, $w_K = \#\mu_K$ die Einheitswurzelanzahl von K und schließlich d_K die Diskriminante von K.

Die Tatsache, daß die Dedekindsche Zetafunktion für *jeden* Zahlkörper K einen einfachen Pol bei $s = 1$ hat, ist die Quelle des nachfolgenden Korollars, dem wir jedoch zunächst eine wichtige Definition vorausschicken müssen:

(3.2) Definition: Sei K ein Zahlkörper und $\mathcal{A}$ eine Menge von maximalen Idealen von K. Dann definiert man die *Dirichletdichte* $d(\mathcal{A})$ als den folgenden Limes – sofern er existiert:

$$d(\mathcal{A}) := \lim_{s \to 1+} \frac{\sum_{\mathfrak{P} \in \mathcal{A}} \mathcal{N}\mathfrak{P}^{-s}}{\sum_{\mathfrak{P} \in \mathcal{P}_K} \mathcal{N}\mathfrak{P}^{-s}} \underset{(5)}{=} \lim_{s \to 1+} \frac{\log \zeta_{K,\mathcal{A}}(s)}{\log \zeta_K(s)}$$

mit der *partiellen* Zetafunktion

$$\zeta_{K,\mathcal{A}}(s) := \prod_{\mathfrak{P} \in \mathcal{A}} (1 - \mathcal{N}\mathfrak{P}^{-s})^{-1}.$$

Diesen Limes als ein Maß für die *Dichte* von $\mathcal{A}$, d. h. für die Größe von $\mathcal{A}$ relativ zur Gesamtprimidealmenge anzusehen, ist zunächst schon durch die Definitionsformel ein wenig gerechtfertigt. Hinzukommt jedoch noch, daß die sogenannte *natürliche Dichte*

$$\delta(\mathcal{A}) := \lim_{N \to \infty} \frac{\#\{\mathfrak{P} \in \mathcal{A} \mid \mathcal{N}\mathfrak{P} \leq N\}}{\#\{\mathfrak{P} \in \mathcal{P}_K \mid \mathcal{N}\mathfrak{P} \leq N\}}$$

– sofern sie existiert – mit der Dirichletdichte, die dann ebenfalls existiert, übereinstimmt (o. Beweis; siehe L. Goldstein: Analytic Number Theory, Ch. 14, Thm.14-1-2.)

Anmerkung: 1) Wegen des Pols der Zetafunktion bei $s = 1$ haben endliche Mengen Dirichletdichte 0. Die Dirichletdichte ändert sich also nicht, wenn man eine Menge um endlich viele Elemente abändert. Insbesondere können die verzweigten Primideale stets unberücksichtigt bleiben und Mengen mit positiver Dirichletdichte müssen notwendig unendlich sein!
2) Ist $\mathcal{A}$ eine beliebige Menge von maximalen Idealen von K und $\mathcal{A}^1$ die Menge der Primideale in $\mathcal{A}$ vom Absolutgrad 1, d.h.

$$\mathcal{A}^1 := \{\mathfrak{P} \in \mathcal{A} \mid f_{K|\mathbb{Q}}(\mathfrak{P}) = 1\},$$

so haben alle Mengen $\mathcal{A}'$ zwischen $\mathcal{A}^1$ und $\mathcal{A}$ dieselbe Dirichletdichte $d(\mathcal{A}) = d(\mathcal{A}')$, sofern diese für nur eine der Mengen existiert: In der Zerlegung

$$\sum_{\mathfrak{P}\in\mathcal{A}} \mathcal{N}\mathfrak{P}^{-s} = \sum_{\mathfrak{P}\in\mathcal{A}'} \mathcal{N}\mathfrak{P}^{-s} + \sum_{\mathfrak{P}\in\mathcal{A}\setminus\mathcal{A}'} \mathcal{N}\mathfrak{P}^{-s}$$

haben im zweiten Summanden alle maximalen Ideale $\mathfrak{P}$ Absolutgrad $f_{K|\mathbb{Q}}(\mathfrak{P}) \geq 2$, also konvergiert diese Reihe bei $s = 1$ (siehe (5)). Zur Berechnung der Dirichletdichte trägt daher dieser Teil nichts bei, da durch $\log \zeta_K(s)$ dividiert wird und ζ_K bei $s = 1$ einen Pol hat.
3) Da alle Zetafunktionen bei $s = 1$ einen Pol *erster* Ordnung haben, gilt $\zeta_K(s) = \frac{1}{(s-1)} \cdot h$ mit h holomorph bei $s = 1$ und $h(1) \neq 0$. Also

$$\log \zeta_K(s) = -\log(s-1) + O(1) \quad \text{für } s \to 1\,,$$

so daß die Dirichletdichte auch definiert werden kann als

$$d(\mathcal{A}) = \lim_{s\to 1+} \frac{\sum_{\mathfrak{P}\in\mathcal{A}} \mathcal{N}\mathfrak{P}^{-s}}{\log \frac{1}{s-1}} \underset{(5)}{=} \lim_{s\to 1+} \frac{\log \prod_{\mathfrak{P}\in\mathcal{A}}(1 - \mathcal{N}\mathfrak{P}^{-s})}{\log(s-1)}\,.$$

(3.3) Korollar: *Sei k ein algebraischer Zahlkörper und $N|k$ eine galoissche Erweiterung. Dann hat die Menge*

$$S(N|k) := \{\mathfrak{p} \in P_k \mid \mathfrak{p} \textit{ ist in } N \textit{ voll-zerlegt } \}$$

die Dirichletdichte

$$\frac{1}{(N\colon k)}\,,$$

ist also insbesondere unendlich.
[Ein Primideal $\mathfrak{p} \in P_k$ ist *voll-zerlegt* in einer Körpererweiterung $K|k$, wenn die Anzahl $r(\mathfrak{p})$ der Primteiler von $\mathfrak{p}$ in K maximal, d.h. gleich dem Körpergrad $(K\colon k)$ ist.]

Beweis: Sei $n := (N\colon k)$ und $S := S(N|k)$. Die Menge $T := \{\mathfrak{P} \in P_N \mid \mathfrak{P} \cap k \in S\}$ ist die Menge der über k unverzweigten Primideale von N mit Restklassengrad 1 über k und hat daher gemäß Anmerkung 1) und 2) die Dichte 1, also gilt gemäß Anmerkung 3):

$$\begin{aligned}
1 &= \lim\nolimits_{s\to 1} \tfrac{\log \prod_{\mathfrak{P}\in T}(1-\mathcal{N}\mathfrak{P}^{-s})}{\log(s-1)} \\
&= \lim_{s\to 1} \frac{\log \prod_{\mathfrak{p}\in S}\prod_{\mathfrak{P}|\mathfrak{p}}(1 - \mathcal{N}\mathfrak{p}^{-s})}{\log(s-1)} && (\mathcal{N}\mathfrak{P} = \mathcal{N}\mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})} = \mathcal{N}\mathfrak{p}) \\
&= \lim_{s\to 1} \frac{\log \prod_{\mathfrak{p}\in S} (1 - \mathcal{N}\mathfrak{p}^{-s})^n}{\log(s-1)} && (r(\mathfrak{p}) = n) \\
&= n \cdot \lim_{s\to 1} \frac{\log \prod_{\mathfrak{p}\in S}(1 - \mathcal{N}\mathfrak{p}^{-s})}{\log(s-1)} \\
&= n \cdot d(S).
\end{aligned}$$

Insbesondere zeigt dieses Korollar, daß eine galoissche Erweiterung von k, in der fast alle Primideale von k voll zerfallen, nur k sein kann. Dieses Resultat läßt sich nun leicht verallgemeinern zum nachfolgenden Satz von *Bauer.* Wir definieren zuvor für eine *beliebige* Erweiterung $K|k$ die sog. *Kroneckermenge*

$$D(K|k) := \{\mathfrak{p} \in P_k \mid \mathfrak{p} \text{ besitzt in } K \text{ einen Primteiler } \mathfrak{P} \text{ vom Grad } 1\}\,.$$

Offenbar gilt für galoissche Erweiterungen $N|k$ $D(N|k) \doteq S(N|k)$. Dabei bezeichne ein $\dot{}$ an Mengeninklusionen stets, daß endlich viele Ausnahmen zugelassen sind:

$$M \dot{\subset} N \;:\Longleftrightarrow\; M \setminus N \text{ ist endlich}\,.$$

Die Bedeutung von $M \doteq N$ ist dann ebenfalls klar.

(3.4) Satz: *Es sei $N|k$ eine galoissche und $K|k$ eine beliebige Zahlkörpererweiterung. Dann gilt:*

a) $$D(N|k) \dot{\supset} D(K|k) \iff N \subset K \iff D(N|k) \supset D(K|k)$$

b) Galoissche Erweiterungen sind durch ihre Kroneckermengen eindeutig bestimmt.

Beweis: Es genügt die erste Implikation ' $\Longrightarrow$ ' von a) zu beweisen. Sei $L = NK$, also ist $L|K$ eine galoissche Erweiterung. Wir zeigen: Fast jedes Primideal von K vom Absolutgrad 1 ist in L voll zerlegt:

$(*)$ $$\mathcal{P}_K^1 \dot{\subset} S(L|K)\,.$$

Dann hat $S(L|K)$ die Dirichletdichte 1 (Anm. 2)), und folglich gilt gemäß Korollar (3.3) $K = L = NK$, also wie behauptet $N \subset K$.

Ad $(*)$: Sei $\mathfrak{P}$ ein maximales Ideal von K vom Absolutgrad 1, $\mathfrak{Q}$ ein beliebiger Primteiler von $\mathfrak{P}$ in L und $\mathfrak{p} = \mathfrak{P} \cap k$ bzw. $\mathfrak{Q}_N = \mathfrak{Q} \cap N$ die darunterliegenden Primideale von k bzw. N. Dann gehört $\mathfrak{p}$ zu $D(K|k)$, also – von endlich vielen Ausnahmen abgesehen – zu $D(N|k) \doteq S(N|k)$. Daher gilt $e(\mathfrak{Q}_N|\mathfrak{p}) = f(\mathfrak{Q}_N|\mathfrak{p}) = 1$ und die Zerlegungsgruppe $\mathcal{Z}(\mathfrak{Q}_N|\mathfrak{p})$ ist trivial (siehe Korollar (2.2),c)). Dann ist aber auch die Zerlegungsgruppe $\mathcal{Z}(\mathfrak{Q}|\mathfrak{P})$ trivial, denn

$$\sigma \in \mathcal{Z}(\mathfrak{Q}|\mathfrak{P}) \implies \sigma\,|_N \in \mathcal{Z}(\mathfrak{Q}_N|\mathfrak{p}) = \{\mathrm{id}\} \implies \sigma\,|_{NK} = \mathrm{id}\,.$$

Folglich ist $e(\mathfrak{Q}|\mathfrak{P}) = f(\mathfrak{Q}|\mathfrak{P}) = 1$ und $\mathfrak{P} \in S(L|K)$.

Anmerkung: Für den Beweis dieses Satzes genügt in (3.3) der Nachweis, daß $S(N|k)$ unendlich ist; und dazu wiederum genügt es zu wissen, daß alle Dedekindschen Zetafunktionen bei $s = 1$ einen Pol haben. Man käme sogar ohne analytische Fortsetzung aus und müßte nur wissen, daß die Zetafunktion $\zeta_K(\sigma)$ für $\sigma \to 1+$ $(\sigma \in \mathbb{R})$ unbeschränkt ist.

b. Dirichletsche L-Reihen

Wir betrachten nun wieder den Frobeniusautomorphismus in galoisschen Erweiterungen $N|k$. Durch die Zuordnung $\mathfrak{P} \mapsto F_{N|k}(\mathfrak{P})$ erhält man eine Abbildung $\mathcal{P}_N^{\mathrm{nr}} \to G(N|k) =: G$ von der Menge $\mathcal{P}_N^{\mathrm{nr}}$ der in $N|k$ unverzweigten Primideale von N in die Galoisgruppe von $N|k$, das sogenannte *Frobeniussymbol.* Da die gebrochenen Ideale eine freie abelsche Gruppe bilden mit den Primidealen als Basis, ist die von $\mathcal{P}_N^{\mathrm{nr}}$ erzeugte Gruppe $\mathcal{I}_N^{\mathrm{nr}}$ der gebrochenen Ideale, die prim sind zu den verzweigten Primidealen, ebenfalls frei mit $\mathcal{P}_N^{\mathrm{nr}}$ als Basis. Für *abelsche* Galoisgruppen G läßt sich deshalb diese Abbildung $\mathcal{P}_N^{\mathrm{nr}} \to G$ zu einem *Gruppenhomomorphismus* $\mathcal{I}_N^{\mathrm{nr}} \to G$ fortsetzen. Im abelschen Fall ist aber der Frobeniusautomorphismus $F_{N|k}(\mathfrak{P})$ bereits durch das unter $\mathfrak{P}$ liegende Primideal $\mathfrak{p}$ von k bestimmt, denn die verschiedenen $F_{N|k}(\mathfrak{P})$ sind in G konjugiert, im abelschen Fall also gleich. Fazit:

(3.5) Bemerkung: Ist $N|k$ eine abelsche Erweiterung (d. h. galoissch mit abelscher Galoisgruppe), $\mathfrak{m}$ ein ganzes Ideal von k, das von allen in N verzweigten Primidealen geteilt wird

(ein sog. *Erklärungsmodul* für N), so hat man einen wohldefinierten Gruppenhomomorphismus $F\colon \mathcal{I}_k^{\mathfrak{m}} \to G(N|k)$, von der Gruppe der zu $\mathfrak{m}$ teilerfremden gebrochenen Ideale (was heißt das?) in die Galoisgruppe. Dieser ist dadurch eindeutig bestimmt, daß er Primidealen $\mathfrak{p} \in \mathcal{I}_k^{\mathfrak{m}}$ gerade den Frobeniusautomorphismus $F_{N|k}(\mathfrak{P})$ zu einem beliebigen Primteiler $\mathfrak{P}$ von $\mathfrak{p}$ in N zuordnet.

Ein genaues Studium dieses Gruppenhomomorphismus $F_{N|k}$ führt zu den Hauptsätzen der sog. *Klassenkörpertheorie*. Die Klassenkörpertheorie ist — in heutiger Sprech- und Sichtweise— die Theorie der abelschen Erweiterungen von Zahl- (und anderen damit zusammenhängenden) Körpern. (siehe J.Neukirch: Class field theory, Springer 1986; für das Folgende speziell Ch. IV; §8.)

Die wichtigsten Ergebnisse:

1) Der oben konstruierte Gruppenhomomorphismus ist ein *Epi*morphismus.
2) Er faktorisiert über die sog. *Strahlklassengruppe* $\mathcal{I}_k^{\mathfrak{m}}/\mathcal{S}_k^{\mathfrak{m}}$, wobei

$$\mathcal{S}_k^{\mathfrak{m}} := \{aZ_k \mid a \equiv 1 \bmod \mathfrak{m}, a \text{ total-positiv}\}$$

   den *Strahl* modulo $\mathfrak{m}$ bezeichnet. Diese Strahlklassengruppe ist *endlich.*
3) Jede Zwischengruppe H zwischen $\mathcal{S}_k^{\mathfrak{m}}$ und $\mathcal{I}_k^{\mathfrak{m}}$ ist Kern des Frobeniussymbol $F_{N|k}$ für genau eine abelsche Erweiterung $N|k$, den sog. *Klassenkörper* zu H. Man erhält als wesentliches Resultat der Klassenkörpertheorie eine *vollständige* Beschreibung aller *abelschen* Erweiterungen von k bereits durch Bestimmungsstücke *im Grundkörper* k.

Der oben erwähnte Klassenkörper zu H besitzt eine Charakterisierung durch die Primidealzerlegung – dies war auch die ursprüngliche Weber'sche Definition: Der Klassenkörper zu H ist *die* galoissche Erweiterung von k, in der (bis auf die Primteiler von $\mathfrak{m}$) genau die Primideale $\mathfrak{p} \in H$ voll zerlegt sind. Die Einschränkung ist in Klammern gesetzt, weil sie entbehrlich wird, wenn man den Begriff des kleinsten Erklärungsmoduls (*Führer)* einführt. Dieser beruht darauf, solche Zwischengruppen H für verschiedene Erklärungsmoduln miteinander zu vergleichen, und sich so von der Willkür eines zusätzlichen Parameters $\mathfrak{m}$ zu befreien.

Daß zwischen dem Kern H des Frobeniussymbol $F_{N|k}$ und der Primzerlegung in $N|k$ ein Zusammenhang besteht, können wir bereits aus den Definitionen entnehmen (siehe Bem. 2.5): Ein Primideal $\mathfrak{p}$ von k gehört genau dann zum Kern von $F_{N|k}$, wenn es in $N|k$ voll zerlegt ist, also zu $S(N|k)$ gehört: $S(N|k) = \mathcal{P}_k \cap \operatorname{Ke} F_{N|k}$. Aus dem Satz von Bauer (3.4)) folgt also sofort die Weber'sche Beschreibung des Klassenkörpers, und sogar mehr: Der Klassenkörper ist die kleinste Erweiterung von k, in der höchstens die Primideale $\mathfrak{p} \in H$ einen Primteiler ersten Grades besitzen. Außerdem folgt aus $S(N|k) = \mathcal{P}_k \cap \operatorname{Ke} F_{N|k}$ gemäß Korollar (3.3), daß es unendlich viele Primideale $\mathfrak{p}$ von k gibt, deren Frobeniusautomorphismus gerade id_N ist; überdies ist ihre Dirichletdichte gerade $1/(N\colon k)$. Diese Tatsache ist ein sehr spezieller Fall des folgenden allgemeineren Resultats:

(3.6) Satz: (Dirichlet) *Zu jedem Automorphismus $\sigma \in G(N|k)$ einer abelschen Erweiterung $N|k$ gibt es unendlich viele Primideale von k, deren Frobeniusautomorphismus gerade σ ist; die Menge all dieser Primideale hat die Dirichletdichte $\frac{1}{(N:k)}$.*

Satz (3.6) bedeutet, daß jedes $\sigma \in G(N|k)$ nicht nur gemäß 1) ein Potenzprodukt von Frobeniusautomorphismen, sondern sogar selbst ein Frobeniusautomorphismus ist, und daß überdies die Frobeniusautomorphismen in G gleichverteilt liegen. Offenbar ist 1) eine Abschwächung von (3.6), wird jedoch im Beweis von (3.6) benutzt. Mittels 1) übersetzt sich (3.6) in folgende Aussage:

> Die Menge aller Primideale von k, die in einer festen Nebenklasse $\mathcal{K}$ des Kerns $H := \operatorname{Ke} F_{N|k}$ liegen, hat die Dirichletdichte $1/(\mathcal{I}_k^{\mathfrak{m}}\colon H)$ (unabhängig von $\mathcal{K}$). Dies bedeutet, daß sich die Primideale auf die Nebenklassen des Kerns gleichmäßig verteilen.

Zum Beweis dieser Tatsache benutzt man die Dirichletschen L-Funktionen $L(s,\chi)$, die Holomorphie ihres Logarithmus $\log L(s,\chi)$ bei $s = 1$ (für nicht-triviale Charaktere χ) und Grundtatsachen über Charaktere abelscher Gruppen.

[Siehe zu diesem Komplex etwa L. Goldstein: Analytic Number Theory, section 9-2; S. Lang: Algebraic Number Theory, VIII,§4; J. Neukirch: l.c., V, §§3,6.]

Definition: Dirichletsche L-Reihen
Sei $\mathfrak{m}$ ein ganzes Ideal von k (etwa ein Erklärungsmodul von $N|k$) und H eine Zwischengruppe zwischen dem Strahl $\mathcal{S}_k^{\mathfrak{m}}$ und $\mathcal{I}_k^{\mathfrak{m}}$ (etwa der Kern des Frobeniussymbols $F_{N|k}: \mathcal{I}_k^{\mathfrak{m}} \to G(N|k)$). Weiter sei $\mathcal{G} := \mathcal{I}_k^{\mathfrak{m}}/H$ die endliche Faktorgruppe und $\chi : \mathcal{G} \to \mathbb{C}^\times$ ein Gruppenhomomorphismus (ein Charakter von $\mathcal{G}$). Vermöge der natürlichen Abbildung $\mathcal{I}_k^{\mathfrak{m}} \to \mathcal{G}$ wird χ auch als Abbildung auf $\mathcal{I}_k^{\mathfrak{m}}$ aufgefaßt. Dann definiert man die *Dirichletsche L-Reihe* des Körpers k zum Charakter χ (und Erklärungsmodul $\mathfrak{m}$) durch

$$L_{k,\mathfrak{m}}(s,\chi) := \sum_{\substack{\mathfrak{A} \lhd Z_k \\ (\mathfrak{A},\mathfrak{m})=1}} \frac{\chi(\mathfrak{A})}{\mathcal{N}\mathfrak{A}^s} = \sum_{\mathcal{K}\in\mathcal{G}} \chi(\mathcal{K}) \sum_{\mathfrak{A}\in\mathcal{K}} \frac{1}{\mathcal{N}\mathfrak{A}^s} = \sum_{\mathcal{K}\in\mathcal{G}} \chi(\mathcal{K}) \cdot \zeta_{\mathcal{K}}(s)$$

mit den sog. *Klassen-Zetafunktionen*

$$\zeta_{\mathcal{K}}(s) := \sum_{\mathfrak{A}\in\mathcal{K}} \frac{1}{\mathcal{N}\mathfrak{A}^s}\,.$$

Wegen der Multiplikativität von χ hat man auch für die L-Funktionen ein Eulerprodukt

$$L_{\mathfrak{m}}(s,\chi) = \prod_{\substack{\mathfrak{p}\in\mathcal{P}_k \\ \mathfrak{p}\nmid\mathfrak{m}}} \frac{1}{1-\chi(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s}}\,.$$

Wie früher für Zetafunktionen erhält man jetzt für die L-Reihen:

$$\log L_{\mathfrak{m}}(s,\chi) \quad \text{und} \quad \sum_{\mathfrak{p}\nmid\mathfrak{m}} \frac{\chi(\mathfrak{p})}{\mathcal{N}\mathfrak{p}^s} = \sum_{\mathcal{K}\in\mathcal{G}} \chi(\mathcal{K}) \sum_{\mathfrak{p}\in\mathcal{K}} \frac{1}{\mathcal{N}\mathfrak{p}^s}$$

unterscheiden sich um eine im Bereich $\operatorname{Re} s > \frac{1}{2}$ holomorphe Funktion.
[Bezeichnung: $f \sim g \;:\Longleftrightarrow\; f-g$ holomorph bei $s=1$.] Also:

$$(*) \qquad \log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathcal{K}\in\mathcal{G}} \chi(\mathcal{K}) S(\mathcal{K},s)$$

mit

$$S(\mathcal{K},s) := \sum_{\mathfrak{p}\in\mathcal{K}} \mathcal{N}\mathfrak{p}^{-s}\,.$$

Benutzt man nun, daß für $\chi \neq 1$ die *Logarithmen* $\log L_{\mathfrak{m}}(s,\chi)$ *bei* $s=1$ *holomorph* sind, so folgt hieraus die Behauptung folgendermaßen:
Für eine feste Klasse $\mathcal{K}_0 \in \mathcal{G}$ multipliziere man nun $(*)$ mit $\chi(\mathcal{K}_0^{-1})$ und summiere auf ($\hat{\mathcal{G}}$ bezeichne die Charaktergruppe von $\mathcal{G}$):

$$(**) \qquad \sum_{\chi\in\hat{\mathcal{G}}} \chi(\mathcal{K}_0^{-1}) \log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathcal{K}\in\mathcal{G}} \sum_{\chi\in\hat{\mathcal{G}}} \chi(\mathcal{K}_0^{-1}\mathcal{K}) S(\mathcal{K},s).$$

Wir benutzen nun die folgende Tatsache über Charaktere abelscher Gruppen G:

$$(\mathrm{C1}) \qquad a \in G, a \neq 1 \Rightarrow \sum_{\chi\in\hat{G}} \chi(a) = 0$$

[Die Charaktere χ einer abelschen Gruppe G 'charakterisieren' die Elemente von G in dem Sinne:

$$a = b \iff \chi(a) = \chi(b) \text{ für alle } \chi \in \hat{G}\,.$$

Zu $a \neq 1$ gibt es also einen Charakter χ' mit $\chi'(a) \neq 1$. Also erhält man

$$\chi'(a) \cdot \sum_{\chi \in \hat{G}} \chi(a) = \sum_{\chi \in \hat{G}} \chi'\chi(a) = \sum_{\chi \in \hat{G}} \chi(a)\,.$$

Daher muß Behauptung (C1) gelten, da man sonst durch Kürzen einen Widerspruch erhielte.]

Völlig 'dual' zu (C1) (mit noch einfacherem Beweis) gilt

(C2) $$\chi \in \hat{G}, \chi \neq 1 \Rightarrow \sum_{a \in G} \chi(a) = 0\,.$$

Wegen (C1) und $\#\hat{\mathcal{G}} = \#\mathcal{G}$ reduziert sich die rechte Seite von $(**)$ auf den Term $\#\mathcal{G} \cdot S(\mathcal{K}_0, s)$, während links wegen der (im Moment vorausgesetzten) Holomorphie von $\log L_{\mathfrak{m}}(s, \chi)$ bei $s = 1$ für $\chi \neq 1$ lediglich $\log \zeta_{k,\mathfrak{m}}(s)$ verbleibt:

$$\log \zeta_{k,\mathfrak{m}}(s) \sim \#\mathcal{G} \cdot S(\mathcal{K}_0, s)\,.$$

[Dabei bedeutet der Index $\mathfrak{m}$, daß die Eulerfaktoren zu Primteilern von $\mathfrak{m}$ weggelassen werden.] Damit ergibt sich für die Dirichletdichten

$$1 = \#\mathcal{G} \cdot d(\{\mathfrak{p} \in \mathcal{P}_k \mid \mathfrak{p} \in \mathcal{K}_0\})\,,$$

wie behauptet.

Das Kernstück des Beweises des Dirichlet'schen Satzes ist also der Nachweis, daß

i) das Frobeniussymbol $F_{N|k}\colon \mathcal{I}_k^{\mathfrak{m}} \to G(N|k)$ surjektiv ist und

ii) alle Dirichletreihen $L_{\mathfrak{m}}(s, \chi)$ mit nicht-trivialem Charakter χ *bei* $s = 1$ *holomorph* sind und dort *nicht verschwinden.*

Die Holomorphie der L-Reihen gewinnt man durch Untersuchung der Klassen-Zetafunktionen: Für Untergruppen H von $\mathcal{I}_k^{\mathfrak{m}}$ (wie den Kern des Frobeniussymbols), die den Strahl $\mathcal{S}_k^{\mathfrak{m}}$ enthalten, setzen sich die Nebenklassen von H aus Strahlklassen (Nebenklassen bzgl. des Strahls) zusammen. Für die Klassen-Zetafunktionen zu Strahlklassen kann man nun (3.1) analog beweisen und erhält dann den folgenden

(3.1′) Satz: *Sei k ein algebraischer Zahlkörper, $\mathfrak{m}$ ein ganzes Ideal von k, H eine Zwischengruppe zwischen dem Strahl zu $\mathfrak{m}$ und der Gruppe $\mathcal{I}_k^{\mathfrak{m}}$ sowie $\mathcal{K}$ eine Nebenklasse von H. Dann ist die Klassen-Zetafunktion $\zeta_{\mathcal{K}}(s)$ analytisch fortsetzbar auf ganz $\mathbb{C}$ mit einzigem Pol bei $s = 1$. Dieser ist einfach und das Residuum bei $s = 1$ ist von der Klasse unabhängig.*

Für uns ist diese letzte Aussage besonders wichtig, denn dies hat zur Folge, daß sich für *nicht-triviale* Charaktere χ von $\mathcal{G}$ in der L-Reihe

$$L_{\mathfrak{m}}(s, \chi) = \sum_{\mathcal{K} \in \mathcal{G}} \chi(\mathcal{K}) \cdot \zeta_{\mathcal{K}}(s)$$

die Residuen bei $s = 1$ wegen (C2) aufheben und daher $L_{\mathfrak{m}}(s, \chi)$ eine ganze Funktion ist.

Damit haben die L-Reihen zu nichttrivialen Charakteren bei $s = 1$ keinen Pol. Daß sie dort aber auch keine Nullstelle haben, und daher auch die Logarithmen der L-Reihen dort holomorph sind, ergibt sich aus der folgenden Zerlegung der Zetafunktion des galoisschen Erweiterungskörpers N von k in L-Reihen *von* k. Zugleich kann damit unter Benutzung von (3.1) die Surjektivität des Frobeniussymbols $F_{N|k}$ bewiesen werden.

(3.7) Satz: *Sei $N|k$ eine abelsche Zahlkörpererweiterung, $\mathfrak{m}$ ein Erklärungsmodul für $N|k$, $H := \operatorname{Ke} F_{N|k} \subseteq \mathcal{I}_k^{\mathfrak{m}}$ der Kern des Frobeniussymbols und $\mathcal{G} := \mathcal{I}_k^{\mathfrak{m}}/H$ $(\hookrightarrow G(N|k))$ die Faktorgruppe. Schließlich sei $\hat{\mathcal{G}}$ die Gruppe der Charaktere von $\mathcal{G}$. Dann gilt:*

a) *$F_{N|k}\colon \mathcal{I}_k^{\mathfrak{m}} \to G(N|k)$ ist surjektiv.*

b) $\zeta_{N,\mathfrak{m}}(s) = \prod_{\chi\in\hat{\mathcal{G}}} L_{k,\mathfrak{m}}(s,\chi) = \zeta_{k,\mathfrak{m}}(s)\cdot\prod_{\chi\neq 1} L_{k,\mathfrak{m}}(s,\chi).$

Aus b) ergibt sich, daß der Quotient der beiden Zetafunktionen von N und k bei $s=1$ holomorph ist. (Die in (3.7), b) ausgeschlossenen endlich vielen Eulerfaktoren zu den Primteilern von $\mathfrak{m}$ sind bei $s=1$ holomorph mit Funktionswert $\neq 0$.) Da beide Zetafunktionen bei $s=1$ einen einfachen Pol haben (Satz (3.1)), ist der Wert dieses Quotienten bei $s=1$ nicht 0, also kann auch keine der L-Reihen bei $s=1$ verschwinden, und Satz (3.6) ist mittels (3.7) bewiesen.

Beweis von (3.7) aus (3.1): Wir setzen d als den Index von $\operatorname{Im} F_{N|k} = F_{N|k}(\mathcal{I}_k^{\mathfrak{m}})$ in $G(N|k)$ an und zeigen

b′) $$\zeta_{N,\mathfrak{m}}(s) = \Big(\zeta_{k,\mathfrak{m}}(s)\cdot\prod_{\chi\neq 1} L_{k,\mathfrak{m}}(s,\chi)\Big)^d .$$

Durch Vergleich der Polordnungen bei $s=1$ folgt $d=1$, und damit sowohl a) als auch b).
Zum Beweis von b′): Es ist

$$\prod_{\chi\in\hat{\mathcal{G}}} L_{\mathfrak{m}}(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}}\Big(\prod_{\chi\in\hat{\mathcal{G}}}(1-\chi(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s})\Big)^{-1} .$$

Wir zeigen nun

$$\prod_{\chi\in\hat{\mathcal{G}}}(1-\chi(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s}) = (1-\mathcal{N}\mathfrak{p}^{-fs})^{n/f} \text{ mit } n=\#\mathcal{G}, f=f_{N|k}(\mathfrak{p})\,.$$

Beweis: $\chi(\mathfrak{p})$ ist nur abhängig von der Restklasse $\bar{\mathfrak{p}}\in\mathcal{G}$ und dem eingeschränkten Charakter $\chi\,|_{\langle\bar{\mathfrak{p}}\rangle} =: \chi'$. Aus der Theorie der Charaktere endlicher abelscher Gruppen ist bekannt:
Jeder Charakter χ' von $\mathcal{G}' := \langle\bar{\mathfrak{p}}\rangle$ ist fortsetzbar zu einem Charakter von $\mathcal{G}$, und zwar auf genau $(\mathcal{G}:\mathcal{G}')$ viele Weisen. (Die Restriktionsabbildung $\hat{\mathcal{G}}\to\widehat{\mathcal{G}'}$ ist surjektiv, Gruppe und Charaktergruppe sind gleichmächtig.) Also erhält man

$$\prod_{\chi\in\hat{\mathcal{G}}}(1-\chi(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s}) = \prod_{\chi'\in\widehat{\mathcal{G}'}}(1-\chi'(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s})^{(\mathcal{G}:\mathcal{G}')} .$$

Es gilt $\#\mathcal{G}' = \operatorname{ord}\bar{\mathfrak{p}} = \operatorname{ord} F_{N|k}(\mathfrak{p}) = f_{N|k}(\mathfrak{p}) = f$ und daher $(\mathcal{G}:\mathcal{G}') = n/f$.
Die verschiedenen Charaktere der *zyklischen* Gruppe $\mathcal{G}' = \langle\bar{\mathfrak{p}}\rangle$ bilden $\bar{\mathfrak{p}}$ gerade auf die f-ten Einheitswurzeln ζ_f^i $(i=0,\dots,f-1)$ ab, also

$$\prod_{\chi'\in\widehat{\mathcal{G}'}}(1-\chi'(\bar{\mathfrak{p}})\mathcal{N}\mathfrak{p}^{-s}) = \prod_{i=0}^{f-1}(1-\zeta_f^i\mathcal{N}\mathfrak{p}^{-s}) = 1-\mathcal{N}\mathfrak{p}^{-fs} .$$

Die letzte Gleichung ergibt sich aus der Polynomidentität

$$Y^f-1 = \prod_{i=0}^{f-1}(Y-\zeta_f^i)$$

nach Einsetzen von $\mathcal{N}\mathfrak{p}^s$ und Division durch $\mathcal{N}\mathfrak{p}^{fs}$. Damit ist die Behauptung bewiesen.

Wegen $f = f_{N|k}(\mathfrak{p})$ ist natürlich die Anzahl der Primteiler $\mathfrak{P}$ von $\mathfrak{p}$ in N ($\mathfrak{p}$ ist in N unverzweigt)

$$r_{N|k}(\mathfrak{p}) = \frac{(N:k)}{f} = \frac{nd}{f} .$$

Also

$$(1-\mathcal{N}\mathfrak{p}^{-fs})^{nd/f}=\prod_{\mathfrak{P}|\mathfrak{p}}(1-\mathcal{N}\mathfrak{P}^{-s})\,,$$

womit b′) aus der bewiesenen Behauptung folgt.

c. Der Čebotarevsche Dichtigkeitssatz

Aufgrund des Dirichletschen Satzes (3.6) erhält man für abelsche Erweiterungen das folgende gruppentheoretische Kriterium:

> Genau dann gibt es Primideale von k, die in einer abelschen Erweiterung $N|k$ vom Grade n in $\frac{n}{f}$ Primfaktoren vom Grade f zerfallen, wenn es in der Galoisgruppe $G(N|k)$ ein Element der Ordnung f gibt.

Beweis als Übung. Allgemeinere Aussagen werden noch folgen. Dazu wollen wir das 'abelsche Resultat' (3.6) ausdehnen auf beliebige galoissche Erweiterungen.

Ist $N|k$ galoissch, so bilden die Frobeniusautomorphismen $F_{N|k}(\mathfrak{P})$ für verschiedene Primteiler $\mathfrak{P}$ eines festen Primideals $\mathfrak{p}$ von k eine Konjugationsklasse in G, die mit $F_{N|k}(\mathfrak{p})$ bezeichnet wird. [Diese Bezeichnung ist konsistent mit der im abelschen Fall benutzten, denn im abelschen Fall sind die Konjugationsklassen einelementig, können also kanonisch mit den Gruppenelementen identifiziert werden.]
Diese Zuordnung $\mathcal{P}_k^{\mathrm{nr}}\to[G(N|k)]$ von den in $N|k$ unverzweigten Primidealen in die Menge $[G]$ der Konjugationsklassen der Galoisgruppe G wird auch *Artinsymbol* für $N|k$ genannt. Aus (3.6) kann man nun leicht das folgende, für uns entscheidende Resultat ableiten:

(3.8) Satz: (Čebotarevscher Dichtigkeitssatz) *Sei $N|k$ eine galoissche Zahlkörpererweiterung mit Galoisgruppe G und C eine beliebige Konjugationsklasse von G. Dann hat die Menge*

$$\{\mathfrak{p}\in\mathcal{P}_k\mid F_{N|k}(\mathfrak{p})=C\}$$

die Dirichletdichte

$$\frac{\#C}{\#G}\,,$$

ist insbesondere unendlich.

Anmerkungen: 1) Der Quotient $\frac{\#C}{\#G}$ sollte angesehen werden als die Wahrscheinlichkeit dafür, daß ein beliebiges Gruppenelement $\sigma\in G$ in C liegt. Nach dem Čebotarev'schen Dichtigkeitssatz ist dies dann zugleich die Wahrscheinlichkeit dafür, daß ein beliebiges Primideal von k einen Primteiler in N hat, dessen Frobeniussymbol in C liegt.
2) (3.6) ist offenbar der abelsche Spezialfall von (3.8), wird jedoch zum Beweis benutzt.
3) (Übung) Die Mengen $\{\mathfrak{P}\in\mathcal{P}_N\mid F_{N|k}(\mathfrak{P})=\sigma\}$ sind für alle $\sigma\in G$ ebenfalls unendlich; ihre Dirichletdichte ist aber 0 für $\sigma\neq\mathrm{id}$.

Beweis von Satz (3.8) mittels (3.6): Sei $\sigma\in C$ und $f:=\operatorname{ord}\sigma$. Weiter sei F der Fixkörper von σ, also $N|F$ zyklisch vom Grad f. Man wendet nun (3.6) auf diese Erweiterung $N|F$ und $\sigma\in G(N|F)$ an und erhält: Die Menge $S_\sigma:=\{\mathfrak{p}\in\mathcal{P}_F\mid F_{N|F}(\mathfrak{p})=\sigma\}$ hat die Dirichletdichte $1/f$. Dann hat aber auch $S_\sigma^1:=\{\mathfrak{p}\in S_\sigma\mid f_{F|k}(\mathfrak{p})=1\}$ die Dichte $1/f$ (siehe Abschnitt a., Anm. 2)). Nun ist aber die uns interessierende Menge

$$S_C:=\{\mathfrak{p}\in\mathcal{P}_k\mid F_{N|k}(\mathfrak{p})=C\}$$

genau die Menge der Primideale, die in F einen Primteiler in S_σ^1 haben bzw. in N einen Primteiler

$\mathfrak{P}$ besitzen mit $F_{N|k}(\mathfrak{P}) = \sigma$:

$$\begin{aligned}
\mathfrak{p} \in S_C &\iff \mathfrak{p} \text{ hat einen Primteiler } \mathfrak{P} \text{ in } N \text{mit } F_{N|k}(\mathfrak{P}) = \sigma \\
&\iff F_{N|F}(\mathfrak{P}) = \sigma \text{ und } f_{F|k}(\mathfrak{P} \cap F) = 1 \quad \text{für ein } \mathfrak{P} \in \mathcal{P}_N, \mathfrak{P}|\mathfrak{p} \\
&\quad \left[\begin{array}{l} \Leftarrow\colon F_{N|F}(\mathfrak{P}) = (F_{N|k}(\mathfrak{P}))^{f_{F|k}(\mathfrak{P}\cap F)} \quad \text{(gemäß (2.6),b)} \\ \Rightarrow\colon \sigma = F_{N|k}(\mathfrak{P}) \in G(N|F) \Rightarrow \sigma = F_{N|F}(\mathfrak{P}), \\ \qquad \text{denn } \langle\overline{\sigma}\rangle = G(\bar{N}|\bar{k}) \subseteq G(\bar{N}|\bar{F}) \Rightarrow \bar{F} = \bar{\cdot} \end{array} \right. \\
&\iff \mathfrak{p} \text{ hat einen Primteiler } \mathfrak{Q} \text{ in } F \text{mit} \mathfrak{Q} \in S_\sigma^1 \,.
\end{aligned}$$

Daraus ergibt sich also (mit $S := S_C$ und $S' := S_\sigma^1$):

$$\sum_{\mathfrak{Q}\in S'} \mathcal{N}\mathfrak{Q}^{-s} = \sum_{\mathfrak{p}\in S} \sum_{\substack{\mathfrak{Q}\in S' \\ \mathfrak{Q}|\mathfrak{p}}} \mathcal{N}\mathfrak{Q}^{-s} = \sum_{\mathfrak{p}\in S} r'_\mathfrak{p} \cdot \mathcal{N}\mathfrak{p}^{-s}$$

mit $r'_\mathfrak{p} := \#\{\mathfrak{Q} \in S' \mid \mathfrak{Q}|\mathfrak{p}\}$.

$$\textit{Behauptung:} \quad r'_\mathfrak{p} = \frac{\#G}{\#C \cdot f} \quad \text{für alle } \mathfrak{p} \in S\,.$$

Ist dies gezeigt, so folgt unmittelbar

$$\frac{1}{f} = d(S') = r'_\mathfrak{p} \cdot d(S) = \frac{1}{f} \cdot \frac{\#G}{\#C} \cdot d(S)\,,$$

und damit die Behauptung des Čebotarevschen Dichtigkeitssatzes.

Zunächst ist

$$r'_\mathfrak{p} = \#\{\mathfrak{P} \in \mathcal{P}_N \mid \mathfrak{P}|\mathfrak{p} \text{ und} F_{N|k}(\mathfrak{P}) = \sigma\}\,,$$

denn für $\mathfrak{Q} \in S'$ und $\mathfrak{P} \in \mathcal{P}_N$, $\mathfrak{P}|\mathfrak{Q}$ ist $F_{N|F}(\mathfrak{P}) = \sigma$, also $f_{N|F}(\mathfrak{P}) = \operatorname{ord}\sigma = f = (N\colon F)$ und $\mathfrak{P}$ daher das einzige Primideal von N über $\mathfrak{Q}$. Da für $\mathfrak{p} \in S$ $r'_\mathfrak{p} \neq 0$ ist, kann man ein festes $\mathfrak{P} \in \mathcal{P}_N$ mit $\mathfrak{P}|\mathfrak{p}$ und $F_{N|k}(\mathfrak{P}) = \sigma$ wählen und es gilt:

$$\begin{aligned}
r'_\mathfrak{p} &= \#\{\delta\mathfrak{P} \mid \delta \in G\,,\, F_{N|k}(\delta\mathfrak{P}) = \sigma\} \\
&= \#\{\delta\mathfrak{P} \mid \delta \in G\,,\, \delta\sigma\delta^{-1} = \sigma\} \\
&= \#\{\delta\mathfrak{P} \mid \delta \in \operatorname{Zentr}_G(\sigma)\} \\
&= (\operatorname{Zentr}_G(\sigma)\colon \operatorname{Zentr}_G(\sigma) \cap \mathcal{Z}(\mathfrak{P}|\mathfrak{p})) \qquad \text{(Bahngleichung)}
\end{aligned}$$

Nun ist $F_{N|k}(\mathfrak{P}) = \sigma$, also $\mathcal{Z}(\mathfrak{P}|\mathfrak{p}) = \langle\sigma\rangle \subseteq \operatorname{Zentr}_G(\sigma)$ und daher

$$r'_\mathfrak{p} = \frac{\#\operatorname{Zentr}_G(\sigma)}{\#\langle\sigma\rangle} = \frac{1}{f} \cdot \frac{\#G}{\#C}\,,$$

denn G operiert auf sich selbst durch Konjugation, die Bahn von σ unter dieser Operation ist gerade die Konjugationsklasse $C = C(\sigma)$ von σ, während die Fixgruppe von σ bzgl. dieser Operation offenbar der Zentralisator von σ in G ist. Damit ergibt die Bahngleichung bzgl. dieser Operation gerade $\#C(\sigma) = (G\colon \operatorname{Zentr}_G(\sigma))$, wie oben behauptet.

Kombiniert man nun die gruppentheoretischen Kriterien aus Abschnitt 2.c. mit dem Čebotarev'schen Dichtigkeitssatz, so kommt man für eine beliebige Erweiterung $K|k$ zu einer gruppentheoretischen Beschreibung der möglichen Zerlegungstypen:

(3.9) Korollar: *Sei $K|k$ eine Zahlkörpererweiterung, $N|k$ eine galoissche Erweiterung mit $N \supseteq K$. Sei $U = G(N|K)$ die Fixgruppe von K in der Galoisgruppe $G = G(N|k)$ und P_U die dazu gehörige Permutationsdarstellung. Dann sind die möglichen Typen der Primzerlegung in $N|k$ genau die möglichen Zyklentypen der Automorphismen $\sigma \in G$ bzgl. P_U.*
Genauer bedeutet dies für jede Sequenz $A = (f_1, \ldots, f_r)$ natürlicher Zahlen:

Es gibt unverzweigte Primideale in k, die in K den Zerlegungstyp A haben

$\iff$ *es gibt Automorphismen $\sigma \in G$, die bzgl. P_U den Zyklentyp A haben.*

Dieses Korollar folgt unmittelbar aus Satz (2.7), weil nach dem Čebotarevschen Dichtigkeitssatz jeder Galoisautomorphismus $\sigma \in G$ ein Frobeniusautomorphismus ist.

§4 Arithmetische Ähnlichkeiten

a. Kronecker-Äquivalenz

Wir wollen nun Zahlkörpererweiterungen studieren, die sich in Bezug auf die Primzerlegung 'ähnlich' verhalten. Etwa im Satz von Bauer (3.4)haben wir gesehen, daß zwei galoissche Erweiterungen $N|k, N'|k$ übereinstimmen, wenn die Mengen der voll-zerlegten Primideale übereinstimmen: $S(N|k) \doteq S(N'|k)$. Da für galoissche Erweiterungen $N|k$ die Beziehung $S(N|k) \doteq D(N|k)$ gilt, bieten sich nun zwei[2)] Möglichkeiten an, dieses Resultat auf beliebige Zahlkörpererweiterungen $K|k, K'|k$ auszudehnen: Man untersucht,
1) wann $S(K|k) \doteq S(K'|k)$, bzw. 2) wann $D(K|k) \doteq D(K'|k)$ gilt.

(4.1) Proposition: *Seien $K|k$ und $K'|k$ zwei beliebige Zahlkörpererweiterungen. Dann sind äquivalent:*

i) $S(K|k) \doteq S(K'|k)$.

ii) *K und K' haben über k dieselbe galoissche Hülle.*

Beweis: Diese Proposition ist ein Korollar zum Satz von Bauer (3.4), denn wir zeigen: Ist N die galoissche Hülle von $K|k$, so gilt:

$$S(K|k) \doteq S(N|k)\,.$$

Zum Beweis benutzen wir Satz (2.7). Sei U die Fixgruppe von K in $G := G(N|k)$ und für ein in N unverzweigtes Primideal $\mathfrak{p}$ von k sei $F := F_{N|k}(\mathfrak{P})$ der Frobeniusautomorphismus zu einem Primteiler $\mathfrak{P}$ von $\mathfrak{p}$ in N. Demzufolge ist $\mathfrak{p} \in \mathcal{P}_k$ in K voll zerlegt, wenn $P_U(F)$ den Zyklentyp $\underbrace{(1, \ldots, 1)}_{(K:k)}$ hat. Dies bedeutet aber nichts anderes als $P_U(F) = \mathrm{id}_{G/U}$ bzw.

$$F \in \operatorname{Ke} P_U = \bigcap_{\sigma \in G} U^\sigma = \{\mathrm{id}_N\}\,,$$

denn nach Definition ist N die kleinste galoissche Erweiterung von k, die K umfaßt, also ist die Fixgruppe $\{\mathrm{id}_N\}$ von N in G nichts anderes als der größte in U enthaltene Normalteiler von G; dies ist offenbar $\bigcap_{\sigma \in G} U^\sigma$. $F = \mathrm{id}_N$ ist aber gleichbedeutend mit $\mathfrak{p} \in S(N|k)$.

Die vollzerlegten Primideale können also nicht zur Charakterisierung beliebiger Zahlkörpererweiterungen benutzt werden. Wir betrachten nun die zweite mögliche Ausdehnung des Bauerschen Satzes. Wir definieren:

(4.2) Definition: (Jehne 1974) Zwei Zahlkörpererweiterungen $K|k$ und $K'|k$ heißen *Kronecker-äquivalent* über k genau dann, wenn ihre Kroneckermengen $D(K|k)$ und $D(K'|k)$ bis auf eventuell endlich viele Ausnahmen übereinstimmen:

$$K \sim_k K' \iff D(K|k) \doteq D(K'|k)\,.$$

Wieder benutzen wir Satz (2.7), um eine gruppentheoretische Beschreibung der Kronecker-Äquivalenz zu erhalten.

[2)] Siehe aber auch Abschnitt 5., Definition (4.2′).

(4.3) Satz: *Seien $K|k$ und $K'|k$ zwei Zahlkörpererweiterungen, $N|k$ eine galoissche Erweiterung von k, die K und K' umfaßt. In der Galoisgruppe $G := G(N|k)$ seien U bzw. U' die Fixgruppen von K bzw. K'. Dann gilt*

a) $$D(K|k) \dot{\subseteq} D(K'|k) \iff U^G := \bigcup_{\sigma \in G} U^\sigma \subseteq U'^G ,$$

also insbesondere

$$K \sim_k K' \iff U^G = U'^G.$$

b) Die Kroneckermenge $D(K|k)$ von K hat in $\mathcal{P}_k$ die Dirichletdichte $\frac{\#U^G}{\#G}$.

Dieser Satz umfaßt den Satz von Bauer, denn ist in a) $K'|k$ *galoissch,* so ist U' ein Normalteiler in G, also wegen $U \subseteq U^G$ und $U'^G = U'$ sind die Aussagen von a) dann äquivalent zu $U \subseteq U'$ bzw. $K \supseteq K'$.

Der *Beweis* von (4.3) beruht auf dem Čebotarevschen Dichtigkeitssatz und der folgenden sich aus Satz (2.7) ableitenden Tatsache:

$(*)$ $$D(K|k) \doteq \{\mathfrak{p} \in \mathcal{P}_k \mid F_{N|k}(\mathfrak{P}) \in U^G \text{ für ein (jedes) } \mathfrak{P}|\mathfrak{p}\}$$

Sei für ein in N unverzweigtes Primideal $\mathfrak{p} \in \mathcal{P}_k$ jeweils $\mathfrak{P}$ ein festgewählter Primteiler in $\mathcal{P}_N$. Nach Satz (2.7) hat $\mathfrak{p}$ einen Primteiler ersten Grades in K genau dann, wenn $P_U(F_{N|k}(\mathfrak{P}))$ wenigstens einen Zyklus der Länge 1, d. h. einen Fixpunkt hat. Nun ist U^σ gerade die Fixgruppe von $U\sigma$, also U^G genau die Menge der Elemente von G, die bzgl. P_U einen Fixpunkt haben.
ad a): Gemäß $(*)$ folgt "$\Leftarrow$", mit dem Čebotarevschen Dichtigkeitssatz, aber auch umgekehrt "$\Rightarrow$", denn wäre $\sigma \in U^G \setminus U'^G$, so existierten unendlich viele (in N unverzweigte) $\mathfrak{p} \in \mathcal{P}_k$ mit $F_{N|k}(\mathfrak{P}) = \sigma$. Gemäß $(*)$ lägen diese Primideale $\mathfrak{p}$ in $D(K|k)$, aber nicht in $D(K'|k)$, im Widerspruch zur Voraussetzung.
b) ist eine unmittelbare Folge von $(*)$ und Čebotarevschem Dichtigkeitssatz.

Mit dieser gruppentheoretischen Beschreibung der Kronecker-Äquivalenz lassen sich leicht Beispiele von über k nicht konjugierten, Kronecker-äquivalenten Körpererweiterungen von k konstruieren:

(4.4) Gegenbeispiele:

1) (Gaßmann 1926) Man betrachte in der symmetrischen Gruppe $\mathcal{S}_6$ von 6 Ziffern die folgenden Untergruppen:

$$U := \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \text{ , die Kleinsche Vierergruppe,}$$
$$U' := \{\mathrm{id}, (12)(34), (12)(56), (34)(56)\}.$$

Beide Gruppen sind in $\mathcal{S}_6$ elementweise konjugiert, aber nicht konjugiert.

[Übung: Bestimmen Sie alle weiteren zu U elementweise konjugierten $V \leq \mathcal{S}_6$.]

2) (Schinzel-Zassenhaus 1965) Man betrachte in der alternierenden Gruppe $\mathcal{A}_4$ von der Ordnung 12 die Kleinsche Vierergruppe $\mathcal{V}_4$ und eine beliebige der Untergruppen $U \subset \mathcal{V}_4$ von der Ordnung 2:

$$U = \{\mathrm{id}, (12)(34)\} \subset \mathcal{V}_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}.$$

Dann sind U und $\mathcal{V}_4$ elementweise in $\mathcal{A}_4$ konjugiert, aber ganz offenbar nicht konjugiert, da von unterschiedlicher Ordnung.

Körpertheoretisch formuliert bedeutet dies

1) In jeder $\mathcal{S}_6$-Erweiterung $N|k$ (vom Grad 720) gibt es über k Kronecker-äquivalente, nicht konjugierte Körpererweiterungen $K_i|k$ (i=0,1,2) mit K_0 vom Grad 360 und K_j (j=1,2) vom Grad 180 über k.

2) In jeder $\mathcal{A}_4$-Erweiterung $N|k$ gibt es einen zyklisch-kubischen Körper L und eine quadratische Erweiterung K von L (also vom Grade 6 über k), die über k Kronecker-äquivalent, aber offenbar nicht konjugiert sind.

Beweise: Wir erinnern an folgende Formel für die Konjugation von Zyklen:

$$a_1, \ldots, a_r \in \{1, \ldots, n\}, \sigma \in \mathcal{S}_n \implies \sigma \circ (a_1, \ldots, a_r) \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_r)) .$$

Aufgrund dieser Beziehung sind in $\mathcal{S}_n$ zwei Permutationen genau dann konjugiert, wenn sie denselben Zyklentyp haben.

a) ist damit dann klar. Daß U und U' nicht konjugiert sind, ergibt sich einfach aus der Tatsache, daß U Fixpunkte hat, U' aber nicht.

b) Offenbar ist $U^{\mathcal{S}_4} = {\mathcal{V}_4}^{\mathcal{S}_4}$. Es gilt aber sogar $U^{\mathcal{A}_4} = {\mathcal{V}_4}^{\mathcal{A}_4} = \mathcal{V}_4$: Die zweite Gleichheit ist die Normalteilereigenschaft von $\mathcal{V}_4$ in $\mathcal{A}_4$. Sei nun $(ab)(cd) \in \mathcal{V}_4$ und $\sigma \in \mathcal{S}_4$ mit $(\,(12)(34)\,)^\sigma = (ab)(cd)$. Ist σ selbst nicht in $\mathcal{A}_4$, so ist $\sigma \circ (ab)$ in $\mathcal{A}_4$ und

$$(\,(12)(34)\,)^{\sigma\circ(ab)} = (\,(ab)(cd)\,)^{(ab)} = (ab)(cd) .$$

Anmerkung: (4.4),c) liefert nur bedingt Beispiele für Kronecker-äquivalente, nicht konjugierte Zahlkörpererweiterungen. Man benötigt nämlich die Existenz von Galois-Erweiterungen $N|k$ mit Gruppe $\mathcal{S}_6$ bzw. $\mathcal{A}_4$. Diese Frage nach der Existenz von Galoiserweiterungen eines festen Grundkörpers k mit vorgegebener Galoisgruppe nennt man das *Umkehrproblem* der Galoistheorie.
Hier nur ganz kurz folgende Bemerkungen:

1) $\mathcal{S}_n$ ist Galoisgruppe über k für alle n; dies ist sogar – in einem zu präzisierenden Sinne – der Regelfall (v.d.Waerden).

2) Alle alternierenden Gruppen $\mathcal{A}_n$ sind Galoisgruppen (Hilbert, Schur,...).

3) Alle auflösbaren Gruppen sind Galoisgruppen (Šafarevič 1954).

4) Viele einfache Gruppen sind Galoisgruppen, z.B. das sog. *Monster* (Matzat et.al.).

5) Man vermutet, daß alle endlichen Gruppen Galoisgruppen über $\mathbb{Q}$ sind.

Wir wollen dieses Problem im Folgenden beiseite lassen, und die jeweils benutzten Resultate lediglich zur Kenntnis nehmen.

Diese Beispiele zeigen, daß Kronecker-äquivalente Körper nicht notwendig (über dem Grundkörper k) konjugiert sind, ja daß sie nicht einmal denselben Grad über k haben, und daß echt ineinander enthaltene Kronecker-äquivalente Körper existieren.

b. Arithmetische Äquivalenz

Nachdem offenbar $D(K|k) \doteq D(K'|k)$ eine zu schwache Forderung ist, wollen wir nun die vollständige Übereinstimmung der *Zerlegungsgesetze* untersuchen:

(4.5) Definition: Zwei endliche Erweiterungskörper K, K' eines Zahlkörpers k sollen *arithmetisch äquivalent über* k heißen (in Zeichen: $K \approx_k K'$), wenn für alle $r \in \mathbb{N}_+$ und $A = (f_1, \ldots, f_r) \in \mathbb{N}^r$ die Mengen $P_A(K|k)$ und $P_A(K'|k)$ der Primideale vom Zerlegungstyp A (bis auf eventuell endlich viele Ausnahmen) übereinstimmen. Explizit setzen wir

$$P_A(K|k) := \{\mathfrak{p} \in \mathcal{P}_k \mid \mathfrak{p} \text{ hat in } K \text{den Zerlegungstyp } A\}$$

und

$$K \approx_k K' :\Longleftrightarrow P_A(K|k) \doteq P_A(K'|k) \text{ für alle } A\,.$$

Aufgrund der gruppentheoretischen Beschreibung des Zerlegungsverhaltens (verweis2.7Satz (2.7)) kann man die arithmetische Äquivalenz sofort gruppentheoretisch charakterisieren durch die Tatsache:
Alle Gruppenelemente $\sigma \in G$ haben bzgl. P_U und $P_{U'}$ denselben Zyklentyp.
[Dabei sind U und U' die Fixgruppen von K bzw. K' in der Galoisgruppe G einer K und K' umfassenden galoisschen Erweiterung $N|k$.]
Dies kann man mit Hilfe des zugehörigen *Permutationscharakters* beschreiben: Für eine Permutationsdarstellung $P\colon G \longrightarrow \mathcal{S}_n$ definiert man den zugehörigen Permutationscharakter Φ durch

$$\Phi(s) := \#\mathrm{Fix}(P(s)) \quad (\text{Anzahl der Fixpunkte von } P(s))\,.$$

[$\Phi(s)$ kann auch beschrieben werden als die Spur der Permutationsmatrix zu $P(s)$.] Es gilt:

(4.6) Satz: *Seien K, K' Zahlkörpererweiterungen von k, $N|k$ eine Galoiserweiterung, die K und K' umfaßt. U bzw. U' seien die Fixgruppen von K bzw. K' in der Galoisgruppe $G := G(N|k)$. Dann sind äquivalent:*

i) K und K' sind über k arithmetisch äquivalent.

ii) Für alle $\sigma \in G$ haben $P_U(\sigma)$ und $P_{U'}(\sigma)$ denselben Zyklentyp.

iii) Die Permutationscharaktere Φ_U, $\Phi_{U'}$ von P_U bzw. $P_{U'}$ stimmen überein:

$$\Phi_U = \Phi_{U'}\,.$$

iv) Alle Konjugationsklassen $C(\sigma)$ von $\sigma \in G$ schneiden U und U' in gleichviel Elementen:

$$\#(C(\sigma) \cap U) = \#(C(\sigma) \cap U') \quad \text{für alle } \sigma \in G\,.$$

Beweis: i)⇔ii) folgt aus Satz (2.7) und dem Čebotarevschen Dichtigkeitssatz (3.8). ii)⇒iii) ist klar, denn die Anzahl der Fixpunkte von $P_U(\sigma)$ ist die Zahl der Zyklen der Länge 1.
iii)⇒ii): Wir berechnen den Zyklentyp von $P_U(\sigma)$ aus dem Permutationscharakter Φ_U, bzw. genauer aus den Fixpunktanzahlen der Potenzen $P_U(\sigma^m)$. Dies ist eine von der Permutationsdarstellung P_U unabhängige Aussage über Permutationen in $\mathcal{S}_n$. Sei daher für den Rest des Beweises dieser Implikation σ eine beliebige Permutation in $\mathcal{S}_n$ und

$$\sigma = \prod_{i=1}^{n} \prod_{j=1}^{r_i} \sigma_{ij}$$

die Zyklenzerlegung, wobei die $\sigma_{ij} = (a_1, \ldots, a_i)$ Zyklen der Länge i seien. [Die Abhängigkeit der a_ν von i, j ist in der Notation unterdrückt.] Für alle $m \in \mathbb{N}$ ist dann σ^m das Produkt der σ_{ij}^m und Fixpunkte von σ^m sind gerade die Fixpunkte der Einschränkungen

$$\sigma_{ij}^m \,|_{\{a_1,\ldots,a_i\}}\,.$$

Für die Anzahl $\Phi(\sigma^m)$ der Fixpunkte von σ^m ergibt sich so

$$\Phi(\sigma^m) = \sum_{ij} \Phi(\sigma_{ij}^m \,|_{\{a_1,\ldots,a_i\}})\,. \tag{1}$$

Nun gilt für einen Zyklus $\sigma_{ij} = (a_1, \ldots, a_i)$ der Länge i:

$$\sigma_{ij}^m \text{ ist auf } \{a_1, \ldots, a_i\} \begin{cases} \text{die Identität} & \text{für } i \mid m \\ \text{fixpunktfrei} & \text{für } i \nmid m. \end{cases} \tag{2}$$

Hat nämlich σ_{ij}^m einen Fixpunkt, o. E. etwa a_1, also $\sigma_{ij}^m(a_1) = a_1$, so ist die Länge der Bahn von a_1 unter $\langle\sigma_{ij}\rangle$ ein Teiler von m, also liegt der erste Fall $i|m$ vor und σ_{ij}^m ist offenbar die Identität. Aus (1) und (2) ergibt sich also

$$\Phi(\sigma^m) = \sum_{i|m} r_i \cdot i = \sum_{\substack{i|m \\ i\neq m}} r_i \cdot i + r_m \cdot m\,.$$

Damit lassen sich offenbar die Größen r_m rekursiv aus den Werten $\Phi(\sigma^m)$, d. h. aus den Fixpunktanzahlen der Potenzen σ^m berechnen. Nun war definitionsgemäß r_i die Zahl der Zyklen der Länge i in σ, so daß iii)⇒ii) bewiesen ist.

iii)⇔iv) ergibt sich aus der folgenden expliziten Formel für den Permutationscharakter Φ_U von G:

$$\Phi_U(\sigma) = \#\,(C(\sigma)\cap U)\cdot\frac{\#\,\mathrm{Zentr}_G(\sigma)}{\#\,U} \quad \text{für alle } \sigma\in G\,. \tag{3}$$

Aus iii) folgt zunächst $(G\colon U) = \Phi_U(1) = \Phi_{U'}(1) = (G\colon U')$, also $\#\,U = \#\,U'$ und daher mit (3) die Behauptung iv). Umgekehrt schließt man genauso, denn auch aus iv) folgt $\#\,U = \#\,U'$. Es bleibt also (3) zu zeigen.
Es gilt für alle $\sigma\in G$:

$$\Phi_U(\sigma) = \#\,\{U\tau \mid U\tau\sigma = U\tau\} = \#\,\{U\tau \mid \tau\sigma\tau^{-1}\in U\} = \frac{1}{\#\,U}\cdot\#\,\{\tau \mid \tau\sigma\tau^{-1}\in U\}\,.$$

Die letzte Gleichung gilt, da $\{\tau \mid \tau\sigma\tau^{-1}\in U\}$ aus vollen Linksnebenklassen von U besteht. Es gilt nun weiter

$$\{\tau \mid \tau\sigma\tau^{-1}\in U\} = \dot{\bigcup_{u\in U}}\{\tau \mid \tau\sigma\tau^{-1} = u\} = \dot{\bigcup_{u\in C(\sigma)\cap U}}\{\tau \mid \tau\sigma\tau^{-1} = u\}\,,$$

wegen $\{\tau \mid \tau\sigma\tau^{-1} = u\} \neq \emptyset$ genau für die $u\in C(\sigma)$. Wählt man nun für $u\in C(\sigma)\cap U$ ein $\tau_0\in G$ mit $\tau_0\sigma\tau_0^{-1} = u$, so folgt

$$\{\tau \mid \tau\sigma\tau^{-1} = u\} = \{\tau \mid \tau\sigma\tau^{-1} = \tau_0\sigma\tau_0^{-1}\} = \tau_0\mathrm{Zentr}_G(\sigma)\,.$$

Zählt man nun zusammen, so erhält man die Behauptung (3).

Aus diesem Satz, insbesondere Kriterium iv) entnehmen wir sofort folgendes

(4.7) Gegenbeispiel: Es gibt Zahlkörpererweiterungen $K_1|k$, $K_2|k$ vom Grade 180, die arithmetisch äquivalent sind, ohne über k konjugiert zu sein, nämlich die schon in (4.4),a) konstruierten.

Zum *Beweis* haben wir lediglich zu bemerken, daß die beiden in (4.4), a) angegebenen Untergruppen U, U' von $\mathcal{S}_6$ neben der Identität jeweils 3 Doppeltranspositionen, also von jedem Zyklentyp gleich viele Elemente enthalten. Dies bedeutet, daß U und U' in $G = \mathcal{S}_6$ die Bedingung iv) von Satz (4.6) erfüllen: Wir wollen dann U und U' *G-äquivalent* (oder auch *Gaßmann-äquivalent)* nennen.
[Wir erinnern daran, daß $\mathcal{S}_6$ Galoisgruppe über k ist und daher auch die angegebenen Körper existieren.]

Nachdem man nun überhaupt arithmetisch äquivalente, nicht konjugierte Zahlkörper gefunden hat, stellt sich wie bei der Kronecker-Äquivalenz die Frage, ob es auch einfachere Gegenbeispiele gibt. Dies ist auch der Fall:

(4.8) Beispiele: a) (Schinzel) $\mathbb{Q}(\sqrt[8]{3})$ und $\mathbb{Q}(\sqrt[8]{48}) = \mathbb{Q}(\sqrt[8]{3}\cdot\sqrt{2})$ sind über $\mathbb{Q}$ arithmetisch äquivalent, aber nicht konjugiert.
b) (Trinks 1969) Die Stammkörper der beiden irreduziblen Polynome $X^7 - 7X + 3$ und $X^7 +$

$14X^4 - 42X^2 - 21X + 9$ vom Grade 7 sind arithmetisch äquivalent, aber nicht konjugiert über $\mathbb{Q}$.
Statt eines Beweises nur folgende
Anmerkungen:
a) Die galoissche Hülle beider Körper ist der Körper $N = \mathbb{Q}(\sqrt[8]{3}, \zeta_8)$ vom Grade 32 mit der Galoisgruppe $G = \mathrm{Aff}(1, 8)$, der Gruppe der affinen Abbildungen von $\mathbb{Z}/8\mathbb{Z}$:

$$G = \{ax + b \mid b \in \mathbb{Z}/8\mathbb{Z}\,,\ a \in (\mathbb{Z}/8\mathbb{Z})^\times\}$$

mit $x = \mathrm{id}_{\mathbb{Z}/8\mathbb{Z}}$ und der Hintereinanderausführung $\circ$ als Gruppenverknüpfung. Mit diesen Angaben ist die Gruppe G hinreichend explizit bekannt, die Fixgruppen der Körper bestimmbar und dann die Bedingung iv) von Satz (4.6) überprüfbar. (Etwas umfangreichere rechnerische Übung).

Dieses Beispiel taucht bei Gerst [On the theory of nth power residues and a conjecture of Kronecker, Acta Arithm. **17** (1970) 121–139] in folgender Form auf: Betrachtet man die Polynome $f = X^8 - 3^7$ und $g = X^8 - 48$, so stimmen die Primteilermengen $P(f)$ und $P(g)$ bis auf endlich viele Ausnahmen überein. Dabei definiert man die Primteilermenge eines Polynoms $f \in \mathbb{Z}[X]$ als

$$P(f) := \{p \text{ Primzahl} \mid p | f(a) \text{ für ein } a \in \mathbb{Z}\}\,.$$

Es gilt dann für irreduzible Polynome $f \in \mathbb{Z}[X]$ und einen Stammkörper K von f: $P(f) \doteq D(K|\mathbb{Q})$. (Beweis als Übung.)

b) Leopoldt und Trinks haben gezeigt, daß das erstgenannte Polynom als Galoisgruppe die einfache Gruppe $G_{168} = PSL_2(7) = PGL_3(2)$ der Ordnung 168 hat. (Dies war das erste Beispiel dieser Art und damit der Nachweis, daß die einfache Gruppe G_{168} der Ordnung 168 Galoisgruppe über $\mathbb{Q}$ ist.) Nun sind die Untergruppen der $PSL_2(7) = G_{168}$ nach Dickson wohlbekannt (siehe Huppert: Endliche Gruppen I, Kap. II, §8, Hauptsatz 8.27). Aufgrund dieser Informationen kann man b) beweisen. Man kann sogar sämtliche Untergruppen $U, U' \subset PSL_2(p^f)$ bestimmen mit $U^G = U'^G$.

R. Perlis [On the equation $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory **9** (1977) 342–360] hat gezeigt, daß es keine Gegenbeispiele kleineren Grades geben kann.
Durch Untersuchung der möglichen Galoisgruppen von Polynomen siebten Grades kann man leicht einsehen, daß zwei arithmetisch äquivalente Zahlkörper vom Grade 7 notwendig die G_{168} als Galoisgruppe ihrer galoisschen Hülle haben. (Siehe Abschnitt 5.)

c. Invarianten

Wie wir gesehen haben, legen selbst die vollständigen Zerlegungsgesetze eine Zahlkörpererweiterung $K|k$ nicht (bis auf Konjugiertheit) eindeutig fest, wohl aber sind eine Reihe von arithmetischen Invarianten dadurch bestimmt. Zum Beispiel gilt der folgende

(4.9) Satz: *Seien $K|k$, $K'|k$ Zahlkörpererweiterungen. Dann gilt: a) Sind K und K' über k arithmetisch äquivalent, so stimmen ihre Zetafunktionen überein: $\zeta_K = \zeta_{K'}$.*
b) Über dem Grundkörper $k = \mathbb{Q}$ gilt sogar die Äquivalenz:

$$K \approx_{\mathbb{Q}} K' \iff \zeta_K = \zeta_{K'}.$$

Unter Verwendung der sogenannten *Artinschen* L-Funktionen (E. Artin: Über eine neue Art von L-Reihen, Abh. Math. Sem. Hamburg **8** (1931), 292-306) ergibt sich Teil a) unmittelbar aus Satz (4.6): Sei wie in (4.6) $N|k$ eine galoissche Erweiterung mit $N \supseteq KK'$ und U, U' die Fixgruppen von K, K' in der Galoisgruppe $G = G(N|k)$. Dann ist die *Artinsche* L-Funktion $L(s, \chi, N|k)$ für jeden linearen Charakter χ von G definiert, und zwar als ein Eulerprodukt über die Primideale von k. Ist der Charakter χ eindimensional, d. h. ein Homomorphismus $\chi: G \to \mathbb{C}^\times$,

so erhält man die Dirichletschen L-Reihen, wie sie in Abschnitt 3. diskutiert worden sind. Aufgrund der für die Bedeutung der Artinschen L-Funktionen fundamentalen *Induktionseigenschaft* erhält man

$$(*) \qquad \zeta_K = L(\ldots, \Phi_U, N|k)$$

mit dem Permutationscharakter Φ_U, wie er in Abschnitt b. diskutiert wurde. Dieser ist nämlich in natürlicher Weise ein linearer Charakter von G, und zwar gerade der vom Hauptcharakter 1_U der Untergruppe U auf G *induzierte* Charakter 1_U^G. Mit dieser fundamentalen Beziehung $(*)$ ist die Zetafunktion jedes Zahlkörpers K als Artinsche L-Funktion zum Grundkörper dargestellt. Mit $(*)$ ergibt sich nun sofort aus Satz (4.6) die Behauptung a) von (4.9).

a) ist aber auch eine Konsequenz von b), da offenbar zwei über k arithmetisch äquivalente Erweiterungskörper K, K' erst recht über jedem in k enthaltenen Zahlkörper k_1 arithmetisch äquivalent sind.

Um in b) die Umkehrung '$\Leftarrow$' einzusehen, genügt es – wieder nach (4.6) – zu zeigen, daß die Artinschen L-Funktionen $L(\ldots, \chi, N|\mathbb{Q})$ *über* $\mathbb{Q}$ den linearen Charakter χ eindeutig bestimmen. Diese Tatsache wurde schon von Artin gezeigt (l.c.).

Die bei Artin verwendeten Methoden benutzt Perlis (l.c.), um b) folgendermaßen direkt zu beweisen: Für $\mathrm{Re}\,(s) > 1$ gilt

$$\zeta_K(s) = \sum_{\mathfrak{A} \neq 0} \mathcal{N}\mathfrak{A}^{-s} = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

mit

$$a(n) = \#\left\{\mathfrak{A} \lhd Z_K \mid \mathcal{N}\mathfrak{A} = n\right\}.$$

Man muß nun zeigen, daß eine *Dirichletreihe* $\sum_n a_n n^{-s}$ ihre Koeffizienten a_n eindeutig bestimmt. Präziser sollte man sagen: Die Funktion

$$\varphi : (s \mapsto \sum_{n=1}^{\infty} \frac{a_n}{n^s})$$

bestimmt die Koeffizienten a_n, – sofern sie existiert, d.h. sofern die Dirichletreihe 'irgendwo' konvergiert. Ist s_0 ein solcher Konvergenzpunkt mit Realteil σ_0, so gilt $a_n = o(n^{\sigma_0})$, also erst recht $|a_n| \leq C n^{\sigma_0}$ für eine Konstante $C \in \mathbb{R}_+$ und alle $n \in \mathbb{N}$. Dies führt für alle $s \in \mathbb{C}$ mit $\sigma = \mathrm{Re}\,(s) > \sigma_0$ zur Abschätzung

$$\left| \sum_{n=2}^{\infty} \frac{a_n}{n^s} \right| \leq \sum_{n=2}^{\infty} \frac{|a_n|}{n^\sigma} \leq C \cdot \sum_{n=2}^{\infty} \frac{1}{n^{\sigma - \sigma_0}}.$$

Die Abschätzungsformel (1) aus Abschnitt 3.a. zeigt, daß die letztgenannte Reihe für $\sigma \to \infty$ gegen 0 konvergiert. Dies bedeutet letztendlich

$$\lim_{s \to \infty} \sum_{n=1}^{\infty} \frac{a_n}{n^s} = a_1.$$

Damit ist a_1 durch die Funktion φ bestimmt. Nun schließt man folgendermaßen induktiv weiter: Sind für $k \geq 1$ die Koeffizienten $a_1, \ldots, a_{k-1}$ durch φ bestimmt, so auch die Funktion

$$\varphi_k(s) := k^s (\sum_{n=k}^{\infty} \frac{a_n}{n^s}) = a_k + \sum_{n=k+1}^{\infty} \frac{a_n}{(n/k)^s}.$$

Analog wie oben für $k = 1$ kann man nun für beliebiges $k \geq 1$ abschätzen

$$\left| \sum_{n=k+1}^{\infty} \frac{a_n}{(n/k)^s} \right| \leq C \cdot k^{\sigma_0} \cdot k \sum_{n=k+1}^{\infty} \frac{1}{k} \cdot (\frac{n}{k})^{\sigma_0 - \sigma}$$
$$\leq C \cdot k^{\sigma_0+1} \int_1^{\infty} x^{\sigma_0-\sigma} dx = C \cdot k^{\sigma_0+1} \cdot \frac{1}{\sigma - \sigma_0 - 1},$$

woraus dann $a_k = \lim_{s \to \infty} \varphi_k(s)$ folgt.

Die Zetafunktionen zweier algebraischer Zahlkörper K und K' stimmen also genau dann überein, wenn die Anzahlen $a(n)$ bzw. $a'(n)$ der ganzen Ideale von K bzw. K' mit Absolutnorm n übereinstimmen. Diese Zahlen $a(n)$ ihrerseits bestimmen die Zerlegungstypen aller Primzahlen p in K: Sei dazu p eine Primzahl. Der Zerlegungstyp von p in K ist festgelegt durch die Anzahlen

$$b_p(f) := \#B_p(f) := \#\left\{\mathfrak{P} \in \mathcal{P}_K \mid \mathfrak{P}|p \ \wedge \ f(\mathfrak{P}|p) = f\right\}, \quad f \in \mathbb{N}_+ .$$

Nun gilt aber wegen der eindeutigen Primidealzerlegung in Z_K

$$\begin{aligned}
a(p^f) &= \#\{\mathfrak{A} \lhd Z_K \mid \mathcal{N}\mathfrak{A} = p^f\} \\
&= \#\{\mathfrak{A} \lhd Z_K \mid \mathfrak{A} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r \text{ mit Primidealen } \mathfrak{P}_i|p\,,\ \sum_{i=1}^{r} f(\mathfrak{P}_i|p) = f\} \\
&= \#\{\mathfrak{A} \mid \mathfrak{A} = \mathfrak{A}_1 \cdot \ldots \cdot \mathfrak{A}_s\,,\ \mathfrak{A}_i = \mathfrak{P}_{i1} \cdot \ldots \cdot \mathfrak{P}_{ir_i}\,,\ \mathfrak{P}_{ij} \in B_p(f_i)\,, \sum r_i f_i = f\} \\
&= \sum_{\substack{1 \leq f_1 < \ldots < f_s \\ 1 \leq r_1, \ldots, r_s \\ r_1 f_1 + \ldots + r_s f_s = f}} \#\{\mathfrak{A} \mid \mathfrak{A} = \mathfrak{A}_1 \cdot \ldots \cdot \mathfrak{A}_s\,,\ \mathfrak{A}_i = \mathfrak{P}_{i1} \cdot \ldots \cdot \mathfrak{P}_{ir_i}\,,\ \mathfrak{P}_{ij} \in B_p(f_i)\} \\
&= \sum_{\substack{1 \leq f_1 < \ldots < f_s \\ 1 \leq r_1, \ldots, r_s \\ r_1 f_1 + \ldots + r_s f_s = f}} \prod_{i=1}^{s} \#\{\mathfrak{A} \mid \mathfrak{A} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_{r_i}\,,\ \mathfrak{P}_j \in B_p(f_i)\} \\
&= \sum_{\substack{1 \leq f_1 < \ldots < f_s \\ 1 \leq r_1, \ldots, r_s \\ r_1 f_1 + \ldots + r_s f_s = f}} \prod_{i=1}^{s} \#(B_p(f_i)^{r_i}/S(r_i)).
\end{aligned}$$

Damit ist das Problem auf die Berechnung der Bahnenanzahl der natürlichen Operation der symmetrischen Gruppe $\mathcal{S}_k$ auf dem k-Tupel-Raum M^k einer n-elementigen Menge M zurückgeführt (mit $M = B_p(f_i)$, $n = \#M$ und $k = r_i$). Es ist klar, daß diese Anzahl $C(n,k) := \#(M^k/\mathcal{S}_k)$ allein durch k und $n = \#M$ bestimmt ist. Dies allein wird für den folgenden Beweisgang benötigt.
(Es sei jedoch erwähnt, daß $C(n,k)$ die sog. Zahl der Auswahl von k Objekten *mit Wiederholungen* aus n Objekten *ohne* Berücksichtigung der Reihenfolge ist, und daß $C(n,k) = \binom{n+k-1}{n}$ gilt. Letzteres beweist man etwa über die Rekursionsformel $C(n,k+1) = \sum_{i=1}^{n} C(i,k)$, die man leicht einsehen kann.)
Da in obiger Formel für $a(p^f)$ der Term $B_p(f)$ nur einmal auftritt, nämlich für $s = 1, f_1 = f, r_1 = 1$, und dann gerade den Beitrag

$$\#(B_p(f_1)^{r_1}/\mathcal{S}_{r_1})) = b_p(f)$$

liefert, erhält man

$$a(p^f) - b_p(f) \text{ ist eine Funktion der } b_p(f') \text{ mit } f' < f\,.$$

Damit sind nicht nur die $a(p^f)$ durch die $b_p(f)$, sondern auch umgekehrt die $b_p(f)$ rekursiv durch die $a(p^f)$ bestimmt.

Wir wollen nun zum Abschluß dieses Paragraphen eine Reihe expliziter arithmetischer Invarianten bestimmen, die für arithmetisch äquivalente Körper übereinstimmen. Zuvor sei jedoch noch erwähnt, daß bei beiden Begriffen arithmetischer Ähnlichkeit die bisher immer zugelassenen endlich vielen Ausnahmeprimideale de facto nicht auftreten:

(4.10) Satz: *Sind $K|k$ und $K'|k$ zwei Zahlkörpererweiterungen, so gelten folgende Äquivalenzen:*

a) $$K \sim_k K' \iff D(K|k) = D(K'|k).$$

b) $$K \approx_k K' \iff P_A(K|k) = P_A(K'|k) \quad \textit{für alle } A\,.$$

Ohne Beweis. (Man muß Satz (2.7) in geeigneter Weise auf verzweigte Primideale ausdehnen.)

Man entnimmt aus diesem Satz, daß in arithmetisch äquivalenten Körpern dieselben Primideale des Grundkörpers verzweigen, denn ein Primideal $\mathfrak{p}$ ist in K genau dann verzweigt, wenn für seinen Zerlegungstyp $A = (f_1, \ldots, f_r)$ in K $\sum f_i < (K\colon k)$ gilt. Gilt nun *ohne* Ausnahme $P_A(K|k) = P_A(K'|k)$, so muß $\mathfrak{p}$ auch in K' verzweigen. Es gilt aber noch mehr, wie der folgende Satz zeigt, der sich wie (4.9)a) im wesentlichen aus der Übereinstimmung der Permutationscharaktere $\Phi_U = \Phi_{U'}$ arithmetisch äquivalenter Körper ergibt (Satz (4.6)).

(4.11) Satz: *Seien K, K' arithmetisch äquivalente Zahlkörpererweiterungen von k. Dann stimmen für K und K' folgende Invarianten überein:*

i) Der Körpergrad: $(K\colon k) = (K'\colon k)$.

ii) Die galoissche Hülle: $\widetilde{K} = \widetilde{K'}$.

iii) Die Diskriminante: $\mathfrak{d}_{K|k} = \mathfrak{d}_{K'|k}$.

iv) Die Mengen der rein-, zahm- und der wild-verzweigten Primideale.

v) Die Zahlen r_1, r_2 der reellen bzw. komplexen Konjugierten: $r_i(K) = r_i(K')$.

vi) Die Einheitswurzelgruppe: $\mu_K = \mu_{K'}$.

vii) Das Produkt aus Klassenzahl h_K und Regulator R_K: $h_K R_K = h_{K'} R_{K'}$.

Zum *Beweis* nur einige Anmerkungen: Die Gültigkeit von i) ergibt sich unmittelbar aus der Definition der arithmetischen Äquivalenz unter Benutzung der fundamentalen Beziehung $\sum e_i f_i = n$ (Satz (1.12)). Wegen i) folgt aus der arithmetischen Äquivalenz die Übereinstimmung der Mengen der voll-zerlegten Primideale, also gemäß Prop. (4.1) die Behauptung ii). iii) ergibt sich aus (4.6) ($\Phi_U = \Phi_{U'}$) aufgrund der *Führerdiskriminantenproduktformel* für lineare Charaktere. Sie besagt (mit den in (4.6) benutzten Bezeichnungen):

$$\mathfrak{d}_{K|k} = \mathfrak{f}(1_U^G, N|k) = \mathfrak{f}(\Phi_U, N|k)\,,$$

wobei $\mathfrak{f}(\chi, N|k)$ den sog. em Artinschen Führer für beliebige lineare Charaktere χ der Galoisgruppe G bezeichne.

Ad iv): Rein-verzweigte Primideale sind gerade die mit Zerlegungstyp $A = (1)$. Verzweigte Primideale sind gerade die Teiler der Diskriminante. Aber auch die zahm-, und komplementär dazu die wild-verzweigten Primideale sind aufgrund des Dedekindschen *Differentensatzes* durch die Diskriminante charakterisierbar, also folgt dieser Teil der Behauptung aus iii).

v) ergibt sich ähnlich wie iii) aus der Übereinstimmung $\Phi_U = \Phi_{U'}$ unter Benutzung einer von S. Kuroda definierten Größe $B(\chi, N|k)$ für lineare Charaktere χ. Es gilt nämlich $B(\Phi_U, N|k) = 2^{r_1(K)+r_2(K)}\pi^{r_2(K)}$.

vi) ergibt sich bereits aus der Kronecker-Äquivalenz von K und K'. Es gilt sogar schärfer die

nachfolgende Proposition (4.12).
vii) schließlich ist eine Konsequenz von Satz (4.9), der Formel für das Residuum der Zetafunktion (Satz (3.1)) und der bisherigen Resultate dieses Satzes. Es sei angemerkt, daß vii) sich nicht verschärfen läßte zur Übereinstimmung von Klassenzahl und Regulator getrennt.

(4.12) Proposition: *Kronecker-äquivalente Körpererweiterungen $K|k$ und $K'|k$ enthalten dieselben galoisschen Erweiterungen von k. Insbesondere stimmen die Einheitswurzelgruppen von K und K' überein.*

Beweis: Mit den Bezeichnungen von Satz (4.3) schließt man: Ist $L \subseteq K$ eine galoissche Erweiterung von k und H die Fixgruppe von L in G, so gilt wegen der Normalteilereigenschaft von H:

$$H \supseteq U \Rightarrow H \supseteq \bigcup_{\sigma \in G} U^\sigma = U^G = U'^G \supseteq U' ,$$

so daß auch K' den Körper L umfaßt.

§5 Starrheit von Zerlegungsgesetzen und Zahlkörpern

Wie wir in Abschnitt 4. gesehen haben, gibt es viele Beispiele für nicht konjugierte Zahlkörpererweiterungen, die Kronecker-äquivalent, ja sogar arithmetisch äquivalent sind. Bevor wir in diesem abschließenden Paragraphen der Vorlesung der Frage nachgehen, ob und wieweit Zahlkörper eventuell doch durch ihr Zerlegungsgesetz festgelegt sind, möchte ich noch eine Bemerkung zum Beginn von Abschnitt 4. nachtragen. Bei der Ausdehnung des Bauerschen Resultates auf beliebige Zahlkörpererweiterungen bietet sich auch noch der folgende Ansatz an:

(4.2′) Definition: Zwei Zahlkörpererweiterungen $K|k$ und $K'|k$ heißen *Bauer-äquivalent* über k (in Zeichen: $K \sim'_k K'$) genau dann, wenn sowohl ihre Kroneckermengen als auch die Mengen der vollzerlegten Primideale bis auf eventuell endlich viele Ausnahmen übereinstimmen:

$$K \sim'_k K' : \Longleftrightarrow \; D(K|k) \doteq D(K'|k) \text{ und } S(K|k) \doteq S(K'|k) .$$

Gemäß Prop.(4.1) bedeutet dies: K und K' sind genau dann Bauer-äquivalent, wenn sie Kronecker-äquivalent sind und dieselbe galoissche Hülle besitzen. Daraus entnimmt man unmittelbar, daß im Gegensatz zur Kronecker-Äquivalenz ein Körper nur zu em endlich vielen anderen Körpern Bauer-äquivalent sein kann. Bei den weiteren Überlegungen wird diese Bauer-Äquivalenz eine wichtige Rolle spielen.

a. Zerlegungsgesetze und Starrheit

Wir fixieren für diesen Paragraphen einen Zahlkörper k als Grundkörper, auf den sich alle folgenden Begriffsbildungen unausgesprochen beziehen.

(5.1) Definition: Sei $K|k$ eine Zahlkörpererweiterung.
A) Dann verstehen wir unter dem

a) *(vollen) Zerlegungsgesetz* von K über k das System aller Mengen $P_A(K|k)$ $(A \in \mathbb{N}^r , r \in \mathbb{N}_+)$,

b) *schwachen Zerlegungsgesetz* die Kroneckermenge $D(K|k)$,

c) *Bauerschen Zerlegungsgesetz* die Kroneckermenge $D(K|k)$ zusammen mit $S(K|k)$, der Menge der voll-zerlegten Primideale.

B) Wir wollen das Zerlegungsgesetz von $K|k$ *starr* bzw. *absolut starr* nennen, wenn es bereits durch das Bauersche bzw. das schwache Zerlegungsgesetz bestimmt ist, m.a.W. (siehe Satz (4.10)) wenn für alle Erweiterungskörper K' von k gilt:

$$\begin{array}{ll} \text{starr:} & K \sim'_k K' \Rightarrow K \approx_k K' \\ \text{absolut starr:} & K \sim_k K' \Rightarrow K \approx_k K' . \end{array}$$

C) Ist das Zerlegungsgesetz von $K|k$ nur unter allen Körpern gleichen Grades durch das schwache Zerlegungsgesetz festgelegt, so wollen wir es *horizontal starr* nennen, also wenn gilt:

$$(K\colon k) = (K'\colon k) \wedge K \sim_k K' \Rightarrow K \approx_k K'.$$

D) Entsprechend wollen wir den Körper K selbst *starr, absolut starr* bzw. *horizontal starr* nennen, wenn in B/C) nicht nur sein Zerlegungsgesetz, sondern er selbst (bis auf Konjugation über k) eindeutig bestimmt ist. Ist der Körper K bis auf Konjugation durch sein volles Zerlegungsgesetz bestimmt, so wollen wir ihn *arithmetisch fixiert* nennen (bei Perlis, l.c.: 'arithmetically solitary').

(5.2) Bemerkung: a) 'Absolut starr' impliziert natürlich 'starr' und 'horizontal starr', für Zerlegungsgesetze wie für Körper selbst.
b) Ein Körper K ist genau dann starr, absolut starr bzw. horizontal starr, wenn sein Zerlegungsgesetz diese Eigenschaften hat und er arithmetisch fixiert ist.
c) Der Grundkörper k selbst ist absolut starr (über k).
d) Ein starrer Körper muß nicht horizontal starr, und ein horizontal starrer Körper nicht starr sein.

Beweis: Ad b): Es ist lediglich zu bemerken, daß für einen Körper K jeder der Starrheitsbegriffe impliziert, daß K arithmetisch fixiert ist. Da aus arithmetischer Äquivalenz aber Kronecker- und Bauer-Äquivalenz bzw. Gradgleichheit folgt, ist dies eine logische Abschwächung.
Ad c): Es genügt zu zeigen, daß $G = U^G$ nur für $U = G$ gelten kann, daß also eine endliche Gruppe nicht Vereinigung aller Konjugierten einer echten Untergruppe sein kann. Wäre $G = U^G$, so folgte:

$$G = U^G = \bigcup_{\sigma\in G} U^\sigma = \bigcup_{\bar\sigma\in U\backslash G} U^\sigma = \bigcup_{\bar\sigma\in U\backslash G} (U\setminus\{1\})^\sigma \cup \{1\},$$

wobei $U\backslash G$ die Menge der Linksnebenklassen von U in G bezeichne und σ jeweils ein beliebig gewählter Repräsentant von $\bar\sigma$ sei. Durch Abzählen erhält man

$$\#G \le (G\colon U)\cdot(\#U - 1) + 1 = \#G - (G\colon U) + 1,$$

also

$$(G\colon U) \le 1.$$

Ad d): Wir konstruieren zunächst Körper K, die starr, aber nicht horizontal starr sind. Wir benutzen dazu das Beispiel (4.4) b). Aus bekannten Resultaten über das Umkehrproblem der Galoistheorie und der damit verwandten Theorie des *Einbettungsproblems* weiß man:

> Eine zyklische kubische Erweiterung $L|k$ ist in unendlich viele $\mathcal{A}_4$-Erweiterungen $N_i|k$ einbettbar.

Seien K_i, K_i', K_i'' die über L quadratischen Teilkörper von N_i. Diese sind sämtlich zu L, also untereinander Kronecker-äquivalent (Beispiel (4.4)b)). (Dies zeigt übrigens, daß Kroneckerklassen unendlich sein können.) Für $i \neq j$ sind K_i und K_j nicht konjugiert, also K_i nicht horizontal starr. Aber K_i ist starr, denn jeder zu K_i Bauer-äquivalente Körper hat N_i als galoissche Hülle, ist daher *echter* Zwischenkörper in $N_i|L$, also einer der untereinander über k konjugierten Körper K_i, K_i', K_i''.

Ein Beispiel von horizontal starren, aber nicht starren Körpern ist gegeben durch Erweiterungen $K|k$ vom Grad 5, deren galoissche Hülle die Galoisgruppe $\mathcal{A}_5$ hat. Gemäß den nachfolgenden Resultaten ist ein solcher Körper horizontal starr, aber zugleich Bauer-äquivalent zu einem Körper L vom Grad 10 über k.

(5.3) Satz: *Sei $K|k$ eine Erweiterung vom Grade n, dessen galoissche Hülle $\tilde K$ über k als Galoisgruppe $\mathcal{S}_n$ oder $\mathcal{A}_n$ hat. Dann gilt:*

a) *Ist die Galoisgruppe nicht $\mathcal{A}_5$, so ist K starr.*

b) *Ist die Galoisgruppe $\mathcal{A}_5$, so sind die zu K Bauer-äquivalenten Körper konjugiert zu K selbst oder einem Erweiterungskörper L vom Grad 10 über k, der im Beweis explizit konstruiert wird. Insbesondere ist K nicht starr.*

c) *In jedem Fall ist K unter den genannten Voraussetzungen horizontal starr und nach (5.2),b) somit auch arithmetisch fixiert: $K \approx_k K' \iff K \simeq_k K'$.*

Dies bedeutet in Termen erzeugender Gleichungen formuliert: Ist $f \in k[X]$ ein Polynom vom Grad n mit Galoisgruppe $\mathcal{A}_n$ oder $\mathcal{S}_n$, so gilt für jedes irreduzible Polynom $g \in k[X]$ vom gleichen Grad: Stimmen die Primteilermengen $P(f) := \{\mathfrak{p} \in \mathcal{P}_k \mid \mathfrak{p} | f(a)$ für ein $a \in Z_k\}$ und $P(g)$ bis auf endlich viele Ausnahmen überein, so haben f und g denselben Stammkörper: $k(\alpha) = k(\beta)$ für Wurzeln α von f und β von g.

Beweis: Ad a): Sei $G = G(\tilde{K}|k)$ die Galoisgruppe, also $G = \mathcal{S}_n$ oder $G = \mathcal{A}_n$, und U die Fixgruppe von K. Dann ist U die Fixgruppe einer Ziffer, also o. E. $U = \mathrm{Fix}_G(n)$, und daher $U = \mathcal{S}_{n-1}$ bzw. $U = \mathcal{A}_{n-1}$. Wir studieren nun Untergruppen U' in G mit $U^G = U'^G$ und wollen zeigen:
U' ist ebenfalls die Fixgruppe einer Ziffer und daher konjugiert zu U. Man erledigt leicht die Fälle $\mathcal{S}_n$ mit $n \leq 3$ und $\mathcal{A}_n$ mit $n \leq 4$. Es verbleiben dann die folgenden drei Fälle
1) $G = \mathcal{S}_n$ mit $n \geq 4$,
2) $G = \mathcal{A}_n$ mit $n \geq 6$ gerade, sowie
3) $G = \mathcal{A}_n$ mit $n \geq 7$ ungerade.

Exemplarisch soll hier Fall 1) diskutiert werden; die beiden übrigen Fällen benötigen keine anderen Hilfsmittel.

Wir stellen zunächst fest, daß aus $U^G = U'^G$ folgt:
α) $U' \ni \sigma = (a_1, \ldots, a_{n-1})$, einen $(n-1)$-Zyklus,
β) $U' \ni \rho = (b_1, \ldots, b_{n-2})$, einen $(n-2)$-Zyklus, und
γ) $U' \ni \tau = (c_1, c_2)$, eine Transposition.

Wir bezeichnen mit a_n bzw. b_{n-1},b_n die Fixpunkte von σ bzw. ρ. Ohne Einschränkung können wir $a_n = b_n$ annehmen. Wäre nämlich $a_n = b_i$ für ein $i \leq n-2$, so wäre U' transitiv auf $\{1, \ldots, n\}$. (Man beachte $n - 2 \geq 2$.) Wegen α) wäre U' dann 2-fach transitiv, enthielte dann wegen γ) alle Transpositionen, wäre also die volle Gruppe $G = \mathcal{S}_n$, im Widerspruch zu Bemerkung (5.2), c) (bzw. explizit zu dessen Beweis.)
Ist nun $a_n = b_n$, so liegen σ und ρ in der Gruppe $U'' := \mathrm{Fix}_{U'}(a_n)$. Wir zeigen, daß U'' auch eine Transposition enthält. Sind beide $c_i \neq a_n$, so liegt natürlich τ in U''. Andernfalls ist (o.E.) $\tau = (a_n, c_2)$. Wählt man nun ein $d \neq a_n, c_2$ und mittels des $(n-1)$-Zyklus σ eine Permutation $\phi \in U'$ mit $\phi(a_n) = a_n$ und $\phi(c_2) = d$, so erhält man

$$U' \ni (a_n, c_2) \circ \phi \circ (a_n, c_2) \circ \phi^{-1} \circ (a_n, c_2) = (c_2, d) =: \tau'.$$

Wegen $a_n \neq d, c_2$ liegt τ' in $\mathrm{Fix}_{U'}(a_n) = U''$ und man schließt mit denselben Schlüssen wie oben: U'' ist die volle symmetrische Gruppe $\mathcal{S}(\{a_1, \ldots, a_{n-1}\}) = \mathrm{Fix}_G(a_n)$. Wir haben somit gezeigt, daß U' eine Obergruppe von $\mathrm{Fix}_G(a_n)$ ist. Diese Fixgruppe aber ist maximal in G, also folgt wegen $U' \neq G$ schließlich $U' = \mathrm{Fix}_G(a_n)$, wie behauptet.
[Es gilt allgemein, daß in 2-fach transitiven Permutationsgruppen G die Fixgruppen $H = \mathrm{Fix}_G(a)$ einer Ziffer maximal sind: Sei etwa B eine echte Obergruppe von H. Dann existiert ein $\phi \in B$ mit $\phi(a) =: b \neq a$. Wegen der 2-fachen Transitivität von G ist H, also erst recht B auf dem Komplement von $\{a\}$ transitiv, so daß B insgesamt transitiv ist. Ist nun $\sigma \in G$ beliebig, so existiert ein $\psi \in B$ mit $\psi(a) = c := \sigma(a)$, also $\sigma^{-1} \circ \psi \in H \subset B$ und daher schließlich $\sigma \in B$.]

Die Fälle 2) und 3) werden mit denselben Methoden bewiesen.

Ad b): Der bei a) ausgelassene Fall $n = 5$, $G = \mathcal{A}_5$ erwies sich als echte Ausnahme. Beim Versuch, den Beweis auch in diesem Fall durchzuführen, stößt man ziemlich zwangsläufig auf die Untergruppe

$$U' := \langle (12)(34), (125) \rangle = \{\mathrm{id}, (12)(34), (125), (152), (15)(34), (25)(34)\}$$

vom Index 10 in $\mathcal{A}_5$. Offenbar gilt $U^{\mathcal{A}_5} = U'^{\mathcal{A}_5}$, so daß die zugehörigen Fixkörper K (vom Grad 5) und K' (vom Grad 10 über k) Kronecker-äquivalent sind. Wegen der Einfachheit von $\mathcal{A}_5$ enthält $\tilde{K} = N$ keinen echten galoisschen Zwischenkörper, so daß N auch die galoissche Hülle von K' ist. Mithin sind K und K' Bauer-äquivalent, aber wegen unterschiedlichen Grades selbstverständlich nicht konjugiert über k. Mit denselben Schlüssen wie bei a) zeigt man, daß die zu K Kronecker-äquivalenten Teilkörper von N zu K oder dem eben konstruierten K' konjugiert sind.

Ad c): Sei K' ein beliebiger, nicht notwendig in $\tilde{K}$ enthaltener Körper mit

$$K \sim_k K' \text{ und } (K'\colon k) = (K\colon k) = n.$$

Die bisherigen Überlegungen über die zu K Kronecker-äquivalenten *Teilkörper von* N kann man auch in dieser Situation nutzen, wegen der nachfolgenden einfachen, aber wichtigen

(5.4) Proposition: *Seien $K|k$ und $K'|k$ Zahlkörpererweiterungen mit galoisschen Hüllen $\tilde{K}$ bzw. $\widetilde{K'}$. Dann gilt:*

a) $$K \sim_k K' \implies K \sim_k K' \cap \tilde{K} \sim_k K \cap \widetilde{K'}\,.$$

b) Die minimalen Körper einer Kroneckerklasse sind untereinander Bauer-äquivalent. Es gibt davon also nur endlich viele.

Beweis: Ist K minimal in seiner Kroneckerklasse, so folgt aus a) für jeden zu K Kronecker-äquivalenten Körper K': $K = K \cap \widetilde{K'}$, also $\tilde{K} \subseteq \widetilde{K'}$. Sind beide Körper minimal in ihrer Kroneckerklasse, so folgt aus Symmetriegründen die Behauptung von b).

Zum Beweis von a) benutzen wir das gruppentheoretische Kriterium (4.3). Sei N die galoissche Hülle von KK' und U bzw. U' die Fixgruppen von K bzw. K' in $G = G(N|k)$. Aus Symmetriegründen genügt es zu zeigen: $K \sim_k K' \cap \tilde{K}$. Die Fixgruppe von $\tilde{K}$ in N ist der Normalteiler $U_G := \bigcap_{\sigma \in G} U^\sigma$ von G. Damit ist die Fixgruppe von $K' \cap \tilde{K}$ gerade die von U' und U_G erzeugte Untergruppe V, und wegen der Normalteilereigenschaft von U_G hat man $V = U' \cdot U_G$. Aus $U^G = U'^G$ ergibt sich nun

$$V^G = (U' \cdot U_G)^G = U'^G \cdot U_G = U^G \cdot U_G = U^G\,,$$

womit die Behauptung gezeigt ist.

Wir kehren nun zurück zum Beweis von (5.3),c): Sei K wie in (5.3) gegeben und K' ein dazu Kronecker-äquivalenter Körper vom Grade n. Da wie erwähnt die Fixgruppe von K maximal ist in G, ist die Erweiterung $K|k$ *atomar,* d. h. sie hat keine echten Zwischenkörper. Damit ist K erst recht minimal in seiner Kroneckerklasse (beachte (5.2),c)). Man wählt nun einen in K' enthaltenen minimalen Körper K_0 der Kroneckerklasse von K'. Gemäß (5.4),b) liegt K_0 in $\tilde{K}$ und es gilt $(K_0\colon k) \le (K'\colon k) = n = (K\colon k)$. Aus den bewiesenen Teilen a) und b) von (5.3) entnimmt man daher (auch im $\mathcal{A}_5$-Fall), daß K_0 zu K konjugiert ist. Damit folgt aber insbesondere $(K_0\colon k) = (K\colon k) = n = (K'\colon k)$ und daraus wiederum $K_0 = K'$. Also sind K und K' konjugiert und (5.3),c) bewiesen.

b. Erweiterungen von Primzahlgrad

Wir hatten in Bemerkung (5.2) gesehen, daß die Begriffe 'starr' und 'horizontal starr' unabhängig voneinander sind. Für Erweiterungen von Primzahlgrad trifft dies nicht zu, wie wir leicht aus Prop. (5.4) entnehmen können. Siehe Teil c) der nachfolgenden

(5.5) Bemerkung: Sei $K|k$ eine Erweiterung von Primzahlgrad $p = (K\colon k)$. Dann gilt:

a) Alle zu K Kronecker-äquivalenten Körper K' haben einen durch p teilbaren Grad über k.
b) Kronecker-äquivalente Körpererweiterungen von Primzahlgrad haben denselben Grad und sind Bauer-äquivalent.
c) Sind K oder sein Zerlegungsgesetz starr, so auch horizontal starr.

Beweis: a) Es gilt allgemeiner für $K \neq k$

$$(*) \qquad K \sim_k K' \implies (KK' : K') < (K : k)\,,$$

d.h. K und K' sind über k *nicht* linear disjunkt. Daher sind insbesondere die Körpergrade $(K : k)$ und $(K' : k)$ nicht teilerfremd, woraus a) folgt.
Ad $(*)$: Wir benutzen wieder das gruppentheoretische Kriterium (4.3) und die dortigen Bezeichnungen. Wäre $(KK' : K') = (K : k)$, so hätte man folgende gruppentheoretische Situation:

$$U^G = U'^G \quad \text{und} \quad (G : U) = (U' : U \cap U')\,.$$

Nun gilt

$$U' = \dot{\bigcup_{i=1}^{n}} (U \cap U')u'_i \implies G \supseteq \dot{\bigcup_{i=1}^{n}} Uu'_i\,,$$

so daß aus der Indexgleichheit $(G : U) = (U' : U \cap U') = n$ dann

$$G = \dot{\bigcup_{i=1}^{n}} Uu'_i$$

folgt. Damit erhält man für G die folgende Darstellung als Komplexprodukt

$$G = U \cdot U' := \{uu' \mid u \in U\,, u' \in U'\}\,.$$

Dann folgt aber aus $U^G = U'^G$ unmittelbar

$$(**) \qquad U^U = (U \cap U')^U\,,$$

denn: Zu jedem $u \in U$ existiert ein $\sigma = \rho \cdot \rho' \in G$ mit $\rho \in U$,$\rho' \in U'$ und $U' \ni u^\sigma = \rho'^{-1}\rho^{-1}u\rho\rho'$, also $\rho^{-1}u\rho \in U' \cap U$.
Gemäß dem Beweis von (5.2),c) folgt aus $(**)$

$$U = U \cap U' \subseteq U'\,, \quad \text{also} \quad K \supseteq K'\,.$$

Aus Symmetriegründen folgt dann $K = K'$ und damit der Widerspruch $(K : k) = (KK' : K') = 1$.
Ad b): Die Gradgleichheit ergibt sich unmittelbar aus a). Die Übereinstimmung der galoisschen Hülle folgt aus (5.4),b), da Erweiterungen von Primzahlgrad selbstverständlich minimal sind in ihrer Kroneckerklasse.
Ad c): Ist K' Kronecker-äquivalent zu K von gleichem Grad p, so sind K und K' nach b) Bauer-äquivalent, so daß aus der Starrheit des Körpers K bzw. seines Zerlegungsgesetzes sofort die horizontale Starrheit folgt.

(5.6) Satz: *Sei k ein Zahlkörper, $f \in k[X]$ ein irreduzibles Polynom von Primzahlgrad p, G seine Galoisgruppe und K der Stammkörper von f. Dann gilt:*
a) $K|k$ hat ein horizontal starres Zerlegungsgesetz.
*b) Ist G auflösbar (*dann ist $G \subseteq \mathrm{Aff}(1,p)$*), so ist der Körper K selbst horizontal starr.*
c) Im allgemeinen kann man weder in a) schließen, daß das Zerlegungsgesetz starr ist, noch in b) auf die Auflösbarkeit verzichten.

Beweis: Die Gegenbeispiele zum Nachweis von c) haben wir schon kennengelernt: Ist $p = 5$ und $G = \mathcal{A}_5$, so ist K Bauer-äquivalent zu einem Körper L vom Grad 10 (siehe (5.3),b)), zu dem K aber nicht arithmetisch äquivalent sein kann, also ist K nicht starr. Ist $p = 7$ und $G = G_{168} = PSL_2(7)$, so gibt es einen zu K arithmetisch äquivalenten, aber nicht konjugierten Körper K' (siehe (4.8),b)). Wegen a) genügt es dabei zu zeigen, daß K' und K Kronecker-äquivalent von gleichem Grad, aber nicht konjugiert sind.

Ad a),b): Sind K und K' Kronecker-äquivalent von gleichem Grad p, so sind sie Bauer-äquivalent, liegen also in derselben galoisschen Hülle $N = \widetilde{K} = \widetilde{K'}$ mit der Galoisgruppe G über k. Als Galoisgruppe eines Polynoms vom Grad p ist G Untergruppe der symmetrischen Gruppe $\mathcal{S}_p$ von der Ordnung p, also p^2 kein Teiler von $\#\,G$. Damit gilt für die Fixgruppen U, U' von K, K' in G:

$$(G\colon U) = (G\colon U') = p \quad \text{und} \quad p \not| \#\,U, \#\,U'\,.$$

Damit sind U und U' sogenannte $\{p\}'$-*Halluntergruppen,* in der auflösbaren Gruppe G also zueinander konjugiert (Satz von P. Hall, siehe etwa B. Huppert, l.c., VI,§1, Hauptsatz (1.8)). [Halluntergruppen sind offenbar Verallgemeinerungen der Sylowuntergruppen, und der Satz von P. Hall ist die Ausdehnung der Sylowsätze auf diese Halluntergruppen für auflösbare Gruppen G.]

Wir müssen nun nur noch a) im nicht-auflösbaren Fall beweisen. Seien P_U bzw. $P_{U'}$ die Permutationsdarstellungen von G zu den Untergruppen U und U'. Diese sind beide von (gleichem) Primzahlgrad. Es gilt nun der folgende fundamentale

Satz: (Burnside) *Eine transitive Permutationsgruppe G von Primzahlgrad ist auflösbar oder 2-fach transitiv.*

Zum *Beweis* siehe etwa Huppert, l.c., V., §21, Satz 21.3.

Dieser Satz ist eines der besonders herausragenden Beispiele für die Anwendung der Darstellungstheorie bei der Strukturuntersuchung endlicher Gruppen. Aus dem Permutationscharakter Φ von G kann man die Transitivität und 2-fache Transitivität von G ablesen, denn es gilt (siehe wieder Huppert, V., §20,Satz 20.2):

$$\frac{1}{\#\,G}\sum_{\sigma\in G}\Phi(\sigma) = \text{Anzahl der Bahnen von } G\,,$$

und im Falle der Transitivität ist

$$\frac{1}{\#\,G}\sum_{\sigma\in G}\Phi(\sigma)^2 = \text{Anzahl der Bahnen der Fixgruppe einer beliebigen Ziffer}\,.$$

Der Beweis des obigen Satzes besteht nun darin, aus der Beziehung

$$\frac{1}{\#\,G}\sum_{\sigma\in G}\Phi(\sigma)^2 = r \geq 3$$

die Auflösbarkeit der Gruppe G zu folgern!

Bevor wir mit der Beweisskizze von Satz (5.6) fortfahren, seien einige Bemerkungen über lineare Charaktere eingeschoben:
Lineare Charaktere χ von G sind Funktionen $\chi\colon G \to \mathbb{C}$ gegeben durch

$$\chi(\sigma) = \mathrm{Spur}(D(\sigma))$$

für einen Gruppenhomomorphismus (eine sog. Matrixdarstellung)

$$D\colon G \to GL_n(\mathbb{C})\,.$$

Insbesondere sind Charaktere Funktionen der Konjugationsklassen von G. Offenbar ist die Summe $\chi_1 + \chi_2$ zweier Charaktere χ_1, χ_2 wieder ein Charakter. Umgekehrt ist jeder Charakter darstellbar als Summe von *irreduziblen* Charakteren, das sind solche, die sich nicht weiter als Summe von Charakteren kleineren Grades zerlegen lassen.

Betrachtet man nun auf dem endlichdimensionalen Vektorraum

$$\mathbb{C}^{[G]} = \{\varphi \mid \varphi\colon [G] \to \mathbb{C}\} = \{\varphi\colon G \to \mathbb{C} \mid \varphi(\sigma) = \varphi(\tau^{-1}\sigma\tau) \text{ für alle } \sigma, \tau \in G\}$$

aller sog. *Klassenfunktionen* die symmetrische Bilinearform $(\ldots,\ldots)_G$

$$(\varphi,\psi)_G := \frac{1}{\#G}\sum_{\sigma\in G}\varphi(\sigma)\psi(\sigma^{-1})\,,$$

so bilden die irreduziblen Charaktere eine *Orthonormalbasis.* Ihre Anzahl ist daher gerade die *Klassenzahl* $h := \#[G]$ von G. Für die Grundbegriffe der Darstellungstheorie siehe etwa Huppert, Endliche Gruppen I, Kapitel V, oder J.-P. Serre: Linear representations of finite groups, Springer GTM 42, 1977, Chapter 1,2.

Wir kehren zum Beweis von (5.6),a) für nicht-auflösbares G zurück. Nach dem Burnside'schen Satz sind dann die beiden Permutationsdarstellungen P_U und $P_{U'}$ 2-fach transitiv. Für die zugehörigen Permutationscharaktere Φ_U und $\Phi_{U'}$ gilt dann wie oben erwähnt:

$$(*)\qquad (\Phi_U,\Phi_U) = 2 \quad\text{und}\quad (\Phi_U,1_G) = 1\,,$$

sowie die analogen Beziehungen für U'. (Dabei bezeichne 1_G den (irreduziblen) *Hauptcharakter,* die konstante Funktion vom Wert 1. Man beachte außerdem, daß für Permutationscharaktere offenbar $\Phi_U(\sigma) = \Phi_U(\sigma^{-1})$ gilt.) Stellt man Φ_U durch die Orthonormalbasis der irreduziblen Charaktere dar:

$$\Phi_U = \sum_{i=1}^{h} e_i\chi_i = e_1 1_G + \sum_{i=2}^{h} e_i\chi_i\,,$$

so sind die e_i natürliche Zahlen und die obigen Gleichungen $(*)$ bedeuten

$$e_1 = (\Phi_U,1_G) = 1 \quad\text{und}\quad \sum_{i=1}^{h} {e_i}^2 = (\Phi_U,\Phi_U) = 2\,.$$

Also folgt

$$\Phi_U = 1_G + \Theta_U \quad \text{mit } \Theta_U \text{ irreduzibel}\,.$$

Dasselbe gilt natürlich auch für $\Phi_{U'}$ mit einem irreduziblen $\Theta_{U'}$.

Da K und K' Kronecker-äquivalent sind, gilt ${U'}^G = U^G$, bzw. mit den Permutationscharakteren formuliert:

$$\Phi_U(\sigma) > 0 \iff \Phi_{U'}(\sigma) > 0 \quad \text{für alle } \sigma\in G\,.$$

Da Permutationscharaktere nur natürliche Zahlen als Werte haben, ergibt sich

$$\Theta_U(\sigma) \geq 0 \iff \Theta_{U'}(\sigma) \geq 0\,,$$

und daher wegen $\Theta_{U'}(\sigma^{-1}) = \Theta_{U'}(\sigma)$

$$(\Theta_U,\Theta_{U'}) = \frac{1}{\#G}\sum_{\sigma\in G}\Theta_U(\sigma)\cdot\Theta_{U'}(\sigma) \geq \frac{1}{\#G}\Theta_U(1)\cdot\Theta_{U'}(1) > 0\,.$$

Damit sind die irreduziblen Charaktere Θ_U und $\Theta_{U'}$ *nicht* orthogonal, also gleich. Dann stimmen aber auch die Permutationscharaktere Φ_U und $\Phi_{U'}$ überein, so daß die Körper K und K' arithmetisch äquivalent sind.

Da man die möglichen Galoisgruppen einer irreduziblen Gleichung kleinen Grades voll überschaut, erhält man aus den Sätzen (5.3) und (5.6) das folgende

(5.7) Korollar: *Sei $K|k$ eine Zahlkörpererweiterung vom Grade $n \leq 7$ mit galoisscher Hülle N und Galoisgruppe $G := G(N|k) \subseteq \mathcal{S}_n$.*
a) Ist $K' \subseteq N$ Kronecker-äquivalent zu K, aber nicht konjugiert, so liegt einer der folgenden Fälle vor:
$\underline{n=5:}$ $G = \mathcal{A}_5\,,\quad (K'\colon k) = 10\,,\quad \mathrm{Fix}_G(K') = \langle(12)(34),(125)\rangle\,.$
$\underline{n=6:}$ $G \simeq \mathcal{A}_4\,,\quad (K'\colon k) = 3\,,\quad \mathrm{Fix}_G(K') \simeq \mathcal{V}_4\,.$
$\underline{n=7:}$ $G = \mathrm{PGL}_3(2)\,,\quad (K'\colon k) = 7\,,\quad \mathrm{Fix}_G(K) \simeq \mathrm{Fix}_G(K') \simeq \mathcal{S}_4\,.$
b) Daraus folgern wir:

α) Außer im Fall $n = 7$, $G = \mathrm{PGL}_3(2)$ ist K arithmetisch fixiert.

β) Ist die Galoisgruppe nicht $G = \mathcal{A}_5$, so hat K ein starres Zerlegungsgesetz.
Ist $n \neq 6$, so hat K ein horizontal starres Zerlegungsgesetz.

γ) Ist $n \neq 6$ und $G \neq \mathrm{PGL}_3(2)$, so ist K horizontal starr.
Ist $G \neq \mathcal{A}_5$ und $G \neq \mathrm{PGL}_3(2)$, so ist K starr.

Keine der Voraussetzungen ist entbehrlich.

Zum *Beweis* von a): Daß die Fälle $n \leq 3$ nicht vorliegen können, überprüft man unmittelbar. (Siehe aber auch Satz (5.3).)

Fall $n = 4$: Ist die Galoisgruppe abelsch, so kann natürlich keine echte Kronecker-Äquivalenz auftreten; die Fälle $\mathcal{A}_4$ und $\mathcal{S}_4$ sind gemäß Satz (5.3) geklärt. Als einzige Galoisgruppe bleibt dann nur noch die Diedergruppe der Ordnung 8, die man unmittelbar überprüfen kann. [Stellt man die Diedergruppe $G = D_8$ als Symmetriegruppe des Quadrats dar, so sieht man sofort, daß die Menge der Permutationen mit einem Fixpunkt (dies ist gerade U^G für die Fixgruppe U einer Ziffer) 3 Elemente umfaßt. Die einzigen darin enthaltenen Untergruppen U' sind die (in G zueinander konjugierten) Fixgruppen einer Ziffer.]

Fall $n = 5$: Gemäß Satz (5.6),b) genügt es, die nicht auflösbaren Galoisgruppen vom Grad 5 zu betrachten. Da die kleinste nicht-auflösbare Gruppe die Ordnung 60 hat, sind dies aber lediglich die Gruppen $\mathcal{A}_5$ und $\mathcal{S}_5$, so daß wieder aus (5.3), a),b) die Behauptung folgt.

Fall $n = 7$: Wir benutzen die bekannte Liste der möglichen Galoisgruppen von Polynomen kleinen Grades (≤ 7). (Siehe etwa J. McKay: Some remarks on computing Galois groups, SIAM J. Comput. **8** (1979) 344-347. Eine umfassendere Liste findet man bei G. Butler, J. McKay: The transitive groups of degree up to eleven, Comm. in Algebra **11** (1983) 863-911.) Wir entnehmen daraus, daß die einzige nicht-auflösbare Galoisgruppe vom Grad 7 verschieden von $\mathcal{A}_7$ und $\mathcal{S}_7$ die $G_{168} = \mathrm{PGL}_3(2)$ mit ihrer durch die natürliche Operation auf $\mathbb{F}_2^3 \setminus \{0\}$ gegebenen Einbettung in $\mathcal{S}_7$. Aus der schon beim Beispiel (4.8),b) erwähnten Übersicht über alle Untergruppen von $G_{168} = \mathrm{PSL}_2(7)$ entnimmt man, daß G genau zwei Konjugationsklassen von Untergruppen vom Index 7 hat, die isomorph sind zu $\mathcal{S}_4$. Daß diese Untergruppen elementweise konjugiert sind, überprüft man relativ leicht. Nach (5.6),b) sind die Gruppen dann auch Gaßmann-äquivalent in G.

Fall $n = 6$: Den für $n = 6$ genannten Ausnahmefall $G \simeq \mathcal{A}_4$ haben wir bereits in (4.4) b) kennengelernt. Zum Nachweis, daß es keine weiteren gibt, benötigt man umfangreichere Rechnungen. Mit den expliziten Angaben der möglichen Galoisgruppen G vom Grad 6 als Untergruppen von $\mathcal{S}_6$, wie sie bei McKay, l.c., zu finden sind, kann man die zur Fixgruppe $U = \mathrm{Fix}_G(6)$ in G elementweise konjugierten Untergruppen mit Hilfe von CAYLEY bestimmen. [CAYLEY ist ein auf dem CDC-Rechner am hiesigen Rechenzentrum implementiertes Programmsystem für gruppentheoretische Rechnungen. Es beinhaltet unter vielem anderem den Neubüser-Algorithmus zur Bestimmung der Untergruppen einer Gruppe nicht zu großer Ordnung und gestattet viele der üblichen gruppentheoretischen Rechnungen. Insbesondere Permutationsgruppen lassen sich gut behandeln, aber auch präsentierte Gruppen.] Da wir wieder nach Satz (5.3) nur Galoisgruppen verschieden von $\mathcal{A}_6$ und $\mathcal{S}_6$ untersuchen müssen, hat die größte auftretende Gruppe, die $\mathrm{PGL}_2(5)$, die Ordnung 120, so daß alle Gruppen einer Untersuchung mittels CAYLEY ohne unzumutbaren (Rechenzeit-)Aufwand zugänglich sind.

Ad b): Da die im Ausnahmefall für $n = 7$ genannten Körper K und K' arithmetisch äquivalent sind (siehe (5.6),a)), folgt α) unmittelbar aus a). Wegen (5.2),b) folgt γ) aus α) und β).

Ad β): Da für die in a) unter $n = 6$ genannten Fälle der Körper K' galoissch ist über k ($\mathcal{V}_4 \triangleleft \mathcal{A}_4$), ist $\widetilde{K'} \neq \tilde{K}$, und daher sind K und K' nicht Bauer-äquivalent. Dies beweist die Starrheit des Zerlegungsgesetzes von K für $G \neq \mathcal{A}_5$. Für $n \neq 6$ ist nach den Resultaten von a) der Körper K minimal, sogar von kleinstem Grad in seiner Kroneckerklasse. Daher sind je zwei

Kronecker-äquivalente Körper dieses Grades Bauer-äquivalent (Prop. (5.4),b)). Aus dem eben bewiesenen Starrheitsresultat folgt also, daß das Zerlegungsgesetz von K auch horizontal starr ist; wegen der geforderten Gradgleichheit gilt dies auch im $\mathcal{A}_5$-Fall.

c. Zerfallende Erweiterungen

In diesem Abschnitt wollen wir Erweiterungen $K|k$ mit sog. *zerfallender* galoisscher Hülle untersuchen. Das soll heißen: Die galoissche Hülle von K ist von der Form $\tilde{K} = KL$ mit einer galoisschen Erweiterung $L|k$, $L \cap K = k$. Die Galoisgruppe $G(\tilde{K}|k)$ ist dann semidirektes Produkt von $U = G(\tilde{K}|K)$ mit dem Normalteiler $H = G(\tilde{K}|L)$, oder mit anderen Worten, die Gruppenerweiterung

$$1 \to U \to G \to G(L|k) \to 1$$

zerfällt. Für das angestrebte Resultat kann man die Forderung $L \cap K = k$ sogar noch modifizieren:

(5.8) Satz: *Sei $K|k$ eine Zahlkörpererweiterung mit galoisscher Hülle $N := KL$ mit $L|k$ galoissch und*

$$\text{a)} \quad L \cap K = k \qquad \textit{oder} \qquad \text{b)} \quad L|k \textit{ abelsch}\,.$$

Dann ist K minimal in seiner Kroneckerklasse und sein Zerlegungsgesetz ist starr und horizontal starr.

Beweis: Sei K' Kronecker-äquivalent zu K und $K' \subseteq N$. (Wir setzen zunächst weder voraus, daß $\widetilde{K'} = \tilde{K} = N$, noch daß $(K\colon k) = (K'\colon k)$ ist.) Mit den Fixgruppen U, U' und H von K, K' bzw. L in $G := G(N|k)$ gilt dann:

$$U^G = U'^G\,, \quad U \cap H = \{1\}\,, \quad UH =: G_0 \lhd G\,.$$

Wir zeigen nun:

$$(*) \qquad U' \cap H = \{1\} \quad \text{und} \quad U'H = G_0 = UH\,,$$

d.h. U' ist ebenfalls ein Komplement zu H in $G_0 = UH$.

Zunächst gilt $U' \subseteq U'^G = U^G \subseteq G_0$, und wegen der Normalteilereigenschaft von H in G folgt

$$U \cap H = \{1\} \implies U'^G \cap H = U^G \cap H = \{1\} \implies U' \cap H = \{1\}\,.$$

Es bleibt zu zeigen:

$$G_0 = UH = U'H.$$

Für $g = uh \in G_0$ mit $u \in U$ und $h \in H$ existieren wegen $U^G = U'^G$ Elemente $\sigma \in G$ und $u' \in U'$ mit $u = \sigma u' \sigma^{-1}$, also $uh = \sigma u' \sigma^{-1} h = \sigma \cdot u'h' \cdot \sigma^{-1}$ mit $h' := \sigma h \sigma^{-1} \in H$. Dies zeigt

$$G_0^G = (UH)^G = (U'H)^G\,.$$

Im Falle a): $G_0 = G$ erhält man $G = (U'H)^G$, woraus bekanntlich $G = U'H$ folgt. Im Falle b) schließt man man zunächst

$$(G_0/H)^{G/H} = (U'H/H)^{G/H}\,,$$

um dann mit der Kommutativität von $G/H = G(L|k)$ zu folgern

$$G_0/H = U'H/H\,, \text{ also } G_0 = U'H\,.$$

Da U und U' Komplemente von H in G_0 sind, induziert die kanonische Abbildung $\bar{}\colon G_0 \to G_0/H$ Isomorphismen $\phi\colon U \xrightarrow{\sim} G_0/H$, $u \mapsto \bar{u}$, und entsprechend ϕ' für U'. Sei $\psi := \phi'^{-1} \circ \phi\colon U \xrightarrow{\sim} U'$ der so entstehende Isomorphismus zwischen U und U'. Um nun für alle Konjugationsklassen $C(\sigma)$ von G

$$\#(C(\sigma) \cap U) = \#(C(\sigma) \cap U')$$

zu zeigen, genügt wegen der Bijektivität von ψ und aus Symmetriegründen der Nachweis von

$$\psi(C(\sigma) \cap U) \subseteq C(\sigma)\,.$$

Sei also $\sigma \in G$ und o. E. $C(\sigma) \cap U \neq \emptyset$. Wegen $U^G = U'^G$ ist dann auch $C(\sigma) \cap U' \neq \emptyset$, also $C(\sigma) = C(u')$ für ein $u' \in U'$. Für $u \in C(\sigma) \cap U = C(u') \cap U$, also $u = u'^\tau = \tau^{-1}u'\tau$ mit $\tau \in G$, gilt im Falle a)

$$\psi(u) = \phi'^{-1}(\bar{\tau}^{-1}\bar{u'}\bar{\tau}) = \phi'^{-1}(\bar{\tau})^{-1} \cdot u' \cdot \phi'^{-1}(\bar{\tau}) \in C(u')\,.$$

Im Falle b) gilt sogar

$$\psi(u) = \phi'^{-1}(\bar{\tau}^{-1}\bar{u'}\bar{\tau}) = \phi'(\bar{u'}) = u'\,.$$

Damit ist gezeigt, daß jeder in $N = \tilde{K}$ enthaltene, zu K über k Kronecker-äquivalente Körper K' bereits arithmetisch-äquivalent zu K ist. Damit ist das Zerlegungsgesetz von K starr. Unter Benutzung von Prop. (5.4) folgt daraus aber auch, daß K minimal ist in seiner Kroneckerklasse, ja daß sogar alle Minimalkörper der Kroneckerklasse denselben Grad $(K\colon k)$ haben. Damit ist das Zerlegungsgesetz auch horizontal starr.

Ein typisches Anwendungsbeispiel dieses Satzes sind die Radikalerweiterungen $K = k(\sqrt[n]{a})$, denn die galoissche Hülle einer solchen Radikalerweiterung ist $\tilde{K} = k(\sqrt[n]{a}, \zeta_n) = KL$ mit dem abelschen Erweiterungskörper $L = k(\zeta_n)$ von k.

(5.9) Korollar: *Reine Erweiterungen $K = k(\sqrt[n]{a})$ von k sind minimal in ihrer Kroneckerklasse und ihr Zerlegungsgesetz ist starr und horizontal starr.*

Dies läßt sich nun noch weiter verschärfen zu folgendem

(5.10) Satz: *Sei $K = \mathbb{Q}(\sqrt[n]{a})$ eine reine Erweiterung n-ten Grades von $\mathbb{Q}$. Dann gilt:*

a) *Ist $n \not\equiv 0 \bmod 8$, so ist K starr und horizontal starr.*

b) *Ist $n \equiv 0 \bmod 8$ und zusätzlich $K \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$, so gibt es bis auf Konjugation genau einen weiteren zu K Kronecker- (und damit arithmetisch) äquivalenten Körper K' mit $K' \subseteq \tilde{K} = \mathbb{Q}(\sqrt[n]{a}, \zeta_n)$ bzw. mit $(K'\colon \mathbb{Q}) = n$.*

Für n=8 ist dieser gegeben durch $K' = \mathbb{Q}(\sqrt[8]{16a})$.

Zu diesem Satz stellen sich unmittelbar folgende Probleme:
1) Man untersuche den allgemeinen Fall mit beliebigem Grundkörper k statt $\mathbb{Q}$.
2) Man verzichte auf die Voraussetzung $K \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.
Auf den Beweis von Satz (5.10) muß hier aus Zeitgründen verzichtet werden.

d. Absolut starre Zahlkörper

In den beiden vorherigen Abschnitten haben wir eine Reihe von Beispielen für starre und horizontal starre Körper und Zerlegungsgesetze kennengelernt, aber – abgesehen vom Grundkörper k selbst – bislang noch kein einziges Beispiel absolut starrer Körper oder Zerlegungsgesetze. Nun gilt der folgende, nach Vorarbeiten von Jehne (1974), Klingen (1975/80) im Jahre 1987 von J. Saxl bewiesene

(5.11) Satz: *Quadratische Körpererweiterungen $L = k(\sqrt{a})$ von k sind absolut starr, d. h. sie sind durch ihr schwaches Zerlegungsgesetz $D(L|k)$ unter allen Körpererweiterungen von k eindeutig festgelegt.*

Der *Beweis* dieses Satzes beruht ganz entscheidend auf der 1983 abgeschlossenen vollständigen Klassifikation aller endlichen einfachen Gruppen. Die Reduktion auf ein Problem über endliche einfache Gruppen beruht auf folgenden Überlegungen (Jehne):

Angenommen, L ist nicht absolut starr, dann existiert ein nicht-konjugierter, über k Kronecker-äquivalenter Körper K. Da $L|k$ galoissch ist, muß K ein echter Oberkörper sein (Satz von Bauer). O. E. sei K minimal mit dieser Eigenschaft, also $K|L$ atomar. Es sei nun $N|k$ die

galoissche Hülle von K, und damit $N \supseteq K \supset L$. Dann ist die Fixgruppe H von L ein Normalteiler vom Index 2 in $G = G(N|k)$, der von den G-Konjugierten der maximalen Untergruppe $U = G(N|K)$ überdeckt wird. Ist $\sigma \in G \setminus H$ beliebig, so sind die G-Konjugierten gerade die H-Konjugierten von U und $U' := U^\sigma$. Man erhält also

$$U \subset H \triangleleft G, \quad (G\colon H) = 2, \quad H = U^H \cup U'^H$$

mit zwei unter $\operatorname{Aut} H$, aber nicht in H konjugierten maximalen Untergruppen U und U' von H. [Die Konjugation mit $\sigma \in G$ induziert einen Automorphismus von H.] Diese Untergruppen induzieren zwei *primitive,* unter $\operatorname{Aut} H$ konjugierte Permutationsdarstellungen gleichen Grades von H. Ein wichtiger Schritt ist nun der Nachweis, daß H einen eindeutig bestimmten minimalen Normalteiler H_0 hat; dieser ist eine einfache, nicht abelsche Gruppe. Die beiden Permutationsdarstellungen von H induzieren durch Einschränkung zwei treue Permutationsdarstellungen von H_0, die wegen der Primitivität auf H immer noch transitiv auf H_0 sind, und so zwei Untergruppen U_0 und U_0' von H_0 von gleichem Grad bestimmen, die unter $\sigma \in G \subset \operatorname{Aut} H_0$ konjugiert sind, und deren H_0-Konjugierte die einfache Gruppe H_0 überdecken.

Da eine Gruppe nicht Vereinigung der Konjugierten einer echten Untergruppe sein kann, muß der Automorphismus $\sigma \in \operatorname{Aut} H_0$ ein äußerer Automorphismus sein:

$$\operatorname{Out} H_0 := \operatorname{Aut} H_0 / H_0) \neq 1\,.$$

Schon diese Tatsache schließt eine Reihe von einfachen Gruppen aus; dazu gehören viele der sporadischen endlichen einfachen Gruppen (siehe An ATLAS of finite groups, ed. J. Conway, R. Curtis, S. Norton, R. Parker).

Da die Untergruppen U_0 und U_0' von H_0 isomorph sind und ihre H_0-Konjugierten H_0 überdecken, treten in der maximalen Untergruppe U_0 dieselben Elementordnungen wie in der einfachen Gruppe H_0 selbst auf. Ein Konzept von R. Brandl zeigt, daß dies für die sporadischen einfachen Gruppen nicht möglich ist; diese haben nämlich die folgende Eigenschaft:

Für jede sporadische einfache Gruppe existieren zwei natürliche Zahlen a und b, so daß je zwei Elemente $\alpha, \beta \in H_0$ mit $\operatorname{ord}\alpha = a$ und $\operatorname{ord}\beta = b$ bereits H_0 erzeugen.

Siehe dazu auch die Diplomarbeit von P. Martens: *Charakterisierung quadratischer Zahlkörper durch ihre Kroneckermengen – Untersuchung der sporadischen und klassischen endlichen einfachen Gruppen –*, U Köln 1987, in der gezeigt wird, daß man die Zahlen a, b einheitlich wählen kann als den maximalen Primteiler der Gruppenordnung und als die größte, davon verschiedene Ordnung eines Elementes der sporadischen Gruppe.

Für die Gruppen vom Lie-Typ ist der Beweis erheblich aufwendiger und kann hier nicht näher erläutert werden. Auch dabei leistet der schon erwähnte 'Atlas' gute Dienste. Klassische einfache Gruppen sind ebenfalls in der Diplomarbeit von P. Martens behandelt.

Angesichts der vielen Beispiele von echter Kronecker-Äquivalenz und des großen Aufwandes, der zum Beweis von Satz (5.11) notwendig war, ist es umso erstaunlicher, daß innerhalb kurzer Zeit weitere absolut starre Körper gefunden werden konnten. Schlüssel dazu war das folgende gruppentheoretische Resultat, dessen Beweis auf dem Beweis von (5.11) basiert.

(5.12) Satz: (Praeger 1987) *Sei G eine endliche Gruppe, H eine Normalteiler vom Index 4 und U eine maximale Untergruppe von H mit*

$$U_G := \bigcap_{\sigma \in G} U^\sigma = \{1\} \quad \textit{und} \quad U^G = H^G = H\,.$$

Dann ist G ein semidirektes Produkt der elementar abelschen Gruppe $A = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ der Ordnung 9 mit der zyklischen oder Quaternionengruppe der Ordnung 8, und H umfaßt A.

Die allgemeine lineare Gruppe $\mathrm{GL}_2(3)$, die Automorphismengruppe von A, hat die Ordnung 48 und enthält als Untergruppen der Ordnung 8 drei konjugierte zyklische, drei konjugierte

Dieder- und eine Quaternionengruppe. Dadurch operieren diese Gruppen der Ordnung 8 auf A und bestimmen so ein semidirektes Produkt G der Ordnung 72. Dabei operieren die zyklische und die Quaternionengruppe *transitiv* auf den zyklischen Untergruppen der Ordnung 3 in A. Daraus ergibt sich, daß in den entsprechenden semidirekten Produkte G Untergruppen H und U mit den Eigenschaften des Satzes existieren.

Daraus entnimmt man nun zunächst folgende

(5.13) Bemerkung: Es gibt Diedererweiterungen, die kubische Erweiterungen besitzen, zu denen sie Kronecker-äquivalent sind. (Für Quaternionenerweiterungen und zyklische Erweiterungen vom Grad 8 war dies bekannt.)

Durch Kombination des Praeger'schen Resultates mit Überlegungen über Einbettungsprobleme erhält man das folgende Starrheitsresultat, das die absolut starren galoisschen Erweiterungen vierten Grades explizit bestimmt:

(5.14) Satz: *Sei k ein Zahlkörper, $L|k$ eine galoissche Erweiterung vom Grad 4. Dann sind äquivalent:*

i) L ist absolut starr.

ii) $L|k$ ist zyklisch und in einer der lokalen Erweiterungen $L_{\mathcal{P}}|k_{\mathfrak{p}}$ ($\mathfrak{p}$ eine Stelle von k, endlich oder unendlich) ist -1 keine Norm

oder

$L = k(\sqrt{a}, \sqrt{b})$ ist eine biquadratische Erweiterung und die quadratische Form $aX^2 + bY^2 + abZ^2$ ist nicht $k_{\mathfrak{p}}$-isomorph zu $X^2 + Y^2 + Z^2$ (für eine Stelle $\mathfrak{p}$ von k).

Im Falle $k = \mathbb{Q}$ sind diese Bedingungen völlig explizit formulierbar und verifizierbar, z. B. im biquadratischen Falle in Termen der Vorzeichen von $a, b \in \mathbb{Z}$) sowie der Legendresymbole $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right)$ (p Primzahl). So sind alle imaginären galoisschen Erweiterungen $L|\mathbb{Q}$ vom Grad 4 absolut starr (über $\mathbb{Q}$), d.h. durch ihr schwaches Zerlegungsgesetz vollständig festgelegt.

Zum Abschluß sei noch angemerkt, daß im Gegensatz zum quadratischen Fall, in dem das Resultat (Satz (5.11)) rein gruppentheoretischer Natur ist und für alle quadratischen Erweiterungen gleichermaßen gilt, im Fall vierten Grades das Ergebnis zahlentheoretischer Natur ist und die absolute Starrheit solcher Erweiterungen vom konkreten Körper abhängt. So ist z. B. der Körper $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ absolut starr, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ hingegen nicht.

Literaturhinweise

Diese Literaturangaben umfassen nur die notwendigsten Hinweise und sind hier weitgehend in der Reihenfolge aufgeführt, in der sie in der Vorlesung benötigt werden.

1. Zahlentheoretische Grundlagen

[L] S. Lang: Algebra. Addison-Wesley, Reading,Mass. 1965
Ch. IX, §§1,2; Ch. XIII, §5; Ch. II, §2

[G] L.J. Goldstein: Analytic Number Theory. Prentice Hall, Englewood Cliffs 1971, Ch. 2

[T] S. Lang: Algebraic Number Theory. Addison Wesley, Reading,Mass. 1968
Ch. I, §2, §6; Ch. III, §3

2. Primzerlegung und Gruppentheorie

[T] Ch. I, §5

[G] Ch. 5-4, 5-5

[L] Ch. I, §5

3. Primzerlegung und Zetafunktionen

[N] J. Neukirch: Class Field Theory, Springer, Berlin-Heidelberg-New York 1986, Ch. V

[G] Ch. 9; Ch. 14-1

[T] Ch. VIII

4. Arithmetische Ähnlichkeiten

W.Jehne: Kronecker classes of algebraic number fields. J. Number Theory **9** (1977) 279-320

M. Bauer: Über Kreisteilungsgleichungen. Arch. Math. Phys. **6** (1904) 220

F. Gaßmann: Bemerkungen zur vorstehenden Arbeit von Hurwitz. Math. Z. **25** (1926) 665-675

A. Schinzel: On a theorem of Bauer and some of its applications. Acta Arithm. **11** (1966) 333-344

W. Jehne: Die Entwicklung des Umkehrproblems der Galoisschen Theorie. Math. Phys. Sem. Berichte **24** (1979) 1-35

B.H. Matzat: Über das Umkehrproblem der Galoisschen Theorie. Erscheint in Jber. DMV **90**.

R. Perlis: On the equation $\zeta_K(s) = \zeta_{K'}(s)$. J. Number Theory **9** (1977) 342-360

I. Gerst: On the theory of nth power residues and a conjecture of Kronecker. Acta Arithm. **17** (1970) 121-139

W. Trinks: Arithmetisch ähnliche Körper. Diplomarbeit, Karlsruhe 1969.

[N] Ch. V, §4

N. Klingen: Zahlkörper mit gleicher Primzerlegung. J. reine angew. Math. **299/300** (1978) 342-384

5. Starrheit von Zerlegungsgesetzen und Zahlkörpern

N. Klingen: Atomare Kronecker-Klassen mit speziellen Galoisgruppen. Abh. Math. Sem. Hamb. **48** (1979) 42-53

[H] B. Huppert: Endliche Gruppen I. Springer, Berlin-Heidelberg-New York 1967. Kap. II, Kap. VI.

[S] J.-P. Serre: Linear representations of finite groups, Springer Grad. Text Math. 42, Berlin-Heidelberg-New York 1977. Ch. 1,2.

J. McKay: Some remarks on computing Galois groups. SIAM J. Comput. **8** (1979) 344-347

G. Butler, J. McKay: The transitive groups of degree up to eleven. Comm. Alg. **11** (1983) 863-911

N. Klingen: Über schwache quadratische Zerlegungsgesetze. Comment. Math. Helvetici **55** (1980) 645-651

J. Saxl: On a question of W. Jehne concerning covering subgroups of groups and Kronecker classes of fields. Erscheint in J. London Math. Soc.

[A] J. Conway, R. Curtis, S. Norton, R. Parker (Eds.): An ATLAS of finite groups. Clarendon Press, Oxford 1985

Ch. Praeger: Covering subgroups of groups and Kronecker classes of fields. Erscheint in J. Algebra