Professor Dr. Jürgen Ritter
Lehrstuhl für Algebra und Zahlentheorie
Institut für Mathematik · Universität Augsburg

Skript zur Vorlesung Algebra 2 , Sommersemester 2007

Kapitel 1. Ringe und Moduln

Es wird zuerst an die Begriffe Ring R, Ideal $\mathfrak{a}$ und Restklassenring $R/\mathfrak{a}$ erinnert: vergleiche dazu das Skript zur Vorlesung Algebra 1 im WS 2006/2007 .

Unsere Ringe in diesem Kapitel sind stets kommutativ (bez. $\cdot$); sie müssen nicht unbedingt eine 1 enthalten. Falls stets $[\, ab = 0 \implies a = 0 \text{ oder } b = 0\,]$ für Elemente $a, b \in R$ gilt, heißt R *nullteilerfrei* oder auch *Integritätsbereich*.

Idealoperationen	sind:	Durchschnitt	$\mathfrak{a} \cap \mathfrak{b} = \{r \in R : r \in \mathfrak{a}, r \in \mathfrak{b}\}$
		Summe	$\mathfrak{a} + \mathfrak{b} = \{a + b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$
		Produkt	$\mathfrak{a}\mathfrak{b} = \{\sum_{i=0}^{n} a_i b_i : n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$

Dies sind wieder Ideale und es gilt $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$, $\mathfrak{a}, \mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}$; die Vereinigung $\mathfrak{a} \cup \mathfrak{b}$ der Ideale $\mathfrak{a}$ und $\mathfrak{b}$ von R ist allerdings i.A. kein Ideal.

Hauptideale $\mathfrak{a}$ sind von der Form $\mathfrak{a} = Ra = \langle a \rangle = \{ra : r \in R\}$ für Elemente $a \in R$. Ein Ideal $\mathfrak{a}$ heißt *endlich erzeugt*, falls $\mathfrak{a}$ Summe von endlich vielen Hauptidealen $\mathfrak{a}_i = Ra_i$, $1 \leq i \leq n$, ist; Notation: $\mathfrak{a} = \langle a_1, \cdots, a_n \rangle$; die a_i heißen *Erzeugende* von $\mathfrak{a}$.

Ringe R, in denen jedes Ideal endlich erzeugt ist, heißen *noethersch*. Beispiel: Hauptidealringe (das sind nullteilerfreie Ringe mit 1, in denen jedes Ideal Hauptideal ist); Gegenbeispiel: der Polynomring $R = \mathbb{Q}[x_1, x_2, \cdots]$ in unendlich (abzählbar) vielen Unbestimmten über $\mathbb{Q}$. Ist R noethersch und $f : R \to S$ ein Ringhomomorphismus, so ist auch $f(R)$ noethersch.

LEMMA. *R ist genau dann noethersch, wenn jede aufsteigende Kette von Idealen*

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \cdots$$

nach endlich vielen Schritten stationär wird, d.h. $\exists\, N : i > N \implies \mathfrak{a}_i = \mathfrak{a}_N$.

SATZ. [Hilbert] *R noethersch $\implies$ $R[x]$ noethersch.*

Hier bezeichnet, wie üblich, $R[x]$ den Polynomring in einer Unbestimmten über R.

Zwei Ideale $\mathfrak{a}, \mathfrak{b}$ heißen *coprim*, wenn $\mathfrak{a} + \mathfrak{b} = R$ gilt. Diese Redeweise hat ihren Ursprung in der Definition $[\, \mathfrak{a} | \mathfrak{b} \iff \mathfrak{b} \subset \mathfrak{a}\,]$, was zu $\mathrm{ggT}(\mathfrak{a}, \mathfrak{b}) \stackrel{\text{def}}{=} \mathfrak{a} + \mathfrak{b}$ führt und jedenfalls in Hauptidealringen gerechtfertigt ist.

Chinesischer Restsatz.

1. *Gegeben seien $x, y \in R$ und Ideale $\mathfrak{a}, \mathfrak{b}$. Dann gilt:*

$$x \equiv y \mod \mathfrak{a}+\mathfrak{b} \implies \exists\, r \in R : r \equiv x \mod \mathfrak{a}\,,\ r \equiv y \mod \mathfrak{b}\,.$$

2. *Gegeben seien $x_1, \cdots, x_n \in R$ und Ideale $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$. Es gilt, falls $1 \in R$:*

$$\mathfrak{a}_i + \mathfrak{a}_j = R\ (\forall\, i \neq j) \implies \exists r \in R : r \equiv x_i \mod \mathfrak{a}_i\,.$$

3. $\mathfrak{a}_i + \mathfrak{a}_j = R\ (\forall\, i \neq j) \implies R/\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n \simeq R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_n$ *(kanonisch)*

Lokalisierungen:

R sei ein Ring mit 1 und $M \ni 1$ eine multiplikativ abgeschlossene Teilmenge von R. Dann wird

$R_M = \{[a,m] : a \in R, m \in M;\ [a_1,m_1] = [a_2,m_2] \iff \exists\, m \in M : m(a_1m_2 - a_2m_1) = 0\}$
über
$[a_1,m_1] + [a_2,m_2] = [a_1m_2 + a_2m_1, m_1m_2]$
$[a_1,m_1] \cdot [a_2,m_2] = [a_1a_2, m_1m_2]$

ein Ring.

Beobachtungen:

1. $0 \in M \implies R_M = \{0\}$
2. Statt $[a,m]$ schreibt man suggestiver $\frac{a}{m}$.
3. $R \to R_M\,,\ a \mapsto \frac{a}{1}$ ist ein Homomorphismus von Ringen.
4. Falls M keinen Nullteiler von R (also kein $a \in R$ mit $a|0$) enthält, gilt

$$\frac{a_1}{m_1} = \frac{a_2}{m_2} \iff a_1m_2 = a_2m_1$$

und $\quad R \to R_M$ ist injektiv.

Sonderfälle:

1. $\mathfrak{p}$ sei ein *Primideal* in R (m.a.W.: $\mathfrak{p}$ ist ein Ideal mit nullteilerfreiem Restklassenring $R/\mathfrak{p}$); $M \overset{\text{def}}{=} R \setminus \mathfrak{p}$. *Wir schreiben dann $R_\mathfrak{p}$ statt R_M!* Ist $\mathfrak{a}$ ein Ideal in R, so ist $\mathfrak{a}_\mathfrak{p} = \{\frac{a}{m} : a \in \mathfrak{a}, m \notin \mathfrak{p}\}$ ein Ideal in $R_\mathfrak{p}$; umgekehrt, ist $\mathfrak{A}$ ein Ideal in $R_\mathfrak{p}$, so ist dessen Zählermenge $\mathfrak{a} = \{a \in R : \exists\, m \notin \mathfrak{p} \text{ mit } \frac{a}{m} \in \mathfrak{A}\}$ ein Ideal in R und $\mathfrak{a}_\mathfrak{p} = \mathfrak{A}$. Insbesondere ist $R_\mathfrak{p}$ mit R noethersch. Die Abbildung $R \to R_\mathfrak{p}$ induziert eine Inklusion $R/\mathfrak{p} \rightarrowtail R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$.
2. Ist R nullteilerfrei, so ist $M = R \setminus \{0\}$ zulässig. Dann ist R_M ein Körper und liegt in jedem R enthaltenden Körper. Wir nennen $R_M = \mathrm{Quot}(R)$ den Quotientenkörper von R. Beispiel: $R = \mathbb{Z}$, $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$.

Ein Ring R heißt *lokal*, falls alle Nichteinheiten ein Ideal $\mathfrak{p}$ bilden. (*Erinnerung:* $u \in R$ heißt *Einheit*, falls $ua = 1$ für ein $a \in R$ gilt; die Gruppe der Einheiten in R wird mit $R^\times$ bezeichnet.) Dieses Ideal $\mathfrak{p}$ ist dann maximal, i.e. $R/\mathfrak{p}$ ein Körper. Beispiel eines lokalen Ringes ist $R_\mathfrak{p}$ mit einem beliebigen Ring R mit 1 und einem Primideal $\mathfrak{p}$. Ein Ring R heißt *semilokal*, falls er nur endlich viele maximale Ideale enthält. Beispiel: $\mathbb{Z}/n$ mit $n \neq 0$. Lokale Ringe sind semilokal:

LEMMA. *Ein Ring ist genau dann lokal, wenn er nur ein einziges maximales Ideal enthält.*

Dazu eine Bemerkung: Zufolge des Zornschen Lemmas enthalten Ringe mit 1 stets maximale Ideale.

NAKAYAMAS LEMMA. *R sei lokal mit maximalem Ideal $\mathfrak{p}$. Ist $\mathfrak{a}$ ein endlich erzeugtes Ideal in R mit $\mathfrak{p}\mathfrak{a} = \mathfrak{a}$, so ist $\mathfrak{a} = 0$.*

ZPE- und Euklidische Ringe R:

Dies sind beides Integritätsbereiche (mit 1). Für ZPE-Ringe wird des weiteren gefordert

> *Jedes Ringelement $\neq 0$ ist bis auf Einheitsfaktoren $e \in R$ eindeutig als (endliches) Produkt von Primelementen schreibbar* [1]*. Dabei heißt ein Element $p \in R$ prim, falls das von ihm erzeugte Hauptideal ein Primideal ist (i.e., $p|ab \implies p|a$ oder $p|b$).*

Für euklidische Ringe R wird gefordert

$$\exists\, N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0} \text{ mit } N(ab) \geq \max(N(a), N(b)) \text{ und}$$

$$[\,\forall\, 0 \neq a\,,\, b \in R\, \exists\, v, r \in R : b = va + r \;\&\; r = 0 \text{ oder } N(r) < N(a)\,]\,.$$

SATZ. *R Euklidisch $\implies$ R Hauptidealring $\implies$ R ZPE*

Moduln über Ringen:

R sei ein Ring mit 1 und M eine abelsche Gruppe. M heißt *R-Modul*, falls es eine Operation von R auf M gibt [i.e. eine Funktion $R \times M \to M$, $(r, m) \mapsto rm$], so daß

$$1m = m,\ (r_1 + r_2)m = r_1 m + r_2 m,\ (r_1 r_2)m = r_1(r_2 m),\ r(m_1 + m_2) = rm_1 + rm_2$$

für alle $m, m_1, m_2 \in M$ und alle $r, r_1, r_2 \in R$ gilt. Der Modulbegriff verallgemeinert also den des Vektorraums. Beachte, daß $rm = 0$ für ein $r \neq 0$ und ein $m \neq 0$ möglich ist. Erstes Beispiel eines Moduls ist jede abelsche Gruppe A, die nämlich auf natürliche Weise als $\mathbb{Z}$-Modul betrachtet werden kann (also $R = \mathbb{Z}$). Ein weiteres direktes Beispiel ist $M = R$; diesen Modul nennen wir auch den *regulären* Modul.

Eine Untergruppe N von M heißt *R-Untermodul* von M, falls $rn \in N$ für alle $r \in R$ und $n \in N$ gilt.

[1] natürlich wird die Reihenfolge der Faktoren nicht betrachtet

Untermoduloperationen sind:	Durchschnitt	$N_1 \cap N_2 = \{m \in M : m \in N_1, m \in M_2\}$
	Summe	$N_1 + N_2 = \{n_1 + n_2 : n_1 \in N_1, n_2 \in N_2\}$
	Idealprodukt	$\mathfrak{a}N = \{\sum_{i=0}^{k} a_i n_i : k \in \mathbb{N}, a_i \in \mathfrak{a}, n_i \in N\}$

Im letzten Fall ist $\mathfrak{a}$ ein Ideal in R. Alle drei Mengen, $N_1 \cap N_2, N_1 + N_2, \mathfrak{a}N$, sind tatsächlich R-Untermoduln von M.

Der Untermodul N von M heißt *zyklisch*, falls $N = Rm = \langle m \rangle = \{rm : r \in R\}$ für ein $m \in M$ gilt. N heißt *endlich erzeugt*, falls N Summe endlich vieler zyklischer Untermoduln Rm_i $(1 \leq i \leq k)$ ist; Notation: $N = \langle m_1, \cdots, m_k \rangle$; die m_i heißen *Erzeugende* von N.

Der R-Modul M heißt *noethersch*, falls alle seine Untermoduln endlich erzeugt sind.

LEMMA. *1. M noethersch, N Untermodul $\Longrightarrow$ N noethersch*

2. M noethersch $\Longleftrightarrow$ jede aufsteigende Kette von Untermoduln von M wird nach endlich vielen Schritten stationär $\Longleftrightarrow$ jede nichtleere Menge von Untermoduln von M besitzt ein im Sinne von ´$\subset$´ maximales Element

3. N sei ein Untermodul von M. Sind N und M/N noethersch, so auch M selbst.

4. $f : M_1 \to M_2$ sei ein Modulhomorphismus, also ein Homomorphismus von abelschen Gruppen mit $f(rm_1) = rf(m_1)$ $(\forall\, r \in R, \forall\, m_1 \in M_1)$. Ist M_1 noethersch, so auch $f(M_1)$.

5. Ist M endlich erzeugt und R noethersch, so auch M.

6. Ist R lokal mit maximalem Ideal $\mathfrak{p}$ und ist M endlich erzeugt, so gilt $\mathfrak{p}M = M$ nur für $M = \{0\}$.

Bemerkung: Wie bei Gruppen und Ringen gilt auch für Moduln

1. Ist $f : M \to N$ ein R-Modulhomomorphismus, so ist $f(M)$ ein Untermodul von N und $\ker(f) = \{m \in M : f(m) = 0\}$ ein Untermodul von M.
2. $M/\ker(f) \simeq \operatorname{im}(f) = f(M)$
3. Die Untermoduln von $f(M)$ entsprechen eineindeutig und inklusionstreu denjenigen von M, die $\ker(f)$ enthalten.

DEFINITION. *1. Ein endlich erzeugter R-Modul F heißt frei, wenn $F \simeq R^n \stackrel{\text{def}}{=} \underbrace{R \oplus \cdots \oplus R}_{n-\text{mal}}$; n heißt der Rang von F.*

2. Ein endlich erzeugter R-Modul P heißt projektiv, wenn P direkter Summand eines freien Moduls F ist.

Beobachtungen:

1. Ist F frei, so ist der Rang von F wohlbestimmt. Ist nämlich $\mathfrak{p}$ ein maximales Ideal von R, so folgt aus $F \simeq R^n$, daß $M/\mathfrak{p}M \simeq (R/\mathfrak{p})^n$, also daß $n = \dim_{R/\mathfrak{p}} M/\mathfrak{p}M$ ist.

2. Jeder endlich erzeugte Modul M ist homomorphes Bild eines freien Moduls F.

3. P ist projektiv genau dann, wenn es in jeder Situation

$$\begin{array}{ccc} & & P \\ & & g\downarrow \\ M & \overset{f}{\twoheadrightarrow} & N\,, \end{array}$$

mit R-Moduln M, N, einem Epimorphismus f und einem Homomorphismus g, einen Homomorphismus $h : P \to M$ mit $fh = g$ gibt:

$$\begin{array}{ccc} & & P \\ & \overset{h}{\swarrow} & g\downarrow \\ M & \overset{f}{\twoheadrightarrow} & N\,. \end{array}$$

DEFINITION. *M sei ein R-Modul mit R* torsionsfrei. *Der Untermodul*

$$\mathrm{tor}(M) = \{m \in M : \exists\, r \neq 0 \text{ mit } rm = 0\}$$

heißt der Torsionsuntermodul von M. Im Falle $M = \mathrm{tor}(M)$ heißt M ein Torsionsmodul; im Falle $tor(M) = 0$ heißt M torsionsfrei.

Beobachtungen:

1. Untermoduln von torsionsfreien Moduln sind torsionsfrei.

2. Freie Moduln (über Integritätsbereichen) sind torsionsfrei.

3. $M/\mathrm{tor}(M)$ ist torsionsfrei.

Nun sei R ein Ring, $\mathfrak{p}$ ein Primideal und M ein R-Modul. Wir *lokalisieren:*

$$M_{\mathfrak{p}} = \{\tfrac{m}{s} : m \in M,\, s \in R \setminus \mathfrak{p};\, \tfrac{m_1}{s_1} = \tfrac{m_2}{s_2} \iff \exists\, t \in R \setminus \mathfrak{p} : t(s_2 m_1 - s_1 m_2) = 0\}$$
$$\tfrac{m_1}{s_1} + \tfrac{m_2}{s_2} = \tfrac{s_2 m_1 + s_1 m_2}{s_1 s_2}\,,\ \tfrac{r}{s}\tfrac{m}{t} = \tfrac{rm}{st} \quad (t \in R \setminus \mathfrak{p})\,.$$

$M_{\mathfrak{p}}$ ist damit ein $R_{\mathfrak{p}}$-Modul. Ist M endlich erzeugt (über R), so auch $M_{\mathfrak{p}}$ (über $R_{\mathfrak{p}}$). Die natürliche Abbildung $M \to M_{\mathfrak{p}}\,,\ m \mapsto \frac{m}{1}$ ist injektiv, falls $[\, s \in R \setminus \mathfrak{p},\, 0 \neq m \in M \implies sm = 0\,]$ gilt; sie induziert $M/\mathfrak{p}M \to M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$.

Moduln über Hauptidealringen:

Vektorräume sind, sofern endlich dimensional, durch ihre Dimension schon vollständig bestimmt. Eine Klassifikation aller endlich erzeugten Moduln über einem gegebenen Ring R ist im allgemeinen nicht zu erreichen, wohl aber über Hauptringen. Im folgenden ist R ein Hauptidealring.

M sei ein endlich erzeugter R-Modul. Da R noethersch ist, ist deshalb auch M noethersch, also jeder Untermodul endlich erzeugt.

LEMMA 1. *Falls M Untermodul eines freien Moduls vom Rang n ist, ist M frei vom Rang $\leq n$.*

Das Lemma beweist man durch Induktion nach n; der Fall $n = 1$ zeigt im wesentlichen schon alles: $F = Rm \supset M \implies M = \langle am \rangle$ für ein $a \in R$.

LEMMA 2. *Falls M torsionsfrei ist, so schon frei.*

Dies erkennt man durch Einbettung von M in einen freien Modul.

LEMMA 3. *$M \simeq F \oplus T$ mit F frei und $T = \mathrm{tor}(M)$.*

Denn M/T ist frei, also projektiv.

DEFINITION. *$M = T$ sei ein Torsionsmodul. Ist $m \in M$, so heißt jedes Erzeugende vom Hauptideal $\{r \in R : rm = 0\}$ Ordnung von m (diese ist also nur bis auf Einheiten in R bestimmt).*

SATZ. *Ist $M = T$ ein Torsionsmodul, so ist M eine direkte Summe von zyklischen Moduln Rm_i $(1 \leq i \leq k)$ mit $\mathrm{ord}\,(m_i) | \mathrm{ord}\,(m_{i+1})$. Diese Ordnungen und die Anzahl k der Summanden sind durch M eindeutig bestimmt.*

Den Satz beweist man genauso wie den Hauptsatz über endlich abelsche Gruppen. Die Ordnungen $\mathrm{ord}\,(m_i)$ heißen übrigens die *Elementarteiler* von M.

FOLGERUNG. *1. Jede Matrix mit Einträgen aus dem Hauptidealring R kann durch die üblichen Zeilen- und Spaltenoperationen sowie durch Rechts- und Linksmultiplikationen mit (quadratischen) Matrizen der Form*

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & a & b & & \\ & & & c & d & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix}, \quad ad - bc = 1 \ [2]$$

auf die Form

$$\begin{pmatrix} a_1 & & & & \\ & \ddots & & & \\ & & a_k & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

mit $a_i \neq 0$ und $a_1 | a_2 | \cdots | a_k$ gebracht werden; k und, bis auf Einheiten, die a_i sind eindeutig.

[2] falls R euklidisch ist, braucht man diese Matrizen nicht

2. *Gilt $N \subset M$ mit endlich erzeugtem torsionsfreiem R-Modul M, so existieren Basen $m_1, \cdots, m_s$ von M und $a_1 m_1, \cdots, a_k m_k$ von N mit $a_i | a_{i+1}$ $(1 \leq i \leq k-1)$; wieder sind k und, bis auf Einheiten, die a_i eindeutig.*

Kapitel 2. Berechnung von Galoisgruppen G_f (über $\mathbb{Q}$)

Sei $f(x) \in \mathbb{Q}[x]$ ein normiertes Polynom vom Grad n, etwa

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0\,, \quad a_i = \frac{b_i}{h}\,,\ b_i, h \in \mathbb{Z}\,.$$

Multiplikation mit h^n führt f über in

$$g(hx) \stackrel{\text{def}}{=} h^n f(x) = (hx)^n + hb_{n-1}(hx)^{n-1} + \cdots + h^{n-1}b_0 \in \mathbb{Z}[x]\,,$$

also in ein normiertes ganzzahliges Polynom g, das offensichtlich denselben Zerfällungskörper L wie f hat. Wir nehmen deshalb von jetzt an $f(x) \in \mathbb{Z}[x]$, also $h = 1$, an.

$\omega_1, \cdots, \omega_n$ seien die Wurzeln von f in L und $\sqrt{d_f} = \prod_{i<j}(\omega_i - \omega_j)$ die Diskriminante. Uns interessieren nur irreduzible f, so daß insbesondere f separabel und $d_f \neq 0$ ist.

Es gilt: $d_f \in \mathbb{Z}$.

Um das einzusehen, und auch wegen unserer gewünschten Berechnung von $G_f = G_{L/\mathbb{Q}}$, müssen wir uns zuerst mit einem neuen *Ganzheitsbegriff* beschäftigen.

Definition. *$K/\mathbb{Q}$ sei eine endliche Körpererweiterung. Ein Element $\alpha \in K$ heiße ganz (über $\mathbb{Z}$ oder über $\mathbb{Q}$), wenn das irreduzible Polynom f_α von α über $\mathbb{Q}$ schon ganzrationale Koeffizienten hat:* $f_\alpha(x) \in \mathbb{Z}[x]$.

Zufolge des Gaußschen Lemmas ist offenbar dazu gleichwertig: $\exists\, h(x) \in \mathbb{Z}[x]$ normiert mit $h(\alpha) = 0$.

Satz 10. *$\alpha, \beta \in K$ seien ganz.*

1. *$\alpha \in \mathbb{Q} \implies \alpha \in \mathbb{Z}$; des weiteren: alle $z \in \mathbb{Z}$ sind ganz*
2. *$\alpha \pm \beta$ und $\alpha\beta$ sind ganz; die ganzen Elemente von K bilden also einen Ring $\mathfrak{o} = \mathfrak{o}_K$*
3. *$\forall\, \gamma \in K \exists\ \alpha \in \mathfrak{o}, 0 \neq n \in \mathbb{Z} : \gamma = \frac{\alpha}{n}$*
4. *$\mathfrak{o}$ ist ein freier $\mathbb{Z}$-Modul vom Rang $[K : \mathbb{Q}]$*
5. *ist $K/\mathbb{Q}$ galoissch mit Gruppe G, so gilt $\sigma(\mathfrak{o}) = \mathfrak{o}$ für alle $\sigma \in G$*
6. *ist p eine ganzrationale Primzahl, so existieren maximale Ideale $\mathfrak{p} \subset \mathfrak{o}$ mit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$; $\mathfrak{o}/\mathfrak{p}$ ist endlich; im galoisschen Fall gilt für zwei solche maximale Ideale $\mathfrak{p}_1, \mathfrak{p}_2$*

$$\exists\, \sigma \in G_{K/\mathbb{Q}} : \sigma(\mathfrak{p}_1) = \mathfrak{p}_2\,.$$

Hauptargument des Beweises von 2. ist:

$$\alpha \in K \text{ ganz } \iff \alpha \cdot M \subset M \text{ für einen endlich erzeugten } \mathbb{Z}-\text{Modul } M \subset K \ ,$$

und das wiederum folgt durch Einbringung eines geeigneten charakteristischen Polynoms in die Diskussion. Und 6. ist eine Konsequenz des chinesischen Restsatzes und der Norm.

Zurück zur Diskriminante. Weil alle ω_i ganz (über $\mathbb{Z}$) sind und $d_f \in \mathbb{Q}$, ist also tatsächlich $d_f \in \mathbb{Z}$.

Wir reduzieren nun die Situation modulo einer Primzahl p mit $p \nmid d_f$. Aus $f(x) \in \mathbb{Z}[x]$ wird $\overline{f}(x) \in \mathbb{F}_p[x]$: $\overline{f}(x) = x^n + \overline{a}_{n-1}x^{n-1} + \cdots + \overline{a}_0$.

Wähle jetzt ein maximales Ideal $\mathfrak{p}$ von $\mathfrak{o}_L$, das p enthält (jedes andere ist dann also $= \sigma(\mathfrak{p})$ mit $\sigma \in G_f$). Bezeichnet $\overline{\omega}_i = \omega_i \mod \mathfrak{p}$, so folgt

$$\overline{f}(x) = \prod_{i=1}^{n}(x - \overline{\omega}_i) \in \mathfrak{o}_L/\mathfrak{p}\,[x]$$

und also $\overline{d}_f = d_{\overline{f}}$. Daher erzwingt $p \nmid d_f$, daß $\overline{f}$ separabel ist.

Sei $\overline{L}$ der Zerfällungskörper von $\overline{f}$; insbesondere $\overline{L} \subset \mathfrak{o}_L/\mathfrak{p}$.

Satz 11. $\overline{L} = \mathfrak{o}_L/\mathfrak{p} \quad \& \quad G_{\overline{L}/\mathbb{F}_p} \leq G_f$

Aus $\overline{f}$ können wir $\overline{L}$ berechnen: hat $\overline{f}(x)$ die irreduzible Zerlegung $\overline{f}(x) = \prod_{i=1}^{t} g_i(x) \in \mathbb{F}_p[x]$ und ist n_i der Grad von g_i, so ist $\overline{L}$ der Körper mit p^{k_p} Elementen für $k_p = \mathrm{kgV}(n_i)$. Die Galoisgruppe $G_{\overline{L}/\mathbb{F}_p}$ ist deshalb zyklisch von der Ordnung k_p (mit dem Frobeniusautomorphismus $\varphi_{\overline{L}/\mathbb{F}_p}$ als Erzeugendem). Obiger Satz garantiert damit die Existenz von Elementen der Ordnung k_p in G_f für Primzahlen $p \nmid d_f$.

Bemerkungen zum Beweis des Satzes:

Definiere $G_\mathfrak{p} = \{\sigma \in G_f : \sigma(\mathfrak{p}) = \mathfrak{p}\}$. Dies ist eine Untergruppe (die Standuntergruppe von $\mathfrak{p}$) in G_f; sie heißt die Zerlegungsuntergruppe von $\mathfrak{p}$ über $\mathbb{Q}$. Jedes $\sigma \in G_\mathfrak{p}$ induziert einen Automorphismus auf $\mathfrak{o}_L/\mathfrak{p}$ und daraus gewinnen wir den Gruppenhomomorphismus $G_\mathfrak{p} \to \overline{G}$ mit $\overline{G}$ als der Galoisgruppe von $\mathfrak{o}_L/\mathfrak{p}$ über $\mathbb{F}_p$. Man zeigt, daß der (unter der genannten Voraussetzung $p \nmid d_f$) ein Isomorphismus ist:

Dazu kann man $\mathbb{Q}$ durch den Fixkörper $L_\mathfrak{p}$ von $G_\mathfrak{p}$ in L ersetzen. Es gilt nämlich: Ist $\wp$ das unterhalb $\mathfrak{p}$ gelegene maximale Ideal von $\mathfrak{o}_{L_\mathfrak{p}}$, so folgt

> über p liegen genau $[L_\mathfrak{p} : \mathbb{Q}]$ viele Primideale von $\mathfrak{o}_L$, nämlich die $\tau(\mathfrak{p})$ für τ aus einem Vertretersystem von $G_\mathfrak{p}$ in G_f
>
> über $\wp$ liegt in $\mathfrak{o}_L$ nur $\mathfrak{p}$
>
> $\mathfrak{o}_{L_\mathfrak{p}}/\wp = \mathbb{F}_p$.

Letzteres ist einmal mehr eine Konsequenz aus dem Chinesischen Restsatz:

$$\forall\, \beta \in \mathfrak{o}_{L_\mathfrak{p}}\ \exists\, \gamma \in \mathfrak{o}_{L_\mathfrak{p}} : \gamma \equiv \beta \mod \wp\,,\ \gamma \equiv 1 \mod \tau(\mathfrak{p}) \cap \mathfrak{o}_{L_\mathfrak{p}}\ (\tau \notin G_\mathfrak{p});$$

verifiziere nun $\mathrm{N}_{L_\mathfrak{p}/\mathbb{Q}}(\gamma) \in \mathbb{Z} \cap \wp$.

Wir haben damit diese Situation erreicht: $G_\mathfrak{p} = G_{L/L_\mathfrak{p}}$ und $\mathfrak{o}_L/\mathfrak{p} \supset \mathfrak{o}_{L_\mathfrak{p}}/\wp = \mathbb{F}_p$. Letzters ist eine Erweiterung endlicher Körper, also galoissch zyklisch mit Gruppe H. Wir zeigen $G_\mathfrak{p} \simeq H$ über

$$\sigma \mapsto \overline{\sigma}\,, \quad \overline{\sigma}(\overline{\alpha}) = \overline{\sigma(\alpha)} \quad (\forall\, \alpha \in \mathfrak{o}_L)\,.$$

Dabei ist $\alpha \mapsto \overline{\alpha}$ die natürliche Abbildung $\mathfrak{o}_L \to \mathfrak{o}_L/\mathfrak{p}$. Weil σ durch seine Wirkung auf den ω_i bestimmt ist und die $\overline{\omega}_i$ alle verschieden sind, ist das tatsächlich ein Isomorphismus und außerdem $\overline{L} = \mathfrak{o}_L/\mathfrak{p}$.

Die Surjektivität und Injektivität von $G_\mathfrak{p} \to H$, und ebenfalls $\overline{L} = \mathfrak{o}_L/\mathfrak{p}$, beruhen nun auf Beobachtungen allgemeiner Art, die wir schon früher im Zusammenhang mit der Entwicklung der Galoistheorie gemacht haben, nämlich:

Es sei L/K galoissch und $f(x) \in K[x]$ ein separables irreduzibles Polynom.

1. Hat f eine Nullstelle in L, so zerfällt f schon über L, i.e alle Wurzeln von f liegen in L. (*Wende auf* $f_\alpha(x) \in \mathbb{Z}[x]$ *mit* $\mathfrak{o}/\mathfrak{p} = \mathbb{F}_p(\overline{\alpha})\,,\ \alpha \in \mathfrak{o}\,,$ *an.*)
2. Sind $\omega_{1,2}$ zwei Wurzeln von f in L, so existiert ein $\sigma \in G_{L/K}$ mit $\sigma(\omega_1) = \omega_2$.

Beispiel: $f(x) = x^5 - x + 1$. Wir ersparen uns Arbeit, indem wir d_f erst gar nicht ausrechnen, sondern einfach am Ergebnis überprüfen, ob $\overline{f}(x) = f(x) \mod p$ separabel ist.

$p = 5$: $\overline{f}(x)$ ist eine Artin-Schreier-Gleichung in Charakteristik 5, und zwar ohne Nullstelle in $\mathbb{F}_5$ ($\alpha^5 = \alpha$ $(\forall \alpha \in \mathbb{F}_5)$), also irreduzibel, also separabel. Das zugehörige $\overline{L}$ liefert die zyklische Gruppe der Ordnung 5, damit ein Element der Ordnung 5 in G_f.

$p = 2$: $\overline{f}(x) = x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$ ist die irreduzible Zerlegung von $f(x)$ mod 2. Insbesondere ist $\overline{f}(x)$ wieder separabel. Das zugehörige $\overline{L}$ ist das Kompositum von $\mathbb{F}_4$ und $\mathbb{F}_8$, also $= \mathbb{F}_{64}$, und liefert die zyklische Gruppe der Ordnung 6, somit ein Element der Ordnung 6 in G_f. In S_5 gelesen, ist dies das Produkt eines 2- und eines 3-Zykels, seine 3. Potenz also eine Transposition.

Damit $G_f = S_5$ aufgrund von

> *Ist p prim und $U \leq S_p$ so, daß $p \mid |U|$ und U eine Transposition enthält, so gilt $U = S_p$.*

Eine überraschende Folgerung aus unserer Galoisgruppenberechnung ist die:

Das Gaußsche Lemma impliziert *ist $f(x) \in \mathbb{Z}[x]$ ein normiertes Polynom, das irreduzibel modulo einer Primzahl p ist, so ist $f(x)$ irreduzibel in $\mathbb{Q}[x]$*. Man beachte, daß das Eisenstein-Kriterium zur Primzahl p sozusagen konträr dazu ist; dort wird nämlich $f(x) \equiv \overline{a}_n x^n \mod p$. Es stellt sich die Frage, ob es, gewissermaßen umgekehrt zu obiger Aussage, denn *irreduzible Polynome $f(x) \in \mathbb{Z}[x]$ gibt, die modulo jeder Primzahl gelesen reduzibel werden?* Das ist tatsächlich der Fall. Nimm etwa das irreduzible Polynom $f(x) \in \mathbb{Z}[x]$ von $\sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$. Dieses hat Grad 4 und die Gruppe $G_f \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$, da $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Über endlichen Körpern kommen aber

nun nur zyklische Galoisgruppen vor und ein irreduzibles $f \mod p$ würde folglich ein Element der Ordnung 4 in G_f liefern.

Das quadratische Reziprozitätsgesetz

Es wurde von Gauß aufgestellt und gibt eine vollständige Antwort auf die Frage

Gegeben sei $z \in \mathbb{Z}$. Für welche Primzahlen p ist $z \mod p$ ein Quadrat in $\mathbb{F}_p$?

Für ungerades p definiere

$$(\frac{z}{p}) = \begin{cases} 0\,, & p \mid z \\ 1\,, & z \mod p \text{ ist Quadrat in } \mathbb{F}_p \\ -1\,, & z \mod p \text{ ist kein Quadrat in } \mathbb{F}_p\,. \end{cases}$$

Damit gilt

1. $(\frac{z}{p}) = (\frac{z_0}{p})$ wenn $z \equiv z_0 \mod p$
2. $(\frac{z_1 z_2}{p}) = (\frac{z_1}{p})(\frac{z_2}{p})$
3. $(\frac{z}{p}) \equiv z^{\frac{p-1}{2}} \mod p$
4. $(\frac{-1}{p}) = \begin{cases} 1\,, & p \equiv 1 \mod 4 \\ -1\,, & p \equiv 3 \mod 4 \end{cases}$
5. $\sum_{i=1}^{p-1} (\frac{i}{p}) = 0$

Dabei ist 1. klar nach Definition und 4. eine sofortige Konsequenz aus 3. Die Punkte 2., 3. und 5. resultieren aus der Existenz einer Primitivwurzel $w \mod p$, also aus

$$\mathbb{F}_p = \{0, 1, \overline{w}, \overline{w}^2, \cdots, \overline{w}^{p-2}\}\,.$$

Denn für $p \nmid z$ folgt $z \equiv w^j \mod p$, und $z \mod p$ ist Quadrat in $\mathbb{F}_p$ genau wenn $2 \mid j$.

Es bleibt, $(\frac{q}{p})$ für ungerade Primzahlen $p \neq q$ und $(\frac{2}{p})$ zu bestimmen. Für ersteres bilde die Gaußsche Summe $\tau = \sum_{i=1}^{p-1} (\frac{i}{p}) \zeta_p^i \in \mathbb{Z}[\zeta_p]$. Weil sowohl $(\frac{i}{p})$ als auch ζ_p^i nur von der Restklasse $i \mod p$ abhängen, erhalten wir

$$\begin{aligned} \tau^2 &= (\textstyle\sum_i (\frac{i}{p}) \zeta_p^i)(\sum_j (\frac{j}{p}) \zeta_p^j) \\ &= \textstyle\sum_{i,j} (\frac{ij}{p}) \zeta_p^{i+j}) = \sum_i (\sum_j (\frac{ij}{p}) \zeta_p^{i+j}) \\ &\doteq \textstyle\sum_i (\sum_j (\frac{i^2 j}{p}) \zeta_p^{i+ij}) = \sum_i (\sum_j (\frac{j}{p}) \zeta_p^{i(1+j)}) \\ &= \textstyle\sum_i [(\frac{-1}{p}) + \sum_{j \neq -1} (\frac{j}{p}) \zeta_p^{i(1+j)}] \\ &= (p-1)(\tfrac{-1}{p}) + \textstyle\sum_{j \neq -1} (\frac{j}{p}) \sum_i \zeta_p^{i(1+j)} \\ &\stackrel{\circ}{=} (p-1)(\tfrac{-1}{p}) - \textstyle\sum_{j \neq -1} (\frac{j}{p}) = p(\tfrac{-1}{p})\,. \end{aligned}$$

Dabei liegt der Gleichheit $\doteq$ die Substitution $j \to ij$, der Gleichheit $\stackrel{\circ}{=}$ die Relation $1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = 0$ und der letzten 5. zugrunde.

Als nächstes beobachten wir

$$\begin{aligned}\tau^q &\equiv \sum_i (\tfrac{i}{p})^q \zeta_p^{iq} = \sum_i (\tfrac{i}{p}) \zeta_p^{iq} \\ &= \sum_i (\tfrac{q}{p})(\tfrac{iq}{p}) \zeta_p^{iq} = (\tfrac{q}{p})\tau \mod q\mathbb{Z}[\zeta_p] \,,\end{aligned}$$

woraus wir

$$(\frac{q}{p})\tau \equiv \tau \cdot \tau^{q-1} = \tau(\tau^2)^{\frac{q-1}{2}} \equiv \tau((\frac{-1}{p})p)^{\frac{q-1}{2}} \equiv \tau(\frac{-1}{p})^{\frac{q-1}{2}}(\frac{p}{q}) \mod q\mathbb{Z}[\zeta_p]$$

(wegen 3.) folgern, also $\tau((\frac{q}{p}) - (\frac{-1}{p})^{\frac{q-1}{2}}(\frac{p}{q})) \in q\mathbb{Z}[\zeta_p]$. Der rechte Faktor ist $= 0, \pm 2$; somit bleibt nur $= 0$ übrig, da $q \neq 2$. Deshalb

6. $(\frac{q}{p}) = (\frac{p}{q})$, wenn p oder $q \equiv 1 \mod 4$,

7. $(\frac{q}{p}) = -(\frac{p}{q})$, wenn $p \equiv q \equiv 3 \mod 4$ ist.

Genauso behandelt man $(\frac{2}{p})$; man ersetzt nur ζ_p durch $\zeta_4 = i$ und erhält

8. $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

4., 6., 7., 8. sind zusammen das quadratische Reziprozitätsgesetz.

Beispiel: Hat $3x^2 + y^2 = 2001$ eine ganzzahlige Lösung x, y? Dann wäre $3x^2 \equiv -y^2 \mod 23$ mit $23 \nmid x$ lösbar, also $(\frac{-3}{23}) = 1$. Aber $(\frac{-3}{23}) = (\frac{-1}{23})(\frac{3}{23}) = (\frac{23}{3}) = (\frac{-1}{3}) = -1$.

Eine Anwendung: Welche ganze Zahlen z sind Summe zweier Quadrate? Natürlich höchstens positive; sicher Quadrate und sicher $z = 2$. Die Gleichung $z = x^2 + y^2$ läßt sich in dem Euklidischen Ring $\mathbb{Z}[i]$ in $z = (x + iy)(x - iy) = N_{\mathbb{Q}(i)/\mathbb{Q}}(x + iy)$ überführen. Die Einheiten des Ringes $\mathbb{Z}[i]$ sind genau die Lösungen der Normgleichung $N(x + iy) = 1$, also $\{\pm 1, \pm i\}$. Des weiteren zeigt die Norm, daß ab Summe von Quadraten ist, falls a und b dies sind. Also fragen wir nur noch, welche ungeraden Primzahlen p Summen von Quadraten sind:

$p = x^2 + y^2 \implies x^2 \equiv -y^2 \not\equiv 0 \mod p \implies (\frac{-1}{p}) = 1 \implies p \equiv 1 \mod 4$
$p = (x + iy)(x - iy) \implies p$ nicht prim in $\mathbb{Z}[i]$
p nicht prim in $\mathbb{Z}[i] \implies p = (x + iy)\alpha\,,\ \alpha \in \mathbb{Z}[i] \implies N(x + iy) = p = x^2 + y^2$
$p \equiv 1 \mod 4 \implies \exists\, w \in \mathbb{Z} : w^2 \equiv -1 \mod p \implies p \mid (w + i)(w - i)$ in $\mathbb{Z}[i]$, aber $\frac{1}{p} \notin \mathbb{Z}$.

Ist nun z Summe von zwei Quadraten und hat z einen Primteiler $p \equiv 3 \mod 4$, so folgt $p|N(\alpha) = z = x^2 + y^2$, also $p|x$, $p|y$ und $p^2|z$. Damit kommt p mit gerader Vielfachheit in z vor.

Kapitel 3. Ein wenig zu allgemeinen Körpererweiterungen

L/K sei eine Erweiterung von Körpern.

DEFINITION. *Die n verschiedenen Elemente $\beta_1, \ldots, \beta_n \in L$ heißen algebraisch unabhängig über K, falls*

$$f(\beta_1, \ldots, \beta_n) = 0 \implies f = 0$$

für $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ (der Polynomring in n unabhängigen Variablen $x_1, \ldots, x_n$ über K) gilt.

Z.B. sind $e, \pi \in \mathbb{R}$ algebraisch unabhängig über $\mathbb{Q}$.

DEFINITION. *Eine Transzendenzbasis von L/K ist eine Teilmenge $B \subset L$ mit*

1. *B ist transzendent über K, d.h. je endlich viele Elemente in B sind algebraisch unabhängig über K*
2. *$L/K(B)$ ist algebraisch.*

Hier bezeichnet (wie üblich) $K(B)$ den kleinsten Teilkörper von L, der K und B enthält.

Mit Zorns Lemma folgt ohne weiteres 1. des nachstehenden Satzes.

SATZ 12. *1. Ist $T \subset L$ eine nichtleere über K transzendente Menge, so existiert eine Transzendenzbasis B von L/K mit $B \supset T$.*

2. Ist L/K endlich erzeugt, i.e.

$$L = K(\gamma_1, \ldots, \gamma_r) = \mathrm{Quot}\Big(\{ \sum_{\text{endlich}} a_{i_1 \ldots i_r} \gamma_1^{i_1} \cdot \ldots \cdot \gamma_r^{i_r} : i_\nu \in \mathbb{Z}_{\geq 0}\,,\, a_{i_1 \ldots i_r} \in K\}\Big)$$

für $\gamma_i \in L$ $(1 \leq i \leq r)$, so haben alle Transzendenzbasen von L/K gleichviele Elemente $t_{L/K}$, $0 \leq t_{L/K} < \infty$; $t_{L/K}$ heißt der Transzendenzgrad von L/K.

3. Für $K \subset L \subset F$ gilt $t_{L/K} + t_{F/L} = t_{F/K}$.

Endlich erzeugte Erweiterungen L/K mit $t_{L/K} = 1$ heißen Funktionenkörper einer Variablen über K. Der einfachste solche ist $L = K(x)$ mit einer Transzendenten x, also der Körper der rationalen Funktionen in einer Variablen (x nämlich) über K,

$$K(x) = \{f(x)/g(x) : f(x), 0 \neq g(x) \in K[x]\}\ .$$

Der *Satz von Lüroth* gibt explizit alle Zwischenkörper in L/K an:

SATZ 13. *i) Jeder Zwischenkörper $\neq K$ in $K(x)/K$ ist ein rationaler Funktionenkörper $K(\alpha)$ über K. Gilt $\alpha = f(x)/g(x)$ mit teilerfremden Polynomen $f(x), g(x) \in K[x]$, so ist (bis auf Normierung)*

$$f(X) - \alpha g(X) \in K(\alpha)[X]$$

das irreduzible Polynom für x über $K(\alpha)$, also $[K(x) : K(\alpha)] = \max(\mathrm{grad}(f), \mathrm{grad}(g))$.

ii) Jeder Körperautomorphismus von $K(x)/K$ ist von der Form

$$x \mapsto \frac{ax + b}{cx + d} \text{ mit } a, b, c, d \in K \text{ und } ad - bc \neq 0\ .$$

DEFINITION. *R sei ein kommutativer Ring mit 1 und G eine endliche Gruppe.Der Gruppenring der Gruppe G über R ist die Menge*

$$RG = \{\textstyle\sum_{g\in G} r_g g : r_g \in R\} \quad \text{mit}$$
$$\textstyle\sum_{g\in G} r_g g = \sum_{g\in G} \tilde{r}_g g \iff r_g = \tilde{r}_g \ (\forall\, g \in G)$$
$$\textstyle\sum_{g\in G} r_g g + \sum_{g\in G} s_g g = \sum_{g\in G}(r_g + s_g)g$$
$$\textstyle(\sum_{g\in G} r_g g)(\sum_{g\in G} s_g g) = \sum_{g\in G}(\sum_{h\in G} r_h s_{h^{-1}g})g\,.$$

Die Elemente von RG kann man sich auch als Funktionen von G nach R vorstellen: $\sum_{g\in G} r_g g$ ordnet dann einem $g \in G$ den Wert $r_g \in R$ zu. Addiert wird so wie im Bildbereich; die Multiplikation ist eine Faltung.

RG ist ein Ring; $R \subset RG$ über $r \mapsto r1 + \sum_{1\neq g\in G} 0g\,;\quad G \subset RG$ über $g \mapsto \sum_{h\neq g} 0h + 1g\,.$

Die Bildung von RG entspringt dem Wunsch, einen R-Modul, auf dem eine Gruppe G R-linear operiert, zu einem Modul über einem Ring zu machen, der aus R und G zusammengesetzt ist.

Die Strukturtheorie dieser Gruppenringe (-algebren, wenn R ein Körper ist) ist i.A. schwer; der einfachste Fall ist $R = \mathbb{C}$, komplizierter werden $R = \mathbb{R}$ oder gar $R = \mathbb{Q}$; die Theorie für Körper R, deren Charakteristik $|G|$ teilt, ist noch nicht ganz verstanden (*modulare Darstellungstheorie*); für $R = \mathbb{Z}$ (*ganzzahlige Darstellungstheorie*) wird sie besonders kompliziert (und interessant).

Beispiele:

1. $G =$ die zyklische Gruppe der Ordnung n. Dann ist $RG = R[x]/x^n - 1$. Man bemerke, daß $x^n - 1$ inseparabel über R ist, falls $n = 0$ in R gilt.

2. G sei abelsch und $R = \mathbb{C}$. Jeder Charakter χ von G, also $\chi \in G^* = \mathrm{Hom}(G, \mathbb{C}^\times)$, liefert einen Homomorphismus $h_\chi : \mathbb{C}G \twoheadrightarrow \mathbb{C}\,, \sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g \chi(g)\,.$ Aus $|G| = |G^*|$ erhalten wir $\mathbb{C}G \to \mathbb{C} \oplus \cdots \oplus \mathbb{C}$ ($|G|$ Summanden). Das h_χ ist im Grunde dasselbe wie $\sum_{g\in G} r_g g \mapsto (\sum_{g\in G} r_g g)e_\chi \in \mathbb{C}e_\chi \simeq \mathbb{C}$, wenn $e_\chi = \frac{1}{|G|}\sum_{g\in G} \chi(g^{-1})g$ ist. Es gilt nämlich $e_\chi g = \chi(g)e_\chi\,,\ e_\chi^2 = e_\chi\,,\ \sum_{\chi\in G^*} e_\chi = 1\,.$ Es folgt: $\mathbb{C}G \simeq \mathbb{C} \oplus \cdots \oplus \mathbb{C}\,.$

Wir werden in diesem Kapitel beweisen, daß für einen Körper der Charakteritik 0

$$KG = \bigoplus_i (D_i)_{n_i \times n_i}$$

gilt, wobei die D_i (endlich viele) den Körper K enthaltende Schiefkörper von endlicher Dimension über K sind. Die Anzahl der Summanden i soll (zumindest in Spezialfällen) angegeben werden, so auch die Matrixgrade n_i. Wir wollen schließlich ein Maß für die vorkommenden Schiefkörper D_i finden.

DEFINITION. *K sei ein Körper. Eine (endlich-dimensionale) Algebra A über K ist ein endlich-dimensionaler K-Vektorraum, in dem das + der additive Teil einer Ringstruktur mit*

$$(\alpha a)(\beta b) = (\alpha\beta)(ab) \ (\forall\, \alpha, \beta \in K\,,\ a, b \in A)$$

ist. Wir fordern der Einfachheit halber noch, daß A ein Einselement enthält; das können und werden wir mit der $1 \in K$ identifizieren und dann K als Teilring von A auffassen. Man beachte, daß A bezüglich $\cdot$ nicht kommutativ sein muß, daß aber $\alpha a = a\alpha$ für alle $\alpha \in K$ und $a \in A$ gilt.

Des weiteren heiße A halbeinfach, wenn A kein nilpotentes Rechtsideal $\mathfrak{r} \neq 0$ enthält.

Ein Rechtsideal $\mathfrak{r}$ heißt nilpotent, wenn $\mathfrak{r}^n = 0$ für ein $n \in \mathbb{N}$ gilt. Ist A kommutativ, so bedeutet obige Bedingung nichts weiter, als daß A kein nilpotentes Element $\neq 0$ enthält. Im Nichtkommutativen ist das falsch.

Die Gruppenalgebra KG der Gruppe G über dem Körper K mit $\mathrm{char}(K) \nmid |G|$ ist halbeinfach. Aber $\mathbb{F}_p C_p = \mathbb{F}_p[x]/x^p - 1 = \mathbb{F}_p[x]/(x-1)^p$ hat das nilpotente Element $x - 1 \mod (x-1)^p$ (C_p ist die Gruppe der Ordnung p).

Zum Beweis obiger Behauptung zerlege $A = \mathfrak{r} \oplus U$ mit einem Teilvektorraum U von A und nenne $\pi : A \to \mathfrak{r}$ die Projektion auf $\mathfrak{r} \neq 0$. Das π ist eine K-lineare Abbildung, aber i.A. keine A-lineare, weil U nur ein Vektorraum ist (also i.A. $\pi(ab) \neq \pi(a)b$ für $a, b \in A$). Für $g \in G$ setze $\pi_g(a) = \pi(ag^{-1})g$ und bilde $\tilde{\pi} = \frac{1}{|G|} \sum_{g \in G} \pi_g$. Dann gilt

$$\tilde{\pi} : A \twoheadrightarrow \mathfrak{r}\,,\ \tilde{\pi}(r) = r \text{ für } r \in \mathfrak{r}\,,\ \ker\tilde{\pi} \text{ ist ein Rechtsideal}\,,\ A = \mathfrak{r} \oplus \ker\tilde{\pi}\,.$$

Die Zerlegung $1 = r_0 + r_1$, $r_0 \in \mathfrak{r}$, $r_1 \in \ker\tilde{\pi}$ zieht $r_0^2 = r_0$ nach sich, also ist $\mathfrak{r}$ nicht nilpotent.

DEFINITION. *1. Ein A-Modul ist ein endlich-dimensionaler K-Vektorraum, auf dem A von rechts wirkt, also $ma \in M$ für $m \in M$ und $a \in A$. Es gilt*

$$(m_1 + m_2)a = m_1a + m_2a,\ m(a_1 + a_2) = ma_1 + ma_2,\ (ma_1)a_2 = m(a_1a_2),\ m1 = m\,,$$

und natürlich $\alpha m = m\alpha$ für $\alpha \in K \subset A$.

2. *Eine A-lineare Abbildung $f : M_1 \to M_2$ von A-Moduln ist eine additive Abbildung mit $f(m_1a) = f(m_1)a$ für alle $m_1 \in M_1$ und alle $a \in A$. Insbesondere sind $\ker(f)$ und $\mathrm{im}\,(f)$ A-Untermoduln von M_1 bzw. M_2 und es gelten m.m. die üblichen Isomorhiesätze (wie auch die übliche Definition einer Unterstruktur).*
3. *Eine K-Algebra A heißt einfach, wenn (0) und A die einzigen zweiseitigen Ideale in A sind.*

Beispiel: Der Matrixring $D_{n\times n}$ ist einfach, wenn D ein über K endlich-dimensionaler Schiefkörper ist (i.e., eine K-Algebra ohne Nullteiler).

Einfache Algebren sind halbeinfach. Wir werden zeigen, daß obiges Beispiel schon die Gesamtheit der einfachen Algebren erschöpft. Halbeinfache Algebren werden sich als endliche direkte Summen von einfachen Algebren herausstellen.

A) Halbeinfache und einfache Algebren

1.) *Ist A eine einfache K-Algebra, so ist sie auch halbeinfach.*
Denn das Annulatorideal $\mathfrak{a}(\mathfrak{r}) \overset{\text{def}}{=} \{a \in A : \mathfrak{r}a = 0\}$ eines Rechtsideals $\mathfrak{r}$ ist ein zweiseitiges Ideal, also $= 0$, wenn $\mathfrak{r} \neq 0$.

2.) *Ist* $\mathfrak{r}$ *ein minimales Rechtsideal in der halbeinfachen Algebra* A*, d.h.* $\mathfrak{r} \neq 0$ *und* $[\,\mathfrak{r}_1 \subsetneqq \mathfrak{r} \implies \mathfrak{r}_1 = 0\,]$*, so gilt* $\mathfrak{r} = eA$ *mit einem Idempotenten* $e^2 = e$*.*
Denn $\exists\, a \in \mathfrak{r}$ mit $a\mathfrak{r} = \mathfrak{r}$, also $ae = a$ mit einem $e \in \mathfrak{r}$, also $e^2 - e \in \{b \in \mathfrak{r} : ab = 0\} \subsetneqq \mathfrak{r}$.

FOLGERUNG. *A sei halbeinfach.*

i. Jedes Rechtsideal $\mathfrak{r} \neq 0$ *ist ein von einem Idempotenten erzeugtes Rechtshauptideal.*

ii. Die zweiseitigen Ideale $0 \neq \mathfrak{a}$ *von* A *sind die Hauptideale* $\mathfrak{a} = Ae = eA$ *mit* $e^2 = e \in Z(A) \stackrel{\text{def}}{=} \{z \in A : za = az\ (\forall\, a \in A)\}$*, dem Zentrum von* A*.*

iii. Ist M *ein* A*-Modul und* N *ein Untermodul, so ist* N *schon direkter Summand in* M*. Insbesondere sind alle* A*-Moduln projektiv* [3]*.*

vi. Ist M *ein einfacher (oder irreduzibler)* A*-Modul, also ohne nichttriviale Untermoduln, so ist* M *A-isomorph zu einem minimalen Rechtsideal* $\mathfrak{r}$ *von* A*.*

Zu letzterer Aussage beachte, daß $[\,M$ einfach $\iff M = mA\ (\forall\, 0 \neq m \in M)\,]$ und $mA \simeq A/\mathfrak{a}_m$ mit $\mathfrak{a}_m = \{a \in A : ma = 0\}$ gilt. Wegen $\mathfrak{a}_m \oplus \mathfrak{r} = A$, ist deshalb $mA \simeq \mathfrak{r}$.

3.) $\mathfrak{r}_0$ *sei ein minimales Rechtsideal in* A*. Dann ist* $\sum_{\mathfrak{r}} \mathfrak{r}$ *ein zweiseitiges Ideal, wenn über alle zu* $\mathfrak{r}_0$ *isomorphen Rechtsideale* $\mathfrak{r}$ *von* A *summiert wird.*

FOLGERUNG. *i. Ist* A *einfach, so gilt* $A \simeq \mathfrak{r} \oplus \cdots \oplus \mathfrak{r}$ *(als* A*-Moduln) für jedes minimale Rechtsideal* $\mathfrak{r}$ *von* A*. Alle diese sind isomorph.*

ii. Ist A *halbeinfach, so gilt* $A = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$ *mit minimalen zweiseitigen Idealen* $\mathfrak{a}_i$*. Es gilt weiter* $\mathfrak{a}_i = Ae_i = e_iA$ *mit einem zentralen Idempotenten* e_i*, d.h.* $e_i^2 = e_i\,,\ e_ia = ae_i\ (\forall\, a \in A)$*.*

Bemerkung: Die $\mathfrak{a}_i$ sind genau alle minimalen zweiseitigen Ideale von A; sie selbst sind einfache Algebren (mit e_i als Einselement). Es gilt

$$1 = e_1 + \cdots + e_m\,,\ e_ie_j = \delta_{ij}e_i\,,\ \mathfrak{a}_i\mathfrak{a}_j = \delta_{ij}\mathfrak{a}_i\,.$$

Die e_i heißen die zentralen primitiven Idempotente von A.

4.) *Das Rechtsideal* $\mathfrak{r}$ *der Algebra* A *ist genau dann minimal, wenn* $D = \mathrm{End}_A(\mathfrak{r})$ *ein Schiefkörper ist.*

FOLGERUNG. *i. Ist* A *einfach, so gilt* $A \simeq D_{n\times n}$*. Dabei ist* $D \simeq \mathrm{End}_A(\mathfrak{r})$ *für ein minimales Rechtsideal* $\mathfrak{r}$ *von* A *und* n *ist die Zahl der Summanden in* $A \simeq \mathfrak{r} \oplus \cdots \oplus \mathfrak{r}$*.*

ii. Ist A *halbeinfach, so gilt* $A \simeq \bigoplus_{i=1}^{m} (D_i)_{n_i\times n_i}$*.*

Bemerkung: 2.) und die Folgerung heißt *Satz von Maschke*, 4.) heißt *Lemma von Schur*. Die Folgerungen zu 3.) und 4.) heißen *Satz von Wedderburn* und die $(D_i)_{n_i\times n_i}$ die Wedderburnkomponenten von A. Als sehr unterschiedliche Monographien zum Thema nenne ich Artin-Nesbitt-Thrall, *Rings with minimum condition* (Ann Arbor, University of Michigan Press 1944), sowie Kersten, *Brauergruppen von Körpern* (Vieweg 1990).

[3] Hieraus folgt, daß die beiden Aussagen über endlich dimensionale K-Algebren A äquivalent sind: 1. A ist halbeinfach, 2. jeder A-Modul ist projektiv.

LEMMA. *Ist K algebraisch abgeschlossen, so gilt $D = K$ für jeden Schiefkörper D über K.*

Denn die Elemente von D sind wegen $\dim_k D < \infty$ algebraisch über K.

Beispiele:

1. Der kanonische Gruppenhomomorphismus $G \to G^{\mathrm{ab}} \stackrel{\mathrm{def}}{=} G/G'$ induziert den Homomorphismus von K-Algebren $KG \twoheadrightarrow KG^{\mathrm{ab}}$ mit Kern $\mathfrak{a} = eKG = KGe$. Also: $KG = \mathfrak{a} \oplus KG(1-e)$ mit $KG(1-e) \simeq KG^{\mathrm{ab}}$. Die halbeinfache K-Algebra $\mathfrak{a}$ hat keine kommutative Wedderburnkomponente! Insbsondere: $\mathbb{C}G \simeq (s \cdot \mathbb{C}) \oplus \mathbb{C}_{n_{s+1} \times n_{s+1}} \oplus \ldots \oplus \mathbb{C}_{n_{s+h} \times n_{s+h}}$ mit allen $n_i \geq 2$ und $s = |G^{\mathrm{ab}}|$. Die Projektionen auf die Komponenten $\mathbb{C}$ werden von den Charakteren $\chi \in \mathrm{Hom}(G, \mathbb{C}^\times) = \mathrm{Hom}(G^{\mathrm{ab}}, \mathbb{C}^\times)$ induziert.
   Frage: was ist h; welche n_i kommen vor (in Abhängigkeit on G)?

2. Nun sei G abelsch und $K = \mathbb{R}$ oder K endlich über $\mathbb{Q}$. Dann gilt $KG = \bigoplus_i K_i$ mit Erweiterungskörpern K_i von K. Wegen $\chi_i : KG \twoheadrightarrow K_i$ (i-te Projektion) und $\chi_i(G) = \langle \zeta_{n_i} \rangle$ (als endliche Untergruppe von $K_i^\times$), folgt $K_i = K(\chi) \stackrel{\mathrm{def}}{=} K(\zeta_{n_i})$. Die χ_i laufen dabei durch $\hat{G}$, aber χ_{i_1} und χ_{i_2} liefern genau dann dieselbe Wedderburnkomponente K_i, falls $\chi_{i_1} = \chi_{i_2} \circ \sigma$ mit einem Galoisautomorphismus $\sigma_i \in G_{K_i/K}$ gilt.

3. Jetzt sei $G = \langle x, y : x^4 = 1,\ x^2 = y^2,\ y^{-1}xy = x^{-1} \rangle$ die 8-elementige Quaternionengruppe und $K = \mathbb{R}$. Wegen $G^{\mathrm{ab}} = V_4$ (die Kleinsche Vierergruppe), gilt $\mathbb{R}G = 4\mathbb{R} \oplus A$ mit einer 4-dimensionalen einfachen Algebra, also $A = \mathbb{R}_{2\times 2}$ oder $A = D$, ein Schiefkörper. Im ersten Fall hätten wir Matrizen $X, Y \in \mathbb{R}_{2\times 2}$ mit $1 \neq X^2 = Y^2$, $X^4 = 1$, $Y^{-1}XY = X^{-1}$. Die reelle Jordanform von X zeigt $X^2 = -1$, also $X^{-1} = -X$ (da $m(x) = x^2 + 1$ das Minimalpolynom von X sein muß). Nun rechnet man ohne weiteres nach, daß jede nichttriviale reelle Linearkombination der Matrizen $1, X, Y, XY$ invertierbar ist,

$$(\alpha_0 + \alpha_1 X + \alpha_2 Y + \alpha_3 XY)(\alpha_0 - \alpha_1 X - \alpha_2 Y - \alpha_3 XY) = (\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)1\,,$$

   womit erstens $1, X, Y, XY$ eine $\mathbb{R}$-Basis von $\mathbb{R}_{2\times 2}$ wäre und des weiteren dann jede 2×2 Matrix $\neq 0$ invertierbar, ein Widerspruch. Also $A = D = \mathbb{H}$; die Matrixbeschreibung von $\mathbb{H}$ durch komplexe 2×2 Matrizen ergibt sich aus $\mathbb{C}G = 4\mathbb{C} \oplus \mathbb{C}_{2\times 2}$.

4. Schließlich sei $G = S_3$ und $K = \mathbb{Q}$. Wegen $G^{\mathrm{ab}} = \{\pm 1\}$, ist $\mathbb{Q}G = 2\mathbb{Q} \oplus A$ mit 4-dimensionaler einfacher $\mathbb{Q}$-Algebra A. Wir testen, ob jetzt $A = \mathbb{Q}_{2\times 2}$ zutrifft. Der 3-Zykel liefert dann die Matrix $X \neq 1$ mit Minimalpolynom $x^2 + x + 1$, also $X = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, nach geeigneter Basiswahl. Es ist nun nicht gerade einfach, die einer Transposition entsprechende Matrix Y zu finden, weil wir keine Freiheit in der Basiswahl mehr haben. Folgender Trick hilft: als 2-dimensionalen $\mathbb{Q}$-Vektorraum nimm $\mathbb{Q}(\zeta_3)$ mit Basis $1, \zeta_3$. Dann laß dem 3-Zykel die Multiplikation mit ζ_3 entsprechen und erhalte so wirklich obiges X; der Transposition laß den Galoisautomorphismus $\sigma \neq 1$ entsprechen und erhalte $Y = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$. Damit ist die S_3 in $\mathbb{Q}_{2\times 2}$ realisiert und $A = \mathbb{Q}_{2\times 2}$.

Einschub: Tensorprodukte von Vektorräumen [4]

V und W seien (nicht notwendig endlich dimensionale) Vektorräume über dem kommutativen Körper K.

DEFINITION 15.1. *Eine Abbildung $a : V \times W \to A$ der Produktmenge $V \times W$ in eine abelsche Gruppe A heißt ausgeglichen, falls*

1. *a linear in jedem Argument ist, also*
   $a(v_1 + v_2, w) = a(v_1, w) + a(v_2, w)$ *und* $a(v, w_1 + w_2) = a(v, w_1) + a(v, w_2)$
   für alle $v, v_1, v_2 \in V$ und alle $w, w_1, w_2 \in W$ gilt,
2. *a der Regel $a(\lambda v, w) = a(v, \lambda w)$ $(\forall\, v \in V, w \in W, \lambda \in K)$ genügt.*

DEFINITION. *Die abelsche Gruppe $V \otimes_K W$ heißt ein Tensorprodukt von V und W (über K), falls*

1. *es eine ausgeglichene Abbildung*
   $$\otimes : V \times W \to V \otimes_K W\,,\ (v, w) \mapsto v \otimes w$$
   gibt
2. *$V \otimes W$ von den $v \otimes w\,,\ v \in V, w \in W$ erzeugt ist,*
3. *jede ausgeglichene Abbildung $a : V \times W \to A$ einen Gruppenhomomorphismus $V \otimes W \to A\,,\ v \otimes w \mapsto a(v, w)$ definiert* [5].

Aus der Definition folgt sofort, daß zwei Tensorprodukte $V \otimes_K W\,,\ V \otimes'_K W$ derselben Vektorräume V, W kanonisch isomorph sind: $v \otimes w \leftrightarrow v \otimes' w$.

SATZ. *Zu V und W existiert ein Tensorprodukt.*

Nämlich $V \otimes_K W = F/T$ mit der freien abelschen Gruppe F auf den Erzeugenden $(v, w)\,,\ v \in V, w \in W$, und der Untergruppe

$$T = \langle (v_1 + v_2, w) - (v_1, w) - (v_2, w)\,,\ (v, w_1 + w_2) - (v, w_1) - (v, w_2)\,,\ (\lambda v, w) - (v, \lambda w) \rangle\,.$$

Wegen der dem Satz vorausgehenden Bemerkung sprechen wir ab jetzt von *dem* Tensorprodukt $V \otimes_K W$.

SATZ. 1. *$V \otimes_K W$ trägt auf natürliche Weise eine Vektorraumstruktur:*
$$\lambda(v \otimes w) \stackrel{\text{def}}{=} \lambda v \otimes w = v \otimes \lambda w\ .$$ [6]
2. *$V \otimes_K W \simeq W \otimes_K V\ ,\ v \otimes w \leftrightarrow w \otimes v$*

[4] I.a. können Tensorprodukte $M \otimes_R N$ eines R-Rechtsmoduls M und eines R-Linksmoduls N über einem nicht notwendig kommutativen Ring R erklärt werden. Die Besonderheit von Vektorräumen über Körpern entsteht nur bei Basisargumenten.

[5] ... i.a. sollte hier $a(v\lambda, w) = a(v, \lambda w)$ stehen

[6] ... i.a. gibt es hierzu kein Analogon, es sei denn, der Ring $K = R$ wäre kommutativ

3. *Ist Z ein dritter K-Vektorraum, so gilt* [7]

$$V \otimes_K (W \otimes_K Z) \simeq (V \otimes_K W) \otimes Z \ , \ v \otimes (w \otimes z) \leftrightarrow (v \otimes w) \otimes z$$

SATZ. 1. *Sind $v_1, \ldots, v_n$ linear unabhängige Vektoren in V und ist $\sum_{i=1}^{n} v_i \otimes w_i = 0$ in $V \otimes_K W$, so sind alle $w_i = 0$ $(1 \le i \le n)$.*

2. *Ist V endlich dimensional und $v_1, \ldots, v_n$ eine Basis, so läßt sich jedes Element des Vektorraums $V \otimes_K W$ eindeutig als $\sum_{i=1}^{n} v_i \otimes w_i$ mit geeigneten Vektoren $w_i \in W$ schreiben.*

3. *Ist auch W endlich dimensional mit Basis $w_1, \ldots, w_m$, so ist $V \otimes_K W$ ein Vektorraum der Dimension $n \cdot m$ $(= \dim V \cdot \dim W)$ und $v_i \otimes w_j$ $(1 \le i \le n, 1 \le j \le m)$ eine Basis von $V \otimes_K W$.*

4. *$K \otimes_K W \simeq W$, $\alpha \otimes w \leftrightarrow \alpha w$.*

Hier resultieren 2. und 3. aus 1., und 1. wiederum aus der kanonischen Isomorphie

$$(V_1 \oplus V_2) \otimes_K W \simeq V_1 \otimes_K W \oplus V_2 \otimes_K W \ .$$

Beispiele:

1. W sei ein K-Vektorraum und L Erweiterungskörper von K (etwa $K = \mathbb{Q}$, $L = \mathbb{R}$ oder $\mathbb{C}$; $K = \mathbb{R}$, $L = \mathbb{C}$). Dann ist L auch ein K-Vektorraum und $L \otimes_K W$ ist definiert. Dies wird durch $\lambda(\mu \otimes w) = \lambda\mu \otimes w$ ein L-Vektorraum. Es gilt $\dim_L(L \otimes W) = \dim_K W$. Des weiteren ist W über die Identifizierung $w \leftrightarrow 1 \otimes w$ ein K-Teilvektorraum von $L \otimes_K W$.

2. $\hat{V} \otimes_K W \simeq \mathrm{Hom}_K(V, W)$ (kanonisch), wobei $\hat{V} = \mathrm{Hom}_K(V, K)$ der Dualraum von V ist: $\varphi \otimes w \mapsto [v \mapsto \varphi(v)w]$; $V = \langle v_i \rangle$, $d_i =$ Dualbasis zu v_i, $f(v_i) = w_i$: $f \mapsto \sum_i d_i \otimes w_i$.

SATZ. 1. *$f : V \to V_1$, $g : W \to W_1$ seien K-lineare Abbildungen von Vektorräumen. Durch*

$$f \otimes g : V \otimes_K W \to V_1 \otimes_K W_1 \ , \ v \otimes w \to f(v) \otimes g(w)$$

ist eine wohldefinierte K-lineare Abbildung von $V \otimes_K W$ nach $V_1 \otimes_K W_1$ definiert.

2. *Es seien $V = V_1$, $W = W_1$ endlich dimensional mit Basen $v_1, \ldots, v_n$ bzw. $w_1, \ldots, w_m$. Zu f gehöre bezüglich $\{v_i\}$ die Matrix $A = (\alpha_{ik})$, zu g bezüglich $\{w_j\}$ die Matrix $B = (\beta_{jl})$. Dann gehört zu $f \otimes g$ bezüglich $\{v_i \otimes w_j\}$ die Matrix $A \otimes B \in K_{nm \times nm}$ mit*

$$\begin{pmatrix}
\alpha_{11}\beta_{11} & \ldots & \alpha_{11}\beta_{1m} & \alpha_{12}\beta_{11} & \ldots & \alpha_{12}\beta_{1m} & \ldots & \alpha_{1n}\beta_{11} & \ldots & \alpha_{1n}\beta_{1m} \\
\alpha_{11}\beta_{21} & \ldots & \alpha_{11}\beta_{2m} & \alpha_{12}\beta_{11} & \ldots & \alpha_{12}\beta_{1m} & \ldots & \alpha_{1n}\beta_{21} & \ldots & \alpha_{1n}\beta_{2m} \\
\vdots & \vdots & & & \vdots & & \vdots & & \vdots & \\
\alpha_{11}\beta_{m1} & \ldots & \alpha_{11}\beta_{mm} & \alpha_{12}\beta_{m1} & \ldots & \alpha_{12}\beta_{mm} & \ldots & \alpha_{1n}\beta_{m1} & \ldots & \alpha_{1n}\beta_{mm} \\
\vdots & \vdots & & & \vdots & & \vdots & & \vdots & \\
\vdots & \vdots & & & \vdots & & \vdots & & \vdots & \\
\alpha_{n1}\beta_{11} & \ldots & \alpha_{n1}\beta_{1m} & \alpha_{n2}\beta_{11} & \ldots & \alpha_{n2}\beta_{1m} & \ldots & \alpha_{nn}\beta_{11} & \ldots & \alpha_{nn}\beta_{1m} \\
\vdots & \vdots & & & \vdots & & \vdots & & \vdots & \\
\alpha_{n1}\beta_{m1} & \ldots & \alpha_{n1}\beta_{mm} & \alpha_{n2}\beta_{11} & \ldots & \alpha_{n2}\beta_{mm} & \ldots & \alpha_{nn}\beta_{m1} & \ldots & \alpha_{nn}\beta_{mm}
\end{pmatrix} .$$

[7] ... i.a. gilt sogar $(M \otimes_R N) \otimes_S O \simeq M \otimes_R (N \otimes_S O)$ für einen Rechts-R-Modul M, einen Links-R-Modul N, der zugleich ein Rechts-S-Modul ist und $r(ns) = (rn)s$ erfüllt, und einen Links-S-Modul O.

Beobachtung: Spur $(A \otimes B) = \text{Spur } A \cdot \text{Spur } B$

SATZ. *1. Sind A und B K-Algebren, so auch $A \otimes_K B$ (über $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2$).*

2. Ist L/K eine Körpererweiterung und $B = D$ ein zentraler Schiefkörper über K [8], so ist $L \otimes_K D$ eine zentraleinfache L-Algebra. Insbesondere ist $\dim_K D = s^2$ ein Quadrat.

s heißt der Schurindex von D.

B) Die Gruppenalgebra $\mathbb{C}G$

G sei eine endliche Gruppe. Die Gruppenalgebra $\mathbb{C}G$ zerfällt in einfache Algebren

$$\mathbb{C}G \simeq \mathbb{C}_{n_1 \times n_1} \oplus \cdots \oplus \mathbb{C}_{n_h \times n_h} ;$$

die Komponente $\mathbb{C}_{n_i \times n_i}$ entspricht dabei dem i-ten minimalen zweiseitigen Ideal $\mathfrak{a}_i$. Und die irreduziblen $\mathbb{C}G$-Moduln sind genau die $V_i \simeq \mathbb{C}^{n_i}$ $(1 \le i \le h)$, und jeder $\mathbb{C}G$-Modul M zerfällt so: $M \simeq \bigoplus_{i=1}^h m_i V_i$ mit $0 \le m_i \in \mathbb{Z}$ und $m_i V_i = V_i \oplus \cdots \oplus V_i$ (m_i Summanden).

Beobachtungen:

1. $h = \dim_{\mathbb{C}}(Z(\mathbb{C}G)) =$ Klassenzahl von G, d.i. die Anzahl der verschiedenen Konjugiertenklassen $K_g = \{y^{-1}gy : y \in G\}$ von G. Denn die Klassensummen $C_g = \sum_{x \in K_g} x$ (für die verschiedenen Konjugiertenklassen K_g) bilden eine $\mathbb{C}$-Basis von $Z(\mathbb{C}G)$.

2. $\dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}G}(V_i, M) = m_i$

e_i, $1 \le i \le h$, seien die zentralen primitiven Idempotenten von $\mathbb{C}G$, also die Komponenten der 1 in den $\mathfrak{a}_i$ (oder $e_i \mathbb{C}G = \mathbb{C}_{n_i \times n_i}$). Wir schreiben $e_i = \frac{n_i}{|G|} \sum_{g \in G} \alpha_i(g^{-1})g \in \mathbb{C}G$ mit Funktionen $\alpha_i : G \to \mathbb{C}$. Das sind sogar Klassenfunktionen: $\alpha_i(y^{-1}gy) = \alpha_i(g)$.

Aus $e_ie_j = \delta_{ij}e_i$ resultiert

$$\frac{n_in_j}{|G|^2} \sum_g \Big(\sum_{xy=g} \alpha_i(x^{-1})\alpha_j(y^{-1}) \Big) g = \delta_{ij} \frac{n_i}{|G|} \sum_{g \in G} \alpha_i(g^{-1})g \,.$$

Für $g = 1$ bleibt

$$\frac{1}{|G|} \sum_{x \in G} \alpha_i(x^{-1})\alpha_j(x) = \begin{cases} 0 & i \ne j \\ \frac{\alpha_i(1)}{n_i} & i = j \end{cases}$$

Was ist $\alpha_i(1)$? Betrachte die reguläre Darstellung, i.e. den Modul $M = \mathbb{C}G$. Jedes $g \in G$ bewirkt eine lineare Abbildung mit Spur $|G|$ oder 0, je nachdem ob $g = 1$ oder $g \ne 1$ ist. Unser e_i bewirkt dann eine mit Spur $\frac{n_i}{|G|}\alpha_i(1)|G| = n_i\alpha_i(1)$. Andererseits zerfällt $M = \mathbb{C}G = \bigoplus_{j=1}^h n_jV_j$, und e_i annuliert alle V_j für $j \ne i$ und ist die Identität auf V_i, hat also die Spur n_i^2, woraus $\alpha_i(1) = n_i$ folgt. Damit sehen wir:

Die α_i bilden eine Orthonormalbasis des h-dimensionalen $\mathbb{C}$-Vektorraums H aller Klassenfunktionen von G nach $\mathbb{C}$, mit dem Skalarprodukt

$$(\varphi, \psi) = \frac{1}{|G|} \sum_{x \in G} \varphi(x^{-1})\psi(x) \,, \;\; \varphi, \psi \in H \,.$$

[8] also ein über K endlich-dimensionaler Schiefkörper mit Zentrum K

Wir berechnen die Spur χ_j der von e_i in $\mathbb{C}_{n_j \times n_j}$ induzierten Matrix

$$\chi_j(e_i) = \begin{cases} 0 & i \neq j \\ \frac{n_i}{|G|} \sum_g \alpha_i(g^{-1})\chi_j(g) = n_i & i = j \end{cases}$$

Es resultiert $\alpha_i = \chi_i$. Wir nennen χ_i den i-ten irreduziblen Charakter von G. Beachte, daß $\chi_i(g) =$ Spur der von g auf V_i vermittelten linearen Abbildung ist. Es gilt

$(\chi_i, \chi_j) = \delta_{ij}$

Ist $M = \bigoplus m_i V_i$ ein $\mathbb{C}G$-Modul und $\chi_M(g) =$ Spur der von g auf M induzierten linearen Abbildung, so ist $\chi_M = \sum_i m_i \chi_i$ und $m_i = (\chi_M, \chi_i)$. Der Modul M ist also durch seinen Charakter χ_M vollständig bestimmt.

Bemerkung: Jeder Modul M liefert eine Matrixdarstellung, d.i. ein Homomorphismus $G \to GL_{\mathbb{C}}(\dim_{\mathbb{C}} M)$ von G durch komplexe Matrizen. Umgekehrt liefert jede Darstellung $G \to GL_{\mathbb{C}}(n)$ einen $\mathbb{C}G$-Modul $M = \mathbb{C}^n$, indem g über sein Bild in $GL_{\mathbb{C}}(n)$ wirkt. Matrizendarstellungen und $\mathbb{C}G$-Moduln sind also dasselbe. Die Darstellung ist bereits durch ihre Spur bestimmt.

SATZ. *Der Grad n_i von χ teilt die Gruppenordnung.*

Denn die Klassensummen efüllen $C_x C_y = \sum_{j=1}^{h} c_{xyj} C_j$, $c_{xyj} \in \mathbb{Z}$. Projiziere C_g in die i-te Komponente und erhalte die Diagonalmatrix $c_g 1$ (Schurs Lemma), damit also $c_x c_y = \sum_j c_{xyj} c_j$. Diese Gleichung zeigt, daß die c_j ganze algebraische Zahlen sind. Anwendung von χ_i auf C_x ergibt $n_i c_x = |K_x| \chi_i(x)$ oder $c_x = \frac{|K_x| \chi_i(x)}{n_i}$. Multipliziere mit $\chi_i(x^{-1})$, summiere über alle x mod Konjugation und erhalte $\frac{|G|}{n_i}$ als Summe ganz algebraischer Zahlen ($\chi(y)$ ist eine Summe von Einheitswurzeln, wie man der Jordanform von y in $\mathbb{C}_{n_i \times n_i}$ abliest, also ganz algebraisch).

DEFINITION. $R(G) = \{\chi_1 - \chi_2 : \chi_{1,2}$ *Charaktere von Darstellungen von* $G\}$ *heißt der Charakterring von G über $\mathbb{C}$. Das wird ein kommutativer Ring über $(\chi_1 \chi_2)(g) = \chi_(g)\chi_2(g)$. $R(G)$ ist ein freier $\mathbb{Z}$-Modul mit Basis χ_i , $1 \leq i \leq h$.*

Der Summe von Charakteren entspricht die direkte Summe der Moduln: $\chi_{M_1} + \chi_{M_2} = \chi_{M_1 \oplus M_2}$; dem Produkt das Tensorprodukt mit

g wirkt auf $M_1 \otimes_{\mathbb{C}} M_2$ diagonal, also $g(m_1 \otimes m_2) = gm_1 \otimes gm_2$.

Daher $\chi_{M_1 \otimes_{\mathbb{C}} M_2} = \chi_{M_1} \chi_{M_2}$.

Sei $N \lhd G$ und $\overline{G} = G/N$. Die irreduziblen Charaktere von $\overline{G}$ seien $\overline{\chi}_1, \cdots, \overline{\chi}_r$; $\overline{\chi}$ sei der Charakter eines $\mathbb{C}\overline{G}$-Moduls $\overline{M}$. Fasse $\overline{M}$ als $\mathbb{C}G$-Modul über $\overline{m}g = \overline{m} \cdot \overline{g}$ auf, wenn $\overline{g} \in \overline{G}$ das Bild von g ist. Der zugehörige Charakter von G heißt $\mathrm{infl}_N^G(\overline{\chi}) = \chi$, die Inflation von $\overline{\chi}$ von $\overline{G}$ nach G; er erfüllt $\chi(g) = \overline{\chi}(\overline{g})$. Offenbar sind die $\chi_i = \mathrm{infl}_N^G(\overline{\chi}_i)$ r verschiedene irreduzible Charaktere von G. Beachte an dieser Stelle auch, daß $\mathbb{C}G \simeq \mathbb{C}\overline{G} \oplus \mathfrak{a}$ mit $\mathfrak{a} = \ker(\mathbb{C}G \twoheadrightarrow \mathbb{C}\overline{G})$ gilt, wobei letzterer $\mathbb{C}$-Algebrenepimorphismus von $g \mapsto \overline{g}$ induziert ist.
Ein Spezialfall ist $N = G'$, die Kommutatoruntergruppe von G. In diesem Fall sind die $\mathrm{infl}_{G'}^G(\overline{\chi}_i)$ genau die Charaktere χ von G vom Grad 1, d.h. $\chi(1) = 1$.

Die auf den Charakterringen induzierte Abbildung $\mathrm{infl}\,_N^G : R(\overline{G}) \to R(G)$ ist ein Homomorphismus von Ringen.

Notation: Ab jetzt ist $\chi_1 = 1$ der 1-Charakter von G, also $\chi_1(g) = 1\ (\forall\, g \in G)$.
$\chi_1 = \mathrm{infl}\,_1^G(1)$; χ_1 ist das 1-Element von $R(G)$.

Sei $U \leq G$ und M ein $\mathbb{C}G$-Modul mit Charakter χ. Die Einschränkung der Wirkung auf die Teilalgebra $\mathbb{C}U \subset \mathbb{C}G$ macht aus M einen $\mathbb{C}U$-Modul. Das induziert einen Ringhomomorphismus $\mathrm{res}\,_U^G : R(G) \to R(U)\,,\ \chi \mapsto \mathrm{res}\,_U^G(\chi) = \chi_{|U}$, die Restriktion von χ auf U. Es gilt $(\mathrm{res}\,_U^G(\chi))(u) = \chi(u)$ für $u \in U$.

Nun sei X ein $\mathbb{C}U$-Modul mit Charakter ξ. Bilde $M = X \otimes_{\mathbb{C}U} \mathbb{C}G$. Das ist ein Tensorprodukt eines $\mathbb{C}U$-Rechtsmoduls, X, mit einem $\mathbb{C}U$-Linksmodul, $\mathbb{C}G$, über einem nichtkommutativen Ring, $\mathbb{C}U$. Es gilt

$$X \otimes_{\mathbb{C}U} \mathbb{C}G = \{\sum_{i=1}^{r} x_i \otimes g_i : x_i \in X, G = \dot{\bigcup}_{i=1}^{r} U g_i\}\,.$$

Die angebenene Darstellung der Elemente des Tensorprodukts ist eindeutig. Die G-Modulstruktur entsteht aus $(n \otimes g_i)g = nu \otimes g_j$ wenn $g_i g = u g_j$. Der zugehörige Charakter heißt der von ξ induzierte Charakter $\mathrm{ind}\,_U^G(\xi)$; es gilt

$$\mathrm{ind}\,_U^G(\xi)(g) = \sum_{i=1}^{r} \dot{\xi}(g_i g g_i^{-1})$$

mit $\dot{\xi} = \xi$ auf U und $\dot{\xi} = 0$ außerhalb U.
Die auf den Charakterringen induzierte Abbildung $\mathrm{ind}\,_U^G : R(U) \to R(G)$ ist nur eine additive Abbildung. Das Bild von $R(U)$ ist allerdings ein Ideal in $R(G)$.

Spezialfälle:

$U \lhd G \implies \mathrm{ind}\,_U^G(\xi) = 0$ außerhalb U.

$U = 1$ – dann ist $\mathrm{ind}\,_1^G(1) = \rho_G$ die reguläre Darstellung von G, also $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}G = \mathbb{C}G$, $\rho_G(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1\,. \end{cases}$

Man beachte, daß alle hier definierten Abbildungen, infl, res, ind, sich transitiv verhalten, z.B. $\mathrm{res}\,_U^G \circ \mathrm{res}\,_V^U = \mathrm{res}\,_V^G$ für $V \leq U \leq G$.

Satz (Frobenius). *1.* $\mathrm{ind}\,_U^G(\xi \cdot \mathrm{res}\,_U^G(\chi)) = \mathrm{ind}\,_U^G(\xi) \cdot \chi$

2. $(\mathrm{ind}\,_U^G(\xi), \chi)_G = (\xi, \mathrm{res}\,_U^G(\chi))_U$

für Charaktere ξ von $U \leq G$ und χ von G.

Bemerkung: Zur Verdeutlichung ist hier das Skalarprodukt $(\,\cdot\,,\,\cdot\,)$ auf G bzw. U mit dem Index G bzw. U verziert. – Es gibt auch eine Formel für $\mathrm{res}\,_V^G(\mathrm{ind}\,_U^G(\xi))$ für Untergruppen $U, V \leq G$ und Charaktere ξ von U: die sogenannte Mackey-Formel, die wir hier aus Zeitgründen unterschlagen müssen (siehe z.B. B. Huppert, Endliche Gruppen 1 (Springer 1967), S.557). Soviel allerdings doch: Ist $N \lhd G$ und ξ ein Charakter von N, so definiert $\xi^x(n) = \xi(xnx^{-1})$ für jedes $x \in G$ einen neuen

Charkter von N, den zu ξ unter x konjugierten Charakter. Ist M ein zu ξ gehörender $\mathbb{C}N$-Modul, so gehört Mx zu ξ^x, wenn $Mx \stackrel{\text{def}}{=} \{mx : m \in M\}$, $m_1x = m_2x \iff m_1 = m_2$. Als Vektorräume gilt also $M \simeq Mx$ unter $m \mapsto mx$ und $n \in N$ wirkt auf Mx über $(Mx)n = M(xnx^{-1})x$. Folgende Formel gilt nun: $\operatorname{res}_N^G \operatorname{ind}_N^G(\xi) = \sum_{x \in G/N} \xi^x$.

Satz. *Ist G eine nilpotente Gruppe, so gibt es zu jedem irreduziblen Charakter χ von G eine Untergruppe U und einen abelschen (oder linearen) Charakter λ von U (das ist ein irreduzibler Charakter von U vom Grad 1) mit $\chi = \operatorname{ind}_U^G(\lambda)$.*

Beweisskizze: *Nilpotenz* vererbt sich auf Unter- und Faktorgruppen – das gestattet einen Induktionsbeweis nach der Gruppenordnung. Für den Induktionsschluß darf G als nichtabelsch angenommen werden. Es sei π_χ die zu χ gehörige Darstellung von G, also $\pi_\chi : \mathbb{C}G \twoheadrightarrow \mathbb{C}_{\chi(1)\times\chi(1)}$, $\chi(g) = \operatorname{Sp}(\pi_\chi(g))$.

Fall 1. $N \stackrel{\text{def}}{=} G \cap \ker \pi_\chi \neq 1$. Dann definiert π_χ eine irreduzible Darstellung von $\overline{G} = G/N$ mit Charakter $\overline{\chi}$, $\overline{\chi}(\overline{g}) = \chi(g)$. Also $\chi = \operatorname{infl}_N^G(\overline{\chi})$. Die aus der Induktion für das Paar $\overline{G}, \overline{\chi}$ gewonnene Relation $\overline{\chi} = \operatorname{ind}_{\overline{U}}^{\overline{G}}(\overline{\lambda})$ mit $\overline{U} \leq \overline{G}$, $\overline{\lambda} : \overline{U} \to \mathbb{C}^\times$ liefert $\chi = \operatorname{ind}_U^G(\lambda)$ mit U als dem vollen Urbild von $\overline{U}$ in G und $\lambda = \operatorname{infl}_N^U(\overline{\lambda})$.

Fall 2. $N = 1$. Wähle

$$A \lhd G\,,\ A \text{ abelsch}\,,\ Z(G) \subsetneqq A$$

(etwa so: $\overline{x} \in Z(G/Z(G))$ habe Primzahlordnung, setze $A = \langle x \rangle Z(G)$.) Der irreduzible Charakter τ von A sei Bestandteil von $\operatorname{res}_A^G(\chi)$. Ist V ein $\mathbb{C}G$-Modul zu χ und $W \subset V$ ein $\mathbb{C}A$-Modul zu τ, so gilt

$V = \sum_{g \in G} Wg$, $A \subset S \stackrel{\text{def}}{=} \{g \in G : Wg \underset{\mathbb{C}A}{\simeq} W\} \leq G$,

$Y \stackrel{\text{def}}{=} \sum_{s \in S} Ws$ ist $\mathbb{C}S$-Modul und $V = \bigoplus_{i=1}^{r} Yg_i$, wenn $G = \dot{\bigcup}_{i=1}^{r} Sg_i$.

Ist ξ der Charakter des $\mathbb{C}S$-Moduls Y, so folgt $\operatorname{ind}_S^G \xi = \chi$; insbesondere ist ξ irreduzibel. Falls $S \neq G$, gibt die Induktion $\xi = \operatorname{ind}_U^S(\lambda)$ und folglich $\chi = \operatorname{ind}_U^G(\lambda)$. Wäre $S = G$, so erzwänge $V = \sum_S Ws$ eine Gleichung $\operatorname{res}_A^G \chi = n\tau$. Bislang haben wir nur $A \lhd G$ ausgenützt, jetzt nützen wir noch aus, daß A abelsch, also $\tau(1) = 1$ ist, und sehen, daß $\pi_\chi(a)$ für alle $a \in A$ eine zentrale Matrix ist. Aus $N = 1$ resultiert dann der Widerspruch $A \subset Z(G)$.

Satz (Brauer). *$R(G) = \sum \operatorname{ind}_U^G(R(U))$, summiert über alle Untergruppen U von G der Form $U = \langle g \rangle \times P$ mit $g \in G$ und $P \leq G$ eine p-Gruppe (für Primzahlen p).*

Solche U heißen p-elementare Untergruppen von G. Man kann offenbar ohne Einschränkung $p \nmid \operatorname{ord}(g)$ annehmen.

Beweisskizze: Es sei $\mathfrak{o}$ der ganze Abschluß von $\mathbb{Z}$ in $\mathbb{Q}(\zeta_{|G|})$. Alle $\chi \in R(U)$, für alle $U \leq G$, nehmen dann ihre Werte in $\mathfrak{o}$. Setze $R(G) \subset \tilde{R}(G) \stackrel{\text{def}}{=} \mathfrak{o} \otimes_{\mathbb{Z}} R(G) \subset A \stackrel{\text{def}}{=} \mathfrak{o}^G = \{f \mid f : G \to \mathfrak{o}\}$ und entsprechend $\tilde{R}(U)$ für $U \leq G$. Obige (kommutative) Ringe sind allesamt endlich erzeugte $\mathbb{Z}$-Moduln; die jeweiligen Ringerweiterungen sind also ganz.

1. Die maximalen Ideale von A (und damit m.m. die von $\tilde{R}(G)$ und $R(G)$) sind die Ideale

$$\mathfrak{P}_{x,\mathfrak{p}} = \{f \in A : f(x) \in \mathfrak{p}\}\,,$$

wobei $x \in G$ und $\mathfrak{p}$ ein maximales Ideal in $\mathfrak{o}$ ist. In der Tat ist $\{f \in A : f(x) \in \mathfrak{p}\}$ Urbild (unter dem Epimorphismus $f \mapsto f(x) : A \twoheadrightarrow \mathfrak{o}$) von $\mathfrak{p}$, also maximal; umgekehrt, ist $\mathfrak{P}$ maximal in A, so existiert ein $x \in G$ mit $x(\mathfrak{P}) = \{f(x) : f \in \mathfrak{P}\} \neq \mathfrak{o}$, weil sonst

$$\forall\, x \exists\, f_x \in \mathfrak{P} : f_x(x) = 1\,,\ \text{also } 1 = \sum_x f_x \varepsilon_x \in \mathfrak{P}\,,$$

mit $\varepsilon_x \in A$, $\varepsilon_x(y) = \delta_{x,y}$.

2. Setze $\wp_{x,\mathfrak{p}} = \mathfrak{P}_{x,\mathfrak{p}} \cap \tilde{R}(G)$. Es gilt $\wp_{x,\mathfrak{p}} = \wp_{x',\mathfrak{p}}$ wenn x' die p-reguläre Komponente von x zur Primzahl $p \in \mathfrak{p}$ ist (also $x = x'x_p = x_p x'$ mit x' p-regulär [9] und x_p von p-Potenzordnung).

3. Es sei jetzt $x = x'$. Dann ist

$$\operatorname{ind}_U^G(\tilde{R}(U)) \not\subseteq \wp_{x,\mathfrak{p}}\,,$$

wenn $U = \langle x\rangle \times P$ mit P als einer p-Sylowuntergruppe von $Z_G(x)$ definiert ist. Denn

$$\psi \in \tilde{R}(U)\,,\ \psi(x^i y) = \begin{cases} 0 & i \not\equiv 1 \mod (\operatorname{ord}(x)) \\ \operatorname{ord}(x) & \text{sonst.} \end{cases}$$

Dabei folgt $\operatorname{res}_{\langle x\rangle}^U \psi \in \tilde{R}(\langle x\rangle)$ aus den Orthogonalitätsrelationen und $\mathfrak{o} \subset \tilde{R}(U)$, und daraus dann natürlich $\psi \in \tilde{R}(U)$. Beachte nun $\operatorname{ind}_U^G(\psi)(x) = \operatorname{ord}(x) \notin \mathfrak{p}$.

4. Aus $\operatorname{ind}_U^G(\tilde{R}(U)) \not\subseteq \wp_{x,\mathfrak{p}}$ resultiert $\operatorname{ind}_U^G(R(U)) \not\subseteq \wp_{x,\mathfrak{p}} \cap R(G)$. Daher existiert zu jedem maximalen Ideal $\mathfrak{m}$ von $R(G)$ eine elementare Untergruppe $U \leq G$ mit $\operatorname{ind}_U^G(R(U)) \not\subseteq \mathfrak{m}$. Da aber $\sum_U \operatorname{ind}_U^G(R(U))$ ein Ideal in $R(G)$ ist, folgt nun Brauers Satz unmittelbar.

FOLGERUNG. *1. Zum irreduziblen Charakter χ von G gibt es elementare Untergruppen $U \leq G$, ganze Zahlen $z_U \in \mathbb{Z}$ und abelsche Charaktere $\lambda : U \to \mathbb{C}^\times$, so daß $\chi = \sum_U z_U \operatorname{ind}_U^G(\lambda_U)$ gilt (die U sind nicht unbedingt paarweise verschieden).*

2. Jede Darstellung von G ist bereits über $\mathbb{Q}(\zeta_{|G|})$ realisierbar.

Zu 1. beachte, daß elementare Untergruppen nilpotent sind; 2. heißt:

$$\mathbb{Q}(\zeta_{|G|})G \simeq \mathbb{Q}(\zeta_{|G|})_{n_1\times n_1} \oplus \cdots \oplus \mathbb{Q}(\zeta_{|G|})_{n_h\times n_h} \quad \text{und} \quad \mathbb{C}G = \mathbb{C} \otimes_{\mathbb{Q}(\zeta_{|G|})} \mathbb{Q}(\zeta_{|G|})G\,.$$

D) Darstellungen über Zahlkörpern

K sei ein Zahlkörper, also eine endliche Körpererweiterung von $\mathbb{Q}$. Wir betrachten $\mathbb{Q}G = \bigoplus_{i=1}^t \mathfrak{b}_i$, wobei die $\mathfrak{b}_i$ die minimalen zweiseitigen Ideale von $\mathbb{Q}G$ sind. Es gilt $\mathfrak{b}_i \simeq (D_i)_{n_i\times n_i}$; K_i bezeichne das Zentrum von $\mathfrak{b}_i$ (oder von D_i) und s_i den Index von D_i, also $[D_i : K_i] = s_i^2$.

[9] i.e. $p \nmid \operatorname{ord}(x')$

Wegen $\mathfrak{b}_i \subset KG \subset \mathbb{C}G$ gibt es einen irreduziblen Charakter χ_i von $\mathbb{C}G$ [10] mit $\chi_i(\mathfrak{b}_i) \neq 0$. Ein solcher sei im folgenden fixiert.

Ein minimales Rechtsideal $\mathfrak{r}_i$ von $\mathfrak{b}_i$ ist ein irreduzibler KG-Modul und liefert eine Darstellung von G durch Matrizen über K. Die zugehörige Spurfunktion werde mit ψ_i bezeichnet; sie heißt ein irreduzibler K-Charakter von G. Beachte: $\psi_i(1) = \dim_K \mathfrak{r}_i = [D_i : K]n_i = [K_i : K]s_i^2 n_i$.

SATZ (Deuring-Noether). *Sind M und N KG-Moduln mit $\mathbb{C} \otimes_K M \simeq \mathbb{C} \otimes_K N$ als $\mathbb{C}G$-Moduln, so sind sie schon isomorph als KG-Moduln. Mit anderen Worten: $R_K(G) \subset R(G)$.*

Natürlich entsteht $R_K(G)$ genauso aus den KG-Moduln wie $R(G)$ aus den $\mathbb{C}G$-Moduln, und die behauptete Inklusion ist von $M \mapsto \mathbb{C} \otimes_K M$ induziert. Man erinnere sich in diesem Zusammenhang an den Satz aus der Linearen Algebra, nach dem zwei reelle Matrizen, die über $\mathbb{C}$ konjugiert sind, schon im reellen Matrixring konjugiert sind.

Eine erste Konsequenz ist, daß auch die KG-Moduln vollständig durch ihre Charaktere bestimmt sind.

SATZ. 1. *$K_i = K(\chi_i) \overset{\text{def}}{=} K(\chi_i(x) : x \in G)$. Insbesondere ist K_i eine galoissch abelsche Erweiterung von K; wir setzen $\mathfrak{G}_i = G_{K_i/K}$.*

2. *$\psi_i = s_i \sum_{\sigma \in \mathfrak{G}_i} \sigma(\chi_i)$*

Dabei bezeichnet $\sigma\chi_i$ den Charakter $\sigma\chi_i(g) = \sigma(\chi_i(g))$. Beachte hier, daß χ_i schon über $K(\zeta_{|G|})$ definiert, also $\chi_i(g)$ Spur einer Matrix mit Koeffizienten aus diesem Körper ist; zu $\sigma\chi_i$ gehört dann die Darstellung, die aus der von χ_i durch Anwendung des auf $K(\zeta_{|G|})$ fortgesetzten Automorphismus σ auf die einzelnen Matrixeinträge entsteht.

Als Folgerung erhalten wir noch:

$$\psi_i(1) = [K_i : K]s_i^2 n_i = s_i[K_i : K]\chi_i(1) \implies s_i \mid \chi_i(1) \mid |G| \,.$$

Der Beweis des letzten Satzes geschieht so. Setze $L = K(\zeta_{|G|})$. Anstatt mit $\mathbb{C}G$ können wir genausogut mit LG arbeiten, z.B. also χ_i als LG-irreduziblen Charakter von G auffassen. (Obiger Satz macht also $R_K(G)$ durch interne Eigenschaften von $R_L(G) = R(G)$ kenntlich.)

$L \otimes_K \mathfrak{b}_i$ ist ein zweiseitiges Ideal von LG und somit direkte Summe einiger der minimalen zweiseitigen Ideale von LG, von denen eines, etwa $\mathfrak{a}_i$, zu χ_i gehöre. Genauer:

$$L \otimes_K (D_i)_{n_i \times n_i} = \Big((L \otimes_K K_i) \otimes_{K_i} D_i\Big)_{n_i \times n_i} = \Big(\bigoplus_{\sigma \in G(K_i/K)} L_\sigma \otimes_{K_i} D_i\Big)_{n_i \times n_i} = \bigoplus_\sigma \Big((L_\sigma)_{s_i \times s_i}\Big)_{n_i \times n_i}$$

wobei $L_\sigma = L$, aber die Wirkung von $g \in G$ auf dem Matrixring $(L_\sigma)_{r \times r}$ (mit $r = s_i n_i$) die von g auf $\mathfrak{a}_i = L_{r \times r}$ gefolgt von der von σ auf den einzelnen Matrixeinträgen ist. Man beachte, daß $K_i \subset L$ aus dem Vergleich der Zentren von KG und $L \otimes_K KG = LG$ resultiert.

Wir sehen, daß die $\sigma \in G(K_i/K)$ (gelesen in $G(L/K)$) genau die verschiedenen einfachen Komponenten von $L \otimes_K \mathfrak{b}_i$ indizieren, insbesondere also $\chi_i \neq \sigma\chi_i$ für $\sigma \neq 1$ gilt. Damit induzieren die

[10] diese heißen ab sofort *absolut irreduzibel*

σ verschiedene Automorphismen auf $K(\chi_i)$; andererseits kommt $\tau\chi$ für jedes $\tau \in G(K(\chi_i)/K)$ (wegen $\tau\psi_i = \psi_i$) in $L \otimes_K \mathfrak{b}_i$ vor. Das beweist $K_i = K(\chi_i)$. Und 2. folgt aus $s_i n_i = \chi_i(1)$.

E) Die Brauergruppe von K

Wir wollen nun für einen beliebigen Körper K einen Überblick über die möglichen Schiefkörper D über K bekommen. Wir nehmen dabei durchweg an, daß K das Zentrum von D ist.

SATZ. *1. Sind A und B zentraleinfache Algebren über K, i.e. einfache Algebren mit $Z(A) = K = Z(B)$, so ist $A \otimes_K B$ auch zentraleinfach.*

2. Ist A zentraleinfach, so auch

$$A^* = \{a^* : a \in A\} \quad \text{mit}$$
$$a_1^* = a_2^* \iff a_1 = a_2\,,\ a^* + b^* = (a+b)^*\,,\ a^*b^* = (ba)^*\,,\ \alpha a^* = (\alpha a)^*\,,$$

und es gilt $A \otimes_K A^* \simeq K_{n\times n}$ mit $n = \dim_K A$.

A^* heißt die zu A antiisomorphe Algebra. Das Tensorprodukt $A \otimes_K B$ der K-Vektorräume A, B bekommt die Algebrenstruktur durch

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2\,.$$

Die Isomorphie $A \otimes_K A^* \simeq K_{n\times n}$ ist von folgender Abbildung induziert. Betrachte A als n-dimensionalen K-Vektorraum (so daß $\mathrm{End}_K(A) = K_{n\times n}$) und sende $a \in A$ auf $l_a\,,\ l_a(x) = ax\,,$ und $a^* \in A^*$ auf $r_a\,,\ r_a(x) = xa$. Der resultierende Homomorphismus $A \otimes_K A^* \to \mathrm{End}_K(A)$ ist injektiv, weil $A \otimes_K A^*$ einfach ist, und aus Dimensionsgründen surjektiv.

DEFINITION. *Zwei zentraleinfache K-Algebren A und B heißen ähnlich, wenn $A \simeq D_{n\times n}$ und $B \simeq D_{m\times m}$ mit demselben Schiefkörper D gilt.*

SATZ. *Die Ähnlichkeitsklassen der zentraleinfachen K-Algebren bilden mit $\otimes_K$ eine abelsche Gruppe $B(K)$, die Brauergruppe von K.*

$B(K)$ beschreibt also die Isomorphietypen der über K zentralen Schiefkörper; K selbst repräsentiert das Einselement in dieser Gruppe (genauso wie $K_{n\times n}$ für $n \in \mathbb{N}$ und D^* das Inverse von D.

Es sei L/K eine (algebraische) Erweiterung. Wir definieren eine Abbildung $B(K) \to B(L)$ durch $A \mapsto L \otimes_K A$. Der Beweis von 1. im vorletzten Satz zeigt, daß $L \otimes_K A$ eine zentraleinfache Algebra ist. Die Abbildung ist offensichtlich wohldefiniert und ein Homomorphismus von Gruppen. A geht auf $1 \in B(L)$ genau wenn $L \otimes_K A \simeq L_{n\times n}$ (mit $n^2 = \dim_K A$) gilt; in diesem Fall heißt L ein *Zerfällungskörper* von A. Wir bezeichnen den Kern der Abbildung mit $B(L/K)$.

Beispiele in diesem Zusammenhang sind

1. $K = \mathbb{R}\,,\ L = \mathbb{C}$ und $A = \mathbb{H}$.
2. $L = K^{\mathrm{c}}$. Also ist $\dim_K(A)$ tatsächlich *immer ein Quadrat.*

3. Ist L Zerfällungskörper von A, so auch jede (algebraische) Erweiterung von L.

SATZ. *Ist D ein über K zentraler Schiefkörper endlicher Dimension, so existiert in D ein maximaler kommutativer Teilkörper L mit $[L:K]^2 = \dim_K(D)$. L zerfällt D.*

Zum Beweis wähle L maximal unter allen in D enthaltenen Körpern (wie etwa K). Setze $Z_D(L) = \{d \in D : d\lambda = \lambda d \ (\forall\, \lambda \in L)\}$; dies ist ein Schiefkörper mit Zentrum $\supset L$. Wähle, falls möglich, $d \in Z_D(L) \setminus L$. Aber dann ist $L(d)$ ein gößerer Körper in D als L. Also $Z_D(L) = L$. Wir zeigen $L \otimes_K D = L_{r\times r}$ mit $r = [D:L]$. Fasse dazu D als L-Linksvektorraum auf und betrachte die Abbildung $L \otimes_K D \to \mathrm{End}_L(D)$ [11]

$\lambda \mapsto$ Linksmultiplikation mit λ auf D,

$d \mapsto$ Rechtsmultiplikation mit d auf D.

Dies ist ein Homomorphismus $\neq 0$ von L-Algebren, also schon ein Monomorphismus, weil $L \otimes_K D$ einfach ist. Wir berechnen die Dimensionen

$$\dim_L(L \otimes_K D) = \dim_K D = n\,,\ \dim_L(\mathrm{End}_L(D)) = (\dim_L(D))^2\,.$$

Der Beweis ist beendet, wenn $n = \dim_K(D) = (\dim_L(D))^2$ gezeigt ist. Nun ist $D \otimes_K D^* \simeq K_{n\times n}$ und $L = L\otimes 1 \subset K_{n\times n}$. Der Zentralisator von $L\otimes 1$ in $D\otimes D^*$ ist $L\otimes D^*$, weil $L = Z_D(L)$. Dessen L-Dimension ist damit n. Nun ist der Zentralisator von L in $K_{n\times n}$ isomorph zu $\mathrm{End}_L(K^n)$, weil K^n über $L \subset K_{n\times n}$ ein L-Vektorraum ist, und folglich $(n/[L:K])^2 = n$ oder $n = [L:K]^2$. Aus $n = s^2$ (mit $s =$ Schurindex von D) folgt dann die Behauptung.

Ab jetzt sei der Einfachheit halber K ein vollkommener Körper. Dann existiert zu jeder zentraleinfachen Algebra ein Zerfällungskörper, der galoissch endlich über K ist:

$$B(K) = \bigcup_{L/K \text{ galoissch}} B(L/K)\,.$$

SATZ (Skolem-Noether). *A sei zentraleinfach über K und $B \subset A$ einfach. Dann existiert zu einem K-Algebrenhomomorphismus $g : B \to A$ ein in A invertierbares Element u mit $g(b) = ubu^{-1}$.*

Der Beweis benutzt die einfache Algebra $C = B \otimes_K A^*$, die auf natürliche Weise von links auf A wirkt. Aus g resultiert eine zweite Wirkung. Da der C-Modul A direkte Summe einfacher C-Moduln ist und die alle isomorph sind, gibt es einen C-Isomorphismus $\gamma : A \to A$ mit

$$(bxa)\gamma = ((b\otimes a^*)x)^\gamma = (b\otimes a^*)(x)^\gamma = g(b)(x)^\gamma a\,,$$

insbesondere also

$$(1)^\gamma b = ((1\otimes b^*)1)^\gamma = (b)^\gamma = ((b\otimes 1^*)1)^\gamma = g(b)(1)\gamma\,.$$

Also $u \overset{\text{def}}{=} (1)^\gamma$.

Anwendungen:

[11] die $f \in \mathrm{End}_L(D)$ werden von rechts geschrieben

1. $K = \mathbb{R} \implies B(\mathbb{R}) = B(\mathbb{C}/\mathbb{R})$. An zentralen Schiefkörpern $D \neq \mathbb{R}$ kommen deshalb nur 4-dimensionale vor und $\mathbb{C}$ ist stets ein maximaler Teilkörper. $g : \mathbb{C} \rightarrowtail D$, $i \mapsto -i$ wird durch ein $u \in D^\times$ geliefert, $i^3 = uiu^{-1}$. Weil $\mathbb{C}$ von u^2 zentralisiert wird und $g(u^2) = uu^2u^{-1} = u$, ist u^2 reell und sicher negativ, also $= -r^2$ mit einem $r \in \mathbb{R}$. Setze $j = u/r$ und rechne nach, daß $D \simeq \mathbb{H}$ unter $i \mapsto i$, $j \mapsto j$. Also $B(\mathbb{R}) = \{\mathbb{R}, \mathbb{H}\} = \mathbb{Z}/2$.

2. K sei endlich. Ist D zentraler Schiefkörper über K und $d \in D$ in dem maximalen Teilköper L enthalten, so ist L bis auf Isomorphie unabhängig von d und zyklisch über K. Es resultiert $D = \bigcup_{u \in D^\times} uLu^{-1}$ oder $D^\times = \bigcup_{u \in D^\times} uL^\times u^{-1}$. Aber eine endliche Gruppe G ist nicht die Vereinigung der Konjugierten einer echten Untergruppe U: $G = \dot{\bigcup} g_i U$ & $G = \bigcup g_i U g_i^{-1} \implies |G| < [G : U]|U|$ weil $1 \in g_i U g_i^{-1}$. – Also $B(K) = 1$.

3. Die reduzierte Norm (eine Verallgemeinerung der Determinante ins Nichtkommutative); die reduzierte Spur:

   A sei eine zentraleinfache K-Algebra und L ein über K galoisscher Zerfällungskörper von A. Über einen Isomorphismus $\varphi : L \otimes_K A \simeq L_{n\times n}$ definiere die reduzierte Norm (Spur) von $a \in A$ durch $\mathrm{nr}(a) = \det(\varphi(1 \otimes a))$, $\mathrm{tr}(a) = \mathrm{Spur}(\varphi(1 \otimes a))$. Dann hängen zufolge des Skolem-Noetherschen Satzes $\mathrm{nr}(a)$ und $\mathrm{tr}(a)$ nicht von der speziellen Wahl von φ ab, und auch nicht von der von L, weil, mit $K \subset L \subset H$, $L \subset H$ die natürliche Abbildung $L \otimes_K A \rightarrowtail H \otimes_K A$ mit $1 \otimes a = 1 \otimes a$ stiftet.

   Erweitere $\sigma \in G(L/K)$ auf natürliche Weise zu einem Automorphismus von $L_{n\times n}$. Dann zeigt eine erneute Verwendung des genannten Satzes $\det(\varphi(1 \otimes a)) = \det((\varphi(1 \otimes a))^\sigma) = \det(\varphi(1 \otimes a))^\sigma$, also $\mathrm{nr}(a) \in K$ (und ebenso $\mathrm{tr}(a) \in K$). Offenbar gilt noch $\mathrm{nr}(ab) = \mathrm{nr}(a)\mathrm{nr}(b)$, $\mathrm{tr}(a + b) = \mathrm{tr}(a) + \mathrm{tr}(b)$ und darüber hinaus $[\,\mathrm{nr}(a) = 0 \iff a$ ist Nullteiler$\,]$.

Verschränkte Produkte:

Es liege der Sonderfall vor, daß L/K galoissch (mit Gruppe G) sei und L genau mittig in der zentraleinfachen K-Algebra A liege (i.e., $\dim_K A = [L : K]^2$). Dann führt jedes $\sigma \in G$ zu einem invertierbaren Element u_σ in A und diese u_σ sind zufolge des Artinschen Lemmas über die L-lineare Unabhängigkeit der $\sigma \in G$ als Funktionen auf L linear unabhängige Elemente in A, damit $A = \bigoplus_\sigma Lu_\sigma$. Wir notieren die Rechenregeln

1. $u_\sigma \lambda = \lambda^{\sigma^{-1}} u_\sigma$ für $\lambda \in L$

2. $u_\sigma u_\tau = c_{\sigma,\tau} u_{\sigma\tau}$ mit $c_{\sigma,\tau} \in L^\times$

3. u_σ kann zu $a_\sigma u_\sigma$ mit einer Funktion $G \ni \sigma \mapsto a_\sigma \in L^\times$ abgeändert werden und diese Funktion verändert $c_{\sigma,\tau}$ zu $a_\sigma a_\tau^{\sigma^{-1}} a_{\sigma\tau}^{-1} c_{\sigma,\tau}$.

Das Assoziativgesetz in A ist dann gleichwertig mit der Relation $c_{\sigma,\tau}^{\omega} c_{\sigma\tau,\omega} = c_{\sigma,\tau\omega} c_{\tau,\omega}$.

Umgekehrt, ist L/K galoissch mit Gruppe G und A der n-dimensionale L-Linksvektorraum mit Basis u_σ (indiziert mit den $\sigma \in G$), so wird A zu einer assoziativen Algebra über $u_\sigma \lambda = \lambda^{\sigma^{-1}} u_\sigma$, $u_\sigma u_\tau = c_{\sigma,\tau} u_{\sigma\tau}$ mit Elementen $c_{\sigma,\tau}$ wie oben. Das Zentrum ist K und A ist tatsächlich einfach (wieder wegen des Artinschen Lemmas).

Können wir nun zeigen, daß $(*)$ es zu jedem Element $D \in B(L/K)$ ein $A \sim D$ gibt, das L genau mittig enthält, so ist $B(L/K)$ durch die Funktionen $c_{\sigma,\tau}$ modulo den a_σ bestimmt und zwar, wie man nachrechnet, auf eineindeutige Weise, i.e., $B(L/K) \simeq H^2(G, L^\times)$ als Gruppen, wenn $H^2(G, L^\times)$ die Gruppe $\{c_{\sigma,\tau}\}/\{a_\sigma\}$ (mit der natürlichen Multiplikation) abkürzt (s.u.).

$(*)$ folgt aus dem Zentralisatorsatz: *A sei zentraleinfach über K und $B \subset A$ einfach. Dann ist der Zentralisator $C = Z_A(B)$ von B in A einfach mit $Z(C) = Z(B)$ und es gilt $C \sim B \otimes_K A$, $[B : K] = [A : C]$ (und insbesondere dann $Z_A(C) = B$).*

Dies resultiert aus $B \otimes 1 \subset A \otimes_K A^* = K_{n^2 \times n^2}$ und: $B \otimes 1$ hat den Zentralisator $C \otimes A^*$ in $K_{n^2 \times n^2}$; B induziert K-lineare Abbildungen auf K^{n^2} und die B-invarianten darunter sind die Elemente aus $C \otimes A^*$, mithin $C \otimes A^* = \mathrm{End}_B(K^{n^2}) = \mathrm{End}_B(tE) = (D)_{t \times t}$ mit dem einfachen B-Modul E und $D \sim B$.

Und $(*)$ selbst folgt dann so: $1 \otimes D \subset L \otimes D = L_{n \times n} \subset K_{nr \times nr}$ mit $r = [L : K]$. Weiter liegt $L \otimes 1$ im Zentralisator $Z_{K_{nr \times nr}}(1 \otimes D) = C \sim D$ nach obigem Satz, der auch die Einfachheit von C mit Zentrum K und die Mittigkeit von L in C impliziert.

Es st nun einfach, folgendes zu erkennen.

1. $(L/K, c_{\sigma,\tau}) \simeq (L/K, b_{\sigma,\tau}) \iff c_{\sigma,\tau} \sim b_{\sigma,\tau}$. Hier bezeichnet
$$(L/K, c_{\sigma,\tau}) = \bigoplus_{\sigma \in G(L/K)} L u_\sigma$$
die zentraleinfache Algebra, die wie weiter oben zu der galoisschen Erweiterung L/K und dem Faktorensystem $c_{\sigma,\tau} \in L^\times$, $c_{\tau,\omega}^{\sigma^{-1}} c_{\sigma,\tau\omega} = c_{\sigma,\tau} c_{\sigma\tau,\omega}$, $u_\sigma \lambda = \lambda^{\sigma^{-1}} u_\sigma$ $(\forall\, \lambda \in L,\, \sigma, \tau, \omega \in G)$ konstruiert wurde, und $\sim$ bedeutet, daß $c_{\sigma,\tau}$ um eine Funktion $G \times G \to L^\times$, $(\sigma, \tau) \mapsto \alpha_\sigma \alpha_\tau^{\sigma^{-1}} \alpha_{\sigma\tau}^{-1}$ mit $\alpha_\sigma \in L^\times$ abgeändert werden darf.

2. $(L/K, c_{\sigma,\tau}) \simeq K_{n \times n} \iff c_{\sigma,\tau} \sim 1$ (mit $n = [L : K]$).

Beispiel: Ist L/K zyklisch und $\langle \sigma \rangle = G = G(L/K)$, so ist jedes Element aus $B(L/K)$ gleich einem $(L/K, \sigma, a) = \bigoplus_{i=0}^{n-1} L u^i$ mit $u^n = a \in K^\times$, $u\lambda = \lambda^{\sigma^{-1}} u$. Genau dann geben a_1 und a_2 dieselbe Algebra, wenn sie sich um ein Normelement $\mathrm{N}_{L/K}(\alpha)$ mit einem $\alpha \in L^\times$ unterscheiden. Man bemerke, daß a von der Wahl des Erzeugenden σ abhängt: wird σ durch σ^r mit $(r, n) = 1$ ersetzt, so muß a durch a^r ersetzt werden.

In diesem zyklischen Fall gilt also $B(L/K) = K^\times / \mathrm{N}_{L/K} L^\times$.

Diejenigen $D \in B(K)$ mit Schurindex 2 enthalten einen über K quadratischen Teilkörper L, der automatisch galoissch über K ist. Damit $D = \langle 1, u, v, uv \rangle_K$ mit $L = K(v)$, $v^2 = b \in K^\times$, $u^2 = a \in K^\times$, $uv = -vu$. Dies sind die sogenannten Quaternionenalgebren $(\frac{a,b}{K})$. Beachte die Symmetrie in a, b. Daß D schief ist, bedeutet genau $a \notin \mathrm{N}_{K(\sqrt{b})/K}$ oder auch $b \notin \mathrm{N}_{K(\sqrt{a})/K}$. Man beobachtet noch

1. Eine Algebra $(\frac{a,b}{K})$, die von $1, u, v, uv$ mit den Relationen $u^2 = a \in K^\times$, $v^2 = b \in K^\times$, $uv = -vu$ über K erzeugt ist, hat die Dimension 4 über K und ist deshalb einfach mit Zentrum K. Ist a ein Quadrat in K, so handelt es sich bei der Algebra um $K_{2\times 2}$ mit (etwa) $u = \sqrt{a} \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ und $v = \left(\begin{smallmatrix} 0 & b \\ 1 & 0 \end{smallmatrix}\right)$.

2. Die reduzierte Norm auf $(\frac{a,b}{K})$ sendet $x = \alpha_0 + \alpha_1 u + \alpha_2 v + \alpha_3 uv$ auf $\alpha_0^2 - \alpha_1^2 a - \alpha_2^2 b + \alpha_3^2 ab$. Denn, mit $\overline{x} = \alpha_0 - \alpha_1 u - \alpha_2 v - \alpha_3 uv$, gilt $\overline{x+y} = \overline{x} + \overline{y}$, $\overline{xy} = \overline{y} \cdot \overline{x}$, $x\overline{x} = \overline{x}x$. Insbesondere ist $K(x, \overline{x})$ ein kommutativer Teilkörper L ($\mathrm{nr}(x) \neq 0$ angenommen) und also (wenn nicht $x \in K$) $\mathrm{nr}(x) = \mathrm{N}_{L/K}(x) = x\overline{x} = \alpha_0^2 - \alpha_1^2 a - \alpha_2^2 b + \alpha_3^2 ab$.

Diese Quaternionenalgebren zusammen mit K sind Elemente $A \in B(K)$ mit $A \otimes_K A \sim 1$ in $B(K)$. Und tatsächlich ist $B(K)$ eine Torsionsgruppe: *Hat $A \in B(K)$ den Schurindex s, so gilt $A^s = 1$ in $B(K)$.*

Das sieht man so. Wird A von dem über K galoisschen L zerfällt, also o.E. $A = (L/K, c_{\sigma,\tau})$, so hat der einfache A-Modul E über L die Dimension s, weil L mittig in A liegt. Man lasse nun A von links auf dem antiisomorphen E^* wirken (gehe von der 'obersten Zeile' zu der 'linken Spalte' über). Das liefert bezüglich einer L-Basis von E^* zu den u_σ Matrizen U_σ, die $c_{\sigma,\tau} U_{\sigma\tau} = U_\sigma U_\tau^{\sigma^{-1}}$ erfüllen. Mit $\alpha_\sigma = \det(U_\sigma)$ findet man dann $c_{si,\tau}^s = \alpha_\sigma \alpha_\tau^{\sigma^{-1}} \alpha_{\sigma\tau}^{-1}$.

Zusatz: *In der Ordnung eines Elementes in $B(K)$ kommen tatsächlich alle Primteiler des Schurindexes dieses Elementes vor.* Das sieht man über ein 'Sylow'-Argument ein. Man wählt zunächst einen über K galoisschen Zerfällungskörper L und nimmt dann den Fixkörper F einer Sylow p-Untergruppe von $G = G_{L/K}$ für eine Primzahl p, die den Schurindex (von $D \in B(K)$) teilt. Nun nützt man folgende Beobachtung aus: *Zerfällt der Körper $M \supset K$ den Schiefkörper D, so gilt $s \mid [M : K]$.* Denn dann gilt $M \otimes_K D = M_{s\times s}$ und der irreduzible Modul M^s erfüllt $\dim_D M^s = \frac{s[M:K]}{s^2}$. Damit zurück zu obigem F: der Schurindex $\tilde{s}$ von $F \otimes_K D$ ist wegen $p \nmid [F : K]$ ungleich 1 und wegen $L \otimes_F (F \otimes_K D) = F_{s\times s}$ eine Potenz von p. Nun teilt offensichtlich die Ordnung von $F \otimes_K D \in B(F)$ die von $D \in B(K)$, da die Abbildung $B(K) \xrightarrow{\otimes_F} B(F)$ ein Homomorphismus abelscher Gruppen ist; darüber hinaus wissen wir bereits, daß erstere ein Teiler von $\tilde{s}$ ist.

Wir skizzieren nun, warum die Abbildung $B(K) \to \langle c_{\sigma,\tau} : G \times G \to L^\times \rangle / \langle (\sigma, \tau) \mapsto \alpha_\sigma \alpha_\tau^{\sigma^{-1}} \alpha_{\sigma\tau}^{-1} \rangle$ multiplikativ ist: Betrachte $C = A \otimes_K B$ mit $A = (L/K, b_{\sigma,\tau})$, $B = (L/K, c_{\sigma,\tau})$. Ist e ein Idempotent $\neq 0$ in C, so ist $eCe = \mathrm{Hom}_C(eC, eC)$ zentraleinfach über K, weil eC ein Vielfaches des einfachen C-Rechtsmoduls ist. Wir geben ein e mit $eCe \simeq (L/K, b_{\sigma,\tau} c_{\sigma,\tau})$ an, nämlich

$$e = \prod_{\sigma \neq 1} (\alpha \otimes 1 - 1 \otimes \sigma(\alpha)) \,/\, (\prod_{\sigma \neq 1} (\alpha - \sigma(\alpha))) \otimes 1$$

mit $L = K(\alpha)$ und $\sigma \in G = G_{L/K}$. Multipliziert man den Zähler aus, so erhält man einen Ausdruck der Form $\sum_{i=0}^{n-2} \alpha^i \otimes b_i \in L \otimes_K L$ mit $n = [L : K]$, also ein Element $\neq 0$. Hingegen ergibt die gleiche Rechnung die Gleichheit $\prod_\sigma (\alpha \otimes 1 - 1 \otimes \sigma(\alpha)) = f_\alpha(\alpha) \otimes 1 = 0$. Daraus folgt der Reihe nach

$$\begin{aligned}
&(\alpha \otimes 1)e = (1 \otimes \alpha)e\,,\ (\lambda \otimes 1)e = (1 \otimes \lambda)e\ (\forall\, \lambda \in L)\,,\\
&e^2 = e\,,\ e(L \otimes 1) \simeq L\,,\\
&e(u_\sigma \otimes v_\tau)e = \begin{cases} 0 & ,\ \sigma \neq \tau \\ (u_\sigma \otimes v_\sigma)e = e(u_\sigma \otimes v_\sigma & ,\ \text{sonst} \end{cases}\\
&eCe = \textstyle\sum_\sigma e(L \otimes 1) w_\sigma \text{ mit } w_\sigma = e(u_\sigma \otimes v_\sigma)e\,,
\end{aligned}$$

und zu w_σ gehört das Faktorsystem $b_{\sigma,\tau} c_{\sigma,\tau}$.

Schlußbemerkungen :

1. Mittels zahlentheoretischer Argumente (aus der *Bewertungs-* und *Klassenkörpertheorie*) kann man $B(K)$ für lokale Körper und Zahlkörper K ausrechnen (also für Körper K, die endlich über den p-adischen Zahlen $\mathbb{Q}_p$ oder über den rationalen Zahlen $\mathbb{Q}$ sind). Haupthilfsmittel in beiden Fällen ist, daß ein Schiefkörper $D \in B(K)$ *zyklisch* ist, d.h. mittig einen über K zyklisch galoisschen maximal kommutativen Teilkörper enthält.

2. Die Theorie der halbeinfachen K-Algebren A ist für zahlentheoretische Anwendungen zu grob. Im Fall eines Zahlkörpers K sind nicht die A das eigentliche Objekt des Interesses, sondern vielmehr die $\mathfrak{o}$-*Ordnungen* Λ in A : dabei ist $\mathfrak{o}$ etwa der Ring der ganzen algebraischen Zahlen von K und $\Lambda \subset A$ ein Ring, der zugleich ein endlich erzeugter $\mathfrak{o}$-Modul ist und eine K-Basis von A enthält. Das Standardbeispiel bei $A = \mathbb{Q}G$, der Gruppenalgebra einer endlichen Gruppe G über $\mathbb{Q}$, ist $\Lambda = \mathbb{Z}G$, der ganzzahlige Gruppenring von G. Diese Ordnungen Λ sind bislang bei weitem nicht vollständig verstanden; recht gut Bescheid weiß man allerdings über die *Maximalordnungen* $\Lambda_{\max}$, das sind solche Ordnungen in A, die in keiner Ordnung von A echt enthalten sind. Ein Beispiel dazu: ist G die zyklische Gruppe der Ordnung 2, so gilt $\Lambda = \mathbb{Z}G \subsetneq \Lambda_{\max} = \mathbb{Z} \oplus \mathbb{Z} \subset \mathbb{Q} \oplus \mathbb{Q} = \mathbb{Q}G$.