

§7. Gruppenalgebren und Charaktere

In §5 haben wir Moduln für beliebige Ringe definiert, dann aber für spezielle kommutative Ringe betrachtet. In diesem Kapitel ~~§7~~ und danach betrachten wir Moduln über im Allgemeinen nicht kommutativen Ringen (und verwenden vorgesetzt an die übliche Abkürzung: "nicht kommutativ" heißt "nicht notwendig kommutativ" - kommutative Ringe sind also Beispiele von nicht kommutativen Ringen). Natürlich stellen wir wieder Bedingungen an die zu betrachtenden Ringe.

7.1 Definition: Sei K ein Körper und A ein Ring, der auch ein K -Vektorraum ist. A ist eine K -Algebra: $(=) \forall \lambda \in K, x, y \in A$:
 $(\lambda x)y = \lambda(xy) = x(\lambda y)$. ↑ oder: eine Algebra über K

(Diese Definition funktioniert auch für K kommutativer Ring und A ein K -Modul. *Jeder Ring ist eine K -Algebra.*)

Eine Algebra ist ein Ring mit einer Zusatzstruktur.

Eine äquivalente Definition von K -Algebra ist: A ist ein Ring und \exists Ringhomomorphismus $K \xrightarrow{\varphi} A$, dessen Bild im Zentrum von A liegt, d.h. $\text{Im}(\varphi) \subset \mathcal{Z}(A) = \{a \in A : ab = ba \forall b \in A\}$. *nachprüfen: das ist äquivalent*

Beispiele: K ist eine K -Algebra

$\text{Mat}(n \times n, K)$ ist eine K -Algebra ($n \times n$ -Matrizen)

V ein K -Vektorraum, $A := \text{End}_K(V)$ ist eine K -Algebra

$\{K$ -lineare Abbildungen $V \rightarrow V\}$

7.2 Definition: Sei K ein Körper und G eine Gruppe. Die Gruppenalgebra KG hat als K -Vektorraum eine Basis $\{b_g : g \in G\}$. Die Multiplikation setzt die

Multiplikation in G linear fort: $(\sum \lambda_g b_g) \cdot (\sum \mu_h b_h) = \sum \lambda_g \mu_h b_{gh}$

*Axiome nachprüfen
Einselement in KG ?*

\uparrow
 $\in K$, nur
 endlich viele $\neq 0$

\uparrow
 $g, h \in G$
 mit $g \cdot h = j$

(Die Abbildung $G \rightarrow KG$ ist multiplikativ und identifiziert die $g \mapsto b_g$ Gruppenelemente mit den Basisvektoren. Wir betrachten G deshalb oft als Teilmenge von KG , genauer als Basis.)
 Uns interessiert die Gruppenalgebra KG , wenn G eine endliche Gruppe ist.
 Die Situation ist dann besonders übersichtlich für $K = \mathbb{C}$ (oder für K algebraisch abgeschlossen von Charakteristik 0). *gibt es außer \mathbb{C} noch andere solche Körper?*

Die Gruppenalgebra "linearisiert" die Gruppe. In KG kann man die Gruppenelemente nicht nur wie in G miteinander multiplizieren, sondern auch addieren und mit Skalaren in K multiplizieren.

7.3 Definition: Seien A und B K -Algebren. Ein Homomorphismus von K -Algebren $\varphi: A \rightarrow B$ ist ein K -linearer Ringhomomorphismus.

$$\uparrow \text{ also insbesondere: } \varphi(1_A) = \sum_{\substack{\# \\ 0}} 1_B$$

Moduln über einer K -Algebra sind automatisch

K -Vektorräume. warum?

Da Algebren nicht kommutativ sein müssen, müssen wir zwischen Links- und Rechtsmoduln unterscheiden. Moduln sind im Folgenden Linksmoduln, wenn nichts anderes gesagt wird.

Der K -Dualraum zu einem A -Linksmodul ist ein A -Rechtsmodul.

7.4 Definition: Ein Modul M heißt einfach (oder irreduzibel) \Leftrightarrow

0 und M selbst sind die einzigen Untermoduln. (0 nennen wir nicht einfach.)
 "simple"
 M

Sei S einfach. Dann ist S endlich erzeugt. Denn: Sei $x \in S, x \neq 0 \Rightarrow$

$A \cdot x = \{a \cdot x : a \in A\}$ ist ein Teilmodul von S ; $A \cdot x \ni x = 1 \cdot x \Rightarrow A \cdot x \neq 0$

$\Rightarrow A \cdot x = S$. S ist also zyklisch (von einem Element erzeugt).

$A = A \cdot 1$ ist auch zyklisch, aber im Allgemeinen nicht einfach.

$A = kG$ ist nur für $|G|=1$ einfach. Denn: Sei $x = \sum_{g \in G} g$ die Summe aller Gruppenelemente (G ist endlich)

Sei $M = k \cdot x = \{ \lambda x : \lambda \in k \}$, das hat k -Dimension 1.

Für $h \in G$ ist $hx = \sum_{g \in G} hg = x$ warum?

$\Rightarrow M$ ist ein Untermodul von kG

M ist einfach weil 1-dimensional.

$M = kG \Leftrightarrow |G|=1$, da $\dim kG = |G|$.

Eine wichtige Eigenschaft einfacher Module ist:

7.5 Theorem (Schurs Lemma): Sei S einfach als A -Modul. Dann ist $\text{End}_A(S)$ ein Schiefkörper, d.h. jedes Element außer 0 ist invertierbar.

Beweis: Sei $\varphi: S \rightarrow S$ ein Endomorphismus, $\varphi \neq 0$. Dann sind $\text{Kern}(\varphi)$ und $\text{Im}(\varphi)$ Teilmodule von S , einfach.

$\text{Kern}(\varphi) = S \Rightarrow \varphi = 0$ & $\Rightarrow \text{Kern}(\varphi) = 0$
 $\text{Im}(\varphi) = 0 \Rightarrow \varphi = 0$ & $\Rightarrow \text{Im}(\varphi) = S$ } $\Rightarrow \varphi$ ist injektiv und surjektiv \square

7.6 Korollar: Sei $k = \bar{k}$ und S endlich-dimensional als k -Vektorraum.

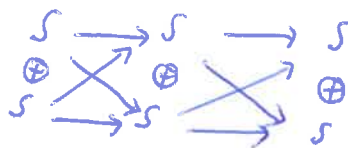
Dann $\text{End}_A(S) = \{ \lambda \cdot \text{id}_S : \lambda \in k \} \cong k$.

Beweis: Sei $\varphi: S \rightarrow S$ ein Endomorphismus $\neq 0$. Insbesondere ist φ eine k -lineare Abbildung $S \rightarrow S$, hat nach Voraussetzung also einen Eigenwert λ , mit Eigenvektor $v_0 \neq 0$. Mit φ ist auch $\varphi := \varphi - \lambda \text{id}_S$ ein A -Endomorphismus und $v_0 \in \text{Kern}(\varphi) \Rightarrow \varphi = 0, \varphi = \lambda \text{id}_S. \square$

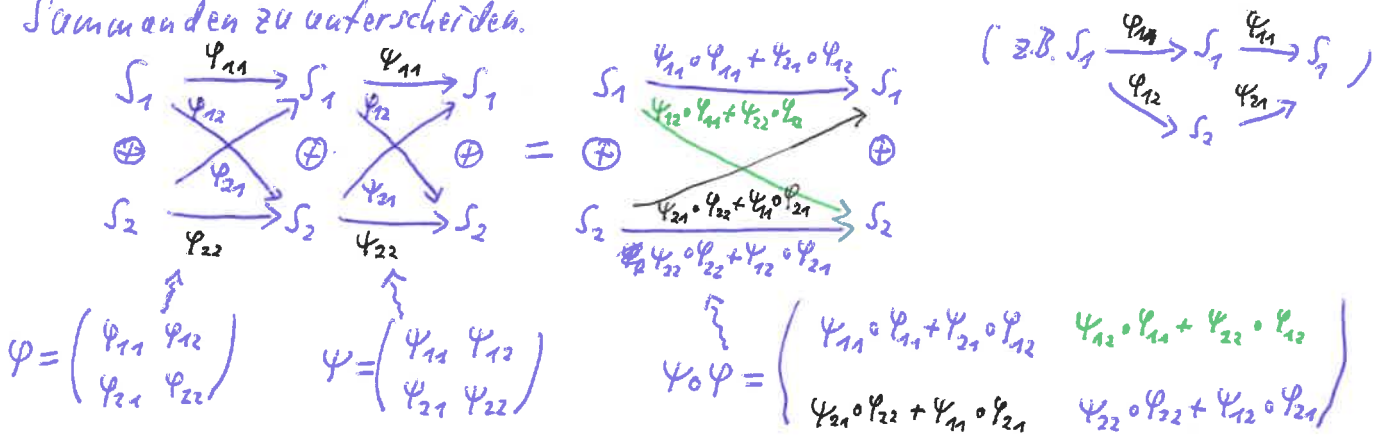
Wie sieht dann der Endomorphismenring vom $M = S \oplus S =: S^2$ mit S

einfach aus? $\text{Hom}_A(S \oplus S, S \oplus S) \Rightarrow$

Au jedem Pfeil steht $\text{Hom}_A(S, S) = D$, ein Schiefkörper.



⇒ Das sind 2x2-Matrizen mit Einträgen in D . Multiplikation = Komposition, da müssen wir auf die Reihenfolge achten: Wir schreiben $S \otimes S$ als $S_1 \oplus S_2$, um die Summanden zu unterscheiden.



$$\begin{pmatrix} \text{Hom}(S_1, S_1) & \text{Hom}(S_1, S_2) \\ \text{Hom}(S_2, S_1) & \text{Hom}(S_2, S_2) \end{pmatrix}$$

Wenn man die Matrizen zu φ und ψ multipliziert, erhält man also die Matrix zu $\psi \circ \varphi$, also gerade umgekehrt angeordnet.

⇒ als Ring (Algebra) ist $\text{End}_A(S \otimes S) \cong \text{Mat}(2 \times 2, \text{End}_A(S))$ ^{op}

Wenn das stört, kann die Multiplikation in $\text{End}_A(S \otimes S)$ undefiniert werden und festlegen: $\psi \circ \varphi$ ist "erst ψ dann φ ". Dann fällt das ^{op} weg (oder ersucht an anderer Stelle wieder auf, siehe unten). Das ist in der Literatur nicht einheitlich geregelt (so wie Links- oder Rechtsmoduln abwechselnd auftaucht).

Für S^n bekommt man natürlich $\text{Mat}(n \times n, \text{End}_A(S))$ ^{op} als Endomorphismenring.

Noch einen Endomorphismenring können wir bestimmen: Die Algebra A können wir als Linksmodul über sich selbst betrachten, ${}_A A$ - das ist der reguläre A -Modul. ${}_A A$ ist frei mit Basis $\{1\}$ ⇒ $\text{Hom}_A({}_A A, A) \cong A$ *als was isomorph?*

(${}_A A$ ist ein Linksmodul, also muß - nach Wahl von $a = \varphi(1)$ - $\varphi(b) = \varphi(b \cdot 1) = b \varphi(1) = ba$ gelten)

$$\begin{aligned} \psi & \longleftarrow \varphi \longleftarrow \varphi(1) \\ \psi: 1 & \mapsto a \longleftarrow a \\ b & \mapsto ba \end{aligned}$$

Wie funktioniert die Komposition?

$$A \xrightarrow{\varphi_a} A \xrightarrow{\varphi_b} A$$

$$\underbrace{1 \mapsto a \quad 1 \mapsto b}$$

$$1 \mapsto \varphi_a(1) = a \mapsto \varphi_b(\varphi_a(1)) = \varphi_b(a) = a \varphi_b(1) = a \cdot b$$

also: $1 \mapsto ab$, das ist φ_{ab}

$\varphi_a: A \rightarrow A$, das ist Rechtsmultiplikation mit a .

$x \mapsto xa$ Rechtsmultiplikation ist ein Linksmodul Homomorphismus,

denn $y(xa) = (yx)a$. (Das funktioniert, weil A ein Bimodul ist: Linksmodul und Rechtsmodul und $x(lyz) = (xy)z$.)

Gezeigt: $\varphi_b \circ \varphi_a = \varphi_{ab}$, also wieder ein op : $\text{End}_A(A) \cong A^{op}$ (wieder vermeidbar, wenn man die Multiplikation von Endomorphismen abändert).

Der Beweis von Schurs Lemma 7.5 impliziert auch:

S, T einfache Moduln $\Rightarrow [\text{Hom}_A(S, T) \neq 0 \Leftrightarrow S = T]$ nachprüfen

7.7 Definition: Ein A -Modul M ist halbeinfach: $\Leftrightarrow M$ ist eine ^{endliche} direkte Summe von einfachen A -Moduln. Die Algebra A ist halbeinfach (als Algebra), wenn sie halbeinfach als A -Linksmodul ist.

Wie sehen die einfachen \mathbb{Z} -Moduln aus? Ist jeder endlich erzeugte \mathbb{Z} -Modul halbeinfach? Ist \mathbb{Z} eine halbeinfache Algebra?

Ist ein Körper eine halbeinfache Algebra?

Wie sehen die einfachen $K[x]$ -Moduln aus? Ist unzerlegbar \Leftrightarrow einfach?

Sei A eine halbeinfache Algebra, also A eine direkte Summe von endlich vielen einfachen Moduln. Die können wir nach Isomorphieklassen sortieren:

$$A \cong_{\text{als Modul}} S_1^{n_1} \oplus S_2^{n_2} \oplus \dots \oplus S_e^{n_e}, \text{ wobei } S_1, \dots, S_e \text{ paarweise nicht isomorph sind}$$

$$\Rightarrow_{\text{nachprüfen}} A \cong_{\text{als Algebra}} (\text{End}(S_1))_{n_1 \times n_1}^{op} \oplus (\text{End}(S_2))_{n_2 \times n_2}^{op} \oplus \dots \oplus (\text{End}(S_e))_{n_e \times n_e}^{op}$$

Spezialfall: $K = \bar{K}$. Dann ist eine halbeinfache K -Algebra eine direkte Summe von endlich vielen Matrizenringen mit Einträgen in K . Man kennt also A , wenn man die Anzahl der Summanden und deren Matrizen-Größe kennt.

Ein halbeinfacher Modul ist nach Definition die Summe von endlich vielen einfachen Teilmodulen. Die Umkehrung gilt auch:

7.8 Lemma: Sei M ein endlich-dimensionaler A -Modul und $M = S_1 + \dots + S_n$, wobei S_1, \dots, S_n einfache Teilmoduln von M sind. Dann ist M halbeinfach. Genauer ist $M = S_{i_1} \oplus \dots \oplus S_{i_k}$ für eine Teilmenge $\{i_1, \dots, i_k\}$ von $\{1, \dots, n\}$.

nicht notwendig direkte Summe

Beweis: Wir wählen die Summandenzahl n minimal und zeigen, daß dann die Summe direkt ist.

Induktion nach n : $n=1$ bedeutet $M = S_1$.

$n > 1$: $S_1 + \dots + S_{n-1}$ ist ein Untermodul von M , also selbst ein Modul, nach Induktion also eine direkte Summe $S_1 \oplus \dots \oplus S_{n-1}$ (weniger Summanden würde der Wahl von n als minimal widersprechen). $z \in (S_1 \oplus \dots \oplus S_{n-1}) \cap S_n = 0$.

Falls nicht: $(S_1 \oplus \dots \oplus S_{n-1}) \cap S_n$ ist jedenfalls ein Teilmodul von S_n einfach, also $= S_n \Rightarrow S_n \subset (S_1 \oplus \dots \oplus S_{n-1}) \nsubseteq$ zu minimal. \square

7.9 Korollar: (a) Ein Quotient eines halbeinfachen Moduls ist selbst halbeinfach (oder 0).

(b) Ein endlich erzeugter Modul über einer halbeinfachen Algebra ist selbst halbeinfach.

(c) Jeder einfache Modul über einer halbeinfachen Algebra ist isomorph zu einem direkten Summanden des regulären Moduls.

Beweis: (a) Sei $X = \bigoplus S_i$ halbeinfach, $\varphi: X \rightarrow Y$ surjektiv. Dann ist

$Y = \varphi(X) = \sum \varphi(S_i)$, also 7.8 anwendbar.

0 oder einfach $\cong S_i$ warum?

(b) M endlich erzeugt $\Rightarrow \exists n$, so daß ${}_A A^n \rightarrow M \rightarrow 0$, d.h. A^n bildet
surjektiv auf M ab

(c) S einfach \Rightarrow endlich erzeugt, $\exists \varphi: {}_A A \rightarrow S \rightarrow 0$ (x beliebig wählbar)

$${}_A A = S_1 \oplus \dots \oplus S_n \quad \begin{array}{c} \psi \\ 1 \mapsto x \neq 0 \end{array}$$

$$\Rightarrow \exists \tilde{\psi}: \varphi|_{S_i}: S_i \xrightarrow{\neq 0} S \Rightarrow S = S_i \oplus 0$$

Was hat das mit Gruppenalgebren zutun?

7.10 Theorem (Satz von Maschke, 1899): Sei G eine endliche Gruppe und K ein Körper. Die Gruppenalgebra KG ist halbeinfach $\Leftrightarrow \text{char}(K) \nmid \text{ord}(G)$.
In diesem Fall ist jeder endlich-dimensionale KG -Modul auch halbeinfach.

Beweis: (1) Sei $\text{char}(K)$ kein Teiler der Gruppenordnung. z.z. KG ist halbeinfach, d.h. der reguläre KG -Modul ist halbeinfach. Wegen 7.9 können wir auch gleich zeigen, daß jeder endlich-dimensionale KG -Modul halbeinfach ist, also auch die letzte Behauptung im Satz gilt.

Wenn M einfach ist, ist es auch halbeinfach. Wenn nicht existiert ein Teilmodul $U \subset M$, mit $U \neq \{0\}$, $U \neq M$. Wir zeigen: Für jedes U existiert ein Teilmodul $V \subset M$ so daß $M = U \oplus V$, d.h. U hat ein Komplement (als Modul). Mit Induktion nach der K -Dimension sind U und V beide halbeinfach, M also auch.

Als K -Vektorraum hat U ein Komplement, sogar viele - und wir suchen ein Komplement, das sogar ein KG -Modul ist. Wir wählen irgendein Vektorraum-Komplement \tilde{V} mit $M = U \oplus \tilde{V}$. Sei $\varphi: M \rightarrow U$ die Projektion mit $\text{Kern}(\varphi) = \tilde{V}$, also die K -lineare Abbildung $\varphi: M \rightarrow M/\tilde{V} = U$. φ wäre ein Modulhomomorphismus, wenn $\tilde{V} = \text{Kern}(\varphi)$ ein Modul wäre - dafür gibt es leider keinen Grund.

Idee: Wir modifizieren φ so, daß es ein Modulhomomorphismus wird, also einen Modul als Kern hat. Dieser Modul V wird sich als Modulkomplement von U herausstellen. Daraus folgt dann die Zerlegung.

Das modifizierte Ψ soll so aussehen:

$$\text{Sei } \Psi: M \rightarrow U \text{ definiert durch } m \mapsto \frac{1}{|G|} \sum_{g \in G} g^{-1} \Psi(gm)$$

Hinweis, daß das sinnvoll ist:

$1 \neq 0$ in K und Voraussetzung

Wäre Ψ selbst ein Modulhomomorphismus, dann wäre

$$\Psi(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \Psi(gm) = \frac{1}{|G|} \sum_{g \in G} g^{-1} g \Psi(m) = \frac{1}{|G|} \sum_{g \in G} \Psi(m) = \Psi(m)$$

Jetzt ist einiges noch zu prüfen:

- Ψ ist eine Abbildung $M \rightarrow U$, d.h. das Bild liegt in U :
 $gm \in M, \Psi(gm) \in U, U$ ist KG -Modul $\Rightarrow g^{-1} \Psi(gm) \in U$ und $\Psi(m) \in U$
- Ψ ist ein KG -Modulhomomorphismus:

- Ψ ist K -linear, weil Ψ K -linear ist

- z.z. $\Psi(hm) = h \Psi(m) \quad \forall h \in G$

$$\Psi(hm) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \Psi(g \cdot hm) = \frac{1}{|G|} \sum_{j \in G} h j^{-1} \Psi(jm) =$$

$$= h \frac{1}{|G|} \sum_{j \in G} j^{-1} \Psi(jm)$$

$$= h \Psi(m)$$

\uparrow sei $j := gh$, also $j^{-1} = h^{-1} g^{-1}$

- Sei $V := \text{Ker}(\Psi)$, das ist also ein KG -Teilmodul von M . Wir zeigen, daß V der gewünschte Komplement ist.

- Sei $u \in U$. Behauptung: $\Psi(u) = u$.

$$\text{Denn: } \Psi(u) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \Psi(gu) = \frac{1}{|G|} \sum_{g \in G} g^{-1} gu = u$$

$u \in U \Rightarrow \Psi(gu) = gu$

* - Daraus folgt: $\text{Im}(\Psi) = U$.

- Also ist $\dim M = \dim V + \dim U$.

• Es gilt $U \cap V = 0$. Denn:

$$\text{Sei } m \in U \cap V \Rightarrow \Psi(m) = 0$$

$\begin{matrix} u \\ m \in U \end{matrix}$

Damit ist (1) bewiesen.

(Wir könnten auch $M = U + V$ direkt noch prüfen: Sei $m \in M$. Dann ist:

$$m = \underbrace{(m - \Psi(m))}_{\in V, \text{ da}} + \underbrace{\Psi(m)}_U$$

$$\Psi(\Psi(m)) = \Psi(m)$$

(2) Die Gegenrichtung: Sei \mathcal{K} ein Teiler der Gruppenordnung.
 \mathcal{K} selbst ist ein $\mathcal{K}G$ -Modul mit $g \cdot 1_{\mathcal{K}} = 1$, d.h. $(\sum_{g \in G} \lambda_g g) \cdot 1 = \sum_{g \in G} \lambda_g \in \mathcal{K}$.
 \uparrow nachprüfen

Behauptung: Sei $V \neq 0$ ein $\mathcal{K}G$ -Teilmodul des regulären Moduls $\mathcal{K}G$.

Dann gilt $V \cap \text{Kern}(\varepsilon) \neq 0$ ~~offenbar~~, wobei $\varepsilon: \mathcal{K}G \rightarrow \mathcal{K}, \sum_{g \in G} \lambda_g g \mapsto \sum_{g \in G} \lambda_g$ Modul-
 homomorph.

Beweis der Behauptung: Sei $x \in V, x \neq 0$. Falls $\varepsilon(x) = 0: \checkmark$

Falls $\varepsilon(x) \neq 0: a = \sum_{g \in G} 1 \cdot g$ liegt in $\text{Kern}(\varepsilon)$, $a \neq 0$, da $\{g: g \in G\}$ Basis.

$$a \cdot x = \left(\sum_{g \in G} 1 \cdot g \right) \left(\sum_{g \in G} \mu_g g \right) = \left(\sum_{g \in G} g \right) \left(\sum_{h \in G} \mu_h h \right) = \left(\sum_{h \in G} \mu_h \left(\sum_{g \in G} gh \right) \right) = \varepsilon(x) \cdot a \neq 0$$

$\sum_{g \in G} \mu_g g \in \mathcal{K}G$
 $\varepsilon(x) \neq 0$
 $= \sum_{j \in G} j = a$

$$a \cdot x \in V \text{ und } \varepsilon(x) \cdot a \in \text{Kern}(\varepsilon)$$

\uparrow $\quad \quad \quad \uparrow$
 V $\quad \quad \quad \text{Kern}(\varepsilon)$

$$\Rightarrow a \cdot x = \varepsilon(x) \cdot a \in V \cap \text{Kern}(\varepsilon) \Rightarrow \text{Behauptung}$$

Aber $\text{Kern}(\varepsilon)$ ist ein echter Teilmodul von $\mathcal{K}G$. Es gibt eine kurze exakte
 Sequenz $0 \rightarrow \text{Kern}(\varepsilon) \rightarrow \mathcal{K}G \rightarrow \mathcal{K} \rightarrow 0 \Rightarrow \dim \text{Kern}(\varepsilon) = \text{ord}(G) - 1 \neq 0$ warum?

Aus der Behauptung folgt: $\text{Kern}(\varepsilon)$ hat kein Modulkomplement V .

$\Rightarrow \mathcal{K}G$ ist nicht halbeinfach. \square

Dies besonders sind also Gruppenalgebren endlicher Gruppen über \mathbb{Q}, \mathbb{R} oder \mathbb{C}
 immer halbeinfach. Die Summanden von $\mathbb{C}G$ (als Algebra) sind Matrizenringe
 $M_n(\mathbb{C})$ mit Einträgen in \mathbb{C} , über \mathbb{Q} und \mathbb{R} sind es Matrizenringe mit vielleicht
 komplizierten Einträgen.

Wie kann man die Gruppenalgebren genauer bestimmen?