Gitter über Schiefgruppenringen und rationale Formen von endlichen Gruppen

Jan Jongen

RWTH-Aachen

29.09.2011

Motivation

Beispiel:

Gegeben sei die Matrixgruppe $\mathrm{Q}_8 := \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} , \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$

Beispiel:

Gegeben sei die Matrixgruppe $Q_8 := \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$

- Der Invariantenring $\mathbb{Q}[i][x_1, x_2]^G$ wird erzeugt durch die Polynome $x_1^2 x_2^2, x_1^4 + x_2^4, x_1 x_2^5 - x_2 x_1^5$.

Motivation

Beispiel:

Gegeben sei die Matrixgruppe $Q_8 := \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$

- Der Invariantenring $\mathbb{Q}[i][x_1, x_2]^G$ wird erzeugt durch die Polynome $x_1^2 x_2^2, x_1^4 + x_2^4, x_1 x_2^5 - x_2 x_1^5$.

Beobachtung:

Motivation

Beispiel:

Gegeben sei die Matrixgruppe $\mathrm{Q}_8 := \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$

- Der Invariantenring $\mathbb{Q}[i][x_1, x_2]^G$ wird erzeugt durch die Polynome $x_1^2 x_2^2, x_1^4 + x_2^4, x_1 x_2^5 - x_2 x_1^5$.

Beobachtung:

- Obwohl Q_8 nicht als Untergruppe von $\mathrm{GL}_2(\mathbb{Q})$ geschrieben werden kann, besitzt der Invariantenring ein Erzeugendensystem mit Polynomen aus $\mathbb{Q}[x_1, x_2]$.

Motivation

Beispiel:

Gegeben sei die Matrixgruppe $Q_8 := \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$

- Der Invariantenring $\mathbb{Q}[i][x_1, x_2]^G$ wird erzeugt durch die Polynome $x_1^2 x_2^2, x_1^4 + x_2^4, x_1 x_2^5 - x_2 x_1^5$.

Beobachtung:

- Obwohl Q_8 nicht als Untergruppe von $\mathrm{GL}_2(\mathbb{Q})$ geschrieben werden kann, besitzt der Invariantenring ein Erzeugendensystem mit Polynomen aus $\mathbb{Q}[x_1, x_2]$.
- Komponentenweises Anwenden der komplexen Konjugation auf Q_8 bewirkt einen Gruppenautomorphismus. Dieser ist realisiert durch Konjugation mit $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Rationale Formen

Satz:

Gegeben sei eine endliche Untergruppe N von $\mathrm{GL}_n(\overline{\mathbb{Q}})$, welche somit auch algebraische Gruppe ist. Dann sind äquivalent:

Rationale Formen

Satz:

Gegeben sei eine endliche Untergruppe N von $\mathrm{GL}_n(\overline{\mathbb{Q}})$, welche somit auch algebraische Gruppe ist. Dann sind äquivalent:

- Es existiert ein System von fundamentalen Invarianten mit Koeffizienten in $\mathbb{Q}$.

Rationale Formen

Satz:

Gegeben sei eine endliche Untergruppe N von $\mathrm{GL}_n(\overline{\mathbb{Q}})$, welche somit auch algebraische Gruppe ist. Dann sind äquivalent:

- Es existiert ein System von fundamentalen Invarianten mit Koeffizienten in $\mathbb{Q}$.
- N ist definiert über $\mathbb{Q}$.

Rationale Formen

Satz:

Gegeben sei eine endliche Untergruppe N von $\mathrm{GL}_n(\overline{\mathbb{Q}})$, welche somit auch algebraische Gruppe ist. Dann sind äquivalent:

- Es existiert ein System von fundamentalen Invarianten mit Koeffizienten in $\mathbb{Q}$.
- N ist definiert über $\mathbb{Q}$.
- $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ operiert durch Anwenden auf N und liefert einen Homomorphismus $^{-} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(N)$

Rationale Formen

Satz:

Gegeben sei eine endliche Untergruppe N von $\mathrm{GL}_n(\overline{\mathbb{Q}})$, welche somit auch algebraische Gruppe ist. Dann sind äquivalent:

- Es existiert ein System von fundamentalen Invarianten mit Koeffizienten in $\mathbb{Q}$.
- N ist definiert über $\mathbb{Q}$.
- $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ operiert durch Anwenden auf N und liefert einen Homomorphismus $^- : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(N)$

Beweis:

- $1 \Rightarrow 2$: Die fundamentalen Invarianten beschreiben N durch algebraische Gleichungen mit rationalen Koeffizienten.

Rationale Formen

Satz:

Gegeben sei eine endliche Untergruppe N von $\mathrm{GL}_n(\overline{\mathbb{Q}})$, welche somit auch algebraische Gruppe ist. Dann sind äquivalent:

- Es existiert ein System von fundamentalen Invarianten mit Koeffizienten in $\mathbb{Q}$.
- N ist definiert über $\mathbb{Q}$.
- $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ operiert durch Anwenden auf N und liefert einen Homomorphismus $^{-} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(N)$

Beweis:

- $1 \Rightarrow 2$: Die fundamentalen Invarianten beschreiben N durch algebraische Gleichungen mit rationalen Koeffizienten.
- $3 \Rightarrow 1$: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ operiert koeffizientenweise auf $\overline{\mathbb{Q}}[x]^N$. Diese Operation ist semilinear und die Aussage folgt aus dem Speiser Lemma.

$\square$

Bemerkung:

Sei $N \leq \mathrm{GL}_n(\overline{\mathbb{Q}})$ endlich und definiert über $\mathbb{Q}$. Dann existiert eine galoische Erweiterung K von $\mathbb{Q}$ mit GALOIS Gruppe Γ, sodass gilt:

Rationale Formen

Bemerkung:

Sei $N \leq \mathrm{GL}_n(\overline{\mathbb{Q}})$ endlich und definiert über $\mathbb{Q}$. Dann existiert eine galoische Erweiterung K von $\mathbb{Q}$ mit GALOIS Gruppe Γ, sodass gilt:

- N ist Untergruppe von $\mathrm{GL}_n(K)$

Rationale Formen

Bemerkung:

Sei $N \leq \mathrm{GL}_n(\overline{\mathbb{Q}})$ endlich und definiert über $\mathbb{Q}$. Dann existiert eine galoische Erweiterung K von $\mathbb{Q}$ mit GALOIS Gruppe Γ, sodass gilt:

- N ist Untergruppe von $\mathrm{GL}_n(K)$
- Die Abbildung $^- : \Gamma \to \mathrm{Aut}(N)$ aus dem letzten Satz ist injektiv.

Rationale Formen

Bemerkung:

Sei $N \leq \mathrm{GL}_n(\overline{\mathbb{Q}})$ endlich und definiert über $\mathbb{Q}$. Dann existiert eine galoische Erweiterung K von $\mathbb{Q}$ mit GALOIS Gruppe Γ, sodass gilt:

- N ist Untergruppe von $\mathrm{GL}_n(K)$
- Die Abbildung $^- : \Gamma \to \mathrm{Aut}(N)$ aus dem letzten Satz ist injektiv.

Beweis:

Existenz von K mit Eigenschaft 1 ist trivial, da N endlich. Ersetze nun ggf. K durch den Fixkörper unter $\mathrm{Kern}(^-)$. □

Rationale Formen

Bemerkung:

Sei $N \leq \mathrm{GL}_n(\overline{\mathbb{Q}})$ endlich und definiert über $\mathbb{Q}$. Dann existiert eine galoische Erweiterung K von $\mathbb{Q}$ mit GALOIS Gruppe Γ, sodass gilt:

- N ist Untergruppe von $\mathrm{GL}_n(K)$
- Die Abbildung $^- : \Gamma \to \mathrm{Aut}(N)$ aus dem letzten Satz ist injektiv.

Beweis:

Existenz von K mit Eigenschaft 1 ist trivial, da N endlich. Ersetze nun ggf. K durch den Fixkörper unter $\mathrm{Kern}(^-)$. $\square$

Von nun an sei N, K, Γ und $^-$ wie in der letzten Bemerkung.

Rationale Formen

Bemerkung:

Sei $N \leq \mathrm{GL}_n(\overline{\mathbb{Q}})$ endlich und definiert über $\mathbb{Q}$. Dann existiert eine galoische Erweiterung K von $\mathbb{Q}$ mit GALOIS Gruppe Γ, sodass gilt:

- N ist Untergruppe von $\mathrm{GL}_n(K)$
- Die Abbildung $^- : \Gamma \to \mathrm{Aut}(N)$ aus dem letzten Satz ist injektiv.

Beweis:

Existenz von K mit Eigenschaft 1 ist trivial, da N endlich. Ersetze nun ggf. K durch den Fixkörper unter $\mathrm{Kern}(^-)$. □

Von nun an sei N, K, Γ und $^-$ wie in der letzten Bemerkung. Insbesondere gilt für die natürliche Darstellung Δ von N:

$$^\sigma\Delta(n) = \Delta(^{\overline{\sigma}}n) \text{ für alle } n \in N \text{ und } \sigma \in \Gamma \tag{1}$$

Bemerkung:

Sei $N \leq \mathrm{GL}_n(\overline{\mathbb{Q}})$ endlich und definiert über $\mathbb{Q}$. Dann existiert eine galoische Erweiterung K von $\mathbb{Q}$ mit GALOIS Gruppe Γ, sodass gilt:

- N ist Untergruppe von $\mathrm{GL}_n(K)$
- Die Abbildung $^{-} : \Gamma \to \mathrm{Aut}(N)$ aus dem letzten Satz ist injektiv.

Beweis:

Existenz von K mit Eigenschaft 1 ist trivial, da N endlich. Ersetze nun ggf. K durch den Fixkörper unter $\mathrm{Kern}(^{-})$. $\square$

Von nun an sei N, K, Γ und $^{-}$ wie in der letzten Bemerkung.
Insbesondere gilt für die natürliche Darstellung Δ von N:

$$^{\sigma}\Delta(n) = \Delta(^{\overline{\sigma}}n) \text{ für alle } n \in N \text{ und } \sigma \in \Gamma \tag{1}$$

Frage: Gibt es eine Modultheoretische Interpretation der letzten Gleichung?

Ein Vorschlag

Ein Vorschlag

Definition:

Sei $G := N \rtimes \Gamma$ und $\pi : G \to \Gamma$ der natürliche Epimorphismus. Der **Schiefgruppenring** $K * G$ ist der freie K-Modul mit Basis G und Multiplikation gegeben durch die $\mathbb{Q}$-lineare Fortsetzung von $gc := {}^{\pi(g)}c g$ für $g \in G$ und $c \in K$. Insbesondere ist $K * G$ eine $\mathbb{Q}$-Algebra.

Ein Vorschlag

Definition:

Sei $G := N \rtimes \Gamma$ und $\pi : G \to \Gamma$ der natürliche Epimorphismus. Der **Schiefgruppenring** $K * G$ ist der freie K-Modul mit Basis G und Multiplikation gegeben durch die $\mathbb{Q}$-lineare Fortsetzung von $gc := {}^{\pi(g)}cg$ für $g \in G$ und $c \in K$. Insbesondere ist $K * G$ eine $\mathbb{Q}$-Algebra.

Bemerkung

- Die natürlichen Einbettungen liefern das kommutative Diagramm:

$$\begin{tikzcd}
\mathbb{Q} \arrow[r] \arrow[d] & \mathbb{Q}\Gamma \arrow[r] \arrow[d] & \mathbb{Q}(N \rtimes \Gamma) \arrow[d] \\
K \arrow[r] & K * \Gamma \arrow[r] & K * G
\end{tikzcd}$$

Ein Vorschlag

Definition:

Sei $G := N \rtimes \Gamma$ und $\pi : G \to \Gamma$ der natürliche Epimorphismus. Der **Schiefgruppenring** $K * G$ ist der freie K-Modul mit Basis G und Multiplikation gegeben durch die $\mathbb{Q}$-lineare Fortsetzung von $gc := {}^{\pi(g)}cg$ für $g \in G$ und $c \in K$. Insbesondere ist $K * G$ eine $\mathbb{Q}$-Algebra.

Bemerkung

- Die natürlichen Einbettungen liefern das kommutative Diagramm:

$$\begin{tikzcd} \mathbb{Q} \arrow[r] \arrow[d] & \mathbb{Q}\Gamma \arrow[r] \arrow[d] & \mathbb{Q}(N \rtimes \Gamma) \arrow[d] \\ K \arrow[r] & K * \Gamma \arrow[r] & K * G \end{tikzcd}$$

- Die natürlichen Operationen von N und Γ auf $K^{n\times 1}$ machen diesen zu einem $K * G$-Modul.

Ein Vorschlag

Lemma (Umkehrung)

Es sei M ein $K * G$-Modul der K-Dimension n. Wähle eine $\mathbb{Q}$-Basis B des Fixraumes M^Γ. Nach dem Speiser-Lemma kann man B als eine K-Basis von M auffassen und dann gilt:

Ein Vorschlag

Lemma (Umkehrung)

Es sei M ein $K * G$-Modul der K-Dimension n. Wähle eine $\mathbb{Q}$-Basis B des Fixraumes M^Γ. Nach dem SPEISER-Lemma kann man B als eine K-Basis von M auffassen und dann gilt:

- Die Darstellung

  $$\Delta_M^{\mathbb{Q}} : N \to \mathrm{GL}_n(K) \ : \ n \mapsto {}^B n^B$$

  erfüllt

  $$^{\sigma}(\Delta_M^{\mathbb{Q}}(n)) = \Delta_M^{\mathbb{Q}}(^{\overline{\sigma}} n)$$

  für alle $\sigma \in \Gamma$ und $n \in N$.

Ein Vorschlag

Lemma (Umkehrung)

Es sei M ein $K * G$-Modul der K-Dimension n. Wähle eine $\mathbb{Q}$-Basis B des Fixraumes M^Γ. Nach dem SPEISER-Lemma kann man B als eine K-Basis von M auffassen und dann gilt:

- Die Darstellung

  $$\Delta_M^{\mathbb{Q}} : N \to \mathrm{GL}_n(K) \ : \ n \mapsto {}^B n^B$$

  erfüllt

  $${}^\sigma(\Delta_M^{\mathbb{Q}}(n)) = \Delta_M^{\mathbb{Q}}({}^{\overline{\sigma}} n)$$

  für alle $\sigma \in \Gamma$ und $n \in N$.
- Sind M_1 und M_2 isomorphe $K * G$-Moduln der K-Dimension n, so existiert ein $Y \in \mathrm{GL}_n(\mathbb{Q})$ mit:

  $$Y^{-1} \Delta_{M_1}^{\mathbb{Q}}(n) Y = \Delta_{M_2}^{\mathbb{Q}}(n) \text{ für alle } n \in N$$

Bemerkung

- $K * G$ ist eine halbeinfache $\mathbb{Q}$-Algebra (MASCHKE)

Bemerkung

- $K * G$ ist eine halbeinfache $\mathbb{Q}$-Algebra (MASCHKE)
- Via Charaktertheorie hat man einen Überblick über die Isomorphieklassen von $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} K * G$-Moduln.

Schiefgruppenringe

Bemerkung

- $K * G$ ist eine halbeinfache $\mathbb{Q}$-Algebra (MASCHKE)
- Via Charaktertheorie hat man einen Überblick über die Isomorphieklassen von $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} K * G$-Moduln.

Es bezeichne $\mathbb{Z}_K$ die Menge der ganzen algebraischen Zahlen in K und es sei $\Lambda := \mathbb{Z}_K * G$, dann gilt:

Bemerkung

- $K * G$ ist eine halbeinfache $\mathbb{Q}$-Algebra (MASCHKE)
- Via Charaktertheorie hat man einen Überblick über die Isomorphieklassen von $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} K * G$-Moduln.

Es bezeichne $\mathbb{Z}_K$ die Menge der ganzen algebraischen Zahlen in K und es sei $\Lambda := \mathbb{Z}_K * G$, dann gilt:

- $\mathbb{Z}_K * G$ ist eine $\mathbb{Z}$-Ordnung in $K * G$

Schiefgruppenringe

Bemerkung

- $K * G$ ist eine halbeinfache $\mathbb{Q}$-Algebra (Maschke)
- Via Charaktertheorie hat man einen Überblick über die Isomorphieklassen von $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} K * G$-Moduln.

Es bezeichne $\mathbb{Z}_K$ die Menge der ganzen algebraischen Zahlen in K und es sei $\Lambda := \mathbb{Z}_K * G$, dann gilt:

- $\mathbb{Z}_K * G$ ist eine $\mathbb{Z}$-Ordnung in $K * G$
- Die natürlichen Einbettungen liefern das kommutative Diagramm:

$$\begin{tikzcd} \mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}\Gamma \arrow[r] \arrow[d] & \mathbb{Z}(N \rtimes \Gamma) \arrow[d] \\ \mathbb{Z}_K \arrow[r] & \mathbb{Z}_K * \Gamma \arrow[r] & \mathbb{Z}_K * G \end{tikzcd}$$

Volle Gitter

Definition:

Für einen endlich erzeugten $K * G$-Modul V heißt ein $\mathbb{Z}_K * G$-Gitter L **volles Gitter** in V, falls:

$$L \leq_{\mathbb{Z}_K * G} V \text{ und } \langle L \rangle_{\mathbb{Q}} = V$$

Die Menge aller vollen Teilgitter von V wird mit $\mathcal{Z}(V)$ bezeichnet.

Volle Gitter

Definition:

Für einen endlich erzeugten $K * G$-Modul V heißt ein $\mathbb{Z}_K * G$-Gitter L **volles Gitter** in V, falls:

$$L \leq_{\mathbb{Z}_K * G} V \text{ und } \langle L \rangle_{\mathbb{Q}} = V$$

Die Menge aller vollen Teilgitter von V wird mit $\mathcal{Z}(V)$ bezeichnet.

Bemerkung

- $\mathrm{Aut}_{K*G}(V)$ operiert auf $\mathcal{Z}(V)$.

Volle Gitter

Definition:

Für einen endlich erzeugten $K * G$-Modul V heißt ein $\mathbb{Z}_K * G$-Gitter L **volles Gitter** in V, falls:

$$L \leq_{\mathbb{Z}_K * G} V \text{ und } \langle L \rangle_{\mathbb{Q}} = V$$

Die Menge aller vollen Teilgitter von V wird mit $\mathcal{Z}(V)$ bezeichnet.

Bemerkung

- $\mathrm{Aut}_{K*G}(V)$ operiert auf $\mathcal{Z}(V)$.
- Genau dann liegen zwei Gitter aus $\mathcal{Z}(V)$ liegen in derselben Bahn, falls sie isomorph als $\mathbb{Z}_K * G$-Moduln sind.

Volle Gitter

Definition:

Für einen endlich erzeugten $K * G$-Modul V heißt ein $\mathbb{Z}_K * G$-Gitter L **volles Gitter** in V, falls:

$$L \leq_{\mathbb{Z}_K * G} V \text{ und } \langle L \rangle_{\mathbb{Q}} = V$$

Die Menge aller vollen Teilgitter von V wird mit $\mathcal{Z}(V)$ bezeichnet.

Bemerkung

- $\operatorname{Aut}_{K*G}(V)$ operiert auf $\mathcal{Z}(V)$.
- Genau dann liegen zwei Gitter aus $\mathcal{Z}(V)$ liegen in derselben Bahn, falls sie isomorph als $\mathbb{Z}_K * G$-Moduln sind.
- Es der gilt der Satz von JORDAN-ZASSENHAUS: $\mathcal{Z}(V)/\operatorname{Aut}_{K*G}(V)$ ist endlich.

Volle Gitter

Definition:

Für einen endlich erzeugten $K * G$-Modul V heißt ein $\mathbb{Z}_K * G$-Gitter L **volles Gitter** in V, falls:

$$L \leq_{\mathbb{Z}_K * G} V \text{ und } \langle L \rangle_{\mathbb{Q}} = V$$

Die Menge aller vollen Teilgitter von V wird mit $\mathcal{Z}(V)$ bezeichnet.

Bemerkung

- $\mathrm{Aut}_{K*G}(V)$ operiert auf $\mathcal{Z}(V)$.
- Genau dann liegen zwei Gitter aus $\mathcal{Z}(V)$ liegen in derselben Bahn, falls sie isomorph als $\mathbb{Z}_K * G$-Moduln sind.
- Es der gilt der Satz von JORDAN-ZASSENHAUS: $\mathcal{Z}(V)/\,\mathrm{Aut}_{K*G}(V)$ ist endlich.

Ziel: Nutze die Algorithmen von PLESKEN, NEBE, KIRSCHMER zur Bestimmung von $\mathcal{Z}(V)/\,\mathrm{Aut}_{K*G}(V)$.

Satz

Es sei $\mathfrak{D}$ die Diskriminante von K und Γ eine $\mathbb{Z}$-Ordnung in $K * G$, welche $\mathbb{Z}_K * G$ enthält. Dann gilt:

$$\mathbb{Z}_K * G \subset \Gamma \subset (|G|\mathfrak{D})^{-1}\mathbb{Z}_K * G$$

Satz

Es sei $\mathfrak{D}$ die Diskriminante von K und Γ eine $\mathbb{Z}$-Ordnung in $K * G$, welche $\mathbb{Z}_K * G$ enthält. Dann gilt:

$$\mathbb{Z}_K * G \subset \Gamma \subset (|G|\mathfrak{D})^{-1}\mathbb{Z}_K * G$$

Beweis

Es sei $A = K * G$, $\{y_i\}$ eine Ganzheitsbasis, $\{y_i^*\}$ die zugehörige Dualbasis und $\mathrm{Tr}_{A/\mathbb{Q}}$ die reguläre Spur. Es gilt:

$$\mathrm{Tr}_{A/\mathbb{Q}}(y_i g) = |G| \,\mathrm{Tr}_K(y_i)\delta_{g,1}$$

Satz

Es sei $\mathfrak{D}$ die Diskriminante von K und Γ eine $\mathbb{Z}$-Ordnung in $K * G$, welche $\mathbb{Z}_K * G$ enthält. Dann gilt:

$$\mathbb{Z}_K * G \subset \Gamma \subset (|G|\mathfrak{D})^{-1}\mathbb{Z}_K * G$$

Beweis

Es sei $A = K * G$, $\{y_i\}$ eine Ganzheitsbasis, $\{y_i^*\}$ die zugehörige Dualbasis und $\mathrm{Tr}_{A/\mathbb{Q}}$ die reguläre Spur. Es gilt:

$$\mathrm{Tr}_{A/\mathbb{Q}}(y_i g) = |G| \, \mathrm{Tr}_K(y_i)\delta_{g,1}$$

Aus $\mathfrak{D} = \det(\mathrm{Tr}_K(y_i y_j))$ folgt $\mathfrak{D} y_i^* \in \mathbb{Z}_K$. Für $\gamma = \sum \alpha_{g,i} y_i g \in \Gamma$ gilt:

Satz

Es sei $\mathfrak{D}$ die Diskriminante von K und Γ eine $\mathbb{Z}$-Ordnung in $K * G$, welche $\mathbb{Z}_K * G$ enthält. Dann gilt:

$$\mathbb{Z}_K * G \subset \Gamma \subset (|G|\mathfrak{D})^{-1}\mathbb{Z}_K * G$$

Beweis

Es sei $A = K * G$, $\{y_i\}$ eine Ganzheitsbasis, $\{y_i^*\}$ die zugehörige Dualbasis und $\mathrm{Tr}_{A/\mathbb{Q}}$ die reguläre Spur. Es gilt:

$$\mathrm{Tr}_{A/\mathbb{Q}}(y_i g) = |G| \, \mathrm{Tr}_K(y_i)\delta_{g,1}$$

Aus $\mathfrak{D} = \det(\mathrm{Tr}_K(y_i y_j))$ folgt $\mathfrak{D} y_i^* \in \mathbb{Z}_K$. Für $\gamma = \sum \alpha_{g,i} y_i g \in \Gamma$ gilt:

$$\mathrm{Tr}(\gamma \underbrace{\mathfrak{D} y^{-1} y_j^*}_{\in \mathbb{Z}_K * G}) = \sum \alpha_{g,i} \mathfrak{D} \, \mathrm{Tr}(y_i g y^{-1} y_j^*) = \alpha_{y,j} \mathfrak{D} |G| \in \mathbb{Z}$$

Satz

Es sei $\mathfrak{D}$ die Diskriminante von K und Γ eine $\mathbb{Z}$-Ordnung in $K * G$, welche $\mathbb{Z}_K * G$ enthält. Dann gilt:

$$\mathbb{Z}_K * G \subset \Gamma \subset (|G|\mathfrak{D})^{-1}\mathbb{Z}_K * G$$

Beweis

Es sei $A = K * G$, $\{y_i\}$ eine Ganzheitsbasis, $\{y_i^*\}$ die zugehörige Dualbasis und $\mathrm{Tr}_{A/\mathbb{Q}}$ die reguläre Spur. Es gilt:

$$\mathrm{Tr}_{A/\mathbb{Q}}(y_i g) = |G| \, \mathrm{Tr}_K(y_i)\delta_{g,1}$$

Aus $\mathfrak{D} = \det(\mathrm{Tr}_K(y_i y_j))$ folgt $\mathfrak{D} y_i^* \in \mathbb{Z}_K$. Für $\gamma = \sum \alpha_{g,i} y_i g \in \Gamma$ gilt:

$$\mathrm{Tr}(\gamma \underbrace{\mathfrak{D} y^{-1} y_j^*}_{\in \mathbb{Z}_K * G}) = \sum \alpha_{g,i}\mathfrak{D}\,\mathrm{Tr}(y_i g y^{-1} y_j^*) = \alpha_{y,j}\mathfrak{D}|G| \in \mathbb{Z}$$

Somit ist $\alpha_{y,j} \in \mathfrak{D}^{-1}|G|^{-1}\mathbb{Z}$ und die Behauptung folgt. □

Anwendung

Korrolar

Es sei $p \in \mathbb{P}$ mit $p \nmid |G|\mathfrak{D}$ und $\mathbb{Z}_{(p)}$ die Lokalisierung von $\mathbb{Z}$ an (p). Dann ist $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} (\mathbb{Z}_K * G)$ eine $\mathbb{Z}_{(p)}$ Maximalordnung in $K * G$.

Anwendung

Korrolar

Es sei $p \in \mathbb{P}$ mit $p \nmid |G|\mathfrak{D}$ und $\mathbb{Z}_{(p)}$ die Lokalisierung von $\mathbb{Z}$ an (p). Dann ist $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} (\mathbb{Z}_K * G)$ eine $\mathbb{Z}_{(p)}$ Maximalordnung in $K * G$.

Korrolar (Absolut irreduzibler Fall)

Es sei V ein absolut irreduzibler $K * G$-Modul und $L \in \mathcal{Z}(V)$. Für eine Primzahl p mit $p \nmid |G|\mathfrak{D}$ ist L/pL ein einfacher $\mathbb{F}_p \otimes_{\mathbb{Z}} (\mathbb{Z}_K * G)$-Modul.

Anwendung

Korrolar

Es sei $p \in \mathbb{P}$ mit $p \nmid |G|\mathfrak{D}$ und $\mathbb{Z}_{(p)}$ die Lokalisierung von $\mathbb{Z}$ an (p). Dann ist $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} (\mathbb{Z}_K * G)$ eine $\mathbb{Z}_{(p)}$ Maximalordnung in $K * G$.

Korrolar (Absolut irreduzibler Fall)

Es sei V ein absolut irreduzibler $K * G$-Modul und $L \in \mathcal{Z}(V)$. Für eine Primzahl p mit $p \nmid |G|\mathfrak{D}$ ist L/pL ein einfacher $\mathbb{F}_p \otimes_{\mathbb{Z}} (\mathbb{Z}_K * G)$-Modul.

Bemerkung

Es sei V absolut irreduzibler $K * G$-Modul und $L \in \mathcal{Z}(V)$. Ein Vertretersystem der $\mathbb{Z}_K * G$-Isomorphieklassen in $\mathcal{Z}(V)$ ist gegeben durch:

$$\mathcal{V}(L) := \{M \leq_{\mathbb{Z}_K * G} L \mid M \nleq pL \text{ für alle p} \in \mathbb{P}\}$$

Anwendung

Korrolar

Es sei $p \in \mathbb{P}$ mit $p \nmid |G|\mathfrak{D}$ und $\mathbb{Z}_{(p)}$ die Lokalisierung von $\mathbb{Z}$ an (p). Dann ist $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} (\mathbb{Z}_K * G)$ eine $\mathbb{Z}_{(p)}$ Maximalordnung in $K * G$.

Korrolar (Absolut irreduzibler Fall)

Es sei V ein absolut irreduzibler $K * G$-Modul und $L \in \mathcal{Z}(V)$. Für eine Primzahl p mit $p \nmid |G|\mathfrak{D}$ ist L/pL ein einfacher $\mathbb{F}_p \otimes_{\mathbb{Z}} (\mathbb{Z}_K * G)$-Modul.

Bemerkung

Es sei V absolut irreduzibler $K * G$-Modul und $L \in \mathcal{Z}(V)$. Ein Vertretersystem der $\mathbb{Z}_K * G$-Isomorphieklassen in $\mathcal{Z}(V)$ ist gegeben durch:

$$\mathcal{V}(L) := \{M \leq_{\mathbb{Z}_K * G} L \mid M \not\leq pL \text{ für alle p} \in \mathbb{P}\}$$

Fazit: Im absolut irreduziblen Fall ist es algorithmisch möglich $\mathcal{Z}(V)$ zu bestimmen.

Beispiel

Es sei:

$$N := \mathrm{SL}_2(25),\ K := \mathbb{Q}(\zeta_7),\ \Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_7))/\mathbb{Q})$$
$$\overline{} : \Gamma \to \mathrm{Aut}(N) : \sigma \mapsto \overline{\sigma}$$

Dabei sei $\overline{\sigma}$ von Ordnung 6 und kein innerer Automorphismus. Dieses $\overline{\sigma}$ ist eindeutig bis auf Konjugation in $\mathrm{Aut}(N)$.

Ergebnisse:

Beispiel

Es sei:

$$N := \mathrm{SL}_2(25),\ K := \mathbb{Q}(\zeta_7),\ \Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_7))/\mathbb{Q})$$
$$\bar{\ } : \Gamma \to \mathrm{Aut}(N) : \sigma \mapsto \overline{\sigma}$$

Dabei sei $\overline{\sigma}$ von Ordnung 6 und kein innerer Automorphismus. Dieses $\overline{\sigma}$ ist eindeutig bis auf Konjugation in $\mathrm{Aut}(N)$.

Ergebnisse:

Ausschnitt aus Charaktertafel von $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} K * (N \rtimes \Gamma)$.

	$1A$	13_6	26_6	$5A$	$5B$	$10A$	$10B$	3	$6B$	12_2	24_4	$2A$	$4A$	8_2
χ_1	6	6	6	6	6	6	6	6	6	6	6	6	6	6
χ_2	72	-6	6	12	-18	-12	18	0	0	0	0	-72	0	0
χ_3	72	-6	6	-18	12	18	-12	0	0	0	0	-72	0	0

Beispiel

Es sei:

$$N := \mathrm{SL}_2(25),\ K := \mathbb{Q}(\zeta_7),\ \Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_7))/\mathbb{Q})$$
$$\bar{\ } : \Gamma \to \mathrm{Aut}(N) : \sigma \mapsto \overline{\sigma}$$

Dabei sei $\overline{\sigma}$ von Ordnung 6 und kein innerer Automorphismus. Dieses $\overline{\sigma}$ ist eindeutig bis auf Konjugation in $\mathrm{Aut}(N)$.

Ergebnisse:

Ausschnitt aus Charaktertafel von $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} K * (N \rtimes \Gamma)$.

	$1A$	13_6	26_6	$5A$	$5B$	$10A$	$10B$	3	$6B$	12_2	24_4	$2A$	$4A$	8_2
χ_1	6	6	6	6	6	6	6	6	6	6	6	6	6	6
χ_2	72	-6	6	12	-18	-12	18	0	0	0	0	-72	0	0
χ_3	72	-6	6	-18	12	18	-12	0	0	0	0	-72	0	0

- Es existiert ein absolut irreduzibler $\mathbb{Q}(\zeta_7) * (N \rtimes \Gamma)$-Modul V mit Charakter χ_2.

Beispiel

Es sei:

$$N := \mathrm{SL}_2(25),\ K := \mathbb{Q}(\zeta_7),\ \Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_7))/\mathbb{Q})$$

$$\bar{\ } : \Gamma \to \mathrm{Aut}(N) : \sigma \mapsto \overline{\sigma}$$

Dabei sei $\overline{\sigma}$ von Ordnung 6 und kein innerer Automorphismus. Dieses $\overline{\sigma}$ ist eindeutig bis auf Konjugation in $\mathrm{Aut}(N)$.

Ergebnisse:

Ausschnitt aus Charaktertafel von $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} K * (N \rtimes \Gamma)$.

	$1A$	13_6	26_6	$5A$	$5B$	$10A$	$10B$	3	$6B$	12_2	24_4	$2A$	$4A$	8_2
χ_1	6	6	6	6	6	6	6	6	6	6	6	6	6	6
χ_2	72	-6	6	12	-18	-12	18	0	0	0	0	-72	0	0
χ_3	72	-6	6	-18	12	18	-12	0	0	0	0	-72	0	0

- Es existiert ein absolut irreduzibler $\mathbb{Q}(\zeta_7) * (N \rtimes \Gamma)$-Modul V mit Charakter χ_2.
- Es gibt <u>keinen</u> $\mathbb{Q}(\zeta_7) * (N \rtimes \Gamma)$-Modul mit Charakter χ_3.

Beispiel

Es sei:

$$N := \mathrm{SL}_2(25),\ K := \mathbb{Q}(\zeta_7),\ \Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_7))/\mathbb{Q})$$
$$^- : \Gamma \to \mathrm{Aut}(N) : \sigma \mapsto \overline{\sigma}$$

Dabei sei $\overline{\sigma}$ von Ordnung 6 und kein innerer Automorphismus. Dieses $\overline{\sigma}$ ist eindeutig bis auf Konjugation in $\mathrm{Aut}(N)$.

Ergebnisse:

Ausschnitt aus Charaktertafel von $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} K * (N \rtimes \Gamma)$.

	$1A$	13_6	26_6	$5A$	$5B$	$10A$	$10B$	3	$6B$	12_2	24_4	$2A$	$4A$	8_2
χ_1	6	6	6	6	6	6	6	6	6	6	6	6	6	6
χ_2	72	-6	6	12	-18	-12	18	0	0	0	0	-72	0	0
χ_3	72	-6	6	-18	12	18	-12	0	0	0	0	-72	0	0

- Es existiert ein absolut irreduzibler $\mathbb{Q}(\zeta_7) * (N \rtimes \Gamma)$-Modul V mit Charakter χ_2.
- Es gibt keinen $\mathbb{Q}(\zeta_7) * (N \rtimes \Gamma)$-Modul mit Charakter χ_3.
- Es gibt 12 volle $\mathbb{Z}_K * G$ Gitter in V d.h. $|\mathcal{Z}(V)| = 12$

Beispiel Fortsetzung

- Jedes Gitter $L \in \mathcal{Z}(V)$ liefert eine ganzzahlige Darstellung der Gruppe $\tilde{G} = (\mathrm{C}_7 \times \mathrm{SL}_2(25)) \rtimes \mathrm{C}_6$.

Beispiel Fortsetzung

- Jedes Gitter $L \in \mathcal{Z}(V)$ liefert eine ganzzahlige Darstellung der Gruppe $\tilde{G} = (\mathrm{C}_7 \times \mathrm{SL}_2(25)) \rtimes \mathrm{C}_6$.
- Je 4 Gitter $L \in \mathcal{Z}(V)$ liefern eine ganzzahlige Darstellung von $\tilde{G}$ mit gerader, unimodularer und postiv definiter $\tilde{G}$-invarianter Bilinearform Φ (vermutlich mit Minimum 8).

Beispiel Fortsetzung

- Jedes Gitter $L \in \mathcal{Z}(V)$ liefert eine ganzzahlige Darstellung der Gruppe $\tilde{G} = (\mathrm{C}_7 \times \mathrm{SL}_2(25)) \rtimes \mathrm{C}_6$.
- Je 4 Gitter $L \in \mathcal{Z}(V)$ liefern eine ganzzahlige Darstellung von $\tilde{G}$ mit gerader, unimodularer und postiv definiter $\tilde{G}$-invarianter Bilinearform Φ (vermutlich mit Minimum 8).

Für die Fixgitter $(L^U, \Phi_{|L^U})$ mit $U \leq \Gamma$ gilt:

U	Dim	Det	Name	KN	$\lvert\mathrm{Aut}\rvert$	Min	$[L : (L^U \otimes \mathbb{Z}_K)]$
Γ	12	1	D_{12}^+	264	x	2	7^{30}
$\langle\sigma^2\rangle$	24	1	LEECH	x	x	4	7^{12}
$\langle\sigma^3\rangle$	36	1	$?$	42840	1440	4	7^6

Wahl einer (reduzierten) $\mathbb{Z}$-Basis von L^Γ liefert eine Darstellung

$$\Delta : \mathrm{SL}_2(25) \to \mathrm{GL}_{12}(\mathbb{Q}(\zeta_7))$$

sodass $\Delta(\mathrm{SL}_2(25))$ eine über $\mathbb{Q}$ definierte Matrixgruppe ist.