Extremale Gitter mit großen Automorphismen

Simon Berger

21. September 2018

Ideal-Gitter

Definition

Ein *Ideal-Gitter* ist ein Gitter $(\mathcal{I}, b)$, sodass $\mathcal{I}$ ein gebrochenes $\mathbb{Z}_K$-Ideal ist und $b : \mathcal{I} \times \mathcal{I} \to \mathbb{R}$ eine symmetrische positiv-definite Bilinearform mit $b(\lambda x, y) = b(x, \overline{\lambda} y)$ für $x, y \in \mathcal{I}$ und $\lambda \in \mathbb{Z}_K$. Die Abbildung $\lambda \mapsto \overline{\lambda}$ bezeichnet dabei die herkömmliche komplexe Konjugation.

Ideal-Gitter

Definition

Ein *Ideal-Gitter* ist ein Gitter $(\mathcal{I}, b)$, sodass $\mathcal{I}$ ein gebrochenes $\mathbb{Z}_K$-Ideal ist und $b : \mathcal{I} \times \mathcal{I} \to \mathbb{R}$ eine symmetrische positiv-definite Bilinearform mit $b(\lambda x, y) = b(x, \overline{\lambda} y)$ für $x, y \in \mathcal{I}$ und $\lambda \in \mathbb{Z}_K$. Die Abbildung $\lambda \mapsto \overline{\lambda}$ bezeichnet dabei die herkömmliche komplexe Konjugation.

Solche Gitter können wir für gegebenen Körper K und Determinante effizient konstruieren!

n \ ℓ	1	2	3	5	6	7	11	14	15	23
4	–	1(1)	1(1)	–	–	–	1(1)	1(1)	–	1(1)
6	–	–	1(1)	–	–	1(1)	–	–	–	–
8	1(1)	1(1)	1(1)	1(1)	1(1)	1(1)	2(1)	2(1)	1(1)	3(−)
10	–	–	–	–	–	–	1(1)	–	–	–
12	–	1(1)	2(1)	1(1)	1(1)	1(−)	1(−)	1(1)	–	1(−)
16	1(1)	2(1)	3(2)	1(−)	2(1)	4(3)	5(−)	5(−)	3(1)	5(−)
18	–	–	1(−)	–	–	–	–	–	–	–
20	–	1(1)	–	–	1(1)	1(−)	2(−)	–	–	–
22	–	–	–	–	–	–	–	–	–	2(−)
24	4(1)	2(1)	7(1)	5(1)	5(2)	8(−)	7(−)	8(−)	5(−)	14(−)
32	7(5)	13(4)	13(7)	10(−)	12(−)	19(−)	42(−)	21(−)	23(−)	–
36	–	6(3)	8(−)	8(−)	–	–	2(−)	36(−)	4(−)	–

Table: Ideal-Gitter der Dimension n, Stufe ℓ und Determinante $\ell^{\frac{n}{2}}$.

Große Automorphismen

Definition

Sei L ein $\mathbb{Z}$-Gitter der Dimension n. Ein *großer Automorphismus* von L ist ein $\sigma \in \mathrm{Aut}(L)$ von Ordnung $m \in \mathbb{N}$, sodass $\Phi_m | \mu_\sigma$ und $\frac{n}{2} < \varphi(m) \leq n$.

Große Automorphismen

Definition

Sei L ein $\mathbb{Z}$-Gitter der Dimension n. Ein *großer Automorphismus* von L ist ein $\sigma \in \mathrm{Aut}(L)$ von Ordnung $m \in \mathbb{N}$, sodass $\Phi_m | \mu_\sigma$ und $\frac{n}{2} < \varphi(m) \leq n$.

$\rightarrow$ Ziel: Gitter mit großen Automorphismen klassifizieren.

Große Automorphismen

Sei L Gitter mit großem Automorphismus σ der Ordnung m in Vektorraum V.

Große Automorphismen

Sei L Gitter mit großem Automorphismus σ der Ordnung m in Vektorraum V.

$$\Rightarrow V = \text{Kern}(\frac{\mu_\sigma}{\Phi_m}(\sigma)) \perp \text{Kern}(\Phi_m(\sigma))$$

$$M := L_1 \perp L_p := L \cap \text{Kern}(\frac{\mu_\sigma}{\Phi_m}(\sigma)) \perp L \cap \text{Kern}(\Phi_m(\sigma))$$

Große Automorphismen

$$M := L_1 \perp L_p := L \cap \mathrm{Kern}(\frac{\mu_\sigma}{\Phi_m}(\sigma)) \perp L \cap \mathrm{Kern}(\Phi_m(\sigma))$$

- Falls ein $p \in \mathbb{P}$ existiert, sodass $\frac{\mu_\sigma}{\Phi_m} \mid (X^{\frac{m}{p}} - 1)$, dann ist
  $L_1 = L \cap \mathrm{Kern}(\sigma^{\frac{m}{p}} - 1)$ das Fixgitter und
  $L_p = L \cap \mathrm{Bild}(\sigma^{\frac{m}{p}} - 1)$ das Bildgitter eines Automorphismus von Primzahlordnung.

Strategie zur Klassifikation

- Primteiler p von m mit $\mathrm{ggT}(p, \ell) = 1$ durchgehen.

Strategie zur Klassifikation

- Primteiler p von m mit $\mathrm{ggT}(p, \ell) = 1$ durchgehen.
- Mögliche Automorphismentypen der Ordnung p durchgehen.

Strategie zur Klassifikation

- Primteiler p von m mit $\mathrm{ggT}(p, \ell) = 1$ durchgehen.
- Mögliche Automorphismentypen der Ordnung p durchgehen.
- Mögliche Bildgitter aufzählen.

Strategie zur Klassifikation

- Primteiler p von m mit $\mathrm{ggT}(p, \ell) = 1$ durchgehen.
- Mögliche Automorphismentypen der Ordnung p durchgehen.
- Mögliche Bildgitter aufzählen.
- Mögliche Fixgitter aufzählen.

Strategie zur Klassifikation

- Primteiler p von m mit $\mathrm{ggT}(p, \ell) = 1$ durchgehen.
- Mögliche Automorphismentypen der Ordnung p durchgehen.
- Mögliche Bildgitter aufzählen.
- Mögliche Fixgitter aufzählen.
- Kandidaten für σ aufzählen.

Strategie zur Klassifikation

- Primteiler p von m mit $\mathrm{ggT}(p, \ell) = 1$ durchgehen.
- Mögliche Automorphismentypen der Ordnung p durchgehen.
- Mögliche Bildgitter aufzählen.
- Mögliche Fixgitter aufzählen.
- Kandidaten für σ aufzählen.
- L als σ-invariantes Obergitter von $L_1 \perp L_p$ konstruieren.

Automorphismen von Primzahlordnung

Satz

Sei L gerade, n-dim. von q.-freier Stufe ℓ, $Det(L) = \ell^k$. Sei zudem $\sigma \in Aut(L)$ von Typ $p - (n_1, n_p) - s - q_1 - (k_{1,1}, k_{p,1}) - \ldots$, wobei $ggT(p, \ell) = 1$. Dann gilt:

- $n_1 + n_p = n$.
- $s \in \{0, \ldots, \min(n_1, \frac{n_p}{p-1})\}$.
- $s \equiv_2 \frac{n_p}{p-1}$ *und für* $p = 2$ *zusätzlich* $s \equiv_2 0$.
- $k_{1,i} \in \{0, \ldots, \min(n_1, k)\}$.
- $k_{1,i} \equiv_2 k$.
- $k_{p,i} \in \{0, \ldots, \min(n_p, k)\}$.
- $k_{p,i} \equiv_2 0$.
- $(2f(q_i)) \,|\, k_{p,i}$, *wobei* $f(q_i)$ *den Trägheitsgrad von* $q_i \mathbb{Z}_{\mathbb{Q}(\zeta_p + \zeta_p^{-1})}$ *bezeichne.*
- $k_{1,i} + k_{p,i} = k$.

Bildgitter

Da $\varphi(m) > \frac{n}{2}$ ist $L_p = L \cap \text{Kern}(\Phi_m)$ ein eindimensionaler $\mathbb{Q}(\zeta_m)$-Vektorraum $\rightsquigarrow$ Ideal-Gitter.

Bildgitter

Da $\varphi(m) > \frac{n}{2}$ ist $L_p = L \cap \text{Kern}(\Phi_m)$ ein eindimensionaler $\mathbb{Q}(\zeta_m)$-Vektorraum $\rightsquigarrow$ Ideal-Gitter.
$\Rightarrow$ Effizient berechenbar mit dem Algorithmus aus dem ersten Teil!

Fixgitter

- Für das Fixgitter kennen wir Dimension, Determinante und Stufe.

Fixgitter

- Für das Fixgitter kennen wir Dimension, Determinante und Stufe.
- $\Rightarrow$ Finden wir nur mittels Geschlechteraufzählung.

Fixgitter

- Für das Fixgitter kennen wir Dimension, Determinante und Stufe.
- $\Rightarrow$ Finden wir nur mittels Geschlechteraufzählung.
- Falls $p > 2$ und ℓ prim, kennen wir genau das Geschlechtssymbol von L_1.

Fixgitter

- Für das Fixgitter kennen wir Dimension, Determinante und Stufe.
- $\Rightarrow$ Finden wir nur mittels Geschlechteraufzählung.
- Falls $p > 2$ und ℓ prim, kennen wir genau das Geschlechtssymbol von L_1.
- Ansonsten zumindest die Elementarteiler.

Fixgitter

- Für das Fixgitter kennen wir Dimension, Determinante und Stufe.
- $\Rightarrow$ Finden wir nur mittels Geschlechteraufzählung.
- Falls $p > 2$ und ℓ prim, kennen wir genau das Geschlechtssymbol von L_1.
- Ansonsten zumindest die Elementarteiler.
- Nach Konstruktion von Vertretern mit passenden Elementarteilern (David Lorch) Aufzählung des gesamten Geschlechts mit der Kneser'schen Nachbarmethode.

Fixgitter

Satz

Sei L ein Gitter von Dimension ≥ 3. Hat für jede Primzahl $q \in \mathbb{P}$ die Jordanzerlegung von $\mathbb{Z}_q \otimes L$ mindestens eine Komponente von Dimension ≥ 2, so besteht der Nachbarschafts-Graph von L aus genau einer Zusammenhangskomponente.

Fixgitter

Satz

Sei L ein Gitter von Dimension ≥ 3. Hat für jede Primzahl $q \in \mathbb{P}$ die Jordanzerlegung von $\mathbb{Z}_q \otimes L$ mindestens eine Komponente von Dimension ≥ 2, so besteht der Nachbarschafts-Graph von L aus genau einer Zusammenhangskomponente.

- Schwache Bedingung ist beinahe immer erfüllt.
- Wir erhalten durch sukzessive Nachbarbildung das gesamte Geschlecht.
- Benutzen als Abbruchbedingung das Maß des Geschlechtes.

Kandidaten für σ

- σ operiert auf den Faktorgruppen $L_1^{\#,p}/L_1$ und $L_p^{\#,p}/L_p$.

Kandidaten für σ

- σ operiert auf den Faktorgruppen $L_1^{\#,p}/L_1$ und $L_p^{\#,p}/L_p$.
- Die Faktorgruppen sind isomorph als $\mathbb{F}_p[\sigma]$-Moduln.

Kandidaten für σ

- σ operiert auf den Faktorgruppen $L_1^{\#,p}/L_1$ und $L_p^{\#,p}/L_p$.
- Die Faktorgruppen sind isomorph als $\mathbb{F}_p[\sigma]$-Moduln.
- $\Rightarrow$ Minimalpolynome der Operationen von σ auf den beiden Faktorgruppen sind identisch.

Kandidaten für σ

- σ operiert auf den Faktorgruppen $L_1^{\#,p}/L_1$ und $L_p^{\#,p}/L_p$.
- Die Faktorgruppen sind isomorph als $\mathbb{F}_p[\sigma]$-Moduln.
- $\Rightarrow$ Minimalpolynome der Operationen von σ auf den beiden Faktorgruppen sind identisch.
- Das Minimalpolynom auf den Faktorgruppen ist $\Phi_{\frac{m}{p}}$, falls $[L : M] > 1$.

Kandidaten für σ

- σ operiert auf den Faktorgruppen $L_1^{\#,p}/L_1$ und $L_p^{\#,p}/L_p$.
- Die Faktorgruppen sind isomorph als $\mathbb{F}_p[\sigma]$-Moduln.
- $\Rightarrow$ Minimalpolynome der Operationen von σ auf den beiden Faktorgruppen sind identisch.
- Das Minimalpolynom auf den Faktorgruppen ist $\Phi_{\frac{m}{p}}$, falls $[L : M] > 1$.
- Wähle Vertreter σ_1 und σ_p der Konjugiertenklassen der Automorphismen von L_1 und L_p, die mit dem richtigen Minimalpolynom auf $L_1^{\#,p}/L_1$ und $L_p^{\#,p}/L_p$ operieren. Setze $\sigma := \mathrm{diag}(\sigma_1, \sigma_p)$.

Konstruktion von Obergittern

- Die ganzen Obergitter von M mit Index p^s haben die Form

$$L_\varphi := \{(x_1, x_p) \in L_1^{\#,p} \perp L_p^{\#,p} \mid \varphi(x_1 + L_1) = x_p + L_p\}$$

für die Isometrien $\varphi : (L_1^{\#,p}/L_1, \overline{b_1}) \to (L_p^{\#,p}/L_p, -\overline{b_p})$

Konstruktion von Obergittern

- Die ganzen Obergitter von M mit Index p^s haben die Form

$$L_\varphi := \{(x_1, x_p) \in L_1^{\#,p} \perp L_p^{\#,p} \mid \varphi(x_1 + L_1) = x_p + L_p\}$$

  für die Isometrien $\varphi : (L_1^{\#,p}/L_1, \overline{b_1}) \to (L_p^{\#,p}/L_p, -\overline{b_p})$
- Damit L_φ invariant unter $\sigma = \mathrm{diag}(\sigma_1, \sigma_p)$ ist, muss $\varphi \circ \sigma_1 = \sigma_p \circ \varphi$ gelten.

Konstruktion von Obergittern

- Die ganzen Obergitter von M mit Index p^s haben die Form

$$L_\varphi := \{(x_1, x_p) \in L_1^{\#,p} \perp L_p^{\#,p} \mid \varphi(x_1 + L_1) = x_p + L_p\}$$

  für die Isometrien $\varphi : (L_1^{\#,p}/L_1, \overline{b_1}) \to (L_p^{\#,p}/L_p, -\overline{b_p})$
- Damit L_φ invariant unter $\sigma = \mathrm{diag}(\sigma_1, \sigma_p)$ ist, muss $\varphi \circ \sigma_1 = \sigma_p \circ \varphi$ gelten.
- Für $c \in C_{\mathrm{Aut}(L_1)}(\sigma_1)$ ist $L_\varphi \cong L_{\varphi c}$.

Konstruktion von Obergittern

- Die ganzen Obergitter von M mit Index p^s haben die Form

$$L_\varphi := \{(x_1, x_p) \in L_1^{\#,p} \perp L_p^{\#,p} \mid \varphi(x_1 + L_1) = x_p + L_p\}$$

  für die Isometrien $\varphi : (L_1^{\#,p}/L_1, \overline{b_1}) \to (L_p^{\#,p}/L_p, -\overline{b_p})$
- Damit L_φ invariant unter $\sigma = \mathrm{diag}(\sigma_1, \sigma_p)$ ist, muss $\varphi \circ \sigma_1 = \sigma_p \circ \varphi$ gelten.
- Für $c \in C_{\mathrm{Aut}(L_1)}(\sigma_1)$ ist $L_\varphi \cong L_{\varphi c}$.
- Damit können wir die Obergitter aufzählen, indem wir die relevanten Isometrien modulo $C_{\mathrm{Aut}(L_1)}(\sigma_1)$ durchgehen.

Konstruktion von Obergittern

- Die ganzen Obergitter von M mit Index p^s haben die Form

$$L_\varphi := \{(x_1, x_p) \in L_1^{\#,p} \perp L_p^{\#,p} \mid \varphi(x_1 + L_1) = x_p + L_p\}$$

  für die Isometrien $\varphi : (L_1^{\#,p}/L_1, \overline{b_1}) \to (L_p^{\#,p}/L_p, -\overline{b_p})$
- Damit L_φ invariant unter $\sigma = \mathrm{diag}(\sigma_1, \sigma_p)$ ist, muss $\varphi \circ \sigma_1 = \sigma_p \circ \varphi$ gelten.
- Für $c \in C_{\mathrm{Aut}(L_1)}(\sigma_1)$ ist $L_\varphi \cong L_{\varphi c}$.
- Damit können wir die Obergitter aufzählen, indem wir die relevanten Isometrien modulo $C_{\mathrm{Aut}(L_1)}(\sigma_1)$ durchgehen.
- Bemerkung: In vielen Fällen können wir einfach alle ganzen Obergitter von M mit Index p^s aufzählen, ohne auf σ-Invarianz zu achten; so erhalten wir ggf. noch mehr Gitter!

Finaler Algorithmus

Alle Teilschritte können nun zu einem Algorithmus zusammengesetzt werden.

n \ ℓ	1	2	3	5	6	7	11	14	15	23
2	–	–	1	–	–	–	–	–	–	–
4	–	1	1	–	–	–	1	1	–	1
6	–	–	1	–	–	1	1	–	–	–
8	1	1	1	1	1	1	1	1	1	–
10	–	–	1	–	–	–	1	–	–	–
12	–	2	1	1	1	–	–	1	1	–
14	–	–	1	–	–	–	–	–	–	–
16	2	1	2	–	1	3	–	–	1	–
18	–	–	1	–	–	–	–	–	–	–
20	–	1	3	–	1	–	–	–	–	–
22	–	–	$2(1^*)$	–	–	–	–	–	–	–
24	1	$8(2^*)$	1	1	$5(3^*)$	–	–	–	–	–
26	–	–	2	–	–	–	–	–	–	–
28	–	$35(25^*)$	$3(2^*)$	–	–	–	–	–	–	–
30	–	–	–	–	–	–	–	–	–	–
32	–	2	$67(65^*)$	–	–	–	–	–	–	–
34	–	–	–	–	–	–	–	–	–	–
36	–	–	–	–	–	–	–	–	–	–

Table: Anzahl der durch den Algorithmus konstruierten extremalen stark ℓ-modularen Gitter in Dimension $n \leq 36$ sowie ggf. der Anzahl der bisher unbekannten Gitter darunter

Vollständigkeit

- Erinnerung: Es muss ein $p \in \mathbb{P}$ mit $\mathrm{ggT}(p, \ell) = 1$ existieren, sodass $\frac{\mu_\sigma}{\Phi_m} \mid (X^{\frac{m}{p}} - 1)$

Vollständigkeit

- Erinnerung: Es muss ein $p \in \mathbb{P}$ mit $\mathrm{ggT}(p, \ell) = 1$ existieren, sodass $\frac{\mu_\sigma}{\Phi_m} \mid (X^{\frac{m}{p}} - 1)$
- $\rightsquigarrow$ Wie stark ist diese Voraussetzung?

Vollständigkeit

- Erinnerung: Es muss ein $p \in \mathbb{P}$ mit $\mathrm{ggT}(p, \ell) = 1$ existieren, sodass $\frac{\mu_\sigma}{\Phi_m} \mid (X^{\frac{m}{p}} - 1)$
- $\rightsquigarrow$ Wie stark ist diese Voraussetzung?
- Dazu: Gitter charakterisieren, die **nicht** auf diese Weise konstruiert werden können.

Vollständigkeit - Beispiel

Sei $\ell = 3$, $n = 24$.

Vollständigkeit - Beispiel

Sei $\ell = 3$, $n = 24$.
Die möglichen Automorphismentypen von Ordnung $\in \mathbb{P}_{\neq 3}$ sind:

$2 - (12, 12) - 12 - (6, 6)$	(1 Fixgitter)
$2 - (0, 24) - 0 - (0, 12)$	(1 Fixgitter)
$5 - (8, 16) - 4 - (8, 4)$	(5 Fixgitter)
$5 - (8, 16) - 4 - (4, 8)$	(4 Fixgitter)
$5 - (0, 24) - 0 - (0, 12)$	(1 Fixgitter)
$7 - (0, 24) - 0 - (0, 12)$	(1 Fixgitter)
$11 - (4, 20) - 2 - (2, 10)$	(1 Fixgitter)
$13 - (0, 24) - 0 - (0, 12)$	(1 Fixgitter)

Vollständigkeit - Beispiel

Sei $\ell = 3$, $n = 24$.
Die möglichen Automorphismentypen von Ordnung $\in \mathbb{P}_{\neq 3}$ sind:

$2 - (12, 12) - 12 - (6, 6)$	(1 Fixgitter)
$2 - (0, 24) - 0 - (0, 12)$	(1 Fixgitter)
$5 - (8, 16) - 4 - (8, 4)$	(5 Fixgitter)
$5 - (8, 16) - 4 - (4, 8)$	(4 Fixgitter)
$5 - (0, 24) - 0 - (0, 12)$	(1 Fixgitter)
$7 - (0, 24) - 0 - (0, 12)$	(1 Fixgitter)
$11 - (4, 20) - 2 - (2, 10)$	(1 Fixgitter)
$13 - (0, 24) - 0 - (0, 12)$	(1 Fixgitter)

Für $12 < \varphi(m) \leq 24$ und da m keine Primteiler > 13 hat:
$m \in \{25, 27, 32, 33, 40, 44, 45, 48, 50, 54, 60, 66, 72, 84, 90\}$.

Vollständigkeit - Beispiel

$m = 25$: $\Phi_{25} \mid \mu_\sigma$, $\frac{\mu_\sigma}{\Phi_{25}} | (X^5 - 1) \Rightarrow$ wird von Alg. gefunden.

Vollständigkeit - Beispiel

$m = 25$: $\Phi_{25} \mid \mu_\sigma$, $\frac{\mu_\sigma}{\Phi_{25}} | (X^5 - 1) \Rightarrow$ wird von Alg. gefunden.

$m = 48$: Ang. σ^{24} hat Typ $2 - (12, 12) - 12 - (6, 6)$, dann $\Phi_{48} \nmid \mu_\sigma$.
Somit $\Phi_{16} \mid \mu_\sigma$ und $\mu_\sigma \mid (X^{24} - 1)\Phi_{16}$.
$\Rightarrow$ Bild$(\sigma^{24} - 1)$ ist $\mathbb{Q}(\zeta_{16})$-VR, aber
Dim(Bild$(\sigma^{24} - 1)) = 12 \lightning$
$\Rightarrow \mu_\sigma \in \{\Phi_{16}\Phi_{48}, \Phi_{48}\}$. Für $\mu_\sigma = \Phi_{48}$ ist L aber ein Ideal-Gitter über $\mathbb{Q}(\zeta_{48})$ und wird gefunden.

Vollständigkeit - Methoden

Sei L ein Gitter mit einem Automorphismus σ der Ordnung m, sodass $\frac{n}{2} < \varphi(m) \leq n$, aber L kann nicht durch den Algorithmus gefunden werden.

Vollständigkeit - Methoden

Sei L ein Gitter mit einem Automorphismus σ der Ordnung m, sodass $\frac{n}{2} < \varphi(m) \leq n$, aber L kann nicht durch den Algorithmus gefunden werden.
Betrachte die charakteristischen Polynome

$$\chi_\sigma := \Phi_{d_1}^{c_1} \dots \Phi_{d_k}^{c_k}$$

für die Teiler $d_1 < d_2 < \dots < d_k$ von m.

Vollständigkeit - Methoden

Sei L ein Gitter mit einem Automorphismus σ der Ordnung m, sodass $\frac{n}{2} < \varphi(m) \leq n$, aber L kann nicht durch den Algorithmus gefunden werden.
Betrachte die charakteristischen Polynome

$$\chi_\sigma := \Phi_{d_1}^{c_1} \dots \Phi_{d_k}^{c_k}$$

für die Teiler $d_1 < d_2 < \dots < d_k$ von m.

- Für Ordnung m: $\text{kgV}\{d_i | c_i > 0\} \stackrel{!}{=} m$.

Vollständigkeit - Methoden

Sei L ein Gitter mit einem Automorphismus σ der Ordnung m, sodass $\frac{n}{2} < \varphi(m) \leq n$, aber L kann nicht durch den Algorithmus gefunden werden.
Betrachte die charakteristischen Polynome

$$\chi_\sigma := \Phi_{d_1}^{c_1} \dots \Phi_{d_k}^{c_k}$$

für die Teiler $d_1 < d_2 < \dots < d_k$ von m.

- Für Ordnung m: $\text{kgV}\{d_i | c_i > 0\} \stackrel{!}{=} m$.
- Wenn

$$c_k = 1 \text{ und } \text{kgV}\{d_i \mid i \in \{1, \dots, k-1\} \text{ und } c_i > 0\} \mid \frac{m}{p}$$

für ein $p \in \mathbb{P}$, $\text{ggT}(p, \ell) = 1$ erfüllt ist, wird L gefunden.

Vollständigkeit - Methoden

Kennt man für eine Menge von Primteilern $p_1, \ldots, p_t \mid m$ die Typen

$$p_1 - (n_{1,1}, \ldots$$
$$\vdots$$
$$p_t - (n_{t,1}, \ldots$$

der Automorphismen $\sigma^{\frac{m}{p_1}}, \sigma^{\frac{m}{p_2}}, \ldots, \sigma^{\frac{m}{p_t}}$, so muss $c := (c_1, \ldots, c_k)$ eine Lösung von $cM = (n_{1,1}, n_{2,1}, \ldots, n_{t,1}, n)$ mit der Matrix

$$M \in \mathbb{N}_0^{k \times (t+1)}, \quad M_{i,j} := \begin{cases} \varphi(d_i) & , d_i \mid \frac{m}{p_j} \text{ oder } j = t+1 \\ 0 & , \text{sonst} \end{cases}$$

sein.

Vollständigkeit - Methoden

Für $p \mid m$ ist

$$|\sigma_1| = \text{kgV}\{d_i \mid \nu_p(d_i) < \nu_p(m) \text{ und } c_i > 0\}.$$

$$|\sigma_p| = \text{kgV}\{d_i \mid \nu_p(d_i) = \nu_p(m) \text{ und } c_i > 0\}.$$

Vollständigkeit - Methoden

Für $p \mid m$ ist

$$|\sigma_1| = \text{kgV}\{d_i \mid \nu_p(d_i) < \nu_p(m) \text{ und } c_i > 0\}.$$

$$|\sigma_p| = \text{kgV}\{d_i \mid \nu_p(d_i) = \nu_p(m) \text{ und } c_i > 0\}.$$

$\rightsquigarrow$ Wenn für $\sigma^{\frac{m}{p}}$ alle möglichen Fix- oder Bildgitter aufgezählt werden können, muss mindestens eines davon einen Automorphismus der passenden Ordnung haben.

Vollständigkeit - Methoden

Seien $p_1, p_2 \mid m$.
Wenn für alle Faktoren $\Phi_{d_i} \mid \chi_\sigma$, immer *entweder* $\nu_{p_1}(d_i) = \nu_{p_1}(m)$ *oder* $\nu_{p_2}(d_i) = \nu_{p_2}(m)$ gilt, induzieren p_1 und p_2 dasselbe Teilgitter.

Vollständigkeit - Methoden

Seien $p_1, p_2 \mid m$.
Wenn für alle Faktoren $\Phi_{d_i} \mid \chi_\sigma$, immer *entweder* $\nu_{p_1}(d_i) = \nu_{p_1}(m)$ *oder* $\nu_{p_2}(d_i) = \nu_{p_2}(m)$ gilt, induzieren p_1 und p_2 dasselbe Teilgitter.
$\rightsquigarrow$ Index 0!

Vollständigkeit - Methoden

Methoden zur Analyse der charakteristischen Polynome in `MAGMA` implementiert und verschiedene ℓ und n ausgewertet.

Ende

Vielen Dank für eure Aufmerksamkeit!