Indexformgleichungen

Michael E. Pohst

Institut für Mathematik
Technische Universität Berlin

4. Februar, 2015

Indizes

Gegeben ist eine kubische Erweiterung $E = F(\alpha)$, für deren Diskriminante d_E die Gleichung $\Delta = d_E I^2$ gilt. In den ganzen Zahlen o_E von E sind dann alle Elemente vom Index I zu berechnen. Wählt man α geeignet, besitzt o_E eine R-basis (**Ganzheitsbasis**) von der Gestalt

$$\omega_1, \omega_2 = \alpha, \omega_3 = (\alpha^2 + u\alpha + v)/d \ .$$

Entsprechend müssen wir dann alle Elemente $\beta \in o_E$ berechnen, die die Bedingung

$$d_E I^2 (R^\times)^2 \ = \ d_{R[\beta]} (R^\times)^2$$

erfüllen, da für sie die Diskriminante ihres Minimalpolynoms mit Δ übereinstimmt. I heißt dann **Index** von β.

Indizes

Gegeben ist eine kubische Erweiterung $E = F(\alpha)$, für deren Diskriminante d_E die Gleichung $\Delta = d_E I^2$ gilt. In den ganzen Zahlen o_E von E sind dann alle Elemente vom Index I zu berechnen. Wählt man α geeignet, besitzt o_E eine R-basis (**Ganzheitsbasis**) von der Gestalt

$$\omega_1, \omega_2 = \alpha, \omega_3 = (\alpha^2 + u\alpha + v)/d \ .$$

Entsprechend müssen wir dann alle Elemente $\beta \in o_E$ berechnen, die die Bedingung

$$d_E I^2 (R^\times)^2 \ = \ d_{R[\beta]} (R^\times)^2$$

erfüllen, da für sie die Diskriminante ihres Minimalpolynoms mit Δ übereinstimmt. I heißt dann **Index** von β.

Indizes

Es sei $f(T) = T^3 - UT^2 + VT - W \in R[T]$ das Minimalpolynom von α. Zwecks Vereinfachung der Darstellung nehmen wir im folgenden noch $\omega_3 = \alpha^2$ an.

Wir suchen folglich $x, y \in R$, so dass $\vartheta = x\alpha + y\alpha^2$ den Index I besitzt. Wie früher bezeichnen $\vartheta^{(j)} = x\alpha^{(j)} + y\alpha^{(j)2}$ $(j = 1, 2, 3)$ die Konjugierten von ϑ. Dann ist die folgende **Indexformgleichung** zu lösen:

$$I = I(\vartheta) = \frac{1}{\sqrt{d_E}} \prod_{1 \le i < j \le 3} (\vartheta^{(i)} - \vartheta^{(j)}) = \prod_{1 \le i < j \le 3} (x + (\alpha^{(i)} + \alpha^{(j)})y)\,, \quad \text{also}$$

$$I = \prod_{1 \le k \le 3} (x_0 - \alpha^{(k)} y_0) =: F(x_0, y_0) = \quad \text{mit} \quad x_0 = x + Uy,\ y_0 = y\ .$$

Indexformgleichungen

Es ist $F(x_0, y_0)$ ein homogenes Polynom vom Grad 3. Falls $F(x_0, 1)$ reduzibel ist, lassen sich die Lösungen der vorangehenden Gleichung einfach berechnen. Wir nehmen daher im folgenden an, dass $F(x_0, 1)$ irreduzibel ist. Dann ist $F(x_0, y_0) = I$ eine sogenannte **Thue** Gleichung.

Mittels $\beta^{(i)} = x_0 - \alpha^{(i)} y_0$ führt die Siegelsche Identität

$$(\alpha^{(1)} - \alpha^{(2)})\beta^{(3)} + (\alpha^{(2)} - \alpha^{(3)})\beta^{(1)} + (\alpha^{(3)} - \alpha^{(1)})\beta^{(2)} \ = \ 0$$

unmittelbar zu einer Einheitengleichung in E :

$$1 = \frac{(\alpha^{(2)} - \alpha^{(3)})\beta^{(1)}}{(\alpha^{(2)} - \alpha^{(1)})\beta^{(3)}} + \frac{(\alpha^{(3)} - \alpha^{(1)})\beta^{(2)}}{(\alpha^{(2)} - \alpha^{(1)})\beta^{(3)}} = \varepsilon + \eta \ .$$

Indexformgleichungen

Man berechnet eine Liste L_1 aller nicht assoziierten Elemente $\mu \in o_E$ mit Norm $\pm I$. $E = F(\alpha)$ besitze die Grundeinheiten ε_i $(1 \leq i \leq r)$. Die Gruppe der Einheitswurzeln von o_E werde von ε_0 erzeugt und besitze die Ordnung w. Für alle $\mu \in L_1$ ist dann zu testen, ob

$$\beta = \mu \varepsilon_0^{a_0} \cdots \varepsilon_r^{a_r}$$

eine Lösung der Indexformgleichung ist. Der Einfachheit halber ersetzen wir im folgenden $\mu \varepsilon^{a_0}$ durch μ.

Indexformgleichungen: Zahlkörper

Aus der Siegelschen Identität

$$(\alpha^{(1)} - \alpha^{(2)})\beta^{(3)} + (\alpha^{(2)} - \alpha^{(3)})\beta^{(1)} + (\alpha^{(3)} - \alpha^{(1)})\beta^{(2)} \;=\; 0$$

bekommenen wir nun Abschätzungen für die Linearform in Logarithmen

$$\Lambda \;=\; \left|\log\left|\frac{(\alpha^{(1)} - \alpha^{(2)})\mu^{(3)}}{(\alpha^{(1)} - \alpha^{(3)})\mu^{(2)}}\right| + a_1 \log\left|\frac{\varepsilon_1^{(3)}}{\varepsilon_1^{(2)}}\right| + a_2 \log\frac{\varepsilon_2^{(3)}}{\varepsilon_2^{(2)}}\right|$$

Eine obere Schranke erhält man mit elementaren Methoden in der Gestalt $c_4 \exp(-c_5 A)$, wobei $A := \max\{a_1, ..., a_r\}$ ist.

Indexformgleichungen: Zahlkörper

Falls Λ nicht verschwindet, liefert die Bakersche Methode eine untere Abschätzung der Form $\exp(-c_6 \log A)$. Beide Schranken zusammen ergeben eine obere Abschätzung von A, die im allgemeinen $> 10^{18}$ ist.

Diese Schranke lässt sich mittels Approximationsmethoden in mehreren Schritten drastisch verkleinern, im allgemeinen auf unter 100.

Beispiel einer Indexformgleichung bei Zahlkörpern

Die Thue Gleichung

$$
\begin{aligned}
& x^3 + \\
& 611210797432150799284926 3 * x^2 y + \\
& 1245262129658818926990026603803742858278034654673 3 * x y^2 + \\
& 845686288089805643439518999323289454828 \\
& 660147759928385569401433849166 01 * y^3 \\
& = 105331612040766266489369 7
\end{aligned}
$$

hat keine Lösung.

Funktionenkörper: Beispiel

Wir betrachten die Mordellgleichung

$$Y^2 = X^3 + (t^2 + 3t - 1)^2$$

über $F = \mathbb{F}_{25}(t)$. Es sei ζ ein Erzeuger der zyklischen multiplikativen Gruppe $\mathbb{F}_{25}^{\times}$.
Wir wollen alle normierten irreduziblen kubischen Polynome mit einer Diskriminante $-108 \cdot (t^2 + 3t - 1)^2$ (beziehungsweise $(t^2 + 3t - 1)^2$) berechnen.

Eine Nullstelle eines solchen Polynoms erzeugt eine zyklische kubische Erweiterung E von F der Form $E = F(\sqrt[3]{\mu})$.

Funktionenkörper: Beispiel

Als Faktorisierung von $\sqrt{d_E} = t^2 + 3t - 1$ in $\mathbb{F}_{25}[t]$ erhalten wir

$$t^2 + 3t - 1 = (t - \zeta^2)(t - \zeta^{10}),$$

es gibt also 4 mögliche Kandidaten für μ:

$$\mu_1 = t^2 + 3t - 1, \;\; \mu_2 = \zeta\mu_1, \;\; \mu_3 = (t - \zeta^{10})\mu_1, \;\; \mu_4 = \zeta\mu_3.$$

Wir zeigen, dass im Fall $\mu = \mu_3$ die betrachtete Mordellgleichung unendlich viele Lösungen besitzt.

Dazu bemerken wir, dass $E = F(\sqrt[3]{\mu})$ derselbe Körper wie $F(\alpha)$ ist, wobei α eine Nullstelle des Polynoms
$f(y) = y^3 - ty^2 - (t+3)y - 1$ ist.

Funktionenkörper: Beispiel

In der Tat lassen sich die Nullstellen von
$f(y) = y^3 - ty^2 - (t+3)y - 1$ in der Ganzheitsbasis

$$(1, \sqrt[3]{\mu}, \frac{\sqrt[3]{\mu}}{t - \zeta^{10}})$$

von $E = F(\sqrt[3]{\mu})$ mit den Koordinaten

$$(2t, -\zeta^{10}, -\zeta^2), (2t, -\zeta^2, -\zeta^{10}), (2t, 2, 2)$$

darstellen.

Wir betrachten im folgenden daher $E = F(\alpha)$ mit Ganzheitsbasis $1, \alpha, \alpha^2$. Die drei Nullstellen des Polynoms f sind dann

$$\alpha_1 = \alpha,\ \alpha_2 = \frac{-1}{1+\alpha_1},\ \alpha_3 = \frac{-1}{1+\alpha_2}\ .$$

Funktionenkörper: Beispiel

Wegen $d_E = d(\alpha) = (t^2+3t-1)^2$ erfordert die Bestimmung ganzer Zahlen von E mit Diskriminante $(t^2+3t-1)^2$ die Berechnung von ganzen Zahlen mit Index 1 in E. Wir suchen folglich $x, y \in \mathbb{F}_{25}[t]$, so dass $\vartheta = x\alpha + y\alpha^2$ den Index 1 in E besitzt. Wir setzen $\vartheta_i = x\alpha_i + y\alpha_i^2$ $(i = 1, 2, 3)$. Dann ist die folgende Gleichung zu lösen:

$$1 = I(\vartheta) = \frac{1}{\sqrt{d_E}} \prod_{1\le i<j\le 3} (\vartheta_i - \vartheta_j) = \prod_{1\le i<j\le 3} (x + (\alpha_i+\alpha_j)y)\,, \quad \text{also}$$

$$1 = \prod_{1\le k\le 3} (x_0 - \alpha_k y_0) \quad \text{mit} \quad x_0 = x + ty,\ y_0 = y\ .$$

Funtionenkörper: Beispiel

Mittels $\beta_i = x_0 - \alpha_i y_0$ ergibt die Siegelsche Identität

$$(\alpha_1 - \alpha_2)\beta_3 + (\alpha_2 - \alpha_3)\beta_1 + (\alpha_3 - \alpha_1)\beta_2 = 0 \ ,$$

aus der wir unmittelbar eine Einheitengleichung in E erhalten:

$$1 = \frac{(\alpha_2 - \alpha_3)\beta_1}{(\alpha_2 - \alpha_1)\beta_3} + \frac{(\alpha_3 - \alpha_1)\beta_2}{(\alpha_2 - \alpha_1)\beta_3} = \varepsilon + \eta \ .$$

Außer Lösungen $(\varepsilon, \eta) \in (\mathbb{F}_q^\times)^2$ erhalten wir die folgenden:

$$(\varepsilon, \eta) = (4\alpha_1\alpha_2, 4\alpha_2)\,, \left(\frac{4}{\alpha_1}, \frac{2}{\alpha_1\alpha_2}\right)\,, \left(4\alpha_1, \frac{2}{\alpha_2}\right) \ .$$

Funktionenkörper: Beispiel

Für alle Lösungen (ε, η) gilt

$$\frac{\beta_1}{\beta_3} = \frac{\alpha_2 - \alpha_1}{\alpha_2 - \alpha_3}\varepsilon\,, \quad \frac{\beta_2}{\beta_3} = \frac{\alpha_2 - \alpha_1}{\alpha_3 - \alpha_1}\eta\,.$$

Mittels

$$1 \;=\; \beta_1\beta_2\beta_3 \;=\; \beta_3^3\frac{\beta_1}{\beta_3}\frac{\beta_2}{\beta_3}$$

können wir daher β_3 berechnen und anschließend β_1 und β_2.
Für jede Lösung $(\varepsilon, \eta) \notin (\mathbb{F}_q^\times)^2$ erhalten wir eine unendliche Familie von Lösungen $(\varepsilon^{5^m}, \eta^{5^m})$. Entsprechend finden wir unendlich viele ganze Zahlen $\vartheta = x\alpha + y\alpha^2$ vom Index 1 in E und unendlich viele Lösungen der ursprünglichen Mordellgleichung.

Funktionenkörper: Beispiel

Abschließend bemerken wir, dass sich das erzeugende Polynom $f(y) = y^3 - ty^2 - (t+3)y - 1$ etwa durch $f(y) = y^3 - h(t)y^2 - (h(t)+3)y - 1$ mit geeigneten quadratfreien Polynomen $h(t) \in F[t]$ ersetzen lässt. Dann liefern dieselben Überlegungen wie zuvor unendliche Familien elliptischer Kurven, die alle eine uneendliche Anzahl ganzer Punkte besitzen.