Berechnung nicht-galoisscher kubischer Erweiterungen mit Mitteln der Klassenkörpertheorie

Michael E. Pohst

Institut für Mathematik
Technische Universität Berlin

4.2.2015

Aufgabenstellung

Zur Berechnung aller ganzen Punkte einer Mordell Kurve

$$y^2 = x^3 + \kappa$$

bestimmt man

$$\Delta := -108\kappa ,$$

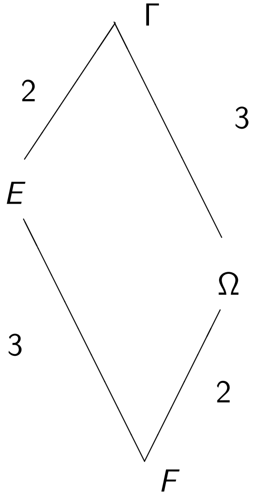
welches im hier betrachteten Fall kein Quadrat ist. Wir schreiben

$$\Delta = d\lambda^2 ,$$

wobei d die Diskriminante einer quadratischen Erweiterung Ω von F ist, also

$$\Omega = F(\sqrt{d}) .$$

Die fraglichen kubischen Erweiterungen E besitzen eine Diskriminante $D = df^2$ mit $f \mid \lambda$. Im letzten Schritt müssen wir dann alle Elemente in E mit Index $I = \lambda/f$ bestimmen.


Γ
2
3
E
Ω
3
2
F

Nicht galoissche kubische Erweiterungen E/F

In Diagramm bezeichnet Γ die galoissche Hülle des Körpers E.
(Γ ist dann eine zyklische kubische Erweiterung von Ω.)

Gemäß Klassenkörpertheorie sind die Diskriminante d der quadratischen Erweiterung Ω und eine Idealgruppe H vom Index 3 in der Strahlklassengruppe Cl_f vom Führer f in Ω die Invarianten von E.

Strahlklassengruppe

Es sei O_K die Maximalordnung eines globalen Körpers K, der F enthält. Wir setzen

$$I := \{\frac{1}{a}\mathbf{a} | 0 \neq a \in R,\ 0 \neq \mathbf{a} \text{ Ideal in } O_K\}\ ,$$

$$P := \{\alpha O_K | 0 \neq \alpha \in K\}\ ,\ Cl := I/P \text{ (Klassengruppe)}\ ,$$

$$I_f := \{\mathbf{a} \in I | \mathbf{a} \text{ koprim zu } f\, O_K\}\ ,$$

$$P_f := \{\alpha O_K | 0 \neq \alpha \in K,\ \alpha \equiv 1 \bmod f\}\ ,\ Cl_f := I_f/P_f$$

Strahlklassengruppe zum Führer f.

Klassenkörpertheorie zur Erweiterung E/F

Gemäß Klassenkörpertheorie sind die Diskriminante d der quadratischen Erweiterung Ω und eine Idealgruppe H vom Index 3 in der Strahlklassengruppe Cl_f vom Führer f in Ω die Invarianten von E.

Man zerlegt Cl_f in ein direktes Produkt zyklischer Untergruppen G_i $(1 \leq i \leq r)$, deren Elementzahlen n_i die Teilbarkeitsbedingungen $n_1|n_2|\ldots|n_r$ erfüllen. Ist dann j minimal mit der Eigenschaft $3|n_j$, so existieren genau $(3^{r-(j-1)} - 1)/2$ Kandidaten für H. (Von diesen besitzen im allgemeinen nicht alle den Führer f.)

Klassenkörpertheorie zur Erweiterung E/F

Gemäß Klassenkörpertheorie sind die Diskriminante d der quadratischen Erweiterung Ω und eine Idealgruppe H vom Index 3 in der Strahlklassengruppe Cl_f vom Führer f in Ω die Invarianten von E.

Man zerlegt Cl_f in ein direktes Produkt zyklischer Untergruppen G_i $(1 \leq i \leq r)$, deren Elementzahlen n_i die Teilbarkeitsbedingungen $n_1|n_2|\ldots|n_r$ erfüllen. Ist dann j minimal mit der Eigenschaft $3|n_j$, so existieren genau $(3^{r-(j-1)} - 1)/2$ Kandidaten für H. (Von diesen besitzen im allgemeinen nicht alle den Führer f.)

Klassenkörpertheorie zur Erweiterung E/F

Lemma Es bezeichne τ den nicht trivialen F-Automorphismus von Ω, der $\sqrt{d}$ auf $-\sqrt{d}$ abbildet.
(i) Γ/F ist genau dann galoissch, wenn $\tau(H) = H$ gilt.
(ii) Γ/F ist genau dann abelsch, wenn $\tau(\mathbf{a}H) = \mathbf{a}H$ gilt.

Führer f bei Zahlkörpern (nach Hasse)

Lemma Der Führer f ist von der Form

$$f = p_o^w p_1 \cdots p_n \ ,$$

wobei die p_i paarweise verschiedene Primzahlen $\neq 3$ sind und $p_0 = 3$ mit $w \in \{0, 1, 2\}$ gilt. Für $w = 1$ muss überdies $d \equiv \pm 3 \bmod 9$ und für $w = 2$ zudem $3 \nmid d$ oder $d \equiv -3 \bmod 9$ gelten. Weiterhin müssen die Primzahlen p_i für $1 \leq i \leq n$ die Kongruenzen

$$\left(\frac{d}{p_i}\right) \equiv p_i \bmod 3$$

erfüllen.

Führer bei Funktionenkörpern $\mathbb{F}_q(t)$

Der Führer f ist ein Produkt verschiedener Primelemente π von o_F.

Für $q \equiv 1 \bmod 3$ müssen alle Primteiler π von f in Ω zerlegt sein.

Für $q \equiv 2 \bmod 3$ können nur solche Primelemente π den Führer f teilen, welche entweder zerlegt mit $\deg(\pi)$ gerade oder träge mit $\deg(\pi)$ ungerade sind.

Der Algorithmus

1. Für $\Delta = -108\kappa$ berechne alle Tripel (D, d, f).

    Für jedes Tripel führe aus:

    2. Berechne die Strahlklassengruppe Cl_f vom Führer f in $\Omega = F(\sqrt{d})$.
    3. Berechne alle Untergruppen H vom Index 3 in Cl_f.

        Für jede Untergruppe H führe aus:

        4. Berechne den Klassenkörper Γ und überprüfe Führer und Galoisgruppe.
        5. Berechne den kubischen Teilkörper E von Γ.
        6. In E (mit Diskriminante D) löse eine Indexformgleichung mit rechter Seite $\sqrt{\Delta/D}$.