Vortrag über die Diplomarbeit zum Thema

Entwicklung und Implementierung eines Algorithmus zur Berechnung von Kommutatoren unipotenter Elemente in Chevalley-Gruppen

auf der

Studentenkonferenz
(Im Rahmen der DMV 2000)
20.-22. September 2000, Dresden

von

Sergei Haller

Sei $\mathfrak{L}_K$ eine einfache Lie-Algebra über dem beliebigen Körper K. Sei $\Phi = \{r_1, \dots, r_{2k}\}$ das Wurzelsystem von $\mathfrak{L}_K$ und $\Pi = \{r_1, \dots, r_l\}$ das zugehörige fundamentale Wurzelsystem. Wir ordnen alle Wurzeln nach einer Ordnungsrelation, die kompatibel zu deren Höhe ist. Die Höhe einer Wurzel r ist

$$h(r) = \sum_{i=1}^{l} \lambda_i, \qquad \text{falls} \qquad r = \sum_{i=1}^{l} \lambda_i r_i \qquad \text{ist.}$$

Sei $\mathfrak{L}(K)$ die Chevalley-Gruppe vom Typ $\mathfrak{L}$ über K. Sie wird von Elementen $x_r(t)$, $r \in \Phi$, $t \in K$ erzeugt. Die Untergruppe

$$U = < x_r(t) \mid r \in \Phi^+, t \in K >$$

ist die unipotente Untergruppe von $\mathfrak{L}(K)$.

Jedes Element von U ist also ein Produkt von *Wurzelelementen* $x_r(t)$ und kann als solches nach einem Satz eindeutig in aufsteigender Reihenfolge der Wurzeln geschrieben werden. Diese eindeutige Form nennen wir die *kanonische Form*.

Zum Berechnen der kanonischen Form benutzen wir einige Relationen, die für die Chevalley-Gruppe gelten. Hauptsächlich die Relation

$$x_r(t)x_r(u) = x_r(t+u)$$

und Chevalleys Kommutatorformel, die eingeschränkt auf U wie folgt lautet:

$$[x_s(u), x_r(t)] = \prod_{i,j>0} x_{ir+js}(C_{ijrs} \cdot (-t)^i \cdot u^j),$$

falls $r, s \in \Phi^+$ linear unabhängig sind und das Produkt über alle positiven Wurzeln der Form $ir + js,\ i > 0,\ j > 0$ läuft, in aufsteigender Reihenfolge. Jedes C_{ijrs} ist dabei eins von $\pm 1, \pm 2, \pm 3$.

Die Berechnung der kanonischen Form eines Elementes ist im allgemeinen aufwendig:

- Als Produkt von Wurzelelementen kann es beliebige Länge haben.

- Falls ein Element $x = x_{r_1}(t_1) \cdots x_{r_n}(t_n)$ kanonische Form hat, so hat sein Inverses niemals die kanonische Form (es sei denn $n = 1$): $x^{-1} = x_{r_n}(-t_n) \cdots x_{r_1}(-t_1)$

- Das Produkt zweier Elemente in kanonischer Form hat im allgemeinen nicht die kanonische Form: $x_{r_1}(t_1)x_{r_2}(t_2) \cdot x_{r_1}(u_1)$

- usw.

Man kann sich also viel mühsame Arbeit ersparen, indem man die Berechnung der kanonischen Formen dem Computer überläßt. Das Entwickeln und Implementieren der entsprechenden Algorithmen ist Inhalt dieser Diplomarbeit.

Als geeignet hat sich das Algebrasystem GAP4.2 erwiesen, für das ich das Share Package `Unipot` geschrieben habe. Es bietet dem Anwender die Möglichkeit, mit Elementen unipotenter Untergruppen von Chevalley-Gruppen über einem beliebigen Körper (in beliebiger Charakteristik) mit den Wurzelsystemen A_l, B_l, C_l, D_l, E_6, E_7, E_8, F_4 und G_2 zu rechnen, insbesondere deren kanonische Form zu bestimmen. Darüberhinaus werden auch Funktionen wie Multiplikation, Invertieren, Potenzieren mit ganzen Zahlen, das Berechnen des Kommutators zweier Elemente zur Verfügung gestellt.

Zunächst generieren wir die unipotente Untergruppe einer Chevalley-gruppe, hier z.B. unipotente Untergruppen von Gruppen $A_4(\mathbb{Q})$, $C_3(2)$ und $D_4(49)$:

```
gap> U_A4 := UnipotChevSubGr( "A", 4, Rationals );
<Unipotent subgroup of a Chevalley group of type A4 over Rationals>
gap> U_C3 := UnipotChevSubGr( "C", 3, GaloisField(2) );
<Unipotent subgroup of a Chevalley group of type C3 over GF(2)>
gap> U_D4 := UnipotChevSubGr( "D", 4, GF(49) );
<Unipotent subgroup of a Chevalley group of type D4 over GF(7^2)>
gap>
gap>
gap> Size(U_A4);
infinity
gap> Size(U_C3);
#I  The order of this group is 2^9 which is
512
gap> Size(U_D4);
#I  The order of this group is 49^12 which is
191581231380566414401
gap>
```

Nun können wir auch einige Elemente in den Gruppen erzeugen, so z.B. mit

```
gap> x := UnipotChevElemByFC( U_A4, [0,0,0,1], 3 );
x_{[ 0, 0, 0, 1 ]}( 3 )
gap> y := UnipotChevElemByFC( U_A4, [0,1,1,0], 7 );
x_{[ 0, 1, 1, 0 ]}( 7 )
gap> z := y*x;
x_{[ 0, 1, 1, 0 ]}( 7 ) * x_{[ 0, 0, 0, 1 ]}( 3 )
gap>
```

die Elemente $x = x_{r_4}(3)$, $y = x_{r_2+r_3}(7)$ und schließlich $z = yx$ in der unipotenten Untergruppe `U_A4` mit dem fundamentalen Wurzelsystem $\Pi = \{r_1, r_2, r_3, r_4\}$.

Die kanonische Form von z ist $x_{r_4}(3)x_{r_2+r_3}(7)x_{(r_2+r_3)+r_4}(-21)$:

```
gap> CanonicalForm(z);
x_{[ 0, 0, 0, 1 ]}( 3 ) * x_{[ 0, 1, 1, 0 ]}( 7 ) * x_{[ 0, 1, 1, 1 ]}( -21 )
gap>
```

Das Inverse von z ist $x_{r_4}(-3)x_{r_2+r_3}(-7)$ und ist bereits in kanonischer Form:

```
gap> z^-1;
x_{[ 0, 0, 0, 1 ]}( -3 ) * x_{[ 0, 1, 1, 0 ]}( -7 )
gap> CanonicalForm(z^-1);
x_{[ 0, 0, 0, 1 ]}( -3 ) * x_{[ 0, 1, 1, 0 ]}( -7 )
gap>
```

Oder wir können den Kommutator von x und y ausrechnen:

```
gap> Comm( x, y, "canonical" );
x_{[ 0, 1, 1, 1 ]}( 21 )
gap>
```

Desweiteren ist auch symbolisches Rechnen mit `unipot` möglich. Anstatt

$$[x_{r_4}(3), x_{r_2+r_3}(7)] = x_{(r_2+r_3)+r_4}(21)$$

möchte man folgende Rechnung durchführen:

$$[x_{r_4}(t), x_{r_2+r_3}(u)] = x_{(r_2+r_3)+r_4}(tu),$$

denn diese sagt wesentlich mehr aus und gilt in einem beliebigen Körper.

```
gap> Q := PolynomialRing( Rationals, ["t", "u"] );
PolynomialRing(..., [ t, u ])
gap> t := IndeterminatesOfPolynomialRing(Q)[1];;
gap> u := IndeterminatesOfPolynomialRing(Q)[2];;
gap>
gap> U1_A4 := UnipotChevSubGr("A", 4, Q);
<Unipotent subgroup of a Chevalley group of type A4 over
PolynomialRing( Rationals, [ t, u ] )>
gap>
```

Jetzt erscheint das obige Beispiel in einem neuen Licht:

```
gap> x := UnipotChevElemByFC( U1_A4, [ 0, 0, 0, 1 ], t);
x_{[ 0, 0, 0, 1 ]}( t )
gap> y := UnipotChevElemByFC( U1_A4, [ 0, 1, 1, 0 ], u);
x_{[ 0, 1, 1, 0 ]}( u )
gap> Comm( x, y, "canonical" );
x_{[ 0, 1, 1, 1 ]}( t*u )
gap>
```

Oder ein Beispiel in der unipotenten Untergruppe der Chevalley-Gruppe $B_2(\mathbb{Q})$ mit dem Wurzelsystem:

$$\begin{array}{ccc} \circ & \Rightarrow & \circ \\ r_1 & & r_2 \end{array}$$

```
gap> U := UnipotChevSubGr( "B", 2, Q );;
gap> Comm(UnipotChevElemByFC( U, [0,1], t ),
>          UnipotChevElemByFC( U, [1,0], u ),
>          "canonical");
x_{[ 1, 1 ]}( -t*u ) * x_{[ 1, 2 ]}( -t^2*u )
gap>
```

Im folgenden möchten wir ein Beispiel demonstrieren, bei dem ein besonderer Effekt der Chevalley-Gruppen mit zweifach-Bindungen zum Vorschein tritt: Wir rechnen den Kommutator von $x_{r_2}(t)$ und $x_{r_1+r_2}(u)$ aus:

```
gap> Comm(UnipotChevElemByFC( U, [0,1], t ),
>          UnipotChevElemByFC( U, [1,1], u ),
>          "canonical");
x_{[ 1, 2 ]}( -2*t*u )
gap>
```

Dies bedeutet, daß die beiden Elemente $x_{r_2}(t)$ und $x_{r_1+r_2}(u)$ genau dann vertauschbar sind, wenn die Charakteristik des zugrundeliegenden Körpers 2 ist.

Über dem Primkörper $GF(2)$ sieht dieses Beispiel so aus:

```
gap> gf2 := PolynomialRing( GF(2), ["t", "u"] );
PolynomialRing(..., [ t, u ])
gap> t := IndeterminatesOfPolynomialRing(gf2)[1];;
gap> u := IndeterminatesOfPolynomialRing(gf2)[2];;
gap>
gap> U := UnipotChevSubGr( "B", 2, gf2 );
<Unipotent subgroup of a Chevalley group of type B2 over
PolynomialRing( GF(2), [ t, u ] )>
gap>
gap> Comm(UnipotChevElemByFC( U, [0,1], t ),
>          UnipotChevElemByFC( U, [1,1], u ),
>         "canonical");
<identity>
gap>
```

Hier haben wir die Zusatzinformation, nämlich die Charakteristik 2, ausgenutzt.

Dipl.-Math. Sergei Haller
eMail: `<Sergei.Haller@math.uni-giessen.de>`

`Unipot` Homepage:
`http://www.uni-giessen.de/~gc1007/unipot.html`