Formale Gruppengesetze

Bachelorarbeit von

Nils Sturma

Betreuerin: Prof. Dr. Annette Huber-Klawitter

11. Januar 2018

Albert-Ludwigs-Universität Freiburg im Breisgau
Fakultät für Mathematik und Physik

Inhaltsverzeichnis

0 Einleitung

Formale Gruppengesetze werden in verschiedenen Bereichen der Mathematik, wie zum Beispiel in der Zahlentheorie, algebraischen Topologie und Lie-Theorie benutzt. Man könnte sich sehr lange mit ihnen beschäftigen, wir werden uns im Rahmen dieser Bachelorarbeit daher nur einzelne Aspekte anschauen. Kurz gesagt, ist ein eindimensionales formales Gruppengesetz F eine formale Potenzreihe in zwei Variablen der Form $F(X,Y) = X + Y +$ (Terme mit Grad ≥ 2), die sich assoziativ verhält ($F(F(X,Y),Z) = F(X,F(Y,Z))$). Wir werden uns zuerst mit der grundlegenden Theorie formaler Gruppengesetze beschäftigen und uns mit einigen Beispielen vertraut machen.

Um Eigenschaften und Sätze über formale Gruppengesetze zu zeigen, bietet es sich häufig an, eine vollständige Induktion über den Grad der vorliegenden Potenzreihen zu führen. Tatsächlich ist dies die häufigste Technik, die wir benutzen werden.

Nachdem wir die grundlegende Theorie formaler Gruppengesetze verstanden haben und wissen, wie Homomorphismen bzw. Isomorphismen zwischen zwei formalen Gruppengesetzen definiert sind, beschäftigen wir uns mit eindimensionalen formalen Gruppengesetzen, die über Körpern definiert sind. Wir werden zeigen, dass alle formalen Gruppengesetze über einem Körper der Charakteristik null isomorph sind.
In Kapitel drei klassifizieren wir formale Gruppengesetze über algebraisch abgeschlossenen Körpern mit positiver Charakteristik. Dazu führen wir eine Invariante ein, die Höhe eines formalen Gruppengesetzes. Wir erhalten, dass alle formalen Gruppengesetze der selben Höhe isomorph sind.

In den letzten beiden Kapiteln der Arbeit beschäftigen wir uns mit interessanten Beispielen formaler Gruppengesetze. Diese stammen von Gruppenstrukturen auf Mannigfaltigkeiten oder algebraischen Varietäten.
So können wir Koordinaten in einer Umgebung des neutralen Elements einer Lie-Gruppe wählen und die Multiplikationsabbildung durch eine Taylorreihenentwicklung ausdrücken. Das führen wir konkret durch und beweisen anschließend, dass die entstandene formale Taylorreihe auch tatsächlich ein formales Gruppengesetz ist. Wir erhalten somit, dass sich aus jeder Lie-Gruppe ein formales Gruppengesetz konstruieren lässt. Um die Angelegenheit etwas zu vereinfachen, werden wir uns dabei auf eindimensionale Lie-Gruppen beschränken.
Zum Schluss führen wir das selbe in ganz ähnlicher Art und Weise für affine algebraische Gruppen durch. Auch hier kann man am neutralen Element eine Taylorreihenentwicklung durchführen und erhält ein formales Gruppengesetz.

1 Formale Potenzreihen und Notation

Dieses Kapitel ist eine Einführung und erklärt einige Begriffe und Konventionen, die wir später benutzen werden.

In der vorliegenden Arbeit ist ein Ring R stets ein kommutativer Ring mit Einselement. Wir schreiben $R[[X_1, \ldots, X_n]]$ für den formalen Potenzreihenring in n Variablen. Die Definition des formalen Potenzreihenrings wird als bekannt vorausgesetzt und findet sich zum Beispiel in [ZS13, Kapitel V.II, Seite 129]. Dort wird auch bewiesen, dass dies wieder ein kommutativer Ring mit Einselement ist.

Zur Notation von Elementen aus $R[[X_1, \ldots, X_n]]$ benötigen wir Multiindizes. Sei dazu im Folgenden $X = (X_1, \ldots, X_n)$,

$$\begin{aligned} \underline{i} = (i_1, \ldots, i_n) \in \mathbb{N}_0^n, \qquad & |\underline{i}| = i_1 + \ldots + i_n, \\ \underline{i}! = i_1! i_2! \ldots i_n!, \qquad & X^{\underline{i}} = X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}. \end{aligned}$$

Für $f \in R[[X]] = R[[X_1, \ldots, X_n]]$ kann man dann schreiben: $f(X) = \sum\limits_{|\underline{i}| \geq 0} a_{\underline{i}} X^{\underline{i}}$.

Satz 1.1. Es gelten die folgenden Eigenschaften:

- Der Polynomring $R[X]$ ist ein Unterring von $R[[X]]$.
- $f(X) = \sum\limits_{|\underline{i}| \geq 0} a_{\underline{i}} X^{\underline{i}}$ ist genau dann invertierbar (bzgl. der Multiplikation), wenn $a_{\underline{0}}$ in R invertierbar ist. Dabei ist $\underline{0} = (0, \ldots, 0)$.

Beweis. Für den ersten Punkt findet sich ein Beweis in [ZS13, Kapitel V.II, Seite 130] und für den zweiten in [Lan05, Kapitel IV.9]. □

An einigen stellen der Arbeit wollen wir formale Potenzreihen differenzieren. Dafür geben wir an dieser Stelle eine Definition.

Definition 1.2. [Hen88, Kapitel 1.4] Sei $f(X) = \sum_{i=0}^{\infty} a_i X^i \in R[[X]]$ eine formale Potenzreihe in einer Variablen. Dann ist die *formale Differentiation* definiert durch

$$f'(X) \coloneqq \sum_{i=1}^{\infty} i a_i X^{i-1}.$$

Genauso definieren wir die *formale partielle Differentiation* für eine Potenzreihe in n Variablen. Sei dazu wieder $X = (X_1, \ldots, X_n)$ und $f(X) = \sum_{|\underline{i}| \geq 0} a_{\underline{i}} X^{\underline{i}} \in R[[X]]$. Dann ist

$$D_j f(X) = \frac{\partial}{\partial X_j} f(X) \coloneqq \sum_{|\underline{i}| \geq 1} i_j a_{\underline{i}} X_1^{i_1} \cdots X_j^{i_j - 1} \cdots X_n^{i_n}.$$

Unter Verwendung der Multiindizes schreiben wir:

$$D^{\underline{i}} = D_1^{i_1} \cdots D_n^{i_n} = \frac{\partial^{|\underline{i}|}}{\partial X_1^{i_1} \cdots \partial X_n^{i_n}}.$$

Für die formale Differentiation von Potenzreihen gelten die gewohnten Ableitungsregeln, wie zum Beispiel die Faktor-, Summen und Produktregel. Ein Beweis steht in [Hen88, Kapitel 1.6].
Ebenso gilt die Kettenregel für ineinander eingesetzte Potenzreihen. Das ineinander Einsetzen ist für beliebige Potenzreihen $f, g \in R[[X_1, \ldots, X_n]]$ aber nicht wohldefiniert. Allerdings wird zum Beispiel in [Hen88, Kapitel 1.6] bewiesen, dass man g in f einsetzen darf, wenn der konstante Term von g null ist, also $g(0) = 0$. Mit anderen Worten kann man sagen, dass in dieser Situation der Ausdruck $f(X_1, \ldots, g(X), \ldots, X_n)$, bei dem für die i-te Variable $g(X)$ eingesetzt wurde, wohldefiniert ist. Für Potenzreihen in einer bzw. zwei Variablen wollen wir die Kettenregel als Satz formulieren, da wir sie in dieser Form später anwenden werden.

Satz 1.3 (Kettenregel in einer bzw. zwei Variablen)**.** [Hen88, Kapitel 1.6] Seien $f, g \in R[[X]]$ Potenzreihen in einer Variablen mit $g(0) = 0$. Dann gilt:

$$D(f \circ g)(X) = Df(g(X)) \cdot Dg(X).$$

Und für Potenzreihen $f, g \in R[[X, Y]]$ in zwei Variablen mit $g(0, 0) = 0$ gilt:

$$D_1(f(g(X, Y), Z)) = (D_1 f)(g(X, Y), Z) \cdot (D_1 g)(X, Y).$$

Beweis. [Hen88, Kapitel 1.6] □

Zum Schluss dieses einführenden Kapitels notieren wir noch einige Abkürzungen, die wir später benutzen werden:

$(\text{mod } \deg n)$	Modulo Grad n bei Polynomen oder Potenzreihen. Es gilt: $\sum_{\lvert\underline{i}\rvert \geq 0} a_{\underline{i}} X^{\underline{i}} = \sum_{\lvert\underline{i}\rvert = 0}^{n-1} a_{\underline{i}} X^{\underline{i}} \ (\text{mod } \deg n)$.
$\mathbb{F}_q$	Der endliche Körper mit $q = p^n$ Elementen. (p prim, $n \in \mathbb{N}$). Wir erinnern daran, dass alle endlichen Körper mit $q = p^n$ Elementen isomorph sind. $\mathbb{F}_q$ hat Charakteristik $p > 0$. Eine gute Quelle ist zum Beispiel [Lan05, Kapitel V.5].
n.V.	nach Voraussetzung
I.V.	nach der Induktionsvoraussetzung/ -annahme
fGG	formales Gruppengesetz
$B(0, \theta) \subseteq \mathbb{R}^n$	Die offene Kugel im $\mathbb{R}^n$ um den Nullpunkt mit Radius θ.

2 Grundlegende Theorie formaler Gruppengesetze

Formale Gruppengesetze der Dimension eins

Wie wir in der Einleitung erklärt haben, werden formale Gruppengesetze in vielen Bereichen der Mathematik benutzt. Aus diesem Grund gibt es auch zahlreiche Bücher, in denen sie eingeführt werden. Zum Beispiel in [Sil09], [Frö68] oder [Haz12]. Wir halten uns in diesem Abschnitt an die Darstellung in [Sil09, Kapitel IV.2].

Definition 2.1. [Sil09, Kapitel IV.2] Sei R ein Ring. Ein *(eindimensionales) formales Gruppengesetz* ist eine Potenzreihe $F \in R[[X,Y]]$ mit den folgenden Eigenschaften:

(a) $F(X,Y) \equiv X+Y \pmod{\deg 2}$,

(b) $F(X,F(Y,Z)) = F(F(X,Y),Z)$ (Assoziativität).

Gilt zusätzlich $F(X,Y) = F(Y,X)$, so nennt man F *kommutativ*.

Wir geben zunächst zwei einfache, aber schon äußerst wichtige Beispiele. Beide sind aus [Sil09, Kapitel IV.2] entnommen, werden dort aber nicht nachgerechnet.

Beispiel 2.2. $\mathbb{G}_a(X,Y) = X+Y$ (*formales additives Gruppengesetz*).
Um zu überprüfen, dass $\mathbb{G}_a$ tatsächlich ein formales Gruppengesetz ist, müssen die beiden Eigenschaften aus Definition 2.1 nachgerechnet werden. (a) ist aber offensichtlich, also bleibt nur noch (b):

$$\begin{aligned}\mathbb{G}_a(X,\mathbb{G}_a(Y,Z)) &= \mathbb{G}_a(X,Y+Z) = X+(Y+Z) = (X+Y)+Z \\ &= \mathbb{G}_a(X+Y,Z) = \mathbb{G}_a(\mathbb{G}_a(X,Y),Z).\end{aligned}$$

Wir haben dabei benutzt, dass im Ring $R[[X,Y]]$ die Addition assoziativ ist.

Beispiel 2.3. $\mathbb{G}_m(X,Y) = X+Y+XY$ (*formales multiplikatives Gruppengesetz*).
Wie im letzten Beispiel überprüfen wir, dass $\mathbb{G}_m$ ein formales Gruppengesetz ist. Eigenschaft (a) ist wieder klar, (b) folgt aus einer kurzen Rechnung, wobei die Eigenschaften von $R[[X,Y]]$ ausgenutzt werden:

$$\begin{aligned}\mathbb{G}_m(X,\mathbb{G}_m(Y,Z)) &= \mathbb{G}_m(X,Y+Z+YZ) \\ &= X+(Y+Z+YZ)+X(Y+Z+YZ) \\ &= X+Y+Z+YZ+XY+XZ+XYZ \\ &= (X+Y+XY)+Z+(X+Y+XY)Z \\ &= \mathbb{G}_m(X+Y+XY,Z) = \mathbb{G}_m(\mathbb{G}_m(X,Y),Z).\end{aligned}$$

In der Definition einer Gruppe wird die Existenz von Inversen und eines neutralen Elements gefordert. In der Definition eines formales Gruppengesetzes finden wir jedoch dazu zunächst kein analoges Axiom, da diese beiden Eigenschaften schon direkt aus (a) und (b) folgen. In anderen Worten kann man sagen, dass für ein formales Gruppengesetz stets $F(X,0) = X$ und $F(0,Y) = Y$ gilt und es außerdem eine (eindeutige) Potenzreihe

$i \in R[[X]]$ gibt, sodass $F(X, i(X)) = 0$ gilt. Hieraus wird auch die Bezeichnung *formale Gruppengesetze* deutlich. Für die Aussagen wollen wir zwei Lemmata formulieren, beide sind Übungsaufgaben in [Sil09, Kapitel IV.2].

Lemma 2.4. Sei $F \in R[[X, Y]]$ ein formales Gruppengesetz. Dann gilt:

$$F(X, 0) = X \text{ und } F(0, Y) = Y.$$

Beweis. Wir beweisen nur $F(X, 0) = X$, $F(0, Y) = Y$ folgt analog. Dazu schreiben wir $F(X, Y) = X + Y + \sum_{i+j \geq 2 \; i,j \geq 0} c_{ij} X^i Y^j$ und definieren:

$$f(X) \coloneqq F(X, 0) = X + \sum_{n \geq 2} a_n X^n, \text{ wobei } a_n = c_{n0} \text{ für alle } n \geq 2.$$

Es ist $F(0, 0) = 0$ und wegen der Assoziativität gilt:

$$f(f(X)) = F(F(X, 0), 0) = F(X, F(0, 0)) = F(X, 0) = f(X).$$

Wir nehmen an, dass $f(X) \neq X$ ist. Sei also $m \in \mathbb{N}$ die kleinste natürliche Zahl ≥ 2, sodass $a_m \neq 0$. Dann ist $f(X) \equiv X + a_m X^m \pmod{\deg m + 1}$. Nach unseren Überlegungen oben ist

$$f(X) = f(f(X)) \equiv f(X) + a_m f(X)^m \pmod{\deg m + 1}$$

und somit muss $a_m f(X)^m \equiv 0 \pmod{\deg m + 1}$ sein. Modulo $\deg m + 1$ erhalten wir:

$$0 \equiv a_m (X + a_m X^m)^m \equiv a_m X^m.$$

Daraus folgt $a_m = 0$, was ein Widerspruch zu unserer Annahme ist. □

Das Lemma erlaubt uns, jedes eindimensionale formale Gruppengesetz $F \in R[[X, Y]]$ folgendermaßen zu schreiben:

$$F(X, Y) = X + Y + \sum_{i,j \geq 1} c_{ij} X^i Y^j.$$

Lemma 2.5. Sei $F \in R[[X, Y]]$ ein formales Gruppengesetz. Dann gibt es genau eine Potenzreihe $i \in R[[T]]$, sodass gilt:

$$F(T, i(T)) = 0 = F(i(T), T).$$

Beweis. Wir beginnen mit der Existenz.
In [Sil09, Kapitel 4.2] wird in Lemma 2.4 eine andere Aussage über formale Gruppengesetze bewiesen, die Idee des Beweises ist in diesem Fall jedoch die gleiche und wir haben sie von dort übernommen. Sie besteht darin, per Induktion eine Folge von Polynomen $i_n \in R[T]$ zu konstruieren, sodass für alle $n \in \mathbb{N}$ gilt:

$$\begin{aligned} F(T, i_n(T)) &\equiv 0 \pmod{\deg n + 1}, \\ F(i_n(T), T) &\equiv 0 \pmod{\deg n + 1}, \\ i_{n+1} &\equiv i_n \pmod{\deg n + 1}. \end{aligned}$$

Wir definieren dann $i \equiv i_n \pmod{\deg n+1} \in R[[T]]$, und sehen, dass i die gewünschte Eigenschaft hat. Für $n = 1$ setzen wir $i_1(T) \coloneqq -T$. Dann gilt modulo $\deg 2$:

$$F(T, i_1(T)) = F(T, -T) \equiv T - T \equiv 0.$$

Mit der gleichen Rechnung folgt: $F(i_1(T), T) \equiv 0 \pmod{\deg 2}$.
Nun nehmen wir an, dass i_n für ein $n \in \mathbb{N}$ konstruiert wurde. Setze $i_{n+1}(T) \coloneqq i_n(T) + \lambda T^{n+1}$ für ein $\lambda \in R$. Unser Ziel ist es, den Wert von λ so zu bestimmen, dass i_{n+1} die gewünschten Eigenschaften hat. Dazu ist es sinnvoll folgende Rechnung zu betrachten, in der die binomische Formel benutzt wird:

$$\begin{aligned}
F(T, i_{n+1}(T)) &= F(T, i_n(T) + \lambda T^{n+1}) \\
&= T + i_n(T) + \lambda T^{n+1} + \sum_{i,j \geq 1} c_{ij} T^i (i_n(T) + \lambda T^{n+1})^j \\
&= T + i_n(T) + \lambda T^{n+1} + \sum_{i,j \geq 1} c_{ij} T^i \left(i_n(T)^j + \sum_{k=1}^{j} \binom{j}{k} i_n(T)^{j-k} (\lambda T^{n+1})^k \right) \\
&\equiv T + i_n(T) + \lambda T^{n+1} + \sum_{i,j \geq 1} c_{ij} T^i i_n(T)^j \pmod{\deg n+2} \\
&\equiv F(T, i_n(T)) + \lambda T^{n+1} \pmod{\deg n+2}.
\end{aligned}$$

Aus der Induktionsvoraussetzung wissen wir, dass es ein $a \in R$ gibt, sodass $F(T, i_n(T)) \equiv aT^{n+1} \pmod{\deg n+2}$. Setze

$$\lambda \coloneqq -a \text{ und somit } i_{n+1}(T) \coloneqq i_n(T) - aT^{n+1}.$$

Nach der Rechnung oben gilt dann $F(T, i_{n+1}(T)) \equiv 0 \pmod{\deg n+2}$ und natürlich auch $i_{n+1}(T) \equiv i_n(T) \pmod{\deg n+1}$. Mit exakt der gleichen Rechnung lässt sich nachrechnen, dass für $i_{n+1}(T) = i_n(T) - aT^{n+1}$ ebenfalls $F(i_{n+1}(T), T) \equiv 0 \pmod{\deg n+2}$ gilt. Damit ist der Induktionsschritt abgeschlossen.

Es bleibt noch die Eindeutigkeit von $i(T)$ zu zeigen. Seien dazu $i, j \in R[[T]]$, sodass $F(T, i(T)) = F(i(T), T) = 0$ und $F(T, j(T)) = F(j(T), T) = 0$. Dann gilt wegen der Assoziativität von F:

$$\begin{aligned}
j(T) &= F(j(T), 0) = F(j(T), F(T, i(T))) = F(F(j(T), T), i(T)) \\
&= F(0, i(T)) = i(T).
\end{aligned}$$

□

Homomorphismen

Nun wollen wir Homomorphismen zwischen zwei Gruppengesetzen einführen und Beispiele dazu geben. Dazu brauchen wir zunächst noch einen anderen wichtigen Begriff.

Definition 2.6. [Sil09, Kapitel IV.2] Eine formale Potenzreihe $f \in R[[T]]$ heißt *invertierbar*, wenn f keinen konstanten Term besitzt und es $g \in R[[T]]$ gibt, sodass

$$f(g(T)) = T = g(f(T)).$$

In diesem Fall nennen wir g ein *Inverses von* f und schreiben $g = f^{-1}$.

Bemerkung 2.7. Diese Definition ist leicht zu verwechseln mit der Invertierbarkeit von Potenzreihen bezüglich der Multiplikation. Man hätte für diese Eigenschaft einen anderen Namen wählen können, zum Beispiel neutralisierbar. Fast alle Autoren benutzen aber invertierbar, daher wollen wir uns dem anschließen. Man muss sich immer bewusst sein, ob mit f^{-1} die inverse Potenzreihe bezüglich der Multiplikation oder das Inverse bezüglich der Definition oben gemeint ist. In dieser Arbeit bezeichnen wir jedoch zur Unterscheidung das Inverse bezüglich der Multiplikation stets mit $\frac{1}{f}$.

Aus der Definition folgt direkt, dass g auch keinen konstanten Term besitzt, da sonst $g(f(T)) \neq T$ wäre.

Definition 2.8. [Sil09, Kapitel IV.2] Seien $F, G \in R[[X, Y]]$ zwei formale Gruppengesetze. Ein *R-Homomorphismus* $f : F \to G$ ist eine Potenzreihe $f(T) = a_1T + a_2T^2 + \ldots \in R[[T]]$ (ohne konstanten Term), sodass

$$f(F(X, Y)) = G(f(X), f(Y))$$

gilt. Man nennt F und G *R-isomorph*, falls es einen invertierbaren Homomorphismus $f : F \to G$ gibt. Ein R-Isomorphismus f heißt *strikt*, falls $a_1 = 1$.
Wir schreiben $Hom_R(F, G)$ für die Menge aller R-Homomorphismen zwischen F ung G.

Für $f \in R[[X]]$ und $F \in R[[X, Y]]$ benutzen wir die Notation:

$$(f \circ F)(X, Y) = f(F(X, Y)) \quad \text{bzw.} \quad (F \circ f)(X, Y) = F(f(X), f(Y).$$

Falls f ein Homomorphismus zwischen zwei formalen Gruppengesetzen F und G ist, so können wir also abkürzend schreiben:

$$f \circ F = G \circ f.$$

Lemma 2.9. Seien $F, G \in R[[X, Y]]$ zwei formale Gruppengesetze und $f \in Hom_R(F, G)$ invertierbar. Dann ist $f^{-1} \in Hom_R(G, F)$.

Beweis. In Bemerkung 2.7 haben wir festgestellt, dass f^{-1} keinen konstanten Term hat. Nach Voraussetzung ist $f(f^{-1}(X)) = f^{-1}(f(X)) = X$ und da f ein Homomorphismus ist, gilt $f(F(X, Y)) = G(f(X), f(Y))$. Daraus folgt:

$$\begin{aligned} f^{-1}(G(X, Y)) &= f^{-1}(G(f(f^{-1}(X)), f(f^{-1}(Y)))) \\ &= f^{-1}(f(F(f^{-1}(X), f^{-1}(Y)))) \\ &= F(f^{-1}(X), f^{-1}(Y)). \end{aligned}$$

□

Bemerkung 2.10. Wir behaupten: Wenn f ein Isomorphismus zwischen zwei formalen Gruppengesetzen F und G ist, so gilt:

$$f \circ F \circ f^{-1} = G.$$

Nach Lemma 2.9 ist $f^{-1} \in Hom_R(G, F)$, also gilt $f^{-1} \circ G = F \circ f^{-1}$. Wenn wir nun beide Seiten der Gleichung in f einsetzen, erhalten wir wegen $f(f^{-1}(T)) = T$ die Behauptung.

Beispiel 2.11. $f(T) = T$. Offensichtlich ist $f \in Hom_R(F, F)$ für jedes formale Gruppengesetz $F \in R[[X, Y]]$, da

$$f \circ F = F = F \circ f.$$

Außerdem gilt für alle $g \in Hom_R(F, F)$:

$$(g \circ f) = g \quad \text{und} \quad (f \circ g) = g.$$

Daher wird f auch oft mit id bezeichnet.

Beispiel 2.12. Dieses Beispiel brauchen wir in Kapitel 3. Es wird in [Frö68, Kapitel 3, §2] ohne Beweis benutzt. Sei $F \in R[[X, Y]]$ formales Gruppengesetz und $u \in R[[T]]$ invertierbar. Dann ist $(u^{-1} \circ F \circ u)$ ein formales Gruppengesetz und R-isomorph zu F. Wir rechnen modulo $\deg 2$:

$$\begin{aligned}(u^{-1} \circ F \circ u)(X, Y) &\equiv u^{-1}(u(X) + u(Y)) \\ &\equiv u^{-1}(u(X + Y)) \equiv X + Y.\end{aligned}$$

Außerdem ist $u^{-1} \circ F \circ u$ assoziativ:

$$\begin{aligned}(u^{-1} \circ F \circ u)((u^{-1} \circ F \circ u)(X, Y), Z) &= (u^{-1} \circ F)(F(u(X), u(Y)), u(Z)) \\ &= (u^{-1} \circ F)(u(X), F(u(Y), u(Z))) \\ &= (u^{-1} \circ F \circ u)(X, (u^{-1} \circ F \circ u)(Y, Z)).\end{aligned}$$

$u^{-1} \circ F \circ u$ ist somit ein formales Gruppengesetz. Weiter ist $u \in Hom_R(u^{-1} \circ F \circ u, F)$, da

$$u \circ (u^{-1} \circ F \circ u) = (u \circ u^{-1}) \circ F \circ u = F \circ u.$$

Nach Voraussetzung ist u invertierbar, also sind $u^{-1} \circ F \circ u$ und F isomorph.

Wir haben in diesem Beispiel gezeigt, dass jede invertierbare Potenzreihe $u \in R[[X]]$ schon ein Isomorphismus von formalen Gruppengesetzen ist. Genauer gesagt, ist u ein Isomorphismus zwischen $u^{-1} \circ F \circ u$ und F für jedes beliebige formale Gruppengesetz F.

Beispiel 2.13. Das Beispiel ist aus [Sil09, Kapitel IV.2], allerdings dort ohne Beweis. Es wird ebenfalls in Kapitel 3 wichtig werden. Sei $F \in R[[X, Y]]$ ein kommutatives formales Gruppengesetz. Wir definieren induktiv für alle $n \in \mathbb{N}$ einen Homomorphismus $[n]_F : F \to F$, den wir die *Multiplikation mit n* nennen:

$$[0]_F(T) = 0, \quad [n + 1]_F(T) = F([n]_F(T), T).$$

Im Folgenden zeigen wir, dass $[n]_F$ für alle $n \in \mathbb{N}$ tatsächlich ein Homomorphismus ist und dass gilt:

$$[n](T) \equiv nT \pmod{\deg 2}.$$

Es ist offensichtlich, dass $[n]_F$ keinen konstanten Term besitzt. Wir zeigen $[n]_F(F(X,Y)) = F([n]_F(X), [n]_F(Y))$ für alle $n \in \mathbb{N}$ per Induktion und beginnen mit $n = 0$. Es folgt aus der Definition:

$$[0]_F(F(X,Y)) = 0 = F(0,0) = F([0]_F(X), [0]_F(Y)).$$

Wir nehmen an, dass für $n \in \mathbb{N}$ gilt: $[n]_F(F(X,Y)) = F([n]_F(X), [n]_F(Y))$. Nun wollen wir diese Identität für $n+1$ überprüfen. Dazu benutzen wir, dass F assoziativ und kommutativ ist:

$$\begin{aligned}
& F([n+1]_F(X), [n+1]_F(Y)) = F(F([n]_F(X), X), F([n]_F(Y), Y)) \\
= \; & F([n]_F(X), F(X, F([n]_F(Y), Y))) = F([n]_F(X), F(F([n]_F(Y), Y), X)) \\
= \; & F([n]_F(X), F([n]_F(Y), F(Y, X))) = F(F([n]_F(X), [n]_F(Y)), F(X, Y)) \\
= \; & F([n]_F(F(X,Y)), F(X,Y)) = [n+1]_F(F(X,Y)).
\end{aligned}$$

Im vorletzten Schritt wurde die Induktionsvoraussetzung benutzt.
Auch den zweiten Teil zeigen wir per Induktion nach n.
Für $n = 0$ ist die Aussage klar. Sei die Aussage also für $n \in \mathbb{N}$ bewiesen. Dann folgt für $n+1$:

$$\begin{aligned}
[n+1](T) &= F([n](T), T) \\
&\equiv nT + T \pmod{\deg 2} \\
&\equiv (n+1)T \pmod{\deg 2}.
\end{aligned}$$

Beispiel 2.14. Das Beispiel ist aus [Haz12, Kapitel 1.4], allerdings dort wieder ohne Beweis. Man betrachte folgende Potenzreihen in $\mathbb{Q}[[T]]$:

$$E(T) = \sum_{n=1}^{\infty} \frac{T^n}{n!} = \exp(T) - 1 \quad \text{und} \quad L(T) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{T^n}{n} = \log(1+T).$$

Wir erinnern uns an das additive formale Gruppengesetz $\mathbb{G}_a$ aus Beispiel 2.2 und an das multiplikative formale Gruppengesetz $\mathbb{G}_m$ aus Beispiel 2.3. Beides sind rationale formale Potenzreihen und wir können folgende Behauptung formulieren:

Für $\mathbb{G}_a, \mathbb{G}_m \in \mathbb{Q}[[X,Y]]$ ist $L : \mathbb{G}_m \to \mathbb{G}_a$ ein Isomorphismus mit Inverse $E : \mathbb{G}_a \to \mathbb{G}_m$.

Beweis. $L(T)$ ist eine Potenzreihe ohne konstanten Term, für die gilt:

$$\begin{aligned}
L(\mathbb{G}_m(X,Y)) &= \log(1 + \mathbb{G}_m(X,Y)) = \log(1 + X + Y + XY) \\
&= \log((1+X)(1+Y)) = \log(1+X) + \log(1+Y) \\
&= L(X) + L(Y) = \mathbb{G}_a(L(X), L(Y)).
\end{aligned}$$

Also ist L ein Homomorphismus. Weiter ist

$$L(E(T)) = \log(1 + E(T)) = \log(1 + \exp(T) - 1) = \log(\exp(T) = T,$$
$$E(L(T)) = \exp(L(T)) - 1 = \exp(\log(1 + T)) - 1 = 1 + T - 1 = T.$$

Damit ist L ein Isomorphismus mit Inverse E. Wir haben die aus den Analysisvorlesungen bekannten Rechenregeln für exp und log benutzt. □

Nun zeigen wir noch ein nützliches Lemma, das uns ein Kriterium für die Invertierbarkeit von Potenzreihen gibt.

Lemma 2.15. [Sil09, Kapitel 4.2] Sei $a \in R^*$ und $f \in R[[T]]$ eine Potenzreihe der Form $f(T) \equiv aT \pmod{\deg 2}$. Dann gibt es genau eine Potenzreihe $g \in R[[T]]$, die die Identität

$$f(g(T)) = T$$

erfüllt. Für die Potenzreihe g gilt außerdem $g(f(T)) = T$.

Beweis. Der Beweis orientiert sich an [Sil09, Kapitel 4.2] und wir beginnen mit der Existenz. Wir konstruieren eine Folge von Polynomen $g_n \in R[T]$, sodass gilt:

$$f(g_n(T)) \equiv T \pmod{\deg n + 1} \quad \text{und} \quad g_{n+1} \equiv g_n \pmod{\deg n + 1}.$$

Wir definieren dann $g \equiv g_n \pmod{\deg n + 1} \in R[[T]]$ und g erfüllt die Eigenschaft $f(g(T)) = T$.
Für $n = 1$ setzen wir $g_1(T) = a^{-1}T$, da dann $f(g_1(T)) \equiv aa^{-1}T \equiv T \pmod{\deg 2}$ gilt. Wir nehmen an, dass g_{n-1} konstruiert wurde und die gewünschten Eigenschaften hat. Setze

$$g_n(T) \coloneqq g_{n-1}(T) + \lambda T^n$$

für ein $\lambda \in R$. Unser Ziel ist es, den Wert von λ so zu bestimmen, dass g_n die gewünschten Eigenschaften hat. Man betrachte folgende Rechnung:

$$\begin{aligned} f(g_n(T)) &= f(g_{n-1}(T) + \lambda T^n) \\ &\equiv f(g_{n-1}(T)) + a\lambda T^n \qquad (\text{mod } \deg n + 1) \\ &\equiv T + bT^n + a\lambda T^n \qquad (\text{mod } \deg n + 1) \quad \text{für ein } b \in R. \end{aligned}$$

Setze $\lambda \coloneqq -a^{-1}b$. Dann ist $f(g_n(T) \equiv T \pmod{\deg n+1}$ und $g_{n+1} \equiv g_n \pmod{\deg n+1}$.

Nun ist noch $g(f(T)) = T$ zu zeigen. Dazu benutzen wir für die Potenzreihe $g(T) \equiv a^{-1}T \pmod{\deg 2}$, was wir gerade gezeigt haben. Es ist $a^{-1} \in R^*$, also gibt es eine Potenzreihe $h \in R[[T]]$, für die $g(h(T)) = T$ gilt. Daraus erhalten wir die Gleichung:

$$g(f(T)) = g(f(g(h(T)))) = g(f \circ g(h(T))) = g(h(T)) = T.$$

Zum Schluss zeigen wir die Eindeutigkeit von g. Wir nehmen also an, dass es eine andere Potenzreihe $G \in R[[T]]$ gibt, sodass $f(G(T)) = T$. Dann folgt aber:

$$g(T) = g(f(G(T))) = (g \circ f)(G(T)) = G(T).$$

□

Lemma 2.16. Seien $F, G \in R[[X,Y]]$ formale Gruppengesetze, $f \in Hom_R(F,G)$ mit $f'(0) = 0$. Dann ist $f' = 0$.

Beweis. Es gilt $f(F(X,Y)) = G(f(X), f(Y))$. Wir leiten nach Y ab, wobei wir die Kettenregel benutzen:

$$f'(F(X,Y)) \cdot D_2F(X,Y) = D_2G(f(X), f(Y)) \cdot f'(Y).$$

$Y = 0$ einsetzen:

$$\underbrace{f'(F(X,0))}_{=f'(X)} \cdot D_2F(X,0) = D_2G(f(X), f(0)) \cdot \underbrace{f'(0)}_{=0} = 0.$$

Es ist $D_2F(X,Y) \equiv 1 \pmod{\deg 1}$ und daher gilt auch für $Y = 0$:

$$D_2F(X,0) \equiv 1 \pmod{\deg 1}.$$

Insbesondere ist $D_2F(X,0) \neq 0$, daher muss $f'(X) = 0$ sein. □

Bemerkung 2.17. Ist f ein Homomorphismus über einem Körper der Charakteristik null, so folgt aus $f' = 0$, dass auch $f = 0$ ist. Tatsächlich gilt für $f(X) = \sum_{n=1}^{\infty} a_n X^n$ mit Ableitung $f'(X) = \sum_{n=1}^{\infty} n a_n X^{n-1} = 0$, dass $na_n = 0$ sein muss für alle $n \geq 1$. In einem Körper der Charakteristik null bedeutet das, $a_n = 0$ für alle $n \geq 1$.
Insgesamt folgt aus $f'(0) = 0$ in diesem Fall somit schon $f = 0$.

In Charakteristik $p > 0$ gelten diese Folgerungen nicht, siehe dazu Lemma 3.7 (i).

Formale Gruppengesetze über einem Körper der Charakteristik null

In diesem Abschnitt beweisen wir, dass jedes eindimensionale formale Gruppengesetz über einem Körper k mit $char(k) = 0$ strikt isomorph zum formalen additiven Gruppengesetz $\mathbb{G}_a$ über k ist.

Theorem 2.18. [FS15, Theorem 5] Sei k ein Körper mit $char(k) = 0$ und $F \in k[[X,Y]]$ ein formales Gruppengesetz der Dimension eins. Sei $\mathbb{G}_a \in k[[X,Y]]$ das formale additive Gruppengesetz. Dann gibt es genau eine Potenzreihe $f \in k[[T]]$ der Form $f(T) \equiv T \pmod{\deg 2}$, sodass $f : F \to \mathbb{G}_a$ ein strikter Isomorphismus ist.

Beweis. Wir folgen der Darstellung in [FS15, Theorem 5]. Für f muss gelten:

$$f(F(X,Y)) = \mathbb{G}_a(f(X), f(Y)) = f(X) + f(Y).$$

Nach X partiell differenzieren ergibt mit der Kettenregel $f'(X) = f'(F(X,Y))D_1F(X,Y)$. Für $X = 0$ folgt $1 = f'(Y)D_1F(0,Y)$, da $F(0,Y) = Y$ und $f'(0) = 1$. Es ist $D_1F(X,Y) \equiv 1 \pmod{\deg 1}$ und daher gilt auch für $X = 0$:

$$D_1F(0,Y) \equiv 1 \pmod{\deg 1}.$$

Da $1 \in k$ eine Einheit ist, ist auch $D_1F(0,Y)$ eine Einheit in $k[[Y]]$. Es ist also

$$f'(Y) = \frac{1}{D_1F(0,Y)} \text{ und damit } f(Y) \coloneqq \int \frac{1}{D_1F(0,Y)} dY.$$

Mit dem Integralzeichen ist gemeint, dass wir jedes Monom in $\frac{1}{D_1F(0,Y)}$ einzeln integrieren. Da $f(0) = 0$ gelten muss, ist f schon eindeutig bestimmt.

Einschub. An dieser Stelle geht ein, dass die Charakteristik von k gleich null ist. In Charakteristik $p > 0$ ist es möglich, dass wir weder einen strikten Isomorphismus noch irgendeinen anderen Isomorphismus zwischen F und $\mathbb{G}_a$ finden. Dafür wollen wir hier zwei Argumente geben. Ein allgemeiner Isomorphismus $f \in Hom_k(F, \mathbb{G}_a)$ hat die Form $f(T) \equiv a_1 T \pmod{\deg 2}$ mit $a_1 \neq 0$. Mit den gleichen Rechnungen wie oben erhalten wir, dass in diesem Fall

$$f'(Y) = a_1 \frac{1}{D_1F(0,Y)} \tag{1}$$

gelten muss. Wir schreiben $\frac{1}{D_1F(0,Y)} = \sum_{n=0}^{\infty} b_n Y^n \in k[[Y]]$.

Beim integrieren erhalten wir die Reihe $\sum_{n=0}^{\infty} \frac{1}{n+1} b_n Y^{n+1}$. Das multiplikative Inverse $\frac{1}{p}$ von p ist in einem Körper der Charakteristik $p > 0$ jedoch nicht wohldefiniert.
Ein anderes Argument, warum wir in Charakteristik $p > 0$ eventuell keinen Isomorphismus finden, ist folgendes: Wir schreiben $f(Y) = \sum_{n=0}^{\infty} a_n Y^n$ und erhalten wegen Gleichung 1:

$$\sum_{n=0}^{\infty} (n+1) a_{n+1} Y^n = \sum_{n=0}^{\infty} b_n a_1 Y^n.$$

Ein Koeffizientenvergleich ergibt: $(n+1)a_{n+1} = b_n a_1$. Für $n = mp - 1$ $(m \in \mathbb{N})$ erhalten wir in Charakteristik $p > 0$: $b_n a_1 = 0$. Falls für eines dieser n gilt $b_n \neq 0$, so folgt $a_1 = 0$. Dann ist f aber in keinem Fall invertierbar, also auch kein Isomorphismus. In Charakteristik null tauchen diese Probleme nicht auf.

Wir machen nun mit dem Beweis weiter und benutzen dieses f, um die Existenz zu zeigen. Es hat nach Konstruktion die Form $f(Y) = Y \pmod{\deg 2}$. Wir zeigen $G(X,Y) \coloneqq f(F(X,Y)) - f(X) - f(Y) = 0$. Nach dem vorangegangen Lemma 2.15 ist $f : F \to \mathbb{G}_a$ dann ein strikter Isomorphismus.
Aus der Assoziativität $F(X, F(Y,Z)) = F(F(X,Y), Z))$ folgt erneut mit der Kettenregel:

$$D_1F(X, F(Y,Z)) = D_1F(F(X,Y), Z) D_1F(X,Y).$$

Da $F(0,Y) = Y$, folgt mit $X = 0$:

$$D_1F(0, F(Y,Z)) = D_1F(Y,Z) D_1F(0,Y).$$

Ersetzen mit $\frac{1}{f'(Y)} = D_1F(0,Y)$ ergibt $\frac{1}{f'(F(Y,Z))} = \frac{D_1F(Y,Z)}{f'(Y)}$ bzw. $f'(Y) = D_1F(Y,Z)f'(F(Y,Z))$. Wenn wir die Variablen wechseln erhält man

$$f'(X) = f'(F(X,Y))D_1F(X,Y).$$

Jetzt leiten wir G partiell nach X ab, wobei wieder die Kettenregel benutzt wird:

$$D_1G(X,Y) = f'(F(X,Y))D_1F(X,Y) - f'(X) = f'(X) - f'(X) = 0.$$

Das heißt $G \in k[[Y]]$, bzw. $G(X,Y) = G(0,Y)$. Aber $G(0,Y) = f(F(0,Y)) - f(0) - f(Y) = f(Y) - 0 - f(Y) = 0$. Also ist $G = 0$, was zu zeigen war. □

Bemerkung 2.19. (siehe Aussagen in [Sil09, Kapitel IV.5])
Der eindeutig durch F bestimmte Homomorphismus $f : F \to \mathbb{G}_a$ aus 2.18 heißt *Logarithmus von* F. Er wird als $\log_F$ notiert. Nach Lemma 2.15 ist die Umkehrabbildung $f^{-1} : \mathbb{G}_a \to F$ ebenfalls eindeutig bestimmt. Diese wird als $\exp_F$ notiert. $F \in k\,[[X,Y]]$ lässt sich also eindeutig schreiben als

$$F(X,Y) = \exp_F(\mathbb{G}_a(\log_F(X), \log_F(Y))) = \exp_F(\log_F(X) + \log_F(Y)).$$

Beispielsweise ist $\log_{\mathbb{G}_m} = \log(1+T)$. Das haben wir in Beispiel 2.14 nachgerechnet.

Aus Theorem 2.18 ergibt sich noch eine wichtige Folgerung:

Korollar 2.20. [Sil09, Kapitel IV.5, Folgerung 5.3] Jedes formales Gruppengesetz $F \in k\,[[X,Y]]$ der Dimension eins über einem Körper k mit $char(k) = 0$ ist kommutativ.

Beweis. $\mathbb{G}_a$ ist kommutativ. Daher gilt:

$$F(X,Y) = \exp_F(\mathbb{G}_a(\log_F(X), \log_F(Y))) = \exp_F(\mathbb{G}_a(\log_F(Y), \log_F(X))) = F(Y,X).$$

□

Formale Gruppengesetze der Dimension n

Der Vollständigkeit halber führen wir in diesem Abschnitt formale Gruppengesetze der Dimension n ein. Da wir aber in dieser Arbeit nur eindimensionale formale Gruppengesetze behandeln werden, ist die Darstellung knapp gehalten und es werden keine Sätze bewiesen. Wir übernehmen die wichtigsten Punkte aus [Haz12, Kapitel 2]. Es seien im Folgenden $X = (X_1, \ldots, X_n)$ und $Y = (Y_1, \ldots, Y_n)$ jeweils Vektoren von n Variablen. Dann ist $R[[X,Y]] = R[[X_1, \ldots X_n, Y_1, \ldots Y_n]]$ der formale Potenzreihenring in $2n$ Variablen.

Definition 2.21. [Haz12, Kapitel 2] Sei R ein Ring. Ein *formales Gruppengesetz F der Dimension n* ist ein n-Tupel von Potenzreihen $F = (F_1, \ldots, F_n)$, $F_i \in R[[X,Y]]$ für alle $i = 1, \ldots, n$, sodass folgende Eigenschaften erfüllt sind:

(a) $F_i(X,Y) = X_i + Y_i \pmod{\deg 2}$ für alle $i = 1, \ldots, n$.

(b) $F_i(F(X,Y),Z) = F_i(X,F(Y,Z))$ für alle $i = 1, \ldots, n$.

Gilt zusätzlich $F_i(X,Y) = F_i(Y,X)$ für alle $i = 1,\dots,n$, so nennt man F *kommutativ*.

Betrachtet man $F(X,Y), X$ und Y als Spaltenvektoren, so schreiben sich (a) und (b) kürzer:

$$F(X,Y) \equiv X + Y \pmod{\deg 2},$$
$$F(F(X,Y),Z) = F(X,F(Y,Z)).$$

Beispiel 2.22. [Haz12, Kapitel 2] $\mathbb{G}_a^n(X,Y) = X+Y$ (*n-dimensionales formales additives Gruppengesetz*). Die Rechnung, die die Eigenschaften (a) und (b) nachweist, ist die gleiche wie in 2.2 für das eindimensionale formale additive Gruppengesetz.

Bemerkung 2.23. [Haz12, Kapitel 2] Auch für n-dimensionale formale Gruppengesetze $F \in R[[X,Y]]$ gilt $F(X,0) = X$ und $F(0,Y) = Y$. Der Beweis ist (wenn man die Schreibweise der Multiindizes benutzt) exakt analog wie im eindimensionalen Fall in Lemma 2.4. Wir können daraus folgern, dass alle Monome von F mit Grad ≥ 2 „gemixt“ sind, d.h. es kommt in jedem Monom mindestens ein X_i und ein Y_j vor, wobei $i,j \in \{1,\dots,n\}$.

Außerdem gibt es genau ein n-Tupel von Potenzreihen $i = (i_1,\dots,i_n)$ (wobei $i_k \in R[[T]]$ für alle $k = 1,\dots n$), sodass $F(T,i(T)) = F(i(T),T) = T$. Der Beweis ist wieder analog zum eindimensionalen Fall in Lemma 2.5.

Definition 2.24. [Haz12, Kapitel 2] Sei $F \in R[[X,Y]]$ ein n-dimensionales formales Gruppengesetz und sei $G \in R[[X,Y]]$ ein m-dimensionales formales Gruppengesetz. Ein *Homomorphismus* $f : F \to G$ ist ein m-Tupel von Potenzreihen $f = (f_1,\dots,f_m)$ in n Variablen (d.h. $f_i \in R[[T]]$ für alle $i = 1,\dots,m$), sodass $f(T) \equiv 0 \pmod{T}$ und

$$f(F(X,Y)) = G(f(X),f(Y)).$$

Man nennt F und G *isomorph über* R, falls es Homomorphismen $f : F \to G$ und $g : G \to F$ gibt, für die gilt:

$$f(g(T)) = g(f(T)) = T.$$

3 Klassifikation von eindimensionalen kommutativen formalen Gruppengesetzen über einem algebraisch abgeschlossenen Körper der Charakteristik p

In diesem Kapitel ist k stets ein Körper der Charakteristik $p > 0$. Außerdem sind alle formalen Gruppengesetze eindimensional und kommutativ.

Zuerst werden wir eine Invariante, die Höhe eines formalen Gruppengesetzes, einführen. Unter der zusätzlichen Voraussetzung, dass k algebraisch abgeschlossen ist, wollen wir dann beweisen, dass zwei formale Gruppengesetze $F, G \in k[[X, Y]]$ genau dann k-isomorph sind, wenn die Höhe von F gleich der Höhe von G ist. Wir halten uns dabei im Wesentlichen an die Darstellung in [Frö68, Kapitel 3]. Man beachte, dass wir zu Beginn in allgemeinen Körpern der Charakteristik $p > 0$ arbeiten, die Voraussetzung algebraisch abgeschlossen fordern wir erst ab Lemma 3.19.

Die Höhe eines formalen Gruppengesetzes

Die Aussagen unserer ersten zwei Lemmata in diesem Abschnitt (Lemma 3.1 und Lemma 3.3) werden in [Frö68, Kapitel 3] häufig benutzt, jedoch nicht bewiesen. Wir wollen das an dieser Stelle nachholen.

Lemma 3.1. Über k gilt:

$$(X+Y)^q = X^q + Y^q \quad \text{genau dann, wenn} \quad q = p^n, n \in \mathbb{N}.$$

Beweis. Sei zuerst $q = p^n$ mit $n \in \mathbb{N}$. Wir führen Induktion nach n. Für $n = 1$ erhalten wir mit der binomischen Formel:

$$(X+Y)^p = \sum_{k=0}^{p} \binom{p}{k} X^{p-k} Y^k.$$

Dabei gilt:

$$\binom{p}{k} = \frac{p!}{(p-k)!k!} = p\frac{(p-1)!}{(p-k)!k!}.$$

Für $0 < k < p$ teilt kein Faktor von $(p-k)!k!$ die Primzahl p. Wir sind in einem Körper der Charakteristik p, daher ist $\binom{p}{k} = 0$. Für $k \in \{0, p\}$ ist $\binom{p}{k} = 1$. Es folgt $(X+Y)^p = X^p + Y^p$.
Nun nehmen wir an, dass sie Aussage für $n \in \mathbb{N}$ bewiesen ist. Dann folgt für $n+1$:

$$(X+Y)^{p^{n+1}} = ((X+Y)^p)^{p^n} = (X^p + Y^p)^{p^n} = (X^p)^{p^n} + (Y^p)^{p^n} = X^{p^{n+1}} + Y^{p^{n+1}}.$$

Jetzt nehmen wir $q \neq p^n$ an. Dann ist $q = p^n s$ mit $s \in \mathbb{N}$ und $ggT(p, s) = 1$. Wir nehmen an, dass $(X+Y)^q = X^q + Y^q$ gilt. Daraus folgt:

$$(X^{p^n} + Y^{p^n})^s = ((X+Y)^{p^n})^s = (X+Y)^q = X^q + Y^q = X^{p^n s} + Y^{p^n s}.$$

Es folgt mit $X^{p^n} = T$ und $Y^{p^n} = U$:

$$(T+U)^s = T^s + U^s.$$

Dies ist ein Widerspruch, da $\binom{s}{1} = \frac{s!}{(s-1)!1!} = s \neq 0$ und $ggT(p,s) = 1$. □

Bemerkung 3.2. Dieses Lemma sagt auch aus: Für $q = p^n$ ist $\binom{q}{k}$ für $0 < k < q$ stets durch p teilbar.
Man sieht leicht, dass mit $q = p^n$ für alle $m \in \mathbb{N}$ gilt:

$$\left(\sum_{i=0}^{m} X_i\right)^q = \sum_{i=0}^{m} X_i^q.$$

Insbesondere erhalten wir:

$$\left(\sum_{i=0}^{\infty} X_i\right)^q = \sum_{i=0}^{\infty} X_i^q.$$

Für ein kommutatives formales Gruppengesetz $F \in k[[X,Y]]$ erinnern wir uns an die *Multiplikation mit n* aus Beispiel 2.13. Die Abbildung ist in diesem Kapitel sehr wichtig, daher wollen wir unsere bisherigen Kenntnisse an dieser Stelle wiederholen. $[n]_F : F \to F$ ist ein k-Homomorphismus und für alle $n \in \mathbb{N}$ induktiv definiert:

$$[0]_F(T) = 0, \quad [n+1]_F(T) = F([n]_F(T), T).$$

Außerdem haben wir $[n]_F(T) \equiv nT \pmod{\deg 2}$ nachgerechnet. Daraus folgt für in Charakteristik p:

$$[p]_F(T) \equiv 0 \pmod{\deg 2}.$$

Im folgenden Lemma beweisen wir zwei weitere Eigenschaften der Multiplikation mit n - Abbildung.

Lemma 3.3. Seien $F, G \in k[[X,Y]]$ formale Gruppengesetze. Dann gilt für alle $n \in \mathbb{N}$:

(i) $[n]_G \circ f = f \circ [n]_F$ für $f \in Hom_k(F,G)$.

(ii) $u^{-1} \circ [n]_F \circ u = [n]_{u^{-1} \circ F \circ u}$ für $u \in k[[X]]$ invertierbar.

Beweis. Wir zeigen beide Aussagen durch Induktion nach n und beginnen mit (i).
Da $[0]_G(X) = [0]_F(X) = 0$ und $f(0) = 0$ ist (i) klar für $n = 0$. Wenn (i) für $n \in \mathbb{N}$ stimmt, dann folgt für $n+1$:

$$\begin{aligned}
(f \circ [n+1]_F)(X) &= f(F([n]_F(X), X)) \\
&= G((f \circ [n]_F)(X), f(X)) \\
&= G(([n]_G \circ f)(X), f(X)) \\
&= ([n+1]_G \circ f)(X).
\end{aligned}$$

Dabei haben wir benutzt, dass f ein Homomorphismus ist.

Um Aussage (ii) zu bewiesen stellen wir zuerst fest, dass $u^{-1} \circ F \circ u$ nach Beispiel 2.12 wieder ein formales Gruppengesetz ist. Für $n = 0$ ist die Aussage klar. Wenn (ii) nun für $n \in \mathbb{N}$ stimmt, dann folgt für $n + 1$:

$$\begin{aligned}
[n+1]_{u^{-1}\circ F\circ u}(X) &= (u^{-1} \circ F \circ u)([n]_{u^{-1}\circ F\circ u}(X), X) \\
&= (u^{-1} \circ F \circ u)((u^{-1} \circ [n]_F \circ u)(X), X) \\
&= (u^{-1} \circ F)(([n]_F \circ u)(X), u(X)) \\
&= (u^{-1} \circ [n+1]_F \circ u)(X).
\end{aligned}$$

□

Wir kommen zur wichtigsten Definition des Kapitels:

Definition 3.4. [Sil09, Kapitel IV.7] Seien $F, G \in k[[X, Y]]$ formale Gruppengesetze, $f \in Hom_k(F, G)$. Die *Höhe von* f ist die größte natürliche Zahl $h \in \mathbb{N}_0$, sodass

$$f(T) = g(T^{p^h})$$

für ein $g \in k[[T]]$, wobei $p = char(k)$. Wir notieren sie als $ht(f)$. Falls $f = 0$ ist, so setze $ht(f) = \infty$.
Die *Höhe eines formalen Gruppengesetzes* F definieren wir durch die Höhe von $[p]_F \in Hom_k(F, F)$ und notieren sie als $Ht(F)$.

Bemerkung 3.5. Die Höhe eines formalen Gruppengesetzes ist nur für kommutative formale Gruppengesetze definiert, da im Allgemeinen nur für diese $[n]_F$ ein Homomorphismus ist. In diesem Kapitel sind aber alle formalen Gruppengesetze kommutativ, die Höhe ist also wohldefiniert.

Beispiel 3.6.

- Sei $F \in k[[X, Y]]$ ein formales Gruppengesetz und $f(X) = X$. In Beispiel 2.11 haben wir gezeigt, dass $f \in Hom_k(F, F)$ ist. Es gilt:

  $$f(X) = X = X^{p^0}.$$

  Daher ist $ht(f) = 0$.

- Für $\mathbb{G}_a \in k[[X, Y]]$ gilt: $Ht(\mathbb{G}_a) = \infty$.
  Wir zeigen per Induktion $[n]_{\mathbb{G}_a}(T) = nT$ für alle $n \in \mathbb{N}$. Daraus folgt $[p]_{\mathbb{G}_a}(T) = 0$, da $char(k) = p$ und das heißt $Ht(\mathbb{G}_a) = ht([p]_{\mathbb{G}_a}) = \infty$. Der Fall $n = 0$ ist klar, da $[0]_{\mathbb{G}_a}(T) = 0$ per Definition. Es gelte die Aussage für $n \in \mathbb{N}$, dann erhalten wir für $n + 1$:

  $$[n+1]_{\mathbb{G}_a}(T) = \mathbb{G}_a([n]_{\mathbb{G}_a}(T), T) = \mathbb{G}_a(nT, T) = nT + T = (n+1)T.$$

- Für $\mathbb{G}_m \in k[[X,Y]]$ gilt: $Ht(\mathbb{G}_m) = 1$.
  Wir zeigen wieder per Induktion: $[n]_{\mathbb{G}_m}(X) = (1+X)^n - 1$ für alle $n \in \mathbb{N}$. Daraus folgt mit Lemma 3.1:

$$[p]_{\mathbb{G}_m}(X) = (1+X)^p - 1 = 1^p + X^p - 1 = X^{p^1}.$$

  Das heißt $Ht(\mathbb{G}_m) = ht([p]_{\mathbb{G}_m}) = 1$.

  Für $n = 0$ ist die Aussage klar und für $n = 1$ gilt:

$$[1]_{\mathbb{G}_m}(X) = \mathbb{G}_m([0]_{\mathbb{G}_m}(X), X) = \mathbb{G}_m(0, X) = X = (1+X)^1 - 1.$$

  Wir nehmen an, dass die Aussage für $n \in \mathbb{N}$ wahr ist und erhalten für $n+1$:

$$\begin{aligned}
[n+1]_{\mathbb{G}_m}(X) &= \mathbb{G}_m([n]_{\mathbb{G}_m}(X), X) = \mathbb{G}_m((1+X)^n - 1, X) \\
&= (1+X)^n - 1 + X + ((1+X)^n - 1)X \\
&= (1+X)^n + (1+X)^n X - 1 \\
&= \sum_{i=0}^{n} \binom{n}{i} X^i + \sum_{i=0}^{n} \binom{n}{i} X^{i+1} - 1 \\
&= \sum_{i=0}^{n} \binom{n}{i} X^i + \sum_{i=1}^{n+1} \binom{n}{i-1} X^i - 1 \\
&= 1 + \sum_{i=1}^{n} \binom{n}{i} X^i + X^{n+1} + \sum_{i=1}^{n} \binom{n}{i-1} X^i - 1 \\
&= 1 + X^{n+1} + \sum_{i=1}^{n} \binom{n+1}{i} X^i - 1 \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} X^i - 1 = (1+X)^{n+1} - 1.
\end{aligned}$$

  Dabei haben wir im vorletzten Schritt die Identität $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$ benutzt.

Lemma 3.7. [Sil09, Kapitel IV.7] Seien $F, G \in k[[X,Y]]$ formale Gruppengesetze, $f \in Hom_k(F,G)$.

(i) Falls $f'(0) = 0$, dann ist $f(X) = \tilde{f}(X^p)$ für ein $\tilde{f} \in k[[X]]$.

(ii) Wir schreiben $f(X) = g(X^{p^h})$ für ein $g \in K[[X]]$ und $h = ht(f)$. Dann ist $g'(0) \neq 0$.

Das Lemma bedeutet, dass für einen Homomorphismus f der Höhe h gilt:

$$f(X) = aX^{p^h} + bX^{2p^h} + \ldots,$$

wobei der erste Koeffizient $a \neq 0$ ist.

Beweis. Der Beweis für (ii) orientiert sich an [Sil09, Kapitel IV.7], (i) beweisen wir anders. (i) Wegen Lemma 2.16 folgt aus $f'(0) = 0$, dass $f'(X) = 0$ ist. Für $f(X) = \sum_{n=1}^{\infty} a_n X^n$ ist also $\sum_{n=1}^{\infty} n a_n X^{n-1} = 0$, woraus $n a_n = 0$ für alle $n \geq 1$ folgt. Dies bedeutet, dass entweder $a_n = 0$ oder $n = pm$ für ein $m \in \mathbb{N}$. Insgesamt gilt:

$$f(X) = \sum_{m=1}^{\infty} a_{pm} X^{pm} = \tilde{f}(X^p) \text{ für } \tilde{f}(X) = \sum_{m=1}^{\infty} a_{pm} X^m.$$

Nun zeigen wir (ii). Sei $q = p^h$ und $F(X,Y) = \sum_{i,j\geq 0} a_{ij} X^i Y^j$das formale Gruppengesetz. Wir setzen $F^{(q)}(X,Y) := \sum_{i,j\geq 0} a_{ij}^q X^i Y^j$ und behaupten, dass dies ein formales Gruppengesetz ist. Es sind die Eigenschaften (a) und (b) aus Definition 2.1 nachzurechnen. Wir sehen sofort:

$$\begin{aligned} &\text{Aus } a_{10} = 1 \quad \text{folgt} \quad a_{10}^q = 1 \text{ (genauso für } a_{01}). \\ &\text{Aus } a_{00} = 0 \quad \text{folgt} \quad a_{00}^q = 0. \end{aligned}$$

Also ist $F^{(q)}(X,Y) = X + Y \pmod{\deg 2}$.
Um die Assoziativität zu zeigen, substituieren wir mit $S^q = X, T^q = Y$ und $U^q = Z$ und stellen zuerst fest, dass $F^{(q)}(X,Y) = F(S,T)^q$ gilt. Dabei benutzen wir Bemerkung 3.2:

$$\begin{aligned} F^{(q)}(X,Y) &= \sum_{i,j\geq 0} a_{ij}^q X^i Y^j = \sum_{i,j\geq 0} a_{ij}^q (S^q)^i (T^q)^j \\ &= \sum_{i,j\geq 0} \left(a_{ij} S^i T^j\right)^q = \left(\sum_{i,j\geq 0} a_{ij} S^i T^j\right)^q = F(S,T)^q. \end{aligned}$$

Daraus folgt wieder mit Bemerkung 3.2:

$$\begin{aligned} F^{(q)}(F^{(q)}(X,Y),Z) &= F^{(q)}(F(S,T)^q, U^q) = \sum_{i,j\geq 0} a_{ij}^q F(S,T)^{qi} U^{qj} \\ &= \sum_{i,j\geq 0} \left(a_{ij} F(S,T)^i U^j\right)^q = F(F(S,T),U)^q. \end{aligned}$$

Genauso ist $F^{(q)}(X, F^{(q)}(Y,Z)) = F(S, F(T,U))^q$ und deshalb ist $F^{(q)}(F^{(q)}(X,Y),Z) = F^{(q)}(X, F^{(q)}(Y,Z))$. $F^{(q)}$ ist somit ein formales Gruppengesetz.

Wir zeigen jetzt, dass g ein Homomorphismus von $F^{(q)}$ nach G ist. Da nach Voraussetzung $f \in Hom_k(F,G)$ und $f(X) = g(X^q)$ ist, gilt:

$$\begin{aligned} g(F^{(q)}(X,Y)) &= g(F(S,T)^q) = f(F(S,T)) \\ &= G(f(S), f(T)) = G(g(S^q), g(T^q)) = G(g(X), g(Y)). \end{aligned}$$

Nun nehmen wir $g'(0) = 0$ an. Wegen (i) wissen wir, dass es dann $\tilde{g} \in k[[X]]$ gibt, sodass $g(X) = \tilde{g}(X^p)$. Daraus folgt:

$$f(X) = g(X^{p^h}) = \tilde{g}(X^{p^{h+1}}).$$

Dies ist ein Widerspruch zu $ht(f) = h$. Daher muss $g'(0) \neq 0$ gelten. □

Aus diesem wichtigen Lemma wollen wir einige Folgerungen ziehen. Die erste ist, dass die Höhe eines formalen Gruppengesetzes, das über einem Körper mit positiver Charakteristik definiert ist, stets größer gleich eins ist.

Korollar 3.8. Sei $F \in k[[X,Y]]$ ein formales Gruppengesetz. Dann ist $Ht(F) \geq 1$.

Beweis. Wir haben nachgerechnet, dass $[p]_F(X) \equiv 0 \pmod{\deg 2}$ ist. Daher ist $[p]'_F(0) = 0$. Mit (i) aus Lemma 3.7 erhalten wir:

$$[p]_F(X) = g(X^p) \text{ für ein } g \in k[[X]].$$

Also ist $Ht(F) = ht([p]_F) \geq 1$. □

Die nächste Proposition ist auch eine Folgerung aus Lemma 3.7 und gibt uns eine Rechenregel für die Höhe von Homomorphismen.

Proposition 3.9. [Frö68, Kapitel 3, §2] Seien $F, G \in k[[X,Y]]$ formale Gruppengesetze, $f, g \in Hom_k(F,G)$. Dann ist

$$ht(f \circ g) = ht(f) + ht(g).$$

Beweis. Der Beweis ist nach [Frö68, Kapitel 3, §2]. Mit Lemma 3.7 (ii) erhalten wir:

$$f(X) = aX^{p^n} + \ldots \text{ ist eine Potenzreihe in } X^{p^n} \text{ mit } n = ht(f) \text{ und } a \neq 0.$$

Und genauso:

$$g(X) = bX^{p^m} + \ldots \text{ ist eine Potenzreihe in } X^{p^m} \text{ mit } m = ht(g) \text{ und } b \neq 0.$$

Daraus folgt, dass $f(g(X)) = ab^{p^n} X^{p^{n+m}} + \ldots$ eine Potenzreihe in $X^{p^{n+m}}$ ist. Das heißt: $ht(f \circ g) \geq n + m$. Andererseits ist $ab^{p^n} \neq 0$, da k nullteilerfrei ist. Somit erhalten wir auch: $ht(f \circ g) \leq n + m$ □

Korollar 3.10. [Frö68, Kapitel 3, §2] Seien $F, G \in k[[X,Y]]$ formale Gruppengesetze, $f, u \in Hom_k(F,G)$. Wenn u ein Isomorphismus ist, dann gilt:

$$ht(u) = 0 \quad \text{und} \quad ht(u \circ f \circ u^{-1}) = ht(f).$$

Beweis. Es ist $u \circ u^{-1} = id$. (Dabei ist $id(X) = X$, siehe Beispiel 2.11.) Daraus folgt mit Proposition 3.9:

$$0 = ht(id) = ht(u \circ u^{-1}) = \underbrace{ht(u)}_{\geq 0} + \underbrace{ht(u^{-1})}_{\geq 0}.$$

Daher ist $ht(u) = ht(u^{-1}) = 0$ und nochmal folgt aus Proposition 3.9:

$$ht(u \circ f \circ u^{-1}) = ht(u) + ht(f) + ht(u^{-1}) = ht(f).$$

□

Korollar 3.11. [Frö68, Kapitel 3, §2] Seien $F, G \in k[[X, Y]]$ formale Gruppengesetze mit $Ht(F) \neq Ht(G)$. Dann ist $Hom_k(F, G) = 0$.

Insbesondere sind F und G nicht isomorph. Oder andersherum gesagt: Wenn F und G isomorph sind, so müssen sie die gleiche Höhe haben.

Beweis. Wir beweisen wieder nach [Frö68, Kapitel 3, §2]. Sei $f \in Hom_k(F, G)$. Wegen Lemma 3.3 wissen wir: $f \circ [p]_F = [p]_G \circ f$. Es folgt mit Proposition 3.9:

$$ht(f) + Ht(F) = Ht(G) + ht(f).$$

Da $Ht(F) \neq Ht(G)$ muss $ht(f) = \infty$. Also ist $f = 0$. □

Beispiel 3.12. Seien $\mathbb{G}_a, \mathbb{G}_m \in k[[X, Y]]$ das formale additive und formale multiplikative Gruppengesetz. Dann sind $\mathbb{G}_a$ und $\mathbb{G}_m$ nicht isomorph. Wir haben nämlich in Beispiel 3.6 nachgerechnet: $Ht(\mathbb{G}_a) = \infty \neq 1 = Ht(\mathbb{G}_m)$.

Ein Satz von Lazard und seine Folgerungen

In diesem Abschnitt gelten die Sätze und Lemmata im Allgemeinen auch über einem kommutativen Ring mit Einselement. Uns interessiert aber nur der Fall für einen Körper mit positiver Charakteristik.

Definition 3.13. [Frö68, Kapitel 3, §1] Wir definieren die *Lazard-Polynome* B_n und $C_n \in k[X, Y]$ für alle $n \in \mathbb{N}$:

$$\begin{aligned} B_n(X, Y) &:= (X + Y)^n - X^n - Y^n, \\ C_n(X, Y) &:= \varepsilon_n B_n(X, Y), \text{ wobei } \varepsilon_n = \begin{cases} \frac{1}{p'} & n = (p')^r, r > 0, p' \text{ prim}, \\ 1 & \text{sonst.} \end{cases} \end{aligned}$$

Da wir in einem Körper der Charakteristik $p > 0$ sind, kann man sich an dieser Stelle die Frage nach der Wohldefiniertheit von C_n stellen. Für $n \neq p^r$ ist dies klar, da jede Primzahl $p' \neq p$ invertierbar in k ist. Das multiplikative Inverse $\frac{1}{p'}$ existiert also.
Für $n = p^r$ betrachten wir:

$$B_n(X, Y) = \sum_{k=1}^{n-1} \binom{n}{k} X^{n-k} Y^k.$$

In Bemerkung 3.2 haben wir festgestellt, dass in $\binom{n}{k}$ für $0 < k < n$ stets der Faktor p vorkommt. Wir können in $C_n = \frac{1}{p} B_n$ also kürzen und somit ist C_n wohldefiniert.

Satz 3.14 (Lazard)**.** [Frö68, Kapitel 3, §1] Seien $F, G \in k[[X, Y]]$ formale Gruppengesetze über k mit $F \equiv G \pmod{\deg n}$. Dann ist

$$F \equiv G + aC_n \pmod{\deg n + 1}$$

für ein $a \in k$.

Beweisskizze. Der Beweis des Satzes ist elementar, aber sehr lang und würde im Umfang über den Rahmen dieser Arbeit hinausgehen. Da der Satz aber zentral ist und wir ihn im Folgenden oft verwenden werden, wollen wir zumindest eine Beweisskizze geben. Diese orientiert sich am Beweis von Theorem 1 in [Frö68, Kapitel 3, §1], wo auch der ausführliche Beweis nachzulesen ist.

Wir schreiben $F \equiv G + \Gamma \pmod{\deg n + 1}$, wobei $\Gamma \in k[[X, Y]]$ ein homogenes Polynom vom Grad n ist. Das Polynom Γ erfüllt dann die folgenden Eigenschaften:

$$(P) \begin{cases} \Gamma(X, Y) = \Gamma(Y, X), \\ \Gamma(X, 0) = 0 = \Gamma(0, X), \\ \Gamma(X, Y) + \Gamma(X + Y, Z) = \Gamma(X, Y + Z) + \Gamma(Y, Z). \end{cases}$$

Nun reicht zu zeigen, dass jedes homogene Polynom Γ von Grad n, dass die Eigenschaften (P) erfüllt, von der Form aC_n für ein $a \in k$ ist. Dazu ist es sinnvoll, die Menge der homogenen Polynome von Grad n als k-Vektorraum aufzufassen und zu zeigen, dass die Menge aller Polynome, die zusätzlich die Bedingungen (P) erfüllen, einen Untervektorraum S der Dimension ≤ 1 bildet. Wenn dies bewiesen ist, stellen wir fest, dass C_n in S liegt und rechnen nach, dass $C_n \neq 0$ gilt. Es ist somit (C_n) eine Basis von S wir erhalten:

$$\Gamma = aC_n \text{ für ein } a \in k.$$

Dass S für alle $n \in \mathbb{N}$ ein Untervektorraum ist, ist leicht zu sehen. Allerdings ist es aufwendig, die Dimensionsaussage zu zeigen. Dazu schreiben wir

$$\Gamma(X, Y) = \sum_{r=0}^{n} a_r X^r Y^{n-r} \in S$$

und nutzen die Eigenschaften in (P) aus. Schlussendlich erhalten wir, dass durch die Kenntnis von a_1 schon alle anderen Koeffizienten bestimmt sind. Das beendet den Beweis. Aus dem Satz folgen mit leichten Rechnungen zwei Lemmata, die wir später noch oft zitieren werden.

Lemma 3.15. [Frö68, Kapitel 3, §1] Seien $F, G \in k[[X, Y]]$ formale Gruppengesetze und $F \equiv G + aB_n \pmod{\deg n + 1}$ für ein $a \in k$. Dann gibt es ein invertierbares $f \in k[[X]]$ mit $f(X) \equiv X \pmod{\deg n}$, sodass

$$f(F(f^{-1}(X), f^{-1}(Y))) \equiv G(X, Y) \pmod{\deg n + 1}.$$

In diesem Fall schreiben wir wieder abkürzend $f \circ F \circ f^{-1} \equiv G \pmod{\deg n + 1}$.

Beweis. Der Beweis ist nach [Frö68, Kapitel 3, §1]. Setze $f(X) \equiv X - aX^n \pmod{\deg n + 1}$. Wir zeigen mit diesem f:

$$f(F(X, Y))) \equiv G(f(X), f(Y)) \pmod{\deg n + 1}.$$

Da f nach Lemma 2.15 invertierbar ist, zeigt dies unsere Behauptung. Wir rechnen modulo $\deg n + 1$:

$$\begin{aligned} f(F(X,Y)) &\equiv F(X,Y) - a(X+Y)^n \\ &\equiv G(X,Y) + aB_n(X,Y) - a(X+Y)^n \\ &\equiv G(X,Y) + a(X+Y)^n - aX^n - aY^n - a(X+Y)^n \\ &\equiv G(X,Y) - aX^n - aY^n \\ &\equiv G(X - aX^n, Y - aY^n) \\ &\equiv G(f(X), f(Y)). \end{aligned}$$

□

Lemma 3.16. [Frö68, Kapitel 3, §1] Seien $F, G \in k[[X,Y]]$ formale Gruppengesetze und $F \equiv G + aC_n \pmod{\deg n + 1}$ für ein $a \in k$. Dann gilt für alle $m \in \mathbb{N}$:

$$[m]_F(X) \equiv [m]_G(X) + a\varepsilon_n(m^n - m)X^n \pmod{\deg n + 1}.$$

In Definition 3.13 haben wir ε_n definiert. Man kann sich wieder die Frage stellen, ob der Ausdruck $\varepsilon_n(m^n - m)$ wohldefiniert ist für $n = p^r$. Dies folgt aus dem kleinen Satz von Fermat, der für alle $m \in \mathbb{N}$ aussagt: $m^p \equiv m \pmod{p}$. Mit einer Induktion über r zeigt man leicht, dass auch $m^{(p^r)} \equiv m \pmod{p}$ gilt, also $m^{(p^r)} - m \equiv 0 \pmod{p}$. Somit ist die natürliche Zahl $m^{(p^r)} - m$ ein Vielfaches von p. Der Ausdruck $\frac{1}{p}(m^{(p^r)} - m)$ ist in einem Körper der Charakteristik p somit wohldefiniert, da wir p herauskürzen.

Beweis. Der Beweis orientiert sich an [Frö68, Kapitel 3, §1]. Wir halten ein $n \in \mathbb{N}$ fest und führen Induktion nach m. Für $m = 1$ ist $[1]_F(X) = [1]_G(X) = X$ und $1^n - 1 = 0$, die Aussage ist also wahr. Wir nehmen an, sie gilt für $m \in \mathbb{N}$ und schreiben $l_m(X) = a\varepsilon_n(m^n - m)X^n$. Für $m + 1$ erhalten wir modulo $\deg n + 1$:

$$\begin{aligned} [m+1]_F(X) &= F([m]_F(X), X) \\ &\overset{\text{n.V.}}{\equiv} G([m]_F(X), X) + aC_n([m]_F(X), X) \\ &\overset{\text{Def. } C_n}{\equiv} G([m]_F(X), X) + aC_n(mX, X) \\ &\overset{\text{I.V.}}{\equiv} G([m]_G(X) + l_m(X), X) + aC_n(mX, X) \\ &\overset{\text{G fGG}}{\equiv} G([m]_G(X), X) + l_m(X) + aC_n(mX, X) \\ &\equiv [m+1]_G(X) + l_m(X) + aC_n(mX, X). \end{aligned}$$

Es bleibt $l_{m+1}(X) = l_m(X) + aC_n(mX, X)$ zu zeigen. Wir stellen fest:

$$B_n(mX, X) = (mX + X)^n - (mX)^n - X^n = ((m+1)^n - m^n - 1)X^n.$$

Daraus ergibt sich:

$$C_n(mX, X) = \varepsilon_n((m+1)^n - m^n - 1)X^n.$$

Daraus folgt:

$$\begin{aligned} l_m(X) + aC_n(mX, X) &= l_m(X) + a\varepsilon_n((m+1)^n - m^n - 1)X^n \\ &\overset{\text{I.V.}}{=} a\varepsilon_n(m^n - m)X^n + a\varepsilon_n((m+1)^n - m^n - 1)X^n \\ &= a\varepsilon_n(m^n - m + (m+1)^n - m^n - 1)X^n \\ &= a\varepsilon_n((m+1)^n - (m+1))X^n \\ &= l_{m+1}. \end{aligned}$$

□

Formale Gruppengesetze unendlicher Höhe

Wir wollen formale Gruppengesetze mit endlicher und unendlicher Höhe getrennt bearbeiten. In diesem Abschnitt zeigen wir, dass alle formalen Gruppengesetze unendlicher Höhe über einem Körper mit positiver Charakteristik isomorph sind. Dies ist der einfachere Teil. Gruppengesetze endlicher Höhe behandeln wir im nächsten Abschnitt, das ist um einiges komplizierter.

Satz 3.17. [Frö68, Kapitel 3, §1] Sei $F \in k[[X, Y]]$ ein formales Gruppengesetz. Dann ist F k-isomorph zu $\mathbb{G}_a$ genau dann wenn $Ht(F) = \infty$.

Da $Ht(\mathbb{G}_a) = \infty$ ist, sind somit alle formalen Gruppengesetze unendlicher Höhe k-isomorph.

Beweis. In [Frö68, Kapitel 3, §1] wird dies etwas allgemeiner bewiesen, wir beschränken uns aber auf den für uns relevanten Fall.

Wenn F und $\mathbb{G}_a$ isomorph sind, so folgt mit 3.11, dass sie die gleichen Höhen haben müssen. Da $Ht(\mathbb{G}_a) = \infty$ ist auch $Ht(F) = \infty$.

Nun nehmen wir $Ht(F) = \infty$ an und konstruieren eine Folge $g_n \in k[T]$, sodass

$$\begin{aligned} g_n \circ F &\equiv \mathbb{G}_a \circ g_n \pmod{\deg n + 1}, \\ g_n &\equiv g_{n-1} \pmod{\deg n}. \end{aligned}$$

Wir definieren $g \in R[[T]]$ durch $g \equiv g_n(T) \pmod{\deg n + 1}$. Dieses g erfüllt dann die Identität $g \circ F = \mathbb{G}_a \circ g$ und ist somit ein Homomorphismus von F nach $\mathbb{G}_a$. Außerdem wird durch unsere nachfolgende Wahl von g_1 sichergestellt, dass jedes g_n und somit auch g invertierbar ist (Lemma 2.15).

Wir definieren $g_1(X) = X$. Die Aussage folgt aus $F(X, Y) = X + Y \pmod{\deg 2}$. Nun nehmen wir an, dass wir $g_1, \ldots, g_{n-1}$ schon konstruiert haben und somit gilt:

$$g_{n-1} \circ F \circ g_{n-1}^{-1} = H \equiv \mathbb{G}_a \pmod{\deg n}.$$

Mit Satz 3.14 von Lazard folgt $H \equiv \mathbb{G}_a + aC_n \pmod{\deg n + 1}$ für ein $a \in k$. Wir stellen sogar folgende Behauptung auf:

$$\text{Es gibt } b \in k, \text{ sodass } H \equiv \mathbb{G}_a + bB_n \pmod{\deg n + 1}.$$

Sei $r \in \mathbb{N}$ und $n \neq p^r$. Dann folgt $aC_n = bB_n$, da alle Primelemente $p' \neq p$ Einheiten in k sind. (Man betrachte dazu Definition 3.13 der Lazard-Polynome.)
Für $n = p^r$ behaupten wir, dass $aC_n = 0$ ist. Mit Lemma 3.16 gilt nämlich:

$$[p]_H(X) \equiv \underbrace{[p]_{\mathbb{G}_a}(X)}_{=0} + a\frac{1}{p}(p^n - p)X^n \pmod{\deg n + 1}.$$

Da H und F nach unserer Konstruktion isomorph sind, folgt mit Korollar 3.11, dass sie die gleiche Höhe haben. Also ist $Ht(H) = \infty$, bzw. $[p]_H = 0$. Insgesamt haben wir somit:

$$0 \equiv a(\underbrace{p^{n-1}}_{=0} - 1)X^n = a(-1)X^n \pmod{\deg n + 1}.$$

Daher ist $a = 0$ und die Behauptung ist bewiesen.

Nun gibt es wegen Lemma 3.15 ein invertierbares $f \in k[X]$ mit $f(X) \equiv X \pmod{\deg n}$, sodass $f \circ H \circ f^{-1} \equiv \mathbb{G}_a \pmod{\deg n + 1}$. Wir setzen $g_n := f \circ g_{n-1}$. Dann gilt: $g_n = f \circ g_{n-1} \equiv g_{n-1} \pmod{\deg n}$ und modulo $\deg n + 1$:

$$\begin{aligned} g_n \circ F \circ g_n^{-1} &= f \circ g_{n-1} \circ F \circ g_{n-1}^{-1} \circ f^{-1} \\ &= f \circ H \circ f^{-1} \\ &\equiv \mathbb{G}_a. \end{aligned}$$

Dies beendet den Induktionsschritt und somit den Beweis. □

Formale Gruppengesetze endlicher Höhe

Ab jetzt sei $h \geq 1$ eine natürliche Zahl und $q = p^h$, wobei $p > 0$ weiterhin die Charakteristik von k ist. Wir erinnern uns an Korollar 3.8, in dem wir bewiesen haben, dass die Höhe eines formalen Gruppengesetzes über einem Körper mit positiver Charakteristik stets größer gleich eins ist.

Lemma 3.18. [Frö68, Kapitel 3, §2] Sei $F \in k[[X, Y]]$ ein formales Gruppengesetz der endlichen Höhe h. Dann ist F k-isomorph zu einem formalen Gruppengesetz $G \in k[[X, Y]]$ der Form

$$G(X, Y) \equiv X + Y + cC_q(X, Y) \pmod{\deg q + 1} \text{ mit } c \in k^*.$$

Dabei meinen wir mit C_q das Lazard-Polynom mit $q = p^h$ aus Definition 3.13.

Beweis. Der Beweis orientiert sich an [Frö68, Kapitel 3, §2], wo er allerdings um einiges knapper ist.
Wir wissen $F(X, Y) \equiv X+Y \pmod{\deg 2}$ und nehmen an: $F(X, Y) \equiv X+Y \pmod{\deg n}$ mit $n < q$. Mit Satz 3.14 von Lazard folgt $F \equiv \mathbb{G}_a + cC_n \pmod{\deg n + 1}$ für ein $c \in k$. Es gilt sogar folgende Behauptung:

$$\text{Es gibt } b \in k, \text{ sodass } F \equiv \mathbb{G}_a + bB_n \pmod{\deg n + 1}$$

Sei $r \in \mathbb{N}$ und $n \neq p^r$. Dann folgt $cC_n = bB_n$, da alle Primelemente $p' \neq p$ Einheiten in k sind. (Man betrachte dazu wieder Definition 3.13 der Lazard-Polynome.)
Für $n = p^r$ mit $r < h$ ist $cC_n = 0$. Mit Lemma 3.16 gilt nämlich:

$$[p]_F(X) \equiv \underbrace{[p]_{\mathbb{G}_a}(X)}_{=0} + c\frac{1}{p}(p^n - p)X^n \pmod{\deg n + 1}.$$

Also:

$$[p]_F(X) \equiv c(\underbrace{p^{n-1}}_{=0} - 1)X^n = c(-1)X^n \pmod{\deg n + 1}.$$

Nach Voraussetzung ist $Ht(F) = h$ und somit $[p]_F(X) = aX^{p^h} + \ldots = aX^q + \ldots \equiv 0 \pmod{\deg q}$. Dies gilt insbesondere auch modulo $\deg n + 1$, da $n < q$. Wir erhalten $0 = c(-1)X^n \pmod{\deg n + 1}$, und das bedeutet $c = 0$. Die Behauptung ist bewiesen.

In Lemma 3.15 haben wir gezeigt, dass es ein $f \in k[X]$ gibt mit $f(X) \equiv X \pmod{\deg n}$, sodass $f(F(f^{-1}(X), f^{-1}(Y))) \equiv X + Y \pmod{\deg n + 1}$. Wenn wir diesen Schritt für $n < q$ wiederholen, erhalten wir, dass F k-isomorph ist zu $G \equiv X + Y \pmod{\deg q}$. Nun wenden wir noch einmal den Satz von Lazard (3.14) an und erhalten $G \equiv X + Y + cC_q \pmod{\deg q + 1}$. Es bleibt $c \neq 0$ zu zeigen.

Sei $c = 0$, also $G \equiv \mathbb{G}_a \pmod{\deg q + 1}$. Dann folgt mit Lemma 3.16:

$$[p]_G \equiv \underbrace{[p]_{\mathbb{G}_a}}_{=0} \pmod{\deg q + 1}.$$

Das heißt aber $Ht(G) = ht([p]_G) > h$. Insbesondere ist $Ht(G) \neq Ht(F)$, also sind G und F nicht isomorph. Dies ist ein Widerspruch. □

Bis hierhin waren alle Sätze und Lemmata über einem beliebigen Körper der Charakteristik $p > 0$ gültig. Für alle folgenden Behauptungen brauchen wir jedoch, dass k zusätzlich algebraisch abgeschlossen ist. Zunächst zeigen wir folgendes Hilfslemma:

Lemma 3.19. [Frö68, Kapitel 3, §2] Sei k algebraisch abgeschlossen und $g \in k[[X]]$ eine Potenzreihe mit $g(X) = f(X^q)$, $g(0) = 0$ und $f'(0) \neq 0$. Dann gibt es eine invertierbare Potenzreihe $v \in k[[X]]$, sodass

$$(v^{-1} \circ g \circ v)(X) = X^q.$$

Beweis. Wir folgen der Darstellung in [Frö68, Kapitel 3, §2] und zeigen zuerst, dass es $v_1 \in k[[X]]$ gibt, sodass $v_1^{-1} \circ g \circ v_1 \equiv X^q \pmod{\deg 2q}$ ist. Nach Voraussetzung ist $g(X) \equiv aX^q \pmod{\deg q + 1}$ mit $a \neq 0$. Da k algebraisch abgeschlossen ist, gibt es ein

$c \in k$, sodass $c^{1-q} = a$. Setze $v_1 \coloneqq cX$ und $g_2(X) \coloneqq (v_1^{-1} \circ g \circ v_1)(X)$. Es ist $v_1^{-1} = c^{-1}X$. Wir rechnen modulo $\deg q + 1$:

$$\begin{aligned} g_2(X) &= v_1^{-1}(g(cX)) \\ &\equiv v_1^{-1}(ac^q X^q) \\ &\equiv v_1^{-1}(\underbrace{c^{1-q}c^q}_{=c} X^q) \\ &\equiv c^{-1}cX^q \equiv X^q. \end{aligned}$$

Das gilt auch modulo $\deg 2q$, da g_2 ebenfalls eine Potenzreihe in X^q ist.

Jetzt zeigen wir induktiv für alle $r \geq 2$: Wenn $g_r(X)$ eine Potenzreihe in X^q ist mit $g_r(X) \equiv X^q \pmod{\deg rq}$, dann finden wir ein $b \in k$, sodass für $v_r(X) = X + bX^r$ gilt:

$$(v_r^{-1} \circ g_r \circ v_r)(X) \equiv X^q \pmod{\deg(r+1)q}.$$

Wir setzen $g_{r+1} \coloneqq v_r^{-1} \circ g_r \circ v_r = v_r^{-1} \circ \cdots \circ v_1^{-1} \circ g \circ v_1 \circ \cdots \circ v_r$. Dies ist wieder eine Potenzreihe in X^q und es ist $g_{r+1} \equiv X^q \pmod{\deg(r+1)q}$. Außerdem erhalten wir eine unendliche Kette $v_1 \circ v_2 \circ \ldots$, für die gilt:

$$(v_1 \circ \cdots \circ v_{r-1} \circ v_r)(X) = (v_1 \circ \cdots \circ v_{r-1})(X + bX^r) \equiv (v_1 \circ \cdots \circ v_{r-1})(X) \pmod{\deg r}.$$

Wir können also $v \in k[[X]]$ durch $v(X) \equiv (v_1 \circ \cdots \circ v_{r-1})(X) \pmod{\deg r}$ definieren und erhalten, was zu zeigen war:

$$(v^{-1} \circ g \circ v)(X) = X^q.$$

Wir führen nun den Induktionsschritt durch. Nach Voraussetzung ist $g_r(X) \equiv X^q + aX^{rq} \pmod{\deg rq + 1}$. Wir rechnen modulo $\deg rq + 1$:

$$\begin{aligned} g_r(v_r(X)) &\equiv v_r(X)^q + a v_r(X)^{rq} \\ &\equiv (X + bX^r)^q + a(X + bX^r)^{rq} \\ &\overset{\text{Lemma 3.1}}{\equiv} X^q + b^q X^{rq} + aX^{rq} \\ &\equiv X^q + (a + b^q)X^{rq}. \end{aligned}$$

$$v_r(X^q) \equiv X^q + bX^{rq}.$$

Um nun $g_r(v_r(X)) = v_r(X^q)$ zu zeigen, ist die Gleichung

$$b^q - b + a = 0$$

zu lösen. Da k algebraisch abgeschlossen ist, gibt es eine Lösung $b \in k$. Wir erhalten:

$$(v_r^{-1} \circ g_r \circ v_r)(X) \equiv X^q \pmod{\deg rq + 1}.$$

Das gilt auch modulo $\deg(r+1)q$, da $v_r^{-1} \circ g_r \circ v_r$ wieder eine Potenzreihe in X^q ist. $\square$

Definition 3.20. [Frö68, Kapitel 3, §2] Sei k algebraisch abgeschlossen und $F \in k[[X,Y]]$ ein formales Gruppengesetz mit endlicher Höhe h. Das formale Gruppengesetz F ist in *Normalform*, falls gilt:

(i) $[p]_F(X) = X^q$ $(q = p^h)$,

(ii) $F(X,Y) \equiv X + Y + cC_q(X,Y) \pmod{\deg q + 1}$ für ein $c \in k^*$.

Wir zeigen in der nächsten Proposition (3.23), dass in einem algebraisch abgeschlossenen Körper mit positiver Charakteristik jedes formale Gruppengesetz endlicher Höhe isomorph zu einem formalen Gruppengesetz in Normalform ist. Der Beweis ist etwas technisch, wir zeigen zur Vorbereitung zwei Lemmata.
Da k ein algebraisch abgeschlossener Körper mit Charakteristik p ist, enthält er einen endlichen Körper mit $q = p^h$ Elementen (Nullstellen von $X^q - X$). Dieser Körper ist isomorph zu $\mathbb{F}_q$, wir können also schreiben: $\mathbb{F}_q = \{a \in k | a^q = a\}$. Wir sagen, dass eine Potenzreihe über $\mathbb{F}_q$ definiert ist, wenn ihre Koeffizienten in $\mathbb{F}_q$ liegen.

Lemma 3.21. Sei k algebraisch abgeschlossen. Eine formale Potenzreihe $g(X) = g(X_1, \ldots, X_n) \in k[[X_1, \ldots, X_n]]$ ist genau dann über $\mathbb{F}_q$ definiert, wenn $g(X)^q = g(X^q)$ gilt. Dabei ist $X^q = (X_1^q, \ldots, X_n^q)$.

Insbesondere sagt dieses Lemma aus, dass für $g \in \mathbb{F}_q[[X]]$ gilt: $g(X)^q = g(X^q)$.

Beweis. Da $\mathbb{F}_q = \{a \in k | a^q = a\}$, erhalten wir für $g(X) = \left(\sum a_{\underline{i}} X^{\underline{i}}\right) \in \mathbb{F}_q[[X]]$ aus Bemerkung 3.2:

$$g(X)^q = \left(\sum a_{\underline{i}} X^{\underline{i}}\right)^q \overset{3.2}{=} \sum a_{\underline{i}}^q (X^{\underline{i}})^q = \sum a_{\underline{i}} (X^q)^{\underline{i}} = g(X^q).$$

Sei jetzt $g(X) \in k[[X]]$ und $g(X)^q = g(X^q)$. Es folgt:

$$\sum a_{\underline{i}}^q (X^q)^{\underline{i}} = \sum \left(a_{\underline{i}} X^{\underline{i}}\right)^q \overset{3.2}{=} \left(\sum a_{\underline{i}} X^{\underline{i}}\right)^q = g(X)^q = g(X^q) = \sum a_{\underline{i}} (X^q)^{\underline{i}}.$$

Somit muss $a_{\underline{i}}^q = a_{\underline{i}}$ für alle $\underline{i} \in \mathbb{N}_0^n$ gelten und das heißt, dass g über $\mathbb{F}_q$ definiert ist. □

Unser nächstes Lemma zeigt, dass wir mit formalen Gruppengesetzen in Normalform über $\mathbb{F}_q$, an Stelle von k, arbeiten können.

Lemma 3.22. [Frö68, Kapitel 3, §2] Sei k algebraisch abgeschlossen, $F \in k[[X,Y]]$ ein formales Gruppengesetz mit endlicher Höhe h und $[p]_F(X) = X^q$. Dann ist F über $\mathbb{F}_q$ definiert und jeder Endomorphismus $f \in Hom_k(F,F)$ ist über $\mathbb{F}_q$ definiert.

Beweis. Der Beweis orientiert sich an [Frö68, Kapitel 3, §2], er ist dort allerdings wieder sehr knapp. Da $[p]_F \in Hom_k(F,F)$ gilt:

$$[p]_F(F(X,Y)) = F([p]_F(X), [p]_F(Y)).$$

Dies ist äquivalent zu $F(X,Y)^q = F(X^q, Y^q)$. Wir wenden das vorangegangene Korollar an und erhalten, dass F über $\mathbb{F}_q$ definiert ist.

Weiter gilt für $f \in Hom_k(F,F)$ mit Lemma 3.3:

$$[p]_F \circ f = f \circ [p]_F.$$

Dies bedeutet $f(X)^q = f(X^q)$ und mit unserem Korollar folgt, dass f über $\mathbb{F}_q$ definiert ist. □

Wir sind jetzt so weit, dass wir die angekündigte Proposition zeigen können. Dort bringen wir die Lemmata 3.18, 3.19 und 3.22 zusammen. Wir haben nur für Lemma 3.19 und Lemma 3.22 gefordert, dass k algebraisch abgeschlossen ist. Lemma 3.18 gilt allgemein über Körpern der Charakteristik $p > 0$, also insbesondere auch für $\mathbb{F}_q$. Für Potenzreihen $v \in \mathbb{F}_q$ gilt $v(X)^q = v(X^q)$ (siehe Lemma 3.21). Dies wollen wir ausnutzen, um die Proposition zu beweisen.

Proposition 3.23. [Frö68, Kapitel 3, §2] Sei k algebraisch abgeschlossen. Dann ist jedes formale Gruppengesetz $F \in k[[X,Y]]$ mit endlicher Höhe h k-isomorph zu einem formalen Gruppengesetz in Normalform.

Beweis. Wir halten uns wieder an die Darstellung in [Frö68, Kapitel 3, §2]. Wir haben gezeigt, dass $[p]_F$ die Voraussetzungen von Lemma 3.19 erfüllt. Damit erhalten wir ein invertierbares $u \in k[[X]]$, sodass

$$u^{-1} \circ [p]_F \circ u = X^q.$$

Nun benutzen wir Lemma 3.3 (ii):

$$u^{-1} \circ [p]_F \circ u = [p]_{u^{-1} \circ F \circ u}.$$

Außerdem ist $u^{-1} \circ F \circ u$ nach Beispiel 2.12 ein formales Gruppengesetz über k und k-isomorph zu F. Wir können somit $[p]_F = X^q$ annehmen. Nun benutzen wir das vorangegangene Lemma und erhalten, dass F über $\mathbb{F}_q$ definiert ist. $\mathbb{F}_q$ ist ein Körper der Charakteristik p. Somit existiert nach Lemma 3.18 ein invertierbares $v \in \mathbb{F}_q[[X]]$, sodass

$$(v^{-1} \circ F \circ v)(X,Y) \equiv X + Y + cC_q \pmod{\deg q + 1} \text{ mit } c \neq 0.$$

Da v über $\mathbb{F}_q$ definiert ist, gilt $v(X)^q = v(X^q)$. Wir erhalten:

$$\begin{aligned} [p]_{v^{-1} \circ F \circ v}(X) &\overset{3.3}{=} (v^{-1} \circ [p]_F \circ v)(X) \\ &= v^{-1}(v(X)^q) \\ &= v^{-1}(v(X^q)) \\ &= (v^{-1} \circ v \circ [p]_F)(X) \\ &= [p]_F(X) = X^q. \end{aligned}$$

Die formale Potenzreihe $v^{-1} \circ F \circ v$ ist also ein formales Gruppengesetz in Normalform und ist (wieder mit Beispiel 2.12) isomorph zu F. □

Wir können ab jetzt annehmen, dass alle formalen Gruppengesetze endlicher Höhe h über einem algebraisch abgeschlossenen Körper mit Charakteristik $p > 0$ in Normalform sind.

Wir definieren einen k-Vektorraum M mit der gewöhnlichen Addition als die Menge aller Polynome der Form $a(X) = \sum_{i=0}^{h-1} a_i X^{p^i}$, wobei $a_i \in k$.

Außerdem definieren wir für $f, g \in Hom_k(F, G)$ folgende Notation:

$$(f +_G g)(X) \coloneqq G(f(X), g(X)).$$

Proposition 3.24. [Frö68, Kapitel 3, §2] Sei k algebraisch abgeschlossen und seien $F, G \in k[[X, Y]]$ formale Gruppengesetze in Normalform der gleichen (endlichen) Höhe h. Wir definieren:

$$\begin{aligned} \phi : Hom_k(F, G) &\longrightarrow M \\ f(X) = \sum_{j=1}^{\infty} f_j X^j &\longmapsto \phi(f)(X) = \sum_{j=1}^{q-1} f_j X^j \end{aligned}$$

Die Abbildung ϕ ist wohldefiniert und es gelten die folgenden Eigenschaften:

(i) $\phi(f +_G g) = \phi(f) + \phi(g)$,

(ii) ϕ ist surjektiv.

Beweis. Der Beweis orientiert sich auch diesmal an [Frö68, Kapitel 3, §2]. Zuerst ist die Wohldefiniertheit von ϕ zu zeigen, also $\phi(f) \in M$ für $f \in Hom_k(F, G)$.
Wir betrachten (ii) in Definition 3.20 eines formalen Gruppengesetzes in Normalform, woraus $F(X, Y) \equiv X + Y \equiv G(X, Y) \pmod{\deg q}$ folgt. Da f ein Homomorphismus ist, erhalten wir:

$$f(X + Y) \equiv f(F(X, Y)) = G(f(X), f(Y)) \equiv f(X) + f(Y) \pmod{\deg q}.$$

Dies bedeutet:

$$\sum_{j=0}^{q-1} f_j (X + Y)^j = \sum_{j=0}^{q-1} f_j (X^j + Y^j)$$

Also muss für alle $j \in \{0, \ldots, q-1\}$ entweder $f_j = 0$ oder $(X + Y)^j = X^j + Y^j$ gelten. Wegen Lemma 3.1 ist $f_j = 0$ für $j \neq p^k$. Das heißt $\phi(f) \in M$.

Um (i) zu zeigen, betrachten wir:

$$(f +_G g)(X) = G(f(X), g(X)) \equiv f(X) + g(X) \pmod{\deg q}.$$

Da $\deg \phi(f) < q$ und $\deg \phi(g) < q$ folgt aus der Definition von ϕ:

$$\phi(f +_G g)(X) = \phi(f(X) + g(X)) = \phi(f)(X) + \phi(g)(X).$$

Es fehlt noch die Surjektivität von ϕ. Dafür reicht zu zeigen, dass es für ein gegebenes $a \in M$ mit erstem Koeffizient $a_0 \neq 0$ ein $f \in Hom_k(F,G)$ gibt, sodass $\phi(f) = a$. Diese Elemente erzeugen schon M als additive Gruppe, Eigenschaft (i) sichert uns dann die Surjektivität.
Für $n \geq q$ konstruieren wir eine Folge $f_n \in k[[X]]$ von Potenzreihen mit den folgenden Eigenschaften:

$$\begin{aligned} f_q &= a, \\ f_n \circ F &\equiv G \circ f_n \pmod{\deg n}, \\ f_{n+1} &\equiv f_n \pmod{\deg n}. \end{aligned}$$

Nach Voraussetzung ist $a_0 \in k^*$ und daher ist bei dieser Konstruktion für jedes $n \geq q$ die Potenzreihe f_n invertierbar. (Lemma 2.15.)
Wir definieren $f \in k[[X]]$ durch $f \equiv f_n \pmod{\deg n}$, dann gilt $f \in Hom_k(F,G)$ und $\phi(f) = a$.

Sei $n = q$. Dann ist $f_q = a$ und wie oben gilt wieder $F(X,Y) \equiv X + Y \equiv G(X,Y) \pmod{\deg q}$. Daher ist $a(F(X,Y)) \equiv G(a(X), a(Y)) \pmod{\deg q}$ genau dann, wenn $a(X+Y) = a(X) + a(Y)$. Diese Identität gilt wegen der Definition von M und Lemma 3.1 aber für alle $a \in M$.

Nehmen wir also an, dass f_n schon konstruiert ist. Nun konstruieren wir f_{n+1} und setzten dazu $H := f_n^{-1} \circ G \circ f_n$. Dies ist (wegen Beispiel 2.12) wieder ein formales Gruppengesetz. Nach Voraussetzung ist $F \equiv H \pmod{\deg n}$. Jetzt benutzen wir Satz 3.14 von Lazard und erhalten ein $c \in k$, sodass

$$F \equiv H + cC_n \pmod{\deg n + 1}.$$

Wieder behaupten wir:

$$F \equiv H + bB_n \pmod{\deg n + 1}, \text{ für ein } b \in k.$$

Wenn $n \neq p^l$, dann folgt wie im Beweis von Lemma 3.18: $cC_n = bB_n$ für ein $b \in k$.

Für $n = p^l$ ist $cC_n = 0$. Wir erhalten nämlich (mit Lemma 3.16):

$$[p]_F(X) \equiv [p]_H(X) + c(-1)X^n \pmod{\deg n + 1}.$$

Es sind aber G und H isomorph (da f_n invertierbar) und daher haben sie nach Korollar 3.11 die gleiche Höhe. Nach Voraussetzung hat auch F die gleiche Höhe. Außerdem können wir H in Normalform annehmen, daher ist $[p]_F(X) = [p]_G(X) = [p]_H(X) = X^q$. Wir erhalten $c = 0$ und somit $cC_n = 0$. Dies zeigt die Behauptung.

Lemma 3.15 sichert uns jetzt die Existenz einer invertierbaren Potenzreihe $u \in k[[X]]$ mit $u(X) \equiv X \pmod{\deg n}$, sodass $u \circ F \circ u^{-1} \equiv H \pmod{\deg n + 1}$. Wir setzen

$f_{n+1} \coloneqq f_n \circ u$. Dann ist $f_{n+1} = f_n \pmod{\deg n}$ und es gilt modulo $\deg n + 1$:

$$\begin{aligned} f_{n+1} \circ F \circ f_{n+1}^{-1} &= f_n \circ u \circ F \circ u^{-1} \circ f_n^{-1} \\ &\equiv f_n \circ H \circ f_n^{-1} \\ &\equiv f_n \circ f_n^{-1} \circ G \circ f_n \circ f_n^{-1} = G. \end{aligned}$$

Das beendet den Induktionsschritt und damit den Beweis. □

Mit dieser Proposition können wir nun unser Theorem formulieren und es relativ schnell beweisen.

Theorem 3.25. [Frö68, Kapitel 3, §2] Zwei formale Gruppengesetze F und G über einem algebraisch abgeschlossenen Körper k der Charakteristik $p > 0$ sind genau dann k-isomorph, wenn die Höhe von F gleich der Höhe von G ist.

Beweis. Der Beweis ist kurz und orientiert sich an [Frö68, Kapitel 3, §2].
Seien F und G isomorph. Dann ist nach Korollar 3.11 $Ht(F) = Ft(G)$.

Nun nehmen wir an, dass F und G gleiche Höhe haben. Den Fall, dass die Höhe unendlich ist, haben wir in Abschnitt 3 bewiesen. Wir können also $Ht(F) = Ht(G) = h \in \mathbb{N}, h \geq 1$ annehmen.
Da k algebraisch abgeschlossen ist, können wir weiter annehmen, dass F und G in Normalform sind (Proposition 3.23). Die Voraussetzungen der Proposition 3.24 sind somit erfüllt und nun nutzen wir die Surjektivität der Abbildung ϕ aus. Da $h \geq 1$ ist, ist $X \in M$. Damit existiert ein Homomorphismus $f \in Hom_k(F, G)$, sodass $\phi(f)(X) = X$. Wegen der Definition von ϕ bedeutet das $f(X) \equiv X \pmod{\deg 2}$ und daher ist f ein Isomorphismus (siehe Lemma 2.15). □

4 Formale Gruppengesetze von Lie-Gruppen

In diesem Kapitel lassen wir die Theorie der Klassifizierung von formalen Gruppengesetzen hinter uns und widmen uns einem anderen Thema. Formale Gruppengesetze wurden 1946 von Salomon Bochner im Artikel [Boc46] anhand von Lie-Gruppen eingeführt, wo sie natürlicherweise auftreten. Wenn man bei der Multiplikation einer Lie-Gruppe am neutralen Element Koordinaten wählt und dann eine Taylorreihenentwicklung durchführt, so verhält sich die entstandene Potenzreihe wie ein formales Gruppengesetz. Das wird in einigen Texten, zum Beispiel in [Haz12, Einleitung] behauptet, jedoch nie explizit nachgerechnet. Daher wollen wir das im Rahmen dieser Bachelorarbeit tun. Es stellt sich schnell heraus, dass es nicht trivial ist und wir etwas Vorarbeit brauchen.
Der Einfachheit halber beschränken wir uns in dieser Arbeit auf eindimensionale Lie-Gruppen und erhalten somit auch eindimensionale formale Gruppengesetze.

Zu Beginn wollen wir die Definition einer Lie-Gruppe geben. Dazu wird vorausgesetzt, dass der Begriff einer glatten (reellen) Mannigfaltigkeit bekannt ist. Eine gute Referenz ist [Lee12, Kapitel 1].

Lemma 4.1. [Lee12, Beispiel 1.8] Sei M eine glatte Mannigfaltigkeit und $\phi : U \to \phi(U) \subset \mathbb{R}^n$ eine Karte. Dann ist $M \times M$ wieder eine glatte Mannigfaltigkeit und

$$\begin{array}{rcl} \phi \times \phi : U \times U & \to & \phi(U) \times \phi(U) \subset \mathbb{R}^{2n} \\ (x, y) & \mapsto & (\phi(x), \phi(y)) \end{array}$$

eine Karte auf $M \times M$.

Beweis. [Lee12, Beispiel 1.8] □

Definition 4.2. [Lee12, Kapitel 2] Seien M und N glatte Mannigfaltigkeiten und sei $f : M \to N$ eine Abbildung. Wir sagen, dass f eine *glatte Abbildung* ist, wenn es für jedes $p \in M$ eine Karte (U, ϕ) mit $p \in U$ und eine Karte (V, ψ) mit $f(p) \in V$ gibt, sodass $f(U) \subset V$ und die Abbildung $\psi \circ f \circ \phi^{-1} : \phi(U) \to \psi(V)$ glatt ist.

Definition 4.3. [Lee12, Kapitel 7] Eine *Lie-Gruppe* G ist eine glatte Mannigfaltigkeit, die mit einer Gruppenstruktur versehen ist, sodass die Multiplikation $m : G \times G \to G$ und die Inversenbildung $i : G \to G$, $x \mapsto x^{-1}$ glatt sind. Das neutrale Element in G wird mit e notiert.

Bemerkung 4.4. Für die Multiplikationsabbildung m einer Lie-Gruppe müssen folgende Eigenschaften gelten:

(1) $m(e, e) = e$,

(2) $m(x, e) = m(e, x) = e$ für alle $x \in G$,

(3) $m(x, m(y, z)) = m(m(x, y), z)$ für alle $x, y, z \in G$.

Es gibt eine Karte (U, ϕ), sodass $e \in U$ und $\phi(e) = 0$. Weil m insbesondere eine stetige Abbildung ist, gibt es eine Umgebung $V \subseteq U$ von e, sodass $m(x, y) \in U$ für alle $x, y \in V$. Dann ist $(V \times V, \phi \times \phi)$ nach Lemma 4.1 eine Karte auf der glatten Mannigfaltigkeit $G \times G$ und es gilt $(\phi \times \phi)(e, e) = (\phi(e), \phi(e)) = (0, 0)$. Wir haben also im eindimensinalen Fall folgendes Diagramm:

$$\begin{array}{ccc} V \times V & \xrightarrow{m|_{V\times V}} & U \\ {\scriptstyle \phi\times\phi}\downarrow & & \downarrow{\scriptstyle \phi} \\ \phi(V) \times \phi(V) \subseteq \mathbb{R}^2 & \xrightarrow[\tilde{m}]{} & \mathbb{R} \end{array} \qquad \begin{array}{ccc} (e, e) & \xmapsto{m} & e \\ {\scriptstyle \phi\times\phi}\downarrow & & \downarrow{\scriptstyle \phi} \\ (0, 0) & \xmapsto[\tilde{m}]{} & 0 \end{array}$$

Satz 4.5. Die Abbildung $\tilde{m} \coloneqq \phi \circ m \circ (\phi \times \phi)^{-1} : \phi(V) \times \phi(V) \subseteq \mathbb{R}^2 \longrightarrow \mathbb{R}$ ist eine glatte Abbildung, für die wie in Bemerkung 4.4 gilt:

(1) $\tilde{m}(0, 0) = 0$,

(2) $\tilde{m}(x, 0) = \tilde{m}(0, x) = 0$ für alle $x \in \phi(V)$.

(3) Sei $W \subseteq \phi(V)$ eine Umgebung von Null, sodass $\tilde{m}(x, y) \in \phi(V)$ für alle $x, y \in W$. Dann ist $\tilde{m}(x, \tilde{m}(y, z)) = \tilde{m}(\tilde{m}(x, y), z)$ für alle $x, y, z \in W$.

Beweis. Nach Definiton 4.2 ist $\tilde{m}$ wieder eine glatte Abbildung. Nun rechnen wir nach, dass die Eigenschaften (1), (2) und (3) gelten:

$$\tilde{m}(0,0) = \phi(m((\phi\times\phi)^{-1}(0,0))) = \phi(m(\phi^{-1}(0), \phi^{-1}(0))) = \phi(m(e,e)) = \phi(e) = 0,$$

$$\begin{aligned} \tilde{m}(x,0) &= \phi(m((\phi\times\phi)^{-1}(x,0))) = \phi(m(\phi^{-1}(x), \phi^{-1}(0))) \\ &= \phi(m(\phi^{-1}(x), e)) = \phi(\phi^{-1}(x)) = x. \end{aligned}$$

Die Rechnung für $\tilde{m}(0, x) = x$ geht analog.

$$\begin{aligned} \tilde{m}(\tilde{m}(x,y),z) &= (\phi\circ m\circ(\phi\times\phi)^{-1})((\phi\circ m\circ(\phi\times\phi)^{-1})(x,y),z) \\ &= (\phi\circ m)((m\circ(\phi\times\phi)^{-1})(x,y),\phi^{-1}(z)) \\ &= (\phi\circ m)(m(\phi^{-1}(x),\phi^{-1}(y)),\phi^{-1}(z)) \\ &= (\phi\circ m)(\phi^{-1}(x), m(\phi^{-1}(y),\phi^{-1}(z))) \\ &= (\phi\circ m)(\phi^{-1}(x), (m\circ(\phi\times\phi)^{-1})(y,z)) \\ &= (\phi\circ m\circ(\phi\times\phi)^{-1})(x, (\phi\circ m\circ(\phi\times\phi)^{-1})(y,z)) \\ &= \tilde{m}(x,\tilde{m}(y,z)). \end{aligned}$$

□

Unser Ziel ist es zu beweisen, dass die formale Taylorentwicklung von $\tilde{m}$ am Nullpunkt ein formales Gruppengesetz ist. Dafür benötigen wir etwas Vorarbeit, die wir ganz allgemein im Mehrdimensionalen erledigen.

Sei $U \subseteq \mathbb{R}^k$ offen, $0 \in U$ und $f \in \mathcal{C}^\infty(U)$. Nach dem Satz über die Taylorsche Formel (z.B. in [For13, Kapitel I.7, Satz 2]), gibt es $B(0,\theta) \subseteq U$, sodass für alle $x \in B(0,\theta)$ gilt:

$$f(x) = T_{f,n}(x) + \phi_{f,n}(x),$$

wobei

$$T_{f,n}(x) = \sum_{|\underline{i}|\leq n} \frac{D^{\underline{i}} f(0)}{\underline{i}!} x^{\underline{i}}$$

und

$$\phi_{f,n}(x) = \sum_{|\underline{i}|=n+1} D^{\underline{i}} f(\xi) x^{\underline{i}} \text{ , mit } \xi \in B(0,x).$$

Es ist $D^{\underline{i}}\phi_{f,n}(0) = 0$ für alle $\underline{i} \in \mathbb{N}_0^k$ mit $|\underline{i}| \leq n$ und aus $D^{\underline{i}} f(0) = 0$ für alle $\underline{i} \in \mathbb{N}_0^k$ mit $|\underline{i}| \leq n$ folgt $T_{f,n} = 0$ und $f = \phi_{f,n}$.
Die formale Taylorentwicklung von f an der Stelle Null ist gegeben durch:

$$T_f(X) = \sum_{|\underline{i}|=0}^{\infty} \frac{D^{\underline{i}} f(0)}{\underline{i}!} X^{\underline{i}} \in \mathbb{R}[[X]].$$

Seien $V \subseteq \mathbb{R}^k$ und $U \subseteq \mathbb{R}^m$ offene Umgebungen von Null und sei $g : V \to U$ glatt. Dann ist $T_g \coloneqq (T_{g_1}, \ldots, T_{g_m})$.

Unser nächstes Zwischenziel ist für $g \in \mathcal{C}^\infty(V,U)$ und $f \in \mathcal{C}^\infty(U)$ mit $f(0) = g(0) = 0$ zu beweisen, dass $T_{f\circ g} = T_f \circ T_g$ gilt. (Wir weisen an dieser Stelle darauf hin, dass $T_g(0) = 0$ ist und somit $T_f \circ T_g$ wohldefiniert ist, siehe Kapitel 1.) Das benötigen wir, um die Assoziativität der formalen Taylorentwicklung von $\tilde{m}$ zu zeigen. Die Aussage wird in der Literatur sehr oft benutzt, allerdings ist es schwierig in den gängigen Analysisbüchern eine Referenz zu finden. Wir haben die Aussage im Vorlesungsskript [Pro, S. 209ff] gefunden, wo sie auch bewiesen wird. Die Beweise von Lemma 4.6, Lemma 4.7 und Satz 4.8 orientieren sich an der Darstellung in diesem Skript.

Lemma 4.6. Sei $U \subseteq \mathbb{R}^k$ Umgebung von Null und seien $f, g \in \mathcal{C}^\infty(U)$. Dann gilt:

(i) $T_{f+g} = T_f + T_g$ und $T_{\lambda\cdot f} = \lambda \cdot T_f$,

(ii) $T_{f\cdot g} = T_f \cdot T_g$.

Beweis. Die Aussage (i) folgt aus

$$D^{\underline{i}}(f+g)(x) = D^{\underline{i}} f(x) + D^{\underline{i}} g(x) \qquad \text{und} \qquad \lambda D^{\underline{i}} f(x) = D^{\underline{i}} \lambda f(x).$$

Um (ii) zu beweisen berechnen wir für $n \in \mathbb{N}$:

$$\begin{aligned} f \cdot g &= (T_{f,n} + \phi_{f,n}) \cdot (T_{g,n} + \phi_{g,n}) \\ &= T_{f,n} \cdot T_{g,n} + \phi_{f,n} \cdot T_{g,n} + T_{f,n} \cdot \phi_{g,n} + \phi_{f,n} \cdot \phi_{g,n}. \end{aligned}$$

Wir erinnern uns an die Leibnizformel für die Ableitung von Produkten von Funktionen in einer Variablen:

$$(h_1 h_2)^{(n)} = \sum_{p=0}^{n} \binom{n}{p} h_1^{(n)} h_2^{(n-p)}.$$

Das kann man für mehrere Variablen verallgemeinern, indem man die Faktoren $D_j^{i_j} = \frac{\partial^{i_j}}{\partial x_j^{i_j}}$ von $D^{\underline{i}}$ nacheinander anwendet:

$$D^{\underline{i}}(h_1 h_2) = \sum_{p_1=0}^{i_1} \cdots \sum_{p_k=0}^{i_k} \binom{i_1}{p_1} \cdots \binom{i_k}{p_k} D^{\underline{p}}(h_1) D^{\underline{i}-\underline{p}}(h_2) = \sum_{\underline{p} \leq \underline{i}} \binom{\underline{i}}{\underline{p}} D^{\underline{p}}(h_1) D^{\underline{i}-\underline{p}}(h_2).$$

Da $D^{\underline{p}}\phi_{f,n}(0) = 0 = D^{\underline{p}}\phi_{g,n}(0)$ für alle $\underline{p} \in \mathbb{N}_0^k$ mit $|\underline{p}| \leq n$, kann man für $|\underline{i}| \leq n$ einfach ablesen:

$$D^{\underline{i}}(\phi_{f,n} \cdot T_{g,n})(0) = 0, D^{\underline{i}}(T_{f,n} \cdot \phi_{g,n})(0) = 0 \text{ und } D^{\underline{i}}(\phi_{f,n} \cdot \phi_{g,n})(0) = 0.$$

Es gilt also

$$T_{f \cdot g, n} = T_{f,n} \cdot T_{g,n} \pmod{\deg n + 1}$$

für alle $n \in \mathbb{N}$. Damit ist die Aussage bewiesen. □

Lemma 4.7. Seien $V \subseteq \mathbb{R}^k$ und $U \subseteq \mathbb{R}^m$ offene Umgebungen von Null und seien $g : V \to U$ und $f : U \to \mathbb{R}$ glatt mit $f(0) = g(0) = 0$. Sei weiter $n \in \mathbb{N}$ und $D^{\underline{i}} f(0) = 0$ für alle $\underline{i} \in \mathbb{N}_0^m$ mit $|\underline{i}| \leq n$. Dann folgt:

$$D^{\underline{i}}(f \circ g)(0) = 0 \text{ für alle } \underline{i} \in \mathbb{N}_0^k \text{ mit } |\underline{i}| \leq n.$$

Beweis. Wir zeigen das durch Induktion nach n für alle Funktionen $\tilde{f} \in \mathcal{C}^\infty(U)$ gleichzeitig. Für $n = 0$ folgt die Aussage aus $(f \circ g)(0) = f(g(0)) = f(0) = 0$.
Nun nehmen wir die Behauptung für $n-1$ an, d.h. für alle $\tilde{f} \in \mathcal{C}^\infty(U)$ gilt: Aus $D^{\underline{i}}\tilde{f}(0) = 0$ für alle $\underline{i} \in \mathbb{N}_0^m$ mit $|\underline{i}| \leq n-1$ folgt $D^{\underline{i}}(\tilde{f} \circ g)(0) = 0$ für alle $\underline{i} \in \mathbb{N}_0^k$ mit $|\underline{i}| \leq n-1$.

Wir erinnern uns an die Kettenregel:

$$D_j(f \circ g)(x) = \frac{\partial}{\partial x_j}(f \circ g)(x) = \sum_{l=1}^{m} (D_l f)(g(x)) \cdot D_j g_l(x).$$

Ist nun $|\underline{i}| = n$ und $i_j > 0$, so erhalten wir mit der Leibnizformel aus dem Beweis von Lemma 4.6 und der Kettenregel:

$$\begin{aligned} D^{\underline{i}}(f \circ g)(0) &= D^{\underline{i}-e_j} D_j(f \circ g)(0) = \sum_{l=1}^{m} D^{\underline{i}-e_j}((D_l(f) \circ g) \cdot D_j g_l)(0) \\ &= \sum_{l=1}^{m} \sum_{\underline{p} \leq \underline{i}-e_j} \binom{\underline{i}-e_j}{\underline{p}} \underbrace{D^{\underline{p}}(D_l(f) \circ g)(0)}_{=0} D^{\underline{i}-\underline{p}}(g_l)(0). \end{aligned}$$

Dabei ist e_j der j-te Einheitsvektor. Wir wenden die Induktionsvoraussetzung auf $\tilde{f} = D_l(f)$ an, da nach Voraussetzung $D^{\underline{p}}(D_l(f))(0) = 0$ für alle $\underline{p} \in \mathbb{N}_0^m$ mit $|\underline{p}| \leq n-1$. Damit ist $D^{\underline{i}}(f \circ g)(0) = 0$. Für $|\underline{i}| < n$ folgt die Aussage direkt aus der Induktionsvoraussetzung. □

Satz 4.8. Seien $V \subseteq \mathbb{R}^k$ und $U \subseteq \mathbb{R}^m$ offene Umgebungen von Null. Weiter seien $g : V \to U$ und $f : U \to \mathbb{R}$ glatt mit $f(0) = g(0) = 0$. Dann ist

$$T_{f \circ g} = T_f \circ T_g.$$

Beweis. Zuerst sei $f = f_1 + f_2$ und $T_{f_1 \circ g} = T_{f_1} \circ T_g$ und $T_{f_2 \circ g} = T_{f_2} \circ T_g$, d.h. die Aussage ist für f_1 und f_2 schon bewiesen. Es ist $(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g$ und mit Lemma 4.6 folgt:

$$T_{f \circ g} = T_{f_1 \circ g + f_2 \circ g} = T_{f_1 \circ g} + T_{f_2 \circ g} = T_{f_1} \circ T_g + T_{f_2} \circ T_g = (T_{f_1} + T_{f_2}) \circ T_g = T_f \circ T_g.$$

Wir haben also gezeigt, dass die Aussage verträglich mit Summenzerlegung in f ist. Nun zeigen wir die Aussage für $f = X^{\underline{i}} = X_1^{i_1} \cdots X_m^{i_m}$ für $\underline{i} \in \mathbb{N}_0^m$.

Dann ist $f \circ g = g_1^{i_1} \cdots g_m^{i_m}$ und $T_f = f$. Wegen $g_i \in \mathcal{C}^\infty(V)$ folgt:

$$T_{f \circ g} \overset{\text{Lemma 4.6}}{=} T_{g_1}^{i_1} \cdots T_{g_m}^{i_m} = f \circ T_g = T_f \circ T_g.$$

Da die Aussage verträglich mit der Summenzerlegung in f ist, gilt sie somit auch für $f = \sum_{|\underline{i}| \leq n} a_{\underline{i}} X^{\underline{i}}$.

Sei nun $n \in \mathbb{N}$ und $h = \phi_{f,n}$. Dann ist $T_{h \circ g, n} = 0$.
Dazu müssen wir $D^{\underline{i}}(h \circ g)(0) = 0$ für $\underline{i} \in \mathbb{N}_0^k$ mit $|\underline{i}| \leq n$ zeigen. Aus der Voraussetzung wissen wir aber: Für $\underline{i} \in \mathbb{N}_0^m$ mit $|\underline{i}| \leq n$ ist $D^{\underline{i}} h(0) = 0$. Jetzt können wir Lemma 4.7 anwenden.

Wir sind jetzt so weit, dass wir für alle $n \in \mathbb{N}$ zeigen können: $T_{f \circ g, n} \equiv T_{f,n} \circ T_{g,n} \pmod{\deg n + 1}$. Dies beweist den Satz.
Dazu schreiben wir $f = f_1 + f_2$, wobei $f_1 = T_{f,n}$ und $f_2 = \phi_{f,n}$. Offensichtlich ist

$T_{f_1,n} = T_{f,n}$. Es folgt mit unseren vorangegangenen Überlegungen:

$$\begin{aligned} T_{f\circ g,n} &= T_{f_1\circ g,n} + \underbrace{T_{f_2\circ g,n}}_{=0} \\ &= T_{f_1\circ g,n} \\ &\equiv T_{f_1,n} \circ T_{g,n} \pmod{\deg n + 1} \\ &\equiv T_{f,n} \circ T_{g,n} \pmod{\deg n + 1}. \end{aligned}$$

□

Wir erinnern uns Satz 4.5, in dem wir die glatte Abbildung $\tilde{m} : \phi(V) \times \phi(V) \subseteq \mathbb{R}^2 \longrightarrow \mathbb{R}$ konstruiert haben. Jetzt sind wir so weit, dass wir folgendes Theorem beweisen können:

Theorem 4.9. $T_{\tilde{m}}(X, Y) \in \mathbb{R}[[X, Y]]$ ist ein formales Gruppengesetz.

Beweis. Wir rechnen die Eigenschaften (a) und (b) aus Definiton 2.1 nach.

$$T_{\tilde{m}}(X, 0) = \sum_{i\geq 0} X^i \frac{a_{i0}}{i!} \quad \text{mit } a_{i0} = \frac{\partial^i}{\partial x^i}\tilde{m}(x, y)\big|_{(x,y)=(0,0)} = \frac{\partial^i}{\partial x^i}\tilde{m}(x, 0)\big|_{x=0} = \frac{\partial^i}{\partial x^i}x\big|_{x=0}.$$

Also ist $a_{00} = 0$ und $a_{10} = 1$. Genauso zeigt man $a_{01} = 1$. Somit haben wir $T_{\tilde{m}}(X, Y) = X + Y \pmod{\deg 2}$.

Um (b) nachzurechnen sei $W \subseteq \phi(V)$ eine Umgebung von Null, sodass $\tilde{m}(x, y) \in \phi(V)$ für alle $x, y \in W$. Dann sind die folgenden Abbildungen wohldefiniert:

$$\begin{array}{rcll} \mathbb{R}^3 \supseteq W^3 & \xrightarrow{g} & \phi(V)^2 \subseteq \mathbb{R}^2 & \xrightarrow{f} \mathbb{R} \\ (x, y, z) & \longmapsto & (\tilde{m}(x, y), z) & \\ & & (x, y) & \longmapsto \tilde{m}(x, y). \end{array}$$

Die Abbildung g ist glatt, es gilt $T_g(X, Y, Z) = (T_{\tilde{m}}(X, Y), Z)$ und $(f \circ g)(x, y, z) = \tilde{m}(\tilde{m}(x, y), z)$.

$$\begin{array}{rcll} \mathbb{R}^3 \supseteq W^3 & \xrightarrow{h} & \phi(V)^2 \subseteq \mathbb{R}^2 & \xrightarrow{f} \mathbb{R} \\ (x, y, z) & \longmapsto & (x, \tilde{m}(y, z)) & \\ & & (x, y) & \longmapsto \tilde{m}(x, y). \end{array}$$

Auch die Abbildung h ist glatt und es gilt $T_h(X, Y, Z) = (X, T_{\tilde{m}}(Y, Z))$ und $(f \circ h)(x, y, z) = \tilde{m}(x, \tilde{m}(y, z))$.
Wir haben nachgerechnet, dass $f \circ g = f \circ h$ ist. Deshalb muss auch $T_{f\circ g} = T_{f\circ h}$ sein. Jetzt wenden wir Satz 4.8 an:

$$\begin{aligned} T_{\tilde{m}}(T_{\tilde{m}}(X, Y), Z) &= (T_f \circ T_g)(X, Y, Z) = T_{f\circ g}(X, Y, Z) \\ &= T_{f\circ h}(X, Y, Z) = (T_f \circ T_h)(X, Y, Z) \\ &= T_{\tilde{m}}(X, T_{\tilde{m}}(Y, Z)). \end{aligned}$$

□

5 Formale Gruppengesetze von affinen algebraischen Gruppen

In diesem Kapitel machen wir im Wesentlichen das gleiche wie im vorangegangenen Kapitel, nur für affine algebraische Gruppen. Wieder werden wir am neutralen Element Koordinaten wählen, was in der Sprache der Varietäten heißt, einen lokalen Parameter zu wählen. Dann werden wir auch hier die formale Taylorreihe der Multiplikationsabbildung betrachten und zeigen, dass diese ein formales Gruppengesetz ist.

Wir beginnen mit der Definition einer affinen algebraischen Gruppe. Dabei wird vorausgesetzt, dass die Begriffe affiner Raum $\mathbb{A}^n$ und affine Varietät $V \subseteq \mathbb{A}^n$ bekannt sind. Wir meinen in diesem Kapitel mit einer Varietät stets eine affine algebraische Varietät im Sinne des Vorlesungsskriptes [HK] über einem algebraisch abgeschlossenen Körper k.

Affine algebraische Gruppen

Definition 5.1. [SR13, Kapitel 3.4.1] Eine (affine) *algebraische Gruppe* ist eine (affine) Varietät $G \subseteq \mathbb{A}^n$, die mit einer Gruppenstruktur versehen ist, sodass die Multiplikation $m : G \times G \to G$ und die Inversenbildung $i : G \to G$, $x \mapsto x^{-1}$ Morphismen von Varietäten sind. Das neutrale Element in G wird mit e notiert.

Wir meinen mit einer algebraischen Gruppe stets eine affine algebraische Gruppe.

Lemma 5.2. Seien G und H zwei algebraische Gruppen. Dann ist das direkte Produkt $G \times H$ wieder eine algebraische Gruppe.

Beweis. Es ist klar, dass $G \times H$ wieder eine Varietät ist. Sei m_G die Multiplikation auf G, m_H die Multiplikation auf H. Die Multiplikation m auf $G \times H$ ist gegeben durch:

$$\begin{aligned} \phi : (G \times H) \times (G \times H) &\longrightarrow G \times H \\ ((x_1, y_1), (x_2, y_2)) &\longmapsto (m_G(x_1, x_2), m_H(y_1, y_2)). \end{aligned}$$

Weiter seien i_G und i_H die Inversenbildung in G und H. Dann ist das Inverse von (x, y) in $G \times H$ gegeben durch:

$$\begin{aligned} i : G \times H &\longrightarrow G \times H \\ (x, y) &\longmapsto (i_G(x), i_H(y)). \end{aligned}$$

Beide Abbildungen sind wieder Morphismen von affinen Varietäten (siehe dazu [HK, Satz 5.15]). Neutrales Element in $G \times H$ ist (e_G, e_H). □

Wir zitieren an dieser Stelle noch einen wichtigen Satz:

Satz 5.3. [SR13, Kapitel 3.4.1] Die Varietät einer algebraischen Gruppe ist nicht-singulär.

Beweis. Theorem 3.14 in [SR13, Kapitel 3.4.1].

□

Da der Ausgangsraum des Morphismus m eine Produktvarietät ist, müssen wir uns mit Produktvarietäten näher beschäftigen. Der nächste Abschnitt soll klären, wie lokale Ringe auf Produktvarietäten aussehen. Damit das nicht zu ausführlich wird, werden wir die wichtigsten Sätze nur zitieren und uns auf die eigentliche Aufgabe konzentrieren, das formale Gruppengesetz einer algebraischen Gruppe auszurechnen.

Lokale Ringe von Produktvarietäten

Sei $V \subseteq \mathbb{A}^n$ eine Varietät, $P \in V$. Wir schreiben $k[V]$ für den Koordinatenring von V und $\mathcal{O}_P$ für den lokalen Ring in P mit maximalem Ideal $m_P \subseteq \mathcal{O}_P$. Sei $W \subseteq \mathbb{A}^m$ eine weitere Varietät, $Q \in W$. Wir definieren folgende Abbildung:

$$\begin{aligned} \phi : k[V] \times k[W] &\longrightarrow k[V \times W] \\ (g, h) &\longmapsto g \cdot h. \end{aligned}$$

Dies ist eine k-bilineare Abbildung in g und h. Wegen der universellen Eigenschaft des Tensorprodukt gibt es genau eine k-lineare Abbildung:

$$\begin{aligned} \Phi : k[V] \otimes_k k[W] &\longrightarrow k[V \times W] \\ g \otimes h &\longmapsto g \cdot h. \end{aligned}$$

Wir erhalten folgenden Satz, den wir aus [Hum12, Kapitel 2.4] entnommen haben:

Satz 5.4. (i) Φ ist ein Isomorphismus.

(ii) $\mathcal{O}_{(P,Q)}$ ist die Lokalisierung von $\mathcal{O}_P \otimes_k \mathcal{O}_Q$ am maximalen Ideal $m_{(P,Q)} = m_P \otimes_k \mathcal{O}_Q + \mathcal{O}_P \otimes_k m_Q$.

Beweis. Proposition in [Hum12, Kapitel 2.4]. □

Daraus folgen drei wichtige Tatsachen, die wir in einem Lemma festhalten wollen:

Lemma 5.5. (i) $\mathcal{O}_P \otimes_k \mathcal{O}_Q \subseteq \mathcal{O}_{(P,Q)}$.

(ii) $m_P \otimes_k m_Q \subseteq m_{(P,Q)}$.

(iii) $m_P^i \otimes_k m_Q^j \subseteq m_{(P,Q)}^n$ für $i, j \in \mathbb{N}$ mit $i + j = n$.

Beweis. (i) und (ii) sind wegen Satz 5.4 klar und für (iii) stellen wir fest:

$$m_{(P,Q)}^n = \sum_{i=0}^{n} m_P^i \otimes_k m_Q^{n-i}.$$

Dabei ist $m_P^0 \coloneqq \mathcal{O}_P$ und $m_Q^0 \coloneqq \mathcal{O}_Q$. □

Als nächstes beweisen wir einen elementaren Satz, für den es allerdings sehr schwierig ist, eine Referenz zu finden. Wir werden im Beweis zwei Lemmata des *Stacks Project* [Sta17] zitieren.

Satz 5.6. Es gilt:

$$m_P/m_P^2 \oplus m_Q/m_Q^2 \quad \cong \quad m_{(P,Q)}/m_{(P,Q)}^2.$$

Beweis. Für eine Varietät X und $x \in X$ ist m_x/m_x^2 ein k-Vektorraum. Wir betrachten den Dualraum $(m_x/m_x^2)^*$. Wegen [Sta17, Tag 0B2E] ist dieser isomorph zum Tangentialraum in x, den wir T_x notieren. In [Sta17, Tag 0BEB] wird bewiesen:

$$T_{(P,Q)} \cong T_P \oplus T_Q.$$

Für zwei k-Vektorräume V und W ist aus der linearen Algebra bekannt:

$$(V \oplus W)^* = V^* \oplus W^* \text{ und aus } V \cong W \text{ folgt } V^* \cong W^*.$$

Dies beweist unseren Satz. □

Wir führen nun lokale Parameter ein. Dabei halten wir uns an die Darstellung in [SR13].

Lokale Parameter in einem Punkt

Definition 5.7. [SR13, Kapitel 2.1.4] Sei $V \subseteq \mathbb{A}^n$ eine algebraische Varietät. Dann heißt:

$$dim_P(V) = \max\{\dim(Z) | P \in Z, Z \text{ irreduzible Komponente von } V\}$$

die *lokale Dimension von V im Punkt P*.

Bemerkung 5.8. [SR13, Kapitel 2.1.4] Für $P \in V$ nicht-singulär gilt nach Theorem 2.3 in [SR13, Kapitel 2.1.4]: $\dim(T_P) = \dim_P(V)$. Daher gilt auch:

$$\dim\left(m_P/m_P^2\right) = \dim_P(V).$$

Diese Bemerkung brauchen wir, damit wir die folgende Definition formulieren können:

Definition 5.9. [SR13, Kapitel 2.2.1] Sei $V \subseteq \mathbb{A}^n$ eine Varietät, $P \in V$ nicht-singulär, $\dim_P(V) = s$. Dann heißen $u_1, \ldots, u_s \in \mathcal{O}_P$ *lokale Parameter* von P, falls jedes $u_i \in m_P$ und die Bilder von $u_1, \ldots, u_s$ eine Basis des k-Vektorraums m_P/m_P^2 bilden.

Satz 5.10. Seien $V \subseteq \mathbb{A}^n, W \subseteq \mathbb{A}^m$ zwei Varietäten, $P \in V, Q \in W$ nicht-singulär und $\dim_P(V) = s$, $\dim_Q(W) = l$. Seien weiter $v_1, \ldots, v_s$ lokale Parameter in $P \in V$ und $w_1, \ldots, w_l$ lokale Parameter in $Q \in W$. Dann sind

$$v_1 \otimes 1, \ldots, v_s \otimes 1, 1 \otimes w_1, \ldots, 1 \otimes w_l$$

lokale Parameter in $(P, Q) \in V \times W$.

Beweis. Offensichtlich sind $v_1 \otimes 1, \ldots, v_s \otimes 1, 1 \otimes w_1, \ldots, 1 \otimes w_l \in m_{(P,Q)} = m_P \otimes \mathcal{O}_Q + \mathcal{O}_P \otimes m_Q$. Wir erinnern uns an die Aussage von Satz 5.6:

$$m_P/m_P^2 \oplus m_Q/m_Q^2 \cong m_{(P,Q)}/m_{(P,Q)}^2.$$

Nach Voraussetzung bilden die Bilder von $v_1, \ldots, v_s$ eine k-Basis von m_P/m_P^2 und ebenso bilden die Bilder von $w_1, \ldots, w_l$ eine k-Basis von m_Q/m_Q^2. Daher müssen auch die Bilder von $v_1 \otimes 1, \ldots, v_s \otimes 1, 1 \otimes w_1, \ldots, 1 \otimes w_l$ eine k-Basis von $m_{(P,Q)}/m_{(P,Q)}^2$ bilden. □

Wir zitieren noch einen nützlichen Satz über lokale Parameter:

Satz 5.11. [SR13, Kapitel 2.2.1] Seien $u_1, \ldots, u_s \in \mathcal{O}_P$ lokale Paramter in $P \in V$. Dann gilt:

$$m_P = \langle u_1, \ldots, u_s \rangle_{\mathcal{O}_P}.$$

Mit den eckigen Klammern ist dabei das von $u_1, \ldots, u_s$ erzeugte Ideal im Ring $\mathcal{O}_P$ gemeint.

Beweis. Theorem 2.5 in [SR13, Kapitel 2.2.1]. □

Taylorreihenentwicklung

Definition 5.12. [SR13, Kapitel 2.2.2] Sei $V \subseteq \mathbb{A}^m$ eine Varietät, $\dim_P(V) = s$ und $P \in V$ nicht-singulär mit $u_1, \ldots, u_s$ lokalen Parametern. Sei $F = \sum_{|\underline{i}|=0}^{\infty} a_{\underline{i}} T^{\underline{i}} \in k[[T]] = k[[T_1, \ldots, T_s]]$ eine formale Potenzreihe. Wir nennen F eine *Taylorreihe von* $f \in \mathcal{O}_P$, falls für jedes $n \geq 0$ gilt:

$$f - F_n(u_1, \ldots, u_s) \in m_P^{n+1}, \text{ mit } F_n = \sum_{|\underline{i}|=0}^{n} a_{\underline{i}} T^{\underline{i}}.$$

Satz 5.13. [SR13, Kapitel 2.2.2] Sei $V \subseteq \mathbb{A}^n$ eine Varietät, $P \in V$ nicht-singulär. Dann gibt es für alle $f \in \mathcal{O}_P$ genau eine Taylorreihe F.

Beweis. Für die Existenz Theorem 2.6 und für die Eindeutigkeit Theorem 2.7 in [SR13, Kapitel 2.2.2]. Der Beweis der Existenz ist dort konstruktiv und es wird beschrieben, wie man die Taylorreihe für ein gegebenes $f \in \mathcal{O}_P$ entwickelt. □

Für einen nicht-singulären Punkt P einer Varietät und ein Element $f \in \mathcal{O}_P$ schreiben wir $F = T_f$ und $F_n = T_{f,n}$ und können f für alle $n \in \mathbb{N}$ eindeutig darstellen:

$$f = T_{f,n}(u_1, \ldots, u_s) + \phi_{f,n}(u_1, \ldots, u_s),$$

wobei $\phi_{f,n}(u_1, \ldots, u_s) \in m_P^{n+1}$.

Wir kommen zur eigentlichen Motivation dieses Kapitels. Für eine algebraische Gruppe wollen wir eine formale Taylorreihe am neutralen Element der Multiplikation konstruieren und dann beweisen, dass dies ein formales Gruppengesetz ergibt. Wir werden dabei die vorangegangenen Lemmata und Sätze verwenden.

Sei also G eine algebraische Gruppe über einem algebraisch abgeschlossenen Körper k. Wir beschränken uns zur Vereinfachung darauf, dass die lokale Dimension im neutralen Element eins ist, d.h. $\dim_e(G) = 1$.

$m : G \times G \to G$ ist die Multiplikation auf G. Dies ist ein Morphismus von Varietäten mit den folgenden Eigenschaften:

(1) $m(e,e) = e$,

(2) $m(x,e) = m(e,x) = e$ für alle $x \in G$,

(3) $m(x, m(y,z)) = m(m(x,y), z)$ für alle $x, y, z \in G$.

Nach Satz 5.3 ist G in e nicht-singulär. Wir wählen in e einen lokalen Parameter $u \in m_e \subseteq \mathcal{O}_e$ und erhalten eine Abbildung $f := u \circ m \in m_{(e,e)} \subseteq \mathcal{O}_{(e,e)}$.

Nach Lemma 5.2 ist $G \times G$ wieder eine algebraische Gruppe, also insbesondere nicht-singulär in (e,e). Es gibt somit nach Satz 5.13 genau eine Taylorreihe $T_f \in k[[X,Y]]$, für die für alle $n \geq 0$ gilt:

$$f = T_{f,n}(u_1, u_2) + \phi_{f,n}(u_1, u_2) \text{ mit } \phi_{f,n}(u_1, u_2) \in m_{(e,e)}^{n+1}.$$

Dabei definieren wir: $u_1 := u \otimes 1$ und $u_2 := 1 \otimes u$. Dies sind nach Satz 5.10 lokale Parameter in $(e,e) \in G \times G$. Es gilt $u_1(x,y) = u(x) \otimes 1 = u(x) \cdot 1 = u(x)$ und genauso $u_2(x,y) = u(y)$.

Theorem 5.14. $T_f \in k[[X,Y]]$ ist ein formales Gruppengesetz.

Beweis. Es sind die Eigenschaften (a) und (b) aus Definiton 2.1 nachzurechnen.

Wir zeigen $T_f(X,0) = X$. Analog folgt $T_f(0,Y) = Y$ und zusammen bedeutet das $T_f(X,Y) = X + Y \pmod{\deg 2}$.

Es ist nach Definition $f(x,e) = u(m(x,e)) = u(x)$. Wie wir uns oben überlegt haben gilt für alle $n \in \mathbb{N}$:

$$f(x,e) = (T_{f,n}(u_1,u_2))(x,e) + (\phi_{f,n}(u_1,u_2))(x,e).$$

Da $u_1(x,e) = u(x)$ und $u_2(x,e) = u(e) = 0$ ist dies äquivalent zu:

$$u(x) = T_{f,n}(u(x), 0) + \phi_{f,n}(u(x), 0).$$

Daraus folgt $X = T_f(X,0)$.

Um die Assoziativität zu zeigen, betrachten wir zuerst die Varietät $G \times G \times G$, die nach Lemma 5.2 wieder eine algebraische Gruppe ist, also insbesondere nicht-singulär in $\tilde{e} := (e,e,e)$. Noch einmal benutzen wir Satz 5.10 und erhalten, dass

$$v_1 = u \otimes 1 \otimes 1, v_2 = 1 \otimes u \otimes 1 \text{ und } v_3 = 1 \otimes 1 \otimes u$$

lokale Parameter in $\tilde{e}$ sind. Es gilt wieder $v_1(x,y,z) = u(x) \otimes 1 \otimes 1 = u(x) \cdot 1 \cdot 1 = u(x)$ und genauso $v_2(x,y,z) = u(y)$, bzw. $v_3(x,y,z) = u(z)$. Wir definieren die folgende Abbildungen, die offensichtlich Morphismen von affinen Varietäten sind:

$$\begin{aligned} h_1 : G \times G \times G &\longrightarrow G \times G \\ (x,y,z) &\longmapsto (m(x,y), z), \\ h_2 : G \times G \times G &\longrightarrow G \times G \\ (x,y,z) &\longmapsto (x, m(y,z)). \end{aligned}$$

Dann gilt:

$$u \circ m \circ h_1 = f \circ h_1 \in m_{\tilde{e}} \subseteq \mathcal{O}_{\tilde{e}},$$
$$u \circ m \circ h_2 = f \circ h_2 \in m_{\tilde{e}} \subseteq \mathcal{O}_{\tilde{e}}.$$

Und nach Voraussetzung:

$$(f \circ h_1)(x,y,z) = u(m(m(x,y),z)) = u(m(x,m(y,z))) = (f \circ h_2)(x,y,z).$$

$\tilde{e}$ ist wieder nicht-singulär in $G \times G \times G$. Da die Taylorreihe nach Satz 5.13 eindeutig ist, ist $T_{f \circ h_1} = T_{f \circ h_2}$. Also reicht zu zeigen:

(i) $T_{f\circ h_1}(X,Y,Z) = T_f(T_f(X,Y),Z)$ und (ii) $T_{f\circ h_2}(X,Y,Z) = T_f(X,T_f(Y,Z))$.

Wir zeigen nur den ersten Teil, (ii) folgt analog. Dazu werden wir nacheinander drei Behauptungen aufstellen und jeweils beweisen. Sei $n \in \mathbb{N}$.

Behauptung 1: $\phi_{f,n}(u_1,u_2) \circ h_1 \in m_{\tilde{e}}^{n+1}$.

Nach Satz 5.11 ist $m_{(e,e)} = \langle u_1, u_2 \rangle$ und daher gilt:

$$\phi_{f,n}(u_1,u_2) \in m_{(e,e)}^{n+1} = \langle u_1,u_2\rangle^{n+1}, \text{ d.h. } \phi_{f,n}(u_1,u_2) = \sum_{i+j=n+1} \phi_{ij} u_1^i u_2^j \text{ mit } \phi_{ij} \in \mathcal{O}_{(e,e)}.$$

Wir erinnern uns, dass nach nach Satz 5.4 $\mathcal{O}_{\tilde{e}}$ die Lokalisierung von $\mathcal{O}_{(e,e)} \otimes_k \mathcal{O}_e$ am maximalen Ideal $m_{\tilde{e}} = m_{(e,e)} \otimes_k \mathcal{O}_e + \mathcal{O}_{(e,e)} \otimes m_e$ ist. Nun erhalten wir:

$$\begin{aligned}
(\phi_{f,n}(u_1,u_2) \circ h_1)(x,y,z) &= \sum_{i+j=n+1} \Big((\phi_{ij} u_1^i u_2^j) \circ h_1 \Big)(x,y,z) \\
&= \sum_{i+j=n+1} \Big(\phi_{ij} u_1^i u_2^j \Big)(m(x,y),z) \\
&= \sum_{i+j=n+1} [(\phi_{ij} \circ h_1)(x,y,z)] \cdot \Big[u(m(x,y))^i \cdot u(z)^j \Big] \\
&= \sum_{i+j=n+1} [\underbrace{(\phi_{ij} \circ h_1)}_{\in \mathcal{O}_{\tilde{e}}} \cdot (\underbrace{f^i}_{\in m_{(e,e)}^i} \otimes \underbrace{u^j}_{\in m_e^j})](x,y,z).
\end{aligned}$$

Wir wenden Lemma 5.5 (iii) an und erhalten $\phi_{f,n}(u_1,u_2) \circ h_1 \in m_{\tilde{e}}^{n+1}$.

Behauptung 2: Aus $\phi_{f,n}(u_1,u_2) \in m_{(e,e)}^{n+1} = \langle u_1,u_2\rangle^{n+1}$ *folgt* $\phi_{f,n}(v_1,v_2) \in m_{\tilde{e}}^{n+1} = \langle v_1,v_2,v_3\rangle^{n+1}$.

Wie in Behauptung 1 schreiben wir:

$$\phi_{f,n}(u_1,u_2) = \sum_{i+j=n+1} \phi_{ij} u_1^i u_2^j \text{ mit } \phi_{ij} \in \mathcal{O}_{(e,e)}.$$

Wir definieren: $\tilde{\phi}_{ij} = \phi_{ij} \otimes 1 \in \mathcal{O}_{\tilde{e}}$, d.h. $\tilde{\phi}_{ij}(x,y,z) = \phi_{ij}(x,y)$. Da $v_1 = u_1 \otimes 1$ und $v_2 = u_2 \otimes 1$, folgt:

$$\phi_{f,n}(v_1, v_2) = \sum_{i+j=n+1} \tilde{\phi}_{ij} v_1^i v_2^j.$$

Dies ist offensichtlich in $m_{\tilde{e}}^{n+1} = \langle v_1, v_2, v_3 \rangle^{n+1}$.

Behauptung 3: $T_{f,n}(u_1, u_2) \circ h_1 = T_{f,n}(T_{f,n}(v_1, v_2) + \phi_{f,n}(v_1, v_2), v_3)$.

$$\begin{aligned}
\left(T_{f,n}(u_1,u_2) \circ h_1\right)(x,y,z) &= T_{f,n}(u_1,u_2)(m(x,y),z) \\
&= T_{f,n}\left(u(m(x,y)), u(z)\right) \\
&= T_{f,n}\left(f(x,y), u(z)\right) \\
&= T_{f,n}\left[(T_{f,n}(u_1,u_2) + \phi_{f,n}(u_1,u_2))(x,y), u(z)\right] \\
&= T_{f,n}\left[T_{f,n}(v_1,v_2) + \phi_{f,n}(v_1,v_2), v_3\right](x,y,z).
\end{aligned}$$

Jetzt erhalten wir im Ring $\mathcal{O}_{\tilde{e}}$ modulo $m_{\tilde{e}}^{n+1}$ unter Benutzung der drei Behauptungen:

$$\begin{aligned}
f \circ h_1 &= T_{f,n}(u_1,u_2) \circ h_1 + \underbrace{\phi_{f,n}(u_1,u_2) \circ h_1}_{\in m_{\tilde{e}}^{n+1} \text{ (Beh. 1)}} \\
&\equiv T_{f,n}(u_1,u_2) \circ h_1 \\
&\overset{\text{Beh. 3}}{\equiv} T_{f,n}(T_{f,n}(v_1,v_2) + \underbrace{\phi_{f,n}(v_1,v_2)}_{\in m_{\tilde{e}}^{n+1} \text{ (Beh. 2)}}, v_3) \\
&\equiv T_{f,n}(T_{f,n}(v_1,v_2), v_3).
\end{aligned}$$

Dies gilt für alle $n \in \mathbb{N}$. Also ist $T_{f \circ h_1}(X,Y,Z) = T_f(T_f(X,Y),Z)$. □

Zum Schluss geben wir zwei Beispiele für algebraische Gruppen mit zugehörigem formalen Gruppengesetz.

Beispiel 5.15. Wir betrachten die algebraische Gruppe $G = \mathbb{A}^1$ mit der üblichen Addition $m(X,Y) = X + Y$. Das neutrale Element ist $e = 0$. Als lokalen Parameter u in e können wir $u(X) = X$ wählen. Wir behaupten, dass

$$T_f(X,Y) = \mathbb{G}_a(X,Y) = X + Y$$

die formale Taylorreihe von $f(X,Y) = u(m(X,Y)) = X + Y \in m_{(e,e)} \subseteq \mathcal{O}_{(e,e)}$ ist.

Wie in der Konstruktion oben ist $u_1(X,Y) = u(X) = X$ und $u_2(X,Y) = u(Y) = Y$. Es ist zu zeigen, dass für alle $n \geq 0$ gilt: $f - T_{f,n}(u_1,u_2) \in m_{(e,e)}^{n+1}$. Für $n = 0$ ist dies klar, da $f \in m_{(e,e)}$ und $T_{f,0} = 0$. Für $n \geq 1$ gilt:

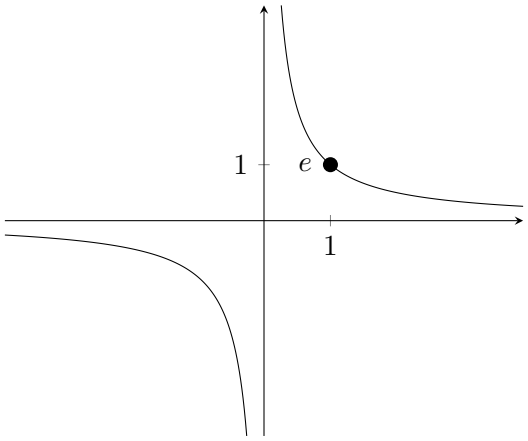
$$T_{f,n}(u_1,u_2)(X,Y) = T_{f,n}(X,Y) = X + Y = f(X,Y).$$

Also ist $f - T_{f,n}(u_1,u_2) = 0$ und es ist $0 \in m_{(e,e)}^{n+1}$ für alle $n \in \mathbb{N}$.

Beispiel 5.16. Wir betrachten die algebraische Gruppe $G = V(X_1X_2 - 1) \in \mathbb{A}^2$ mit der Multiplikation:

$$\begin{array}{rcl} & m : G \times G & \longrightarrow & G \\ (X,Y) = \left(\begin{pmatrix} X_1 \\ X_2 \end{pmatrix}, \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} \right) & \longmapsto & \begin{pmatrix} X_1Y_1 \\ X_2Y_2 \end{pmatrix} \end{array}$$

Das neutrale Element ist $e = \binom{1}{1}$.



Als lokalen Paramter u in e wählen wir $u(X) = X_1 - 1$. Wir erhalten also $f(X,Y) = u(m(X,Y)) = X_1Y_1 - 1 \in m_{(e,e)} \subseteq \mathcal{O}_{(e,e)}$ und behaupten:

$$T_f(X,Y) = \mathbb{G}_m(X,Y) = X + Y + XY.$$

Mit $u_1(X,Y) = u(X) = X_1 - 1$ und $u_2(X,Y) = u(Y) = Y_1 - 1$ ist wieder $f - T_{f,n}(u_1,u_2) \in m_{(e,e)}^{n+1}$ für alle $n \geq 0$ zu zeigen. Für $n = 0$ gilt dies mit der gleichen Argumentation wie in Beispiel 5.15. Für $n = 1$ erhalten wir:

$$\begin{array}{rcl} f(X,Y) - T_{f,1}(u_1,u_2)(X,Y) & = & X_1Y_1 - 1 - T_{f,1}(X_1 - 1, Y_1 - 1) \\ & = & X_1Y_1 - 1 - (X_1 - 1 + Y_1 - 1) \\ & = & X_1Y_1 - X_1 - Y_1 + 1 \\ & = & \underbrace{(X_1 - 1)}_{\in m_{(e,e)}} \underbrace{(Y_1 - 1)}_{\in m_{(e,e)}} \in m_{(e,e)}^2. \end{array}$$

Und für $n \geq 2$ gilt:

$$\begin{array}{rcl} T_{f,n}(u_1,u_2)(X,Y) & = & T_{f,n}(X_1 - 1, Y_1 - 1) \\ & = & (X_1 - 1) + (Y_1 - 1) + (X_1 - 1)(Y_1 - 1) \\ & = & X_1 + Y_1 - 2 + X_1Y_1 - X_1 - Y_1 + 1 \\ & = & X_1Y_1 - 1 = f(X,Y). \end{array}$$

Also ist $f - T_{f,n}(u_1,u_2) = 0 \in m_{(e,e)}^{n+1}$.

Das nächste typische Beispiel wären elliptische Kurven. Das sind grob gesagt spezielle algebraische Kurven, auf denen eine Addition definiert ist. Auch hier kann man am neutralen Element die formale Taylorreihe entwickeln, die dann wieder ein formales Gruppengesetz ist. Für elliptische Kurven, die über einem Körper mit positiver Charakteristik definiert sind, erhält man, dass die Höhe des zugehörigen formalen Gruppengesetzes stets eins oder zwei ist. Wer die Theorie der elliptischen Kurven genauer studieren möchte, dem sei das Buch von Silverman - The Arithmetic of Elliptic Curves [Sil09] empfohlen. Dort werden auch Teile der Theorie über formale Gruppengesetze benutzt, die wir in Kapitel zwei und drei entwickelt haben.

Ich versichere hiermit, dass ich die vorliegende Arbeit ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen habe ich unter Angabe der Quellen kenntlich gemacht. Die vorliegende Arbeit ist oder war weder vollständig noch in wesentlichen Teilen Gegenstand eines anderen Prüfungsverfahrens.

.....	.....
Ort, Datum	Nils Sturma

6 Literatur

[Boc46] S. Bochner. Formal Lie groups. *Ann. of Math. (2)*, 47:192–201, 1946.

[For13] O. Forster. *Analysis 2: Differentialrechnung im $\mathbb{R}^n$, gewöhnliche Differentialgleichungen*. Grundkurs Mathematik. Springer Fachmedien, Wiesbaden, 2013.

[Frö68] A. Fröhlich. *Formal groups*. Lecture Notes in Mathematics, No. 74. Springer-Verlag, Berlin-New York, 1968.

[FS15] Harald Fripertinger and Jens Schwaiger. On one-dimensional formal group laws in characteristic zero. *Aequationes Math.*, 89(3):857–862, 2015.

[Haz12] Michiel Hazewinkel. *Formal groups and applications*. AMS Chelsea Publishing, Providence, RI, 2012. Corrected reprint of the 1978 original.

[Hen88] Peter Henrici. *Applied and computational complex analysis. Vol. 1.* Wiley Classics Library. John Wiley & Sons, Inc., New York, 1988. Power series—integration—conformal mapping—location of zeros, Reprint of the 1974 original, A Wiley-Interscience Publication.

[HK] Prof. Dr. Annette Huber-Klawitter. Vorlesungsskript Kommutative Algebra und Einführung in die algebraische Geometrie im Sommersemester 2017. Online erhältlich unter http://home.mathematik.uni-freiburg.de/arithgeom/lehre/ss17/kommalg/kommalg.pdf; abgerufen am 16. November 2017.

[Hum12] J.E. Humphreys. *Linear Algebraic Groups*, volume 21 of *Graduate Texts in Mathematics*. Springer, New York, 2012.

[Lan05] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005.

[Lee12] J.M. Lee. *Introduction to Smooth Manifolds: Second Edition*, volume 218 of *Graduate Texts in Mathematics*. Springer Verlag, New York, second edition, 2012.

[Pro] Prof. Dr. Karl-Hermann Neeb, TU Darmstadt. Vorlesungsskript Analysis II, WS 07/08. Online erhältlich unter http://www.mathematik.tu-darmstadt.de/fbereiche/AlgGeoFA/staff/neeb/skripten/ana2-ws07.pdf; abgerufen am 28. November 2017.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[SR13] I.R. Shafarevich and M. Reid. *Basic Algebraic Geometry 1: Varieties in Projective Space*. SpringerLink : Bücher. Springer, Berlin Heidelberg, third edition, 2013.

[Sta17] The Stacks Project Authors. exitStacks Project. http://stacks.math.columbia.edu, 2017.

[ZS13] O. Zariski and P. Samuel. *Commutative Algebra*. Number Bd. 2 in Graduate Texts in Mathematics. Springer, Berlin Heidelberg, 2013.