Algebraische Definition von Drinfeld-Moduln

J. Brugger (jbrugger@student.ethz.ch)

5. Mai, 2008

Sei von nun an K ein Körper mit $\mathrm{char}(K) = p > 0$ sowie $q = p^k$ für $k \in \mathbb{N}^*$. Wir betrachten den nicht notwendigerweise kommutativen Ring $(K\{\tau\}, +, \circ)$, der $\mathbb{F}_q$-linearen Polynome in $K[T]$, wobei wir τ mit dem Polynom T^q identifizieren. Beachte, dass $\tau^i \circ x = x^{q^i} \circ \tau^i$ gilt, für alle $x \in K$.

Definition 1. Der Grad bzw. die Höhe ist definiert als die Funktion

$$\deg : K\{\tau\} \to \mathbb{N} \cup \{-\infty\} \ , \ \beta(\tau) = \sum_{i=0}^{n} b_i \tau^i \mapsto \begin{cases} -\infty & , \quad \beta(\tau) = 0 \\ \max\{i \ ; \ b_i \neq 0\} & , \quad \beta(\tau) \neq 0 \end{cases}$$

bzw.

$$\mathrm{ht} : K\{\tau\} \to \mathbb{N} \cup \{\infty\} \ , \ \beta(\tau) = \sum_{i=0}^{n} b_i \tau^i \mapsto \begin{cases} \infty & , \quad \beta(\tau) = 0 \\ \min\{i \ ; \ b_i \neq 0\} & , \quad \beta(\tau) \neq 0. \end{cases}$$

Bemerkung 2. Für $\alpha, \beta \in K\{\tau\}$ gelten offenbar

(i) $\deg(\alpha\beta) = \deg(\alpha) + \deg(\beta)$

(ii) $\deg(\alpha + \beta) \leq \max\{\deg(\alpha), \deg(\beta)\}$

(iii) $\mathrm{ht}(\alpha\beta) = \mathrm{ht}(\alpha) + \mathrm{ht}(\beta)$

(iv) $\mathrm{ht}(\alpha + \beta) \geq \min\{\mathrm{ht}(\alpha), \mathrm{ht}(\beta)\}$.

Definition 3. Die Abbildung ∂_0 sei definiert als $\partial_0 : K\{\tau\} \to K \ , \ \sum_{i=0}^{n} b_i \tau^i \mapsto b_0$. Es handelt sich hierbei um einen Ringhomomorphismus.

Definition 4. Wir sagen ein Element $\beta(\tau) = \sum_{i=0}^{n} b_i \tau^i \in K\{\tau\}$ sei genau dann separabel, wenn das zugehörige Polynom $\sum_{i=0}^{n} b_i T^{q^i} \in K[T]$ separabel ist.

Bemerkung 5. Offenbar ist $\beta \in K\{\tau\}$ genau dann separabel, wenn $\partial_0(\beta) \neq 0$, da additive Polynome genau dann separabel sind, wenn der Koeffizient von T nicht verschwindet.

Proposition 6. Sei $0 \neq \alpha \in K\{\tau\}$. Dann existieren ein eindeutiges $h \in \mathbb{N}$ und ein eindeutiges $\beta \in K\{\tau\}$ so, dass β separabel ist und $\alpha = \beta \circ \tau^h$ gilt. Es gilt dann $h = \mathrm{ht}(\alpha)$.

Beweis. Sei $\alpha = \sum_{i=0}^{n} a_i \tau^i$. Setze $h := \min\{i \; ; \; a_i \neq 0\}$ sowie $\beta = \sum_{i=h}^{n} a_i \tau^{i-h}$. Die Existenz folgt aus Bemerkung 5, die Eindeutigkeit folgt durch Koeffizientenvergleich. □

Proposition 7. (i) Für alle $\alpha, \beta \in K\{\tau\}$ mit $\beta \neq 0$ existieren eindeutige $\gamma, \delta \in K\{\tau\}$ mit

$$\alpha = \gamma \circ \beta + \delta \quad , \quad \deg \delta < \deg \beta.$$

(ii) Die Linksideale von $K\{\tau\}$ sind genau die Linkshauptideale von $K\{\tau\}$.

Beweis. (i) Wir beweisen zunächst den Existenzteil mit Induktion nach $\deg(\alpha)$. Ist $\deg(\alpha) = -\infty$, d.h. $\alpha = 0$, können wir $\gamma = 0$ und $\delta = 0$ wählen und sind fertig. Sei jetzt $m := \deg(\alpha) \geq 0$. O.B.d.A. können wir $\deg(\alpha) \geq \deg(\beta) =: n$ annehmen (sonst setzen wir $\gamma = 0$ und $\delta = \alpha$). Sei also $\alpha = \sum_{i=0}^{m} a_i \tau^i$ und $\beta = \sum_{j=0}^{n} b_j \tau^j$, wobei $a_m \neq 0 \neq b_n$. Setze $\gamma' := a_m (b_n^{q^{m-n}})^{-1} \tau^{m-n}$. Da $\alpha' := \alpha - \gamma' \circ \beta$ kleineren Grad hat als α, gibt es nach Induktionsvoraussetzung $\gamma'', \delta \in K\{\tau\}$ mit $\deg(\delta) < \deg(\beta)$ so, dass $\alpha' = \gamma'' \circ \beta + \delta$. Setzen wir jetzt $\gamma := \gamma' + \gamma''$, sind wir fertig.

Sei nun $\alpha = \gamma' \circ \beta + \delta'$, wobei $\deg(\delta') < \deg(\beta)$, eine weitere solche Zerlegung. Daraus folgt $(\gamma - \gamma') \circ \beta = \delta' - \delta$. Wegen Bemerkung 2 (i) und (ii) gilt $\deg(\gamma - \gamma') + \deg(\beta) < \deg(\beta)$, was unmittelbar $\gamma = \gamma'$ impliziert. Daraus folgt jetzt auch $\delta = \delta'$, was zeigt, dass γ, δ eindeutig bestimmt sind.

(ii) Sei $\mathfrak{a} \subseteq K\{\tau\}$ ein Linksideal. Ist $\mathfrak{a} = 0$, so ist $\mathfrak{a}$ ein Linkshauptideal und wir sind fertig. Sei jetzt $\mathfrak{a}$ nichttrivial. Dann finden wir ein $0 \neq \beta \in \mathfrak{a}$ mit minimalem Grad in $\mathfrak{a}$. Es gilt $K\{\tau\} \circ \beta \subseteq \mathfrak{a}$. Umgekehrt hat jedes $\alpha \in \mathfrak{a}$ nach (i) eine Darstellung der Form $\alpha = \gamma \circ \beta + \delta$ mit $\gamma, \delta \in K\{\tau\}$ und $\deg(\delta) < \deg(\beta)$. Da $\alpha, \gamma \circ \beta \in \mathfrak{a}$ ist auch $\delta \in \mathfrak{a}$. Da jedoch β minimalen Grad hat, ist offenbar $\delta = 0$. Somit ist $\mathfrak{a} \subseteq K\{\tau\} \circ \beta$ und daher $\mathfrak{a}$ ein Linkshauptideal. □

Definition 8. Ein Erweiterungskörper F von $\mathbb{F}_q$ heisst Funktionenkörper, falls $F/\mathbb{F}_q$ endlich erzeugt ist und Transzendenzgrad 1 hat.

Definition 9. Sei jetzt $F \supseteq \mathbb{F}_q$ ein Funktionenkörper zusammen mit einer fest gewählten diskreten Bewertung v_∞. Wir definieren A als die Teilmenge von F, die aus allen $x \in F$ besteht mit $v(x) \geq 0$ für sämtliche diskrete Bewertungen v von F, die nicht äquivalent zu v_∞ sind. Man verifiziert sofort, dass A ein Ring ist. Man kann sogar zeigen, dass A ein Dedekindring ist. Dedekindringe sind höchstens eindimensionale, noethersche, normale (= ganzabgeschlossen im Quotientenkörper) Integritätsbereiche. Beispiele von Dedekindringen sind integre Hauptidealringe.

Beispiel 10. Wir wählen $F = \mathbb{F}_q(T)$ und $v_\infty : \mathbb{F}_q(T) \to \mathbb{Z}$, $\frac{f}{g} \mapsto \deg(g) - \deg(f)$. Jede nichttriviale Bewertung, die nicht äquivalent zu v_∞ ist, muss zu einer Bewertung v_p äquivalent sein, wobei p ein irreduzibles, normiertes Polynom ist. Offensichtlich gilt dann $\mathbb{F}_q[T] \subseteq A$. Sei umgekehrt $x = g/h \in \mathbb{F}_q(T) \backslash \mathbb{F}_q[T]$ mit teilerfremden $g, h \in \mathbb{F}_q[T]$ und $h \neq 0$. Somit existiert ein irreduzibles Polynom p mit $p \mid h$ und $p \nmid g$. D.h. $v_p(x) < 0$, also $x \notin A$. Wir haben insgesammt $A = \mathbb{F}_q[T]$ gezeigt.

Definition 11. Gegeben seien der Ring A, so definiert wie in Definition 9, sowie ein Tupel (K, γ), wobei $\gamma : A \to K$ ein Homomorphismus von Ringen ist. Ein Drinfeld A-Modul über K ist ein Ringhomomorphismus

$$\phi : A \to K\{\tau\} \ , \ a \mapsto \phi_a$$

so, dass gelten:

(i) $\partial_0 \circ \phi = \gamma$

(ii) $\phi(A) \nsubseteq K$.

Bemerkung 12. Der Einfachheit halber werden wir nur Drinfeld $\mathbb{F}_q[T]$-Moduln, gemäss Beispiel 10, betrachten. In der obigen Definition kann man somit A durch $\mathbb{F}_q[T]$ ersetzen. Wenn wir von Drinfeld-Moduln sprechen, sind immer Drinfeld $\mathbb{F}_q[T]$-Moduln gemeint. Dies vereinfacht Beweise erheblich, da $\mathbb{F}_q[T]$ ein integrer Hauptidealbereich ist, also insbesondere faktoriell.

Bemerkung 13. Die Einschränkung von ϕ auf $\mathbb{F}_q$ ist gleich der Einschränkung von γ auf $\mathbb{F}_q$, da $\phi(\mathbb{F}_q) \subseteq K$ (Einheiten werden unter Ringhomomorphismen auf Einheiten abgebildet). Diese Einschränkung $\gamma|_{\mathbb{F}_q} : \mathbb{F}_q \hookrightarrow K$ ist ein Körperhomomorphismus, also insbesondere injektiv. Daher enthält K ein isomorphes Bild von $\mathbb{F}_q$. Wenn wir dieses wieder mit $\mathbb{F}_q$ identifizieren, ist ein Drinfeld $\mathbb{F}_q[T]$-Modul ϕ ein Homomorphismus von $\mathbb{F}_q$-Algebren.

Wenn wir von Algebren sprechen, beziehen wir uns auf folgende Definition.

Definition 14. Sei R ein kommutativer Ring. Ein R-Modul A zusammen mit einer R-bilinearen Verknüpfung $\cdot : A \times A \to A$ heisst eine R-Algebra. Die Algebra heisst assoziativ, falls $\cdot$ assoziativ ist. In diesem Fall ist $(A, +, \cdot)$ ein Ring. Gilt die Kommutativität der Verknüpfung $\cdot$, spricht man von einer kommutativen Algebra. Existiert ein neutrales Element, spricht man von einer unitären Algebra. Wir wollen im Folgenden stillschweigend voraussetzen, dass Algebren assoziativ, kommutativ und unitär sind.

Definition 15. Die Charakteristik eines Drinfeld-Moduls ist definiert als das Primideal

$$\mathrm{char}(\phi) := \mathfrak{p}_0 := \ker(\partial_0 \circ \phi) = \ker(\gamma) \subseteq \mathbb{F}_q[T].$$

Wir sagen, ϕ habe generische Charakteristik, wenn $\mathrm{char}(\phi) = 0$. Sonst sagen wir, ϕ habe endliche Charakteristik.

Proposition 16. Sei ϕ ein Drinfeld-Modul über K. Dann ist der Homomorphismus ϕ injektiv.

Beweis. Aus $\phi(\mathbb{F}_q[T]) \nsubseteq K$ folgt die Existenz eines $f \in \mathbb{F}_q[T]$ mit $\deg(\phi_f) > 0$. Aus $(\phi_f)^n = \phi_{f^n} \in \phi(\mathbb{F}_q[T])$ für $n \in \mathbb{N}$, folgt mit Bemerkung 2 (i), dass $\mathrm{card}(\phi(\mathbb{F}_q[T])) = \infty$. Sei widerspruchsweise $(p) = \mathfrak{p} := \ker(\phi) \neq 0$, wobei $0 \neq p \in \mathbb{F}_q[T]$. Da jedoch $\mathbb{F}_q[T]/\mathfrak{p}$ endlich ist, erhalten wir einen Widerspruch zu $\mathbb{F}_q[T]/\mathfrak{p} \cong \phi(\mathbb{F}_q[T])$. $\square$

Proposition 17. Sei ϕ ein Drinfeld-Modul über K. Dann existiert ein eindeutiges $r \in \mathbb{N}^*$ so, dass für alle $f \in \mathbb{F}_q[T]$ gilt

$$\deg(\phi_f) = -rv_\infty(f) = r\deg(f).$$

Beweis. Sei $f = \sum_{i=0}^n f_i T^i \in \mathbb{F}_q[T]$. Dann gilt $\phi_f = \phi(f) = \sum_{i=0}^n \phi(f_i) \circ (\phi_T)^i$. Da $\phi(\mathbb{F}_q[T]) \nsubseteq K$ ist $r := \deg(\phi_T) \in \mathbb{N}^*$. Mit Bemerkung 2 (i) schliessen wir $\deg(\phi_f) = \deg(\phi_T)\deg(f)$. □

Definition 18. Sei ϕ ein Drinfeld-Modul. Die Zahl r aus der obigen Proposition heisst der Rang von ϕ und wird mit $\mathrm{rank}(\phi)$ bezeichnet.

Proposition 19. Sei ϕ ein Drinfeld-Modul über K von endlicher Charakteristik $\mathrm{char}(\phi) = (p)$, für ein normiertes, irreduzibles $p \in \mathbb{F}_q[T]$. Dann existiert ein eindeutiges $h \in \mathbb{Q}_{>0}$ so, dass für alle $f \in \mathbb{F}_q[T]$ gilt

$$\mathrm{ht}(\phi_f) = hv_p(f)\deg(p).$$

Beweis. Sei $\mathrm{char}(\phi) = (p)$. Wir setzen $h := \frac{\mathrm{ht}(\phi_p)}{\deg(p)} \in \mathbb{Q}_{>0}$. Man findet für jedes $f \in \mathbb{F}_q[T]$ eine Zerlegung $f = p^n g$, wobei $p \nmid g$. Dann gilt mit Bemerkung 2 (iii) $\mathrm{ht}(\phi_f) = \mathrm{ht}(\phi_p^n) + \mathrm{ht}(\phi_g) = n\mathrm{ht}(\phi_p) = v_p(f)\mathrm{ht}(\phi_p) = hv_p(f)\deg(p)$. □

Definition 20. Sei ϕ ein Drinfeld-Modul von endlicher Charakteristik. Die Zahl h aus der obigen Proposition heisst die Höhe von ϕ und wird mit $\mathrm{height}(\phi)$ bezeichnet.

Bemerkung 21. Sei ϕ ein Drinfeld-Modul über K und sei B eine K-Algebra. Dann wird B zu einem unitären $\mathbb{F}_q[T]$-Modul bzgl. der Multiplikation $fb := \phi_f(b)$, für $f \in \mathbb{F}_q[T], b \in B$. Hier steht $\phi_f(b)$ für die Substitution $\tau \mapsto b^q$, also $\left(\sum_{i=0}^n a_i\tau^i\right)(b) := \sum_{i=0}^n a_i b^{q^i}$.

Beweis. Seien $f, f' \in \mathbb{F}_q[T]$ sowie $b, b' \in B$. Beachte, dass wegen $(1_K + \cdots + 1_K)1_B = 1_B + \cdots + 1_B$ entweder $B = 0$ oder $\mathrm{char}(B) = p$ gilt. Dann ist offensichtlich $(f + f')b = (\phi_f + \phi_{f'})(b) = fb + f'b$ sowie $1b = \tau^0(b) = b$. Seien jetzt $\phi_f = \sum_{i=0}^n f_i\tau^i$ bzw. $\phi_{f'} = \sum_{i=0}^n f_i'\tau^i$. Dann gilt $f(b+b') = \sum_{i=0}^n f_i(b+b')^{q^i} = \sum_{i=0}^n f_i(b^{q^i} + b'^{q^i}) = fb + fb'$. Schlussendlich gilt auch $f'(fb) = \sum_{i=0}^n f_i'\tau^i(\sum_{j=0}^n f_j b^{q^j}) = \sum_{k=0}^{2n}\sum_{i+j=k} f_i' f_j^{q^i} b^{q^k} = (\phi_f' \circ \phi_f)(b) = (f'f)b$. □

Definition 22. Sei $\mathfrak{a}$ ein Ideal von $\mathbb{F}_q[T]$. Dann ist

$$\ker(\phi_{\mathfrak{a}})(B) := (0 :_B \mathfrak{a}) := \{b \in B \,;\, \forall f \in \mathfrak{a} : fb = 0\}$$

ein $\mathbb{F}_q[T]$-Untermodul von B. Sind nämlich $g \in \mathbb{F}_q[T]$ und $b, b' \in \ker(\phi_{\mathfrak{a}})(B)$, so ist auch $gb + b' \in \ker(\phi_{\mathfrak{a}})(B)$, da $f(gb + b') = f(gb) + fb' = (fg)b + 0 = 0$ für alle $f \in \mathfrak{a}$ gilt. Da $\ker(\phi_{\mathfrak{a}})(B) \neq \emptyset$, ist dies tatsächlich ein Untermodul. Es handelt sich sogar um einen $\mathbb{F}_q[T]/\mathfrak{a}$-Modul. Aufgefasst als $\mathbb{F}_q[T]/\mathfrak{a}$-Modul bezeichnen wir $\ker(\phi_{\mathfrak{a}})(B)$ als den $\mathfrak{a}$-Torsionsuntermodul von B.

Definition 23. Sei $\mathfrak{a}$ ein Ideal von $\mathbb{F}_q[T]$. Die Abbildung $\ker(\phi_{\mathfrak{a}}) : K{-}\mathrm{Alg} \to \mathbb{F}_q[T]/\mathfrak{a}{-}\mathrm{Mod}$, $B \mapsto \ker(\phi_{\mathfrak{a}})(B)$ von der Kategorie der K-Algebren in die Kategorie der $\mathbb{F}_q[T]/\mathfrak{a}$-Moduln heisst der $\mathfrak{a}$-Torsionsfunktor von ϕ.

Behauptung 24. Der $\mathfrak{a}$-Torsionsfunktor $\ker(\phi_{\mathfrak{a}})$ ist ein Funktor.

Beweis. Seien B, C gegebene K-Algebren, sowie $\psi : B \to C$ ein Morphismus von K-Algebren. Wir müssen lediglich zeigen, dass die Abbildung $\ker(\phi_{\mathfrak{a}})(\psi) : \ker(\phi_{\mathfrak{a}})(B) \to \ker(\phi_{\mathfrak{a}})(C)$, $b \mapsto \psi(b)$ ein wohldefinierter Homomorphismus von $\mathbb{F}_q[T]/\mathfrak{a}$-Moduln ist, d.h. dass $\psi(\ker(\phi_{\mathfrak{a}})(B)) \subseteq \ker(\phi_{\mathfrak{a}})(C)$; die Funktoreigenschaften folgen dann sofort. Dies ist aufgrund der Eigenschaften von Morphismen von K-Algebren offensichtlich, da mit $fb = 0$ auch $f\psi(b) = \psi(fb) = 0$ folgt. $\square$

Bemerkung 25. Da $\mathfrak{a} = (f)$ für ein $f \in \mathbb{F}_q[T]$, gilt

$$\ker(\phi_{\mathfrak{a}})(B) = \ker(\phi_f)(B) := \{b \in B \ ; \ fb = 0\}.$$

Den folgenden Satz kennt man unter dem Begriff „Struktursatz für endlich erzeugte Moduln über integren Hauptidealringen“ bzw. „Hauptsatz für endlich erzeugte Moduln über integren Hauptidealringen“. Einen Beweis findet man z.B. im Bosch, Kapitel 2.9, Elementarteilertheorie.

Satz 26. Seien R ein integrer Hauptidealbereich und M ein endlich erzeugter R-Modul. Dann existiert eine endliche Menge P von paarweise nichtassoziierten Primelementen aus R sowie natürliche Zahlen d, r_p, $1 \leq \nu(p,1) \leq \ldots \leq \nu(p, r_p)$ für alle $p \in P$, so dass ein Isomorphismus

$$M \cong R^d \oplus \bigoplus_{p \in P} \bigoplus_{j_p=1}^{r_p} R/p^{\nu(p,j_p)}R$$

von R-Moduln existiert. Die Primzahlen aus P sind bis auf Einheiten eindeutig, die natürlichen Zahlen $d, r_p, \nu(p,1), \ldots, \nu(p, r_p)$ sind eindeutig.

Satz 27. Seien ϕ ein Drinfeld-Modul mit Charakteristik $\mathrm{char}(\phi) = (p)$, $p \in \mathbb{F}_q[T]$, und $\overline{K}$ ein algebraischer Abschluss von K. Dann gelten:

(i) Ist $f \in \mathbb{F}_q[T]$ ein Polynom mit $p \nmid f$, dann ist $\ker(\phi_f)(\overline{K})$ ein freier $\mathbb{F}_q[T]/(f)$-Modul vom Rang $\mathrm{rank}(\phi)$.

(ii) Ist $p \neq 0$, dann ist $\ker(\phi_{p^n})(\overline{K})$ ein freier $\mathbb{F}_q[T]/(p^n)$-Modul vom Rang $\mathrm{rank}(\phi) - \mathrm{height}(\phi)$, für alle $n \in \mathbb{N}^*$.

Beweis. Sei zunächst $f = s^n, n \in \mathbb{N}^*$, wobei $s \in \mathbb{F}_q[T]$ irreduzibel ist. Der Modul $\ker(\phi_{s^n})(\overline{K})$ hat Kardinalität $q^{n(\deg(\phi_s) - \mathrm{ht}(\phi_s))}$; dies folgt aus Proposition 6 und der Bijektivität von $\tau : \overline{K} \to \overline{K}$, $x \mapsto x^q$ (algebraisch abgeschlossene Körper sind perfekt). Nach dem Struktursatz 26 ist der endlich erzeugte $\mathbb{F}_q[T]$-Modul $\ker(\phi_{s^n})(\overline{K})$ isomorph zu einem Modul der Form

$$\mathbb{F}_q[T]^d \oplus \mathbb{F}_q[T]/(g_1) \oplus \cdots \oplus \mathbb{F}_q[T]/(g_r),$$

wobei $d, r \in \mathbb{N}$, und g_i die Potenz eines irreduziblen Polynoms ist, für alle $i = 1, \ldots, r$. Wegen der endlichen Kardinalität ist $d = 0$. Weil dies sogar ein $\mathbb{F}_q[T]/(s^n)$ Modul ist, gilt $s^n + (g_i) = (g_i)$, also $g_i \mid s^n$, für alle $i = 1, \ldots, r$. Wir haben daher gezeigt, dass

$$\ker(\phi_{s^n})(\overline{K}) \cong \mathbb{F}_q[T]/(s^{j_1}) \oplus \cdots \oplus \mathbb{F}_q[T]/(s^{j_r})$$

gilt, mit $1 \leq j_1 \leq \ldots \leq j_r \leq n$. Dieser Modul hat Kardinalität $q^{\deg(s) \sum_{i=1}^r j_i}$, woraus wir $\deg(s) \sum_{i=1}^r j_i = n(\deg(\phi_s) - \mathrm{ht}(\phi_s))$ schliessen.

(i) Sei jetzt $p \nmid s$. Dann impliziert Proposition 17 die Beziehung $\sum_{i=1}^r j_i = n\mathrm{rank}(\phi)$. Wir beweisen mit Induktion nach n, dass $r = \mathrm{rank}(\phi)$ und $j_1 = \ldots = j_r = n$ gilt. Für $n = 1$ ist die Aussage klar. Sei also $n > 1$. Es gilt die Inklusion $s \ker(\phi_{s^n})(\overline{K}) \subseteq \ker(\phi_{s^{n-1}})(\overline{K})$. Ist umgekehrt $x \in \ker(\phi_{s^{n-1}})(\overline{K})$, dann hat $\phi_s(\tau) - x \in \overline{K}[T]$ eine Nullstelle $y \in \overline{K}$; d.h. $sy = x$. Daraus folgt $y \in \ker(\phi_{s^n})(\overline{K})$, also $x \in s \ker(\phi_{s^n})(\overline{K})$. Damit ist diese Inklusion sogar eine Gleichheit. Offenbar gilt dann $s \ker(\phi_{s^n})(\overline{K}) = \ker(\phi_{s^{n-1}})(\overline{K}) \cong \mathbb{F}_q[T]/(s^{j_1 - 1}) \oplus \cdots \oplus \mathbb{F}_q[T]/(s^{j_r - 1})$. Aus der Induktionsvoraussetzung folgt nun unmittelbar die Behauptung.

Sei nun $f = s_1^{n_1} \cdots s_l^{n_l}$ eine Primfaktorzerlegung, wobei $n_i \in \mathbb{N}$ und $p \nmid s$, für $i = 1, \ldots, l$. Wir wollen nun mit Induktion nach l zeigen, dass

$$\ker(\phi_f)(\overline{K}) \cong (\mathbb{F}_q[T]/(f))^{\mathrm{rank}(\phi)}$$

gilt, und sind dann fertig. Ist $l = 1$, so haben wir die Aussage bereits oben gezeigt. Sei also $l > 1$. Zur Abkürzung setzen wir $g := s_1^{n_1} \cdots s_{l-1}^{n_{l-1}}$. Dann gilt nach Induktionsvoraussetzung $\ker(\phi_g)(\overline{K}) \cong (\mathbb{F}_q[T]/(g))^{\mathrm{rank}(\phi)}$ und $\ker(\phi_{s_l^{n_l}})(\overline{K}) \cong (\mathbb{F}_q[T]/(s_l^{n_l}))^{\mathrm{rank}(\phi)}$. Sei $x \in \ker(\phi_g)(\overline{K}) \cap \ker(\phi_{s_l^{n_l}})(\overline{K})$. Aufgrund dieser Isomorphien kann, da g und $s_{l-1}^{n_{l-1}}$ teilerfremd sind, nur $x = 0$ gelten. Daher ist $\ker(\phi_g)(\overline{K}) + \ker(\phi_{s_{l-1}^{n_{l-1}}})(\overline{K}) \subseteq \ker(\phi_f)(\overline{K})$ eine direkte Summe. Wenn wir den Chinesischen Restsatz anwenden, so sehen wir, dass $\ker(\phi_f)(\overline{K})$ einen zu

$$\ker(\phi_g)(\overline{K}) \oplus \ker(\phi_{s_{l-1}^{n_{l-1}}})(\overline{K}) \cong (\mathbb{F}_q[T]/(f))^{\mathrm{rank}(\phi)}$$

isomorphen Untermodul enthält. Da die Kardinalitäten von $(\mathbb{F}_q[T]/(f))^{\mathrm{rank}(\phi)}$ und $\ker(\phi_f)(\overline{K})$ jeweils $q^{\mathrm{rank}(\phi)\deg(f)}$ beträgt, muss bereits $\ker(\phi_f)(\overline{K}) \cong (\mathbb{F}_q[T]/(f))^{\mathrm{rank}(\phi)}$ gelten.

(ii) Sei schliesslich $s = p$ und $p \neq 0$. Dann gilt $\sum_{i=1}^r j_i = n(\mathrm{rank}(\phi) - \mathrm{height}(\phi))$, wobei wir Proposition 17 und 19 verwendet haben. Mit Induktion nach n wie in (i) zeigt man jetzt $r = \mathrm{rank}(\phi) - \mathrm{height}(\phi)$ und $j_1 = \ldots = j_r = n$, woraus wir $\ker(\phi_{p^n})(\overline{K}) \cong (\mathbb{F}_q[T]/(p^n))^{\mathrm{rank}\phi - \mathrm{height}(\phi)}$ schliessen. $\square$

Korollar 28. Sei ϕ ein Drinfeld-Modul endlicher Charakteristik. Dann ist $\mathrm{height}(\phi) \in \mathbb{N}^*$.

Beispiel 29. Ein Drinfeld-Modul über K ist bereits durch $\phi_T = \gamma(T) + c_1\tau + \cdots + c_r\tau^r$ wobei $c_1, \ldots, c_r \in K$ eindeutig festgelegt. Ist $c_r \neq 0$ handelt es sich um einen Drinfeld-Modul vom Rang r. Umgekehrt definiert jede Wahl $c_1, \ldots, c_r \in K$ mit $c_r \neq 0, r \in \mathbb{N}^*$ einen Drinfeld-Modul vom Rang r.

Beispiel 30. Sei $\gamma(T) = 0$. Dann ist $\mathrm{char}(\phi) = (T)$ und es gilt $\mathrm{height}(\phi) = \mathrm{ht}(\phi_T)$.

Definition 31. Seien ϕ und ϕ' Drinfeld $\mathbb{F}_q[T]$-Moduln über K. Ein Morphismus von ϕ nach ϕ' über K ist ein Element $\rho(\tau) \in K\{\tau\}$ mit

$$\forall f \in \mathbb{F}_q[T] : \rho \circ \phi_f = \phi'_f \circ \rho$$

Ist ρ eine Einheit, also $\rho \in K^*$, so heissen ϕ und ϕ' isomorph.

Bemerkung 32. Seien ϕ und ϕ' isomorph, d.h. es existiert ein $\rho \in K^*$ mit $\phi = \rho^{-1} \circ \phi' \circ \rho$; dies ist äquivalent zu $\phi_T = \rho^{-1} \circ \phi'_T \circ \rho$. Ist $\phi'_T = \gamma(T) + c_1\tau + \cdots + c_r\tau^r$, so ist $\phi_T = \gamma(T) + \rho^{q-1}c_1\tau + \rho^{q^2-1}c_2\tau^2 + \cdots + \rho^{q^r-1}c_r\tau^r$. Isomorphe Drinfeld-Moduln haben somit den gleichen Rang.

Beispiel 33. Sei K algebraisch abgeschlossen. Ist $r = 1$, so existiert nur eine Isomorphieklasse von Drinfeld $\mathbb{F}_q[T]$-Moduln vom Rang 1, da $K \to K : x \mapsto x^{q-1}$ surjektiv ist. Die Standardwahl, Carlitz Modul genannt, ist durch $\phi_T = \gamma(T) + \tau$ gegeben.

Proposition 34. Sei K algebraisch abgeschlossen. Dann steht die Menge der Isomorphieklassen von Drinfeld $\mathbb{F}_q[T]$-Moduln über K vom Grad 2 in Bijektion zu K.

Beweis. Sei ϕ ein Drinfeld-Modul vom Grad 2 mit $\phi_T = \gamma(T) + c_1\tau + c_2\tau^2$. Wir definieren

$$j(\phi) := \left(\frac{c_1^{q+1}}{c_2}\right) \in K.$$

Ist ϕ' isomorph zu ϕ, dann folgt mit Bemerkung 32 und wegen $(q+1) = (q^2-1)/(q-1)$, dass $j(\phi) = j(\phi')$. Sei jetzt $x \in K$. Wir wählen $c_2 = 1$. Da K algebraisch abgeschlossen ist, finden wir auch ein c_1 mit $c_1^{q+1} = x$. Somit wird der Drinfeld-Modul ϕ mit $\phi_T = \gamma(T) + c_1\tau + c_2\tau^2$ durch j auf x abgebildet. Seien nun ϕ, ϕ' Drinfeld-Moduln vom Rang 2 mit $j(\phi) = j(\phi')$. Es gilt $c_1 = 0$ genau dann, wenn $c' = 0$ gilt. Ist dies der Fall, sind ϕ und ϕ' isomorph, da $x \mapsto x^{q^2-1}$ surjektiv ist. Nehmen wir also $c_1 \neq 0 \neq c'_1$ an. Wir finden ein $\rho \in K^*$ mit $c'_1 = \rho^{q-1}c_1$. Daraus folgt dann aber auch $c'_2 = (c'_1/c_1)^{q+1} \cdot c_2 = \rho^{q^2-1}c_2$. Daher sind ϕ und ϕ' isomorph. Wir haben zusammengefasst gezeigt, dass j eine Bijektion zwischen den Isomorphieklassen von Drinfeld-Moduln vom Rang 2 und K induziert. $\square$