# 3. The Carlitz Module

We present here the details of the *Carlitz module.* This is the simplest of all Drinfeld modules and may be given in a concrete, elementary fashion. At the same time, most essential ideas about Drinfeld modules appear in the theory of the Carlitz module. Thus it is an excellent example for the reader to master and keep in mind when reading the more abstract general theory. Our basic reference is [C1], but see also [Go2].

## 3.1. Background

Let $\mathbf{A} = \mathbb{F}_r[T]$, $r = p^m$, and put $\mathbf{k} = \mathbb{F}_r(T)$. Let $v_\infty\colon \mathbf{k} \to \mathbb{R} \cup \{\infty\}$ be the valuation associated to $1/T$ as in our last section; so $v_\infty(1/T) = 1$. We denote the associated completion ("$\mathbf{k}_\infty$") of $\mathbf{k}$ by $\mathbf{K}$. The field $\mathbf{K}$ is, therefore, complete and is easily seen to be locally compact in the $1/T$-topology.

The reader will note that $\mathbf{k}$ is the field of functions on $\mathbb{P}^1/\mathbb{F}_r$, while $\mathbf{A}$ is the subring of those functions regular outside $\infty$.

**Proposition 3.1.1.** *The ring* $\mathbf{A}$ *is a discrete subring of* $\mathbf{K}$. *Moreover,* $\mathbf{K}/\mathbf{A}$ *is compact (i.e.,* $\mathbf{A}$ *is "co-compact" in* $\mathbf{K}$*).*

*Proof.* Let $a \in \mathbf{A}$ with $v_\infty(a) > 0$. Then $a = 0$. Indeed, if $v_\infty(a) > 0$, then $a$ has a zero at $\infty \in \mathbb{P}^1$; thus $a$ is regular everywhere. Therefore, it is a constant function with zeros at $\infty$. The fact that $\mathbf{A}$ is discrete in $\mathbf{K}$ follows immediately.

To see the co-compactness of $\mathbf{A}$, one has but to observe that the "polar-part" of a Laurent series in $1/T$ is precisely a polynomial in $T$. Thus $\mathbf{K}/\mathbf{A}$ is isomorphic to $\frac{1}{T}\mathbb{F}_r[[\frac{1}{T}]]$. The ring $\mathbb{F}_r[[1/T]]$ is the inverse limit of the finite rings $\mathbb{F}_r[[1/T]]/(T^{-n})$, as $n \to \infty$, and is compact. Thus so is $1/T\mathbb{F}_r[[1/T]]$. □

*Remark.* 3.1.2. Henceforth, the reader should be aware of the following basic analogy:

$$\mathbf{A} \sim \mathbb{Z}\,, \quad \mathbf{k} \sim \mathbb{Q}\,, \qquad \text{and} \qquad \mathbf{K} \sim \mathbb{R}\,.$$

Indeed, both $\mathbf{A}$ and $\mathbb{Z}$ possess division algorithms and $\mathbb{Z}$ is discrete inside $\mathbb{R}$ (= "$\mathbb{Q}_\infty$"). Moreover, $\mathbb{R}/\mathbb{Z} \simeq S^1$ is compact. This analogy is at the heart of the theory presented in this book.

Thus $\mathbf{A}$ will be the "bottom ring" of the theory described here and $\mathbf{k}$ will be the "bottom field." Of course, in the classical approach to function fields there is no bottom.

Let $\overline{\mathbf{K}}$ be a fixed algebraic closure of $\mathbf{K}$ equipped with the canonical extension of $v_\infty$. One thinks of $\overline{\mathbf{K}}$ as being analogous to $\mathbb{C}$ in that it is algebraically closed. However, it is neither locally compact *nor* complete. We let $\mathbf{C}_\infty$ be the completion of $\overline{\mathbf{K}}$. By Proposition 2.1, $\mathbf{C}_\infty$ is also algebraically closed and will be used in those occasions where a complete *and* algebraically closed field is needed.

For $d \geq 0$, we let $\mathbf{A}(d) := \{\alpha \in \mathbf{A} \mid \deg(\alpha) < d\}$; thus $\mathbf{A}(d)$ is the $d$-dimensional $\mathbb{F}_r$-vector space of polynomials of degree $< d$. Clearly

$$\mathbf{A} = \bigcup \mathbf{A}(d)\,.$$

**Definition 3.1.3.** We set, $e_0(x) = x$, and for $d > 0$

$$e_d(x) := \prod_{\alpha \in \mathbf{A}(d)} (x - \alpha) = \prod_{\alpha \in \mathbf{A}(d)} (x + \alpha)\,.$$

By Corollary 1.2.2, one sees that $e_d(x)$ is an $\mathbb{F}_r$-linear polynomial. Thus, in the notation of Section 1,

$$e_d(\tau) \in \mathbf{A}\{\tau\}\,.$$

We now want to give a closed form expression for the coefficients of $e_d(x)$.

**Definition 3.1.4.**

1. Let $i > 0$. We set
$$[i] := T^{r^i} - T \in \mathbf{A}\,.$$
2. We set $D_0 = 1$, and for $i > 0$,
$$D_i := [i][i-1]^r \cdots [1]^{r^{i-1}}\,.$$
3. We set $L_0 = 1$, and for $i > 0$,
$$L_i := [i][i-1] \cdots [1]\,.$$

The numbers $[i]$, $D_i$ and $L_i$ are fundamental for the arithmetic of $\mathbb{F}_r[T]$. Their properties will be discussed at various points in this book. We note that $\deg[i] = r^i$, $\deg D_i = ir^i$ and $\deg L_i = r \cdot \frac{(r^i-1)}{(r-1)}$ and that their valuations at $\infty$ are the negatives of these numbers.

Let $L$ be some field extension of $\mathbf{k}$ containing an indeterminate $x$. Let $\{w_0, \dots, w_d\}$ be $d+1$ elements of $L$ which are linearly independent over $\mathbb{F}_r$. As in Section 1, we set

$$\Delta(w_0, \dots, w_d) = \det \begin{pmatrix} w_0 & \cdots & w_d \\ w_0^r & \cdots & w_d^r \\ \vdots & & \vdots \\ w_0^{r^d} & \cdots & w_d^{r^d} \end{pmatrix} .$$

By Moore's formula (Corollary 1.3.7) we see that

$$\frac{\Delta(w_0, \dots, w_d)}{\Delta(w_0, \dots, w_{d-1})} = \prod_{\{\beta_j\} \subseteq \mathbb{F}_r} (w_d + \beta_0 w_0 + \cdots + \beta_{d-1} w_{d-1}) .$$

We now substitute $x$ for $w_d$ and $T^i$ for $w_i$, $i = 0, \dots, d-1$. We obtain

$$\prod_{\alpha \in \mathbf{A}(d)} (x + \alpha) = \frac{\Delta(1, \dots, T^{d-1}, x)}{\Delta(1, \dots, T^{d-1})} .$$

Write

$$\Delta(1, \dots, T^{d-1}, x) = \sum_{j=0}^{d} (-1)^{d-j} x^{r^j} M_j ,$$

where $M_j$ is the determinant of the minor obtained by crossing out the last column and $j^{\text{th}}$ row. The reader will readily see that $M_j$ is a determinant of Vandermonde type. Therefore,

$$\begin{aligned} M_j &= \prod_{h>i} (T^{r^h} - T^{r^i}), \qquad h, i = 1, \dots, d; \quad h \neq j, \quad i \neq j \\ &= \frac{\prod\limits_{h>i} (T^{r^h} - T^{r^i})}{\prod\limits_{h>j} (T^{r^h} - T^{r^j}) \prod\limits_{i<j} (T^{r^j} - T^{r^i})} \\ &= \left( \prod_{i=1}^{d} D_i \right) \Bigg/ D_j L_{d-j}^{r^j} . \end{aligned}$$

In a similar fashion, one finds

$$\Delta(1, \dots, T^{d-1}) = \prod_{i=1}^{d-1} D_i .$$

Thus, we obtain the following results of Carlitz.

**Theorem 3.1.5 (Carlitz).** *We have*

$$e_d(x) = \prod_{\alpha \in \mathbf{A}(d)} (x+\alpha) = \sum_{i=0}^{d} (-1)^{d-i} x^{r^i} \frac{D_d}{D_i L_{d-i}^{r^i}}\,. \qquad \square$$

The reader should immediately note that the coefficients $D_d/D_iL_{d-i}^{r^i}$ are actually integral, i.e., $\in \mathbf{A}$. Indeed, this is a trivial consequence of the product expansion for $e_d(x)$. We sometimes denote these coefficients by "$\begin{bmatrix} d \\ i \end{bmatrix}$" or "$\begin{bmatrix} d \\ i \end{bmatrix}_{\mathbf{A}}$".

Theorem 3.1.5 is so basic that we present a rather different derivation of it without using the Moore Determinant.

We begin by presenting some properties of $D_i$ and $L_i$ that are "factorial-like;" for more such formulas we refer the reader to Subsection 9.1.

**Proposition 3.1.6.**

1. $[i] = \prod_{\substack{f \text{ monic prime} \\ \deg(f) \mid i}} f$.
2. $D_i = [i]D_{i-1}^r$.
3. $D_i = \prod_{\substack{g \text{ monic} \\ \deg g = i}} g$.
4. $L_i$ *is the least common multiple of all polynomials of degree* $i$.

*Proof.* 1. Note that

$$\frac{d}{dT}[i] = -1\,.$$

Thus $[i]$ is a separable polynomial. Part 1 is now an elementary exercise in the use of finite fields. Part 2 follows immediately from the definition. Parts 3 and 4 follow from Part 1 upon counting the number of times a given monic prime $f$ divides the product of all monic polynomials of degree $i$ (or, for Part 4, their least common multiplier). □

**Corollary 3.1.7.** $e_d(h) = D_d$ *for any monic polynomial* $h$ *of degree* $d$.

*Proof.* A monic $g$ of degree $d$ can be uniquely written as $g = h + \alpha$, $\deg \alpha < d$. Thus the result follows from 3.1.6.3. □

*Second Proof of* Theorem 3.1.5. We claim that $e_d(x)$ may be written as

$$e_d(x) = e_{d-1}^r(x) - D_{d-1}^{r-1} e_{d-1}(x)\,. \qquad (*)$$

Both sides of the above equation are monic of the same degree. Thus we need only establish that they have the same set of roots $= \mathbf{A}(d)$. Thus let $\alpha \in \mathbf{A}(d)$. If $\alpha \in \mathbf{A}(d-1)$, then clearly $\alpha$ is a root of $*$. Thus assume that

$$\alpha = \zeta h\,,$$

with $\zeta \in \mathbb{F}_r^*$, and $\deg h = d-1$. By 3.1.7, the right hand side of $*$ is

$$\zeta^r D_{d-1}^r - D_{d-1}^{r-1}\zeta D_{d-1} = 0\,,$$

as $\zeta^r = \zeta$. The result now follows by using induction and the properties of $D_i$ and $L_i$. □

## 3.2. The Carlitz Exponential

In this subsection, we "pass to the limit" (as $d \to \infty$) in the formula we have obtained for $e_d(x)$ to obtain the *Carlitz exponential.*

From Theorem 3.1.5, we have

$$\prod_{\alpha\in\mathbf{A}(d)} (x+\alpha) = \sum_{j=0}^{d} (-1)^{d-j} x^{r^j} \frac{D_d}{D_j L_{d-j}^{r^j}}\,.$$

By 3.1.6.3, we have

$$D_i = \prod_{\substack{\deg g = i\\ g \text{ monic}}} g\,.$$

Thus

$$\begin{aligned}\prod_{\deg g=i} g &= \prod_{\substack{\deg g = i\\ g \text{ monic}}} g^{r-1}\left(\prod_{\zeta\in\mathbb{F}_r^*}\zeta\right)\\ &= \prod_{\substack{\deg g = i\\ g \text{ monic}}} -g^{r-1} = (-1)^{r^i}\prod_{\substack{\deg g = i\\ g \text{ monic}}} g^{r-1}\\ &= -D_i^{r-1}\,.\end{aligned}$$

Consequently,

$$\begin{aligned}\prod_{0\neq\alpha\in\mathbf{A}(d)} \alpha &= (-1)^d (D_0\cdots D_{d-1})^{r-1}\\ &= (-1)^d D_d/L_d\,.\end{aligned}$$

We now divide the formula of Theorem 3.1.5 by $\prod\limits_{0\neq\alpha\in\mathbf{A}(d)} \alpha$. We obtain

$$x\prod_{0\neq\alpha\in\mathbf{A}(d)}(1+x/\alpha) = \sum_{j=0}^{d}(-1)^j \frac{x^{r^j}}{D_j}\,\frac{L_d}{L_{d-j}^{r^j}}\,.$$

Let us put

$$\xi_d := \frac{[1]^{\frac{r^d-1}{r-1}}}{L_d}\,.$$

**Lemma 3.2.1.** *We have*

$$\xi_d = \prod_{j=1}^{d-1}(1-[j]/[j+1])\,.$$

*Proof.* Note that

$$\prod_{j=1}^{d-1}(1-[j]/[j+1]) = \prod_{j=1}^{d-1}\left(\frac{[j+1]-[j]}{[j+1]}\right)\,.$$

Now $[j+1]-[j]=[1]^{r^j}$. Thus,

$$\prod_{j=1}^{d-1}\left(\frac{[j+1]-[j]}{[j+1]}\right) = \prod_{j=1}^{d-1}\frac{[1]^{r^j}}{[j+1]} = \frac{\prod\limits_{j=0}^{d-1}[1]^{r^j}}{L_d}\,.$$

But $\sum\limits_{j=0}^{d-1} r^j = \frac{r^d-1}{r-1}$ giving the result. □

Thus we see that the sequence $\{\xi_d\}_{d=1}^{\infty}$ has a limit in $\mathbf{K}$ which we denote by $\xi_*$. By Lemma 3.2.1 we see that

$$\xi_* = \prod_{j=1}^{\infty}\left(1-\frac{[j]}{[j+1]}\right)\,.$$

Note that $\xi_*$ is clearly a 1-unit in $\mathbf{K}$ (i.e., it is a unit in the ring $R_{\mathbf{K}} = \{x \in \mathbf{K} \mid v_\infty(x) \geq 0\}$ and is congruent to 1 modulo the maximal ideal $M_{\mathbf{K}} = \{x \in \mathbf{K} \mid v_\infty(x) > 0\}$). In particular, $v_\infty(\xi_*) = 0$.

Let $d > 0$.

**Lemma 3.2.2.**

1. $v_\infty(\xi_{d+1}-\xi_d) = r^d(r-1)$.
2. *Set* $\delta_d := \xi_d - \xi_*$. *Then*

$$v_\infty(\delta_d) = r^d(r-1)\,.$$

*Proof.* Note that

$$\xi_{d+1}-\xi_d = -\frac{[d]}{[d+1]}\xi_d\,.$$

Thus

$$v_\infty(\xi_{d+1} - \xi_d) = r^{d+1} - r^d$$

giving Part 1.

To see Part 2, note that

$$-\delta_d = (\xi_{d+1} - \xi_d) + (\xi_{d+2} - \xi_{d+1}) + \cdots .$$

Thus, Part 2 follows from Part 1. □

Set $\beta_j := [1]^{\frac{r^j-1}{r-1}}$ and so $\xi_d = \frac{\beta_d}{L_d}$.

**Lemma 3.2.3.**

$$\frac{L_d}{L_{d-j}^{r^j}} = \frac{\beta_j \xi_{d-j}^{r^j}}{\xi_d}\,.$$

*Proof.* The right hand side of the statement of the lemma is equal to

$$\frac{[1]^{\frac{r^j-1}{r-1}} L_d [1]^{r^j\left(\frac{r^{d-j}-1}{r-1}\right)}}{[1]^{\frac{r^d-1}{r-1}} L_{d-j}^{r^j}}\,.$$

But $0 = r^j - 1 + r^j(r^{d-j} - 1) - (r^d - 1)$. □

Thus from Lemma 3.2.3, we see that

$$\begin{aligned} x \prod_{0 \neq \alpha \in \mathbf{A}(d)} (1 + x/\alpha) &= x \prod_{0 \neq \alpha \in \mathbf{A}(d)} (1 - x/\alpha) \\ &= \sum_{j=0}^{d} (-1)^j \frac{x^{r^j}}{D_j}\, \frac{L_d}{L_{d-j}^{r^j}} \\ &= \sum_{j=0}^{d} (-1)^j \frac{x^{r^j}}{D_j} \beta_j \frac{\xi_{d-j}^{r^j}}{\xi_d} \\ &= \frac{1}{\xi_d} \sum_{j=0}^{d} (-1)^j \frac{x^{r^j}}{D_j} \beta_j \xi_{d-j}^{r^j}\,. \end{aligned}$$

Recalling that $\delta_j = \xi_j - \xi_*$, we find that the above equals

$$\frac{1}{\xi_d} \sum_{j=0}^{d} (-1)^j \frac{x^{r^j}}{D_j} \beta_j (\delta_{d-j}^{r^j} + \xi_*^{r^j})\,.$$

**Lemma 3.2.4.** *For any $x \in \mathbf{C}_\infty$, as $d \to \infty$*

$$\sum_{j=0}^{d}(-1)^j \frac{x^{r^j}}{D_j}\beta_j \delta_{d-j}^{r^j} \to 0$$

*in $\mathbf{C}_\infty$.*

*Proof.* Note that

$$v_\infty(D_j) = -jr^j$$

and

$$v_\infty(\beta_j) = -r\frac{(r^j-1)}{r-1}\,.$$

Thus, by Lemma 3.2.2, we find

$$\begin{aligned} v_\infty\left((-1)^j\frac{x^{r^j}}{D_j}\beta_j\delta_{d-j}^{r^j}\right) &= r^j v_\infty(x) + jr^j - r\frac{(r^j-1)}{r-1} + r^j r^{d-j}(r-1) \\ &= \frac{r^j((v_\infty(x)+j+r^{d-j}(r-1))(r-1)-r)+r}{r-1}\,. \end{aligned}$$

We now split

$$\sum_{j=0}^{d}(-1)^j\frac{x^{r^j}}{D_j}\beta_j\delta_{d-j}^{r^j}$$

into two sums, $\sum_1 + \sum_2$, where $\sum_1 := \sum_{2j<d}$, and $\sum_2 := \sum_{2j\geq d}$. With a little thought, one checks that both $\sum_1$ and $\sum_2$ tend to 0 as $d \to \infty$. This gives the lemma. □

**Lemma 3.2.5.** *For any $x \in \mathbf{C}_\infty$, the series*

$$\sum_{j=0}^{\infty}(-1)^j\frac{x^{r^j}}{D_j}\beta_j\xi_*^{r^j}$$

*converges in $\mathbf{C}_\infty$.*

*Proof.* This follows as in the proof of Lemma 3.2.4. □

**Corollary 3.2.6.** *Let $x \in \mathbf{C}_\infty$. Then*

$$x\prod_{0\neq\alpha\in\mathbf{A}}(1-x/\alpha) = \frac{1}{\xi_*}\sum_{j=0}^{\infty}\frac{x^{r^j}}{D_j}(-1)^j\beta_j\xi_*^{r^j}\,.$$

*Proof.* This follows from Lemma 3.2.4 and 3.2.5 and the expression for the left hand side given above. □

**Definition 3.2.7.** 1. Let $\lambda$ be any $(r-1)$-st root of $-[1]$ in $\overline{\mathbf{K}}$. Then we set

$$\xi := \xi_C = \lambda\xi_* \,.$$

2. Let $x \in \mathbf{C}_\infty$. Then we set

$$e_C(x) = \sum_{j=0}^{\infty} \frac{x^{r^j}}{D_j} \,.$$

(This sum converges to an element of $\mathbf{C}_\infty$ as in the proof of Lemma 3.2.5.) The function $e_C(x)$ is the *Carlitz exponential.*

Summarizing, we have the following result due to Carlitz.

**Theorem 3.2.8.** *Let $x \in \mathbf{C}_\infty$. Then*

$$x \prod_{0\neq\alpha\in\mathbf{A}} (1 - x/\alpha) = \frac{1}{\xi} \sum \frac{(\xi x)^{r^j}}{D_j} = \frac{1}{\xi} e_C(\xi x) \,. \qquad \square$$

**Corollary 3.2.9.** *Put $L := \xi\mathbf{A} \in \overline{\mathbf{K}}$. Then for all $x \in \mathbf{C}_\infty$, we have*

$$x \prod_{0\neq\alpha\in L} (1 - x/\alpha) = e_C(x) \,.$$

*Proof.* If we substitute $x/\xi$ for $x$ in 3.2.8, we obtain

$$\frac{1}{\xi} e_C(x) = \frac{x}{\xi} \prod_{0\neq\alpha\in L} (1 - x/\alpha) \,,$$

which is equivalent to the statement of the corollary. □

*Remarks.* 3.2.10. 1. Note that Corollary 3.2.9 gives the factorization of $e_C(x)$ guaranteed by Theorem 2.14.
2. Let $0 \neq \alpha \in L$, $\alpha \in L = \xi\mathbf{A}$. As $\xi_* \in \mathbf{K}$, we see that

$$\mathbf{K}(\alpha) = \mathbf{K}(\lambda) \,,$$

and $\mathbf{K}(\lambda)$ is separable over $\mathbf{K}$. This is in keeping with 2.10.3.
3. By using the binomial theorem, for instance, we can choose an $(r-1)$-st root $\theta$ of $(1 - T^{1-r})$ in $\mathbf{K}$ which is a 1-unit. It is simple to see that $\theta$ is unique. We set

$$\xi_u = \theta\xi_* \,;$$

the element $\xi_u$ is a 1-unit. Thus

$$\xi = \sqrt[r-1]{-T^r} \cdot \xi_u \,.$$

The reader will immediately see the analogy with

$$2\pi i = 2i\pi\,.$$

For more properties of $\xi$ we refer the reader to Subsection 9.4.
4. We have normalized $e_C(x)$ in a slightly different fashion than in Carlitz's original paper. We do this in order to have a simpler time using $e_C(x)$ to describe abelian extensions.
5. The element $\xi$ was shown to be transcendental over $\mathbf{k}$ by L.I Wade [Wad1].

## 3.3. The Carlitz Module

We now use $e_C(x)$ to describe a new module action of $\mathbf{A} = \mathbb{F}_r[T]$ on $\mathbf{C}_\infty$. This action is called the *Carlitz module.* It is the simplest example of a Drinfeld module.

**Proposition 3.3.1.** *Let $x \in \mathbf{C}_\infty$. Then*

$$e_C(Tx) = Te_C(x) + e_C(x)^r\,.$$

*Proof.* We have

$$e_C(x) = \sum_{i=0}^{\infty} \frac{x^{r^i}}{D_i}\,.$$

So

$$e_C(Tx) = \sum_{i=0}^{\infty} T^{r^i} \frac{x^{r^i}}{D_i}\,,$$

or

$$e_C(Tx) - Te_C(x) = \sum_{i=0}^{\infty} (T^{r^i} - T) \frac{x^{r^i}}{D_i}\,.$$

But $D_i = (T^{r^i} - T)D_{i-1}^r$; so

$$e_C(Tx) - Te_C(x) = \sum_{i=1}^{\infty} \frac{x^{r^i}}{D_{i-1}^r} = \left( \sum_{i=0}^{\infty} \frac{x^{r^i}}{D_i} \right)^r\,. \qquad \square$$

Let $a \in \mathbf{A}$ with $a = \sum_{j=0}^{d} a_j T^j$, $\{a_j\} \subseteq \mathbb{F}_r$, $a_d \neq 0$.

**Corollary 3.3.2.** *Let $x \in \mathbf{C}_\infty$. Then*

$$e_C(ax) = ae_C(x) + \sum_{j=1}^{d} C_a^{(j)} e_C(x)^{r^j}$$

*where $\{C_a^{(j)}\} \subset \mathbf{A}$ and $C_a^{(d)} = a_d$.*

*Proof.* Note that for $i \geq 1$,

$$e_C(T^i x) = e_C(T(T^{i-1}x))\,.$$

Thus $\{C_{T^i}^{(j)}\}$ can be computed via recursion. For instance,

$$\begin{aligned} e_C(T^2 x) &= T e_C(Tx) + e_C(Tx)^r \\ &= T(Te_C(x) + e_C(x)^r) + (Te_C(x) + e_C(x)^r)^r \\ &= T^2 e_C(x) + (T^r + T)e_C^r(x) + e_C(x)^{r^2}\,. \end{aligned}$$

Thus the coefficients for $e_C(ax)$ can now be computed using $\mathbb{F}_r$-linearity. The result follows easily. □

As in Section 1, let $\tau\colon \mathbf{C}_\infty \to \mathbf{C}_\infty$ be the $r^{\text{th}}$ power mapping, $\tau(x) = x^r$, and, for any subfield $M$ of $\mathbf{C}_\infty$, we let $M\{\tau\}$ be the composition ring of $\mathbb{F}_r$-linear polynomials.

**Definition 3.3.3.** Let $\{C_a^{(j)}\}$ be as in Corollary 3.3.2. Then we set

$$C_a(\tau) = a\tau^0 + \sum_{j=1}^{d} C_a^{(j)}\tau^j\,,$$

where $d = \deg a$.

Thus, we have the fundamental functional equation for $e_C(x)$

$$e_C(ax) = C_a(e_C(x))\,.$$

**Theorem 3.3.4.** *The mapping from* $\mathbf{A}$ *to* $\mathbf{k}\{\tau\}$*,* $a \mapsto C_a$*, is an injection of* $\mathbb{F}_r$*-algebras.*

*Proof.* It is clear that the map $a \mapsto C_a$ is $\mathbb{F}_r$-linear and injective. Thus we need only show that it is a mapping of algebras; i.e., for $a, b \in \mathbf{A}$

$$C_{ab} = C_a \cdot C_b\,,$$

where $C_a \cdot C_b$ is the multiplication in $\mathbf{k}\{\tau\}$ (and so is multiplication of additive polynomials). But

$$C_{ab}(e_C(x)) = e_C(abx) = e_C(a(bx)) = C_a(e_C(bx)) = C_a(C_b(e_C(x)))\,,$$

which gives the result. □

**Definition 3.3.5.** We call the mapping $\mathbf{A} \mapsto \mathbf{k}\{\tau\}$, $a \mapsto C_a$, the *Carlitz module.* It is denoted by "$C$."

*Remarks.* 3.3.6. 1. In fact, with the obvious definitions, $C_a \in \mathbf{A}\{\tau\}$ for all $a \in \mathbf{A}$.
2. What is "really" going on with the Carlitz module is the following: from Theorem 2.14, one knows that every non-constant entire function (in non-Archimedean analysis) is *surjective.* Let $L = \mathbf{A}\xi$ be the zeros of $e_C(x)$; we then have an isomorphism

$$\mathbf{C}_\infty / L \xrightarrow{\sim} \mathbf{C}_\infty$$

via $e_C(x)$. Now the group on the left is obviously an $\mathbf{A}$-module; thus by transport of structure, we obtain a new $\mathbf{A}$-action on $\mathbf{C}_\infty$. This action *is* the Carlitz module.
3. If one recalls that $D_i = \prod_{\substack{g \text{ monic} \\ \deg g = i}} g$, one sees immediately that $e_C(x)$ is analogous to the classical exponential function

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

*except* that the expansion for $e_C(x)$ only involves the monomials $\{x^{r^i}\}$. In particular, the Carlitz module is an $\mathbf{A}$-analog of the multiplicative group $\mathbb{G}_m$ (as algebraic group) with the usual $\mathbb{Z}$-action. This analogy will be used very often in this work.

**Definition 3.3.7.** The *division values* (or *division points*) of the Carlitz module (or exponential) are the values $\{e_C(a\xi) \mid a \in \mathbf{k}\} \subset \mathbf{C}_\infty$.

Let $a = b/f \in \mathbf{k}$, $\{b, f\} \subset \mathbf{A}$ with $f \neq 0$. Then $e_C(a\xi)$ is a root of $C_f(x) = 0$; thus it belongs to the algebraic closure of $\mathbf{k}$ in $\mathbf{C}_\infty$.

For now, we establish the following weak, but very important, result. The reader should immediately see the analogy with cyclotomic fields.

**Proposition 3.3.8.** *Let $L \subseteq \mathbf{C}_\infty$ be an extension of $\mathbf{k}$. Let $a \in \mathbf{k}$ and let*

$$L_1 = L(e_C(a\xi))\,.$$

*Then $L_1$ is an abelian extension of $L$.*

*Proof.* Let $a = b/f$ be an irreducible rational function. Then

$$e_C\left(\frac{b}{f}\xi\right) = C_b(e_C(\xi/f))\,;$$

thus $L_1 \subseteq L(e_C(\xi/f))$. Thus, by the standard arguments of Galois theory, we may assume that $L_1 = L(e_C(\xi/f))$. Put $\rho := e_C(\xi/f)$.

Since the coefficients of $C_g(\tau)$ are in $\mathbf{A}$ for all $g$, we see immediately that $L_1$ contains *all* values

$$e_C\left(\frac{g}{f}\xi\right)\ ;$$

i.e., $L_1$ contains all $f$-division points. As an $\mathbf{A}$-module, the Carlitz exponential assures us that the $\mathbf{A}$-module of $f$-division points is isomorphic to $\mathbf{A}/(f)$.

Since $L_1$ contains all $f$-division points, it is easy to see that it is Galois over $L$. Let $G$ be the Galois group. As $C_g(\tau) \in \mathbf{A}\{\tau\}$ for all $g$, we see that the action of $G$ on the $f$-division points *commutes* with the action of $\mathbf{A}$. Thus, for $\sigma \in G$, we see that $\sigma(\rho)$ is also an $\mathbf{A}$-module generator of the $f$-division points. We, therefore, obtain an injection $G \hookrightarrow \mathbf{A}/(f)^*$ giving the result. □

**Definition 3.3.9.** Let $g \in \mathbf{A}$. We set

$$C[g] := \left\{e_C\left(\frac{b}{g}\xi\right) \mid b \in \mathbf{A}\right\} \subset \mathbf{C}_\infty\,.$$

We call $C[g]$ the *module of $g$-division points.* It is $\mathbf{A}$-module isomorphic to $\mathbf{A}/(g)$. A generator of $C[g]$ as an $\mathbf{A}$-module is called a *primitive $g$-th division point.*

We have seen that, as $\mathbf{A}$-module, $C[g] \simeq \mathbf{A}/(g)$. Note also that if $\zeta \in \mathbb{F}_r^*$, then

$$C[g] = C[\zeta g]\,.$$

Thus, $C[g]$ depends *only* on the *ideal* in $\mathbf{A}$ generated by $g$. Consequently let $I \subseteq \mathbf{A}$ be an ideal. We set

$$C[I] := C[i]\,,$$

for *any* generator $i$ of $I$.

Finally we finish this section with a formula for the coefficients $\{C_a^{(j)}\}$ of $C_a(\tau)$ as in [Go3]. Our next section will present another formula due to Carlitz.

Let $a \in \mathbf{A}$ and, as above, put

$$C_a(\tau) = a\tau^0 + \sum_{j=1}^{d} C_a^{(j)}\tau^j\,.$$

For the moment and for the sake of simplicity let us put

$$a_j := C_a^{(j)}\,.$$

**Proposition 3.3.10.** *Let $a$, $a_j$, etc. be as above. Then we have*

$$a_1 = \frac{a^r - a}{T^r - T}\,,\quad a_2 = \frac{a_1^r - a_1}{T^{r^2} - T}\,,\ldots,\, a_i = \frac{a_{i-1}^r - a_{i-1}}{T^{r^i} - T}\,,\ldots\,.$$

*Moreover, if $a = \zeta f$, for $\zeta \in \mathbb{F}_r^*$ and $f$ monic of degree $d$, then $a_d = \zeta$.*

Before turning to the proof, we remark that once $a_d = \zeta$, then $a_{d+1} = a_{d+2} = \cdots = 0$.

*Proof.* Write $C_a = a\tau^0 + \chi_a$, where $\chi_a \in \mathbf{A}\{\tau\}$. Thus, $\chi_T = \tau$. Now $C_aC_T = C_TC_a$ in $\mathbf{k}\{\tau\}$. Therefore,

$$(a\tau^0 + \chi_a)C_T = C_T(a\tau^0 + \chi_a)\,,$$

or

$$C_Ta\tau^0 - a\tau^0C_T = \chi_aC_T - C_T\chi_a\,. \tag{$*$}$$

The result now follows upon equating coefficients of $\tau^j$ on both sides of the above equation. □

*Remarks.* 3.3.11. 1. One sees that $a_i \neq 0$ for $i = 1, \ldots, d$. Moreover, $\deg(a_i)$ can be easily found from the proposition.
2. Let $u, v \in \mathbf{k}\{\tau\}$ and set, as usual,

$$[u, v] = uv - vu\,.$$

One sees easily that, as $[u, v]$ is the commutator, the map $v \mapsto [u, v]$ is a derivation of $\mathbf{k}\{\tau\}$. (Indeed: $u(v_1v_2) - (v_1v_2)u = (uv_1 - v_1u)v_2 + v_1(uv_2 - v_2u)$.) Moreover, the equation $(*)$ given just above can be written

$$[C_T, a\tau^0] = -[C_T, \chi_a]\,.$$

One thinks of this equation as being a *derivation equation* which defines the Carlitz module.
3. Proposition 3.3.10 is different from the one in [Go3] due to our normalization of $e_C(x)$.

## 3.4. The Carlitz Logarithm

Recall that

$$e_C(x) = \sum_{i=0}^{\infty} \frac{x^{r^i}}{D_i}\,,$$

$D_0 = 1$. Thus the derivative $e'_C(x)$ is identically 1. Consequently, we may formally derive an *inverse* for $e_C(x)$ about the origin with a non-trivial radius of convergence. We call this function "$\log_C(x)$." It is clearly $\mathbb{F}_r$-linear, as $e_C(x)$ is.

By definition, as formal power series,

$$e_C(\log_C(x)) = \log_C(e_C(x)) = x\,,$$

(see, [C1], Theorem 6.1). Now, $e_C(x)$ has the functional equation,

$$e_C(Tx) = Te_C(x) + e_C(x)^r\,.$$

Thus

$$\log_C(e_C(Tx)) = Tx = \log_C(Te_C(x)) + \log_C(e_C(x)^r)\,.$$

Substituting $\log_C(x)$ for $x$, we obtain

$$T\log_C(x) = \log_C(Tx) + \log_C(x^r)\,.$$

As $\log'_C(x)$ is also identically 1, one finds

$$\begin{aligned}\log_C(x) &= x + \frac{x^r}{-[1]} + \frac{x^{r^2}}{[1][2]} + \frac{x^{r^3}}{-[1][2][3]} + \cdots \\ &= \sum_{i=0}^{\infty}(-1)^i\frac{x^{r^i}}{L_i}\,.\end{aligned}$$

Recall that in Definition 2.3 we discussed the order of convergence of a non-Archimedean power series – the order of convergence being the valuation theoretic version of the standard radius of convergence.

**Proposition 3.4.1.** *The order of convergence of* $\log_C(x)$*,* $\rho(\log_C(x))$*, is* $-\frac{r}{r-1} = \frac{r}{1-r}$.

*Proof.* This follows immediately once one notices that

$$v_\infty(L_i) = r\frac{(1-r^i)}{(r-1)}\,. \qquad \square$$

The reader should note that

$$v_\infty(\xi) = -\frac{r}{r-1}\,.$$

Thus the logarithm converges "up to the smallest non-zero period of $e_C(x)$."

## 3.5. The Polynomials $E_d(x)$

In this subsection, we present another formula for the Carlitz module due to Carlitz [C1]. Our exposition is modeled on that of [AT1].

Let $\log(x)$, $e^x$ be the usual complex-valued functions. Simple calculus gives the identity

$$(1+t)^x = e^{x\log(1+t)}\,,$$

which one expands about $t = 0$ as

$$(1+t)^x = \sum_{n=0}^{\infty}\binom{x}{n}t^n\,.$$

Of course $\left\{\binom{x}{n}\right\}$ are the binomial polynomials

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}\,.$$

We now do a very similar thing with the Carlitz module. Let $e_C(x)$ and $\log_C(x)$ be the Carlitz exponential and logarithm as in the previous subsections.

**Definition 3.5.1.** We set

$$e_C(z\log_C(x)) = \sum_{j=0}^{\infty} E_j(z)x^{r^j}\,.$$

Note that, as $e_C(x)$ is entire, $e_C(z\log(x))$ converges (at least) for all $\{(z,x)\}$ with $v_\infty(x) > \frac{r}{1-r}$ by Proposition 3.4.1.

**Proposition 3.5.2.**

1. *$E_j(z)$ is an $\mathbb{F}_r$-linear polynomial of degree $r^j$.*
2. *$E_j(a) = 0$ for all $a \in \mathbf{A}(j)$.*
3. *$E_j(T^j) = 1$.*

*Proof.* Part 1 follows from the power series definition of $E_j(z)$. To see Part 2, put $z = a \in \mathbf{A}(j)$. Then

$$e_C(a\log_C(x)) = C_a(e_C(\log_C(x))) = C_a(x)$$

is a polynomial in $x$ of degree $r^{\deg(a)} < r^j$. Thus $E_j(a) = 0$. Now set $a = T^j$. Then the above formula and our knowledge of $C_{T^j}(x)$ imply that $E_j(T^j) = 1$ giving Part 3. □

**Corollary 3.5.3.** *We have $E_j(z) = \dfrac{e_j(z)}{D_j}$.*

*Proof.* The polynomial $e_j(z)$ has degree $r^j$. Its zero set is $\mathbf{A}(j)$. Finally by 3.1.7 we see that

$$\frac{e_j(T^j)}{D_j} = 1\,.$$

We therefore obtain the corollary. □

**Corollary 3.5.4 (Carlitz).** *Let $\{C_a^{(j)}\}$ be as in* Definition 3.3.2. *Then, for all $j$,*

$$C_a^{(j)} = E_j(a) = \frac{e_j(a)}{D_j}\,.$$

*Proof.* We have seen that

$$e_C(a \log_C(x)) = C_a(x) = \sum_{j=0}^{\infty} E_j(a) x^{r^j} .$$

Thus the result follows from 3.5.3. □

**Corollary 3.5.5 (Carlitz).** *Let* $a \in \mathbf{A}$. *Then* $e_j(a)/D_j \in \mathbf{A}$ *also.*

*Proof.* The coefficients of $C_a(x)$ are in $\mathbf{A}$. □

Corollary 3.5.4 gives another description of the coefficients of $C_a$. It should be compared with Proposition 3.3.10. In fact, it would be interesting to know the exact relationship between the two. Moreover, Corollary 3.5.5 shows how close the analogy between $E_j(z)$ and $\binom{x}{j}$ really is.

## 3.6. The Carlitz Module over Arbitrary A-fields

We now want to study the Carlitz module over arbitrary fields, not just those containing $\mathbf{k}$. Let $L$ be a field containing $\mathbb{F}_r$. As with $\mathbf{k}$, it is reasonable to expect that the Carlitz module over $L$ will give rise to a map $\mathbf{A}$ to $L\{\tau\}$. If we compose this map with the derivative map $L\{\tau\} \to L$ (i.e., the ring homomorphism $L\{\tau\} \to L$ given by taking an $\mathbb{F}_r$-linear polynomial to its coefficient of $\tau^0$) we obtain our first definition.

**Definition 3.6.1.** Let $L$ be a field. We say that $L$ is an $\mathbf{A}$-field if and only if there is a morphism $\iota\colon \mathbf{A} \to L$. Let $\wp = \ker(\iota)$. We call $\wp$ the *characteristic* of $L$. We say that $L$ has *generic characteristic* if and only if $\wp = (0)$.

Thus if $L$ has generic characteristic, then $L$ contains $\mathbf{k}$ as a subfield. Let $\overline{L}$ be a fixed algebraic closure of $L$ with the $\mathbf{A}$-structure coming from $\iota$.

The procedure for considering the Carlitz module over $L$ is now clear: One simply applies $\iota$ to the coefficients of $C_a(\tau)$, for $a \in \mathbf{A}$ — which are elements of $\mathbf{A}$ — to obtain elements in $L\{\tau\}$.

Let $a \in \mathbf{A}$. Note that

$$C_a'(x) = \iota(a) .$$

Thus if $a \notin \wp$, then $C_a(x)$ is still a separable polynomial. Note also the similarity between the above normalization and the standard normalization in the theory of complex multiplication of elliptic curves.

Via $C$, the field $\overline{L}$ now becomes an $\mathbf{A}$-module: Let $a \in \mathbf{A}$ and $\alpha \in \overline{L}$. Then we have

$$(a, \alpha) \mapsto C_a(\alpha) .$$

One says that $\alpha$ is an "$a$-torsion point" if and only if $C_a(\alpha) = 0$ and so on. One sets $C[a] \subset \overline{L}$ to be the roots of $C_a(x) =$ the module of $a$-torsion points.

As before, one sees that $C[a]$ depends only on the ideal generated by $a$. And, if $I=(i)$ is an $\mathbf{A}$-ideal, then we set

$$C[I] := C[i]\,.$$

In general, if $K$ is any $\mathbf{A}$-field, we will use the notation "$C(K)$" to denote $K$ viewed as $\mathbf{A}$-module via $C$.

Our main goal in this subsection is to describe the torsion points of $C$ in $C(\overline{L})$ as $\mathbf{A}$-modules. The reader will note the similarity between our arguments and those standard ones used classically for roots of unity.

**Theorem 3.6.2.**

1. *Let* $a \notin \wp = \ker(\iota)$. *Then* $C[a] \subset C(\overline{L})$ *is isomorphic to* $\mathbf{A}/(a)$.
2. *Let* $(f)=\wp$. *Then* $C[f^i] = \{0\} \subset \overline{L}$.

*Proof.* 1. We know that $C[a]$ is a finite $\mathbf{A}$-module of order $r^{\deg(a)}$. As $\mathbf{A}$ is a principal ideal domain, we can decompose

$$C[a] \simeq \oplus \mathbf{A}/(f_i)^{e_i}\,,$$

where $f_i$ is prime and $e_i>0$. The elements in $\mathbf{A}$ which are prime to $a$ act as automorphisms of $C[a]$. Thus $f_i \mid a$ for all $i$ and so $f_i \notin \wp$ for all $i$. Moreover, the number of elements in $\mathbf{A}/(f_i)$ is $r^{\deg f_i}$. Thus by simply counting $f_i$-division points, one sees that $f_i \neq f_j$ for $i \neq j$ implying that $C[a]$ is cyclic. One now sees easily that $C[a]$ is $\mathbf{A}$-module isomorphic to $\mathbf{A}/(a)$.

To see Part 2 look first at $C[f]=$ roots of $C_f(x)$. Since $C'_f(x)=\iota(f)=0+(\wp)$, we see that $C_f(x)$ is no longer separable. Thus it has $< r^{\deg(f)}$ roots in $\overline{L}$. However, the arguments in Part 1 imply that $C[f]$ must be $\mathbf{A}$-module isomorphic to $\mathbf{A}/(f^i)$ for some $i$. Counting again implies that $i=0$ or

$$C_f(x) \equiv x^{r^{\deg f}} (\wp\mathbf{A}[x])\,.$$

The result follows.

Alternatively, Part 2 can be seen directly through Proposition 3.3.10. □

Of course, $C[f^i]$, etc., should actually be viewed as a *finite group scheme* with the induced $\mathbf{A}$-action. In this case, $C[f^i]$ is isomorphic to

$$\overline{L}[x]/(x^{r^{i \deg f}})\,.$$

Recall that $\mathbb{Z}/(p)^* \simeq \mathbb{Z}/(p-1)$ as abelian groups, etc. We now present the analogous result for the Carlitz module. Let $f$ be a monic prime of $\mathbf{A}$. Set $\wp=(f)$ and $\mathbb{F}_\wp = \mathbf{A}/\wp$. Let $\mathbb{F}_{\wp^n}$ be the unique (up to isomorphism) extension of $\mathbb{F}_\wp$ of degree $n$. Thus $\mathbb{F}_{\wp^n}$ is an $\mathbf{A}$-field via the map $\mathbf{A} \to \mathbf{A}/\wp \hookrightarrow \mathbb{F}_{\wp^n}$, and is an $\mathbf{A}$-module via $C$.

**Theorem 3.6.3.** *Via* $C$, $\mathbb{F}_{\wp^n}$ *is* $\mathbf{A}$*-module isomorphic to* $\mathbf{A}/(f^n-1)$.

*Proof.* $\mathbb{F}_{\wp^n}$ is a finite $\mathbf{A}$-module and must be cyclic by Theorem 3.6.2. Now by Part 2 of Theorem 3.6.2 we see that

$$C_{f^n}(x) \equiv x^{r^{n \deg f}} (\wp\mathbf{A}[x]) \,.$$

Thus $C_{f^n-1}$ annihilates $\mathbb{F}_{\wp^n}$. A simple count now implies the result. □

Theorem 3.6.3 illustrates again the remarkable similarities between $C$ and the multiplicative group $\mathbb{G}_m$. One can try to push this similarity in a number of directions and we present one such direction here.

Thus, let $a$ be an integer $\neq -1$, 0 or 1. We assume that $a$ is *square free.* Let $N_a(x)$ be the number of primes $p \leq x$ for which $a$ is primitive modulo $p$, i.e., a generates $\mathbb{Z}/p^*$. Then, in 1927, E. Artin conjectured that $N_a(x)$ had a positive density (of a certain given form). This result is now known modulo certain generalized Riemann Hypotheses. For a good reference, we refer the reader to [Le1].

We now try to do an analogous thing with $\mathbf{A}$, $C$, etc. For the moment, let $M$ be the set of all *monic* primes of $\mathbf{A}$. Standard arguments on primes in arithmetic progression imply that the greatest common divisor of

$$\{f - 1 \mid f \in M \text{ and } \deg f > 1\}$$

is 1 *unless* $r = 2$ in which case it is easily seen to be $T(T+1)$.

As will be seen in later sections, the classical proofs of cyclotomic theory also work for division points of the Carlitz module. One finds that $C(\mathbf{k})$ has non-trivial $\mathbf{A}$-torsion only when $r = 2$. In this case, the torsion submodule is

$$C[T(T+1)] = \{0, T, T+1, 1\} \,.$$

The reader may profit by comparing what we have seen for $T(T+1)$ and what happens classically for 2, the odd primes, and $\{\pm 1\}$.

Thus let $a \in \mathbf{A}$ be nonzero. If $r = 2$, we also require $a \notin \{0, T, T+1, 1\}$ *and* $a$ is *not* of the form $C_T(b)$ or $C_{T+1}(b)$ for some $b \in \mathbf{A}$. For example, $a$ might be a prime of degree $> 1$. Let $N_a(x)$ be the set of primes $\wp$ of $\mathbf{A}$ where the residue of $a$ generates $C(\mathbb{F}_\wp)$. The analogy with classical theory leads one to expect an analog of Artin's conjecture for the Carlitz module and, in fact, this has been established in [Hsu1].

## 3.7. The Adjoint of the Carlitz Module

Let $\mathbf{k}^{\text{perf}} \subset \mathbf{C}_\infty$ be the perfection of $\mathbf{k}$. Our goal in this short subsection is to show how Section 1.7 allows us to deduce the existence of the "$\tau$-adjoint," or "adjoint," to the Carlitz module $C$.

Recall that

$$C_a(\tau) = a\tau^0 + \sum_{i=1}^{\deg(a)} C_a^{(i)}\tau^i \in \mathbf{k}\{\tau\}\,.$$

By using Definition 1.7.1, we are led to our next definition.

**Definition 3.7.1.** We set

$$C_a^*(\tau) = \tau^0 + \sum_{i=1}^{\deg(a)} (C_a^{(i)})^{1/r^i}\tau^{-i} \in \mathbf{k}^{\mathrm{perf}}\{\tau^{-1}\}\,,$$

where $\mathbf{k}^{\mathrm{perf}}\{\tau^{-1}\}$ is the ring of Frobenius polynomials in $\tau^{-1}$.

**Lemma 3.7.2.** *$C_{ba}^*(\tau) = C_a^*(\tau)C_b^*(\tau) = C_b^*(\tau)C_a^*(\tau) = C_{ab}^*(\tau)$.*

*Proof.* We have

$$C_{ba}(\tau) = C_b(\tau)C_a(\tau) = C_a(\tau)C_b(\tau) = C_{ab}(\tau)\,.$$

Thus the result follows by applying Lemma 1.7.3. □

*Remarks.* 3.7.3. 1. Just as $C$ is generated by $C_T$, so $C_T^*$ is generated by $C_T^* = T\tau^0 + \tau^{-1}$. Thus

$$\begin{aligned} C_{T^2}^* &= (T\tau^0 + \tau^{-1})(T\tau^0 + \tau^{-1}) \\ &= T^2\tau^0 + (T^{1/r} + T)\tau^{-1} + \tau^{-2}\,. \end{aligned}$$

In general, one obtains $C_a^*$ for $C_a$ by formally treating $r$ as a variable and then replacing $r^i$ by $r^{-i}$.

2. Proposition 3.3.10 can be adapted to $C^*$. We leave this as an exercise for the reader.

3. All the ideas of torsion points etc., make sense for $C^*$. We note, however, that the torsion points of $C^*$ are actually algebraic over $\mathbf{k}$ (just raise $C_a^*$ to the $r^d$-th power for $d = \deg a$). By 1.7.11 we see that the $I$-torsion points of $C$ and $C^*$ generate the *same* extension of $\mathbf{k}$.