Centralizers in Free Group Algebras and Nonsingular Curves

Nikita Miasnikov

Abstract. The centralizer of any non-scalar element of a free group algebra over a field is the coordinate ring of a nonsingular curve.

1. Introduction

Let $k$ be a field with algebraic closure $\overline{k}$. G. Bergman showed in [Ber69] (see also [Lot02] for an exposition) that the centralizer $C$ of a non-scalar element $u$ in a free associative algebra over $k$ is isomorphic to $k[t]$, the ring of polynomials in one indeterminate over $k$. His proof can be split into two parts.

First he showed [Ber69, Lemma 1.5, Prop. 2.2 and Prop. 4.5] that, to paraphrase the original formulation, $C$ is the affine coordinate ring of the complement of a $k$-point in a proper nonsingular curve over $k$. Such rings are discussed in Section 3.4.

The second part of his proof went as follows. Bergman proved [Ber69, Prop. 5.2] that Every finitely generated subalgebra $R \neq k$ of a free $k$-algebra admits a homomorphism $f : R \to k[t]$ which is non-trivial in the sense $f(R) \neq k$. Since from the first part of the proof one knows that $C$ is a 1-dimensional integral domain, it follows that any non-trivial homomorphism $C \to k[t]$ must be an embedding. To complete the argument, Bergman invoked the following result due to P.M. Cohn [Coh64, Prop. 2.1] which uses Luroth’s Theorem: Any integrally closed subalgebra of $k[t]$, other than $k$, is of the form $k[y]$.

Fix a finite alphabet $A$. The free associative algebra $k\langle A \rangle$ on $A$ is contained in the free skew field $k\langle A \rangle$ on the same alphabet over $k$. We can think of the elements of $k\langle A \rangle$ as non-commutative polynomials and of elements of $k\langle A \rangle$ as non-commutative rational functions. Perhaps the next simplest subalgebra of the free skew field is the $k$-algebra generated by the elements of $A$ and their inverses.

This is none other than the free group algebra on the set of generators $A$, and its elements can be thought of as non-commutative Laurent polynomials.

Let $F$ be a free group on $A$. In this paper, we transplant the first part of Bergman’s proof into the setting of the free group algebra $kF$. Our main results are Proposition 6.6 and Theorem 6.5.

Theorem 6.5 combined with Corollary 6.3 give the following description of the centralizer $C$ of a non-scalar element $u \in kF$.

Either $C$ is isomorphic to the ring of Laurent polynomials $k[t, t^{-1}]$ (Corollary 6.3), or else $C$ is the affine coordinate ring of the complement of a $k$-point in a proper nonsingular curve $W$ over $k$. (Theorem 6.5).

Proposition 6.6 says that for a class of elements, which we call homogeneous, the centralizer $C \cong k[t]$, i.e. the curve $W$ is in fact a line.
We do not have an example in which that curve is not a line.

2. Acknowledgments

I thank the referee, Marian Anton, Maggie Habeeb, Andrew Stout, and Phillip Williams for all of their comments and suggestions. I thank my father for too many things to list.

3. Preliminaries

3.1. Free group algebras. Let $F$ be a free group on a finite alphabet $A$. For $u \in F$, we denote by $\overline{u}$ the reduced word in the alphabet $A^\pm := \{a, a^{-1} | a \in A\}$ which represents $u$.

We denote by $kF$ the group algebra of $F$ over $k$. By definition, $kF$ is a $k$-vector space. One thinks of $F$ as a subset of $kF$, and in fact, $F$ is a $k$-basis of $kF$. Moreover, $kF$ is equipped with multiplication which linearly extends multiplication of $F$. Every element $u$ of $kF$ can be uniquely written as

$$u = \sum_{g \in F} a_g g$$

where $a_g \in k$ and only finitely many of $a_g$ are nonzero. For $u \in kF$, $\text{Supp}(u)$ will denote the support of $u$, i.e. the set of elements of $F$ which appear with non-zero coefficients in $u$. By a monomial or term we mean an element of $kF$ whose support consists of one element.

Let $X = \{x_a | a \in A\}$ be distinct letters indexed by the alphabet $A$. A very useful fact about $kF$ due to W. Magnus and R. Fox [Fox53, Theorem 4.3], which we use, is that $kF$ can be embedded into the algebra of non-commutative formal power series $k\langle X \rangle$ in the indeterminates $x_a (a \in A)$. This embedding, called the Magnus-Fox embedding, is effected by sending each letter $a \in A$ to $1 + x_a$. Note that this embedding induces an isomorphism onto $k\langle X \rangle$ of the completion of $kF$ with respect to the augmentation ideal.

A free group can be bi-ordered by pulling back an ordering along the embedding $\mathbb{Z}F \to \mathbb{Z}\langle X \rangle$. For any bi-ordered group $G$, it is easy to show, that $kG$ is an integral domain in which the only units are the monomials. In particular, $kF$ has these properties.

Moreover, $kF$ is a free ideal ring or fir [Coh06, Corollary 7.11.8, page 507]. A fir is a ring in which every one-sided ideal, left or right, is a free module of a unique rank (see [Coh08, Ch. 2] for an exposition of firs).

3.2. Degree functions.

Definition 3.1. Given a $k$-algebra $R$, a degree function on $R$ over $k$ is a map

$$d : R \to \{-\infty\} \cup \mathbb{R}$$

which satisfies the properties: $\forall x, y \in R$,

$$d(x) = -\infty \iff x = 0, \quad x \in k \setminus \{0\} \implies d(x) = 0$$

(1)

$$d(xy) = d(x) + d(y)$$

(2)

$$d(x + y) \leq \max\{d(x), d(y)\}$$

A degree function is discrete if it maps $R \setminus \{0\}$ into a cyclic subgroup of $(\mathbb{R}, +)$. 
Remark 3.2. Identity (1) shows that any \( R \) that admits a degree function is an integral domain (i.e. \( R \) has no zero-divisors). When \( R \) is a commutative integral domain, \( d \) is a degree function if and only if \(-d\) extends to a real-valued valuation on \( \text{Frac} C \), the field of fractions of \( C \). In fact \( d \) determines the resulting valuation \( v \) because \(-d\) extends to \( v \) uniquely via
\[
v \left( \frac{x}{y} \right) = d(y) - d(x).
\]
Finally \( v \) is discrete whenever \( d \) is discrete and non-trivial (i.e. not identically zero on \( R \setminus\{0\} \)).

Remark 3.3. The following property, usually seen with ultra-metrics (and interpreted as “triangles are isosceles”), holds here as well:
\[
d(x + y) = d(x) + d(y) \quad \text{if} \quad d(x) \leq d(y).
\]
Indeed, denote \( z = x + y \). By (2), \( d(z) \leq d(x) \). If \( d(z) < d(x) \), then \( x = z - y \) gives \( d(x) \leq \max\{d(z), d(-y)\} < d(x) \), a contradiction.

A group homomorphism
\[
h : F \rightarrow (\mathbb{R},+)
\]
defines a grading on \( kF \) with indices in \( \mathbb{R} \). Thus
\[
kF = \bigoplus_{a \in \mathbb{R}} kF_a \quad \text{where} \quad kF_a = k\text{-span}(h^{-1}(a)).
\]
Note that multiplication in \( kF \) is compatible with grading: \((kF_a)(kF_b) \subseteq kF_{a+b}\). The \( k \)-vector spaces \( kF_a \) are the \( h \)-homogeneous components of \( kF \). If \( u \in (kF)_a \) is non-zero, we say that \( u \) is \( h \)-homogeneous. For \( u \in kF \setminus\{0\} \), we denote by \( u_h \) its highest-degree homogeneous component. A key observation is that since \( kF \) is an integral domain,
\[
(uv)_h = u_h v_h.
\]
We extend \( h \) to \( kF \) by setting
\[
h(u) = h(u_h) = \max\{h(u)|u \in \text{Supp}(u)\}, \quad h(0) = -\infty.
\]
With the aid of (3) one can see that the resulting map \( h : kF \rightarrow \{-\infty\} \cup \mathbb{R} \) is a degree function on \( kF \) over \( k \). We refer to this degree as \( h \)-degree. When no confusion is possible we may drop explicit references to the homomorphism \( h \) and use the plain terms homogeneous and degree.

3.3. Basic properties of centralizers. In \( kF \), the centralizer \( C \) of an element \( u \notin k \) is a commutative and integrally closed integral domain. Commutativity follows from the Magnus-Fox embedding of \( kF \) into the non-commutative power series ring \( k\langle X \rangle \) (cf. Section 3.1), since in \( k\langle X \rangle \), the centralizer of any element which is not contained in \( k \) is isomorphic to the ring of formal power series \( k[[t]] \) (See [Coh06, Corollary 6.7.2, p. 375]).

The assertion that \( kF \) is integrally closed is a consequence of the following proposition due to G. Bergman [Ber69, Corollary 4.4] which relies on the notion of a 2-fir. For any cardinal \( n \), a right \( n \)-fir is a ring in which all right ideals generated by \( n \) or fewer elements are free and have unique rank. For finite \( n \), the notions of left \( n \)-fir and right \( n \)-fir are equivalent ([Coh06, Ch 2]). Clearly any fir is a 2-fir.
Proposition 3.4 (G. Bergman). Let $R$ be a $k$-algebra which is an integral domain, such that $k(t) \otimes R$ is a 2-fir and such that $R$ remains an integral domain under tensoring with all finite algebraic extensions of $k$. Let $C$ be a commutative subring of $R$ and $\hat{C}$ the integral closure of $C$ in its field of fractions. Then the inclusion of $C$ in $R$ extends uniquely to an embedding of $\hat{C}$ in $R$.

The centralizer group $Z$ of an element $g \in F$, $g \neq 1$ is cyclic. Indeed, $Z$ is a commutative subgroup of $F$, as can be seen, for example, using the Magnus-Fox embedding; and it is also free, since by Nielsen-Schreier theorem any subgroup of a free group is free. That makes $Z$ cyclic, necessarily the maximal cyclic subgroup of $F$ which contains $g$.

The next lemma allows one to assume that a free group is finitely generated when dealing with centralizers.

Lemma 3.5. Suppose that $F$ is a free group of arbitrary, possibly infinite, rank. Suppose that $G$ is a free factor of $F$, i.e. that $F = G \ast H$, the free product of the free groups $G$ and $H$. Let $u \in kG$, $u \notin k$. Then the centralizer of $u$ in $kF$ is contained in $kG$.

Proof. Suppose there is an element $v \in kF \backslash kG$ which commutes with $u$. We will conclude that $u \in k$, a contradiction. It is enough to consider the case when $G$ and $H$ are finitely generated because we only need enough generators to express both $u$ and $v$.

Let us bi-order the free group $F$ (cf. Section 3.1). Denote by $u$ the lowest element in $\text{Supp}(u)$ and by $v$ the lowest element in $\text{Supp}(v) \backslash G$. Since a bi-ordering is preserved by multiplication from both sides, the lowest element of $\text{Supp}(uv) \backslash G = \text{Supp}(vu) \backslash G$ is both $uv$ and $vu$, and so $u$ and $v$ commute. That means $u = r^m$ and $v = r^n$ for some element $r \in F$. $v \notin G$ implies that $r \notin G$. We will now deduce that $m = 0$.

Let $\{g_1, \ldots\}$ be a free generating set for $G$, $\{t_1, \ldots\}$ a free generating set for $H$. Working in the free generating set $\{g_1, \ldots, t_1, \ldots\}$ for $F$, write

$$r = p^{-1}sp$$

so that $\bar{r}^{-1} \bar{x} \bar{p}$ is a reduced word and $\bar{r}$ cyclically reduced, i.e. so that the first letter of $\bar{r}$ is not the inverse of the last letter. Since $r \notin G$, at least one of $p$ or $s$ must contain a letter from $\{t_1, \ldots\}$.

Now, $r^m$ is represented by the word $\bar{p}^{-1} \bar{x}^m \bar{p}$. If $m \neq 0$, this word is reduced and contains a letter from $\{t_1, \ldots\}$, which implies that $r^m \notin G$. Since $r^m = u \in G$, it follows that $m = 0$ and $u = 1$. Thus the lowest element in $\text{Supp}(u)$ is 1. Similarly we conclude that the highest element in $\text{Supp}(u)$ is 1. Hence $u \in k$, a contradiction. \hfill \square

3.4. The complement of a regular $k$-point in a proper curve over $k$. Parts of the following characterization are in Propositions 2.1 and 2.2 in [Ber69]. We prove this lemma in Section 8 for the sake of completeness of the exposition. See [Liu02 Sec. 4.1, in particular Exercise 1.17] for a treatment of algebraic curves over an arbitrary field. We denote by $\text{Frac} C$ the field of fractions of $C$.

Lemma 3.6. Let $C \neq k$ be a $k$-algebra which is a commutative integral domain. Then the following are equivalent:
Lemma 4.1. Let \( k \) be a field and \( V, U, Z \) be vector spaces over \( k \) such that the vector spaces associated to the point “at infinity” \( p \) is the rank of the element \( t \in U \). If \( \mu \) is a bilinear product induced by \( \mu \) and \( \ast \) is a bilinear map \( * : (U \otimes V) \times (U \otimes V) \to U \otimes Z \otimes V \), then whenever \( \mu'(x, y) = 0 \) with \( x \in U \otimes U \) and \( y \in U \otimes V \), it follows that \( x = 0 \) or \( y = 0 \). Consider the following proof is due to the referee. A proof using duality is also possible.

Remark 3.7. Any \( k \)-algebra \( C \) satisfying condition i) of the lemma is automatically a commutative integral domain \( \text{[Ber69, Proposition 2.1]} \).

Remark 3.8. Suppose \( C \) satisfies the conditions of the lemma and \( d' \) is a degree function on \( C \) over \( k \) with at least one positive value. Then for some \( \lambda > 0 \), \( d' = \lambda \cdot d \). This is due to the fact that \( -d \) and \( -d' \) both are valuations (cf. Remark 3.2) associated to the point “at infinity” \( p \).

4. A LINEAR ALGEBRA LEMMA

Lemma 4.1. Let \( U, V, Z \) be vector spaces over \( k \) and \( \mu : V \times U \to Z \) a bilinear map without zero divisors over \( k \), i.e., such that if we denote \( \mu' = k \otimes \mu \), then whenever \( \mu'(x, y) = 0 \) with \( x \in k \otimes U \) and \( y \in k \otimes V \), it follows that \( x = 0 \) or \( y = 0 \). Consider the following bilinear product induced by \( \mu \):

\[
* : (U \otimes V) \times (U \otimes V) \to U \otimes Z \otimes V,
\]

\[
(x \otimes y) * (z \otimes u) = x \otimes \mu(y, z) \otimes u.
\]

If \( t \ast s = s \ast t \) for \( t, s \in U \otimes V \), then \( t, s \) are linearly dependent over \( k \).

The following proof is due to the referee. A proof using duality is also possible.

Proof. Since linear dependence of \( t, s \) over \( k \) is equivalent to their dependence over \( k \), we can assume without loss of generality that \( k = \overline{k} \). Assume also without loss of generality again that the vector spaces \( U \) and \( V \) are finite-dimensional.

Given \( s \in U \otimes V \), one can write

\[
s = \sum_{i=1}^{n} u_i \otimes v_i
\]

with \( u_1, \ldots, u_n \) linearly independent, and \( v_1, \ldots, v_n \) likewise linearly independent; and though that expression is not unique, the subspace \( U_s \) of \( U \) spanned by \( u_1, \ldots, u_n \), and the subspace \( V_s \) of \( V \) spanned by \( v_1, \ldots, v_n \) can be shown to be unique. In \( \text{[5]} \), any basis of \( U_s \) can be used as \( (u_i) \), and once \( (u_i) \) are chosen, there is only one tuple of \( (v_i) \) which satisfies the equation. The common dimension \( n \) of \( U_s \) and \( V_s \) is the rank of the element \( s \) in the tensor product space \( U \otimes V \).

Now suppose \( t \ast s = s \ast t \), with \( s \) and \( t \) nonzero. We claim that \( U_s = U_t \) and \( V_s = V_t \). For if these are not true, assume without loss of generality that \( U_s \neq U_t \).
Let us construct a basis of $U_s + U_t$ by starting with a basis of $U_s \cap U_t$, taking bases of $U_s$ and $U_t$ which contain it, and forming their union. In particular, by the above "$\subseteq$" condition, the basis of $U_s$ will contain some element $x$ not in the basis of $U_t$.

We will now express the common value of $t * s = s * t$ in terms of the above basis of $U_s + U_t$ and arbitrary bases for $Z$ and $V$, and will find that the expression for $s * t$ contains terms $x \otimes \cdots$ for the $x$ referred to above, but the expression for $t * s$ contains no such terms. That will be a contradiction.

Let $\{u_i\}$ be the basis for $U_s + U_t$ just constructed. Thus $x \in \{u_i\}$. Let $\{v_j\}$ be a basis for $V$. We can now express $s, t$ in terms of these bases grouping terms as follows:

$$s = \sum u_i \otimes \left( \sum_j \alpha_{ij} v_j \right), \quad t = \sum_l \left( \sum_k \beta_{kl} u_k \right) \otimes v_l$$

Now let us calculate

$$s * t = \sum_{il} u_i \otimes \mu \left( \sum_j \alpha_{ij} v_j, \sum_k \beta_{kl} u_k \right) \otimes v_l.$$

Since $t \neq 0$, for some value of $l$ the second argument of $\mu$ is non-zero in the above. When $u_i = x$, the first argument of $\mu$ is also non-zero. Since $\mu$ has no zero-divisors the value of $\mu$ for those arguments is non-zero. It follows that regardless of the choice of basis for $Z$, $s * t$ will contain a tensor element of the type $x \otimes z \otimes v_l$ with a nonzero coefficient. On the other hand, repeating this analysis with the roles of $s$ and $t$ switched, we see that the same is not true of $t * s$.

So $U_s = U_t$ and $V_s = V_t$. Let us write $t = \sum u_i \otimes v_i$ where $\{u_i\}$ and $\{v_i\}$ are appropriate bases of these subspaces. We can express $s$ using these same bases as $s = \sum_{i=1}^n u_i \otimes (\sum_j \alpha_{ij}) v_i$, where $((\alpha_{ij}))$ is a matrix over $k$. (The matrix will actually be invertible, because the elements $\sum_j \alpha_{ij} v_i$ in the expression for $s$ must form a basis of $V_s$; but we won’t need this fact.) Now since $k$ is algebraically closed, this matrix has an eigenvalue $\lambda$. Defining $s' = s - \lambda t$, we get $s' = \sum_{i=1}^n u_i \otimes \sum_j (\alpha_{ij} - \lambda \delta_{ij}) v_j$.

Now $V_{s'}$ is spanned by the vectors $\sum_j (\alpha_{ij} - \lambda \delta_{ij}) v_j$ ($i = 1, \ldots, n$). Since the matrix $((\alpha_{ij} - \lambda \delta_{ij}))$ is singular, $V_{s'} \subseteq V_s = V_t$. Thus $V_{s'} \neq V_t$, and of course $s'$ again satisfies $s' * t = t * s'$. If $s' \neq 0$, this would contradict the result of the two preceding paragraphs. So $s' = 0$; i.e., $s = \lambda t$.

\[\Box\]

5. Commuting homogeneous elements

The terminology and notation used in this section are introduced in Sections 3.1 and 3.2.

**Definition 5.1.** We say a product $w_1 \cdot \cdots \cdot w_n$, where $w_i \in F$, is a reduced factorization or a reduced product if no $w_i$ equals 1, and the word $\overline{w_1 \cdot \cdots \cdot w_n}$ is reduced, in other words, if no cancellation takes place at the juncture of $\overline{w_i}$ and $\overline{w_{i+1}}$ for $i = 1, \ldots, n - 1$. In this section, we reserve the notation "$\cdot$" for reduced products in $F$.

For $z, w \in F$, we say that $z$ is a prefix (suffix) of $w$ whenever the word $\overline{z}$ is a prefix (resp. suffix) of the word $\overline{w}$, or equivalently, whenever $z = 1$, $z = w$, or for some $v \in F$, there is a reduced factorization $w = z \cdot v$ (resp. $w = v \cdot z$). By $z \leq w$ ($z < w$) we mean that $z$ is a prefix (resp. proper prefix) of $w$. 


Observation 5.2. If $n < m$, and $v_1 \cdot \cdots \cdot v_n$ and $v_n \cdot \cdots \cdot v_m$ are reduced factorizations, so is
\[ v_1 \cdot \cdots \cdot v_m. \]

Observation 5.3. If $v_1 \cdot \cdots \cdot v_n$ and $w_1 \cdot \cdots \cdot w_m$ are reduced factorizations and neither $\overline{v_n}$ nor $\overline{w_1}$ cancel completely in $\overline{v_nw_1}$, then
\[ v_1 \cdot \cdots \cdot v_{n-1} \cdot (v_n w_1) \cdot w_2 \cdot \cdots \cdot w_m \]
is a reduced factorization when $v_n w_1$ is regarded as one factor.

Indeed, the first letter of $\overline{v_n w_1}$ is the same as the first letter of $\overline{v_n}$ while the last letter of $\overline{v_n w_1}$ is the same as the last letter of $\overline{w_1}$.

We intend to capitalize on this observation by introducing certain sets of homogeneous elements of $kF$ in the following definition. Although these sets, denoted by $T(r)$, may seem quite restricted, we shall find that for every $w \in kF \setminus \{0\}$ homogeneous of positive degree, all sufficiently large powers $w^n$ belong to $T(r)$ for appropriate values of $r$, and this will allow us to apply the properties of $T(r)$ in studying commuting elements.

**Definition 5.4.** Let $r > 0$. Let
\begin{itemize}
  \item $T_1(r)$ be the set of homogeneous elements $w \in kF$ for which
    \[ h(w) \geq 2 \left( r + \max\{|h(a)| \mid a \in A\} \right); \]
  \item $T_2(r)$ be the set of homogeneous elements $w \in kF$ for which
    \[ h(w) > 0 \quad \text{and} \quad (\forall w \in \text{Supp}(w) \quad \forall p \leq w) \quad -r < h(p) < h(w) + r; \]
  \item $T(r) = T_1(r) \cap T_2(r)$.
\end{itemize}

We will omit $r$ from this notation when there is no risk of confusion.

Figure[11] illustrates elements of $T \cap F$. In that diagram, $F$ is free on generators $a$ and $b$. In each path shown, every rightward, leftward, upward or downward 1-unit step represents a factor $a$, $a^{-1}$, $b$, $b^{-1}$ respectively. Moving along a path towards the arrowhead corresponds to reading the factors from left to right. The function $h$ is represented by perpendicular projection onto the slanting line at the left. The factorizations $u = u(0) \cdot u(1) \cdot u(2)$ and $v = v(0) \cdot v(1) \cdot v(2)$ to be discussed later in this section are shown by dots in the paths separating the indicated factors. For visual clarity, the two expressions $u$ and $v$ are shown as paths with different initial points, so that their diagrams do not overlap, but both initial points are taken on the line $h = 0$.

Let us fix an $r > 0$. We claim that the sets $T_1$, $T_2$, and $T$ are closed under multiplication. It is obvious that $T_1$ is closed under multiplication. Let us show now that the same holds for $T_2$. Suppose $u, v \in T_2$. We want to show that $uv \in T_2$. Let $u \in \text{Supp}(u)$ and $v \in \text{Supp}(v)$ and $p \leq uv$. There are two possibilities: $p \leq u$ or $p = uq$ where $q \leq v$. In the first case we have
\[ -r < h(p) < h(u) + r < h(u) + h(v) + r \]
while in the second
\[ -r < h(q) < h(uq) = h(u) + h(q) < h(u) + h(v) + r = h(uv) + r. \]
Thus $uv \in T_2$. Lastly, it follows that $T$ is closed under multiplication as well.

Our next goal is to obtain certain reduced factorizations of elements of $T \cap F$. 
Figure 1. Factorization of elements of $T \cap F$ when rank $F = 2$. The group elements are depicted as walks in $F^{ab}$.

Define

$\mathcal{O} = \{ w \in F \mid h(w) \geq r, \quad (\forall p < w) \quad |h(p)| < r \}$

$\tilde{\mathcal{O}} = \{ w \in F \mid h(w) \geq r, \quad (\forall \text{ proper suffix } s \text{ of } w) \quad |h(s)| < r \}$.

It helps to notice that $\tilde{\mathcal{O}}$ is the reversal of $\mathcal{O}$ and so statements about $\mathcal{O}$ translate into dual statements about $\tilde{\mathcal{O}}$. By comparing $h$-degrees we get these

**Lemma 5.5 (Properties of $\mathcal{O}$ and $\tilde{\mathcal{O}}$).**

- No element in $\mathcal{O}$ is a prefix of another element in $\mathcal{O}$
- No element in $\tilde{\mathcal{O}}$ is a suffix of another element in $\tilde{\mathcal{O}}$
- No element in $\mathcal{O}^{-1} := \{ u^{-1} \mid u \in \mathcal{O} \}$ is a suffix of an element in $\tilde{\mathcal{O}}$
- No element in $\tilde{\mathcal{O}}^{-1} := \{ v^{-1} \mid v \in \tilde{\mathcal{O}} \}$ is a prefix of an element in $\mathcal{O}$

The last two properties can be equivalently stated as:

- For any $u \in \mathcal{O}$ and $v \in \tilde{\mathcal{O}}$, neither $u$ nor $v$ cancels completely in the product $uv$.

**Proof.**

- If $v, w \in \mathcal{O}$ and $p < v$, then $h(w) \geq r$ but $h(p) < r$, hence $w \neq p$.
- Dual to the previous one.
- If $t \in \mathcal{O}^{-1}$, then $h(t) \leq -r$. But if $s$ is a suffix, proper or not, of an element of $\tilde{\mathcal{O}}$, then $h(s) > -r$. Hence $t \neq s$.
- Dual to the previous one.
Let \( w \in T \cap F \). Define \( w^{(0)} \) to be the prefix of \( w \) of the shortest word length such that \( h(w^{(0)}) \geq r \). Likewise define \( w^{(2)} \) to be the suffix of \( w \) of the shortest word length with \( h(w^{(2)}) \geq r \). By the definition of \( T_1 \), \( w^{(0)} \) and \( w^{(2)} \) exist. We claim that there is a gap between them, i.e. that there is a word length with following reduced factorization of \( (8) \)

\[
\text{For otherwise } s = \left( w^{(0)} \right)^{-1} w \text{ would be a suffix of } w^{(2)} \text{ and then by the definition of } w^{(2)},
\]

\[
h(s) < r + \max \{ h(a) \mid a \in A \}.
\]

On the other hand, by the definition of \( w^{(0)} \),

\[
h(w^{(0)}) < r + \max \{ h(a) \mid a \in A \}.
\]

Putting these together we get

\[
h(w) = h(w^{(0)} s) = h(w^{(0)}) + h(s) < 2 \left( r + \max \{ h(a) \mid a \in A \} \right),
\]

a contradiction with the definition of \( T_1 \).

Since \( w \in T_2 \), it follows from the definition of \( T_2 \) that \( w^{(0)} \in O \) and \( w^{(2)} \in \tilde{O} \). Finally it is evident from the first two Properties of \( O \) and \( \tilde{O} \) in Lemma 5.5 that the reduced factorization of \( w \) we have constructed,

\[
w = w^{(0)} \cdot w^{(1)} \cdot w^{(2)},
\]

is the only one with the property that

\[
w^{(0)} \in O, \ w^{(2)} \in \tilde{O}.
\]

Now take two elements \( u, v \in F \cap T \). We have the reduced factorizations \( w^{(0)} \cdot u^{(1)} \cdot w^{(2)} \) and \( v^{(0)} \cdot v^{(1)} \cdot v^{(2)} \). Next, by the last Property of \( O \) and \( \tilde{O} \), neither \( u^{(2)} \) nor \( v^{(0)} \) cancel completely in \( w^{(2)} v^{(0)} \). Therefore, by Observation 5.3, we have the following reduced factorization of \( u v \) (into 5 factors with \( u^{(2)} v^{(0)} \) as one):

\[
(7) \quad u v = w^{(0)} \cdot u^{(1)} \cdot \left( u^{(2)} v^{(0)} \right) \cdot v^{(1)} \cdot v^{(2)}.
\]

Since \( u^{(0)} \in O \) and \( v^{(2)} \in \tilde{O} \), it follows from uniqueness of (6) with \( w = u v \), that

\[
(8) \quad (u v)^{(0)} = w^{(0)}, \quad (u v)^{(1)} = u^{(1)} \cdot \left( u^{(2)} v^{(0)} \right) \cdot v^{(1)}, \quad \text{and} \quad (u v)^{(2)} = v^{(2)}.
\]

Moreover, we have

**Lemma-Definition 5.6.** Let \( u, v \in F \cap T \), \( w = u v \), and \( \ell = h(u) \).

(a) Define the following elements:

\[
w^{(10)} = u^{(1)}, \quad w^{(11)} = u^{(2)} v^{(0)}, \quad w^{(12)} = v^{(1)}.
\]

(b) \( w^{(10)}, w^{(11)}, \) and \( w^{(12)} \) depend only on \( w \) and \( \ell \). In other words, if \( f, g \in F \cap T \) satisfy \( f g = w \) and \( h(f) = \ell \), then

\[
f^{(1)} = u^{(1)}, \quad f^{(2)} v^{(0)} = u^{(2)} v^{(0)}, \quad g^{(1)} = v^{(1)}.
\]

(c) We have a reduced factorization:

\[
w^{(1)} = w^{(10)} \cdot w^{(11)} \cdot w^{(12)}.
\]
Proof. (b): Let \( p = u^{(0)} u^{(1)} = w^{(0)} w^{(10)} \) and \( q = u v^{(0)} = w^{(0)} w^{(10)} w^{(11)} \). The factorization (7) shows that \( p < q < w \). Now we observe that “\( w \) crosses the interval \( (\ell - r, \ell + r) \)” only once; the crossing begins with \( p \) and ends with \( q \)” (Figure 1b). To be precise,

this holds... because...

\[
\begin{array}{ll}
t < p & \iff h(t) < \ell + r, \\
t = p & \iff h(t) \leq \ell - r, \\
p < t < q & \iff \ell - r < h(t) < \ell + r, \\
t = q & \iff h(t) \geq \ell + r, \\
t > q & \iff h(t) > \ell - r,
\end{array}
\]

(t < u and \( u \in T_2 \))

(\( u = p \cdot u^{(2)} \) and \( u^{(2)} \in \tilde{O} \))

(either \( t^{-1} u \) is a proper suffix of \( u^{(2)} \in \tilde{O} \)

or \( u^{-1} t < v^{(0)} \in O \))

(\( q = u w^{(0)} \) and \( v^{(0)} \in O \))

(\( u^{-1} t \leq v \) and \( v \in T_2 \)).

One can see from these conditions that \( p \) is the prefix of \( w \) of the longest word length which satisfies \( h(p) \leq \ell - r \), while \( q \) is the prefix of \( w \) of the shortest word length satisfying \( h(q) \geq \ell + r \). Evidently \( p \) and \( q \) depend only on \( w \) and \( \ell \). But with the aid of (8), we can write

\[
w^{(10)} = (w^{(0)})^{-1} p, \quad w^{(11)} = p^{-1} q, \quad w^{(12)} = q^{-1} w (w^{(2)})^{-1}.
\]

Hence \( w^{(10)}, w^{(11)}, \) and \( w^{(12)} \) depend only on \( w \) and \( \ell \).

(c) This is the middle equation in (8). □

While so far we have looked at elements of \( T \cap F \), now let us see what this lemma implies about general elements of \( T \). Suppose \( u, v \in T \) and \( w = uv \). Denote \( \ell = h(u) \). We have well-defined decompositions into sums obtained by grouping terms (where \( a \) and \( b \) run through \( F \) but only finitely many terms are non-zero):

\[
\begin{align*}
\text{u} &= \sum_a u_a, & \text{where} \ & \forall u \in \text{Supp}(u_a), \quad u^{(1)} = a \\
\text{v} &= \sum_b v_b, & \text{where} \ & \forall v \in \text{Supp}(v_b), \quad v^{(1)} = b \\
\text{w} &= \sum_{a,b} w_{a,b}, & \text{where} \ & \forall w \in \text{Supp}(w_{a,b}), \quad w^{(10)} = a \text{ and } w^{(12)} = b.
\end{align*}
\]

The last decomposition depends only on \( w \) and \( \ell \) and not on the factors \( u \) and \( v \).

From \( w = uv \) and Lemma-Definition 5.6 parts (a) and (b), we get

\[
w_{a,b} = u_a v_b.
\]

In particular, and this is the case of interest for us at the moment, suppose \( h(u) = h(v) \) and \( uv = vu \). Then we arrive at

(9)

\[
(\exists a, b) \quad u_a v_b = v_a u_b.
\]

This right away gives two things. First, by letting \( b = a \) in the above,

\[
(\exists a) \quad u_a v_a = v_a u_a.
\]

Second, \( u \in T \) implies \( u \neq 0 \) and so there is a \( b \) such that \( u_b \neq 0 \). With that value of \( b \) and with the aid of the fact that \( kF \) is an integral domain, (9) shows that
\[ u_a = 0 \iff v_a = 0. \] Similarly \( v_a = 0 \iff u_a = 0. \) Thus
\[(\forall a)\quad u_a = 0 \iff v_a = 0. \]
As \( \{u^{(1)}| u \in \text{Supp}(u)\} = \{a|u_a \neq 0\} \) and \( \{v^{(1)}| v \in \text{Supp}(v)\} = \{a|v_a \neq 0\} \), we get
\[ \{u^{(1)}| u \in \text{Supp}(u)\} = \{v^{(1)}| v \in \text{Supp}(v)\}. \]

**Proposition 5.7.** Suppose \( u, v \in kF \) are homogeneous of the same non-zero degree with respect to a homomorphism \( h : F \to (\mathbb{R}, +) \). If \( uv = vu \), then \( u = \lambda v \) for a scalar \( \lambda \).

**Proof.** Let us suppose without loss of generality that \( h(u) = h(v) > 0 \), for otherwise we can replace the homomorphism \( h : F \to (\mathbb{R}, +) \) with \( -h \).

Suppose first that \( u, v \in T(r) \) for some \( r > 0 \).
Denote \( S = \text{Supp}(u) \bigcup \text{Supp}(v) \). For \( a \in S^{(1)} := \{w^{(1)}| w \in S\} \), let \( S_a = \{w \in S| w^{(1)} = a\} \), obtaining a partition of \( S \): \( S = \bigsqcup_a S_a \).
Recapping the discussion prior to the present proposition, let us decompose uniquely
\[ u = \sum_a u_a \text{ where } \text{Supp}(u_a) \subseteq S_a, \quad v = \sum_b v_b \text{ where } \text{Supp}(v_b) \subseteq S_b, \]
arriiving at \( \forall a, b, \)
\[ u_a v_b = v_a u_b, \quad u_a v_a = v_a u_a, \quad u_a \neq 0 \iff v_a \neq 0 \iff a \in S^{(1)}. \]
Let us now set the stage for an application of Lemma 4.1.
Fix any \( a \in S^{(1)} \). Let
\[ S_a^{(0)} := \{w^{(0)}| w \in S_a\}, \quad S_a^{(2)} := \{w^{(2)}| w \in S_a\}, \]
and define
\[ U = k\text{-span}(S_a^{(0)}) \quad V = k\text{-span}(S_a^{(2)}) \quad \text{(Note that } U, V \subset kF) \]
\[ Z = VU \subset kF \]
and define
\[ \mu : V \otimes U \to Z \]

\[ \text{to be the multiplication from } kF. \]
Let us verify that \( \mu \) has no zero divisors over \( \overline{k} \) (cf. Lemma 4.1). Tensoring by \( \overline{k} \) the inclusions
\[ U, V, Z \subset kF, \]
we get
\[ \overline{k} \otimes U, \overline{k} \otimes V, \overline{k} \otimes Z \subset \overline{k} \otimes (kF) \approx \overline{k}F. \]
Moreover, \( \overline{k} \otimes \mu \) coincides with the multiplication in \( \overline{k}F \) under these inclusions. A free group algebra over any field is an integral domain. In particular, so is \( \overline{k}F \).
Hence \( \mu \) has no zero divisors over \( \overline{k} \).
Thus Lemma 4.1 applies, but in order to benefit from it, we need to establish a couple of isomorphisms.
Observe that for any \( u \in S_a^{(0)} \subseteq \mathcal{O} \) and \( v \in S_a^{(2)} \subseteq \mathcal{O} \),
\[ u \cdot a \cdot v \]
is a reduced factorization because \( u \cdot a \) and \( a \cdot v \) have this property.
This observation shows that $u$ is a prefix of $uav$. As $u \in O$ and as no element of $O$ is a prefix of another (the first of the Properties of $O$ and $O$), $u$ is the unique prefix of $uav$ contained in $O$. Likewise $v$ is the unique suffix of $uav$ contained in $O$. We conclude that the map

$$S_a^{(0)} \times S_a^{(2)} \to S_a^{(0)}aS_a^{(2)}, \quad (u, v) \to uav$$

is injective. As it is also clearly surjective, it is bijective. Passing from a bijection of bases to an isomorphism of vector spaces, we get

$$U \otimes V \cong UaV.$$  

The second isomorphism which we need to demonstrate is

$$U \otimes Z \otimes V \cong UaVUaV \subset kF$$

Looking at the bases, it suffices to show that the map

$$S_a^{(0)} \times S_a^{(2)}S_a^{(0)} \times S_a^{(2)} \to F$$

$$(u, gf, v) \to uagfav$$

is injective. To show that, we start with $w = uagfav$ and from it we will now recover $u, v$ and $gf$. We have the reduced factorizations $u \cdot a \cdot g$ and $f \cdot a \cdot v$. By the last Property of $O$ and $O$, neither $g$ nor $f$ cancel completely in $gf$. Therefore by Observation 5.3

$$w = u \cdot a \cdot (gf) \cdot a \cdot v$$

is a reduced factorization (with $gf$ as a single factor). By the first two Properties of $O$ and $O$, $u$ is the only prefix of $w$ contained in $O$ and $v$ is the only suffix of $w$ contained in $O$. So we have recovered $u$ and $v$. Then we recover $gf$ via $gf = (ua)^{-1}w(av)^{-1}$. This shows that the above map is indeed injective and therefore (13) holds.

Finally observe that $u_a, v_a \in UaV \cong U \otimes V$.

For every $a \in S^{(1)}$, we can now apply Lemma 4.1 taking the images of $u_a$ and $v_a$ in $U \otimes V$ as $t$ and $s$. Recall that for $a \in S^{(1)}$, both $u_a$ and $v_a$ are non-zero. So the lemma gives

$$v_a = \lambda_a u_a.$$ 

It remains to show that $\lambda_a$ is independent of $a$. Indeed,

$$u_a v_b = v_a u_b,$$

$$\lambda_a u_a u_b = \lambda_b u_a u_b$$

and since $kF$ is an integral domain, we can cancel $u_a u_b$ and conclude that $\lambda_a = \lambda_b$ for all $a, b$.

We have just shown that the conclusion of the present proposition holds when $u, v \in T$. Now let us consider the general case. Thus, now $u$ and $v$ are arbitrary commuting $h$-homogeneous elements of $kF$ with $h(u) = h(v)$. Moreover as mentioned in the beginning of the proof, we can assume that $h(u) = h(v) > 0$.

We will see now that for some $r > 0$ and some $n > 0$, $u^n, v^n \in T(r)$.

By the definition of $T_2$ and by finiteness of supports, for $r >> 0$ we have $u, v \in T_2(r)$. Let us fix such $r$. It follows from the fact that $T_2$ is closed under multiplication, that $\forall n > 0, u^n, v^n \in T_2$. On the other hand, from the definition
of $T_1$ and the Archimedean property of $\mathbb{R}$ it follows that for $n >> 0$, we also have that $u^v, v^u \in T_1$. For any such $n$, it follows that $u^n, v^n \in T$.

Since $u$ and $v$ commute, $u^n, v^n$ commute as well. By what we have just shown,\begin{equation}
    u^n = cv^n, \quad c \in k.
\end{equation}

Regarding $kF$ as a subring of $kF$, we can work in $kF$. Since $kF$ is an integral domain and $u$ and $v$ commute, the sub-algebra $k[u, v] \subseteq kF$ is a commutative integral domain. This commutative integral domain is contained in its field of fractions $\text{Frac}k[u, v]$. Equation (14) implies that $u/v$ is an $n$-th root of $c$ in $\text{Frac}k[u, v]$, and since $kF$ is algebraically closed, it is algebraically closed in that overfield; so the $n$-th root of $c$ in that overfield must lie in $kF$; so $u \in kFv$. Hence, since within $kF$, $u$ and $v$ have coefficients in $k$, we must have $u \in kv$.

**Corollary 5.8.** Suppose $u, v \in kF/k$ and $uv = vu$. Let $h : F \to (\mathbb{R}, +)$ be a group homomorphism and let $F^{ab}$ denote the abelianization of $F$ (with the group operation written additively).

(a) If $u$ is $h$-homogeneous of degree 0, then $v$ is also $h$-homogeneous of degree 0.

(b) If $u, v$ are arbitrary, not necessarily homogeneous, the images of $\text{Supp}(u)$ and $\text{Supp}(v)$ in $\mathbb{Q} \otimes \mathbb{Z} F^{ab}$ span the same $\mathbb{Q}$-vector space.

(c) Let $u, v$ be $h$-homogeneous, then $Qh(u) = Qh(v)$.

(d) If $u, v$ are $h$-homogeneous, $h(u) > 0, h(v) < 0$, then $u$ and $v$ are monomials.

**Proof.** (a) Suppose the contrary. Then either the lowest- or highest-degree homogeneous component of $v$ has a non-zero degree. Denote that homogeneous component by $w$. Then we have:

\[
    uw = wu
\]
\[
    \implies (uw)w = w(uw)
\]
\[
    \implies uw = \lambda w \quad \text{for some} \; \lambda \in k \quad \text{(by Proposition 5.7)}
\]
\[
    \implies u = \lambda \quad \text{(because $kF$ is an integral domain)}
\]

which is a contradiction.

(b) Apply (a) to all possible degree functions $h$ which vanish on one of the two supports.

(c) Let

\[
    q : F \to \mathbb{Q} \otimes \mathbb{Z} F^{ab}
\]

be the canonical homomorphism. Then $h$ factors through $q$: $h = \eta \circ q$.

Let $V = \mathbb{Q} q(\text{Supp}(u)) = \mathbb{Q} q(\text{Supp}(v))$ be the common (due to part b) $\mathbb{Q}$-span of the images of $\text{Supp}(u)$ and $\text{Supp}(v)$ in $\mathbb{Q} \otimes \mathbb{Z} F^{ab}$. Then

\[
    \eta(V) = \eta(\mathbb{Q} q(\text{Supp}(u))) = \mathbb{Q} \eta(q(\text{Supp}(u))) = \mathbb{Q} h(\text{Supp}(u)) = \mathbb{Q} h(u),
\]

where the last equality holds because $u$ is $h$-homogeneous. Likewise, $\eta(V) = \mathbb{Q} h(v)$.

(d) By (c), we can write $h(u)/h(v) = -n/m$ with $n, m$ positive integers. Then $h(u^mv^n) = 0$, and, since $u^mv^n$ commutes with $u$, by (a), $u^mv^n \in k$. Moreover, since $kF$ is a domain, $u^mv^n \neq 0$. Hence $u, v$ are invertible, and all invertible elements in $kF$ are monomials (cf. Section 3.1). \qed
6. Centralizers

**Lemma 6.1.** Let $C$ be the centralizer of an element in $kF \setminus k$. If $h$ does not vanish on $C \setminus \{0\}$ then $h$ restricted to $C$ is a degree function over $k$ which is discrete (cf. Definition 3.3) and which satisfies:

\[(15) \ (\forall u, v \in C \setminus \{0\}) \quad h(u) = h(v) \implies (\exists \lambda \in k) \quad h(u - \lambda v) < h(u). \quad (\text{cf. (4)})\]

**Proof.** As shown in Section 3.2, $h$ is a degree function on $kF$ and so $h|C$ is a degree function on $C$. We just need to show that $h|C$ is discrete and has property (15).

Before we continue, let us recall useful notation (cf. Section 3.2): for any element $w \in kF \setminus \{0\}$, we denote by $u_h$ the highest-degree homogeneous component of $w$. Recall also that

\[(16) \quad h(u) = h(u_h).\]

Let $w \in C \setminus \{0\}$ be such that $h(w) \neq 0$. Note that this implies that $w_h \notin k$.

First, let us show that $h$ is discrete on $C$. Let $v \in C \setminus \{0\}$ be another element with $h(v) \neq 0$. This implies that $v_h \notin k$. Since $w$ and $v$ commute, $w_h, v_h$ commute as well. Now, applying Corollary 5.8a to $w_h$ and $v_h$, we see that $h(v_h) \in \mathbb{Q}h(w_h)$. Therefore, by (16), $h(v) \in \mathbb{Q}h(w)$. Thus, $h(C \setminus \{0\}) \subseteq \mathbb{Q}h(w)$. So

\[(17) \quad h(C \setminus \{0\}) \subseteq \mathbb{Q}h(w) \bigcap h(F).\]

Since $F$ is finitely generated, $h(F)$ is finitely generated abelian. The right-hand side of (17), being a subgroup of $h(F)$, is also finitely generated, but, given that it is also a subgroup of $\mathbb{Q}h(w) \cong \mathbb{Q}$, the right-hand side is cyclic.

Let us now establish property (15). Suppose first $h(u) = h(v) = 0$. Then it is enough to show that $u_h, v_h \in k$. Since $w_h$ and $u_h$ commute, by Corollary 5.8a, it follows that $u_h \in k$. For the same reason, $v_h \in k$.

Now suppose $h(u) = h(v) \neq 0$. Then $u_h$ and $v_h$ commute and the property follows directly from Proposition 5.7. \qed

To set the notation of the next proposition and its corollaries, let $u \in kF \setminus k$ and let $C$ be the centralizer of $u$. Let $H < F$ be the subgroup of $F$ generated by the union of the supports of all elements of $C$:

\[H = \langle \bigcup_{v \in C} \text{Supp}(v) \rangle.\]

Let us call $H$ the **centralizer-supporting group of $u$**.

**Proposition 6.2.** The centralizer-supporting group $H$ of $u \in kF \setminus k$ is finitely generated. Moreover, the image of $\text{Supp}(u)$ in $H^{ab}$, the abelianization of $H$, generates a subgroup of $H^{ab}$ whose rank equals the rank of $H$.

**Proof.** Being a subgroup of $F$, the group $H$ is free; and the centralizer of $u$ in $kH$ is clearly again $C$. Now $\text{Supp}(u)$ is finite, hence contained in a finitely generated free factor of $H$, hence by Lemma 3.5 that free factor is all of $H$, so $H$ is finitely generated.

If the subgroup of $H^{ab}$ generated by the image of $\text{Supp}(u)$ in $H^{ab}$ had rank less than $\text{rank}(H) = \text{rank}(H^{ab})$, that image would lie in the kernel of a nonzero homomorphism $H^{ab} \to \mathbb{Z}$, so by Corollary 5.8a, the supports of all elements of $C$ would lie in that kernel, contradicting the assumption that they generate $H$. \qed
In the following corollaries and below, when we say that an element of \(kF\) is supported on a cyclic group we simply mean that its support is contained in a cyclic subgroup of \(F\).

**Corollary 6.3.** Suppose that \(u \in kF\) is supported on a cyclic group. Then the centralizer of \(u\) in \(kF\) is of the form \(kZ\) where \(Z\) is the largest cyclic subgroup of \(F\) supporting \(u\).

**Corollary 6.4.** Suppose that \(u \in kF\) is not supported on a cyclic group. Then the image of \(\text{Supp}(u)\) in \(H^{ab}\), the abelianization of \(H\), generates a subgroup of \(H^{ab}\) whose rank is at least 2.

We now arrive at our main result.

**Theorem 6.5.** Suppose that \(u \in kF\) is not supported on a cyclic group. Let \(C\) be the centralizer of \(u\). Then \(C\) is the affine coordinate ring of the complement of a \(k\)-point in a proper nonsingular curve over \(k\).

**Proof.** As discussed in Section 3.3, \(C\) is a commutative integrally closed integral domain. Our proof will consist of showing that \(C\) admits a discrete degree function \(d\) which satisfies condition (i) of Lemma 3.6. For in that case, that \(C\) is integrally closed will imply that the curve \(W\) in condition (iv) of the lemma is nonsingular.

Since \(\text{Supp}(u)\) is not contained in a cyclic group, by Corollary 6.4, we can, if necessary, replace \(F\) by the centralizer-supporting group of \(u\) (cf. above Proposition 6.2) and thereafter assume that the image of \(\text{Supp}(u)\) in \(F^{ab}\), the abelianization of \(F\), generates a subgroup of rank at least 2.

Under this assumption, we will construct a group homomorphism \(h: F \to (\mathbb{R}, +)\), (cf. Section 3.2) with respect to which \(h(u) > 0\) and the highest degree homogeneous component \(u_h\) of \(u\) is not a monomial (cf. Section 3.2). Although it is not necessary, we can make the resulting degree function \(h\) discrete without extra effort.

We will use the following geometric fact: If \(K\) is a bounded convex polytope (=the convex hull of a finite set in \(\mathbb{R}^s\)), the intersection of all the facets (=faces of codimension 1) of \(K\) is empty.

To prove this fact, suppose \(O \in \mathbb{R}^s\) belongs to every facet of \(K\). Let us translate \(K\) so that \(O\) is at the origin. We can assume without loss of generality that \(K\) is not contained in a proper subspace of \(\mathbb{R}^s\) for otherwise we could pass to such a subspace.

Since \(K\) is convex, it is an intersection of finitely many half-spaces. In other words, there are finitely many \(\mathbb{R}\)-linear forms \(l_i: \mathbb{R}^s \to \mathbb{R}\) and constant terms \(b_i \in \mathbb{R}\), such that

\[
K = \left\{ x \in \mathbb{R}^s \mid (\forall i) \ l_i(x) \leq b_i \right\}.
\]

Assuming that none of the inequalities \(l_i(x) \leq b_i\) above are redundant, facets of \(K\) are the sets \(Y_i = \left\{ x \in K \mid l_i(x) = b_i \right\}\). Since \(O\) belongs to every facet of \(K\), it follows that \(b_i = 0\) for all \(i\). Hence \(K\) is a cone with the apex at 0 in the sense that

\[
\lambda > 0, \ x \in K \implies \lambda x \in K.
\]

This contradicts boundedness of \(K\).
Let $F^{ab}$ be the abelianization of $F$, with the group operation written additively. Let

$$q : F \to \mathbb{R} \otimes \mathbb{Z} F^{ab}$$

be the canonical homomorphism.

We are now ready to construct $h$ with the properties stated in the 3rd paragraph of this proof. Let $V$ be the $\mathbb{R}$-span of $q(\text{Supp}(u))$ in $\mathbb{R} \otimes \mathbb{Z} F^{ab}$ and let $K$ be the bounded polytope which is the convex hull of

$$q(\text{Supp}(u)) \cup \{0\}.$$

By our assumption, $\dim K = \dim V \geq 2$. By the above fact about bounded convex polytopes, $K$ has a facet $Y$ which does not contain the origin $0$. Choose an $\mathbb{R}$-linear form $l : V \to \mathbb{R}$ and $b \in \mathbb{R}$ so that

$$(18) \quad l \leq b \text{ on } K \text{ and } l = b \text{ on } Y. $$

It follows that $l < b$ on $K \setminus Y$, and since $0 \in K \setminus Y$, we get $0 < b$.

Now extend $l$ to an $\mathbb{R}$-linear form $\eta : \mathbb{R} \otimes \mathbb{Z} F^{ab} \to \mathbb{R}$ anyhow and define

$$h = \eta \circ q.$$

Let us verify that $h$ has the desired properties. We continue working inside $V$. Since $K$ is the convex hull of $q(\text{Supp}(u)) \cup \{0\}$, and $0 \notin Y$, it follows that the vertices of $Y$ are in $q(\text{Supp}(u))$. Therefore, $(18)$ implies that

$$h(u) = \max \{h(u) | u \in \text{Supp}(u)\} = \max \{l(x) | x \in q(\text{Supp}(u))\} = b > 0.$$

Now, if we write

$$u = \sum_{u} a_{u} u,$$

we get

$$u_{h} = \sum_{q(u) \in Y} a_{u} u.$$

Hence $\text{Supp}(u_{h}) = \{u \in \text{Supp}(u) | q(u) \in Y\}$, which implies that the vertices of $Y$ are not only in $q(\text{Supp}(u))$, but also in $q(\text{Supp}(u_{h}))$. Since $\dim K \geq 2$, we have $\dim Y \geq 1$, and thus $Y$ has at least 2 vertices. Therefore, $\text{Supp}(u_{h})$ contains at least 2 elements, or, in other words, $u_{h}$ is not a monomial.

We now define our degree function $d$ to be the restriction of $h : kF \to \mathbb{R} \cup \{\infty\}$ to $C$. Let us verify that $d$ satisfies condition (i) of Lemma 3.6. Let $w \in \text{Supp}(u_{h})$. Since $w$, the leading homogeneous component of $w$, commutes with $u_{h}$ and $h(u_{h}) > 0$, by part (d) of Corollary 5.8, $h(w) \geq 0$. □

The following says that in the special case of a homogeneous element, the non-singular curve in the conclusion of the theorem is a line.

**Proposition 6.6.** If $u$ is homogeneous of non-zero degree, and not a monomial, then its centralizer is isomorphic to the polynomial ring $k[t]$.

**Proof.** After replacing the group homomorphism $h : F \to (\mathbb{R}, +)$ by $-h$ if necessary, we can assume without loss of generality that $h(u) > 0$. Let $C$ be the centralizer of $u$. As $u$ is homogeneous of non-zero degree and yet not a monomial, $u$ cannot be supported on a cyclic group. Thus from Theorem 6.5 we know that $C$ satisfies the equivalent conditions of Lemma 3.6. Moreover, Remark 3.8 (or the proof of the theorem) shows that under our assumptions about $u$, the restriction of $h$ to
$C$ can be used as the degree function $d$ that appears in the lemma. Since $u$ is homogeneous, $C$ is in fact graded by $h$: indeed, if $v$ commutes with $u$, so does each homogeneous component of $v$.

Let $t \in C$ be a homogeneous element of the smallest positive degree. Let $v \in C$ be homogeneous. If $h(v) = 0$, by property (4) in Lemma 3.6, $v \in k$. Otherwise, since $h$ is discrete on $C$, there are coprime positive integers $n$ and $m$ for which $h(v^n) = h(t^m)$. Then by property (4) again and homogeneity it follows that for some $\lambda \in k$, $v^n = \lambda t^m$. Now $C$ is integrally closed (cf. Section 3.3), therefore the equation $v^n = \lambda t^m$ implies that both $v$ and $t$ are scalar multiples of powers of an element in $C$, and since $t$ has the smallest positive degree possible, that element can be taken to be $t$. Thus $v = \lambda t^m$ and since $v$ was an arbitrary homogeneous element of $C$, we conclude that $C = k[t]$. Finally, by Lemma 3.6 $t$ is transcendental over $k$. \[ \square \]

7. Open Question

Recall that in the Introduction we divided G. Bergman’s proof of his theorem into two steps. By analogy with the second step, we would like to ask the following:

Open Question 7.1. Does every finitely generated subalgebra $R \neq k$ of a free group algebra $kF$ over $k$ admit a $k$-algebra homomorphism $f : R \to k[t, t^{-1}]$ into the ring of Laurent polynomials of a single variable $k[t, t^{-1}] \cong k[\mathbb{Z}]$ which is nontrivial in the sense that $f(R) \neq k$?

8. Proof of Lemma 3.6

By a function field of one variable over $k$ we mean a finitely generated field extension $K/k$ of transcendence degree 1. By a place of $K/k$ we mean an equivalence class of discrete valuations (cf. [Liu02, Ch 3, Definition 3.22]) on $K$ which are trivial on $k$.

Recall that if $K$ and $L$ are function fields of one variable over $k$, and $K \subset L$, then for any place $q$ of $K$,

$$ (19) \quad [L : K] = \sum_p e_{p/q} [k(p) : k(q)] $$

where the summation is over all places $p$ above $q$, $e_{p/q}$ is the ramification index (cf. [Liu02, Ch 7, Exercise 1.8]) at $p$ and $k(p)$ and $k(q)$ are the residue fields at $p$ and $q$ resp. (cf [Liu02 (4.8), p. 290]). Clearly for any place $p$ above $q$,

$$ (20) \quad e_{p/q} \leq [L : K]. $$

When we say that $q$ is totally ramified in $L$ we mean that for some $p$ above $q$,

$$ e_{p/q} = [L : K]. $$

Formula (19) shows that this happens if and only if there is a sole place $p$ above $q$ and moreover $k(p) = k(q)$.

Proof of Lemma 3.6

(i) $\implies$ (ii): By property (4), all elements of $C$ of degree 0 are in $k$. Since we assume that $C \neq k$, it follows that $d$ is not identically zero on $C \setminus \{0\}$. Since $d$ is discrete, we can normalize $d$ so that it maps $C \setminus \{0\}$ into $\mathbb{Z}$ but not into any proper subgroup of $\mathbb{Z}$. Also, since $d(xy) = d(x) + d(y)$, $d(C \setminus \{0\})$ is closed under addition. Given a set of positive integers $x_1, \ldots, x_s$ with $g.c.d.(x_1, \ldots, x_s) = 1$, it is
well-known that all sufficiently large integers can be written as linear combinations of the \( x_i \) with non-negative integer coefficients. This is best known in the context of the coin problem, which asks for the largest integer, known as the Frobenius number, which is not equal to such a linear combination (see for example, [EG72]). Thus, by the finiteness of the Frobenius number, \( d(C \setminus \{0\}) \) contains all large enough integers.

Let \( x \in C \setminus k \) and denote \( n := d(x) \). Note that \( n > 0 \).

- \( x \) is transcendental:
  - Suppose \( f(t) = a_0 + a_1 t + \cdots + t^s \) is a non-zero polynomial over \( k \). Then \( f(x) = a_0 + a_1 x + \cdots + x^s \neq 0 \) because, using Remark 3.3 we obtain \( d(f(x)) = ns \neq d(0) = -\infty \).

- \( C \) is a finitely generated \( k[x] \)-module:
  - We are reproducing here the argument in the proof of [Ber69, Proposition 2.2].
    Let \( e_1, \ldots, e_n \in C \) be chosen so that each congruence class modulo \( n \) contains exactly one \( d(e_i) \) and this is equal to the minimal member of this class in \( d(C \setminus \{0\}) \).

This is possible because we assume that \( d \geq 0 \) on \( C \setminus \{0\} \). Let \( M \) be the \( k[x] \)-module generated by \( e_1, \ldots, e_n \). We claim that \( M = C \). Suppose the contrary and let \( y \in C \setminus M \) be of the least \( d \)-degree. Let \( j \) be such that \( d(y) \equiv d(e_j) \pmod{n} \).

Then for some \( s \geq 0 \), \( d(y) = d(x^s e_j) \) and by property \( \{4\} \), for some \( \lambda \in k \),

\[
d(y - \lambda x^s e_j) < d(y).
\]

Since \( y \) has the least degree for an element outside of \( M \), \( m = y - \lambda x^s e_j \in M \), and thus \( y = m + \lambda x^s e_j \in M \), a contradiction. Thus \( M = C \) and therefore the \( k[x] \)-module \( C \) is generated by \( e_1, \ldots, e_n \).

- \( \infty \) is totally ramified in \( \text{Frac} \ C \):
  - Let \( v_\infty \) denote the valuation of \( k(x) \) at \( \infty \). Thus for any polynomial \( f \in k[x] \),

\[
v_\infty(f) = -\deg f.
\]

Let \( v \) denote the valuation on \( \text{Frac} \ C \) which coincides with \(-d \) on \( C \) (cf. Remark 3.2) and let \( p \) denote the corresponding place of \( \text{Frac} \ C \). Since \( d \) maps \( C \setminus \{0\} \) into \( \mathbb{Z} \) but not into any of its proper subgroups, our \( v \) sends \( \text{Frac} C \setminus \{0\} \) surjectively onto \( \mathbb{Z} \), i.e. \( v \) is normalized. Applying Remark 3.3 \( \forall f \in k[x] \),

\[
d(f) = n \deg f, \quad \text{hence} \quad v(f) = n v_\infty(f).
\]

Thus \( v \) is an extension of \( v_\infty \) to \( \text{Frac} \ C \) with ramification index \( e_{p/\infty} = n \).

Since \( C \) is generated as a \( k[x] \)-module by the \( n \) elements \( e_1, \ldots, e_n \),

\[
e_{p/\infty} = n \geq [\text{Frac} C : k(x)].
\]

After comparing this with (20), we conclude that \( \infty \) is totally ramified in \( \text{Frac} C \) and get as a side consequence that \( e_1, \ldots, e_n \) is a basis for \( C \) as a free \( k[x] \)-module.

- \( (ii) \implies (iii) \): Trivial.

- \( (iii) \implies (iv) \): Let \( U = \text{Spec} \ C \). Let \( W \) be the proper completion of \( U \) obtained by adding to \( U \) the regular points corresponding to all the places of \( \text{Frac} C \) which are not over any point in \( U \). This is the smallest proper completion of \( U \) (cf. [Liu02, Section 4.1 Exercise 1.17]) in the sense that any morphism from \( U \) to a proper scheme \( Y \) extends uniquely to a morphism \( W \to Y \). The curve \( W \) is reduced and irreducible.

The element \( x \) determines a morphism of algebraic curves over \( k \):

\[
\varphi : U \to \mathbb{A}^1_k.
\]
As \( A_k^1 \rightarrow \mathbb{P}_k^1 \), and \( \mathbb{P}_k^1 \) is proper, \( \varphi \) extends uniquely to a morphism \( \varphi : W \rightarrow \mathbb{P}_k^1 \):

\[
\begin{array}{ccc}
U & \longrightarrow & W \\
\varphi & \downarrow & \varphi \\
A_k^1 & \longrightarrow & \mathbb{P}_k^1
\end{array}
\]

Clearly \( \varphi^{-1}(\infty) \subseteq W\setminus U \), so \( \varphi^{-1}(\infty) \) consists of regular points. Thus the local rings of points in the set \( \varphi^{-1}(\infty) \) are valuation rings of places of \( \text{Frac} \ C \) above \( \infty \). Since \( \infty \) is totally ramified in \( \text{Frac} \ C \), by (19), there is a unique place of \( \text{Frac} \ C \) above \( \infty \), and moreover the residue field at that place is \( k \). Thus \( \varphi^{-1}(\infty) \) consists of a unique point \( p \in W \).

It remains to show that \( U = W\setminus \{ p \} \). As we are about to see, this follows from the finiteness of \( k[x] \rightarrow C \). We have

\[
U \hookrightarrow W\setminus \{ p \} \rightarrow A_k^1
\]

which gives

\[
k[x] \hookrightarrow \mathcal{O}_W(W\setminus \{ p \}) \rightarrow C.
\]

Since \( k[x] \rightarrow C \) is finite, so is

\[
(22) \quad \mathcal{O}_W(W\setminus \{ p \}) \hookrightarrow C.
\]

Here we will use the following important fact: Any curve over \( k \) which is not proper is affine ([Liu02, Sec. 7.5, Ex. 5.5]). By this fact \( W\setminus \{ p \} \) is affine, and it follows from finiteness of (22) that \( U \hookrightarrow W\setminus \{ p \} \) is finite and hence integral. Hence, by the Going-up theorem for integral homomorphisms, it is surjective. Thus \( U = W\setminus \{ p \} \).

(iv) \implies (v): Let \( v \) denote the discrete valuation at \( p \). Suppose \( v(x) \geq 0 \) for some \( x \in C \). Then \( x \) is a global section of \( W \) and since \( W \) is proper, it follows (see for example [Liu02, Sec. 7.3.2, Corollary 3.18]) that \( v(x) = 0 \). Thus \( v \) is non-positive on \( C \). The residue field of \( v \) is \( k \) because \( p \) is \( k \)-rational.

(v) \implies (i):

Define \( d \) to be the restriction of \(-v\) to \( C \). From the definition of a discrete valuation it follows that \( d \) is a discrete degree function (cf. Remark[3.2]). It remains to show property (4), which, when expressed in terms of \( v \), becomes:

\[
(23) \quad (\forall x, y \in C\setminus \{ 0 \}) \quad v(x) = v(y) \implies (\exists \lambda \in k) \quad v(x - \lambda y) > v(x).
\]

Let \( R \) be the local ring of \( v \) and \( t \) be a uniformizer, i.e., an element of \( R \) with \( v(t) = 1 \). The quotient \( R/tR \) is the residue field. Thus \( R/tR = k \). We have for all \( n \):

\[
v(x) \geq n \iff x \in R t^n
\]

\[
R t^n / R t^{n+1} \cong R / R t = k.
\]

Hence property \([23]\) holds for all \( x, y \in \text{Frac} \ C \).

The isomorphism \((24)\) also shows that every element \( x \in \text{Frac} \ C \) can be expanded into a Laurent series in \( t \) with coefficients in \( k \). Then \( v(x) \) is the degree of the lowest term. Viewed from this vantage point, property \([23]\) is clear. \( \Box \)
References

[Ber69] G. Bergman. Centralizers in free associative algebras. Trans. Am. Math. Soc., pages 327–344, 1969.
[Coh64] P. M. Cohn. Subalgebras of free associative algebras. Proc. London Math. Soc., 14(3):618–632, 1964.
[Coh06] P. M. Cohn. Free Ideal Rings and Localization in General Rings. Cambridge Univ. Press, 2006.
[EG72] P. Erdős and R. L. Graham. On a linear diophantine problem of Frobenius. Acta Arith., 21:399–408, 1972.
[Fox53] Ralph H. Fox. Free differential calculus. I. Derivation in the free group ring. Ann. of Math. (2), 57:547–560, 1953.
[Liu02] Qing Liu. Algebraic geometry and arithmetic curves, volume 6 of Oxford Graduate Texts in Mathematics. Oxford University Press, Oxford, 2002.
[Lot02] M. Lothaire. Algebraic combinatorics on words, volume 90 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 2002.

SUNY Oswego, Oswego, NY 13126
E-mail address: nikita.miasnikov@oswego.edu