# ON FREE SUBALGEBRAS OF
# CERTAIN DIVISION ALGEBRAS

Martin Lorenz

Sonderforschungsbereich 40
Theoretische Mathematik
Beringstraße 4
D - 5300 Bonn 1

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
D - 5300 Bonn 3

MPI/SFB 84-60

# ON FREE SUBALGEBRAS OF CERTAIN DIVISION ALGEBRAS

Martin Lorenz

The goal of this note is to prove the following

<u>Theorem</u>. Let $K = k(t)$ be the rational function field over the field $k$, let $\alpha \in \mathrm{Aut}_k(K)$ be of infinite order, and let $K_\alpha[X]$ denote the skew polynomial ring. Then the classical division ring of fractions $D = Q(K_\alpha[X])$ contains non-commutative free $k$-subalgebras.

For example, if $\alpha$ sends $t$ to $\lambda \cdot t$, where $\lambda \in k^*$ is not a root of unity, then $D = Q(K_\alpha[X])$ equals the division algebra $E_\lambda$ studied in [L] and the theorem gives [L, Theorem 2.2]. Also, if $t^\alpha = t-1$ and $\mathrm{char}\, k = 0$, then $D = Q(K_\alpha[X])$ is the Weyl division algebra $D_1 = Q(k[X,Y]/(XY-YX-1))$ (take $t = XY$). Thus we also recover the main result of Makar-Limanov's article [ML 1]. We emphasize, however, that the crucial ideas used in the proof of the theorem come directly from Makar-Limanov's papers [ML 1] and [ML 2]. In fact, if $k$ is algebraically closed, then every $\alpha \in \mathrm{Aut}_k(K)$

of infinite order is conjugate to one of the above two types of automorphisms and so the theorem could be deduced from the above special cases. Thus we only take credit for the presentation and the unified approach to Makar-Limanov's results.

Throughout, $k$ will denote a commutative field.

## 1. Lemmas on $\mathrm{Aut}_k(k(t))$ .

Let $K = k(t)$ be the rational function field over $k$ . Then every $\sigma \in \mathrm{Aut}_k(K)$ acts by a fractional linear transformation

$$t \longmapsto \frac{at+b}{ct+d} \quad \text{with} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} =: M(\sigma;t) \in PGL_2(k) .$$

The effect of replacing the primitive element $t$ of $K/k$ by $t^\tau$ , $\tau \in \mathrm{Aut}_k(K)$ , is described by the formula

$$M(\sigma;t^\tau) = M(\tau;t)\cdot M(\sigma;t)\cdot M(\tau;t)^{-1} .$$

$PGL_2(k)$ also operates by fractional linear transformations on $\mathbb{P}^1(k) = k \cup \{\infty\}$ , and $\infty$ is a fixed point for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL_2(k)$ if and only if $c = 0$ .

Lemma 1. Let $K = k(t)$ and let $\sigma \in \mathrm{Aut}_k(K)$ be such that $S = M(\sigma;t)$ satisfies $S^i\cdot\infty \neq \infty$ for all $i \neq 0$ . Then

$$\{f^\sigma - f \mid f \in K\} \cap k[t] \subseteq k \ .$$

<u>Proof</u>. We use the valuations $v_\gamma : K \longrightarrow \mathbb{Z} \cup \{\infty\} (\gamma \in \mathbb{P}^1(k))$ given by $v_\infty(g)$ = deg (denominator of $g$ ) - deg (numerator of $g$ ) and $v_\gamma(g) = \mathrm{ord}_{t-\gamma}(g) \quad (g \in K, \gamma \in k)$ . Then, for all $g \in K^*$ , $v_\gamma(g) = 0$ for almost all $\gamma \in \mathbb{P}^1(k)$ , and

$$v_\gamma(g^\tau) = v_{T\cdot\gamma}(g) \quad (\gamma \in \mathbb{P}^1(k), \tau \in \mathrm{Aut}_k(K), T = M(\tau;t)) \ .$$

(It suffices to check this for $\gamma = \infty$ , as $PGL_2(k)$ operates transitively on $\mathbb{P}^1(k)$ . Also, by passing to an algebraic closure $\bar{k}$ of $k$ , one can assume that $g = t-\alpha$ , $\alpha \in \bar{k}$ .)

Now suppose that, for some $f \in K$ , $f^\sigma - f \in k[t]$ and $\deg(f^\sigma - f) > 0$ . Then $v_\infty(f^\sigma - f) < 0$ but $v_\gamma(f^\sigma - f) \geq 0$ for all $\gamma \neq \infty$ . Therefore, $\min\{v_\infty(f^\sigma), v_\infty(f)\} < 0$ , say $v_\infty(f) < 0$ . Then, setting $S = M(\sigma;t)$ , we have

$$v_{S^{-1}\cdot\infty}(f^\sigma) = v_\infty(f) < 0, \ v_{S^{-1}\cdot\infty}(f^\sigma - f) \geq 0$$

and thus $v_{S^{-1}\cdot\infty}(f^\sigma) = v_{S^{-1}\cdot\infty}(f) < 0$ . Continuing in this way, we see that $v_{S^{-i}\cdot\infty}(f) = v_\infty(f) < 0$ holds for all $i \geq 0$ , contradiction! Similarly, $v_\infty(f^\sigma) < 0$ leads to a contradiction and so the lemma is proved.

<u>Lemma 2</u>. Let $K = k(t)$ and let $\sigma \in \mathrm{Aut}_k(K)$ be of infinite order. Then there exists a primitive element $a$ for $K/k$

such that $A = M(\sigma;a)$ satisfies $A^i\cdot\infty \neq \infty$ for all $i \neq 0$ .

<u>Proof</u>. Set $T = M(\sigma;t) \in PGL_2(k)$ . It suffices to show that there exists $\xi \in \mathbb{P}^1(k) = k \cup \{\infty\}$ with $T^i\cdot\xi \neq \xi$ for all $i \neq 0$ . Indeed, if $\xi$ is such an element, choose $X \in PGL_2(k)$ with $X\cdot\xi = \infty$ and set $a = t^\tau$ , where $M(\tau;t) = X$ . Then $a$ is a primitive element for $K/k$ , and $A = M(\sigma;a) = XTX^{-1}$ satisfies $A^i\cdot\infty \neq \infty$ for all $i \neq 0$ , as required.

To establish the existence of $\xi$ as above, first note that, by the theory of Jordan canonical form, there exists a matrix $Y \in PGL_2(\bar{k})$ ($\bar{k}$ = algebraic closure of $k$ ) such that $T_1 = Y^{-1}T\,Y \in PGL_2(\bar{k})$ has one of the following two forms:

$$T_1 = \begin{pmatrix} \mu_1 & 1 \\ 0 & \mu_1 \end{pmatrix} = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}, \quad \mu=\mu_1^{-1} \in \bar{k}^* , \quad \operatorname{char} k = 0$$

or

$$T_1 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}, \quad \lambda=\lambda_1\lambda_2^{-1} \in \bar{k}^* \text{ a non-root of unity.}$$

Thus $T_1$ acts on $\mathbb{P}^1(\bar{k})$ via $\xi \longmapsto \xi+\mu$ or $\xi \longmapsto \lambda\xi$ . In either case, $T_1^i\cdot\xi_1 \neq \xi_1$ for all $i \neq 0$ and $\xi_1 \in \mathbb{P}^1(\bar{k}) \setminus \{0,\infty\}$ . As $\mathbb{P}^1(\bar{k}) \setminus \{0,\infty\}$ intersects $Y^{-1}\cdot\mathbb{P}^1(k) \leq \mathbb{P}^1(\bar{k})$ non-trivially ($k$ must be infinite for $\sigma$ to exist) we can choose $\xi_1 \in \mathbb{P}^1(\bar{k}) \setminus \{0,\infty\}$ with

$\xi = Y\cdot\xi_1 \in \mathbb{P}^1(\bar{k})$ . But then $T^i\cdot\xi = YT_1^i\cdot\xi_1 \neq Y\cdot\xi_1 = \xi$ for all $i \neq 0$ , as required.

Examples. (a). If $\sigma$ is given by $t^\sigma = t+\mu$ , $\mu \in k^*$ and char $k = 0$ , then $T = M(\sigma;t)$ satisfies $T^i\cdot\xi \neq \xi$ for all $\xi \in k$ and $i \neq 0$ . Thus we can take $X = \begin{pmatrix} 0 & 1 \\ 1 & -\xi \end{pmatrix}$ in the above argument and get $a = (t-\xi)^{-1}$ $(\xi \in k)$ as possible choices for $a$ .

(b). Similarly, if $t^\sigma = \lambda t$ , $\lambda \in k^*$ a non-root of unity, then we can take $a$ of the form $\alpha = (t-\xi)^{-1}(\xi \in k^*)$ .

## 2. Proof of the theorem.

Let $K = k(t)$ and let $\alpha \in \mathrm{Aut}_k(K)$ be of infinite order. Set $D = Q(K_\alpha[X])$ , the classical division algebra of fractions of the skew polynomial ring $K_\alpha[X]$ . The theorem will be a consequence of the following

Proposition. Let $a \in K$ be as in Lemma 2 and set $b = a(1-X)^{-1} \in D$ . Then the subalgebra $k[a,b] \subseteq D$ is free on $\{a,b\}$ .

The rest of this section is devoted to the proof of this proposition. We will proceed in a number of steps. First note that the localization of the skew power series ring $K_\alpha [[X]]$

at the powers of $X$ is a skew field containing $K_\alpha[X]$, and hence a copy of $D$. Here, $(1-X)^{-1} \in D$ corresponds to $1+X+X^2+\ldots \in K_\alpha[\![X]\!]$ and so the images of a and b lie in $K_\alpha[\![X]\!]$. In the following, we work in $K_\alpha[\![X]\!]$. Note that, as K-vector space, $K_\alpha[\![X]\!]$ can be identified with the set of functions $\varphi : \mathbb{N}_0 = \{0,1,2,\ldots\} \longrightarrow K$.

(A) Equivalence classes of functions $\mathbb{N}_0 \longrightarrow K$. Let $F$ denote the set of equivalence classes of functions $\varphi : \mathbb{N}_0 \longrightarrow K$ modulo the relation $\sim$ given by

$$\varphi \sim \psi :\Longleftrightarrow \varphi(n) = \psi(n) \quad \text{for almost all } n .$$

Then $F$ becomes a commutative ring under pointwise addition and multiplication of functions. In the sequel, we use the same notation for a function $\varphi : \mathbb{N}_0 \longrightarrow K$ and its class modulo $\sim$. For $\varphi \in F$ define $\varphi^\sigma \in F$ by

$$\varphi^\sigma(n) = \varphi(n+1) \qquad (n \gg 0) .$$

Then $\sigma$ is an automorphism of $F$ which acts trivially on the set of constant functions $C \subseteq F$. Clearly, $C \cong K$ and we will identify constants with their values $\in K$. Finally, define $\gamma \in F$ by

$$\gamma(n) = a^{\alpha^n} \qquad (n \gg 0) ,$$

and let $A \subseteq F$ be the subring of $F$ generated by $C$ and $\gamma$ .

<u>Claim</u>. $A = C[\gamma]$ is a polynomial algebra over $C$ . Moreover, all nonzero elements of $A$ are units in $F$ and so $K := Q(A) \subseteq F$ . Finally, $\sigma$ operates on $K$ and $\{\varphi^{\sigma}-\varphi \mid \varphi \in K\} \cap A \subseteq C$ .

<u>Proof</u>. First note that $\gamma : \mathbb{N}_0 \longrightarrow K$ is injective, because otherwise a would have a finite $\alpha$-orbit and hence $\alpha$ would have finite order. Therefore, each nontrivial polynomial $\sum_{i \in I} c_i \gamma^i$ $(I \neq \emptyset,\ c_i \in C^*)$ has only finitely many zeroes in $\mathbb{N}_0$ . It follows that $\sum_{i \in I} c_i \gamma^i$ is a unit in $F$ . In particular, $\gamma$ is transcendental over $C$ and $K = Q(A) \cong C(\gamma) \subseteq F$ . Moreover, if $M(\alpha;a) = \begin{pmatrix} r & s \\ u & v \end{pmatrix} \in PGL_2(k)$ , then for all $n >> 0$ we have

$$\gamma^{\sigma}(n) = (a^{\alpha})^{\alpha^n} = \left(\frac{ra+s}{ua+v}\right)^{\alpha^n} = \frac{r\gamma(n)+s}{u\gamma(n)+v}$$

so that $\gamma^{\sigma} = \frac{r\gamma+s}{u\gamma+v} \in K = C(\gamma)$ and $M(\sigma;\gamma) = M(\alpha;a)$ . Therefore, by our choice of $a$ , we have $M(\sigma;\gamma)^{i}\cdot\infty \neq \infty$ for all $i \neq 0$ and Lemma 1 implies that $\{\varphi^{\alpha}-\varphi \mid \varphi \in K\} \cap C[\gamma] \subseteq C$ .

(B) For $J = (j_1, j_2, \ldots, j_s) \in \mathbb{N}^s$ $(s \geq 1)$ set

$$\beta_J(n) = \sum_{n \geq n_1 \geq \ldots \geq n_s \geq 0} \gamma(n_1)^{j_1} \cdot \gamma(u_2)^{j_2} \cdot \ldots \cdot \gamma(n_s)^{j_s} \quad (n \in \mathbb{N}_0) .$$

For $s \leq 0$ let $J = (\emptyset)$ and $\beta_{(\emptyset)}(n) = 1$ for all $n$ .

Claim. In order to prove the proposition, it suffices to show that the functions $\beta_J \in F$ $(J \in \bigcup_s \mathbb{N}^s)$ are linearly independent over $K \subseteq F$ .

Proof. We have to show that formally distinct monomials in $a$ and $b = a(1-X)^{-1} = a(1+X+X^2+\ldots)$ are linearly independent over $k$ . Each such monomial has the form

$$m_{(i_0,i_1\ldots,i_v)} = a^{i_0}\ (1-X)^{-1}\ a^{i_1}\ \ldots\ (1-X)^{-1} a^{i_v}\ ,$$

where $0 \leq v = \#$ b-factors , $i_v \in \mathbb{N}_\circ$ and $i_0,\ldots,i_{v-1} \in \mathbb{N}$ for $v \geq 1$ . In $K_\alpha[\![X]\!]$ , we have

$$m_{(i_0,i_1,\ldots,i_v)} = \sum_{n\geq 0} X^n (a^{\alpha^n})^{i_0} \cdot \Big(\sum_{n\geq n_1\geq\ldots\geq n_{v-1}\geq 0} \Big(a^{\alpha^{n_1}}\Big)^{i_1} \cdot\ldots\cdot \Big(a^{\alpha^{n_{v-1}}}\Big)^{i_{v-1}}\Big)\ a^{i_v}$$

$$= \sum_{n\geq 0} X^n \gamma(n)^{i_0} \cdot a^{i_v} \cdot \beta_{(i_1,\ldots,i_{v-1})}(n)$$

(where $(i_1,\ldots,i_{v-1}) = (\emptyset)$ for $v \leq 1$ and the $\gamma(n)^{i_0}$ -term is zero for $v = 0$ and $n > 0$ ). For each multiindex $I = (i_0,i_1,\ldots,i_v)$ as above write $I' = (i_1,\ldots,i_{v-1}) \in \mathbb{N}^{v-1}$ $(I' = (\emptyset)$ for $v \leq 1$ ). Suppose that

$$\sum_{I\in\mathcal{I}} \xi_I m_I \qquad (\xi_I \in k)$$

is a $k$-linear relation between different monomials $m_I$ $(I \in \mathcal{I})$ and set $\mathcal{I}_0 = \{(i_0,\dots,i_v) \in \mathcal{I} \mid v = 0\}$ , $\mathcal{I}_{>0} = \mathcal{I} \setminus \mathcal{I}_0$ . Then, in $F$ , we have

$$m_I = 0 \quad \text{for all} \quad I \in \mathcal{I}_0$$

and

$$\sum_{I \in \mathcal{I}_{>0}} \xi_I \gamma^{i_0} a^{i_v} \beta_{I'} = 0$$

For $I \in \mathcal{I}_{>0}$ , $\xi_I \gamma^{i_0} a^{i_v}$ belongs to $K$ and $\xi_I a^{i_v} \in C$ . By assumption, the $\beta_{I'}$'s are $K$-independent. Furthermore, by Step(A) , $\gamma$ is transcendantal over $C$ . Finally, a is transcendental over $k$ , by definition. Thus we conclude that $\xi_I = 0$ for all $I \in \mathcal{I}_{>0}$ and so the given relation reduces to $\sum_{I \in \mathcal{I}_0} \xi_I m_I = 0$ . But this is a polynomial equation for a over $k$ which must be trivial. Therefore, $\xi_I = 0$ for all $I \in \mathcal{I}_0$ also, as it was to be shown.

(C) <u>Conclusion</u>. For $\varphi \in F$ define $\Delta\varphi \in F$ by

$$\Delta\varphi = \varphi^{\sigma} - \varphi .$$

The following formulas are straightforward to verify:

i. $\Delta(\varphi\psi) = \varphi^{\sigma} \cdot \Delta\psi + \Delta\varphi \cdot \psi \quad (\varphi,\psi \in F)$ , and

ii. $\Delta\beta_J = \sum_{\ell=1}^{s}\left(\gamma^{j_1+\dots+j_\ell}\right)^{\sigma}\cdot\beta_{J(\ell)}$ (=0 for $s = 0$) ,

where $J = (j_1,\dots,j_s) \in \mathbb{N}^s$ and $J(\ell) := (j_{\ell+1},\dots,j_s)$ .

Moreover, by Step(A) , we have

$$\Delta K \cap C[\gamma] \subseteq C \ .$$

Now suppose that $\sum_J e_J\beta_J = 0$ ($J \in {}_{s\geq 0}\mathbb{N}^s$ , $e_J \in K$ almost all = 0 ) is a nontrivial $K$-linear relation which is chosen so that

$u = \max\{\ell(J) \mid e_J \neq 0\}$ is minimal, where we

have set $\ell(J) = s$ for $J \in \mathbb{N}^s$ ($s \geq 0$) ,

and

the number of summands with $\ell(J) = u$ is minimal.

Clearly, $u \geq 1$ . Rewrite the above relation by isolating the "long" J's to the left:

$$\sum_{J \in \mathcal{J}} e_J\beta_J = \sum_{J \in \bigcup_{s<u}\mathbb{N}^s} d_J\beta_J \quad ,$$

where $\emptyset \neq \mathcal{J} \subseteq \mathbb{N}^u$ and all $e_J$ ($J \in \mathcal{J}$) are nonzero. We can and will also assume that $e_J = 1$ for some $J \in \mathcal{J}$ . Using (i) and (ii) above, we see that

iii. $\Delta(e_J\beta_J) = \Delta e_J\cdot\beta_J + \delta$ , where $\Delta e_J \in \mathcal{K}$ and $\delta$ is a $\mathcal{K}$-linear combination of $\beta_I$'s with $\ell(I) < \ell(J)$ .

As $e_J = 1$ for some $J \in \mathcal{J}$ , and hence $\Delta e_J = 0$ , the relation

iv. $$\Delta(\sum_{J\in\mathcal{J}} e_J\beta_J) = \Delta(\sum_{\substack{J\in\cup\mathbb{N}^s\\ s<u}} d_J\beta_J)$$

involves fewer summands with $\ell(J) = u$ . Therefore, our minimality assumption implies that the latter relation is trivial. In particular, in view of (iii), we deduce that $\Delta e_J = 0$ for all $J \in \mathcal{J}$ , i.e.

$$e_J \in \mathcal{C}^* \qquad \text{for all} \quad J \in \mathcal{J} \ .$$

Moreover, for all $J = (j_1, j_2, \ldots, j_u) \in \mathcal{J}$ , the coefficients of $\beta_{J(1)}$ (recall that $J(1) = (j_2, \ldots, j_u)$) in (iv) must be equal on both sides, i.e.

v. $$\Delta d_{J(1)} = \sum_{\substack{I=(i_1,\ldots,i_u)\in\mathcal{J}\\ I(1) = J(1)}} e_I^\sigma(\gamma^{i_1})^\sigma$$

holds for all $J \in \mathcal{J}$ . Thus, as $e_I \in \mathcal{C}$ for all $I$ on the right, we see that $(\Delta d_{J(1)})^{\sigma^{-1}} = ( d_{J(1)}^{\sigma^{-1}} ) = \sum_{\substack{I=(i_1,\ldots,i_u)\in\mathcal{J}\\ I(1) = J(1)}} e_I\gamma^{i_1}$

belongs to $\Delta K \cap \gamma C[\gamma] = 0$ . But, by Step(A) , $\gamma$ is transcendental over $C$ and so all $e_I$ in (v) must be $0$ , contradiction! This completes the proof of the proposition, and hence the theorem is proved.

ACKNOWLEDGEMENT. Research supported by the DeutscheForschungsgemeinschaft/Heisenberg Programm (Lo 261/2-1).