El. Math. *51* (1996) 0013-6018/96/010035-03$1.50 + 0.20/0

Three-Dimensional Non-Commutative Algebras

Günter Heimbeck and Alfred H. Kamupingene

Born in 1946, Günter Heimbeck studied at Würzburg University where he attained his Dr.rer.nat.habil. in 1981. After having lectured for two and a half years at Würzburg University he joined the University of the Witwatersrand, Johannesburg in 1984. Since 1987 he is a member of the Department of Mathematics of the University of Namibia in Windhoek. His main interest pertains to geometric algebra and translation planes.

Alfred H. Kamupingene was born in 1956 in Namibia. He studied at Sofia University specializing in mathematical physics. After completing his Ph.D. in 1988 on representations of Lie superalgebras and their applications to Wigner quantum systems he spent two years at the Bulgarian Academy of Sciences as a post-doctoral fellow. Currently he is an Associate Professor at the University of Namibia. His main interest is in algebra, topology and mathematical physics.

As it is well-known, for any prime p, there exists, up to isomorphism, exactly one non-commutative ring of order p^3 ([1], p. 195, Further exercises (6)). The purpose of this short note is to generalize this result to algebras.

Theorem. *For any field F, there exists, up to isomorphism, exactly one 3-dimensional non-commutative F-algebra, namely*

$$\left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \,\middle|\, \alpha, \beta, \gamma \in F \right\}.$$

In jeder axiomatischen Theorie bemüht sich die Mathematik, über die verschiedenen (nichtisomorphen) "kleinen" Modelle einen Überblick zu gewinnen. So versucht man etwa in der Gruppentheorie, alle Gruppen von kleiner Ordung aufzuzählen, oder man versucht, für eine Primzahl p, die p-Gruppen der Ordung p, p^2, p^3, etc. der Reihe nach zu beschreiben. Ein derartiges Vorgehen liefert in jeder axiomatischen Theorie eine Reihe von interessanten Beispielen. Auch wenn ein tieferes Verständnis gewöhnlich erst auf Grund weiterführender theoretischer Methoden möglich ist, so handelt es sich bei der Behandlung "kleiner" Modelle immer um einen wichtigen Teilschritt. — Der vorliegende Text liefert einen Beitrag zur Aufzählung kleiner Modelle für die Theorie der nichtkommutativen assoziativen Algebren: Es wird gezeigt, dass es zu einem vorgegebenen Körper F bis auf Isomorphie nur *eine* nichtkommutative Algebra der Dimension 3 gibt. *ust*

Proof. Let A be a 3-dimensional non-commutative F-algebra. F will be considered as a subalgebra of A. For any $a \in A$, let $L_a\colon A \to A$ be defined by $L_a(x) := ax$. The map $a \in A \mapsto L_a \in \operatorname{End} A$ is obviously an injective algebra homomorphism of A into the F-algebra of the endomorphisms of the F-vector space A. We are going to break up the following proof into several small steps.

a) For any $a \in A \setminus F$,

$$F[a] = \{\lambda + \mu a \mid \lambda, \mu \in F\} \cong \begin{cases} F \times F, \\ F[x]/(x^2). \end{cases}$$

Moreover, $F[a]$ contains some $u \in F[a]$ such that $\operatorname{rk} L_u = 1$.

Proof. Since $F[a]$ is commutative, $F[a] \neq A$. On the other hand, $F[a] \neq F$. Therefore, $F[a]$ is 2-dimensional and $(1, a)$ is a basis of $F[a]$. The minimum polynomial $m \in F[x]$ of a over F is of degree 2, and since $F[a] \cong F[x]/(m)$ is not a field, m is reducible. If m has two distinct roots, by the Chinese Remainder Theorem, $F[x]/(m) \cong F \times F$. If m has a double root, $F[x]/(m) \cong F[x]/(x^2)$. Since m is also the minimum polynomial of L_a, L_a has an eigenvalue λ of geometric multiplicity 2. Now $u := a - \lambda \in F[a]$ and $L_u = L_{a-\lambda} = L_a - \lambda \operatorname{id}_A$ is of rank 1.

b) The commutators of A form a 1-dimensional nilpotent ideal C.

Proof. We choose $a, b \in A \setminus F$ such that $F[a] \neq F[b]$. By a), there exist $u \in F[a]$ and $v \in F[b]$ such that L_u and L_v are both of rank 1. Then $(1, u, v)$ is a basis of A. Since $[\alpha + \beta u + \gamma v, \alpha' + \beta' u + \gamma' v] = \beta\gamma'[u, v] + \gamma\beta'[v, u] = (\beta\gamma' - \gamma\beta')[u, v]$ for all $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in F$, any commutator of A is a multiple of $c := [u, v] \neq 0$. Since $\operatorname{rk} L_c = \operatorname{rk} L_{[u,v]} = \operatorname{rk}(L_u \circ L_v - L_v \circ L_u) \leq 2$, $I := \operatorname{im} L_c = \{cx \mid x \in A\}$ and $K := \ker L_c = \{x \in A \mid cx = 0\}$ are proper non-trivial right ideals of A. For any $a \in A$, $[a, c]$ is a multiple of c, i.e. $[a, c] = \lambda c$ for some $\lambda \in F$. Hence $ac = c(a + \lambda)$ and therefore, I is also a left ideal of A. Similarly, $ca = (a - \lambda)c$ shows that K is a left ideal. Therefore, I and K are ideals and none of them is equal to the zero ideal. Thus the algebras A/I and A/K are of dimension at most 2 and hence commutative. This implies $\operatorname{span}\{c\} \subset I, K$. Since $\dim I + \dim K = 3$, one of the ideals I and K is 1-dimensional and hence equal to $\operatorname{span}\{c\}$. Therefore, $C := \operatorname{span}\{c\}$ is an ideal. Since $c \in K$, $c^2 = 0$ and hence C is nilpotent.

c) A contains an idempotent element unequal to 0 or 1.

Proof. The proof will be carried out by assuming the converse, i.e. that 0 and 1 are the only idempotent elements of A. By a), we obtain $F[a] \cong F[x]/(x^2)$ for each $a \in A \setminus F$. In particular, if $a \in A$ is a non-unit, then $a^2 = 0$ and $\operatorname{rk} L_a \leq 1$. If $a, b \in A$ are any two non-units, $\operatorname{rk} L_{a+b} = \operatorname{rk}(L_a + L_b) \leq \operatorname{rk} L_a + \operatorname{rk} L_b \leq 2$ and hence, $a + b$ is a non-unit. Therefore, $0 = (a + b)^2 = a^2 + ab + ba + b^2 = ab + ba$, i.e. $ab = -ba$. Now we choose non-zero non-units $a, b \in A$ and $c \in C \setminus \{0\}$ such that $F[a], F[b], F[c]$ are distinct in pairs. Then a and bc commute and hence $bc \in F[a] \cap C = \{0\}$. Therefore, b and c commute as $bc = -cb$. Since $(1, b, c)$ is a basis of A, A is commutative and this constitutes a contradiction.

d)

$$A \cong \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \middle| \, \alpha, \beta, \gamma \in F \right\}.$$

Proof. Let $c \in C \setminus \{0\}$. By c), there exists some idempotent element $p \in A \setminus F$. Since $pc \in C$, $pc = \xi c$ for some $\xi \in F$. Since $\xi c = pc = p^2 c = p(pc) = p(\xi c) = \xi(pc) = \xi(\xi c) = \xi^2 c$ and $c \neq 0$, $\xi^2 = \xi$ and hence, $\xi = 0$ or $\xi = 1$. Therefore, $pc \in \{0, c\}$. Similarly, we obtain $cp \in \{0, c\}$. We may assume that $pc = 0$ because otherwise we are going to replace p by $1 - p$. Then $cp = c$ as $cp \neq pc$. The 2-dimensional subspace $U := \mathrm{span}\{c, p\}$ is obviously an ideal and hence $a \in A \mapsto L_{a|U} \in \mathrm{End}\, U$ is an algebra homomorphism. The matrices representing $L_{x|U}$ with respect to the basis (c, p) of U for $x \in \{1 - p, p, c\}$ are $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. This suffices to ensure the existence of the asserted isomorphism.

The result about rings of order p^3 mentioned at the beginning of this note becomes, of course, a corollary to our Theorem.

Corollary. *For any prime p, there exists, up to isomorphism, exactly one non-commutative ring of order p^3.*

Proof. If R is a non-commutative ring of order p^3, then the additive group of R is an elementary-abelian p-group and hence, R is a 3-dimensional non-commmutative GF(p)-algebra.

References

[1] P. M. Cohn, Algebra, Volume 2, Second Edition, John Wiley & Sons, Chichester-New York-Brisbane-Toronto-Singapore 1989.

[2] N. Jacobson, Basic Algebra I, W. H. Freeman and Company, San Francisco 1974.

G. Heimbeck
A. H. Kamupingene
University of Namibia
Department of Mathematics
Private Bag 13301
Windhoek, Namibia