COMMUNICATIONS IN ALGEBRA, 16(10), 2133-2135 (1988)

FINITE UNISERIAL RINGS OF PRIME CHARACTERISTIC

S. K. Jain
Department of Mathematics
Ohio University
Athens, Ohio 45701

Jiang Luh
Department of Mathematics
North Carolina State University
Raleigh, North Carolina 27695

B. Zimmermann-Huisgen
Department of Mathematics
University of California
Santa Barbara, California 93106

This note gives a selfcontained and completely elementary proof for the fact that the finite uniserial rings of prime characteristic are (up to isomorphism) precisely the truncated twisted polynomial rings, i.e., of the form $F[x,\sigma]/(x^n)$, where F is a finite field and σ an automorphism of F (scalar multiplication being $\alpha x = x\sigma(\alpha)$ for $\alpha \in F$). While the result itself is known (see [1, Theorem 2] for instance), our short argument is new. As a supplement we show that the group of units U(R) of a noncommutative finite uniserial ring R is nonnilpotent.

Recall that a ring with identity is said to be right uniserial if it possesses a unique finite composition series of right ideals; a uniserial ring is a ring which is both left and right uniserial.

Theorem: Given any prime number p, the finite (right) uniserial rings of characteristic p are (up to isomorphism) exactly the rings $F[x,\sigma]/(x^n)$, where F is a finite field of characteristic p, $\sigma \in \mathrm{Aut}(F)$ and $n \in \mathbb{N}$. Furthermore, any finite uniserial ring of prime characteristic has a solvable

group of units and is commutative if and only if its group of units is nilpotent.

Proof: Let R be a finite right uniserial ring, and let $R/J = GF(p^k)$, where J denotes the Jacobson radical of R.

First we make sure that R/J embeds into R as a subring. Clearly, R contains a copy of $\mathbb{Z}_p$. If $\bar{\beta}$ is a generator for the cyclic group $(R/J)^*$, then the multiplicative order of β in R is a multiple of $p^k - 1$, whence the cyclic group $\langle\beta\rangle$ contains an element α of order $p^k - 1$. Denoting the subring $\mathbb{Z}_p[\alpha]$ of R by F, we observe $x^{p^k} = x$ for all $x \in F$ since $\alpha^{p^k} = \alpha$. Thus each element of F is either zero or nonnilpotent, which implies that $F\setminus\{0\}$ consists of units of R. Consequently, F is a finite integral domain and hence a field. Since $|F| = p^k$, we have $F \cong R/J$. Moreover, from $F \cap J = 0$ we obtain that $R = F \oplus J$ as an abelian group.

Let n be the smallest positive integer with $J^n = 0$. Since the right ideals of R form a chain, they are all principal, and, given any $a \in J \setminus J^2$, the elements $a, a^2, \ldots, a^{n-1}$ form a basis for the right F-vector space J. In particular, for $\gamma \in F$ we have

$$\gamma a = \sum_{i=1}^{n-1} a^i \sigma_i(\gamma)$$

with $\sigma_1(\gamma) \in F$, and $\sigma = \sigma_1 \in \mathrm{Aut}(F)$. If we can find an element $b \in J \setminus J^2$ such that

$$\gamma b = b\sigma(\gamma) \quad \text{for all} \quad \gamma \in F,$$

or equivalently,

$$\alpha b = b\sigma(\alpha),$$

where $F^* = \langle\alpha\rangle$, then the map $F[x,\sigma]/(x^n) \to R$ that sends x to b will be an isomorphism as desired.

We will guarantee the existence of such an element b by induction on n. The cases n = 1,2 are trivial; so let us suppose $n \geq 3$. We start by observing that $\bar{R} = R/J^{n-1}$ inherits the properties we hypothesized for R and that $\bar{R} = F \oplus \bar{J}$, where we identify the field F with its canonical image in $\bar{R}$;

moreover, note that $\gamma\bar{a} - \bar{a}\sigma(\gamma) \in \bar{J}^2$. By induction hypothesis, we can therefore find an element $\bar{c} \in \bar{J}^2$ with $c \in J/J^2$ such that

$$\alpha\bar{c} = \bar{c}\sigma(\alpha).$$

From $J^{n-1} = c^{n-1}F$ we deduce

(1) $\alpha c = c\sigma(\alpha) + c^{n-1}\tau(\alpha)$ for some $\tau(\alpha) \in F$.

Next, a straightforward induction yields

(2) $\alpha c^j = c^j\sigma^j(\alpha)$ for all $j \geq 2$.

We will distinguish two cases.

Case 1: If $\sigma(\alpha) \neq \sigma^{n-1}(\alpha)$, we define $b = c + c^{n-1}\dfrac{\tau(\alpha)}{\sigma(\alpha) - \sigma^{n-1}(\alpha)}$ and verify that $\alpha b = b\sigma(\alpha)$.

Case 2: If $\sigma(\alpha) = \sigma^{n-1}(\alpha)$, then (2) yields $\alpha c^{n-1} = c^{n-1}\sigma(\alpha)$, and by induction it follows from (1) that

(3) $\alpha^j c = c(\sigma(\alpha))^j + jc^{n-1}\tau(\alpha)(\sigma(\alpha))^{j-1}$ for $j \geq 1$.

Set $j = p^k = |F|$ in (3) to obtain $\alpha c = c\sigma(\alpha)$. The choice $b = c$ thus meets our requirements in the second case.

To prove the supplementary statements, note that $U(R) = F^* \cdot H$, where $H = \{1 + x \mid x \in J\}$ is a normal subgroup of $U(R)$. Since $|F^*| = p^k - 1$, whereas $|H| = |J|$ is a power of p, we see that $F^* \cap H = 1$ and that H is solvable; consequently, $U(R)/H \cong F^*$, and $U(R)$ is solvable.

If $U(R)$ is nilpotent, in other words, if the group $U(R)$ is the direct product of its Sylow subgroups, then F^* and H commute elementwise, since H is the Sylow p-subgroup of $U(R)$, while F^* is the direct product of the Sylow q-subgroups for $q \neq p$. But this shows $\alpha x = x\alpha$ for all $\alpha \in F$ and $x \in J$, and we conclude that R is commutative.

References

1. J. L. Fisher, Finite principal ideal rings, Canad. Math. Bull 19, 277-283 (1976).

Received: March 1987