COMPOSITIO MATHEMATICA

CHRISTINE W. AYOUB

On finite primary rings and their groups of units

Compositio Mathematica, tome 21, nº 3 (1969), p. 247-252
<http://www.numdam.org/item?id=CM_1969__21_3_247_0>

COMPOSITIO MATHEMATICA, Vol. 21, Fasc. 3, 1969, pag. 247-252
Wolters-Noordhoff Publishing
Printed in the Netherlands

On finite primary rings and their groups of units

by

Christine W. Ayoub

In a recent paper [1] Gilmer determined those rings R which have a cyclic group of units. He showed that it is sufficient to consider (finite) primary rings. In this note after proving a preliminary result (Theorem 1) we restrict attention to finite primary rings and show some connections between the additive group of N, the radical of the ring R, and the multiplicative group $1+N$. In Theorem 2 we prove that if either N or $1+N$ is cyclic, R is homogeneous (provided $N \neq 0$ — i.e. R is not a field) in the sense that there is a positive integer k such that

$$R/N,\ N/N^2, \dots N^k/N^{k+1}$$

are isomorphic elementary abelian groups under addition and $N^{k+1} = 0$. Furthermore, if $p \geqq 3$, N is cyclic if, and only if $1+N$ is cyclic. As a consequence of this theorem we are able to determine the rings for which N is cyclic and those for which $1+N$ is cyclic (Corollary to Theorem 2). Thus we obtain a quite different proof of Gilman's results as well as a proof of the well-known fact that there is a primitive root, mod p^k when $p \geqq 3$. In a subsequent paper we hope to discuss finite homogeneous rings in general and to determine conditions under which the radical N is isomorphic (as an additive group) to the multiplicative group $1+N$.

1. Terminology and notation

We recall that a primary ring is a commutative ring with 1 which contains a unique prime ideal N (see [2] p. 204). The facts we need about primary rings are:

(1) A finite primary ring is a p-ring — i.e. every element has additive order a power of a prime p.
(2) R/N is a field
(3) N is nilpotent

The notation used is standard. We mention only the following:

$\otimes$ is used for direct product (of multiplicative groups), $\oplus$ is used for direct sum (of additive groups); and for a finite set S, $|S|$ denotes the cardinality of S.

2. A preliminary result

THEOREM 1. *Let R be a ring with 1 and N a nil ideal. If G is the group of units of R then $H = 1+N$ is a normal subgroup of G and G/H is isomorphic to the group of units of R/N. Furthermore, the additive group N^i/N^{i+1} is isomorphic to the multiplicative group $1+N^i/1+N^{i+1}$ (for each integer $i \geqq 1$).*

PROOF. We show first that $1+N$ is contained in G. Let $a \in 1+N$ so that $a = 1+x$ with $x \in N$. Since x is nilpotent, x is regular in the sense of Jacobson. Hence a has an inverse. Thus $1+N \subseteqq G$.

If ν is the natural map from R to $\bar{R} = R/N$, ν maps G homomorphically onto a multiplicative subgroup $\bar{G}$ of $\bar{R}$. Let H be the kernel of the mapping from G to $\bar{G}$. It is clear that $H = 1+N$ so that $H = 1+N$ is a normal subgroup of G and $G/H \simeq \bar{G}$.

We verify next that $\bar{G}$ is the group of (all) units of $\bar{R}$. In fact, let $r+N$ be a unit of $\bar{R}$; then there is an

$$s \in R \ni (r+N)(s+N) = (s+N)(r+N) = 1+N \Rightarrow rs+N = sr+N$$
$$= 1+N \Rightarrow rs,\ sr \in 1+N \Rightarrow rs,\ sr \in G \Rightarrow r \in G.$$

Hence $\bar{G}$ is the group of units of $\bar{R}$.

Since N^i and N^{i+1} ($i \geqq 1$) are nil ideals, $1+N^i$ and $1+N^{i+1}$ are normal subgroups of G and $1+N^{i+1} \lhd 1+N^i$: hence we can form the quotient group $1+N^i/1+N^{i+1}$.

Now consider the mapping η from N^i onto $1+N^i/1+N^{i+1}$ defined by: $x\eta = (1+x)(1+N^{i+1})$ for $x \in N^i$. Let $x, y \in N^i$ and let $z \in N^i$ be such that $(1+x+y)(1+z) = 1$ (z exists since $1+N^i$ is a multiplicative group). Then

$$(1+x)(1+y) = (1+x+y)(1+(1+z)xy)$$

so that:

$$[(1+x)(1+N^{i+1})][(1+y)(1+N^{i+1})] = (1+x+y)(1+N^{i+1})$$

since $1+(1+z)xy \in 1+N^{i+1}$. But this last equation shows that:

$$(x\eta)(y\eta) = (x+y)\eta \text{ for } x, y \in N^i \text{ — i.e. } \eta \text{ is a homomorphism.}$$

Now $K(\eta)$, the kernel of η, $= \{x \in N^i | 1+x \in 1+N^{i+1}\} = N^{i+1}$ Hence $N^i/N^{i+1} \simeq 1+N^i/1+N^{i+1}$ as we claimed.

REMARK. The same method establishes the isomorphism $N^i/N^{2i} \simeq 1+N^i/1+N^{2i}$.

3. Finite primary rings

PROPOSITION 1. *Let R be a finite primary p-ring with prime ideal N. Let G be the group of units of R and $H = 1+N$. Then*

(a) *$H \leqq G$ and $G/H \simeq (R/N)^*$ = the group of non-zero elements of R/N. Furthermore, $G = H \otimes U$, where $U \simeq (R/N)^*$.*

(b) *$N^i/N^{i+1} \simeq 1+N^i/1+N^{i+1}$ for each integer $i \geqq 1$ (the left hand side as an additive group and the right hand side as a multiplicative group).*

(c) *N^i/N^{i+1} is an elementary p-group (under $+$) and*

$$|R/N| \leqq |N^i/N^{i+1}|$$

for each $i \geqq 1$ such that $N^i \neq 0$.

PROOF. (a) The first statement follows from Theorem 1 since $(R/N)^*$ is the group of units of the field R/N. Now R/N is a Galois field with p^l elements and hence $|(R/N)^*| = p^l-1$; on the other hand, $|H| = |N|$ = a power of p. Hence $|G| = |H|(p^l-1)$ and thus $G = H \otimes U$, where $U \simeq G/H \simeq (R/N)^*$.

(b) This follows directly from Theorem 1.

(c) N^i/N^{i+1} is an R-module but since $N(N^i) = N^{i+1}$, it can also be considered as an R/N-module — i.e. as a vector space over the field R/N. But R/N has characteristic p so that $p\ (N^i/N^{i+1}) = 0$ which shows that N^i/N^{i+1} is an elementary p-group — provided $N^i \neq 0$.

Since $N^i \neq 0$ implies N^i/N^{i+1} is a vector space over R/N of dimension $\geqq 1$, it has a basis of t elements, say ($t \geqq 1$). Then $|N^i/N^{i+1}| = tp^l$, where $|R/N| = p^l$. Hence $|R/N| \leqq |N^i/N^{i+1}|$ provided $N^i \neq 0$.

DEFINITION. The finite primary ring R with radical N is *homogeneous of type p* if $\exists$ an integer k such that

$$R/N,\ N/N^2, \ldots, N^k/N^{k+1}$$

all have order p and $N^{k+1} = 0$.

THEOREM 2. *Let R be a finite primary p-ring with prime ideal $N \neq 0$ and let $H = 1+N$. Then*

(a) *if either the additive group N or the multiplicative group H is cyclic, R is homogeneous of type p.*

(b) *For* $p \geqq 3$, *N is cyclic if, and only if H is cyclic.*

(c) *For* $p = 2$:

(i) *If N is cyclic, H is cyclic if, and only if* $N^2 = 0$. *In case* $N^2 \neq 0$, $H = (-1) \otimes H^{(2)}$, *where* $H^{(2)} = 1+N^2$ *is cyclic.*

(ii) *If H is cyclic and N is not cyclic,* $N \simeq$ *Klein 4-group.*

Proof. Let $0 = N^{k+1} < N^k$

(a) Since $N^i/N^{i+1} \simeq 1+N^i/1+N^{i+1}$ by Proposition 1 (b), either of our hypotheses guarantees that N^i/N^{i+1} is cyclic. But by Proposition 1 (c) N^i/N^{i+1} is an elementary p-group for $N^i \neq 0$, and $|R/N| \leqq |N^i/N^{i+1}|$. Hence each of the groups

$$R/N, N/N^2, \ldots, N^k/N^{k+1}$$

has order p. Note that $|N| = p^k$.

We prove next the following assertion: (*) Assume that H is cyclic and that N^{i+1} is cyclic. If $p \geqq 3$ and $i \geqq 1$ or if $p = 2$ and $i \geqq 2$, N^i is cyclic.

Proof of (*). We can assume $i < k$ since we already know that N^i is cyclic for $i \geqq k$. We show that every element of order p in N^i is in N^{i+1}; this will establish that N^i has a unique subgroup of order p — since by assumption N^{i+1} is cyclic. Indeed, let $x \in N^i$ and assume that $px = 0$. Then $(1+x)^p = 1+x^p$ and $x^p \in N^{i+2}$. Since $(1+x)^p \in 1+N^{i+2}$ and since $1+N^i/1+N^{i+2}$ is cyclic and hence has $1+N^{i+1}/1+N^{i+2}$ as its only subgroup of order p, $1+x \in 1+N^{i+1}$. Thus $x \in N^{i+1}$. This proves the validity of (*). In particular, applying induction we have that if $p \geqq 3$ and H is cyclic, N is cyclic (i.e. the "if" part of (b)), and if $p = 2$ and H is cyclic, N^2 is cyclic.

Now assume that H is cyclic and that N is not cyclic. Then $p = 2$, $k \geqq 2$ (since N^k is cyclic); we show that $N^3 = 0$. Assume to the contrary that $N^3 \neq 0$ and let $x \in N$ with $2x = 0$. Then $(1+x)^4 = 1+x^4 \in 1+N^4$. $|1+N^4| = 2^{k-3}$ so that

$$1 = (1+x^4)^{2^{k-3}} = (1+x)^{2^{k-1}}$$

and this implies that $x \in N^2$. Thus N is cyclic. Hence if N is not cyclic, $p = k = 2$ and N is isomorphic to the Klein 4-group. This establishes (c) (ii).

We now prove a statement analogous to (*), viz. (**). Assume that N is cyclic and that $1+N^{i+1}$ is cyclic. If $p \geqq 3$ and $i \geqq 1$ or if $p = 2$ and $i \geqq 2$, $1+N^i$ is cyclic.

PROOF OF (**). We can assume that $i < k$. Let $1+x \in 1+N^i$ and assume $(1+x)^p = 1$. Then

$$1 = (1+x)^p = 1+px+\frac{p(p-1)}{2}x^2+\ldots+x^p = 1+(px)u+x^p,$$

where

$$u = 1+\frac{p-1}{2}x+\ldots \in 1+N \qquad (u=1 \text{ if } p=2).$$

Letting $uv = 1$ (u is a unit) we obtain $px = -x^p v \in N^{ip} \leqq N^{i+2}$ since $x \in N^i$. But N^i/N^{i+2} is cyclic of order p^2 and N^{i+1}/N^{i+2} is its only subgroup of order p. Hence $x \in N^{i+1}$. Therefore $1+x \in 1+N^{i+1}$ and (**) is established. Thus the "only if" part of (b) is proved and we have only (c) (i) left to verify.

So assume that N is cyclic and that $p = 2$. If $N^2 = 0$, $H \simeq N$ and H is cyclic. So assume $N^2 \neq 0$. By (**), $H^{(2)} = 1+N^2$ is cyclic. We show that $-1 \in H \setminus H^{(2)}$. Indeed

$$-1 = 1+(-2) \in 1+N = H$$

but if $-1 \in H^{(2)}$, $2 \in N^2$ and this implies that $2 = 2a$ for some $a \in N$ since $N^2 = 2N$. But then $2(1-a) = 0$ so that $2 = 0$ since $1-a$ is a unit. But this implies that $N^2 = 2N = 0$ — a contradiction. Hence $H = (-1) \otimes H^{(2)}$ and (c) (i) is established.

COROLLARY. *Let R be a finite primary p-ring with prime ideal $N \neq 0$, let G be its group of units and let $H = 1+N$. Then G is cyclic if and only if H is cyclic. Furthermore, G is cyclic if and only if R is isomorphic to one of the following*:

(i) Z_pk+1, where $p \geqq 3$ and $k \geqq 1$.

(ii) Z_r

(iii) $Z_p[x]/(x^2)$

(iv) $Z_2[x]/(x^3)$

(v) $\dfrac{Z[x]}{Id\{4, 2x, x^2-2\}}$.

On the other hand, N is cyclic if and only if either:

(1) $$R \simeq Z_pk+1$$

or

(2) $$R \simeq Z_p[x]/(x^2)$$

Note: We are using the notation: $Z_n = Z/(n)$.

PROOF. Assume that N is cyclic, and suppose that $p = pa$ for some $a \in N$. Then $p(1-a) = 0$ and this implies that $p = 0$ ($1-a \in 1+N$ is a unit). Thus either p is a generator of N or N is of order p.

In the first case, R has characteristic p^{k+1}, where $p^k = |N|$. But $|R| = p^{k+1}$ so that $R \simeq Z_p k+1$. Theorem 2(b) and (c) (i) tells us that H is cyclic if, and only if either $p \geqq 3$ or if $p = 2$ and $k = 1$.

In the second case, R has characteristic p and $N^2 = 0$. Thus $R \simeq Z_p[x]/(x^2)$ and it follows immediately that in this case H is cyclic.

If the characteristic of R is 2, $R = Z_2 + (a) + (a^2)$ and $R \simeq Z_2[x]/(x^3)$. If the characteristic of R is 4 and if $2 \in N \setminus N^2$, we can take $a = 2$ and then $2^2 = 4 = 0$ — a contradiction. Hence $b = 2$. Then $R = Z_4 + (a)$ with $2a = 0$ and $a^2 = 2$ so that $R \simeq Z[x]/Id\{4, 2x, x^2-2\}$.

Finally we verify that for these two rings with 8 elements, H is cyclic. $|H| = 4$ and $(1+a)^2 = 1+a^2 = 1+b \neq 1$ (in both cases). Thus H is not the 4-group so must be cyclic.

If R is an infinite primary ring, its group of units cannot be cyclic. For if $0 = N^{k+1} < N^k$, N^k is a vector space over the field R/N and thus N^k cannot be cyclic. But $N^k \simeq 1+N^k$, a subgroup of the group G of units of R. Hence G cannot be cyclic if $N \neq 0$. If $N = 0$, R is a field and it is easy to see that its non-zero elements do not form an (infinite) cyclic group.

If R is a commutative ring with identity and with descending chain condition, then R is a direct sum of a finite number of primary rings (see [2] Theorem 3 on p. 205). Now if R has a cyclic group of units each of the primary rings has a cyclic group of units — and hence must be finite. Thus we have proved:

PROPOSITION 2. *Let R be a commutative ring with identity which satisfies the descending chain condition. If the group of units of R is cyclic, R is finite.*

REFERENCES

ROBERT W. GILMER, JR.

[1] "Finite rings having a cyclic multiplicative group of units". American Journal of Mathematics, vol. 85 (1963), pp. 447—452.

OSCAR ZARISKI and PIERRE SAMUEL

[2] Commutative Algebra. D. Van Nostrand Company, 1958.

(Oblatum 11–6–68) The Pennsylvania State University