NILPOTENT RINGS AND FINITE PRIMARY RINGS WITH CYCLIC GROUPS OF UNITS

Cora Stack

Abstract. In this paper, we use properties of nilpotent rings to reprove an old theorem of R. Gilmer which classifies finite commutative primary rings having a cyclic group of units.

Introduction

The following properties of primary rings are required for our proof (see [8]). A finite ring R is *primary* if its set of zero divisors forms an additive group, or equivalently, if it is an ideal. If we denote the set of zero divisors of the primary ring R by M, then M is the unique maximal ideal of R and hence is the Jacobson radical of R, and is therefore nilpotent. This implies in particular that $M^i \supset M^{i+1}$ for each non-zero M^i. The quotient field R/M is a finite field called the residue field. Thus R/M is the Galois field $\mathrm{GF}(p^t)$ of p^t elements, where p is a prime and t a positive integer. The quotient spaces M^i/M^{i+1} may be regarded as vector spaces over the residue field R/M via the action defined by

$$(r+M)(m+M^{i+1}) = rm + M^{i+1},$$

for $r \in R$ and $m \in M^i$. Moreover, $|R| = p^{tk}$ for some positive integer k. Finally, in case R is commutative, the group of units is the direct product of the p-subgroup $1+M$ and a cyclic group of order $p^t - 1$, that is, $R^* = (1+M) \times C_{p^t-1}$, where C_s denotes the cyclic group of order s. Thus the group of units of a finite commutative primary ring is cyclic if and only if the p-subgroup $1+M$ is cyclic.

In [4], it is shown that to determine the structure of the group of units of a finite commutative ring, it is sufficient to consider the primary case. In what follows, we show how the properties above can be used to obtain in a straightforward way yet another proof of the main result in [4], namely, the theorem which classifies finite commutative primary rings having cyclic groups of units. We remark that a number of interesting, elementary proofs of this result have been obtained by Ayoub, [1], Pearson and Schneider, [7], Eldridge and Fisher, [3].

The following easily proved result is also needed.

Lemma *Let n and r be positive integers and let p be a prime integer. If p is odd, then p^{n-r+1} divides the binomial coefficient $\binom{p^{n-1}}{r}$ provided that $1 < r \leq n-1$. If $p = 2$, the same result is true if $2 < r \leq n-1$.*

Proof. We use an easily proved property of binomial coefficients, namely, that

$$b\binom{a}{b} = a\binom{a-1}{b-1}.$$

Thus for $r \geq 1$, we have

$$r\binom{p^{n-1}}{r} = p^{n-1}\binom{p^{n-1}-1}{r-1}.$$

It follows that p^{n-r+1} divides $\binom{p^{n-1}}{r}$ unless p^{r-1} divides r. But as $r < p^{r-1}$ if $r > 1$ and p is odd, and $r < 2^{r-1}$ if $r > 2$, the required result is clear. ■

We proceed to the proof of the main result of the paper.

Theorem *Let R be a finite commutative primary ring with identity. R has a cyclic group of units if and only if R is isomorphic to precisely one of the following:*

- $\mathrm{GF}(p^k)$, *where p is a prime;*
- $\mathbb{Z}_{p^k}$, *where $k \geq 2$ and p is an odd prime;*
- $\mathbb{Z}_4$;
- $\mathbb{Z}_p[X]/(X^2)$, *where p is a prime;*
- $\mathbb{Z}_2[X]/(X^3)$;

- $\mathbb{Z}_4[X]/(2X, X^2-2)$.

Proof. It is a routine exercise to check that each of the rings above is primary and has a cyclic group of units, and that no two are isomorphic.

Let us assume that R is a finite commutative primary ring whose set of zero divisors is M, say, and let the characteristic of R be p^l, where p is a prime and $l \geq 1$. We also assume that the group of units R^* is cyclic. This is equivalent to saying that the p-subgroup $1+M$ is cyclic. Since $1+M$ is a multiplicative p-group, we may suppose that

$$1 + M \cong C_{p^n},$$

for some $n \geq 0$. Assume further that the residue field R/M has order p^k for some $k \geq 1$. Now $|M| = |1+M| = p^n$ and so $|R| = p^{k+n}$ and $M^{n+1} = 0$ by the nilpotency of M. If $M = 0$, then $R \cong \mathrm{GF}(p^k)$, which is the first case above.

Suppose next that $M \neq 0$. We consider the different possibilities for the integer n. This will force certain restrictions on the characteristic p^l and hence on l. Consider first the case that $n = 1$. Then $M^2 = 0$. Since in this case $M = M/M^2$ is a vector space over the residue field, we must have

$$p^r \leq |M| = p.$$

Thus $r = 1$, and hence $|R/M| = p$ and $|R| = p^2$. Since R has characteristic p^l, $M \supseteq p\mathbb{Z}_{p^l}$ and so $p = |M| \geq p\mathbb{Z}_{p^l} = p^{l-1}$. It follows that $l \leq 2$ and thus the characteristic of R must be p or p^2. If the characteristic is p^2, then clearly $R \cong \mathbb{Z}_{p^2}$. If the characteristic of R is p, choose $x \in M$, $x \neq 0$. Then $x^2 \in M^2 = 0$. The set $\{1, x\}$ is evidently linearly independent over $\mathbb{Z}_p$ and therefore forms a basis of R, as $|R| = p^2$. Thus we have $R \cong \mathbb{Z}_p[X]/(X^2)$ in this case.

Suppose now that $n \geq 2$. In this case $|M| \geq p^2$. We claim that if $l = 1$, there exists an element $x \in M$ with $x^{p^{n-1}} \neq 0$. For suppose that $z^{p^{n-1}} = 0$ for all $z \in M$. Then the binomial theorem implies that

$$(1+z)^{p^{n-1}} = 1 + z^{p^{n-1}} = 1,$$

and this contradicts the fact that the multiplicative group $1+M$ is cyclic of order p^n. Thus our claim is established. As M is nilpotent, the powers x, x^2, $\ldots$, $x^{p^{n-1}}$ are linearly independent over $\mathbb{Z}_p$. It follows that

$$p^n = |M| \geq p^{p^{n-1}}$$

and therefore $n \geq p^{n-1}$. We deduce that $n = p = 2$. In particular, $M^3 = 0$ and $|R| = 8$. Now $x^2 \neq 0$ and $x^3 = 0$. The linear independence of 1, x and x^2 over $\mathbb{Z}_2$ now implies that $R \cong \mathbb{Z}_2[X]/(X^3)$.

Suppose next that $l \geq 2$. For convenience we will first consider the case that p is an odd prime. Since $p1 \in M$, we have $p^i 1 \in M^i$ for each positive integer i. Now if $x \in M$,

$$(1+x)^{p^{n-1}} = 1 + p^{n-1}x + \binom{p^{n-1}}{2}x^2 + \cdots + x^{p^{n-1}}.$$

Now the Lemma implies that

$$\binom{p^{n-1}}{r}x^r \in M^{n+1} = 0$$

for $2 \leq r \leq n-1$. Since p divides $\binom{p^{n-1}}{n}$, we also have

$$\binom{p^{n-1}}{n}x^n \in M^{n+1} = 0$$

and thus

$$(1+x)^{p^{n-1}} = 1 + p^{n-1}x.$$

Hence $l \geq n$, since otherwise $p^{n-1}1 = 0$ and then the exponent of $1+M$ is less than p^n, contrary to assumption.

Consider now the principal ideal pR generated by p and suppose that $M \neq pR$. Consider the additive group homomorphism $f : R \to R$ given by $f(x) = p^{n-1}x$. If $M \neq pR$, then $|pR| \leq p^{n-1}$ and so $|p^{n-1}R| \leq p$ since $p^iR \supset p^{i+1}R$ by the nilpotency of M. Thus

$$|R/\ker f| = |p^{n-1}R| \leq p$$

and it follows that $|\ker f| \geq p^{n+r-1} \geq p^n$ since $r \geq 1$. But now as $\ker f \leq M$, we deduce that $\ker f = M$ and hence $p^{n-1}x = 0$ for all $x \in M$, a contradiction to our earlier work. It follows therefore that $M = pR$. Since M^i/M^{i+1} is at most one-dimensional over R/M (it is generated by $p^i + M^{i+1}$) and since $M^{l-1} \neq 0$ and $M^l = p^l R = 0$, we have

$$|R| = p^{rl} = p^{n+r}.$$

Since $l \geq n$ and $M^{n+1} = 0$, either $l = n$ or $l = n+1$. If $l = n$, then $nr = n + r$ and so $n = r = 2$. But then $|M| = p^2$ and so $M^2 = 0$. This would again force the exponent of $1 + M$ to be less than p^2, contrary to assumption. Hence $l = n+1$. This implies that $(n+1)r = n+r$ and therefore $r = 1$. Now we obtain $|R| = p^{n+1}$ and $R \cong \mathbb{Z}_{p^{n+1}}$.

Finally we consider the case that $l \geq 2$ (and hence $n \geq 2$) and $p = 2$. It follows from the Lemma that for $x \in M$,

$$(1+x)^{2^{n-1}} = 1 + 2^{n-1}x + \alpha 2^{n-2}x^2,$$

where α is an odd integer. Thus $l \geq n-1$, since otherwise we obtain a contradiction. As in the previous paragraph, we consider the two cases $M = 2R$ and $M \neq 2R$. Now if $M = 2R$, an identical argument to that used in the previous paragraph shows that $R \cong \mathbb{Z}_{2^{n+1}}$. But the group of units of $\mathbb{Z}_{2^{n+1}}$ is cyclic only if $n+1 \leq 2$. Thus $n = 1$, which is contrary to our hypothesis. Thus $M \neq 2R$.

We now examine the situation when $M \neq 2R$. Suppose that $n \geq 3$. Again by the nilpotency of M,

$$M \supset 2R \supset 2M \supset 2^2M \supset \ldots$$

and so $|2^iM| \leq 2^{n-i-1}$. Thus $2^{n-1}M = 0$ if $n \geq 2$. Similarly, $2^{n-2}M^2 = 0$ for $n \geq 3$. Thus for $n \geq 3$ and for every $x \in M$, we see from the expansion above that $(1+x)^{2^{n-1}} = 0$, a contradiction. It follows therefore that $n = 2$. Since $l = n-1$ or n, we must have $l = 2$. It follows then that $2M = 0$, $|M^2| = 2$, $M \supset 2R \supset 0$, and $|M| = 4$. Hence $r = 1$. Moreover, $x \neq 0$ for some $x \in M$. Now M/M^2 is a one-dimensional vector space over $\mathbb{Z}_2$ with basis vector $x + M^2$ and $M^3 = 0$. If $2 \in M \setminus M^2$, then $2 \equiv x \bmod M^2$ and so $x^2 = 0$, which is not true. Hence $2 \in M^2$ and so $x^2 = 2$. Hence $2x = 0$ and $x^2 - 2 = 0$. It now follows that

$$R \cong \mathbb{Z}_4[X]/(2X, X^2 - 2).$$

Since we have considered all cases, the theorem is proved. ∎

References

[1] C. Ayoub, *On finite primary rings and their group of units*, Compositio Mathematicae **21** (1969), 247-252.

[2] B. R. McDonald, Finite Rings with Identity. Marcel Dekker: New York, 1974.

[3] K. E. Eldridge and I. Fisher, *DCC rings with a cyclic group of units*, Duke Math. J. **34** (1967), 243-248.

[4] R. W. Gilmer (jnr),*Finite rings having a cyclic multiplicative group of units*, Amer. J. of Math. **85** (1963), 447-452.

[5] I. Kaplansky, Fields and Rings. Chicago Lectures in Mathematics. University of Chicago Press: Chicago and London, 1969.

[6] N. H. McCoy, The Theory of Rings. Macmillan: New York, 1966.

[7] K. R. Pearson and J. E. Schneider, *Rings with a cyclic group of units*, J. Algebra **16** (1970), 243-251.

[8] R. Raghavendran, *Finite associative rings*, Compositio Mathematicae **21** (1969), 195-229.

Cora Stack
Institute of Technology
Tallaght
Dublin
Ireland