UNITS IN CYCLIC MODULES OVER POLYNOMIAL RINGS

Arunas Liulevicius [1]

In this note we determine the structure of the group of units in the ring $F[x]/(x^{n+1})$ where $F = F_p = Z/(p)$ is the field of p elements with p a prime. The general case of F a finite field and the structure of the group of units in $F[x]/(a)$ will be treated elsewhere. The special case treated here is of pedagogical interest, since it exhibits quite nicely the way one applies the structure theorem on finite abelian groups. Indeed, one would like to suggest that after treating the structure of the group of units in $Z/(p^r)$ (with the odd behavior at p=2) one should go on in the introductory algebra course to treat the group of units in $F[x]/(x^{n+1})$, since this has several satisfactory features - the structure is sufficiently complicated so that it is not apparent at first glance, yet it is pleasantly periodic; secondly, the analysis of structure is easy and uses the Frobenius map as the key idea.

Notice that if $m \leq n$ then the inclusion $(x^{n+1}) \subset (x^{m+1})$ yields a homomorphism of rings $F[x]/(x^{n+1}) \longrightarrow F[x]/(x^{m+1})$ which is onto when we look at groups of units. If we denote by U(R) the group of units in the ring R, we define

$$K_n = \text{Kernel } U(F[x]/(x^{n+1})) \longrightarrow U(F)=U(F[x]/(x)) .$$

Since $F = F_p$, $U(F)$ is a cyclic group of order p-1, K_n is an abelian group of order p^n (since the elements of K_n are given by the cosets of $1 + a_1x + \ldots + a_nx^n \bmod (x^{n+1})$ with a_i in F). This means that $U(F[x]/(x^{n+1}))$ is the product of U(F) with K_n, so it only remains to exhibit the structure of K_n.

THEOREM. Let #(k) be the number of summands in the decomposition of K_n into a sum of cyclic groups which are isomorphic to $Z/(p^k)$. Then

$$\#(k) = [n/p^{k-1}] - 2[n/p^k] + [n/p^{k+1}] ,$$

where $[x]$ denotes the greatest natural number less than or equal to the positive real number x .

YPI/SFB 83-10

1) Partially supported by NSF grant MCS 80-02730 and by SFB 40 at Universität Bonn.

For example, if p=2, the structure of $K_n = U(F x /(x^{n+1}))$ is given as follows. Here the symbol $[e_1, \ldots, e_m]$ denotes the group $Z/(2^{e}1) \times \ldots \times Z/(2^{e}m)$:

$K_1 = [1]$
$K_2 = [2]$
$K_3 = [2,1]$
$K_4 = [3,1]$
$K_5 = [3,1,1]$
$K_6 = [3,2,1]$
$K_7 = [3,2,1,1]$
$K_8 = [4,2,1,1]$
$K_9 = [4,2,1,1,1]$
$K_{10} = [4,2,2,1,1]$
$K_{11} = [4,2,2,1,1,1]$
$K_{12} = [4,3,2,1,1,1]$

The periodicity of structure becomes evident if we write the n and #(k) in binary notation:

p=2

n	#(1)	#(2)	#(3)	#(4)
0	0	0	0	0
1	1	0	0	0
10	0	1	0	0
11	1	1	0	0
100	1	0	1	0
101	10	0	1	0
110	1	1	1	0
111	10	1	1	0
1000	10	1	0	1
1001	11	1	0	1
1010	10	10	0	1
1011	11	10	0	1
1100	11	1	1	1
1101	100	1	1	1
1110	11	10	1	1
1111	100	10	1	1

Just as in the case of $U(\mathbb{Z}/(p^n))$ the prime $p=2$ behaves oddly: here the periodicity blocks come in multiples of 4, but for the remaining primes the periodicity blocks come in multiples of p.

Let A be a finite abelian group (written additively) of order a power of a prime p. Suppose A is isomorphic to

$$\mathbb{Z}/(p^{e_1}) \times \ldots \times \mathbb{Z}/(p^{e_k})$$

and for each natural number n let w(n) be the number of e_i with $n \leq e_i$. Thus for example w(1) is the number of cyclic summands, or in other words

$$p^{w(1)} = |A/A.p| ,$$

where $|B|$ denotes the order of the finite group B. More generally,

$$p^{w(k)} = |A.p^{k-1}/A.p^k| .$$

If we let $p^{d_k} = |A.p^k|$, this means that $w(k) = d_{k-1} - d_k$. Finally, if we let $\#(k)$ be the number of e_i equal to k, then of course we have

$$\#(k) = w(k)-w(k+1) = d_{k-1} - 2d_k + d_{k+1} .$$

The moral of this is that we should determine the d_k in our case of $A = K_n$. Indeed, as we have just seen, the theorem will be completely proved if we can show that $d_k = [n/p^k]$, the greatest integer in n/p^k.

Since the group K_n is written multiplicatively, $.p : A \longrightarrow A$ is now the Frobenius map $\varphi : K_n \longrightarrow K_n$, $\varphi(u) = u^p$. Notice that φ is induced by the Frobenius map $\varphi : F_p[x] \longrightarrow F_p[x]$ which is a homomorphism of rings and is the identity on F_p - said in another way, φ is an F_p-linear homomorphism. Let $V_n \subset F_p[x]/(x^{n+1})$ be the subspace consisting of elements having representatives of the form $a_1x + \ldots + a_nx^n$ with a_i in F_p. Notice that φ maps V_n into itself. We have a one-to-one correspondence

$$f : V_n \longrightarrow K_n$$

defined by $f(v) = 1 + v$. Notice that f is not in general a homomorphism, since $(1+u)(1+v) = 1+u+v+uv$. However (and this is a pleasant surprise indeed!) f commutes with the Frobenius homomorphism, since $\varphi(1+v) = (1+v)^p = 1 + v^p = 1 + \varphi(v)$. We are interested in determining the image of φ^k in K_n, but under f this corresponds to the image of φ^k in V_n. Here however φ is an F_p-linear map, and the basis vectors

$x, \ldots, x^n \bmod (x^{n+1})$ are mapped by φ either to basis vectors or to zero. We now just count the number of x^j with $1 \leq j \leq n$ such that $\varphi^k(x^j) = x^{jp^k}$ is non-zero in $F_p[x]/(x^{n+1})$ - the condition $jp^k \leq n$ is of course equivalent to $j \leq [n/p^k]$, so we have

$$|\varphi^k(K_n)| = |\varphi^k(V_n)| = p^{[n/p^k]},$$

hence $d_k = [n/p^k]$, and the theorem is proved.

Notice that the number of cyclic summands in K_n is $w(1) = d_0 - d_1 = n - [n/p]$, so it grows quite fast. The task of finding generators for the cyclic decomposition of K_n is non-trivial. This example should convince the student that in general it is much easier to determine the abstract structure of a finite abelian group A than to exhibit an explicit isomorphism to a product of cyclic groups.

June 1983

Department of Mathematics
The University of Chicago
5734 University Avenue
Chicago, IL 60637 U S A

Max Planck Institut für Mathematik
Gottfried Claren Straße 26
5300 Bonn 3
Federal Republic of Germany