Revista Colombiana de Matemáticas
Volumen VII (1973), págs. 93 - 98

A REMARK ON PRIMITIVE ROOTS AND RAMIFICATION

by

Víctor S. ***ALBIS GONZÁLEZ***

In memoriam L. I. Soriano

SUMMARY

The problem on primitive roots modulo the powers of a prime ideal in a ring of algebraic integers is solved, and a connection with ramification is remarked.

1. Introduction. The theory of primitive roots modulo the powers of a rational prime number is a well known fact. It consists essentially of the determination of the rings $\mathbb{Z}/p^m\mathbb{Z}$, p a prime, n an integer ≥ 1, which admit cyclic groups of units; a generator (when it exists) of the group $(\mathbb{Z}/p^m\mathbb{Z})^\times$ of units of $\mathbb{Z}/p^m\mathbb{Z}$ is then called *a primitive root of* $\mathbb{Z}$ *modulo* p^m. In his "Zahlbericht" [4: p.83], Hilbert asks about the corresponding problem for the rings of algebraic integers. Here we give an answer to this last problem and see how it can be related to some properties on ramification. Our task is simplified by the results of R. W. Gilmer about finite rings whose groups of units are cyclic. These results are contained in the following

THEOREM (GILMER ; [2]). Let A be a finite primary ring whose group of *units is cyclic. Then A is isomorphic to one element and only one of the following classes :*

(a) $\mathbb{F}_q$, *a Galois field with $q = p^k$ elements, where p is a prime number .*

(b) $\mathbb{F}_p[X]/(X^2)$, *where p is prime.*

(c) $\mathbb{F}_2[X]/(X^3)$.

(d) $\mathbb{Z}/p^k\mathbb{Z}$, *where p is an odd prime and $k > 1$.*

(e) $\mathbb{Z}/4\mathbb{Z}$.

(f) $\mathbb{Z}[X]/(4, 2X, X^2-2)$.

Moreover, the rings in (b) have p^2 elements, and those is (c) and (f), 2^3 .

We proceed now to introduce some notation and facts from algebraic number theory. For this we follow [3] . If K is a field of algebraic numbers, we denote by $\mathcal{O}$ its ring of integers and by small case german letters its ideals. Let $\mathfrak{p}$ be a maximal prime ideal of $\mathcal{O}$ and p be the unique rational prime satisfying $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. We know then (*opus cit.*) that $p\mathcal{O} = \mathfrak{p}^e\mathfrak{a}$, $\mathfrak{p} \nmid \mathfrak{a}$, where $e = e(\mathfrak{p} \mid p)$ is the so called ramification index of $\mathfrak{p}$ over $\mathbb{Z}$. Also the number of elements of $\mathcal{O}/\mathfrak{p}$ is called the norm $N(\mathfrak{p})$ of $\mathfrak{p}$ and we have $N(\mathfrak{p}) = p^f$, where $f = f(\mathfrak{p} \mid p) = [\mathcal{O}/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$ is the residual degree of $\mathfrak{p}$ over $\mathbb{Z}$. More generally, if $\mathfrak{a}$ is any ideal of $\mathcal{O}$, then $\mathcal{O}/\mathfrak{a}$ is a finite ring whose cardinality is the norm $N(\mathfrak{a})$ of $\mathfrak{a}$; further, since $N(\mathfrak{a})\,N(\mathfrak{b})$ when $\mathfrak{a}$ and b are ideals of $\mathcal{O}$, we have $N(\mathfrak{p}^n) = p^{nf}$. Finally, we shall denote by $|A|$ the cardinality of a set A .

The problem now becomes : *Given a field K of algebraic numbers, to determine all prime ideals $\mathfrak{p}$ in the ring of integers $\mathcal{O}$ of K, and all the values $n = 1, 2, \ldots$, for which the group of units $(\mathcal{O}/\mathfrak{p}^n)^\times$ of $\mathcal{O}/\mathfrak{p}^n$ is cyclic.*

Since each $\mathcal{O}/\mathfrak{p}^n$ is a finite primary ring we observe that by comparison with

Gilmer's list we are able to do such determination. Also, the classical list ((a),(d) and (e)) is not substantially increased ; thus, in a sense, a theory of primitive roots modulo $\mathfrak{p}^n$ is superfluous.

2. *The results.* We shall express our results in terms of the invariants $e(\mathfrak{p} \mid p)$ and $f(\mathfrak{p} \mid p)$ of the ideal $\mathfrak{p}$. Also the following two properties of the rings $O/\mathfrak{p}^n$ will facilitate our comparison.

PROPOSITION 1. *Let K be a field of algebraic numbers, O its ring of integers and $\mathfrak{p}$ one of its prime ideals with ramification index $e = e(\mathfrak{p} \mid p)$. Then $O/\mathfrak{p}^n$ has characteristic p^m, $m > 1$, when, and only when, $n > e$.*

Proof: Let us suppose that $n > e$ and that $O/\mathfrak{p}^n$ has characteristic p, so that $p \in \mathfrak{p}^n$. Then $pO = \mathfrak{p}^e \mathfrak{a} \subseteq \mathfrak{p}^n$, where $\mathfrak{p} \nmid \mathfrak{a}$, thus $\mathfrak{p}^e \subseteq \mathfrak{p}^n$, i. e., $e \leq n$, which contradicts the choice of n. Conversely, if $n \leq e$, it suffices to show that $O/\mathfrak{p}^n$ has characteristic p, because, *a fortiori*, $O/\mathfrak{p}^n$ has the same characteristic if $1 \leq n \leq e$. From $pO \subseteq \mathfrak{p}^e$ we get that $pO \cap \mathbb{Z} = p\mathbb{Z} \subseteq \mathfrak{p}^e \cap \mathbb{Z} \subseteq \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, that is, $\mathfrak{p}^e \cap \mathbb{Z} = p\mathbb{Z}$. The proposition then follows remarking that the characteristic of $O/\mathfrak{p}^n$ is p^m where $p^m \mathbb{Z} = \mathfrak{p}^n \cap \mathbb{Z}$.

PROPOSITION 2. *Let K be a field of algebraic numbers, O its ring of integers and $\mathfrak{p}$ one of its prime ideals. Then $(O/\mathfrak{p}^n)^{\times}$ is isomorphic to $(1 + \mathfrak{p}/\mathfrak{p}^n) \times (O/\mathfrak{p})^{\times}$ and its order is*

$$|(O/\mathfrak{p}^n)^{\times}| = p^{f(n-1)}(p^f - 1) \;,$$

where $f = f(\mathfrak{p} \mid p)$. Further, $(O/\mathfrak{p}^n)^{\times}$ is cyclic when, and only when, $1 + \mathfrak{p}/\mathfrak{p}^n$ is cyclic.

Proof. Using the exact sequence

$$1 \to 1+\mathfrak{p}/\mathfrak{p}^n \to (\mathcal{O}/\mathfrak{p}^n)^{\times} \to (\mathcal{O}/\mathfrak{p})^{\times} \to 1$$

the proposition follows easily.

We start our comparison stating the following result.

PROPOSITION 3. Let $\mathcal{O}$ *and* $\mathfrak{p}$ *as in proposition 2. If* $f = f(\mathfrak{p}\,|\,p) > 1$ *, then* $(\mathcal{O}/\mathfrak{p}^n)^{\times}$ *is cyclic when, and only when,* $n = 1$ *.*

Proof: We could prove this proposition by brute force comparison with Gilmer's list, using also proposition 2. However , since $1+\mathfrak{p}/\mathfrak{p}^2 \approx \mathfrak{p}/\mathfrak{p}^2 \approx \mathcal{O}/\mathfrak{p} = (p,\dots,p)$, where the p's appear f times, we get a shorter proof.

Recalling now that $\mathfrak{p}$ is said to *ramify totally* over $\mathbb{Z}$ if $f(\mathfrak{p}|\,p) = 1$ and $e(\mathfrak{p}\,|\,p) > 1$, we obtain from proposition 3 the following

THEOREM 1. $(\mathcal{O}/\mathfrak{p}^n)^{\times}$ *is cyclic for some* $n>1$ *if, and only if,* $f(\mathfrak{p}\,|p) = 1$ *. In particular, if* $\mathfrak{p}$ *ramifies over* $\mathbb{Z}$ *, then* $(\mathcal{O}/\mathfrak{p}^n)^{\times}$ *is cyclic for some* $n>1$ *if, and only if, it does it totally.*

Let us suppose then that $f(\mathfrak{p}|\,p) = 1$. If $e(\mathfrak{p}|\,p) = 1$, it is easy to see that $\mathcal{O}/\mathfrak{p}^n = \mathbb{Z}/p^n\mathbb{Z}$, so we are in the classical case. If $e = e(\mathfrak{p}\,|\,p) > 1$ we see that $(\mathcal{O}/\mathfrak{p}^2)^{\times}$ is cyclic by virtue of theorem 1. If $p \neq 2$, that is the only possibility(this is the moment to take a glance at Gilmer's list). If $p = 2$, we claim that always $(\mathcal{O}/\mathfrak{p}^3)^{\times}$ is cyclic, thus completing the whole picture. Indeed, by proposition 2, it suffices to show that $1+\mathfrak{p}/\mathfrak{p}^3$ is cyclic. Since this group has four elements, it suffices to exhibit an element of order four. Let $\pi \in \mathfrak{p}-\mathfrak{p}^2$ and consider $1+\pi \in 1+\mathfrak{p}$; then

$$(1+\pi)^2 = 1 + 2\pi + \pi^2 = 1 \quad (\mathit{mod}\ \mathfrak{p}^3)$$

implies that

$$2\pi + \pi^2 \equiv 0 \quad (\mathit{mod}\ \mathfrak{p}^3) \ ;$$

if $\mathcal{O}/\mathfrak{p}^3$ has characteristic 2, then $\pi^2 \equiv 0 \ (\mathit{mod}\ \mathfrak{p}^3)$, i. e., $\mathcal{O}\pi^2 = \mathfrak{p}^2 \mathfrak{a} \subseteq \mathfrak{p}^3$, where $\mathfrak{p} \nmid \mathfrak{a}$; but this is a contradiction. If $\mathcal{O}/\mathfrak{p}^3$ has characteristic 4, and since $\mathcal{O}2\pi = \mathfrak{p}^{e+1}\mathfrak{b}$, $\mathfrak{p} \nmid \mathfrak{b}$, and $e \geq 2$, by proposition 1, we get $\mathcal{O}2\pi \subseteq \mathfrak{p}^3$; so that again $\pi^2 \equiv 0 \ (\mathit{mod}\ \mathfrak{p}^3)$, contradicting as before the choice of π . In fact we have proved our next theorem,

THEOREM 2. Let K be field of algebraic numbers, $\mathcal{O}$ *its ring of integers and* $\mathfrak{p}$ *one if its prime ideals. Then :*

i) If $f(\mathfrak{p} \mid p) > 1$, $(\mathcal{O}/\mathfrak{p}^n)^\times$ *is cyclic when* $n = 1$.

ii) If $f(\mathfrak{p} \mid p) = e(\mathfrak{p} \mid p) = 1$, *then* $\mathcal{O}/\mathfrak{p}^n \approx \mathbb{Z}/p^n\mathbb{Z}$ *and* $(\mathcal{O}/\mathfrak{p}^n)^\times$ *is cyclic for all* n *if* $p \neq 2$, *and for* $n = 1, 2$ *if* $p = 2$.

iii) If $f(\mathfrak{p} \mid p) = 1$ *and* $e(\mathfrak{p} \mid p) > 1$ *(i.e., if* $\mathfrak{p}$ *ramifies totally), then* $(\mathcal{O}/\mathfrak{p}^n)^\times$ *is cyclic if, and only if,* $n = 1, 2$ *and* $p \neq 2$ *or* $n = 1, 2, 3$ *and* $p = 2$. *Moreover, in the last case,* $\mathcal{O}/\mathfrak{p}^3 \approx \mathbb{Z}[X]/(4, 2X, X^2 - 2)$ *if* $e(\mathfrak{p}/2) = 2$, *and* $\mathcal{O}/\mathfrak{p}^3 \approx \mathbb{F}_2[X]/(X^3)$ *if* $e(\mathfrak{p} \mid 2) \geq 3$.

We conclude thus that the existence of primitive roots in $\mathcal{O}$ modulo $\mathfrak{p}^n$, $n > 1$, amounts to the determination of the primes $\mathfrak{p}$ satisfying $f(\mathfrak{p} \mid p) = 1$. But, in general, this can not be done *explicitly* ; however if the extension $K/\mathbb{Q}$ is abelian, the decomposition theorem of class field theory gives us all the primes in the case ii) of the theorem above. On the other hand, the case iii), in thre same theorem, supplements the decomposition theorem since the primes of this case are the totally ramified ones. The natural question is now the following :

Is it possible to characterize the way a prime $p \in \mathbb{Z}$ *decomposes in* $\mathcal{O}$ *in terms of simple properties of the groups* $(\mathcal{O}/\mathfrak{p}^n)^\times$, $\mathfrak{p} \mid p$ *, when* $K/\mathbb{Q}$ *is not necessarily abelian ?*

It seems this is always possible if $K/\mathbb{Q}$ is Galois using the results in [1] . If $K/\mathbb{Q}$ is not Galois the situation is somewhat different.

BIBLIOGRAPHY

1. C. AYOUB, *On the group of units of certain rings (to appear).*
2. R. W. GILMER, *Finite rings having a cyclic group of units,* Amer. J. Math., 85 (1963), 447-452.
3. L. J. GOLDSTEIN, *Analytic number theory,* Prentice-Hall, Inc., Englewoods Cliffs, 1971.
4. D. HILBERT , *Gesammelte Abhandlungen,Band I,* Springer-Verlag, Berlin,1970.
5. I. M. VINOGRÁDOV , *Fundamentos de la teoría de los números,* Mir, Moscú , 1970.

Departamento de Matemáticas y Estadística
Universidad Nacional de Colombia
Bogotá, Colombia, S. A..

(Recibido en mayo de 1973).