Author: Dimitrios Poulakis

Title: On the homomorphisms of a family of finite rings

Creator: HDML

BULLETIN THE
GREEK MATHEMATICAL SOCIETY
VOLUME 30, 1989

ON THE HOMOMOPRHISMS OF A FAMILY OF FINITE RINGS

BY

DIMITRIOS POULAKIS

Abstract. In this note we determine the number of ring -homomorphisms from $Z_n[\zeta]$ to $Z_m[\zeta]$, where ζ is a primitive root of unity, using arithmetical properties of the ring $Z[\zeta]$.

1. Introduction

In [2] it was determined the number of ring-homomorphisms from Z_m into Z_n and in [3] the number of ring-homomorphisms from $Z_m[i]$ into $Z_n[i]$ and from $Z_m[\rho]$ into $Z_n[\rho]$, where $\rho^2+\rho+1=0$. In this note we determine the number of ring-homomorphisms from $Z_n[\zeta]$ into $Z_m[\zeta]$, where ζ is a primitive root of 1. More precisely, we prove the following result:

Theorem. Let ζ be a α-th primitive root of 1, $\alpha = p^{\alpha_1}\dots p^{\alpha_\kappa}$ the prime power decomposition of α and f_i the common residue class degree of prime ideals of $Z[\zeta]$ that divide p_i. Suppose that

$$p_i \nmid n \text{ or } p_i \mid (n/\text{g.c.d}(m,n)) \qquad i=1,2,\dots,r$$

$$p_i \mid n,\ p_i \nmid n \text{ and } p_i \nmid (n/\text{g.c.d}(m,n)) \qquad i=r+1,\dots,s$$

$$p^{\varepsilon_i} \mid n,\ p^{\varepsilon_i+1} \nmid n \text{ and } p_i \nmid (n/\text{g.c.d}(m,n)) \qquad i=s+1,\dots,t,\ 2\leqslant \varepsilon_i \leqslant \alpha_i$$

$$p^{\alpha_i+1} \mid n \text{ and } p_i \nmid (n/\text{g.c.d}(m,n)) \qquad i=t+1,\dots,\kappa.$$

Then the number of ring-homomorphisms from $Z_m[\zeta]$ into $Z_n[\zeta]$ is

$$(1+\phi(\alpha))^{\omega(n)\cdot\sum_{i=r+1}^{\kappa}\omega(p_i)\cdot\omega(n/\text{g.c.d}(m,n))}\times$$

$$\times\prod_{i=r+1}^{s}[1+\phi(\alpha/p_i^{\alpha_i})p_i^{f_i(\phi(p_i^{\alpha_i})-1)}]^{\omega(p_i)}\times$$

$$\times \prod_{i=s+1}^{t} [1+\phi(a/p_i^{\alpha_i})p_i^{\varepsilon_i\cdot 1+f_i p_i^{\varepsilon_i\cdot 1}(\varepsilon_i\phi(p_i^{\alpha_i-\varepsilon_i+1})-1)}]^{\omega(p_i)} \times$$

$$\theta \times \prod_{i=t+1}^{k} [1+\phi(a/p_i^{\alpha_i})p^{\alpha_i+f_i p_i^{\alpha_i\cdot 1}(\alpha_i(p_i-1)-1)}]^{\omega(p_i)}$$

where ϕ is the Euler's function and $\omega(\beta)$ denotes the number of prime ideals of $Z[\zeta]$ that divide the ideal $<\beta>$.

The homomorphisms $f: Z_m[\zeta] \to Z_n[\zeta]$ we consider have not, in general, the property $f(1)=1$.

Therefore for the determination of the number of elements of $\mathrm{Hom}_{\mathrm{Ring}}(Z_m[\zeta], Z_n[\zeta])$ it is sufficient to know the decomposition of the ideal $<n>$ in product of prime ideals of $Z[\zeta]$. But we can easily have this decomposition using a well-known result of Dedekind [4, prop. 25, page 27].

2. Examples

a) Let ζ be a 12-th primitive root of 1 and $m=245=5\cdot 7^2$, $n=45=3^2\cdot 5$. The 12-th cyclotomic polynomial is $\Phi_{12}(X)=X^4-X^2+1$. The decomposition of ideals $<3>$ and $<5>$ in product of prime ideals in $Z[\zeta]$ is:

$$<3>=P^2 \quad \text{where} \quad P=<3>+<\zeta^2+1> \quad \text{and}$$

$$<5>=P_1P_2 \quad \text{where} \quad P_1=<5>+<\zeta^2-2\zeta-1> \quad \text{and}$$

$$P_2=<5>+<\zeta^2+2\zeta-1>.$$

Then we get from the theorem that $\mathrm{Hom}_{\mathrm{Ring}}(Z_{245}[\zeta], Z_{45}[\zeta])$ has 25 elements.

b) Let ζ be a 125-th primitive root of 1 and $m=600=2^3\cdot 3\cdot 5^2$, $n=45=3^2\cdot 5$. The 125-th cyclotomic polynomial is $F_{125}(X)=X^{100}+X^{75}+X^{50}+X^{25}+1$. The ideal $<3>$ is prime in $Z[\zeta]$ and $<5>=<\zeta-1>^{100}$. Then we get that $\mathrm{Hom}_{\mathrm{Ring}}[(Z_{600}[\zeta], Z_{45}[\zeta])$ has $1+5^{99}$ elements.

3. Proof of the theorem

First we shall determine the number of ring-homomorphisms from $Z[\zeta]$ into $Z[\zeta]/<n>$. A homomorphism is completely determined by its action on 1 and ζ. We put $f(1)=\bar{a}$ and $f(\zeta)=\bar{b}$, where $\bar{a}, \bar{b} \in Z[\zeta]$ and a, b are the images of a, b in $Z[\zeta]/_{<n>}$. Let

$$F(X)=\prod_{\substack{\nu=1\\(\nu,\alpha)=1}}^{\alpha}(X-\zeta^{\nu})=X^{\phi(\alpha)}+c_1X^{\phi(\alpha)-1}+\cdots+c_{\phi(\alpha)}$$

be the α-th cyclotomic polynomial. Since $1\cdot 1=1$, $1\cdot\zeta=\zeta$ and $F(\zeta)=0$, we have $\bar{a}^2=\bar{a}$, $\bar{a}\,\bar{b}=\bar{b}$ and $\bar{b}^{\phi(\alpha)}+c_1\bar{a}\,\bar{b}^{\phi(\alpha)-1}+\cdots+c_{\phi(\alpha)}\bar{a}=\bar{0}$.

Let $<n>=P^{n_1}\ldots P^{n_\lambda}$ be the decomposition of ideal $<n>$ in prime ideals of $Z[\zeta]$. Then we have a canonical isomorphism:

$$(\star)\qquad \Phi: Z[\zeta]/_{<n>}\cong Z[\zeta]/_{P_1^{n_1}}\oplus\ldots\oplus Z[\zeta]/_{P_\lambda^{n_\lambda}}.$$

If $F(\bar{a})=(\bar{a}_1,\ldots,\bar{a}_\lambda)$ and $F(\bar{b})=(\bar{b}_1,\ldots,\bar{b}_\lambda)$, we have $\bar{a}_j^2=\bar{a}_j$ and it follows that $a_j\in P^{n_j}$ or $a_j-1\in P^{n_j}$. Hence we have $\bar{a}_j=\bar{0}$ or $\bar{a}_j=\bar{1}$. If $\bar{a}_j=\bar{0}$, then $\bar{b}_j=\bar{a}_j\bar{b}_j=\bar{0}$. If $\bar{a}_j=\bar{1}$, then $\bar{b}_j^{\phi(\alpha)}+c_1\bar{b}_j^{\phi(\alpha)-1}+\cdots+c_{\phi(\alpha)}\bar{1}=\bar{0}$, so

$$P_j^{n_j}\mid\prod_{\substack{\nu=1\\(\nu,\alpha)=1}}^{\alpha}<b_j-\zeta^{\nu}>.$$

Let P be a prime ideal such that $P\mid<b_j-\zeta^{\mu}>$ and $P\mid<b_j-\zeta^{\nu}>$, where $(\mu,\alpha)=1=(\nu,\alpha)$, $\mu>\nu$. We deduce that $P\mid<\zeta^{\mu-\nu}-1>$.

If $\beta\in N$ and two at least of $p_i^{\alpha_i}$ do not divide β, then the algebraic integer $\zeta^{\beta}-1$ is a unit in $Z[\zeta]$. If $p_s^{\alpha_s}$ is the only one of the $p_i^{\alpha_i}$ that do not divide β and $p_s^{\gamma}\mid\beta$, $p_s^{\gamma+1}\nmid\beta$, $0\leqslant\gamma<a_s$, then $\zeta^{\beta}-1$ is a $p_s^{\alpha_s-\gamma}$-th primitive root of 1.

Therefore, if two at least of $p_i^{\alpha_i}$ do not divide $\mu-\nu$, we obtain a contradiction. Otherwise there exists i such that $P\mid<p_i>$.

If $P_j\nmid<p_i>$, $i=1,2,\ldots,\kappa$, there exists δ such that $(\alpha,\delta)=1$ and $P_j^{n_j}\mid<b_j-\zeta^{\delta}>$, so $\bar{b}_j=\bar{\zeta}^{\delta}$. Therefore we have $\phi(\alpha)$ choises for $\bar{b}_j$.

Suppose that $P_j\nmid<p_i>$. The decomposition of $<p_i>$ in product of prime ideals in $Z[\zeta]$ is:

$$<p_i>=(Q_{i1}\ldots Q_{ig_i})^{\phi(p_i^{\alpha_i})}$$

and if f_i is the common residue class degree of Q_{ij} we have $f_ig_i\phi(p_i^{\alpha_i})=\phi(\alpha)$, [1, page 337]. Then, there exists r such that $P_j=Q_{ir}$ and since n is an integer we obtain $Q_{ij}\mid<n>$, $j=1,2,\ldots,g_i$. We denote by $N(I)$ the norm of an ideal I. We have,

$$n^{\phi(\alpha)}=N(P_1)^{n_1}\ldots p^{g_if_in_j}\ldots N(P_\lambda)^{n_\lambda}$$

and we get $\phi(p_i^{\alpha_i})\mid n_j$.

If $\alpha_i'=\alpha/p_i^{\alpha_i}$, the algebraic integer $\zeta^{\alpha_i'\beta p_i^{\gamma}}$ where $p_i\nmid\beta$ and $0\leqslant\gamma<\alpha_i$, is a $p_i^{\alpha_i-\gamma}$-th primitive root of 1 and

$$<\zeta^{\alpha_i\beta p_i^{\gamma}}-1>=(Q_{i1}\dots Q_{ig_i})^{p_i}.$$

Suppose $n_j=\phi(p^{\alpha_i})$. Then there exists ν such that $P_j \mid <b_j-\zeta^{\nu}>$. Since $b_j-\zeta^{\nu+\alpha_i\pi}=(b_j-\zeta^{\nu})-\zeta^{\nu}(\zeta^{\alpha_i\pi}-1)$, where $\pi\in N$, it follows that $P_j \mid <b_j-\zeta^{\nu+\alpha_i'\pi}>$. Hence there exists $\upsilon\in Z$, $p_i \nmid \upsilon$, $1\leqslant\upsilon<\alpha_i'$, such that $P_j \mid <b_j-\zeta^{\upsilon+\mu\alpha_i'}>$, where $\mu\in Z$, $0\leqslant\mu<p^{\alpha_i}$ and $p_i/\upsilon+\mu\alpha_i'$.
If $P_j \mid <b_j-\zeta^{\rho}>$ and $\rho\neq\upsilon+\mu\alpha_i'$ we get $P_j \mid <\zeta^{\upsilon-\tau}-1>$, where $\rho=\sigma\alpha_i'+\tau$, $0\leqslant\tau<\alpha_i$. Since $0<|\upsilon-\tau|<\alpha_i'$, $\zeta^{\upsilon-\tau}-1$ is a unit and we obtain a constradiction. Therefore we have $\phi(\alpha_i')p^{f_i(\phi(p^{\alpha_i})-1)}$ choises for $\bar{b}_j$.

Suppose $n_j=\varepsilon\phi(p^{\alpha_i})$, where $2\leqslant\varepsilon\leqslant\alpha_i$. The factors of the product $\prod_{\substack{\nu=1\\(\nu,\alpha_i')=1}}^{\alpha}<b_j-\zeta^{\nu}>$ that P_j divide are the ideals $<b_j-\zeta^{\upsilon+\mu\alpha_i'}>$, where $1\leqslant\upsilon<\alpha_i'$, $p_i \mid \upsilon+\mu\alpha_i'$ and $0\leqslant\mu<p_i^{\alpha_i}$. Since $\varepsilon\geqslant 2$, there exists ρ such that $P_j^2 \mid <b_j-\zeta^{\upsilon+\rho\alpha_i'}>$ and it follows that there exists $\sigma\in Z$, $0\leqslant\sigma<p_i$ such that $P_j^2 \mid <b_j-\zeta^{(\mu+\sigma)\alpha_i'+\upsilon}>$ where $p_i \mid \mu$.
If $P_j^2 \mid <b_j-\zeta^{(\mu+\sigma)\alpha_i'+\upsilon}>$, where $p_i \nmid \mu$, we get $P_j^2 \mid <\zeta^{\mu\alpha_i'}-1>$, a contradiction. Therefore $P_j^{p_i} \mid <b_j-\zeta^{(\mu+\sigma)\alpha_i'+\upsilon}>$ where $p_i \mid \mu$ and $P_j \mid <b_j-\zeta^{(\mu+\sigma)\alpha_i'+\upsilon}>$, $P_j^2 \mid <b_j-\zeta^{(\mu+\sigma)\alpha_i'+\upsilon}>$ where $p_i \nmid \mu$. We continue this process and we deduce there exists $\sigma_s\in Z$ $0\leqslant\sigma_s<p_i$, $s=0,1,\dots,\varepsilon-2$ such that

$P^{p_i^{\varepsilon-1}} \mid <b_j-\zeta^{(\mu+\sum_{s=0}^{\varepsilon-2}\sigma_s p_i^s)\alpha_i'+\upsilon}>$, where $p_i^{\varepsilon-1} \mid \mu$, $p_i \nmid s_o\alpha_i'+\upsilon$ and $P_i^{p^{\varepsilon-2}}$ divide exactly $<b_j-\zeta^{(\mu+\sum_{s=0}^{\varepsilon-2}\sigma_s p_i^s)\alpha_i'+\upsilon}>$, where $p_i^{\varepsilon-2} \mid \mu$, $p^{\varepsilon-1} \nmid \mu$, ... and P_j divide exactly $<b_j-\zeta^{(\mu+\sigma_o)\alpha_i'+\upsilon}>$ where $p_i \nmid \mu$. Then we have

$p_i^{\varepsilon-1}\phi(\alpha_i')p_i^{f_i p_i^{\varepsilon-1}[ep_i^{\varepsilon-\varepsilon}(p_i-1)-1]}$ choises for $\bar{b}_j$.

Suppose that $n_j=(\alpha_i+\delta)\phi(p_i^{\alpha_i})$, where $\delta>0$. Applying the former process we deduce that $P^{p^{\alpha_i-1}+\delta\phi(p_i^{\alpha_i})}$ divide only one of the ideals $<b_j-\zeta^{(\mu+\sum_{s=0}^{\alpha_i-2}\sigma_s p_i^s)\alpha_i+\upsilon}>$, where $p^{\alpha_i-1} \mid \mu$. Therefore we have

$p_i^{\alpha_i}\phi(\alpha_i')p_i^{f_i p^{\alpha_i-1}[\alpha_i(p_i-1)-1]}$ choises for $\bar{b}_j$.

The above process gives us necessary conditions on $\bar{a}_j$, $\bar{b}_j$, for the existence of a homomorphism from $Z[\zeta]$ into $Z[\zeta]/<n>$. Conversely, if $(\bar{a}_1,\dots,\bar{a}_\lambda)$ and $(\bar{b}_1,\dots,\bar{b}_\lambda)$ are any elements of the direct sum (*) which satisfy the above conditions, then there exists a homomorphism from $Z[\zeta]$ into $Z[\zeta]/<n>$. Thus we have proved the following result:

Lemma: Suppose that $p_i \nmid n$ $i=1,...,r$ and $p_i \mid n$ and $p_i^2 \nmid n$ $i=r+1,...,s$, $p^{\varepsilon_i} \nmid n$ and $p_i^{\varepsilon_i+1} \nmid n$, $2 \leqslant \varepsilon_i \leqslant \alpha_i$ $i=s+1,...,t$ and $p_i^{\alpha_i+1} \mid n$, $i=t+1,...,\kappa$. Then the number of ring-homomorphisms from $Z[\zeta]$ into $Z[\zeta]/<n>$ is:

$$(1+\phi(\alpha))^{\omega(n)\cdot\sum_{i=r+1}^{\kappa}\omega(p_i)} \times \prod_{i=r+1}^{s}[1+\phi(\alpha/p^{\alpha_i})p_i^{f_i(\phi(p_i^{\alpha_i})-1)}]^{\omega(p_i)} \times$$

$$\times \prod_{i=s+1}^{t}[1+\phi(\alpha/p^{\alpha_i})p_i^{\varepsilon_i\cdot 1+f_ip_i^{\varepsilon_i\cdot 1}(\varepsilon_i\phi(p_i^{\alpha_i-\varepsilon_i+1})-1)}]^{\omega(p_i)} \times$$

$$\times \prod_{i=t+1}^{\kappa}[1+\phi(\alpha/p_i^{\alpha_i})p^{\alpha_i+f_ip_i^{\alpha_i\cdot 1}(\alpha_i(n_i-1)-1)}]^{\omega(p_i)}.$$

To determine the number of homomorphisms from $Z_n[\zeta]$ into $Z_m[\zeta]$ we observe that the same conditions as above are necessary. Furthermore, if $\bar{a}_j=1$, we haye $\bar{m}=m\bar{a}_j=\bar{0}$, so $P_j^{n_j} \mid <m>$. Hence if $P_j^{n_j} \mid <m>$, we have $\bar{a}_j=\bar{0}$. This completes the proof of the theorem.

REFERENCES

[1] Z.I. BORERICH - I.R. SHAFAREVICH, Number Theory, 1966, Academic Press.

[2] J.A. GALLIAN and J.V. BUSKIRK, The Number of Homomorphisms from Z_m into Z_n, American Math. Monthly, 91(1984), 196-197.

[3] J.A. GALLIAN and D.S. JUNGREIS, Homomorphisms from $Z_m[i]$ into $Z_n[i]$ and from $Z_m[\rho]$ into $Z_n[\rho]$, where $i^2+1=0$ and $\rho^2+\rho+1=0$, American Math. Montly 95(1988), 247-249.

[4] S. LANG, Algebraic Number Theory, 1970 Addisson-Wesley.

Aristotle University of Thessaloniki
Department of Mathematics
54006 - Thessaloniki, Greece