ABSTRACT

Title of thesis: CLASSIFICATION OF PRIME IDEALS IN INTEGRAL GROUP ALGEBRAS OF FINITE ABELIAN GROUPS

Heather Mallie McDonough, Master of Arts, 2005

Thesis directed by: Professor William Adams
Department of Mathematics

Let $\mathbb{Z}[G]$ be the integral group algebra of the group G. In this thesis, we consider the problem of determining all prime ideals of $\mathbb{Z}[G]$ where G is both finite and abelian. Because of Krull dimension arguments, there are only two types of prime ideals in $\mathbb{Z}[G]$. First, we show that we can think of $\mathbb{Z}[G]$ as the quotient of a polynomial ring. Using this fact, and some Galois theory, we then classify the minimal prime ideals of our $\mathbb{Z}[G]$ where we restrict our group to having one or two generators. Next, we determine the form of the maximal ideals of $\mathbb{Z}[G]$ for the same case. However, the maximal ideals in our list need not be distinct. We further explore this issue restricting ourselves to cyclic groups. Using our previous work and cyclotomic field theory we are able to determine the duplication in our previous list.

CLASSIFICATION OF PRIME IDEALS IN INTEGRAL GROUP ALGEBRAS OF FINITE ABELIAN GROUPS

by

Heather Mallie McDonough

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Master of Arts
2005

Advisory Committee:

Professor William Adams, Chair/Advisor
Professor Lawrence Washington
Professor Michael Boyle

TABLE OF CONTENTS

Chapter 1

Introduction

Let G be a finite abelian group. We will denote $\mathbb{Z}_n$ as the cyclic group with order n. Then the fundamental theorem of finitely generated abelian groups gives $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t}$ where $n_1 \mid n_2 \mid \cdots \mid n_t$, although this property will not be necessary for the purposes of this paper. We define the integral group algebra $\mathbb{Z}[G]$ as the set whose additive abelian group is the free $\mathbb{Z}$-module having a basis labelled by the elements of G. That is, every element in $\mathbb{Z}[G]$ is a unique linear combination of the elements from G with coefficients in $\mathbb{Z}$. The multiplication in $\mathbb{Z}[G]$ is given by

$$(\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{k \in G}(\sum_{gh=k; g,h \in G} a_g b_h)k.$$

The purpose of this paper is to classify the prime ideals of $\mathbb{Z}[G]$. Since, if $|G| = n$, we have $g^n = 1$ for all $g \in G$, we see $\mathbb{Z}[G]$ is an integral extension over Z. Because $\mathbb{Z}$ has Krull dimension one, we see that $\mathbb{Z}[G]$ has Krull dimension one as well (See [1]). Therefore, the prime ideals of $\mathbb{Z}[G]$ fall into one of two categories: minimal and maximal. We will first discuss relevant theory of commutative rings. Then we will explicitly determine the minimal prime ideals of $\mathbb{Z}[G]$ using that commutative ring theory and Galois theory. Finally, the maximal ideals of $\mathbb{Z}[G]$ will be categorized using the minimal prime ideals previously determined and the classification of prime ideals in rings of cyclotomic polynomials.

With the exception of Theorem 1, we will restrict to the case where G has 2 generators, i.e. $t = 2$ above. The general case can be done similarly, although the arguments will have significant complications in the details.

Chapter 2

Preliminaries

The integral group algebra of a finite abelian group has several useful properties. First we note that we will be able to work with $\mathbb{Z}[G]$ as a quotient of a polynomial ring over $\mathbb{Z}$.

Theorem 1. *Given $G \cong \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_t \rangle$ such that $\mid g_i \mid = n_i$ for all i, we have $\mathbb{Z}[G] \cong \mathbb{Z}[x_1, x_2, \ldots, x_t]/\langle x_i^{n_i} - 1, 1 \leq i \leq t\rangle := R$.*

Proof: Define the $\mathbb{Z}$-algebra homomorphism $\mathbb{Z}[x_1, x_2, \ldots, x_t] \longrightarrow \mathbb{Z}[G]$ by $x_i \longmapsto g_i$. Because the g_i generate G, we know this homomorphism is surjective. Since $g_i^{n_i} = 1$ for all i, $x_i^{n_i} - 1$ belongs to the kernel of the above $\mathbb{Z}$- algebra homomorphism. Thus, this gives the $\mathbb{Z}$-algebra homomorphism [1]

$$\theta : \mathbb{Z}[x_1, x_2, \ldots, x_t]/\langle x_i^{n_i} - 1, 1 \leq i \leq t\rangle \longrightarrow \mathbb{Z}[G].$$

Because the map $\mathbb{Z}[x_1, x_2, \ldots, x_t] \longrightarrow \mathbb{Z}[G]$ is an epimorphism, we know that θ is also surjective.

Let $n = n_1 \cdot n_2 \cdots n_t$. Now R is a free abelian group with n generators, $x_1^{\nu_1} \cdot x_2^{\nu_2} \cdots x_t^{\nu_t}$, where $0 \leq \nu_i < n_i$, $1 \leq i \leq t$. Thus, $rank(R) = n$ as an abelian group. Also $rank(\mathbb{Z}[G]) = n$, so $\mathbb{Z}[G] \cong \mathbb{Z}^n$ as abelian groups. Thus, we have an abelian group epimorphism,

$$\psi : \mathbb{Z}^n \twoheadrightarrow R.$$

Consequently,

$$\mathbb{Z}^n \overset{\psi}{\twoheadrightarrow} R \overset{\theta}{\twoheadrightarrow} \mathbb{Z}[G] \cong \mathbb{Z}^n.$$

Because the composition of two surjective functions is surjective, we have $\mathbb{Z}^n \twoheadrightarrow \mathbb{Z}[G]$. We claim that $\theta \circ \psi$ is also an injective function. If not, then $\ker(\theta \circ \psi)$ is nontrivial, which implies that it must have rank greater than one. Also, we could factor $\mathbb{Z}^n$ by the kernel and get $\mathbb{Z}^n/\ker(\theta \circ \psi) \cong \mathbb{Z}^n$. Because the rank of the kernel is greater than one, the left side of the isomorphism would have rank smaller than n, which would be a contradiction. Thus, $\theta \circ \psi$ is injective. In particular, θ is injective. Hence θ is an isomorphism.

Q.E.D.

Now we can think of $\mathbb{Z}[G]$ as a quotient of a polynomial ring, which is a more familiar object. In particular, $\mathbb{Z}[x_1, x_2, \ldots, x_t]$, is an integral domain. It will be imperative to have a division algorithm for polynomials in an integral domain if certain criteria are met.

Lemma 1. *Let A be an integral domain, and let $f(x) \in A[x]$ be a monic polynomial in $A[x]$. If $g(x) \in A[x]$, then there exist unique polynomials $q(x)$ and $r(x)$ both in $A[x]$ with*

$$g(x) = q(x)f(x) + r(x),$$

where deg$(r) <$ deg(f).

(We note that $\deg(0) := -\infty$.)

Proof: Consider all polynomials $g-qf$ as q varies over $A[x]$. Choose q such that $r = g - qf$ has least degree. Thus, $g = qf + r$. Now we need to show that $\deg(r) < \deg(f)$. If $r(x) = 0$, then we are done. If not, let $f(x) = x^n + s_{n-1}x^{n-1} + \ldots + s_1x + s_0$, and $r(x) = t_mx^m + t_{m-1}x^{m-1} + \ldots + t_1x + t_0$. By way of contradiction, suppose $\deg(r) \geq \deg(f)$. Then define $h(x) = r(x) - t_mx^{m-n}f(x)$. By assumption, $m \geq n$, which implies that $h(x) \in A[x]$. We know then that $h = 0$ or $\deg(h) < \deg(r)$. If $h = 0$, then $r(x) = t_mx^df(x)$, which implies that $g(x) = q(x)f(x) + t_mx^df(x)$, which implies that $f(x) \mid g(x)$. So $r(x) = 0$, which has degree $-\infty$. If $h \neq 0$, then $\deg(h) < \deg(r)$ and $g - qf = r = h + t_mx^df$. Thus, $g - f(q + t_mx^d) = h$, which contradicts the minimality of the $\deg(r)$. Hence, $\deg(r) \not\geq \deg(f)$, which implies that $\deg(r) < \deg(f)$ as desired. To prove uniqueness, assume two different ways to write g, and a contradiction is quickly reached, as usual.

Q.E.D.

The intersection of ideals will prove to be very important in the classification of minimal prime ideals of $\mathbb{Z}[G]$.

Theorem 2. *Let A be a unique factorization domain, and let x, y be independent variables. Also, let $f(x)$ be monic in $A[x]$ and $g(y), h(y) \in A[y]$ be relatively prime. Then*

$$\langle f(x), g(y)\rangle \cap \langle f(x), h(y)\rangle = \langle f(x), g(y)h(y)\rangle$$

in $A[x, y]$.

Proof:

$\underline{\supseteq}$: Let $k(x, y) \in \langle f(x), g(y)h(y) \rangle$. Then

$$k(x, y) = a(x, y)f(x) + b(x, y)g(y)h(y)$$

for $a(x, y), b(x, y) \in A[x, y]$.

Thus, it is clear that $k(x, y)$ belongs to both

$I_1 := \langle f(x), g(y) \rangle$ and $I_2 := \langle f(x), h(y) \rangle$.

$\underline{\subseteq}$: Let $k(x, y) \in I_1 \cap I_2$. Thus, we can write

$$k(x, y) = a(x, y)f(x) + b(x, y)g(y)$$

$$= c(x, y)f(x) + d(x, y)h(y).$$

It is clear we may view $k(x, y) \in R[x]$ such that $R = \mathbb{Z}[y]$. Because $f(x)$ is a monic polynomial, application of Lemma 1 yields:

$$k(x, y) = \sum_{\nu=0}^{N-1} k_\nu(y)x^\nu + \alpha(x, y)f(x),$$

where $\deg(f) = N$. Also, we can write similarly,

$$b(x, y) = \sum_{\nu=0}^{N-1} b_\nu(y)x^\nu + \beta(x, y)f(x),$$

and

$$d(x, y) = \sum_{\nu=0}^{N-1} d_\nu(y)x^\nu + \gamma(x, y)f(x).$$

Thus,

$$\sum_{\nu=0}^{N-1} k_\nu(y)x^\nu = k(x,y) - \alpha(x,y)f(x)$$

$$= a(x,y)f(x) + b(x,y)g(y) - \alpha(x,y)f(x)$$

$$= b(x,y)g(y) + [a(x,y) - \alpha(x,y)]f(x)$$

$$= \sum_{\nu=0}^{N-1} b_\nu(y)x^\nu g(y) + \beta(x,y)g(y)f(x) + [a(x,y) - \alpha(x,y)]f(x)$$

$$= \sum_{\nu=0}^{N-1} b_\nu(y)x^\nu g(y) + \delta(x,y)f(x)$$

where $\delta(x,y) = \beta(x,y)g(y) + a(x,y) - \alpha(x,y)$.

By similar argument we also have

$$\sum_{\nu=0}^{N-1} k_\nu(y)x^\nu = \sum_{\nu=0}^{N-1} d_\nu(y)x^\nu h(y) + \epsilon(x,y)f(x)$$

where $\epsilon(x,y) = \gamma(x,y)h(y) + c(x,y) - \alpha(x,y)$. Thus, we can conclude that $k_\nu(y) = b_\nu(y)g(y) = d_\nu(y)h(y)$ for all $0 \leq \nu \leq N-1$. If not, then there exists ν between 0 and $N-1$ such that

$$k_\nu(y) \neq b_\nu(y)g(y),$$

which implies that

$$f(x) | \sum_{\nu=0}^{N-1} (k_\nu(y) - b_\nu(y)g(y))x^\nu.$$

Consequently, the $\deg(f(x)) \leq N-1$ in $A[x,y]$, which is a contradiction. Therefore, $b_\nu(y)g(y) = d_\nu(y)h(y)$ for all $0 \leq \nu \leq N-1$, and so $h(y)|b_\nu(y)$ because g and h are relatively prime. We can write $b_\nu(y) = h(y)b'_\nu(y)$. Thus,

$$k(x,y) = (\sum_{\nu=0}^{N-1} b'_\nu(y)x^\nu)g(y)h(y) + (a(x,y) + \alpha(x,y))f(x),$$

which implies that $k(x,y) \in \langle f(x), g(y)h(y) \rangle$.

Having established containment in both directions, we now have equality as desired.

Q.E.D.

We would like to be able to extend Theorem 2 so we can further break down the structure of the integral group algebra.

Corollary 1. *Let x, y be distinct variables and A a unique factorization domain. Let $f(x)$ be monic in $A[x]$, and let $g_1(y), \ldots, g_m(y) \in A[y]$ be pairwise relatively prime. Then,*

$$\langle f(x), g_1(y) \rangle \cap \langle f(x), g_2(y) \rangle \cap \ldots \cap \langle f(x), g_m(y) \rangle$$

$$= \langle f(x), g_1(y) \cdots g_m(y) \rangle$$

in $A[x, y]$.

Proof: We will use induction on m, the number of pairwise relative prime polynomials.

Let $m = 2$. Then we are done by Theorem 2.

Assume the statement we desire to prove is true for m pairwise relatively prime polynomials. That is,

$$\langle f(x), g_1(y)\rangle \cap \langle f(x), g_2(y)\rangle \cap \ldots \cap \langle f(x), g_m(y)\rangle$$

$$= \langle f(x), g_1(y) \cdots g_m(y)\rangle$$

in $A[x_1, \ldots, x_n, y]$.

Now consider $m+1$ pairwise relatively prime polynomials:

$$\langle f(x), g_1(y)\rangle \cap \langle f(x), g_2(y)\rangle \cap \ldots \cap \langle f(x), g_m(y)\rangle \cap \langle f(x), g_{m+1}(y)\rangle$$

$$= \langle f(x), g_1(y) \cdots g_m(y)\rangle \cap \langle f(x), g_{m+1}(y)\rangle$$

by the induction hypothesis.

We note that $gcd(g_1(y) \cdots g_m(y), g_{m+1}(y)) = 1$. If not, there exists a prime polynomial, $h(y)$, such that $h \mid (g_1 \cdots g_m)$ and $h \mid g_{m+1}$. Because $g_1, \ldots, g_m$ are pairwise relatively prime, $h \mid g_i$ for some $1 \leq i \leq m$. This contradicts the relative primality of g_i and g_{m+1}. Thus, we can apply Theorem 2, and we get:

$$\langle f(x), g_1(y) \cdots g_m(y)\rangle \cap \langle f(x), g_{m+1}(y)\rangle$$

$$= \langle f(x), g_1(y) \cdots g_m(y) \cdot g_{m+1}\rangle.$$

Thus, by induction we have:

$$\langle f(x), g_1(y)\rangle \cap \langle f(x), g_2(y)\rangle \cap \ldots \cap \langle f(x), g_m(y)\rangle$$

$$= \langle f(x), g_1(y) \cdots g_m(y)\rangle$$

in $A[x, y]$ as desired.

Q.E.D.

Chapter 3

Recognizing Minimal Prime Ideals

Let A be a commutative ring. The nilradical of A is defined as $N(A) = \{a \in A | a^m = 0 \text{ for some } m \geq 1\}$. That is, $N(A)$ is the set of nilpotents of A. There are several facts we need to establish concerning the nilradical of A before we can begin to classify the minimal prime ideals of our group algebra. We define $\text{Spec}(A) = \{P | P \text{ is a prime ideal of } A\}$

Proposition 1. $N(A) = \bigcap_{P\in \ Spec(A)} P$.

Proof:

$\subseteqq$: Let $f \in N(A)$. Then $f^n = 0$ for some $n \geq 1$. We know that $0 \in \bigcap_{P\in \text{ Spec}(A)} P$. Thus, $f^n \in \bigcap_{P\in \text{ Spec}(A)} P$. Because each P is a prime ideal, f^{n-1} or f belongs to P. Suppose $f^{n-1} \in P$, then f or f^{n-2} belongs to P. We repeat this process for each $P \in$ Spec(A). And so, $f \in \bigcap_{P\in \text{ Spec}(A)} P$.

$\supseteqq$: Let $f \in \bigcap_{P\in \text{ Spec}(A)} P$. By way of contradiction, assume $f \notin N(A)$, i.e. there does not exist a positive integer n such that $f^n = 0$. Now define the set $S = \{1, f, f^2, \ldots\}$. We know that $0 \notin S$ because f is not a nilpotent element. By Proposition 1.9 in [6], there exists a prime ideal Q such that $Q \cap S = \emptyset$ [6]. Thus, $f \notin Q$, but $f \in \bigcap_{P\in \text{ Spec}(A)} P$, which is a contradiction. Hence, $f \in N(A)$.

We have established containment in both directions, and thus, equality, as desired.

Q.E.D.

Proposition 2. *Let P, I be ideals of the commutative ring A with P prime and $I \subseteq P$. Then there exists a prime ideal Q such that $I \subseteq Q \subseteq P$ and Q is minimal over I, i.e. there is no prime ideal containing I strictly contained in Q.*

Proof: Define $\Omega := \{P' \in \text{Spec(A)} | I \subseteq P' \subseteq P\}$. Clearly Ω is a nonempty set because $P \in \Omega$. We will partially order Ω by reverse inclusion. That is, for P_i, $P_j \in \Omega$,

$$P_i \preceq P_j \text{ if and only if } P_i \supseteq P_j.$$

Thus a maximal element of this partially ordered set is actually a minimal element of Ω. Let Γ be a nonempty subset of Ω, which is totally ordered with respect to the above partial ordering. Define

$$J := \bigcap_{P' \in \Gamma} P'.$$

We first note that by construction J is a proper ideal of A. We now need to show that J is a prime ideal of A. Assume $ab \in J$. Then $ab \in P'$ for all $P' \in \Gamma$. Assume that $a \notin J$. Then we wish to show that $b \in J$. Because $a \notin J$, there exists a $P_i \in \Gamma$ such that $a \notin P_i$. Recall that Γ is totally ordered with respect to reverse inclusion. Thus, if $P' \in \Gamma$, either $P' \subseteq P_i$ or $P' \supseteq P_i$. If $P' \subseteq P_i$, then we know that $a \notin P'$ and so $b \in P'$ because P' is a prime ideal. If $P' \supseteq P_i$, then $a \notin P_i$ and the fact that P_i is a prime ideal, implies that $b \in P_i \subseteq P'$. Thus, if $a \notin J$, then $b \in P'$ for all

$P' \in \Gamma$, which implies that $b \in J$. Hence, J is a prime ideal, and therefore belongs to $Spec(A)$. By construction, $J \supseteq I$. Thus J, which is nonempty, is the upperbound of Γ required for application of Zorn's Lemma. Therefore, Γ has a a maximal element, which is actually a minimal element of Ω, say Q. Hence, there is a minimal prime ideal, Q, contained in an arbitrary prime ideal P, containing I [8].

Q.E.D.

Corollary 2. *$N(A) = \cap m$, where m ranges over the minimal prime ideals of A.*

Proof: We need only show that $\cap m = \cap P$, where $P \in \text{Spec}(A)$. It is clear that $\cap P \subseteq \cap m$. Thus, to show containment in the other direction, assume $f \in \cap m$. According to the former proposition, every prime ideal contains a minimal prime ideal. For all P, we can find some m such that $m \subseteq P$ Hence, $f \in \cap P$.

We have established equality. By Proposition 1, we now have that
$N(A) = \cap m$.

Q.E.D.

Proposition 3. *Let $I_1, I_2, \ldots, I_t$ be ideals in A, and P be a prime ideal of A. If $I_1 \cap I_2 \cap \cdots \cap I_t \subseteq P$, then there exists i, $1 \leq i \leq t$, such that $I_i \subseteq P$.*

Proof: By way of contradiction, assume there exist $f_i \in I_i$ such that $f_i \notin P$ for all $1 \leq i \leq t$. Because each I_i is an ideal, $\prod_{i=1}^{t} f_i \in I_i$ for all $1 \leq i \leq t$, which implies that

$$\prod_{i=1}^{t} f_i \in I_1 \cap I_2 \cap \cdots \cap I_t \subseteq P.$$

Because P is a prime ideal, there exists $1 \leq i \leq t$ such that $f_i \in P$, which is a contradiction to our assumption. Thus, there exists $1 \leq i \leq t$ such that $I_i \subseteq P$.

Q.E.D.

Lemma 2. *Let $m_1, m_2, \ldots, m_t$ be minimal prime ideals of A such that $m_1 \cap m_2 \cap \cdots \cap m_t = \{0\}$. Then, $m_1, m_2, \ldots, m_t$ are exactly the minimal prime ideals of A.*

Proof: Let m be another minimal prime ideal of A that is not contained in the above list. We know that $\cap_{i=1}^{t} m_i = \{0\} \subseteq m$. Thus, by Proposition 3, there exists i, $1 \leq i \leq t$, such that $m_i \subseteq m$. Because m is a minimal prime, $m = m_i$. Thus, $m_1, m_2, \ldots, m_t$ are all of the minimal prime ideals of A.

Q.E.D.

We are now ready to consider minimal prime ideals in $\mathbb{Z}[G]$.

Chapter 4

Minimal Primes in $\mathbb{Z}[G]$

We now specialize to the case where G has two generators. Thus, by Corollary 1 we write $\mathbb{Z}[G] \cong \mathbb{Z}[x,y]/\langle x^m - 1, y^n - 1\rangle$. (We do not need to assume that $m \mid n$ because no work will require this property.) The purpose of this section is to determine all of the minimal prime ideals of this $\mathbb{Z}[G]$. Thus, we need to determine the prime ideals in $\mathbb{Z}[x,y]$ minimal over the ideal $\langle x^m - 1, y^n - 1\rangle$. With this goal in mind we first observe:

Proposition 4. *We have in $\mathbb{Z}[x,y]$,*

$$\bigcap_{d_1|m, d_2|n} \langle \Phi_{d_1}(x), \Phi_{d_2}(y)\rangle = \langle x^m - 1, y^n - 1\rangle,$$

where $\Phi_j(x)$ is the j^{th} cyclotomic polynomial.

Proof: While holding $\Phi_{d_2}(y)$ constant, range through all $\Phi_{d_1}(x)$. By repeatedly applying Corollary 1 in Chapter 2 we get

$$\bigcap_{d_1|m, d_2|n} \langle \Phi_{d_1}(x), \Phi_{d_2}(y)\rangle$$

$$= \bigcap_{d_2|n} \langle x^m - 1, \Phi_{d_2}(y)\rangle.$$

Again, we apply Corollary 1 to the previous statement. Then we get:

$$\bigcap_{d_1|m, d_2|n} \langle \Phi_{d_1}(x), \Phi_{d_2}(y) \rangle = \langle x^m - 1, y^n - 1 \rangle$$

Q.E.D.

Now we have

$$\mathbb{Z}[G] \cong \mathbb{Z}[x, y] / \bigcap_{d_1|m, d_2|n} \langle \Phi_{d_1}(x), \Phi_{d_2}(y) \rangle.$$

In order to explicitly classify the minimal prime ideals of our $\mathbb{Z}[G]$, we must be able to decompose $\langle \Phi_{d_1}(x), \Phi_{d_2}(y) \rangle$ into an intersection of prime ideals.

We first note that $\mathbb{Z}[x, y]/\langle \Phi_{d_1}(x), \Phi_{d_2}(y) \rangle \cong \mathbb{Z}[\zeta_{d_1}][y]/\langle \Phi_{d_2}(y) \rangle$ by the Third Isomorphism Theorem, where ζ_{d_i} is a primitive ${d_i}^{\text{th}}$ root of unity. Hence, we need to determine the factorization of $\Phi_{d_2}(y)$ in $\mathbb{Z}[\zeta_{d_1}][y]$.

Consider the following diagram:

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_l) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_{d_1}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_{d_2}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

We define $l = lcm(d_1, d_2)$. Thus, $\mathbb{Q}(\zeta_l)$ is the compositum field of $\mathbb{Q}(\zeta_{d_1})$ and $\mathbb{Q}(\zeta_{d_2})$. We know that

$$[\mathbb{Q}(\zeta_l) : \mathbb{Q}] = \phi(l),$$

$$[\mathbb{Q}(\zeta_{d_1}) : \mathbb{Q}] = \phi(d_1),$$

and

$$[\mathbb{Q}(\zeta_{d_2}) : \mathbb{Q}] = \phi(d_2),$$

where ϕ is the Euler Phi function.

All extensions are clearly abelian. Also,

$$[\mathbb{Q}(\zeta_l) : \mathbb{Q}(\zeta_{d_1})] = \phi(l)/\phi(d_1)$$

and

$$[\mathbb{Q}(\zeta_l) : \mathbb{Q}(\zeta_{d_2})] = \phi(l)/\phi(d_2).$$

We define

$$F := Gal(\mathbb{Q}(\zeta_l)/\mathbb{Q})$$

and

$$H := Gal(\mathbb{Q}(\zeta_l)/\mathbb{Q}(\zeta_{d_1})).$$

We can think of F as isomorphic to $\mathbb{Z}_l^*$ the multiplicative group of $\mathbb{Z}_l$. That is, k with $\gcd(k, l) = 1$ corresponds to $\sigma_k \in \mathrm{Aut}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ such that $\sigma_k(\zeta_l) = \zeta_l^k$. Then H is the subgroup $\{\sigma_k \in F | k \equiv 1 \bmod d_1\}$. Recall that $\Phi_{d_2}(y) = irr_{\mathbb{Q}}(\zeta_{d_2})$, the irreducible polynomial of ζ_{d_2} over $\mathbb{Q}$. Hence, we would like to be able to factor $\Phi_{d_2}(y)$ into polynomials, $p_j(y)$, such that $p_j(y) \in (\mathbb{Q}(\zeta_{d_1}))[y]$. Let $X = \{\zeta_{d_2}^a | gcd(a, d_2) = 1\}$, which are the primitive d_2^{th} roots of unity, and so the roots of Φ_{d_2}.

Proposition 5. *The group H acts on X by $\sigma_k(\zeta_{d_2}^a) = \zeta_{d_2}^{ak}$. Define $O_1, \ldots, O_t$ to be the orbits of the action of H on X. We know that these orbits, by construction, partition X. Now define $p_j(x) = \prod_{\alpha \in O_j}(x - \alpha)$. Then the following are true:*

(i) $\Phi_{d_2}(y) = p_1(y)\cdots p_t(y)$,

(ii) $p_j(y) \in (\mathbb{Z}(\zeta_{d_1}))[y]$,

(iii) $p_j(y)$ *is irreducible over* $\mathbb{Q}(\zeta_{d_1})$,

(iv) The number of orbits is $\phi(gcd(d_1, d_2))$, *i.e.* $t = \phi(gcd(d_1, d_2))$.

Proof:

(i): Because the orbits partition the roots of unity, the polynomial $p_1(y)\cdots p_k(y)$ has exactly all the primitive d_2^{th} roots of unity as its own roots. Recall that

$$\Phi_{d_2}(y) = irr_{\mathbb{Q}}(\zeta_{d_2}) = \prod_{\text{gcd}(a,d_2)=1} (y - \zeta_{d_2}^a),$$

Thus,

$$p_1(y)\cdots p_t(y) = \prod_{\text{gcd}(a,d_2)=1} (y - \zeta_{d_2}^a) = \Phi_{d_2}(y).$$

(ii): Because $\mathbb{Q}(\zeta_l)/\mathbb{Q}(\zeta_{d_1})$ is a Galois extension, this implies that the fixed field of H is exactly $\mathbb{Q}(\zeta_{d_1})$. Let $\sigma \in H$. Then

$$\sigma(p_j(y))$$

$$= \sigma(\prod_{\alpha\in O_j}(y-\alpha)) = \prod_{\alpha\in O_j}(y - \sigma(\alpha)).$$

The $\alpha \in O_j$ get permuted by $\sigma \in H$ because O_j is an orbit of H, and so

$$\sigma(p_j(y)) = \prod_{\alpha\in O_j}(y-\alpha)$$

$$= p_j(y).$$

Thus, $p_j(y)$ is fixed by H, which implies that $p_j(y) \in (\mathbb{Q}(\zeta_{d_1})[y]$. Furthermore, we know that α is an algebraic integer, which implies that all coefficients of $p_j(y)$ are algebraic integers in $\mathbb{Q}(\zeta_{d_1})$. Thus, we may conclude that $p_j(y) \in \mathbb{Z}(\zeta_{d_1})$.

<u>(iii)</u>: Define $p(y) = irr_{\mathbb{Q}(\zeta_{d_1})}(\zeta_{d_2})$ for a given pair (d_1, d_2). That is, we will have a different $p(y)$ for each element in X because $\mathbb{Q}(\zeta_{d_1}, \zeta_{d_2}^a) = \mathbb{Q}(\zeta_l)$ for all a such that $\gcd(a, d_2) = 1$. Since any element of X is a primitive d_2^{th} root of unity, it is sufficient to show the proof for $\zeta_{d_2} \in O_1$. Recall that $[\mathbb{Q}(\zeta_l) : \mathbb{Q}(\zeta_{d_1})] = \phi(l)/\phi(d_1)$. This implies that $\deg(p(y)) = \phi(l)/\phi(d_1)$. We claim that H acts faithfully on X. A group G acts faithfully on a set S if the only element in G that sends an element in S back to itself is the identity element of G. By way of contradiction, suppose H does not act faithfully on X. Then there exists a nontrivial $\sigma \in H$ such that $\sigma(\zeta_{d_2}) = \zeta_{d_2}$. Because the fixed field of H is $\mathbb{Q}(\zeta_{d_1})$, we know that $\sigma(\zeta_{d_1}) = \zeta_{d_1}$. Thus, σ fixes $\mathbb{Q}(\zeta_l)$, which is a contradiction. Thus, H acts faithfully on X. Now we know that

$$\mid O_1 \mid = \mid H \mid / \mid H_x \mid,$$

where H_x is the stabilizer of $x \in X$. That is

$$H_x = \{\sigma \in H \mid \sigma(x) = x\}.$$

Because H acts faithfully, $\mid H_x \mid = 1$. Thus,

$$\mid O_1 \mid = \underbrace{\mid H \mid = [\mathbb{Q}(\zeta_l) : \mathbb{Q}(\zeta_{d_1})]} = \phi(l)/\phi(d_1).$$

by the fundamental theorem of Galois extensions.

Consequently,

$$\deg(p_1(y)) = \deg(\Pi_{\alpha \in O_1}(y-\alpha)) = \phi(l)/\phi(d_1).$$

We know that $p(y) \mid p_1(y)$, but these polynomials have the same degree. Thus, $p(y) = p_1(y)$, and we may conclude $p_1(y)$ is irreducible in $\mathbb{Q}(\zeta_l)/\mathbb{Q}(\zeta_{d_1})$. Since the order of O_j is the same for all $1 \leq j \leq t$, we can conclude that $p_j(y)$ is irreducible for all j.

(iv): Let $gcd(d_1, d_2) = q_1^{e_1} q_2^{e_2} \cdots q_t^{e_t}$, where q_i is a distinct prime. We know by part (iii) that

$$t = \phi(d_2)/\deg(p(y)) = \phi(d_2)/(\phi(l)/\phi(d_1)) = \frac{\phi(d_2)\phi(d_1)}{\phi(l)}$$
$$= \frac{d_1 d_2}{l} \frac{(1-\frac{1}{q_1})^2(1-\frac{1}{q_2})^2 \cdots (1-\frac{1}{q_t})^2}{(1-\frac{1}{q_1})(1-\frac{1}{q_2}) \cdots (1-\frac{1}{q_t})},$$

because it is the primes in the gcd that show up in both $\phi(d_1)$ and $\phi(d_2)$, and these same primes show up only once in the lcm; all the other primes of d_1 and d_2 divide out because they appear in the lcm exactly once. Hence we have

$$= \frac{d_1 d_2}{l}(1-\frac{1}{q_1})(1-\frac{1}{q_2}) \cdots (1-\frac{1}{q_t})$$

$$= \phi(gcd(d_1, d_2)),$$

since $gcd(d_1, d_2) = \frac{d_1 d_2}{l}$.

Q.E.D.

Now we see how to factor $\Phi_{d_2}(y)$ in $\mathbb{Q}[\zeta_{d_1}][y]$. We note that all of the $p_j(y)$ we constructed above are monic with integer coefficients. Consequently, the work we did with the Galois groups is applicable to $\mathbb{Z}$. Thus, we have a way of factoring

$\Phi_{d_2}(y)$ in $\mathbb{Z}[\zeta_{d_1}][y]$. Write for each j, $1 \leq j \leq t$

$$p_j(y) = \sum p_{\nu j}(\zeta_{d_1})y^{\nu}$$

where $p_{\nu j}(y)$ is a polynomial with coefficients in $\mathbb{Z}$ anddeg$_x(p_{\nu j}(y)) < \phi(d_1)$. Also write

$$p_j(x, y) = \sum p_{\nu j}(x)y^{\nu}.$$

This polynomial is monic in y.

Lemma 3. *Given $p_j(x, y)$ as constructed above,*

$$\langle \Phi_{d_1}(x), p_1(x, y)\rangle \cap \langle \Phi_{d_1}(x), p_2(x, y)\rangle = \langle \Phi_{d_1}(x), p_1(x, y)p_2(x, y)\rangle.$$

Proof: It is clear that

$$\langle \Phi_{d_1}(x), p_1(x, y)\rangle \cap \langle \Phi_{d_1}(x), p_2(x, y)\rangle \supseteq \langle \Phi_{d_1}(x), p_1(x, y)p_2(x, y)\rangle.$$

To get containment in the other direction, assume

$$f \in \langle \Phi_{d_1}(x), p_1(x, y)\rangle \cap \langle \Phi_{d_1}(x), p_2(x, y)\rangle.$$

Then we can write

$$f = a(x, y)\Phi_{d_1}(x) + b(x, y)p_1(x, y).$$

Because $p_2(x, y)$ is monic in y, we can apply Lemma 1:

$$b(x, y) = q(x, y)p_2(x, y) + r(x, y),$$

where $\deg_y(r) < \deg_y(p_2)$. We can apply the same lemma again because $\Phi_{d_1}(x)$ is monic in x :

$$r(x, y) = q'(x, y)\Phi_{d_1}(x) + r'(x, y),$$

where $\deg_y(r') < \deg_y(p_2)$ and $\deg_x(r') < \deg_x(\Phi_{d_1}(x)) = \phi(d_1)$. Thus,

$$f = a(x,y)\Phi_{d_1}(x) + q(x,y)p_1(x,y)p_2(x,y) + q'(x,y)\Phi_{d_1}(x)p_1(x,y) + r'(x,y)p_1(x,y).$$

By construction, we know we can choose a $\zeta_{d_2}^{\nu}$, which will be a root of $p_2(\zeta_{d_1}, y)$, but not a root of $p_1(\zeta_{d_1}, y)$. By assumption, $f \in \langle \Phi_{d_1}(x), p_2(x,y)\rangle$, and therefore we have

$$0 = f(\zeta_{d_1}, \zeta_{d_2}^{\nu}) =$$

$$a(\zeta_{d_1}, \zeta_{d_2}^{\nu})\Phi_{d_1}(\zeta_{d_1}) + q(\zeta_{d_1}, \zeta_{d_2}^{\nu})p_1(\zeta_{d_1}, \zeta_{d_2}^{\nu})p_2(\zeta_{d_1}, \zeta_{d_2}^{\nu}) +$$

$$q'(\zeta_{d_1}, \zeta_{d_2}^{\nu})\Phi_{d_1}(\zeta_{d_1})p_1(\zeta_{d_1}, \zeta_{d_2}^{\nu}) + r'(\zeta_{d_1}, \zeta_{d_2}^{\nu})p_1(\zeta_{d_1}, \zeta_{d_2}^{\nu})$$

$$= r'(\zeta_{d_1}, \zeta_{d_2}^{\nu})p_1(\zeta_{d_1}, \zeta_{d_2}^{\nu}).$$

However, $p_1(\zeta_{d_1}, \zeta_{d_2}^{\nu}) \neq 0$ by our choice of $\zeta_{d_2}^{\nu}$. Because $\mathbb{Z}[\zeta_l]$ is an integral domain, we may conclude that $r'(\zeta_{d_1}, \zeta_{d_2}^{\nu}) = 0$. Thus, $\zeta_{d_2}^{\nu}$ is a root of $r'(\zeta_{d_1}, y)$. But then $r'(\zeta_{d_1}, y) = 0$ because $\deg_y(r') < \deg_y(p_2)$. We can write $r'(x,y) = \sum a_\nu(x)y^\nu$. Because $r'(\zeta_{d_1}, y) = 0$, it is true that $a_\nu(\zeta_{d_1}) = 0$ for all ν. Recall that the division algorithm gave us $\deg_x(r') < \phi(d_1)$. Thus, $\deg_x(a_\nu(x)) < \phi(d_1)$. Because our division algorithm gave us a remainder with least degree, we know that $a_\nu(x) = 0$. Consequently, $r'(x,y) = 0$, which implies that $r(x,y) = q'(x,y)\Phi_{d_1}(x)$. Thus,

$$f = a(x,y)\Phi_{d_1}(x) + [q(x,y)p_2(x,y) + q'(x,y)\Phi_{d_1}(x)]p_1(x,y)$$

$$= [a(x,y) + q'(x,y)p_1(x,y)]\Phi_{d_1}(x) + q(x,y)p_1(x,y)p_2(x,y).$$

Hence, $f \in \langle \Phi_{d_1}(x), p_1(x,y)p_2(x,y)\rangle$.

Having established containment in both directions, we now have equality, as desired. **Q.E.D.**

Example 1

We will illustrate the previous lemma using $G \cong \mathbb{Z}_8 \times \mathbb{Z}_8$. Let's consider the intersection of the following two ideals when $d_1 = 4$ and $d_2 = 4$: $\langle x^4+1, y+x\rangle$ and $\langle x^4+1, y-x\rangle$, both in $\mathbb{Z}[x,y]$. By the previous corollary, $\langle x^4+1, y+x\rangle \cap \langle x^4+1, y-x\rangle = \langle x^4+1, (y+x)(y-x)\rangle = \langle x^4+1, y^2-x^2\rangle$, because it is easy to observe that $y+x$ and $y-x$ are two distinct $p_j(x,y)$'s in $\mathbb{Z}[x,y]$.

We will now check this directly by proving containment in both directions of the statement:

$$\langle x^4+1, y+x\rangle \cap \langle x^4+1, y-x\rangle = \langle x^4+1, y^2-x^2\rangle.$$

$\supseteq$: Let $k(x,y) \in \langle x^4+1, y^2-x^2\rangle$. Then we can write

$$k(x,y) = a(x,y)(x^4+1) + b(x,y)(y^2-x^2)$$

$$= a(x,y)(x^4+1) + b(x,y)(y-x)(y+x)$$

This implies that $k(x,y)$ belongs to both $\langle x^4+1, y+x\rangle$ and $\langle x^4+1, y-x\rangle$.

$\subseteq$: Let $k(x,y) \in \langle x^4+1, y+x\rangle \cap \langle x^4+1, y-x\rangle$. Thus, we can write:

$$k(x,y) = a(x,y)(x^4+1) + b(x,y)(y+x)$$

$$= c(x,y)(x^4+1) + d(x,y)(y-x)$$

Now let y=x. Then we have

$$a(x,x)(x^4+1)+b(x,x)(2x)=c(x,x)(x^4+1),$$

which implies that $(x^4+1)[c(x,x)-a(x,x)]=b(x,x)2x$.

We know that $gcd(x^4+1,2x)=1$. Thus, $(x^4+1) \mid b(x,x)$, and so we can write $b(x,x)=b'(x,x)(x^4+1)$. By Lemma 1 we have $b(x,y)=(y-x)q(x,y)+r(x)$, where $r(x)=b(x,x)=b'(x,x)(x^4+1)$. Hence we have,

$$k(x,y)=a(x,y)(x^4+1)+[(y-x)q(x,y)+(x^4+1)b'(x,x)](y+x)$$

$$=(x^4+1)[a(x,y)b'(x,x)(x+y)]+q(x,y)(y^2-x^2),$$

which belongs to $\langle x^4+1, y^2-x^2\rangle$. Thus we have equality, illustrating the validity of our previous theorem.

Lemma 3 can be generalized to give,

Corollary 3. *Given $p_j(x,y)$ defined in Lemma 3, then*

$$\langle \Phi_{d_1}(x), p_1(x,y)\rangle \cap \langle \Phi_{d_1}(x), p_2(x,y)\rangle \cap \ldots \cap \langle \Phi_{d_1}(x), p_m(x,y)\rangle$$

$$=\langle \Phi_{d_1}(x), p_1(x,y)p_2(x,y)\cdots p_m(x,y)\rangle.$$

Proof: We will use induction on Lemma 3. If $m=2$, then we are done by Lemma 3. Assume our hypothesis is true for all $p_j(x,y)$ for $1\leq j\leq m$. That is,

$$\langle \Phi_{d_1}(x), p_1(x,y)\rangle \cap \langle \Phi_{d_1}(x), p_2(x,y)\rangle \cap \ldots \cap \langle \Phi_{d_1}(x), p_m(x,y)\rangle.$$

$$= \langle \Phi_{d_1}(x), p_1(x,y)p_2(x,y)\cdots p_m(x,y)\rangle.$$

Now consider

$$\langle \Phi_{d_1}(x), p_1(x,y)\rangle \cap \langle \Phi_{d_1}(x), p_2(x,y)\rangle \cap$$

$$\ldots \cap \langle \Phi_{d_1}(x), p_m(x,y)\rangle \cap \langle \Phi_{d_1}(x), p_{m+1}(x,y)\rangle.$$

By our induction hypothesis,

$$\langle \Phi_{d_1}(x), p_1(x,y)\rangle \cap \langle \Phi_{d_1}(x), p_2(x,y)\rangle \cap$$

$$\ldots \cap \langle \Phi_{d_1}(x), p_m(x,y)\rangle \cap \langle \Phi_{d_1}(x), p_{m+1}(x,y)\rangle$$

$$= \langle \Phi_{d_1}(x), p_1(x,y)p_2(x,y)\cdots p_m(x,y)\rangle \cap \langle \Phi_{d_1}(x), p_{m+1}(x,y)\rangle.$$

It is clear that

$$\langle \Phi_{d_1}(x), p_1(x,y)p_2(x,y)\cdots p_m(x,y)\rangle \cap \langle \Phi_{d_1}(x), p_{m+1}(x,y)\rangle \supseteq$$

$$\langle \Phi_{d_1}(x), p_1(x,y)p_2(x,y)\cdots p_m(x,y)p_{m+1}(x,y)\rangle.$$

To get containment in the other direction, assume

$$f \in \langle \Phi_{d_1}(x), p_1(x,y)p_2(x,y)\cdots p_m(x,y)\rangle \cap \langle \Phi_{d_1}(x), p_{m+1}(x,y)\rangle.$$

Then we can write

$$f = a(x,y)\Phi_{d_1}(x) + b(x,y)p_{m+1}(x,y).$$

Because each $p_j(x,y)$ is monic in y, and hence, $p_1(x,y)p_2(x,y)\cdots p_m(x,y)$ is monic in y, we can follow the same argument as that in the proof of Lemma 3. We will choose $\zeta_{d_2}^{\nu}$, which will be a root of $p_1(\zeta_{d_1}, y)$, but not a root of $p_{m+1}(\zeta_{d_1}, y)$. Thus,

$\zeta_{d_2}^{\nu}$ is a root of $p_1(\zeta_{d_1}, y)p_2(\zeta_{d_1}, y)\cdots p_m(\zeta_{d_1}, y)$. Using the same degree argument, we are able to conclude that

$$f = [a(x,y) + q'(x,y)p_{m+1}(x,y)]\Phi_{d_1}(x) +$$

$$q(x,y)p_1(x,y)p_2(x,y)\cdots p_m(x,y)p_{m+1}(x,y).$$

Hence, $f \in \langle \Phi_{d_1}(x), p_1(x,y)p_2(x,y)\cdots p_m(x,y)p_{m+1}(x,y)\rangle$.

Having established containment in both directions, we now have equality, as desired. **Q.E.D.**

Corollary 4.

$$\langle \Phi_{d_1}(x), \Phi_{d_2}(y)\rangle = \bigcap_{j=1}^{t} \langle \Phi_{d_1}(x), p_j(x,y)\rangle.$$

Proof: Use repeated applications of the former corollary and the fact from page 15 that

$$\Phi_{d_2}(y) \equiv p_1(x,y)p_2(x,y)\cdots p_t(x,y) \bmod \Phi_{d_1}(x).$$

Q.E.D.

Corollary 5. *If* $G \cong \mathbb{Z}_m \times \mathbb{Z}_n$, *then*

$$\mathbb{Z}[G] \cong \mathbb{Z}[x,y] / \bigcap_{d_1|m, d_2|n} (\cap_{j=1}^{t} \langle \Phi_{d_1}(x), p_j(x,y)\rangle).$$

Proof: This follows immediately from the previous corollary.

Q.E.D.

We are now ready to explicitly classify the minimal prime ideals of $\mathbb{Z}[G]$.

Theorem 3. *Given $G = \langle a, b | a^m = b^n = 1, aba^{-1} = b\rangle \cong \mathbb{Z}_m \times \mathbb{Z}_n$, the minimal prime ideals of $\mathbb{Z}[G]$ are the ideals*

$$\langle \Phi_{d_1}(a), p_j(a, b)\rangle$$

such that $d_1 \mid m$, $d_2 \mid n$, and $1 \leq j \leq t$.

Proof: Because there is a correspondence between the presentation elements a, b and the indeterminates x, y, respectively, we need only show

$$\langle \Phi_{d_1}(x), p_j(x, y)\rangle$$

such that $d_1 \mid m$, $d_2 \mid n$, and $1 \leq j \leq t$ are the prime ideals minimal over $\langle x^m - 1, y^n - 1\rangle$. By construction, for all $1 \leq j \leq t$

$$\mathbb{Z}[x, y]/\langle \Phi_{d_1}(x), p_j(x, y)\rangle \cong \mathbb{Z}[\zeta_l],$$

which is an integral domain. It is a well-known fact that if A is a commutative ring and I an ideal, then A/I is an integral domain if and only if I is a prime ideal. Thus,

$$\langle \Phi_{d_1}(x), p_j(x, y)\rangle$$

such that $d_1 \mid m$, $d_2 \mid n$, and $1 \leq j \leq t$ are prime ideals of $\mathbb{Z}[x, y]$.

We now wish to show that these prime ideals are minimal. As stated before, we have determined that for all $1 \leq j \leq t$

$$\mathbb{Z}[x, y]/\langle \Phi_{d_1}(x), p_j(x, y)\rangle \cong \mathbb{Z}[\zeta_l].$$

Because $\mathbb{Z}[\zeta_l]$ has Krull dimension one, $\langle \Phi_{d_1}(x), p_j(x,y)\rangle$ has to be a minimal ideal. If not, then the Krull dimension of $\mathbb{Z}[x,y]/\langle \Phi_{d_1}(x), p_j(x,y)\rangle$ would be greater than one, a clear contradiction. Also,

$$\bigcap_{d_1|m, d_2|n} \langle \Phi_{d_1}(x), \Phi_{d_2}(y)\rangle = \langle x^m - 1, y^n - 1\rangle.$$

Putting everything together, we have

$$\bigcap_{d_1 m, d_2|n} (\bigcap_{j=1}^{t} \langle \Phi_{d_1}(x), p_j(x,y)\rangle) = \bigcap_{d_1|m, d_2|n} \langle \Phi_{d_1}(x), \Phi_{d_2}(y)\rangle = \langle x^m - 1, y^n - 1\rangle.$$

This is the kernel of the isomorphism:

$$\theta : \mathbb{Z}[x,y]/\langle x^m - 1, y^n - 1\rangle \longrightarrow \mathbb{Z}[G].$$

Thus, through the correspondence

$$\bigcap_{d_1|m, d_2|n} (\bigcap_{j=1}^{t} \langle \Phi_{d_1}(a), p_j(a,b)\rangle) = \{0\}.$$

Consequently, by application of Lemma 2 from Chapter 3,

$$\langle \Phi_{d_1}(a), p_j(a,b)\rangle$$

such that $d_1 \mid m$, $d_2 \mid n$, and $1 \leq j \leq t$. are exactly the minimal ideals of G.

Q.E.D.

We will now illustrate the algorithm and classify the minimal prime ideals of a specific group.

Example 2

Let $G \cong \mathbb{Z}_8 \times \mathbb{Z}_8 = \{a, b | a^8 = b^8 = 1, aba^{-1} = b\}$. By the previous theorem, we know that the minimal prime ideals of $\mathbb{Z}[G]$ are

$$\langle \Phi_{d_1}(a), p_j(a, b) \rangle$$

such that $d_1 \mid 8$, $d_2 \mid 8$, and $1 \leq j \leq t$. Thus, we will consider all such pairs of (d_1, d_2).

$\mathbf{d_1 = 1, d_2 = 1}$

$\Phi_{d_1}(x) = \Phi_1(x) = x - 1$

$t = \frac{\phi(1)\phi(1)}{\phi(1)} = 1 \Rightarrow p_1(x, y) = y - 1$

Thus, $\langle x - 1, y - 1 \rangle \leftrightarrow \langle a - 1, b - 1 \rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\mathbf{d_1 = 1, d_2 = 2}$

$\Phi_{d_1}(x) = \Phi_1(x) = x - 1$

$t = \frac{\phi(1)\phi(2)}{\phi(2)} = 1 \Rightarrow p_1(x, y) = y + 1$

Thus, $\langle x - 1, y + 1 \rangle \leftrightarrow \langle a - 1, b + 1 \rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\mathbf{d_1 = 1, d_2 = 4}$

$\Phi_{d_1}(x) = \Phi_1(x) = x - 1$

$t = \frac{\phi(1)\phi(4)}{\phi(4)} = 1 \Rightarrow p_1(x, y) = y^2 + 1$

Thus, $\langle x - 1, y^2 + 1 \rangle \leftrightarrow \langle a - 1, b^2 + 1 \rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 1, d_2 = 8}}$

$\Phi_{d_1}(x) = \Phi_1(x) = x - 1$

$t = \frac{\phi(1)\phi(8)}{\phi(8)} = 1 \Rightarrow p_1(x, y) = y^4 + 1$

Thus, $\langle x - 1, y^4 + 1\rangle \leftrightarrow \langle a - 1, b^4 + 1\rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 2, d_2 = 1}}$

$\Phi_{d_1}(x) = \Phi_2(x) = x + 1$

$t = \frac{\phi(2)\phi(1)}{\phi(2)} = 1 \Rightarrow p_1(x, y) = y - 1$

Thus, $\langle x + 1, y - 1\rangle \leftrightarrow \langle a + 1, b - 1\rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 2, d_2 = 2}}$

$\Phi_{d_1}(x) = \Phi_2(x) = x + 1$

$t = \frac{\phi(2)\phi(2)}{\phi(2)} = 1 \Rightarrow p_1(x, y) = y + 1$

Thus, $\langle x + 1, y + 1\rangle \leftrightarrow \langle a + 1, b + 1\rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 2, d_2 = 4}}$

$\Phi_{d_1}(x) = \Phi_2(x) = x + 1$

$t = \frac{\phi(2)\phi(4)}{\phi(4)} = 1 \Rightarrow p_1(x, y) = y^2 + 1$

Thus, $\langle x + 1, y^2 + 1\rangle \leftrightarrow \langle a + 1, b^2 + 1\rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 2, d_2 = 8}}$

$\Phi_{d_1}(x) = \Phi_2(x) = x + 1$

$t = \frac{\phi(2)\phi(8)}{\phi(8)} = 1 \Rightarrow p_1(x,y) = y^4 + 1$

Thus, $\langle x+1, y^4+1 \rangle \leftrightarrow \langle a+1, b^4+1 \rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 4, d_2 = 1}}$

$\Phi_{d_1}(x) = \Phi_4(x) = x^2 + 1$

$t = \frac{\phi(4)\phi(1)}{\phi(4)} = 1 \Rightarrow p_1(x,y) = y - 1$

Thus, $\langle x^2+1, y-1 \rangle \leftrightarrow \langle a^2+1, b-1 \rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 4, d_2 = 2}}$

$\Phi_{d_1}(x) = \Phi_4(x) = x^2 + 1$

$t = \frac{\phi(4)\phi(2)}{\phi(4)} = 1 \Rightarrow p_1(x,y) = y + 1$

Thus, $\langle x^2+1, y+1 \rangle \leftrightarrow \langle a^2+1, b+1 \rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 4, d_2 = 4}}$

In this case, x is acting as the fourth root of unity, i. Thus, we are attempting to factor y^2+1 in $\mathbb{Q}[i]$. Clearly, $y^2+1 = (y-i)(y-i^3)$, and so $y^2+1 \equiv (y-x)(y-x^3) \bmod x^2+1$. Explicitly,

$\Phi_{d_1}(x) = \Phi_4(x) = x^2 + 1$

$t = \frac{\phi(4)\phi(4)}{\phi(4)} = 2 \Rightarrow p_1(x,y) = y - x, p_2(x,y) = y - x^3$

Thus, $\langle x^2+1, y-x \rangle \leftrightarrow \langle a^2+1, b-a \rangle$ and $\langle x^2+1, y-x^3 \rangle \leftrightarrow \langle a^2+1, b-a^3 \rangle$ are minimal prime ideals of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 4, d_2 = 8}}$

$\Phi_{d_1}(x) = \Phi_4(x) = x^2 + 1$

$t = \frac{\phi(4)\phi(8)}{\phi(8)} = 2 \Rightarrow p_1(x,y) = y^2 - x, p_2(x,y) = y^2 - x^3$

Thus, $\langle x^2+1, y^2-x\rangle \leftrightarrow \langle a^2+1, b^2-a\rangle$ and $\langle x^2+1, y^2-x^3\rangle \leftrightarrow \langle a^2+1, b^2-a^3\rangle$ are minimal prime ideals of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 8, d_2 = 1}}$

$\Phi_{d_1}(x) = \Phi_8(x) = x^4 + 1$

$t = \frac{\phi(8)\phi(1)}{\phi(8)} = 1 \Rightarrow p_1(x,y) = y - 1$

Thus, $\langle x^4 + 1, y - 1\rangle \leftrightarrow \langle a^4 + 1, b - 1\rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 8, d_2 = 2}}$

$\Phi_{d_1}(x) = \Phi_8(x) = x^4 + 1$

$t = \frac{\phi(8)\phi(2)}{\phi(8)} = 1 \Rightarrow p_1(x,y) = y + 1$

Thus, $\langle x^4 + 1, y + 1\rangle \leftrightarrow \langle a^4 + 1, b + 1\rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 8, d_2 = 4}}$

$\Phi_{d_1}(x) = \Phi_8(x) = x^4 + 1$

$t = \frac{\phi(8)\phi(4)}{\phi(8)} = 2 \Rightarrow p_1(x,y) = y - x^2, p_2(x,y) = y - x^6$

Thus, $\langle x^4+1, y-x^2\rangle \leftrightarrow \langle a^4+1, b-a^2\rangle$ and $\langle x^4+1, y-x^6\rangle \leftrightarrow \langle a^4+1, b-a^6\rangle$ are minimal prime ideals of $\mathbb{Z}[G]$.

$\underline{\mathbf{d_1 = 8, d_2 = 8}}$

$\Phi_{d_1}(x) = \Phi_8(x) = x^4 + 1$

$t = \frac{\phi(8)\phi(8)}{\phi(8)} = 4 \Rightarrow p_1(x, y) = y - x, p_2(x, y) = y - x^3, p_3(x, y) = y - x^5, p_4(x, y) = y - x^7$

Thus, $\langle x^4 + 1, y - x\rangle \leftrightarrow \langle a^4 + 1, b - a\rangle$, $\langle x^4 + 1, y - x^3\rangle \leftrightarrow \langle a^4 + 1, b - a^3\rangle$, $\langle x^4 + 1, y - x^5\rangle \leftrightarrow \langle a^4 + 1, b - a^5\rangle$, and $\langle x^4 + 1, y - x^7\rangle \leftrightarrow \langle a^4 + 1, b - a^7\rangle$ are minimal prime ideals of $\mathbb{Z}[G]$.

We note that we have many symmetric cases; clearly $\langle \Phi_{d_1}(a), \Phi_{d_2}(b)\rangle$ and $\langle \Phi_{d_2}(b), \Phi_{d_1}(a)\rangle$ should give the same answer. This was indeed obvious in the above example for all cases except when $\{d_1, d_2\} = \{4, 8\}$ where we got

$$\langle \Phi_4(a), \Phi_8(b)\rangle = \langle a^2 + 1, b^2 - a\rangle \cap \langle a^2 + 1, b^2 - a^3\rangle$$

the first time we looked at 4 and 8, and after interchanging a and b we got

$$\langle \Phi_8(b), \Phi_4(a)\rangle = \langle b^4 + 1, a - b^2\rangle \cap \langle b^4 + 1, a - b^6\rangle$$

the second time we looked at 4 and 8. But one can readily check that

$$\langle a^2 + 1, b^2 - a\rangle = \langle b^4 + 1, a - b^2\rangle \text{ and}$$

$$\langle a^2 + 1, b^2 - a^3\rangle = \langle b^4 + 1, a - b^6\rangle.$$

Having run through all pairs (d_1, d_2), we have found the 22 minimal prime ideals of $\mathbb{Z}[G]$, where $G \cong \mathbb{Z}_8 \times \mathbb{Z}_8$.

Chapter 5

Maximal Primes in $\mathbb{Z}[G]$

Now that we have classified all the minimal prime ideals of $\mathbb{Z}[G]$ where G has two generators, we would like to be able to do the same with the maximal ideals of $\mathbb{Z}[G]$. We note that in any ring, all maximal ideals are prime. We chose to determine the minimal prime ideals first because they will play an important role in the classifiction of the maximal ideals. Several facts about maximal ideals follow.

Lemma 4. *Every maximal ideal contains a minimal prime ideal.*

Proof: In Theorem 3, we showed that every prime ideal contains a minimal prime ideal. Because a maximal ideal is prime, we immediately get our result.

Q.E.D.

Proposition 6. *Let M be a maximal ideal in $\mathbb{Z}[G]$. Then M contains a unique prime integer.*

Proof: Define the quotient map

$$\theta : \mathbb{Z}[G] \twoheadrightarrow \mathbb{Z}[G]/M$$

via $u \mapsto u + M$. It is clear that there exists an embedding of $\mathbb{Z}$ into $\mathbb{Z}[G]$. Because M is a prime ideal, it is sufficient to find any nonzero integer in M since then one of its prime factors would be in M. By way of contradiction, assume M contains no such integer. Then we claim the restriction of θ to $\mathbb{Z}$ is an injective function:

$$\theta_{\mathbb{Z}} : \mathbb{Z} \longrightarrow \mathbb{Z}[G]/M$$

$$z \mapsto z + M.$$

Assume $\theta_{\mathbb{Z}}(z_1) = \theta_{\mathbb{Z}}(z_2)$ for $z_1 \neq z_2$. Then $z_1 + M = z_2 + M$, which occurs if and only if $z_1 - z_2 \in M$. However, $z_1 - z_2$ is an integer, which would contradict the assumption that M contains no nonzero integers. Therefore, $z_1 = z_2$, which shows $\theta_{\mathbb{Z}}$ is injective. Hence, $\mathbb{Z} \hookrightarrow \mathbb{Z}[G]/M$. Because M is a maximal ideal, $\mathbb{Z}[G]/M$ is a field, which implies that it contains an isomorphic copy of $\mathbb{Q}$. But we know that $\mathbb{Z}[G]/M$ is a finitely generated abelian group. Hence, $\mathbb{Z}[G]/M$ cannot contain a copy of $\mathbb{Q}$, and so we have reached a contradiction. Thus, M must contain a nonzero integer, as desired.

To prove uniqueness, assume there exists another prime
$q' \in M$. Then, $\gcd(q, q') = 1$. By the division algorithm, there exists $r, s \in \mathbb{Z}$ such that $1 = rq + sq'$. Because M is an ideal, $1 = rq + sq' \in M$, which implies that M is the entire ring, a contradiction. Hence, q is unique.

Q.E.D.

Let M be a maximal ideal of $\mathbb{Z}[G]$. By previous work, M must contain a minimal prime ideal, say μ. Recall that we are considering $G = \langle a, b \mid a^m = b^n = 1, aba^{-1} = b\rangle \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Previous work shows that all minimal prime ideals of $\mathbb{Z}[G]$ are then of the form $\mu = \langle \Phi_{d_1}(a), p_j(a, b)\rangle \subseteq M$, where d_1 is a divisor of m and p_j

is an irreducible factor of $\Phi_{d_2}(y)$ such that $d_2|n$ over $\mathbb{Z}[\zeta_{d_1}]$. Now let q be the prime belonging to M as we got in Proposition 3. Define $I := \langle q, \Phi_{d_1}(a), p_j(a,b)\rangle \subseteq M$. By the Third Isomorphism Theorem, we have

$$\mathbb{Z}[G]/I \cong \mathbb{Z}[G]/q\mathbb{Z}[\zeta_l]/I/q\mathbb{Z}[\zeta_l] \cong \mathbb{Z}[\zeta_l]/q\mathbb{Z}[\zeta_l].$$

Thus, there is a one-to-one correspondence between ideals in $\mathbb{Z}[\zeta_l]/q\mathbb{Z}[\zeta_l]$ and $\mathbb{Z}[G]/I$.

We note that in $\mathbb{Z}[\zeta_l]$ we can factor

$$q\mathbb{Z}[\zeta_l] = Q_1^e Q_2^e \cdots Q_r^e,$$

where each Q_i is a prime ideal in $\mathbb{Z}[\zeta_l]$ and $e \geq 1$ [5]. Lift each Q_i back to M_i in $\mathbb{Z}[G]$. We observe

$$M_i \supseteq I \text{ for every } i$$

and

$$\mathbb{Z}[\zeta_l]/Q_i \text{ is a field.}$$

Thus, each M_i is maximal because

$$\mathbb{Z}[G]/M_i \cong Z[\zeta_l]/Q_i, \text{ which is a field.}$$

Theorem 4. *All the maximal ideals of $\mathbb{Z}[G]$ are attained as follows:*

1. *choose a minimal prime idealof $\mathbb{Z}[G]$ $\langle \Phi_{d_1}(a), p_j(a,b)\rangle$ as described in Theorem 3*

2. *choose any prime integer q of $\mathbb{Z}$*

3. *for $l = lcm(d_1, d_2)$ (see Theorem 3), let Q_i be a factor of q in $\mathbb{Z}[\zeta_l]$ as above*

4. in the isomorphism $\mathbb{Z}[G]/I \equiv \mathbb{Z}[\zeta_l]/q\mathbb{Z}[\zeta_l]$ lift Q_i to a maximal ideal M_i of $\mathbb{Z}[G]$.

Then these M_i as q ranges through primes of $\mathbb{Z}$, $\langle \Phi_{d_1}(a), p_j(a,b)\rangle$ range through all minimal primes of $\mathbb{Z}[G]$, and Q_i range through factors of $q\mathbb{Z}[\zeta_l]$ are all the maximal ideals of $\mathbb{Z}[G]$.S

We make a very important observation: these maximal ideals are not necessarily distinct, as we will see for cyclic groups in Chapter 6.

We will explore maximal ideals more explicitly for cyclic groups in the next section.

Chapter 6

Application to Cyclic Groups

In this section we will assume $G \cong \mathbb{Z}_n$, a finite cyclic group of order n. Applying work from previous sections with $m = 1$, we have

Proposition 7. *Given* $G = \langle a \rangle \cong \mathbb{Z}_n$,

$$\mathbb{Z}[G] \cong \mathbb{Z}[x]/\langle x^n - 1\rangle = \mathbb{Z}[x]/\bigcap_{d|n}\langle \Phi_d(x)\rangle$$

and

$$\langle x^n - 1\rangle = \bigcap_{d|n}\langle \Phi_d(x)\rangle.$$

Proof: This result follows immediately from application of Theorem 1 and Proposition 4, from Section 2 and Section 4, respectively.

Q.E.D.

We note that there is a clear correspondence between the generator, a, of G and the variable x. Thus, we arrive at the following:

Theorem 5. *Let* $G = \langle a \rangle \cong \mathbb{Z}_n$. *Then the minimal prime ideals of* $\mathbb{Z}[G]$ *are exactly the set* $\langle \Phi_d(a)\rangle$, *where* $d \mid n$. *Moreover, these ideals are all different.*

Proof: By work from Section 4, it is clear that $\mathbb{Z}[G]/\langle \Phi_d(a)\rangle \cong \mathbb{Z}[\zeta_d]$, which is an integral domain. Thus, $\langle \Phi_d(a)\rangle$ is a prime ideal. Furthermore, the Krull dimension of of $\mathbb{Z}[\zeta_d]$ is one, which implies that $\langle \Phi_d(a) \rangle$ is a minimal prime ideal of $\mathbb{Z}[G]$ for all $d \mid n$.

Because

$$\langle x^n - 1 \rangle = \prod\nolimits_{d|n} \langle \Phi_d(x) \rangle = \bigcap_{d|n} \langle \Phi_d(x) \rangle,$$

and using the fact that we have correspondence between the presentation element a and the variable x, we have

$$\bigcap_{d|n} \langle \Phi_d(a) \rangle = \{0\}.$$

Thus, by application of Lemma 2 in Section 3, the $\langle \Phi_d(a) \rangle$ for all $d \mid n$ are exactly the minimal prime ideals of $\mathbb{Z}[G]$.

For every $d, b \mid n$ such that $b \neq d$, we have that $\langle \Phi_d(a) \rangle$ and $\langle \Phi_b(a) \rangle$ are relatively prime. Thus, there exist $f(x)$ and $g(x)$ both in $\mathbb{Q}[x]$ such that

$$f(x)\Phi_d(x) + g(x)\Phi(x) = 1.$$

Thus, over $\mathbb{Z}$, we have

$$f'(x)\Phi_d(x) + g'(x)\Phi(x) = z,$$

where $f'(x)$, $g'(x)$ are the functions that result when we clear denominators of $f(x)$, $g(x)$, and $z \in \mathbb{Z}$. If

$$\langle \Phi_d(a) \rangle = \langle \Phi_b(a) \rangle,$$

then $z \in \langle \Phi_d(a) \rangle$, which is a contradiction. Thus, the ideals are each distinct.

Q.E.D.

Now we turn our attention to the maximal ideals of $\mathbb{Z}[G]$, with $G = \langle a \rangle \cong \mathbb{Z}_n$.

As shown in the previous sections, each maximal ideal contains a unique prime integer, q. For a given $d \mid n$, we can factor

$$q\mathbb{Z}[\zeta_d] = Q_1^e Q_2^e \cdots Q_r^e$$

where the Q_j are distinct primes in $\mathbb{Z}[\zeta_d]$. We also have the map

$$\pi : \mathbb{Z}[G] \to \mathbb{Z}[G]/\langle \Phi_d(a) \rangle \cong \mathbb{Z}[\zeta_d]$$

via $a \mapsto \zeta_d$. Indeed if $\Phi_d(x) \equiv g_1(x)^e \cdots g_r(x)^e \bmod q$ such that $g_j(x)$ is irreducible mod$q$, then

$$Q_j = \langle q, g_j(\zeta_d) \rangle.$$

Define $M_{1dq}, M_{2dq}, \cdots, M_{rdq}$ to be the inverse images of $Q_1, Q_2, \cdots, Q_r$, respectively in $\mathbb{Z}[G]$. Thus,

$$M_{jdq} = \langle q, g_j(a), \Phi_d(a) \rangle = \langle q, g_j(a) \rangle.$$

Then a more explicit version of Theorem 4 in Chapter 5 can be given.

Theorem 6. *The maximal ideals of $\mathbb{Z}[G]$ are exactly the set M_{jdq}, where q is a prime of $\mathbb{Z}$, $1 \leq j \leq r$, and $d \mid n$.*

Proof: We know $M_{jdq} \cap \mathbb{Z} = q\mathbb{Z}$ and $\mathbb{Z}[G]/M_{jdq} \cong \mathbb{Z}[\zeta_d]/Q_j$, which is a field. Thus, M_{jdq} are maximal ideals of $\mathbb{Z}[G]$ for all q prime, $1 \leq j \leq r$, and $d \mid n$.

Conversely, let M be a maximal ideal of $\mathbb{Z}[G]$. Also, let q be the unique prime integer contained in M, i.e. $q\mathbb{Z} = M \cap \mathbb{Z}$. Because all minimal prime ideals of $\mathbb{Z}[G]$ are of the form $\langle \Phi_d(a) \rangle$, where $d \mid n$, and every prime ideal contains a minimal prime ideal, we know there exists $d \mid n$ such that $\Phi_d(a) \in M$. Thus, $M_{jdq} = \langle q, \Phi_d(a) \rangle \subseteq M$. By the maximality of M_{jdq}, we may conclude that $M_{jdq} = M$.

Hence, the set of maximal ideals of $\mathbb{Z}[G]$ are exactly given by M_{jdq}, where q is a prime of $\mathbb{Z}$, $1 \leq j \leq r$, and $d \mid n$.

Q.E.D.

As mentioned in the last section, these maximal ideals are not necessarily distinct. In fact we shall show that it is possible to have $M_{jdq} = M_{jd'q}$ for $d \neq d'$, both divisors of n. We would like to know when such a situation occurs. We make the following observation:

Theorem 7. *If $q \nmid n$, then M_{jdq} contains a unique minimal prime ideal.*

Proof: Because $q \nmid n$, $x^n - 1$ has n distinct roots in its splitting field over $\mathbb{Z}/q\mathbb{Z}$. By way of contradiction, suppose there exists $e \mid n$ such that $e \neq d$ and $\Phi_e(a) \in M_{jdq}$. Then $\gcd(\Phi_d(x), \Phi_e(x)) \equiv 1 \bmod q$. By the division algorithm, there exists $f(x), g(x), h(x) \in \mathbb{Z}[x]$ such that

$$f(x)\Phi_e(x) + g(x)\Phi_d(x) = 1 + qh(x).$$

This implies that $1 \in M_{jdq}$, which is a contradiction. Thus, $d = e$, and we have only one minimal prime ideal.

Q.E.D.

Now consider the case where $q \mid n$. We focus on the minimal primes $\langle \Phi_d(a) \rangle$ for $d \mid n$. If $q \mid d$, then we will compare $\langle \Phi_d(a) \rangle$ and $\langle \Phi_b(a) \rangle$ such that $d = qb$. If $q \nmid d$, we compare $\langle\Phi_d(a)\rangle$ and $\langle\Phi_{qd}(a)\rangle$, which is valid because $qd \mid n$. In both cases we will show that there exist maximal ideals containing both of these minimal prime ideals. Indeed we will show $M_{jdq} = M_{jbq}$ if the former situation holds and thus, as a direct application we get $M_{jcq} = M_{jdq}$, where $qd = c$ if the later situation holds.

Assume $d = qb$. For simplicity we only consider the case where $q \nmid b$. Then we know by Proposition 13.2.5 in [2] that

$$q\mathbb{Z}[\zeta_b] = Q_1Q_2\cdots Q_r$$

for distinct primes $Q_1, Q_2, \ldots, Q_r$, and by Proposition 13.2.9

$$q\mathbb{Z}[\zeta_d] = \mathcal{Q}_1^{q-1}\mathcal{Q}_2^{q-1}\cdots\mathcal{Q}_r^{q-1}[2],$$

where $\mathcal{Q}_j$ lies over Q_j for $1 \leq j \leq t$, i.e. $Q_j\mathbb{Z}[\zeta_d] = \mathcal{Q}_j^{q-1}$.

These ideals give rise to maximal ideals M_{jbq} and M_{jdq} in $\mathbb{Z}[G]$ as discussed in Theorem 6. Because the $Q_1, Q_2, \ldots, Q_r$ are pairwise comaximal and $\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_r$ are pairwise comaximal as well, we have that $M_{ibq} \neq M_{jbq}$ and $M_{idq} \neq M_{jdq}$ for all $i \neq j$.

Theorem 8. *For $1 \leq j \leq t$ and $d = qb$, $q \nmid b$, we have $M_{jbq} = M_{jdq}$.*

Proof: Define

$$\pi_b : \mathbb{Z}[G]/\langle\Phi_b(a)\rangle \xrightarrow{\cong} \mathbb{Z}[\zeta_b]$$

via $a \mapsto \zeta_b$. So Q_j lifts back to an ideal in $\mathbb{Z}[G]$ we have denoted by M_{jbq}. Say

$$\langle\Phi_b(x)\rangle \equiv f_1(x)f_2(x)\cdots f_r(x) \bmod q,$$

where $f_j(x)$ is irreducible mod$q$ for all $1 \leq j \leq r$. Then, $Q_j = \langle q, f_j(\zeta_b)\rangle$, [5] and so

$$M_{jbq} = \langle q, f_j(a), \Phi_b(a)\rangle = \langle q, f_j(a)\rangle.$$

Because

$$q\mathbb{Z}[\zeta_d] = \mathcal{Q}_1^{q-1}\mathcal{Q}_2^{q-1}\cdots\mathcal{Q}_r^{q-1},$$

we have

$$\Phi_d(x) \equiv \Phi_b(x)^{q-1} \equiv f_1(x)^{q-1}f_2(x)^{q-1}\cdots f_r(x)^{q-1} \bmod q.$$

Thus, $\mathcal{Q}_j = \langle q, f_j(\zeta_d)\rangle$, which implies that

$$M_{jdq} = \langle q, f_j(a), \Phi_d(a)\rangle = \langle q, f_j(a)\rangle = M_{jbq}.$$

Q.E.D.

Now we have recovered a special result in *Structure of Witt rings and quotients of Abelian group rings* by Knebusch, Rosenberg, and Ware: the only maximal ideals that contain more than one minimal prime ideal are those that contain a prime dividing the order of the group.

We will illustrate this work using the example of $G = \langle a\rangle \cong \mathbb{Z}_6$.

The minimal prime ideals of $\mathbb{Z}[G]$ are the following:

$$\langle\Phi_1(a)\rangle = \langle a-1\rangle,$$

$$\langle\Phi_2(a)\rangle = \langle a+1\rangle,$$

$$\langle\Phi_3(a)\rangle = \langle a^2+a+1\rangle,$$

and

$$\langle\Phi_6(a)\rangle = \langle a^2-a+1\rangle.$$

We will now consider the maximal ideals of $G = \langle a \rangle \cong \mathbb{Z}_6$. By Theorem 7 and Theorem8, we know that M_{jdq} are distinct for all primes $q > 3$. The only primes of concern then are 2 and 3 because they divide the order of our group, and thus lead to non-distinct M_{jdq}.

Let's consider $q = 3$.

If $d = 1$, then we produce only $M_{113} = \langle 3, a - 1 \rangle$.

If $d = 2$, then we produce only $M_{123} = \langle 3, a + 1 \rangle$.

If $d = 3$, then 3 factors in $\mathbb{Z}[\zeta_3]$. This corresponds to $d = 3$, $b = 1$ in Theorem 8. Explicitly, $3 = (1 + \zeta_3)(\zeta_3 - 1)^2$, where $1 + \zeta_3$ is a unit in $\mathbb{Z}[\zeta_3]$. Thus, $3\mathbb{Z}[\zeta_3] = Q_1^2$ such that $Q_1 = \langle \zeta_3 - 1 \rangle$, $(r = 1)$. Therefore, $3 \equiv (a + 1)(a - 1)^2 \bmod a^2 + a + 1$. So we have $M_{133} = \langle a - 1, a^2 + a + 1 \rangle$. We observe that

$$(a^2 + a + 1)(a - 2) - (a + 1)(a - 1)^2 = 3,$$

which implies that $\langle 3, a - 1 \rangle \subseteq \langle a - 1, a^2 + a + 1 \rangle$. We also note that

$$(a - 1)(a - 1) + 3a = a^2 + a + 1,$$

which implies that $\langle 3, a - 1 \rangle \supseteq \langle a - 1, a^2 + a + 1 \rangle$. Consequently,

$$M_{113} = \langle 3, a - 1 \rangle = \langle a - 1, a^2 + a + 1 \rangle = M_{133},$$

which confirms our Theorem 8.

If $d = 6$, then 3 factors in $\mathbb{Z}[\zeta_6] = \mathbb{Z}[-\zeta_3]$. This corresponds to $d = 6$, $b = 2$ in Theorem 8. Explicitly, $3 = (\zeta_6 - 1)(1 + \zeta_6)^2$, where $Q_1 = \langle 1 + \zeta_3 \rangle$ $(r = 1)$. Therefore, $3 \equiv (a - 1)(a + 1)^2 \bmod a^2 - a + 1$. So we have $M_{163} = \langle a + 1, a^2 - a + 1 \rangle$. We observe that

$$(a^2 - a + 1)(a + 2) - (a - 1)(a + 1)^2 = 3,$$

which implies that $\langle 3, a + 1 \rangle \subseteq \langle a + 1, a^2 - a + 1 \rangle$. We also note that

$$(a + 1)(a + 1) - 3a = a^2 - a + 1,$$

which implies that $\langle 3, a + 1 \rangle \supseteq \langle a + 1, a^2 - a + 1 \rangle$.Consequently,

$$M_{123} = \langle 3, a + 1 \rangle = \langle a + 1, a^2 - a + 1 \rangle = M_{163},$$

which confirms Theorem 8 because $3 \mid 6$.

We can do similarly for $d = 2$.

BIBLIOGRAPHY

[1] D.S. Dummit and R.M. Foote, *Abstract Algebra* (John Wiley & Sons, Inc., New York, 1999).

[2] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Springer-Verlag, New York, 1990).

[3] G. Karpilovsky, *Commutative Group Algebras* (Marcel Dekker, Inc., New York, 1983).

[4] M. Knebusch, A. Rosenberg, R. Ware, ”Structure of Witt rings and quotients of Abelian group rings,” American Journal of Mathematics **94**, 119-155 (1972).

[5] S. Lang, *Algebraic Number Theory* (Addison-Wesley, Reading, MA, 1970).

[6] M. Reid, *Undergraduate Commutative Algebra* (Cambridge University Press, Cambridge, UK, 1995).

[7] J.J. Rotman, *Advanced Modern Algebra* (Pearson Education, Inc., Upper Saddle, NJ, 2002).

[8] R.Y. Sharp, *Steps in Commutative Algebra* (Cambridge University Press, Cambridge, UK, 1990).