Chapter 3

FINITE COMMUTATIVE RINGS. REGULAR POLYNOMIALS

In this chapter we want to analyze the structure of finite, commutative rings with identity. We shall prove that any such ring can be uniquely expressed as a direct sum of finite local rings.

Next, we shall study the polynomial ring $R[x]$, where $R$ is a local ring with maximal ideal $M$ and residue field $K = R/M$; our attention will be focused to particular polynomials, the so called regular polynomials. They will play a fundamental role in Galois ring theory.

3.1 Finite Commutative Ring Structure

All through this chapter, $R$ will denote a finite, commutative ring with identity. Local rings were defined in 1.2.9. Here it will be shown they are the "bricks" of the whole theory of finite, commutative rings with identity. The main ideas of this section follow [56].

Let $I_1, I_2, \ldots, I_n$ be proper ideals of a ring $R$; $I_j$ and $I_k$, $1 \leq j \neq k \leq n$, are said to be relatively prime ideals if $I_j + I_k = R$, where

$$ I_j + I_k := \{a + b \mid a \in I_j \land b \in I_k\}. $$

Consider the ring homomorphism

$$ \Phi : R \longrightarrow R/I_1 \oplus \cdots \oplus R/I_n. $$

(3.1)
such that
\[ \Phi(r) := (r + I_1, \ldots, r + I_n), \]
for each \( r \in R \).

**Proposition 3.1.1** Let \( R \) be a finite, commutative ring with identity.

1. If \( I_j \) and \( I_k \), \( 1 \leq j \neq k \leq n \), are relatively prime ideals of \( R \), then
   \[
   \bigcap_{j=1}^{n} I_j = \prod_{j=1}^{n} I_j,
   \]
   where \( \prod_{j=1}^{n} I_j := \{ \sum_{i} x_i^1 \cdots x_i^j \cdots x_i^n \mid x_i^j \in I_j, \ 1 \leq j \leq n \} \).

2. If \( I_j \) and \( I_k \) are relatively prime, so are \( I_j^m \) and \( I_k^m \), for all \( m \in \mathbb{N} \).
   (Recall that, if \( J \) is an ideal of \( R \), \( J^m \) is its \( m \)-th power, i.e. the ideal generated by the elements \( x_1 \cdots x_m \), where \( x_k \in J, 1 \leq k \leq m \).)

3. The ring homomorphism \( \Phi \) in (3.1) is injective if and only if
   \[ \bigcap_{j=1}^{n} I_j = 0. \]

4. The ring homomorphism \( \Phi \) is surjective if and only if \( I_j \) and \( I_k \) are relatively prime, \( 1 \leq j \neq k \leq n \).

**Proof:**

1. We prove the statement in the case of two ideals and then use induction on their number. If \( I_1, I_2 \) are relatively prime ideals of \( R \), then
   \[ I_1 \cap I_2 = \{ h \in R \mid h \in I_1 \land h \in I_2 \} \]
   is a proper ideal of \( R \). Similarly, \( I_1I_2 \) is a proper ideal of \( R \), such that
   \[ I_1I_2 = \{ \sum_{i} x_i y_i \mid x_i \in I_1, y_i \in I_2 \}. \]
   The trivial inclusion is \( I_1I_2 \subseteq I_1 \cap I_2 \). (Note that, in general this is a proper inclusion; in fact, if we take, for example, \( R = \mathbb{Z} \) and \( I_1 = (6) \), \( I_2 = (10) \) then \( (60) = I_1I_2 \subset I_1 \cap I_2 = (30) \).)
   For the converse, since \( I_1 \) and \( I_2 \) are relatively prime, there exist \( x \in I_1 \) and \( y \in I_2 \) such that \( 1 = x + y \). So, if \( r \in I_1 \cap I_2 \), then
   \[ r = r \cdot 1 = r \cdot x + r \cdot y \in I_1I_2. \]
   Observe that this is a generalization of what occurs in the ring of integers, when we consider proper ideals \( (m) \) and \( (n) \), with \( m \) and \( n \) relatively prime integers.