In this chapter we firstly want to analyze the structure of Galois rings which are, in our terminology, Galois extensions of local rings of the form $\mathbb{Z}_{p^n}$, where $p$ is a prime and $n$ a positive integer. The importance of such rings is mainly due to the following facts:

1. In some problems of Combinatorics one deals with finite fields and, at the same time, with local rings of the form $\mathbb{Z}_{p^n}$; the two objects obviously share very few properties. Galois rings constitute the common "point of view" of these clearly so different families;

2. As already said in the previous chapters, Galois rings can be viewed as "bricks" of all of Finite Commutative Algebra; indeed, in Section 3 of this chapter we will show that each finite, commutative ring can be considered as a suitable algebra over a fixed Galois ring.

At the end of this chapter, we will focus on another class of finite, local rings. Such rings will be called Quasi-Galois rings since, as we shall show, the expressions of their elements are very similar to those of Galois ring elements. On the other hand, the properties of such rings are very different from those of Galois rings. In fact, it suffices to notice that the Galois ring $GR(p^n,r)$ is a finite, commutative, local ring of cardinality $p^{nr}$ and characteristic $p^n$, whereas the Quasi-Galois ring $A(p^r,n) := \mathbb{F}_{p^r}[x]/(x^n)$ is a finite, commutative, local ring with the same
cardinality but of characteristic \( p \) (\( p \) a prime), since it contains \( \mathbb{F}_{p^r} \) as a subring.

Quasi-Galois rings are very interesting especially from the application point of view (e.g. Coding Theory or Finite Geometry) since they have the nicer property of having a prime characteristic.

### 6.1 Classical Constructions

This section is a survey of the main classical approaches to the study of Galois rings, which we will denote by \( GR(p^n, r) \), where \( p \) is a prime and \( n, r \) are positive integers.

Some trivial examples are the following:

(i) if \( n = 1 \), we are considering the Galois extension of degree \( r \) of the field \( \mathbb{Z}_p \cong \mathbb{F}_p \); hence,

\[
GR(p, r) = GF(p^r) = \mathbb{F}_{p^r};
\]

(ii) if \( r = 1 \), then \( GR(p^n, 1) = \mathbb{Z}_{p^n} \).

The existence of Galois rings was already known to Krull in 1924 [47] but it was only after more than fourth years that Janusz ([38], 1966) and Raghavendran ([63], 1969) independently rediscovered and studied the properties of such rings. By taking into account what we proved about Galois extensions of local rings, \( GR(p^n, r) \) is isomorphic to the quotient ring \( \mathbb{Z}_{p^n}[x]/(f(x)) \), where \( f(x) \in \mathbb{Z}_{p^n}[x] \) is a monic, basic irreducible polynomial of degree \( r \) (see Def. 3.2.12, Theorem 4.3.1 and Theorem 5.1.6). These theorems also show that this construction is well-defined.

Equivalently, if \( f(x) \in \mathbb{Z}[x] \) is a monic polynomial, of degree \( r \), which is irreducible modulo \( (p) = p\mathbb{Z} \), then \( GR(p^n, r) \cong \mathbb{Z}[x]/(p^n, f(x)) \). This ring is local and its unique maximal ideal is the principal ideal \( pGR(p^n, r) \). More precisely, we will observe in the next section that each ideal of this local ring is principal of the form \( (p^i) = p^iGR(p^n, r) \), with \( 0 \leq i \leq n \).

We can also give explicit representations of the elements of such a ring. By taking into account the notation and what we have proved in Theorem 1.4.4, let \( \xi \) be a root of the unique monic, basic irreducible polynomial \( h_n(x) \in \mathbb{Z}_{p^n}[x] \) related to the primitive polynomial \( h_1(x) \in \mathbb{Z}_p[x] \), which is used to construct the Galois field \( GF(p^r) \cong \mathbb{Z}_p[x]/(h_1(x)) \), \( r = \text{deg}(h_1(x)) \) (we remark that, in this context, the word "primitive" is used in the sense of Definition 2.2.7). Since \( h_n(x) \) divides \( x^k - 1 \) in