Chapter 5

GALOIS THEORY FOR LOCAL RINGS

In this chapter we want to extend some classical results of the Galois theory of fields to finite, local rings. For general ideas on Galois theory and related topics (Abel-Ruffini's Theorem, cyclotomic extensions and so on) the reader is referred to [2], [24] or [64]. For interesting examples and a historical point of view of this theory we suggest [22] and [68].

5.1 Basic Facts

Let $R$ and $S$ be two finite, commutative, local rings such that $R \subset S$. In this situation, we can generalize to the ring case the definition of $K$-morphism given in Section 4.1.

Definition 5.1.1 An $R$-automorphism $\varphi$ of $S$ is an automorphism $\varphi : S \to S$ such that $\varphi|_R = 1_R$, where $1_R$ is the identity map on $R$.

From now on, $S$ and $R$ will denote two finite, commutative, local rings with maximal ideals $M$ and $m$ and residue fields $K = S/M$ and $\mathcal{K} = R/m$, respectively.

We recall that, if $H$ is a group of $R$-automorphisms of $S$, then the set

$$S^H := \{ s \in S \mid \sigma(s) = s, \ \forall \sigma \in H \}$$

is a ring with respect to the operations on $S$. Therefore, if $S$ is an extension of $R$, it makes sense to give the following definition.
Definition 5.1.2 S is a Galois extension of R, with Galois group G, if G is a group of R-automorphisms of S such that
(i) $S^G = R$;
(ii) $S$ is a separable extension of $R$.

In the remaining part of this section we describe the basic tools to construct Galois extensions of rings, whereas in Section 5.2 some important examples and some related questions will be dealt with.

Lemma 5.1.3 Let $f(x)$ be a regular polynomial in $R[x]$ and suppose that $\mu(f(x))$ has a simple root $\bar{\alpha}$ in $K$, where $\mu$ is again the epimorphism $\mu : R \to K$. Then $f(x)$ admits one and only one root $\alpha$ in $R$, s.t. $\mu(\alpha) = \bar{\alpha}$.

Proof: By hypothesis, $\mu(f(x)) = (x - \alpha)\overline{h}(x)$, with $\overline{h}(x) \in K[x]$. By Hensel's Lemma 3.2.6,

$$f(x) = (x - \alpha + g_1(x))(h(x) + g_2(x)),$$

where $g_1(x), g_2(x) \in m[x]$ and $\mu(h(x)) = \overline{h}(x)$. If $g_1(x) = a_nx^n + \ldots + a_0$, with $a_i \in m$, then

$$x - \alpha + g_1(x) = a_nx^n + \ldots + a_2x^2 + (a_1 + 1)x + (a_0 - \alpha).$$

By Theorem 3.2.8, there exists an invertible element $e(x)$ in $R[x]$ such that

$$x - \alpha + g_1(x) = e(x)(x - \beta)$$

with $\beta \in R$ and $\mu(\beta) = \overline{\alpha} = \mu(\alpha)$. Therefore, $f(x) = e(x)(x - \beta)(h(x) + g_2(x))$ and $\beta$ is the desired root. If $\beta'$ were another root of $f(x)$ such that $\mu(\beta') = \overline{\alpha}$, then we would have

$$0 = f(\beta') = (\beta' - \beta)g(\beta'),$$

with $g(x) = (h(x) + g_2(x))e(x)$.

On the other hand, $\mu(g(\beta')) = \overline{h}(\overline{\alpha}) \neq 0$, since $\overline{\alpha}$ is a simple root of $f(x)$. Therefore, $g(\beta')$ is a unit and $\beta' = \beta$. \qed

Now, we want to consider the "lifting" theorem which allows to extend automorphisms of $R$ to $R$-automorphisms of $S$. This is a generalization of what occurs in the Galois theory of fields ([7], [22] or [44]).