CHAPTER 3
THE GALOIS THEORY OF PRIME RINGS

The contribution of the Galois theory for a class of rings is commonly understood as a proof of the principal correspondence theorem of definite types of finite (or reduced-finite) groups of automorphisms and those of subrings from a given class.

Let $R$ be a ring, $S$ a subring and $G$ a group of automorphisms (i.e., a subgroup of the group of all automorphisms) of the ring $R$. An element $a \in R$ is called $G$-invariant if $a^g = a$ for every $g \in G$. A set of all $G$-invariants is denoted by $R^G$ or by $\mathcal{I}(G)$. A set of all automorphisms for which the elements of $S$ serve as invariants is denoted by $A(S)$. It is evident that $\mathcal{I}(G)$ is a subring of the ring $R$, and $A(S)$ is a group of automorphisms.

As was the case in the classical theory of fields, the group $A(S)$ is called a Galois group of the ring $R$ over $S$. A subring $S$ is called a Galois subring of $R$, and $R$ is, respectively, a Galois extension of the ring $S$, if $S = \mathcal{I}(G)$ for a group of automorphisms $G$.

The correspondences $G \rightarrow \mathcal{I}(G)$ and $S \rightarrow A(S)$ invert the inclusion relations, i.e., if $G_1 \subseteq G_2$, then $\mathcal{I}(G_1) \supseteq \mathcal{I}(G_2)$ and if $S_1 \subseteq S_2$, then $A(S_1) \supseteq A(S_2)$. We also have

$$A(\mathcal{I}(G)) \supseteq G, \mathcal{I}(A(S)) \supseteq S,$$

which immediately yield

$$\mathcal{I}(A(\mathcal{I}(G))) = \mathcal{I}(G), A(\mathcal{I}(A(S))) = A(S).$$

Therefore, the mappings under discussion set a one-to-one correspondence between Galois groups and Galois subrings. And, hence, the groups $A(S)$ and the subrings $\mathcal{I}(G)$ are of primary interest in the Galois theory.

In order to prove the correspondence theorem in a class of rings $\mathfrak{N}$,
it is necessary (and sufficient) to answer the following questions:

1. Under what conditions does a subring of fixed elements for a group $G$ of automorphisms of a ring $R \in \mathfrak{R}$ belong to $\mathfrak{R}$?
2. When will a group $G$ which obeys condition (1), be a Galois group?
3. Under what conditions is an intermediate ring $S \in \mathfrak{R}$, $l(G) \subseteq S \subseteq R$ a Galois subring?

An analogous approach is also possible for studying derivations. In this case the role of Galois objects is played by differential (restricted) Lie $\mathfrak{g}$-algebras and the subrings of constants of such algebras. In this case the same problems as for groups, i.e., (1) - (3) arise.

In the three chapters to follow we are going to develop the Galois theory for automorphisms and derivations in classes of prime and semiprime rings. As above, we shall consider a somewhat more general situation, assuming that the automorphisms lie in $A(R)$, while derivations in $D(R)$ (see 1.7).

### 3.1. Basic Notions

Let $R$ be a prime ring, $G$ be a group of automorphisms. It should be recalled that by $\Phi_g$ we denote a set of all elements $\varphi \in R_F$ such that $x\varphi = \varphi x^g$ for all $x \in R_F$ (see 1.7.5, 1.7.6). For these sets valid are the relations $\Phi_g \Phi_h \subseteq \Phi_{gh}$ (see formula (8) in 1.7) which, in particular, afford that $\Phi_g$ is a linear space over a generalized centroid of the ring $R$. Moreover, corollary 1.7.9 states that $\Phi_g$ will be nonzero iff $g$ is an inner automorphism for $Q$.

#### 3.1.1. Definition. The algebra of a group of automorphisms $G$ is a C-algebra $B(G) = \sum_{g \in G} \Phi_g$.

Therefore, the algebra of the group has a basis of elements which correspond to the automorphisms which are inner for $Q$, i.e., it is an inner part of the group in a ring form.

If $G$ is a finite group, then its algebra $B(G)$ will be finite-dimensional over $C$. Of a finite order will also be a factor-group $G / G_{in}$, where $G_{in}$ is a normal subgroup of all inner for $Q$ automorphisms.

#### 3.1.2. Definition. A group $G$ is called reduced-finite if its algebra $B(G)$ is finite-dimensional, while the factor-group $G / G_{in}$ is finite. In this case the number $\dim_C B(G) \cdot |G / G_{in}|$ is called a reduced order of the group $G$. 