2. Resolvent rings and parametrizations

Before introducing the notion of resolvent ring, it is necessary first to understand a formal construction of “Galois closure” at the level of rings, which we call “$S_k$-closure”. We view this construction as a formal analogue of Galois closure because if $R$ is an order in an $S_k$-field of degree $k$, then it turns out that its $S_k$-closure $\bar{R}$ is an order in the usual Galois closure $\bar{K}$ of $K$. More generally, the $S_k$-closure operation gives a way of attaching to any ring $R$ with unit that is free of rank $k$ over $\mathbb{Z}$, a ring $\bar{R}$ with unit that is free of rank $k!$ over $\mathbb{Z}$.

Let us fix some terminology. By a ring of rank $k$ we will always mean a commutative ring with unit that is free of rank $k$ over $\mathbb{Z}$. To any such ring $R$ of rank $k$ we may attach the trace function $\text{Tr}: R \to \mathbb{Z}$, which assigns to an element $\alpha \in R$ the trace of the endomorphism $m_\alpha : R \ni x \mapsto x\alpha$ given by multiplication by $\alpha$. The discriminant $\text{Disc}(R)$ of such a ring $R$ is then defined as the determinant $\det(\text{Tr}(\alpha_i \alpha_j)) \in \mathbb{Z}$, where $\{\alpha_i\}$ is any $\mathbb{Z}$-basis of $R$.

The discriminants of individual elements in $R$ may also be defined and will play an important role in what follows. Let $F_\alpha$ denote the characteristic polynomial of the linear transformation $m_\alpha : R \to R$ associated to $\alpha$. Then the discriminant $\text{Disc}(\alpha)$ of an element $\alpha \in R$ is defined to be the discriminant of the characteristic polynomial $F_\alpha$. In particular, if $R = \mathbb{Z}[\alpha]$ for some $\alpha \in R$, then we have $\text{Disc}(R) = \text{Disc}(\alpha)$.

2.1. The $S_k$-closure of a ring of rank $k$. Let $R$ be any ring of rank $k$ having nonzero discriminant, and let $R^\otimes k$ denote the $k$th tensor power $R^\otimes k = R \otimes \mathbb{Z} R \otimes \mathbb{Z} \cdots \otimes \mathbb{Z} R$ of $R$. Then $R^\otimes k$ is seen to be a ring of rank $k^k$ in which $\mathbb{Z}$ lies naturally as a subring via the mapping $n \mapsto n(1 \otimes 1 \otimes \cdots \otimes 1)$.

Denote by $I_R$ the ideal in $R^\otimes k$ generated by all elements of the form

$$(x \otimes 1 \otimes \cdots \otimes 1) + (1 \otimes x \otimes \cdots \otimes 1) + \cdots + (1 \otimes 1 \otimes \cdots \otimes x) - \text{Tr}(x)$$

for $x \in R$. Let $J_R$ denote the $\mathbb{Z}$-saturation of the ideal $I_R$; i.e., let

$$J_R = \{r \in R^\otimes k : nr \in I_R \text{ for some } n \in \mathbb{Z}\}.$$

With these definitions, it is easy to see that if $\alpha \in R$ satisfies the characteristic equation $F_\alpha(x) = x^k - a_1x^{k-1} + a_2x^{k-2} - \cdots - a_k = 0$ with $a_i \in \mathbb{Z}$, then the $i$th elementary symmetric polynomial in the $k$ elements $\alpha \otimes 1 \otimes \cdots \otimes 1$, $1 \otimes \alpha \otimes \cdots \otimes 1$, $\ldots$, $1 \otimes 1 \otimes \cdots \otimes \alpha$ will be congruent to $a_i$ modulo $J_R$ for all $1 \leq i \leq k$.

For example, if $k = 2$ and $\alpha \in R$ satisfies $F_\alpha(x) = x^2 - a_1x + a_2 = 0$, then

$$2 \alpha \otimes \alpha = (\alpha \otimes 1 + 1 \otimes \alpha)^2 - (\alpha^2 \otimes 1 + 1 \otimes \alpha^2) \equiv \text{Tr}(\alpha)^2 - \text{Tr}(\alpha^2) = 2a_2 \pmod{J_R}$$

and hence $\alpha \otimes \alpha \equiv a_2 \pmod{J_R}$. An analogous argument works for all $k$. 
It is therefore natural to make the following definition:

Definition 6. The $S_k$-closure of a ring $R$ of rank $k$ is the ring $\bar{R}$ given by $R^{S_k}/J_R$.

This notion of $S_k$-closure is precisely the formal analogue of “Galois closure” we seek. We may write $\text{Gal}(\bar{R}/\mathbb{Z}) = S_k$, since the symmetric group $S_k$ acts naturally as a group of automorphisms on $\bar{R}$. Furthermore, the sub-ring $\bar{R}^{S_k}$ consisting of all elements fixed by this action is simply $\mathbb{Z}$. Indeed, it is known by the classical theory of polarization that the $S_k$-invariants of $R^{S_k}$ are spanned by elements of the form $x \otimes \cdots \otimes x$ ($x \in R$), and the latter is simply $N(x)$ modulo $J_R$. A similar argument shows that we also have $\text{Gal}(\bar{R}/R) = S_{k-1}$, where $R$ naturally embeds into $\bar{R}$ by $x \mapsto x \otimes 1 \otimes \cdots \otimes 1$.

For example, let us consider the case where $R$ is an order in a number field $K$ of degree $k$ such that $\text{Gal}(\bar{K}/\mathbb{Q}) = S_k$. Then $\bar{R}$ is isomorphic to the ring generated by all the Galois conjugates of elements of $R$ in $\bar{K}$, i.e.,

$$\bar{R} = \mathbb{Z}[\{\alpha : \alpha \ S_k\text{-conjugate to some element of } R\}]$$

More generally, if $R$ is an order in a number field $K$ of degree $k$ whose associated Galois group has index $n$ in $S_k$, then the “$S_k$-closure” of $K$ will be a direct sum of $n$ copies of the Galois closure of $K$ (and hence will have dimension $k!$ over $\mathbb{Q}$), and the $S_k$-closure of $R$ will be a subring of this having $\mathbb{Z}$-rank $k!$.

In the next two subsections, we use the notion of $S_k$-closure to attach rings of lower rank to orders in cubic and quartic fields.

2.2. The quadratic resolvent of a cubic ring. Given a cubic ring, there is a natural way to associate to $R$ a quadratic ring $S$, namely the unique quadratic ring $S$ having the same discriminant as $R$. Since the discriminant $D = \text{Disc}(R)$ of $R$ is necessarily congruent to 0 or 1 modulo 4, the quadratic ring $S(D)$ of discriminant $D$ always exists; we call $S = S(D)$ the quadratic resolvent ring of $R$.

Definition 7. For a cubic ring $R$, the quadratic resolvent ring $S^{\text{res}}(R)$ of $R$ is the unique quadratic ring $S$ such that $\text{Disc}(R) = \text{Disc}(S)$.

Given a cubic ring $R$, there is a natural map from $R$ to its quadratic resolvent ring $S$ that preserves discriminants. Indeed, for an element $x \in R$, let $x, x', x''$ denote the $S_3$-conjugates of $x$ in the $S_3$-closure $\bar{R}$ of $R$. Then the element

$$\tilde{\phi}_{3,2}(x) = \frac{[(x - x')(x' - x'')(x'' - x) + (x - x')(x' - x'')(x'' - x)]^2}{2}$$

is contained in some quadratic ring, and $\tilde{\phi}_{3,2}(x)$ has the same discriminant as $x$. (Notice that the expression (4) is only interesting modulo $\mathbb{Z}$, for $\tilde{\phi}_{3,2}(x)$ could