3

Multiplicative Actions

3.1 Introduction

In this chapter, we take up the subject of multiplicative actions and their invariants proper along with some of its ramifications. In Section 3.3 we show that, in investigating multiplicative invariant algebras, one can always reduce to the case where the acting group is finite and we may always work over $\mathbb{Z}$. A number of explicit calculations of multiplicative invariant algebras over $\mathbb{Z}$ for various finite groups, including all finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$, are carried out in Section 3.5. Section 3.6 features a theorem of Bourbaki [24] which states that multiplicative invariant algebras of weight lattices under the action of the Weyl group are polynomial algebras. Finally, we discuss twisted multiplicative actions and their connections with algebraic tori.

3.2 The Group Algebra of a G-Lattice

3.2.1 Group Algebras

Let L be a lattice. The group algebra of L over the commutative base ring $\Bbbk$ will be written as $\Bbbk[L]$; it contains a copy of L as a subgroup of the group of multiplicative units $\mathrm{U}(\Bbbk[L])$ and this copy of L forms a $\Bbbk$-basis of $\Bbbk[L]$. Working inside $\Bbbk[L]$, we must pass from the additive notation of L to a multiplicative notation. In order to make this passage explicit, we will write the basis element of $\Bbbk[L]$ corresponding to the lattice element $m \in L$ as

$$\mathbf{x}^m \ ;$$

so $\mathbf{x}^0 = 1$, $\mathbf{x}^{m+m'} = \mathbf{x}^m \mathbf{x}^{m'}$, and $\mathbf{x}^{-m} = (\mathbf{x}^m)^{-1}$. When a subset $M \subseteq L$ is to be explicitly viewed inside the group algebra $\Bbbk[L]$, it will be denoted by $\underline{M}$; so $\underline{M} = \{\mathbf{x}^m \mid m \in M\}$.

Every $f \in \Bbbk[L]$ has a unique expression as

$$f = \sum_{m \in L} k_m \mathbf{x}^m \tag{3.1}$$

with $k_m \in \Bbbk$ and $\{m \in L \mid k_m \neq 0\}$ a finite subset of L, called the *support* of f and denoted by $\operatorname{Supp} f$. A fixed choice of $\mathbb{Z}$-basis $\{e_i \mid i = 1, \dots, n\}$ of L, or a fixed isomorphism $L \cong \mathbb{Z}^n$, gives rise to a $\Bbbk$-algebra isomorphism of $\Bbbk[L]$ with the Laurent polynomial algebra $\Bbbk[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ via $\mathbf{x}^{e_i} \mapsto x_i$. Therefore, we may think of the representatives $\mathbf{x}^m \in \Bbbk[L]$ of lattice elements $m \in L$ as monomials in $x_1^{\pm 1}, \dots, x_n^{\pm 1}$.

3.2.2 Multiplicative Actions

If L is a G-lattice for some group G then the action of G on L extends uniquely to an action by $\Bbbk$-algebra automorphisms on $\Bbbk[L]$ via

$$g\Big(\sum_{m \in L} k_m \mathbf{x}^m\Big) = \sum_{m \in L} k_m \mathbf{x}^{g(m)} \ . \tag{3.2}$$

This type of action is called a *multiplicative action*. More general G-actions, called *twisted multiplicative*, will be considered in Section 3.8.

3.3 Reduction to Finite Groups, $\mathbb{Z}$-structure, and Finite Generation

Let L be a G-lattice, where G is an arbitrary group. The multiplicative action (3.2) of G on $\Bbbk[L]$ is a permutation action: $\{\mathbf{x}^m \mid m \in L\}$ is a G-stable $\Bbbk$-basis of $\Bbbk[L]$. Therefore, the $\Bbbk$-linear structure of $\Bbbk[L]^G$ is easily described: The support $\operatorname{Supp} f$ of any invariant $f \in \Bbbk[L]^G$ is a finite G-stable subset of L, and hence $\operatorname{Supp} f$ is contained in the G-sublattice

$$L_{\text{fin}} = \{m \in L \mid \text{the } G\text{-orbit } G(m) \text{ is finite}\} \ . \tag{3.3}$$

More precisely, f is a $\Bbbk$-linear combination of *G-orbit sums*

$$\mathsf{orb}(m) = \mathsf{orb}_{G,\Bbbk}(m) := \sum_{m' \in G(m)} \mathbf{x}^{m'} \in \Bbbk[L]^G$$

with $m \in L_{\text{fin}}$. Different orbit sums have disjoint supports, and hence they are $\Bbbk$-independent. Thus:

$$\Bbbk[L]^G = \bigoplus_{m \in G \backslash L_{\text{fin}}} \Bbbk \, \mathsf{orb}(m) \ , \tag{3.4}$$

where $G\backslash L_{\text{fin}}$ denotes a transversal for the finite G-orbits in L.

Note that, since L_{fin} is finitely generated, the subgroup $\operatorname{Ker}_G(L_{\text{fin}})$ has finite index in G; so G acts on L_{fin} through the finite quotient $\mathcal{G} = G/\operatorname{Ker}_G(L_{\text{fin}})$.

Further, the group ring $\Bbbk[L]$ is defined over $\mathbb{Z}$, $\Bbbk[L] = \Bbbk \otimes_{\mathbb{Z}} \mathbb{Z}[L]$, and each orbit sum has the form $\mathsf{orb}_{G,\Bbbk}(m) = 1_{\Bbbk} \otimes_{\mathbb{Z}} \mathsf{orb}_{G,\mathbb{Z}}(m)$. Hence, by (3.4), $\mathbb{Z}[L]^G$ is a *$\mathbb{Z}$-structure* for the multiplicative invariant algebra $\Bbbk[L]^G$. To summarize:

Proposition 3.3.1. *Let L be a G-lattice for an arbitrary group G and let $\Bbbk$ be a commutative base ring. Then $L_{\text{fin}} = \{m \in L \mid G(m) \text{ is finite}\}$ is a faithful $\mathcal{G}$-lattice, where $\mathcal{G} = G/\operatorname{Ker}_G(L_{\text{fin}})$ is a finite group . Furthermore:*

(a) $\Bbbk[L]^G = \Bbbk[L_{\text{fin}}]^{\mathcal{G}}$, *and*
(b) $\Bbbk[L]^G = \Bbbk \otimes_{\mathbb{Z}} \mathbb{Z}[L]^G$.

These observations have the following consequences.

Corollary 3.3.2. *Each multiplicative invariant algebra $\Bbbk[L]^G$ is an affine $\Bbbk$-algebra. Moreover, given a base ring $\Bbbk$ and a bound N, there is only a finite supply of multiplicative invariant algebras $\Bbbk[L]^G$ (up to isomorphism) with $\operatorname{rank} L \leq N$.*

Proof. Since $\mathbb{Z}[L_{\text{fin}}]$ is affine over the noetherian ring $\mathbb{Z}$ and $\mathcal{G} = G/\operatorname{Ker}_G(L_{\text{fin}})$ is finite, Noether's finiteness theorem (e.g., [22, Théorème V.1.2]) implies that $\mathbb{Z}[L_{\text{fin}}]^{\mathcal{G}}$ is an affine $\mathbb{Z}$-algebra. Therefore, by the proposition, $\Bbbk[L]^G = \Bbbk \otimes \mathbb{Z}[L_{\text{fin}}]^{\mathcal{G}}$ is affine over $\Bbbk$.

The finite group $\mathcal{G}$ embeds into $\mathrm{GL}_n(\mathbb{Z})$, where $n = \operatorname{rank} L_{\text{fin}}$. By the foregoing, the number of isomorphism classes of multiplicative invariant algebras $\Bbbk[L]^G$, with $\operatorname{rank} L$ is bounded by N, is at most equal to the sum of the numbers of conjugacy classes of finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ with $n \leq N$; see Section 1.10. $\square$

3.4 Units and Semigroup Algebras

Even though multiplicative invariant algebras arise from an action on a group algebra $\Bbbk[L]$, it turns out that $\Bbbk[L]^G$ is never a group algebra over $\Bbbk$ unless G acts trivially on the sublattice L_{fin} in (3.3). In order to justify this claim, we use the following simple lemma on unit groups.

Lemma 3.4.1. *Let L be a G-lattice and $\Bbbk$ a commutative domain. Then $\mathrm{U}(\Bbbk[L]) = \mathrm{U}(\Bbbk) \times \underline{L}$ and $\mathrm{U}(\Bbbk[L]^G) = \mathrm{U}(\Bbbk) \times \underline{L}^G$.*

Proof. It suffices to show that $\mathrm{U}(\Bbbk[L]) = \mathrm{U}(\Bbbk) \times \underline{L}$, because this implies that $\mathrm{U}(\Bbbk[L]^G) = \mathrm{U}(\Bbbk[L])^G = \mathrm{U}(\Bbbk) \times \underline{L}^G$. Note also that $k\mathbf{x}^m \in \mathrm{U}(\Bbbk) \times \underline{L}$ has inverse $k^{-1}\mathbf{x}^{-m}$; so $\mathrm{U}(\Bbbk) \times \underline{L} \subseteq \mathrm{U}(\Bbbk[L])$. In order to show that equality holds here, fix a *monomial order* for $\Bbbk[L]$. By definition, this is a total order $\succ$ on L that is compatible with addition: $m \succ n$ implies $m + \ell \succ n + \ell$ for $m, n, \ell \in L$. (For example, the lexicographic order with respect to any $\mathbb{Z}$-basis of L will do.) For any nonzero $f \in \Bbbk[L]$, define $\mathbf{max}(f)$ and $\mathbf{min}(f)$ to be the largest and the smallest element of the support $\operatorname{Supp} f$ with respect to $\succ$. Since $\Bbbk$ is a domain, it is easy to see that

$$\mathbf{max}(ff') = \mathbf{max}(f) + \mathbf{max}(f') \quad \text{and} \quad \mathbf{min}(ff') = \mathbf{min}(f) + \mathbf{min}(f')$$

holds for all nonzero $f, f' \in \Bbbk[L]$. Now suppose that $ff' = 1$. Then $\mathbf{max}(f) + \mathbf{max}(f') = 0 = \mathbf{min}(f) + \mathbf{min}(f')$. Since $\mathbf{max}(f) + \mathbf{max}(f') \geq \mathbf{min}(f) + \mathbf{max}(f') \geq \mathbf{min}(f) + \mathbf{min}(f')$, we conclude that $\mathbf{max}(f) = \mathbf{min}(f)$ and similarly for f'. This implies that f and f' belong to $\mathrm{U}(\Bbbk) \times \underline{L}$. $\square$

Corollary 3.4.2. *Let L be a G-lattice, where G is an arbitrary group, and let $\Bbbk$ be a commutative ring. The invariant algebra $\Bbbk[L]^G$ is a group algebra over $\Bbbk$ precisely if the action of G on the lattice L_{fin} in* (3.3) *is trivial. In particular, if G is finite then $\Bbbk[L]^G$ is a group algebra over $\Bbbk$ only if G acts trivially.*

Proof. One direction is immediate from Proposition 3.3.1. Conversely, suppose that $\Bbbk[L]^G$ is isomorphic to a group algebra over $\Bbbk$. By Proposition 3.3.1, we may replace L by L_{fin}, thereby reducing to the case where G is finite, and we may also replace $\Bbbk$ by some prime factor; so $\Bbbk$ is a domain. Since group algebras are generated, as $\Bbbk$-algebras, by their units, we conclude from Lemma 3.4.1 that $\Bbbk[L]^G = \Bbbk[L^G]$. Thus, on the one hand, $\Bbbk[L]$ is integral over $\Bbbk[L]^G$, since G is finite, while on the other, L/L^G is $\mathbb{Z}$-free and hence $\Bbbk[L]$ is a Laurent polynomial algebra in $r = \operatorname{rank} L/L^G$ many variables over $\Bbbk[L]^G$. Thus, we must have $r = 0$. □

While multiplicative invariant algebras $\Bbbk[L]^{\mathcal{G}}$ of finite groups $\mathcal{G}$ can never be group algebras if $\mathcal{G}$ acts nontrivially, it turns out that in many cases $\Bbbk[L]^{\mathcal{G}}$ is at least a *semigroup algebra*. Explicit examples will be presented in Section 3.5 and the phenomenon will be fully explained in Theorem 6.1.1. Recall that a $\Bbbk$-algebra R is a semigroup algebra (or monoid algebra) if R has a $\Bbbk$-basis, M, that is a submonoid of the multiplicative monoid $(R, \cdot)$; so $1 \in M$ and M is closed under multiplication. In analogy with the notation $\Bbbk[L]$ for group algebras, $\Bbbk[M]$ will denote the semigroup algebra over $\Bbbk$ of a monoid M. For example, the semigroup algebra of the monoid $M = \mathbb{Z}_+^r \oplus \mathbb{Z}^s$ is isomorphic to the mixed Laurent polynomial algebra $\Bbbk[x_1, \ldots, x_r, x_{r+1}^{\pm 1}, \ldots, x_{r+s}^{\pm 1}]$ over $\Bbbk$. We will only be concerned with commutative monoids M and, as with lattices, it is customary to write them additively. Gilmer [73] is a good reference for the algebraic structure of general commutative semigroup algebras $\Bbbk[M]$. We mention the following basic facts:

- $\Bbbk[M]$ is an affine (f.g.) $\Bbbk$-algebra if and only if the monoid M is finitely generated, and
- $\Bbbk[M]$ is a domain if and only if $\Bbbk$ is a domain and M is *cancellative* ($a + c = b + c \Rightarrow a = b$ for all $a, b, c, \in M$) and *torsion-free* ($na = nb \Rightarrow a = b$ for $a, b \in M$ and $n \in \mathbb{N}$).

The first assertion is obvious; for the second, see [73, Theorem 8.1]. Commutative monoids M that are cancellative and torsion-free are exactly the monoids that are isomorphic to submonoids of torsion-free abelian groups. If M is also finitely generated then M embeds into some lattice L, and we may clearly assume that $\langle M \rangle_{\text{group}} = L$. Finitely generated commutative monoids that are cancellative and torsion-free are often simply referred to as *affine semigroups*; see, e.g., Bruns and Herzog [32, 6.1]. An affine semigroup M is called *normal* if $nm \in M$ for $m \in \langle M \rangle_{\text{group}}$ and $n \in \mathbb{N}$ implies $m \in M$.

- $\Bbbk[M]$ is an affine $\Bbbk$-algebra that is a normal domain if and only if $\Bbbk$ is a normal domain and the monoid M is an affine normal semigroup.

For a proof, see [73, Corollary 12.11]. An affine semigroup M is called *positive* if M has no units other than 0 and an element $0 \neq m \in M$ is called *indecomposable* if $m = a + b$ $(a, b \in M)$ implies $a = 0$ or $b = 0$.

Lemma 3.4.3. *Let M be a positive affine semigroup. Then M has finitely many indecomposable elements, say $m_1, \ldots, m_s$. The m_i generate M, and every generating set for M contains $\{m_1, \ldots, m_s\}$.*

Proof. Clearly, all indecomposable elements must be contained in every generating set of M. Thus, it suffices to show that the indecomposable elements of M do indeed generate M. For this, we use the fact that there is a monoid homomorphism $\varphi : M \to \mathbb{Z}_+$ satisfying $\varphi(m) > 0$ for all $0 \neq m \in M$; see, e.g., Swan [210, Theorem 4.5]. Now consider an element $0 \neq m \in M$. If m is not indecomposable, then write $m = a + b$ with $0 \neq a, b \in M$. Then $\varphi(a), \varphi(b) < \varphi(m)$. By induction we know that a and b can be written as sums of indecomposable elements of M, and hence so can m. □

The unique smallest generating set constructed in the above lemma is called the *Hilbert basis* of M. An algorithm computing the Hilbert basis for any affine semigroup without non-trivial units can be found in Sturmfels [206, Algorithm 13.2].

3.5 Examples

In this section, we explicitly calculate the multiplicative invariant algebras of certain $\mathcal{G}$-lattices L for various finite groups $\mathcal{G}$. Throughout, we will work over $\Bbbk = \mathbb{Z}$. The results over arbitrary commutative base rings $\Bbbk$ then follow by base change; see Proposition 3.3.1(b). Examples 3.5.1, 3.5.4, 3.5.5, 3.5.6 and 3.5.7 below describe the multiplicative invariant algebras of certain reflection groups, while the group in Example 3.5.3 is a bireflection group. Table 3.1 list the multiplicative invariant algebras for lattices of rank 2; the groups in question are those in Table 1.2. The invariant algebras for the groups $\mathcal{G}_7$, $\mathcal{G}_8$ and $\mathcal{G}_9$ were obtained by direct calculation; the details for all other groups in Table 3.1 are given below.

We will repeatedly use the following obvious observation, valid for any base ring $\Bbbk$. Suppose that we have decompositions $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ and $L = L_1 \oplus L_2$ with $\mathcal{G}$-sublattices L_i such that $\mathcal{G}_j$ acts trivially on L_i for $i \neq j$. Then

$$\Bbbk[L]^{\mathcal{G}} \cong \Bbbk[L]_1^{\mathcal{G}_1} \otimes_{\Bbbk} \Bbbk[L]_2^{\mathcal{G}_2} . \tag{3.5}$$

Example 3.5.1 (The diagonal subgroup of $\mathrm{GL}_n(\mathbb{Z})$)**.** Let

$$\mathcal{T}_n = \mathrm{diag}(\pm 1, \ldots, \pm 1)_{n \times n} \subseteq \mathrm{GL}_n(\mathbb{Z})$$

be the group of diagonal matrices, with the canonical action on $L = \bigoplus_{i=1}^n \mathbb{Z}e_i$: $t = \mathrm{diag}(t_1, \ldots, t_n) \in \mathcal{T}_n$ acts by $t(e_i) = t_i e_i$. Put $x_i = \mathbf{x}^{e_i} \in \mathbb{Z}[L]$ and $\xi_i = x_i + x_i^{-1}$. We claim that

$$\mathbb{Z}[L]^{\mathcal{T}_n} = \mathbb{Z}[\xi_1, \ldots, \xi_n] , \tag{3.6}$$

a polynomial algebra in n variables. Indeed, formula (3.5) reduces the claim to the case $n = 1$. Then $\mathbb{Z}[L] = \mathbb{Z}[x^{\pm 1}]$ and $\mathcal{T}_1 = \langle t \rangle \cong \mathcal{C}_2$ acts by $t(x) = x^{-1}$. Writing $\mathbb{Z}[x^{\pm 1}] = \mathbb{Z}[\xi] \oplus x\mathbb{Z}[\xi]$ with $\xi = x + x^{-1}$, it is easy to see that $\mathbb{Z}[x^{\pm 1}]^{\mathcal{T}_1} = \mathbb{Z}[\xi]$, as claimed.

The next example will make use of the following lemma on adding a summand of rank 1.

Lemma 3.5.2. *Let $L = L' \oplus \mathbb{Z}_\varphi$, where L' is a $\mathcal{G}$-lattice and $\mathbb{Z}_\varphi = \mathbb{Z}$ with $\mathcal{G}$ acting via a non-trivial homomorphism $\varphi\colon \mathcal{G} \to \{\pm 1\}$. Put $\mathcal{N} = \operatorname{Ker}\varphi$ and suppose that $\Bbbk[L']^{\mathcal{N}} = \Bbbk[L']^{\mathcal{G}} + \sum_{j=1}^m \alpha_j \Bbbk[L']^{\mathcal{G}}$. Then:*

$$\Bbbk[L]^{\mathcal{G}} = \Bbbk[L']^{\mathcal{G}}[\xi] + \sum_{j=1}^{m} (\alpha_j x + s(\alpha_j)x^{-1}) \Bbbk[L']^{\mathcal{G}}[\xi] \ ,$$

where $x = \mathbf{x}^{(0_{L'},1)} \in \Bbbk[L]$, $\xi = x + x^{-1}$, and $s \in \mathcal{G} \setminus \mathcal{N}$.

Proof. Put $R = \Bbbk[L']^{\mathcal{G}} \oplus \bigoplus_{i \geq 1} \Bbbk[L']^{\mathcal{N}} \xi^i$; this is a $\mathcal{G}$-stable subalgebra of $\Bbbk[L]^{\mathcal{N}}$ such that $R^{\mathcal{G}} = \Bbbk[L']^{\mathcal{G}}[\xi]$. Define additive maps $D, \rho\colon R \to \Bbbk[L]^{\mathcal{N}}$ by $D(r) = \frac{s(r)-r}{\xi}$ and $\rho(r) = r + xD(r)$.

Claim. $\Bbbk[L]^{\mathcal{G}} = \rho(R)$.

First, $s(\rho(r)) = s(r) - x^{-1}D(r) = \rho(r)$ holds for $r \in R$; so $\rho(R) \subseteq \Bbbk[L]^{\mathcal{G}}$. For the reverse inclusion, write $\Bbbk[L]$ in the form $\Bbbk[L] = \Bbbk[L'][\xi] \oplus x\Bbbk[L'][\xi]$ and consider an element $f = f_0 + xf_1 \in \Bbbk[L]$, with $f_i \in \Bbbk[L'][\xi]$. Then $s(f) = (s(f_0) + \xi s(f_1)) - xs(f_1)$ while for $g \in \mathcal{N}$, one has $g(f) = g(f_0) + xg(f_1)$. Hence, $f \in \Bbbk[L]^{\mathcal{G}}$ if and only if f_0 and f_1 belong to $\Bbbk[L'][\xi]^{\mathcal{N}} = \bigoplus_{i \geq 0} \Bbbk[L']^{\mathcal{N}} \xi^i$ and the following two conditions are satisfied:

$$\begin{aligned} s(f_1) &= -f_1 \\ s(f_0) &= f_0 + \xi f_1 \end{aligned}$$

The last equation gives: $f_0 \in R$ and $f_1 = D(f_0)$. Therefore, $f = \rho(f_0) \in \rho(R)$ and the claim is proved.

To complete the proof of the lemma, we use our hypothesis that $\Bbbk[L']^{\mathcal{N}} = \Bbbk[L']^{\mathcal{G}} + \sum_{j=1}^m \alpha_j \Bbbk[L']^{\mathcal{G}}$. This results in the following expression for R:

$$\begin{aligned} R &= \Bbbk[L']^{\mathcal{G}} \oplus \bigoplus_{i \geq 1} \left(\Bbbk[L']^{\mathcal{G}} + \sum_{j=1}^{m} \alpha_j \Bbbk[L']^{\mathcal{G}} \right) \xi^i \\ &= \Bbbk[L']^{\mathcal{G}}[\xi] + \sum_{j=1}^{m} \alpha_j \xi \Bbbk[L']^{\mathcal{G}}[\xi] \ . \end{aligned}$$

The map ρ is $R^{\mathcal{G}}$-linear and its restriction to $R^{\mathcal{G}} = \Bbbk[L']^{\mathcal{G}}[\xi]$ is the identity. Therefore, the claim implies that

$$\Bbbk[L]^{\mathcal{G}} = \Bbbk[L']^{\mathcal{G}}[\xi] + \sum_{j=1}^{m} \rho(\alpha_j \xi)\Bbbk[L']^{\mathcal{G}}[\xi] \, .$$

Finally, $\rho(\alpha_j \xi) = \alpha_j x^{-1} + s(\alpha_j)x$. To obtain the exact expression for $\Bbbk[L]^{\mathcal{G}}$ as stated in the lemma, replace α_j by $s(\alpha_j)$ throughout. □

Example 3.5.3 (The diagonal subgroup of $\mathrm{SL}_n(\mathbb{Z})$)**.** Let $\mathcal{T}_n = \mathrm{diag}(\pm 1, \ldots, \pm 1)_{n \times n}$ be as in Example 3.5.1 and consider the group

$$\mathcal{G} = \mathcal{T}_n \cap \mathrm{SL}_n(\mathbb{Z})$$

with the canonical action on $L = \bigoplus_{i=1}^{n} \mathbb{Z}e_i$. As in Example 3.5.1, put $x_i = \mathbf{x}^{e_i}$, $\xi_i = x_i + x_i^{-1} \in \mathbb{Z}[L]$. We claim that

$$\mathbb{Z}[L]^{\mathcal{G}} = \mathbb{Z}[\xi_1, \ldots, \xi_n] \oplus \theta_n \mathbb{Z}[\xi_1, \ldots, \xi_n] \, , \tag{3.7}$$

where $\theta_n = \sum_{g \in \mathcal{G}} g(x_1 x_2 \ldots x_n) = \mathsf{orb}(\sum_i e_i)$. We argue by induction on n. For $n = 1$, the claim says that $\mathbb{Z}[x^{\pm 1}] = \mathbb{Z}[x + x^{-1}] \oplus x\mathbb{Z}[x + x^{-1}]$, which is clear. For the inductive step, we invoke Lemma 3.5.2, with $L' = \bigoplus_{i=1}^{n-1} \mathbb{Z}e_i$ and $\mathcal{N} = \mathcal{T}_{n-1} \cap \mathrm{SL}_{n-1}(\mathbb{Z})$. Since $\mathcal{G}$ acts on L' as the full diagonal group $\mathcal{T}_{n-1}$, we know by Example 3.5.1 that $\mathbb{Z}[L']^{\mathcal{G}} = \mathbb{Z}[\xi_1, \ldots, \xi_{n-1}]$. Moreover, by induction, $\mathbb{Z}[L']^{\mathcal{N}} = \mathbb{Z}[\xi_1, \ldots, \xi_{n-1}] \oplus \theta_{n-1}\mathbb{Z}[\xi_1, \ldots, \xi_{n-1}]$. Thus, Lemma 3.5.2 with $s = \mathrm{diag}(-1, 1, \ldots, 1, -1)$ gives:

$$\begin{aligned} \mathbb{Z}[L]^{\mathcal{G}} &= \mathbb{Z}[\xi_1, \ldots, \xi_{n-1}][\xi_n] + (\theta_{n-1}x_n + s(\theta_{n-1})x_n^{-1})\mathbb{Z}[\xi_1, \ldots, \xi_{n-1}][\xi_n] \\ &= \mathbb{Z}[\xi_1, \ldots, \xi_n] + \theta_n \mathbb{Z}[\xi_1, \ldots, \xi_n] \, . \end{aligned}$$

Since the sum is clearly direct, (3.7) is proved.

Specializing to $n = 2$, we obtain the invariants of multiplicative inversion in rank 2; this is group $\mathcal{G}_{10}$ in Table 1.2:

$$\mathbb{Z}[L]^{\mathcal{G}_{10}} = \mathbb{Z}[\xi_1, \xi_2] \oplus \theta\mathbb{Z}[\xi_1, \xi_2] \quad \text{with } \theta = x_1 x_2 + x_1^{-1} x_2^{-1}.$$

The generating invariants satisfy the relation $\theta\xi_1\xi_2 = \theta^2 + \xi_1^2 + \xi_2^2 - 4$; so

$$\mathbb{Z}[L]^{\mathcal{G}} \cong \mathbb{Z}[x, y, z]/(x^2 + y^2 + z^2 - xyz - 4) \, .$$

The invariant rings in this example are not semigroup algebras over $\mathbb{Z}$; see Section 10.2.

Example 3.5.4 (Multiplicative invariants of the root lattice B_n)**.** The root lattice of the root system of type B_n will simply be written as B_n; so $B_n = \bigoplus_{i=1}^{n} \mathbb{Z}e_i$. By [24, Planche II],

$$\mathrm{Aut}(B_n) = \mathcal{W}(B_n) = \{\pm 1\} \wr \mathcal{S}_n \, .$$

This group can be written as $\mathcal{W}(B_n) = \mathcal{T}_n \rtimes \mathcal{S}_n$, where $\mathcal{T}_n = \mathrm{diag}(\pm 1, \ldots, \pm 1)_{n \times n}$ acts as in Example 3.5.1 and $s(e_i) = e_{s(i)}$ for $s \in \mathcal{S}_n$. Putting $x_i = \mathbf{x}^{e_i} \in \mathbb{Z}[B_n]$, as usual, the invariants of the normal subgroup $\mathcal{T}_n$ are given by Example 3.5.1:

$\mathbb{Z}[B_n]^{\mathcal{T}_n} = \mathbb{Z}[\xi_1, \ldots, \xi_n]$ with $\xi_i = x_i + x_i^{-1}$. The group $\mathcal{S}_n$ acts on the polynomial ring $\mathbb{Z}[B_n]^{\mathcal{T}_n}$ by $s(\xi_i) = \xi_{s(i)}$ for $s \in \mathcal{S}_n$. Hence, the fundamental theorem for $\mathcal{S}_n$-invariants (e.g., [27, p. A IV.58]) yields that

$$\mathbb{Z}[B_n]^{\{\pm 1\} \wr \mathcal{S}_n} = \mathbb{Z}[\xi_1, \ldots, \xi_n]^{\mathcal{S}_n} = \mathbb{Z}[\sigma_1, \ldots, \sigma_n] , \tag{3.8}$$

where

$$\sigma_i = \sum_{j_1 < \ldots < j_i} \xi_{j_1} \xi_{j_2} \ldots \xi_{j_i}$$

is the i^{th} elementary symmetric function in $\xi_1, \ldots, \xi_n$. Thus, $\mathbb{Z}[B_n]^{\{\pm 1\} \wr \mathcal{S}_n}$ is a polynomial ring in n variables. The special case $n = 2$ yields the invariants for group $\mathcal{G}_2$ in Table 3.1.

Example 3.5.5 (Multiplicative $\mathcal{S}_n$-invariants of U_n)**.** Restricting the lattice B_n in Example 3.5.4 to the symmetric group $\mathcal{S}_n$ we obtain the standard permutation lattice U_n for $\mathcal{S}_n$; see §1.3.3. As before, let $\{e_i\}_1^n$ denote the permutation basis of U_n and write $x_i = \mathbf{x}^{e_i} \in \mathbb{Z}[U_n]$. Then the element $\mathbf{x}^{\sum_1^n e_i} \in \mathbb{Z}[U_n]$ becomes the n^{th} elementary symmetric function $s_n = \prod_1^n x_i$. Moreover,

$$\mathbb{Z}[U_n] = \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] = \mathbb{Z}[x_1, \ldots, x_n][s_n^{-1}] ,$$

and $\mathcal{S}_n$ acts via $s(x_i) = x_{s(i)}$ $(s \in \mathcal{S}_n)$. By the fundamental theorem for $\mathcal{S}_n$-invariants, $\mathbb{Z}[x_1, \ldots, x_n]^{\mathcal{S}_n} = \mathbb{Z}[s_1, \ldots, s_n]$, where s_i is the i^{th} elementary symmetric function in $x_1, \ldots, x_n$. Therefore,

$$\mathbb{Z}[U_n]^{\mathcal{S}_n} = \mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}] \cong \mathbb{Z}[\mathbb{Z}_+^{n-1} \oplus \mathbb{Z}] , \tag{3.9}$$

a mixed Laurent polynomial algebra in n variables, with 1 variable inverted.

Example 3.5.6 (Multiplicative $\mathcal{S}_n$-invariants of A_{n-1})**.** We continue with the notation of Example 3.5.5. Note that $\mathbb{Z}[U_n] = \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ is $\mathbb{Z}$-graded by total degree in the x_i's and the action of $\mathcal{S}_n$ respects this grading. Using the standard basis $a_i = e_i - e_{i+1}$ $(i = 1, \ldots, n-1)$ of the root lattice A_{n-1}, as in Example 1.8.1, and putting $y_i = \mathbf{x}^{a_i} = \frac{x_i}{x_{i+1}}$, the group ring $\mathbb{Z}[A_{n-1}]$ can be written as

$$\mathbb{Z}[A_{n-1}] = \mathbb{Z}[y_1^{\pm 1}, \ldots, y_{n-1}^{\pm 1}] = \mathbb{Z}[\frac{x_i}{x_j} \mid 1 \le i, j \le n] .$$

This is the degree 0-component $\mathbb{Z}[U_n]_0$ of $\mathbb{Z}[U_n]$. Hence,

$$\mathbb{Z}[A_{n-1}]^{\mathcal{S}_n} = \mathbb{Z}[U_n]_0^{\mathcal{S}_n} ,$$

the ring of $\mathcal{S}_n$-invariants of total degree 0 in $\mathbb{Z}[U_n]$. By equation (3.9), a $\mathbb{Z}$-basis of $\mathbb{Z}[U_n]_0^{\mathcal{S}_n}$ is given by the elements $s_1^{t_1} \ldots s_{n-1}^{t_{n-1}} / s_n^{t_n}$ with $t_i \in \mathbb{Z}_+$ and $\sum_{i=1}^{n-1} i t_i = n t_n$. Therefore,

$$\mathbb{Z}[A_{n-1}]^{\mathcal{S}_n} \cong \mathbb{Z}[M] ,$$

where M is the submonoid of $\mathbb{Z}_+^{n-1}$ consisting of all $(t_1, \ldots, t_{n-1})$ so that $\sum_i it_i$ is divisible by n. The isomorphism sends the element $m = (t_1, \ldots, t_{n-1}) \in M$ to the basis element

$$\mu_m = s_n^{-\frac{1}{n}\sum_i it_i} \cdot \prod_{i=1}^{n-1} s_i^{t_i} \in \mathbb{Z}[A_{n-1}]^{\mathcal{S}_n} .$$

Taking $n = 2$, for example, the monoid M is generated by $m = (2)$ and we obtain the fundamental invariant $\mu_m = s_1^2/s_2 = y_1 + y_1^{-1} + 2$. Thus, $\mathbb{Z}[A_1]^{\mathcal{S}_2} = \mathbb{Z}[y_1 + y_1^{-1}]$ is a polynomial algebra. This is just the special case $n = 1$ of Example 3.5.1, since A_1 is the sign lattice $\mathbb{Z}^-$ for $\mathcal{S}_2$.

For $n = 3$, the monoid M has generators $m_1 = (3, 0)$, $m_2 = (0, 3)$ and $m_3 = (1, 1)$. This yields the fundamental invariants $\mu_1 = s_1^3/s_3$, $\mu_2 = s_2^3/s_3^2$ and $\mu_3 = s_1 s_2/s_3$ for $\mathbb{Z}[A_2]^{\mathcal{S}_3}$. Note that $\mu_1\mu_2 = \mu_3^3$; so we obtain the presentation

$$\mathbb{Z}[A_2]^{\mathcal{S}_3} \cong \mathbb{Z}[x, y, z]/(z^3 - xy) .$$

A more economical system of fundamental invariants for $\mathbb{Z}[A_2]^{\mathcal{S}_3}$ is given by

$$\begin{aligned}
\mu_3 - 3 &= y_1 + y_1^{-1} + y_2 + y_2^{-1} + y_1y_2 + y_1^{-1}y_2^{-1} &&= \mathsf{orb}(a_1) \\
\mu_1 - 3\mu_3 + 3 &= y_1^2y_2 + y_1^{-1}y_2 + y_1^{-1}y_2^{-2} &&= \mathsf{orb}(2a_1 + a_2) \\
\mu_2 - 3\mu_3 + 3 &= y_1y_2^2 + y_1y_2^{-1} + y_1^{-2}y_2^{-1} &&= \mathsf{orb}(a_1 + 2a_2)
\end{aligned}$$

Example 3.5.7 (non-diagonal Klein 4-group)**.** Consider the group $\mathcal{G} = \mathcal{G}_6 = \langle s, -s\rangle \cong \mathcal{C}_2 \times \mathcal{C}_2$ of Table 1.2. Here, $s = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Note that both generators s and $-s$ act as (non-diagonalizable) reflections on $L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$. Their product, $g = s(-s) \in \mathcal{G}$, acts as $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, as in Example 3.5.3 above. Thus, using Example 3.5.3 and its notation, we obtain $\mathbb{Z}[L]^{\mathcal{G}} = R^{\langle s\rangle}$ with $R = \mathbb{Z}[L]^{\langle g\rangle} = \mathbb{Z}[\xi_1, \xi_2] \oplus \theta\mathbb{Z}[\xi_1, \xi_2]$. Since s interchanges ξ_1 and ξ_2 and leaves θ invariant, the invariant ring is given by

$$\mathbb{Z}[L]^{\mathcal{G}} = \mathbb{Z}[\sigma_1, \sigma_2] \oplus \theta\mathbb{Z}[\sigma_1, \sigma_2] ,$$

where $\sigma_1 = \xi_1 + \xi_2$ and $\sigma_2 = \xi_1\xi_2$ are the 1st and 2nd elementary symmetric functions in ξ_1, ξ_2. An alternative set of fundamental invariants is

$$\begin{aligned}
\mu_1 &= \theta + 2 = x_1x_2 + x_1^{-1}x_2^{-1} + 2 , \\
\mu_2 &= \sigma_2 - \theta + 2 = x_1x_2^{-1} + x_1^{-1}x_2 + 2 , \\
\mu_3 &= \sigma_1 = x_1 + x_1^{-1} + x_2 + x_2^{-1} .
\end{aligned}$$

These invariants satisfy the relation $\mu_3^2 = \mu_1\mu_2$; so we obtain the presentation

$$\mathbb{Z}[L]^{\mathcal{G}} \cong \mathbb{Z}[x, y, z]/(z^2 - xy) .$$

This shows that $\mathbb{Z}[L]^{\mathcal{G}}$ is isomorphic to the semigroup algebra $\mathbb{Z}[M]$, where M is the submonoid of $\mathbb{Z}_+^2$ that is generated by the elements $(2, 0)$, $(0, 2)$ and $(1, 1)$.

Table 3.1. Multiplicative invariants in rank 2

group $\mathcal{G}$ (cf. Table 1.2)	invariant algebra $\mathbb{Z}[L]^{\mathcal{G}}$	reference
$\mathcal{G}_1 \cong \mathcal{D}_{12}$	polynomial algebra $\mathbb{Z}[\alpha, \beta]$ $\alpha = x_1 + x_1^{-1} + x_2 + x_2^{-1} + x_1x_2 + x_1^{-1}x_2^{-1}$ $\beta = x_1x_2^{-1} + x_1^{-1}x_2 + x_1^2x_2 + x_1x_2^2 + x_1^{-2}x_2^{-1} + x_1^{-1}x_2^{-2}$	Example 3.7.1
$\mathcal{G}_2 \cong \mathcal{D}_8$	polynomial algebra $\mathbb{Z}[\xi_1 + \xi_2, \xi_1\xi_2]$ with $\xi_i = x_i + x_i^{-1}$	Example 3.5.4 for $n = 2$
$\mathcal{G}_3 \cong \mathcal{S}_3$	semigroup algebra $\mathbb{Z}[\mu_1, \mu_2] \oplus \mu_3\mathbb{Z}[\mu_1, \mu_2]$ $\mu_1 = s_1^3/s_3$, $\mu_2 = s_2^3/s_3^2$, $\mu_3 = s_1s_2/s_3$ $s_i = s_i(x_1, x_2, x_3)$ the i^{th} elem. symm. function relation: $\mu_1\mu_2 = \mu_3^3$	Example 3.5.6 for $n = 3$
$\mathcal{G}_4 \cong \mathcal{S}_3$	polynomial algebra $\mathbb{Z}[\eta_+, \eta_-]$ $\eta_+ = x_1 + x_2 + x_1^{-1}x_2^{-1}$, $\eta_- = x_1^{-1} + x_2^{-1} + x_1x_2$	Example 3.7.1 for $n = 3$
$\mathcal{G}_5 \cong \mathcal{C}_2 \times \mathcal{C}_2$	polynomial algebra $\mathbb{Z}[\xi_1, \xi_2]$ with $\xi_i = x_i + x_i^{-1}$	Example 3.5.1 for $n = 2$
$\mathcal{G}_6 \cong \mathcal{C}_2 \times \mathcal{C}_2$	semigroup algebra $\mathbb{Z}[\mu_1, \mu_2] \oplus \mu_3\mathbb{Z}[\mu_1, \mu_2]$ $\mu_1 = x_1x_2 + x_1^{-1}x_2^{-1} + 2$, $\mu_2 = x_1x_2^{-1} + x_1^{-1}x_2 + 2$, $\mu_3 = x_1 + x_1^{-1} + x_2 + x_2^{-1}$ relation: $\mu_1\mu_2 = \mu_3^2$	Example 3.5.7
$\mathcal{G}_7 \cong \mathcal{C}_6$	$\mathbb{Z}[\tau_1, \tau_2] \oplus \sigma\mathbb{Z}[\tau_1, \tau_2]$ $\tau_1 = \eta_+ + \eta_-$, $\tau_2 = \eta_+\eta_-$, $\sigma = \eta_+\varphi + \eta_-\varphi_-$ with η_+, η_-, φ as for $\mathcal{G}_9$ and $\varphi_- = x_1^{-1}x_2^{-2} + x_1^2x_2 + x_1^{-1}x_2 + 6$ relation: $\sigma^2 = \tau_1(\tau_2+9)\sigma - \tau_2(\tau_2+9)^2 + (\tau_1^2 - 4\tau_2)(3\tau_1\tau_2 - \tau_1^3 - 27)$	
$\mathcal{G}_8 \cong \mathcal{C}_4$	$\mathbb{Z}[\sigma_1, \sigma_2] \oplus \rho\mathbb{Z}[\sigma_1, \sigma_2]$ $\sigma_1 = \xi_1 + \xi_2$, $\sigma_2 = \xi_1\xi_2$, where $\xi_i = x_i + x_i^{-1}$, and $\rho = x_1x_2^2 + x_1^{-1}x_2^{-2} + x_1^2x_2^{-1} + x_1^{-2}x_2 + 3\sigma_1$ relation: $\rho^2 = \rho\sigma_1(\sigma_2 + 4) + 4\sigma_1^2\sigma_2 - \sigma_1^4 - \sigma_2(\sigma_2 + 4)^2$	
$\mathcal{G}_9 \cong \mathcal{C}_3$	$\mathbb{Z}[\eta_+, \eta_-] \oplus \varphi\mathbb{Z}[\eta_+, \eta_-]$ $\eta_+ = x_1 + x_2 + x_1^{-1}x_2^{-1}$, $\eta_- = x_1^{-1} + x_2^{-1} + x_1x_2$, $\varphi = x_1x_2^2 + x_1^{-2}x_2^{-1} + x_1x_2^{-1} + 6$ relation: $\varphi\eta_+\eta_- = \eta_+^3 + \eta_-^3 + \varphi^2 - 9\varphi + 27$	

Table 3.1. (continued)

group $\mathcal{G}$ (cf. Table 1.2)	invariant algebra $\mathbb{Z}[L]^{\mathcal{G}}$	reference
$\mathcal{G}_{10} \cong \mathcal{C}_2$	$\mathbb{Z}[\xi_1, \xi_2] \oplus \theta\mathbb{Z}[\xi_1, \xi_2]$ $\xi_i = x_i + x_i^{-1}, \theta = x_1x_2 + x_1^{-1}x_2^{-1}$ relation: $\theta\xi_1\xi_2 = \theta^2 + \xi_1^2 + \xi_2^2 - 4$	Example 3.5.3
$\mathcal{G}_{11} \cong \mathcal{C}_2$	Laurent polynomial algebra $\mathbb{Z}[x_1 + x_1^{-1}, x_2^{\pm 1}]$	Example 3.5.1 for $n = 1$ and (3.5)
$\mathcal{G}_{12} \cong \mathcal{C}_2$	Laurent polynomial algebra $\mathbb{Z}[x_1 + x_2, (x_1x_2)^{\pm 1}]$	Example 3.5.5 for $n = 2$

3.6 Multiplicative Invariants of Weight Lattices

The following result is classical; see [24, Théorème VI.3.1 and Exemple 1]. We use the notation and terminology of Section 1.8.

Theorem 3.6.1 (Bourbaki)**.** *Let $\Lambda = \Lambda(\Phi)$ be the weight lattice of a reduced root system Φ and let $\mathcal{W} = \mathcal{W}(\Phi)$ denote its Weyl group. Then the multiplicative invariant algebra $\mathbb{Z}[\Lambda]^{\mathcal{W}}$ is a polynomial algebra over $\mathbb{Z}$: the $\mathcal{W}$-orbit sums of a set of fundamental weights are algebraically independent generators.*

Proof. Fix a base $\Delta = \{a_i\}$ of Φ and let $\{m_j\} \subseteq \Lambda$ be the corresponding set of fundamental weights; so $\langle a_i^\vee, m_j \rangle = \delta_{i,j}$. Put

$$\Lambda_+ = \{m \in \Lambda \mid \langle a^\vee, m\rangle \geq 0 \text{ for all } a \in \Delta\} = \bigoplus_j \mathbb{Z}_+ m_j \,. \tag{3.10}$$

The argument depends on the following standard facts about root systems:

(a) Every $\mathcal{W}$-orbit in Λ meets the set Λ_+ in exactly one point; see [24, Théorème VI.1.2(ii)].
(b) Define a partial order on Λ by $m \geq m' \iff m - m' \in \bigoplus_{a\in\Delta} \mathbb{R}_+ a$. Then $m \geq g(m)$ holds for all $m \in \Lambda_+$ and $g \in \mathcal{W}$; see [24, Prop. VI.1.18].
(c) The restriction of $\geq$ to Λ_+ satisfies the descending chain condition. In fact, for each $m \in \Lambda_+$, there are only finitely many $m' \in \Lambda_+$ with $m \geq m'$; see [24, p. 187] or [93, Lemma 13.2.B].

By (a) and (3.4), we have:

$$\mathbb{Z}[\Lambda]^{\mathcal{W}} = \bigoplus_{m\in\Lambda_+} \mathbb{Z}\,\mathsf{orb}(m) \,. \tag{3.11}$$

Define elements $f_m \in \mathbb{Z}[\Lambda]^{\mathcal{W}}$ ($m \in \Lambda_+$) by

$$f_m = \prod_j \mathsf{orb}(m_j)^{z_j} \ ,$$

where $m = \sum_j z_j m_j$ with (uniquely determined) $z_j \in \mathbb{Z}_+$. The theorem asserts that the family $F = \{f_m\}_{m \in \Lambda_+}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\Lambda]^{\mathcal{W}}$.

To prove this, note that, with respect to the partial order $\geq$ of (b), each $m \in \Lambda_+$ is the unique largest element of the support $\mathrm{Supp}(\mathsf{orb}(m)) = \mathcal{W}(m)$. Since $\geq$ is compatible with addition (i.e., $m \geq m' \Rightarrow m + w \geq m' + w$ for $m, m', w \in \Lambda$), we deduce that m is the unique largest element in $\mathrm{Supp}\, f_m$ and its $\mathbb{Z}$-coefficient is 1. Therefore, by (3.11), f_m can be written as a finite sum

$$f_m = \mathsf{orb}(m) + \sum_{\substack{m' \in \Lambda_+ \\ m' < m}} z_{m,m'}\, \mathsf{orb}(m') \ . \tag{3.12}$$

This formula implies that the family $F = \{f_m\}_{m \in \Lambda_+}$ is $\mathbb{Z}$-independent, because $\{\mathsf{orb}(m)\}_{m \in \Lambda_+}$ is. Also, each orbit sum $\mathsf{orb}(m)$ ($m \in \Lambda_+$) is a $\mathbb{Z}$-linear combination of elements in F. Otherwise (c) would allow us to pick a counterexample m that is minimal with respect to $\geq$. Thus, all $\mathsf{orb}(m')$ in (3.12) can be expressed in terms of F, and hence $\mathsf{orb}(m)$ as well, a contradiction. This completes the proof that F is a $\mathbb{Z}$-basis of $\mathbb{Z}[\Lambda]^{\mathcal{W}}$. □

The converse of Bourbaki's theorem is also true: all multiplicative invariant algebras that are polynomial algebras come from weight lattices; see Corollary 7.1.2 below. Since the root lattice B_n is equal to the weight lattice for C_n, Example 3.5.4 provides an illustration of Theorem 3.6.1. Here is a second example:

Example 3.6.2 (Multiplicative $\mathcal{S}_n$-invariants of A^*_{n-1})**.** As was pointed out in Example 1.8.1, we may think of A^*_{n-1} as the weight lattice $\Lambda(A_{n-1})$ of the root system A_{n-1}. Put $\ell_i = e_i - \frac{1}{n}\sum_{j=1}^n e_j \in \Lambda(A_{n-1}) = A^*_{n-1}$, where $\{e_i\}_1^n$ denotes the canonical permutation basis of U_n as in Example 3.5.5. Then the elements $m_i = \sum_{j=1}^i \ell_j = \sum_{j=1}^i e_j - \frac{i}{n}\sum_{j=1}^n e_j$ are the fundamental weights of A_{n-1} corresponding to the base $\Delta = \{e_i - e_{i+1}\}_1^{n-1}$. Putting $x_i = \mathbf{x}^{e_i} \in \mathbb{Z}[U_n]$ and $\xi_i = \mathbf{x}^{\ell_i} \in \mathbb{Z}[A^*_{n-1}]$ and letting s_i denote the i^{th} elementary symmetric function we calculate the $\mathcal{S}_n$-orbit sum of m_i as follows:

$$\begin{aligned} \mathsf{orb}(m_i) &= \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I| = i}} \mathbf{x}^{\sum_{j \in I} e_j - \frac{i}{n}\sum_{j=1}^n e_j} \\ &= s_i(x_1, \ldots, x_n) \cdot s_n(x_1, \ldots, x_n)^{-i/n} \\ &= s_i(\xi_1, \ldots, \xi_n) \ . \end{aligned} \tag{3.13}$$

By Theorem 3.6.1, the elements $s_i(\xi_1, \ldots, \xi_n)$ are algebraically independent generators of $\mathbb{Z}[A^*_{n-1}]^{\mathcal{S}_n}$. A direct verification, independent of Theorem 3.6.1, will be given in Example 3.7.1 below.

3.7 Passage to an Effective Lattice

Let L be a lattice for the finite group $\mathcal{G}$ and let $\overline{L} = L/L^{\mathcal{G}}$ denote its effective quotient; see Section 1.6. The canonical map $\overline{} : L \twoheadrightarrow \overline{L}$ extends to $k[L]$:

$$\overline{} : \Bbbk[L] \twoheadrightarrow \Bbbk[\overline{L}] = k[L/L^{\mathcal{G}}] , \quad \mathbf{x}^m \mapsto \mathbf{x}^{m+L^{\mathcal{G}}} \ (m \in L) .$$

It follows from (1.17) that the orbit sum of an element $m \in L$ satisfies

$$\overline{\mathsf{orb}(m)} = \mathsf{orb}(\overline{m}) .$$

Moreover, $\mathsf{orb}(\overline{a}) = \mathsf{orb}(\overline{b})$ is equivalent to $\mathsf{orb}(a) = \mathsf{orb}(b)\mathbf{x}^c$ for some $c \in L^{\mathcal{G}}$. Consequently, (3.4) implies that

$$\Bbbk[\overline{L}]^{\mathcal{G}} = \overline{\Bbbk[L]^{\mathcal{G}}} \cong \Bbbk[L]^{\mathcal{G}} / \left(\mathbf{x}^m - 1 \mid m \in L^{\mathcal{G}}\right) . \tag{3.14}$$

Here, it suffices to let m run over a $\mathbb{Z}$-basis of $L^{\mathcal{G}}$. The isomorphism (3.14) cannot in general be strengthened to $\Bbbk[L]^{\mathcal{G}} \cong \Bbbk[\overline{L}]^{\mathcal{G}} \otimes_k \Bbbk[L^{\mathcal{G}}]$; cf. Example 4.2.1 below.

Example 3.7.1 (Multiplicative $\mathcal{S}_n$-invariants of A_{n-1}^*, revisited)**.** The invariant algebra $\mathbb{Z}[A_{n-1}^*]^{\mathcal{S}_n}$ can also be calculated from (3.14). Indeed, dualizing the augmentation sequence (1.10) and using the fact that $\mathbb{Z}$ and U_n are self-dual (being permutation lattices) one obtains an exact sequence of $\mathcal{S}_n$-lattices

$$0 \to \mathbb{Z} \longrightarrow U_n \longrightarrow A_{n-1}^* \to 0 .$$

Thus,

$$A_{n-1}^* \cong U_n / U_n^{\mathcal{S}_n} = \overline{U_n} , \tag{3.15}$$

and so (3.14) applies. In detail, using the notation of Example 3.5.5, the $\mathcal{S}_n$-invariants $U_n^{\mathcal{S}_n}$ are spanned by the element $\sum_1^n e_i$ and $\mathbf{x}^{\sum_1^n e_i} \in \mathbb{Z}[U_n]$ is the n^{th} elementary symmetric function $s_n = \prod_1^n x_i$. By (3.9), $\mathbb{Z}[U_n]^{\mathcal{S}_n} = \mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}]$, and so (3.14) yields that $\mathbb{Z}[A_{n-1}^*]^{\mathcal{S}_n}$ is isomorphic to $\mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}]/(s_n - 1)$. Thus,

$$\mathbb{Z}[A_{n-1}^*]^{\mathcal{S}_n} \cong \mathbb{Z}[\overline{U_n}]^{\mathcal{S}_n} \cong \mathbb{Z}[s_1, \ldots, s_{n-1}] , \tag{3.16}$$

a polynomial algebra in $n - 1$ variables.

To make the connection with the description of $\mathbb{Z}[A_{n-1}^*]^{\mathcal{S}_n}$ given in Example 3.6.2, we use the $\mathcal{S}_n$-lattice isomorphism

$$\overline{U_n} \xrightarrow{\sim} \Lambda(A_{n-1}) , \quad \overline{e_i} \mapsto \ell_i = e_i - \frac{1}{n}\sum_{j=1}^n e_j . \tag{3.17}$$

This isomorphism yields an isomorphism $\mathbb{Z}[\overline{U_n}]^{\mathcal{S}_n} \xrightarrow{\sim} \mathbb{Z}[\Lambda(A_{n-1})]^{\mathcal{S}_n}$ sending the generators s_i in (3.16) to the generators $s_i(\xi_1, \ldots, \xi_n)$ constructed in Example 3.6.2.

Finally, we point put how the foregoing yields the fundamental invariants for the groups $\mathcal{G}_1$ and $\mathcal{G}_4$ in Table 3.1. Under the second isomorphism in (3.16), i^{th} elementary symmetric function s_i becomes the orbit sum $\mathsf{orb}(\overline{e_1} + \cdots + \overline{e_i})$. Thus, writing $y_i = \mathbf{x}^{\overline{e_i}} \in \mathbb{Z}[\overline{U_n}]$, we obtain the following fundamental invariants in $\mathbb{Z}[A_{n-1}^*]^{\mathcal{S}_n} \cong \mathbb{Z}[\overline{U_n}]^{\mathcal{S}_n}$ for $n = 3$:

$$\eta_1 = \mathsf{orb}(\overline{e_1}) = y_1 + y_2 + y_1^{-1}y_2^{-1}$$
$$\eta_2 = \mathsf{orb}(\overline{e_1} + \overline{e_2}) = y_1y_2 + y_1^{-1} + y_2^{-1}$$

This takes care of group $\mathcal{G}_4$. For $\mathcal{G}_1$, note that $\mathcal{G}_1 = \langle \mathcal{G}_4, -\operatorname{Id}\rangle$ and $-\operatorname{Id}$ interchanges the above two invariants η_1 and η_2. Thus we have the following fundamental invariants for $\mathcal{G}_1$:

$$\eta_1 + \eta_2 = y_1 + y_1^{-1} + y_2 + y_2^{-1} + y_1y_2 + y_1^{-1}y_2^{-1}$$
$$\eta_1\eta_2 - 3 = y_1y_2^{-1} + y_1^{-1}y_2 + y_1^2y_2 + y_1^{-2}y_2^{-1} + y_1y_2^2 + y_1^{-1}y_2^{-2}$$

3.8 Twisted Multiplicative Actions

3.8.1 The Setting

Let R be some commutative domain and let $R[L]$ be the group algebra of the lattice L over R. Suppose a group G acts by ring automorphisms on $R[L]$ in such a way that $g(R) \subseteq R$ holds for all $g \in G$. In short, $R \subseteq R[L]$ is an extension of G-rings. Then G stabilizes the unit groups of $\mathrm{U}(R)$ and $\mathrm{U}(R[L])$. By Lemma 3.4.1, $\mathrm{U}(R[L]) = \mathrm{U}(R) \times \underline{L}$. Hence, the lattice L becomes a G-lattice that fits into an exact sequence of G-modules

$$1 \to \mathrm{U}(R) \to \mathrm{U}(R[L]) \to L \to 1\ . \qquad (3.18)$$

This extension of G-modules need not split. The G-action on $R[L]$ is called *twisted multiplicative* and the group ring $R[L]$ will be called a *twisted multiplicative G-ring*. We will use the notation

$$R[L]_\gamma$$

to denote $R[L]$ with a twisted multiplicative action. Explicitly, the action of $g \in G$ on $R[L]_\gamma$ is given by the formula

$$g(\sum_{m\in L} r_m\mathbf{x}^m) = \sum_{m\in L} g(r_m)\gamma_{g(m)}(g)\mathbf{x}^{g(m)} \qquad (3.19)$$

for suitable elements $\gamma_{g(m)}(g) \in \mathrm{U}(R)$. The map $\gamma(g)\colon m \mapsto \gamma_m(g)$ belongs to $\operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R))$. Moreover, viewing $\operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R))$ as G-module as in §1.4.2, we have the identity

$$\gamma(gg') = (g\gamma(g'))\gamma(g) \qquad (3.20)$$

for $g, g' \in G$. Thus, $\gamma\colon G \to \operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R))$ is a 1-cocycle. Let γ' be a 1-cocycle in the same cohomology class as γ; so $\gamma'(g) = \gamma(g)fg(f)^{-1}$ for some $f \in \operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R))$. Then the map $R[L]_\gamma \to R[L]_{\gamma'}$, $r\mathbf{x}^m \mapsto rf(m)\mathbf{x}^m$, is an isomorphism of G-rings that is the identity on R. Therefore, we may view γ as an element of $H^1(G, \operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R)))$. Under the standard isomorphism $H^1(G, \operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R))) \cong \operatorname{Ext}_{\mathbb{Z}[G]}(L, \mathrm{U}(R))$ (see Brown [31, Proposition III.2.2]), γ becomes the class of the extension (3.18).

Example 3.8.1. Twisted multiplicative actions often arise in the investigation of ordinary multiplicative actions as follows. Given an extension of G-lattices $0 \to N \to M \to L \to 0$, the ordinary multiplicative action of G on $\Bbbk[M]$ can be viewed as a twisted multiplicative action on $R[L]_\gamma$, with $R = \Bbbk[N]$ and γ the image of the class in $\mathrm{Ext}_{\mathbb{Z}[\mathcal{G}]}(L, N)$ of the given lattice extension under the G-embedding $N \hookrightarrow \mathrm{U}(R)$.

3.8.2 The Split Case

Twisted multiplicative actions with trivial extension class γ will simply be written as

$$R[L] \; .$$

In this case, the action (3.19) simplifies to

$$g(\sum_{m \in L} r_m \mathbf{x}^m) = \sum_{m \in L} g(r_m)\mathbf{x}^{g(m)} \; . \tag{3.21}$$

Of course, if G acts trivially on R then (3.19) is an ordinary multiplicative action (3.2). In the following, the notation $\Bbbk[L]$, for a G-lattice L, will always stand for the group algebra of L over $\Bbbk$ with the ordinary multiplicative action (3.2). In other words, all group actions on $\Bbbk$ are assumed trivial.

Twisted multiplicative actions of the form (3.21) are particularly important in the case where $R = K$ is a field and G is a finite group acting faithfully by automorphisms on K. The invariant algebra $K[L]^G$ is then called an *algebra of torus invariants*. The connection with algebraic tori will be explained in Section 3.10 below.

3.8.3 Linearization via Permutation Lattices

Let L be a lattice and $\Bbbk$ a commutative domain. Any group action by $\Bbbk$-algebra automorphisms on $\Bbbk[L]$ is twisted multiplicative. Thus, the remarks in §3.8.1 lead to the following description of the automorphism group of $\Bbbk[L]$:

$$\mathrm{Aut}_{\Bbbk\text{-alg}}(\Bbbk[L]) = \mathrm{Hom}(L, \mathrm{U}(\Bbbk)) \rtimes \mathrm{GL}(L) \tag{3.22}$$

with $\mathrm{GL}(L)$ acting by the ordinary multiplicative action (3.2) and with

$$f(\mathbf{x}^m) = f(m)\mathbf{x}^m$$

for $f \in \mathrm{Hom}(L, \mathrm{U}(\Bbbk))$ and $m \in L$. These actions commute by the rule $gf = g(f)g$ for $g \in \mathrm{GL}(L)$ and $f \in \mathrm{Hom}(L, \mathrm{U}(\Bbbk))$, where $g(f) \in \mathrm{Hom}(L, \mathrm{U}(\Bbbk))$ is defined as in §1.4.2.

As an application, we present the following linearization result which is essentially proved in Barge [4].

Proposition 3.8.2. *Let $\Bbbk$ be an algebraically closed field of characteristic* 0 *and let* $\mathcal{G}$ *be a finite group acting by* $\Bbbk$*-algebra automorphisms on* $\Bbbk[L]$*. Assume that, viewed as* $\mathcal{G}$*-lattice as in* (3.18)*,* L *is rationally isomorphic to some permutation* $\mathcal{G}$*-lattice. Then there exists a finite extension* $\widetilde{\mathcal{G}}$ *of* $\mathcal{G}$ *and a linear* $\Bbbk$*-representation* $\widetilde{\mathcal{G}} \to \mathrm{GL}(V)$ *so that*

$$\Bbbk[L]^{\mathcal{G}} \cong \mathsf{S}(V)^{\widetilde{\mathcal{G}}}[1/f]$$

for some $0 \neq f \in \mathsf{S}(V)^{\widetilde{\mathcal{G}}}$.

Proof. We may assume that $\mathcal{G}$ acts faithfully on $\Bbbk[L]$; so $\mathcal{G} \subseteq \mathrm{Aut}_{\Bbbk\text{-alg}}(\Bbbk[L]) = \mathrm{Hom}(L, \Bbbk^*) \rtimes \mathrm{GL}(L)$. The action of $\mathcal{G}$ on L is given by the map $\varphi\colon \mathcal{G} \hookrightarrow \mathrm{Hom}(L, \Bbbk^*) \rtimes \mathrm{GL}(L) \overset{\text{can.}}{\twoheadrightarrow} \mathrm{GL}(L)$. Furthermore, $\mathcal{G} \subseteq \mathrm{Hom}(L, \Bbbk^*) \rtimes \varphi(\mathcal{G})$. By hypothesis, there is a permutation $\mathcal{G}$-lattice P with $L \subseteq P$ and P/L finite. Let $\psi\colon \mathcal{G} \to \mathrm{GL}(P)$ denote its structure map. Restriction from P to L gives an isomorphism $\psi(\mathcal{G}) \overset{\sim}{\to} \varphi(\mathcal{G})$ and an exact sequence $0 \to \mathrm{Hom}(P/L, \Bbbk^*) \to \mathrm{Hom}(P, \Bbbk^*) \to \mathrm{Hom}(L, \Bbbk^*) \to 0$, and these maps combine to give an epimorphism $\rho\colon \mathrm{Hom}(P, \Bbbk^*) \rtimes \psi(\mathcal{G}) \twoheadrightarrow \mathrm{Hom}(L, \Bbbk^*) \rtimes \varphi(\mathcal{G})$ with kernel $\mathcal{N} = \mathrm{Hom}(P/L, \Bbbk^*) \cong P/L$. Let $\widetilde{\mathcal{G}}$ denote the inverse image of $\mathcal{G}$ under ρ; so we have an extension of groups $1 \to \mathcal{N} \to \widetilde{\mathcal{G}} \overset{\rho}{\to} \mathcal{G} \to 1$. It is easy to see that $\Bbbk[P]^{\mathcal{N}} = \Bbbk[L]$. Therefore, $\Bbbk[P]^{\widetilde{\mathcal{G}}} = \Bbbk[L]^{\mathcal{G}}$. Finally, let $\{m_1, \ldots, m_n\}$ be a $\mathbb{Z}$-basis of P that is permuted by the action of $\mathcal{G}$. Then $\mathrm{Hom}(P, \Bbbk^*) \rtimes \psi(\mathcal{G})$ stabilizes the $\Bbbk$-subspace $V = \bigoplus_i \Bbbk\mathbf{x}^{m_i}$ of $\Bbbk[P]$, and hence so does $\widetilde{\mathcal{G}}$. Moreover, $\Bbbk[P] = \mathsf{S}(V)[1/f]$, where $f = \prod_i \mathbf{x}^{m_i}$ is a $\widetilde{\mathcal{G}}$-semiinvariant, that is, $g(f) = \lambda(g)f$ for some $\lambda \in \mathrm{Hom}(\widetilde{\mathcal{G}}, \Bbbk^*)$. Replacing f by $f^{|\widetilde{\mathcal{G}}|}$ we can make f invariant. Hence, $\Bbbk[L]^{\mathcal{G}} = \Bbbk[P]^{\widetilde{\mathcal{G}}} = \mathsf{S}(V)^{\widetilde{\mathcal{G}}}[1/f]$, as desired. □

3.9 Hopf Structure

The group algebra $\Bbbk[L]$ is a *Hopf algebra* over $\Bbbk$: the comultiplication $\Delta\colon \Bbbk[L] \to \Bbbk[L] \otimes_{\Bbbk} \Bbbk[L]$, counit (or augmentation) $\varepsilon\colon \Bbbk[L] \to \Bbbk$, and antipode $S\colon \Bbbk[L] \to \Bbbk[L]$ are given by $\Bbbk$-linear extension of the rules

$$\Delta(\mathbf{x}^m) = \mathbf{x}^m \otimes \mathbf{x}^m \ , \ \varepsilon(\mathbf{x}^m) = 1 \ , \ S(\mathbf{x}^m) = \mathbf{x}^{-m}$$

for $m \in L$. If $\Bbbk$ has no idempotents other than 0 and 1, the set of "monomials" $\underline{L} = \{\mathbf{x}^m \mid m \in L\}$ can be characterized as the set of group-like elements of $\Bbbk[L]$,

$$\underline{L} = \{f \in \Bbbk[L] \mid \Delta(f) = f \otimes f, \varepsilon(f) = 1\} \ . \tag{3.23}$$

Thus, every Hopf morphism $\Bbbk[L] \to \Bbbk[L]$ must map $\underline{L}$ to itself. In particular,

$$\mathrm{Aut}_{\mathrm{Hopf}}(\Bbbk[L]) \cong \mathrm{GL}(L) \ .$$

3.10 Torus Invariants

We briefly sketch the connection of algebras of torus invariants as introduced in Section 3.8 with algebraic tori. For background on algebraic groups, we refer to Borel [19]. The algebra of regular functions of an algebraic group G will be denoted by $\mathcal{O}(G)$.

By definition, an algebraic $\Bbbk$-torus, for a field $\Bbbk$, is an affine algebraic group T defined over $\Bbbk$ so that, over the algebraic closure of $\Bbbk$, T becomes isomorphic to $\mathbb{G}_{\mathrm{m}}^n = \mathbb{G}_{\mathrm{m}} \times \cdots \times \mathbb{G}_{\mathrm{m}}$ (n factors) for some n. Here, $\mathbb{G}_{\mathrm{m}} = \mathrm{GL}_1$ is the multiplicative group, that is, the algebraic group defined by the Hopf algebra $\mathcal{O}(\mathbb{G}_{\mathrm{m}}) = \Bbbk[t^{\pm 1}] \cong \Bbbk[\mathbb{Z}]$. It is known that T already becomes isomorphic to $\mathbb{G}_{\mathrm{m}}^n$ over some finite Galois extension $K/\Bbbk$; see [19, 8.11]. Explicitly, this means that the Hopf algebra $\mathcal{O}(K \otimes_{\Bbbk} T) = K \otimes_{\Bbbk} \mathcal{O}(T)$ is isomorphic to the group algebra $K[L]$ with $L \cong \mathbb{Z}^n$; see [19, 8.5]. By (3.23), the lattice L can be identified with the character group

$$X(K \otimes_{\Bbbk} T) = \mathrm{Hom}_{\mathrm{Hopf}}(K[t^{\pm 1}], K \otimes_{\Bbbk} \mathcal{O}(T)) \; .$$

The action of the Galois group $\mathcal{G} = \mathrm{Gal}(K/\Bbbk)$ on K induces $\mathcal{G}$-actions on $\mathcal{O}(K \otimes_{\Bbbk} T)$ and on $X(K \otimes_{\Bbbk} T)$, thereby making L a $\mathcal{G}$-lattice. Moreover,

$$\mathcal{O}(T) = (K \otimes_{\Bbbk} \mathcal{O}(T))^{\mathcal{G}} \cong K[L]^{\mathcal{G}} \; ;$$

so $\mathcal{O}(T)$ is an algebra of torus invariants as in Section 3.8. Conversely, given a field K with a faithful action by a finite group $\mathcal{G}$ and a $\mathcal{G}$-lattice L, the Galois descent lemma (Lemma 9.4.1 below) implies that $K[L] = K \otimes_{\Bbbk} K[L]^{\mathcal{G}}$, where $\Bbbk = K^{\mathcal{G}}$ is the subfield of $\mathcal{G}$-invariants; so $K[L]^{\mathcal{G}} = \mathcal{O}(T)$ for some $\Bbbk$-torus T.

http://www.springer.com/978-3-540-24323-6

Multiplicative Invariant Theory
Lorenz, M.
2005, XII, 180 p. 5 illus., Hardcover
ISBN: 978-3-540-24323-6