COMMUNICATIONS IN ALGEBRA, 24(3), 1051-1055 (1996)

REGULARITY OF MULTIPLICATIVE INVARIANTS

MARTIN LORENZ

Department of Mathematics
Temple University
Philadelphia, PA 19122-2585
e-mail: lorenz@math.temple.edu

ABSTRACT. The group $\mathrm{GL}_d(\mathbf{Z})$ acts on the Laurent polynomial ring $k[X_1^{\pm 1}, \ldots, X_d^{\pm 1}]$ over the field k via its natural action on the multiplicative group generated by the variables $X_1, \ldots, X_d$ ($\cong \mathbf{Z}^d$). For G a finite subgroup of $\mathrm{GL}_d(\mathbf{Z})$ with order $|G|$ not divisible by $\mathrm{char}\, k$, we show that the algebra of G-invariants in $k[X_1^{\pm 1}, \ldots, X_d^{\pm 1}]$ is regular precisely if G is a reflection group and $\mathrm{H}^1(G/D, (\mathbf{Z}^d)^D) = 0$. Here, D is the subgroup of G that is generated by the reflections which are diagonalizable over $\mathbf{Z}$, and $(\mathbf{Z}^d)^D$ are the D-invariants in $\mathbf{Z}^d$. The results of some machine computations are also discussed.

INTRODUCTION

This note continues our investigaton of multiplicative invariants in [L] and ultimately depends on Farkas's work in [F]. In fact, our main result does little more than add some finishing ring theoretic touches to [F], Corollary 13 (which is largely credited to Steinberg [St] by Farkas). In particular, we use the structure of the class group of multiplicative invariants ([L]) to give the result a form that lends itself conveniently to computational applications.

Specifically, let $S = kA$ denote the group algebra of a finitely generated free abelian group A over the field k and let G be a finite subgroup of $\mathrm{GL}(A)$. Then G acts on S by means of the unique extension of the natural G-action on A. Our aim is to characterize regularity of the algebra of invariants $R = S^G$ of this action:

Theorem. *Assume that the order of G is not divisible by $\mathrm{char}\, k$. Then the following assertions are equivalent:*

i. *The algebra of invariants $R = S^G$ is regular;*
ii. *S is free as R-module;*
iii. *R is a mixed polynomial algebra, i.e., $R \cong k[X_1^{\pm 1}, \ldots, X_r^{\pm 1}, X_{r+1}, \ldots, X_d]$ for some r, d;*
iv. *G is a reflection group and $\mathrm{H}^1(G, A^D) = 0$, where D is the subgroup of G generated by the reflections that are diagonalizable over $\mathbb{Z}$ and A^D denotes the D-invariants in A.*

We remark that, in (iii), one necessarily has $d = \mathrm{rank}\, A$ and $r = \mathrm{rank}\, A^G$. This follows from dimension considerations and the fact that all units of S have the form ca ($c \in k^*, a \in A$), and

1991 *Mathematics Subject Classification.* 13A50, 13F20, 13H05, 13-04, 16W20, 16S34, 20H15.
Key words and phrases. multiplicative group action, algebra of invariants, regular ring, unique factorization domain, reflection group, root system.
The author was supported in part by NSF Grant DMS-9400643.

hence the units of R have the same form, with $a \in A^G$ Thus regularity completely determines the structure of R. Also, in (ii), the rank of S as R-module equals the order of G, by Galois theory.

As is often the case with multiplicative actions, the above Theorem is similar to, but more complicated than the corresponding result for "linear" actions of a finite group $G' \subseteq \mathrm{GL}(V)$ on the symmetric (polynomial) algebra $S(V)$ of a finite dimensional k-vector space V. Indeed, under the same assumption on the order of G', the classical theorem of Shephard-Todd, Chevalley, and Serre ([Bou], p. 115 or [BH], p. 275) establishes the equivalence of (i), (ii), (iii)': *the algebra of invariants is a polynomial algebra*, and (iv)': *G' is a pseudoreflection group.*

Condition (iv) of the Theorem is quite amenable to machine computations. To illustrate this point, we list in §2 all reflection groups G in ranks 2 and 3 which yield nonregular invariant algebras.

Notations and conventions. The above notations A, $G \subseteq \mathrm{GL}(A)$, $S = kA$, and $R = S^G$ will retain their meaning throughout this article. In addition, we put

$$p = \mathrm{char}\, k \ (\geq 0) \qquad \text{and} \qquad d = \mathrm{rank}\, A\ .$$

So $A \cong \mathbb{Z}^d$ and G can be viewed as a subgroup of the group $\mathrm{GL}_d(\mathbb{Z})$ of integer $d \times d$-matrices of determinant ± 1. We will work under the standing hypothesis that p does not divide the order of G.

1. Proof of the Theorem

1.1 If R is regular then G is a reflection group. Let $\Omega = (a - 1 |\ a \in A)$ denote the augmentaton ideal of S. Since Ω is G-invariant, G acts on the localized algebra $S' = S_\Omega$ and the algebra of invariants $R' = (S')^G$ is canonically isomorphic with R localized at $\Omega \cap R$ ([Bou2], Prop. 23, p. 34). Thus S' and R' are both local rings with residue field k, and our assumption on p implies that S' is a Noetherian R'-module (e.g., [M], Theorem 7.6). Furthermore, S' and R' are both regular, the latter by assumption on R. Therefore, by [S], Théorème 2' (or see [Bou], Exerc. 7(b), p. 138), G acts as a pseudoreflection group on the Zariski tangent space Ω/Ω^2 of S'. Using the kG-isomorphism

$$\begin{aligned} V := A \otimes_{\mathbb{Z}} k \ &\xrightarrow{\cong}\ \ \Omega/\Omega^2 \\ a \otimes 1 \ &\longmapsto\ a - 1 + \Omega^2 \qquad (a \in A)\ , \end{aligned}$$

we conclude that G acts as a pseudoreflection group on V. In other words, letting $\pi : \mathrm{GL}(A) \to \mathrm{GL}(V)$ denote the canonical map ("reduction mod p"), $\pi(G)$ is generated by pseudoreflections. Our hypothesis on p implies that π is mono on G (cf. [Bou], Exerc. 7(c), p. 138). Thus it suffices to show that, if $g \in G$ is such that $\pi(g)$ is a pseudoreflection, that is, $\mathrm{rank}(\pi(g) - \mathrm{Id}_V) = 1$, then g is a reflection. Indeed, since $\det(g) = \pm 1$, we have $\mu = \det(\pi(g)) = \pm 1$ in k, and since $\pi(g)$ is conjugate in $\mathrm{GL}(V)$ to the diagonal matrix $\mathrm{diag}(\mu, 1, \ldots, 1)$, we actually have $\mu = -1$ and $g^2 = 1$ (and $p \neq 2$). Thus, putting $A_\pm = \mathrm{ann}_A(g \mp 1)$ and $V_\pm = \mathrm{ann}_V(\pi(g) \mp 1)$, we have $2A \subseteq A_+ \oplus A_- \subseteq A$ and $A_\pm \otimes_{\mathbb{Z}} k = V_\pm$. Since $\dim_k V_+ = d - 1$ and $\dim_k V_- = 1$, we conclude that $\mathrm{rank}(A_+) = d - 1$ and $\mathrm{rank}(A_-) = 1$, which proves that g is a reflection.

1.2 If R is regular then R is a mixed polynomial algebra. By §1.1, we know that G is a reflection group which enables us to use the results of [F]. In particular, it has been shown in [F], proof of Theorem 10, that the invariant algebra R of any finite reflection group is a semigroup algebra kC, where C is a multiplicative semigroup with 1 that embeds as a subsemigroup into a free abelian group of finite rank. (We remark that, even though Farkas works over $k = \mathbb{C}$, his methods pertain more generally to the situation where p does not divide the order of G.) Furthermore, since R is an affine k-algebra, by Noether's theorem ([Bou2], Théorème 2, p. 33), the semigroup C is finitely generated. Thus C is an *affine semigroup* in the sense of [BH], §6.1. It is known (cf. [BH], Exercise 6.1.11) that kC is regular if and only if C is of the form $\mathbb{Z}^u \oplus \mathbb{N}^v$, in additive notation. In other words, kC is regular precisely if $kC \cong k[X_1^{\pm 1}, \ldots, X_u^{\pm 1}, X_{u+1}, \ldots, X_{u+v}]$, whence our assertion.

1.3 R is regular iff S is free as R-module. Inasmuch as projective modules over mixed polynomial algebras are known to be free (e.g., [Lam], p. 144), §1.2 reduces the assertion to the following one:

R is regular iff S is projective as R-module.

The validity of this is a consequence of a general fact from commutative algebra which we include for the reader's convenience.

Lemma. *Let $U \subseteq V$ be an extension of commutative Noetherian domains such that V is finitely generated as U-module.*

(a) If V is Cohen-Macaulay and U is regular then V is projective as U-module.

(b) Suppose that V is regular and there is a Reynolds operator $\rho : V \to U$ (i.e., ρ is a U-module map that is the identity on U). Then U is regular if and only if V is projective as U-module.

Proof. (a) We have to show that, for each maximal ideal $\mathfrak{m}$ of U, the localized ring $V_{\mathfrak{m}}$ is free over $U_{\mathfrak{m}}$. Note that $U_{\mathfrak{m}} \subseteq V_{\mathfrak{m}}$ is a finite extension of Noetherian domains, with $V_{\mathfrak{m}}$ Cohen-Macaulay and $U_{\mathfrak{m}}$ regular local. Freeness of $V_{\mathfrak{m}}$ over $U_{\mathfrak{m}}$ now follows from [Mat], (18.H) Theorem 46.

(b) The "only if" direction is a special case of (a). Conversely, assume that V is projective as U-module and fix a maximal ideal $\mathfrak{m}$ of U. Then $V_{\mathfrak{m}}$ is free over $U_{\mathfrak{m}}$ and the extension $U_{\mathfrak{m}} \subseteq V_{\mathfrak{m}}$ has Reynolds operator $\rho_{\mathfrak{m}} = \rho \otimes_U \mathrm{Id}_{U_{\mathfrak{m}}}$. Therefore, [Kap], Theorem 5, p. 173 implies that $\mathrm{gldim}\, U_{\mathfrak{m}} \leq \mathrm{gldim}\, V_{\mathfrak{m}}$. Finally, $V_{\mathfrak{m}}$ is a regular semi-local ring and so $\mathrm{gldim}\, V_{\mathfrak{m}}$ is finite. Hence $\mathrm{gldim}\, U_{\mathfrak{m}}$ is finite as well, which proves regularity of U. □

The Lemma applies to the extension $R \subseteq S$, since $S = kA$ is a regular affine k-algebra and, by Noether's theorem, R is affine and S is finitely generated as R-module. (All this is independent of our hypothesis on p.) Furthermore, a Reynolds operator $\rho : S \to R$ is given by $\rho(s) = |G|^{-1} \sum_{g \in G} s^g$.

1.4 Conclusion. §1.2 proves that (i) implies (iii) and the converse is obvious. Thus (i) and (iii) are equivalent and so are (i) and (ii), by §1.3. In view of [L], Theorem 2.5, assertion (iv) is equivalent with

G is a reflection group and R is a UFD.

In this form, the implication (iv) ⇒ (iii) is part of [F], Corollary 13. Since mixed polynomial algebras are UFD, (iii) ⇒ (iv) follows from §1.1 (or from [F2], Theorem 8+). This completes the proof of the Theorem.

2. Computations

2.1. In this section, we list the results of computations that were carried out using the computer group theory package GAP version 3.4, in particular its crystallographic groups library which contains all finite subgroups of $\mathrm{GL}_d(\mathbb{Z})$ for $d = 2, 3, 4$, up to conjugation. The program `multinv.g` is available via anonymous ftp to `ftp.math.temple.edu` in the directory `/pub/lorenz/programs`. Besides our standing hypothesis on $p = \mathrm{char}\, k$, the field k is assumed throughout to be a splitting field for $(G/N)^{\mathrm{ab}}$, where N denotes the subgroup of G that is generated by the reflections in G. Furthermore, the matrices given below are understood to act from the right on rows.

2.2 Rank 2 (cf. [L], §2.7). Among the 12 conjugacy classes of nontrivial finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$, exactly 8 consist of reflection groups, and 2 of these give rise to a nonregular invariant algebra R. They are represented by the groups

$$G = \langle y, -y \rangle \cong C_2 \times C_2 : \qquad \mathrm{Cl}\, R \cong \mathbb{Z}/2\mathbb{Z}\,,$$
$$G = \langle x, y \rangle \cong D_6 : \qquad \mathrm{Cl}\, R \cong \mathbb{Z}/3\mathbb{Z}\,,$$

Here, $\mathrm{Cl}\, R$ denotes the class group of R, and $x = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$, $y = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. In both cases, a suitable $\mathrm{GL}_2(\mathbb{Q})$-conjugate of G in $\mathrm{GL}_2(\mathbb{Z})$ yields a regular invariant algebra. All instances where R is a UFD come from reflection groups G, and so R is actually a mixed polynomial algebra.

2.3 Rank 3. There are 72 conjugacy classes of nontrivial finite subgroups of $\mathrm{GL}_3(\mathbb{Z})$ of which 28 consist of reflection groups. Among the latter, 11 give rise to a nonregular invariant algebra. The above two rank 2 groups G yield 4 of these: $\begin{pmatrix} G & \\ & 1 \end{pmatrix}$ produces the invariant algebra $R[X^{\pm 1}]$ and $\begin{pmatrix} G & \\ & \pm 1 \end{pmatrix}$ produces $R[X]$, both with the same class group as R. In addition, there are the following 7 classes of $\mathbb{Z}$-indecomposable groups, given by a representative group:

$$
\begin{array}{ll}
G_1 = \langle x, -sxs^{-1} \rangle \cong C_2 \times C_2 : & \mathrm{Cl}\, R \cong \mathbb{Z}/2\mathbb{Z}\ , \\
G_2 = \langle -\mathrm{Id}, x, sxs^{-1} \rangle \cong C_2 \times C_2 \times C_2 : & \mathrm{Cl}\, R \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\ , \\
G_3 = G_2^{\mathrm{tr}} \cong C_2 \times C_2 \times C_2 : & \mathrm{Cl}\, R \cong \mathbb{Z}/2\mathbb{Z}\ , \\
G_4 = \langle -\mathrm{Id}, x^{\mathrm{tr}}, y \rangle \sim D_8 \times C_2 : & \mathrm{Cl}\, R \sim \mathbb{Z}/2\mathbb{Z} \\
G_5 = \langle s, e, d \rangle \cong S_4 : & \mathrm{Cl}\, R \cong \mathbb{Z}/2\mathbb{Z}\ , \\
G_6 = \langle r, s, -x^{\mathrm{tr}} \rangle \cong S_4 : & \mathrm{Cl}\, R \cong \mathbb{Z}/4\mathbb{Z}\ , \\
G_7 = \langle -\mathrm{Id}, r, s, x^{\mathrm{tr}} \rangle \cong S_4 \times C_2 : & \mathrm{Cl}\, R \cong \mathbb{Z}/2\mathbb{Z}\ .
\end{array}
$$

Here, tr denotes transpose matrices, and $x = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 1 & 1 \\ -1 & 0 & 0 \end{pmatrix}$, $y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & -1 \\ -1 & 1 & 0 \end{pmatrix}$, $e = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $d = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $s = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, $r = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & -1 \end{pmatrix}$. In $\mathrm{GL}_3(\mathbb{Q})$, the group G_1 is conjugate to $\begin{pmatrix} G & \\ & 1 \end{pmatrix}$, and G_2 and G_3 are conjugate to $\begin{pmatrix} G & \\ & \pm 1 \end{pmatrix}$, where G is the first group ($\cong C_2 \times C_2$) in §2.2. Furthermore, G_5 and G_6 are also conjugate in $\mathrm{GL}_3(\mathbb{Q})$. Again, whenever R is a UFD then R is actually a mixed polynomial algebra.

2.4 Rank 4. The number of rank 4 cases makes their explicit listing prohibitive: $\mathrm{GL}_4(\mathbb{Z})$ has 709 conjugacy classes of nontrivial finite subgroups including 101 conjugacy classes of reflection groups. Of these, 51 give rise to a nonregular invariant algebra. In rank 4, for the first time, one finds a nonregular invariant algebra that is a UFD. The group in question is isomorphic with A_5 and is generated by the matrices $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

2.5 Reflection groups and root systems. Following the referee's suggestions, we briefly sketch how the groups exhibited in §§2.2, 2.3 can also be arrived at non-computationally working in the context of root systems. So let $G \subseteq \mathrm{GL}(A)$ be a finite reflection group and assume, for simplicity, that G is effective, that is, $A^G = 0$. Then, by [F2], Theorem 16 (or [St]), the invariant algebra R is regular or, equivalently, a polynomial algebra, precisely if there exists a root system Φ with Weyl group G so that A is G-isomorphic to the weight lattice $\widehat{L}(\Phi)$ of Φ. Now there always is a root system Φ so that G is the Weyl group of Φ and $L(\Phi) \subseteq A \subseteq \widehat{L}(\Phi)$, where $L(\Phi)$ denotes the root lattice of Φ (cf. [F2], Proposition 12). As we are looking for nonregular invariant algebras, we must certainly choose A to be a *proper* subgroup of $\widehat{L}(\Phi)$. The structure of the groups $\overline{L}(\Phi) = \widehat{L}(\Phi)/L(\Phi)$ is known; it is listed, for all irreducible root systems Φ, in [Bou], pp. 250–275. For example, if Φ has type B_n then $\overline{L}(\Phi)$ has order 2 so that the only choice for A in this case would be the root lattice. However, the root lattice for type B_n is isomorphic, as a module over its Weyl group, to the weight lattice for type C_n (cf. [F3], Note added in proof). So type B_n never leads to a nonregular invariant algebra. Further, the root and weight lattices for A_1 are clearly isomorphic as well.

In case $\mathrm{rank}\, A = 2$, the possible root systems are of types A_2, B_2, or $A_1 \times A_1$, and the two groups in §2.2 come from taking A to be the preimage of the "diagonal" subgroup of $\overline{L}(A_1 \times A_1) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or of the trivial subgroup of $\overline{L}(A_2) \cong \mathbb{Z}/3\mathbb{Z}$.

If $\mathrm{rank}\, A = 3$, the available root systems Φ are of types A_3, B_3, C_3, $A_2 \times A_1$, $B_2 \times A_1$, $G_2 \times A_1$, or $A_1 \times A_1 \times A_1$, with B_3 being irrelevant for our purposes. Likewise, $G_2 \times A_1$ can be discarded, because $\overline{L}(G_2) = 0$ and so the only choice for A is $\widehat{L}(G_2) \times L(A_1)$ which, however, is isomorphic to the weight lattice $\widehat{L}(G_2) \times \widehat{L}(A_1)$. For A_3, we have $\overline{L}(A_3) \cong \mathbb{Z}/4\mathbb{Z}$, and the two proper subgroups lead to G_6 and G_5 in §2.3. Since $\overline{L}(C_3) \cong \mathbb{Z}/2\mathbb{Z}$, type C_3 produces only one example, which turns out to be the group G_7. The three proper subgroups of $\overline{L}(A_2 \times A_1) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ yield

the lattices $L(A_2) \times L(A_1)$, $L(A_2) \times \widehat{L}(A_1)$, and $\widehat{L}(A_2) \times L(A_1)$. The latter is isomorphic with the weight lattice $\widehat{L}(A_2) \times \widehat{L}(A_1)$, and the former two are isomorphic to each other and yield the group $\begin{pmatrix} G & \\ & \pm 1 \end{pmatrix}$, where G is the second group ($\cong D_6$) of §2.2. Similarly, the group G_4 in §2.3 comes from type $B_2 \times A_1$, and type $A_1 \times A_1 \times A_1$ is responsible for the groups G_1, G_2, G_3, and $\begin{pmatrix} G & \\ & \pm 1 \end{pmatrix}$, where G is the first group ($\cong C_2 \times C_2$) in §2.2. The remaining two groups in §2.3 are non-effective and thus, strictly speaking, they are not covered by the above discussion. However, non-effective groups can in fact also be treated in a very similar manner by using Farkas's method of "rooting sections" (see [F]).

ACKNOWLEDGMENTS

It is a pleasure to thank Kenny Brown (Glasgow) for an informative correspondence concerning regularity of invariant algebras (in a broader context than discussed here). In particular, I learned the equivalence 1.3 from him. I would also like to thank Professor Neubüser and Dr. Werner Nickel (both Aachen) for help with GAP. The program `multinv.g` incorporates preliminary versions of some GAP functions that were generously made available to the author by Dr. Werner Nickel. Finally, I gratefully acknowledge the referee's comments about root systems which lead to §2.5.

REFERENCES

[Bou] N. Bourbaki, *Groupes et algèbres de Lie, chap. 4–6*, Hermann, Paris, 1968.
[Bou2] ———, *Algèbre commutative, chap. 5–6*, Hermann, Paris, 1964.
[BH] W. Bruns and J. Herzog, *Cohen-Macaulay rings*, Cambridge University Press, Cambridge, 1993.
[F] D. R. Farkas, *Reflection groups and multiplicative invariants*, Rocky Mt. J. 16 (1986), 215–222.
[F2] ———, *Multiplicative invariants*, Enseign. Math. 30 (1984), 141–157.
[F3] ———, *The stretched weight lattices of a Weyl group*, Proc. Amer. Math. Soc. 92 (1984), 473–477.
[Kap] I. Kaplansky, *Fields and rings*, 2nd ed., University of Chicago Press, Chicago, 1972.
[Lam] T. Y. Lam, *Serre's conjecture*, Springer Lecture Notes in Math., Vol. 635, Springer-Verlag, Berlin Heidelberg, 1978.
[L] M. Lorenz, *Class groups of multiplicative invariants*, J. Algebra (to appear).
[Mat] H. Matsumura, *Commutative algebra*, 2nd ed., Benjamin/Cummings Publ. Co., Reading, 1980.
[M] S. Montgomery, *Fixed rings of finite automorphism groups of associative rings*, Lect. Notes in Math., No. 818, Springer, Berlin, 1980.
[S] J. P. Serre, *Groupes finis d'automorphismes d'anneaux locaux réguliers*, Colloque d'algèbre, No. 8, École Norm. Sup. des Jeunes Filles, Paris, 1967.
[St] R. Steinberg, *On a theorem of Pittie*, Topology 14 (1975), 173–177.

Received: July 1995

Revised: September 1995