Illinois Journal of Mathematics
Volume 52, Number 2, Summer 2008, Pages 645–652
S 0019-2082

ORBITS OF AUTOMORPHISMS OF INTEGRAL DOMAINS

PRAMOD K. SHARMA

ABSTRACT. Let R be an integral domain. We study the structure of R under the condition that the orbit space $R/Aut(R)$ is finite. It is proved that if R is Noetherian, then $|R/Aut(R)| = \infty$ unless R is a finite field (Theorem 15 and Corollary 16). Furthermore, we give an example of an infinite integral domain with $|R/Aut(R)| < \infty$.

1. Introduction

All rings are commutative with identity $\neq 0$. Kiran Kedlaya and Bjorn Poonen [3, Theorem 1.1] have proved if K is a field on which the number of orbits of $Aut(K)$ is finite, then K is finite. Furthermore, in [3, Remark 1.11], it is stated that "we do not know whether there exists an infinite integral domain R such that $Aut(R)$ has finitely many orbits on R". In this note, we prove the existence of such an integral domain. In Section 2, we collect some facts, essentially from [3], to be used freely in sequel. If R is an integral domain, then orbit of any $\lambda \in R$ is denoted by $o(\lambda)$.

In Section 3, we study orbit space of integral domains. Apart from other results, we prove that if A is an integral domain such that $|A/Aut(A)| < \infty$, then elements of A with finite orbits form a subfield which is integrally closed in A (Lemma 11). Moreover, if $Aut(A)$ is torsion, then it is finite and A is a finite field (Theorem 12).

In Section 4, we prove that for any Noetherian integral domain R if $|R/Aut(R)| < \infty$, R is a finite field (Corollary 16). We also give a characterization of the structure of integral domains R having characteristic $p > 2$ and $|R/Aut(R)| < \infty$ (Theorem 17). Finally, we give an example of an infinite integral domain with finitely many orbits.

Received March 9, 2007; received in final form March 29, 2007.
2000 *Mathematics Subject Classification.* 13G05, 13A99.

2. Some basic facts

We shall collect here some basic facts, which either appear in [3] or are immediate from results therein to be used freely in sequel. Throughout this section, R is an integral domain, such that $|R/Aut(R)| < \infty$. Thus, characteristic of R is $p > 0$. Let $\mathbb{F}_p$ be the prime subfield of R. Then E, the integral closure of $\mathbb{F}_p$ in R, is a finite field. Thus, R contains finitely many roots of unity. For any subset S, of a ring R and $n \geq 1$, we shall write $S^n = \{a^n : a \in S\}$. We now note the following:

(i) Let S be a subset of R invariant under the action of $Aut(R)$. Then $S = S^p$. In particular $R = R^p$.

As S is invariant under the action of $Aut(R)$,

$$S \supset S^p \supset S^{p^2} \supset \cdots \supset S^{p^n} \supset \cdots$$

is a chain of $Aut(R)$ invariant subsets of R. As $|R/Aut(R)| < \infty$, there exists $n \geq 1$, such that $S^{p^n} = S^{p^{n+1}}$. Therefore, for any $\lambda \in S$, there exists $\mu \in S$ such that

$$\begin{aligned} \lambda^{p^n} &= \mu^{p^{n+1}} \\ &\implies \quad (\lambda - \mu^p)^{p^n} = 0 \\ &\implies \quad \lambda = \mu^p. \end{aligned}$$

Hence, $S = S^p$, and the result follows.

(ii) If R is integrally closed and contains no primitive qth root of unity for a prime q, then for any $Aut(R)$ invariant subset S of R, $S = S^q$. Thus, in particular, $R = R^q$.

Proceeding as in (i), there exists $n \geq 1$, such that $S^{q^n} = S^{q^{n+1}}$. Therefore, for any $\lambda \in S$, there exists $\mu \in S$ such that

$$\begin{aligned} \lambda^{q^n} &= \mu^{q^{n+1}} \\ &\implies \quad (\lambda \mu^{-q})^{q^n} = 1 \\ &\implies \quad \lambda = \mu^q. \end{aligned}$$

Therefore $S = S^q$, and hence, $R = R^q$.

Following almost verbatim the proof of [3, Theorem 1.1], we get that $R = E \oplus I$ where I is the divisible submodule of the $\mathbb{F}_p[X]$-module R where $X : R \longrightarrow R$ is the Frobenius automorphism of R. Lemmas 1.7 and 1.8 in [3] also hold for any integral domain R such that $|R/Aut(R)| < \infty$. Unfortunately, [3, Theorem 1.1] fails to hold for integral domains in general since the last part of the proof needs $x \in R^*$, such that $Tr(x) = 0$ and $x^{-1} \in R^*$.

If we assume $Char.R = p > 2$, then by [3, Remark 1.9], I is an ideal. Hence, we have the following.

Let R be an integral domain of characteristic $p > 2$. If $|R/Aut(R)| < \infty$, then $R = E \oplus I$, where E is the integral closure of $\mathbb{F}_p$ in R and I is a maximal ideal of R.

The ideal I is invariant under the action of $Aut(R)$. Hence, $I^p = I$. This implies that the ideal I is equal to its pth power. Hence, I is an idempotent ideal. Therefore, if R contains no idempotent ideal, then R is a field. This, in particular, implies that if R is a Noetherian domain of characteristic $p > 2$ with $|R/Aut(R)| < \infty$, then R is a field.

3. Overture

In this section, unless otherwise specified, (R, m) is a quasi-local domain $\neq$(field), i.e., an integral domain with exactly one maximal ideal which is not a field.

LEMMA 1. *If each orbit of m under the action of $Aut(R)$ is finite, then each orbit of R under the action of $Aut(R)$ is finite.*

Proof. Let $\lambda \in R$. Choose a nonzero element $x \in m$. Then for any $\sigma \in Aut(R)$,

$$\begin{aligned} &\sigma(\lambda x) = \sigma(\lambda)\sigma(x) \\ \implies \quad &\sigma(\lambda) = \sigma(\lambda x)/\sigma(x). \end{aligned}$$

Hence, as $x, \lambda x \in m$, and each orbit of m under the action of $Aut(R)$ is finite, $|o(\lambda)|$ is finite. □

LEMMA 2. (i) *If $|R/Aut(R)| < \infty$, then $|m/Aut(R)| < \infty$ and also*

$$|(R/m)/Aut(R/m)| < \infty.$$

(ii) *Assume $|m/Aut(R)| < \infty$ and $|(R/m)/Aut(R/m)| < \infty$. We have*

(a) *If characteristic of R is 0, then*

$$|R/Aut(R)| < \infty.$$

(b) *If $|R/m| = t + 1$, and R has no nontrivial tth root of unity, then*

$$|R/Aut(R)| < \infty.$$

Proof. (i) As m is invariant under the action of $Aut(R)$, the inclusion map from m to R induces an injection

$$m/Aut(R) \to R/Aut(R).$$

Furthermore, the natural map from R to R/m induces a surjection

$$R/Aut(R) \to \big((R/m)/Aut(R/m)\big).$$

Hence, as $|R/Aut(R)| < \infty$, the result follows.

(ii) By assumption, $|(R/m)/Aut(R/m)| < \infty$. Hence, by [3, Theorem 1.1], R/m is finite. Let the characteristic of R/m be $p > 0$. We now prove the following.

(a) Multiplication by p induces the bijection

$$R/Aut(R) \backsimeq pR/Aut(R).$$

Hence, as $pR/Aut(R) \subset m/Aut(R)$ and $|m/Aut(R)| < \infty$, the result follows.

(b) Since $|m/Aut(R)| < \infty$, it suffices to prove the assertion that $|(R - m)/Aut(R)| < \infty|$. As $|R/m| = t + 1$, for any $\lambda \in R - m$, $\lambda^t - 1 \in m$. Furthermore, as R is an integral domain with no nontrivial tth root of unity, the map

$$R - m \longrightarrow m,$$
$$\lambda \mapsto \lambda^t - 1$$

is injective. This induces the injection

$$(R - m)/Aut(R) \longrightarrow m/Aut(R).$$

Therefore, $|(R - m)/Aut(R)| < \infty$. $\square$

Lemma 3. *If (R, m) is Noetherian domain such that $|m/Aut(R)| < \infty$, then R is a field.*

Proof. Clearly, m^i is closed under the action of $Aut(R)$ for all $i \geq 1$. As $|m/Aut(R)| < \infty$, and

$$m \supset m^2 \supset \cdots \supset m^i \supset m^{i+1} \supset \cdots,$$

there exists $n \geq 1$, such that $m^n = m^{n+1}$. Hence, $m = 0$. Therefore, R is a field. $\square$

Remark 4. (i) If (R, m) is Noetherian which is not a field, then $|R/Aut(R)| = \infty$.

(ii) Lemma is true even if R is not an integral domain, but $m \neq Nil(R)$.

Lemma 5. *Let A be a ring such that $|A/Aut(A)| < \infty$. If λ is a nonzero divisor in A such that $|o(\lambda)| = 1$, then λ is a unit.*

Proof. Note that

$$A \supset \lambda A \supset \lambda^2 A \supset \cdots \supset \lambda^m A \supset \cdots,$$

is a descending chain of orbit closed subsets of A. As $|A/Aut(A)| < \infty$, there exists $m \geq 1$, such that $\lambda^m A = \lambda^{m+1} A$. Therefore, $1 = \lambda a$ for some $a \in A$. Hence, λ is a unit. $\square$

Remarks 6. (i) If A is an integral domain, then

$$L = A^{Aut(A)} = \{\lambda \in A | \sigma(\lambda) = \lambda \text{ for all } \sigma \in Aut(A)\}$$

is a finite subfield of A. Furthermore, the integral closure of L in A is a finite field.

(ii) Let A be an integral domain. If $\lambda \in A$ and $o(\lambda) < \infty$, then λ is integral over $A^{Aut(A)} = L$, since if $o(\lambda) = \{\lambda = \lambda_1, \lambda_2, \ldots, \lambda_t\}$, then λ is root of the polynomial $p(X) = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_t) \in L[X]$. Therefore, $\{\lambda \in A : |o(\lambda)| < \infty\}$ is the integral closure of L in A.

Corollary 7. *Let λ be a nonzero divisor in a ring A such that $|A/Aut(A)| < \infty$. If $|o(\lambda)| < \infty$, then λ is a unit.*

Proof. Let $o(\lambda) = \{\lambda = \lambda_1, \lambda_2, \ldots, \lambda_t\}$. Then $\mu = \lambda_1 \cdot \lambda_2 \cdots \lambda_t \in A^{Aut(A)}$. Hence μ is unit. Therefore, λ is a unit. □

Corollary 8. *Let for a quasi-local domain (R, m), $|R/Aut(R)| < \infty$. Then for any $x\,(\neq 0) \in m, |o(x)| = \infty$.*

Theorem 9. *Let A be a Noetherian integral domain such that $|A/Aut(A)| < \infty$. Let $J = J(A)$ be the Jacobson radical of A. Then $J = (0)$.*

Proof. Clearly, for any $\sigma \in Aut(A), \sigma(J) \subset J$. Therefore, $\sigma(J^m) \subset J^m$ for all $m \geq 1$. As $|A/Aut(A)| < \infty$, and

$$J \supset J^2 \supset \cdots \supset J^i \supset \cdots,$$

there exists $m \geq 1$, such that $J^m = J^{m+1}$. Hence, $J = (0)$. □

Corollary 10. *If R is a Noetherian semi-local integral domain and $|R/Aut(R)| < \infty$, then R is a field.*

Lemma 11. *Let A be an integral domain such that $|A/Aut(A)| < \infty$. Then $E = \{\lambda \in A : |o(\lambda)| < \infty\}$ is a finite subfield of A and is integrally closed in A.*

Proof. By Corollary 7, nonzero elements in E are units in A. It is clear that for any $\lambda, \mu \in E, \lambda + \mu \in E, \lambda\mu \in E$ and if $\lambda \neq 0$, then $\lambda^{-1} \in E$. Therefore, E is a finite subfield of A. Furthermore, let $a \in A$ be integral over E. Then since for any $\sigma \in Aut(A)$, $\sigma(E) \subset E, \sigma(a)$ is integral over E. Thus, as $|o(\lambda)| < \infty$ for all $\lambda \in E$, $|o(a)| < \infty$, and hence, $a \in E$. Therefore, E is integrally closed in A. □

Theorem 12. *Let A be an integral domain and $|A/Aut(A)| < \infty$. Then $Aut(A)$ is a torsion group if and only if the Frobenius automorphism of A is of finite order. Moreover, in this case $Aut(A)$ is finite and A is a finite field.*

Proof. As $|A/Aut(A)| < \infty$, from Section 2, A has characteristic $p > 0$ and the Frobenius endomorphism τ of A is an automorphism. Thus, if $Aut(A)$ is torsion τ is of finite order. Conversely, if τ has finite order, say n. Then every element of A is root of the polynomial $X^{p^n} - X$. Hence, $|A| \leq p^n$. Thus, A being finite integral domain is a field, and $Aut(A)$ is finite. □

4. Main results

In this section, we shall prove that for any integral domain R which contains a prime element, $|R/Aut(R)| = \infty$. We also show that if R is a Noetherian integral domain, which is not a field, $|R/Aut(R)| = \infty$ (Theorem 15). Finally, we give an example of an infinite integral domain which has finite number of orbits under the action of its automorphism group.

THEOREM 13. *Let R be an integral domain which contains a prime element π. Then $|R/Aut(R)| = \infty$.*

Proof. Assume $|R/Aut(R)| < \infty$. Note that the set $\{\pi^n : n \geq 1\}$ is infinite. Thus, there exist $m > n$ and $\sigma \in Aut(R)$ such that $\sigma(\pi^n) = \pi^m$. Then σ induces the ring isomorphism:

$$R/(\pi^n) \xrightarrow{\overline{\sigma}} R/(\pi^m),$$
$$\overline{\lambda} = \lambda + (\pi^n) \longmapsto \sigma(\lambda) + (\pi^m) = \overline{\sigma(\lambda)}.$$

The element $\overline{\pi}$ in $R/(\pi^m)$ is nilpotent of degree m. Further, $R/(\pi^n)$ has no nilpotent element of degree m. Hence, the ring $R/(\pi^n)$ is not isomorphic to the ring $R/(\pi^m)$ for $m > n$. Therefore, π^m cannot be in $o(\pi^n)$ for $m > n$. This implies $|R/Aut(R)| = \infty$. $\square$

REMARK 14. Theorem is true for any ring R having a prime element which is not a zero divisor. Hence, if R is a ring which is not necessarily an integral domain, then for the polynomial ring $R[X] = A$, $|A/Aut(A)| = \infty$.

THEOREM 15. *Let R be a Noetherian integral domain which is not a field. Then $|R/Aut(R)| = \infty$.*

Proof. Let c be a nonzero, nonunit element of R. Then for any $m, n \in \mathbb{N}, m \neq n, c^m \neq c^n$. Assume $|R/Aut(R)| < \infty$. Then there exists $m < n$ and $\sigma \in Aut(R)$, such that $\sigma(c^n) = c^m$. Let $I = Rc^n$. Then $I \subsetneqq \sigma(I)$, and hence

$$I \subsetneqq \sigma(I) \subsetneqq \cdots \subsetneqq \sigma^n(I) \subsetneqq \cdots$$

is an infinite ascending chain of ideals in R. As R is Noetherian, this is not possible. Thus, the result follows. $\square$

COROLLARY 16. *Let R be a Noetherian integral domain. If $|R/Aut(R)| < \infty$, then R is a finite field.*

Proof. By Theorem 15, R is a field. Hence, by [3, Theorem 1.11], R is a finite. $\square$

THEOREM 17. *Let R be an integral domain of characteristic $p > 2$. Let E be the integral closure in R of the prime subfield $\mathbb{F}_p$ of R. Then $|R/Aut(R)| < \infty$ if and only if E is a finite field and $R = E \oplus m$ where m is a maximal ideal of R such that $\sigma(m) = m$ for every $\sigma \in Aut(R)$ and $|m/Aut(R)| < \infty$.*

Proof. If $|R/Aut(R)| < \infty$, then the result is noted in Section 2. Conversely, let $m = o(x_1) \cup \cdots \cup o(x_k)$. For any $\lambda \in R$, $\lambda = b + y$ where $b \in E$ and $y \in m$. Assume $y \in o(x_1)$. Then there exists $\sigma \in Aut(R)$ such that $\sigma(x_1) = y$. Hence, as $\sigma(E) = E$, we have $a \in E$ such that $\lambda = \sigma(a + x_1)$. Therefore, $|R/Aut(R)| = \infty$.

We shall now give an infinite integral domain with finite number of orbits under the action of its automorphism group.

We follow the following strategy.

Let (R, m) be a quasi-local integral domain of characteristic $p > 0$, which is not a field and $|m/Aut(R)| < \infty$. Then $A = \mathbb{F}_p + m$ is a local domain with maximal ideal m. For any $\sigma \in Aut(R), \sigma(A) = A$. Hence, $|m/Aut(A)| < \infty$. This implies $|A/Aut(A)| < \infty$. As m is infinite, A is the required example. Thus, to complete the proof, it is sufficient to give a quasi-local integral domain (R, m) with the required properties. We shall do this below. □

Examples 18. Let (S, n) be a Noetherian, complete local integral domain which is not a field. Assume S contains a field of characteristic $p > 0$. Let K be the field of fractions of S and let R be the integral closure of S in the algebraic closure $\overline{K}$ of K. As (S, n) is Henselian, R is quasi-local [5, (30.5)]. Let m be the maximal ideal of R. Then (R, m) is quasi-local integral domain with field of fractions $\overline{K}$. We claim the following below.

For any two nonzero elements $x, y \in m$, there exists $\sigma \in Aut(R)$, such that $\sigma(x) = y$. Thus, $|m/Aut(R)| = 2$. We shall prove the claim in steps.

Step 1. $S[x]$ is complete local integral domain.

We have $S \subset S[x] \subset R$, where each step is an integral ring extension. As R is quasi-local, $m \cap S[x]$ is the unique maximal ideal of $S[x]$. Thus, $S[x]$ is local. As x is integral over S, $S[x]$ is a finitely generated S-module. Hence, as (S, n) is complete local ring, the ring $S[x]$ is complete with respect to the ideal $nS[x]$ [1, Proposition 10.13]. Now, as the radical of $nS[x]$ is the unique maximal ideal of $S[x]$, $S[x]$ is a complete local integral domain.

Step 2. The element x is part of a system of parameters of $S[x]$. Note that $x \in m \cap S[x]$. Therefore, x is in the maximal ideal of $S[x]$. Since $x \neq 0$, using [4, Chapter V, Proposition 4.11], we get that x is a part of a system of parameters of the complete local ring $S[x]$.

Step 3. $|m/Aut(R)| = 2$.

Let $dim.S = dim.S[x] = d$. Then by Step 2, $S[x]$ has a system of parameters $\{x = x_1, \ldots, x_d\}$. If L is a coefficient field of S, then it is also coefficient field of $S[x]$ and $S[x]$ is finite module over $L[[x_1, \ldots, x_d]]$ in a natural way [5, Corollary 31.6]. Therefore, $S[x]$ is integral over $L[[x_1, \ldots, x_d]]$ and so is R. Consequently, $\overline{K}$ is algebraic closure of the field of fractions of $L[[x_1, \ldots, x_d]]$ and R is the integral closure of $L[[x_1, \ldots, x_d]]$ in $\overline{K}$. Similarly, $S[y]$ is a complete local integral domain with a system of parameters $\{y = y_1, \ldots, y_d\}$ with coefficient field L. Moreover, $L[[y_1, \ldots, y_d]] \subset S[y] \subset R$ is a chain of integral extensions. Using [4, Chapter V, Corollary 4.19], we note that the map

$$L[[x_1,\ldots,x_d]] \xrightarrow{\sigma} L[[y_1,\ldots,y_d]],$$
$$p((x_1,\ldots,x_d)) \longmapsto p((y_1,\ldots,y_d))$$

is an isomorphism such that $\sigma|L = id$, and $\sigma(x_i) = y_i$ for all $i \geq 1$. As $\overline{K}$ is algebraic closure of the field of fractions of $L[[x_1,\ldots,x_d]]\,(L[[y_1,\ldots,y_d]])$, σ extends to an automorphism of $\overline{K}$ (not necessarily unique). Restriction of this automorphism to R gives an automorphism of R which maps x to y since R is the integral closure of $L[[x_1,\ldots,x_d]]\,(L[[y_1,\ldots,y_d]])$ in $\overline{K}$. Therefore, $|m/Aut(R)| = 2$. In view of above, the quasi-local ring $(R.m)$ is the required quasi-local domain. Hence, the assertion follows.

Acknowledgments. I am thankful to Melvin Hochster for some very useful e-mail exchanges which helped in the construction of the example. I am also thankful to Moshe Roitman and George Bergman for some valuable discussions. Finally, thanks are due to the referee who has suggested several improvements in presentation of the article.

References

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, 1969. MR 0242802

[2] D. Eisenbud, *Commutative algebra with a view towards algebraic geometry*, Graduate Texts in Mathematics, Springer, 1994. MR 1322960

[3] K. S. Kedlaya and B. Poonen, *Orbits of automorphisms of groups of fields*, J. Algebra **293** (2005), 167–184. MR 2173971

[4] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser, 1985. MR 0789602

[5] M. Nagata, *Local rings*, Robert E. Krieger Publishing Company, 1975. MR 0460307

Pramod K. Sharma, School of Mathematics, Vigyan Bhawan, Khandwa Road, Indore-452 017, India

E-mail address: pksharma1944@yahoo.com