Canad. Math. Bull. Vol. **25** (4), 1982

RINGS WITH AUTOMORPHISMS LEAVING NO NONTRIVIAL PROPER IDEALS INVARIANT

BY
AHMAD SHAMSUDDIN

ABSTRACT. If an automorphism σ on a ring R (with 1) leaves no non-trivial proper ideals of R invariant then we say that R is σ-simple. We construct examples of σ-simple rings and prove that finitely generated σ-simple algebras over fields are regular. A geometric interpretation of these concepts is also discussed.

Let R be a commutative ring, always with 1, and let σ be a ring endomorphism on R. We say that a subset S of R is invariant under σ if $\sigma S \subseteq S$. Denote by $\text{Aut}(R)$ the group of all automorphisms on R. If G is a subgroup of $\text{Aut}(R)$ then S is said to be G-invariant in case $\sigma S \subseteq S$ for all $\sigma \in G$. We say that R is G-simple in case R has no G-invariant non-trivial proper ideals of R, and when $G = \langle \sigma \rangle$ we say R is σ-simple if it is G-simple. When R is a finitely generated algebra over an algebraically closed field k and G is a group of k-automorphisms on R then R is the coordinate ring of some affine closed subset X of the affine space $A^n(k)$ and each $\sigma \in G$ induces a homeomorphism on X; the set of all such homeomorphisms forms a group $\bar{G}$. If R is G-simple then no non-empty proper affine closed subset of X is $\bar{G}$-invariant.

In the first section of this paper we study the general properties of these rings and prove that if R is a finitely generated algebra over a field such that R is a G-simple domain then $R_{\mathbf{p}}$ is regular for every prime ideal $\mathbf{p}$ of R. The second section contains examples of σ-simple rings.

1. **General properties of G-simple rings.** Throughout this section, G is a subgroup of $\text{Aut}(R)$.

1.1. If R is G-simple then $R^G = \{a \in R : \sigma a = a \text{ for all } \sigma \in G\}$ is a subfield of R.

1.2. If R is a domain and R is G-simple then R is also H-simple for every subgroup H of G of finite index.

Idea of proof. Suppose that I is an H-invariant non-zero proper ideal of R. If

$$G = H \cup \sigma_1 H \cup \cdots \cup \sigma_r H$$

Received by the editors October 28, 1980 and, in revised form, March 31, 1981.
(1980) AMS subject classification index: 13B10

is a coset decomposition of H in G then

$$J = I \cap \sigma_1 I \cap \cdots \cap \sigma_r I$$

is a non-zero proper G-invariant ideal of R.

1.3. Let R be a noetherian ring. If no subgroup of G of finite index leaves any non-zero *prime* ideal of R invariant then R is G-simple. To see this, note first that an ideal I of R is G-invariant if and only if $\sigma I = I$ for all $\sigma \in G$. Suppose that I is a G-invariant ideal and let $\mathbf{p}$ be a prime ideal of R minimal over I so that $\sigma\mathbf{p}$ is also minimal over I for every $\sigma \in G$. But because R is noetherian, there are only finitely many primes minimal over I, thus

$$\{\sigma\mathbf{p} : \sigma \in G\} = \{\mathbf{p}, \sigma_1\mathbf{p}, \ldots, \sigma_r\mathbf{p}\}$$

where $\mathbf{p}$, $\sigma_1\mathbf{p}, \ldots, \sigma_r\mathbf{p}$ are all distinct. If $H = \{\tau \in G : \tau\mathbf{p} = \mathbf{p}\}$ then H is a subgroup of G and

$$G = H \cup \sigma_1 H \cup \cdots \cup \sigma_r H$$

is a coset decomposition of H in G.

1.4. If R is G-simple then it has zero Jacobson radical; in particular, R does not have non-zero nilpotent elements.

1.5. If some maximal ideal m of a G-simple ring R has finite orbits under G then R is a finite product of fields. For, let $\mathbf{m}$, $\sigma_1\mathbf{m}, \ldots, \sigma_r\mathbf{m}$ denote the distinct members of the set $\{\sigma\mathbf{m} : \sigma \in G\}$. Then $\mathbf{m} \cap \sigma_1\mathbf{m} \cap \cdots \cap \sigma_r\mathbf{m} = 0$ and we have an injective ring homomorphism

$$f : R \to R/\mathbf{m} \times R/\sigma_1\mathbf{m} \times \cdots \times R/\sigma_r\mathbf{m}$$

given by

$$f(a) = (a + \mathbf{m}, a + \sigma_1\mathbf{m}, \ldots, a + \sigma_r\mathbf{m}).$$

It follows from the Chinese Remainder Theorem that f is also onto. Hence f is an isomorphism.

The above shows that if G is finite then R is a finite direct product of fields.

1.6. Let B a commutative integral domain and let A be a subring of B such that B is integral over A. Let G be a subgroup of $\mathrm{Aut}(B)$ such that A is G-invariant. Then A is G-simple if and only if B is G-simple.

Proof. Let I be a non-trivial proper G-invariant ideal of B. Then because B is integral over A, $I \cap A$ is non-trivial and clearly it is a G-invariant ideal of A. Conversely, if I is non-zero proper G-invariant ideal of A then it follows from the Going-Up theorem that BI is a non-trivial proper G-invariant ideal of B.

1.7. If F is any field then any F-automorphism on $F[x, y]$ leaves a non-trivial proper ideal invariant.

Proof. Let k denote the algebraic closure of F. Lane in [3] proved that

https://doi.org/10.4153/CMB-1982-069-0 Published online by Cambridge University Press

every k-automorphism leaves a non-trivial proper ideal of $k[x, y]$ invariant. Now $k[x, y]$ is integral over $F[x, y]$, so the result follows from 1.6.

In particular, $\mathbb{R}[x, y]$ is never G-simple for any cyclic subgroup G of $\mathrm{Aut}(R[x, y])$.

I am grateful to the referee for pointing out the following additional property of G-simple rings.

1.8. Let R be a finitely generated algebra over a finite field k and suppose that R is an integral domain. If R is G-simple for some G then it is a finite field.

Proof. Let $\mathbf{m}$ be a maximal ideal of R then $K = R/\mathbf{m}$ is a finitely generated k-algebra which is a field. Hence K is algebraic over k and since k is finite, K is itself finite. Thus there exist finitely many maximal ideals $\mathbf{m}'$ of R such that $R/\mathbf{m}' \cong K$ as fields. Since $R/\mathbf{m} \cong R/\sigma_{\mathbf{m}}$ (as fields) for each $\sigma \in G$, there are $\sigma_1, \ldots, \sigma_r \in G$ such that $\mathbf{m}$, $\sigma_1\mathbf{m}, \ldots, \sigma_r\mathbf{m}$ are the distinct members of $\{\sigma\mathbf{m} : \sigma \in G\}$. It follows that $\mathbf{m} = 0$ and so $R = K$ is a finite field.

The examples of σ-simple algebras constructed in §2 are all regular at each of their prime ideals. This leads one to conjecture that a noetherian G-simple domain is always regular. We shall now show that this is indeed the case for finitely generated algebras over fields.

Let $X = \mathrm{Spec}\, R$ and recall that X is a topological space in which the closed sets are of the form $V(I) = \{\mathbf{p} \in X : I \subset \mathbf{p}\}$, where I is an ideal of R. Note that each $\sigma \in G$ induces a homeomorphism on X, denoted by $\bar{\sigma}$. Suppose that $\bar{\sigma}(V(I)) = V(I)$ for all $\sigma \in G$ then $V(\sigma I) = V(I)$ and hence $\sqrt{\sigma I} = \sigma \sqrt{I} = \sqrt{I}$ for all $\sigma \in G$. Thus $I = 0$ or $I = R$ which shows that either $V(I) = X$ or $V(I) = \emptyset$. It follows that $\bar{G} = \{\bar{\sigma} : \sigma \in G\}$ leaves no non-empty closed subset of X invariant.

Suppose now that R is noetherian and

$$\mathrm{Reg}\, X = \{\mathbf{p} \in X : R_{\mathbf{p}} \text{ is a regular local ring}\}$$

$$\mathrm{Sing}\, X = X - \mathrm{Reg}\, X.$$

If $\mathbf{p} \in X$ then for every $\sigma \in G$ we have a ring isomorphism $R_{\mathbf{p}} \cong R_{\sigma\mathbf{p}}$ defined in the obvious way. Hence $\bar{G}$ leaves $\mathrm{Reg}\, X$ and $\mathrm{Sing}\, X$ invariant.

Following Matsumura [1], p. 246, we say that the ring R is a J-1 ring if $\mathrm{Sing}\, X$ is closed in X.

Theorem 1.9. *If R is a J-1 G-simple domain then R is regular at every prime* $\mathbf{p}$.

Proof. Since $\mathrm{Sing}\, X$ is $\bar{G}$-invariant, either $\mathrm{Sing}\, X = \emptyset$ or $\mathrm{Sing}\, X = X$. But clearly $(0) \notin \mathrm{Sing}\, X$, so $\mathrm{Sing}\, X = \emptyset$ and the result is now clear.

Corollary 1.10. *If R is a G-simple finitely generated algebra over a field then R is regular at every prime ideal* $\mathbf{p}$.

Proof. A f.g. algebra over a field is a J-1 ring, by Matsumura [1], p. 246.

We now mention briefly the geometric significance of the last Corollary. Let k be an algebraically closed field, let R be a finitely generated k-algebra which is a domain, let G be a group of k-automorphisms on R, and let $X = V(\mathbf{p})$ be the irreducible algebraic variety determined by R. If $a = (a_1, \ldots, a_n) \in X$, let $T_{X,a}$ denote the tangent space to X at a. Recall that $T_{X,a}$ is the linear subspace of A^n defined as the set of zeros of the polynomials

$$\sum_{i=1}^{n} \frac{\partial f}{\partial t_i}(a)(t_i - a_i), \quad f \in \mathbf{p}.$$

Then $T_{X,a}$ is a k-vector space, with origin at a. If m is an integer then the set

$$\{a \in X : \dim_k T_{X,a} \geq m\}$$

is closed in X (see Mumford [2], p. 3). We say that a point $a \in X$ is singular or regular according as $\dim_k T_{X,a} > \dim X =$ Krull dimension of R or $\dim T_{X,a} = \dim X$. It follows that the *singular locus*, namely the set

$$V = \{a \in X : \dim_k T_{X,a} > \dim X\}$$

is closed in X. If $a \in V$ then the maximal ideal $\mathbf{m}$ determined by a is a singular maximal ideal (that is $R_{\mathbf{m}}$ is not regular) and conversely, if $\mathbf{m}$ is a maximal ideal of R then the corresponding point of X determined by $\mathbf{m}$ is singular (see Shafarevich [4], pp. 81–84). The above Corollary then says that if R is G-simple then X has no singular points. In other words, X must be a smooth algebraic variety.

2. Examples of $\boldsymbol{\sigma}$-simple rings. We begin this section with the following

THEOREM 2.1. *Let A be a commutative domain and let σ be an injective ring endomorphism on $R = A[x]$, the ring of polynomials in the indeterminate x over A, such that $\sigma A \subset A$, and assume that A is σ-simple. Suppose that*

$$\sigma x = ax + b,\ a, b \in A,\ a \text{ invertible in } A.$$

If char $A = 0$ then R is σ-simple if and only if the equation

$$\sigma\xi = a\xi + b$$

has no solution $\xi \in A$.

If char $A = p > 0$ and the equations

$$\sigma u = a^i u \quad (i = 1, 2, \ldots)$$

have no solutions $u \in A$, then R is σ-simple if and only if the equations

$$\sigma\xi = a^{p^i}\xi + b^{p^i} \quad (i = 0, 1, 2, \ldots)$$

have no solutions in A.

Proof. Let I be a non-zero proper ideal of R invariant under σ and let C

denote the ideal of A consisting of all leading coefficients of all polynomials in I with minimum degree n together with 0. Because a is invertible in A, C is a (non-zero) ideal of A invariant under σ. Since A is σ-simple, $C=A$. Hence there is

$$f=\sum_{i=0}^{n} a_i x^i \in I, \quad a_i \in A, \quad a_n = 1.$$

Note that $g=\sigma f - a^n f \in I$, yet if $g \neq 0$ then $\deg g < n$, a contradiction. Hence $\sigma f = a^n f$ and so

$$\begin{aligned}\sigma f &= \sum_{i=0}^{n} (\sigma a_i)(ax+b)^i = \sum_{i=0}^{n} \sigma a_i \sum_{j=0}^{i} \binom{i}{j} a^j b^{i-j} x^j \\ &= \sum_{j=0}^{n} \left[\sum_{i=j}^{n} a^j (\sigma a_i)\binom{i}{j} b^{i-j}\right] x^j = \sum_{j=0}^{n} a^n a_j x^j\end{aligned}$$

from which we deduce that

$$\sum_{i=j}^{n} (\sigma a_i)\binom{i}{j} b^{i-j} = a^{n-j} a_j, \quad 0 \le j \le n. \tag{1}$$

If $1/n \in A$ (which is certainly the case if char $A=0$ in view of 1.1) then the substitution $j=n-1$ in (1) gives

$$\sigma\xi = a\xi + b \quad \text{where} \quad \xi = -\frac{1}{n} a_{n-1}$$

Conversely, if $\sigma\xi = a\xi + b$ for some $\xi \in A$ then $R(x-\xi)$ is invariant under σ.

If n is not invertible in A then write $n = p^r m$, $p \nmid m$. Note that

$$\binom{n}{j} \equiv 0 \pmod p \quad \text{if} \quad 0 \le j < p^r$$

$$\binom{n}{p^r} \equiv m \pmod p$$

so by substituting $j=n-1, n-2, \ldots, n-p^r$ successively in (1) and using the fact that the equations $\sigma u = a^i u$ $(i>1)$ have no solutions in A we find that

$$a_{n-j} = 0 \quad \text{if} \quad 1 \le j < p^r$$

and

$$\sigma\xi = a^{p^r}\xi + b^{p^r} \quad \text{where} \quad \xi = -\frac{1}{m} a_{n-p^r}.$$

Conversely, if $\sigma\xi = a^{p^r}\xi + b^{p^r}$ for some $\xi \in A$ then $x^{p^r} - \xi$ is invariant under σ. The proof is complete.

Suppose now that $a=1$ and let's try to find a criterion for σ-simplicity of R in the characteristic $p>0$ case. Put

$$A^{(\sigma)} = \{a \in A : \sigma a = a\}$$

https://doi.org/10.4153/CMB-1982-069-0 Published online by Cambridge University Press

and

$$A' = \{\sigma a - a : a \in A\}$$

so that A' is an $A^{(\sigma)}$-module. We prove that R is σ-simple if and only if the sum

$$A' + A^{(\sigma)}b + A^{(\sigma)}b^p + A^{(\sigma)}b^{p^2} + \cdots$$

is direct.

Assume first that the above sum is direct; we show that the system of equations (1) has no solution. Indeed, write $n = p^r m$ with $p \nmid m$. As above, we note that $\binom{n}{j} \equiv 0 \pmod p$ if $1 \leq j < p^r$ and $\binom{n}{p^r} \equiv m \pmod p$. Then by substituting $j = n-1, n-2, \ldots, n-p^r$ successively in (1) and using the assumption that the above sum is direct, we find that $a_{n-j} = 0$ if $1 \leq j < p^r$ and $a_{n-p^r} = \sigma\, a_{n-p^r} + mb^{p^r}$ which contradicts our assumption.

Conversely, if $(\sigma a - a) + \sum_{i=0}^r a_i b^{p^i} = 0$ where $a_i \in A^{(\sigma)}$ then the polynomial $a + \sum_{i=0}^r a_i x^{p^i}$ is invariant under σ.

THEOREM 2.2. *Let k be a field of characteristic* 0 *and let σ be the k-automorphism on $k[x]$ given by*

$$\sigma x = x + b, \quad b \neq 0 \in k.$$

Then $k[x]$ is σ-simple.

Proof. If there is $c \in k$ with $b + \sigma c = c$ then $b = 0$, a contradiction. k is clearly σ-simple, so the above theorem yields the result.

THEOREM 2.3. *Let k be a field of characteristic zero and let $k[t, x, y]$ denote the ring of polynomials in the indeterminates t, x, and y over k. Define a k-monomorphism σ on $k[t, x, y]$ by putting*

$$\sigma t = t + 1, \quad \sigma x = tx + 1, \quad \sigma y = ty + x.$$

Then σ extends uniquely to an automorphism on $k(t)[x, y] = R$, also denoted by σ, such that R is σ-simple.

Proof. We first show that there is no $p(t) \in k(t)$ such that

(1) $$p(t+1) = tp(t) + 1$$

and this will prove that $k(t)[x]$ is σ-simple, by Theorem 2.1. Thus suppose that $p(t) = f(t)/g(t)$ where $f(t)$, $g(t) \in k[t]$ are relatively prime and $g(t)$ is a monic polynomial. Then $p(t)$ satisfies (1) if and only if

(2) $$g(t)[f(t+1) - g(t+1)] = tf(t)g(t+1).$$

Hence $g(t) \mid tg(t+1)$. If $t \nmid g(t)$ then $g(t) \mid g(t+1)$ and so $g(t) \in k$. If $g(t) = tg_1(t)$

https://doi.org/10.4153/CMB-1982-069-0 Published online by Cambridge University Press

then $g_1(t) \mid (t+1)g_1(t+1)$, hence if $(t+1) \nmid g_1(t)$ then $g_1(t)$ is a constant. Continue in this fashion to conclude that

$$g(t) = t(t+1) \cdots (t+n).$$

It follows from (2) that $(t+n+1) \mid f(t+1)$ or $(t+n) \mid f(t)$ which contradicts the assumption that $f(t)$ and $g(t)$ are coprime. This shows that $k(t)[x]$ is σ-simple.

Next suppose that there is a polynomial $f(t, x) \in k(t)[x]$ that satisfies the equation

$$\sigma f(t, x) = tf(t, x) + x; \tag{3}$$

write

$$f(t, x) = \sum_{i=0}^{n} a_i(t)x^i, \quad a_i(t) \in k(t)$$

where $a_n(t) \neq 0$. If $n > 1$ then by comparing the leading coefficients of the polynomials in (3) we get

$$a_n(t+1)t^n = ta_n(t)$$

which is impossible in $k(t)$. Since $n \neq 0$ we must have $n = 1$, in which case

$$ta_1(t+1) = ta_1(t) + 1 \tag{4}$$

and an argument similar to that used in the first paragraph shows that equation (4) is impossible. It follows now from Theorem 2.1 that $k(t)[x, y]$ is σ-simple.

The above example must probably be contrasted with a result in [3], referred to previously, stating that if k is algebraically closed then every k-automorphism on $k[x, y]$ leaves a proper non-trivial ideal of $k[x, y]$ invariant.

THEOREM 2.4. *Let k be a field and let $R = k[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$ where $x_1, \ldots, x_n$ are indeterminates over k. Let $a_1, \ldots, a_n$ be elements of k such that*

$$a_1^{m_1} \cdots a_n^{m_n} = 1 (m_1, \ldots, m_n \in \mathbb{Z}) \Rightarrow m_1 = \cdots = m_n = 0.$$

Define a k-automorphism σ on R by

$$\sigma x_i = a_i x_i.$$

Then R is σ-simple.

Proof. We show this by induction on n, the case $n = 0$ being trivial. Assume that $n \geq 1$ and that $A = k[x_1, x_1^{-1}, \ldots, x_{n-1}, x_{n-1}^{-1}]$ is σ-simple. Let I be a non-zero proper ideal of $R = A[x_n, x_n^{-1}]$ invariant under σ. Then by the proof of Theorem 2.1, $I \cap R[x_n]$ contains a monic polynomial of degree m such that $\sigma f = a_n^m f$. Write $f = \sum_{i=0}^m g_i x_n^i$, $g_i \in A$ and $g_m = 1$. Then $\sigma g_i = a_n^{m-i} g_i$ for each i, so either $g_i = 0$ or g_i is invertible in A. In the second case, g_i must have the form $bx_1^{t_1} \cdots x_{n-1}^{t_{n-1}}$ where $t_1, \ldots, t_{n-1} \in \mathbb{Z}$ and $b \in k$, $b \neq 0$. Thus

$$a_1^{t_1} \cdots a_{n-1}^{t_{n-1}} a_n^{i-m} = 1$$

and this gives $i-m=t_1=\cdots=t_{n-1}=0$. Thus $I=R$, a contradiction. The proof is complete by induction.

THEOREM 2.5. *Let $A=\mathbb{R}[x_1, x_2, \ldots, x_{2n}]$ be the $\mathbb{R}$-algebra generated by the indeterminates $x_1, \ldots, x_{2n}$ subject to the conditions*

$$x_1^2+x_2^2=x_3^2+x_4^2=\cdots=x_{2n-1}^2+x_{2n}^2=1.$$

Let $\alpha_1, \ldots, \alpha_n$ be real numbers such that $1, \alpha_1, \ldots, \alpha_n$ are linearly independent in $\mathbb{R}$ over $\mathbb{Z}$. Define the $\mathbb{R}$-automorphism σ on A by

$$\sigma x_1=x_1 \cos 2\pi\alpha_1-x_2 \sin 2\pi\alpha_1, \quad \sigma x_2=x_1 \sin 2\pi\alpha_1+x_2 \cos 2\pi\alpha_1$$

$$\sigma x_{2n-1}=x_{2n-1} \cos 2\pi\alpha_n-x_{2n} \sin 2\pi\alpha_n, \quad \sigma x_{2n}=x_{2n-1} \sin 2\pi\alpha_n+x_{2n}\pi\alpha_n.$$

Then A is σ-simple.

Proof. Note that $(\sigma x_1)^2+(\sigma x_2)^2=\sigma(x_1^2+x_2^2)=1$, etc. so σ is indeed an automorphism on A. Extend σ to a $\mathbb{C}$-automorphism on $B=\mathbb{C}[x_1, x_2, \ldots, x_{2n-1}, x_{2n}]$ in the obvious way. It is sufficient to show that B is σ-simple.

Note that

$$(x_1+ix_2)(x_1-ix_2)=\cdots=(x_{2n-1}+ix_{2n})(x_{2n-1}-ix_{2n})=1$$

so with $y_1=x_1+ix_2, \ldots, y_n=x_{2n-1}+ix_{2n}$ it is easy to see that

$$B=\mathbb{C}[y_1, y_1^{-1}, \ldots, y_n, y_n^{-1}].$$

Note that

$$\sigma y_1=e^{2\pi i\alpha_1}y_1, \ldots, \sigma y_n=e^{2\pi i\alpha_n}y_n.$$

Put $a_1=e^{2\pi i\alpha_1}, \ldots, a_n=e^{2\pi i\alpha_n}$. The condition that $1, \alpha_1, \ldots, \alpha_n$ are $\mathbb{Z}$-linearly independent is equivalent to the condition that

$$a_1^{m_1}\cdots a_n^{m_n}=1(m_1, \ldots, m_n \in \mathbb{Z}) \Rightarrow m_1=\cdots=m_n=0.$$

Theorem 2.4 now finishes the proof.

ACKNOWLEDGEMENT. I wish to thank Mr. R. Hart for his help during the preparation of this paper. I also wish to thank the referee for making many remarks that helped considerably in sharpening the results; in particular, the characteristic p case in Theorem 2.1 is due to him.

REFERENCES

1. H. Matsumura, *Commutative Algebra*, Benjamin, New-York.
2. D. Mumford, *Algebraic Geometry I: Complex Projective Varieties*, Springer-Verlag, Berlin, Heidelberg, New York.

3. D. R. Lane, Fixed points of affine Cremona transformations of the plane over an algebraically closed field, Amer. J. Math., Vol. 97, No. 3, pp. 707–732.

4. I. R. Shafarevich, *Basic Algebraic Geometry*, Springer-Verlag.

Mathematics Department
American University of Beirut
Beirut, Lebanon

https://doi.org/10.4153/CMB-1982-069-0 Published online by Cambridge University Press