AUTOMORPHISMS OF THE TWO-DIMENSIONAL GENERAI LINEAR GROUP OVER A EUCLIDEAN RING

JOSEPH LANDIN AND IRVING REINER

1. **Introduction.** Let E denote a free R-module of rank n over a ring R, and let $GL_n(R)$ be the group of one-to-one R-linear maps of E into itself. When R is (i) a skew-field, (ii) the ring Z of rational integers, (iii) the ring $Z[i]$ of Gaussian integers, or (iv) a noncommutative principal ideal domain ($n \geqq 3$ in this case), it has been proved that the group A_n of automorphisms of $GL_n(R)$ is generated by automorphisms of the following types:

(a) $u \rightarrow tut^{-1}$, $\quad t \in GL_n(R)$, (inner),

(b) $u \rightarrow \chi(u)u$,

where χ is a homorphism of $GL_n(R)$ into the group of units of the center of R satisfying $\chi(\lambda I) = \lambda^{-1}$ if and only if $\lambda = 1$.

(c) $u \rightarrow u^\sigma$, σ an automorphism of R,

(d) $u \rightarrow t^{-1}\check{u}t$, $\check{u}$ = contragredient of u, where $t: E \rightarrow E^*$ is a correlation mapping E onto its dual E^*. (For references concerning these results see [1].)

On the other hand, for the case where $R = K[x]$ is the ring of polynomials in an indeterminate x over a field K, it has been shown [1] that the above types of automorphisms do not generate all the automorphisms of $GL_2(R)$. It is thus clear that one cannot expect these types of automorphisms to generate A_2 unless fairly restrictive conditions are imposed on the ring R.

We shall assume henceforth:

(I) R is a commutative principal ideal domain, integrally closed in its quotient field.

(II) R is Euclidean.

(III) The group of units of R contains more than two elements.

(IV) There exist units α_λ, $\lambda \in \Lambda$, in R such that each $t \in R$ is expressible in the form

$$t = \sum_{i=1}^{m} n_i \alpha_i, \qquad n_i \in Z$$

where Z is the ring of rational integers and Λ is a set of indices. (If char $R = p \neq 0$, then the n_i are chosen from $GF(p)$.)

Integral domains satisfying these conditions certainly exist. For example, let R be the ring of all algebraic integers in a cyclotomic field over the rationals; if R is Euclidean it will satisfy (I)–(IV). As

Presented to the Society, June 15, 1957; received by the editors May 31, 1957.

another example, let R be the ring consisting of all expressions $x^k f(x)$ where $f(x) \in K[x]$ is a polynomial in an indeterminate x over a field K, and where k ranges over all rational integers.[1] Conditions (I)–(IV) are also valid for this ring.

We shall use the following notations:

K = quotient field of R; $(R, +)$ = additive group of R;

U = multiplicative group of units of R. We shall identify $GL_2(R)$ with the group of 2×2 matrices over R with determinant in U. Hereafter let

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad J = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$X(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \qquad t \in R.$$

Let ${}^tX$ denote the transpose of X and let $[\alpha, \beta]$ denote a diagonal matrix with diagonal entries α, β.

We shall find it convenient to introduce the subgroup V of $(R, +)$ generated by all differences of units:

$$V = \sum_{\alpha,\beta \in U} Z(\alpha - \beta),$$

where (as above) Z is replaced by $GF(p)$ if char $R = p \neq 0$. Since R has a unity element we see that $1-(-1) = 2 \in V$. Assume that (IV) holds and let $t \in R$ be arbitrary, so that there are units $\{\alpha_i\}$ and integers $\{n_i\}$ such that

$$t = \sum_{i=1}^{m} n_i \alpha_i.$$

Since $\alpha_i - 1 \in V$ for each i, we find that

$$t \equiv \sum_{i=1}^{m} n_i \pmod{V}.$$

If $1 \overline{\in} V$, then since $2 \in V$ we see that

$$\sum_{i=1}^{m} n_i \equiv 0 \text{ or } 1 \pmod{2}$$

according as $t \in V$ or $t \overline{\in} V$. Let $P(t)$ denote the residue of $\sum_{i=1}^{m} n_i$ (mod 2). Then $P(t)$ is a well-defined function of t whenever $1 \overline{\in} V$, even though the expression for t as a sum of units may not be unique.

On the other hand, if $1 \in V$ then there is an equation

[1] This example was given by Professor N. T. Hamilton.

$$(1) \qquad 1 = \sum_{i=1}^{m} n_i(\alpha_i - \beta_i), \qquad n_i \in Z, \qquad \alpha_i, \beta_i \in U.$$

We may remark that $1 \in V$ if and only if some sum of an odd number of units can be zero. Thus $1 \overline{\in} V$ for the cases $R = Z$ and $R = Z[i]$ (ring of Gaussian integers), while $1 \in V$ for the case where $R = K[x]$ is a polynomial domain over a field K of characteristic $\neq 2$.

Further we note that by virtue of (IV), the subgroup V is an ideal of R. For,

$$\left(\sum n_i\alpha_i\right) \cdot \left(\sum m_j(\beta_j - \gamma_j)\right) = \sum n_i m_j(\alpha_i\beta_j - \alpha_i\gamma_j) \in V,$$

where $n_i, m_j \in Z$, $\alpha_i, \beta_j, \gamma_j \in U$.

2. **Transvections in GL_2 (R).** We begin by assuming that R satisfies (I) and (III). If char $R = 0$ an element $u \in GL_2(R)$ will be called a *transvection* if there are more than two elements in $GL_2(R)$ conjugate to u and commuting with u. If char $R = p \neq 0$, an element $u \in GL_2(R)$, $u \neq I$, is called a transvection if $u^p = I$.

LEMMA 1. *An element $u \in GL_2(R)$ is a transvection if and only if u is conjugate in $GL_2(R)$ to an element of the form $\alpha X(t)$, $\alpha \in U$, $t \neq 0$. Furthermore, if* char $R = p \neq 0$, *then* $\alpha = 1$.

PROOF. (1) Char $R = 0$. Consider u as an element of $GL_2(K)$. If u has distinct characteristic roots, then in some extension field of K, u is similar to $[a, b]$, $a \neq b$. On the one hand, only diagonal matrices commute with $[a, b]$; on the other, any matrix similar to $[a, b]$ must have the same characteristic roots. Hence, there are at most two elements in $GL_2(R)$ conjugate to u and commuting with it, contrary to the definition of transvection. Therefore u has a repeated characteristic root.

Since R is a principal ideal domain, then (as is well known) u is conjugate in $GL_2(R)$ to an element of the form $rX(t)$, $t \in R$. Then r^2 is a unit, whence so is r.

Conversely, let $u \in GL_2(R)$ be conjugate in $GL_2(R)$ to $\alpha X(t)$, $t \neq 0$, $\alpha \in U$. Let $\beta_1, \beta_2, \beta_3 \in U$ be distinct. Then the three matrices

$$[\beta_i, 1] \cdot \alpha X(t) \cdot [\beta_i^{-1}, 1] = \alpha X(\beta_i t), \qquad (i = 1, 2, 3)$$

commute with and are conjugate to $\alpha X(t)$, whence it is clear that U is a transvection.

(2) Char $R = p \neq 0$. If $u \neq I$ is a transvection it satisfies the equation $\lambda^p - 1 = (\lambda - 1)^p = 0$. Hence the characteristic polynomial of u is $(\lambda - 1)^2$, so the characteristic roots are both 1. Therefore u is conjugate in $GL_2(R)$ to an element of the form $X(t)$.

Conversely, any element $u \in GL_2(R)$ conjugate to $X(t)$ clearly satisfies $u^p = I$. This completes the proof of the lemma.

Fix an element $t_0 \in R$, and let $\tau \in A_2$. It follows at once from Lemma 1 that to within inner automorphism

$$X(t_0)^\tau = \epsilon(t_0) X(\sigma(t_0)). \tag{2}$$

Since for each $t \in R$, $X(t)$ is a transvection commuting with $X(t_0)$ it follows (assuming (2)) that $X(t)^\tau$ is a transvection commuting with $X(\sigma(t_0))$. Consequently

$$X(t)^\tau = \epsilon(t) X(\sigma(t)), \qquad \sigma(t) \in R, \qquad \epsilon(t) \in U, \tag{3}$$

for all $t \in R$.

Lemma 2. *The mapping $t \to \epsilon(t)$ is a homomorphism of* $(R, +)$ *into* U; *the mapping $t \to \sigma(t)$ is an automorphism of* $(R, +)$.

Proof. It follows immediately from $X(s)X(t) = X(s+t)$ that ϵ and σ are both homomorphisms.

We now show that σ is an automorphism. If $\sigma(t) = 0$ then $X(t)$ is in the center of $GL_2(R)$, whence $t = 0$. Further, since

$$\{\alpha X(t) : \alpha \in U, \, t \in R, \, t \neq 0\}$$

is the set of all transvections commuting with $X(t_0)$ for fixed $t_0 \neq 0$, therefore $\{\alpha X(\sigma(t)) : \alpha \in U, \, t \in R, \, t \neq 0\}$ must be the entire set of transvections commuting with $X(\sigma(t_0))$. Hence σ is "onto," and therefore is an automorphism.

Lemma 3. *For all $t \in R$, $\epsilon(t) = \pm 1$.*

Proof. For $\tau \in A_2$ set

$$J^\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where $J = [-1, 1]$. Then $a^2 + bc = d^2 + bc = 1$, $b(a+d) = c(a+d) = 0$. From $JX(t) = X(-t)J$ we deduce $c\sigma(t) + d = \alpha d$ and $c = \alpha c$, where $\alpha = \epsilon(t)^{-2}$. Consequently $c = 0$ or $= 1$. However, $c = 0$ implies $\alpha = 1$; therefore $\epsilon(t) = \pm 1$.

Lemma 4. *Let $\tau \in A_2$. Changing τ by an inner automorphism we may assume* (3) *and $S^\tau = S$.*

Proof. Set $Y = ST$; then $Y^3 = I$ implies $(Y^\tau)^3 = I$ for any $\tau \in A_2$. Therefore, the minimum and characteristic polynomials of Y^τ are equal and divide $\lambda^3 - 1$.

If char $R = 3$ then $\lambda^3 - 1 = (\lambda - 1)^3$ whence the characteristic polynomial of Y^τ is $\lambda^2 - 2\lambda + 1 = \lambda^2 + \lambda + 1$, and therefore

$$\text{Trace } Y^\tau = -1. \tag{4}$$

On the other hand, if char $R \neq 3$ and $\lambda^2+\lambda+1$ is irreducible over R equation (4) again holds. However, suppose $\lambda^2+\lambda+1$ is reducible over R; then the characteristic polynomial of Y is either

$$(\lambda - 1)(\lambda - \omega),\ (\lambda - 1)(\lambda - \omega^2) \text{ or } (\lambda - \omega)(\lambda - \omega^2) = \lambda^2 + \lambda + 1.$$

Now we have $T^\tau = \pm X(\sigma(1))$, whence det $T^\tau = 1$. From $S^2 = -1$ we deduce det $S^\tau = 1$. Therefore det $Y^\tau = 1$, whence the characteristic polynomial of Y^τ can only be $\lambda^2+\lambda+1$. Consequently (4) holds in all cases.

Set

$$S^\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then $a^2+bc = d^2+bc = -1$, $b(a+d) = c(a+d) = 0$. Suppose first $b = c = 0$; then $a^2 = d^2 = -1$ implies $a = \pm i = d$. Now $a = d = \pm i$ is impossible since this would imply that S^τ is in the center of $GL_2(R)$. On the other hand, $a = -d = \pm i$ contradicts (4). Consequently $d = -a$.

For $t \in R$ we have

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a + ct & b - 2at - ct^2 \\ c & -(a + ct) \end{pmatrix}.$$

Since

$$Y^\tau = \pm \begin{pmatrix} a & a\sigma(1) + b \\ c & c\sigma(1) - a \end{pmatrix}$$

and trace $Y^\tau = -1$, we have $c\sigma(1) = \pm 1$, whence $c \in U$. Hence there exists $t_0 \in R$ such that $a + ct_0 = 0$. Changing τ by an inner automorphism with factor $X(t_0)$, we now have

$$S^\tau = \begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix}.$$

Finally, applying the inner automorphism with factor $[1, b]$ we obtain Lemma 4.

LEMMA 5. *If τ is any automorphism of $GL_2(R)$ leaving S invariant and satisfying* (3) *then*

$${}^tX(t)^\tau = \epsilon(t)\,{}^tX(\sigma(t)).$$

This follows from ${}^tX(-t) = S^{-1}X(t)S$.

If τ is an automorphism of $GL_2(R)$ satisfying the hypotheses of Lemma 5 then $(T^\tau S)^3 = I$ implies $\epsilon(1)\sigma(1) = 1$. If $\sigma(1) = -1$, by introducing a further inner automorphism with factor J, we may obtain a new τ with $\sigma(1)=1$, but now $S^\tau=\pm S$. Then also $\epsilon(1)=\pm 1$.

The foregoing results may be summarized as

THEOREM 1. *If $\tau\in A_2$, then after changing τ by an inner automorphism if necessary, we have*

$$\begin{aligned} X(t)^\tau &= \epsilon(t)X(\sigma(t)), \qquad t\in R,\\ {}^tX(t)^\tau &= \epsilon(t)\,{}^tX(\sigma(t)), \qquad (5)\\ S^\tau &= \pm S,\ \epsilon(1) = \pm 1,\ \sigma(1) = 1, \end{aligned}$$

where τ induces the autmorphism σ: $(R, +)\rightarrow(R, +)$ and the homomorphism ϵ: $(R, +)\rightarrow U$, and where the plus signs go together as do the minus signs.

LEMMA 6. *If $\tau\in A_2$ satisfies* (5) *then*

$$[\alpha, 1]^\tau = \lambda(\alpha)[\rho(\alpha), 1]$$

where both λ and ρ are endomorphisms of U.

PROOF. Set

$$G = \{\alpha X(t) : \alpha \in U, t\in R\}, \qquad H = \{\alpha\,{}^tX(t) : \alpha\in U, t\in R\},$$

and let K denote the intersection of the normalizers of G and H. Then K consists of all diagonal matrices. Since $G^\tau=G$ and $H^\tau=H$ imply $K^\tau=K$, we see that $[\alpha, \beta]^\tau$ is also diagonal. In particular $[\alpha, 1]^\tau=\lambda(\alpha)[\rho(\alpha), 1]$.

LEMMA 7. *For all $\alpha\in U$, $t\in R$ we have*

$$\epsilon(\alpha t) = \epsilon(t), \qquad \rho(\alpha) = \sigma(\alpha), \qquad \sigma(\alpha t) = \sigma(\alpha)\sigma(t).$$

PROOF. The decomposition $X(\alpha t)=[\alpha, 1]\cdot X(t)\cdot[\alpha, 1]^{-1}$ yields $\epsilon(\alpha t)=\epsilon(t)$, $\sigma(\alpha t)=\rho(\alpha)\sigma(t)$, which implies the result.

Assuming next that R satisfies condition (IV) we prove

LEMMA 8. *Let $\tau\in A_2$ satisfy condition* (5). *Then the automorphism σ of $(R, +)$ induced by τ is a ring automorphism of R.*

PROOF. If $a\in Z$ (Char $R=0$) or if $a\in GF(p)$ (Char $R=p\neq 0$), then $\sigma(a)=a$. Hence, using (IV) it follows immediately that $\sigma(xy)=\sigma(x)\sigma(y)$ for all $x, y\in R$.

We henceforth assume that R satisfies condition (I)–(IV) of the introduction. We have seen that starting with an automorphism $\tau\in A_2$, after changing τ by an inner automorphism we obtain a new automorphism (again denoted by τ) satisfying

$$X(t)^\tau = \epsilon(t)X(\sigma(t)), \qquad S^\tau = \epsilon(1)S, \qquad [\alpha, 1]^\tau = \lambda(\alpha)[\sigma(\alpha), 1],$$

where $\epsilon: (R, +)\rightarrow U$ is a homomorphism satisfying $\epsilon(\alpha t)=\epsilon(t)$, $\alpha\in U$, where $\sigma: R\rightarrow R$ is a ring automorphism, and where λ is an endomorphism of U. Now replace τ by a new automorphism

$$U \rightarrow (U^{\tau})\sigma^{-1}$$

where σ^{-1} is the automorphism of $GL_2(R)$ induced by the ring automorphism σ^{-1} of R. Again calling this new automorphism τ, we now have an automorphism satisfying

$$X(t)^{\tau} = \epsilon(t)X(t), \qquad S^{\tau} = \epsilon(1)S, \qquad [\alpha, 1]^{\tau} = \lambda(\alpha)[\alpha, 1],$$

with possibly new maps ϵ and λ.

We find readily from the above that $[1, \alpha]^{\tau}=\lambda(\alpha)[1, \alpha]$, whence

$$[\alpha, \alpha]^{\tau} = \lambda^2(\alpha)[\alpha, \alpha].$$

From this equation we see that as α ranges over all elements of U so does $\alpha\lambda^2(\alpha)$. Thus $\alpha\rightarrow\alpha\lambda^2(\alpha)$ must be an automorphism of U, and from this it follows easily that

$$u \rightarrow \lambda(\det u)\cdot u$$

is an automorphism μ of $GL_2(R)$. Replacing τ by $\tau\mu^{-1}$, the new automorphism τ now satisfies

$$X(t)^{\tau} = \epsilon(t)X(t), \qquad S^{\tau} = \epsilon(1)S, \qquad [\alpha, 1]^{\tau} = [\alpha, 1].$$

Now let $t=\sum_{i=1}^{m} n_i\alpha_i$, $\alpha_i\in U$, $n_i\in Z$ (char $R=0$) or $n_i\in GF(p)$ (char $R=p\neq 0$). Then

$$\epsilon(t) = \prod_1^m \epsilon(n_i\alpha_i) = \prod_1^m \epsilon(n_i) = \prod_1^m (\epsilon(1))^{n_i} = \epsilon(1)^{\Sigma n_i}.$$

Set $\gamma=\epsilon(1)=\pm 1$. Then the automorphism τ satisfies

$$X(t)^{\tau} = \gamma^{\Sigma n_i}X(t), \qquad S^{\tau} = \gamma S, \qquad [\alpha, 1]^{\tau} = [\alpha, 1]. \tag{6}$$

We now show that if we define V (as before) to be the subgroup of $(R, +)$ generated by $\{\alpha-\beta; \alpha, \beta\in U\}$, then if $1\in V$ we must have $\gamma=1$, while if $1\notin V$ then equations (6) with $\gamma=-1$ define an automorphism η of $GL_2(R)$.

Indeed, if $1\in V$, then $1=\sum n_i (\alpha_i-\beta_i)$, α_i, $\beta_i\in U$, so

$$\begin{aligned}\gamma &= \epsilon(1) = \prod \epsilon(n_i\alpha_i - n_i\beta_i) = \prod\epsilon(n_i\alpha_i)(\epsilon(n_i\beta_i))^{-1}\\ &= \prod \epsilon(n_i)(\epsilon(n_i))^{-1} = 1.\end{aligned}$$

On the other hand, if $1\notin V$, define $P(t)$ as in the introduction. Let $\eta: GL_2(R)\rightarrow GL_2(R)$ be defined by

$$\eta : \begin{cases} X(t) \to (-1)^{P(t)} X(t); \\ S \to -S, \\ [\alpha, 1] \to [\alpha, 1]. \end{cases} \tag{7}$$

We shall prove that η induces an automorphism of $GL_2(R)$, and for this it suffices to show that η is well-defined. Thus, we need only prove that if a power product

$$\prod \{X(t_i), S, [\alpha_j, 1]\} = I$$

in $GL_2(R)$, then $n_s + \sum P(t_i) \equiv 0 \pmod 2$, where n_s is the number of factors equal to $S^{\pm 1}$.

For $t \in R$ we have $t = \sum n_i \alpha_i$ whence

$$X(t) = \prod X^{n_i}(\alpha_i) \equiv \prod X^{n_i}(1) \equiv T^{P(t)} \pmod{V},$$

where $T = X(1)$. Also, $[\alpha, 1] \equiv I \pmod{V}$ for $\alpha \in U$. Hence, if

$$\prod \{X(t_i), S, [\alpha_j, 1]\} = I$$

then since the subgroup V of $(R\ +)$ is also an ideal in R we have

$$\prod \{T^{P(t_i)}, S, I\} \equiv I \pmod{V}.$$

However since $2 \in V$, the only power products of S and T which are distinct mod V are I, S, T, ST, TS and STS. Of these, only the first can be $\equiv I \pmod{V}$ because $1 \overline{\in} V$. But if a power product of S and T is $\equiv I \pmod 2$ then the total number of factors of S and T must be even. Hence $n_s + \sum P(t_i) \equiv 0 \pmod 2$. This completes the proof that $\eta \in A_2$ whenever $1 \overline{\in} V$.

To summarize our results we have:

THEOREM 2. *The qroup A_2 of automorphisms of $GL_2(R)$ is generated by:*

(1) *The inner automorphisms $u \to vuv^{-1}$, $v \in GL_2(R)$,*

(2) *The automorphisms induced by automorphisms of R,*

(3) *The scalar multiplications $U \to \lambda(\det u)u$, where λ is an endomorphism of U for which the map $\alpha \to \alpha\lambda^2(\alpha)$, $\alpha \in U$, is an automorphism of U,*

(4) *The automorphism η described in* (7), *provided that* $1 \overline{\in} V$.

REFERENCES

1. I. Reiner, *A new type of automorphism of the general linear group over a ring*, Ann. of Math. vol. 66 (1957) pp. 461–466.

2. J. Landin and I. Reiner, *Automorphisms of the Gaussian unimodular group*, Trans. Amer. Math. Soc. vol. 87 (1958) pp. 76–89.

UNIVERSITY OF ILLINOIS