ON $GL(n)$ OF A DEDEKIND DOMAIN

By J. E. CREMONA

[Received 9 December 1987]

LET R be a Dedekind domain, with field of fractions K, and ideal class group C. Let $G = GL(n, K)$ and $\Gamma = GL(n, R)$ be the groups of invertible $n \times n$ matrices over K and over R, respectively, and let Z_G be the centre of G. In the following theorem, we determine the normalizer N of Γ in G, and the structure of the quotient $N/Z_G.\Gamma$.

In the case where $n = 2$ and R is the ring of integers of a number field, the result is mentioned without proof by Hurwitz in [**5**]. For K an imaginary quadratic number field and $n = 2$ the result was proved by Bianchi [**4**].

Some related results appear in [**1**], [**2**], and [**3**] where different methods are used.

For a matrix M in G, let $\mathbf{a}(M)$ denote the fractional ideal generated by the entries of M.

THEOREM 1. *With notation as above, let* $N = N_G(\Gamma)$ *and* $C_n = \{c \in C\colon c^n = 1\}$. *Then*

(1) *For a matrix* $M \in G$ *with* $\det M = \Delta$,

$$M \in N \Leftrightarrow \mathbf{a}(M)^n = (\Delta);$$

(2) *There exists a group isomorphism*

$$\phi\colon N/Z_G.\Gamma \cong C_n.$$

In particular, if C *has no* n*-torsion then* $N = Z_G.\Gamma$.

From (1), the function $M \mapsto \mathbf{a}(M)$ induces a map $\phi\colon N \to C_n$. To prove (2) we will then show that ϕ is a surjective group homomorphism with kernel $Z_G.\Gamma$.

First we prove an elementary lemma.

LEMMA 1. *Let* L *be the* R*-linear span of* $SL(n, R)$ *in* $M(n, R)$, *the algebra of all* $n \times n$ *matrices over* R. *Then* $L = M(n, R)$.

Proof. Clearly it suffices to prove the Lemma in the case $R = \mathbf{Z}$. Let E_{ij} denote the $n \times n$ matrix with a 1 in position (i, j) and 0 elsewhere. If $i \neq j$ then $I + E_{ij} \in SL(n, \mathbf{Z})$, so $E_{ij} \in L$. If $i < n$ then $I - E_{ii} + E_{i,i+1} - E_{i+1,i} \in SL(n, \mathbf{Z})$, so $E_{ii} \in L$. Finally $I - E_{nn} + E_{n-1,n} - E_{n,n-1} \in SL(n, \mathbf{Z})$, so $E_{nn} \in L$.

LEMMA 2. *Let* $M \in G$; *set* $\mathbf{a} = \mathbf{a}(M)$, $\mathbf{b} = \mathbf{a}(M^{-1})$, *and* $\Delta = \det M$. *Then*

Quart. J. Math. Oxford (2), 39 (1988), 423–426 © 1988 Oxford University Press

0033-5606/88 $3.00

the following are equivalent:

(1) $M \in N$;

(2) $\mathbf{ab} = R$;

(3) $\mathbf{a}^n = (\Delta)$.

Proof. First observe that for any $M \in G$ we have $R \subseteq \mathbf{ab}$ and $\Delta \in \mathbf{a}^n$.

By definition of N, we have $M \in N$ if and only if $M^{-1}\gamma M \in \Gamma$ for all $\gamma \in \Gamma$. Since $\det(M^{-1}\gamma M) = \det \gamma \in R^*$, it follows that $M^{-1}\gamma M \in \Gamma$ if and only if $M^{-1}\gamma M \in M(n, R)$. By Lemma 1 this will be true for all $\gamma \in \Gamma$ if and only if for all i, j,

$$M^{-1}E_{ij}M \in M(n, R),$$

which is if and only if for all i, j, k, l we have

$$(M^{-1})_{kl}(M)_{jl} \in R.$$

This is equivalent to $\mathbf{ab} \subseteq R$, and hence to $\mathbf{ab} = R$ by the remark made above. Thus (1) is equivalent to (2).

Suppose $\mathbf{ab} = R$, so that $\mathbf{b} = \mathbf{a}^{-1}$. We have $\Delta \in \mathbf{a}^n$ and $\Delta^{-1} = \det(M^{-1}) \in \mathbf{b}^n$. Hence $(\Delta) \supseteq \mathbf{b}^{-n} = \mathbf{a}^n$, so $(\Delta) = \mathbf{a}^n$. Conversely, if $\mathbf{a}^n = (\Delta)$ then by Cramer's rule we have $\mathbf{b} \subseteq \Delta^{-1}\mathbf{a}^{n-1} = \mathbf{a}^{-1}$, so $\mathbf{ab} \subseteq R$ and hence $\mathbf{ab} = R$. Thus (2) is equivalent to (3).

Proof of the Theorem. Assertion (1) is just Lemma 2. The map $M \mapsto \mathbf{a}(M)$ then induces a map ϕ: $N \to C_n$, which we must show to be a surjective group homomorphism with kernel $Z_G.N$.

ϕ is a homomorphism: For $i = 1, 2$ let $M_i \in N$ with $\mathbf{a}_i = \mathbf{a}(M_i)$ and $\mathbf{b}_i = \mathbf{a}(M_i^{-1})$. Then

$$R \subseteq \mathbf{a}(M_1M_2)\mathbf{a}((M_1M_2)^{-1}) \subseteq \mathbf{a}_1\mathbf{a}_2\mathbf{a}((M_1M_2)^{-1}) \subseteq \mathbf{a}_1\mathbf{a}_2\mathbf{b}_1\mathbf{b}_2 = R$$

by Lemma 2. Hence we have equality throughout, so $\mathbf{a}(M_1M_2) = \mathbf{a}_1\mathbf{a}_2$ as required.

$\ker(\phi) = Z_G.\Gamma$: If $M \in \Gamma$ then $\mathbf{a}(M) = (1)$, and if $M \in Z_G$ then $\mathbf{a}(M)$ is principal; so $\ker(\phi) \supseteq Z_G.\Gamma$. Conversely, if $\phi(M) = 1$ then $\mathbf{a}(M)$ is principal, say $\mathbf{a}(M) = (\alpha)$, and $(\alpha)^n = (\Delta)$ since $M \in N$, by Lemma 2. But then $\alpha^{-1}M \in \Gamma$, so $M \in Z_G.\Gamma$.

ϕ is surjective: We give two proofs.

Let $\mathbf{a}$ be an ideal of R with $\mathbf{a}^n$ principal, say $\mathbf{a}^n = (\Delta)$. Then by Steinitz's Theorem [**6**, Theorem 1.6] there is an isomorphism of R-modules

$$\psi\colon \underbrace{R \oplus R \oplus \cdots \oplus R}_{n} \cong \underbrace{\mathbf{a} \oplus \mathbf{a} \oplus \cdots \oplus \mathbf{a}}_{n}.$$

One easily sees that ψ is given by an $n \times n$ matrix M with entries in $\mathbf{a}$ and $(\det M) = (\Delta)$. (See the proof of [**6**, Theorem 1.6]). Thus $\mathbf{a}(M) = \mathbf{a}$ and by Lemma 2, $M \in N$.

For the second proof we use the fact that every fractional ideal of R can be generated by two elements. Let $\mathfrak{a}$ be an ideal with $\mathfrak{a}^n = (\Delta)$ and $\mathfrak{a} = (\alpha, \beta)$. Then

$$\mathfrak{a}^{n-1} = (\alpha^{n-1}, \alpha^{n-2}\beta, \ldots, \alpha\beta^{n-2}, \beta^{n-1}).$$

Since $\Delta \in \mathfrak{a}^n = \mathfrak{a}\mathfrak{a}^{n-1}$ we can write

$$\Delta = \gamma_1\alpha^{n-1} - \gamma_2\alpha^{n-2}\beta + \cdots + (-1)^{n-1}\gamma_n\beta^{n-1},$$

for some $\gamma_1, \gamma_2, \ldots, \gamma_n \in \mathfrak{a}$. Let M be the $n \times n$ matrix

$$\begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \cdots & \cdots & \gamma_n \\ \beta & \alpha & 0 & \cdots & \cdots & 0 \\ 0 & \beta & \alpha & 0 & & \vdots \\ \vdots & 0 & \beta & \alpha & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & \beta & \alpha \end{pmatrix}.$$

Then $\mathfrak{a}(M) = \mathfrak{a}$, and expanding by the top row one sees easily that $\det(M) = \Delta$. It follows from Lemma 2 that $M \in N$, and $\phi(M)$ is the class of the ideal $\mathfrak{a}$.

Remarks. 1. The map $M \mapsto \mathfrak{a}(M)$ is not a homomorphism from the whole of G to C, for by Lemma 2.

$$\mathfrak{a}(M^{-1}) = \mathfrak{a}(M)^{-1} \Leftrightarrow M \in N.$$

2. It follows from Lemma 2 and its proof that for $M \in N$, the ideal $\mathfrak{a}(M)$ is generated by the entries in any one row or column of M. For since $MM^{-1} = I$ we have, for all i,

$$1 = \sum_{j=1}^{n} (M)_{ij}(M^{-1})_{ji}$$

so that for all i, p, q,

$$(M)_{pq} = \sum_{j=1}^{n} (M)_{ij}(M^{-1})_{ji}(M)_{pq} \in \sum_{j=1}^{n} (M)_{ij}R.$$

Hence $\mathfrak{a}(M)$ is generated by the entries in row i. Similarly for the columns, using $M^{-1}M = I$.

Now suppose that R is an arbitrary (commutative) integral domain, not necessarily Dedekind. If we replace the ideal class group by the group of classes of invertible fractional ideals of R, then all the above is still valid except (possibly) for the surjectivity of ϕ. Hence we can state the following partial generalization of Theorem 1.

THEOREM 2. *Let R be an integral domain with field of fractions K; let C be the group of classes of invertible fractional ideals of R and $C_n = \{c \in C\colon c^n = 1\}$. Let $G = GL(n, K)$, $\Gamma = GL(n, R)$, $N = N_G(\Gamma)$ and Z_G the centre of G. Then*

(1) *For a matrix M in G with* $\det(M) = \Delta$,

$$M \in N \Leftrightarrow \mathbf{a}(M)^n = (\Delta);$$

(2) *There exists an injective group homomorphism*

$$\phi\colon N/Z_G.\Gamma \hookrightarrow C_n.$$

On the surjectivity of ϕ we can make the following observations:

If some class $c \in C_n$ contains two comaximal ideals then the first proof above that $c \in \operatorname{im}(\phi)$ is still valid, as can be seen from the proof of Steinitz's Theorem in [6]. In particular, this is true when R is an order in a number field, so that ϕ is then surjective.

If R has Krull dimension 1 then every invertible ideal of R can be generated by two elements, so the second proof above is valid, and ϕ is again surjective.

If R is a unique factorization domain, then C is torsion-free, so ϕ is trivially surjective.

From the second remark made above, for ϕ to be surjective it is necessary that every ideal of R whose nth power is principal should be generated by at most n elements.

The question of whether ϕ is always surjective remains open.

REFERENCES

1. Nelo D. Allen, *The problem of the maximality of arithmetic groups*, in Algebraic Groups and Discontinuous Subgroups, (Proc. Symp. Pure Math., Boulder Co., 1965), Amer. Math. Soc., Providence R.I., 1966, pp. 104–109.
2. Nelo D. Allen, '*Maximality of some arithmetic groups,*' *An. Acad. Brasil Ci.* **38** (1966), 223–227.
3. Nelo D. Allen, '*Arithmetic subgroups of some classical groups,*' *An. Acad. Brasil Ci.* **39** (1967), 15–18.
4. L. Bianchi, '*Sui gruppi di sostituzioni lineari con coefficienti appartenenti a corpi quadratici immaginarii, Math. Ann.* **40** (1892), 332–412.
5. A. Hurwitz, '*Die unimodularen Substitutionen in einem algebraischen zahlenkörper,*' *Nachr. Akad. Wiss. Göttingen Math-Phys. Kl.II* (1895), 332–356.
6. J. Milnor, *Introduction to algebraic K-theory*, Princeton University Press, 1971.

Department of Mathematics
University of Exeter
Exeter EX4 4QE