

## CONJUGACY CLASSES OF HYPERBOLIC MATRICES IN $Sl(n, \mathbf{Z})$ AND IDEAL CLASSES IN AN ORDER

BY

D. I. WALLACE

ABSTRACT. A bijection is proved between  $Sl(n, \mathbf{Z})$ -conjugacy classes of hyperbolic matrices with eigenvalues  $(\lambda_1, \dots, \lambda_n)$  which are units in an  $n$ -degree number field, and narrow ideal classes of the ring  $R_k = \mathbf{Z}[\lambda_i]$ . A bijection between  $Gl(n, \mathbf{Z})$ -conjugacy classes and the wide ideal classes, which had been known, is repeated with a different proof.

In 1980, Peter Sarnak was able to obtain an estimate of the growth of the class number of real quadratic number fields using the Selberg Trace Formula and a bijection between hyperbolic elements of  $Sl(2, \mathbf{Z})$  and quadratic forms. The “class number” counted was the number of congruence classes of quadratic forms as studied by Gauss [1]. In this paper we will translate this bijection into modern number-theoretic terms by counting ideal classes in a ring of integers associated to a given field. In this way a bijection is proved between conjugacy classes of hyperbolic matrices in  $Sl(2, \mathbf{Z})$  with a given set of eigenvalues and ideal classes in a certain order (i.e. subring of dimension  $n$  over  $\mathbf{Z}$ ) associated to the ring of integers  $O_K$  in a real  $n$ th degree number field  $K$ . This more direct method is necessary for generalizing the bijection to higher dimensional cases because Sarnak’s result depends upon quadratic forms, Pell’s equation and other things which are well understood only in the case of  $Sl(2, \mathbf{Z})$ .

We must mention the work of Latimer and MacDuffee [3] who first proved Theorem 2 in a slightly different fashion. Important also is the extensive work of Taussky [7–9], who simplified the results of Latimer and MacDuffee and extended them in certain directions, as well as doing much work on the  $Sl(2, \mathbf{Z})$  case.

It follows from a brief examination of the characteristic polynomial for a matrix  $A$  in  $Sl(n, \mathbf{Z})$  that the eigenvalues of  $A$  are conjugate units in an extension of  $\mathbf{Q}$ . We shall insist in the remainder of this paper that  $A$  be “hyperbolic” with irreducible characteristic polynomial, that is,  $A$  will have distinct real eigenvalues  $\lambda^{(i)}$ , each of which is of degree  $n$  over  $\mathbf{Q}$ .

**PROPOSITION 1.** *If  $\lambda$  is an eigenvalue for a matrix  $A \in SL(n, \mathbf{Z})$ , then for any field  $K$  containing  $\lambda$  there exists an eigenvector  $\omega$ ,  ${}^T\omega = (\omega_1, \dots, \omega_n)$ , with  $\omega_i \in O_K$ .*

---

Received by the editors March 30, 1983.

1980 *Mathematics Subject Classification.* Primary 10-02, 15-02; Secondary 15A18, 15A36, 10C07.

©1984 American Mathematical Society  
0025-5726/84 \$1.00 + \$.25 per page

PROOF. We can construct an eigenvector for  $A$  by solving  $A \circ x = \lambda x$  for  $x = (1, x_2, \dots, x_n)^T$ . This matrix identity yields  $n$  simultaneous equations with coefficients in  $Z \oplus Z\lambda$ . Therefore the solution constructed lies in  $\mathbf{Q}(\lambda)$ . If we multiply the solution vector by a constant it will still be an eigenvector, so this allows us to clear the denominators of  $x_2, \dots, x_n$ . The resulting vector  $\omega$  has entries which all lie in  $O_K$ .

PROPOSITION 2. For a given ideal  $I$  in  $O_K$  and ordered set of elements  ${}^T\omega = (\omega_1, \dots, \omega_n)$  which are a  $\mathbf{Z}$ -basis of  $I$ , and for  $\lambda$  a unit with norm equal to 1, there exists a matrix  $A$  in  $\text{Sl}(n, \mathbf{Z})$  such that  $A \circ \omega = \lambda\omega$ .

PROOF. Because  $\lambda$  is a unit,  $\lambda{}^T\omega = (\lambda\omega_1, \dots, \lambda\omega_n)$  is also a  $\mathbf{Z}$ -basis of  $I$ . Therefore, some matrix  $A$  in  $\text{Gl}(n, \mathbf{Z})$  takes  $\omega$  to  $\lambda\omega$ . If we inspect the action of  $A$  on  $K^{(j)}$ , the  $j$ th conjugate field of  $K$ , we see that  $I^{(j)}$  has a  $\mathbf{Z}$ -basis  ${}^T\omega^{(j)} = (\omega_1^{(j)}, \dots, \omega_n^{(j)})$ . Furthermore,  $A\omega^{(j)} = \lambda^{(j)}\omega^{(j)}$ . Thus the eigenvalues of  $A$  are  $\lambda^{(1)}, \dots, \lambda^{(n)}$ , conjugate units in a field. Therefore  $\det A = \prod_j \lambda^{(j)} = 1$  and  $A$  is in  $\text{Sl}(n, \mathbf{Z})$ .

PROPOSITION 3. Let  $I, \omega, A, \lambda$  be as in Proposition 2. Let  ${}^T\alpha$  be another vector whose elements are a basis of  $I$ . Then there exists  $B$  in  $\text{Sl}(n, \mathbf{Z})$  with eigenvalues  $\lambda^{(1)}, \lambda^{(2)}, \dots, \lambda^{(n)}$  and eigenvectors  $\alpha^{(1)}, \dots, \alpha^{(n)}$ , and  $B$  is conjugate to  $A$  by an element of  $\text{Gl}(n, \mathbf{Z})$ .

PROOF. Because  $\{\omega_i\}$  and  $\{\alpha_i\}$  are bases of  $I$  there exists  $C$  in  $\text{Gl}(n, \mathbf{Z})$  with  $C \circ \alpha = \omega$ . Let  $B = C^{-1}AC$ . Thus

$$B \circ \alpha = C^{-1}AC\alpha = C^{-1}A \circ \omega = C^{-1} \circ \lambda\omega = \lambda C^{-1} \circ \omega = \lambda\alpha.$$

COROLLARY TO PROPOSITION 3. If  $n$  is odd then we can choose the  $C$  of Proposition 3 to be in  $\text{Sl}(n, \mathbf{Z})$ .

PROOF. If  $\det C = -1$  then replace  $C$  by  $-1 \cdot C$ .

PROPOSITION 4. An ideal class in  $K = \mathbf{Q}(\lambda)$  uniquely determines a conjugacy class in  $\text{Gl}(n, \mathbf{Z})$  of matrices with eigenvalue  $\lambda$  (and determinant  $+1$ ).

PROOF. If  $\omega$  is a vector whose entries are a basis for an ideal  $I$  and if  $J$  is another ideal in the same ideal class as  $I$ , then there is a constant  $k$  such that  $k\omega$  is a basis of  $J$ . By Proposition 2 there is a matrix  $A$  with eigenvalue  $\lambda$  and eigenvector  $\omega$ , thus  $k\omega$  is also on eigenvector of  $A$ . We can therefore take  $\omega$  to represent an entire ideal class, of which each ideal has a basis  $k\omega$  which is an eigenvector of  $A$ . It suffices then to show the converse of Proposition 3; this is, if  $B$  is conjugate to  $A$  then it corresponds to the same ideal class. But the eigenvector of  $B = C^{-1}AC$  with eigenvalue  $\lambda$  is exactly  $C^{-1} \circ \omega$ , and  $C^{-1} \circ \omega$  has entries which are also a basis of  $I$ .

Gauss [1] showed several examples of symmetric  $2 \times 2$ -matrices for which the number of equivalence classes under  $\text{Sl}(2, \mathbf{Z})$  is twice the number of classes under  $\text{Gl}(2, \mathbf{Z})$ . The import of these examples for our purposes lies in calculating conjugacy classes of a determinant 1 hyperbolic. Sarnak [5] shows that a correspondence exists between congruence classes of symmetric matrices of a given determinant and  $\text{Sl}(2, \mathbf{Z})$ -conjugacy classes of associated hyperbolic matrices in  $\text{Sl}(2, \mathbf{Z})$  with certain



**PROPOSITION 6.** *Let  $\{I\}$  be the ideal class containing  $I$ . Then  $\{I\}$  is well defined; that is, membership to an ideal class is an equivalence relation on ideals.*

**PROOF.** Suppose  $J \in \{I\}$ . Then there is  $c \in$  (quotient field of  $R$ ) such that  $cJ = I$ . Therefore  $c^{-1}I = J$  and  $I \in \{J\}$ . Also if  $J \in \{I\}$  and  $H \in \{J\}$ , then there are  $c$  and  $d$  in the quotient field of  $R$  with  $cJ = I$  and  $dH = J$ . Thus  $cdH = I$  and  $H \in \{I\}$ . Obviously  $J \in \{J\}$ . Therefore membership to an ideal class in  $R$  is an equivalence relation on ideals. Thus  $\{I\}$  is well defined.

It is worthwhile to note here the need for Proposition 6.  $R = \mathbf{Z}[\lambda]$  is a ring consisting of integers but is not in general the complete ring of integers for a field  $K$ , although it is contained in  $O_K$ ;  $K = \mathbf{Q}(\lambda)$ .  $R$  is not necessarily Dedekind, although principal ideals in  $R$  are invertible. Thus, if we wished to make ideals in the same class differ by a principal ideal or principal inverse ideal, we could do so without changing or invalidating Definition 1. However, because  $R$  is not necessarily Dedekind we do not have an ideal class group, as in the case of  $O_K$ .

**PROPOSITION 7.** *Let  $A$  be in  $\text{Sl}(n, \mathbf{Z})$  with eigenvalues  $\{\lambda^{(1)}, \dots, \lambda^{(n)}\}$  distinct conjugate units. Let  $R = \mathbf{Z}[\lambda]$ . Suppose  $A \cdot \omega = \lambda\omega$  for some vector  ${}^T\omega = (\omega_1, \dots, \omega_n)$ . Then  $\{\omega_1, \dots, \omega_n\}$  are a  $\mathbf{Z}$ -basis for an ideal in  $R$ .*

**PROOF.** It suffices to show that for  $r \in R$ ,  $r\omega_i \in \bigoplus_i \mathbf{Z}\omega_i$ . But  $r = \sum_{j=0}^{n-1} \alpha_j \lambda^j$ ,  $\alpha_j \in \mathbf{Z}$ . Thus it suffices to show that  $\lambda^j \cdot \omega_i$  is in  $\bigoplus_i \mathbf{Z}\omega_i$ . But  ${}^T\omega = (\omega_1, \dots, \omega_n)$  is an eigenvector of  $A^j$  with eigenvalue  $\lambda^j$ . Thus  $\lambda^j \omega_i$  is a linear combination of the  $\omega_i$ . Therefore  $\bigoplus_i \mathbf{Z}\omega_i$  is an ideal in  $R$ .

**THEOREM 2.** *Let  $U_\lambda$  be the set of  $\text{Gl}(n, \mathbf{Z})$ -conjugacy classes of matrices in  $\text{Sl}(n, \mathbf{Z})$  whose elements have eigenvalues  $\{\lambda^{(1)}, \lambda^{(2)}, \dots, \lambda^{(n)}\}$ . Let  $R = \mathbf{Z}[\lambda]$ . Let  $\{I\}$  be the set of ideal classes of  $R$ . Then there is a well-defined map  $\Phi_\lambda: U_\lambda \rightarrow \{I\}$  which is one-to-one and onto.*

**PROOF.** We choose  $\Phi_\lambda(\{A\})$  to be the ideal generated by the entries of the  $\lambda$ -eigenvector of any representative of  $\{A\}$ .  $\Phi_\lambda(\{A\})$  exists and is an ideal generated as a  $\mathbf{Z}$ -module by  $\{\omega_i\}$ , (the entries of the eigenvector) by Proposition 7.  $\Phi_\lambda$  is thus well defined by Proposition 3 and onto by Proposition 2. By Proposition 4,  $\Phi_\lambda^{-1}$  is also well defined and onto. Therefore  $\Phi_\lambda$  is one-to-one and onto.

For convenience, let  $h(K)$  denote the class number of  $K$  and let  $H(\lambda)$  denote the number of  $\text{Gl}(n, \mathbf{Z})$ -conjugacy classes of matrices with eigenvalues  $\{\lambda^{(1)}, \lambda^{(2)}, \dots, \lambda^{(n)}\}$ . Then from Theorem 2 we have

**COROLLARY TO THEOREM 2.** *If  $R = O_K$  then  $h(K) = H(\lambda)$ .*

**PROOF.** The proof follows immediately from Theorem 2.

The following proposition and theorem give yet another criterion for the equality of  $h(K)$  and  $H(\lambda)$ . They will yield a large class of discriminants for which the number field has the desired property.

**PROPOSITION 8.** *Let  $\lambda$  be a unit with minimal polynomial of degree  $n$  and let  $A \circ \omega = \lambda\omega$  for  $A \in \text{Sl}(n, \mathbf{Z})$  and  $\omega \in \mathbf{R}^n$ . Let  ${}^T\omega = (\omega_1, \omega_2, \dots, \omega_n)$ . Then  $\{\omega_i\}$  is a linearly independent set over  $\mathbf{Q}$ .*

PROOF. Suppose not. Then  $\lambda\omega_i = \sum_{s=1}^{n-1} b_s \omega_s$  for all  $i$ . Thus  $B \circ \omega = \lambda\omega$ , where  $B$  has rational entries and the  $n$ th column is zero. Therefore  $\lambda$  is an eigenvector of the  $((n - 1) \times (n - 1))$ -matrix in the upper left-hand corner of  $B$ . Therefore the minimal polynomial of  $\lambda$  has degree less than  $n$ .

THEOREM 3. Suppose  $K = \mathbf{Q}(\lambda)$  is a number field of degree  $n$  and  $\lambda$  is a unit. If the discriminant of  $\Lambda$  is square-free then  $h(K) = H(\lambda)$ , where  $\Lambda = (1, \lambda, \dots, \lambda^{n-1})$ .

PROOF.  $\Lambda = (1, \lambda, \lambda^2, \dots, \lambda^{n-1})$  is a  $\mathbf{Z}$ -basis for  $R$ . It is also a  $\mathbf{Q}$ -basis for  $K$ . Let  $\epsilon = (\epsilon_1, \dots, \epsilon_n)$  be a  $\mathbf{Z}$ -basis of  $O_K$ . By a theorem in Samuel [4], if  $D_K(1, \lambda, \dots, \lambda^{n-1})$  is square-free then  $(1, \lambda, \dots)$  is a  $\mathbf{Z}$ -basis of  $O_K$ . But  $D_K(1, \lambda, \dots, \lambda^{n-1}) = D(K)$ , which is assumed to be square-free. Therefore  $R = O_K$  and by Corollary to Theorem 2,  $h(K) = H(\lambda)$ .

We should note that in the Selberg trace formula the conjugacy classes of hyperbolics are always taken to be conjugates by elements of  $\text{Sl}(2, \mathbf{Z})$ . The bijection obtained in Theorem 2 of this paper, however, is between (wide) ideal classes in a ring  $R_K$  associated to a field  $K$  and  $\text{Gl}(n, \mathbf{Z})$ -conjugacy classes of hyperbolic matrices. We can convert the problem of study of  $\text{Sl}(n, \mathbf{Z})$ -conjugacy classes if we count the narrow ideal classes of  $R_K$  instead of the usual (wide) ideal classes.

DEFINITION 2. Two ideals  $I$  and  $J$  of a ring  $O_K$  of integers of a number field  $K$  are said to be *narrowly equivalent* if  $I = rJ$ ,  $r \in O_K$ , or  $J = rI$ ,  $r \in K$ , such that  $r$  is a number of positive norm.

It is well known that the above equivalence relation divides the set of ideals of  $O_K$  into classes which are called the *narrow ideal classes*. The number of these is the *narrow class number*. It is easy to see that if  $R_K$  is the order described previously which is associated to the number field  $K$ , the ideals of  $R_K$  can be grouped into narrow ideal classes by the same definition. For the remainder of this paper we will be referring (unless otherwise stated) to the narrow ideal classes and narrow class number of  $R_K$  rather than  $O_K$ .

Let  $\lambda$  be a unit of degree  $n$  and let  $\mathbf{Q}(\lambda) = K$ . Let  $R_K$  and  $O_K$  be the rings associated with  $K$  as before, namely,  $O_K$  being the ring of integers and  $R_K = \mathbf{Z}[\lambda]$ . Let  $R = R_K$  or  $O_K$  in general. We now begin a process of associating to every narrow ideal class a basis vector and two sets of basis vectors on which we will study the action of  $\text{Sl}(n, \mathbf{Z})$ .

Let  $\{I_1\}, \dots, \{I_k\}$  be the wide ideal classes of ring  $R$ . Let  $I_1, \dots, I_k$  be arbitrary choices of representatives of each class. Let  $\omega^1, \dots, \omega^k$  be arbitrary choices of vectors consisting of ordered bases for  $I_j$ , respectively. To each ideal  $J_j$  in the same wide ideal class as  $I_j$  associate the basis vector  $r \cdot \omega^j$ ,  $r \in K$ , choosing  $r$  such that  $n(r) > 0$  if  $I_j$  and  $J_j$  are in the same narrow ideal class. Thus to every ideal  $J_j$  in  $R$  we have associated a basis  $r\omega^j$  which, although  $\omega^j$  is chosen arbitrarily, we shall consider fixed.

We know that all bases of  $I_j$  can be obtained by the action of  $\text{Gl}(n, \mathbf{Z})$  on  $\omega^j$ . We can then split the set of bases elements of an ideal  $I_j$  into two sets, namely those which arise from the action of elements of  $\text{Sl}(n, \mathbf{Z})$  on  $\omega^j$  and the rest. Define  $\Omega_j^+$  to be the set of all  $\nu = A \cdot \omega^j$ ,  $A \in \text{Sl}(n, \mathbf{Z})$ , and define  $\Omega_j^-$  to be all the other basis



PROOF. By Theorem 2 it suffices to show that if  $I_j$  and  $I_K$  are two widely equivalent ideal classes ( $rI_j = I_K$ ) with associated bases  $\omega^j$  and  $\omega^k$  such that  $r\omega^j = \omega^k$ , and if  $A\omega^j = \lambda\omega^j$  and  $B(\omega^k) = \lambda\omega^k$ , we have the following:

(1) If  $CAC^{-1} = B$  and if  $\det C = +1$  then  $I_j$  and  $I_k$  are narrowly equivalent.

(2) If  $I_j$  and  $I_k$  are narrowly equivalent then there exists  $C$  with  $\det C = +1$  such that  $CAC^{-1} = B$ .

PROOF OF (1). Suppose  $CAC^{-1} = B$  and  $\det C = +1$ . Note that  $\omega^j \in \Omega_{I_j}^+$  and  $r\omega^j = \omega^k \in \Omega_{I_k}^+$ . Let  $\hat{\omega}^k = C^{-1}\omega^k$ . Then  $\hat{\omega}^k \in \Omega_{I_k}^+$  by the definition of  $\Omega_{I_k}^+$ . Also we have that  $A\omega^j = \lambda\omega^j$  and

$$A\hat{\omega}^k = C^{-1}BC \cdot C^{-1}\omega^k = C^{-1}B \cdot \omega^k = C^{-1} \cdot \lambda\omega^k = \lambda \cdot \hat{\omega}^k.$$

Therefore  $\hat{\omega}^k = \hat{r} \cdot \omega^j$  and by Lemma 1,  $n(\hat{r}) > 0$ . Therefore  $I_j$  and  $I_k$  are narrowly equivalent.

PROOF OF (2). Suppose  $I_j$  and  $I_k$  are narrowly equivalent and  $A\omega^j = \lambda\omega^j$ ,  $B\omega^k = \lambda\omega^k$ . Then there exists  $r$  ( $n(r) > 0$ ) such that  $\hat{\omega}^k = r\omega^j$  is a basis of  $I_K$ . By Lemma 1,  $\hat{\omega}^k \in \Omega_{I_K}^+$ . By the definition of  $\Omega_{I_K}^+$  there exists a matrix  $C \in \text{Sl}(n, \mathbf{Z})$  such that  $C\hat{\omega}^k = \omega^k$ . We then have  $A\hat{\omega}^k = \lambda\hat{\omega}^k$  because  $\hat{\omega}^k$  is a multiple of  $\omega^j$  and

$$CAC^{-1}\omega^k = CA\hat{\omega}^k = C \cdot \lambda\hat{\omega}^k = \lambda \cdot \omega^k.$$

By noting the action of  $CAC^{-1}$  on conjugate fields of  $K$ , we have the  $CAC^{-1}$  has the same eigenvalues and eigenvectors as  $B$  and hence  $CAC^{-1} = B$ .

By comparing the result of this theorem with the Corollary to Proposition 3, Proposition 5, and Theorem 1, we can conclude the following corollaries. Let  $K$  be a field with irreducible minimal polynomial  $P(\lambda)$  for  $\lambda$  a unit.

COROLLARY 1. *If the degree  $n$  of  $K$  is odd, then the wide class number of  $R_K$  equals the narrow class number.*

COROLLARY 2. *The narrow class number of  $R_K$  is less than or equal to twice the wide class number of  $R_K$ .*

COROLLARY 3. *The narrow class number of  $O_K$  is less than or equal to the narrow class number of  $R_K$ .*

Thus we see that for a hyperbolic element of  $\text{Sl}(n, \mathbf{Z})$  with  $n$ th degree irreducible characteristic polynomial  $P(\lambda)$ , the coefficient associated to that term in the  $n$ -dimensional version of the trace formula will, in part, be the narrow class number of the ring  $R_K = \mathbf{Z}[\lambda]$ . When  $n$  is odd it will also be the wide class number of  $R_K$ . In either case there will be number-theoretic information associated to that particular term which may possibly be retrieved by estimates involving the trace formula. For further information on the Selberg trace formula and number-theoretic applications thereof, please see [2, 6, 10, 12].

#### REFERENCES

1. C. F. Gauss, *Disquisitiones arithmeticae*, Chelsea, New York, 1889, 1965, p. 18. (German)
2. Dennis Hejhal, *The Selberg trace formula for  $PSL(2, R)$* , Vol. I, Lecture Notes in Math., Springer-Verlag, New York, 1976, p. 5.
3. C. G. Latimer and C. C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math. (2) **34** (1933), 313–316.

4. P. Samuel, *Algebraic theory of numbers*, Houghton Mifflin, Boston, Mass., 1979, p. 24.
5. Peter Sarnak, *Prime geodesic theorems*, Ph. D. thesis, Stanford University, 1980, pp. 1, 10, 19, 44.
6. P. Sarnak and P. Cohen, *Discrete groups and harmonic analysis* (to appear).
7. Olga Taussky, *Classes of matrices and quadratic fields*, Pacific J. Math. **1** (1951), 127–132.
8. \_\_\_\_\_, *Composition of binary integral quadratic forms via integral  $2 \times 2$  matrices and composition of matrix classes*, Linear and Multilinear Algebra **10** (1981), 309–318.
9. \_\_\_\_\_, *On a theorem of Latimer and MacDuffee*, Reprinted from Canad. J. Math. **1** (1949), 300–302.
10. Audrey Terras, *Harmonic analysis on symmetric spaces and applications*, UCSD lecture notes.
11. \_\_\_\_\_, *Analysis on positive matrices as it might have occurred to Fourier*, Lecture Notes in Math., vol. 899, Springer-Verlag, Berlin and New York, 1981, pp. 442–478.
12. D. I. Wallace, *Explicit form of the hyperbolic term in the trace formula for  $SL(3, \mathbf{R})$  and Pell's equation for hyperbolics in  $Sl(3, \mathbf{Z})$*  (to appear).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA AT SAN DIEGO, LA JOLLA, CALIFORNIA 92093

*Current address:* Department of Mathematics, Florida International University, Miami, Florida 33199