#A32 INTEGERS 9 (2009), 423-426

CONJUGACY CLASSES AND CLASS NUMBER

Ashay Burungale
Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560059, India
ashayburungale@gmail.com

Received: 12/15/08, Revised: 4/9/09, Accepted: 4/22/09

Abstract

It is shown that the conjugacy classes of integral matrices with a given irreducible characteristic polynomial is in bijection with the class group of a corresponding order in an algebraic number field.

1. Main Results

The classical work of Gauss on integral, positive-definite, binary quadratic forms yields the class number of imaginary quadratic fields (see [3], [1]). For a general algebraic number field K, the class group can be viewed in terms of the ideles of K as a set of double cosets (see description below). However, the following simpler-looking result asserting that one could easily relate the class numbers of fields with the numbers of conjugacy classes in $GL_n(\mathbb{Z})$ with a given trace does not seem to be well-known. We prove such a result here. The precise relation involves class numbers of more general orders in number fields. We show that the ideal classes of an order $\mathbb{Z}[\alpha]$ correspond bijectively with the $GL_n(\mathbb{Z})$-conjugacy classes of integral matrices whose characteristic polynomial is the minimal polynomial of α. Before stating the result, let us recall the basic definitions. Let K be a number field of degree n over $\mathbb{Q}$ and let $\mathbf{O}_K$ be its ring of integers.

Definitions (see [2], Chapter 1, section 12). $\mathbf{O}$ is an *order* of K if it is a subring of $\mathbf{O}_K$ which contains a $\mathbb{Q}$-basis of K. Thus, K is the quotient field of $\mathbf{O}$ and the ring $\mathbf{O}_K$ is the unique maximal order. A *fractional ideal* of $\mathbf{O}$ is a finitely generated non-zero $\mathbf{O}$-submodule of K. A fractional ideal I is called invertible if there exists a fractional ideal I' such that, $II' = \mathbf{O}$. For the ring $\mathbf{O}_K$, all fractional ideals are invertible and thus, they form a group under the operation of multiplication of fractional ideals. Unfortunately, the fractional ideals of $\mathbf{O}$ do not form a group for a general order $\mathbf{O}$. However, if we consider only the invertible ideals of $\mathbf{O}$, they form a group. Let $J(\mathbf{O})$ denote the set of invertible fractional ideals of $\mathbf{O}$ and let $P(\mathbf{O})$ denote the subset of principal ideals $k\mathbf{O}$, $k \in K^*$ among them.

Definition The *Picard group (or class group)* $\text{Pic}(\mathbf{O})$ of $\mathbf{O}$ is defined as the quotient $J(\mathbf{O})/P(\mathbf{O})$.

A basic result is that this is always finite; denote its order by $h(\mathbf{O})$. Indeed, it can be described in terms of the class group of $\mathbf{O}_K$, whose finiteness is a more standard result usually established in all textbooks on algebraic number theory. To describe this relation, define the conductor f of $\mathbf{O}$ to be the largest ideal of $\mathbf{O}_K$ contained in $\mathbf{O}$.

Proposition (see [2], 12.12) We have $h(\mathbf{O}) = \frac{h(\mathbf{O}_K)}{[\mathbf{O}_K^* : \mathbf{O}^*]} \frac{|(\mathbf{O}_K/f)^*|}{|(\mathbf{O}/f)^*|}$.

The ideal class group of the maximal order $\mathbf{O}_K$ can also be described as double cosets in the so-called idele class group. The ideles I_K of K are defined as the elements $(x_v)_v$ of the product $\prod_v K_v^*$ of completions of K in which all but finitely many components x_v are in $\mathbf{O}_v^*$. Then K^* sits diagonally in I_K and the quotient $C_K := I_K/K^*$ is called the idele class group, which may be infinite. There is a natural surjective map from C_K to the class group Cl_K whose kernel is $I_K^\infty := \prod_{v \in \infty} K_v^* \times \prod_{v \notin \infty} \mathbf{O}_v^*$.

Our main result is :

Theorem. *Let α be an algebraic integer whose minimal polynomial is of degree n. The $GL_n(\mathbb{Z})$-conjugacy classes of matrices in $M_n(\mathbb{Z})$ which have α as an eigenvalue, are in one to one correspondence with the class group of the order $\mathbb{Z}[\alpha]$. In particular, when α is a unit, the class group of $\mathbb{Z}[\alpha]$ is in one to correspondence with the conjugacy classes in $GL_n(\mathbb{Z})$ with α an eigenvalue.*

For any $g \in GL_n(\mathbb{Q})$, let us recall its rational canonical form. This is obtained as follows. If $\chi_g(X)$ is the characteristic polynomial of g, there are polynomials $f_1, f_2, \cdots, f_d$ where f_i divides f_{i+1}, where f_d is the minimal polynomial of g and where $\chi_g = f_1 f_2 \cdots f_d$. Recall that the companion matrix of a monic polynomial $p(X) = \sum_{i=0}^{r-1} a_i X^i + X^r$ is the $r \times r$ matrix

$$C(p) := \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{r-1} \end{pmatrix}.$$

Note that this amounts to writing the matrix representing multiplication by X on the ordered basis $\{1, X, \cdots, X^{r-1}\}$ of $\mathbb{Q}[X]/(p(X))$. Then, the rational canonical form of $g \in GL_n(\mathbb{Q})$ which is a conjugate PgP^{-1} for some $P \in GL_n(\mathbb{Q})$, is the block matrix

$$\begin{pmatrix} C(f_1) & 0 & 0 & \cdots & 0 \\ 0 & C(f_2) & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & C(f_{d-1}) & 0 \\ 0 & 0 & \cdots & 0 & C(f_d) \end{pmatrix}.$$

Let $g \in GL_n(\mathbb{Z})$ and let α be an eigenvalue of g; this is an algebraic integer whose minimal polynomial is f_d as above.

Proof of theorem. The rational canonical form of g is

$$PgP^{-1} = C(\chi) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

where $\chi_g(X) = \sum_{i=0}^{n-1} a_i X^i + X^n$ holds; that is, with respect to the ordered basis $\{1, \alpha, \cdots, \alpha^{n-1}\}$ of $\mathbb{Q}(\alpha)$, multiplication by α corresponds to the matrix PgP^{-1} on the canonical ordered basis of $\mathbb{Q}^n$. Hence, $I_g :=$ $\mathbb{Z}$-span of $P^{-1}\begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \end{pmatrix}^t$ is a $\mathbb{Z}[\alpha]$-submodule of $\mathbb{Q}(\alpha)$ containing a $\mathbb{Q}$-basis of the latter vector space.

Note that if g' is conjugate to g in $GL_n(\mathbb{Z})$, then $I_{g'}$, I_g are in the same equivalence class in the class group. Thus, we have associated to a class $[g] \in M_2(\mathbb{Z})$ a unique class $[I]$ of the order $\mathbb{Z}[\alpha]$ (when the characteristic polynomial of α is irreducible).

Conversely, consider an invertible fractional ideal I of the order $\mathbb{Z}[\alpha]$. Choose an integral basis, say $(b_i)_{1 \le i \le n}$, of I. Multiplication by α is a $\mathbb{Q}$-linear transformation from I to I. Let g be the matrix of this linear transformation with respect to the above chosen basis of I. Clearly it is an integral matrix and α is an eigenvalue of this matrix. If $(b'_i)_{1 \le i \le n}$ is some other integral basis of I, g would be changed to a matrix conjugate to itself over $\mathbb{Z}$. Also, if I' is another invertible fractional ideal belonging to the class of I i.e., $I' = \gamma I$ for some γ, then the corresponding basis will be $(\gamma b_i)_{i=1}^{i=n}$ and g will be simply changed to a matrix similar to itself over $\mathbb{Z}$. So, we have a map from a class of the order $\mathbb{Z}[\alpha]$ to a unique class in $M_n(\mathbb{Z})$ which has α as an eigenvalue. □

Remarks - a question. It would be interesting to deduce results about the Picard group from the results about conjugacy classes. For instance, an interesting question which arises is, whether the following result about the divisibility of class numbers can be proved in this way; it is usually proved (see [4]) using the Hilbert class field:

Theorem*If m, n are natural numbers such that $m|n$, then the class number of $\mathbb{Q}(\zeta_m)$ divides that of $\mathbb{Q}(\zeta_n)$.*

This can be shown for example using the Hilbert class field (see [4]).

2. Some Examples

Example 1. Let $\alpha = \sqrt{-5}$. The minimal polynomial of α is $x^2 + 5$. Any matrix in $M_2(\mathbb{Z})$ whose characteristic polynomial is $x^2 + 5$ is $GL_2(\mathbb{Z})$-conjugate to exactly one of the two matrices :

$$A = \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} -1 & -3 \\ 2 & 1 \end{pmatrix}$$

This is in harmony with the fact that the class group of $\mathbb{Z}[\sqrt{-5}]$ is two. Indeed, by the theorem, A corresponds to the unit ideal and B corresponds to the ideal generated by 2 and $\sqrt{-5}$.

Example 2. Let $\beta = 1 + \sqrt{-23}/2$. Then $x^2 - x + 6$ is the minimal polynomial of β. Any matrix in $M_2(\mathbb{Z})$ whose characteristic polynomial is $x^2 - x + 6$ is $GL_2(\mathbb{Z})$-conjugate to exactly one of the three matrices :

$$P = \begin{pmatrix} 0 & -6 \\ 1 & 1 \end{pmatrix}, Q = \begin{pmatrix} -1 & -4 \\ 2 & 2 \end{pmatrix} \text{ and } R = \begin{pmatrix} -1 & -2 \\ 4 & 2 \end{pmatrix}.$$

This again is in harmony with the fact that the class number of $\mathbb{Z}[\beta]$ is three. The above matrices correspond by the theorem, respectively, to the three ideal classes 'trivial', $[2, 1 + \beta]$ and $[4, 1 + \beta]$.

In the case of quadratic number fields, a connection between the class group of the quadratic forms and the class group emerges naturally via the theorem.

Acknowledgments. This article is written under the guidance of Professor B. Sury. I thank him for his encouragement and support. Thanks are also due to the referee who suggested that some examples be added.

References

[1] David Cox, *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, 1989.

[2] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999.

[3] I. Niven, H. S. Zuckermann, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons, 5th Ed. , 1991.

[4] L.Washington, *Introduction to Cyclotomic fields*, Graduate Texts in Mathematics No. 83, Springer, 2nd Ed., 1996.