AN ELEMENTARY ACCOUNT OF SELBERG'S LEMMA

Autor(en): **Alperin, Roger C.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **33 (1987)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **23.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-87896

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

L'Enseignement Mathématique, t. 33 (1987), p. 269-273

AN ELEMENTARY ACCOUNT OF SELBERG'S LEMMA

by Roger C. ALPERIN

A basic result in the theory of linear groups which is of great utility in algebra and topology is known as "Selberg's Lemma". This lemma is both a generalization of earlier results of Minkowski on congruence subgroups of $GL_n(Z)$ and also of Burnside's Theorem (Corollary 3 below) which suggested the famous Burnside Problem [H].

SELBERG'S LEMMA. *A finitely generated group of matrices over a field of characteristic zero has a torsion free subgroup of finite index.*

In fact, Selberg's Lemma follows easily from the theorem below where we let A be the finitely generated ring containing all the entries of the n by n matrices of the given finitely generated group. We present an "elementary" proof of this theorem using basic results from field theory and algebraic number theory. With deeper results from ring theory the theorem can be extended further [W].

For convenience we include a discussion of the important notion of residual finiteness. Roughly speaking, a group is residually finite if there are lots of finite quotients; more precisely, we say a group G is residually finite if for each element $g \neq 1$ there is a finite homomorphic image H_g so that the image of g in H_g is not the identity.

THEOREM. *The group of matrices $G = GL_n(A)$, for a finitely generated integral domain A, is residually finite. If A is of characteristic zero then G contains a normal subgroup of finite index which is torsion free. If A is of finite characteristic then G contains a normal subgroup of finite index in which every element of finite order is unipotent.*

Proof. The quotient field of A is a finitely generated field F which is a finite algebraic extension of degree k over the purely transcendental field $K = P(x_1, x_2, ..., x_m)$ where P is the prime field, Q or F_q. By expressing the finite set of generators of A in terms of the basis for F over K we

see that the coefficients involve certain "denominators" which are elements in a finitely generated ring B. In the characteristic zero case we may take $B = Z[1/s][x_1, x_2, \ldots x_m, 1/f]$ for suitable integer s and polynomial f, while in the characteristic q case, $B = F_q[x_1, x_2, \ldots x_m, 1/f]$.

Now if V is an n-dimensional vector space over F we can use the natural representation

$$\mathrm{End}_F(V) \to \mathrm{End}_K(V)$$

to get another representation of our group; by considering $V = F^n$ we obtain an injective homomorphism

$$\rho: GL_n(F) \to GL_{nk}(K);$$

thus $\rho(G)$ is a group of $N(=nk)$ by N matrices with entries in the purely transcendental field K. Furthermore, the homomorphism ρ represents the group $GL_n(A)$ as a subgroup of $GL_N(B)$. Thus, in order to prove this theorem we shall demonstrate it for $G = GL_N(B)$.

We first show that G is residually finite. For a non-identity element g of $GL_N(B)$ there is a non-zero entry $w(x_1, x_2, \ldots, x_m, 1/f)$ in the matrix $g - 1$. In the characteristic zero case choose a prime p not dividing s so that mod p not all the coefficients of w are 0. Now choose a sufficiently large integer v so that $u = f^v w$ is a polynomial in $x_1, x_2, \ldots, x_m$; choose a substitution of elements $a_1, a_2, \ldots, a_m$ from the algebraic closure of the finite field F_r, $r = p$ or q (finite characteristic) so that $u(a_1, a_2, \ldots, a_m) \neq 0$ and thus $w(a_1, a_2, \ldots, a_m, 1/f(a_1, a_2, \ldots, a_m)) \neq 0$. Thus the kernel $\mathfrak{b}$ of the homomorphism

$$\pi: B \to F_r(a_1, a_2, \ldots, a_m)$$

is a maximal ideal of finite index; consequently, the induced homomorphism

$$\Pi: GL_N(B) \to GL_N(B/\mathfrak{b})$$

has finite image and $\Pi(g) \neq 1$.

We proceed with the rest of the proof by separating the cases of zero characteristic and finite characteristic. In both cases we show first that the torsion has bounded exponent.

Characteristic zero. Consider an element g of finite order α in G; g satisfies the polynomial $x^\alpha - 1$ for some integer $\alpha \neq 1$. It follows that the minimal polynomial of g has distinct roots since the field has characteristic zero; furthermore, the eigenvalues are roots of unity. Since the coefficients of the characteristic polynomial of g are the symmetric functions in its roots

(of unity) these coefficients are algebraic integers in $K = Q(x_1, x_2, ..., x_m)$. Consequently, the trace of an element of finite order in G is an integer and moreover its absolute value is less than or equal to N; thus, there are only a finite number of traces of these elements of finite order. Denote this set of traces as T. (In fact, if p^e is the highest power of p dividing α then $\Phi(p^e) \leqslant N$, where Φ is Euler's totient function.)

Consider a prime number p which does not divide the integer s, the coefficients of the polynomial f and the non-zero integers $t - N$ for any t in T; there are an infinite number of such primes. Let Ω_p denote the algebraic closure of the field with p elements. Consider a homomorphism $\sigma: A \to \Omega_p$ obtained by extending the natural reduction mod p on $Z[1/s]$ by sending x_i to a_i in Ω_p where $f(a_1, a_2, ..., a_m) \neq 0$. This is possible since Ω_p is an infinite field. It follows from this construction that $\sigma(A) = F_p(a_1, a_2, ..., a_m)$ is a finite field; thus kernel $(\sigma) = \mathfrak{a}$ is a maximal ideal of finite index in A.

The natural homomorphism $\Sigma: GL_N(A) \to GL_N(A/\mathfrak{a})$ has kernel $G(\mathfrak{a})$, the congruence subgroup of level $\mathfrak{a}$, which is of finite index. The trace of any element of $G(\mathfrak{a})$ is equal to N mod $\mathfrak{a}$. Consider now the subgroup $G_0 = G \cap G(\mathfrak{a})$; it is of finite index in G. Furthermore, any element g of G_0 of finite order has trace $(g) = t$, for t in T, and also since g is in the congruence subgroup of level $\mathfrak{a}$, trace $(g) = N$ mod $\mathfrak{a}$. Thus $t - N$ is an integer which reduces mod $\mathfrak{a}$ to 0 and thus p divides $t - N$; hence, it follows from our choice of p that $t = N$. Since the minimal polynomial of g has distinct roots it follows that g is diagonalizable, and finally, since its trace is N, $g = 1$. Thus G_0 is a torsion free subgroup of finite index in G and the characteristic zero part of the theorem is proved.

Finite characteristic. Any eigenvalue λ of an element of finite order in $GL_N(B)$ is algebraic of degree less than or equal to N over the prime field F_q and thus λ lies in the finite field with $r = q^N$ elements; consequently $\lambda^{r-1} = 1$. Hence, there is a bound on the order of the torsion elements of G. For convenience we now adjoin all the $(r-1)$st roots of unity to F_q to obtain a larger ring $C = F_r[x_1, x_2, ..., x_m, 1/f]$. In this way we have represented $G = GL_N(B)$ as a subgroup of $GL_N(C)$ so that the eigenvalues of all elements of finite order in G are in F_r.

Let $\mathfrak{c}$ be any maximal ideal of C of finite index; such an ideal is obtained as the kernel of a homomorphism which specializes x_i to a_i in Ω_p so that $f(a_1, a_2, ..., a_m) \neq 0$. Now, the characteristic polynomial of an element of finite order in $G(\mathfrak{c}) = \ker(GL_N(C) \to GL_N(C/\mathfrak{c}))$ is $(x-1)^N$ mod $\mathfrak{c}$;

therefore since any eigenvalue λ of an element of finite order in $G(\mathfrak{c})$ satisfies this characteristic polynomial, $(\lambda-1)^N$ is in $\mathfrak{c}$. Since this ideal is maximal it follows that $\lambda - 1$ is in $\mathfrak{c}$. However, λ is algebraic and hence also $\lambda - 1$; therefore $\lambda - 1$ is in $F_r \cap \mathfrak{c}$ which is 0. Therefore all the eigenvalues of an element of finite order in $G(\mathfrak{c})$ are 1 and this means that any element of finite order in $G(\mathfrak{c})$ is unipotent. Hence, the subgroup $G_0 = G \cap G(\mathfrak{c})$ satisfies the conclusion of the theorem.

COROLLARY 1. *A finitely generated group G of matrices over a field F is residually finite. If F is of characteristic zero then G contains a normal subgroup of finite index which is torsion free. If F is of finite characteristic then G contains a normal subgroup of finite index in which every element of finite order is unipotent.*

The proof of this corollary follows immediately from the theorem and the remarks preceeding it.

COROLLARY 2. *The torsion subgroups of a finitely generated linear group G are finite; moreover, in characteristic zero, these finite groups have bounded order.*

Proof. We may assume that the group G is a finitely generated subgroup of $GL_n(A)$ where A is a finitely generated domain. Choose the normal subgroup M of finite index in $GL_n(A)$ so that it satisfies the conclusion of the theorem. Let $M_0 = G \cap M$, and $G_0 = G/M_0$. Suppose that H is a torsion subgroup of of G. In characteristic zero, we see that $H \cap M = (1)$ so $\# \mid H \mid \leqslant \# \mid G_0 \mid$. In finite characteristic $H \cap M$ is contained in a finitely generated group of unipotent matrices. This finitely generated unipotent subgroup is solvable (also nilpotent) and torsion; consequently, by an easy induction on the solvable length, we see that it's finite. Hence, also, the torsion subgroups are finite.

NOTE. It follows easily, by similar reasoning, that the finite subgroups of $GL_n(A)$ have bounded order in case A has characteristic zero.

COROLLARY 3 (Burnside's Theorem). *A finitely generated torsion group of matrices over a field is finite.*

The proof of this corollary follows immediately from Corollary 2.

We thank M. Feighn for a critical reading of an earlier version of this note.

BIBLIOGRAPHY

[H] HERSTEIN, I. *Noncommutative Rings.* Carus Mathematical Monographs, No. 15, Mathematical Association of America, 1968.

[S] SELBERG, A. On Discontinuous Groups in Higher Dimensional Symmetric Spaces. *Contributions to Function Theory*, Tata (1960), 147-164.

[W] WEHRFRITZ, B. *Infinite Linear Groups.* Springer, 1973.

(Reçu le 18 novembre 1986)

Roger Alperin

Department of Mathematics and Computer Science
San Jose State University
San Jose, CA 95192
USA