ISRAEL JOURNAL OF MATHEMATICS 88 (1994), 31–72

BETTI NUMBERS OF CONGRUENCE GROUPS

BY

PETER SARNAK

Department of Mathematics
Princeton University, Princeton, NJ 08544, USA
e-mail: sarnak@math.princeton.edu

AND

SCOT ADAMS

Department of Mathematics
University of Minnesota, Minneapolis, MN 55455, USA
e-mail: adams@math.umn.edu

AND

APPENDIX
ON REPRESENTATIONS OF COMPACT p-ADIC GROUPS

ZE'EV RUDNICK

Department of Mathematics
Princeton University, Princeton, NJ 08544, USA
e-mail: rudnick@math.princeton.edu

ABSTRACT

It is shown that, for certain congruence families of Galois coverings of a manifold, the individual Betti numbers are polynomial periodic functions of the level. Similar results are proved for the dimensions of other spaces of automorphic forms.

Received March 1, 1990 and in revised form September 1, 1993

0. Preface

This paper constitutes a revised version of the Australian Mathematical Society reprint [Sa]. The revision concerns the proof of Theorem 1.2 for the general unipotent case. Since the writing of [Sa], a number of related publications have occurred. E. Hironaka [Hi2, Hi3] has used the results below to prove polynomial periodicity for Hirzebruch and more general surfaces. The recent paper of Ruppert [Ru] is closely related to Proposition 1.6 below and gives moreover bounds for torsion points.

1. Introduction

It is well known that the genus of the Fermat curve $F(N)$; $x^N + y^N = 1$, is $(N-1)(N-2)/2$. This is easily seen by realizing $F(N)$ as a $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ branched covering of $\mathbb{P}^1$ and applying Hurwitz's formula. In this paper we give a general result about families of manifolds which ensures that their Betti numbers are polynomial periodic.

Let K be a finite simplicial complex and let $\Gamma = \pi_1(K)$ be its fundamental group. As usual let $\tilde{K}$ denote the universal covering of K. For $\Gamma' \lhd \Gamma$ of finite index we get a Γ/Γ' Galois covering $K' = \tilde{K}/\Gamma'$ of K. We are interested in the q-dimensional Betti numbers $\beta^q(K')$ as Γ' varies over "congruence groups". To define these congruence groups we assume that we have a homomorphism

$$(1.1) \qquad \varphi\colon \Gamma \overset{\text{onto}}{\longrightarrow} H(\mathbf{Z}),$$

where H is a matrix algebraic group defined over $\mathbf{Q}$ and $H(\mathbf{Z})$ denotes the $\mathbf{Z}$-points of H. Moreover, we assume that H has strong approximation [K]. For each integer $N \geq 1$, let

$$(1.2) \qquad R_N\colon H(\mathbf{Z}) \to H(\mathbf{Z}/N\mathbf{Z})$$

denote reduction mod N. The congruence groups $\Gamma(N)$ are then defined by

$$(1.3) \qquad \Gamma(N) = \ker(R_N \circ \varphi).$$

Let $H_N := R_N(H(\mathbf{Z}))$. Clearly $\Gamma/\Gamma(N) \simeq H_N$ and $K(N) := \tilde{K}/\Gamma(N)$ is an H_N Galois covering of $K(1)$.

The two most interesting examples of congruence groups are the cases

(C.i) The map φ in (1.1) is an isomorphism in which case $\Gamma(N)$ is the familiar principal congruence subgroup of $H(\mathbf{Z})$ of level N.

(C.ii) The group H is Abelian and hence the homomorphism φ factors through $H_1(K,\mathbf{Z}) \simeq \Gamma/[\Gamma,\Gamma]$. The most interesting case is that of $H(\mathbf{Z}) = \mathbf{Z}^r$, r being $\beta_1(K)$. Some concrete examples of (ii) are the following:

(A) Fermat Curves. The Fermat curves $F(N)$ may be uniformized as $\Phi(N)\backslash\mathcal{H}$, where

$$\begin{aligned}\Phi(1) &= \Gamma(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2 \right\}, \\ \Phi(N) &= \ker(R_N \circ \varphi),\end{aligned}$$

where $\varphi\colon \Gamma(2) \to \mathbf{Z}^2$ is the projection on homology. $R_N\colon \mathbf{Z}^2 \to (\mathbf{Z}/N\mathbf{Z})^2$ is as above, reduction mod N and $\mathcal{H}$ is the upper half plane. For more details see Lang [L1]. Actually to be more precise $F(N)$ is the compactification (branched) of $\Phi(N)\backslash\mathcal{H}$. Note that while $\Phi(N)$ is a congruence group in our sense it is not so according to the usual definition [S].

(B) Links in S^3. Let $L \subset S^3$ be a μ-component link; that is disjoint union of μ circles. Let $\Gamma = \pi_1(S^3 \setminus L)$. It is well known and easily seen that $H_1(S^3 \setminus L) \simeq \mathbf{Z}^\mu$. Let $\varphi\colon \Gamma \to \mathbf{Z}^\mu$ be the Abelianizer and R_N as above. We get in this way for each N a uniquely defined $(\mathbf{Z}/N\mathbf{Z})^\mu$ covering $M(N)$ of $S^3 \setminus L$. When L is a knot (i.e., $\mu = 1$) these are the well studied cyclic covers [F–1].

(C) Hirzebruch Surfaces [Hh]. Let $\ell_1, \ldots, \ell_r$ be an arrangement of lines in $\mathbf{P}^2(\mathbf{R}) \subset \mathbf{P}^2(\mathbf{C})$. The Hirzebruch surface $E(N)$ for $N \geq 1$ is the $(\mathbf{Z}/N\mathbf{Z})^{r-1}$ branched cover of $\mathbf{P}^2(\mathbf{C})$ branched over $\ell_1, \ldots, \ell_r$, see [Ha] for a discussion. Hirzebruch computed the characteristic numbers of $E(N)$. Their Betti numbers for certain $\ell_1, \ldots, \ell_r$ and N were computed by Ishida [I] and Hironaka [Ha].

Before turning to our results we consider a related problem. Let G be a semisimple real, complex, or p-adic group. Let $\Gamma \leq G$ be a cocompact lattice. The right regular representation of G on $L^2(\Gamma\backslash G)$ decomposes into $\bigoplus_{i=1}^\infty V_i$ where V_i are irreducible unitary representations of G. We denote by $\hat{G}$ the set of equivalence classes of such representations. One of the fundamental problems in automorphic form theory is to determine $m(\pi,\Gamma)$, the multiplicity with which some $\pi \in \hat{G}$ appears in the above decomposition. It is known [B–W] that for certain π's this multiplicity corresponds to cohomology of Γ. We call such π's cohomological. Now let $\Gamma(N) < \Gamma$ be a congruence family in the sense defined above. Our aim is to study $m(\pi, \Gamma(N))$ as a function of N.

Note that the group $H_N \times G$ acts unitarily on $L^2(\Gamma(N) \setminus G)$ by

$$(h,g)\, f(x) \to f(h^{-1}x\, g)\,. \tag{1.4}$$

Decomposing this into irreducibles we get multiplicities $m(\rho \otimes \pi, \Gamma(N))$ with $\rho \in \hat{H}_N$. For $\nu \geq 1$ and integer, we define the ν–dimensional part of $m(\pi, \Gamma(N))$ to be

$${}^{\nu}m(\pi, \Gamma(N)) = \sum_{\substack{\dim \rho = \nu \\ \rho \in \hat{H}_N}} m(\rho, \Gamma(N))\,.$$

We can recover $m(\pi, \Gamma(N))$ by

$$m(\pi, \Gamma(N)) = \sum_{\nu=1}^{\infty} {}^{\nu}m\,(\pi, \Gamma(N))$$

(the sum of course is finite).

Returning to the simplicial complex setting, we have H_N acting as Galois group of $K(N)\backslash K(1)$ and hence H_N acts on the cohomology groups $H^q(K(N))$. Decomposing this action into irreducible gives

$$H^q(K(N)) = \bigoplus_i W_i\,.$$

We define the ν–dimensional part of the qth Betti number ${}^{\nu}\beta^q(K(N))$ to be

$${}^{\nu}\beta^q(K(N)) = \dim \left(\sum_{\dim W_i = \nu} W_i \right)\,. \tag{1.5}$$

We observe that if H is Abelian then ${}^{1}\beta^q(K(N)) = \beta^q(K(N))$ and ${}^{1}m\,(\pi, \Gamma(N)) = m(\pi, \Gamma)$ since all irreducibles of H are 1–dimensional.

Definition 1.1: A sequence $a(n)$, $n \geq 1$, is polynomial periodic if there are periodic $b_j(n)$, $j = 1, \ldots, q$ such that $a(n) = \sum_{j=0}^{q} b_j(n)\, n^j$. ∎

We can now state the periodicity theorem

THEOREM 1.2: *Assume that H is either unipotent or semisimple then*

(i) *If $\Gamma = \pi_1(K)$ is as above and $\Gamma(N)$, $N \geq 1$, a congruence family, then ${}^{\nu}\beta^q(K(N))$ is polynomial periodic in N.*

(ii) *If G is Archimedian and π is cohomological or if G is p–adic and π is arbitrary, then ${}^{\nu}m\,(\pi, \Gamma(N))$ is polynomial periodic in N.*

Remark 1.3: Since the general H is roughly a semidirect product of a unipotent part with a semisimple part (recall that H has strong approximation) we expect that the Theorem is valid for the general H. In [Ad, Theorems 6.7 and 6.8], this question is mostly settled in the affirmative; however, some additional hypotheses are needed.

COROLLARY 1.4: *Let L be a μ–component link in S^3 and set $M(N)$ to be the $(\mathbf{Z}/N\mathbf{Z})^\mu$ cover ốf S^3 branched along L; then $\beta^1(M(N))$ is polynomial periodic.*

This Corollary in the case of knots is known and due to Goeritz [G] and Zariski [Z] and to Sumners [Su] in higher dimensions. In fact, for knots one can show that the sequence is periodic (i.e., $q = 0$ in Definition 1.1). In general this is not so as the following example shows: The link L in Figure 1.5 has two components. We can write down $\beta^1(M^u(N))$ compactly for all N by use of the generating function $\sum_{N=1}^{\infty} \beta^1(M^u(N))/N^s$. In Section 4 we show

$$(1.6) \qquad \sum_{N=1}^{\infty} \frac{\beta^1(M^u(N))}{N^s} = 2\,(1 + 2^{-s} + 6^{-s})\,\zeta(s) + 2 \cdot 6^{-s}\zeta(s-1)\,,$$

where $\zeta(s) = \sum_{N=1}^{\infty} N^{-s}$. Here $M^u(N)$ in the unbranched $(\mathbf{Z}/N\,\mathbf{Z})^2$ covering of $S^3 \setminus L$.

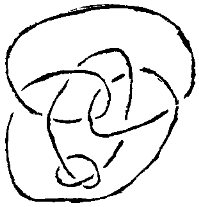

Figure 1.5.

COROLLARY 1.5: *Let $E^u(N)$ be the unbranched Hirzebruch surfaces over a fixed configuration of lines; then the Betti numbers $\beta^1(E^u(N))$ are polynomial periodic in N.*

In [Ha], E. Hironaka developed a method for computing the difference between the Betti numbers of the branched and unbranched surface. Using this result, she has proved periodicity in the branched covers $E(N)$ (see [Ha2]), as well as more general such surfaces [Ha3]. For cyclic coverings of P^2, such results follow from Libgober [Lr2].

Our Theorem does not apply to $m(\pi, \Gamma(N))$ when G is Archimedean and π is not cohomological. In these cases we only get asymptotic results. An analysis of

$m(\pi, \Phi(N))$ for $\Phi(N)$ the Fermat groups and $\pi \in \widehat{\mathrm{PSL}(2, \mathbf{R})}$, with π principal or complementary series will be given elsewhere ([P-S]). Suffice it to say here that it still appears to be the case that $m(\pi, \Phi(N))$ is periodic in N, though a proof of this seems out of reach at present.

There are a number of ingredients that go into the proof of Theorem 1.2. In Section 2 we discuss the variety of representations of Γ into $\mathrm{GL}(\nu, \mathbf{C})$ and the important algebraic subsets connected with the cohomology problem. In Section 3 the problem of counting torsion points on algebraic subsets is studied. Specifically let T be an r–dimensional real torus and let $W \subset T$ be an algebraic subset (i.e., the zero set of a trigonometric polynomial or intersection of such sets). Denote by $\mathrm{tor}\,(T)$ the set of torsion points (i.e., elements of finite order in T). The following was conjectured by Lang [L2]:

PROPOSITION 1.6: *There are a finite number of rational planes $\pi_1, \ldots, \pi_\ell$ (a rational plane is a closed connected subgroup of T or a translate thereof by a torsion point) contained in W such that*

$$\mathrm{tor}\,(T) \cap W = \mathrm{tor}\,(T) \bigcap \left(\bigcup_{j=1}^{\ell} \pi_j \right) .$$

In Section 3 an elementary and algorithmic proof of this Proposition is given. Given W it produces the planes $\pi_1, \ldots, \pi_\ell$ which is crucial for the purposes of computing the periodicities and polynomials. Another proof of this conjecture is contained in the work of Laurant [Lt]. The importance of Proposition 1.6 lies in the fact that as far as torsion goes we may linearize W, that is replace it by planes. It is this that is responsible for the polynomial periodicity. In Section 4 we complete the proof of the Theorem and its Corollary. Sections 5–11 are devoted to the proof of a technical fact (Theorem 11.3) which is crucial to the proof of Theorem 1.2, when H is unipotent.

ACKNOWLEDGEMENT: The first author would like to thank A. Adem, P. Cohen, D. Fried, A. Lubotzky and J.–P. Serre for illuminating discussions on various aspects of this paper.

2. Representation varieties and cohomology

Let K be a finite simplicial complex $\tilde{K}$ and $\Gamma = \pi_1(K)$ as in Section 1. If R is a finite-dimensional unitary representation of Γ in $\mathrm{GL}(V)$, then the R–twisted cochain complex $C(\tilde{K}, R)$ is defined by

(2.1)
$$C^q(\tilde{K}, R) = \{F\colon C_q(\tilde{K}) \to V,\ F \text{ is linear and } F(\gamma\sigma) = R(\gamma)\,F(\sigma) \text{ for } \gamma \in \Gamma\}.$$

We have a coboundary operator

$$\delta^q\colon C^q(\tilde{K}, R) \to C^{q+1}(\tilde{K}, R)$$

given by

$$(\delta^q F)\,(\sigma) = F(\partial\sigma)\,. \tag{2.2}$$

The cohomology groups $H^*(\tilde{K}, R)$ are defined in the usual way (here and elsewhere $C_q(\tilde{K})$ is to be taken with complex coefficients). Our first problem is to determine the behavior of $\beta^q(\tilde{K}, R) = \dim H^q(\tilde{K}, R)$ as a function of R. While the variety of all (up to equivalence) representations of Γ in $\mathrm{GL}(\nu, \mathbf{C})$ can be quite complicated, the set of those which have finite image (which are all that we need consider) is much more tractable. In fact as is shown in Lubotzky–Magid [L–M], it follows from a theorem of Jordan, see [C–R], that all such R's which are irrducible and of dimension ν factor through a fixed quotient Δ of Γ. Moreover Δ is Abelian by finite. Rudnick [R] gives a description of the variety $V(\Delta, \nu)$ of *all* irreducible representations (up to equivalence) of such a Δ. In what follows we will denote by $T(B)$ the torus of 1–dimensional unitary characters of a group B. Rudnick shows that there are finite index subgroups $H_1, \ldots, H_L$ of Δ such that

$$V(\Delta, \nu) \subseteq \bigcup_{j=1}^{L} \left(\bigcup_{\chi \in T(H_j)} \mathrm{Ind}_{H_j}^{\Delta}(\chi) \right)\,. \tag{2.3}$$

We are thus led to examine the functions

$$F_j(\chi) = \beta^{(k)}(\tilde{K}, \mathrm{Ind}_{H_j}^{\Delta}(\chi)), \quad \chi \in T(H_j). \tag{2.4}$$

To do so we will use Hodge theory in the form of the finite combinatorial Laplacian. For our purposes this has the advantage of dealing with the automorphic form problem in the same way.

As in Ray–Singer [R–S] choose a preferred basis $F_{i,j}^q = \widetilde{\sigma_i^q \otimes e_j}$ of $C^q(\tilde{K}, R)$ as follows: Let $e_1, \ldots, e_m$ be an orthonormal basis of V and let $\sigma_1^q, \ldots, \sigma_{\nu_q}^q$ be the set of q-simplices of K (which we think of as embedded in $\tilde{K}$). For $i = 1, \ldots, \nu_q$, $j = 1, \ldots, m$

$$\widetilde{\sigma_i^q \otimes e_j}\,(\gamma\,\sigma_\ell^q) = \begin{cases} 0 & \text{if } i \neq \ell, \\ R(\gamma)\,e_j & \text{if } i = \ell. \end{cases} \tag{2.5}$$

Then δ has a matrix representation relative to the bases $F_{i,j}^q$ and $F_{i,j}^{(q+1)}$. Using these bases we may define δ^* and also the combinatorial Laplacian $\Delta_{(c)}^q$: $C^q(\tilde{K}, R) \to C^q(\tilde{K}, R)$ by

$$\Delta_{(c)}^q = (\delta^{(q+1)})^*\,\delta^q + \delta^{q-1}(\delta^q)^*\,. \tag{2.6}$$

As with the usual Hodge theory

$$\dim\ker\Delta_{(c)}^q = \beta^q(\tilde{K}, R)\,. \tag{2.7}$$

Returning to our R's of the form (2.4), let ψ: $\Gamma \to \Delta$ be the projection and denote by $R(\chi)$ the representation of Γ given by

$$R(\chi) = \operatorname{Ind}_H^\Delta(\chi) \circ \psi\,. \tag{2.8}$$

Let $H\,\delta_1, H\,\delta_2, \ldots, H\,\delta_\mu$ be coset representatives of H in Δ. An orthonormal basis of $V = V(\operatorname{Ind}_H^\Delta(\chi))$ can be chosen in the form $e_1, \ldots, e_\mu$ when

$$e_j(h\,\delta_r) = \begin{cases} \chi(h) & \text{if } j = t, \\ 0 & \text{otherwise.} \end{cases} \tag{2.9}$$

Proposition 2.1: *The matrix of $\Delta_{(c)}^q(R(\chi))$ relative to the basis $\widetilde{\sigma_i^q \otimes e_j}$ of $C^q(\tilde{K}, R(\chi))$ has entries which are trigonometric polynomials in χ.*

The proof is a straightforward verification. We note for later that Proposition 2.1 holds equally well with $R(\chi)$ replaced by

$$\tilde{R}(\chi) = R_0 \otimes \chi\,, \tag{2.10}$$

where R_0 is a ν-dimensional representation of Γ. For $\lambda \in \mathbf{C}$ and $\chi \in T(H)$ let $p(\lambda, \chi)$ denote the characteristic polynomial

$$p(\lambda, \chi) = \det(\lambda - \Delta_{(c)}^q(R(\chi))). \tag{2.11}$$

Define the algebraic subsets of $T(H)$, $V_0 \supset V_1 \supset V_2 \cdots$ by

$$V_1 = \{\chi \mid p(0, \chi) = 0\}, \qquad V_k = \left\{\chi \;\middle|\; \frac{\partial^{k-1} p}{\partial\lambda^{k-1}}(0, \chi) = 0\right\} \cap V_{k-1}. \tag{2.12}$$

In view of Proposition 2.1 the V_k's are indeed algebraic. Note that

$$V_k = \{\chi \mid \beta^q(\tilde{K}, R(\chi)) \geq k\}\,. \tag{2.13}$$

Hence

$$\beta^q(\tilde{K}, R(\chi)) = \sum_{k \geq 1} \varepsilon(\chi, V_k)\,, \qquad \text{where } \varepsilon(\chi, V) = \begin{cases} 1 & \text{if } \chi \in V, \\ 0 & \text{if } \chi \notin V. \end{cases} \tag{2.14}$$

The last sum is finite since $V_k = \emptyset$ for large k.

Now recall that only the $R(\chi)$'s which are of finite image play a role in our analysis. For these clearly $\chi \in T(H)$ must be a torsion point, that is we are interested in $\beta^q(\tilde{K}, R(\chi))$ for $\chi \in \operatorname{tor}(T(H))$. Applying the linearization Proposition 1.6 we conclude that for each V_k there are planes $\pi_1^{(k)}, \ldots, \pi_{\ell_k}^{(k)}$ and integers $m_1^{(k)}, \ldots, m_{\ell_k}^{(k)}$ (which come from inclusion–exclusion) such that for $\chi \in \operatorname{tor}(T(H))$

$$\varepsilon(\chi, V_k) = \sum_{\mu=1}^{\ell_k} m_\mu^{(k)}\, \varepsilon(\chi, \pi_m^{(k)})\,. \tag{2.15}$$

Combining this with (2.14) we obtain our basic formula for $F_k(\chi)$ in (2.4) (we drop the index k).

Proposition 2.2: *There are planes $\pi_1, \ldots, \pi_L$ and integers $m_1, \ldots, m_L$ such that for $\chi \in \operatorname{tor}(T(H))$*

$$\beta^q(\tilde{K}, R(\chi)) = \sum_{\mu=1}^{L} m_\mu\, \varepsilon(\chi, \pi_\mu)\,.$$

Thus far we have examined only the cohomological case, $\Gamma = \pi_1(K)$. To deal with part (ii) of Theorem 1.2 when Γ is a lattice in a p-adic group G, one proceeds along similar lines. Let $m(\pi, \Gamma, R(\chi))$ have the obvious meaning, where $\chi \in T(H)$ as above. Now say G is rank 1 (actually it is only for rank 1 that the variety of representation of Γ into $\mathrm{GL}(\nu, \mathbf{C})$ is not zero dimensional); then by the duality theorem [G–G–P], $m(\pi, \Gamma, R(\chi))$ may be realized as the dimension of a certain eigenvalue of a vector valued Laplacian over the finite graph $\Gamma \backslash G/U$, U being a maximal compact subgroup of G. Hence the setup is identical to what we have and the only change needed is that in (2.6) we are interested in the general eigenvalue of Δ rather than just $\lambda = 0$. Of course there was nothing special about $\lambda = 0$ in what followed. One proceeds to derive an expression for $m(\pi, \Gamma, R(\chi))$ where $\chi \in \operatorname{tor}(T(H))$, just like the one in Proposition 2.2.

We remark that in the Archimedean case $\Gamma\backslash G/U$ is a compact manifold but unfortunately $\det(\Delta(R(\chi)))$ is no longer a trigonometric polynomial in χ. One can show that it is real analytic in χ but we will not pursue this here.

3. Torsion points on varieties and linearization

We turn to the proof of Proposition 1.6. The approach below is simpler than our original and was suggested by Paul Cohen.

LEMMA 3.1: *Let $\alpha_1, \dots, \alpha_R$ be nonzero complex numbers; then there is a number $M = M(\alpha_1, \dots, \alpha_R)$ such that any solution in roots of unity $\varepsilon_1, \dots, \varepsilon_R$ of*

$$\sum_{j=1}^{R} \alpha_j \, \varepsilon_j = 0 \tag{3.1}$$

satisfies

$$(\varepsilon_j \, \varepsilon_k^{-1})^{\nu} = 1 \tag{3.1$'$}$$

for some $j \neq k$ and some $1 \leq \nu \leq M$.

Proof: We begin by assuming that $\alpha_1, \dots, \alpha_R \in \mathbf{Q}$, in which case we show M may be chosen to be $(R+1)^{R+1}$. Let $\varepsilon_1, \dots, \varepsilon_R$ be a solution of (3.1) and assume the conclusion of (3.1)$'$ fails. Let n be the l.c.m. of the orders of $\varepsilon_1, \dots, \varepsilon_R$. If the factorization of n is $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ then we may write

$$\varepsilon_j = (\zeta_{p_1^{e_1}})^{\nu_j^{(1)}} \, (\zeta_{p_2^{e_2}})^{\nu^{(2)}} \, \dots (\zeta_{p_k^{e_k}})^{\nu_j^{(k)}} \, , \tag{3.2}$$

where $\zeta_m = e(1/m) = \exp(2\pi i/m)$. Now if some p_j, say p_1, is larger than $R+1$, then we proceed as follows:

There is some ε_j for which $(\nu_j^{(1)}, p_1) = 1$. We may write (3.1) as

$$\sum_{j=1}^{R} (\alpha_j \eta_j \, \zeta_{p_1^{e_1 - 1}}^{\lambda_j}) \, \zeta_{p_1^{e_1}}^{\nu_j} = 0 \, , \tag{3.3}$$

where $\eta_j \zeta_{p_1^{e_1 - 1}}^{\lambda_j} \, \zeta_{p_1^{e_1}}^{\nu_j} = \varepsilon_j$, $0 \leq \nu_j \leq p_1 - 1$, η_j is a $p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}$ root of 1 and $(\nu_1, p_1) = 1$. Thus (3.3) gives an equation for $\zeta_{p_1^{e_1}}$ over the field $K =$

$\mathbf{Q}\,(\zeta_{p_1^{e_1-1}}, \zeta_{p_2^{e_2}}, \dots, \zeta_{p_k^{e_k}})$ of degree at most $p_1 - 1$. The extension $K(\zeta_{p_1^{e_1}})$ over K has degree p_1 or $p_1 - 1$ and, since $R < p_1 - 1$, (3.3) is impossible (since then (3.3) is not the cyclotomic equation) unless the equation trivializes. In this case one can proceed inductively since the power e_1 has been reduced and the side conditions of the Lemma persist.

We may therefore assume that $p_j \leq R + 1$ for each j. We write (3.1) as

$$\sum_{j=1}^{R} \alpha_j\, e\left(\frac{m_1^{(j)}}{p_1^{e_1}} + \frac{m_2^{(j)}}{p_2^{e_2}} + \ldots + \frac{m_k^{(j)}}{p_k^{e_k}}\right) = 0\,, \tag{3.4}$$

where now

$$\varepsilon_j = e\left(\frac{m_1^{(j)}}{p_1^{e_1}} + \ldots + \frac{m_k^{(j)}}{p_k^{e_k}}\right).$$

For $r = (r_1, r_2, \dots, r_k)$ with $p_j \not| r_j$ we obtain from (3.2) and the Galois action of $\mathbf{Q}\,(\zeta_n)/\mathbf{Q}$

$$\sum_{j=1}^{R} \alpha_j\, e\left(\frac{r_1\, m_1^{(j)}}{p_1^{e_1}} + \ldots + \frac{r_k\, m_k^{(j)}}{p_k^{e_k}}\right) = 0\,.$$

Multiplying this equation by $\overline{e\left(\frac{r_1\, m_1^{(1)}}{p_1^{e_1}} + \ldots + \frac{r_k\, m_k^{(1)}}{p_k^{e_k}}\right)}$ and summing over r_j mod $p_j^{e_j}$, $p_j \not| r_j$, we get

(3.5)

$$0 = \alpha_1\, \varphi(n) \pm \sum_{j=2}^{R} \alpha_j \sum_{r_j \bmod p_j^{f_j}} e\left(\frac{r_1\,(m_1^{(j)} - m_1^{(1)})}{p_1^{e_1}} + \ldots + \frac{r_k\,(m_k^{(j)} - m_k^{(1)})}{p_k^{e_k}}\right),$$

where $f_j = e_j$ or $e_j - 1$. Let $m^{(j)} = \left[m_1^{(j)} p_2^{(e_2)} \cdots p_k^{e_k}\right] + \cdots + \left[p_1^{e_1} \cdots p_{k-1}^{e_{k-1}} m_k^{(j)}\right]$ so that $\varepsilon_j = e(m^{(j)}/n)$. If for a fixed j in the above type of sum $m_\nu^{(j)} - m_\nu^{(1)}$ are all divisible by $p_\nu^{f_\nu}$, then $m^{(j)} \equiv m^{(1)}$ mod $\left(\frac{n}{p_1 p_2 \cdots p_k}\right)$ and hence

$$(\varepsilon_1 \varepsilon_j^{-1})^{p_1 p_2 \cdots p_k} = 1\,.$$

This is contrary to our assumption since $p_1 p_2 \dots p_k < (R+1)^{R+1}$. Hence for each j at least one of $m_\nu^{(j)} - m_\nu^{(1)}$ is not divisible by $p_\nu^{f_\nu}$. It follows that all the series in (3.5) vanish and hence $\alpha_1 = 0$. This completes the proof for the case of most interest to us viz. $\alpha_j \in \mathbf{Q}$. In general one argues in a similar case with $\mathbf{Q}$ replaced by the finitely generated field $K = \mathbf{Q}(\alpha_1, \dots, \alpha_r)$ and the Galois group of $\mathbf{Q}\,(\zeta_n)$ replaced by that of $K(\zeta_n)$ over K. We leave the details to the reader.

We proceed now with the proof of Proposition 1.6. The proof is by induction on the dimension of the torus T. We are allowing here a torus to be of the form $T = (\mathbf{R}/\mathbf{Z})^k \times A$, where A is a finite Abelian group. In such a case T is of dimension k and the algebraic sets are algebraic sets at each connected component of T. When $\dim T = 1$ the result is clear since in this case a connected component of T is either all of the set W, or W meets the component in a finite set. In the general case, if $\dim T = r$ and W is given by equations

$$p_1(t) = p_2(t) = \ldots = p_m(t) = 0$$

on a connected component of T, then either these equations are all redundant and W contains this connected component which is then one of the π's, or say $p_1(t)$ is not trivially true. Say

$$p_1(t) = \sum_{\lambda \in F} a_\lambda \, \lambda(t) \, , \tag{3.6}$$

where F is a finite subset of the dual group T^*. The sets

$$\Pi_{\lambda,\mu,\nu} = \{t \mid (\lambda \, \mu^{-1})^\nu(t) = 1\} \tag{3.7}$$

for $\lambda \neq \mu$, $\lambda, \mu \in F$, and $1 \leq \nu \leq M(a_\lambda)$, where M is the constant from Lemma 3.1, are all finite unions of rational planes of dimension $r-1$. Hence since the restriction of an algebraic set to a plane is algebraic, we conclude by induction that the torsion points of $T \cap W$ contained in the union of the finite set of $\Pi_{\lambda,\mu,\nu}$'s are all on a finite number of rational planes in W. On the other hand Lemma 3.1 asserts that there are no torsion points of $T \cap W$ outside of this union. This completes the proof of Proposition 1.6.

We note that the above proof is effective and produces the planes inductively. An example of this procedure is carried out in the next Section.

4. Proof of the Theorem

We now complete the proof of Theorem 1.2 part (i). Part (ii) is proved similarly. Fix a positive integer q and, as in the introduction, let R_N: $H(\mathbf{Z}) \to H(\mathbf{Z}/N\mathbf{Z})$ denote reduction mod N. From our setup $H_N := R_N(H(\mathbf{Z}))$ is the Galois group of the covering $\tilde{K}/\Gamma(N)$ over $\tilde{K}/\Gamma(1)$. Hence we may decompose $C^q(\tilde{K}/\Gamma(N))$ into invariant subspaces according to the irreducible representations of H_N. Since the action of H_N on fibers of the covering is simple and transitive, it follows from the decomposition of the regular representation that

$$\beta^q(\tilde{K}/\Gamma(N)) = \sum_{R\in\hat{H}_N} d(R)\,\beta^q(\tilde{K},R)\,, \tag{4.1}$$

where $d(R) = \dim R$. Hence

$$^{\nu}\beta^q\,(\tilde{K}/\Gamma(N)) = \nu \sum_{\substack{R\in\hat{H}_N\\ \dim R=\nu}} \beta^q(\tilde{K},R)\,. \tag{4.2}$$

These R's are irreducible ν–dimensional and of course finite representations of Γ—this explains the assumption made in Section 2. To use the formula for $\beta^q(\tilde{K},R(\chi))$ developed in Proposition 2.2 we need to know which χ's come up in (4.2).

Assume H is unipotent, then $H(\mathbf{Z})$ is a finitely generated nilpotent (discrete) group. In this case, the representation variety $V(\Delta,\nu)$ in (2.3) takes an even simpler form (see Lubotzky–Magid [L–M])

$$V(\Delta,\nu) = \bigcup_{j=1}^{L}\ \bigcup_{\chi\in T(H(\mathbf{Z}))} R_j\otimes\chi\,, \tag{4.3}$$

where R_j is an irreducible (finite) representation of $H(\mathbf{Z})$ of dimension ν. Moreover, the representations in different classes $R_j\otimes T(H(\mathbf{Z}))$ and $R_k\otimes T(H(\mathbf{Z}))$ for $k\neq j$ are inequivalent. It is possible that $R_j\otimes\chi'\simeq R_j\otimes\chi$ for some $\chi\neq\chi'$ and in this case $\{\chi\colon R_j\otimes\chi\simeq R_j\}$ is a finite subgroup of $T(H(\mathbf{Z}))$. For simplicity we assume this group is $\{1\}$—the modifications needed to deal with the general case dividing by this finite group are straightforward.

Let $B(N,j)$ denote the set of all characters $\chi\in T(H(\mathbf{Z}))$ such that $R_j\otimes\chi$ factors to H_N, i.e., such that the kernel of $R_j\otimes\chi$ contains $H(N)$. By equation (4.2) and the above description of the representation theory of $H(\mathbf{Z})$, we have

$$^{\nu}\beta^q(\tilde{K}/\Gamma(N)) = \nu\sum_{j=1}^{L}\ \sum_{\chi\in B(N,j)} \beta^q(\tilde{K},R_j\otimes\chi).$$

For all j, choose rational planes $\pi_1,\dots,\pi_{l_j}$ and integers $m_1,\dots,m_{l_j}$ as in Proposition 2.2. Then

$$^{\nu}\beta^q(\tilde{K}/\Gamma(N)) = \nu\sum_{j=1}^{L}\sum_{\mu=1}^{l_j} m_\mu|B(N,j)\cap\pi_\mu|,$$

where $|S|$ denotes the cardinality of a set S.

It therefore suffices to show, for all j and μ, that $|B(N,j)\cap\pi_\mu|$ is polynomial periodic in N. In the case that $H(\mathbf{Z})=\mathbf{Z}^r$ as in (C.ii) of the introduction, this polynomial periodicity is easily seen. For the general case, we proceed as follows. Fix j and μ; for all integers $N>0$, define $S_N:=B(N,j)\cap\pi_\mu$. We wish to show that $|S_N|$ is polynomial periodic in N.

Let $\mathcal{N}$ be the collection of integers $N>0$ such that, for some $\chi\in T(H(\mathbf{Z}))$, we have $\ker(R_j\otimes\chi)\supseteq H(N)$. Let $N_1:=\min\mathcal{N}$. By [Ad, Lemma 5.6] (which depends only on strong approximation for H at the infinite place, and not on any of the results in this paper), we find, for all integers $N>0$, that: $N_1\,|\,N$ iff $N\in\mathcal{N}$. In particular, for all integers $N>0$ such that $N_1\not|\,N$, we have $S_N=\emptyset$, so $|S_N|=0$. Therefore, it suffices to show that $|S_{N_1N}|$ is polynomial periodic in N.

Choose $\chi_1\in T(H(\mathbf{Z}))$ such that $\ker(R_j\otimes\chi_1)\supseteq H(N_1)$. Then, for all integers $N>0$, we have $S_{N_1N}=\chi_1\{\chi\in\chi_1^{-1}\pi_\mu\,|\,\ker(\chi)\supseteq H(N_1N)\}$. Fix any $\chi_0\in\chi_1^{-1}\pi_\mu$ and define $\pi:=\chi_0^{-1}\chi_1^{-1}\pi_\mu$. For all integers $N>0$, define $S'_N:=\{\chi\in\pi\,|\,\ker(\chi_0\chi)\supseteq H(N)\}$. Then, for all integers $N>0$, we have $S_{N_1N}=\chi_0\chi_1S'_{N_1N}$, so $|S_{N_1N}|=|S'_{N_1N}|$. By Theorem 10.1, we see that $|S'_N|$ is polynomial periodic in N, so $|S'_{N_1N}|$ is as well, concluding the proof.

This completes the proof if H is unipotent. If H is semisimple then the above analysis gives the result (but without any of the analysis of torsion points in tori) because of the following result, a proof of which is given by Z. Rudnick in the Appendix. (Also see [Ad, Theorem 5.12].)

PROPOSITION 4.1: *Let H be a semisimple group over $\mathbf{Q}_p$. Let $\mathbf{Z}_p$ denote the p-adic integers. There are only finitely many irreducible representations of the compact group $H(\mathbf{Z}_p)$ in any given dimension.*

With this one finds that there are only a finite number of R's (independent of N but depending on ν) that come into play in (4.2). As a result the Theorem is easy to establish.

The Corollaries for unbranched covers follow directly from the Theorem since H in these cases is Abelian and hence we need only take $\nu=1$ to get the complete picture. For computational purposes say with links in S^3 we relate the varieties $V_1,V_2,\ldots$ of Section 2 to Alexander ideals [F–2]. In fact let L be a μ–component link; we can think of $T(\Gamma)=(S^1)^\mu$, where $\Gamma=\pi_1(S^3\setminus L)$, as sitting in $(\mathbf{C}^*)^\mu$.

The following Proposition follows easily from Fox [F–2], see also [M–M] and Libgober [Lr].

PROPOSITION 4.2: *Let $W_1 \supset W_2 \supset W_3 \cdots$ be the zero sets in $(\mathbf{C}^*)^\mu$ of the elementary Alexander ideals $E_1, E_2, \dots$ of the link L. Then*

$$W_k \cap T = V_k \quad \text{for } k \neq \mu$$

and $(W_\mu \cap T) \cup \{1\} = V_\mu$.

Here the V_k's are the sets defined in (2.12) for β^1 and $H(\mathbf{Z}) = \mathbf{Z}^\mu = H_1(\Gamma, \mathbf{Z})$. The point is that the Alexander ideals are easy to compute. Thus for the link L in Figure 1.5 one finds (see [F–T])

$$\begin{aligned} E_1 &: \quad (t_1 - 1, t_2 - 1)\,(1 - t_1 + t_1^2)\,(1 - 2\,t_1 - t_1^2\,t_2\,(2 - t_1)) \\ E_2 &: \quad (1 - t_1 + t_1^2, (1 + t_1)\,(1 + t_2)) \\ E_3 &: \quad (1) \end{aligned}$$

Hence using linear torus variables $t_j = e(\theta_j)$ and Proposition 4.2 we have

$$\begin{aligned} V_1 &= \{(0,0)\} \cup \{1 - e(\theta_1) + e(2\,\theta_1) = 0\} \\ &\qquad\qquad \cup \{1 - 2\,e(\theta_1) - e(2\,\theta_1)\,e(\theta_2)\,(2 - e(\theta_1)) = 0\}, \\ V_2 &= \left\{(0,0), \left(\frac{1}{6}, \frac{1}{2}\right), \left(\frac{5}{6}, \frac{1}{2}\right)\right\}, \\ V_3 &= \emptyset. \end{aligned}$$

Thus V_3 and V_2 are already linear. We apply the method of Section 3 to linearize V_1 and find two 1–dimensional rational planes viz.

$$\pi_1 = \{\theta_1 = 1/6\}, \qquad \pi_2 = \{\theta_1 = 5/6\}$$

and three zero-dimensional planes

$$\pi_3 = \{(0, 1/2)\}, \qquad \pi_4 = \{(1/2, 0)\}, \qquad \pi_5 = \{(0,0)\}\,.$$

Using this, one obtains (1.6) after a little calculation.

Concerning Corollary 1.4 for branched coverings, one uses instead of the Alexander polynomial of L the reduced Alexander polynomial as described in Mayberry and Murasugi [M–M]. Other than that the techniques apply directly and yield Corollary 1.4. The rest of the paper (Sections 5 to 9) is concerned with establishing the polynomial periodicity of the sequence $|S'_N|$ described in the proof of Theorem 1.2.

5. A division algorithm for polynomial periodic functions

Let $\mathbf{N} := \{1,2,3,\ldots\}$. For all $s \in \mathbf{N}$, define $\mathbf{N}_s := \{1,\ldots,s\}$. For all $s,t \in \mathbf{Z}$ satisfying $s \leq t$, we define $\mathbf{Z}_s^t := \{s,\ldots,t\}$. A function $a\colon \mathbf{N} \to \mathbf{Z}$ is said to be **positive** if $a(N) > 0$, for all $N \in \mathbf{N}$.

Definition 5.1: Let $a\colon \mathbf{N} \to \mathbf{Z}$ be any function, let $m \in \mathbf{N}$ and $s \in \mathbf{Z}$. We say that a is a **polynomial along $m\mathbf{Z} + s$** if there exists a polynomial function $u\colon \mathbf{R} \to \mathbf{R}$ such that u and a agree on $(m\mathbf{Z}+s) \cap \mathbf{N}$. If, in addition, the function u satisfies $u(0) = 0$, then we say that a is a **0-vanishing polynomial along $m\mathbf{Z} + s$**.

Definition 5.2: Let $a\colon \mathbf{N} \to \mathbf{Z}$. We define $\mathrm{MOD}(a)$ to be the set of all $m \in \mathbf{N}$ such that, for all $s \in \mathbf{N}_m$, the function a is a polynomial along $m\mathbf{Z}+s$. We define $\mathrm{MOD}_0(a)$ to be the set of all $m \in \mathbf{N}$ such that, for all $s \in \mathbf{N}_m$, the function a is a 0-vanishing polynomial along $m\mathbf{Z} + s$.

Definition 5.3: Let $a\colon \mathbf{N} \to \mathbf{Z}$ be any function. We say that a is **polynomial periodic**, or **p.p.**, if $\mathrm{MOD}(a) \neq \emptyset$. We say that a is **0-vanishing polynomial periodic**, or **0-v.p.p.**, if $\mathrm{MOD}_0(a) \neq \emptyset$. ∎

If $a\colon \mathbf{N} \to \mathbf{Z}$ is 0-v.p.p., then $\mathrm{MOD}(a) = \mathrm{MOD}_0(a)$.

Definition 5.4: Let $a\colon \mathbf{N} \to \mathbf{Z}$ be polynomial periodic and not identically zero. Fix any $m \in \mathrm{MOD}(a)$ and choose, for each $s \in \mathbf{N}_m$, the polynomial function $u_s\colon \mathbf{R} \to \mathbf{R}$ such that $a = u_s$ on $(m\mathbf{Z} + s) \cap \mathbf{N}$. Let S denote the collection of $s \in \mathbf{N}_m$ such that u_s is not identically zero. For each $s \in S$, let $u'_s\colon \mathbf{R} \to \mathbf{R}$ be defined by $u'_s(t) := u_s(mt + s)$. For $s \in S$, let $d_s := \deg(u'_s) = \deg(u_s)$ and let c_s denote the leading coefficient of u'_s. We define the **degree** of a to be $\deg(a) := \max\{d_s \,|\, s \in S\}$. Let $R := \{s \in S \,|\, d_s = \deg(a)\}$. We define the **full mth set of leading coefficients** and the **mth set of significant leading coefficients** to be, respectively,

$$\mathrm{FLC}_m(a) := \{c_s \,|\, s \in S\}, \qquad \mathrm{SLC}_m(a) := \{c_r \,|\, r \in R\}.$$

We will say that a is **nonvanishing on arithmetic sequences** if $S = \mathbf{N}_m$.

LEMMA 5.5: *Let $a\colon \mathbf{N} \to \mathbf{Z}$ be p.p. Then there exists $m_0 \in \mathbf{N}$ such that, for all $n \in \mathbf{N}$, we have: $m_0 n \in MOD(a)$ and $FLC_{m_0 n}(a) \subseteq \mathbf{Z}$.*

Proof: Let $d := \deg(a)$. Choose $m \in \mathrm{MOD}(a)$. Choose, for each $s \in \mathbf{N}_m$, the polynomial function $u_s\colon \mathbf{R} \to \mathbf{R}$ such that $a = u_s$ on $(m\mathbf{Z} + s) \cap \mathbf{N}$. For each $s \in S$, let $u'_s\colon \mathbf{R} \to \mathbf{R}$ be defined by $u'_s(t) := u_s(mt + s)$.

For each $i \in \mathbf{Z}_0^d$, let S_i denote the set of $s \in \mathbf{N}_m$ such that $\deg(u_s) = i$ and let C_i denote the set of leading coefficients of the polynomials in $\{u'_s \mid s \in S_i\}$.

Then $C_0 \subseteq \mathbf{Z}$ since $a(\mathbf{N}) \subseteq \mathbf{Z}$. By [Jac, Proposition 7.26, p. 444], $C_1 \cup \cdots \cup C_d \in \mathbf{Q}$. Choose an integer n_0 such that $n_0(C_1 \cup \cdots \cup C_d) \subseteq \mathbf{Z}$.

For all $n \in \mathbf{N}$,

$$\mathrm{FLC}_{mn}(a) = C_0 \cup nC_1 \cup n^2 C_2 \cup \cdots \cup n^d C_d,$$

so we conclude the proof by setting $m_0 := mn_0$. ∎

Definition 5.6: If $S, T \subseteq \mathbf{Z}$, and if $0 \notin S$, then we use the notation $S|T$ to mean: $s|t$, for all $s \in S$, $t \in T$, i.e., every element of S divides evenly into every element of T. We make the convention that $S|\emptyset$, for all $S \subseteq \mathbf{Z}\backslash\{0\}$.

LEMMA 5.7: *Let $a, b\colon \mathbf{N} \to \mathbf{Z}$ be p.p. and assume that b is not identically zero. Assume that* $\deg(a) > \deg(b)$. *Then there exists $m \in MOD(a) \cap MOD(b)$ such that*

$$FLC_m(a) \cup FLC_m(b) \subseteq \mathbf{Z} \qquad \textit{and} \qquad FLC_m(b) | SLC_m(a).$$

Proof: By Lemma 5.5, choose $m_0 \in \mathbf{N}$ such that, for all $n \in \mathbf{N}$, we have:

$$m_0 n \in \mathrm{MOD}(a) \cap \mathrm{MOD}(b) \qquad \text{and} \qquad \mathrm{FLC}_{m_0 n}(a) \cup \mathrm{FLC}_{m_0 n}(b) \subseteq \mathbf{Z}.$$

Let $n_0 := \prod \mathrm{FLC}_{m_0}(b)$, i.e., let n_0 denote the product of all the elements of the full m_0th set of leading coefficients of b.

Let $c := \deg(a)$ and $d := \deg(b)$, so, by assumption, $d < c$. Now, for all $n \in \mathbf{N}$, we have

$$\mathrm{FLC}_{m_0 n}(b) | n^d \mathrm{FLC}_{m_0}(b) \qquad \text{and} \qquad \mathrm{SLC}_{m_0 n}(a) = n^c \mathrm{SLC}_{m_0}(a),$$

so we conclude the proof by defining $m := m_0 n_0$. ∎

LEMMA 5.8: *Let $a, b\colon \mathbf{N} \to \mathbf{Z}$ be p.p. and assume that b is nonvanishing on arithmetic sequences. Let $m \in MOD(a) \cap MOD(b)$ and assume that*

$$FLC_m(a) \cup FLC_m(b) \subseteq \mathbf{Z} \qquad \text{and} \qquad FLC_m(b) | SLC_m(a).$$

Then there exist p.p. functions $q_0, a_0\colon \mathbf{N} \to \mathbf{Z}$ such that $\deg(a_0) < \deg(a)$ and such that $a = bq_0 + a_0$.

Proof: Fix $s \in \mathbf{N}_m$. Choose polynomial functions $u_s, v_s\colon \mathbf{R} \to \mathbf{R}$ such that $u_s = a$ and $v_s = b$ on $(m\mathbf{Z} + s) \cap \mathbf{N}$. Define $u'_s, v'_s\colon \mathbf{R} \to \mathbf{R}$ by $u'_s(t) := u_s(mt + s)$ and $v'_s(t) := v_s(mt + s)$.

Let $R := \{s \in \mathbf{N}_m \mid \deg(u_s) = \deg(a)\}$. For each $s \in R$, since the leading coefficient of v'_s divides the leading coefficient of u'_s, we may choose polynomial functions $w_s, u^0_s\colon \mathbf{R} \to \mathbf{R}$ such that

$$\deg(u^0_s) < \deg(u_s) \qquad \text{and} \qquad u'_s = v'_s w_s + u^0_s$$

and such that the coefficients of w_s and of u^0_s are all integers. For all $s \in \mathbf{N}_m \backslash R$, define $w_s := 0$ and $u^0_s := u'_s$.

Define $q_0, a_0\colon \mathbf{N} \to \mathbf{Z}$ by the rule: for all $s \in \mathbf{N}_m$, for all $N \in \mathbf{N} \cup \{0\}$,

$$q_0(mN + s) = w_s(N) \qquad \text{and} \qquad a_0(mN + s) = u^0_s(N). \qquad ∎$$

We can now give an analogue for the division algorithm for polynomial periodic functions. Notice that the degree of the remainder may equal the degree of the divisor, so it is not possible to obtain an Euclidean algorithm in this case.

PROPOSITION 5.9: *Let $a, b\colon \mathbf{N} \to \mathbf{Z}$ be p.p. and assume that b is nonvanishing on arithmetic sequences. Then there exist p.p. functions $q, r\colon \mathbf{N} \to \mathbf{Z}$ such that $\deg(r) \leq \deg(b)$ and such that $a = bq + r$.*

Proof: The proof is by induction on $\deg(a)$. If $\deg(a) \leq \deg(b)$, then we set $q := 0$ and $r := a$; we therefore assume $\deg(a) > \deg(b)$. Choose m as in Lemma 5.7. Choose q_0 and a_0 as in Lemma 5.8. By induction, there exist p.p. functions $q_1, r_1\colon \mathbf{N} \to \mathbf{Z}$ such that $\deg(r_1) \leq \deg(b)$ and such that $a_0 = bq_1 + r_1$. Let $q := q_0 + q_1$ and let $r := r_1$. ∎

In the case where both divisor and dividend are 0-v.p.p, we can conclude that the remainder is as well:

PROPOSITION 5.10: *Let $a, b\colon \mathbf{N} \to \mathbf{Z}$ be 0-v.p.p., let $q, r\colon \mathbf{N} \to \mathbf{Z}$ be p.p. Assume that $a = bq + r$. Then r is 0-v.p.p.*

Proof: By Lemma 5.5, choose $m \in \mathrm{MOD}(a) \cap \mathrm{MOD}(b) \cap \mathrm{MOD}(q) \cap \mathrm{MOD}(r)$. For each $s \in \mathbf{N}_m$, choose polynomial functions $u_s, v_s, y_s, z_s\colon \mathbf{R} \to \mathbf{R}$ such that, on $(m\mathbf{Z} + s) \cap \mathbf{N}$, we have $u_s = a$, $v_s = b$, $y_s = q$ and $z_s = r$.

Fix $s \in \mathbf{N}_m$; we wish to show that $z_s(0) = 0$. However, we know that $u_s(0) = v_s(0) = 0$ and that $u_s = v_s y_s + z_s$, so the result is immediate. ∎

6. Further generalities on polynomial periodic functions

We will say that a function $\mathbf{N} \to \mathbf{Z}$ is **linear periodic**, or **l.p.** if it is polynomial periodic of degree ≤ 1, or if it is identically zero. A function $\mathbf{N} \to \mathbf{Z}$ is **homogeneous linear periodic** or **h.l.p.** if it is 0-v.p.p. and linear periodic.

If $t \in \mathbf{N}$ and $(x_1, \ldots, x_t) \in \mathbf{Z}^t \backslash \{(0, \ldots, 0)\}$ then we define

$$\gcd(x_1, \ldots, x_t) := \max\{u \in \mathbf{N} \mid x_1, \ldots, x_t \in u\mathbf{Z}\}.$$

LEMMA 6.1: *Assume $a, b\colon \mathbf{N} \to \mathbf{Z}$ are h.l.p. Assume further that $a(N) \neq 0$, for all $N \in \mathbf{N}$. Then*

$$N \mapsto \gcd(a(N), b(N))\colon \mathbf{N} \to \mathbf{Z}$$

is positive and h.l.p.

Proof: By definition of gcd, for all $N \in \mathbf{N}$, we have $\gcd(a(N), b(N)) > 0$.

Let $Y \subseteq \mathbf{N}$ be an arithmetic sequence on which there exist $s, t, v \in \mathbf{Z}\backslash\{0\}$ and $u \in \mathbf{Z}$ such that, for all $N \in Y$, we have

$$a(N) = sN/t, \qquad b(N) = uN/v.$$

We wish to show that there exist $w \in \mathbf{Z}$ and $x \in \mathbf{Z}\backslash\{0\}$ such that, for all $N \in Y$, we have

$$\gcd(a(N), b(N)) = wN/x.$$

Now, for all $N \in Y$, we know that

$$tv\gcd(a(N), b(N)) = \gcd(tva(N), tvb(N)) = \gcd(svN, tuN) = [\gcd(sv, tu)]N.$$

So let $w := \gcd(sv, tu)$ and $x := tv$. ∎

COROLLARY 6.2: *Assume that $b_1, \ldots, b_t$: $\mathbf{N} \to \mathbf{Z}$ are h.l.p. functions and that $b_1(N) \neq 0$, for all $N \in \mathbf{N}$. Then*

$$N \mapsto \gcd(b_1(N), \ldots, b_t(N)) \colon \mathbf{N} \to \mathbf{Z}$$

is positive and h.l.p.

LEMMA 6.3: *Suppose that a: $\mathbf{N} \to \mathbf{Z}$ is h.l.p. Then*

$$N \mapsto \min\{u \in \mathbf{N} \mid ua(N) \in N\mathbf{Z}\} \colon \mathbf{N} \to \mathbf{Z}$$

is periodic.

Proof: Since, for all $N \in \mathbf{N}$ and all $a \in \mathbf{Z}$, we have

$$N|ua \iff \frac{N}{\gcd(N,a)}\Big| u\frac{a}{\gcd(N,a)} \iff \frac{N}{\gcd(N,a)}\Big| u,$$

it follows that

$$\min\{u \in \mathbf{N} \mid ua(N) \in N\mathbf{Z}\} = \frac{N}{\gcd(N, a(N))}.$$

By Lemma 6.1, the gcd of a positive h.l.p. function and an h.l.p. function is positive h.l.p.; it follows the the denominator above is positive h.l.p. Finally, we note that the quotient of an h.l.p. function by a positive h.l.p. function is periodic. ∎

The next lemma has a proof very similar to the last; we omit it.

LEMMA 6.4: *If a: $\mathbf{N} \to \mathbf{Z}$ is periodic, then*

$$N \mapsto \min\{u \in \mathbf{N} \mid ua(N) \in N\mathbf{Z}\} \colon \mathbf{N} \to \mathbf{Z}$$

is h.l.p.

LEMMA 6.5: *Suppose that $a, b_1, \ldots, b_t$: $\mathbf{N} \to \mathbf{Z}$ are all h.l.p. and that b_t is positive. For all $N \in \mathbf{N}$, let*

$$a'(N) := \min\{N \in \mathbf{N} \mid ua(N) \in b_1(N)\mathbf{Z} + \cdots + b_t(N)\mathbf{Z}\}.$$

Then $a' : \mathbf{N} \to \mathbf{Z}$ is periodic and there exist periodic functions $b'_1, \ldots, b'_t$: $\mathbf{N} \to \mathbf{Z}$ such that, for all $N \in \mathbf{N}$, we have

$$a(N)a'(N) = b_1(N)b'_1(N) + \cdots + b_t(N)b'_t(N).$$

Proof: For all $N \in \mathbf{N}$, define

$$g(N) := \gcd(b_1(N), \ldots, b_t(N)), \qquad c(N) := N/g(N).$$

Then, by Corollary 6.2, g: $\mathbf{N} \to \mathbf{Z}$ is positive, h.l.p. and so c: $\mathbf{N} \to \mathbf{Z}$ is periodic. For all $u, N \in \mathbf{N}$, we have

$$\begin{aligned} ua(N) \in b_1(N)\mathbf{Z} + \cdots + b_t(N)\mathbf{Z} \quad &\iff \quad ua(N) \in \frac{N}{c(N)}\mathbf{Z} \\ &\iff \quad ua(N)c(N) \in N\mathbf{Z}. \end{aligned}$$

Since $N \mapsto a(N)c(N)$: $\mathbf{N} \to \mathbf{Z}$ is h.l.p., it follows from Lemma 6.3 that a': $\mathbf{N} \to \mathbf{Z}$ is periodic.

By definition of a', for all $N \in \mathbf{N}$, we have $g(N) | a(N)a'(N)$.

Let $a'', b_1'', \ldots, b_t''$: $\mathbf{N} \to \mathbf{Z}$ be defined by

$$a'' := aa'/g, \quad b_1'' := b_1/g, \ldots, b_t'' := b_t/g.$$

Then $a'', b_1'', \ldots, b_t''$: $\mathbf{N} \to \mathbf{Z}$ are periodic.

For all $N \in \mathbf{N}$, there exist $x_1, \ldots, x_t \in \mathbf{Z}$ such that

$$(*) \qquad a''(N) = b_1''(N)x_1 + \cdots + b_t''(N)x_t.$$

Since the coefficients of $(*)$ are periodic in N, we may solve $(*)$ for finitely many values of N, then repeat these solutions periodically in N. So there exist $b_1', \ldots, b_t'$: $\mathbf{N} \to \mathbf{Z}$ periodic such that, for all $N \in \mathbf{N}$,

$$a''(N) = b_1''(N)b_1'(N) + \cdots + b_t''(N)b_t'(N).$$

Multiplying this equation by $g(N)$, we obtain the desired conclusion. ∎

LEMMA 6.6: *Let $a, b_1, \ldots, b_t$: $\mathbf{N} \to \mathbf{Z}$ be h.l.p., and let c: $\mathbf{N} \to \mathbf{Z}$ be periodic. Assume, for all $N \in \mathbf{N}$, that $c(N) \neq 0$. For all $N \in \mathbf{N}$, define*

$$a'(N) := \min\{u \in \mathbf{N} \,|\, ua(N) \in b_1(N)\mathbf{Z} + \cdots + b_t(N)\mathbf{Z} + c(N)\mathbf{Z}\}.$$

Then a': $\mathbf{N} \to \mathbf{Z}$ is periodic and there exist periodic functions $b_1', \ldots, b_t'$: $\mathbf{N} \to \mathbf{Z}$ and an h.l.p. function c': $\mathbf{N} \to \mathbf{Z}$ such that, for all $N \in \mathbf{N}$,

$$a(N)a'(N) = b_1(N)b_1'(N) + \cdots + b_t(N)b_t'(N) + c(N)c'(N).$$

Proof: By Proposition 5.9, there exist periodic functions $a'', b_1'', \ldots, b_t'' \colon \mathbf{N} \to \mathbf{Z}$ such that, for all $N \in \mathbf{N}$, $a(N) \equiv a''(N) \bmod c(N)$ and

$$b_1(N) \equiv b_1''(N) \bmod c(N) \qquad , \qquad \ldots \qquad , \qquad b_t(N) \equiv b_t''(N) \bmod c(N).$$

For all $N \in \mathbf{N}$,

$$a'(N) = \min\{u \in \mathbf{N} \mid ua''(N) \in b_1''(N)\mathbf{Z} + \cdots + b_t''(N)\mathbf{Z} + c(N)\mathbf{Z}\}.$$

Since $a'', b_1'', \ldots, b_t'', c \colon \mathbf{N} \to \mathbf{Z}$ are periodic, it follows that $a' \colon \mathbf{N} \to \mathbf{Z}$ is as well.

For all $N \in \mathbf{N}$, there exist $x_1, \ldots, x_t \in \mathbf{Z}$ such that

$$a''(N)a'(N) \in b_1''(N)x_1 + \cdots + b_t''(N)x_t + c(N)\mathbf{Z}.$$

Since $a'', a', b_1'', \ldots, b_t'', c \colon \mathbf{N} \to \mathbf{Z}$ are periodic, we may choose periodic $b_1', \ldots, b_t' \colon \mathbf{N} \to \mathbf{Z}$ such that, for all $N \in \mathbf{N}$, we have

$$a''(N)a'(N) \in b_1''(N)b_1'(N) + \cdots + b_t''(N)b_t'(N) + c(N)\mathbf{Z}.$$

Then, for all $N \in \mathbf{N}$, we have

$$a(N)a'(N) \in b_1(N)b_1'(N) + \cdots + b_t(N)b_t'(N) + c(N)\mathbf{Z}.$$

Define $c' \colon \mathbf{N} \to \mathbf{Z}$ by

$$c' := \frac{aa' - b_1b_1' - \cdots - b_tb_t'}{c}.$$

Then c' is the quotient of an h.l.p. function by a nonvanishing periodic function and is therefore h.l.p. ∎

7. Generators for the integer points

Fix a positve integer n and a $\mathbf{Q}$-subgroup $H \leq \mathrm{SL}_n$.

We assume that H is a subgroup of the upper triangular unipotent matrices. (In §11, we will show that it is only necessary to assume that H is unipotent; the element which conjugates such a group into the upper triangular unipotents may be chosen to be a $\mathbf{Z}$-point.) We assume that H is not the trivial (one-element) group.

For each $i, j \in \mathbf{N}_n$, let $p_{ij} \colon \mathrm{SL}_n \to \mathbf{A}^1$ be the map which associates to each matrix in SL_n its (i, j)-entry, which lies in affine 1-space.

Define $m := n(n-1)/2$ and let $\pi_1, \dots, \pi_m$ denote, respectively, the maps

$$\begin{aligned}
&p_{12}|H,\, p_{23}|H\,, \dots, p_{n-2,n-1}|H,\, p_{n-1,n}|H,\\
&p_{13}|H,\, p_{24}|H\,, \dots, p_{n-2,n}|H,\\
&\quad\dots\\
&p_{1,n-1}|H\,,\, p_{2n}|H\\
&p_{1n}|H.
\end{aligned}$$

Let $F_1 := H$. If $\pi_1|F_1$ is not identically zero, then we set $s_0 := 0$. Otherwise, we define $s_0 := \max\{s \in \mathbf{Z}_1^m \mid \pi_1|F_1 = \cdots = \pi_s|F_1 = 0\}$. Note that $s_0 < m$, since $F_1 = H \neq \{e\}$.

Define $r_1 := s_0 + 1$ and

$$F_2 := \{h \in F_1 \mid \pi_{r_1}(h) = 0\}, \qquad s_1 := \max\{s \in \mathbf{Z}_{r_1}^m \mid \pi_{r_1}|F_2 = \cdots = \pi_s|F_2 = 0\}.$$

If $s_1 < m$, then we define $r_2 := s_1 + 1$ and

$$F_3 := \{h \in F_2 \mid \pi_{r_2}(h) = 0\}, \qquad s_2 := \max\{s \in \mathbf{Z}_{r_2}^m \mid \pi_{r_2}|F_3 = \cdots = \pi_s|F_3 = 0\}.$$

Continue until, at some $l \in \mathbf{N}$, we have $s_l = m$. Define $F_{l+1} = \{e\}$.

For all $i \in \mathbf{N}_l$, define $S_i := \mathbf{Z}_{r_i}^{s_i}$.

Lemma 7.1: *For all $i \in \mathbf{N}_l$, the map $\rho_i := \pi_{r_i}|F_i(\mathbf{Z})$ is a homomorphism from $F_i(\mathbf{Z})$ onto an infinite cyclic group. The kernel of ρ_i is $F_{i+1}(\mathbf{Z})$.*

Proof: Fix $i \in \mathbf{N}_l$. One verifies from matrix multiplication that ρ_i is, in fact a homomorphism. It is clear that $\rho_i(F_i(\mathbf{Z})) \subseteq \mathbf{Z}$ and that $\ker(\rho_i) = F_{i+1}(\mathbf{Z})$. We must show that $\rho_i(F_i(\mathbf{Z})) \neq \{0\}$.

Let V denote the (algebraic) Lie algebra of F_i; it is a subalgebra of the Lie algebra of SL_n. Let Γ denote a deep enough congruence subgroup of $V(\mathbf{Z})$ that $\exp(\Gamma) \subseteq F_i(\mathbf{Z})$. Since Γ is Zariski dense in V, it follows that $F_i(\mathbf{Z})$ is Zariski dense in $\exp(V) = F_i$.

Then $\rho_i(F_i(\mathbf{Z}))$ must be Zariski dense in $\rho_i(F_i)$. It follows from the definition of ρ_i and F_i that $\rho_i(F_i)$ is not the trivial group. Consequently, $\rho_i(F_i(\mathbf{Z})) \neq \{0\}$, as desired. ∎

For each $i \in \mathbf{N}_l$, let A_i be a preimage in $F_i(\mathbf{Z})$ of a positive generator for $\rho_i(F_i(\mathbf{Z}))$; see Lemma 7.1. For each i, note that $\rho_1(A_i) = \cdots = \rho_{i-1}(A_i) = 0$, while $\rho_i(A_i) > 0$.

LEMMA 7.2: *For all $h \in H(\mathbf{Z})$, there exists a unique $(n_1, \dots, n_l) \in \mathbf{Z}^l$ such that $h = A_1^{n_1} \cdots A_l^{n_l}$.*

Proof: By definition of A_1, there exists $n_1 \in \mathbf{Z}$ such that $A_1^{-n_1} h \in F_2(\mathbf{Z})$. By definition of A_2, there exists $n_2 \in \mathbf{Z}$ such that $A_2^{-n_2}(A_1^{-n_1} h) \in F_3(\mathbf{Z})$. Continuing, we find $n_1, \dots, n_l \in \mathbf{Z}$ such that $A_l^{-n_l} \cdots A_1^{-n_1} h \in F_{l+1}(\mathbf{Z}) = \{e\}$. So $h = A_1^{n_1} \cdots A_l^{n_l}$, proving existence.

Now suppose $A_1^{m_1} \cdots A_l^{m_l} = A_1^{n_1} \cdots A_l^{n_l}$; we wish to show that $m_i = n_i$, for all $i \in \mathbf{N}_l$.

By Lemma 7.1,

$$m_1 \rho_1(A_1) = \rho_1(A_1^{m_1} \cdots A_l^{m_l}) = \rho_1(A_1^{n_1} \cdots A_l^{n_l}) = n_1 \rho_1(A_1),$$

so $m_1 = n_1$. Then $A_2^{m_2} \cdots A_l^{m_l} = A_2^{n_2} \cdots A_l^{n_l}$, and we continue using ρ_2. ∎

The same proof shows

COROLLARY 7.3: *For all $i \in \mathbf{N}_l$, for all $h \in F_i(\mathbf{Z})$, there exists a unique $(n_i, \dots, n_l) \in \mathbf{Z}^{l-i+1}$ such that $h = A_i^{n_i} \cdots A_l^{n_l}$.* ∎

8. Generators for the Nth congruence subgroup

Let H, l and m be as in §7. For all $k \in \mathbf{N}_m$, let π_k be as in §7. For each $i \in \mathbf{N}_l$ let F_i, r_i, s_i, S_i, A_i and ρ_i be as in §7.

Definition 8.1: For all $i \in \mathbf{N}_l$, for all $k \in \mathbf{Z}_{r_i}^m$, for all $N \in \mathbf{N}$, let $F_i(k, N)$ denote the set of all $h \in F_i(\mathbf{Z})$ such that

$$\pi_{r_i}(h), \pi_{r_i+1}(h), \dots, \pi_k(h) \in N\mathbf{Z}.$$

Definition 8.2: For all $i \in \mathbf{N}_l$, let $\mathcal{F}_i$ denote the set of all maps $B\colon \mathbf{N} \to F_i(\mathbf{Z})$ such that $\pi_{r_i} \circ B$ is h.l.p. and positive and such that $\pi_{r_{i+1}} \circ B, \dots, \pi_{r_l} \circ B$ are all 0-v.p.p.

For all $v \in \mathbf{N}$, for all $M_1, \dots, M_v \in \mathrm{SL}_n(\mathbf{Z})$, define

$$\langle\langle M_1, \dots, M_v \rangle\rangle := \{M_1^{w_1} \cdots M_v^{w_v} \mid w_1, \dots, w_v \in \mathbf{Z}\};$$

in general this is a set, not a subgroup.

LEMMA 8.3: *Fix $i \in \mathbf{N}_l$ and let $k := r_i$. Then there exists $B \in \mathcal{F}_i$ such that, for all $N \in \mathbf{N}$,*

$$\langle\langle B(N), A_{i+1}, \cdots, A_l \rangle\rangle = F_i(k, N).$$

Proof: Let b: $\mathbf{N} \to \mathbf{Z}$ be defined by

$$b(N) := \min\{u \in \mathbf{N} \mid u\rho_i(A_i) \in N\mathbf{Z}\}.$$

By Lemma 6.4, b is h.l.p. Now define B: $\mathbf{N} \to H(\mathbf{Z})$ by $B(N) := A_i^{b(N)}$. ∎

LEMMA 8.4: *Let $i \in \mathbf{N}_l$ and let $k \in S_i$. Then there exists $B \in \mathcal{F}_i$ such that, for all $N \in \mathbf{N}$,*

$$\langle\langle B(N), A_{i+1}, \cdots, A_l \rangle\rangle = F_i(k, N).$$

Proof: The proof is by induction on k. By Lemma 8.3, we may assume that $r_i < k \leq s_i$.

By the induction hypothesis, there exists $C \in \mathcal{F}_i$ such that, for all $N \in \mathbf{N}$, we have

$$\langle\langle C(N), A_{i+1}, \ldots, A_l \rangle\rangle = F_i(k-1, N).$$

The map $\pi_k \circ C$: $\mathbf{N} \to \mathbf{Z}$ is 0-v.p.p. By Propositions 5.9 and 5.10, choose an h.l.p. a: $\mathbf{N} \to \mathbf{Z}$ such that, for all $N \in \mathbf{N}$,

$$\pi_k(C(N)) \equiv a(N) \bmod N.$$

Define b: $\mathbf{N} \to \mathbf{Z}$ by $b(N) := \min\{u \in \mathbf{N} \mid ua(n) \in N\mathbf{Z}\}$. By Lemma 6.3, b is periodic. Define $B \in \mathcal{F}_i$ by $B(N) := C(N)^{b(N)}$. ∎

LEMMA 8.5: *Let $i, j \in \mathbf{N}_l$ and assume that $i \leq j$. Let $k \in S_j$. Then there exist $B_i \in \mathcal{F}_i, \ldots, B_j \in \mathcal{F}_j$ such that, for all $N \in \mathbf{N}$, we have*

$$\langle\langle B_i(N), \ldots, B_j(N), A_{j+1}, \ldots, A_l \rangle\rangle = F_i(k, N).$$

Proof: The proof is by induction on $k - r_i$. By Lemma 8.4, we may assume that $i < j$.

CASE 1: $k = r_j$.

By induction, choose $C_{i+1} \in \mathcal{F}_{i+1}, \ldots, C_j \in \mathcal{F}_j$ such that, for all $N \in \mathbf{N}$, we have

$$\langle\langle C_{i+1}(N), \ldots, C_j(N), A_{j+1}, \ldots, A_l \rangle\rangle = F_{i+1}(k, N).$$

Since $k = r_j$, it follows that $k-1 \in S_{j-1}$. By induction, choose $D_i \in \mathcal{F}_i, \ldots, D_{j-1} \in \mathcal{F}_{j-1}$ such that, for all $N \in \mathbf{N}$, we have

$$\langle\langle D_i(N), \ldots, D_{j-1}(N), A_j, \ldots, A_l \rangle\rangle = F_i(k-1, N).$$

Let $t := j - i$. The maps $\pi_k \circ D_i, \ldots, \pi_k \circ D_{j-1}$ are 0-v.p.p. By Propositions 5.9 and 5.10, choose h.l.p. functions $a, b_1, \ldots, b_{t-1}$: $\mathbf{N} \to \mathbf{Z}$ such that, for all $N \in \mathbf{N}$,

$$\begin{aligned} a(N) &\equiv \pi_k(D_i(N)) \bmod N, \\ b_1(N) &\equiv \pi_k(D_{i+1}(N)) \bmod N, \\ &\cdots \\ b_{t-1}(N) &\equiv \pi_k(D_{j-1}(N)) \bmod N. \end{aligned}$$

Define b_t, c: $\mathbf{N} \to \mathbf{Z}$ by $b_t(N) := N$ and $c(N) := \pi_k(A_j)$. For all $N \in \mathbf{N}$, let

$$a'(N) := \min\{u \in \mathbf{N} \mid ua(N) \in b_1(N)\mathbf{Z} + \cdots + b_t(N)\mathbf{Z} + c(N)\mathbf{Z}\}.$$

Then, for all $u, N \in \mathbf{N}$,

$$(*) \quad ua(N) \in b_1(N)\mathbf{Z} + \cdots + b_t(N)\mathbf{Z} + c(N)\mathbf{Z} \qquad \Longleftrightarrow \qquad u \in a'(N)\mathbf{Z}.$$

By Lemma 6.6, we find that a': $\mathbf{N} \to \mathbf{Z}$ is periodic and we may choose periodic functions $b'_1, \ldots, b'_t$: $\mathbf{N} \to \mathbf{Z}$ and an h.l.p. function c': $\mathbf{N} \to \mathbf{Z}$ such that, for all $N \in \mathbf{N}$, we have

$$a(N)a'(N) = b_1(N)b'_1(N) + \cdots + b_t(N)b'_t(N) + c(N)c'(N).$$

For all $N \in \mathbf{N}$, define

$$\begin{aligned} B_i(N) &:= D_i(N)^{a'(N)} D_{i+1}(N)^{b'_1(N)} \cdots D_{j-1}(N)^{b'_{t-1}(N)} A_j^{c'(N)}, \\ B_{i+1}(N) &:= C_{i+1}(N)\ , \ \ldots\ ,\ B_j(N) := C_j(N); \end{aligned}$$

then $B_i(N), \ldots, B_j(N) \in F_i(k, N)$. Fix $N \in \mathbf{N}$ and $E \in F_i(k, N)$. To finish CASE 1, we must show that

$$E \in \langle\langle B_i(N), \ldots, B_j(N), A_{j+1}, \ldots, A_k \rangle\rangle.$$

Since $E \in F_i(k, N) \subseteq F_i(k-1, N)$, there exist $n_i, \ldots, n_l \in \mathbf{Z}$ such that

$$E = D_i(N)^{n_i} \cdots D_{j-1}(N)^{n_{j-1}} A_j^{n_j} \cdots A_l^{n_l}.$$

For all $N \in \mathbf{N}$, let $\mathrm{Rd}_N\colon \mathbf{Z} \to \mathbf{Z}/N\mathbf{Z}$ denote reduction modulo N; then

$$(\mathrm{Rd}_N \circ \pi_k)|\{h \in H \mid \pi_1(h), \ldots, \pi_{k-1}(h) \in N\mathbf{Z}\}$$

is a homomorphism. Furthermore, $\pi_k(E) \in N\mathbf{Z}$ and $b_t(N) = N$, $\forall N \in N$; it follows from $(*)$ that $n_i \in a'(N)\mathbf{Z}$. Choose $m \in \mathbf{Z}$ such that $n_i = a'(N)m$. By Lemma 7.1, ρ_i is a homomorphism, which implies that $\rho_i(B_i(N)^{-m}E) = 0$, or

$$B_i(N)^{-m}E \in F_{i+1}(k, N) = \langle\langle B_{i+1}(N), \ldots, B_j(N), A_{j+1}, \ldots, A_l\rangle\rangle.$$

It follows that $E \in \langle\langle B_i(N), \ldots, B_j(N), A_{j+1}, \ldots, A_l\rangle\rangle$, as desired to finish CASE 1.

CASE 2: $r_j < k \leq s_j$.

By induction, choose $C_{i+1} \in \mathcal{F}_{i+1}, \ldots, C_j \in \mathcal{F}_j$ such that, for all $N \in \mathbf{N}$, we have

$$\langle\langle C_{i+1}(N), \ldots, C_j(N), A_{j+1}, \ldots, A_l\rangle\rangle = F_{i+1}(k, N).$$

Since $r_j < k \leq s_j$, it follows that $k - 1 \in S_j$. By induction, choose $D_i \in \mathcal{F}_i, \ldots, D_j \in \mathcal{F}_j$ such that, for all $N \in \mathbf{N}$, we have

$$\langle\langle D_i(N), \ldots, D_j(N), A_{j+1}, \ldots, A_l\rangle\rangle = F_i(k-1, N).$$

Let $t := j - i + 1$. By Propositions 5.9 and 5.10, choose h.l.p. functions $a, b_1, \ldots, b_{t-1}\colon \mathbf{N} \to \mathbf{Z}$ such that, for all $N \in \mathbf{N}$, we have

$$\begin{aligned} a(N) &\equiv \pi_k(D_i(N)) \bmod N, \\ b_1(N) &\equiv \pi_k(D_{i+1}(N)) \bmod N, \\ &\cdots \\ b_{t-1}(N) &\equiv \pi_k(D_j(N)) \bmod N. \end{aligned}$$

Let $b_t\colon \mathbf{N} \to \mathbf{Z}$ be defined by $b_t(N) := N$.

For all $N \in \mathbf{N}$, let

$$a'(N) := \min\{u \in \mathbf{N} \mid ua(N) \in b_1(N)\mathbf{Z} + \cdots + b_t(N)\mathbf{Z}\}.$$

By Lemma 6.5, we find that $a'\colon \mathbf{N} \to \mathbf{Z}$ is periodic and we may choose periodic functions $b'_1, \ldots, b'_t\colon \mathbf{N} \to \mathbf{Z}$ such that, for all $N \in \mathbf{N}$, we have

$$a(N)a'(N) = b_1(N)b'_1(N) + \cdots + b_t(N)b'_t(N).$$

For all $N \in \mathbf{N}$, define

$$B_i(N) := D_i(N)^{a'(N)} D_{i+1}(N)^{b'_1(N)} \cdots D_j(N)^{b'_{t-1}(N)},$$
$$B_{i+1}(N) := C_{i+1}(N) \ , \ \ldots \ , \ B_j(N) := C_j(N);$$

then $B_i(N), \ldots, B_j(N) \in F_i(k, N)$.

The conclusion of CASE 2 is very similar to the conclusion of CASE 1; we omit it. ∎

Recall from Lemma 7.1 that $\rho_i := \pi_{r_i} | F_i(\mathbf{Z})$.

COROLLARY 8.6: *There exist $B_1 \in \mathcal{F}_1, \ldots, B_l \in \mathcal{F}_l$ such that: for all $i \in \mathbf{N}_l$, for all $N \in \mathbf{N}$, we have*

$$F_i(m, N) = \langle\langle B_i(N), \ldots, B_l(N) \rangle\rangle.$$

Proof: By the $i = 1$, $j = l$, $k = m$ case of Lemma 8.5, choose $B_1 \in \mathcal{F}_1, \ldots, B_l \in \mathcal{F}_l$ such that, for all $N \in \mathbf{N}$, we have

$$F_1(m, N) = \langle\langle B_1(N), \ldots, B_l(N) \rangle\rangle.$$

Fix $i \in \mathbf{N}_l$, $N \in \mathbf{N}$ and $E \in F_i(m, N)$; we wish to show that

$$E \in \langle\langle B_i(N), \ldots, B_l(N) \rangle\rangle.$$

Since $E \in F_1(m, N)$, choose $n_1, \ldots, n_l \in \mathbf{Z}$ such that $E = B_1(N)^{n_1} \cdots B_l(N)^{n_l}$.

If $i = 1$, then we are done. So assume $i > 1$. Then $\rho_1(E) = 0$ and so $n_1 = 0$. So if $i = 2$, then we are done. So assume $i > 2$. Then $\rho_2(E) = 0$, so $n_2 = 0$. If $i = 3$, then we are done.

Continuing this way, the proof will eventually be complete, for any value of i. ∎

For each $N \in \mathbf{N}$, let Rd_N: $H(\mathbf{Z}) \to H(\mathbf{Z}/N\mathbf{Z})$ denote reduction mod N and let $H(N) := \ker(\mathrm{Rd}_N)$.

For any subset S of a group, we denote the subgroup generated by S as $\langle S \rangle$.

For all $v \in \mathbf{N}$, for all $M_1, \ldots, M_v \in \mathrm{SL}_n(\mathbf{Z})$, let $\langle M_1, \ldots, M_v \rangle$ denote the subgroup of $\mathrm{SL}_n(\mathbf{Z})$ generated by $M_1, \ldots, M_v$.

COROLLARY 8.7: *There exists a collection of h.l.p. functions*

$$a^i_j \colon \mathbf{N} \to \mathbf{Z} \qquad (i, j \in \mathbf{N}_l,\ i \le j)$$

such that, for all $N \in \mathbf{N}$, we have

$$H(N) := \left\langle A_i^{a^i_i(N)} \cdots A_l^{a^i_l(N)} \,\middle|\, i \in \mathbf{N}_l \right\rangle,$$

and such that, for all $i \in \mathbf{N}_l$, a^i_i is positive.

Proof: Choose $B_1 \in \mathcal{F}_1, \ldots, B_l \in \mathcal{F}_l$ as in Corollary 8.6.

Fix $i \in \mathbf{N}_l$. Define $b^i_i\colon \mathbf{N} \to \mathbf{Z}$ by

$$b^i_i(N) := \rho_i(B_i(N))/\rho_i(A_i);$$

b^i_i is h.l.p. Since $B_i \in \mathcal{F}_i$ and since $\rho_i(A_i) > 0$, it follows that b^i_i is positive. For each $j = i+1, \ldots, l$, define $b^i_j\colon \mathbf{N} \to \mathbf{Z}$ inductively by the recursive formula

$$b^i_j(N) := \rho_j\left(A_{j-1}^{-b^i_{j-1}(N)} \cdots A_i^{-b^i_i(N)} B_i(N)\right) \Big/ \rho_j(A_j);$$

b^i_j is 0-v.p.p.

Then, for all $i \in \mathbf{N}_l$ and $N \in \mathbf{N}$,

$$B_i(N) = A_i^{b^i_i(N)} \cdots A_l^{b^i_l(N)}.$$

Fix $i \in \mathbf{N}_l$. Define $a^i_i := b^i_i$. Using Propositions 5.9 and 5.10, choose h.l.p. functions $a^i_{i+1}, \ldots, a^i_l\colon \mathbf{N} \to \mathbf{Z}$ such that, for all $N \in \mathbf{N}$, we have

$$\forall j \in \mathbf{Z}^l_{i+1}, \qquad a^i_j(N) \equiv b^i_j(N) \bmod N(n!)^2.$$

It is an exercise to use the expansions of the exponential and logarithm maps on unipotent matrices to show: If M is an upper triangular, unipotent $n \times n$ matrix, if $s, t \in \mathbf{Z}$, if $N \in \mathbf{N}$ and if $s \equiv t \bmod N(n!)^2$, then $M^s \equiv M^t \bmod N$.

Applying this, we find: for all $i \in \mathbf{N}_l$, for all $j \in \mathbf{Z}^l_i$, for all $N \in \mathbf{N}$, we have

$$A_i^{b^i_j(N)} \equiv A_i^{a^i_j(N)} \bmod N.$$

Let $C_i(N) := A_i^{a^i_i(N)} \cdots A_l^{a^i_l(N)}$. Then, for all $i \in \mathbf{N}_l$, for all $N \in \mathbf{N}$,

$$C_i(N) = A_i^{a^i_i(N)} \cdots A_l^{a^i_l(N)} \equiv A_i^{b^i_i(N)} \cdots A_l^{b^i_l(N)} = B_i(N) \bmod N,$$

so $C_i(N) \in F_i(m, N)$.

CLAIM: *For all $i \in \mathbf{N}_l$, for all $N \in \mathbf{N}$,*

$$F_i(m,N) = \langle C_i(N), \ldots, C_l(N) \rangle.$$

The proof of the CLAIM is by (downward) induction on $i = l, \ldots, 1$. When $i = l$, the result follows from Corollary 8.6, because $C_l(N) = A_l^{a_l^l(N)} = B_l(N)$.

Now fix $i \in \mathbf{N}_{l-1}$, $N \in \mathbf{N}$ and $E \in F_i(m,N)$; we wish to show that

$$E \in \langle C_i(N), \ldots, C_l(N) \rangle,$$

under the induction assumption

$$F_{i+1}(m,N) = \langle C_{i+1}(N), \ldots, C_l(N) \rangle.$$

By Corollary 8.6, we may choose $n_i, \ldots, n_l \in \mathbf{Z}$ such that

$$E = B_i(N)^{n_i} \cdots B_l(N)^{n_l}.$$

Since $a_i^i(N) = b_i^i(N)$, it follows from Lemma 7.1 that

$$\rho_i\left(C_i(N)^{-n_i} E\right) = \rho_i\left(\left(A_i^{a_i^i(N)} \cdots A_l^{a_l^i(N)}\right)^{-n_i} E\right) = 0,$$

so $C_i(N)^{-n_i} E \in F_{i+1}(m,N) = \langle C_{i+1}(N), \ldots, C_l(N) \rangle$, which proves the CLAIM.

But then the special case $i = 1$ of the CLAIM reads: For all $N \in \mathbf{N}$,

$$\langle C_1(N), \ldots, C_l(N) \rangle = F_1(m,N) = H(N).$$

By definition of $C_1, \ldots, C_l$, this is exactly what we wish to prove. ∎

9. Rational planes and polynomial periodicity

Let H and l be as in §7. For the remainder of this section, fix a positive integer d.

Let $\mathbf{T}^0$ denote the trivial group.

Fix $c \in \mathbf{N}$. Let $\mathbf{T}^c$ denote the c-torus, thought of as a multiplicative, compact, Abelian group. Let $\operatorname{tor} \mathbf{T}^c$ denote the subgroup of all elements in $\mathbf{T}^c$ of finite order. A subset $\pi \subseteq \mathbf{T}^c$ is a **rational plane** if there exists an element $\zeta \in \operatorname{tor} \mathbf{T}^c$ such that $\zeta\pi$ is a closed, connected subgroup of $\mathbf{T}^c$.

LEMMA 9.1: *Let $c \in \mathbf{N}$ and let $b\colon \mathbf{N} \to \mathbf{Z}$ be 0-v.p.p. Let $\pi \subseteq \mathbf{T}^c$ be a rational plane and let $w \in \operatorname{tor} \mathbf{T}^c$. For all $N \in \mathbf{N}$, let $f(N)$ be the cardinality of the set*

$$\{\chi \in \pi \mid \chi^{b(N)} = w\}.$$

Then $f\colon \mathbf{N} \to \mathbf{Z}$ is 0-v.p.p.

Proof: Choose $\zeta \in \operatorname{tor} \mathbf{T}^c$ such that $S := \zeta\pi$ is a closed, connected subgroup of $\mathbf{T}^c$. Let $e := \dim S$. Let u denote the order of ζ. By Proposition 1.9, there exists a periodic function $b'\colon \mathbf{N} \to \mathbf{Z}$ such that, for all $N \in \mathbf{N}$, we have $b(N) \equiv b'(N) \bmod u$.

Fix $N \in \mathbf{N}$. Then

$$\chi \mapsto \zeta\chi\colon \pi \to S$$

is 1-to-1, while

$$\chi \mapsto \chi^{b(N)}\colon S \to S$$

is $b(N)^e$-to-1, while

$$\chi \mapsto \zeta^{-b(N)}\chi\colon S \to \pi^{b(N)}$$

is 1-to-1. We conclude that the composite map

$$\chi \mapsto \chi^{b(N)}\colon \pi \to \pi^{b(N)}$$

is $b(N)^e$-to-1.

For all $N \in \mathbf{N}$, we have $\pi^{b(N)} = \zeta^{-b(N)}S$; define

$$a(N) := \begin{cases} 0, & \text{if } w \notin \zeta^{-b(N)}S \\ 1, & \text{if } w \in \zeta^{-b(N)}S. \end{cases}$$

For all $N \in \mathbf{N}$, we have $\zeta^{-b(N)} = \zeta^{-b'(N)}$. Since b' is periodic, the function $a\colon \mathbf{N} \to \mathbf{Z}$ is periodic. Now, for all $N \in \mathbf{N}$, we have $f(N) = a(N)b(N)^e$; it follows that $f\colon \mathbf{N} \to \mathbf{Z}$ is 0-v.p.p., as asserted. ∎

Definition 9.2: For all $c \in \mathbf{N}$, $\chi = (\chi_1, \ldots, \chi_c) \in \mathbf{T}^c$, $\alpha = (\alpha_1, \ldots, \alpha_c) \in \mathbf{Z}^c$, we define

$$\langle \chi, \alpha \rangle := \chi_1^{\alpha_1} \cdots \chi_c^{\alpha_c} \in \mathbf{T}^1.$$

Definition 9.3: Let $\chi = (\chi_1, \ldots, \chi_d) \in \mathbf{T}^d$. Let $i, j \in \mathbf{N}_d$ and assume $i \leq j$. We define $\chi_{ij} := (\chi_i, \ldots, \chi_j) \in \mathbf{T}^{j-i+1}$. We will abbreviate χ_{ii} as χ_i, for simplicity.

Let $\mathcal{R}$ denote the set of all rational planes in $\mathbf{T}^d$.

For all $c, k \in \mathbf{N}$ satisfying $c \leq k$, let $\mathcal{S}(c,k)$ denote the set of all $(\beta_1, \ldots, \beta_k) \in (\mathbf{Z}^c)^k$ such that $\mathbf{Z}^c = \beta_1\mathbf{Z} + \cdots + \beta_k\mathbf{Z}$.

Definition 9.4: Let b: $\mathbf{N} \to \mathbf{Z}$ be 0-v.p.p. Let $c \in \mathbf{N}_d$, $k \in \mathbf{N}_l$ satisfy $c \leq k$. Let $\pi \in \mathcal{R}$, $\beta = (\beta_1, \ldots, \beta_k) \in \mathcal{S}(c,k)$. Let $s = (s_1, \ldots, s_k) \in \operatorname{tor}\mathbf{T}^k$, $w = (w_{c+1}, \ldots, w_d) \in \operatorname{tor}\mathbf{T}^{d-c}$. For all $N \in \mathbf{N}$, let $\mathcal{E}(N)$ denote the set of all $\chi \in \pi$ such that

$$\forall i \in \mathbf{N}_k,\ \langle \chi_{1c}, b(N)\beta_i \rangle = s_i \qquad \text{and} \qquad \forall j \in \mathbf{Z}^d_{c+1},\ \chi_j^{b(N)} = w_j.$$

We define $F_{b\pi\beta sw}$: $\mathbf{N} \to \mathbf{Z}$ by letting $F_{b\pi\beta sw}(N)$ be the cardinality of $\mathcal{E}(N)$. Similarly, for all $N \in \mathbf{N}$, we let $\mathcal{E}'(N)$ denote the set of all $\chi \in \pi$ such that

$$\forall j \in \mathbf{Z}^d_1,\ \chi_j^{b(N)} = w_j.$$

We define $F'_{b\pi w}$: $\mathbf{N} \to \mathbf{Z}$ by letting $F'_{b\pi w}(N)$ be the cardinality of $\mathcal{E}'(N)$.

We define $\mathbf{T}^0$ to be the trivial group $\{1\}$. When $c = d$ and $w = 1$, we define $F_{b\pi\beta sw}$ as in Defintion 9.4, but with the convention that $\mathcal{E}(N)$ denotes the set of all $\chi \in \pi$ such that

$$\forall i \in \mathbf{N}_k,\ \langle \chi_{1d}, b(N)\beta_i \rangle = s_i.$$

Definition 9.5: Let b: $\mathbf{N} \to \mathbf{Z}$ be 0-v.p.p. Let $c \in \mathbf{N}_d$, $k \in \mathbf{N}_l$. If $c \leq k$, then we define $\mathcal{F}_b(c,k)$ to be the $\mathbf{Z}$-span of the set of functions

$$\{F_{b\pi\beta sw} \mid \pi \in \mathcal{R},\ \beta \in \mathcal{S}(c,k),\ s \in \operatorname{tor}\mathbf{T}^k,\ w \in \operatorname{tor}\mathbf{T}^{d-c}\}.$$

If $c > k$, then we define $\mathcal{F}_b(c,k)$ to be the set consisting of $\mathbf{0}$ alone, where $\mathbf{0}$: $\mathbf{N} \to \mathbf{Z}$ is the function which is identically zero. Finally, we define $\mathcal{F}'_b$ to be the $\mathbf{Z}$-span of

$$\{F'_{b\pi w} \mid \pi \in \mathcal{R},\ w \in \operatorname{tor}\mathbf{T}^{d-c}\}.$$

LEMMA 9.6: *Let b: $\mathbf{N} \to \mathbf{Z}$ be 0-v.p.p. Let $c \in \mathbf{Z}^d_2$, $k \in \mathbf{Z}^l_2$ satisfy $c \leq k$. Then $\mathcal{F}_b(c,k) \subseteq \mathcal{F}_b(c-1,k-1) \cup \mathcal{F}_b(c,k-1)$.*

Proof: Fix $c \in \mathbf{Z}^d_2$, $k \in \mathbf{Z}^l_2$, $\beta = (\beta_1, \ldots, \beta_k) \in \mathcal{S}(c,k)$, $s = (s_1, \ldots, s_k) \in \operatorname{tor}\mathbf{T}^k$, $w \in \operatorname{tor}\mathbf{T}^{d-c}$. Let $g := F_{b\pi\beta sw}$; we wish to show that $g \in \mathcal{F}_b(c-1,k-1) \cup \mathcal{F}_b(c,k-1)$.

If $\beta_k = 0$ and $s_k \neq 1$, then g: $\mathbf{N} \to \mathbf{Z}$ is identically zero and we are done.

Let $\tilde{\beta} := (\beta_1, \ldots, \beta_{k-1})$ and $\tilde{s} := (s_1, \ldots, s_{k-1})$. If $\beta_k = 0$ and $s_k = 1$, then we have $g = F_{b\pi\tilde{\beta}\tilde{s}w} \in \mathcal{F}_b(c, k-1)$ and, again, we are done.

We may therefore assume that $\beta_k \neq 0$. We will prove in this case that $g \in \mathcal{F}_b(c-1, k-1)$.

Let $\epsilon := (0, 0, \ldots, 0, 0, 1) \in \mathbf{Z}^c$. Choose an automorphism η: $\mathbf{Z}^c \to \mathbf{Z}^c$ such that $\beta_k \in \eta(\epsilon)\mathbf{Z}$. Let I: $\mathbf{Z}^{d-c} \to \mathbf{Z}^{d-c}$ denote the identity map. Let $\theta := \eta \times I$: $\mathbf{Z}^d \to \mathbf{Z}^d$.

Then η induces an automorphism $\tilde{\eta} := \eta^k$: $(\mathbf{Z}^c)^k \to (\mathbf{Z}^c)^k$, and θ induces an adjoint automorphism $\hat{\theta}$: $\mathbf{T}^d \to \mathbf{T}^d$ defined by $\langle \hat{\theta}(\chi), \theta(\alpha) \rangle = \langle \chi, \alpha \rangle$, for all $\chi \in \mathbf{T}^d$ and all $\alpha \in \mathbf{Z}^d$.

Replacing π by $(\hat{\theta})^{-1}(\pi)$ and β by $(\tilde{\eta})^{-1}(\beta)$, we may assume that $\beta_k \in \epsilon\mathbf{Z}$. Choose $n_1, \ldots, n_k \in \mathbf{Z}$ and $\gamma_1, \ldots, \gamma_{k-1} \in \mathbf{Z}^{c-1}$ such that

$$\beta_1 = (\gamma_1, n_1), \ldots, \beta_{k-1} = (\gamma_{k-1}, n_{k-1}),\ \beta_k = (0, n_k).$$

Let $\tilde{c} := c - 1$. Then, for all $N \in \mathbf{N}$, $g(N)$ is the number of $\chi \in \pi$ satisfying

$$\forall i \in \mathbf{N}_{k-1},\ \langle \chi_{1\tilde{c}}, b(N)\gamma_i \rangle \chi_c^{b(N)n_i} = s_i, \quad \chi_c^{b(N)n_k} = s_k, \quad \forall j \in \mathbf{Z}_{c+1}^d,\ \chi_j^{b(N)} = w_j.$$

Let $V := \{v \in \operatorname{tor} \mathbf{T}^1 \,|\, v^{n_k} = s_k\}$. For all $v \in V$, for all $N \in \mathbf{N}$, let $h_v(N)$ denote the number of $\chi \in \pi$ satisfying

$$\forall i \in \mathbf{N}_{k-1},\ \langle \chi_{1\tilde{c}}, b(N)\gamma_i \rangle = s_i v^{-n_i}, \qquad \chi_c^{b(N)} = v, \qquad \forall j \in \mathbf{Z}_{c+1}^d,\ \chi_j^{b(N)} = w_j.$$

Then, for all $v \in V$, $h_v \in \mathcal{F}_b(c-1, k-1)$ and it follows from inclusion-exclusion that g is a $\mathbf{Z}$-linear combination of elements of $\{h_v \,|\, v \in V\}$. Thus $g \in \mathcal{F}_b(c-1, k-1)$, as desired. ∎

We omit the proof of the next lemma since its proof is similar to, but easier than that of Lemma 9.6.

LEMMA 9.7: *Let b: $\mathbf{N} \to \mathbf{Z}$ be 0-v.p.p. Let $k \in \mathbf{N}_d$. Then $\mathcal{F}_b(1, k) \subseteq \mathcal{F}'_b$.*

COROLLARY 9.8: *Let b: $\mathbf{N} \to \mathbf{Z}$ be 0-v.p.p. Let $c \in \mathbf{N}_d$, $k \in \mathbf{N}_l$. Then $\mathcal{F}_b(c, k) \subseteq \mathcal{F}'_b$.*

Proof: The proof is by induction on k. If $c > k$, then $\mathcal{F}_b(c, k)$ consists of the zero function alone, and we are done. If $c = 1$, then we are done by Lemma 9.7.

We therefore assume $2 \leq c \leq k$. The induction hypothesis and Lemma 9.6 now complete the proof. ∎

LEMMA 9.9: *Let b: $\mathbf{N} \to \mathbf{Z}$ be 0-v.p.p. Let $\pi \in \mathcal{R}$, $(\alpha_1, \ldots, \alpha_l) \in \mathcal{S}(d, l)$, $(r_1, \ldots, r_l) \in tor\mathbf{T}^l$. For all $N \in \mathbf{N}$, let $f(N)$ denote the cardinality of*

$$\{\chi \in \pi \mid \forall i \in \mathbf{N}_l,\ \langle \chi, b(N)\alpha_i \rangle = r_i\}.$$

Then f: $\mathbf{N} \to \mathbf{Z}$ is 0-v.p.p.

Proof: Let $\alpha := (\alpha_1, \ldots, \alpha_l)$, $r := (r_1, \ldots, r_l)$ and $v := 1 \in \mathbf{T}^0$. Then

$$f = F_{b\pi\alpha rv} \in \mathcal{F}_b(d, l),$$

so, by Corollary 9.8, $f \in \mathcal{F}'_b$.

From the definition of $\mathcal{F}'_b$ and from Lemma 9.1, it follows that $\mathcal{F}'_b$ is the $\mathbf{Z}$-span of a set of 0-v.p.p. functions. Consequently, every element of $\mathcal{F}'_b$ is 0-v.p.p.; in particular, f is. ∎

COROLLARY 9.10: *Let $\pi \in \mathcal{R}$. Let b: $\mathbf{N} \to \mathbf{Z}$ be 0-v.p.p. and let $(\alpha_1, \ldots, \alpha_l) \in \mathcal{S}(d, l)$. Let $\mathcal{T}$ denote the collection of all finite subsets of $tor\mathbf{T}^l$. Let T: $\mathbf{N} \to \mathcal{T}$ be a periodic function. For all $i \in \mathbf{N}_l$, for all $N \in \mathbf{N}$, let $\psi_i(\chi, N) := \langle \chi, b(N)\alpha_i \rangle$. For all $N \in \mathbf{N}$, let $f(N)$ denote the cardinality of the set*

$$\{\chi \in \pi \mid (\psi_1(\chi, N), \ldots, \psi_l(\chi, N)) \in T(N)\}.$$

Then f: $\mathbf{N} \to \mathbf{Z}$ is 0-v.p.p.

Proof: If T: $\mathbf{N} \to \mathcal{T}$ is constant, then the result follows from Lemma 9.9 and the fact that a sum of 0-v.p.p functions is again 0-v.p.p.

Choose $m \in \mathbf{N}$ such that, for all $i \in \mathbf{N}_m$, T is constant on $(m\mathbf{Z} + i) \cap \mathbf{N}$. Then, for all $i \in \mathbf{N}_m$, the constant case demonstrates that f agrees with a 0-v.p.p. function on $(m\mathbf{Z} + i) \cap \mathbf{N}$.

It follows that f is 0-v.p.p. ∎

10. A technical result

Let H be as in §7. For each $i \in \mathbf{N}_l$, let A_i be as in §7.

For all $N \in \mathbf{N}$, let $H(N)$ denote the kernel of the map $H(\mathbf{Z}) \to H(\mathbf{Z}/N\mathbf{Z})$ defined by reduction mod N.

THEOREM 10.1: *Let Γ denote the Abelianization of $H(\mathbf{Z})$. Let $\hat{\Gamma}$ denote the dual group to Γ and let $\hat{\Gamma}^0$ denote its connected component of the identity; $\hat{\Gamma}^0$ is a (compact, connected) torus group. Fix an element $\chi_0 \in \hat{\Gamma}$. Fix a rational plane $\pi \subseteq \hat{\Gamma}^0$. For all $N \in \mathbf{N}$, let $\Gamma(N)$ denote the image in Γ of $H(N)$. For all $N \in \mathbf{N}$, let $f(N)$ denote the cardinality of $\{\chi \in \pi \mid (\chi_0\chi)|\Gamma(N) = 1\}$. Then $f\colon \mathbf{N} \to \mathbf{Z}$ is p.p.*

Proof: We will denote the group operation on Γ as addition. Let Γ^{tor} and Γ^{tf} denote the torsion and torsion-free parts of Γ, respectively.

Let pr: $\Gamma \to \Gamma^{\mathrm{tf}}$ denote the natural projection and define $\chi_1 := \chi_0 \circ \mathrm{pr}$. Then $(\chi_0\chi_1^{-1})|\Gamma^{\mathrm{tf}} = 1$ and $\chi_1 \in \hat{\Gamma}^0$. Replacing χ_0 by $\chi_0\chi_1^{-1}$ and π by $\chi_1\pi$, we may assume that $\chi_0|\Gamma^{\mathrm{tf}} = 1$.

Let $d := \mathrm{rank}(\Gamma^{\mathrm{tf}})$. Choose an isomorphism between Γ^{tf} and $\mathbf{Z}^d$; this gives rise to an isomorphism between $\hat{\Gamma}^0$ and the multiplicative group $\mathbf{T}^d$.

Let $a^i_j\colon \mathbf{N} \to \mathbf{Z}$ $\quad(i, j \in \mathbf{N}_l,\ i \leq j)$ be as in Corollary 8.7. Let $\alpha_1, \ldots, \alpha_l$ denote the images of $A_1, \ldots, A_l$ in Γ. Let $\alpha_1^{\mathrm{tor}}, \ldots, \alpha_l^{\mathrm{tor}}$ denote the torsion parts of $\alpha_1, \ldots, \alpha_l$. Let $\alpha_1^{\mathrm{tf}}, \ldots, \alpha_l^{\mathrm{tf}}$ denote the torsion-free parts of $\alpha_1, \ldots, \alpha_l$. Note that $(\alpha_1^{\mathrm{tf}}, \ldots, \alpha_l^{\mathrm{tf}}) \in \mathcal{S}(d, l)$, after the identification of Γ^{tf} with $\mathbf{Z}^d$.

For all $i \in \mathbf{N}_l$, for all $N \in \mathbf{N}$, let

$$\beta_i(N) := a^i_i(N)\alpha_i + \cdots + a^i_l(N)\alpha_l.$$

Then, for all $N \in \mathbf{N}$, $\Gamma(N) = \beta_1(N)\mathbf{Z} + \cdots + \beta_l(N)\mathbf{Z}$, so $f(N)$ is the cardinality of

$$S(N) := \{\chi \in \pi \mid \langle \chi_0\chi, \beta_1(N)\rangle = \cdots = \langle \chi_0\chi, \beta_l(N)\rangle = 1\}.$$

For all $i \in \mathbf{N}_l$, for all $N \in \mathbf{N}$, let

$$b_i(N) := \gcd(a^i_i(N), \ldots, a^i_l(N)).$$

For all $N \in \mathbf{N}$, let $b(N) := \gcd(b_1(N), \ldots, b_l(N))$. Then $b\colon \mathbf{N} \to \mathbf{Z}$ is positive and h.l.p., by Corollary 6.2. For all $i \in \mathbf{N}_l$, for all $j \in \mathbf{Z}^l_i$, let $q^i_j := a^i_j/b$; then $q^i_j\colon \mathbf{N} \to \mathbf{Z}$ is periodic.

For all $i \in \mathbf{N}_l$, define $\psi_i\colon \hat{\Gamma} \times \mathbf{N} \to \mathbf{T}^1$ by $\psi_i(\chi, N) = \langle \chi, b(N)\alpha_i \rangle$. Recall that $(\alpha_1^{\mathrm{tf}}, \ldots, \alpha_l^{\mathrm{tf}}) \in \mathcal{S}(d, l)$. As in Corollary 9.10, for all $i \in \mathbf{N}_l$, define $\psi_i^{\mathrm{tf}}\colon \hat{\Gamma} \times \mathbf{N} \to \mathbf{T}^1$ by $\psi_i^{\mathrm{tf}}(\chi, N) = \langle \chi, b(N)\alpha_i^{\mathrm{tf}} \rangle$. For all $i \in \mathbf{N}_l$, for all $N \in \mathbf{N}$, let $\psi_i^{\mathrm{tor}}(\chi, N) := \langle \chi, b(N)\alpha_i^{\mathrm{tor}} \rangle$.

Fix $i \in \mathbf{N}_l$. For all $\chi \in \hat{\Gamma}^0$, for all $N \in \mathbf{N}$, we have

$$\psi_i(\chi\chi_0, N) = \psi_i^{\mathrm{tor}}(\chi\chi_0, N)\psi_i^{\mathrm{tf}}(\chi\chi_0, N) = \psi_i^{\mathrm{tor}}(\chi_0, N)\psi_i^{\mathrm{tf}}(\chi, N).$$

Let k_i be the order of α_i^{tor}. By Proposition 9.5, choose a periodic function $b_i'\colon \mathbf{N} \to \mathbf{Z}$ such that $b_i'(N) \equiv b(N) \bmod k_i$. Then, for all $N \in \mathbf{N}$, $\psi_i^{\mathrm{tor}}(\chi_0, N) = \langle \chi_0, b_i'(N)\alpha_i^{\mathrm{tor}} \rangle$, so the function $N \mapsto \psi_i^{\mathrm{tor}}(\chi_0, N)\colon \mathbf{N} \to \mathbf{T}^1$ is periodic.

Let $\mathcal{T}$ denote the set of all finite subsets of $\operatorname{tor}\mathbf{T}^l$. For all $N \in \mathbf{N}$, for all $i \in \mathbf{N}_l$, for all $\zeta = (\zeta_1, \ldots, \zeta_l) \in \mathbf{T}^l$, define

$$\lambda_i(\zeta, N) := \zeta_i^{q_i^i(N)} \cdots \zeta_l^{q_l^i(N)}.$$

For all $N \in \mathbf{N}$, let

$$\begin{aligned} T_0(N) &:= \{\zeta \in \mathbf{T}^l \mid \lambda_1(\zeta, N) = \cdots = \lambda_l(\zeta, N) = 1\}, \\ T(N) &:= (\psi_1^{\mathrm{tor}}(\chi_0, N)^{-1}, \ldots \psi_l^{\mathrm{tor}}(\chi_0, N)^{-1})T_0(N). \end{aligned}$$

The functions $T_0, T\colon \mathbf{N} \to \mathcal{T}$ are periodic.

For all $N \in \mathbf{N}$, we have

$$\begin{aligned} S(N) &= \{\chi \in \pi \mid \ \forall i \in \mathbf{N}_l, \ \ \psi_i(\chi_0\chi, N)^{q_i^i(N)} \cdots \psi_l(\chi_0\chi, N)^{q_l^i(N)} = 1\} \\ &= \{\chi \in \pi \mid (\psi_1(\chi_0\chi, N), \ldots, \psi_l(\chi_0\chi, N)) \in T_0(N)\} \\ &= \{\chi \in \pi \mid (\psi_1^{\mathrm{tf}}(\chi, N), \ldots, \psi_l^{\mathrm{tf}}(\chi, N)) \in T(N)\} \end{aligned}$$

But, for all $N \in \mathbf{N}$, $f(N)$ is the cardinality of $S(N)$; the result follows from Corollary 9.10. ∎

11. Reduction to the upper triangular case

Lemma 11.1: *Let $n \in \mathbf{N}$. Let $v_1, \ldots, v_n$ be an ordered $\mathbf{Q}$-basis for $\mathbf{Q}^n$. Then there is an ordered $\mathbf{Z}$-base $w_1, \ldots, w_n$ for $\mathbf{Z}^n$ such that the full flag is unchanged, i.e., such that*

$$\mathbf{Q}v_1 = \mathbf{Q}w_1, \quad \mathbf{Q}v_1 + \mathbf{Q}v_2 = \mathbf{Q}w_1 + \mathbf{Q}w_2, \quad \ldots, \\ \mathbf{Q}v_1 + \cdots + \mathbf{Q}v_n = \mathbf{Q}w_1 + \cdots + \mathbf{Q}w_n.$$

Proof: We construct the w_is inductively. Let w_1 be a generator of the infinite cyclic group $\mathbf{Z}^n \cap (\mathbf{Q}v_1)$.

Now assume that $w_1, \ldots, w_m \in \mathbf{Z}^n$ have been chosen so that

$$\mathbf{Z}v_1 + \cdots + \mathbf{Z}v_m = \mathbf{Z}^n \cap (\mathbf{Q}v_1 + \cdots + \mathbf{Q}v_m)$$

and so that

$$\mathbf{Q}v_1 = \mathbf{Q}w_1, \quad \mathbf{Q}v_1 + \mathbf{Q}v_2 = \mathbf{Q}w_1 + \mathbf{Q}w_2, \quad \ldots, \\ \mathbf{Q}v_1 + \cdots + \mathbf{Q}v_m = \mathbf{Q}w_1 + \cdots + \mathbf{Q}w_m.$$

The image C of $\mathbf{Z}^n \cap (\mathbf{Q}v_1 + \cdots + \mathbf{Q}v_{m+1})$ in the one-dimensional quotient vector space

$$(\mathbf{Q}v_1 + \cdots + \mathbf{Q}v_{m+1})/(\mathbf{Q}v_1 + \cdots + \mathbf{Q}v_m)$$

is nonzero and discrete, hence infinite cyclic. Let c be a generator of C and let w_{m+1} be a preimage in $\mathbf{Z}^n \cap (\mathbf{Q}v_1 + \cdots + \mathbf{Q}v_{m+1})$ of c. ∎

COROLLARY 11.2: *Let n be a positive integer. Let H be a unipotent algebraic subgroup of SL_n. Then there exists an element $w \in SL_n(\mathbf{Z})$ such that $w^{-1}Hw$ is contained in the upper triangular unipotent matrices in SL_n.*

Proof: Let V denote the (algebraic) vector space $\mathbf{A}^{n\times 1}$ of $n \times 1$ column matrices. Let V_1' denote the $\mathbf{Q}$-subspace of V consisting of those vectors fixed by every element of H under matrix multiplication. By [Hum, Corollary 17.5, p. 113], $V_1 \neq \{0\}$. Since it is a linear subspace defined over $\mathbf{Q}$, we may choose a $\mathbf{Q}$-point $v_1 \in V_1 \backslash \{0\}$. Let V_1 denote the linear space spanned by v_1. Then H acts by special linear transformations on V/V_1. Furthermore, the image of H in $\mathrm{SL}(V/V_1)$ is again unipotent. By using induction on $\dim V$, we obtain $\mathbf{Q}$-vectors $v_1, \ldots, v_n$ with linear spans $V_1, \ldots, V_n$ such that every element of H fixes the full flag

$$0 \subseteq V_1 \subseteq V_1 \oplus V_2 \subseteq \cdots \subseteq V_1 \oplus \cdots \oplus V_n = V.$$

Let v denote the matrix with columns $v_n, \ldots, v_1$. It follows that $v^{-1}Hv$ consists of upper triangular unipotent matrices.

Then Lemma 11.1 (with $\mathbf{Q}^n$ replaced by the isomorphic vector space $\mathbf{Q}^{n\times 1}$) yields column vectors $w_1, \ldots, w_n \in \mathbf{Z}^{n\times 1}$. Replacing w_1 by $-w_1$ if necessary, we may assume that the $n \times n$ matrix w with columns $w_n, \ldots, w_1$ satisfies $\det w =$

1. Then $w^{-1}Hw = v^{-1}Hv$, so $w^{-1}Hw$ is contained in the upper triangular unipotent matrices in SL_n. ∎

The following technical result has been the main goal of §§5-11.

THEOREM 11.3: *Let n be a positive integer and let H be a unipotent $\mathbf{Q}$-subgroup of SL_n. Let Γ denote the Abelianization of $H(\mathbf{Z})$. Let $\hat{\Gamma}$ denote the dual group* $\hom(\Gamma, \mathbf{T}^1)$ *of Γ, where $\mathbf{T}^1 \subseteq \mathbf{C}$ denotes the complex numbers of modulus one. Fix an element $\chi_0 \in \hat{\Gamma}$. Let $\hat{\Gamma}^0$ denote the connected component of the identity in $\hat{\Gamma}$. Let $\pi \subseteq \hat{\Gamma}^0$ be a translate of a closed connected subgroup of $\hat{\Gamma}^0$ by: an element in $\hat{\Gamma}^0$ of finite order. For all integers $N > 0$, let Rd_N: $H(\mathbf{Z}) \to H(\mathbf{Z}/N\mathbf{Z})$ be the map defined by reduction mod N and let $H(N)$ denote the kernel of Rd_N; $H(N)$ is the N***th* congruence subgroup of** H. For each $N > 0$, let $\Gamma(N)$ denote the image of $H(N)$ in the Abelianization Γ of $H(\mathbf{Z})$. For each $N > 0$, let $f(N)$ denote the number of elements $\chi \in \pi$ such that $(\chi_0\chi)|\Gamma(N)$ is identically 1. Then the function $f\colon \mathbf{N} \to \mathbf{Z}$ is* **polynomial periodic**. *That is, there exist*

(1) *a positive integer m; and*

(2) *a finite set of polynomial functions $f_1, \ldots, f_m\colon \mathbf{R} \to \mathbf{R}$*

such that: if q and r are integers satisfying $q \geq 0$ and $1 \leq r \leq m$, then $f(qm+r) = f_r(q)$.

Proof: This follows immediately from Theorem 10.1 combined with Corollary 11.2. ∎

References

[Ad] S. Adams, *Representation varieties of arithmetic groups and polynomial periodicity of Betti numbers,* Israel Journal of Mathematics, this issue, pp. 73–124.

[B–W] A. Borel and N. Wallach, *Continuous cohomology, discrete groups and representations of reductive groups,* Annals of Math. Studies 94, Princeton University Press, 1976.

[C–R] C. Curtis and I. Reiner, *Methods of Representation Theory,* Wiley, New York, 1981.

[F–T] R.H. Fox and A. Torres, *Dual presentations of the group of a knot,* Annals of Mathematics **59** (1954), 211–218.

[F–1] R. H. Fox, *A quick trip through knot theory,* in *Topology of 3-Manifolds* (M. K. Fort, Jr., ed.), Prentice-Hall, Englewood Cliffs, NJ, 1961.

[F–2] R. H. Fox, *Free differential calculus I, II, III*, Annals of Mathematics **364** (1956), 407–447.

[G–G–P] I. Gelfand, M. Graev and I. Piatetsky–Shapiro, *Representation Theory and Automorphic Functions*, W.B. Saunders, London, 1969.

[G] L. Georite, *Die Bettischen Zahlen der Zyklische Voerlangerung der Knotenauschenraume*, American Journal of Mathematics **56** (1934), 194–198.

[Ha] E. Hironaka, *Ph.D. Thesis*, Brown, 1989.

[Ha2] E. Hironaka, *Polynomial periodicity for Betti numbers of covering surfaces*, Inventiones Mathematicae **108** (1992), 289–321.

[Ha3] E. Hironaka, *Intersection theory on branched covering surfaces and polynomial periodicity*, preprint.

[Hh] F. Hirzebruch, *Arrangements of lines and algebraic surfaces*, in *Arithmetic Geometry*, Vol. II (M. Artin and J. Task, eds.), Birkhäuser, Boston, 1983.

[I] M. N. Ishida, *The irregularities of Hirzebruch's surfaces of general type with $C_1^2 = 3C_2$*, Mathematische Annalen **262** (1983), 407–420.

[Jac] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Co., San Francisco, 1980.

[K] M. Kneser, *Strong approximation*, in *Algebraic Groups*, Proceedings of Symposia in Pure Mathematics **IX** (1966), 187–196.

[L1] S. Lang, *Introduction to Algebraic and Abelian Functions*, Springer–Verlag, Berlin, 1982.

[L2] S. Lang, *Fundamentals of Diophantine geometry*, Springer–Verlag, Berlin, 1983.

[Lt] M. Laurant, *Equations diophantine exponentielles*, Inventiones Mathematicae **78** (1984), 299–327.

[Lr] A. Libgober, *Betti numbers of Abelian covers*, Preprint, 1989.

[Lr2] A. Libgober, *Alexander polynomials of algebraic curves*, Duke Mathematical Journal **49** (1982), 833–851.

[L–M] A. Lubotzky and A. Magid, *Varieties of representations of finitely generated groups*, Memoirs of the American Mathematical Society**58** (1985).

[M–M] J. Mayberry and K. Murasugi, *Torsion groups of Abelian coverings of links*, Transactions of the American Mathematical Society **271** (1982), 143–173.

[P–S] R. Phillips and P. Sarnak, *The spectrum of fermat groups*, Geometry Functional Annalysis **1** (1991), 80–146.

[R–S] D. Ray and I. Singer, *R–torsion and the Laplacian*, Advances in Mathematics **7** (1975), 145–210.

[R] Z. Rudnick, *Representation varieties of solvable groups*, Journal of Pure and Applied Algebra **45** (1987), 261–272.

[Ru] W. Ruppert, *Solving algebraic equations in roots of unity*, Journal für die Reine und Angewandte Mathematik **435** (1992), 119–156.

[Sa] P. Sarnak, *Betti numbers of congruence groups*, preprint.

[S] B. Schoenberg, *Elliptic Modular Functions*, Springer–Verlag, New York, 1974.

[Su] D. Sumners, *On the homology of cyclic coverings of higher dimensional links*, Proceedings of the American Mathematical Society **46** (1974), 143–149.

[Z] O. Zariski, *On the topology of algebraic singularities*, American Journal of Mathematics **54** (1932), 453–465.

Appendix: On Representations of Compact p–adic Groups

Let $\mathcal{G}$ be a Chevally group, $\mathcal{G}(R)$ the corresponding group over the ring of integers R of a p–adic field of characteristic zero. In this note we give an a priori proof of the finiteness of representations of $\mathcal{G}(R)$ in a given dimension; here, as throughout the rest of this note, all representations are assumed to be continuous.

We begin by noting that it suffices to prove this theorem for some normal open subgroup $\Gamma \lhd \mathcal{G}(R)$—since if ρ is any irreducible representation of $\mathcal{G}(R)$, then ρ injects into the induced representation:

$$\rho \hookrightarrow \mathrm{Ind}_{\Gamma}^{\mathcal{G}(R)} \mathrm{Res}_{\Gamma}^{\mathcal{G}(R)} \rho$$

and because $\mathcal{G}(R)/\Gamma$ is a finite group, there are only finitely many possibilities for ρ given its restriction to Γ.

From now on, for simplicity of exposition, I take $\mathcal{G} = \mathrm{SL}(N)$, $R = \mathbf{Z}_p$, the p–adic integers, and $p \neq 2, 3$. Let

$$\Gamma_\ell = \Gamma(p^\ell) = \{\gamma \in \mathrm{SL}(N, \mathbf{Z}_p) | \, \gamma \equiv I \mod p^\ell \mathfrak{sl}(N, \mathbf{Z}_p)\}$$

be the principal congruence subgroup of level p^ℓ; here $\mathfrak{sl}(N, \mathbf{Z}_p)$ is the Lie algebra of $\mathrm{SL}(N, \mathbf{Z}_p)$. We take $\Gamma = \Gamma_1$.

If ρ is a continuous finite dimensional representation of Γ, the **level** ℓ_ρ of ρ is the least integer $\ell \geq 1$ such that ρ is trivial on Γ_ℓ. In this case, ρ factors through the finite group $\Gamma_\ell = \Gamma/\Gamma_\ell$.

The finiteness result will follow from the following estimate:

PROPOSITION A.1: *Let ρ be an irreducible representation of Γ of dimension n and level ℓ. Then*

$$\ell \ll J(n)^{1/\log_2 p} = f(n) \tag{A.1}$$

where $J(n)$ is the index of a normal, Abelian subgroup of $\rho(\Gamma) = \rho(G_\ell)$; $J(n)$ depends only on n, not on ρ.

Indeed, assuming (A.1), any ρ of dimension n will factor through one of a finite number of finite groups, so the number of such representations is finite.

To prove (A.1), we need a couple of lemmas. First, recall that since G_ℓ is a p–group, it is in particular *solvable* (even nilpotent).

LEMMA A.1: *G_ℓ has solvable length given by*

$$\text{length}\,(G_\ell) = [\log_2(\ell - 1)] + 1\,, \qquad \ell \geq 2\,, \tag{A.2}$$

i.e., if $2^{k-1} < \ell \leq 2^k$ then $\text{length}\,(G_\ell) = k$.

Proof: This follows from computing the commutator subgroups of Γ:

$$(\Gamma_k, \Gamma_k) = \Gamma_{2k}\,.$$

The inclusion $(\Gamma_k, \Gamma_k) \subseteq \Gamma_{2k}$ is obvious, and equality follows by applying the Campbell–Baker–Hausdorff formula. It is here that one has to use the exponential

$$\exp : \mathfrak{sl}\,(N, p\,\mathbf{Z}_p) \to \Gamma\,.$$

Recall that the exponential series:

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

is p–adically convergent only for $|x|_p < 1$. ∎

LEMMA A.2: *If ℓ is the level of ρ, and n its dimension, we have*

$$\text{length}\,(G_\ell) \leq 1 + \log_p J\,. \tag{A.3}$$

Proof: First note that since ρ is trivial on Γ_ℓ, but not on $\Gamma_{\ell-1}$, we have

$$\text{length}\,\rho(\Gamma) = \text{length}\,G_\ell\,.$$

However, if $A \lhd \rho(\Gamma)$ is a normal abelian subgroup of index $\leq J$, then:

$$\begin{aligned} \operatorname{length} \rho(\Gamma) &\leq \operatorname{length} A + \operatorname{length} \rho(\Gamma)/A \\ &= 1 + \operatorname{length} \rho(\Gamma)/A \\ &\leq 1 + \log_p J . \qquad \blacksquare \end{aligned}$$

Putting together (A.2) and (A.3), we find:

$$\log_2 p \ll \log_p J$$

which proves (A.1), except that we have to show that J can be taken independent of ρ. This is precisely the content of Jordan's theorem [CR], which asserts that any finite subgroup of $\mathrm{GL}(n, \mathbf{C})$ contains the normal Abelian subgroup of index at most

$$J(n) = (\sqrt{8n}+1)^{2n^2} - (\sqrt{8n}-1)^{2n^2} . \tag{A.4}$$

This proves (A.1). $\blacksquare$

Remark: The estimate (A.4) is very far from the truth; Howe's Theory [H] provides us with a normal Abelian subgroup of index (exactly!) n^2.

References

[CR] C. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras,* Wiley–Interscience, New York, 1962.

[H] R. Howe, *Kirilov theory for compact p–adic groups,* Pacific Journal of Mathematics **73** (1977), 365–381.