ACTA ARITHMETICA
107.1 (2003)

Cohomology sets inside arithmetic groups

by

Stefan Kühnlein (Karlsruhe)

0. Introduction. In [O1], T. Ono calculates the cohomology set $H^1(\langle\theta\rangle, \Gamma(N))$, where $\theta = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{Z})$ and $\Gamma(N)$ is the principal congruence subgroup of some level $N \geq 3$ in $\Gamma := \mathrm{PSL}_2(\mathbb{Z})$. The cardinality of this set is $\frac{1}{2}\#\,\mathrm{SO}_2(\mathbb{Z}/N)$ if N is no multiple of 4, and half of this otherwise. Here, of course, $\mathrm{SO}_2(\mathbb{Z}/N) = \{A \in \mathrm{SL}_2(\mathbb{Z}/N) \mid A^\top A = 1\}$, where $A^\top$ is the transpose of A.

In Ono's paper, everything comes down to using the fact that conjugation with $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ is the same as inversion + transposition in Γ, and the whole result seems to be without a more general perspective.

In this paper we will give another proof of Ono's result and show that in general we will not have to look at orthogonal groups, but rather at the centralizer of θ in the quotient $\Gamma/\Gamma(N)$. In Ono's two-dimensional situation these two groups by accident almost coincide.

Moreover, there is a link between the cardinality of the cohomology set under consideration and ray class groups of cyclotomic fields. This is even more interesting, as the more recent papers [O2] and [O3] of Ono give a similar description of the cohomology sets coming from the action of the Atkin–Lehner involution on $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$.

1. Algebraic aspects. Let Γ be a group, Δ a normal subgroup of Γ, and $\Theta \subset \Gamma$ a subgroup. We want to study the set $H^1(\Theta, \Delta)$, where Θ acts on Δ by conjugation. By definition, $H^1(\Theta, \Delta)$ is the quotient of $Z^1(\Theta, \Delta)$ by the relation $\sim$, where

$$Z^1(\Theta, \Delta) := \{f : \Theta \to \Delta \mid f(st) = f(s)sf(t)s^{-1}\}, \quad \text{and}$$
$$f \sim f' :\Leftrightarrow \exists k \in \Delta : \forall s \in \Theta : f'(s) = k^{-1}f(s)sks^{-1}.$$

Denote by $\mathrm{Hom}_{\Gamma/\Delta}(\Theta, \Gamma)$ the set of group homomorphisms η from Θ to Γ over Γ/Δ (i.e. $\forall\theta \in \Theta : \eta(\theta) \in \theta\Delta$). In our situation, this leads to an "intrinsic" way to describe the torseurs from [S, §5]. We get the following.

2000 *Mathematics Subject Classification*: 11F06, 11R29, 57M12.

1.0. Lemma. *There is a natural bijection between $H^1(\Theta,\Delta)$ and the set of Δ-conjugacy classes in* $\mathrm{Hom}_{\Gamma/\Delta}(\Theta,\Gamma)$, *induced by*

$$Z^1(\Theta,\Delta)\ni f\mapsto\eta\in\mathrm{Hom}_{\Gamma/\Delta}(\Theta,\Gamma),\qquad \text{where } \eta(h):=f(h)h.$$

Proof. For given $f\in Z^1(\Theta,\Delta)$, the corresponding map η commutes with the projection to Γ/Δ; furthermore, it is a homomorphism, as we find

$$\eta(h_1h_2)=f(h_1h_2)h_1h_2=f(h_1)h_1f(h_2)h_1^{-1}h_1h_2=\eta(h_1)\eta(h_2).$$

The rest of the assertion is clear. ∎

From now on we will be interested in the case when $\Theta=\langle\theta\rangle$ is a finite cyclic group of order e inside Γ. We then write $H^1(\theta,\Delta):=H^1(\Theta,\Delta)$. Using Lemma 1.0 we find:

1.1. Lemma. *Let $\theta\in\Gamma$ be an element of finite order e, Δ a normal subgroup of Γ. Then there is a bijection between $H^1(\theta,\Delta)$ and the set of Δ-conjugacy classes of elements of order dividing e in the coset $\Delta\theta$.*

Proof. This follows from 1.0 and the fact that a homomorphism from $\langle\theta\rangle$ to Γ is given by its value at θ. It lies in $\Delta\theta$ if and only if the homomorphism is one over Γ/Δ. ∎

1.2. An interpretation of the cohomology sets can in some situations be given as follows.

If $\kappa(\Gamma,d)$ denotes the number of conjugacy classes in Γ of order d, then

$$\#H^1(\theta,\Gamma)=\sum_{d|e}\kappa(\Gamma,d).$$

If Γ acts properly discontinuously and faithfully on a simply connected space X, then $H^1(\theta,\Delta)$ carries important information on the geometry of the orbifold $\Gamma\backslash X$ which has Γ as its (orbifold-)fundamental group, namely information concerning the fixed points of the action.

Therefore, in contrast to the title of Ono's paper, I would like to associate the cohomology set not to the Riemann surface $S=\Gamma(N)\backslash\mathbb{H}$ itself (where $\mathbb{H}$ is the upper half-plane), but rather to the covering $S\to\widetilde{S}:=\langle\Gamma(N),\theta\rangle\backslash\mathbb{H}$. In Ono's situation, the size of $H^1(\theta,\Delta)$ says how many ramified points for this covering exist.

We get the same information in the following even more classical situation. Let $\Lambda\subset\mathbb{C}$ be a full lattice and let $\varrho=-1$. Then the semidirect product $\Gamma:=\langle\varrho\rangle\ltimes\Lambda$ acts by affine isometries on the euclidean space $\mathbb{C}$. The elliptic curve $\Lambda\backslash\mathbb{C}$ covers the quotient $\Gamma\backslash\mathbb{C}$ which has genus zero. The degree of this covering is 2, and so by Riemann–Hurwitz we get 4 ramified points. These correspond to the conjugacy classes of elements of order 2 in Γ, and so there are four of these. In fact, they are given by $H^1(\langle\varrho\rangle,\Lambda)=\Lambda/2\Lambda$, and the ramified points are the 2-division points of the elliptic curve.

Denote the centralizer of an element h in Γ by $C_\Gamma(h)$. We now study an abstract situation which is very close to the one from Ono's example.

1.3. Lemma. *Let Γ be a group, Δ a normal subgroup of Γ and θ an element in Γ of order e. Suppose further that the order of $\Delta\theta$ in Γ/Δ also is e, that all elements of order e in $\Delta\theta$ are conjugate under Γ, and that $C_\Delta(\theta) := C_\Gamma(\theta) \cap \Delta$ has finite index, say i, in $C_\Gamma(\theta)$. Then*

$$\#H^1(\theta, \Delta) = \frac{1}{i} \# C_{\Gamma/\Delta}(\Delta\theta).$$

Proof. An element of order dividing e in $\Delta\theta$ does have order e, as by the assumption on θ modulo K the order has to be a multiple of e as well. This element can be written as $\gamma\theta\gamma^{-1}$ for some $\gamma \in \Gamma$. The element γ is only defined modulo $C_\Gamma(\theta)$. This leads to $H^1(\theta, \Delta) = (C_\Gamma(\theta)\Delta)\backslash C_{\Gamma/\Delta}(\Delta\theta)$. As $(C_\Gamma(\theta)\Delta)/\Delta \cong C_\Gamma(\theta)/C_\Delta(\theta)$, we get the desired assertion. ∎

NB: The assumption on the order of θ modulo Δ holds if Δ is without torsion. It also holds if $\theta \notin \Delta$ has prime order.

1.4. We apply this and treat the case $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$, $\Delta = \Gamma(N)$ with $N \geq 3$ and θ of order $p \in \{2, 3\}$. The elements of order p in Γ all are conjugate. We therefore get

$$H^1(\theta, \Delta) = \#C_{\Gamma/\Delta}(\Delta\theta)/p,$$

using the fact that $C_\Gamma(\theta) = \langle\theta\rangle$.

In case $p = 2$ and $4 \nmid N$, the centralizer of θ in Γ/Δ turns out to have the same number of elements as $\mathrm{SO}_2(\mathbb{Z}/N\mathbb{Z})$, because it is covered by a subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ which contains $\mathrm{SO}_2(\mathbb{Z}/N\mathbb{Z})$ with index 2. This is Ono's result. Note that for prime $N = \ell$ half of the centralizer of $\theta\Delta$ is rather the unit group $\mathbb{F}_\ell^\times/\{\pm 1\}$ in case $\ell \equiv 1 \bmod 4$ and the group of norm-1-units in $\mathbb{F}_{\ell^2}$ modulo ± 1 otherwise. This gives formula (1.2) in [O1]:

$$\#H^1(\theta, \Gamma(\ell)) = \frac{1}{2}(\ell - (-1)^{(\ell-1)/2}).$$

In case $p = 3, (6, N) = 1$, we get something similar: $\#H^1(\theta, \Delta) = \#\,\mathrm{SO}\left(\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right), \mathbb{Z}/N\mathbb{Z}\right)/3$, and, using the same calculation of the centralizer as above, for prime numbers ℓ different from 2 or 3:

$$\#H^1(\theta, \Gamma(\ell)) = \frac{1}{3}\left(\ell - \left(\frac{3}{\ell}\right)(-1)^{(\ell-1)/2}\right),$$

where $\left(\frac{3}{\ell}\right)$ is the Legendre symbol.

In both examples, orthogonal groups play a part. This is explained by the following well known lemma.

1.5. Lemma. *If Γ acts on some set X, and if the action of Δ is trivial, then $C_{\Gamma/\Delta}(\Delta\theta)$ acts on X^θ, the set of fixpoints of θ on X.* ∎

In particular we find in 1.4 for $p = 2$ that the centralizer of $\theta = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ in $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on the space of θ-invariant quadratic forms of the type $A^\top A$ for $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, which turns out to be a subset of $\left\{\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$, depending on N mod 4. In particular, the centralizer is contained in $\mathrm{GSO}_2(\mathbb{Z}/N\mathbb{Z}) := \left\{A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \mid A^\top A = \pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$, and in fact the centralizer here is the whole GSO_2, which either contains SO_2 with index 2 (if 4 does not divide N) or just is SO_2.

Similar calculations hold in the other example in 1.4. It therefore is fair to say that Ono exploits an exceptional isomorphism between orthogonal groups and unit groups in the two-dimensional situation.

In the general situation, however, the link with quadratic forms is not really essential, as we will see immediately.

2. A more general arithmetic situation. In this section we want to analyse the situation where the finite group $\Theta \subset \mathrm{GL}_n(\mathbb{Z})$ is cyclic and acts irreducibly on $\mathbb{Q}^n$. More concretely, this means the following.

Let e be a natural number, $n = \varphi(e)$ (Euler's φ-function), and θ an element of order e in $\Gamma := \mathrm{GL}_n(\mathbb{Z})$. The matrix θ is a zero of the eth cyclotomic polynomial Φ_e. Let $N \geq 3$ be a natural number and $\Delta = \Gamma(N) \subset \Gamma$ the principal congruence subgroup of level N. It is known that Δ is torsion free.

NB: In principle, this is Ono's situation, despite the fact that he works in PSL_2. In his paper, θ is represented by an element of order 4 in GL_2, which acts irreducibly on $\mathbb{Q}^2$, and $2 = \phi(4)$.

It is well known from [B] that in Γ there are only finitely many conjugacy classes of elements of finite order; therefore, by 1.2, $H^1(\theta, \Gamma)$ is finite. See also the proof of Corollary 2.4 for this finiteness.

2.1. Let us first of all get rid of the suspicion that $H^1(\theta, \Delta)$ could have something to do with orthogonal groups when $n \geq 3$. Namely, if $p \equiv 1 \bmod e$ is a prime number, then the image of θ in $\mathrm{GL}_n(\mathbb{F}_p)$ is conjugate to the diagonal matrix $A := \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, where the entries run through the primitive eth roots of unity in $\mathbb{F}_p$. We sort these in such a way that $\lambda_i \lambda_{n+1-i} = 1$ for all i, and then the quadratic forms on $\mathbb{F}_p^n$ which are A-invariant are the forms given by matrices of the type

$$\begin{pmatrix} 0 & \ldots & 0 & d_1 \\ 0 & 0 & d_2 & 0 \\ 0 & \iddots & 0 & 0 \\ d_n & 0 & \ldots & 0 \end{pmatrix}.$$

The centralizer of A consists of all diagonal matrices, but a general diagonal matrix B will not be in the generalized orthogonal group of any (non-degenerate) quadratic form under consideration. Namely, this holds if

and only if any pair of diagonal entries of B gives the same product, and for this to hold, B must be a multiple of the identity, as $n \geq 3$.

2.2. The centralizer of θ in general will be infinite, as θ generates the ring $\mathbb{Z}[\theta]$ inside the matrix ring $M_n(\mathbb{Z})$, and this is isomorphic to the integer ring $\mathbb{Z}[\zeta_e]$ for a primitive eth root of unity. It intersects Γ in its group of units which (by Dirichlet's unit theorem) is finitely generated of rank $n/2-1$. As the characteristic polynomial of θ is irreducible, it is well known that the centralizer of θ inside the matrix ring $M_n(\mathbb{Q})$ is $\mathbb{Q}[\theta]$. Therefore, $C_\Gamma(\theta) = \mathbb{Z}[\theta]^\times$. As the index of $C_\Delta(\theta)$ in $C_\Gamma(\theta)$ tends to vary very unregularly (cf. [K, Prop. 3.1]), it will not be possible to find a polynomial formula for the cardinality of $H^1(\theta, \Delta)$. To be more concrete, let $e = 5,\ n = 4$. Then $\mathbb{Z}[\zeta]^\times = \langle \pm\zeta, 1+\zeta \rangle$, and this contains the unitgroup $\mathbb{Z}[(1+\sqrt{5})/2]^\times = \langle \pm 1, (1+\sqrt{5})/2 \rangle$. The index of this subgroup is finite (namely 5), and every nice behaviour of the size of $C_\Gamma(\theta)/C_\Delta(\theta)$ would convert into the same kind of behaviour of the order of $(1+\sqrt{5})/2$ modulo p for varying prime numbers p. Now we really are in the situation of *loc. cit.*, where any kind of polynomial regularity of growth was excluded.

On the other hand, if we fix a prime p not dividing e, the Leopoldt conjecture, which holds for abelian extensions of $\mathbb{Q}$ (cf. [W, Cor. 5.32]), says that for large f we will have

$$\#(\mathbb{Z}[\theta]^\times / \Gamma(p^f)) = p^{n/2-1} \#(\mathbb{Z}[\theta]^\times / \Gamma(p^{f-1})),$$

so that for fixed p we have some kind of stabilization for $\#H^1(\theta, \Gamma(p^f))$ as f goes to infinity.

2.3. Theorem. *Let $e \geq 3$ be a natural number, $n = \phi(e)$, $\theta \in \Gamma := \mathrm{GL}_n(\mathbb{Z})$ an element of order e and $\Delta := \Gamma(p)$ the principal congruence subgroup of level p for some prime number $p \geq 3$ not dividing e. Let further ζ be a primitive eth root of unity in $\mathbb{C}$ and i the index of $\Delta \cap \mathbb{Z}[\theta]^\times$ in $\mathbb{Z}[\theta]^\times$. Then*

$$\#H^1(\theta, \Delta) = h_K \, \frac{\#C_{\Gamma/\Delta}(\theta)}{i},$$

where h_K is the class number of the cyclotomic field $K = \mathbb{Q}(\zeta)$. For the centralizer $C_{\Gamma/\Delta}(\theta)$ we find

$$\#C_{\Gamma/\Delta}(\theta) = \frac{2}{p-1}\,(p^o - 1)^{n/o},$$

where o is the (multiplicative) order of p modulo e.

Proof. First of all, the number of conjugacy classes of elements of order e in Γ is the class number h_K, as a given matrix of order e makes $\mathbb{Z}^n$ into a projective $\mathcal{O} = \mathbb{Z}[\zeta]$-module of rank one, and so it is isomorphic to an ideal

in $\mathcal{O}$. Two matrices are conjugate if and only if the ideals are isomorphic as $\mathcal{O}$-modules, which is equivalent to lying in the same ideal class.

All elements of order e in Γ/Δ which come from elements of order e in Γ are conjugate under $\mathrm{GL}_n(\mathbb{F}_p)$, as they share the characteristic polynomial which splits as a product of pairwise distinct irreducible factors over $\mathbb{F}_p$. As the determinant map on $C_{\mathrm{GL}_2(\mathbb{F}_p)}(\theta)$ is still surjective (being the norm on a product of finite fields), the elements are even conjugate under Γ/Δ. This means that every Γ-conjugacy class in Γ of order e has a representative in $\Delta\theta$. For every Γ-conjugacy class in $\Delta\theta$ we get the same decomposition as in Lemma 1.3, and the index i is independent of the conjugacy class, as for any $\widetilde{\theta} \in \Gamma$ of order e we get

$$\mathbb{Z}[\widetilde{\theta}]^\times/(\Gamma(p) \cap \mathbb{Z}[\widetilde{\theta}]^\times) \cong \mathbb{Z}[\zeta_e]^\times/((1+p\mathbb{Z}[\zeta_e]) \cap \mathbb{Z}[\zeta_e]^\times).$$

Now use 1.1.

The assertion on the centralizer is obvious, as $\mathbb{F}_p[\theta]$ is a product of n/o fields of order p^o and we want elements of determinant ± 1. ∎

2.4. Corollary. *Under the conditions of Theorem* 2.3 *let* $\widetilde{h}_{K,p}$ *be the cardinality of the ray class group* Cl_K^p *of* K *with modulus* $p\mathcal{O}$. *Then*

$$\widetilde{h}_{K,p} = \frac{p-1}{2}\,\#H^1(\theta, \Delta).$$

Proof. The cardinality of the centralizer of θ is $(2/(p-1))\#(\mathcal{O}/p\mathcal{O})^\times$. This gives the assertion, due to [N, Kap. VI.2, Aufgabe 13], as the field is totally imaginary. ∎

In view of this corollary it might be interesting to get a somewhat more quantitative idea of the sizes of the cohomology sets. We therefore study an example.

2.5. Example. We go back to the example from 2.2, namely the element θ of order 5 in $\mathrm{GL}_4(\mathbb{Z})$ (there is just one conjugacy class). We get the following table, using the fact that the centralizer of θ in Γ is generated by θ and $1+\theta$ and that—in all cases I did calculate—for every prime number p not dividing 10 the order of $1+\theta$ modulo p is divisible by 10, whence $1+\theta$ generates $C_\Gamma(\theta)/C_\Delta(\theta)$ and the order is the index i.

p	i	o	$\#C_{\Gamma/\Delta}(\theta)$	$\#H^1(\theta,\Delta)$
3	40	4	80	2
7	80	4	800	10
11	10	1	2000	200
13	140	4	4760	34
17	180	4	10440	58
19	90	2	14400	160
23	240	4	25440	106
29	70	2	50400	720

For $p \equiv 1 \bmod 10$ the index i has to divide $p-1$, and $o = 1$, hence $2(p-1)^2 \le \#H^1(\theta, \Delta) \le 2(p-1)^3$. In reality, the index i seems to be a "large" divisor of $p-1$: for $p < 1000$ there are 26 (out of 40) with index $p-1$, seven with index $(p-1)/2$, five with index $(p-1)/3$, one with index $(p-1)/4$, and one with index $(p-1)/13$ (namely 911). The question we are discussing here is the same as the following: let $z_1, \dots, z_4$ be the roots of Φ_5 in $\mathbb{F}_p$. How large is the group generated by $z_1+1, \dots, z_4+1$?

For $p \equiv 9 \bmod 10$ the index i has to divide p^2-1 and turns out to be a large divisor of $10(p-1)/2$. Namely, if $z \in \mathbb{F}_{p^2}$ is a fifth root of unity, then

$$(z+1)^{5(p-1)} = ((z^p+1)/(z+1))^5 = ((z^4+1)/(z+1))^5 = z^{4\cdot 5} = 1.$$

For $p \equiv 2$ or $3 \bmod 5$ the index i is a divisor of $10(p+1)$ (similar calculation as above). Apart from the proof by calculation, this comes from the fact that a subgroup of finite index in the unit group already lies in $\mathbb{Q}(\sqrt{5})$.

Questions/Remarks. (a) Is there anything nice to say about the size of the image of $C_\Gamma(\theta)$ in Γ/Δ? Is there any kind of density result?

(b) Can one use the group generated by θ and Δ (via automorphic forms or Hecke operators on cohomology) in order to construct the corresponding ray class field?

(c) Similar questions may be asked if we replace $\mathrm{GL}_n(\mathbb{Z})$ by $\mathrm{GL}_n(\mathcal{O})$ for some S-arithmetic ring of integers $\mathcal{O}$, and also in the function field situation.

References

[B] A. Borel, *Arithmetic properties of linear algebraic groups*, in: Proceedings ICM Stockholm 1962, Inst. Mittag-Leffler, Djursholm, 1963, 10–22.

[K] S. Kühnlein, *Some families of finite groups and their rings of invariants*, Acta Arith. 91 (1999), 133–146.

[N] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, 1992.

[O1] T. Ono, *On certain cohomology sets attached to Riemann surfaces*, Proc. Japan Acad. Ser. A 76 (2000), 116–117.

[O2] —, *On certain cohomology sets for $\Gamma_0(N)$*, ibid. 77 (2001), 39–41.

[O3] —, *On certain cohomology sets for $\Gamma_0(N)$, II*, ibid. 77 (2001), 108–110.

[S] J.-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Math. 5, Springer, Berlin, 1964.

[W] L. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, New York, 1997.

Mathematisches Institut II der Universität (TH)
D-76128 Karlsruhe, Germany
E-mail: stefan.kuehnlein@mi2.uni-karlsruhe.de

Received on 25.6.2001
and in revised form on 26.8.2002 (4058)