On certain exact sequences for $\Gamma_0(m)$

By Takashi Ono

Department of Mathematics, The Johns Hopkins University, Baltimore, Maryland, 21218-2689, U. S. A.

(Communicated by Shokichi Iyanaga, M. J. A., June 11, 2002)

Abstract: We consider cohomology sets and exact sequences of groups with involutions. In particular,we study congruence subgroups of type $\Gamma_0(m)$ which are acted by the group generated either by the map $z \mapsto (-1/mz)$ of the upper half plane or by the map $x \mapsto (1/mx)$ of the set of irrational real numbers.

Key words: Congruence subgroups of level m; involutions; cohomology sets; quadratic fields; Pell's equations; ideal class groups.

1. Groups with involutions. Let G be a group and $*$ be an involution on it: $(ab)^* = b^*a^*$, $a^{**} = a$, $a, b \in G$. Consider the subgroup of unitary elements of G

$$\mathcal{U}(G) := \{a \in G;\ a^*a = 1\}$$

and a subset of symmetric elements of G

$$\mathcal{S}(G) := \{a \in G;\ a^* = a\}.$$

The group G acts on $\mathcal{S}(G)$ to the right: $a \mapsto a \circ g := g^*ag$. We denote the orbit space of this action by

$$\mathcal{H}(G) := \mathcal{S}(G)/G.$$

The orbit $1_G \circ G$ is the origin of the space $\mathcal{H}(G)$.

Let G' be another group with an involution $*$. A homomorphism $G \to G'$ commuting with involutions induces following maps with obvious nice properties:

$$\mathcal{U}(G) \to \mathcal{U}(G'),\ \ \mathcal{S}(G) \to \mathcal{S}(G'),\ \ \mathcal{H}(G) \to \mathcal{H}(G').$$

Now let N be a normal subgroup of G stable under an involution $*$ of $G : N^* = N$. Then one can speak of an involution $*$ of $G/N : (aN)^* = a^*N$. The short exact sequence

$$1 \to N \longrightarrow G \longrightarrow G/N \to 1$$

induces naturally the exact sequence of spaces with origins:

$$\begin{aligned} 1 \longrightarrow \mathcal{U}(N) \longrightarrow \mathcal{U}(G) \longrightarrow \mathcal{U}(G/N) \xrightarrow{\delta} \mathcal{H}(N) \\ \longrightarrow \mathcal{H}(G) \longrightarrow \mathcal{H}(G/N), \end{aligned}$$

where the map δ is given by

$$\mathcal{U}(G/N) \ni aN \mapsto (a^*a) \circ N \in \mathcal{H}(N).$$

The exactness can be checked easily. [If one lets the group $g = \langle\, s\, \rangle$ of order 2 act on a group G with $*$ by $a^s = a^{-*} := (a^*)^{-1}$, then the exactness follows from a basic theorem of nonabelian cohomology ([3]). In case of involutions, however, one needs only geometric language like *orthogonality* and *symmetry* instead of *cocycles* etc.]

Every group G has a built-in involution $\iota : a \mapsto a^{-1}$. Any involution $*$ of G can be written $* = \sigma\iota$ with an automorphism σ of G. For that matter, any pair (α, β) of involutions of a group determines an automorphism σ so that $\alpha = \sigma\beta$.

2. Groups $\boldsymbol{\Gamma_\nu(m)}$. Here is a scenario where G is a group of matrices whose involution $*$ is closely related to the transposition of matrices. To be more precise, let R be a subring of a field Ω containing $1 = 1_\Omega$. Consider a matrix $U \in \mathrm{GL}_n(\Omega)$ and a subgroup $G \subset \mathrm{SL}_n(R)$ such that

$$U^t = U, \quad U^{-1}GU = G^t := \{A^t : A \in G\}.$$

Then we set

$$A^* = UA^tU^{-1}, \quad A \in G.$$

Since the map $A \mapsto A^*$ is an involution of G, we can speak of $\mathcal{U}(G)$, $\mathcal{S}(G)$ and $\mathcal{H}(G)$ as in Section 1.

Now, let $R = \mathbf{Z}, \Omega = \mathbf{Q}$ and $n = 2$. For a nonzero integer m and an integer $\nu \geq 0$ we set

$$\Gamma_\nu(m) = \left\{ A = \begin{bmatrix} a & b \\ mc & d \end{bmatrix};\ a, b, c, d \in \mathbf{Z}, \right.$$
$$\left. \det A = 1,\ a^\nu \equiv 1 \pmod m \right\}.$$

Note that, when $m > 0$, $\Gamma_0(m)$, $\Gamma_1(m)$ are compatible with the conventional notation for congruence groups. Each $\Gamma_\nu(m)$ is normal in $\Gamma_0(m)$. Needless

2000 Mathematics Subject Classification. 11F75.

to say, the group $\Gamma_\nu(m)$ depends only on the class of ν modulo $\varphi(|m|)$. As for the matrix U, we put

$$U = \begin{bmatrix} 1 & 0 \\ 0 & -m \end{bmatrix} \in \mathrm{GL}_2(\mathbf{Q}).$$

Then, we find that

$$U^{-1}\Gamma_\nu(m)U = \Gamma^\nu(m) := \Gamma_\nu(m)^t.$$

Consequently

$$A \mapsto A^* = UA^tU^{-1} = \begin{bmatrix} a & -c \\ -mb & d \end{bmatrix}$$

defines an involution of $\Gamma_\nu(m)$.

Here are descriptions of $\mathcal{U}(G)$, $\mathcal{S}(G)$, $\mathcal{H}(G)$ for $G = \Gamma_\nu(m)$.

(i) $\mathcal{U}(\Gamma_\nu(m))$. One verifies that

$$\mathcal{U}(\Gamma_\nu(m)) = \left\{ A = \begin{bmatrix} a & b \\ mb & a \end{bmatrix}, \quad a^2 - mb^2 = 1,\ a^\nu \equiv 1 \pmod{m} \right\}.$$

So if $m < 0$ or square, $\mathcal{U}(\Gamma_\nu(m))$ is a finite group and if $m > 0$ and nonsquare, it is an infinite group isomorphic to the group of Pell's equation $a^2 - mb^2 = 1$ (ν even) or its subgroup with $a \equiv 1 \pmod{m}$ (ν odd).

(ii) $\mathcal{S}(\Gamma_\nu(m))$. One verifies that

$$\mathcal{S}(\Gamma_\nu(m)) = \left\{ A = \begin{bmatrix} a & b \\ -mb & d \end{bmatrix}, \quad ad + mb^2 = 1,\ a^\nu \equiv 1 \pmod{m} \right\}.$$

(iii) $\mathcal{H}(\Gamma_\nu(m)) = \mathcal{S}(\Gamma_\nu(m))/\Gamma_\nu(m) = \{A \circ \Gamma_\nu(m)\}$, where $A \circ T = T^*AT$, $A \in \mathcal{S}(\Gamma_\nu(m))$, $T \in \Gamma_\nu(m)$.

3. A reduction theorem. As an application of the exact sequence in Section 1, we shall prove a theorem on the group $\Gamma_\nu(m)$ introduced in Section 2. Let us start with a short exact sequence:

$$1 \to N \longrightarrow G \longrightarrow G' \to 1$$

where $G = \Gamma_0(m)$, $N = \Gamma_\nu(m)$, $G' = ((\mathbf{Z}/m\mathbf{Z})^\times)^\nu$. The involution $*$ introduced in Section 2 for G induces the one on the normal subgroup N and so on $G/N \approx G'$. We have

$$\mathcal{U}(G') = \{\alpha \in G' : \alpha^2 = 1\},$$
$$\mathcal{S}(G') = G', \quad \mathcal{H}(G') = G'/(G')^2$$

and the exact sequence

$$1 \longrightarrow \mathcal{U}(N) \xrightarrow{\beta} \mathcal{U}(G) \xrightarrow{\gamma} \mathcal{U}(G') \xrightarrow{\delta} \mathcal{H}(N) \xrightarrow{\epsilon} \mathcal{H}(G) \xrightarrow{\eta} \mathcal{H}(G').$$

By the reduction we mean to find an N so that $\beta : \mathcal{U}(N) \cong \mathcal{U}(G)$ and $\epsilon : \mathcal{H}(N) \cong \mathcal{H}(G)$. As for $\mathcal{U}$, the matter is trivial because

$$\mathcal{U}(N) \cong \mathcal{U}(G) \Longleftrightarrow \nu \equiv 0 \pmod{2}.$$

So we will search even ν so that $\mathcal{H}(N) \cong \mathcal{H}(G)$. Actually it turns out that the choice

$$\nu = 2^g, \quad \text{with} \quad \varphi(|m|) = 2^g \cdot h, \quad h \equiv 1 \pmod{2}$$

is good to make ϵ bijective. [Note that $g = 0$ only when $m = \pm 1$, or ± 2 and the matter is trivial in these cases.]

(i) ϵ is *injective*. By definition, $\epsilon : \mathcal{H}(N) \to \mathcal{H}(G)$ is given by

$$A \circ N \mapsto A \circ G, \quad A = \begin{bmatrix} a & b \\ -mb & d \end{bmatrix},$$
$$ad + mb^2 = 1, \quad a^\nu \equiv 1 \pmod{m}.$$

So we need to show that, for $A, A' \in \mathcal{S}(N)$, $A' \circ G = A \circ G$ implies $A' \circ N = A \circ N$. Now the assumption means that

$$A' = T^*AT, \quad T = \begin{bmatrix} t & u \\ mv & w \end{bmatrix}, \quad tw - muv = 1.$$

Reducing the relation $T^*A = A'T^{-1}$ modulo m, we find $ta \equiv wa' \pmod{m}$ where a' is the $(1,1)$ component of A'. Since $a^\nu \equiv a'^\nu \equiv 1 \pmod{m}$ we have $t^\nu \equiv w^\nu \pmod{m}$. We have also $t^{2\nu} \equiv 1 \pmod{m}$. As $\varphi(m) = \nu \cdot h$ with h odd, we conclude that $t^\nu \equiv 1 \pmod{m}$, which means that $T \in N$, q.e.d.

(ii) ϵ is *surjective*. Since $\operatorname{Im}\epsilon = \operatorname{Ker}\eta$ it is enough to prove that η is trivial. In other words, having

$$A = \begin{bmatrix} a & b \\ -mb & d \end{bmatrix}, \quad ad + mb^2 = 1, \quad A \in \mathcal{S}(G)$$

in mind, we shall show that:

For any $a \in \mathbf{Z}$, $(a, m) = 1$, there is an integer x so that $a^\nu \equiv x^{2\nu} \pmod{m}$.

In fact, one reduces the proof of this to the case where $|m| = p^e$ a power of a prime p. If $p = 2$, then $\varphi(2^e) = 2^{e-1} = \nu$, with $h = 1$, i.e., $N = G$ and the matter is trivial. If $p \neq 2$, then, with a primitive root r modulo p^e, write $a \equiv r^\alpha \pmod{p^e}$, $x \equiv r^\xi \pmod{p^e}$. Then one has to solve

$$\nu\alpha \equiv 2\nu\xi \pmod{\varphi(p^e)}.$$

As $\varphi(p^e) = p^{e-1}(p-1) = \nu h$, h odd, *where* $\nu = 2^g$, *with* $g \geq e$, we are reduced to solve

$$\alpha \equiv 2\xi \pmod{h}$$

which has certainly a solution because h is odd, q.e.d.

Summing up our arguments:

Theorem. *Notation being as in Section* 3, *let* $\varphi(|m|) = 2^g h$, *h odd. Then*

$$\mathcal{U}(\Gamma_0(m)) \cong \mathcal{U}(\Gamma_{2^g}(m)), \quad \mathcal{H}(\Gamma_0(m)) \cong \mathcal{H}(\Gamma_{2^g}(m)).$$

4. Certain real quadratic fields. To avoid technical complications, we shall assume from now on that m is a positive squarefree integer such that $m \equiv 3 \pmod 4$. Let $k = \mathbf{Q}(\sqrt{m})$, the quadratic field corresponding to m. Since $m \equiv 3 \pmod 4$, $1, \sqrt{m}$ form the standard basis of the ring $\mathfrak{o}_k$ of integers of k with the discriminant $4m$. The assumption implies also that the group $\mathfrak{o}_k{}^\times$ of units of k is identical with the solutions of Pell's equation $x^2 - my^2 = 1$. Denote by H_k^+ the ideal class group in the narrow sense of k. There is a well-known bijection

$$\begin{aligned} &i_k : H_k^+ \cong \Phi(4m)/\operatorname{SL}_2(\mathbf{Z}), \\ &\Phi(4m) := \{f = ax^2 + bxy + cy^2; \\ &\qquad\qquad a, b, c \in \mathbf{Z},\ b^2 - 4ac = 4m\}. \end{aligned}$$

Now back to materials in Section 2, for the integer m above, put

$$U = \begin{bmatrix} 1 & 0 \\ 0 & -m \end{bmatrix}, \quad A = \begin{bmatrix} a & b \\ mc & d \end{bmatrix} \in \Gamma_0(m),$$
$$A^* = UA^tU^{-1}.$$

Then we have three sets

$$\mathcal{U}(\Gamma_0(m)), \quad \mathcal{S}(\Gamma_0(m)), \quad \mathcal{H}(\Gamma_0(m)).$$

First of all, we have $\mathcal{U}(\Gamma_0(m)) \cong \mathfrak{o}_k{}^\times$.

Next, observe that there is a map from $*$-symmetric matrices to quadratic forms: $\mathcal{S}(\Gamma_0(m)) \longrightarrow \Phi(4m)$ defined by

$$\mathcal{S}(\Gamma_0(m)) \ni A = \begin{bmatrix} a & b \\ -mb & d \end{bmatrix}$$
$$\mapsto AU : ax^2 - 2mbxy - mdy^2 \in \Phi(4m).$$

This map then induces a *bijection*:

$$\pi : \mathcal{H}(\Gamma_0(m)) \cong H_k{}^+.$$

The proof of this important fact on real quadratic fields follows *mutatis mutandis* from that of theorems on imaginary quadratic fields in [1, 2].

5. $\boldsymbol{\Gamma_0(\ell)}$ and $\boldsymbol{\Gamma_1(\ell)}$. The reduction theorem in Section 3 cannot compare $\Gamma_0(m)$ with $\Gamma_1(m)$ except $m = \pm 1, \pm 2$. Here we shall compare their $\mathcal{U}$ and $\mathcal{H}$ in a special case. So let ℓ be a prime $\equiv 3 \pmod 4$. Let $k = \mathbf{Q}(\sqrt{\ell})$. As for $\mathcal{U}$, we have

$$\mathcal{U}(\Gamma_0(\ell)) \cong \mathfrak{o}_k{}^\times.$$

By definition

$$\Gamma_1(\ell) = \left\{ A = \begin{bmatrix} a & b \\ \ell c & d \end{bmatrix},\ a \equiv 1 \pmod{\ell} \right\} \subset \Gamma_0(\ell).$$

Hence, from (i) in Section 2, we have

$$\begin{aligned} &\mathcal{U}(\Gamma_1(\ell)) \\ &\quad \cong \{(a, b) \in \mathbf{Z}^2;\ a^2 - \ell b^2 = 1,\ a \equiv 1 \pmod{\ell}\}. \end{aligned}$$

If (a, b), a solution to the Pell's equation, is such that $a \equiv -1 \pmod{\ell}$, then $(-a, -b)$ is one in the subgroup $\mathcal{U}(\Gamma_1(\ell))$. This means that

$$\mathcal{U}(\Gamma_0(\ell)) \cong \mathbf{Z}/2\mathbf{Z} \times \mathcal{U}(\Gamma_1(\ell)).$$

As for $\mathcal{H}$, using the Legendre character $a \mapsto (a/\ell)$, we split the set $\mathcal{S}(\Gamma_0(\ell))$ into two disjoint parts:

$$\mathcal{S}(\Gamma_0(\ell)) = \mathcal{S}^+(\Gamma_0(\ell)) \cup \mathcal{S}^-(\Gamma_0(\ell)),$$

$$\begin{aligned} &\mathcal{S}^\pm(\Gamma_0(\ell)) \\ &\quad = \left\{ A = \begin{bmatrix} a & b \\ -\ell b & d \end{bmatrix} \in \mathcal{S}(\Gamma_0(\ell)), \left(\frac{a}{\ell}\right) = \pm 1 \right\}. \end{aligned}$$

Since $(at^2/\ell) = (a/\ell)$, $a, t \in (\mathbf{Z}/\ell\mathbf{Z})^\times$, we see easily that $\mathcal{S}^\pm(\Gamma_0(\ell))$ are stable under the action of $\Gamma_0(\ell)$. Consequently, we obtain the following natural splitting:

$$\mathcal{H}(\Gamma_0(\ell)) = \mathcal{H}^+(\Gamma_0(\ell)) \cup \mathcal{H}^-(\Gamma_0(\ell)),$$
$$\text{where} \quad \mathcal{H}^\pm(\Gamma_0(\ell)) := \mathcal{S}^\pm(\Gamma_0(\ell))/\Gamma_0(\ell).$$

For $a \in (\mathbf{Z}/\ell\mathbf{Z})^\times$ we have

$$\left(\frac{-a}{\ell}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{a}{\ell}\right) = -\left(\frac{a}{\ell}\right)$$

because $\ell \equiv 3 \pmod 4$. Therefore $A \in \mathcal{S}^+(\Gamma_0(\ell))$ if and only if $-A \in \mathcal{S}^-(\Gamma_0(\ell))$. Hence $\sharp\mathcal{H}^+(\Gamma_0(\ell)) = \sharp\mathcal{H}^-(\Gamma_0(\ell))$. The basic bijection π in Section 4 implies that $\sharp\mathcal{H}(\Gamma_0(\ell)) = \sharp H_k{}^+ = h_k{}^+$. If we put $h_k = \sharp H_k$, then we have $h_k{}^+ = 2h_k$ when $\ell \equiv 3 \pmod 4$. Consequently we obtain

$$\sharp\mathcal{H}^+(\Gamma_0(\ell)) = h_k.$$

Since $(a/\ell) = 1$ when $a \equiv 1 \pmod{\ell}$, we have $\mathcal{S}(\Gamma_1(\ell)) \subset \mathcal{S}^+(\Gamma_0(\ell))$. This induces naturally the following map

$$\epsilon^+ : \mathcal{H}(\Gamma_1(\ell)) \longrightarrow \mathcal{H}^+(\Gamma_0(\ell)).$$

We claim that ϵ^+ is *bijective*.

(i) ϵ^+ is *injective*. Let

$$A = \begin{bmatrix} a & b \\ -\ell b & d \end{bmatrix}, \quad A' = \begin{bmatrix} a' & b' \\ -\ell b' & d' \end{bmatrix}$$

be matrices in $\mathcal{S}(\Gamma_1(\ell))$ such that

$$A' = T^* A T, \quad T = \begin{bmatrix} t & u \\ \ell v & w \end{bmatrix} \in \Gamma_0(\ell).$$

Reducing the relation $T^* A = A' T^{-1}$ modulo ℓ, we obtain $t \equiv w \pmod{\ell}$ since $a \equiv a' \equiv 1 \pmod{\ell}$. On the other hand, we have $tw - \ell uv = 1$, so $tw \equiv 1 \pmod{\ell}$. Hence $t^2 \equiv 1 \pmod{\ell}$ or $t \equiv \pm 1$. If $t \equiv -1 \pmod{\ell}$, then, on replacing T by $-T$, we can assume that $t \equiv 1 \pmod{\ell}$. This means $T \in \Gamma_1(\ell)$; in other words, ϵ^+ is injective.

(ii) ϵ^+ is *surjective*.

Take a matrix

$$A = \begin{bmatrix} a & b \\ -\ell b & d \end{bmatrix} \in \mathcal{S}^+(\Gamma_0(\ell)).$$

We should find an $A' \in \mathcal{S}(\Gamma_1(\ell))$ so that $A' = T^* A T$ for some $T \in \Gamma_0(\ell)$. Now, by the assumption on A, there is a $t \in (\mathbf{Z}/\ell\mathbf{Z})^\times$ such that $at^2 \equiv 1 \pmod{\ell}$. Next, find u, w so that $tw - \ell u = 1$ and put

$$T = \begin{bmatrix} t & u \\ \ell & w \end{bmatrix} \in \Gamma_0(\ell).$$

Then we find

$$\begin{aligned} T^* A T &\equiv \begin{bmatrix} t & -1 \\ 0 & w \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} t & u \\ 0 & w \end{bmatrix} \\ &\equiv \begin{bmatrix} at^2 & * \\ 0 & * \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{\ell}, \end{aligned}$$

i.e., $T^* A T = A' \in \Gamma_1(\ell)$, q.e.d.

Summarizing, we have proved

Theorem. *Let ℓ be a prime $\neq 2$, $\equiv 3 \pmod 4$, $k = \mathbf{Q}(\sqrt{\ell})$ and h_k the class number of k. Then we have*

$$\sharp\mathcal{H}(\Gamma_1(\ell)) = h_k.$$

References

[1] Ono, T.: On certain cohomology set for $\Gamma_0(N)$. Proc. Japan Acad., **77A**, 39–41 (2001).

[2] Ono, T.: On certain cohomology set for $\Gamma_0(N)$. II. Proc. Japan Acad., **77A**, 108–110 (2001).

[3] Serre, J.-P.: Galois Cohomology. Springer-Verlag, Berlin-Heidelberg-New York (1997).