A note on Poincaré sums for finite groups

By Takashi Ono

Department of Mathematics, The Johns Hopkins University, Baltimore, Maryland 21218-2689, U. S. A.
(Communicated by Shokichi Iyanaga, M. J. A., April 14, 2003)

Abstract: A simple and beautiful idea of Poincaré on Poincaré series in automorphic functions can be applied to an arbitrary ring R acted by a group G. When G is finite, the key is to look at the 0-dimensional Tate cohomology of (G, R) twisted by the 1-cohomology class of the group of units of R. As a simplest case, we examine when R is the ring of integers of a quadratic field.

Key words: Finite group; cohomology set; cohomology group; Poincaré sum; quadratic field.

1. Introduction. Let R be the ring of holomorphic functions on the upperhalf plane and G be a modular group. The action of G on the ring R and on the group $R^\times$ of units enables one to speak of the the space M_c of modular forms belonging to a cocycle c (a weight) of the G-group $R^\times$. Poincaré constructed the subspace P_c of Poincaré series and showed that $M_c = P_c$ for many important cases. Since this story is quite algebraic, it is natural to generalize Poincaré's construction starting from arbitrary ring R acted by a group G. As a simplest case, I examined the case where R is the ring of integers of a quadratic field acted by the Galois group of order two. In this case the group M_c/P_c is of order 1 or 2, but even here it's determination for real quadratic fields seems to be a nontrivial question. (See [3] for Poincaré sums attached to Galois representations).

2. $\boldsymbol{H^1(G, R^\times)}$. Let G be a finite group, R a ring and $R^\times$ the group of units of R. We assume that G acts on the ring R to the left: $a \mapsto {}^s a$, $s \in G$, $a \in R$. Then G acts naturally on the group $R^\times$ and we can speak of the cohomology set $H^1(G, R^\times)$. A 1-cocycle is a map $c : G \to R^\times$ such that

$$c_{st} = c_s {}^s c_t, \quad s, t \in G.$$

We denote by $Z^1(G, R^\times)$ the set of all 1-cocycles. Two cocycles c, c' are equivalent: $c \sim c'$ if there is an element $u \in R^\times$ such that

$$c'_s = u^{-1} c_s {}^s u, \quad s \in G.$$

The cohomology set is, by definition,

$$H^1(G, R^\times) = Z^1(G, R^\times)/\sim.$$

We shall denote by $[c]$ the cohomology class containing a cocycle c. The trivial class $[1]$ consists of c's such that $c_s = u^{-1} {}^s u$, $u \in R^\times$.

3. $\boldsymbol{M_c}$ and $\boldsymbol{P_c}$. To each cocycle $c \in Z^1(G, R^\times)$, we set

$$M_c = \{a \in R;\ c_s {}^s a = a, \quad s \in G\},$$

$$P_c = \Big\{p_c(x) := \sum_{t \in G} c_t {}^t x, \quad x \in R\Big\}.$$

M_c, P_c are $\mathbf{Z}$-modules in the ring R. The definition of cocycles implies that

$$|G| M_c \subseteq P_c \subseteq M_c.$$

Here the first inequality follows from the equality:

$$p_c(a) = |G| a, \quad \text{when} \quad a \in M_c.$$

If, in particular, $|G| 1_R$ is invertible in R then we have

$$P_c = M_c \quad \text{for any cocycle} \quad c \in Z^1(G, R^\times).$$

4. $\boldsymbol{M_c/P_c}$. We shall verify that the structure of the $|G|$-torsion module M_c/P_c depends only on the cohomology class $[c] \in H^1(G, R^\times)$. So let $c' \sim c$, i.e.,

$$c'_s = u^{-1} c_s {}^s u, \quad u \in R^\times.$$

Then one verifies that

$$uM_{c'} = M_c, \quad uP_{c'} = P_c. \tag{4.1}$$

Consequently, we find that the quotient module M_c/P_c depends only on the class $[c]$. If, in particular, $c \sim 1$, then we have

$$M_c/P_c = M_1/P_1 = R^G/N_G R = \widehat{H}^0(G, R).$$

2000 Mathematics Subject Classification. 11F75.

In general, for any $\gamma = [c] \in H^1(G, R^\times)$, we can modify the above interpretation in the following way.

5. $\widehat{H}^0(G,R)_\gamma$. Using a cocycle $c \in Z^1(G, R^\times)$, we introduce a new G-module $(G, R)_c$ by

$$^{s'}a = c_s{}^s a, \quad s \in G.$$

Denote by G' the group G with this new action on R. Then we have

$$M_c = \{a \in R; c_s{}^s a = a\} = \{a \in R; {}^{s'}a = a\} = R^{G'},$$

$$P_c = \Big\{p_c(x) = \sum_{t\in G} c_t{}^t x, \quad x \in R\Big\}$$
$$= \Big\{\sum_{t'\in G'} {}^{t'}x\Big\} = N_{G'}R.$$

Hence

$$M_c/P_c = \widehat{H}^0(G, R)_c.$$

In view of (4.1), we have a G-module isomorphism $(G, R)_c \approx (G, R)_{c'}$. So the G-module (class) $(G, R)_\gamma$, $\gamma = [c] \in H^1(G, R^\times)$ makes sence.

In other words, we have

$$M_c/P_c = \widehat{H}^0(G, R)_\gamma, \quad \gamma = [c] \in H^1(G, R^\times).$$

6. Quadratic fields. Let m be a square free integer, $K = \mathbf{Q}(\sqrt{m})$ the quadratic field and $R = \mathsf{O}_K$ the ring of integers of K. Let $G = \mathrm{Gal}(K/\mathbf{Q})$ be generated by the automorphism s of order 2. G acts naturally on R and the group $R^\times$ of units of K. Let us first list the structure of the group $H^1(G, R^\times)$:

$$\mathbf{Z}/2\mathbf{Z} \text{ if } m < 0 \text{ or } m > 0 \text{ with } N\varepsilon = -1,$$

and

$$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \text{ if } m > 0 \text{ with } N\varepsilon = 1,$$

where (and from now on) ε means the fundamental unit of K when $m > 0$. As for cocycles c representing the cohomology group, we can choose the following:

$$c = 1, i \text{ if } m = -1, \ c = \pm 1 \text{ if } m < -1$$
$$\text{or } m > 0 \text{ with } N\varepsilon = -1,$$
$$c = \pm 1 \text{ or } \pm\varepsilon \text{ if } m > 0 \text{ with } N\varepsilon = 1.$$

As G is cyclic (of order 2) we may identify a cocycle $c : G \to R^\times$ with a unit $c \in R^\times$ with $Nc = 1$. To each such c, we have a module

$$M_c = \{\alpha \in R; \ c^s\alpha = \alpha\}$$

and its submodule

$$P_c = \{p_c(z) := z + c^s z, \quad z \in R\}$$

such that the quotient M_c/P_c is a 2-torsion group. As we saw, this group depends only on the class $\gamma = [c] \in H^1(G, R^\times)$ and can be considered as a group $\widehat{H}^0(G, R)_\gamma$, a twisted Tate group.

To describe the structure of groups M_c/P_c, we set following notations:

$$\omega = \sqrt{m} \text{ or } \frac{1+\sqrt{m}}{2}$$

for standard integral basis 1, ω for R,

$$c = u + v\omega, \ u, v \in \mathbf{Z} \text{ for a cocycle } c,$$

and

$$\alpha = a + b\omega, \quad z = x + y\omega, \quad \alpha, z \in R.$$

Here are some basic relations. First of all, for a cocycle c, we have

$$(6.1) \qquad 1 = Nc = u^2 + v^2 N\omega + uvT\omega$$

where T means the trace. We find it convenient to put

$$(6.2) \qquad t = uT\omega + vN\omega.$$

Then we can rewrite (6.1) as

$$(6.3) \qquad 1 - u^2 = tv.$$

Using (6.2), we find that

$$(6.4) \quad \alpha \in M_c \Longleftrightarrow a(1-u) = bt \text{ and } av = b(u+1)$$

and

$$(6.5) \quad z + c^s z = (1+u)x + ty + (vx + (1-u)y)\omega.$$

Notice, by (6.3), that the second equality in (6.4) implies the first one whenever $v \neq 0$. If $v = 0$, then (6.3) implies that $u = \pm 1$. In other words $c = \pm 1$, and $\alpha \in M_c$ means α is symmetric or antisymmetric with respect to the involution s. In this case one verifies that

$$(6.6) \quad \frac{M_c}{P_c} = \begin{cases} 0 & \text{when } m \equiv 1 \pmod 4, \\ \mathbf{Z}/2\mathbf{Z} & \text{otherwise.} \end{cases}$$

Now back to the more interesting case $v \neq 0$, let us put

$$(6.7) \qquad A = (1+u)x + ty.$$

$$(6.8) \qquad B = vx + (1-u)y.$$

Then one verifies that

$$(6.9) \qquad vA = (1+u)B.$$

As we assume that $v \neq 0$, we have from (6.9)

$$A + B\omega = \frac{B}{v}((1+u) + v\omega),$$

and hence, in view of (6.3), (6.5), (6.8), (6.9), we find that

$$M_c \approx \{(a,b) \in \mathbf{Z}^2;\ av = b(u+1)\}$$

$$P_c \approx \{(A,B) \in \mathbf{Z}^2;\ Av = B(u+1),\ d\,|B\},$$
$$d = (v, u-1).$$

In other words, if we put $e = (v, u+1)$ and define C, D by $u+1 = Ce$, $v = De$, then we find that

$$M_c = D\mathbf{Z} \supseteq P_c = D\mathbf{Z} \cap d\mathbf{Z}$$

and we end up with the isomorphism

$$\frac{M_c}{P_c} \approx \frac{\mathbf{Z}}{d/(D,d)\mathbf{Z}}. \tag{6.10}$$

7. Comments. Since M_c is $\mathbf{Z}$-free of rank 1 and (M_c/P_c) is 2-torsion, the index $[M_c : P_c]$ in (6.10) is either 1 or 2. Our problem is to determine it in terms of the quadratic field k. In view of the structure of $H^1(G, R^\times)$, it is enough to consider cocycles of the form $c = \pm\epsilon$ of real quadratic field with $N\epsilon = 1$. In fact, one verifies easily that the index is unchanged if c is replaced by $-c$.

I owe Seok-Min Lee [2] the determination of the index

$$\Delta_m = [M_\epsilon : P_\epsilon], \quad k = \mathbf{Q}(\sqrt{m}), \quad \text{with} \quad m < 1000.$$

His table seems to support the following conjectural statement:

$$\text{(i)} \qquad m \equiv 1 \pmod 4 \ \Rightarrow \Delta_m = 1,$$
$$\text{(ii)} \qquad m \equiv 2 \pmod 4 \ \Rightarrow \Delta_m = 2.$$

As for the remaining case $m \equiv 3 \pmod 4$, both values 1 and 2 occur; they begin as follows:

$$\Delta_m = 1 \ \text{ for } \ m = 3, 7, 11, 15, 19, 23, 31, 35, 43, 47, 51, 59, 67, 71, 79, 83, 87, 91, 103,$$

$$\Delta_m = 2 \ \text{ for } \ m = 39, 55, 95, 111, 155, 183, 203, 259, 295, 299, 327, 355, 371, 395.$$

As you see, the second case appears much less frequently.

References

[1] Gunning, R. C.: Lectures on modular forms. Annals of Mathematics Studies, no. 48, Princeton University Press, Princeton (1962).

[2] Lee, S. M.: A Table of Δ_m. Feb. 20, (2003). (Personal letter).

[3] Ono, T.: A note on Poincaré sums of Galois representations. I. Proc. Japan Acad., **67A**, 145–147 (1991); A note on Poincaré sums of Galois representations. II. Proc. Japan Acad., **67A**, 240–242 (1991); A note on Poincaré sums of Galois representations. III. Proc. Japan Acad., **67A**, 274–277 (1991).