GENERALIZED BERNOULLI NUMBERS AND THE THEORY OF CYCLOTOMIC FIELDS

BY

ROBERT SEGAL

Massachusetts Institute of Technology, Cambridge, Mass., U.S.A.
Rutgers, the State University, New Brunswick, N.J., U.S.A. (1)

Let p be a fixed odd prime. Let $q=p^m$, for some fixed integer $m\geqslant 1$. Let ζ be a primitive qth root of unity. Let G be the Galois group of the cyclotomic field of the qth roots of unity over the rational field, Q. Let $\mathfrak{R}$ (**R**) be the group ring of G over the rational integers (the rational p-adic integers, Z_p).

The main idea of the first part of this paper is a generalization of Iwasawa's work [3] on the group index of certain additive sub-groups of $\mathfrak{R}$ (**R**). The main result of this part is contained in the Corollary to Proposition 3, namely:

If $\sigma(a)\in G$ be such that $\sigma(a)(\zeta)=\zeta^a$, and if $B_n(x)=n$th Bernoulli polynomial, then let

$$\omega_n=\sum_a q^{n-1}B_n(a/q)\,\sigma(a)^{-1}\quad(0\leqslant a<q,\ (a,p)=1).$$

ω_n is an element of the group algebra of G over the p-adic number field. Let

$$\mathbf{I}_n^+=(\sigma(1)+\sigma(-1))\,\mathbf{R}\cap\mathbf{R}\omega_n\quad(n\text{ even})$$

$$\mathbf{I}_n^-=(\sigma(1)-\sigma(-1))\,\mathbf{R}\cap\mathbf{R}\omega_n\quad(n\text{ odd});$$

then,

$$[\mathbf{R}^+:\mathbf{I}_n^+]=q\cdot[p\text{th part of }(\prod_{\substack{\chi\text{ residue character mod }q\\ \chi(-1)=1}}B_\chi^n)]\quad(n\text{ even})$$

$$[\mathbf{R}^-:\mathbf{I}_n^-]=q\cdot[p\text{th part of }(\prod_{\substack{\chi\text{ residue character mod }q\\ \chi(-1)=-1}}B_\chi^n)]\quad(n\text{ odd}).$$

(1) The present research was supported in part by the National Science Foundation grant GP-2496. The author is currently at the Belfer Graduate School of Science, Yeshiva University, New York, N.Y.

(See the appendix for the definition of B_χ^n, the nth generalized Bernoullli number associated with the residue character $\chi \bmod q$.) There is an analogous but more complicated result for the group ring over the rational integers.

The second part of this paper has two foci of interest. First, an elementary computation shows that $p \mid [\mathbf{R}^- : \mathbf{I}_1^-]$ if and only if $p \mid [\mathbf{R}^+ : \mathbf{I}_2^+]$. This suggests the existence of an isomorphism of $\mathbf{R}^-/\mathbf{I}_1^-$ and $\mathbf{R}^+/\mathbf{I}_2^+$ and more generally of the additive groups $\mathbf{R}^-/\mathbf{I}_n^-$ and $\mathbf{R}^+/\mathbf{I}_{n+1}^+$ (n odd), $\mathbf{R}^+/\mathbf{I}_n^+$ and $\mathbf{R}^-/\mathbf{I}_{n+1}^-$ (n even). We don't quite obtain these isomorphisms. We do obtain the following. If $\pi : \mathbf{R} \to \mathbf{R}/q\mathbf{R}$ is the canonical coset mapping, then Theorem 1 says that if $p \neq 2$, $p \nmid n$, $p \nmid n+1$, then

$$\pi(\mathbf{R}^+)/\pi(\mathbf{I}_n^+) \cong \pi(\mathbf{R}^-)/\pi(\mathbf{I}_{n+1}^-) \quad (n \text{ even})$$

$$\pi(\mathbf{R}^-)/\pi(\mathbf{I}_n^-) \cong \pi(\mathbf{R}^+)/\pi(\mathbf{I}_{n+1}^+) \quad (n \text{ odd}).$$

As Corollary to Theorem 1, we have if $p \neq 2$, $p \nmid n$, $p \nmid n+1$, then

$$p \mid \{q \cdot [p\text{th part } (\prod_{\substack{\chi \bmod q \\ \chi(-1)=-1}} B_\chi^n)]\} \text{ if and only if } p \mid \{q \cdot [p\text{th part } (\prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} B_\chi^{n+1})]\} \quad (n \text{ odd}).$$

An analogous result holds for n even.

The other focus of the second part of this paper is related to Iwasawa's work in [4]. For each $m \geqslant 1$, define $q_m = p^m$, $F_m =$ cyclotomic field of the q_mth roots of unity, $G_m =$ Galois group of F_m over the rational number field. We have for each m: $\mathbf{R}_m$, $\mathbf{R}_m^+$, $\mathbf{R}_m^-$, ${}_n\mathbf{I}_m^+$ (n even), ${}_n\mathbf{I}_m^-$ (n odd). The additive groups form inverse systems with respect to the mappings "generated" by the restriction mappings on the Galois groups. If $F = \bigcup_{m \geqslant 1} F_m$, then the group ring $Z_p[G(F/Q)]$(1) operates naturally on $\mathbf{R}_m$, $\mathbf{R}_m^+$, $\mathbf{R}_m^-$, ${}_m\mathbf{I}_n^+$ (n even), and ${}_m\mathbf{I}_n^-$ (n odd). Iwasawa defines a $\varkappa$-isomorphism of $Z_p[G(F/Q)]$-modules to be an additive isomorphism such that

$$v(x^\sigma) = \varkappa(\sigma)\, v(x)^\sigma \quad (x \in \text{the module},\ \sigma \in G(F/Q)),$$

where $\varkappa$ is the isomorphism

$$\varkappa : G(F/Q) \to \text{group of units in the } p\text{-adic number field}$$

given by $$\zeta^\sigma = \zeta^{\varkappa(\sigma)}$$

for any $\sigma \in G$ and ζ any q_mth root of unity.

Iwasawa [4] introduces various $Z_p[G(F/Q)]$-modules which are of interest in determining the arithmetic structure of the cyclotomic fields. Two such modules are $(X/Z)^+$

(1) $G(\ /\ )$ shall denote the Galois group of the Galois extension in the parentheses.

and $(\mathfrak{X}/\mathfrak{Z})^-$. To study the algebraic structure of $(X/Z)^+$ it would suffice to find a $Z_p[G(F/Q)]$-module M whose structure is known and for which we have a $\varkappa$-isomorphism of $M \to (\mathfrak{X}/\mathfrak{Z})^-$; indeed, we would have induced a $Z_p[G/Q]$-isomorphism

$$M \to (X/Z)^+$$

and we could then recover the structure of $(X/Z)^+$. (See section 2.4 of this paper for details.) Our choice for M is $\lim_m \mathbf{R}_m^+/{}_m\mathbf{I}_2^+$ (inverse limit). We define a map

$$v : \lim_m \mathbf{R}_m^+/{}_m\mathbf{I}_2^+ \to (\mathfrak{X}/\mathfrak{Z})^-$$

which has the property of being an additive isomorphism, but $v(x^\sigma) = \varkappa(\sigma)\, v(x)^{\sigma^{-1}}$. While failing to obtain the $\varkappa$-isomorphism, we do obtain a theorem of interest in itself: (Theorem 2) If $p \nmid n$, $p \nmid n+1$, $p \neq 2$, then

$$\lim_m \mathbf{R}_m^-/{}_m\mathbf{I}_n^- \cong \lim_m \mathbf{R}_m^+/{}_m\mathbf{I}_{n+1}^+ \quad (n \text{ odd})$$

$$\lim_m \mathbf{R}_m^+/{}_m\mathbf{I}_n^+ \cong \lim_m \mathbf{R}_m^-/{}_m\mathbf{I}_{n+1}^- \quad (n \text{ even})$$

(all limits being inverse).

This paper is based upon my doctoral dissertation done under the direction of Professor K. Iwasawa at M.I.T. I gratefully acknowledge Professor Iwasawa's assistance and encouragement in writing the dissertation.

§ 1

1.1. Let Z and Q denote the ring of rational integers and the rational field, respectively. Let ζ be a primitive qth root of unity. As above let G be the Galois group of the cyclotomic field of the qth roots of unity over the field of rational numbers. The elements of G are isomorphic with the group $(Z/qZ)^*$ of invertible elements of the residue class ring Z/qZ under the mapping:

$$(Z/qZ)^* \to G$$

$$a \bmod q \to \sigma(a) \text{ where } \sigma(a)(\zeta) = \zeta^a \quad (a,p) = 1.$$

Let $\tau \in G$ correspond to -1 under this mapping, i.e. $\tau(\zeta) = \zeta^{-1}$. For the rest of the paper we adopt the following notation:

$$\sum\nolimits_a = \sum_{\substack{0 \leqslant a < q \\ (a,p)=1}}; \quad \sum\nolimits'_a = \sum_{\substack{0 \leqslant a < q/2 \\ (a,p)=1}}; \quad \sum\nolimits''_a = \sum_{\substack{1 < a < q/2 \\ (a,p)=1}}.$$

Let $\mathfrak{R} = Z[G]$ and $\mathfrak{S} = Q[G]$. Iwasawa [3] put $\mathfrak{R}^- = \{x \in \mathfrak{R} \mid (1+\tau)x = 0\}$ which is an ideal in $\mathfrak{R}$. He then defined

$$\omega = q^{-1} \sum_a a\sigma(a)^{-1}$$

and put $\mathfrak{J}^- = \mathfrak{R}^- \cap \mathfrak{R}\omega$. Iwasawa calculated

$$[\mathfrak{R}^- : \mathfrak{J}^-] = 2q \prod_\chi \left(-\frac{1}{2q} \sum_a a\chi^{-1}(a) \right).$$

where χ ranges in the product over all characters of $(Z/qZ)^*$ such that $\chi(-1) = -1$, or, otherwise stated, over all residue characters mod q such that $\chi(-1) = -1$.

A key part of the proof is the fact that $(1-\tau)q\omega$ is regular in the ring $\mathfrak{R}^-$ which in turn follows from the fact that $\sum_a a\chi(a) \neq 0$ if and only if $\chi(-1) = -1$.

In considering one possible generalization of Iwasawa's work, we define

$$\omega = q^{-1} \sum_a a^2 \sigma(a)^{-1} \qquad \omega_0 = q\omega.$$

If χ is a character on $(Z/qZ)^*$ and $\xi = \sum_a x_a \sigma(a)$ is an element in S, we define

$$\chi(\xi) = \sum_a x_a \chi(a).$$

If we let $\varepsilon^+ = \frac{1}{2}(1+\tau)$, $\varepsilon^- = \frac{1}{2}(1-\tau)$, then

$$S = \varepsilon^+ S \oplus \varepsilon^- S.$$

$\varepsilon^+ S$ is a semi-simple commutative algebra over Q with identity ε^+, and its absolutely irreducible (one-dimensional) representations φ are obtained from the characters χ of G with $\chi(\tau) = 1$ in the obvious manner. Hence the determinant of the matrix for $\varepsilon^+\omega_0$ in a regular representation of $\varepsilon^+ S$ is given by

$$\prod_\varphi \varphi(\varepsilon^+ \omega_0) = \prod_\chi \chi(\omega_0),$$

where the product is taken over all χ mod q such that $\chi(-1) = 1$. For $\chi \neq 1$, $\chi^{-1}(\omega_0) = \sum_a a^2 \chi(a) = qB_\chi^2$ where by B_χ^n we mean the nth generalized Bernoulli number associated with the character χ. See statement (A 8) in appendix of this paper for proof of this assertion. In general (A n) refers to the nth numbered formula or statement of the appendix. Also for $\chi \neq 1$, $B_\chi^2 \neq 0$ if and only if $\chi(-1) = 1$ (by (A 6)). Finally if $\chi = 1$, the principal character, then $1(\omega_0) = \dfrac{q(p-1)(2q^2-p)}{6p}$. Hence $\prod\limits_{\substack{\chi \bmod q \\ \chi(-1)=1}} \chi(\omega_0) \neq 0$ and $\varepsilon^+\omega_0$ is regular in $\varepsilon^+ S$. Thus it is natural to define $\mathfrak{R}^+ = \{x \in \mathfrak{R} \mid (1-\tau)x = 0\}$ and define:

$$\mathfrak{J} = \mathfrak{R} \cap \mathfrak{R}\omega, \qquad \mathfrak{J}^+ = \mathfrak{R}^+ \cap \mathfrak{R}\omega.$$

We then have:

PROPOSITION 1. $\quad [\mathfrak{R}^+ : \mathfrak{J}^+] = q \left| \prod\limits_{\substack{\chi \bmod q \\ \chi(-1)=1}} q^{-1} \sum_a a^2 \chi(a) \right|.$

Proof. Let $\mathcal{A}$ be the additive group in $\mathcal{R}$ generated by q and $\sigma(a)-a^2$, $(a,p)=1$. Then $\mathcal{A}$ has a basis over Z consisting of q, $2\varepsilon^-$, $\sigma(a)-a^2$, and $\sigma(-a)-a^2$, $1<a<q/2$, $(a,p)=1$. Then, we have

$$\mathfrak{J}=\mathcal{A}\omega, \quad q\mathfrak{J}=\mathcal{A}\omega_0, \quad \text{and} \quad q\mathfrak{J}^+=\mathcal{A}\omega_0\cap\varepsilon^+\mathcal{S}.$$

Let $\mathcal{B}=\{\varepsilon^+\alpha\,|\,\alpha\in\mathcal{A},\ \alpha\omega\in\varepsilon^+\mathcal{S}\}$, $\mathcal{B}\subseteq\varepsilon^+\mathcal{R}$. Then

$$\mathfrak{J}^+=\mathcal{B}\varepsilon^+\omega, \qquad q\mathfrak{J}^+=\mathcal{B}\varepsilon^+\omega_0$$

and
$$[\varepsilon^+\mathcal{R}:q\mathfrak{J}^+]=[\varepsilon^+\mathcal{R}:\varepsilon^+\mathcal{R}\,\varepsilon^+\omega_0]\,[\varepsilon^+\mathcal{R}\,\varepsilon^+\omega_0:\mathcal{B}\varepsilon^+\omega_0].$$

But $\varepsilon^+\omega_0$ is regular in $\varepsilon^+\mathcal{S}$, hence

$$[\varepsilon^+\mathcal{R}:q\mathfrak{J}^+]=[\varepsilon^+\mathcal{R}:\varepsilon^+\mathcal{R}\,\varepsilon^+\omega_0]\,[\varepsilon^+\mathcal{R}:\mathcal{B}].$$

$\varepsilon^+\mathcal{R}$ is a free Z-module with basis over Z consisting of $\varepsilon^+\sigma(a)=\frac{1}{2}(\sigma(a)+\sigma(-a))$, $(a,p)=1$, $0\leqslant a<q/2$. Let $\tau(a)=\varepsilon^+\sigma(a)$. Thus,

$$[\varepsilon^+\mathcal{R}:\varepsilon^+\mathcal{R}\,\varepsilon^+\omega_0]=\Big|\prod_{\substack{\chi \bmod q\\ \chi(-1)=1}}\chi(\omega_0)\Big|=\Big|\prod_{\substack{\chi \bmod q\\ \chi(-1)=1}}\chi^{-1}(\omega_0)\Big|=\Big|\prod_{\substack{\chi \bmod q\\ \chi(-1)=1}}\textstyle\sum_a a^2\chi(a)\Big|.$$

Thus,
$$[\varepsilon^+\mathcal{R}:q\mathfrak{J}^+]=\Big|\prod_{\substack{\chi \bmod q\\ \chi(-1)=1}}\textstyle\sum_a a^2\chi(a)\Big|\,[\varepsilon^+\mathcal{R}:\mathcal{B}].$$

If $\alpha\in\mathcal{A}$, then $\alpha=sq+t(2\varepsilon^-)+\sum_a''\{s_a(\sigma(a)-a^2)+s_{-a}(\sigma(-a)-a^2)\}$ for unique choice of $s,t,s_a,s_{-a}\in Z$. Thus $\varepsilon^+\alpha\in\varepsilon^+\mathcal{R}$ and $\varepsilon^+\alpha=\sum_a' u_a\tau(a)$ where

$$u_1=sq+\textstyle\sum_a''-a^2(s_a+s_{-a})$$

$$u_a=s_a+s_{-a} \quad \text{for } 1<a<q/2,\ (a,p)=1.$$

Thus
$$\textstyle\sum_a' a^2u_a=qs \quad \text{or} \quad \sum' a^2u_a\equiv 0\ (q);$$

hence
$$\varepsilon^+\mathcal{A}\subseteq\{\textstyle\sum_a' u_a\tau(a)\in\varepsilon^+\mathcal{R}\,|\,\sum_a' a^2u_a\equiv 0\ (q)\}.$$

Conversely, suppose for $u_a\in Z$, $\sum_a' u_a\tau(a)\in\varepsilon^+\mathcal{R}$ satisfies the condition $\sum_a' a^2u_a\equiv 0\ (q)$ then letting

$$\alpha=sq+t(2\varepsilon^-)+\textstyle\sum_a''\{s_a(\sigma(a)-a^2)+s_{-a}(\sigma(-a)-a^2)\},$$

where $s=q^{-1}\sum_a' a^2u_a$, $s_{-a}=u_a-s_a$, and t and s_a $(1<a<q/2,\ (a,p)=1)$ arbitrary, we have that

$$\textstyle\sum' u_a\tau(a)=\varepsilon^+\alpha.$$

Hence $\varepsilon^+\mathcal{A}=\{\sum_a' u_a\tau(a)\in\varepsilon^+\mathcal{R}\,|\,\sum_a' a^2u_a\equiv 0\ (q)\}$. On the other hand, if $\xi\in\mathcal{S}$, $\xi=\sum_a x_a\sigma(a)$, $x_a\in Q$, then $\xi\omega\in\varepsilon^+\mathcal{S}$ if and only if $2\varepsilon^-\xi\omega=0$. But $2\varepsilon^-\omega=\sum_a(-q+2a^*)\,\sigma(a)$, where

from now on $R(a)$ = least positive residue of $a \bmod q$ and $a^* = R(a^{-1})$ for $(a,p)=1$. Hence $2\varepsilon^- \xi\omega = 0$ if and only if for all c, $0 \leqslant c < q$, $(c,p)=1$, we have $\sum x_b(-q+2a^*)=0$ (summation taken over all a, b such that $ab \equiv c\ (q)$, $0 \leqslant a, b < q$). Combining all of the above we have if $\beta \in \varepsilon^+ \mathcal{R}$, $\beta = \sum'_a u_a \tau(a)$, then $\beta \in \mathcal{B}$ if and only if $\beta = \varepsilon^+ \alpha$, for $\alpha \in \mathcal{A}$ and $\alpha\omega \in \varepsilon^+ \mathcal{S}$ where

$$\begin{aligned}\alpha &= sq + t(2\varepsilon^-) + \sum''_a \{s_a(\sigma(a) - a^2) + s_{-a}(\sigma(-a) - a^2)\} \\ &= [sq + t + \sum''_a - a^2(s_a + s_{-a})]\,\sigma(1) + (-t)\,\sigma(q-1) + \sum''_a s_a \sigma(a) + \sum''_a s_{-a}\sigma(-a)\end{aligned}$$

for some $s, t, s_a, s_{-a} \in Z$, which is true if and only if $\sum'_a a^2 u_a \equiv 0\ (q)$ and there exist integers t and s_a $(1 < a < q/2, (a,p)=1)$ such that

$$u_1(q - 2c^*) + (\sum''_a (2R(ac^*) - q)\, u_a) - 2\{(2c^* - q)\, t + \sum''_a (2R(ac^*) - q)\, s_a\} = 0$$

for all c, $0 \leqslant c < q$, $(c,p)=1$; the latter assertion is true if and only if there exist integers t and s_a $(1 < a < q/2, (a,p)=1)$ such that

$$(q - 2c^*)\,(u_1 + 2t) + \sum''_a (2R(ac^*) - q)\,(u_a - 2s_a) = 0$$

for all c, $0 \leqslant c < q$, $(c,p)=1$. But the square-matrix

$$\|2R(ac^*) - q\| \quad (0 \leqslant a, c \leqslant q/2,\ (a,p) = (c,p) = 1)$$

has non-vanishing determinant; indeed the determinant is equal, up to a factor of $\pm$ a positive integral power of two, to the value of Maillet's determinant. Carlitz and Olson [1] showed for $q=p$ that Maillet's determinant does not vanish. Their method generalizes completely to the case $q=p^m$, $m \geqslant 2$. Hence the above system of homogeneous equations is solvable if and only if $u_a \equiv 0\ (2)$ for $0 \leqslant a < q/2$, $(a,p)=1$. Therefore, $\beta = \sum'_a u_a \tau(a)$ is in $\mathcal{B}$ if and only if

(i) $\sum'_a a^2 u_a \equiv 0\ (q)$

(ii) $u_a \equiv 0\ (2)$ for $0 \leqslant a < q/2\ (a,p)=1$.

Therefore,
$$[\varepsilon^+ \mathcal{R} : \mathcal{B}] = q2^M,$$

where $M = \varphi(q)/2$ and φ is Euler's totient function. Therefore,

$$[\varepsilon^+ \mathcal{R} : q\mathcal{J}^+] = \Big| \prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} \chi(\omega) \Big| q2^M.$$

Hence $q\mathcal{J}^+$ is a Z-module of the same rank as $\varepsilon^+\mathcal{R}$, namely M. Therefore $[\mathcal{J}^+ : q\mathcal{J}^+] = q^M$. Also $[\varepsilon^+\mathcal{R} : \mathcal{R}^+] = 2^M$ because $\mathcal{R}^+ = 2(\varepsilon^+\mathcal{R})$. Putting all these indices together we conclude that

$$[\mathcal{R}^+ : \mathcal{J}^+] = q \Big| \prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} \chi(\omega) \Big|.$$

1.2. Considerations of such sums as $q^{-1}\sum_a a^3\sigma(a)^{-1}$ and $q^{-1}\sum_a a^4\sigma(a)^{-1}$ as generators of ideals do not prove fruitful since they lead to difficult to evaluate determinants. Also it is not clear that $\varepsilon^-\sum_a a^3\sigma(a)^{-1}$ and $\varepsilon^+\sum_a a^4\sigma(a)^{-1}$ are regular in $\varepsilon^-\mathcal{S}$ and $\varepsilon^+\mathcal{S}$ respectively. However, the fact that for a non-principal character χ on $(Z/qZ)^*$ with conductor $\chi = f$ and the nth Bernoulli polynomial $B_n(x)$, we have (v. A 7)

$$\sum_{a=1}^{f} \chi(a) B_n(a/f) \neq 0$$

if and only if $\chi(-1)$, n even or $\chi(-1) = -1$, n odd (where it is understood that $\chi(a) = 0$, if $(a, f) \neq 1$) leads one to consider elements in $\mathcal{S}$ of the form

$$q^{n-1}\sum_a B_n(a/q)\,\sigma(a)^{-1}.$$

This leads to consider the following more general situation:

PROPOSITION 2. *Let $f(x) = \sum_{i=0}^{n} c_i x^i$ be a polynomial of degree n such that:*

a) $c_i \in Z$ *for* $0 \leqslant i < n$, $c_n = c/q$, $c \in Z$, $c \neq 0$

b) $f(q-x) = (-1)^n f(x)$.

Let

$$\omega (= \omega_f) = \sum_a f(a)\,\sigma(a)^{-1} \in \mathcal{S}$$

and suppose that $\varepsilon^+\omega \in \varepsilon^+\mathcal{S}$ is regular in $\varepsilon^+\mathcal{S}$ if n is even and $\varepsilon^-\omega \in \varepsilon^-\mathcal{S}$ is regular in $\varepsilon^-\mathcal{S}$ if n is odd, then

$$[\mathcal{R}^+ : \mathcal{R}^+ \cap \mathcal{R}\omega] = q' 2^{-M} \Big| \prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} \chi(\omega) \Big| \quad \textit{for } n \textit{ even}$$

$$[\mathcal{R}^- : \mathcal{R}^- \cap \mathcal{R}\omega] = q' 2^{-M} \Big| \prod_{\substack{\chi \bmod q \\ \chi(-1)=-1}} \chi(\omega) \Big| \quad \textit{for } n \textit{ odd},$$

where q' is defined by $c_n = c/q = c'/q'$, $(c', q') = 1$, $q' > 0$, and $M = \varphi(q)$.

Proof. It follows from assumption b) that

$$\omega \in \varepsilon^+\mathcal{S} \quad \text{for } n \text{ even}$$

$$\omega \in \varepsilon^-\mathcal{S} \quad \text{for } n \text{ odd}.$$

We give the proof of the proposition for n even, although a completely analogous proof holds for n odd. Let $\mathcal{A}$ be the additive group in $\mathcal{R}$ generated by q', and $\sigma(a) - a^n$, $(a, p) = 1$. A basis for $\mathcal{A}$ over Z is q', $2\varepsilon^-$, $\sigma(a) - a^n$, and $\sigma(-a) - a^n$, $1 < a < q/2$, $(a, p) = 1$. Clearly $\mathcal{A}\omega \subseteq \mathcal{R}^+ \cap \mathcal{R}\omega$. Conversely, if $\xi = \sum_a x_a\sigma(a) \in \mathcal{R}$ $(x_a \in Z)$, then $\xi\omega \in \mathcal{R}$ implies that

$(\sum_a x_a\sigma(a))(\sum_a a^n\sigma(a)^{-1}) \equiv 0 \mod q'\mathcal{R}$ (because $q' \mid q$ and $\omega \equiv cq^{-1}\sum_a a^n\sigma(a)^{-1} \mod \mathcal{R}$) which in turn implies that $\sum_a x_{ab}a^n \equiv 0\ (q')$ for any b, $(b,p)=1$. This implies, in particular, for $b=1$ that $\sum_a x_a a^n \equiv 0\ (q')$. Thus $\sum_a x_a a^n = q'v$, for some $v \in Z$. Thus $\xi\omega = [\sum_a x_a(\sigma(a)-a^n) - vq']\,\omega$ or $\xi\omega \in \mathcal{A}\omega$. Thus,

$$\mathcal{R}^+ \cap \mathcal{R}\omega = \mathcal{A}\omega.$$

Let $\mathcal{B} = \varepsilon^+\mathcal{A}$, $\mathcal{B} \subseteq \varepsilon^+\mathcal{R}$; further put $\omega_0 = q\omega$. Then

$$\mathcal{R}^+ \cap \mathcal{R}\omega = \mathcal{B}\omega, \quad q(\mathcal{R}^+ \cap \mathcal{R}\omega) = \mathcal{B}\omega_0.$$

By assumption ω is regular in $\varepsilon^+\mathcal{S}$, hence

$$[\varepsilon^+\mathcal{R} : q(\mathcal{R}^+ \cap \mathcal{R}\omega)] = [\varepsilon^+\mathcal{R} : \varepsilon^+\mathcal{R}\omega_0]\,[\varepsilon^+\mathcal{R}\omega_0 : \mathcal{B}\omega_0] = q^M \Big| \prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} \chi(\omega) \Big|\,[\varepsilon^+\mathcal{R} : \mathcal{B}].$$

To calculate $[\varepsilon^+\mathcal{R} : \mathcal{B}]$ we consider the epimorphism

$$\theta : \mathcal{R} \to \varepsilon^+\mathcal{R}$$

$$\theta(\xi) = \varepsilon^+\xi \quad \text{for } \xi \in \mathcal{R}.$$

The kernel of θ is $\mathcal{R}^-$. Moreover $\mathcal{A} \supseteq \mathcal{R}^-$, for $\mathcal{R}^-$ is generated over Z by $(\sigma(a)-a^n) - (\sigma(-a)-a^n) \in \mathcal{A}$. Hence

$$[\mathcal{R} : \mathcal{A}] = [\theta(\mathcal{R}) : \theta(\mathcal{A})] = [\varepsilon^+\mathcal{R} : \varepsilon^+\mathcal{A}] = [\varepsilon^+\mathcal{R} : \mathcal{B}].$$

But $[\mathcal{R} : \mathcal{A}] = q'$, since $1, 2\varepsilon^-, \sigma(a)-a^n, \sigma(-a)-a^n$ for all a, $1 < a < q/2$, $(a,p)=1$ constitute a basis for $\mathcal{R}$ over Z. Hence we have that:

$$[\varepsilon^+\mathcal{R} : q(\mathcal{R}^+ \cap \mathcal{R}\omega)] = q' \cdot q^M \Big| \prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} \chi(\omega) \Big|.$$

Thus $q(\mathcal{R}^+ \cap \mathcal{R}\omega)$ is a Z-module of rank M. Thus $[\mathcal{R}^+ \cap \mathcal{R}\omega : q(\mathcal{R}^+ \cap \mathcal{R}\omega)] = q^M$; also $[\varepsilon^+\mathcal{R} : \mathcal{R}^+] = 2^M$. Hence $[\mathcal{R}^+ : \mathcal{R}^+ \cap \mathcal{R}\omega] = q'2^{-M} \Big| \prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} \chi(\omega) \Big|$, q.e.d.

For $n \geqslant 1$, the nth Bernoulli polynomial $B_n(x)$ can be written as:

$$B_n(x) = x^n + \sum_{\nu=0}^{n-1} (a_{\nu,n}/b_{\nu,n})\,x^\nu,$$

where $a_{\nu,n}, b_{\nu,n} \in Z$ $(\nu = 0, \ldots, n-1)$, $b_{\nu,n} \geqslant 1$, and $(a_{\nu,n}, b_{\nu,n}) = 1$. Let $\alpha_n =$ the least common multiple of $b_{\nu,n}$, $\nu = 0, \ldots, n-1$. Let q_n' be defined by $\alpha_n/q = \alpha_n'/q_n'$, $(\alpha_n', q_n') = 1$ and $q_n' > 0$.

COROLLARY. *With the notation as above, let* $h_n(x) = \alpha_n q^{n-1} B_n(x/q)$ *and* $\omega_n = \sum_a h_n(a)\,\sigma(a)^{-1}$; *then*

$$[R^+ : R^+ \cap R\omega_n] = q_n' 2^{-M} \Big| \prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} \chi(\omega_n) \Big| = q_n'(\alpha_n/2)^M (1-p^{n-1}) \Big| \prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} B_\chi^n \Big| \quad \textit{for } n \textit{ even;}$$

$$[R^- : R^- \cap R\omega_n] = q_n' 2^{-M} \Big| \prod_{\substack{\chi \bmod q \\ \chi(-1)=-1}} \chi(\omega_n) \Big| = q_n'(\alpha_n/2)^M \Big| \prod_{\substack{\chi \bmod q \\ \chi(-1)=-1}} B_\chi^n \Big| \quad \textit{for } n \textit{ odd,}$$

where $M = \varphi(q)$.

Proof. We notice that $h_n(x)$ has integral coefficients except for the leading coefficient, which is α_n/q. In order to apply the previous proposition we must verify that $h_n(q-x) = (-1)^n h_n(x)$ and that ω_n is regular in $\varepsilon^+ S$ for n even and regular in $\varepsilon^- S$ for n odd. As for the first assertion:

$$\begin{aligned} h_n(q-x) &= \alpha_n q^{n-1} B_n((q-x)/q) = \alpha_n q^{n-1} B_n\left(1 - \frac{x}{q}\right) \\ &= (-1)^n \alpha_n q^{n-1} B_n(x/q) \qquad \text{by (A 2)} \\ &= (-1)^n h_n(x). \end{aligned}$$

As for the latter assertion, it suffices to calculate $\chi(\omega_n)$ and show that $\chi(\omega_n) \neq 0$ if and only if n even, $\chi(-1) = 1$ or n odd, $\chi(-1) = -1$, for χ a character mod q. Let f = conductor of χ, $f \mid q$. We first consider non-principal χ, so $f > 1$. If $(a, p) \neq 1$, we agree to let $\chi(a) = 0$. Then $\chi(\omega) \neq 0$ if and only if

$$q^{n-1} \sum_{0 \leqslant b < q} \chi(b)\, B_n(b/q) \neq 0.$$

But

$$\begin{aligned} q^{n-1} \sum_{0 \leqslant b < q} \chi(b)\, B_n(b/q) &= q^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{\substack{0 \leqslant a < q \\ a \equiv b (f)}} B_n(a/q) \\ &= q^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{k=0}^{(q/f)-1} B_n((b+kf)/q) \quad \text{(by A 4)} \\ &= q^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{k=0}^{(q/f)-1} \sum_{r=0}^{n} C_{n,r} (b/q)^r B_{n-r}(kf/q) \\ &= q^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{r=0}^{n} C_{n,r} \frac{(b/q)^r}{(q/f)^{n-r-1}} \left[(q/f)^{n-r-1} \sum_{k=0}^{(q/f)-1} B_{n-r}\left(k/\frac{q}{f}\right) \right] \quad \text{(by A 3)} \\ &= f^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{r=0}^{n} C_{n,r} (b/f)^r B_{n-r}\left(\frac{q}{f} \cdot 0\right) \\ &= f^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{r=0}^{n} C_{n,r} (b/f)^r B_{n-r}(0) \quad \text{(by A 1)} \\ &= f^{n-1} \sum_{b=1}^{f} \chi(b)\, B_n(b/f) \neq 0 \end{aligned}$$

if and only if n even, $\chi(-1)=1$ or n odd, $\chi(-1)=-1$ (by A7). It remains to treat the case $\chi=1$:

$$1(\omega_n)\neq 0 \text{ *if and only if* } q^{n-1}\sum_{\substack{0\leqslant b<q\\(b,p)=1}} B_n(b/q)\neq 0.$$

But

$$\begin{aligned}
q^{n-1}\sum_{\substack{0\leqslant b<q\\(b,p)=1}} B_n(b/q) &= q^{n-1}\sum_{b=0}^{q-1} B_n(b/q) - q^{n-1}\sum_{t=0}^{(q/p)-1} B_n(pt/q)\\
&= q^{n-1}\sum_{b=0}^{q-1} B_n(0+b/q) - q^{n-1}\sum_{t=0}^{(q/p)-1} B_n(pt/q) \quad \text{(by A3)}\\
&= B_n(0\cdot q) - q^{n-1}\sum_{t=0}^{(q/p)-1} B_n(pt/q) = B_n(0) - q^{n-1}\sum_{t=0}^{(q/p)-1} B_n\left(t/\frac{q}{p}\right)\\
&= B_n(0) - q^{n-1}(p/q)^{n-1}\left\{(q/p)^{n-1}\sum_{t=0}^{(q/p)-1} B_n\left(0+t/\frac{q}{p}\right)\right\} \quad \text{(by A3)}\\
&= B_n(0) - q^{n-1}(p/q)^{n-1} B_n(0\cdot q/p)\\
&= B_n(0) - p^{n-1}B_n(0) = (1-p^{n-1})B_n(0)\neq 0
\end{aligned}$$

if n is even, because then $B_n(0)=\pm B_{n/2}\neq 0$. We may now apply Proposition 2 to $h_n(x)=\alpha_n q^{n-1}B_n(x/q)$. It remains only to observe that:

$$\text{for } \chi\neq 1,\ \chi(\omega_n)=\alpha_n B_\chi^n$$

$$\text{for } \chi=1,\ 1(\omega_n)=\alpha_n(1-p^{n-1})B_n(0)=\alpha_n(1-p^{n-1})B_1^n.$$

(The fact that $B_n(0)=B_1^n$ is adduced as follows:

$$\begin{aligned}
B_n(0) &= B_n(1) \qquad \text{(for } B_n(x)=(-1)^n B_n(1-x) \text{ and } B_n(0)=0 \text{ for } n \text{ odd)}\\
&= B_n^*(0) \qquad \text{(by (A5))}\\
&= B_n^* = B_1^n \qquad \text{(from definitions in the appendix).)}
\end{aligned}$$

Thus,

$$[\mathfrak{R}^+:\mathfrak{R}^+\cap\mathfrak{R}\omega_n]=q_n'(\alpha_n/2)^M(1-p^{n-1})\Big|\prod_{\substack{\chi \bmod q\\ \chi(-1)=1}} B_\chi^n\Big| \quad (n \text{ even})$$

$$[\mathfrak{R}^-:\mathfrak{R}^-\cap\mathfrak{R}\omega_n]=q_n'(\alpha_n/2)^M\Big|\prod_{\substack{\chi \bmod q\\ \chi(-1)=-1}} B_\chi^n\Big| \quad (n \text{ odd}).$$

1.3. Let Q_p be the p-adic number field and Z_p be the subring of p-adic integers ($p\neq 2$). Put

$$\mathbf{R}=Z_p[G],\quad \mathbf{S}=Q_p[G]$$

$$\mathbf{S}^+=\varepsilon^+\mathbf{S},\quad \mathbf{S}^-=\varepsilon^-\mathbf{S}$$

$$\mathbf{R}^+=\mathbf{R}\cap\mathbf{S}^+=\varepsilon^+\mathbf{R};\quad \mathbf{R}^-=\mathbf{R}\cap\mathbf{S}^-=\varepsilon^-\mathbf{R}.$$

If $u \in Q$, and $u = (r/s)\, p^{v}$, $(r, p) = (s, p) = 1$, $r, s, v \in Z$, then define:

$$(u)_p = p^{v}.$$

Analogous to the classical results used for the group ring over the rational numbers, we recall the following facts:

1) Let $\xi \in \mathbf{S}$, $\xi = \sum_a x_a\, \sigma(a)$, $x_a \in Q_p$. Define

$$\chi(\xi) = \sum_a x_a\, \chi(a)$$

for any residue character $\bmod q$. Then ξ is regular in $\mathbf{S}$ if and only if $\prod_{\chi \bmod q} \chi(\xi) \neq 0$. Similarly, if $\xi \in \mathbf{S}^+$ $(\mathbf{S}^-)$ then ξ is regular in $\mathbf{S}^+$ $(\mathbf{S}^-)$ if and only if

$$\prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} \chi(\xi) \neq 0, \quad \Big(\prod_{\substack{\chi \bmod q \\ \chi(-1)=-1}} \chi(\xi) \neq 0\Big).$$

2) If $\xi \in \mathbf{R}$ is regular in $\mathbf{S}$, then $[\mathbf{R} : \xi\mathbf{R}] = \big(\prod_{\chi \bmod q} \chi(\xi)\big)_p$. Similarly if $\xi \in \mathbf{R}^+$ is regular in $\mathbf{S}^+$, then $[\mathbf{R}^+ : \xi\mathbf{R}^+] = \big(\prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} \chi(\xi)\big)_p$ and if $\xi \in \mathbf{R}^-$ is regular in $\mathbf{S}^-$, then $[\mathbf{R}^- : \xi\mathbf{R}^-] = \big(\prod_{\substack{\chi \bmod q \\ \chi(-1)=-1}} \chi(\xi)\big)_p$. We now state a proposition analogous to Proposition 2.

Let $f(x) = \sum_{i=0}^{n} c_i x^i$ be a polynomial of degree n such that

1) $c_i \in Z_p$, for $0 \leqslant i < n$ and $c_n = c/q$, $c \in Z_p$, $c \neq 0$

2) $f(q - x) = (-1)^n f(x)$.

Let

$$\omega_f = \sum_a f(a)\, \sigma(a)^{-1}.$$

Let q' be defined by $c_n = c/q = c'/q'$, $(c', q') = 1$, and $q' > 0$. Let $\mathbf{A}$ be the additive group generated over Z_p by q' and $\sigma(a) - a^n$. Let $\mathbf{B} = \varepsilon^+\mathbf{A}$ for n even, $\mathbf{B} = \varepsilon^-\mathbf{A}$ for n odd.

PROPOSITION 3. *With the above definitions and hypotheses, suppose now that w_f is regular in $\mathbf{S}^+$ for n even, w_f is regular in $\mathbf{S}^-$ for n odd. Then*

(i) $[\mathbf{R}^+ : \mathbf{R}^+ \cap \mathbf{R}\omega_f] = q'\big(\prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} \chi(\omega_f)\big)_p$ *for n even*

$[\mathbf{R}^- : \mathbf{R}^- \cap \mathbf{R}\omega_f] = q'\big(\prod_{\substack{\chi \bmod q \\ \chi(-1)=-1}} \chi(\omega_f)\big)_p$ *for n odd.*

(ii) $\mathbf{R}^+ \cap \mathbf{R}\omega_f = \mathbf{B}\omega_f$ *for n even*

$\mathbf{R}^- \cap \mathbf{R}\omega_f = \mathbf{B}\omega_f$ *for n odd.*

Proof. Proof proceeds exactly as in Proposition 2, but the formula simplifies since $\mathbf{R}^{\pm} = \varepsilon^{\pm}\mathbf{R}$ (for $p \neq 2$).

For each $n \geqslant 1$, let

$$\omega_n = \sum_a q^{n-1} B_n(a/q)\, \sigma(a)^{-1} \in \mathbf{S}.$$

(Note the omission of the constant α_n.) Let $\mathbf{I}_n^+ = \mathbf{R}^+ \cap \mathbf{R}\omega_n$ (n even); $\mathbf{I}_n^- = \mathbf{R}^- \cap \mathbf{R}\omega_n$ (n odd). Let $\mathbf{A}_n$ be the additive group generated over Z_p in $\mathbf{R}$ by q and $\sigma(a) - a^n$. Let $\mathbf{B}_n = \varepsilon^+ \mathbf{A}_n$ for n even; $\mathbf{B}_n = \varepsilon^- \mathbf{A}_n$ for n odd.

COROLLARY. *With the above definitions*

(i) $$[\mathbf{R}^+ : \mathbf{I}_n^+] = q\Big(\prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} B_\chi^n\Big)_p \quad (n \text{ even})$$

$$[\mathbf{R}^- : \mathbf{I}_n^-] = q\Big(\prod_{\substack{\chi \bmod q \\ \chi(-1)=-1}} B_\chi^n\Big)_p \quad (n \text{ odd}).$$

(ii) $$\mathbf{I}_n^+ = \mathbf{B}_n \omega_n \quad (n \text{ even})$$

$$\mathbf{I}_n^- = \mathbf{B}_n \omega_n \quad (n \text{ odd}).$$

Proof. For any $n \geqslant 1$,

$$B_n(x) = x^n - \tfrac{1}{2} n x^{n-1} + \sum_{u=1}^{[n/2]} (-1)^{u-1} C_{n,2u} B_u x^{n-2u}$$

and

$$q^{n-1} B_n(x/q) = q^{-1}\Big(x^n - \tfrac{1}{2} nqx^{n-1} + \sum_{u=1}^{[n/2]} (-1)^{u-1} C_{n,2u} B_u x^{n-2u} q^{2u}\Big).$$

By the von Staudt–Clausen theorem, B_u has square-free denominator; hence because $p \neq 2$, we have that all the coefficients of $q^{n-1} B_n(x/q)$, except the leading coefficient, are p-adic integers. The leading coefficient is $1/q$ and so in all cases $q' = q$. In the proof of the corollary to Proposition 2 we saw that $q^{n-1} B_n((q-x)/q) = (-1)^n q^{n-1} B_n(x/q)$. Also just as we derived in the proof of the same corollary, we have: for $\chi \neq 1$, $\chi(\omega_n) = B_\chi^n \neq 0$ if and only if $\chi(-1) = 1$, n even or $\chi(-1) = -1$, n odd; for $\chi = 1$, $1(\omega_n) = (1 - p^{n-1}) B_1^n \neq 0$ for n even. As previously noted, $\omega_n \in \mathbf{S}^+$ if n is even and $\omega_n \in \mathbf{S}^-$ if n is odd. Hence we have that ω_n is regular in $\mathbf{S}^+$ for n even and ω_n is regular in $\mathbf{S}^-$ for n odd. All the hypotheses of Proposition 3 are fulfilled. It only remains to remark that $(1 - p^{n-1})_p = 1$ if $n \geqslant 2$.

We recall that $\mathbf{R}^+ = \varepsilon^+ \mathbf{R}$ and $\mathbf{R}^- = \varepsilon^- \mathbf{R}$ have bases over Z_p consisting of $\sigma(a) + \sigma(-a)$, $0 \leqslant a < q/2$, $(a, p) = 1$ and $\sigma(a) - \sigma(-a)$, $0 \leqslant a < q/2$, $(a, p) = 1$, respectively. It is a simple calculation to show that

$$\mathbf{B}_n = \varepsilon^+ \mathbf{A}_n = \Big\{ \sum_a{}' u_a(\sigma(a) + \sigma(-a)) \,\Big|\, u_a \in Z_p,\ \sum_a{}' a^n u_a \equiv 0 \ (q) \Big\} \quad n \text{ even}$$

$$\mathbf{B}_n = \varepsilon^- \mathbf{A}_n = \Big\{ \sum_a{}' u_a(\sigma(a) - \sigma(-a)) \,\Big|\, u_a \in Z_p,\ \sum_a{}' a^n u_a \equiv 0 \ (q) \Big\} \quad n \text{ odd}.$$

Let $$\mathbf{B}_n^* = \{\sum_a{}' u_a(\sigma(a)+\sigma(-a)) \mid u_a \in Z_p, \sum_a{}' a^n u_a \equiv 0 \ (q^2)\} \quad n \text{ even}$$

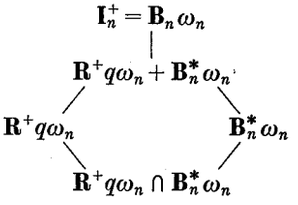
and $$\mathbf{B}_n^* = \{\sum_a{}' u_a(\sigma(a)-\sigma(-a)) \mid u_a \in Z_p, \sum_a{}' a^n u_a \equiv 0 \ (q^2)\} \quad n \text{ odd}.$$

Clearly $\mathbf{B}_n^*$ is an additive subgroup of $\mathbf{B}_n$.

LEMMA 1. $$\mathbf{I}_n^+ = \mathbf{B}_n\omega_n = \mathbf{R}^+q\omega_n + \mathbf{B}_n^*\omega_n \quad \textit{for } n \textit{ even}$$
$$\mathbf{I}_n^- = \mathbf{B}_n\omega_n = \mathbf{R}^-q\omega_n + \mathbf{B}_n^*\omega_n \quad \textit{for } n \textit{ odd}.$$

Proof. We do proof for n even, and proof for n odd is entirely analogous.

We have from corollary to Proposition 3 that $\mathbf{I}_n^+ = \mathbf{B}_n\omega_n$. It is also clear from the definition of $\mathbf{I}_n^+ = \mathbf{R}^+ \cap \mathbf{R}\omega_n$ that $\mathbf{R}^+q\omega_n \subseteq \mathbf{I}_n^+$; also $\mathbf{B}_n^* \subseteq \mathbf{B}_n$ implies that $\mathbf{B}_n^*\omega_n \subseteq \mathbf{B}_n\omega_n = \mathbf{I}_n^+$. Thus $\mathbf{R}^+q\omega_n + \mathbf{B}_n^*\omega_n \subseteq \mathbf{I}_n^+ = \mathbf{B}_n\omega_n$. Consider the following diagram



Because $\mathbf{B}_n$ and $\mathbf{B}_n^*$ are additive subgroups of $\mathbf{R}^+$ and ω_n is regular in $\mathbf{S}^+$, therefore

$$[\mathbf{B}_n\omega_n : \mathbf{B}_n^*\omega_n] = [\mathbf{B}_n : \mathbf{B}_n^*] = q.$$

Going to the bottom part of the diagram, we obtain

$$\mathbf{B}_n^*\omega_n \cap \mathbf{R}^+q\omega_n = \mathbf{B}_nq\omega_n.$$

Indeed, if $\xi \in \mathbf{B}_n^*\omega_n \cap \mathbf{R}^+q\omega_n$, then $\xi = y\omega_n = qz\omega_n$ where $y \in \mathbf{B}_n^*$ and $z \in \mathbf{R}^+$. Because ω_n is regular in $\mathbf{S}^+$ we obtain $qz = y$. Using the basis of $\mathbf{R}^+$, we see that $z = y/q \in \mathbf{B}_n$. Hence $\xi \in \mathbf{B}_nq\omega_n$. Conversely, $\mathbf{B}_nq\omega_n \subseteq \mathbf{B}_n^*\omega_n \cap \mathbf{R}^+q\omega_n$.

[*Remark.* If one tries to prove this lemma for group rings over the rational numbers and integers, an obstacle to the proof is encountered on the latter inclusion; for $\mathcal{B}_n \subseteq \varepsilon^+\mathcal{R}$, and $\mathcal{R}^+ \nsubseteq \varepsilon^+\mathcal{R}$ in the case where $\mathcal{R} = Z[G]$.]

Finally, $[\mathbf{R}^+q\omega_n : \mathbf{B}_nq\omega_n] = [\mathbf{R}^+ : \mathbf{B}_n]$ because ω_n is regular in $\mathbf{S}^+$. A simple calculation gives $[\mathbf{R}^+ : \mathbf{B}_n] = q$.

Applying the well-known isomorphism theorem to the diagram we obtain:

$$[\mathbf{R}^+q\omega_n + \mathbf{B}_n^*\omega_n : \mathbf{B}_n^*\omega_n] = q.$$

But we proved $[\mathbf{B}_n\omega_n : \mathbf{B}_n^*\omega_n] = q$. Therefore

$$[\mathbf{B}_n\omega_n : \mathbf{R}^+q\omega_n + \mathbf{B}_n^*\omega_n] = 1$$

or

$$\mathbf{I}_n^+ = \mathbf{B}_n\omega_n = \mathbf{R}^+q\omega_n + \mathbf{B}_n^*\omega_n.$$

§ 2

2.1. Define an additive homomorphism

$$f : \mathbf{R} \to \mathbf{R}$$

by

$$f(\sigma(a)) = a^{-1}\sigma(a), \quad 0 \leqslant a < q, \ (a, p) = 1$$

$$f(\sigma(a')) = a^{-1}\sigma(a), \quad \text{for } (a', p) = 1, \ a' \equiv a \ (q), \ 0 \leqslant a < q.$$

f extends by linearity to a Z_p-homomorphism of $\mathbf{R}$ into $\mathbf{R}$ such that $f(q\mathbf{R}) \subseteq q\mathbf{R}$. Hence f induces an additive homormorphism:

$$\bar{f} : \mathbf{R}/q\mathbf{R} \to \mathbf{R}/q\mathbf{R}.$$

$\bar{f}$ is also a multiplicative homomorphism. It is clearly injective; and since $f(a\sigma(a)) \equiv \sigma(a) \bmod q\mathbf{R}$ we have that $\bar{f}$ is surjective, and hence an automorphism. (Remark: f itself is not multiplicative.)

Let $\pi : \mathbf{R} \to \mathbf{R}/q\mathbf{R}$ be canonical coset mapping.

LEMMA 2. *If* $p \neq 2$, $p \nmid n$, *and* $p \nmid n+1$, *then*

$$\bar{f}(\pi(\mathbf{B}_n^*\omega_n)) = \pi(\mathbf{B}_{n+1}^*\omega_{n+1})$$

except in case $q = p = 3$ *and* $n = 1$.

Proof. Recall that

$$\omega_n = \textstyle\sum_a q^{n-1} B_n(a/q)\, \sigma(a)^{-1},$$

where

$$B_n(a) = a^n - \tfrac{1}{2}\, na^{n-1} + \sum_{u=1}^{[n/2]} (-1)^{u-1} C_{n,2u} B_u a^{n-2u}.$$

Hence,

$$\omega_n \equiv q^{-1} \textstyle\sum_a (a^n - \frac{1}{2}\, qna^{n-1})\, \sigma(a)^{-1} \bmod q\mathbf{R}.$$

By a simple calculation:

$$\mathbf{B}_n^*\omega_n \equiv \{q^{-1} \textstyle\sum_c [\sum_a{}' u_a (2\, R(ca^{-1})^n - qn(ca^{-1})^{n-1}]\, \sigma(c); \ u_a \in Z_p, \ \sum_a{}' a^n u_a \equiv 0 \ (q^2)\} \bmod q\mathbf{R}.$$

(The above characterization of $\mathbf{B}_n^*\omega_n$ is valid whether n is even or odd. Recall that $R(a)$ is the least positive residue of a mod q.)

Let $\alpha \in \mathbf{B}_n^*\omega_n$, then

$$f(\alpha)\equiv q^{-1}\sum_c[\sum_a' u_a(2R(c^{-1}a)^n c^{-1}-qnc^{-n}a^{n-1})]\,\sigma(c) \mod q\mathbf{R},$$

where $u_a\in Z_p$, $\sum_a' a^n u_a\equiv 0 \mod q^2 Z_p$. We wish to show that $\pi(f(\alpha))\in\pi(B_{n+1}^*\omega_{n+1})$.

For $0\leqslant a<q/2$, $(a,p)=1$, let $v_a=nu_a/(n+1)a$, then $v_a\in Z_p$ (because $p\nmid n+1$) and $\sum_a' a^{n+1}v_a\equiv 0\,(q^2)$. Let $\beta=q^{-1}\sum_c[\sum_a' v_a(2R(c^{-1}a)^{n+1}-q(n+1)(c^{-1}a)^n)]\,\sigma(c)$. Then $\beta\in\mathbf{R}$ and $\pi(\beta)\in\pi(\mathbf{B}_{n+1}^*\omega_{n+1})$. $\pi(f(\alpha))=\pi(\beta)$ if and only if $f(\alpha)\equiv\beta \mod q\mathbf{R}$ which is if and only if

$$q^{-1}\sum_c(\sum_\alpha' u_a 2R(c^{-1}a)^n c^{-1})\,\sigma(c)\equiv q^{-1}\sum_c\left(\sum_a'\frac{n}{n+1}u_a 2R(c^{-1}a)^{n+1}a^{-1}\right)\sigma(c) \mod q\mathbf{R}$$

which is true if and only if

$$\sum_a'(n+1)u_a c^{-1}R(c^{-1}a)^n\equiv\sum_a' nu_a R(c^{-1}a)^{n+1}a^{-1} \mod q^2 \qquad (*)$$

for c, $0\leqslant c<q$, $(c,p)=1$.

But $$R(c^{-1}a)^n-(c^{-1}a)^n=qt(c^{-1}a) \quad\text{and}\quad R(c^{-1}a)-(c^{-1}a)=qs(c^{-1}a)$$

for some $s(c^{-1}a)$ and $t(c^{-1}a)\in Z$. Multiplying both equations together, we have

$$R(c^{-1}a)^{n+1}-(c^{-1}a)^n R(c^{-1}a)-(c^{-1}a)R(c^{-1}a)^n+(c^{-1}a)^{n+1}\equiv 0 \mod q^2$$

or $$R(c^{-1}a)^{n+1}a^{-1}\equiv c^{-n}a^{n-1}R(c^{-1}a)+c^{-1}R(c^{-1}a)^n-c^{-(n+1)}a^n \mod q^2.$$

Substituting this result in the congruence (*), we have $f(\alpha)\equiv\beta \mod q\mathbf{R}$ if and only if

$$\sum_a' u_a c^{-1}R(c^{-1}a)^n\equiv\sum_a' nu_a[R(c^{-1}a)c^{-n}a^{n-1}-c^{-(n+1)}a^n] \mod q^2$$

for c, $0\leqslant c<q$, $(c,p)=1$. But by hypothesis $\sum' u_a a^n\equiv 0\,(q^2)$, hence $f(\alpha)\equiv\beta \mod q\mathbf{R}$ if and only if

$$\sum' u_a(c^{-1}R(c^{-1}a)^n-nR(c^{-1}a)c^{-n}a^{n-1})\equiv 0 \mod q^2 \qquad (**)$$

for c, $0\leqslant c<q$, $(c,p)=1$. But $R(c^{-1}a)=(c^{-1}a)+qt(c^{-1}a)$, $t(c^{-1}a)\in Z$; therefore

$$R(c^{-1}a)^n\equiv(c^{-1}a)^n+nq\cdot(c^{-1}a)^{n-1}\cdot t(c^{-1}a) \mod q^2.$$

Hence $$c^{-1}R(c^{-1}a)^n\equiv c^{-(n+1)}a^n+nqc^{-n}a^{n-1}t(c^{-1}a) \mod q^2$$

$$-nR(c^{-1}a)c^{-n}a^{n-1}\equiv -nc^{-(n+1)}a^n-nc^{-n}a^{n-1}qt(c^{-1}a) \mod q^2.$$

Substituting these congruences in (**) we have $f(\alpha)\equiv\beta \mod q\mathbf{R}$ if and only if: $\sum_a' u_a(1-n)a^n c^{-(n+1)}\equiv 0 \mod q^2$ for all c, $0\leqslant c<q$, $(c,p)=1$. But $\sum_a' a^n u_a\equiv 0\,(q^2)$. Thus $f(\alpha)\equiv\beta \mod q\mathbf{R}$ and hence $f(\pi(\mathbf{B}_n^*\omega_n))\subseteq\pi(\mathbf{B}_{n+1}^*\omega_{n+1})$.

Conversely, let $\pi(\beta)\in\pi(\mathbf{B}_{n+1}^*\omega_{n+1})$, then

$$\beta \equiv q^{-1} \sum_c [\sum_a' v_a (2R(c^{-1}a)^{n+1} - q(n+1)(c^{-1}a)^n)]\, \sigma(c) \mod q\mathbf{R},$$

where $v_a \in Z_p$ and $\sum_a' a^{n+1} v_a \equiv 0\ (q^2)$. Let $u_a = (n+1/n)\, a v_a$; then $u_a \in Z_p$ (for $p \nmid n$) and $\sum_a' a^n u_a \equiv 0\ (q^2)$.

Let $$\alpha = q^{-1} \sum_c [\sum_a' u_a (2R(c^{-1}a)^n - qnR(c^{-1}a)^{n-1})]\, \sigma(c)$$

then $\alpha \in \mathbf{R}$ and $\pi(\alpha) \in \pi(\mathbf{B}_n^* \omega_n)$. Then, we prove, just as in the first part of the proof, that $f(\alpha) \equiv \beta \mod q\mathbf{R}$. Thus

$$\bar{f}(\pi(\mathbf{B}_n^* \omega_n)) = \pi(\mathbf{B}_{n+1}^* \omega_{n+1})).$$

THEOREM 1. *Let $\bar{f}: \mathbf{R}/q\mathbf{R} \to \mathbf{R}/q\mathbf{R}$ be the automorphism previously defined. Let $\pi: \mathbf{R} \to \mathbf{R}/q\mathbf{R}$ be the canonical coset mapping. Suppose $p \neq 2$, $p \nmid n$ and $p \nmid n+1$, then $\bar{f}$ induces the following isomorphisms:*

$$\pi(\mathbf{R}^+)/\pi(\mathbf{I}_n^+) \cong \pi(\mathbf{R}^-)/\pi(\mathbf{I}_{n+1}^-) \qquad (n \text{ even})$$

$$\pi(\mathbf{R}^-)/\pi(\mathbf{I}_n^-) \cong \pi(\mathbf{R}^+)/\pi(\mathbf{I}_{n+1}^+) \qquad (n \text{ odd})$$

Proof. We do the proof first for n even. We first note that

$$\bar{f}(\pi(\mathbf{R}^+)) = \pi(\mathbf{R}^-)$$

for $f(\sigma(a) + \sigma(-a)) \equiv a^{-1}(\sigma(a) - \sigma(-a)) \mod q\mathbf{R}$; and thus $f(a^{-1}(\sigma(a) + \sigma(-a))) \equiv \sigma(a) - \sigma(-a) \mod q\mathbf{R}$. Sinee $\sigma(a) + \sigma(-a)$ and $\sigma(a) - \sigma(-a)$ generate $\mathbf{R}^+$ and $\mathbf{R}^-$ respectively, we have $\bar{f}(\pi(\mathbf{R}^+)) = \pi(\mathbf{R}^-)$. Secondly, because $\bar{f}$ and π are multiplicative it follows that

$$\bar{f}(\pi(\mathbf{R}^+ q\omega_n)) = \pi(\mathbf{R}^+ q\omega_{n+1})$$

since clearly $\bar{f}(\pi(q\omega_n)) = \pi(q\omega_{n+1})$.

Hence
$$\begin{aligned}
\bar{f}(\pi(\mathbf{I}_n^+)) &= \bar{f}(\pi(\mathbf{B}_n^* \omega_n + \mathbf{R}^+ q\omega_n)) \qquad \text{(Lemma 1)} \\
&= \bar{f}(\pi(\mathbf{B}_n^* \omega_n) + \pi(\mathbf{R}^+ q\omega_n)) = \bar{f}(\pi(\mathbf{B}_n^* \omega_n) + \bar{f}(\pi(\mathbf{R}^+ q\omega_n)) \\
&= \pi(\mathbf{B}_{n+1}^* \omega_{n+1}) + \pi(\mathbf{R}^- q\omega_{n+1}) \qquad \text{(Lemma 2)} \\
&= \pi(\mathbf{B}_{n+1}^* \omega_{n+1} + \mathbf{R}^- q\omega_{n+1}) = \pi(\mathbf{I}_{n+1}^-).
\end{aligned}$$

Thus $\bar{f}$ induces an isomorphism:

$$\pi(\mathbf{R}^+)/\pi(\mathbf{I}_n^+) \cong \pi(\mathbf{R}^-)/\pi(\mathbf{I}_{n+1}^-).$$

In case n is odd, everything is analogous, except for the case $n = 1$ and $q = p = 3$ where Lemma 1 is inapplicable. In case $q = p = 3$, Corollary to Proposition 3 shows that

$$[\mathbf{R}^+ : \mathbf{I}_2^+] = [\mathbf{R}^- : \mathbf{I}_1^-] = 1, \text{ so } \mathbf{R}^+ = \mathbf{I}_2^+ \text{ and } \mathbf{R}^- = \mathbf{I}_1^-$$

and the isomorphism still holds.

COROLLARY. *If* $p \neq 2$, $p \nmid n$, *and* $p \nmid n+1$, *then*

(1) $p \mid [R^- : \mathbf{I}_n^-]$ *if and only if* $p \mid [\mathbf{R}^+ : \mathbf{I}_{n+1}^+]$ (n *odd*)

(1′) $p \mid [\mathbf{R}^+ : \mathbf{I}_n^+]$ *if and only if* $p \mid [\mathbf{R}^- : \mathbf{I}_{n+1}^-]$ (n *even*).

Otherwise stated,

(2) $p \mid q(\prod_{\substack{\chi \bmod q \\ \chi(-1)=-1}} B_\chi^n)_p$ *if and only if* $p \mid q(\prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} B_\chi^{n+1})_p$ (n *odd*)

(2′) $p \mid q(\prod_{\substack{\chi \bmod q \\ \chi(-1)=1}} B_\chi^n)_p$ *if and only if* $p \mid q(\prod_{\substack{\chi \bmod q \\ \chi(-1)=-1}} B_\chi^{n+1})_p$ (n *even*).

Proof. Reformulations (2) and (2′) follow from (1) and (1′) by Corollary to Proposition 3. We prove only (1), since (1′) is proved completely analogously. Define a homomorphism:

$$\theta : \mathbf{R}^-/\mathbf{I}_n^- \to \mathbf{R}^-/(\mathbf{I}_n^- + q\mathbf{R}^-)$$

$$\theta(x + \mathbf{I}_n^-) = x + (\mathbf{I}_n^- + q\mathbf{R}^-) \quad (x \in \mathbf{R}^-)$$

θ induces an isomorphism

$$\tilde{\theta} : (\mathbf{R}^-/\mathbf{I}_n^-)/q(\mathbf{R}^-/\mathbf{I}_n^-) \to \mathbf{R}^-/(\mathbf{I}_n^- + q\mathbf{R}^-)$$

Define a homomorphism

$$\psi : \mathbf{R}^-/(\mathbf{I}_n^- + q\mathbf{R}^-) \to \pi(\mathbf{R}^-)/\pi(\mathbf{I}_n^-)$$

by $$\psi(x + (\mathbf{I}_n^- + q\mathbf{R}^-)) = \pi(x) + \pi(\mathbf{I}_n^-) \quad (x \in \mathbf{R}^-).$$

ψ is an isomorphism. Hence,

$$\psi \circ \tilde{\theta} : (\mathbf{R}^-/\mathbf{I}_n^-)/q(\mathbf{R}^-/\mathbf{I}_n^-) \to \pi(\mathbf{R}^-)/\pi(\mathbf{I}_n^-)$$

is an isomorphism. Analogously,

$$(\mathbf{R}^+/\mathbf{I}_{n+1}^+)/q(\mathbf{R}^+/\mathbf{I}_{n+1}^+) \cong \pi(\mathbf{R}^+)/\pi(\mathbf{I}_{n+1}^+).$$

From the isomorphism of Theorem 1, just derived, we have the following isomorphism:

$$(\mathbf{R}^-/\mathbf{I}_n^-)/q(\mathbf{R}^-/\mathbf{I}_n^-) \cong (\mathbf{R}^+/\mathbf{I}_{n+1}^+)/q(\mathbf{R}^+/\mathbf{I}_{n+1}^+).$$

It is clear from Corollary to Proposition 3 that $\mathbf{R}^-/\mathbf{I}_n^-$ and $\mathbf{R}^+/\mathbf{I}_{n+1}^+$ are additive p-groups. Therefore, $p \mid [\mathbf{R}^- : \mathbf{I}_n^-]$ if and only if $\mathbf{R}^-/\mathbf{I}_n^- \neq q(\mathbf{R}^-/\mathbf{I}_n^-)$ which is if and only if $\mathbf{R}^+/\mathbf{I}_{n+1}^+ \neq q(\mathbf{R}^+/\mathbf{I}_{n+1}^+)$ which is if and only if $p \mid [\mathbf{R}^+ : \mathbf{I}_{n+1}^+]$.

5 – 682903 *Acta mathematica.* 121. Imprimé le 18 septembre 1968.

2.2. Until now we have considered $q=p^m$ to be defined for some fixed integer m, $m\geqslant 1$. We now consider m to vary and let $q_m=p^m$, $m\geqslant 1$, $p\neq 2$. Let ζ_m be a primitive q_mth root of unity. Let $F_m=Q(\zeta_m)$, and let $G_m=$ Galois group of F_m over Q. Let $\sigma(a)_m\in G_m$, $(a,p)=1$, be the automorphism of F_m over Q such that $\sigma(a)_m(\zeta_m)=\zeta_m^a$.

Let
$$\mathbf{S}_m = Q_p[G_m], \quad \mathbf{R}_m = Z_p[G_m],$$
$$\varepsilon_m^- = \tfrac{1}{2}(\sigma(1)_m-\sigma(-1)_m), \quad \varepsilon_m^+ = \tfrac{1}{2}(\sigma(1)_m+\sigma(-1)_m)$$
$$\mathbf{R}_m^- = \varepsilon_m^-\mathbf{R}_m, \quad \mathbf{R}_m^+ = \varepsilon_m^+\mathbf{R}_m$$
$${}_m\omega_n = q_m^{n-1}\sum_{\substack{0\leqslant a<q_m\\(a,p)=1}} B_n(a/q_m)\,\sigma(a)_m^{-1}$$
$${}_m\mathbf{I}_n^- = \mathbf{R}_m^- \cap \mathbf{R}_m\,{}_m\omega_n \ (n \text{ odd}), \quad {}_m\mathbf{I}_n^+ = \mathbf{R}_m^+ \cap \mathbf{R}_m\,{}_m\omega_n \ (n \text{ even}).$$

Let
$${}_m\mathbf{B}_n = \Big\{\sum_{\substack{0\leqslant a<q_m/2\\(a,p)=1}} u_a(\sigma(a)_m-\sigma(-a)_m)\,\Big|\,u_a\in Z_p,\ \sum_{\substack{0\leqslant a<q_m/2\\(a,p)=1}} a^n u_a\equiv 0\ (q_m)\Big\} \quad (n \text{ odd}),$$
$${}_m\mathbf{B}_n = \Big\{\sum_{\substack{0\leqslant a<q_m/2\\(a,p)=1}} u_a(\sigma(a)_m+\sigma(-a)_m)\,\Big|\,u_a\in Z_p,\ \sum_{\substack{0\leqslant a<q_m/2\\(a,p)=1}} a^n u_a\equiv 0\ (q_m)\Big\} \quad (n \text{ even})$$

then ${}_m\mathbf{I}_n^- = {}_m\mathbf{B}_n\cdot{}_m\omega_n$ (n odd), ${}_m\mathbf{I}_n^+ = {}_m\mathbf{B}_n\cdot{}_m\omega_n$ (n even). $\{\mathbf{S}_m\}_{m\geqslant 1}$, $\{\mathbf{R}_m\}_{m\geqslant 1}$, $\{\mathbf{R}_m^-\}_{m\geqslant 1}$, $\{\mathbf{R}_m^+\}_{m\geqslant 1}$, $\{{}_m\mathbf{I}_n^-\}_{m\geqslant 1}$ (for fixed odd n), $\{{}_m\mathbf{I}_n^+\}_{m\geqslant 1}$ (for fixed even n), form inverse systems with respect to homomorphisms to be defined presently.

Define
$$t_{m,m+1}:\mathbf{S}_{m+1}\to\mathbf{S}_m \quad (m\geqslant 1)$$

by
$$t_{m,m+1}\Big(\sum_{0\leqslant a<q_{m+1}} x_a\,\sigma(a)_{m+1}\Big) = \sum_{0\leqslant a<q_{m+1}} x_a\,\sigma(a)_m \quad (x_a\in Q_p).$$

(It will be understood that all summations are over integers prime to p.) $t_{m,m+1}$ is clearly additive ($m\geqslant 1$). It is also multiplicative. Clearly, $t_{m,m+1}(\mathbf{R}_{m+1}^+)=\mathbf{R}_m^+$, $t_{m,m+1}(\mathbf{R}_{m+1}^-)=\mathbf{R}_m^-$. We now take a fixed even n. Let $\tau(a)_m=\sigma(a)_m+\sigma(q_m-a)_m$, then

$${}_{m+1}\mathbf{B}_n = \Big\{\sum_{\substack{0\leqslant a<q_{m+1}/2\\(a,p)=1}} u_a\,\tau(a)_{m+1}\,\Big|\,u_a\in Z_p,\ \sum_{0\leqslant a<q_{m+1}/2} a^n u_a\equiv 0\ (q_{m+1})\Big\}.$$

We will show $t_{m,m+1}({}_{m+1}\mathbf{B}_n)\subseteq{}_m\mathbf{B}_n$. Indeed,

$$t_{m,m+1}\Big(\sum_{0\leqslant a<q_{m+1}/2} u_a\,\tau(a)_{m+1}\Big) = t_{m,m+1}\Big(\sum_{\substack{0\leqslant a<q_{m+1}/2\\a\equiv b(q_m)\\0\leqslant b<q_m/2}} u_a\,\tau(a)_{m+1} + \sum_{\substack{0\leqslant a<q_{m+1}/2\\a\equiv b(q_m)\\q_m/2\leqslant b<q_m}} u_a\,\tau(a)_{m+1}\Big)$$

$$= \sum_{0\leqslant b<q_m/2}\Big(\sum_{\substack{0\leqslant a<q_{m+1}/2\\ a\equiv b(q_m)}} u_a\Big)\,\tau(b)_m + \sum_{q_m/2\leqslant b<q_m}\Big(\sum_{\substack{0\leqslant a<q_{m+1}/2\\ a\equiv b(q_m)}} u_a\Big)\,\tau(b)_m$$

$$= \sum_{0\leqslant b<q_m/2}\Big(\sum_{\substack{0\leqslant a<q_{m+1}/2\\ a\equiv b(q_m)}} u_a\Big)\,\tau(b)_m + \sum_{0\leqslant b<q_m/2}\Big(\sum_{\substack{0\leqslant a'<q_{m+1}/2\\ a'\equiv -b(q_m)}} u_{a'}\Big)\,\tau(b)_m$$

(for $\tau(-b)_m=\tau(b)_m$)

$$= \sum_{0\leqslant b<q_m/2}\Big(\sum_{\substack{0\leqslant a<q_{m+1}/2\\ a\equiv b(q_m)}} u_a + \sum_{\substack{0\leqslant a'<q_{m+1}/2\\ a'\equiv -b(q_m)}} u_{a'}\Big)\,\tau(b)_m.$$

To show that $t_{m,\,m+1}\big(\sum_{0\leqslant a<q_{m+1}/2} u_a\,\tau(a)_{m+1}\big)\in {}_m\mathbf{B}_n$, we must show that

$$\sum_{0\leqslant b<q_m/2} b^n\Big(\sum_{\substack{0\leqslant a<q_{m+1}/2\\ a\equiv b(q_m)}} u_a + \sum_{\substack{0\leqslant a'<q_{m+1}/2\\ a'\equiv -b(q_m)}} u_{a'}\Big)\equiv 0\ (q_m).$$

By hypothesis $\sum_{0\leqslant a<q_{m+1}/2} a^n u_a\equiv 0\ (q_{m+1})$. Hence $\sum_{0\leqslant a<q_{m+1}/2} a^n u_a\equiv 0\ (q_m)$. Thus

$$0\equiv \sum_{\substack{0\leqslant a<q_{m+1}/2\\ a\equiv b(q_m)\\ 0\leqslant b<q_m/2}} a^n u_a + \sum_{\substack{0\leqslant a<q_{m+1}/2\\ a\equiv b(q_m)\\ q_m/2\leqslant b<q_m}} a^n u_a$$

$$\equiv \sum_{0\leqslant b<q_m/2} b^n\Big(\sum_{\substack{0\leqslant a<q_{m+1}/2\\ a\equiv b(q_m)}} u_a\Big) + \sum_{0\leqslant b<q_m/2}(q_m-b)^n\Big(\sum_{\substack{0\leqslant a<q_{m+1}/2\\ a\equiv -b(q_m)}} u_a\Big)$$

$$\equiv \sum_{0\leqslant b<q_m/2} b^n\Big(\sum_{\substack{0\leqslant a<q_{m+1}/2\\ a\equiv b(q_m)}} u_a + \sum_{\substack{0\leqslant a'<q_{m+1}/2\\ a'\equiv -b(q_m)}} u_{a'}\Big) \bmod q_m$$

(because n is even, so $(q_m-b)^n\equiv b^n \bmod q_m$), which implies what we wanted to prove; hence, $t_{m.\,m+1}({}_{m+1}\mathbf{B}_n)\subseteq {}_m\mathbf{B}_n$. A quite similar argument is valid for n odd.

Secondly,

$$t_{m,\,m+1}({}_{m+1}\omega_n) = t_{m,\,m+1}\Big(q_{m+1}^{n-1}\sum_{0\leqslant a<q_{m+1}} B_n(a/q_{m+1})\,\sigma(a)_{m+1}^{-1}\Big)$$

$$= q_{m+1}^{n-1}\sum_{0\leqslant a<q_m}\Big(\sum_{\substack{0\leqslant b<q_{m+1}\\ b\equiv a(q_m)}} B_n(b/q_{m+1})\Big)\,\sigma(a)_m^{-1}$$

$$= q_{m+1}^{n-1}\sum_{0\leqslant a<q_m}\left(\sum_{t=0}^{p-1} B_n\left(\frac{a+q_m t}{q_{m+1}}\right)\right)\sigma(a)_m^{-1}$$

$$= q_{m+1}^{n-1}\sum_{0\leqslant a<q_m} p^{1-n}\left(p^{n-1}\sum_{t=0}^{p-1} B_n\left(\frac{a}{q_{m+1}}+\frac{t}{p}\right)\right)\sigma(a)_m^{-1} \quad \text{(by A 3)}$$

$$= q_{m+1}^{n-1} \sum_{0 \leqslant a < q_m} p^{1-n} B_n(p \cdot a/q_{m+1})\, \sigma(a)_m^{-1}$$

$$= q_m^{n-1} \sum_{0 \leqslant a < q_m} B_n(a/q_m)\, \sigma(a)_m^{-1} = {}_m\omega_n$$

that is, $t_{m,m+1}({}_{m+1}\omega_n) = {}_m\omega_n$.

Because $t_{m,m+1}$ is multiplicative, we have that

$$t_{m,m+1}({}_{m+1}\mathbf{I}_n^+) = t_{m.m+1}({}_{m+1}\mathbf{B}_n)\, t_{m,m+1}({}_{m+1}\omega_n) \subseteq {}_m\mathbf{B}_n \cdot {}_m\omega_n = {}_m\mathbf{I}_n^+$$

for n even. Similarly for n odd.

If we compose the maps $t_{m,m+1}$ we thus obtain by suitable restriction the maps of our inverse system.

2.3. Let $\pi_m : \mathbf{R}_m \to \mathbf{R}_m/q_m\mathbf{R}_m$ be the canonical coset map ($m \geqslant 1$). Since $t_{m,m+1}(q_{m+1}\mathbf{R}_{m+1}) \subseteq q_m\mathbf{R}_m$, we have that $t_{m,m+1}$ induces a map $t_{m,m+1} : \pi_{m+1}(\mathbf{R}_{m+1}) \to \pi_m(\mathbf{R}_m)$ given by:

$$t_{m,m+1}\Big(\sum_{0 \leqslant a < q_{m+1}} x_a \sigma(a)_{m+1}\Big) \equiv \sum_{0 \leqslant a < q_{m+1}} x_a \sigma(a)_m \mod q_m\mathbf{R}_m \quad (x_a \in Z_p).$$

By abuse of notation, we denote the homomorphisms of our inverse systems $\{\pi_m(\mathbf{R}_m)\}_{m\geqslant}$ by $t_{m,m+1}$. Clearly $\{\pi_m(\mathbf{R}_m^-)\}$, $\{\pi_m(\mathbf{R}_m^+)\}$, $\{\pi_m({}_n\mathbf{I}_m^+)\}$ (n even), $\{\pi_m({}_n\mathbf{I}_m^-)\}$ (n odd) ($m \geqslant 1$) form inverse systems with respect to these homomorphisms. We therefore also have that the finite p-groups $\mathbf{R}_m^+/{}_m\mathbf{I}_n^+$, $\mathbf{R}_m^-/{}_m\mathbf{I}_n^-$, $\pi_m(\mathbf{R}_m^+)/\pi_m({}_m\mathbf{I}_n^+)$, $\pi_m(\mathbf{R}_m^-)/\pi_m({}_m\mathbf{I}_n^-)$ ($m \geqslant 1$) all form inverse systems of groups with respect to the homomorphisms $t_{m,m+1}$ (for the finiteness of these groups v. Corollary to Proposition 3 and the proof of Corollary to Theorem 1). What is more, if we endow our finite groups with the discrete topology then our groups are compact and our homomorphisms $t_{m,m+1}$ are continuous.

As in Section 2.1, we define for $m \geqslant 1$, the automorphism $\bar{f}_m : \mathbf{R}_m/q_m\mathbf{R}_m \to \mathbf{R}_m/q_m\mathbf{R}_m$ by

$$\bar{f}(\sigma(a)_m + q_m\mathbf{R}_m) = a^{-1}\sigma(a)_m + q_m\mathbf{R}_m$$

and then extend by linearity to the whole ring.

Clearly, $t_{m,m+1} \circ \bar{f}_{m+1} = \bar{f}_m \circ t_{m,m+1}$. On the other hand (v. Theorem 1), we have proved that if $p \neq 2$, $p \nmid n$, $p \nmid n+1$ then $\bar{f}_m$ induces isomorphisms:

$$\bar{f}_m : \pi_m(\mathbf{R}_m^-)/\pi_m({}_m\mathbf{I}_n^-) \cong \pi_m(\mathbf{R}_m^+)/\pi_m({}_m\mathbf{I}_{n+1}^+) \quad (n \text{ odd})$$

$$\bar{f}_m : \pi_m(\mathbf{R}_m^+)/\pi_m({}_m\mathbf{I}_n^+) \cong \pi_m(\mathbf{R}_m^-)/\pi_m({}_m\mathbf{I}_{n+1}^-) \quad (n \text{ even})$$

(for all $m \geqslant 1$). Because $\bar{f}_m$ and $t_{m,m+1}$ commute, we have that $\{\bar{f}_m\}_{m\geqslant 1}$ is a map of the inverse system

$$\{\pi_m(\mathbf{R}_m^-)/\pi_m({}_m\mathbf{I}_n^-)\}_{m\geqslant 1} \text{ into } \{\pi_m(\mathbf{R}_m^+)/\pi_m({}_m\mathbf{I}_{n+1}^+)\}_{m\geqslant 1} \quad (n \text{ odd})$$

and $\{\pi_m(\mathbf{R}_m^+)/\pi_m({}_m\mathbf{I}_n^+)\}_{m\geq 1}$ into $\{\pi_m(\mathbf{R}_m^-)/\pi_m({}_m\mathbf{I}_{n+1}^-)\}_{m\geq 1}$ (n even).

Hence when we pass to the inverse limit we have that the isomorphism is preserved and therefore if $p \nmid n$, $p \nmid n+1$, $p \neq 2$

$$\lim_m \pi_m(\mathbf{R}_m^-)/\pi_m({}_m\mathbf{I}_n^-) \cong \lim_m \pi_m(\mathbf{R}_m^+)/\pi_m({}_m\mathbf{I}_{n+1}^+) \quad \text{(inverse limit) } (n \text{ odd}) \qquad (*)$$

$$\lim_m \pi_m(\mathbf{R}_m^+)/\pi_m({}_m\mathbf{I}_n^+) \cong \lim_m \pi_m(\mathbf{R}_m^-)/\pi_m({}_m\mathbf{I}_{n+1}^-) \quad \text{(inverse limit) } (n \text{ even}). \qquad (*)$$

On the other hand, we have from the proof of Corollary to Theorem 1 that

$$(\mathbf{R}_m^-/{}_m\mathbf{I}_n^-)/q_m(\mathbf{R}_m^-/{}_m\mathbf{I}_n^-) \cong \pi_m(\mathbf{R}_m^-)/\pi_m({}_m\mathbf{I}_n^-) \quad (n \text{ odd})$$
$$(\mathbf{R}_m^+/{}_m\mathbf{I}_n^+)/q_m(\mathbf{R}_m^+/{}_m\mathbf{I}_n^+) \cong \pi_m(\mathbf{R}_m^+)/\pi_m({}_m\mathbf{I}_n^+) \quad (n \text{ even}).$$

Furthermore, the isomorphisms involved commute with $t_{m,m+1}$, hence when we pass to the limit we have

$$\lim_m (\mathbf{R}_m^-/{}_m\mathbf{I}_n^-)/q_m(\mathbf{R}_m^-/{}_m\mathbf{I}_n^-) \cong \lim_m \pi_m(\mathbf{R}_m^-)/\pi_m({}_m\mathbf{I}_n^-) \quad (n \text{ odd}))$$
$$\lim_m (\mathbf{R}_m^+/{}_m\mathbf{I}_n^+)/q_m(\mathbf{R}_m^+/{}_m\mathbf{I}_n^+) \cong \lim_m \pi_m(\mathbf{R}_m^+)/\pi_m({}_m\mathbf{I}_n^+) \quad (n \text{ even})$$

Combining these results with (*) we have that, if $p \nmid n$, $p \nmid n+1$, $p \neq 2$ then

$$\lim_m (\mathbf{R}_m^-/{}_m\mathbf{I}_n^-)/q_m(\mathbf{R}_m^-/{}_m\mathbf{I}_n^-) \cong \lim_m (\mathbf{R}_m^+/{}_m\mathbf{I}_{n+1}^+)/q_m(\mathbf{R}_m^+/{}_m\mathbf{I}_{n+1}^+) \quad (n \text{ odd})$$

and $$\lim_m (\mathbf{R}_m^+/{}_m\mathbf{I}_n^+)/q_m(\mathbf{R}_m^+/{}_m\mathbf{I}_n^+) \cong \lim_m (\mathbf{R}_m^-/{}_m\mathbf{I}_{n+1}^-)/q_m(\mathbf{R}_m^-/{}_m\mathbf{I}_{n+1}^-) \quad (n \text{ even}).$$

Because all the factor groups involved are compact, the operations of passing to the inverse limit and constructing factor groups commute. Hence if we can show

$$\lim_m q_m(\mathbf{R}_m^-/{}_m\mathbf{I}_n^-) = 0 \quad (n \text{ odd})$$
$$\lim_m q_m(\mathbf{R}_m^+/{}_m\mathbf{I}_n^+) = 0 \quad (n \text{ even}),$$

then we will have proved that if $p \nmid n$, $p \nmid n+1$, $p \neq 2$

$$\lim_m \mathbf{R}_m^-/{}_m\mathbf{I}_n^- \cong \lim_m \mathbf{R}_m^+/{}_m\mathbf{I}_{n+1}^+ \quad \text{(inverse limit) } (n \text{ odd})$$
$$\lim_m \mathbf{R}_m^+/{}_m\mathbf{I}_n^+ \cong \lim_m \mathbf{R}_m^-/{}_m\mathbf{I}_{n+1}^- \quad \text{(inverse limit) } (n \text{ even}).$$

We show that $\lim_m q_m(\mathbf{R}_m^-/{}_m\mathbf{I}_n^-) = 0$ (n odd) (proof same for n even). Indeed, if

$$(u_m)_{m\geqslant 1} \in \lim_m q_m(\mathbf{R}_m^-/{}_m\mathbf{I}_n^-),$$

then for any $m \geqslant 1$, and for any $r > m$,

$$u_m = t_{m,m+1} \cdots t_{r-1,r}(q_r v_r) = q_r t_{m,m+1} \cdots t_{r-1,r}(v_r) \quad (u_m \in q_m(\mathbf{R}_m^-/{}_m\mathbf{I}_n^-),\ v_r \in \mathbf{R}_r^-/{}_r\mathbf{I}_n^-).$$

Suppose order $(\mathbf{R}_m^-/{}_m\mathbf{I}_n^-) = q_{r_0}$ (recall $\mathbf{R}_m^-/{}_m\mathbf{I}_n^-$ is a p-group). Let $r > \max(m, r_0)$, then

$$u_m = q_r t_{m,m+1} \cdots t_{r-1,r}(v_r) = q_{r-r_0}(q_{r_0} t_{m,m+1} \cdots t_{r-1,r}(v_r)) = q_{r-r_0} \cdot 0 = 0.$$

Thus $(u_m)_{m\geqslant 1} = (0)_{m\geqslant 1}$ or $\lim_m q_m(\mathbf{R}_m^-/{}_m\mathbf{I}_n^-) = 0$. Hence we have proved:

THEOREM 2. *If $p \nmid n$, $p \nmid n+1$ and $p \neq 2$, then*

$$\lim_m \mathbf{R}_m^-/{}_m\mathbf{I}_n^- \cong \lim_m \mathbf{R}_m^+/{}_m\mathbf{I}_{n+1}^+ \quad (\textit{inverse limit})\ (n\ \textit{odd})$$

$$\lim_m \mathbf{R}_m^+/{}_m\mathbf{I}_n^+ \cong \lim_m \mathbf{R}_m^-/{}_m\mathbf{I}_{n+1}^- \quad (\textit{inverse limit})\ (n\ \textit{even}).$$

2.4. Recall that $q_m = p^m$, $p \neq 2$, ζ_m is a primitive q_mth root of unity, $F_m = Q(\zeta_m)$, and $G_m = G(F_m/Q)$. Now let $F = \bigcup_{m\geqslant 1} F_m$. Then F/Q is an abelian extension. Let $G = G(F/Q)$. Further, let $\Phi_m = Q_p(\zeta_m)$ $(m \geqslant 1)$; let U be the multiplicative group of all p-adic units in Q. There exists an isomorphism $\varkappa : G \to U$ such that $\zeta^\sigma = \zeta^{\varkappa(\sigma)}$ for any $\sigma \in G$ and ζ any q_mth root of unity $(m \geqslant 1)$ in F. Let $\tau \in G$ be such that $\varkappa(\tau) = -1$. (There is no need to worry about confusing this τ with previously defined τ in Section 1.1 or $\sigma(-1)_m$.)

Let $\varepsilon^+ = \frac{1}{2}(1+\tau)$, $\varepsilon^- = \frac{1}{2}(1-\tau)$; then ε^+, $\varepsilon^- \in Z_p[G]$. If M is a $Z_p[G]$-module, we define submodules of M by $M^+ = \varepsilon^+ M$, $M^- = \varepsilon^- M$ (our notation is slightly different from Iwasawa [4]). If T is a commutative ring and H is any group, let $T[H]$ be the group ring of H over T. If there is a homomorphism $G \to H$, we also make $T[H]$ into a G-module by defining $\sigma(\sum_{\varrho\in H} a_\varrho \varrho)$ $(a_\varrho \in T,\ \sigma \in G)$ to be $\sum_{\varrho\in H} a_\varrho s\varrho$ where s denotes the image of σ under $G \to H$. Hence $\mathbf{R}_m$ and $\mathbf{S}_m$ are both G-modules by means of the natural homomorphism $G \to G_m$, hence also $Z_p[G]$-modules.

If M_1 and M_2 are $Z_p[G]$-modules and if $h : M_1 \to M_2$ is such that

(i) $h(x+y) = h(x) + h(y)$ $(x, y \in M_1)$

(ii) $h(x^\sigma) = \varkappa(\sigma)\, h(x)^\sigma$ $(\sigma \in G)$

then h will be called a $\varkappa$-homomorphism. The definition of a $\varkappa$-isomorphism of two $Z_p[G]$-modules is clear.

Iwasawa introduces (v. [4]) two $Z_p[G]$-modules (among others) $\mathfrak{X}$ and $\mathfrak{Z}$ which are defined as inverse limits of certain subgroups $\mathfrak{X}_m$ and $\mathfrak{Z}_m$ respectively of the additive group of Φ_m, $m \geqslant 1$; $\mathfrak{Z}$ is a sub-module of $\mathfrak{X}$. He also introduces two $Z_p[G]$-modules $\mathfrak{A}$ and $\mathfrak{B}$ which are defined as inverse limits of certain submodules $\mathfrak{A}_m$ and $\mathfrak{B}_m$ respectively of the $Z_p[G]$-modules $\mathbf{S}_m$, $m \geqslant 1$. In detail, let $\mathfrak{R}_m^0$ denote the sub-module of all $\sum_\sigma a_\sigma \sigma$ ($\sigma \in G$, $a_\sigma \in Z_p$) in $\mathbf{R}_m$ such that $\sum_\sigma a_\sigma = 0$, and let

$$\mathfrak{A}_m = \mathfrak{B}_m + \mathfrak{R}_m^0, \quad \mathfrak{B}_m = \mathbf{R}_m \xi_m,$$

where

$$\xi_m = q_m^{-1} \sum_a \left(a - \frac{q_m - p}{2}\right) \sigma(a)_m, \quad 0 \leqslant a < q_m, \quad (a, p) = 1.$$

It is then shown that there exists a $Z_p[G]$-isomorphism of

$$\mathfrak{A}_m \to \mathfrak{X}_m, \quad \mathfrak{B}_m \to \mathfrak{Z}_m, \quad \mathfrak{A}_m/\mathfrak{B}_m \to \mathfrak{X}_m/\mathfrak{Z}_m \quad (m \geqslant 1).$$

Since the isomorphism commutes with the homomorphisms of the associated inverse systems, we have that the isomorphism induces a $Z_p[G]$-isomorphism of $\mathfrak{A}/\mathfrak{B} \to \mathfrak{X}/\mathfrak{Z}$ ([4], Theorem 2). Furthermore, the algebra $\mathbf{S}_m$ has an involution $\alpha \to \alpha^*$ such that $\sigma^* = \sigma^{-1}$ for any $\sigma \in G_m$. If we denote by $\mathfrak{A}^*$ the inverse limit of $\mathfrak{A}_m^*$, $m \geqslant 1$, then the maps $\mathfrak{A}_m \to \mathfrak{A}_m^*$, $m \geqslant 1$ define a Z_p-isomorphism (not a G-isomorphism) $\mathfrak{A} \to \mathfrak{A}^*$ such that $(\sigma\alpha)^* = \sigma^{-1}\alpha^*$ ($\sigma \in G$, $\alpha \in \mathfrak{A}$). The inverse limit of $\mathfrak{B}_m^*$, $m \geqslant 1$, gives a $Z_p[G]$-submodule $\mathfrak{B}^*$ of $\mathfrak{A}^*$; the above isomorphism induces similar isomorphisms $\mathfrak{B} \to \mathfrak{B}^*$ and $\mathfrak{A}/\mathfrak{B} \to \mathfrak{A}^*/\mathfrak{B}^*$ (again not G-isomorphisms).

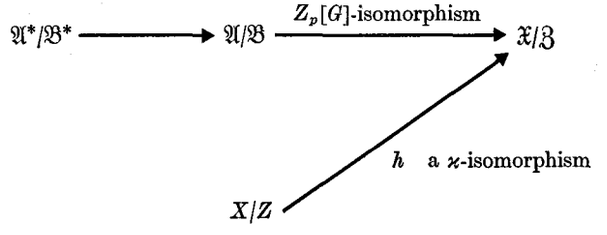
Iwasawa further introduces two more $Z_p[G]$-modules X and Z. They are defined as the inverse limit of certain subgroups X_m and Z_m respectively of the multiplicative group of non-zero elements in Φ_m, $m \geqslant 1$; Z is a submodule of X. He then defines a $\varkappa$-isomorphism

$$h : X \to \mathfrak{X}$$

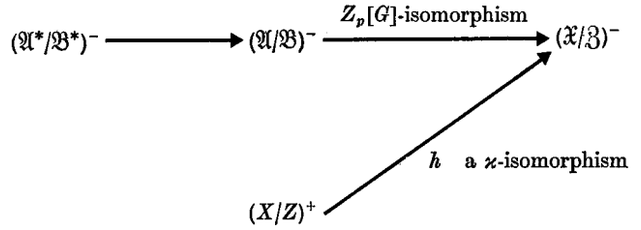
such that $h(Z) = \mathfrak{Z}$, and hence h induces a $\varkappa$-isomorphism

$$h : X/Z \to \mathfrak{X}/\mathfrak{Z}.$$

Putting all the isomorphisms together we have the following diagram:



Because $(\varepsilon^{\pm})^* = \varepsilon^{\pm}$, and $h(x^{\tau}) = \varkappa(\tau)\, h(x)^{\tau} = -h(x)^{\tau}$, we have the following diagram of isomorphisms:



Iwasawa (Prop. 1 and Prop. 2, [4]) gives the algebraic structure of $\mathfrak{A}/\mathfrak{B}$ and hence the algebraic structure of $\mathfrak{X}/\mathfrak{Z}$. However, since $h: X/Z \to \mathfrak{X}/\mathfrak{Z}$ is only a $\varkappa$-isomorphism, knowing the structure of $\mathfrak{X}/\mathfrak{Z}$ does not provide us with such knowledge of X/Z. As asserted in the introduction, in order to study $(X/Z)^+$ in particular, it would suffice to find a $Z_p[G]$-module M whose structure is known and for which we have a $\varkappa$-isomorphism of $M \to (\mathfrak{X}/\mathfrak{Z})^-$ or $(\mathfrak{A}/\mathfrak{B})^-$; indeed, we would have induced a $Z_p[G]$-isomorphism $M \to (X/Z)^+$ and we could then recover the structure of $(X/Z)^+$. Our ultimate goal had been to find such an M. Our M was supposed to have been $\lim \mathbf{R}_m^+/{}_m\mathbf{I}_2^+$. We do obtain an isomorphism of $\lim \mathbf{R}_m^+/{}_m\mathbf{I}_2^+ \to (\mathfrak{X}/\mathfrak{Z})^-$, but it is not a $\varkappa$-isomorphism as we will presently see.

It follows immediately from the definitions of $\mathfrak{A}_m$ and $\mathfrak{B}_m$ that ([4], p. 76):

$$\mathfrak{A}_m^{*-}/\mathfrak{B}_m^{*-} \cong \mathbf{R}_m^-/(\mathbf{R}_m^- \cap \mathbf{R}_m \xi_m).$$

Because $\xi_m = {}_m\omega_1 + \frac{1}{2}\, q_{m-1}^{-1} \sum_{\substack{0 \leqslant a < q_m \\ (a,p)=1}} \sigma(a)_m$, we have

$${}_m\mathbf{I}_1^- = {}_m\mathbf{B}_1\, {}_m\omega_1 \subseteq \mathbf{R}_m^- \cap \mathbf{R}_m \xi_m \quad \text{(v. Corollary to Prop. 3.)}$$

Thus we have an epimorphism of finite groups:

$$\mathbf{R}_m^-/{}_m\mathbf{I}_1^- \to \mathbf{R}_m^-/(\mathbf{R}_m^- \cap \mathbf{R}_m \xi_m).$$

The order of $\mathbf{R}_m^-/{}_m\mathbf{I}_1^- = q_m\Big(\prod_{\substack{\chi \bmod q_m \\ \chi(-1)=-1}} B_{\chi}^1\Big)_p$ (v. Corollary to Prop. 3.)

The order of

$$\begin{aligned}\mathbf{R}_m^-/\mathbf{R}_m^- \cap \mathbf{R}_m \xi_m &= \text{order } \mathfrak{A}_m^{*-}/\mathfrak{B}_m^{*-} \quad \text{(by isomorphism)} \\ &= \text{order } \mathfrak{A}_m^-/\mathfrak{B}_m^- \quad \text{(again by isomorphism)} \\ &= \text{exact power of } p \text{ dividing the first factor} \\ &\quad h_m^- \text{ of the class number of } F_m \text{ (v. [4], Prop. 4)}\end{aligned}$$

$$= q_m\Big(\prod_{\substack{\chi \bmod p_m \\ \chi(-1)=-1}} B_\chi^1\Big)_p \qquad \text{(v. [3], p. 171 and proof of Corollary to Proposition 3 of this paper.)}$$

Thus, $$\mathbf{R}_m^-/{}_m\mathbf{I}_1^- \cong \mathbf{R}_m^-/(\mathbf{R}_m^- \cap \mathbf{R}_m \xi_m) \quad (m \geqslant 1).$$

And hence, for each $m \geqslant 1$, we have a $Z_p[G]$-isomorphism

$$\mathfrak{A}_m^{*-}/\mathfrak{B}_m^{*-} \to \mathbf{R}_m^-/{}_m\mathbf{I}_1^-;$$

furthermore, this isomorphism commutes with the homomorphisms of the associated inverse systems. Therefore,

$$\lim \mathfrak{A}_m^{*-}/\mathfrak{B}_m^{*-} \cong \lim \mathbf{R}_m^-/{}_m\mathbf{I}_1^- \quad (Z_p[G]\text{-isomorphism}).$$

But $(\mathfrak{A}^*/\mathfrak{B}^*)^- = \lim \mathfrak{A}_m^{*-}/\mathfrak{B}_m^{*-}$, thus we have that

$$\lim \mathbf{R}_m^-/{}_m\mathbf{I}_1^- \cong (\mathfrak{A}^*/\mathfrak{B}^*)^- \quad (Z_p[G]\text{-isomorphism}).$$

Recall from Theorem 2 that since $p \nmid 1$, $p \nmid 2$ we have an isomorphism of $\lim \mathbf{R}_m^+/{}_m\mathbf{I}_2^+ \to \lim \mathbf{R}_m^-/{}_m\mathbf{I}_1^-$. Call this isomorphism u. A little consideration of how u was constructed shows that u is a $\varkappa$-isomorphism. We thus have the following diagram:

$$\lim \mathbf{R}_m^+/{}_m\mathbf{I}_2^+ \xrightarrow{u} \lim \mathbf{R}_m^-/{}_m\mathbf{I}_1^- \to (\mathfrak{A}^*/\mathfrak{B}^*)^- \to (\mathfrak{A}/\mathfrak{B})^- \to (\mathfrak{X}/\mathfrak{Z})^-$$
$$\nearrow h$$
$$(X/Z)^+$$

If we compose the maps from $\lim \mathbf{R}_m^+/{}_m\mathbf{I}_2^+ \to (\mathfrak{X}/\mathfrak{Z})^-$, calling this composition v, we have $v(x^\sigma) = \varkappa(\sigma)\, v(x)^{\sigma^{-1}}$ (where $x \in \lim \mathbf{R}_m^+/{}_m\mathbf{I}_2^+$, $\sigma \in G$). Thus we failed to obtain a $\varkappa$-isomorphism.

Appendix

Define the sequence of Bernoulli numbers B_n, by: $B_0 = 1$, and for $n \geqslant 1$, by the generating function,

$$(1 - e^{-t})^{-1} = t^{-1} + \tfrac{1}{2} - \sum_{n=1}^{\infty} (-1)^n B_n t^{2n-1}/(2n)!$$

The Bernoulli numbers are rational, and, for example, $B_1 = 1/6$, $B_2 = 1/30$, $B_3 = 1/42$, etc. Define the sequence of Bernoulli polynomials, $B_n(x)$, $n \geqslant 0$, by

$$\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x)\, \frac{t^n}{n!}.$$

Then $B_n(x)=x^n-\frac{1}{2}nx^{n-1}+\sum_{u=1}^{[n/2]}(-1)^{u-1}C_{n,2u}B_u x^{n-2u}$. Notice that $B_n(x)$ has rational coefficients. $B_n(x)$, $n\geqslant 0$, satisfy the following relations. (Davis, [2], p. 183):

(A 1) $B_n(x)=[x+B(0)]^n$ where by $B(0)^n$ we understand $B_n(0)$

(A 2) $B_n(1-x)=(-1)^n B_n(x)$

(A 3) $B_n(kx)=k^{n-1}\sum_{r=0}^{k-1} B_n\left(x+\frac{r}{k}\right)$

(A 4) $B_n(x+h)=\sum_{r=0}^{n} C_{n,r}B_{n-r}(x)h^r$.

Leopoldt ([5], p. 131) defines a different sequence of Bernoulli numbers B_n^* by:

$$\frac{te^t}{e^t-1}=\sum_{n=0}^{\infty} B_n^* t^n/n!$$

and the nth Bernoulli polynomial by:

$$B_n^*(x)=(B^*+x)^n \quad (n\geqslant 0) \text{ where by } B^{*n} \text{ we understand } B_n^*.$$

The $B_n^*(x)$ can also be defined with the aid of a generating function:

$$\frac{te^{(1+x)t}}{e^t-1}=\sum_{n=0}^{\infty} B_n^*(x)t^n/n!$$

Note that:

(A 5) $B_n^*(x)=B_n(x+1)$.

For a residue character χ with conductor f, Leopoldt defines the nth generalized Bernoulli number associated with the character χ, B_χ^n, by:

$$\sum_{\mu=1}^{f}\chi(\mu)\frac{te^{\mu t}}{e^{ft}-1}=\sum_{n=0}^{\infty} B_\chi^n t^n/n!$$

where $\chi(\mu)=0$ if $(\mu,f)>1$. Of course, for $\chi=1$ (principal character), $B_1^n=B_n^*$. Leopoldt then shows that for $\chi\neq 1$, $n\geqslant 1$:

(A 6) $B_\chi^n\neq 0$ if and only if either $\chi(-1)=1$, n even or

$$\chi(-1)=-1,\ n \text{ odd}.$$

Furthermore, if $\chi\neq 1$, $B_\chi^0=0$. He expresses B_χ^n in terms of B_n^* and $B_n(x)$. Indeed,

$$B_\chi^n = \frac{1}{f}\sum_{\mu=1}^{f}\chi(\mu)\,(fB^*+\mu-f)^n \quad \text{(where } B^{*n}=B_n^*\text{)}$$

$$= f^{n-1}\sum_{\mu=1}^{f}\chi(\mu)\,(B^*+\mu/f-1)^n$$

$$= f^{n-1}\sum_{\mu=1}^{f}\chi(\mu)\,B_n^*\left(\frac{\mu}{f}-1\right) \quad \text{(by definition of } B_n^*(x)\text{)}$$

$$= f^{n-1}\sum_{\mu=1}^{f}\chi(\mu)\,B_n(\mu/f) \quad \text{(by A 5)}.$$

Hence for $\chi \neq 1$,

(A 7) $f^{n-1}\sum_{\mu=1}^{f}\chi(\mu)\,B_n(\mu/f)\neq 0$ if and only if either $\chi(-1)=1$, n even or $\chi(-1)=-1$, n odd.

Leopoldt further proves that for χ a character with conductor f:

$$\sum_{a=1}^{kf}\chi(a)\,a^n = \frac{1}{n+1}\{(B_\chi+kf)^{n+1}-B_\chi^{n+1}\} \quad (n\geqslant 0),$$

where $\chi(a)=0$ if $(a,q)\neq 1$ and $(B_\chi)^n$ is symbolic and means B_χ^n. In particular for χ a character mod q, $\chi(-1)=1$, $\chi\neq 1$:

(A 8) $\sum_{a=1}^{q}\chi(a)\,a^2 = \frac{1}{3}\{(B_\chi+q)^3-B_\chi^3\} = qB_\chi^2\neq 0$

(for by (A 7), $B_\chi^1=B_\chi^3=0$; $\chi\neq 1$ implies $B_\chi^0=0$; and $B_\chi^2\neq 0$, also by (A 7)).

References

1]. Carlitz, L., & Olson, F. R., Maillet's determinant. *Proc. Amer. Math. Soc.*, 6 (1955), 265–269.

[2]. Davis, H. T., *Tables of Higher Mathematical Functions, vol. 2.* Bloomington, Indiana, 1935.

[3]. Iwasawa, K., A class number formula for cyclotomic fields. *Ann. of Math.*, 76 (1962), 171–179.

[4]. —— On some modules in the theory of cyclotomic fields. *J. Math. Soc. Japan*, 16 (1964), 42–82.

[5]. Leopoldt, H. W., Eine Verallgemeinerung der Bernoullischen Zahlen. *Abh. Math. Sem. Univ. Hamburg*, 22 (1958), 131–140.

Received July 24, 1967