AN APPLICATION OF BERNOULLI POLYNOMIALS TO THE THEORY OF CYCLOTOMIC FIELDS

by

Robert Segal

A.B. Columbia College

(1960)

submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June, 1965

Signature of Author.. Signature redacted ....
Department of Mathematics, April 26, 1965

Certified by.......... Signature redacted ....
Thesis Supervisor

Accepted by........... Signature redacted ....
Chairman, Departmental Committee
on Graduate Students

Abstract

An application of Bernoulli polynomials to the theory of cyclotomic fields

by Robert Segal

submitted to the Department of Mathematics on April 26, 1965 in partial fulfillment of the requirement for the degree of Doctor of Philosophy.

Let Q, Z, and Z_p be the rational field, the ring of rational integers and the ring of p-adic integers, respectively. Let ζ_m be a primitive p^m-th root of unity, $m \geq 1$. Let $F_m = Q(\zeta_m)$ and let G_m = Galois group of F_m/Q .

Generalizing Iwasawa's work in [4], we study certain ideals in the group rings $Z[G_m]$ and $Z_p[G_m]$, (m fixed). We compute the orders of the factor groups formed with these ideals and find that the orders are finite and involve the so-called generalized Bernoulli numbers defined by Leopoldt, ([6]). We then look at a certain homomorphic image of these ideals of $Z_p[G_m]$ and form the factor groups of these homomorphic images. In certain cases there exists an isomorphism between factor groups of these images (again for fixed m).

Let $m \geq m' \geq 1$, then the natural homomorphism $G_m \to G_{m'}$ defines a homomorphism $t_{m',m}: Z_p[G_m] \to Z_p[G_{m'}]$. We form with respect to these maps $t_{m',m}$ inverse systems of the factor groups of these ideals in $Z_p[G_m]$. Taking the inverse limits (over m), we obtain in certain cases an isomorphism between the inverse limits of the factor groups of these ideals. Finally, we discuss how our results are related to those of Iwasawa in his paper [5].

Thesis supervisor: Kenkichi Iwasawa
Title: Professor of Mathematics

Acknowledgement

I wish to thank Professor Iwasawa for his suggestion of the thesis problem and for his advice and encouragement during the writing of the thesis.

Contents

AN APPLICATION OF BERNOULLI POLYNOMIALS TO THE THEORY OF CYCLOTOMIC FIELDS

by

Robert Segal

CHAPTER 1.

Numerical and Structural Results

1.1 Preliminaries. Let p be an odd rational prime. Let $q = p^m$, for some fixed integer m, $m \geq 1$. Let $\zeta = \zeta_q$ be a primitive q^{th} root of unity. Let Q be the rational field, Z the ring of rational integers. Let $F = Q(\zeta)$ and G = Galois group of F/Q. The multiplicative group of units in the residue field Z/qZ is canonically isomorphic with G under the map $a \to \sigma_a$ for all a, $(a,p) = 1$ where $\sigma_a(\zeta) = \zeta^a$. A character of G is thus just a residue character mod q. Let $\hat{G}$ denote the character group of G. Let ϕ denote the Euler ϕ-function.

Let $R = Z[G]$ be the group ring of G over Z. Let $S = Q[G]$ be the group algebra of G over Q. Let $\tau = \sigma_{-1}$ denote the complex conjugation of the imaginary field F. Let $R^- = \{x \in R \mid (1 + \tau)x = 0\}$, $R^+ = \{x \in R \mid (1 - \tau)x = 0\}$. Both R^+ and R^- are ideals in R. Let $\varepsilon^+ = \frac{1}{2}(1 + \tau)$, $\varepsilon^- = \frac{1}{2}(1 - \tau)$, then $R^+ = 2(\varepsilon^+R)$, $R^- = 2(\varepsilon^-R)$.

Let $K = Q(\bigcup_{\chi \in \hat{G}} \chi(G))$. Let $T = K[G]$, then $T \supseteq S$.

If χ is a character mod q and $\xi = \sum_{\substack{0 \leq a < q \\ (a,p)=1}} x_a \sigma_a \in T$, $x_a \in K$, we define

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

Note that $\chi(\xi) \in K$. Let $\varepsilon_\chi = \phi(q)^{-1} \sum_{\substack{0 \leq a < q \\ (a,p)=1}} \chi(a) \sigma_a^{-1}$, for any character χ mod q. Then $\varepsilon_\chi \in T$, $\sum_{\chi \in \hat{G}} \varepsilon_\chi = 1$, $\sum_{\chi(-1)=1} \varepsilon_\chi = \varepsilon^+$, $\sum_{\chi(-1)=-1} \varepsilon_\chi = \varepsilon^-$, $\varepsilon_\chi^2 = \varepsilon_\chi$, and $\varepsilon_\chi \varepsilon_{\chi'} = 0$ if $\chi \neq \chi'$. Moreover, if $u \in T$, $u \varepsilon_\chi = \chi(u) \varepsilon_\chi$. Let $T^- = \varepsilon^- T$, $T^+ = \varepsilon^+ T$, then from the above facts we have

$$T = \bigoplus \sum_{\substack{0 \leq a < q \\ (a,p)=1}} K\sigma_a = \bigoplus \sum_{\chi \in \hat{G}} K\varepsilon_\chi$$

$$T^+ = \bigoplus \sum_{\substack{0 \leq a < q/2 \\ (a,p)=1}} K\varepsilon^+ \sigma_a = \bigoplus \sum_{\chi(-1)=1} K\varepsilon_\chi$$

$$T^- = \bigoplus \sum_{\substack{0 \leq a < q/2 \\ (a,p)=1}} K\varepsilon^- \sigma_a = \bigoplus \sum_{\chi(-1)=-1} K\varepsilon_\chi$$

We have two regular representations of T (resp. T^+, resp. T^-). If $u \in T$ (resp. $u \in T^+$, resp. $u \in T^-$) and

$$u\sigma_a = \sum_{\substack{0 \leq b < q \\ (b,p)=1}} x_{ab} \sigma_b ,$$

(resp. $u\varepsilon^+ \sigma_a = \sum_{0 \leq b \leq q/2} x_{ab} \varepsilon^+ \sigma_b$, resp. $u\varepsilon^- \sigma_a = \sum_{0 \leq b < q/2} x_{ab} \varepsilon^- \sigma_b$)

then the regular representation with respect to the basis σ_a , $0 \leq a < q$, $(a,p) = 1$ (resp. $\varepsilon^+\sigma_a$, $0 \leq a < q/2$; resp. $\varepsilon^-\sigma_a$, $0 \leq a < q/2$) is

$$r_1(u) = (x_{ab})_{\substack{0 \leq a < q \quad (a,p)=1 \\ 0 \leq b < q \quad (b,p)=1}}$$

$$\text{(resp. } r_1(u) = (x_{ab})_{\substack{0 \leq a < q/2 \quad (a,p)=1 \\ 0 \leq b < q/2 \quad (b,p)=1}} ,$$

$$\text{resp. } r_1(u) = (x_{ab})_{\substack{0 \leq a < q/2 \quad (a,p)=1 \\ 0 \leq b < q/2 \quad (b,p)=1}} \text{).}$$

On the other hand another regular representation r_2 of T (resp. T^+ , resp. T^-) is given with respect to the basis ε_χ , $\chi \varepsilon \hat{G}$; (resp. ε_χ , $\chi(-1) = 1$; resp. ε_χ , $\chi(-1) = -1$) . For convenience, let $N = \frac{1}{2}\,\phi(q)$, and let $\chi_1, \ldots, \chi_N$ denote χ such that $\chi(-1) = 1$, $\chi_{N+1}, \ldots, \chi_{\phi(q)}$ denote χ such that $\chi(-1) = -1$. Then if $u \varepsilon T$ (resp. T^+ , resp. T^-) , then we have

$$r_2(u) = \begin{pmatrix} \chi_1(u) & 0 \cdots\cdots 0 \\ 0 & \chi_2(u) \cdots 0 \\ \cdots & \cdots\cdots\cdots \\ 0 & 0 \cdots \chi_{\phi(q)}(u) \end{pmatrix} \quad \phi(q) \times \phi(q) \text{ matrix}$$

$$\text{[resp. } r_2(u) = \begin{pmatrix} \chi_1(u) & 0 \cdots\cdots & 0 \\ 0 & \chi_2(u) \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & 0 \cdots & \chi_N(u) \end{pmatrix} ;$$

N × N matrix

$$\text{resp. } r_2(u) = \begin{pmatrix} \chi_{N+1}(u) & 0 \cdots\cdots & 0 \\ 0 & \chi_{N+2}(u) \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & 0 \cdots & \chi_{\phi(q)}(u) \end{pmatrix}$$

N × N matrix].

Because r_1 and r_2 are equivalent representations, we have that $\det r_1(u) = \det r_2(u)$ for any $u \in T$ (resp. $u \in T^+$, resp. $u \in T^-$) . Hence, $|x_{ab}| = \prod_{\chi} \chi(u)$,

(resp. $|x_{ab}|_{\substack{0 \le a < q/2 \\ 0 \le b < q/2}} = \prod_{\chi(-1)=1} \chi(u)$, resp. $|x_{ab}|_{\substack{0 \le a < q/2 \\ 0 \le b < q/2}} = \prod_{\chi(-1)=-1} \chi(u)$).

From all of the above it follows that:

1.1.1) if $\xi \in S$ (resp. $\xi \in S^+$, resp. $\xi \in S^-$) , then ξ is regular in S , (resp. in S^+, resp. in S^-) iff $\prod_{\chi \in \hat{G}} \chi(\xi) \neq 0$ (resp. $\prod_{\chi(-1)=1} \chi(\xi) \neq 0$, resp. $\prod_{\chi(-1)=-1} \chi(\xi) \neq 0$). The proof follows from the fact that since r_2 is a regular representation it is injective. Thus ξ is regular in S iff

$r_2(\xi)$ is regular in the ring of complex $\phi(q) \times \phi(q)$ matrices, which is iff $\det r_2(\xi) \neq 0$ or $\prod_{\chi} \chi(\xi) \neq 0$. A similar argument is valid for $\xi \in S^+$ and $\xi \in S^-$.

(1.1.2) If $\xi \in R$ (resp. $\xi \in \varepsilon^+ R$, resp. $\xi \in \varepsilon^- R$) and ξ is regular in S, (resp. ξ is regular in S^+, resp. ξ is regular in S^-), then

$$[R: \xi R] = \left| \prod_{\chi \bmod q} \chi(\xi) \right|$$

(resp. $[\varepsilon^+ R: \xi \varepsilon^+ R] = \left| \prod_{\chi(-1)=1} \chi(\xi) \right|$, resp. $[\varepsilon^- R: \xi \varepsilon^- R] = \left| \prod_{\chi(-1)=-1} \chi(\xi) \right|$).

The proof is given for R. We have $R = \oplus \sum_a Z \sigma_a$. Because ξ is regular in R, we have $\xi R = \oplus \sum_a Z \xi \sigma_a$, and $\xi \sigma_a$, $(0 \leq a < q, (a,p)=1)$ is a basis of ξR over Z. From a fundamental theorem on modules over principal ideal domains, it follows that

$$[R: \xi R] = \text{absolute value of } |x_{ab}|$$

$$= \left| \prod_{\chi} \chi(\xi) \right| .$$

<u>1.2</u> <u>Bernoulli</u> <u>polynomials.</u> Define the sequence of Bernoulli numbers B_n, by: $B_0 = 1$, and for $n \geq 1$, by the generating function,

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

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, $B_n(x)$, $n \geq 0$, by

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

Then $B_n(x) = x^n - \frac{1}{2} nx^{n-1} + \sum_{u=1}^{\leq n/2} (-1)^{u-1} \binom{n}{2u} B_u \, x^{n-2u}$.

Notice that $B_n(x) \in Q[X]$. $B_n(x)$, $n \geq 0$, satisfy the following relations. (Davis, [3], p. 183):

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

(1.2.2) $B_n(1 - x) = (-1)^n B_n(x)$.

(1.2.3) $B_n(kx) = k^{n-1} \sum_{r=0}^{k-1} B_n(x + \frac{r}{k})$.

(1.2.4) $B_n(x + h) = \sum_{r=0}^{n} \binom{n}{r} B_{n-r}(x) h^r$.

Leopoldt ([6], 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 n^{th} Bernoulli polynomial by:

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

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

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

We note that $B_n^*(x) = B_n(x+1)$. (1.2.5)

For a residue character χ with conductor f , Leopoldt defines the n^{th} 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 $\chi = 1$ (trivial character), $B_1^n = B_n^*$. Leopoldt then shows that for $\chi \neq 1$, $n \geq 1$: $B_\chi^n \neq 0$ iff either $\chi(-1) = 1$, n even or $\chi(-1) = -1$, n odd. Furthermore, if $\chi \neq 1$, $B_\chi^0 = 0$. (1.2.6)

He expresses B_χ^n in terms of B_n^* and $B_n(x)$. Indeed,

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

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

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

$$= f^{n-1} \sum_{\mu=1}^{f} \chi(\mu)B_n(\mu/f) \quad (\text{by } 1.2.5) .$$

Hence for $\chi \neq 1$, $f^{n-1} \sum_{\mu=1}^{f} \chi(\mu)B_n(\mu/f) \neq 0$ iff either

$\chi(-1) = 1$, n even or $\chi(-1) = -1$, n odd (1.2.7).

<u>1.3</u> <u>The</u> <u>index</u> <u>$[R^+ : I_\Omega^+]$</u>. Following Iwasawa's lead ([4]), we thought it natural to consider the element

$$\Omega = q^{-1} \sum_{\substack{0 \le a < q \\ (a,p)=1}} a^2 \sigma_a^{-1} \in S$$

and to let $I_\Omega = R \cap R\Omega$, $I_\Omega^+ = R^+ \cap R\Omega$. We wanted, at least, to study the index $[R^+ : I_\Omega^+]$ of the R-modules R^+ and I^+.

We first lay some groundwork. Let A be the additive group in R generated by q and $\sigma_a - a^2$, $(a,p) = 1$. A has a basis over Z consisting of q, $2\varepsilon^-$, $\sigma_{-a} - a^2$, $\sigma_a - a^2$, $1 < a < q/2$, $(a,p)=1$. Let

$$B_\Omega = \left\{ \varepsilon^+ \alpha \mid \alpha \in A, \alpha\Omega \in S^+ \right\}.$$

B_Ω is an additive subgroup of $\varepsilon^+ R$. For convenience, we adopt the following notation throughout the rest of the paper:

$$\sum_a = \sum_{\substack{0 \le a < q \\ (a,p)=1}} \; ; \; \sum_a{}' = \sum_{\substack{0 \le a < q/2 \\ (a,p)=1}} \; ; \; \sum_a{}'' = \sum_{\substack{1 < a < q/2 \\ (a,p)=1}} \; ;$$

$R(a)$ = least positive residue of a mod q; $a^* = R(a^{-1})$ for $(a,p) = 1$.

<u>Lemma</u> <u>1.3.1:</u> $[\varepsilon^+ R : B_\Omega] = 2^N q$ $(N = \phi(q)/2)$

<u>Proof:</u> Let $\tau_a = \varepsilon^+ \sigma_a = \frac{1}{2}(\sigma_a + \sigma_{-a})$, $(a,p) = 1$. Then

$\tau_a = \tau_{-a}$, and hence $\{\tau_a | 0 \leq a < q/2, (a,p)=1\}$ form a basis of $\varepsilon^+ R$ over Z . If $\alpha \varepsilon A$, $\alpha = sq + t(2\varepsilon^-) + \Sigma''_a \{s_a(\sigma_a - a^2) + s_{-a}(\sigma_{-a} - a^2)\}$, for $s, t, s_a, s_{-a} \varepsilon Z$, then $\varepsilon^+\alpha \varepsilon \varepsilon^+ R$ and $\varepsilon^+\alpha = \Sigma'_a u_a \tau_a$ where

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

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

Thus we have that $\Sigma'_a a^2 u_a \equiv 0 \ (q)$ and $s = q^{-1}\Sigma'_a a^2 u_a$. Hence $\varepsilon^+ A \subseteq \{\Sigma'_a u_a \tau_a \ \varepsilon \ \varepsilon^+ R | \ \Sigma'_a a^2 u_a \equiv 0 \ (q)\}$. Conversely, if $\Sigma'_a u_a \tau_a \ \varepsilon \ \varepsilon^+ R$, and $\Sigma'_a a^2 u_a \equiv 0 \ (q)$, then letting

$$\alpha = sq + t(2\varepsilon^-) + \Sigma''_a \{s_a(\sigma_a - a^2) + s_{-a}(\sigma_{-a} - a^2)\}$$

where $s = q^{-1} \Sigma'_a a^2 u_a$, $s_{-a} = u_a - s_a$, and t and s_a are arbitrary, we have that $\Sigma'_a u_a \tau_a = \varepsilon^+\alpha$. We conclude from this that

$$\varepsilon^+ A = \{\Sigma'_a u_a \tau_a \ \varepsilon \ \varepsilon^+ R | \ \Sigma'_a a^2 u_a \equiv 0 \ (q)\} .$$

On the other hand, if $\xi \ \varepsilon \ S$, $\xi = \Sigma_a x_a \sigma_a$, then $\xi\Omega \ \varepsilon \ S^+$ iff $2\varepsilon^- \xi\Omega = 0$. But $2\varepsilon^-\Omega = \Sigma_a (-q+2a^*)\sigma_a$. Hence $2\varepsilon^- \xi\Omega = 0$ iff, for all c , $0 \leq c < q$, $(c,p) = 1$,
$\sum_{\substack{ab \equiv c(q) \\ 0 \leq a,b < q}} x_b(-q+2a^*) = 0$. Combining all of the above, we

have, if $\beta \in \varepsilon^{+}R$, $\beta = \sum_a{}' \; u_a\tau_a$: then $\beta \in B_\Omega$ iff $\beta = \varepsilon^{+}\alpha$ for $\alpha \in A$ and $\alpha\Omega \in S^{+}$, where

$$\alpha = sq + t(2\varepsilon^{-}) + \sum_a{}'' \left\{ s_a(\sigma_a - a^2) + s_{-a}(\sigma_{-a} - a^2) \right\}$$

$$= [sq + t + \sum_a{}'' - a^2(s_a + s_{-a})]\sigma_1 + (-t)\sigma_{q-1} + \sum_a{}'' s_a\sigma_a + \sum_a{}'' s_{-a}\sigma_{-a}$$

for some s, t, s_a, $s_{-a} \in Z$,

which is iff $\sum_a{}' a^2u_a \equiv 0 \; (q)$ and there exist integers t and s_a $(1<a<q/2,\ (a,p)=1)$ such that

$$u_1(q - 2c^*) + \sum_a{}''(2R(ac^*)-q)u_a = 2\left\{(2c^* - q)t + \sum_a{}''(2R(ac^*)-q)s_a\right\}$$

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

$(0\leq c<q,\ (c,p)=1)$ (1.3.2)

But the matrix $(2R(ac^*)-q)_{\substack{0\leq a<q/2 \quad (a,p)=1 \\ 0\leq c<q/2 \quad (c,p)=1}}$ has non-vanishing determinant; indeed, the determinant is equal, up to a factor of $\pm$ a positive power of two, to the value of Maillet's determinant. Carlitz and Olson ([2]) showed for $q = p$, that Maillet's determinant does not vanish. Their method generalizes completely to the case $q = p^m$, $m \geq 2$. Hence the latter system of homogeneous equations (1.3.2) is solvable if and only if $u_a \equiv 0 \; (2)$ for $0\leq a<q/2$, $(a,p)=1$. Therefore, we conclude, $\beta \in B_\Omega$ iff

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

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

Define a map $\psi: \varepsilon^+ R \to Z/qZ \times (Z/2Z)^N$ where

$$\psi(\Sigma' u_a \tau_a) = (\sum_a' a^2 u_a \bmod q \ , \ (u_a \bmod 2))_{\substack{0 \leq a < q/2 \\ (a,p)=1}} .$$

The kernel of $\psi = B_\Omega$ and ψ is surjective by the Chinese Remainder Theorem (for $p \neq 2$) . Hence

$$[\varepsilon^+ R: B_\Omega] = q \cdot 2^N \qquad \text{Q.E.D.}$$

<u>Theorem</u> <u>1.3.3:</u> If Ω, I_Ω, I_Ω^+ are defined as above we have that $[R^+: I_\Omega^+] = q|\prod_{\chi(-1)=1} \chi(\Omega)| = q|\prod_{\chi(-1)=1} \frac{1}{q} \sum_a a^2 \chi(a)|$ where χ is a character mod q.

<u>Proof:</u> By Remark 1.1.1, $\varepsilon^+\Omega$ is regular in S^+ iff

$$\prod_{\chi(-1)=1} \chi(\varepsilon^+\Omega) = \prod_{\chi(-1)=1} \chi(\Omega) = \prod_{\chi(-1)=1} q^{-1} \sum_a a^2 \chi(a) \neq 0 .$$

From Leopoldt (op. cit.), we have that if $\chi \neq 1$,

$$\sum_a \chi(a) a^2 = \frac{1}{3} \{ (B_\chi + q)^3 - B_\chi^3 \} . \ (\ddagger)$$

But $\chi(-1) = 1$ implies $B_\chi^1 = B_\chi^3 = 0$; also $\chi \neq 1$ implies $B_\chi^0 = 0$ (v. 1.2.6 and 1.2.7). Hence for $\chi \neq 1$, $\chi(-1) = 1$, we have that

$$\sum_a \chi(a) a^2 = q B_\chi^2 \neq 0 \qquad \text{(by 1.2.6)} .$$

(‡) Powers of B_χ in the expansion are symbolic.

If $\chi = 1$, a simple calcuation shows that:

$$\sum_{\substack{0\leq a<q \\ (a,p)=1}} a^2 = \frac{q(p-1)(2q^2-p)}{6p} \neq 0 .$$

Hence $\prod_{\chi(-1)=1} \chi(\Omega) \neq 0$, and, thus $\varepsilon^+\Omega$ is regular in S^+ .

Let A be the additive group in R generated by q and $\sigma_a - a^2$, $(a,p) = 1$. Clearly $q\Omega \in R$, and for any $b \in Z$, $(b,p) = 1$, we have

$$\begin{aligned}(\sigma_b - b^2)q^{-1} \sum_a a^2\sigma_a{}^{-1} &= q^{-1}[\sum_a a^2\sigma_b\sigma_a{}^{-1} - b^2 \sum_a a^2\sigma_a{}^{-1}] \\ &\equiv \frac{b^2}{q} \sum_a (ab^*)^2 \sigma_{a^*b} - \frac{b^2}{q} \sum_a a^2\sigma_a{}^{-1} \\ &\equiv b^2\Omega - b^2\Omega \equiv 0 \mod R .\end{aligned}$$

Therefore, $A\Omega \subseteq R$ or $A\Omega \subseteq I_\Omega$. Let $C = \{\xi \in R | \xi\Omega \in R\}$. If $\xi \in R$, then we can write $\xi = t \cdot 1 + \sum_{\substack{1<a<q \\ (a,p)=1}} t_a(\sigma_a - a^2)$. We know $A \subseteq C$, thus $\xi\Omega \in R$ iff $t\Omega \in R$ iff $q|t$ iff $\xi \in A$. Therefore $C = A$ or $A\Omega = I_\Omega$.

Let $B_\Omega = \{\varepsilon^+\alpha | \alpha \in A, \alpha\Omega \in S^+\}$. Then

$$I_\Omega^+ = B_\Omega\, \varepsilon^+\Omega \quad \text{or} \quad qI_\Omega^+ = B_\Omega\, \varepsilon^+q\Omega .$$

Because $\varepsilon^+\Omega$ is regular in S^+ , it follows from remark (1.1.2) that

$$\begin{aligned}[\varepsilon^+R: qI_\Omega^+] &= [\varepsilon^+R: \varepsilon^+R\varepsilon^+q\Omega][\varepsilon^+R\varepsilon^+q\Omega: B_\Omega\, \varepsilon^+q\Omega] \\ &= q^N|\prod_{\chi(-1)=1} \chi(\Omega)|\, [\varepsilon^+R: B_\Omega] .\end{aligned}$$

It follows from Lemma 1.3.1 that

$$[\varepsilon^+R: qI_\Omega^+] = q^{N+1}2^N \left| \prod_{\chi(-1)=1} \chi(\Omega) \right|$$

Thus qI_Ω^+ is a free abelian group of the same rank as ε^+R , viz. N . Therefore, $[I_\Omega^+: qI_\Omega^+] = q^N$. Also $[\varepsilon^+R: R^+] = 2^N$, for $R^+ = 2(\varepsilon^+R)$. Combining all our equations, we obtain:

$$[R^+: I_\Omega^+] = q \left| \prod_{\chi(-1)=1} \chi(\Omega) \right| \qquad \text{Q.E.D.}$$

1.4 More general ideals in R^+ and R^- . Considerations of such sums as $\sum_a a^3\sigma_a^{-1}$, $\sum_a a^4\sigma_a^{-1}$ etc. do not prove fruitful as they lead to difficult-to-evaluate determinants. Also, it is not clear, for example, that $\varepsilon^-\sum_a a^3\sigma_a^{-1}$ ($\varepsilon^+\sum_a a^4\sigma_a^{-1}$ resp.) is regular in S^- (S^+ resp.). However, the fact that for $\chi \neq 1$, conductor $\chi = f$, we have

$$\sum_{a=1}^{f} \chi(a)\, B_n(a/f) \neq 0 \text{ iff } \chi(-1) = 1 \text{ , n even, or}$$

$\chi(-1) = -1$, n odd (see remark 1.2.7), leads one to consider sums of the form $q^{n-1}\sum_a B_n(a/q)\sigma_a^{-1}$. Indeed, we consider the following general situation.

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

i) $c_i \in Z$ for $0 \leq i < n$, and $c_n = c/q$, $c \in Z$, $c \neq 0$

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

Let $\omega = (\omega_f) = \sum_a f(a)\sigma_a^{-1} \in S$. It follows from ii) that:

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

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

Theorem 1.4.1: With the above hypotheses, suppose that ω is regular in S^+ if n is even or ω is regular in S^- if n is odd, then

$$[R^+ : R^+ \cap R\omega] = \frac{q'}{2^N} \Big| \prod_{\chi(-1)=1} \chi(\omega) \Big| \quad \text{for } n \text{ even}$$

$$[R^- : R^- \cap R\omega] = \frac{q'}{2^N} \Big| \prod_{\chi(-1)=-1} \chi(\omega) \Big| \quad \text{for } n \text{ odd}$$

where q' denotes the reduced denominator of the fraction $c_n = c/q$.

Proof: (for n even). Let A be the additive group in R generated by q' and $\sigma_a - a^n$, $(a,p) = 1$. A basis for A over Z is q', $2\varepsilon^-$, $\sigma_a - a^n$, $\sigma_{-a} - a^n$, $1<a<q/2$, $(a,p) = 1$. Clearly $A\omega \subseteq R^+ \cap R\omega$, because $\omega \in R^+$ and $A\omega \subseteq R$. Conversely, if $\xi = \sum_a x_a\sigma_a \in R$, it follows from the fact that $q'|q$ and $\omega \equiv \frac{c}{q} \sum_a a^n\sigma_a^{-1}$ mod R:

$$\xi\omega \in R^+ \cap R\omega = R \cap R\omega \text{ implies } (\sum_a x_a\sigma_a)(\sum_a a^n\sigma_a^{-1}) \equiv 0 \quad (q'R)$$

which implies $\sum_a x_{ab}a^n \equiv 0\ (q')$ for any b , $(b,p) = 1$, which implies $\sum_a x_a a^n \equiv 0\ (q')$. Thus if $\sum x_a a^n = q'v$, $v \in Z$, we have $\xi\omega = [\sum_a x_a(\sigma_a - a^n) - vq']\omega$ or $\xi\omega \in A\omega$. Thus, $R^+ \cap R\omega = A\omega$. Letting $B = \varepsilon^+ A$, we have that

$$R^+ \cap R\omega = B\omega \quad \text{or} \quad q(R^+ \cap R\omega) = Bq\omega \text{ , and } B \subseteq \varepsilon^+ R .$$

We have by (1.1.2) , since ω is regular in S^+ , that $[\varepsilon^+ R : q(R^+ \cap R\omega)] = [\varepsilon^+ R : \varepsilon^+ Rq\omega][\varepsilon^+ Rq\omega : Bq\omega]$

$$= q^N \left| \prod_{\chi(-1)=1} \chi(\omega) \right| [\varepsilon^+ R : B] .$$

To calculate $[\varepsilon^+ R : B]$, we consider the map

$$\theta : R \to \varepsilon^+ R$$

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

θ is surjective and kernel $\theta = R^-$. Furthermore, $A \supseteq R^-$, for R^- is generated over Z by $\sigma_a - \sigma_{-a} = (\sigma_a - a^n) - (\sigma_{-a} - a^n) \in A$. Hence, we may conclude from this that:

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

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

$$[\varepsilon^+ R : q(R^+ \cap R\omega)] = q' \cdot q^N \left| \prod_{\chi(-1)=1} \chi(\omega) \right| .$$

But $[\varepsilon^+ R : R^+] = 2^N$ and $[R^+ \cap R\omega : q(R^+ \cap R\omega] = q^N$ together imply that $[R^+ : q(R^+ \cap R\omega)] = \frac{q'}{2^N} \left| \prod_{\chi(-1)=1} \chi(\omega) \right|$. Similarly for n odd. Q.E.D.

Recall from 1.2 our definition of the Bernoulli polynomials $B_n(x)$. Write for $n \geq 1$,

$$B_n(x) = x^n + \sum_{\nu=0}^{n-1} \frac{a_{\nu,n}}{b_{\nu,n}} x^\nu \qquad a_{\nu,n}, b_{\nu,n} \in Z \quad (a_{\nu,n}, b_{\nu,n}) = 1 .$$

Let α_n = least common multiple of $b_{\nu,n}$ $\nu=0,\dots,n-1$. Let q_n' = reduced denominator of the fraction α_n/q .

<u>Corollary</u> <u>1.4.2:</u> With the notation as above, let

$h_n(x) = \alpha_n q^{n-1} B_n(x/q)$ and $\omega_n = \sum_a h_n(a)\sigma_a^{-1}$, $\omega_n \in S$

then

$$[R^+: R^+ \cap R\omega_n] = \frac{q_n'}{2^N} \Big| \prod_{\chi(-1)=1} \chi(\omega_n)\Big| = q_n' \left(\frac{\alpha_n}{2}\right)^N (1-p^{n-1}) \Big| \prod_{\chi(-1)=1} B_\chi^n \Big|$$

if n is even;

$$[R^-: R^- \cap R\omega_n] = \frac{q_n'}{2^N} \Big| \prod_{\chi(-1)=-1} \chi(\omega_n)\Big| = q_n' \left(\frac{\alpha_n}{2}\right)^N \Big| \prod_{\chi(-1)=-1} B_\chi^n \Big|$$

if n is odd.

<u>Proof:</u> 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 validate that $h_n(q-x) = (-1)^n h_n(x)$ and that ω_n is regular in S^+ for n even and in S^- for n odd. As for the first matter:

$h_n(q-x) = \alpha_n q^{n-1} B_n((q-x)/q) = \alpha_n q^{n-1} B_n(1 - \frac{x}{q})$ which by

1.2.2 = $(-1)^n \alpha_n q^{n-1} B_n(\frac{x}{q}) = (-1)^n h_n(x)$. As for the latter statement, let χ be a residue character mod q , $\chi \neq 1$. Let $f(\chi) = f$ be the conductor of χ , then $f|q$. If $(a,p) \neq 1$, we agree to let $\chi(a) = 0$. Recalling 1.1.1, we see that it suffices to evaluate

$$q^{n-1} \sum_{0 \leq b < q} \chi(b) B_n(b/q) =$$

$$q^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{\substack{0 < a < q \\ a \equiv b(f)}} B_n(a/q) =$$

$$q^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{k=0}^{q/f-1} B_n((b+kf)/q) =$$

(by 1.2.4)

$$q^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{k=0}^{q/f-1} \sum_{r=0}^{n} \binom{n}{r} (\frac{b}{q})^r B_{n-r}(\frac{kf}{q}) =$$

$$q^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{r=0}^{n} \binom{n}{r} \frac{(b/q)^r}{(q/f)^{n-r-1}} [(q/f)^{n-r-1} \sum_{k=0}^{q/f-1} B_{n-r}(k/\frac{q}{f})] =$$

(by 1.2.3)

$$f^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{r=0}^{n} \binom{n}{r} (b/f)^r B_{n-r}(\frac{q}{f} \cdot 0) =$$

$$f^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{r=0}^{n} \binom{n}{r} (b/f)^r B_{n-r}(0) =$$

(by 1.2.1)

$$f^{n-1} \sum_{b=1}^{f} \chi(b) B_n(b/f) = B_\chi^n \neq 0 \text{ iff}$$

n even, $\chi(-1) = 1$, or n odd, $\chi(-1) = -1$ (v. 1.2.6).

Hence for n odd, $\chi(-1) = -1$, then $\chi(\omega_n) \neq 0$; thus $\omega_n \in S_n^-$ is regular by 1.1.1. If n is even, we have if $\chi(-1) = 1$, $\chi \neq 1$, then $\chi(\omega_n) \neq 0$. To prove $\omega_n \in S^+$ is regular in S^+, it remains to treat the case $\chi = 1$:

$$q^{n-1} \sum_{\substack{0 \le b < q \\ (b,p)=1}} B_n(b/q) = q^{n-1} \sum_{0 \le b \le q-1} B_n(b/q) - q^{n-1} \sum_{t=0}^{\frac{q}{p}-1} B_n(pt/q)$$

$$= q^{n-1} \sum_{0 \le b \le q-1} B_n(0 + b/q) - q^{n-1} \sum_{t=0}^{\frac{q}{p}-1} B_n(pt/q)$$

(by 1.2.3)
$$= B_n(0 \cdot q) - q^{n-1} \sum_{t=0}^{\frac{q}{p}-1} B_n(pt/q)$$

$$= B_n(0) - q^{n-1} \sum_{t=0}^{\frac{q}{p}-1} B_n(pt/q) .$$

So it remains to evaluate

$$q^{n-1} \sum_{t=0}^{q/p-1} B_n(pt/q) = q^{n-1} \sum_{t=0}^{q/p-1} B_n(t/\tfrac{q}{p})$$

$$= q^{n-1}(p/q)^{n-1} \left\{ (q/p)^{n-1} \sum_{t=0}^{q/p-1} B_n(0 + t/\tfrac{q}{p}) \right\}$$

by (1.2.3)
$$= q^{n-1}(p/q)^{n-1} B_n(0 \cdot q/p) = p^{n-1} B_n(0) .$$

Therefore,
$$q^{n-1} \sum_{\substack{b=0 \\ (b,p)=1}}^{q-1} B_n(b/q) = B_n(0) - p^{n-1} B_n(0)$$

$$= (1 - p^{n-1}) B_n(0) \neq 0$$

because if n is even, $B_n(0) = \pm B_{n/2} \neq 0$ and $p^{n-1} \neq 1$. We may now say that ω_n is regular in S^+ for n even. Furthermore, for $n \geq 1$,

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

$$\text{for } \chi = 1 , \quad \chi(\omega_n) = \alpha_n(1 - p^{n-1})B_n(0) \qquad (1.4.3)$$

$$= \alpha_n(1 - p^{n-1})B_1^n$$

where 1 is the trivial character. (To go from $B_n(0)$ to B_1^n , we know that $B_n(0) = B_n(1)$, because $B_n(x) = (-1)^n B_n(1-x)$ and $B_n(0) = 0$ for n odd, but $B_n(1) = B_n^*(0)$ by (1.2.5) and $B_n^*(0) = B_n^* = B_1^n$ by the definitions in 1.2.)

Thus $[R^+ : R^+ \cap R\omega_n] = q_n'(\frac{\alpha_n}{2})^N (1 - p^{n-1}) | \prod_{\chi(-1)=1} B_\chi^n |$ (n even)

$$[R^- : R^- \cap R\omega_n] = q_n'(\tfrac{\alpha_n}{2})^N \, | \prod_{\chi(-1)=-1} B_\chi^n | \quad (n \text{ odd}) .$$

<u>1.5</u> <u>The p-adic case.</u> Let Q_p be the p-adic number field and Z_p be the subring of p-adic integers $(p \neq 2)$.

$$\text{Let } R_p = Z_p[G] , \quad S_p = Q_p[G]$$

$$S_p^+ = \varepsilon^+ S_p , \quad S_p^- = \varepsilon^- S_p$$

$$R_p^+ = R_p \cap S_p^+ = \varepsilon^+ R_p ; \; R_p^- = R_p \cap S_p^- = \varepsilon^- R_p .$$

If $u \in Q$, and $u = \frac{r}{s} p^{\nu}$, $(r,p) = (s,p) = 1$ $r,s,\nu \in Z$, then define:
$$(u)_p = p^{\nu} .$$

Analogous to 1.1.1 and 1.1.2 we have:

1.5.1) Let $\xi \in S_p$, $\xi = \sum_a x_a \sigma_a$, $x_a \in Q_p$. Define
$$\chi(\xi) = \sum_a x_a \chi(a)$$

for any character mod q. Then ξ is regular in S_p iff $\prod_{\chi \in \hat{G}} \chi(\xi) \neq 0$. Similarly, if $\xi \in S_p^+(S_p^-)$ then ξ is regular in $S_p^+(S_p^-)$ iff $\prod_{\chi(-1)=1} \chi(\xi) \neq 0$, $(\prod_{\chi(-1)=-1} \chi(\xi) \neq 0)$.

1.5.2) If $\xi \in R_p$ is regular in S_p, then $[R_p : \xi R_p] = (\prod_{\chi} \chi(\xi))_p$. Similarly if $\xi \in R_p^+$ is regular in S_p^+, then $[R_p^+ : \xi R_p^+] = (\prod_{\chi(-1)=1} \chi(\xi))_p$ and if $\xi \in R_p^-$ is regular in S_p^-, then $[R_p^- : \xi R_p^-] = (\prod_{\chi(-1)=-1} \chi(\xi))_p$.

Remark 1.5.2 follows from the fact that Z_p is a principal ideal domain with unique prime ideal pZ_p.

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 $0 \leq i < n$, and $c_n = c/q$ $c \in Z_p$, $c \neq 0$

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

Let $\omega (= \omega_f) = \sum_a f(a) \sigma_a^{-1}$.

It follows from 2) that

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

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

Furthermore, let q' denote the "reduced" denominator of the fraction $c_n = c/q$ (with respect to the ring Z_p). Let A_p be the additive group generated over Z_p by q' and $\sigma_a - a^n$. $A \subseteq R_p$. Let $B_p = \varepsilon^+ A_p$ for n even, $B_p = \varepsilon^- A_p$ for n odd.

<u>Theorem 1.5.3:</u> With the above definitions and hypotheses suppose now that ω is regular in S_p^+ for n even

ω is regular in S_p^- for n odd ,

then

i) $[R_p^+ : R_p^+ \cap R_p\omega] = q'(\prod_{\chi(-1)=1} \chi(\omega))_p$ for n even and

$[R_p^- : R_p^- \cap R_p\omega] = q'(\prod_{\chi(-1)=-1} \chi(\omega))_p$ for n odd .

ii) $R_p^+ \cap R_p\omega = B_p\omega$ n even

$R_p^- \cap R_p\omega = B_p\omega$ n odd .

<u>Proof:</u> Account being taken of remarks 1.5.1 and 1.5.2 and the fact that $\varepsilon^{\pm} R_p = R_p^{\pm}$ (because $p \neq 2$) we can proceed as in the proof of Theorem 1.4.1. ∎

For each $n \geq 1$, let $\omega_n = \sum_a q^{n-1} B_n(a/q)\sigma_a^{-1} \in S_p$ (note omission of the constant α_n). Let ${}_nI_p^+ = R_p^+ \cap R_p\omega_n$ (n even), ${}_nI_p^- = R_p^- \cap R_p\omega_n$ (n odd). Let ${}_nA_p$ be the additive group generated over Z_p in R_p by q and $\sigma_a - a^n$. Let ${}_nB_p = \varepsilon^+ {}_nA_p$ for n even; ${}_nB_p = \varepsilon^- {}_nA_p$ for n odd.

Corollary 1.5.4: With the above definitions

i) $[R_p^+ : {}_nI_p^+] = q(\prod_{\chi(-1)=+1} B_\chi^n)_p$ (n even)

$[R_p^- : {}_nI_p^-] = q(\prod_{\chi(-1)=-1} B_\chi^n)_p$ (n odd)

ii) ${}_nI_p^+ = {}_nB_p\omega_n$ (n even)

${}_nI_p^- = {}_nB_p\omega_n$ (n odd) .

Proof: For any $n \geq 1$, $B_n(a) = a^n - \frac{1}{2}na^{n-1}$

$$+ \sum_{u=1}^{\leq n/2} (-1)^{u-1}\binom{n}{2u} B_u a^{n-2u}$$

and $q^{n-1}B_n(a/q) = \frac{1}{q}(a^n - \frac{1}{2}nqa^{n-1} + \sum_{u=1}^{\leq n/2}(-1)^{u-1}\binom{n}{2u}B_u a^{n-2u}q^{2u})$.

By the von Staudt-Clausen theorem, B_u has square free denominator; hence, because $p \nmid 2$, we have that all the coefficients of $q^{n-1}B_n(a/q)$, except the leading coefficient, are p-adic integers. The leading coefficient is $1/q$ and hence it has reduced denominator q . In the proof of corollary 1.4.2, we saw that

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

Just as was derived in the proof of corollary 1.4.2 (see 1.4.3) we may derive:

$$\text{for } \chi \neq 1 , \ \chi(\omega_n) = B^n_\chi \neq 0 \text{ iff } n \text{ even, } \chi(-1) = 1$$
$$\text{or } n \text{ odd, } \chi(-1) = -1$$

$$\text{for } \chi = 1 , \ \chi(\omega_n) = (1 - p^{n-1})B^n_1 \neq 0 \text{ iff } n \text{ even} \quad (1.5.5)$$

and thus we have ω_n is regular in S^+_p (n even)

ω_n is regular in S^-_p (n odd)

by remark 1.5.1.

It just remains to remark that $(1 - p^{n-1})_p = 1$. ∎

We recall that $R^+_p = \varepsilon^+ R_p$ ($R^-_p = \varepsilon^- R_p$, resp.) has a basis over Z_p consisting of $\sigma_a + \sigma_{-a}$, $0 \leq a < q/2$, $(a,p) = 1$ (of $\sigma_a - \sigma_{-a}$, $0 \leq a < q/2$, $(a,p) = 1$) and it is a simple calculation to show that:

$${}_nB_p = \varepsilon^+ {}_nA_p = \left\{ \sum_a{}' u_a(\sigma_a + \sigma_{-a}) \mid u_a \in Z_p, \sum_a{}' a^n u_a \equiv 0 \ (q) \right\} \ n \text{ even}$$

$${}_nB_p = \varepsilon^- {}_nA_p = \left\{ \sum_a{}' u_a(\sigma_a - \sigma_{-a}) \mid u_a \in Z_p, \sum_a{}' a^n u_a \equiv 0 \ (q) \right\} \ n \text{ odd} .$$

Let $${}_nB^*_p = \left\{ \sum_a{}' u_a(\sigma_a + \sigma_{-a}) \mid u_a \in Z_p, \sum_a{}' a^n u_a \equiv 0 \ (q^2) \right\} \ n \text{ even}$$

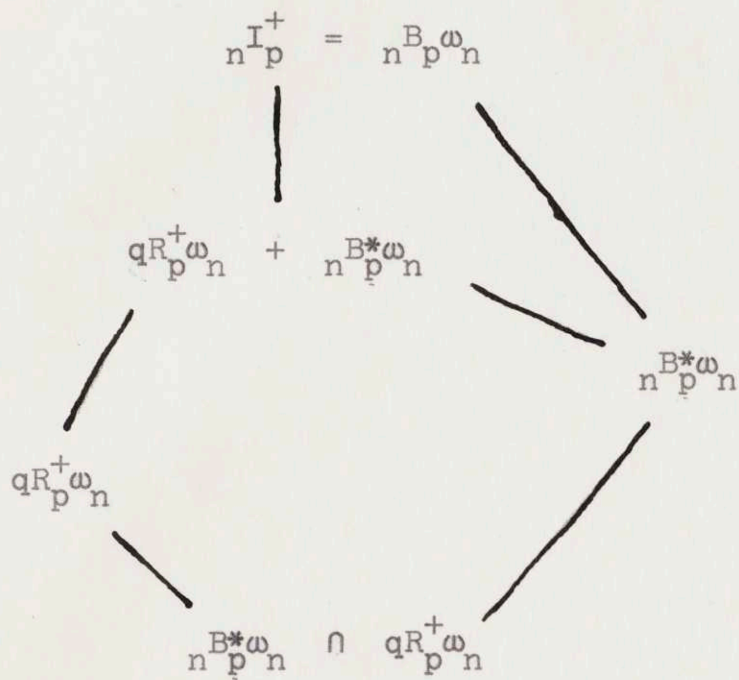
and $${}_nB^*_p = \left\{ \sum_a{}' u_a(\sigma_a - \sigma_{-a}) \mid u_a \in Z_p, \sum_a{}' a^n u_a \equiv 0 \ (q^2) \right\} \ n \text{ odd} .$$

Clearly, ${}_nB^*_p$ is an additive subgroup of ${}_nB_p$.

<u>Lemma 1.5.6:</u> $${}_nI^+_p = {}_nB_p\omega_n = qR^+_p\omega_n + {}_nB^*_p\omega_n \quad \text{for } n \text{ even}$$

$${}_nI^-_p = {}_nB_p\omega_n = qR^-_p\omega_n + {}_nB^*_p\omega_n \quad \text{for } n \text{ odd} .$$

<u>Proof:</u> (n even) From Corollary 1.5.4, we have ${}_nI_p^+ = {}_nB_p\omega_n$. It is also clear that $qR_p^+\omega_n \subseteq {}_nI_p^+$ and ${}_nB_p^*\omega_n \subseteq {}_nI_p^+$. Consider the following diagram:



Because ${}_nB_p$, ${}_nB_p^*$ and $\{\omega_n\} \subseteq R_p^+$, and ω_n is regular in R_p^+ , we have that:

$$[{}_nI_p^+ : {}_nB_p^*\omega_n] = [{}_nB_p\omega_n : {}_nB_p^*\omega_n] = [{}_nB_p : {}_nB_p^*] \ .$$

If we consider the map ψ: ${}_nB_p \to Z_p/q^2Z_p$ given by

$$\psi(\sum_a{}' \, u_a(\sigma_a + \sigma_{-a})) \equiv \sum_a{}' \, a^n u_a \bmod q^2 \, Z_p \qquad (u_a \in Z_p)$$

we have kernel $\psi = {}_nB_p^*$ and image ψ = set of elements in $Z_p/q^2Z_p \equiv 0 \bmod q \, Z_p$. Hence,

$$[{}_nB_p : {}_nB_p^*] = [{}_nB_p : \ker \psi] = \text{order (image } \psi) = q \ .$$

So we have $[{}_nI_p^+ : {}_nB_p^*\omega_n] = q$.

Going to the bottom part of the diagram, we obtain:

$$ {}_nB_p^*\omega_n \cap qR_p^+\omega_n = q_nB_p\omega_n = q_nI_p^+ \ . $$

Indeed, if $\xi \varepsilon {}_nB_p^*\omega_n \cap qR_p^+\omega_n$, then $\xi = y\omega_n = qz\omega_n$ where $y \varepsilon {}_nB_p^*$ and $z \varepsilon R_p^+$. Because ω_n is regular in S_p^+ we obtain $qz = y$. Using the basis of R_p^+ , we see that $z = y/q \varepsilon {}_nB_p$. Hence $\xi \varepsilon q_nB_p\omega_n$.

Conversely $q_nB_p\omega_n \subseteq {}_nB_p^*\omega_n \cap qR_p^+\omega_n$.

[N.B. If one tries to state this lemma for R^+ , an obstacle to the proof is encountered on the latter inclusion, for $R^+ \subsetneqq \varepsilon^+R$.]

Finally, $[qR_p^+\omega_n : q_nB_p\omega_n] = [qR_p^+ : q_nB_p]$, because ω_n is regular in S_p^+ . If we define the map

$$ \theta : qR_p^+ \to Z_p/q^2Z_p \quad \text{by} $$

$$ \theta(q \sum_a{}' u_a(\sigma_a + \sigma_{-a})) \equiv q \sum_a{}' a^n u_a \mod q^2 Z_p \quad (u_a \varepsilon Z_p) , $$

then kernel $\theta = q_nB_p$ and image θ = set of elements in Z_p/q^2Z_p which are $\equiv 0 \bmod q$. Hence we see that:

$$ [qR_p^+ : q_nB_p] = q \ . $$

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

$$[qR_p^+\omega_n + {}_nB_p^*\omega_n : {}_nB_p^*\omega_n] = [qR_p^+\omega_n : {}_nB_p^*\omega_n \cap qR_p^+\omega_n]$$

$$= [qR_p^+\omega_n : q_nB_p\omega_n] = q \ .$$

But we proved $[{}_nI_p^+ : {}_nB_p^*\omega_n] = q$. Hence multiplicativity of indices gives

$$[{}_nI_p^+ : qR_p^+\omega_n + {}_nB_p^*\omega_n] = 1$$

or $${}_nI_p^+ = qR_p^+\omega_n + {}_nB_p^*\omega_n \ .$$

Similarly, for n odd. Q.E.D.

CHAPTER 2.

Relations Between Ideals and Divisibility of Indices of Ideals

2.1 Motivation. Consider the case $q = p$, and $n = 1$ and 2. We have $B_1(x) = x - \frac{1}{2}$ and $B_2(x) = x^2 - x + \frac{1}{6}$, thus

$$\omega_1 = \frac{1}{p}\sum_{a=1}^{p-1}(a - \tfrac{1}{2}p)\sigma_a^{-1}, \quad \omega_2 = \frac{1}{p}\sum_{a=1}^{p-1}(a^2 - ap + \tfrac{1}{6}p^2)\sigma_a^{-1}.$$

By Corollary 1.5.4

$$[R_p^-: {}_1I_p^-] = p\Big(\prod_{\chi(-1)=-1}\chi(\omega_1)\Big)_p \qquad \chi \text{ a character mod } p$$

$$[R_p^+: {}_2I_p^+] = p\Big(\prod_{\chi(-1)=1}\chi(\omega_2)\Big)_p .$$

If $\chi \neq 1$, $\chi(\omega_1) = \frac{1}{p}\sum_a (a - \frac{1}{2}p)\,\chi^{-1}(a) = \frac{1}{p}\sum_a a\,\chi^{-1}(a)$.

If $\chi(-1) = 1$, $\chi \neq 1$, then

$$\sum_a \chi^{-1}(a)a = \sum_a{}'[\chi^{-1}(a)a + \chi^{-1}(p-a)(p-a)]$$

$$= \sum_a{}' \chi^{-1}(a)a + \chi^{-1}(a)(p-a) = 0 .$$

Thus for $\chi(-1) = 1$, $\chi \neq 1$, $\chi(\omega_2) = \frac{1}{p}\sum_a a^2\chi(a)$.

If $\chi = 1$, by 1.5.5 $(1(\omega_2))_p = (B_1^2)_p = (B_2^*)_p = (B_2^*(0))_p$ by definitions in 1.2

$= (B_2(1))_p = (\frac{1}{6})_p$ by 1.2.5.

On the other hand $\frac{1}{p}\sum_{a=1}^{p-1} a^2 = \frac{1}{6}(p-1)(2p-1)$. Hence $(1(\omega_2))_p = (\frac{1}{p}\sum_{a=1}^{p-1} a^2)_p$. Thus we may rewrite our formulae as:

$$[R_p^-: {}_1I_p^-] = p(\prod_{\chi(-1)=-1} \frac{1}{p}\sum_{a=1}^{p-1} a\,\chi(a))_p \quad \chi \text{ a character mod } p$$

$$[R_p^+: {}_2I_p^+] = p(\prod_{\chi(-1)=1} \frac{1}{p}\sum_{a=1}^{p-1} a^2\chi(a))_p \ .$$

Remark: $p|[R_p^-: {}_1I_p^-]$ iff $p|[R_p^+: {}_2I_p^+]$.

Proof: If χ is a character mod p, then the values that χ assumes are $(p-1)^{st}$ roots of unity, and hence lie in Q_p . There is a unique integer i , $0\le i\le p-2$ such that $\chi(a) \equiv a^i$ mod p, for all a , $(a,p) = 1$. Conversely, for a given i , $0\le i\le p-2$, there is a character χ with $\chi(a) \equiv a^i$ mod p for all a , $(a,p) = 1$. Furthermore, since $\chi(a)$ is a $(p-1)^{st}$ root of unity, we have $\chi^p(a) = \chi(a)$. Hence if $\chi(a) \equiv a^i$ mod p, then $\chi(a) = \chi^p(a) \equiv a^{ip}$ mod p^2. If χ is such that $\chi(-1) = -1$, and $\chi(a) \equiv a^i$ mod p, then i is odd. If χ' is such that $\chi'(-1) = 1$, and $\chi'(a) \equiv a^j$ mod p, then j is even.

Consider the sums involving such a χ and χ' :

$$\sum_{a=1}^{p-1} a\chi(a) \equiv \sum_{a=1}^{p-1} a \cdot a^{ip} = \sum_{a=1}^{p-1} a^{1+ip} \equiv p\, B_{\frac{1+ip}{2}} \mod p^2$$

$$(\text{where } \chi(-1) = -1,\ \chi(a) \equiv a^i(p))$$

$$\sum_a a^2 \chi'(a) \equiv \sum_a a^2 \cdot a^{jp} = \sum_a a^{2+jp} \equiv p\, B_{\frac{2+jp}{2}} \mod p^2$$

(where $\chi'(-1) = 1$, $\chi'(a) \equiv a^j (p)$)

(v. Nielsen [7], p. 277 or p. 296).

We know that $\frac{B_\mu}{\mu} \equiv (-1)^{k \cdot \frac{p-1}{2}} \frac{B_{\mu+k \cdot p-1/2}}{\mu+k \cdot p-1/2} \mod p$ if μ is not a multiple of $(p-1)/2$ (v. Bachmann [1], p. 41).

Also note that

$$1 \leq i \leq p-2 \text{ , hence } 1 \leq \frac{i+1}{2} \leq \frac{p-1}{2}$$

$$0 \leq j \leq p-3 \text{ , hence } 1 \leq \frac{j+2}{2} \leq \frac{p-1}{2} \text{ .}$$

Hence if $i \neq p-2$, $j \neq p-3$, we have that

$$\frac{2}{1+ip} B_{\frac{i+1}{2} + i \frac{(p-1)}{2}} \equiv (-1)^{\frac{1}{2}(i-ip)} \frac{2}{1+i} \cdot B_{\frac{1+i}{2}} \mod p$$

$$\frac{2}{2+jp} B_{\frac{2+j}{2} + j \frac{(p-1)}{2}} \equiv (-1)^{\frac{1}{2}(j-jp)} \frac{2}{2+j} \cdot B_{\frac{2+j}{2}} \mod p \text{ .}$$

Hence $p\, B_{\frac{1+ip}{2}} \equiv (-1)^{\frac{i-ip}{2}} p \cdot \frac{1+ip}{1+i} B_{\frac{1+i}{2}} \mod p^2$

$$p\, B_{\frac{2+jp}{2}} \equiv (-1)^{\frac{j-jp}{2}} p \cdot \frac{2+jp}{2+j} B_{\frac{2+j}{2}} \mod p^2 \text{ .}$$

Also for $i \neq p-2$, $j \neq p-3$ (that is, $i \leq p-4$, $j \leq p-5$)

$B_{\frac{2+j}{2}}$ and $B_{\frac{1+i}{2}}$ are in Z_p by the v. Staudt-Clausen theorem.

Hence we may conclude in this case that, if we specify $j = i-1$, then

$\frac{1}{p} \sum_a \chi(a)a$, $\frac{1}{p} \sum_a \chi'(a)a^2 \varepsilon Z_p$ and $p|\frac{1}{p} \sum_a \chi(a)a$ iff $p|\frac{1}{p} \sum_a \chi'(a)a^2$.

If $i = p-2$ and $j = p-3$, then $B_{\frac{1+ip}{2}} = B_{\frac{(p-1)^2}{2}} = \frac{1}{p} u$, u being a unit in Z_p and $B_{\frac{2+jp}{2}} = B_{\frac{(p-1)(p-2)}{2}} = \frac{1}{p} v$, v being a unit in Z_p, also by the von Staudt-Clausen theorem. Hence for such χ and χ', we have that $\sum_a a\chi(a)$ and $\sum a^2 \chi'(a)$ are units in Z_p. Putting all these facts together we have:

$$p|[R_p^-: {}_1I_p^-] \text{ iff } p|[R_p^+: {}_2I_p^+] .$$

This equivalence suggests that the factor groups $R_p^-/{}_1I_p^-$ and $R_p^+/{}_2I_p^+$ bear some relation to each other and further, that for any $n \geq 1$, and $q = p^m$, $m \geq 1$, we have a relation between $R_p^-/{}_nI_p^-$ and $R_p^+/{}_{n+1}I_p^+$ or $R_p^+/{}_nI_p^+$ and $R_p^-/{}_{n+1}I_p^-$, depending on whether n is odd or even.

<u>2.2 The main isomorphism theorem.</u> Define an additive homomorphism $f: R_p \to R_p$ by

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

f then extends by linearity to a homomorphism of R_p into R_p. f is thus a Z_p-homomorphism and $f(qR_p) \subseteq qR_p$. Hence f induces an additive homomorphism:

$$\overline{f}\colon R_p/qR_p \to R_p/qR_p .$$

$\overline{f}$ is, indeed, a ring homomorphism, because

$$f\left\{(\sum_a u_a\sigma_a)(\sum v_b\sigma_b)\right\} = f\left\{\sum_c(\sum_{\substack{ab\equiv c(q)\\ 0<a<q\\ 0\leq b<q}} u_a v_b)\sigma_c\right\}$$

$$\equiv \sum_c c^{-1}(\sum_{\substack{ab\equiv c(q)\\ 0<a<q\\ 0\leq b<q}} u_a v_b)\sigma_c \mod qR_p$$

$$f(\sum_a u_a\sigma_a)f(\sum_b u_b\sigma_b) \equiv (\sum_a a^{-1}u_a\sigma_a)(\sum_b b^{-1}v_b\sigma_b) = \sum_c(\sum_{\substack{ab\equiv c(q)\\ a,b}} a^{-1}b^{-1}u_a v_b)\sigma_c$$

$$\equiv \sum_c c^{-1}(\sum_{\substack{ab\equiv c(q)\\ a,b}} u_a v_b)\sigma_c \mod qR_p .$$

Note that by definition $\overline{f}$ is a Z_p-homomorphism; also we have that $\overline{f}(a\sigma_a) \equiv a\overline{f}(\sigma_a)$

$$\equiv a \cdot a^{-1}\sigma_a \equiv \sigma_a \mod qR_p .$$

Hence by linearity $\overline{f}$ is surjective. Finally, it is clear that $\overline{f}$ is injective; hence $\overline{f}$ is an automorphism. Let $\pi\colon R_p \to R_p/qR_p$ be the canonical projection.

<u>Lemma</u> <u>2.2.1:</u> If $p \nmid n$, $p \nmid n+1$, then

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

<u>Proof:</u> Recall that $\omega_n = \sum_a q^{n-1} B_n(a/q)\sigma_a^{-1}$ where

$$B_n(a) = a^n - \frac{1}{2} na^{n-1} + \sum_{u=1}^{\leq n/2} (-1)^{u-1} \binom{n}{2u} B_u a^{n-2u} .$$

Hence $\omega_n \equiv q^{-1} \sum_a (a^n - \frac{1}{2} qna^{n-1})\sigma_a^{-1} \mod qR_p$. By a simple calculation:

$${}_n B_p^* \omega_n \equiv \left\{ q^{-1} \sum_c [\sum_a{}' u_a(2R(c^{-1}a)^n - qnR(c^{-1}a)^{n-1})]\sigma_c ; \right.$$

$$\left. u_a \in Z_p , \sum_a{}' a^n u_a \equiv 0 \ (q^2) \right\} \mod qR_p$$

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

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

$$\alpha \equiv q^{-1} \sum_c [\sum_a{}' u_a(2R(c^{-1}a)^n - qnR(c^{-1}a)^{n-1})]\sigma_c \mod qR_p$$

where

$$u_a \in Z_p , \sum_a{}' a^n u_a \equiv 0 \ (q^2 Z_p) .$$

Then $f(\alpha) \equiv q^{-1} \sum_c [\sum_a{}' u_a(2R(c^{-1}a)^n c^{-1} - qnc^{-n}a^{n-1})]\sigma_c \mod qR_p$.

For $0 \leq a < q/2$, $(a,p) = 1$, 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 $\beta = q^{-1} \sum_{c}[\sum_{a}' v_a(2R(c^{-1}a)^{n+1} - q(n+1)R(c^{-1}a)^n)]\sigma_c$,

then $\beta \in R_p$, and $\pi(\beta) \in \pi({}_{n+1}B^*_p\omega_{n+1})$. We claim that $\pi(f(\alpha)) = \pi(\beta)$ or $f(\alpha) \equiv \beta \mod qR_p$ which will show that $\bar{f}(\pi({}_nB^*_p\omega_n)) \subseteq \pi({}_{n+1}B^*_p\omega_{n+1})$.

We have
$$\beta = q^{-1} \sum_{c}[\sum_{a}' \frac{n}{n+1} u_a \cdot 2R(c^{-1}a)^{n+1} a^{-1} - qnu_aR(c^{-1}a)^n a^{-1}]\sigma_c$$

$$\equiv q^{-1} \sum_{c}[\sum_{a}' \frac{n}{n+1} u_a \cdot 2R(c^{-1}a)^{n+1} a^{-1} - qnu_a c^{-n}a^{n-1}]\sigma_c \mod qR_p .$$

Hence $f(\alpha) \equiv \beta \mod qR_p$ iff

$$q^{-1} \sum_{c}(\sum_{a}' u_a 2R(c^{-1}a)^n c^{-1})\sigma_c \equiv q^{-1} \sum_{c}(\sum_{a}' \frac{n}{n+1} u_a 2R(c^{-1}a)^{n+1}a^{-1})\sigma_c \mod qR_p$$

which is true if and only if

(*) $\sum_{a}'(n+1)u_a c^{-1}R(c^{-1}a)^n \equiv \sum_{a}' nu_aR(c^{-1}a)^{n+1} a^{-1} \mod q^2$,

for c , $0 \leq c < q$, $(c,p) = 1$. But $R(c^{-1}a)^n - (c^{-1}a)^n = qt_{c^{-1}a}$, $R(c^{-1}a) - (c^{-1}a) = qs_{c^{-1}a}$ for some $s_{c^{-1}a}, t_{c^{-1}a} \in Z$; hence $R(c^{-1}a)^{n+1} - (c^{-1}a)^nR(c^{-1}a) - (c^{-1}a)R(c^{-1}a)^n + (c^{-1}a)^{n+1} \equiv 0 \mod q^2$, 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 congruence (*), we have

$f(\alpha) \equiv \beta \mod qR_p$ if and only if

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

which is 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, $0 \leq c < q$, $(c,p) = 1$. But by hypothesis $\Sigma' u_a a^n \equiv 0 \ (q^2)$, hence if and only if

$$(\ddagger) \quad \Sigma' u_a(c^{-1}R(c^{-1}a)^n - nR(c^{-1}a)c^{-n}a^{n-1}) \equiv 0 \mod q^2 .$$

But $R(c^{-1}a) = (c^{-1}a) + qt_{c^{-1}a}$, $t_{c^{-1}a} \in Z$; therefore

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

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

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

Substituting these results in congruence $(\ddagger)$, we have

$f(\alpha) \equiv \beta \mod qR_p$ iff

$$\sum_a{}' u_a(1-n)a^n c^{-(n+1)} \equiv 0 \mod q^2 \text{ for all } c,\ 0 \leq c < q,\ (c,p) = 1 .$$

But $\sum_a{}' a^n u_a \equiv 0 \ (q^2)$, therefore $f(\alpha) \equiv \beta \mod qR_p$ and hence $\overline{f}(\pi({}_nB_p^*\omega_n)) \subseteq \pi({}_{n+1}B_p^*\omega_{n+1})$.

We now show that the reverse inclusion holds.

Let $\pi(\beta) \in \pi({}_{n+1}B_p^*\omega_{n+1})$, then

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

where $v_a \in Z_p$, and $\sum_a{}' a^{n+1}v_a \equiv 0\ (q^2)$.

Let $u_a = \frac{n+1}{n} av_a$, 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 $\pi(\alpha) \in \pi({}_nB_p^*\omega_n)$. Then $f(\alpha) \equiv \beta \mod qR_p$ if and only if

$$q^{-1} \sum_c [\sum_a{}' av_a 2 \frac{n+1}{n} R(c^{-1}a)^n c^{-1}]\sigma_c \equiv q^{-1} \sum_c [\sum_a{}' v_a 2R(c^{-1}a)^{n+1}]\sigma_c \mod qR_p$$

iff $\sum_a{}' av_a(n+1)R(c^{-1}a)^n c^{-1} \equiv \sum_a{}' v_a nR(c^{-1}a)^{n+1} \mod q^2$,

for all c , $0 \leq c < q$, $(c,p) = 1$. But

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

and $\sum_a{}' a^{n+1} v_a \equiv 0\ (q^2)$ hence $f(\alpha) \equiv \beta \mod qR_p$ iff $\sum_a{}' c^{-1}av_aR(c^{-1}a)^n \equiv$

$\sum_a v_a nc^{-n}a^n R(c^{-1}a) \mod q^2$ iff $\sum_a{}' v_a[ac^{-1}R(c^{-1}a)^n -$

$n(c^{-1}a)^n R(c^{-1}a)] \equiv 0\ (q^2)$ for all c , $0 \leq c < q$, $(c,p) = 1$.

Just as in the first part of the proof, we have iff $(1-n)c^{-(n+1)} \sum_a{}' v_a a^{n+1} \equiv 0\ (q^2)$, which is, indeed, true by assumption. Hence $f(\alpha) \equiv \beta \mod qR_p$. Q.E.D.

<u>Lemma</u> <u>2.2.2:</u> i) $\bar{f}(\pi(R_p^-)) = \pi(R_p^+)$, $\bar{f}(\pi(R_p^+)) = \pi(R_p^-)$

ii) $\bar{f}(\pi(qR_p^-\omega_n)) = \pi(qR_p^+\omega_{n+1})$

$\bar{f}(\pi(qR_p^+\omega_n)) = \pi(qR_p^-\omega_{n+1})$.

<u>Proof:</u> i) $f(\sigma_a - \sigma_{-a}) \equiv a^{-1}\sigma_a - (-a)^{-1}\sigma_{-a}$

$$\equiv a^{-1}\sigma_a + a^{-1}\sigma_{-a}$$

$$\equiv a^{-1}(\sigma_a + \sigma_{-a}) \mod qR_p .$$

Because $\{\sigma_a - \sigma_{-a}\}$ generate R_p^- over Z_p , it follows that $\bar{f}(\pi(R_p^-)) \subseteq \pi(R_p^+)$. Conversely, the set $\{\sigma_a + \sigma_{-a}\}$ generates R_p^+ over Z_p , and $f(a(\sigma_a - \sigma_{-a})) \equiv \sigma_a + \sigma_{-a}$ mod qR_p , hence we have that $\pi(R_p^+) \subseteq \bar{f}(\pi(R_p^-))$ or $\bar{f}(\pi(R_p^-)) = \pi(R_p^+)$. Similarly $\bar{f}(\pi(R_p^+)) = \pi(R_p^-)$.

ii) Because $\bar{f}$ and π are multiplicative, it suffices to prove that $f(q\omega_n) \equiv q\omega_{n+1}$ mod qR_p , but this is trivial because $q\omega_n \equiv \sum_a a^n\sigma_a^{-1}$ and $q\omega_{n+1} \equiv \sum_a a^{n+1}\sigma_a^{-1}$ mod qR_p .

<u>Theorem</u> <u>2.2.3:</u> Let $\bar{f}: R_p/qR_p \to R_p/qR_p$ be the automorphism previously defined. Let $\pi: R_p \to R_p/qR_p$ be the canonical projection. Suppose $p \nmid n$, $p \nmid n+1$, then

i) $\bar{f}(\pi({}_nI_p^+)) = \pi({}_{n+1}I_p^-)$ (n even)

$\bar{f}(\pi({}_nI_p^-)) = \pi({}_{n+1}I_p^+)$ (n odd)

ii) $\overline{f}$ induces the following isomorphisms:

$$\pi(R_p^+)/\pi({}_nI_p^+) \cong \pi(R_p^-)/\pi({}_{n+1}I_p^-) \quad \text{(n even)}$$

$$\pi(R_p^-)/\pi({}_nI_p^-) \cong \pi(R_p^+)/\pi({}_{n+1}I_p^+) \quad \text{(n odd)} \quad .$$

Proof: i) for n even (entirely analogous for n odd)

$$_nI_p^+ = {}_nB_p^*\omega_n + qR_p^+\omega_n \qquad \text{(Lemma 1.5.6)} .$$

Hence,

$$\begin{aligned}
\overline{f}(\pi({}_nI_p^+)) &= \overline{f}(\pi({}_nB_p^*\omega_n)) + \overline{f}(\pi(qR_p^+\omega_n)) && \text{(by additivity)}\\
&= \pi({}_{n+1}B_p^*\omega_{n+1}) + \pi(qR_p^-\omega_{n+1}) && \text{(Lemmas 2.2.1 and 2.2.2)}\\
&= \pi({}_{n+1}B_p^*\omega_{n+1} + qR_p^-\omega_{n+1}) && \text{(again additivity)}\\
&= \pi({}_{n+1}I_p^-) && \text{(again Lemma 1.5.6)} .
\end{aligned}$$

ii) Follows immediately from part i) of this theorem and Lemma 2.2.2 part i) . Q.E.D.

Corollary 2.2.4: If $p \nmid n$, $p \nmid n+1$, then

$$p \mid [R_p^-: {}_nI_p^-] \text{ if and only if } p \mid [R_p^+: {}_{n+1}I_p^+] \quad \text{(n odd)}$$

and

$$p \mid [R_p^+: {}_nI_p^+] \text{ if and only if } p \mid [R_p^-: {}_{n+1}I_p^-] \quad \text{(n even)} .$$

Proof: (n odd) Define a homomorphism

$$\theta: R_p^-/{}_nI_p^- \to R_p^-/({}_nI_p^- + qR_p^-),$$

if $x \in R_p^-$, then $\Theta(x \bmod {}_nI_p^-) \equiv x \bmod({}_nI_p^- + qR_p^-)$.

Θ is surjective and kernel Θ is $q(R_p^-/{}_nI_p^-)$. Thus Θ induces an isomorphism:

$$\tilde{\Theta}:(R_p^-/{}_nI_p^-)/q(R_p^-/{}_nI_p^-) \to R_p^-/({}_nI_p^- + qR_p^-) .$$

Recall π: $R_p \to R_p/qR_p$ is the canonical projection. Define a homomorphism

$$\psi: R_p^-/({}_nI_p^- + qR_p^-) \to \pi(R_p^-)/\pi({}_nI_p^-) ,$$

if $x \in R_p^-$, $\psi(x \bmod ({}_nI_p^- + qR_p^-)) \equiv \pi(x) \bmod \pi({}_nI_p^-)$. ψ is well-defined. Indeed, if $x, y \in R_p^-$ and

$$x \equiv y \bmod {}_nI_p^- + qR_p^- , \text{ then}$$

$$\pi(x) \equiv \pi(y) \bmod \pi_n(I_p^-) \quad .$$

Clearly, ψ is surjective. Furthermore, for $x \in R_p^-$,

$\psi(x \bmod ({}_nI_p^- + qR_p^-)) \equiv 0 \bmod \pi_n(I_p^-)$ iff $x \in {}_nI_p^- \bmod qR_p$

iff $x = y + qz$, $y \in {}_nI_p^-$, $z \in R_p$.

But $x \in R_p^-$, hence iff $x = y + qz$, $y \in {}_nI_p^-$, $z \in R_p^-$.

iff $x \in {}_nI_p^- + qR_p^-$ iff $x \equiv 0 \bmod {}_nI_p^- + qR_p^-$.

Thus ψ is an isomorphism.

Hence

$\psi \circ \tilde{\Theta}:(R_p^-/{}_nI_p^-)/q(R_p^-/{}_nI_p^-) \to \pi(R_p^-)/\pi({}_nI_p^-)$ is an isomorphism.

Analogously, $(R_p^+/{}_{n+1}I_p^+)/q(R_p^+/{}_{n+1}I_p^+) \cong \pi(R_p^+)/\pi({}_{n+1}I_p^+)$. From the isomorphism of Theorem 2.2.3 part ii), and the isomorphisms just derived, we have the following isomorphism:

$$(R_p^-/{}_nI_p^-)/q(R_p^-/{}_nI_p^-) \cong (R_p^+/{}_{n+1}I_p^+)/q(R_p^+/{}_{n+1}I_p^+) \quad .$$

It is clear from the formulae of corollary 1.5.4 that $R_p^-/{}_nI_p^-$ and $R_p^+/{}_{n+1}I_p^+$ are p-groups. Therefore, $p \mid [R_p^- : {}_nI_p^-]$ iff $R_p^-/{}_nI_p^- \nmid q(R_p^-/{}_nI_p^-)$ iff $R_p^+/{}_{n+1}I_p^+ \nmid q(R_p^+/{}_{n+1}I_p^+)$ iff $p \mid [R_p^+ : {}_{n+1}I_p^+]$. Similarly for n even.

2.3 Inverse systems. Until now we have considered $q = p^m$ to be defined for some fixed m , $m \geq 1$. We consider m to vary and let $q_m = p^m$, $m \geq 1$, $p \nmid 2$. 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 $S_m = Q_p[G_m]$, $R_m = Z_p[G_m]$,

$$\varepsilon_m^- = \tfrac{1}{2}(\sigma(1)_m - \sigma(-1)_m) \ , \ \varepsilon_m^+ = \tfrac{1}{2}(\sigma(1)_m + \sigma(-1)_m)$$

$$R_m^- = \varepsilon_m^- R_m \ , \quad R_m^+ = \varepsilon_m^+ R_m$$

$${}_n\omega_m = q_m^{n-1} \sum_{\substack{0 \leq a < q_m \\ (a,p)=1}} B_n(a/q_m)\sigma(a)_m^{-1}$$

$${}_nI_m^- = R_m^- \cap R_m\, {}_n\omega_m \ \ (n \text{ odd}) \ , \ {}_nI_m^+ = R_m^+ \cap R_m\, {}_n\omega_m \ \ (n \text{ even}) .$$

Let $${}_nB_m = \Big\{ \sum_{\substack{0\le a<q_m/2 \\ (a,p)=1}} u_a(\sigma(a)_m - \sigma(-a)_m) \,|\, u_a \in Z_p \;, \quad \sum_{\substack{0\le a<q_m/2 \\ (a,p)=1}} a^n u_a \equiv 0 \quad (q_m) \Big\} \quad (n \text{ odd})$$

$${}_nB_m = \Big\{ \sum_{\substack{0\le a<q_m/2 \\ (a,p)=1}} u_a(\sigma(a)_m + \sigma(-a)_m) \,|\, u_a \in Z_p \;, \quad \sum_{\substack{0\le a<q_m/2 \\ (a,p)=1}} a^n u_a \equiv 0 \quad (q_m) \Big\} \quad (n \text{ even})$$

then ${}_nI_m^- = {}_nB_m \cdot {}_n\omega_m$ (n odd), ${}_nI_m^+ = {}_nB_m \cdot {}_n\omega_m$ (n even) .

$\{S_m\}_{m\ge1}$, $\{R_m\}_{m\ge1}$, $\{R_m^-\}_{m\ge1}$, $\{R_m^+\}_{m\ge1}$, $\{{}_nI_m^-\}_{m\ge1}$ (for fixed odd n), $\{{}_nI_m^+\}_{m\ge1}$ (for fixed even n), form inverse systems with respect to homomorphisms to be defined presently.

Define $t_{m,m+1}: S_{m+1} \to S_m$ $(m\ge1)$

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

(It will be understood that all summations are over integers prime to p .)

$t_{m,m+1}$ is clearly additive $(m\ge1)$. It is also multiplicative.

Indeed, $t_{m,m+1}(\sum_{0\le a<q_{m+1}} v_a\sigma(a)_{m+1})t_{m,m+1}(\sum_{0\le c<q_{m+1}} u_c\sigma(c)_{m+1})$

$(v_a, u_c \in Q_p)$

$$= [\sum_{0\le b<q_m}(\sum_{\substack{0\le a<q_{m+1}\\ a\equiv b(q_m)}} v_a)\sigma(b)_m][\sum_{0\le d<q_m}(\sum_{\substack{0\le c<q_{m+1}\\ c\equiv d(q_m)}} u_c)\sigma(d)_m]$$

$$= \sum_{0\le e<q_m}\left\{\sum_{\substack{0\le b<q_m\\ 0\le d<q_m\\ bd\equiv e(q_m)}}(\sum_{\substack{0\le a<q_{m+1}\\ a\equiv b(q_m)}} v_a)(\sum_{\substack{0\le c<q_{m+1}\\ c\equiv d(q_m)}} u_c)\right\}\sigma(e)_m \ .$$

On the other hand, $t_{m,m+1}[\sum_{0\le a<q_{m+1}} v_a\sigma(a)_{m+1} \sum_{0\le c<q_{m+1}} u_c\sigma(c)_{m+1}]$

$$= t_{m,m+1}[\sum_{0\le i<q_{m+1}}(\sum_{\substack{0\le a<q_{m+1}\\ 0\le c<q_{m+1}\\ ac\equiv i(q_{m+1})}} v_a u_c)\sigma(i)_{m+1}]$$

$$= \sum_{0\le e<q_m}\left\{\sum_{\substack{0\le i<q_{m+1}\\ i\equiv e(q_m)}}(\sum_{\substack{0\le a<q_{m+1}\\ 0\le c<q_{m+1}\\ ac\equiv i(q_{m+1})}} v_a u_c)\right\}\sigma(e)_m \ .$$

We wish to show

$$\sum_{\substack{0\le i<q_{m+1}\\ i\equiv e(q_m)}}(\sum_{\substack{0\le a<q_{m+1}\\ ac\equiv i(q_{m+1})}} v_a u_c{}_{0\le c<q_{m+1}}) = \sum_{\substack{0\le b<q_m\\ 0\le d<q_m\\ bd\equiv e(q_m)}}(\sum_{\substack{0\le a<q_{m+1}\\ a\equiv b(q_m)}} v_a)(\sum_{\substack{0\le c<q_{m+1}\\ c\equiv d(q_m)}} u_c)$$

for all $0\le e<q_m$, $(e,p) = 1$.

The left hand-side $= \sum_{\substack{0\le a<q_{m+1}\\ 0\le c<q_{m+1}\\ ac\equiv e(q_m)}} v_a u_c = \sum_{\substack{0\le b<q_m\\ 0\le d<q_m\\ bd\equiv e(q_m)}} \sum_{\substack{0\le a<q_{m+1}\\ 0\le c<q_{m+1}\\ a\equiv b(q_m)\\ c\equiv d(q_m)}} v_a u_c$

$$= \sum_{\substack{0\le b<q_m\\ 0\le d<q_m\\ bd\equiv e(q_m)}} \Big(\sum_{\substack{0\le a<q_{m+1}\\ a\equiv b(q_m)}} v_a\Big)\Big(\sum_{\substack{0\le c<q_{m+1}\\ c\equiv d(q_m)}} u_c\Big)$$

= right hand side .

Hence $t_{m,m+1}: S_{m+1} \to S_m$ is a multiplicative homomorphism. Clearly, $t_{m,m+1}(R^+_{m+1}) = R^+_m$, $t_{m,m+1}(R^-_{m+1}) = R^-_m$. We now take a fixed even n . Let $\tau(a)_m = \sigma(a)_m + \sigma(q_m-a)_m$, then

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

We will show $t_{m,m+1}({}_nB_{m+1}) \subseteq {}_nB_m$. Indeed,

$$t_{m,m+1}\Big(\sum_{0\le a<q_{m+1}/2} u_a\tau(a)_{m+1}\Big)$$

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

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

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

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

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

To show that $t_{m,m+1}\Big(\sum_{0\le a<q_{m+1}/2} u_a \tau(a)_{m+1} \Big) \in {}_nB_m$, we must show that

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

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

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

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

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

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

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

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

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

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

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

(by 1.2.3) $$= q_{m+1}^{n-1} \sum_{0\le a<q_m} p^{1-n} B_n(p \cdot a/q_{m+1})\sigma(a)_m^{-1}$$

$$= q_m^{n-1} \sum_{0\le a<q_m} B_n(a/q_m)\sigma(a)_m^{-1} = {}_n\omega_m$$

that is, $t_{m,m+1}({}_n\omega_{m+1}) = {}_n\omega_m$.

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

$$t_{m,m+1}({}_nI_{m+1}^+) = t_{m,m+1}({}_nB_{m+1})t({}_n\omega_{m+1}) \subseteq {}_nB_m \cdot {}_n\omega_m = {}_nI_m^+$$

for n even. Similarly for n odd.

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

2.4 <u>Isomorphisms of inverse limits.</u> Let $\pi_m\colon R_m \to R_m/q_mR_m$ be the canonical projection $(m\ge 1)$. Since $t_{m,m+1}(q_{m+1}R_{m+1}) \subseteq q_mR_m$, we have that $t_{m,m+1}$ induces a map $t_{m,m+1}\colon \pi_{m+1}(R_{m+1}) \to \pi_m(R_m)$ given by:

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

By abuse of notation, we denote the homomorphisms of our inverse systems $\{\pi_m(R_m)\}_{m\ge 1}$ by $t_{m,m+1}$. Clearly $\{\pi_m(R_m^-)\}$, $\{\pi_m(R_m^+)\}$, $\{\pi_m({}_nI_m^+)\}$ (n even), $\{\pi_m({}_nI_m^-)\}$ (n odd) $(m\ge 1)$ form inverse systems with respect to these homomorphisms.

We therefore also have that the finite p-groups $R_m^+/{}_nI_m^+$, $R_m^-/{}_nI_m^-$, $\pi_m(R_m^+)/\pi_m({}_nI_m^+)$, $\pi_m(R_m^-)/\pi_m({}_nI_m^-)$ $(m\geq 1)$ all form inverse systems of groups with respect to the homomorphisms $t_{m,m+1}$ (for the finiteness of these groups v. Corollary 1.5.4 and the proof of Corollary 2.2.4). 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 2.2, we define for $m \geq 1$, the automorphism $\overline{f}_m: R_m/q_mR_m \to R_m/q_mR_m$ by $\overline{f}_m(\sigma(a)_m) \equiv a^{-1}\sigma(a)_m$ mod $q_m R_m$. Clearly, $t_{m,m+1} \circ \overline{f}_{m+1} = \overline{f}_m \circ t_{m,m+1}$. On the other hand (v. Theorem 2.2.3) we have proven that if $p \nmid n$, $p \nmid n+1$ then $\overline{f}_m$ induces isomorphisms:

$$\overline{f}_m: \pi_m(R_m^-)/\pi_m({}_nI_m^-) \cong \pi_m(R_m^+)/\pi_m({}_{n+1}I_m^+) \quad \text{(n odd)}$$

$$\overline{f}_m: \pi_m(R_m^+)/\pi_m({}_nI_m^+) \cong \pi_m(R_m^-)/\pi_m({}_{n+1}I_m^-) \quad \text{(n even)}$$

(for all $m \geq 1$). Because $\overline{f}_m$ and $t_{m,m+1}$ commute, we have that $\{\overline{f}_m\}_{m\geq 1}$ is a map of the inverse system $\{\pi_m(R_m^-)/\pi_m({}_nI_m^-)\}_{m\geq 1}$ into $\{\pi_m(R_m^+)/\pi_m({}_{n+1}I_m^+)\}_{m\geq 1}$ (n odd) and $\{\pi_m(R_m^+)/\pi_m({}_nI_m^+)\}_{m\geq 1}$ into $\{\pi_m(R_m^-)/\pi_m({}_{n+1}I_m^-)\}_{m\geq 1}$ (n even).

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

$$(*) \quad \varprojlim_m \pi_m(R_m^-)/\pi_m({}_nI_m^-) \cong \varprojlim_m \pi_m(R_m^+)/\pi_m({}_{n+1}I_m^+) \quad (n \text{ odd})$$

$$(*) \quad \varprojlim_m \pi_m(R_m^+)/\pi_m({}_nI_m^+) \cong \varprojlim_m \pi_m(R_m^-)/\pi_m({}_{n+1}I_m^-) \quad (n \text{ even}) .$$

On the other hand we have from the proof of Corollary 2.2.4 that

$$(R_m^-/{}_nI_m^-)/q_m(R_m^-/{}_nI_m^-) \cong \pi_m(R_m^-)/\pi_m({}_nI_m^-) \quad (n \text{ odd})$$

$$(R_m^+/{}_nI_m^+)/q_m(R_m^+/{}_nI_m^+) \cong \pi_m(R_m^+)/\pi_m({}_nI_m^+) \quad (n \text{ even}) .$$

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

$$\varprojlim_m (R_m^-/{}_nI_m^-)/q_m(R_m^-/{}_nI_m^-) \cong \varprojlim_m \pi_m(R_m^-)/\pi_m({}_nI_m^-) \quad (n \text{ odd})$$

$$\varprojlim_m (R_m^+/{}_nI_m^+)/q_m(R_m^+/{}_nI_m^+) \cong \varprojlim_m \pi_m(R_m^+)/\pi_m({}_nI_m^+) \quad (n \text{ even}) .$$

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

$$\varprojlim_m (R_m^-/{}_nI_m^-)/q_m(R_m^-/{}_nI_m^-) \cong \varprojlim_m (R_m^+/{}_{n+1}I_m^+)/q_m(R_m^+/{}_{n+1}I_m^+) \quad (n \text{ odd})$$

and

$$\varprojlim_m (R_m^+/{}_nI_m^+)/q_m(R_m^+/{}_nI_m^+) \cong \varprojlim_m (R_m^-/{}_{n+1}I_m^-)/q_m(R_m^-/{}_{n+1}I_m^-) \quad (n \text{ even}) .$$

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

$$\varprojlim_m q_m(R_m^-/{}_nI_m^-) = 0 \quad (n \text{ odd})$$

$$\varprojlim_m q_m(R_m^+/{}_nI_m^+) = 0 \quad (n \text{ even}) ,$$

then we will have proven that if $p \nmid n$ and $p \nmid (n+1)$

$$\varprojlim_m R_m^-/{}_nI_m^- \cong \varprojlim_m R_m^+/{}_{n+1}I_m^+ \qquad (n \text{ odd})$$

$$\varprojlim_m R_m^+/{}_nI_m^+ \cong \varprojlim_m R_m^-/{}_{n+1}I_m^- \qquad (n \text{ even}) .$$

We show that $\varprojlim_m q_m(R_m^-/{}_nI_m^-) = 0$ (n odd) (proof same for n even). Indeed, if $(u_m)_{m\geq 1} \in \varprojlim_m q_m(R_m^-/{}_nI_m^-)$, then for any $m \geq 1$, and for any $r > m$,

$$u_m = t_{m,m+1} \cdots t_{r-1,r}\,(q_r v_r)$$

$$= q_r t_{m,m+1} \cdots t_{r-1,r}(v_r) \quad (u_m \in q_m(R_m^-/{}_nI_m^-), v_r \in R_r^-/{}_nI_r^-) .$$

Suppose order $(R_m^-/{}_nI_m^-) = q_{r_0}$ (recall $R_m^-/{}_nI_m^-$ 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 $(u_m)_{m\geq 1} = (0)_{m\geq 1}$ or $\varprojlim_m q_m(R_m^-/{}_nI_m^-) = 0$. Hence we have proven:

<u>Theorem 2.4.1:</u> If $p \nmid n$ and $p \nmid n+1$ then

$$\varprojlim_m R_m^- / {}_n I_m^- \cong \varprojlim_m R_m^+ / {}_{n+1} I_m^+ \qquad (n \text{ odd})$$

$$\varprojlim_m R_m^+ / {}_n I_m^+ \cong \varprojlim_m R_m^- / {}_{n+1} I_m^- \qquad (n \text{ even}) .$$

<u>2.5</u> <u>Conclusion.</u> Recall that $q_m = p^m$, ζ_m is a primitive $q_m{}^{th}$ root of unity, $F_m = Q(\zeta_m)$, and $G_m = G(F_m/Q)$. Now let $F = \bigcup_{m\geq 1} F_m$. Then F/Q is an abelian extension. Let $G = G(F/Q)$. Further, let $\Phi_m = Q_p(\zeta_m)$ $(m\geq 1)$; let U be the multiplicative group of all p-adic units in Q_p. There exists an isomorphism

$$\kappa : G \rightarrow U$$

such that

$$\zeta^\sigma = \zeta^{\kappa(\sigma)}$$

for any $\sigma \in G$ and ζ any $q_m{}^{th}$ root of unity $(m\geq 1)$ in F. Let $\tau \in G$ be such that $\kappa(\tau) = -1$. (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 [5]). 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 $\sigma(\sum_{\rho \varepsilon H} a_\rho \rho)$ $(a_\rho \varepsilon T, \sigma \varepsilon G)$ to be $\sum_{\rho \varepsilon H} a_\rho s^{-1} \rho$ where s denotes the image of σ under $G \to H$. Hence R_m and S_m are both G-modules by means of the natural homomorphism $G \to G_m$, hence also $Z_p[G]$-modules. We note that as $Z_p[G]$-modules, $R_m^{\pm}$ and $S_m^{\pm}$ have the same meaning as before.

If M_1 and M_2 are G-modules and if $h: M_1 \to M_2$ is such that i) $h(x + y) = h(x) + h(y)$

ii) $h(x^\sigma) = \kappa(\sigma)\, h(x)^\sigma \quad (\sigma \varepsilon G)$

then h will be called a κ-isomorphism. The definition of a κ-isomorphism of two G-modules is clear.

Iwasawa introduces (v. [5]) two $Z_p[G]$-modules (among others) $\underset{\sim}{X}$ and $\underset{\sim}{Z}$ which are defined as inverse limits of certain subgroups $\underset{\sim}{X}_m$ and $\underset{\sim}{Z}_m$ respectively of the additive group of Φ_m , $m \geq 1$; Z is a sub-module of X . He also introduces two $Z_p[G]$-modules $\underset{\sim}{A}$ and $\underset{\sim}{B}$ which are defined as inverse limits of certain submodules $\underset{\sim}{A}_m$ and $\underset{\sim}{B}_m$ respectively of the $Z_p[G]$-modules S_m , $m \geq 1$. In detail, let R_m^0 denote the sub-module of all $\sum_\sigma a_\sigma \sigma (\sigma \varepsilon G_m, a_\sigma \varepsilon Z_p)$ in R_m such that $\sum_\sigma a_\sigma = 0$, and let

$$\underset{\sim}{A}_m = \underset{\sim}{B}_m + R_m^0 , \quad \underset{\sim}{B}_m = R_m \xi_m ,$$

where $\xi_m = q_m^{-1} \sum_a (a - \frac{q_m - p}{2})\sigma(a)_m$, $0 \leq a < q_m$, $(a,p) = 1$.

It is then shown that there exists a $Z_p[G]$ isomorphism of $(m \geq 1)$ $\underset{\sim}{A}_m \to \underset{\sim}{X}_m$, $\underset{\sim}{B}_m \to \underset{\sim}{Z}_m$, $\underset{\sim}{A}_m/\underset{\sim}{B}_m \to \underset{\sim}{X}_m/\underset{\sim}{Z}_m$.

Since the isomorphism commutes with the homomorphisms of the associated inverse systems, we have that the isomorphism induces a $Z_p[G]$-isomorphism of $\underset{\sim}{A}/\underset{\sim}{B} \to \underset{\sim}{X}/\underset{\sim}{Z}$ ([5], Thm. 2). Furthermore, the algebra S_m has an involution $\alpha \to \alpha^*$ such that $\sigma^* = \sigma^{-1}$ for any $\sigma \in G_m$. If we denote by $\underset{\sim}{A}^*$ the inverse limit of $\underset{\sim}{A}_m^*$, $m \geq 1$, then the maps $\underset{\sim}{A}_m \to \underset{\sim}{A}_m^*$, $m \geq 1$ define a Z_p-isomorphism (not a G-isomorphism) $\underset{\sim}{A} \to \underset{\sim}{A}^*$ such that $(\sigma\alpha)^* = \sigma^{-1}\alpha^*$ $(\sigma \in G, \alpha \in A)$. The inverse limit of $\underset{\sim}{B}_m^*$, $m \geq 1$, gives a $Z_p[G]$-submodule $\underset{\sim}{B}^*$ of $\underset{\sim}{A}^*$; the above isomorphism induces similar isomorphisms $\underset{\sim}{B} \to \underset{\sim}{B}^*$ and $\underset{\sim}{A}/\underset{\sim}{B} \to \underset{\sim}{A}^*/\underset{\sim}{B}^*$ (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 , $m \geq 1$; Z is a submodule of X . He then defines a κ-isomorphism

$$h: X \to \underset{\sim}{X}$$

such that $h(Z) = \underset{\sim}{Z}$, and hence h induces a κ-isomorphism

$$h: X/Z \to \underset{\sim}{X}/\underset{\sim}{Z} .$$

Putting all the isomorphisms together we have the following diagram:

$$\begin{array}{ccccc} \mathbf{A}^*/\mathbf{B}^* & \longrightarrow & \mathbf{A}/\mathbf{B} & \xrightarrow{Z_p[G]\text{-isom.}} & \mathbf{X}/\mathbf{Z} \\ & & & \kappa\text{-isom.} \nearrow & \\ & & X/Z & & \end{array}$$

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

$$\begin{array}{ccccc} (\mathbf{A}^*/\mathbf{B}^*)^- & \longrightarrow & (\mathbf{A}/\mathbf{B})^- & \xrightarrow{Z_p[G]\text{-isom.}} & (\mathbf{X}/\mathbf{Z})^- \\ & & & \kappa\text{-isom.} \nearrow & \\ & & (X/Z)^+ & & \end{array}$$

Iwasawa (Prop. 1 and Prop. 2, [5]) gives the algebraic structure of $\mathbf{A}/\mathbf{B}$ and hence the algebraic structure of $\mathbf{X}/\mathbf{Z}$. However, since $h: X/Z \to \mathbf{X}/\mathbf{Z}$ is only a κ-isomorphism, knowing the structure of $\mathbf{X}/\mathbf{Z}$ does not provide us with such knowledge of X/Z . To study $(X/Z)^+$ in particular, it would suffice to find a G-module M whose structure is known and for which we have a κ-isomorphism of $M \to (\mathbf{X}/\mathbf{Z})^-$ or $(A/B)^-$; indeed, we would have induced a $Z_p[G]$-isomorphism

$$M \rightarrow (X/Z)^{+}$$

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 $\varprojlim R_m^{+}/{}_2I_m^{+}$. We do obtain an isomorphism of $\varprojlim R_m^{+}/{}_2I_m^{+} \rightarrow (\underset{\sim}{X}/\underset{\sim}{Z})^{-}$, but it is not a κ-isomorphism as we will presently see.

It follows immediately from the definitions of $\underset{\sim}{A}_m$ and $\underset{\sim}{B}_m$ that ([5], p. 76):

$$\underset{\sim}{A}_m^{*-}/\underset{\sim}{B}_m^{*-} \cong R_m^{-}/(R_m^{-} \cap R_m\xi_m) .$$

Because $\xi_m = {}_1\omega_m + \frac{1}{2} q_{m-1}^{-1} \sum_a \sigma(a)_m$, we have

${}_1I_m^{-} = {}_1B_m\, {}_1\omega_m \subseteq R_m^{-} \cap R_m\xi_m$ (v. Corollary 1.5.4); thus we have an epimorphism of finite groups:

$$R_m^{-}/{}_1I_m^{-} \rightarrow R_m^{-}/(R_m^{-} \cap R_m\xi_m) .$$

The order of $R_m^{-}/{}_1I_m^{-} = q_m\Big(\prod_{\substack{\chi \bmod q_m \\ \chi(-1)=-1}} B_\chi^1\Big)_p$ (v. Corollary 1.5.4) .

The order of $R_m^{-}/R_m^{-} \cap R_m\xi_m$ = order $\underset{\sim}{A}_m^{*-}/\underset{\sim}{B}_m^{*-}$ (by isomorphism)

= order $\underset{\sim}{A}_m^{-}/\underset{\sim}{B}_m^{-}$ (again by isomorphism)

= exact power of p dividing the first factor h_m^{-} of the class number of F_m (v. [5], Prop. 4).

$= q_m\Big(\prod_{\substack{\chi \bmod q_m \\ \chi(-1)=-1}} B_\chi^1\Big)_p$ (v. [4], p. 171 and line 1.5.5 this paper).

Thus,

$$R_m^-/{}_1I_m^- \cong R_m^-/(R_m^- \cap R_m\xi_m) \qquad (m \geq 1) .$$

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

$$\underset{\sim}{A}{}_m^{*-}/\underset{\sim}{B}{}_m^{*-} \to R_m^-/{}_1I_m^- ;$$

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

$$\varprojlim \underset{\sim}{A}{}_m^{*-}/\underset{\sim}{B}{}_m^{*-} \cong \varprojlim R_m^-/{}_1I_m^- \quad (Z_p[G]\text{-isomorphism}) .$$

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

$$\varprojlim R_m^-/{}_1I_m^- \cong (\underset{\sim}{A}{}^*/\underset{\sim}{B}{}^*)^- \quad (Z_p[G]\text{-isomorphism}) .$$

Recall from Theorem 2.4.1 that since $p \nmid 1$, $p \nmid 2$ we have an isomorphism of $\varprojlim R_m^+/{}_2I_m^+ \to \varprojlim R_m^-/{}_1I_m^-$. Call this isomorphism u. A little consideration of how u was constructed shows that u is a κ-isomorphism. We thus have the following diagram:

$$\varprojlim R_m^+/{}_2I_m^+ \xrightarrow{u} \varprojlim R_m^-/{}_1I_m^- \to (\underset{\sim}{A}{}^*/\underset{\sim}{B}{}^*)^- \to (\underset{\sim}{A}/\underset{\sim}{B})^- \to (\underset{\sim}{X}/\underset{\sim}{Z})^-$$

$$(X/Z)^+ \xrightarrow{h} (\underset{\sim}{X}/\underset{\sim}{Z})^-$$

If we compose the maps from $\varprojlim R_m^+/{}_2I_m^+ \to (\underset{\sim}{X}/\underset{\sim}{Z})^-$, calling this composition v, we have $v(x^\sigma) = \kappa(\sigma)v(x)^{\sigma^{-1}}$ (where $x \in \varprojlim R_m^+/{}_2I_m^+$, $\sigma \in G$). Thus we failed to obtain a

κ-isomorphism.

For completeness, we conclude by giving an example of the kind of algebraic property which is preserved by a G-isomorphism but not by a κ-isomorphism. Let $\gamma \varepsilon G$ be such that $\kappa(\gamma) = 1 + p$. Let $\gamma_n = 1 - \gamma^{p^n}$, $n \geq 0$, $\gamma_n \varepsilon Z_p[G]$. If M is a $Z_p[G]$-module, we will say, according to Iwasawa, that M is <u>strictly</u> <u>Γ-finite</u> if M/M^{γ_n} is a finite group for all $n \geq 0$. This property is preserved under G-isomorphisms but not necessarily under κ-isomorphism.

Bibliography

1. P. Bachmann, Niedere Zahlentheorie, Teil 2, Leipzig, 1910.

2. L. Carlitz and F. R. Olson, "Maillet's determinant", Proc. Amer. Math. Soc. vol. 6 (1955), 265-269.

3. H. T. Davis, Tables of Higher Mathematical Functions, vol. 2, Bloomington, Indiana, 1935.

4. K. Iwasawa, "A class number formula for cyclotomic fields", Ann. of Math. vol. 76 (1962), 171-179.

5. K. Iwasawa, "On some modules in the theory of cyclotomic fields", J. Math. Soc. of Japan vol. 16 (1964), 42-82.

6. H. W. Leopoldt, "Eine Verallgemeinerung der Bernoullischen Zahlen", Abh. Math. Sem. Univ. Hamburg, Band 22 (1958). 131-140.

7. N. Nielsen, Traite elementaire des nombres de Bernoulli, Paris, 1923.

Biographical Note

I was born in Elizabeth, New Jersey on September 9, 1938. I entered Columbia College in September, 1956 and received the A.B. degree, *magna cum laude*, in June, 1960. I was elected to the Phi Beta Kappa Society of Columbia College in the spring of 1960. I entered M.I.T. in September, 1960; since then, I have been a teaching assistant for three and a half years and a research assistant for a year and a half. For the summers of 1962, 1963, and 1964, I held a National Science Foundation Summer Fellowship for Teaching Assistants.

I was married to Miss Susan Jane Buchalter on August 26, 1962; we have one daughter.