Abelian p-adic Group Rings.

Autor(en): **Spiegel, Eugene**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **50 (1975)**

PDF erstellt am: **27.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-38789

Comment. Math. Helvetici 50 (1975) 27–32 Birkhäuser Verlag, Basel

Abelian p-adic Group Rings

EUGENE SPIEGEL

Introduction

In the following we investigate the question of when two finite abelian groups G and H have isomorphic group-algebras over the p-adic integers and p-adic field.

We use the following notation: N denotes the positive integers, p and q are distinct primes in N, Z_n is the ring of integers modulo n ($n \in N$), P is the ring of p-adic integers, Q_p is the field of p-adic numbers and C_n denotes a cyclic group of order n ($n \in N$). If G is a finite group and R is a principal ideal domain, $RG = R(G)$ will be the group algebra of G over R.

§1

Throughout this section, G and H denote finite abelian groups of order q^n. If F is a field of characteristic $k \neq q$, by the theorem of Perlis-Walker [3], $F(G) \simeq \sum_{d=1}^{n} (n_d/v_d) F(\zeta_d)$, where ζ_d is a primitive q^dth root of unity over F, $v_d = \text{degree}(F(\zeta_d)/F)$ and n_d is the number of elements of order q^d in G. Also, n_d/v_d is a non-negative integer.

As $(q^d, p) = 1$, the splitting field of the polynomial $g(x) = x^{q^d} - 1$ over Q_p, is a totally unramified extension of Q_p. This says that degree $(Q_p(\zeta_d)/Q_p) = \text{degree}(Z_p(\zeta_d)/Z_p)$, where ζ_d is a primitive q^dth root of unity over Z_p. Hence we can write

$$Q_p G \simeq \sum_{d=1}^{n} a_d Q_p(\zeta_d) \qquad (*)$$

and

$$Z_p G \simeq \sum_{d=1}^{n} a_d Z_p(\zeta_d)$$

for a common collection of integers $a_d = n_d/v_d$, $d = 1, 2, \ldots, n$.

The following generalization of the Perlis-Walker result is due to Raggi Cárdenas.

PROPOSITION 1.1. *Let A be a local ring, with maximal ideal M, and residue field K of characteristic p. Suppose M is finite, and $\bigcap_{n=0}^{\infty} M^n = \{0\}$. Then $AG \simeq \sum_{d=1}^{n} (n_d/v_d) A(\zeta_d)$ where ζ_d is a primitive q^dth root of unity, $v_d = \text{degree}(K(\zeta_d)/K)$ and n_d is the number of elements of order q^d in G.*

Proof. See [4].

LEMMA 1.2. *If a_d, $d=1, 2, \ldots, n$, are defined as in $(*)$, then $PG \simeq \sum_{d=1}^{n} a_d P(\zeta_d)$.*

Proof. If $m \in N$, the residue field of the local ring Z_{p^m} is Z_p. Due to Proposition 1.1 we must have

$$Z_{p^m} G \simeq \sum_{d=1}^{n} a_d Z_{p^m}(\zeta_d).$$

By taking injective limits, (the injective limit of Z_{p^m} is P), the above isomorphism leads to an isomorphism

$$PG \simeq \sum_{d=1}^{n} a_d P(\zeta_d).$$

COROLLARY 1.3. *If a_d, $d=1, 2, \ldots, n$, are defined as in $(*)$, and R is either Z_p, P or Q_p then*

$$RG \simeq \sum_{d=1}^{n} a_d R(\zeta_d)$$

where ζ_d is a primitive q^dth root of unity.

We define the function $\gamma: N \to N$ by $\gamma_q(m)$ is the least positive integer such that $p^{\gamma_q(m)} \equiv 1$ (modulo q^m). Then $\gamma_q(1) \leqslant \gamma_q(2) \leqslant \ldots$ and $\gamma_q(d) \to \infty$. If $d \in N$, and ζ_d is a primitive q^dth root of unity over Z_p, $1 = \zeta^{q^d} = \zeta^{p^{v_d}-1}$, so that $\gamma_q(d) = v_d$, and $\gamma_q(d) \mid \gamma_q(d+1)$, $d = 1, 2, \ldots$.

Define the sequence $\{\alpha_m\}$, $m = 1, 2, \ldots$, by $\alpha_1 = 1$, and if α_m is defined, α_{m+1} is the smallest positive integer such that $\gamma_q(\alpha_{m+1}) > \gamma_q(\alpha_m)$. Thus $\gamma_q(\alpha_1) < \gamma_q(\alpha_2) < \ldots$ and

$$\{\gamma_q(\alpha_i) \mid i \in N\} = \{\gamma_q(i) \mid i \in N\}.$$

If R is Z_p, P or Q_p, then $R(\zeta_d) = R(\zeta_{d+1}) \Leftrightarrow \gamma_q(d) = \gamma_q(d+1)$ so that we define the sequence $b_1, b_2, \ldots, b_n$ by

$$b_i = \sum_{j=\alpha_i}^{\alpha_{i+1}-1} a_j$$

where $a_r = 0$ if $r > n$ and $a_1, a_2, \ldots, a_n$ are as in $(*)$.

In terms of this notation, we can restate Corollary 1.3 as

COROLLARY 1.3'. *If $R = Z_p$, P or Q_p, then there exist non-negative integers $b_1, b_2, \ldots, b_n$ such that*

$$RG \simeq \sum_{i=1}^{n} b_i R(\zeta_{\alpha_i}^{i})$$

where ζ_{α_i} is a primitive q^{α_i}th root of unity.

We now show that the sequence $b_1, b_2, \ldots, b_n$ are invariants of RG.

If $m \in N$, and r is a non-negative integer, by the symbol rC_m we mean the direct sum of r copies of C_m. Let $s_1, s_2, \ldots, s_n$ be a sequences of non-negative integers such that $s_i \mid s_{i+1}$, $i=1, \ldots, n-1$. Suppose that A and B are finite abelian groups of the the same order and $A \simeq \sum_{i=1}^n r_i C_{p^{s_i}-1}$ $B \simeq \sum_{i=1}^n \bar{r}_i C_{p^{s_i}-1}$ where r_i, $\bar{r}_i$ are non-negative integers for $i=1, \ldots, n$. Since $(p^{s_i}-1) \mid (p^{s_{i+1}}-1)$, the fundamental theorem of abelian groups tells us that $A \simeq B$ if and only if $r_i = \bar{r}_i$, $i=1, \ldots, n$.

If S is a commutative ring with identity, let $S^* = \{\delta \in S \mid \delta$ is of finite multiplicative order$\}$.

THEOREM 1.4. *Let R be Z_p, P, or Q_p. If G and H are finite abelian groups of order q^n, then*

$$RG \simeq RH \Leftrightarrow (RG)^* \simeq (RH)^*.$$

Proof. Since adjoining ζ_{α_i} to Q_p gives a totally unramified extension of Q_p, $(Q_p(\zeta_{\alpha_i}))^* \simeq (Z_p(\zeta_{\alpha_i}))^* \simeq C_{p^{\gamma_q(\alpha_i)}-1}$. But any element of finite order in $Q_p(\zeta_{\alpha_i})$ is in fact in $P(\zeta_{\alpha_i})$ so that $(P(\zeta_{\alpha_i}))^* \simeq C_{p^{\gamma_q(\alpha_i)}-1}$.

By Corollary 1.3′, there exist non-negative integers $b_1, b_2, \ldots, b_n$ such that $RG \simeq \sum_{i=1}^n b_i R(\zeta_{\alpha_i})$. Thus $(RG)^* \simeq \sum_{i=1}^n b_i C_{p^{\gamma_q(\alpha_i)}-1}$. If $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n$ is another sequence of non-negative integers such that $RG \simeq \sum_{i=1}^n \bar{b}_i R(\zeta_{\alpha_i})$, $(RG)^* \simeq \sum \bar{b}_i C_{p^{\gamma_q(\alpha_i)}-1}$. By the fundamental theorem of abelian groups, we must have $\bar{b}_i = b_i$, $i=1, \ldots, n$. Thus the sequence $b_1, b_2, \ldots, b_n$ is determined by RG and in turn determines, via a one-one correspondence, the group $(RG)^*$. Therefore $RG \simeq RH \Leftrightarrow (RG)^* \simeq (RH)^*$.

COROLLARY 1.5. *Let R be Z_p, P or Q_p. If G is a finite abelian group of order q^n, and $RG \simeq \sum_{i=1}^n b_i R(\zeta_{\alpha_i})$, $RG \simeq \sum_{i=1}^n \bar{b}_i R(\zeta_{\alpha_i})$, where b_i, $\bar{b}_i$, $i=1, \ldots, n$, are non-negative integers then $b_i = \bar{b}_i$, $i=1, 2, \ldots, n$.*

COROLLARY 1.6. *Suppose G and H are finite abelian groups of order q^n. The following are equivalent.*

(i) $Z_pG \simeq Z_pH$, (ii) $PG \simeq PH$, (iii) $Q_pG \simeq Q_pH$.

Proof. Note that $(Z_pG)^* \simeq (PG)^* \simeq (Q_pG)^*$ and use Theorem 1.4

§2

If A is a finite abelian group of order $n = p^e q_1^{e_1} q_2^{e_2} \ldots q_r^{e_r}$, we let A_p be the p-Sylow subgroup of A and A_{q_i} the q_i-Sylow subgroup of A. Again we start from a result of Perlis-Walker.

PROPOSITION 2.1. *If A and B are finite abelian groups of order $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ where p_i, $i=1,\dots,r$, are distinct primes, and F is a field of characteristic k, where $k=0$ or $(k,n)=1$, then $FA\simeq FB \Leftrightarrow FA_{p_i}\simeq FB_{p_i}$, $i=1,\dots,r$.*

Proof. See [3] and [1].

PROPOSITION 2.2. *Let A and B be finite abelian groups of order p^n. Then $Q_pA\simeq Q_pB \Leftrightarrow A\simeq B$.*

Proof. By the result of Perlis-Walker (of the last section), $Q_pA\simeq\sum_{d=1}^{n} a_dQ_p(\zeta_d)$ where ζ_d is a primitive p^dth root of unity, $a_d=n_d/v_d$, n_d is the number of elements in A of order p^d, and $v_d=\text{degree}(Q_p(\zeta_d)/Q_p)$. Similarly, $Q_pB\simeq\sum_{d=1}^{n}\bar a_dQ_p(\zeta_d)$, where $\bar a_d=\bar n_d/v_d$, and $\bar n_d$ is the number of elements in B of order p^d. $Q_pA\simeq Q_pB$ implies

$$(Q_pA)^*\simeq\sum_{d=1}^{n} a_d(Q_p(\zeta_d))^*\simeq\sum_{d=1}^{n}\bar a_d(Q_p(\zeta_d))^*\simeq(Q_pB)^*.$$

Q_p contains only the $(p-1)$st roots of unity, and $Q_p(\zeta_d)$ is a totally ramified extension of Q_p, so that $(Q_p(\zeta_d))^*\simeq C_{p^d(p-1)}$. By the fundamental theorem of abelian groups we have $a_d=\bar a_d$, $d=1,\dots,n$, and so $n_d=\bar n_d$, $d=1,\dots,n$. Thus $A\simeq B$.

COROLLARY 2.3. *If A and B are finite abelian groups of order n, and Q is the field of rational numbers, then $QA\simeq QB\Leftrightarrow A\simeq B$.*

Proof. By Proposition 2.1, it is sufficient to suppose that $n=p^m$. If $QA\simeq QB$, then $QA\otimes Q_p\simeq QB\otimes Q_p$; i.e., $Q_pA\simeq Q_pB$. But by Proposition 2.2, $A\simeq B$.

COROLLARY 2.4. *If A and B are finite abelian groups of order p^n, then $PA\simeq PB\Leftrightarrow A\simeq B$.*

Proof. $PA\simeq PB$ implies $PA\otimes Q_p\simeq PB\otimes Q_p$. By Proposition 2.2 $A\simeq B$.

Note that if A and B are finite abelian groups of order p^n, then $Z_pA\simeq Z_pB\Leftrightarrow A\simeq B$. See [2], e.g.

THEOREM 2.5. *Suppose R is Z_p, P or Q_p. If G and H are finite abelian groups of order $n=p^eq_1^{e_1}\dots q_r^{e_r}$ where $p, q_1,\dots,q_r$ are distinct primes, then*

$$RG\simeq RH\Leftrightarrow RG_p\simeq RH_p \quad\text{and}\quad RG_{q_i}\simeq RH_{q_i} \qquad i=1,\dots,r.$$

Proof. If $R=Q_p$, the result follows immediately by Proposition 2.1.

Suppose $R=Z_p$, and $Z_pG\simeq Z_pH$. By the results in May [2], $G_p\simeq H_p$. Suppose $|G_p|=p^{c_1}$, $|H_p|=p^{c_2}$, and $c=\max(c_1,c_2)$. Let $(Z_pG)^{p^c}=\{\delta^{p^c}\mid\delta\in Z_pG\}$. $(Z_pG)^{p^c}\simeq(Z_pH)^{p^c}$. As $Z_p^p\simeq Z_p$, we have $(Z_pG)^{p^c}\simeq Z_p(G/G_p)\simeq(Z_pH)^{p^c}\simeq Z_p(H/H_p)$. By Proposition 2.1, $Z_p(G/G_p)\simeq Z_p(H/H_p)\Rightarrow Z_p(G_{q_i})\simeq Z_p(H_{q_i})$, $i=1,\dots,r$. Thus $Z_p(G)\simeq Z_p(H)\Rightarrow Z_pG_p\simeq Z_pH_p$ and $Z_p(G_{q_i})\simeq Z_p(H_{q_i})$, $i=1,\dots,r$. The opposite implication follows from the tensor product.

If $R=P$, and $PG\simeq PH$, we let $J=(p)$ be the ideal of P generated by p. The epimorphism $P\to P/J\simeq Z_p$, induces an isomorphism $Z_pG\simeq Z_pH$. By the previous case $Z_pG\simeq Z_pH\Rightarrow G_p\simeq H_p$ and $Z_pG_{q_i}\simeq Z_pH_{q_i}$, $i=1,\dots,r$. But by Corollary 1.6 $Z_pG_{q_i}\simeq Z_pH_{q_i}\Leftrightarrow PG_{q_i}\simeq PH_{q_i}$, so that $PG\simeq PH\Rightarrow PG_p=PH_p$ and $PG_{q_i}\simeq PH_{q_i}$, $i=1,\dots,r$. The opposite implication follows from the tensor product.

COROLLARY 2.6. *Let G and H be finite abelian groups of order n. The following are equivalent.*

(i) $Z_pG\simeq Z_pH$, (ii) $PG\simeq PH$, (iii) $Q_pG\simeq Q_pH$.

§3

In this section we investigate for which integers $m\in N$, is it true that two abelian groups G and H of order m have isomorphic p-adic group rings if and only if G and H are isomorphic. To study this question, it is sufficient, by Theorem 2.5, to again suppose that G and H are abelian groups of order q^n. We will use the notation of Section 1.

DEFINITION. We let $\mathscr{I}(q)=r$, if there is an $r\in N$ such that $\alpha_r=r$ and $\alpha_{r+1}\neq(r+1)$. Otherwise, we define $\mathscr{I}(q)=\infty$. We will call $\mathscr{I}(q)$, the index of q, (relative to p).

THEOREM 3.1. *Let R be Z_p, P or Q_p. Let $n\in N$.*
(i) *If $n<2\mathscr{I}(q)$, and G and H are abelian groups of order q^n, then*

$$RG\simeq RH\Leftrightarrow G\simeq H.$$

(ii) *If $n\geqslant 2\mathscr{I}(q)$, there exist non-isomorphic abelian groups G and H, of order q^n such that $RG\simeq RH$.*

Proof. (i) Suppose $G\simeq C_{q^{y_1}}\times C_{q^{y_2}}\times\cdots\times C_{q^{y_r}}$ and $H\simeq C_{q^{z_1}}\times C_{q^{z_2}}\times\cdots\times C_{q^{z_r}}$ where $y_1\geqslant y_2\geqslant\cdots\geqslant y_r\geqslant 0$, $z_1\geqslant z_2\geqslant\cdots\geqslant z_r\geqslant 0$ and $y_1+y_2+\cdots+y_r=z_1+z_2+\cdots+z_r=n$. By Corollary 1.3′, there exist non-negative integers $b_1, b_2,\dots, b_n$ and $\bar b_1, \bar b_2,\dots, \bar b_n$ such that $RG\simeq\sum_{i=1}^n b_iR(\zeta_{\alpha_i})$ and $RH\simeq\sum_{i=1}^n \bar b_iR(\zeta_{\alpha_i})$. By Corollary 1.5, $RG\simeq RH\Leftrightarrow b_i=\bar b_i$, $i=1,\dots,n$. We suppose $RG\simeq RH$. $b_i=n_i/\gamma_q(i)$ for $i=1,\dots,\mathscr{I}(q)-1$, where n_i denotes the number of elements of G of order q^i. Similarly, $\bar b_i=m_i/\gamma_q(i)$, where m_i denotes the number of elements of H of order q^i. Thus if $y_1<\mathscr{I}(q)$ or $z_1<\mathscr{I}(q)$ we must have $n_i=m_i$, $i=1,\dots,n$, and $G\simeq H$.

We will assume now $y_1\geqslant\mathscr{I}(q)$ and $z_1\geqslant\mathscr{I}(q)$.

Suppose $y_1>z_1\geqslant\mathscr{I}(q)$. Let $\bar G\simeq C_{q^{y_2}}\times C_{q^{y_3}}\times\cdots\times C_{q^{y_r}}$ and $\bar H\simeq C_{q^{z_2}}\times C_{q^{z_3}}\times\cdots\times C_{q^{z_r}}$. Then $G\simeq C_{q^{y_1}}\times\bar G$, $H\simeq C_{q^{z_1}}\times\bar H$, $|\bar H|>|\bar G|$, $|\bar G|\leqslant q^{n-\mathscr{I}(q)-1}\leqslant q^{\mathscr{I}(q)-2}$ and

$|\bar{H}| \leqslant q^{n-\mathscr{I}(q)} \leqslant q^{\mathscr{I}(q)-1}$

$$b_{\mathscr{I}(q)-1} = \frac{n_{\mathscr{I}(q)-1}}{\gamma_{q(\mathscr{I}(q)-1)}} = \bar{b}_{\mathscr{I}(q)-1} = \frac{m_{\mathscr{I}(q)-1}}{\gamma_{(q,\mathscr{I}(q)-1)}}.$$

Clearly, $n_{\mathscr{I}(q)-1} = \phi(q^{\mathscr{I}(q)-1})|\bar{G}|$ (ϕ = Euler "phi" functions) while $m_{\mathscr{I}(q)-1} \geqslant \phi(q^{\mathscr{I}(q)-1})|\bar{H}| > \phi(q^{\mathscr{I}(q)-1})|\bar{G}| = n_{\mathscr{I}(q)-1}$. This contradiction shows $y_1 = z_1$.

Finally, we assume $y_i = z_i$, $i = 1, \ldots, t$, $t \geqslant 1$, and $z_{t+1} < y_{t+1} < \mathscr{I}(q)$. Let

$$G' = C_{q^{y_1}} \times C_{q^{y_2}} \times \cdots \times C_{q^{y_r}}$$
$$G'' = C_{q^{y_{t+1}}} \times \cdots \times C_{q^{y_r}}$$
$$H'' = C_{q^{z_{t+1}}} \times \cdots \times C_{q^{z_r}}$$

then $G \simeq G' \times G''$, $H \simeq G' \times H''$ and $|G''| = |H''| < q^{\mathscr{I}(q)}$.

Let $\mu = y_{t+1}$. Then

$$b_\mu = \frac{n_\mu}{\gamma_{q(\mu)}} = \frac{m_\mu}{\gamma_{q(\mu)}} = \bar{b}_\mu.$$

If λ is the number of elements of G' of order q^μ, then $m_\mu = \lambda|H''|$. But $n_\mu \geqslant \lambda|G''| + |G'|\ (\phi(q^\mu)) > \lambda|G''| = m_\mu$. This is the desired contradiction, and we conclude $y_i = z_i$, $i = 1, \ldots, r$, and $G \mathrm{w} H$.

(ii) If $n = 2\mathscr{I}(q)$, let

$$G \simeq C_{q^{\mathscr{I}(q)}} \times C_{q^{\mathscr{I}(q)}}$$

and

$$H \simeq C_{q^{\mathscr{I}(q)+1}} \times C_{q^{\mathscr{I}(q)-1}}.$$

A straightforward verification shows that $b_i = \bar{b}_i$, $i = 1, \ldots, \mathscr{I}(q) - 1$ and $b_i = \bar{b}_i = 0$, $i > \mathscr{I}(q)$. Since $|G| = |H|$, we must have $b_{\mathscr{I}(q)} = \bar{b}_{\mathscr{I}(q)}$ and $RG \simeq RH$.

If $n > 2\mathscr{I}(q)$, we merely tack on a sufficient number of copies of C_q to each of the above examples.

REFERENCES

[1] Cohen, D. E., *On abelian group algebra*, Math. Z. *105* (1968), 267–268.
[2] May, W., *Commutative group algebras*, Trans. Am. Math. Soc. *136* (1969), 139–149.
[3] Perlis, S. and Walker, G., *Abelian group algebras of finite order*, Trans. Am. Math. Soc. *68* (1950), 420–426.
[4] Raggi Cárdenas, *Units in group rings with coefficients in K_{p^n}, Z_{p^n} and $\hat{Z}_p$*. (Spanish) An. Inst. Mat. Univ. Nac. Autonoma Mexico *10* (1970), 29–65.

École Polytechnique Fédérale – Lausanne
The University of Connecticut
Storrs, Connecticut, 06268, U.S.A.

Received March 9, 1974