JOURNAL OF ALGEBRA 144, 88–93 (1991)

Incomplete j-Diagrams Fail to Capture Group Structure

M. A. DE LUIS

3 Lichen Green, Cannon Park, Coventry CV4 7DH, England

Communicated by Walter Feit

Received November 13, 1989

In this note we show, by counterexamples, that various results in two papers of Ayoub (On diagrams for abelian groups, *J. Number Theory* **2** (1970), 442–458; On the group of units of certain rings, *J. Number Theory* **4** (1972), 383–403) fail. In essence, if A is a bounded p-group, an incomplete j-diagram for A will not, in general, suffice to determine the structure of A. © 1991 Academic Press, Inc.

One of the major results in Ayoub [1] is Theorem 4 (p. 456). This, in essence, states that if an abelian group A admits an incomplete j-diagram (see Definition 2), then A is a bounded p-group and its structure is determined by the said diagram. In this note we show that the latter assertion is false, for essentially identical (incomplete) j-diagrams can be defined on non-isomorphic finite abelian p-groups. As a consequence of this, Corollary [1, p. 458] fails. Furthermore, this error propagated to Theorem 3 of [2, p. 402], in that the one-groups of Ayoub's exceptional rings [2, Definition 1, p. 397] do not necessarily have the structure dictated by this theorem. Surprisingly, these errors appear to have been unnoticed for over 18 years, ever since the time of publication of [1] and [2].

Let R be a finite commutative ring with $1 \neq 0$. We recall that R is said to be a chain ring iff the lattice of ideals of R is a chain. Chain rings are the same thing as local principal ideal rings [3, Theorem 1.1]. We use the following notation regarding such rings:

(i) M is the maximal ideal of R, i.e., the unique maximal ideal of R.

(ii) K is the residue field of R; i.e., $K = R/M$.

(iii) R^* is the group of units of R; it should be clear that $R^* = R \backslash M$

(iv) Ring parameters:

$p^d = |K|$, p a prime, d is called the residual degree of R;
e is the nilpotency index of M;
r is the ramification index of R, i.e., $p1_R \in M^r \backslash M^{r+1}$ (R is assumed not to have prime char).

0021-8693/91 $3.00

With regard to the ramification index, we note that if we choose a generator π for M, then $p1_R = \varepsilon\pi^r$ ($\varepsilon \in R^*$). The subgroup $1+M$ of R^* is called the one-group of R. The cardinality of the powers of the maximal ideal M is given by $|M^s| = |K|^{e-s}$, $0 \leqslant s \leqslant e$, where M^0 is, by convention, R [3, Lemma 1.2].

We recall Ayoub's definitions of admissible function [1, p. 445] and incomplete j-diagram [1, pp. 449–450].

DEFINITION 1. Let n be a positive integer, j: $\{1, 2, ..., n\} \to \{1, 2, ..., n\}$ is said to be admisible iff (1) $s < j(s)$, for $1 \leqslant s < n$; $j(n) = n$, (2) $j(s) = j(s') < n \Rightarrow s = s'$.

DEFINITION 2. Let A be an abelian group. The series $A = A_1 \supset A_2 \supset \cdots \supset A_n = \{1\}$ is said to be an incomplete j-diagram at $s = u$ (with respect to the prime p) for A iff (a) j is an admissible function from $\{1, 2, ..., n\}$ to $\{1, 2, ..., n\}$. (b) $j(s) = n \Rightarrow A_s^p = \{1\}$. (c) For $j(s) < n$, the prescriptions

$$\gamma_s\colon A_s/A_{s+1} \to A_{j(s)}/A_{j(s)+1}$$
$$xA_{s+1} \mapsto x^p A_{j(s)+1}$$

define maps, such that γ_s is an isomorphism for $s \neq u$, and γ_u is a homomorphism.

An Incomplete j-Diagram. Let R be a finite commutative chain ring, with parameters $p = 2$, $d = 1$, $r = 2$, $e = 6$. Note that these parameter values force $R^* = 1 + M$ ($1 + M \subseteq R^*$, and $|M^s| = |K|^{e-s}$; hence $|R^*| = |R| - |M| = |K|^e - |K|^{e-1} = 64 - 32 = 32 = |M| = |1 + M|$). We shall specify an incomplete j-diagram, in fact a special case of the j-diagram in Theorem 2 of [2, p. 401].

Take the series $H_s = 1 + M^s$, $1 \leqslant s \leqslant 6$. Define j: $\{1, 2, ..., 6\} \to \{1, 2, ..., 6\}$ by

$$j(s) = \begin{cases} \min(2s, 6), & 1 \leqslant s \leqslant 2, \\ \min(2 + s, 6), & 2 \leqslant s \leqslant 6. \end{cases}$$

We can depict j as

$$j \quad \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 5 & 6 & 6 & 6. \end{array} \tag{1}$$

Theorem 2 of [2, p. 401] tells us that the series (H_s) is an incomplete j-diagram. However, we shall check this directly. Condition (a) of

Definition 2 is clear, on inspection of (1). For condition (b), note that if we fix a generator π for M: $x \in H_s \Leftrightarrow x = 1 + \alpha\pi^s$ ($\alpha \in R^*$). Then,

$$(1 + \alpha\pi^s)^2 = 1 + 2\alpha\pi^s + \alpha^2\pi^{2s} = 1 + \varepsilon\alpha\pi^{2+s} + \alpha^2\pi^{2s},$$

where $2 = \varepsilon\pi^2$ ($\varepsilon \in R^*$). As the nilpotency index of π is 6, it is clear that for $s \geqslant 4$ (i.e., $j(s) = 6$; see (1)), $(1 + \alpha\pi^s)^2 = 1$. A simple check gives that $x \in H_s \Rightarrow x^2 \in H_{j(s)}$ and $x \in H_{s+1} \Rightarrow x^2 \in H_{j(s)+1}$, for $1 \leqslant s \leqslant 3$ (i.e., for $j(s) < 6$). Therefore the prescriptions in Definition 2(c) do define maps. It then follows immediately that they are homomorphisms.

Finally, we claim that γ_1, γ_3 are onto, whereas γ_2 is trivial. Note that the factor groups H_s/H_{s+1} are cyclic with order 2. This follows from the formula $|M^s| = |K|^{e-s}$,

$$|H_s/H_{s+1}| = \frac{|H_s|}{|H_{s+1}|} = \frac{|1 + M^s|}{|1 + M^{s+1}|} = \frac{|M^s|}{|M^{s+1}|} = \frac{|K|^{e-s}}{|K|^{e-s-1}} = |K| = p^d = 2. \tag{2}$$

Thus $H_s/H_{s+1} = \{H_{s+1}, H_s \backslash H_{s+1}\}$. Now to obtain the image under γ_s of the coset $H_s \backslash H_{s+1}$, note that $x \in H_s \backslash H_{s+1} \Leftrightarrow x = 1 + \alpha\pi^s$ ($\alpha \in R^*$). In particular, $1 + \pi^s$ is a representative for the coset $H_s \backslash H_{s+1}$. As π is a generator for M, the definition of ramification index gives $21_R = \varepsilon\pi^2$ ($\varepsilon \in R^*$). Hence

$$\begin{aligned}
(1 + \pi)^2 &= 1 + 2\pi + \pi^2 = 1 + \varepsilon\pi^3 + \pi^2 = 1 + \pi^2(\varepsilon\pi + 1) \in H_2 \backslash H_3, \\
(1 + \pi^2)^2 &= 1 + 2\pi^2 + \pi^4 = 1 + \varepsilon\pi^4 + \pi^4 = 1 + \pi^4(\varepsilon + 1), \\
(1 + \pi^3)^2 &= 1 + 2\pi^3 + \pi^6 = 1 + \varepsilon\pi^5 + \pi^6 = 1 + \pi^5(\varepsilon + \pi) \in H_5 \backslash H_6.
\end{aligned} \tag{3}$$

From the first and last of these γ_1 and γ_3 are isomorphisms. Now note that as $R^* = 1 + M$, if $\alpha_1, \alpha_2 \in R^*$, then $\alpha_1 - \alpha_2 \in M$. But $\alpha_1 + \alpha_2 = \alpha_1 - (-\alpha_2)$; and as $-\alpha_2 \in R^*$, $\alpha_1 + \alpha_2 \in M$. Hence $1 + \varepsilon \in M$, and thus by (3), γ_2 is trivial. In conclusion, the series

$$R^* = 1 + M \supset 1 + M^2 \supset \cdots \supset 1 + M^6 = \{1\}$$

is an incomplete j-diagram at $s = 2$ (with respect to the prime 2) for R^*.

Theorem 4 of [1, p. 456] tells us how to retrieve the structure of R^* from the above j-diagram. We observe that H_s/H_{s+1} and $\mathrm{Ker}(\gamma_2)$, as $\mathbb{Z}_2$-vector spaces, are 1-dimensional, since $|H_s/H_{s+1}| = 2$ (by (2)) and γ_2 is trivial. As the various other parameters in the statement of Theorem 4 of [1] are readily computed, on inspection of (1), it follows that if R is a finite commutative chain ring with parameter values $p=2$, $d=1$, $r=2$, $e=6$; then

$$R^* \cong C_4 \otimes C_2 \otimes C_4 \tag{4}$$

(where C_n denotes a cyclic group of order n).

However, we shall construct two such rings R_1, R_2, of which R_2^* is as in (4), whereas R_1^* is not.

We need the following elementary observation.

LEMMA 1. *Let D be a finite residue principal ideal domain, q a prime such that $q1_D = \pi^t\alpha$ (π an irreducible; α, π coprime), n a positive integer. Then $R = D/(\pi^n)$ is a finite commutative chain ring; and if $n > t$, the ring parameters of R are $p = q$, $p^d = |D/(\pi)|$, $r = t$, $e = n$.*

Remark. The condition $n > t$ is due to our usage of the term "ramification index," which requires the ring not to have prime char.

Proof. Easy check. ∎

The Counterexamples. Choose the quadratic number fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$. Their rings of integers are $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, respectively, and these are principal ideal domains [4, Theorem 4.2, p. 60, Theorem 4.20, p. 45]. It is clear that $\sqrt{2}$ is an irreducible in $\mathbb{Z}[\sqrt{2}]$ and $1+\sqrt{3}$ in $\mathbb{Z}[\sqrt{3}]$, because their norms are prime ($N(\sqrt{2}) = -2$, $N(1+\sqrt{3}) = (1+\sqrt{3})(1-\sqrt{3}) = -2$). Also, $2 = (\sqrt{2})^2$ and $2 = (2-\sqrt{3})(1+\sqrt{3})^2$, with $2-\sqrt{3}$ a unit in $\mathbb{Z}[\sqrt{3}]$; for $N(2-\sqrt{3}) = (2-\sqrt{3})(2+\sqrt{3}) = 1$. Finally, the size of the fields $\mathbb{Z}[\sqrt{2}]/(\sqrt{2})$ and $\mathbb{Z}[\sqrt{3}]/(1+\sqrt{3})$ is clearly 2, i.e., the absolute value of the norms of $\sqrt{2}$ and $1+\sqrt{3}$ [4, Corollary 5.9, p. 121].

Let $R_1 = \mathbb{Z}[\sqrt{2}]/((\sqrt{2})^6) = \mathbb{Z}[\sqrt{2}]/(8)$ and $R_2 = \mathbb{Z}[\sqrt{3}]/((1+\sqrt{3})^6) = \mathbb{Z}[\sqrt{3}]/(8)$. Lemma 1 gives that both these rings are finite commutative chain rings with parameter values $p=2$, $d=1$, $r=2$, $e=6$, i.e., as in the construction of the above j-diagram.

We shall determine the structure of R_i^* ($i=1,2$), by specifying a basis in each case. Recall that for a finite chain ring R, $|R^*| = |R| - |M| = |K|^e - |K|^{e-1}$ ($|K| = p^d$); thus our groups R_i^* ($i=1,2$) both have order 32. The following elementary fact is useful for order computations in R_i^* ($i=1,2$). Let d be a square-free rational integer, $m \in \mathbb{Z}$. Then in $\mathbb{Z}[\sqrt{d}]$,

$$a + b\sqrt{d} \equiv a' + b'\sqrt{d} \pmod m \quad \text{iff} \quad a \equiv a' \pmod m \quad \text{and} \quad b \equiv b' \pmod m. \tag{5}$$

In the determination of the group structures below, if G is a group and $g \in G$, then $o(g)$ denotes the order of g and $\langle g \rangle$ the subgroup generated by g.

The Structure of R_1^*. Choose $[-1]$, $[5]$, $[1+\sqrt{2}]$, where the square brackets mean class mod 8 in $\mathbb{Z}[\sqrt{2}]$. It is clear that $o([-1]) = o([5]) = 2$, i.e., as in $\mathbb{Z}_8$. Squaring successively $1+\sqrt{2}$ and using (5) for mod 8 reduction, we obtain $o([1+\sqrt{2}]) = 8$. Also, the element of order 2 in $\langle [1+\sqrt{2}] \rangle$ is $[1+4\sqrt{2}]$. We assert that $R_1^* = \langle [-1] \rangle \oplus \langle [5] \rangle \oplus \langle [1+\sqrt{2}] \rangle$. Note that $\langle [-1] \rangle \cap \langle [5] \rangle = \{[1]\}$, because $-1 \not\equiv 5 \pmod 8$ and both subgroups have order 2. Next, any element in $\langle [-1] \rangle \langle [5] \rangle$ has a rational integer representative, whereas for no $m \in \mathbb{Z}$ is $m \equiv 1 + 4\sqrt{2} \pmod 8$. Then the product $\langle [-1] \rangle \langle [5] \rangle \langle [1+\sqrt{2}] \rangle$ is direct; hence $|\langle [-1] \rangle \langle [5] \rangle \langle [1+\sqrt{2}] \rangle| = 2 \cdot 2 \cdot 8 = 32$, i.e., the order of R_1^*. Therefore $R_1^* \cong C_2 \otimes C_2 \otimes C_8$, contradicting (4).

It is then clear that Theorem 4 of [1, p. 456] fails.

The Structure of R_2^*. Choose $[-1]$, $[1+2\sqrt{3}]$, $[2+\sqrt{3}]$, where the square brackets mean class mod 8 in $\mathbb{Z}[\sqrt{3}]$. Computations similar to those for R_1^* above yield $o([1+2\sqrt{3}] = o([2+\sqrt{3}]) = 4$. The elements of order 2 in $\langle [1+2\sqrt{3}] \rangle$ and $\langle [2+\sqrt{3}] \rangle$ are respectively $[5+4\sqrt{3}]$, $[7+4\sqrt{3}]$. As these are different (by (5)), it follows that $\langle [1+2\sqrt{3}] \rangle \cap \langle [2+\sqrt{3}] \rangle = \{[1]\}$. Furthermore $\langle [-1] \rangle \cap \langle [1+2\sqrt{3}] \rangle \langle 2+\sqrt{3}] \rangle = \{[1]\}$, because

$$-1 \not\equiv 5 + 4\sqrt{3} \pmod 8, \qquad -1 \not\equiv 7 + 4\sqrt{3} \pmod 8,$$
$$-1 \not\equiv (5+4\sqrt{3})(7+4\sqrt{3}) \pmod 8.$$

The first two are obvious (by (5)). As to the third, note that $5+4\sqrt{3}$ is self-inverse mod 8; hence it reduces to $-5-4\sqrt{3} \not\equiv 7+4\sqrt{3} \pmod 8$, which is obviously true. Consequently, the product $\langle [-1] \rangle \langle 1+2\sqrt{3}] \rangle \langle [2+\sqrt{3}] \rangle$ is direct and thus $|\langle [-1] \rangle \langle [1+2\sqrt{3}] \rangle \langle [2+\sqrt{3}] \rangle| = 2 \cdot 4 \cdot 4 = 32$, i.e., the order of R_2^*. Therefore, $R_2^* \cong C_2 \otimes C_4 \otimes C_4$, which agrees with (4).

Although R_2^* has the structure demanded by Theorem 4 of [1, p. 456], when taken together with R_1^*, they contradict the Corollary to Theorem 4 in [1, p. 458].

Finally, as R_1 is a commutative chain 2-ring and the nilpotency index of its maximal ideal is 6, it is clear that it satisfies the definition of exceptional ring in [2, Definition 1, p. 397]. A simple application of Theorem 3 of [2, p. 402] gives that $R_1^* \cong C_4 \otimes C_2 \otimes C_4$, which as we have seen earlier is not the case. Thus, the said theorem fails to give the correct structure for the one-group of Ayoub's exceptional rings (recall that the parameter values of R_1 force $R_1^* = 1 + M$).

Remark. There are numerous, in fact infinitely many, counterexamples similar to those just given. The crucial thing is to select quadratic number fields $\mathbb{Q}(\sqrt{d_i})$ $(i = 1, 2)$ with a ring of integers D_i such that $\langle 2 \rangle = P_i^2$ (where $\langle 2 \rangle$ denotes the ideal generated by 2 and P_i a prime ideal of D_i). In addition, the d_i's have to be chosen appropriately.

In conclusion, contrary to Ayoub's assertion, in the introduction to [1], the structure of the unit group of D/P^n (where D is the ring of integers of some number field and P a prime ideal of D) cannot be read off from the theorems in that paper.

References

1. C. W. Ayoub, On diagrams for abelian groups, *J. Number Theory* **2** (1970), 442–458.
2. C. W. Ayoub, On the group of units of certain rings, *J. Number Theory* **4** (1972), 383–403.
3. A. A. Nečaev, Finite rings of principal ideals, *Mat. Sb.* **91**, No. 3 (1973), 350–366 [*Math. USSR* **20** (1973), 364–382].
4. I. N. Stewart and D. O. Tall, "Algebraic Number Theory," Chapman & Hall, London, 1979.