Annales Mathematicae Silesianae 12 (1998), 23–29

Prace Naukowe Uniwersytetu Śląskiego nr 1751, Katowice

ON REDUCED RINGS AND NUMBER THEORY

JAN KREMPA

Abstract. In this note we exhibit a connection between theory of associative rings and number theory by an example of necessary and sufficient conditions under which the integral group ring of a finite group is reduced.

1. Reduced rings

In this note we will use rather standard notation and terminology for rings, groups and numbers, similar to those in quoted books. In particular, if R is a ring (associative with $1 \neq 0$), then $U(R)$ denotes the group of invertible elements (units) of the ring R, $H(R)$ – the standard quaternion algebra over R, and RG – the group ring of a group G with coefficients in R. Recall that a ring R is *reduced* if it has no nontrivial nilpotent elements. Such rings have many interesting properties. Some of them are consequences of the following celebrated result of Andrunakievič and Rjabukhin (see [Row, Kr96]).

THEOREM 1.1. *For a ring R the following conditions are equivalent:*

(1) *R is reduced.*
(2) *R is semiprime and R/P is a domain for any minimal prime ideal P of R.*
(3) *R is a subdirect product of domains.*

Received on July 8, 1998.
1991 *Mathematics Subject Classification.* 11A15, 11E25, 16S34.
Key words and phrases: Reduced ring, level of a field, prime numbers.
Partially supported by the State Committee for Scientific Research (KBN) of Poland.

Another reason to consider reduced rings, in particular reduced group rings, is connected with investigation of groups of units (see [Sehg, Kr95a]). An interesting example in this direction is provided by a new result in [MS].

THEOREM 1.2. [Marciniak and Sehgal, 1998]
Let R be a commutative domain of characteristic 0 and let G be a group. If $U(RG)$ contains no nontrivial free subgroup, then RG has to be reduced.

Using elementary properties of group rings and their bicyclic units (see [Sehg]) one can easily obtain the following reduction result for being reduced.

PROPOSITION 1.3. *Let R be a ring, G a group and H the subgroup of G generated by all elements of finite order. If RG is reduced then:*

(1) *R is reduced;*
(2) *H is a periodic subgroup of G and every its subgroup is normal in G;*
(3) *G/H is torsion free.*

If one is going to describe all reduced group rings then, by the above Proposition, it is convenient to consider the case of torsion free groups, and independently the case of periodic groups. The first case is connected with a famous conjecture of Kaplansky and, even over fields, is only partially solved (see [Sehg, Kr95a]). The second case is just connected with our considerations. As an immediate consequence of Proposition 1.3 we have

COROLLARY 1.4. *Let R be a ring and G be a periodic group such that the ring RG is reduced. Then any subgroup of G is normal, hence G is either abelian or a hamiltonian group.*

By a classical result of Dedekind and Baer (see [Rob]) we know that any hamiltonian group, say G, is of the form:

$$G \cong Q_8 \times A \times E,$$

where Q_8 is the quaternion group of order 8, E is an elementary abelian 2-group, and A is an abelian group with all elements of odd order. In particular G is locally finite. Hence, by the above corollary, we can replace in our considerations periodic groups by finite groups. For integral group rings we have the following decisive result.

THEOREM 1.5. [Pascaud 1973, Sehgal 1975]
Let G be a group of order $2^k \cdot n$, where n is odd. Then the integral group ring $\mathbb{Z}G$ is reduced if and only if either G is abelian, or G is hamiltonian and 2 has an odd order in $U(\mathbb{Z}_n)$.

Complete proof of this result can be found in [Sehg]. Here we are going to sketch a modified version of it. As a very special case of Connell's theorem, (see [Sehg]), or by direct arguments, we have

LEMMA 1.6. *If G is an abelian group, not necessarily finite, and R is any domain of characteristic 0, then the ring RG is reduced.*

In this way, for integral group rings, we are left with the case of nonabelian groups. This case is usually considered with the help of number theory. It is possible because of Chinese Reminder Theorem for rings, which leads to the following observation.

LEMMA 1.7. *Let $G = Q_8 \times F$, where F is a finite abelian group of exponent n. Then:*

$$\mathbb{Z}G \subseteq H(\mathbb{Z}[\zeta_n]) \oplus R_1 \oplus \cdots \oplus R_k,$$

where all R_i's are isomorphic to subrings of $H(\mathbb{Z}[\zeta_n])$, and

$$\mathbb{Q}G \cong H(\mathbb{Q}(\zeta_n)) \oplus A_1 \oplus \cdots \oplus A_k,$$

where all A_i's are isomorphic to $\mathbb{Q}-$subalgebras of $H(\mathbb{Q}(\zeta_n))$.
In particular $\mathbb{Z}G$ is reduced if and only if $H(\mathbb{Q}(\zeta_n))$ is reduced.

Sketch of proof. We have a canonical isomorphism

$$\mathbb{Q}G \cong (\mathbb{Q}F)Q_8.$$

From the Chinese Reminder Theorem, the assumption on F, and induction on its order (starting with $|F| = n$) we can prove that

$$\mathbb{Q}F \cong K_1 \oplus \cdots \oplus K_l,$$

where $l \geqslant 1$, all K_i's are subfields of the field $\mathbb{Q}(\zeta_n)$, and at least one of them is equal to $\mathbb{Q}(\zeta_n)$. For any field K of characteristic 0 and for the quaternion group we have

$$KQ_8 \cong H(K) \oplus K \oplus K \oplus K \oplus K.$$

From the above arguments the required decomposition of $\mathbb{Q}(G)$ follows. The case of decomposing $\mathbb{Z}(G)$ is similar, but we obtain only inclusion instead of isomorphism (comp. [Kr95b]).

2. Level of number fields

By Lemma 1.7 instead of studying all integral group rings we need consider only quaternion algebras over cyclotomic fields. For this, if K is a field then, as usual, (see [Lam, N, Sz]), let $s(K)$ be the level (stufe) of K, i.e.

$$s(K) = \begin{cases} m & \text{if } m = \inf_{n\in\mathbb{N}} \sum_{i=1}^{n} x_i^2 = -1, \text{where} \quad x_i \in K, \\ \infty & \text{if such } m \text{ does not exist.} \end{cases}$$

Due to Pfister (see [Lam, N, Sz]) we know that, if $s(K) < \infty$ then $s(K) = 2^m$ for some $m \geqslant 0$. Moreover, for any $m \geqslant 0$ there exists a field K_m such that $s(K_m) = 2^m$.

Many results about level of concrete fields related to number theory one can find for example in [Lam, Sz, KS, N]. The following one, rather nontrivial, is due to Hilbert and Hasse.

THEOREM 2.1. *Let K be a finite extension of $\mathbb{Q}$. Then*

(1) $s(K) = 1, 2, 4$ *or* ∞.
(2) $s(K) = \infty$ *if and only if K has an embedding into the field $\mathbb{R}$.*
(3) *If $s(K) < \infty$, then $s(K) = 4$ if and only if there exists a prime ideal P of the integers of K such that $2 \in P$ and $s(K_P) = 4$, where K_P denotes the P-adic completion of K.*

The level function is useful for our consideration because of the following observation (see [Lam, Sz]).

PROPOSITION 2.2. *Let K be a field. Then $H(K)$ is reduced if and only if $s(K) \geqslant 4$.*

For another connection of level with extensions of 2-adic fields see for example [KS, Lam]. Investigation of level values for cyclotomic fields was stimulated rather by Pfister's result mentioned above, than by properties of quaternion algebras. As an immediate consequence of the above theorem we have

COROLLARY 2.3. *Let* $n \geqslant 3$. *Then:*

(1) $s(\mathbb{Q}(\zeta_n)) = 1, 2,$ *or* 4.
(2) $s(\mathbb{Q}(\zeta_n)) = 1$ *if and only if* $4 \mid n$.
(3) $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ *for any odd* n.
Hence in this case $s(\mathbb{Q}(\zeta_n)) = s(\mathbb{Q}(\zeta_{2n}))$.

From less obvious results of [C] and [CC], extended in [Mo] we have for cyclotomic fields

THEOREM 2.4. [Moser, 1973]
Let $n \geqslant 3$ *be an odd number. Then* $s(\mathbb{Q}(\zeta_n)) = 4$ *if and only if* 2 *has an odd order in the group* $U(\mathbb{Z}_n)$.

3. A contribution of Wacław Sierpiński

Now we will show that the condition from the theorem of Moser was in fact successfully discussed much earlier. For this purpose let $\mathcal{P}$ denote the set of all odd natural primes. Over 40 years ago Wacław Sierpiński distinguished the following subsets of the set $\mathcal{P}$:

- $\mathcal{P}_1 = \{p \in \mathcal{P};\ p \mid 2^r + 1 \text{ for some } r \geqslant 1\}$,
- $\mathcal{P}_{-1} = \{p \in \mathcal{P};\ p \mid 2^{2r+1} - 1 \text{ for some } r \geqslant 1\}$.

Possibly, the reason for him to introduce such classes was to extend the Fermat and the Mersenne prime numbers (see [Si87]). Sierpiński himself (see [Si58]) proved several properties of these sets. We summarize his, and further results obtained by Mąkowski (see [Si58]), Aigner ([Aig]), and Brauer ([Brau]) in the following two theorems:

THEOREM 3.1.

(1) $\mathcal{P}_1 \cup \mathcal{P}_{-1} = \mathcal{P}$ *and* $\mathcal{P}_1 \cap \mathcal{P}_{-1} = \emptyset$.
(2) *If* $p \equiv \pm 3 \pmod 8$, *then* $p \in \mathcal{P}_1$.
(3) *If* $p \equiv 7 \pmod 8$, *then* $p \in \mathcal{P}_{-1}$.
(4) *There exist infinitely many primes* $p \in \mathcal{P}_1$ *such that* $p \equiv 1 \pmod 8$.
(5) *There exist infinitely many primes* $p \in \mathcal{P}_{-1}$ *such that* $p \equiv 1 \pmod 8$.

THEOREM 3.2. *Let* $p \in \mathcal{P}$. *Then* $p \in \mathcal{P}_1$ *if and only if* 2 *has an even order as an element of* $U(\mathbb{Z}_p)$. *Hence* $p \in \mathcal{P}_{-1}$ *if and only if* 2 *has an odd order as an element of* $U(\mathbb{Z}_p)$.

The classes $\mathcal{P}_1$ and $\mathcal{P}_{-1}$ were studied later for example by Hasse and Odoni, but results about these classes were not used in [C, CC, Mo].

As an immediate consequence of facts quoted earlier in this paper and elementary calculation in residue rings we obtain

THEOREM 3.3. *Let $n \in \mathbb{N}, n \geqslant 3$ be an odd number. Then $s(\mathbb{Q}(\zeta_n)) = 4$ if and only if for any prime divisor p of n we have $p \in \mathcal{P}_{-1}$.*
Hence, if G is a nonabelian group of order $2^k \cdot n$, then the integral group ring $\mathbb{Z}G$ is reduced if and only if G is a hamiltonian group and $p \in \mathcal{P}_{-1}$ for any prime p dividing n.

Acknowledgment. I should like to express my gratitude to A. Schinzel and A. Mąkowski for valuable remarks and very helpful conversation about the subject of this note.

REFERENCES

[Aig] A. AIGNER, *Bemerkung und Lösung zum Problem Nr. 29*, Elemente der Mathematik, **15** (1960), 66–67.

[Brau] A. BRAUER, *A note on a number theoretical paper of Sierpiński*, Proc. Amer. Math. Soc., **11** (1960), 406–409.

[C] P. CHOWLA, *On the representation of -1 as sum of squares in a cyclotomic field*, J. Number Theory, **1** (1969), 208–210.

[CC] P. CHOWLA AND S. CHOWLA, *Determination of the stufe of certain cyclotomic fields*, J. Number Theory, **2** (1970), 271–272.

[Kr95a] J. KREMPA, *On finite generation of unit group for group rings*, Groups '93 Galway/St Andrews, vol. 2, London Math. Soc. Lecture Note 212, Cambridge University Press, Cambridge (1995), 352–367.

[Kr95b] J. KREMPA, *Rings with periodic unit groups*, Abelian groups and modules, A. Facchini and C. Menini, Kluwer Academic Publishers, Dordrecht (1995), 313–321.

[Kr96] J. KREMPA, *Some examples of reduced rings*, Algebra Colloqium, **3** (1996), 289–300.

[KS] R. KUČERA, K. SZYMICZEK, *Witt equivalence of cyclotomic fields*, Math. Slovaca, **42** (1992), 663–676.

[Lam] T. Y. LAM, *The algebraic theory of quadratic forms*, W. A. Benjamin Inc., Reading Massachusetts (1973).

[MS] Z. S. MARCINIAK AND S. K. SEHGAL, *Units in group rings and geometry*, Methods in Ring Theory, V. Drensky, A. Giambrouno and S. K. Sehgal, Marcel Dekker Inc., New York (1998), 185–198.

[Mo] C. MOSER, *Representation de -1 comme somme de carres dans un corps cyclotomique quelconque*, J. Number Theory, **5** (1973), 139–141.

[N] W. NARKIEWICZ, *Elementary and analytic theory of algebraic numbers*, Second ed., PWN and Springer-Verlag, Warszawa–Berlin–Heidelberg–New York (1990).

[Rob] D. J. S. ROBINSON, *A course in the theory of groups*, 2nd, extended edition, Springer-Verlag, Berlin (1996).

[Row] L. H. ROWEN, *Ring theory*, vol. I, Academic Press, New York (1988).

[Sehg] S. K. SEHGAL, *Topics in group rings*, Marcel Dekker Inc., New York (1978).

[Si58] W. SIERPIŃSKI, *Sur une décomposition des nombres premiers en deux classes*, Colloq. Math., **10** (1958), 81–83.

[Si87] W. SIERPIŃSKI, *Elementary theory of numbers*, 2nd edition, revised by A. Schinzel, PWN, Warszawa (1987).

[Sz] K. SZYMICZEK, *Bilinear algebra. An introduction to the algebraic theory of quadratic forms*, Algebra, Logic and Applications Series Volume 7, Gordon and Breach Science Publishers, Amsterdam (1997).

INSTITUTE OF MATHEMATICS
WARSAW UNIVERSITY
BANACHA 2
02-097 WARSZAWA
POLAND

e-mail:
jkrempa@mimuw.edu.pl