Acta Universitatis Carolinae. Mathematica et Physica

Tomáš Kepka; Petr Němec

Commutative radical rings. I.

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 48 (2007), No. 1, 11--41

Persistent URL: http://dml.cz/dmlcz/142760

2007 ACTA UNIVERSITATIS CAROLINAE – MATHEMATICA ET PHYSICA VOL. 48, NO. 1

Commutative Radical Rings I

TOMÁŠ KEPKA AND PETR NĚMEC

Praha

Received 2. October 2006

In this paper, basic properties and examples of commutative radical rings (i.e., rings equal to their Jacobson radical) are collected. Among other results, a construction of free radical rings is presented.

0. Introduction and notations

This paper is the first part of a comprehensive treatment concerning commutative radical rings, i.e., rings (generally without unit) which arise as Jacobson radical of some (unitary) ring. Radical rings are closely related to so called adjoint groups. Let R be as associative ring and define $x \circ y = x + y + xy$ for all $x, y \in R$. Under this operation, R forms a monoid (with neutral element 0) which is called the *adjoint semigroup* of the ring R. Then $R(\circ)$ is a group (called the *adjoint group* of R) if and only if $R = \mathcal{J}(R)$, where $\mathcal{J}(R)$ denotes the Jacobson radical of the ring R. (Adjoint semigroups are also defined via $x * y = x + y - xy$, however the semigroups $R(\circ)$ and $R(*)$ are clearly isomorphic, since $(-x) * (-y) = - (x \circ y)$ for all $x, y \in R$.)

Department of Algebra, MFF UK, Sokolovská 83, 186 75 Praha 8, Czech Republic

Department of Mathematics, ČZU, Kamýcká 129, 165 21 Praha 6–Suchdol, Czech Republic

2000 *Mathematics Subject Classification.* 13A10.

Key words and phrases. Commutative ring, Dorroh extension, Jacobson radical, Hilbert ring, radical ring.

The work is a part of the research project MSM 0021620839 financed by MŠMT and partly supported by the Grant Agency of the Czech Republic, grant #201/03/0937 (the first author) and #201/05/0002 (the second author).

E-mail: kepka@karlin.mff.cuni.cz

E-mail: nemec@tf.czu.cz

The first (at least implicit) appearance of the adjoint semigroup seems to be in [10] (see the introduction to [9]). As mentioned in [9], radical rings (and their adjoint groups) have been intensively studied along three main lines:
(1) implications of ring theoretic conditions on the adjoint group;
(2) implications of group theoretic conditions (imposed on the adjoint group) on the ring;
(3) implications of mixed conditions (group and ring theoretic) on the ring and its adjoint group.
Another important line of investigations is to seek for relations between the adjoint group $R(\circ)$ and the additive group $R(+)$ of a radical ring R. The class of radical rings is rather extensive, it contains e.g. all nil-rings. Some pieces of information on (commutative) radical rings and their adjoint groups can be seen e.g. in [1], [2], [3], [4], [5], [6], [8], [9], [10], [11], [12], [14], [15].

As radical rings can never have a unit element, it is often useful to consider a ring R as an ideal in the unitary ring $\mathbb{D}(R) = \mathbb{Z} \times R$, where $\mathbb{Z}$ is the ring of integers, the addition is defined componentwise and $(m,x)(n,y) = (mn, nx + my + xy)$ for all $m,n \in \mathbb{Z}$ and $x,y \in R$. The ring $\mathbb{D}(R)$ is called the *Dorroh extension* of R and its construction appeared for the first time in [7] (usually, references to the Dorroh extension are given to later papers ofr monographs, as e.g. [13], and it was a rather detective task to trace the original source).

In this paper, we concentrate only on commutative radical rings. We present a survey of this theory, starting from the very beginnings. We also summarize many more or less known results from a unifying point of view. Many of these results are fairly basic and we do not try to attribute them to any particular source, because it would require an enormous and perhaps unnecessary effort.

1. Preliminaries

Throughout the paper, a *ring* is a non-zero commutative and associative ring with or without unit element. The fact that R has the unit element $1 = 1_R$ will be denoted by $1_R \in R$. In the same way, the fact that R is without unit will be denoted by $1_R \notin R$.

Let R be a ring. For a subset A of R, we put $[A]_R = \sum Ra$, $a \in A$, and $[\![A]\!]_R = \sum Ra + \sum \mathbb{Z}a$, $a \in A$ ($[A]_R = 0 = [\![A]\!]_R$ if $A = \emptyset$). Clearly, both $[A]_R$ and $[\![A]\!]_R$ are ideals of R and $[A]_R \subseteq [\![A]\!]_R$. Moreover, $[\![A]\!]_R$ is the smallest ideal containing A, and hence it is the ideal generated by the set A.

A ring R will be called *finitely id-generated* if $R = [\![A]\!]_R$ for a finite subset A.

If I, J are ideals of a ring R then $IJ = \{\sum a_i b_i \mid a_i \in I, b_i \in J\}$. Clearly, IJ is an ideal of R and $IJ \subseteq I \cap J$. Further, we put $I^0 = R$, $I^1 = I$ and $I^{n+1} = I^n I$ for every $n \geq 1$.

1.1 Lemma. *Let A be a subset of a ring $R, I = [A]_R$ and $J = [\![A]\!]_R$. Then:*

(i) *I and J are ideals of R and $I \subseteq J$.*

(ii) *$I^2 = \sum R^2ab$ and $J^2 = \sum Rab + \sum \mathbb{Z}ab, a, b \in A$.*

(iii) *$I^2 \subseteq J^2 \subseteq I$.*

(iv) *If K is an ideal of R such that $I \subseteq K \subseteq J$ and $K^2 = K$ then $K = I = J^2$ and $J^4 = J^2$.*

Proof. Easy. $\square$

1.2 Lemma. *Let K be a finitely generated ideal of a ring R. If $K^2 = K$ then $K = Re$ for an idempotent element $e \in K$.*

Proof. Let K be generated by a set $\{a_1, \dots, a_m\}, m \geq 1$. Put $L_{m+1} = 0$ and, for $1 \leq k \leq m$, denote by L_k the ideal generated by $\{a_k, \dots, a_m\}$. Then $K = L_1 \supseteq \supseteq L_2 \supseteq \dots \supseteq L_m \supseteq L_{m+1} = 0$ and, proceeding by induction on k, $1 \leq k \leq \leq m + 1$, we are going to find elements $e_k \in K$ such that $x - e_kx \in L_k$ for every $x \in K$.

Put $e_1 = 0$. Now, assume that $1 \leq k \leq m$ and we already have elements $e_1, \dots, e_k$. We have $uv - e_kuv = u(v - e_kv) \in KL_k$ for all $u, v \in K$ and, since $K^2 = K$, we conclude that $x - e_kx \in KL_k$ for every $x \in K$. In particular, $a_k - e_ka_k = ba_k + c$ for some $b \in K$ and $c \in L_{k+1}$. Now, put $e_{k+1} = 2e_k - - e_k^2 + b - e_kb \in K$. It $v \in K$ then $v - e_kv = da_k + f$, $d \in K$, $f \in L_{k+1}$, and, for every $u \in K$, we have $uv - e_{k+1}uv = (u - e_ku - bu)(v - e_kv) = (u - e_ku - - bu)(ca_k + f) = du(a_k - e_ka_k - ba_k) + (u - e_ku - bu)f = duc + (u - - e_ku - bu)f \in L_{k+1}$. Consequently, $x - e_{k+1}x \in L_{k+1}$ for every $x \in K$.

Finally, put $e = e_{m+1}$. Then $x - ex = 0$ for every $x \in K$ and we see that $e^2 = e$ and $K = Re$. $\square$

1.3 Lemma. *If I and J are finitely generated ideals then IJ is a finitely generated ideal.*

Proof. Easy. $\square$

1.4 Lemma. *Let A be a finite subset of a ring $R, I = [A]_R$, $J = [\![A]\!]_R$, and let K be an ideal of R such that $K^2 = K$ and $I \subseteq K \subseteq J$. Then there is an idempotent element $e \in K$ such that $K = I = J^2 = Re$.*

Proof. By 1.1(iv), $K = I = J^2$, and hence K is finitely generated by 1.3. The rest follows from 1.2. $\square$

1.5 Lemma. *Let R be a ring such that $R^2 = R$. If R is finitely id-generated (or finitely generated or if $R(+)$ is finitely generated) then R has the unit element.*

Proof. The result follows immediately from 1.2. $\square$

1.6 Lemma. *Let I be an ideal and A a subset of a ring R. Then the set* $(I : A) = (I : A)_R = \{a \in R \mid aA \subseteq I\}$ is an ideal of *R and $I \subseteq (I : A)$.*

Proof. Obvious. □

An ideal P of a ring R is said to be *prime* if $P \neq R$ *and* $ab \notin P$ for all $a, b \in R \backslash P$ (i.e., $R \backslash P$ is a subsemigroup of the multiplicative semigroup $R(\cdot)$). The ring R is said to be a *domain* if the zero ideal is prime.

For a ring R, let $\mathcal{N}(R)$ denote the set of nilpotent elements of R.

1.7 Lemma. (i) *$\mathcal{N}(R)$ is an ideal of R.*
(ii) *If $\mathcal{N}(R) \neq R$ then $\mathcal{N}(R)$ is just the intersection of all prime ideals of R.*

Proof. Assume that $\mathcal{N}(R) \neq R$. If $a \in R \backslash \mathcal{N}(R)$ then $0 \notin A = \{a, a^2, a^3, \dots\}$ and $\mathscr{A} \neq \emptyset$, where $\mathscr{A}$ is the set of all ideals I with the property $I \cap A = \emptyset$. Now, $\mathscr{A}$ is upwards inductive and we can find a maximal element $P \in \mathscr{A}$. Clearly, P is a prime ideal and $a \notin P$. It follows that the set $\mathscr{P}$ of prime ideals is non-empty and $\bigcap \mathscr{P} \subseteq \mathcal{N}(R)$. The converse inclusion is obvious. □

1.8 Lemma. *A ring R has no prime ideals if and only if $\mathcal{N}(R) = R$ (i.e., R is a nil-ring).*

Proof. An immediate consequence of 1.7. □

1.9 Lemma. (i) *If $\mathcal{N}(R) \neq R$ then $\mathcal{N}(R/\mathcal{N}(R)) = 0$.*
(ii) *If $\mathcal{N}(R) \neq 0$ then $\mathcal{N}(\mathcal{N}(R)) = \mathcal{N}(R)$.*

Proof. Obvious. □

1.10 Lemma. *Let K be a finitely generated ideal of a ring R. If K is a nil-ideal then K is nilpotent (i.e., $K^n = 0$ for some $n \geq 1$).*

Proof. Let K be generated by a set $\{a_1, \dots, a_m\}$, $m \geq 1$. There is a positive integer k such that $a_1^k = \dots = a_m^k = 0$. Further, every element $x \in K$ can be expressed as $x = r_1 a_1 + + \dots + r_m a_m + l_1 a_1 + \dots + l_m a_m$, $r_i \in R$, $l_i \in \mathbb{Z}$, and it follows easily that $K^{km} = 0$. □

1.11 Lemma. *Let A be a finite subset of a ring R, $I = [A]_R$, $J = [\![A]\!]_R$, and let K be a nil-ideal of R such that $I \subseteq K \subseteq J$. Then J is nilpotent.*

Proof. By 1.1(iii), $J^2 \subseteq I$, and hence J is a nil-ideal. Now, J is nilpotent by 1.10. □

1.12 Lemma. *Let R be a nil-ring. Then:*
(i) *If R is finitely id-generated (or finitely generated or if $R(+)$ is finitely generated) then R is nilpotent.*
(ii) *R is locally nilpotent.*

Proof. The result follows immediately from 1.10. □

1.13 Lemma. *Let R be a ring. Then:*
(i) *The torsion part T of $R(+)$ is an ideal of R.*

(ii) *The divisible part Q of $R(+)$ is an ideal of R.*
(iii) $QT = 0$ *and* $(Q \cap T)^2 = 0$.
(iv) *If* $\mathcal{N}(R) = 0$ *then* $T(+)$ *is reduced.*

Proof. (i) and (ii). Easy.
(iii) If $a \in Q$ and $b \in T$ then $nb = 0$ and $nc = a$ for some $n \geq 1$ and $c \in R$. Now, $ab = nc \cdot b = c \cdot nb = 0$.
(iv) Use (iii). □

1.14 Lemma. *Let R be a ring such that the additive group $R(+)$ is torsion and divisible. Then $R^2 = 0$ (i.e., R is a zero multiplication ring).*

Proof. An immediate consequence of 1.13. □

Let R be a ring. Then $\operatorname{char}(R)$ denotes the smallest positive integer m such that $mR = 0$. If no such integer exists then $\operatorname{char}(R) = 0$.

1.15 Lemma. *Let R be a domain. Then either* $\operatorname{char}(R) = 0$ *and $R(+)$ is torsion-free or* $\operatorname{char}(R) = p > 0$ *is a prime number and $R(+)$ is a p-elementary group.*

Proof. Let $ma = 0$ for some $a \in R$, $a \neq 0$, and $m \geq 1$. *Ten* $a \cdot mx = 0$ for every $x \in R$ and, since R is a domain, we get $mR = 0$. Thus $n = \operatorname{char}(R) > 0$ and, if $n = kl$, $k \geq 1$, $l \geq 1$, then $kx \cdot ly = 0$ for all $x, y \in R$. Consequently, either $kx = 0$ or $ly = 0$ and it follows easily that n is prime. □

1.16 Lemma. *Let R be a ring and $Z(R)$ the set of integers $m \in \mathbb{Z}$ such that $mx + ax = 0$ for some $a \in R$ and all $x \in R$. Then:*
(i) *$Z(R)$ is a subgroup of $\mathbb{Z}(+)$ and there is a uniquely determined non-negative integer $\zeta(R)$ such that $Z(R) = \mathbb{Z}\zeta(R)$.*
(ii) $\zeta(R) = 0$ *if and only if* $Z(R) = 0$.
(iii) $\zeta(R) = 1$ *if and only if R has the unit element.*
(iv) $\zeta(R)$ *divides* $\operatorname{char}(R)$.
(v) *If R is a domain and* $\operatorname{char}(R) > 0$ *then* $\zeta(R) = \operatorname{char}(R)$ *is a prime number.*

Proof. Easy. □

If R is a ring with unit then R^* denotes the multiplicative group of invertible elements of $R, R^* = \{a \in R \mid Ra = R\}$.

1.17 Lemma. *Let R be a ring. Then R has the unit element if and only if $Ra = R$ for at least one $a \in R$.*

Proof. Put $A = \{a \in R \mid Ra = R\}$ and assume that $A \neq \emptyset$. If $a, b \in A$ then $Rab = Rb = R$, and so $ab \in A$. Further, $ac = b$ for some $c \in R$ and $Rc = Rac = = Rb = R$. It follows that the multiplicative semigroup $A(\cdot)$ is a group with neutral element e. Then $e^2 = e$, $Re = R$ and we see that e is the unit of R. (Notice that the result follows immediately from 1.5). □

1.18 Lemma. *Let $1_R \in R$ and $\pi : R \to S = R/\mathcal{N}(R)$ be the natural projection. Then $\pi(R^*) = S^* \simeq R^*/G$, where $G = \mathcal{N}(R) + 1$.*

Proof. Clearly, $\pi(R^*) \subseteq S^*$ and if $a \in R$ is such that $\pi(a) \in S^*$ then $c = ab - 1 \in \mathcal{N}(R)$ for some $b \in R$, $c^m = 0$ for some $m > 1$ and $(c + 1)(c^{m-1} - c^{m-2} + \dots + (-1)^{m-1}) = \pm 1$. Thus $ab = c + 1 \in R^*$, $a \in R^*$ and the rest is clear. □

1.19 Example. Let R be a (whether commutative or non-commutative) ring with unit. We show that the multiplicative group R^* of invertible elements of R cannot have five elements.

Assume the contrary. We may also assume that R is generated by $R^* \cup \{1_R\}$, and hence that R is commutative (we have $R^* \simeq \mathbb{Z}_5(+)$). Further, $(-1)^2 = 1$, $-1 \in R^*$ and, since R^* has no element of order 2, we get $-1 = 1$ and $2R = 0$. Now, let $R^* = \{1, a, a^2, a^3, a^4\}$. Then $(1 + a + a^2)(a + a^2 + a^4) = 1$, and hence $1 + a + a^2 \in R^*$ and $(1 + a + a^2)^{-1} = a + a^2 + a^4$. If $1 + a + a^2 = 1$ then $a = a^2$ and $1 = a$, a contradiction. If $1 + a + a^2 = a$ then $1 = a^2$, a contradiction. If $1 + a + a^2 = a^2$ then $1 = a$, a contradiction. If $1 + a + a^2 = a^3$ then $a^2 = (a^3)^{-1} = (1 + a + a^2)^{-1} = a + a^2 + a^4$, hence $a = a^4$ and $1 = a^3$, a contradiction. Finally, if $1 + a + a^2 = a^4$ then $a = (a^4)^{-1} = a + a^2 + a^4$, hence $a^2 = a^4$ and $1 = a^2$, the final contradiction.

1.20 Lemma. *A ring R has no proper subring if and only if either $R \simeq \mathbb{Z}_p$ or $R^2 = 0$ and $R(+) \simeq \mathbb{Z}_p(+)$ for a prime p.*

Proof. Assume that R has no proper subring, the converse implication being trivial. If $R^2 = 0$ then every non-zero subgroup of $R(+)$ is a subring, and hence $R(+)$ is a simple group and $R(+) \simeq \mathbb{Z}_p(+)$. On the other hand, if $R^2 \neq 0$ then $R^2 = R$, R has the unit element by 1.17 and $R = \mathbb{Z} \cdot 1_R$. Consequently, $R \simeq \mathbb{Z}_n$ for some $n \geq 0$ and, clearly, $n \geq 2$ is a prime. □

1.21 Lemma. *Let R be a ring. Then $(R/I)(+)$ is torsion for every non-zero ideal I of R if and only if at least (and then just) one of the following three cases takes place:*

(1) *$R(+)$ is torsion;*
(2) *$R^2 = 0$ and $R(+)$ is isomorphic to a subgroup of the additive group $\mathbb{Q}(+)$ of rationals;*
(3) *R is a domain, $\mathrm{char}(R) = 0$ and for all $a, b \in R\setminus\{0\}$ there exist $r \in R$ and a positive integer n such that $nb = ra$.*

Proof. Assume that $(R/I)(+)$ is torsion for every $I \neq 0$ and that $R(+)$ is not torsion. Then, clearly, $R(+)$ is torsionfree and, for every $a \in R$, the additive group $(Ra)(+)$ is torsionfree and $(Ra)(+) \simeq (R/(0:a))(+)$. Consequently, either $(0:a) = 0$, or $(0:a) = R$ and $a \in (0:R)$. In particular, if $(0:R) = 0$ then R is a domain. Now, assume that $(0:R) \neq 0$. If $a \in R$ then $na \in (0:R)$ for some $n \geq 1$

and we have $a \cdot nb = 0$ for every $b \in R$. If $a \notin (0:R)$ then $nb = 0$ and $nR = 0$, a contradiction. Thus $R^2 = 0$. The rest is clear. $\square$

1.22 Remark. Let R be a ring such that $R(+)$ is torsionfree of rank 1. According to 1.21, either $R^2 = 0$ or R is a domain.

1.23 Remark. Let R be a ring such that $R(+)$ is torsionfree. Denote by $\mathscr{K}$ the set of ideals K such that $(R/K)(+)$ is non-zero and torsionfree.

(i) $\mathscr{K} \neq \emptyset$ and $K \neq R$ for every $K \in \mathscr{K}$.

(ii) Let $K \in \mathscr{K}$ be such that K is maximal in $\mathscr{K}$. Now, it follows from 1.21 that either $R^2 \subseteq \mathscr{K}$ (and then $R \neq R^2$ and $(R/R^2)(+)$ is not torsion) or K is a prime ideal (and then R is not nil).

(iii) Let $\mathscr{I}$ be a non-empty chain of ideals from $\mathscr{K}$ and $I = \bigcup \mathscr{I}$. Then either $I \in \mathscr{K}$ or $I = R$ (and then R is not finitely id-generated).

(iv) If R is finitely id-generated then every ideal from $\mathscr{K}$ is contained in an ideal that is maximal in $\mathscr{K}$.

(v) Assume that the additive group $R(+)$ has finite rank, $\operatorname{rnk}(R(+)) = r$. If $K, L \in \mathscr{K}$ are such that $K \subseteq L$ and $K \neq L$ then $\operatorname{rnk}((R/L)) < \operatorname{rnk}((R/K)(+)) \leq r$. Consequently, every chain of ideals from $\mathscr{K}$ is finite and contains at most r members. In particular, every ideal from $\mathscr{K}$ is contained in an ideal that is maximal in $\mathscr{K}$.

1.24 Lemma. *Let R be a ring such that $R(+)$ is torsionfree. Then the additive groups $(R/\mathscr{N}(R))(+)$, $(R/(0:R))(+)$, $(R/(0:a))(+)$, $a \in R$, are torsionfree.*

Proof. Easy. $\square$

1.25 Lemma. *Let R be a ring such that $\mathscr{N}(R) = 0$.*

(i) *If $T \neq R$, where T is the torsion part of R, then $\mathscr{N}(R/T) = 0$.*

(ii) *$\mathscr{N}(R/(0:a)) = 0$ for every $0 \neq a \in R$.*

Proof. (i) If $a^m \in T$ for some $a \in R$ and $m \geq 1$ then there is $n \geq 1$ wih $na^m = 0$, and so $(na)^m = 0$, $na = 0$ and $a \in T$.

(ii) Clearly, $(0:a) \neq R$. If $b^m \in (0:a)$ for some $b \in R$ and $m \geq 1$ then $(ba)^m = 0$, $ba = 0$ and, finally, $b \in (0:a)$. $\square$

2. The adjoint (or circle) semigroup

Let R be a ring. We put $a \circ b = a + b + ab$ for all $a, b \in R$.

2.1 Proposition. (i) *$R(\circ)$ isa commutative semigroup* (called the *adjoint* or the *circle semigroup* of the ring R).

(ii) *0 $(= 0_R)$ is the neutral element of $R(\circ)$.*

(iii) *$R(\circ)$ has the absorbing element if and only if $1_R \in R$ (then -1 is that absorbing element).*

(iv) *The set* $\mathscr{L}(R) = \{a \in R \mid 0 \in a \circ R\}$ *is a subgroup of* $R(\circ)$ *(it is the group of invertible elements of* $R(\circ)$*).*
(v) $R(\circ)$ *is a group if and only if* $\mathscr{L}(R) = R$.
(vi) $R(\circ)$ *is cancellative if and only if* $ab \neq b$ *for all* $a, b \in R$, $b \neq 0$.
(vii) $R(\circ) = R(+)$ *if and only if* R *is a zero multiplication ring.*

Proof. (i) $a \circ (b \circ c) = a + b + c + ab + bc + abc = (a \circ b) + c$.
(ii), (iii), (iv) and (v) are easy.
(vi) If $a \circ b = a \circ c$ then $a_1 b_1 = b_1$, where $a_1 = -a$ and $b_1 = b - c$.
(vii) Obvious. □

2.2 Remark. Let R be a ring. For every $a \in R$ there exists at most one $b \in R$ with $a + b + ab = 0$. This follows immediately from 2.1(i), but a direct argument is very easy: If $a + b + ab = 0 = a + c + ac$ then $ac + bc + abc = 0 = ab + bc + acb$, $ac = bc$, $a + b = a + c$ and $b = c$.

For every $a \in \mathscr{L}(R)$, the uniquely determined element $b \in R$ with $a + b + ab = 0$ will be denoted by $b = \tilde{a}$. Clearly, $\tilde{b} = a$, i.e., $\tilde{\tilde{a}} = a$.

2.3 Lemma. *Let* $a \in R$ *and* $m \geq 1$. *Then the m-th power* $a \circ a \circ \ldots \circ a$ *(m-times) is just* $\sum_{i=1}^{m} \binom{m}{i} a^i$.

Proof. By induction on m. □

2.4 Lemma. *Let* $a \in R$ *and* $m \geq 1$ *be such hat* $a^m = 0$. *Then* $a \in \mathscr{L}(R)$, $\tilde{a} = -a + a^2 - a^3 + \ldots + a^{m-1}$ *for m odd and* $\tilde{a} = -a + a^2 - a^3 + \ldots - a^{m-1}$ *for m even.*

Proof. Easy. □

2.5 Corollary. $\mathscr{N}(R) \subseteq \mathscr{L}(R)$. □

2.6 Lemma. *Let* $e \in R$ *be such that* $-e \in \mathscr{L}(R)$ and $e^2 = e$. *Then* $e = 0$.

Proof. We have $-e + f - ef = 0$, where $f = \widetilde{-e}$, and hence $0 = e0 = -e + ef - ef = -e$. Thus $e = 0$. □

2.7 Lemma. *Let* $a, b \in R$ *be such that* $-b \in \mathscr{L}(R)$ *and* $ab = a$. *Then* $a = 0$.

Proof. For $c = \widetilde{-b}$, we have $-b + c - bc = 0$ and $0 = a0 = -ab + ac - abc = -a + ac - ac = -a$. Thus $a = 0$. □

2.8 Proposition. *Let R be a domain. Then:*

(i) *If* $1_R \notin R$ *then* $R(\circ)$ *is a cancellative semigroup.*
(ii) *If* $1_R \in R$ *then* -1 *is the absorbing element of* $R(\circ)$, $A = R \setminus \{1\}$ *is a subsemigroup of* $R(\circ)$ *and* $A(\circ)$ *is cancellative.*

Proof. Easy (use 2.1(vi)). □

2.9 Proposition. *Assume that* $1_R \in R$. *Then:*

(i) *The mapping* $a \mapsto a - 1$, $a \in R$, *is an isomorphism of the multiplicative semigroup* $R(\cdot)$ *onto the adjoint semigroup* $R(\circ)$.

(ii) *The mapping* $a \mapsto a - 1$, $a \in R^*$, *is an isomorphism of the multiplicative group* $R^*(\cdot)$ *onto the group* $\mathscr{L}(R)(\circ)$.

(iii) *If* $a \oplus b = a + b + 1$ *for all* $a, b \in R$ *then* $R(\oplus, \circ)$ *is a ring and the mapping* $a \mapsto a - 1$, $a \in R$, *is an isomorphism of the ring* $R(= R(+,\cdot))$ *onto the ring* $R(\oplus, \circ)$.

Proof. We have $ab - 1 = (a - 1) \circ (b - 1)$ for all $a, b \in R$. □

2.10 Lemma. *Let S be a subring of a ring R. Then* $S(\circ)$ *is a subgroup of* $R(\circ)$ *in each of the following cases:*

(1) $\mathscr{L}(S) = S$;

(2) *S is a nil-ring;*

(3) *for every* $a \in S$ *there exists a positive integer m such that* $\sum_{i=1}^{m} \binom{m}{i} a^i = 0$;

(4) $\mathscr{L}(R) = R$ *and S is an ideal of R.*

Proof. Any of the conditions (2), (3) and (4) implies the condition (1) (see 2.3 and 2.5). □

2.11 Remark. Define an operation $*$ on R by $a * b = a + b - ab$ for all $a, b \in R$. Then $(-a) * (-b) = -(a \circ b)$, and so the mapping $x \mapsto -x$ is an isomorphism of $R(\circ)$ onto $R(*)$. Notice also that an elementt $a \in R$ is invertible in $R(*)$ if and only if $a + b = ab$ for some $b \in R$.

3. Maximal ideals

An ideal I of a ring R is said to be *maximal* if $I \neq R$ and $K = I$ whenever K is an ideal such that $I \subseteq K \neq R$. We denote by $\mathrm{Mxi}(R)$ the set of all maximal ideals of R.

A ring R is said to be *simple* if 0 is a maximal ideal of R.

3.1 Proposition. *A ring R is simple if and only if R is a field or a zero multiplication ring of finite prime order (then* $R(+) \simeq \mathbb{Z}_p(+)$ *for a prime p).*

Proof. Let R be a simple ring and $I = (0 : R)$. Then I is an ideal of R and if $I \neq 0$ then $I = R$ and R is a zero multiplication ring. In such a case, every subgroup of $R(+)$ is an ideal of R, and consequently $R(+) \simeq \mathbb{Z}_p(+)$. On the other hand, if $I = 0$ then, for every $a \in R \setminus \{0\}, Ra \neq 0$, and hence $Ra = R$. By 1.17, R has the unit element and it is clear that R is a field. □

3.2 Lemma. *Let R be a ring,* $a \in R$ *and* $L_a = \{x + ax \mid x \in R\}$. *Then* L_a *is an ideal of R ad* $L_a + Ra = R$. *Moreover,* $L_a = 0$ *if and only if* $1_R \in R$ *and* $a = -1_R$.

Proof. Easy. □

3.3 Lemma. Let R *be a ring. The following conditions are equivalent for* $a \in R$:

(i) $a \in \mathscr{L}(R)$.
(ii) $a \in L_a$.
(iii) $Ra \subseteq L_a$.
(iv) $L_a = R$.

Proof. Easy. □

An ideal I of a ring R is called *modular* if $I \neq R$ and $L_a \subseteq I$ for some $a \in R$ (then $a \notin \mathscr{L}(R)$).

3.4 Lemma. *Every proper ideal of a ring* R *is modular if and only if* $1_R \in R$.

Proof. Easy. □

3.5 Lemma. *The following conditions are equivalent for a proper ideal* K *of a ring* R:

(i) K *is maximal and modular.*
(ii) K *is maximal and* $R^2 \nsubseteq K$.
(iii) *The factor-ring* R/K *is a field.*

Proof. (i) implies (ii). There is $a \in R$ with $L_a \subseteq K$. Since $L_a + Ra = R \neq K$, *we have* $Ra \nsubseteq K$, and so $R^2 \nsubseteq K$.

(ii) implies (iii). $S = R/K$ is a simple ring and $S^2 \neq 0$. By 3.1, S is a field.

(iii) implies (i). We have $R^2 \nsubseteq K$, and so $Rb \nsubseteq K$, for some $b \in R$. Further, $K \subseteq J = (K : b) \neq R$. Since K is maximal, $J = K$, $K + Rb = R$, $b + ab \in K$ for at least one $a \in R$, $b(x + ax) = x(b + ab) \in K$ for every $x \in R$, $x + ax \in$ $\in J = K$ and $L_a \subseteq K$. □

3.6 Lemma. *The following conditions are equivalent for a proper ideal* K *of a ring* R:

(i) K *is maximal and not modular.*
(ii) K *is maximal and* $R^2 \subseteq K$.
(iii) *The factor-ring* R/K *is a zero multiplication ring of finite prime order* p (*then* $R^2 + pR \subseteq K$).

Proof. Use 3.5. □

3.7 Lemma. *Let* R *be a ring and* $a \in R \setminus \mathscr{L}(R)$. *Then there exists at least one modular maximal ideal* K *of* R *such that* $L_a \subseteq K$ *and* $a \notin K$.

Proof. Denote by $\mathscr{I}$ the set of all modular ideals I with $a \notin I$. Then $L_a \in \mathscr{I}$, $\mathscr{I}$ is upwards inductive and $\mathscr{I}$ contains a maximal element K such that $L_a \subseteq K$. Now, if L is an ideal such that $K \subseteq L \neq K$ then $a \in L$ and $L = R$, since $L_a + Ra = R$. Thus K is a maximal ideal. □

3.8 Corollary. (i) *A ring R has at least one modular maximal ideal if and only if $\mathscr{L}(R) \neq R$ (i.e., $R(\circ)$ is not a group).*

(ii) *A ring R has at least one maximal ideal if and only if either $\mathscr{L}(R) \neq R$ or $R^2 + pR \neq R$ for at least one prime number p.* □

3.9 Corollary. *A ring R has no maximal ideals if and only if $\mathscr{L}(R) = R$ and $R^2 + pR = R$ for every prime p.* □

3.10 Lemma. *If R is a ring with unit then $R \setminus \bigcup \mathrm{Mxi}(R) = R^*$.*

Proof. Obvious. □

4. The Jacobson radical

Let R be a ring. We define the *Jacobson radical* $\mathscr{J}(R)$ of R in the following way: If $\mathscr{L}(R) = R$ then $\mathscr{J}(R) = R$. If $\mathscr{L}(R) \neq R$ then $\mathscr{J}(R)$ is the intersection of all modular maximal ideals of R (see 3.8 (i)).

4.1 Proposition. *$\mathscr{J}(R)$ is an ideal of R, $\mathscr{J}(R) \subseteq \mathscr{L}(R)$ and $\mathscr{J}(R)$ is the greatest ideal contained in $\mathscr{L}(R)$.*

Proof. Clearly, $\mathscr{J}(R)$ is an ideal and we may assume that $\mathscr{L}(R) \neq R$. Then $\mathscr{J}(R) \subseteq \mathscr{L}(R)$ by 3.7. Now, let I be an ideal of R such that $I \subseteq \mathscr{L}(R)$ and $I \nsubseteq \mathscr{J}(R)$. Then there exists a modular maximal ideal K such that $I \nsubseteq K$. Since $R^2 \nsubseteq K$, we have $(K : R) = K$. Consequently, $IR \nsubseteq K$ and $Ia \nsubseteq K$ for some $a \in R$. Then $K + Ia = R$, $a + ba \in K$ for some $b \in I$, $0 = (b + \tilde{b} + b\tilde{b})a = ba + \tilde{b}(a + ba)$ and $ba = -\tilde{b}(a + ba) \in K$. Thus $a \in K$, a contradiction with $Ia \nsubseteq K$. □

4.2 Remark. (i) Let R be a ring with $\mathrm{Mxi}(R) \neq \emptyset$. Then $\bigcap \mathrm{Mxi}(R) = \mathscr{J}(R) \cap \bigcap (R^2 + pR)$, p running through all prime numbers.

(ii) Let R be a ring with unit. Then $\mathscr{J}(R) = \bigcap \mathrm{Mxi}(R)$ and $R \setminus R^* = \bigcup \mathrm{Mxi}(R)$.

4.3 Lemma. *R be a ring. Then:*

(i) *If $\mathscr{J}(R) \neq R$ then $\mathscr{L}(R/\mathscr{J}(R)) = \mathscr{L}(R)/\mathscr{J}(R)$ and $\mathscr{J}(R/\mathscr{J}(R)) = 0$.*

(ii) *If $\mathscr{J}(R) \neq 0$ then $\mathscr{J}(\mathscr{J}(R)) = \mathscr{J}(R)$.*

Proof. (i) Let $\pi : R \to S = R/\mathscr{J}(R)$ be the natural projection. If $a \in \mathscr{L}(R)$ then $\widetilde{\pi(a)} = \pi(\tilde{a})$, and so $\pi(a) \in \mathscr{L}(S)$. Conversely, if $a \in R$ is such that $\pi(a) \in \mathscr{L}(S)$ then $\pi(b) = \widetilde{\pi(a)}$ for some $b \in R$ and $0 = \pi(a) \circ \widetilde{\pi(a)} = \pi(a \circ b)$, $a \circ b \in \mathrm{Ker}(\pi) = \mathscr{J}(R)$ and $(a \circ b) \circ c = 0$, where $c = \widetilde{a \circ b}$. Now, $0 = (a \circ b) \circ c = a \circ (b \circ c)$ and $a \in \mathscr{L}(R)$. Thus $\mathscr{L}(R)/\mathscr{J}(R)) = \mathscr{L}(S)$. Finally, $I = \pi^{-1}(\mathscr{J}(S))$ is an ideal of R and $I \subseteq \mathscr{L}(R)$. Consequently, $I \subseteq \mathscr{J}(R)$ by 4.1, and so $\mathscr{J}(S) = \pi(I) = 0$.

(ii) We have $\tilde{a} \in \mathscr{J}(R)$ for every $a \in \mathscr{J}(R)$. □

4.4 Lemma. *Let R be a ring. Then $\mathcal{N}(R) \subseteq \mathcal{J}(R)$.*

Proof. Combine 2.5 and 4.1. $\square$

4.5 Lemma. *Let R be a ring with unit and $\pi : R \to S = R/\mathcal{J}(R)$ the natural projection. Then $\pi(R^*) = S^* \simeq R^*/G$, where $G = \mathcal{J}(R) + 1$. Moreover, the mapping $a \mapsto a + 1$ is an isomorphism of the group $\mathcal{J}(R)(\circ)$ onto the multiplicative group G.*

Proof. Clearly, $\pi(R^*) \subseteq S^*$. If $a \in R$ is such that $\pi(a) \in S^*$ then $\pi(b) = \pi(a)^{-1}$ for some $b \in R$ and we have $ab - 1 \in \mathcal{J}(R)$, $ab \in \mathcal{J}(R) + 1 = G \subseteq R^*$ and $a \in R^*$. The rest is clear. $\square$

4.6 Lemma. *Let $R \subseteq S$ be integral extension of domains with unit. Then $1_R = 1_S$, $\mathcal{J}(R) = R \cap \mathcal{J}(S)$, $\mathcal{J}(R) = 0$ if and only if $\mathcal{J}(S) = 0$.*

Proof. Easy and well known. $\square$

4.7 Lemma. *Let S be a domain wth unit such that $S(+)$ is finitely generated. Then $\mathcal{J}(S) = 0$.*

Proof. If $\operatorname{char}(S) > 0$ then $S(+)$ is a finitely generated torsion group, S is finite, and hence S is a field and $\mathcal{J}(S) = 0$. *If char*$(S) = 0$ then $R \simeq \mathbb{Z}$, R being the prime subring of S, and, since S is a finitely generated $\mathbb{Z}$-module, S is integral over R. By 4.6, $\mathcal{J}(S) = 0$. $\square$

4.8 Proposition. *The following conditions are equivalent for a ring R:*

(i) *$\mathcal{J}(R/I) = \mathcal{N}(R/I)$ for every proper ideal I of R.*

(ii) *$\mathcal{J}(R/P) = 0$ for every prime ideal P of R.*

(iii) *Every prime ideal of R is an intersection of modular maximal ideals.*

Proof. Clearly, (i) implies (ii) and (ii) is equivalent to (iii).

(iii) implies (i). We have $\mathcal{N}(R/I) \subseteq \mathcal{J}(R/I)$ and we may assume that $\mathcal{N}(R/I) = = K/I$, $K \neq R$. Then $K = \bigcap P$, $K \subseteq P$, P prime, hence K is an intersection of modular maximal ideals and $\mathcal{J}(R/I) \subseteq K/I$. Thus $\mathcal{J}(R/I) = = \mathcal{N}(R/I)$. $\square$

A ring satisfying the equivalent conditions of 4.8 is called a *Hilbert ring.*

4.9 Proposition. (i) *Let I be a proper ideal of a Hilbert ring R. Then the factor-ring R/I is a Hilbert ring.*

(ii) *Every nil-ring is a Hilbert ring.*

Proof. Obvious. $\square$

5. The Dorroh extension

5.1 Let R be a ring Put $S = \mathbb{Z} \times R$ and define an addition and a multiplication on S by $(m, a) + (n, b) = (m + n,\ a + b)$ and $(m, a)(n, b) = (mn, na + mb + ab)$.

5.1.1 Lemma. (i) *$S(=S(+,\cdot))$ is a ring with unit $1_S = (1,0)$.*

(ii) *The mapping $m \mapsto (m,0)$ is a ring isomorphism of $\mathbb{Z}$ onto a subring Z of S, $Z = \{(m,0) \mid m \in \mathbb{Z}\}$.*

(iii) *Z is the prime subring of S.*

(vi) char$(S) = 0$.

(v) *The mapping $a \mapsto (0,a)$ is a ring isomorphism of R onto a subring $R^{\triangle}$ of S, $R^{\triangle} = \{(0,a) \mid a \in R\}$.*

(vi) *$R^{\triangle}$ is a prime ideal of S and $S/R^{\triangle} \simeq \mathbb{Z}$.*

(vii) *Every ideal of $R^{\triangle}$ is an ideal of S.*

Proof. All the assertions are readily checked. □

The ring S is called the *Dorroh extension* of R; *we will denote it by* $S = \mathbb{D}(R)$.

5.1.2 Lemma. (i) *For every prime $p \geq 2$, the set $K_p = R^{\triangle} + pS = \{(mp,a) \mid m \in \mathbb{Z}, a \in R\}$ is a maximal ideal of S and $S/K_p \simeq \mathbb{Z}_p$.*

(ii) *If K is a maximal ideal of S such that $R^{\triangle} \subseteq K$ then $K = K_p$ for a prime p.*

(iii) *$R^{\triangle} = \bigcap K_p$, p running through all prime numbers.*

Proof. Everything is clear from the isomorphism $S/R^{\triangle} \simeq \mathbb{Z}$. □

5.1.3 Lemma. *Let K be a maximal ideal of S with $R^{\triangle} \nsubseteq K$. Then $I = K \cap R^{\triangle}$ is a modular maximal ideal of $R^{\triangle}$.*

Proof. Clearly, I is a prime ideal of $R^{\triangle}$ and $R^{\triangle}/I$ is a domain. Further, if $r,s \in R^{\triangle} \setminus I$ then $r,s \in S \setminus K$ and, since S/K is a field, $rx - s \in K$ for some $x \in S$. On the other hand, $S = R^{\triangle} + K$, hence $x = t + y$, $t \in R^{\triangle}$, $y \in K$, and $rx - s = rt + ry - s \in K$. Consequently, $rt - s \in I$ and we conclude that $R^{\triangle}/I$ is a field. By 3.5, I is a modular maximal ideal of $R^{\triangle}$. □

5.1.4 Lemma. $\mathscr{J}(S) = \mathscr{J}(R^{\triangle})$.

Proof. It follows from 5.1.2 that $\mathscr{J}(S) \subseteq R^{\triangle}$. Then $\mathscr{J}(S) \subseteq \mathscr{L}(R^{\triangle})$ and, since $\mathscr{J}(S)$ is an ideal, we have $\mathscr{J}(S) \subseteq \mathscr{J}(R^{\triangle})$ (see 4.1). On the other hand, by 5.1.1 (vii), $\mathscr{J}(R^{\triangle})$ is an ideal of S and $\mathscr{J}(R^{\triangle}) \subseteq \mathscr{L}(R^{\triangle}) \subseteq \mathscr{L}(S)$. Using 4.1 again, we get $\mathscr{J}(R^{\triangle}) \subseteq \mathscr{J}(S)$. □

5.1.5 Corollary. $\mathscr{J}(S) = R^{\triangle}(\simeq R)$ *if and only if* $\mathscr{J}(R) = R$. □

5.1.6 Lemma. $\mathscr{N}(S) = \mathscr{N}(R^{\triangle})(\simeq \mathscr{N}(R))$.

Proof. Obvious. □

5.1.7 Corollary. $\mathscr{N}(S) = R^{\triangle}$ *if and only if R is a nil-ring.* □

5.1.8 Lemma. $S^* \simeq \mathscr{L}(R)(\circ) \times \mathbb{Z}_2(+)$.

Proof. If is easy to see that $(m,a) \in S^*$ if and only if either $m = 1$ and $a \in \mathscr{L}(R)$ or $m = -1$ and $-a \in \mathscr{L}(R)$. □

5.1.9 Lemma. (i) *The ring S is generated by the set $R^{\triangle} \cup \{1_S\}$.*
(ii) *S is a finitely generated ring if and only if R is so.*
(iii) *$S(+)$ is a finitely generated group if and only if $R(+)$ is so.*
(iv) *R^* is a finitely generated group if and only if $\mathscr{L}(R)(\circ)$ is so.*

Proof. Obvious. □

5.1.10 Proposition. (i) *$S = \mathbb{D}(R)$ is a ring with unit and R is isomorphic to a subring $R^{\triangle}$ of S.*
(ii) *$R^{\triangle}$ is an ideal of S, $S/R^{\triangle} \simeq \mathbb{Z}$ and $S = R^{\triangle} + \mathbb{Z} \cdot 1_S$.*
(iii) *$\mathscr{J}(S) = \mathscr{J}(R^{\triangle})$ and $\mathscr{N}(S) = \mathscr{N}(R^{\triangle})$.*
(iv) *$S^* \simeq \mathscr{L}(R)(\circ) \times \mathbb{Z}_2(+)$.*

Proof. See the preceding lemmas. □

5.2 Remark. Let $\varphi : R_1 \to R_2$ be a homomorphism of rings. Then there exists a uniquely determined ring homomorphism $\psi : \mathbb{D}(R_1) \to \mathbb{D}(R_2)$ such that $\psi(1) = 1$ and $\psi\alpha = \beta\varphi$, $\alpha : R_1 \to \mathbb{D}(R_1)$ and $\beta : R_2 \to \mathbb{D}(R_2)$ being the natural injections. We have $\psi(m, a) = (m, \varphi(a))$ for all $m \in \mathbb{Z}$, $a \in R_1$. Moreover, ψ is injective (projective, resp.) if and only if φ is so. Consequently, ψ is an isomorphism if and only if φ is an isomorphism.

5.3 Remark. Let $\varphi : R \to T$ be a homorphism of a ring R into a ring T with unit. Put $\psi(m, a) = m \cdot 1_T + \varphi(a)$ for all $m \in \mathbb{Z}$ and $a \in R$. Then ψ is a homomorphism of $S = \mathbb{D}(R)$ into $T, \psi(1_S) = 1_T$ and $\psi\alpha = \varphi$, $\alpha : R \to S$ being the natural injection. Moreover, $\psi(S) = \varphi(R) + \mathbb{Z} \cdot 1_T \simeq S/\mathrm{Ker}(\psi)$.

If $T = \varphi(R) + \mathbb{Z} \cdot 1_T$ then ψ is projective and $T \simeq S/\mathrm{Ker}(\psi)$.

If φ is injective and $(m, a) \in \mathrm{Ker}(\psi)$ then $mx + ax = 0$ for every $x \in R$ (cf. 1.16).

5.4 Consider the situation from 5.1 and put $W_1 = (0 : R^{\triangle})_S$, $W_2 = (0 : R^{\triangle})_{R^{\triangle}} = W_1 \cap R^{\triangle}$.

5.4.1 Lemma. (i) *Both W_1 and W_2 are proper ideals of $S = \mathbb{D}(R)$ and $W_2 \subseteq W_1$.*
(ii) *$W_1 = \{(m,a) \mid mx + ax = 0$ for every $x \in R\}$ (see 1.16).*
(iii) *$\mathbb{Z}\zeta(R) = \{m \mid (m, a) \in W_1\}$.*
(iv) *$\zeta(R) = 0$ if and only if $W_1 = W_2$.*
(v) *$\zeta(R) = 1$ if and only if $1_R \in R$.*

Proof. Easy. □

5.4.2 Lemma. *Let $a \in R$ be such that $u = (\zeta(R), a) \in W_1$. Then $W_1 = W_2 + \mathbb{Z}u$.*

Proof. If $(n, b) \in W_1$ then $n = k\zeta(R)$ for some $k \in \mathbb{Z}$ and $(0, b - ka) \in W_1$. Now, $(0, b - ka) \in W_2$ and $(n, b) = (0, b - ka) + ku$. □

5.4.3 Corollary. *If $(0 : R) = 0$ then $W_1 = \mathbb{Z}u$ for at least one $u \in W_1$.* □

5.4.4 Lemma. (i) *$\mathbb{Z}u$ is an ideal of S and $\mathbb{Z}u \subseteq W_1$ for every $u \in W_1$.*

(ii) *$\mathbb{Z}u \subseteq \mathbb{Z}v$ if and only if $u = kv$ for some $k \in \mathbb{Z}$.*

(iii) *If $u = (m, a) \in W_1$ is such that $m \neq 0$ then $\mathbb{Z}u \cap W_2 = 0$.*

Proof. Easy. □

5.4.5 Lemma. *Let I be an ideal of S. Then:*

(i) *$I \cap R^{\triangle} = 0$ if and only if $I \subseteq W_1$ and $I \cap W_2 = 0$.*

(ii) *If $I \neq 0$ and $I \cap R^{\triangle} = 0$ then $I = \mathbb{Z}u (= Su)$ for some $u = (m, a) \in W_1$, $m \geq 1$.*

Proof. (i) Obvious.

(ii) Clearly, $\{n \mid (n, b) \in I\} = \mathbb{Z}m$ and $u = (m, a) \in I$ for some $m \geq 1$ and $a \in R$. Now, $\mathbb{Z}u \subseteq I$ and if $v = (n, b) \in I$ then $n = km$ for some $k \in \mathbb{Z}$, $v - ku \in I \cap \cap R^{\triangle} = 0$ and $v = ku$. Thus $I = \mathbb{Z}u$. □

Let $\mathscr{I}_1$ denote the set of ideals I of S such that $I \cap R^{\triangle} = 0$ and $\mathscr{I}_2$ the set of maximal elements from $\mathscr{I}_1$. Since $\mathscr{I}_1$ is non-empty and upwards inductive, every ideal from $\mathscr{I}_1$ is contained in an ideal from $\mathscr{I}_2$ (see 5.4.5).

5.4.6 Lemma. (i) *$\mathscr{I}_1 = \mathscr{I}_2 = \{0\}$ if and only if $W_1 = W_2 (= (0 : R^{\triangle})_{R^{\triangle}})$.*

(ii) *$\mathscr{I}_2 = \{W_1\}$ if and only if $(0 : R) = 0$.*

(iii) *If* $\operatorname{char}(R) = q > 0$ *then $(q, 0) \in W_1$ and there exists $I \in \mathscr{I}_2$ such that $(q, 0) \in I$.*

Proof. Easy. □

5.4.7 Remark. Let $I \in \mathscr{I}_1$ and let $\pi : S/I$ denote the natural projection. Then $\pi(R^{\triangle}) = (R^{\triangle} + I)/I$ and the mapping $a \mapsto (0, a) + I$ is an isomorphism of R onto $\pi(R^{\triangle})$. Clearly, $\pi(R^{\triangle})$ is an ideal of $\pi(S)$.

If $I \in \mathscr{I}_2$ then $\pi(R^{\triangle})$ is an essential ideal of $\pi(S)$.

If $\mathscr{J}(R) = R$ then $\pi(R^{\triangle}) \subseteq \mathscr{J}(\pi(S))$.

5.5 Consider the situation from 5.1 and 5.4 and, moreover, assume that $(0 : R) = 0$.

5.5.1 Lemma. (i) *$W_2 = 0$ and $W_1 \cap R^{\triangle} = 0$.*

(ii) *$W_1 = \mathbb{Z}u$, where $u = (\zeta(R), a) \in W_1$.*

(iii) *$\zeta(R) = 0$ if and only if $W_1 = 0$.*

(iv) *If $p \geq 2$ is a prime then $W_1 \subseteq R^{\triangle} + pS$ if and only if p divides $\zeta(R)$.*

Proof. Easy (use 5.4). □

In the remaining part of 5.5, assume that $\zeta(R) \geq 2$ (e.g., if $\operatorname{char}(R) > 0$). Let $\zeta(R) = p_1^{r_1} \dots p_s^{r_s}$, where $p_1, \dots p_s$ are primes, $p_1 < p_2 < \dots < p_s$, and $s, r_1, \dots, r_s$ are positive integers. Also, put $t = p_1 p_2 \dots p_s$ and $S_1 = S/W_1$.

5.5.2 Lemma. (i) *$S/(R^{\triangle} + W_1) \simeq \mathbb{Z}_{\zeta(R)}$.*

(ii) *If $\mathscr{J}(R) = R$ then $S_1/\mathscr{J}(S_1) \simeq \mathbb{Z}_t$.*

Proof. Easy (use 5.1.2 and 5.5.1(iv)). □

5.5.3 Corollary. *Assume that $\mathscr{J}(R) = R$. Then $\mathscr{J}(S_1) = (R^\triangle + W_1)/W_1(\simeq R)$ if and only if $\zeta(R) = t$ (i.e., $\zeta(R)$ is squarefree).* □

5.6 Consider the situation from 5.1, 5.4 and 5.5 and, moreover, assume that R is a domain.

5.6.1 Lemma. (i) *W_1 is a prime ideal of S.*

(ii) *$S_1 = S/W_1$ is a domain.*

(iii) *If $\mathscr{J}(R) = R$ then $(R \simeq)(R^\triangle + W_1)/W_1 \subseteq \mathscr{J}(S_1)$.*

(iv) *If $\mathscr{J}(R) = R$ and $\zeta(R) = t$ then $(R^\triangle + W_1)/W_1 = \mathscr{J}(S_1)$.*

Proof. (i) Let $(m,a),(n,b) \in S$ be such that $(m,a)(n,b) \in W_1$ and $(m,a) \notin W_1$. Then $0 = n(mx + ax) + b(mx + ax)$ and $0 = (ny + by)(mx + ax)$ for all $x, y \in R$. Now, since $(m,a) \notin W_1$ and R is a domain, we have $(n,b) \in W_1$.

The remaining assertions are clear from (i) and 5.5. □

5.6.2 Lemma. *If* $\operatorname{char}(R) = q > 0$ *then* $\zeta(R) = t = q$. Moreover, if $\mathscr{J}(R) = R$ *then* $(R \simeq)(R^\triangle + W_1)/W_1 = \mathscr{J}(S_1)$.

Proof. By 1.15, q is a prime number. □

5.7 Summary. We shall say that a ring S is a *unitary envelope* of a ring R if R is a subring of S, S has a unit and $S = R + \mathbb{Z} \cdot 1_S$. Moreover, such a unitary envelope S will be called *essential* if R is an essential ideal of S.

5.7.1 Proposition. *Let R be a ring. Then:*

(i) *The Dorroh extension $\mathbb{D}(R)$ is a unitary envelope of its subring $R^\triangle = \alpha(R)$, $\alpha : R \to \mathbb{D}(R)$ being the natural injection.*

(ii) *$\mathbb{D}(R)$ is an essential unitary envelope of $R^\triangle$ if and only if $Z(R) = 0$* (see 1.16) *(i.e., for every positive integer m and every element $a \in R$ there exists at least one $b \in R$ with $mb \notin ab$).*

(iii) *$\mathscr{J}(\mathbb{D}(R)) = \mathscr{J}(R^\triangle)$ and $\mathscr{N}(\mathbb{D}(R)) = \mathscr{N}(R^\triangle)$.*

(iv) *If $\mathscr{J}(R) = R$ then $\mathscr{J}(\mathbb{D}(R)) = R^\triangle$.*

(v) *The set $\mathscr{I}$ of ideals I of $\mathbb{D}(R)$ maximal with respect to $I \cap R^\triangle = 0$ is non-empty and if $I \in \mathscr{I}$ then $\mathbb{D}(R)/I$ is an essential unitary envelope of $(R^\triangle + I)/I(\simeq R)$*

(vi) *If S is a unitary envelope of R then R is an ideal of S and there exists a uniquely determined projective homomorphism $\psi : \mathbb{D}(R) \to S$ such that $\psi(1) = 1$ and $\psi\alpha = \mathrm{id}_R$. Moreover, S is an essential unitary envelope of R if and only if $\operatorname{Ker}(\psi) \in \mathscr{I}$.*

Proof. (i) See 5.1.9(i), (ii).

(ii) See 5.4.6(i).

(iii) See 5.1.9(iii).

(iv) This assertion follows immediately from (iii).
(v) See 5.4.
(vi) See 5.3. □

5.7.2 Proposition. *Let R be a ring such that $(0:R) = 0$. Then:*
(i) *There exists just one ideal W of $\mathbb{D}(R)$ maximal with respect to $W \cap R^{\triangle} = 0$.*
(ii) $W = (0:R^{\triangle})_{\mathbb{D}(R)} = \{(m,a) \mid mx + ax = 0$ *for every* $x \in R\}$.
(iii) $\mathbb{D}(R)/W$ *is an essential unitary envelope of* $(R^{\triangle} + W)/W(\simeq R)$.
(iv) *If $\mathscr{J}(R) = R$ then $(R^{\triangle} + W)/W \subseteq \mathscr{J}(\mathbb{D}(R)/W)$ and the equaliy holds if and only if either $\zeta(R) = 0$ (then $W = 0$) or $\zeta(R) \geq 2$* and *$\zeta(R)$ is a squarefree number.*
(v) *If S is an essential unitary envelope of R then there exists a uniquely determined isomorphism $\varphi : \mathbb{D}(R)/W \to S$ such tat $\varphi\pi\alpha = \mathrm{id}_R$, $\alpha : R \to \mathbb{D}(R)$ being the natural injection and $\pi : \mathbb{D}(R) \to \mathbb{D}(R)/W$ the natural projection.*

Proof. (i) and (ii). See 5.5.1(i) and 5.4.1(ii).
(iii) See 5.7.1(v).
(iv) See 5.6.2.
(v) See 5.7.1(vi). □

5.7.3 Proposition. *Let R be a domain. Then:*
(i) $W = (0:R^{\triangle})_{\mathbb{D}(R)} = \{(m,0) \mid mx + ax = 0$ *for every* $x \in R\}$ *is a prime ideal of $\mathbb{D}(R)$ and it is the only ideal of $\mathbb{D}(R)$ maximal with respect to zero intersection with $R^{\triangle}$.*
(ii) *$\mathbb{D}(R)/W$ is a domain, it is an essential unitary envelope of $(R^{\triangle} + W)/W(\simeq R)$ and $\mathbb{D}(R)/(R^{\triangle} + W) \simeq \mathbb{Z}/\mathbb{Z}\zeta(R) = \mathbb{Z}_{\zeta(R)}$.*
(iii) *If $\mathscr{J}(R) = R$ then $(R^{\triangle} + W)/W \subseteq \mathscr{J}(\mathbb{D}(R)/W)$ and the equality holds if and only if either $\zeta(R) = 0$ (then $W = 0$ and $\mathbb{D}(R)$ is a domain) or $\zeta(R) \geq 2$ is a squarefree number.*
(iv) *If* $\mathrm{char}(R) > 0$ *and* $\mathscr{J}(R) = R$ *then* $(R^{\triangle} + W)/W = \mathscr{J}(\mathbb{D}(R)/W)$.
(v) *If S is an essential unitary envelope of R then S is a domain and there exists a uniquely determined isomorphism $\varphi : \mathbb{D}(R)/W \to S$ with $\varphi\pi\alpha = \mathrm{id}_R$ (see 5.7.2(v)).*

Proof. Combine 5.7.2 and 5.6. □

5.7.4 Corollary. *Let R be a domain such that* $\mathrm{char}(R) > 0$ *and* $\mathscr{J}(R) = R$. *Then there exists a domain S with unit such that R is a subring of S and* $R = \mathscr{J}(S)$. □

5.7.5 Proposition. *Let R be a ring. Then there exists an essential unitary envelope S of R such that* $\mathrm{char}(R) = \mathrm{char}(S)$.

Proof. Combine 5.7.1(v) and 5.4.6(iii). □

6. The Dorroh extension – examples

6.1 EXAMPLE. Consider the following two-element ring $R = \{0,a\}$:

$+$	0	a
0	0	a
a	a	0

$.$	0	a
0	0	0
a	0	0

Then R is a zero multiplication ring, $R(+) \simeq \mathbb{Z}_2(+)$, $\mathcal{J}(R) = R$, $R \simeq \mathcal{J}(\mathbb{Z}_4)$, $\operatorname{char}(R) = 2$ and $(0:R) = R$. Moreover:

(i) $W_2 = \{(0,0),(0,a)\}$ and $W_1 = \{(2k,0),(2k,a) \mid k \in \mathbb{Z}\}$ (see 5.4).

(ii) $\mathcal{J}_2 = \{\mathbb{Z}(2,0), \mathbb{Z}(2^k,a) \mid k \geq 1\}$ (see 6.4).

(iii) $\operatorname{card}(S_0) = 4$, where $S_0 = \mathbb{D}(R)/\mathbb{Z}(2,0)$, $\operatorname{char}(S_0) = 2$, $\mathcal{J}(S_0) \simeq R$ and $\mathbb{D}(R)/(R^{\triangle} + \mathbb{Z}(2,0)) \simeq \mathbb{Z}_2$.

(iv) $\operatorname{card}(S_k) = 2^{k+1}$, where $S_k = \mathbb{D}(R)/\mathbb{Z}(2^k,a)$, $k \geq 1$, $\operatorname{char}(S_k) = 2^{k+1}$, $\operatorname{card}(\mathcal{J}(S_k)) = 2^k$ and $\mathbb{D}(R)/(R^{\triangle} + \mathbb{Z}(2^k,a)) \simeq \mathbb{Z}_{2^k}$.

(v) $S_1 \simeq \mathbb{Z}_4$.

6.2 EXAMPLE. Consider the following four-element ring $R = \{0,a,2a,3a\}$:

$+$	0	a	$2a$	$3a$
0	0	a	$2a$	$3a$
a	a	$2a$	$3a$	0
$2a$	$2a$	$3a$	0	a
$3a$	$3a$	0	a	$2a$

$.$	0	a	$2a$	$3a$
$+$	0	0	0	0
a	0	$2a$	0	$2a$
$2a$	0	0	0	0
$3a$	0	$2a$	0	$2a$

Then $R(+) \simeq \mathbb{Z}_4(+)$, $\mathcal{J}(R) = R$, $R \simeq \mathcal{J}(\mathbb{Z}_8)$, $\operatorname{char}(R) = 4$ and $(0:R) = \{0,2a\}$. Moreover:

(i) $W_2 = \{(0,0),(0,2a)\}$ and $W_1 = \{(4k,0), (4k,2a),(2+4k,a),(2+4k,3a) \mid k \in \mathbb{Z}\}$ (see 5.4).

(ii) $\mathcal{J}_2 = \{\mathbb{Z}(4,0), \mathbb{Z}(2,a), \mathbb{Z}(2,3a), \mathbb{Z}(2^k,2a) \mid k \geq 3\}$ (see 5.4).

(iii) $\mathbb{D}(R)/\mathbb{Z}(2,a) \simeq \mathbb{Z}_8 \simeq \mathbb{D}(R)/\mathbb{Z}(2,3a)$ (and $R \simeq \mathcal{J}(\mathbb{Z}_8)$, $\operatorname{char}(\mathbb{Z}_8) = 8$).

(iv) $\operatorname{card}(S_k) = 2^{k+2}$, where $S_k = \mathbb{D}(R)/\mathbb{Z}(2^k,2a)$, $k \geq 3$, $\operatorname{char}(S_k) = 2^{k+1}$, $\operatorname{card}(\mathcal{J} S_k)) = 2^{k+1}$ and $\mathbb{D}(R)/(R^{\triangle} + \mathbb{Z}(2^k,2a)) \simeq \mathbb{Z}_{2^k}$.

(v) $\operatorname{card}(S_0) = 16$, where $S_0 = \mathbb{D}(R)/\mathbb{Z}(4,0)$, $\operatorname{char}(S_0) = 4$, $\operatorname{card}(\mathcal{J}(S_0)) = 8$ and $\mathbb{D}(R)/(R^{\triangle} + \mathbb{Z}(4,0)) \simeq \mathbb{Z}_4$.

(vi) There exists no ring A (whether commutative or non-commutative) with unit such that $4A = 0$ and $\mathcal{J}(A) \simeq R$.

Let, on the contrary, $\mathcal{J}(A) = R$ and $K = \{x \in A \mid 2x = 0\}$. Then K is an ideal of A, $2A \subseteq K$ and $K \cap R = \{0,2a\}$. Moreover, if I is a maximal left ideal of A then $M = A/I$ is a simple left A-module, $4M = 0$ and $2M$ is a proper submodule of M. Consequently, $2M = 0$ and $2A \subseteq I$. Thus $2A \subseteq \mathcal{J}(A) = R$ and $2A \subseteq K \cap R = \{0,2a\}$. Now, for every $u \in A$, either $2u = 0$ and $u \in K$ or

$2u = 2a$ and $u \in K + a$. It follows that $\operatorname{card}(A/K) = 2$, K is a maximal left ideal of A and $R = \mathscr{J}(A) \subseteq K$, a contradiction.

6.3 Remark. (i) Let R be a ring such that $\mathscr{N}(R) = 0$, R has not a unit element and $m = \zeta(R) > 0$ (see 1.6). Further, assume that R is a subring of a ring A (possibly non-commutative) with unit and $\mathscr{J}(A) = R$. Put $\alpha = m \cdot 1_A + a \in A$, where $a \in R$ is such that $mx + ax = 0$ for every $x \in R$. The set $I = A\alpha A$ is a (two-sided) ideal of A and $IR = 0 = RI$. Consequently, $(I \cap R)^2 = 0$ and, since $\mathscr{N}(R) = 0$, it follows that $I \cap R = 0$. Further, since R has not a unit element, we have $m \geq 2$ and $m = p_1^{r_1} \dots p_s^{r_s}$, where $p_1 < p_2 < \dots < p_s$ are primes and $s, r_1, \dots, r_s$ positive integers. Now, assume that $I = 0$ (i.e., $\alpha = 0$). We claim that $r_1 = \dots = r_s = 1$ (i.e., m is squarefree).

Indeed, let K be a maximal left ideal of A. Then $R \subseteq K$, A/K is a simple left A-module and $m(A/K) = 0$ (since $m \cdot 1_A = -a \in K$). It follows that $p_i(A/K) = 0$ for some i, $1 \leq i \leq s$, and then $p_i A \subseteq K$ and $m_1 A \subseteq K$, where $m_1 = p_1 p_2 \dots p_s$. Consequently, $m_1 A \subseteq \mathscr{J}(A) = R$, $m_1 \cdot 1_A = b \in R$, $m_1 x - bx = 0$ for every $x \in R$ and m divides m_1. Thus $m = m_1$.

(ii) Let R be a ring such that $\mathscr{N}(R) = 0$, R has not a unit element and $m = \zeta(R) > 0$. If R is a subring of a (possibly non-commutative) ring A with unit such that $\mathscr{J}(A) = R$ then either m is squarefree or $I \cap R = 0$ for a non-zero ideal I of A (i.e., R is not an essential ideal of A). In the latter case, $I \subseteq (0 : R) = (0 : \mathscr{J}(A)) \neq 0$ and A is not a prime ring.

6.4 Proposition. *The following conditions are equivalent for a ring R:*

(i) *R is a domain, $\mathscr{J}(R) = R$ and either $\zeta(R) = 0$ or $\zeta(R) \geq 2$ is a squarefree number (e.g.,* $\operatorname{char}(R) > 0$*).*

(ii) *$R \simeq \mathscr{J}(A)$ for a domain A with unit.*

(iii) *There exists an essential unitary envelope S of R such that $R = \mathscr{J}(S)$ and S is a domain.*

Proof. Combine 5.7.3 and 6.3(ii). □

6.5 Example. Let $k \geq 2$ be an integer and let R be the set of rational numbers $\frac{kn}{m}$, $n, m \in \mathbb{Z}$, m odd. Then R is a subring of $\mathbb{Q}$, R is a domain, $\mathscr{J}(R) = R$ and $\zeta(R) = k$ (cf. 6.4).

7. Radical rings – introduction

7.1 Proposition. *The following conditions are equivalent for a ring R:*

(i) *$R(\circ)$ is a group (i.e., $\mathscr{L}(R) = R$).*

(ii) *For every $a \in R$ there exists $b \in R$ such that $a + b + ab = 0$ (or $a + b = -ab$).*

(iii) *For every $a \in R$ there exists $b \in R$ such that $a - b + ab = 0$ (or $a - b = -ab$).*

(iv) *For every* $a \in R$ *there exists* $b \in R$ *such that* $a - b - ab = 0$ *(or* $a - b = ab$*).*

(v) *For every* $a \in R$ *there exists* $b \in R$ *such that* $a + b - ab = 0$ *(or* $a + b = ab$*).*

(vi) $\mathscr{J}(R) = R$.

(vii) *There exists a ring* S *such that* $R \simeq \mathscr{J}(S)$ *(a ring isomorphism).*

(viii) *There exists a ring* S *with unit element such that* $R = \mathscr{J}(S)$ *(and* $S = R + \mathbb{Z} \cdot 1_S$*).*

(ix) *No homomorphic image of* R *is a field.*

(x) $R^2 \subseteq K$ *for every maximal ideal* K *of* R.

Proof. See 2.1(iv), 2.11, 3.5, 4.3(ii) and 5.7.1(iv). □

A ring R satisfying the equivalent conditions of 7.1 is said to be a *radical ring*. The group $R(\circ)$ is called the *adjoint* (or *circle*) *group* of R.

7.2 Proposition. *The class of radical rings is closed under forming factor-rings, direct sums and direct products.*

Proof. Obvious. □

7.3 Proposition. *Every non-zero ideal of a radical ring is again a radical ring.*

Proof. Obvious. □

7.4 Proposition. *Every nil-ring is a radical ring.*

Proof. See 4.4. □

7.5 Proposition. *Let* R *be a ring such that either* R *is a nil-ring or* $R(\circ)$ *is a torsion group. Then every subring of* R *is a radical ring.*

Proof. Use 2.10. □

7.6 Remark. The class of radical rings is not closed under taking subrings. For example, consider the radical domain R from 6.5 (where $k = 2$). Then R contains the ring $\mathbb{Z}2$ of even integers as a subring. Clearly, $\mathbb{Z}2$ is not a radical ring.

7.7 Lemma. *The only idempotent element of a radical ring is 0.*

Proof. See 2.6. □

7.8 Corollary. *No radical ring has the unit element.* □

7.9 Lemma. *Let* R *be a radical ring. Then* $ab \neq a$ *for all* $a, b \in R$, $a \neq 0$.

Proof. See 2.7. □

7.10 Lemma. *Let* I *be a finitely generated ideal of a radical ring* R. *If* $I^2 = I$ *then* $I = 0$.

Proof. Combine 1.2 and 7.7. □

7.11 Proposition. *Let R be a finitely id-generated radical ring. Then either R is nilpotent or $R^n \neq R^{n+1}$ for every $n \geq 1$.*

Proof. Assume that $R^m = R^{m+1} = I$ for some $m \geq 1$. Then I is a finitely generated ideal and $I^2 = I$. By 7.10, $I = 0$ and R is nilpotent. $\square$

7.12 Corollary. *Every finite radical ring is nilpotent.* $\square$

7.13 Remark. Examples of non-nilpotent finitely id-generated radical rings are given in 9.11 and 11.1.

7.14 Lemma. *Let I be an ideal of a radical ring R. Then:*

(i) *If I is a maximal ideal then $R^2 + pR \subseteq I$ and $(R/I)(+) \simeq \mathbb{Z}_p(+)$ for a prime p.*

(ii) *If I is a minimal ideal then $I \subseteq (0 : R)$ and $I(+) \simeq \mathbb{Z}_p(+)$ for a prime p.*

Proof. (i) See 3.6.

(ii) Assume that I is minimal and $Ra \neq 0$ for some $a \in I$. Since $Ra \subseteq I$, we have $Ra = I$ and $\tilde{a} = ba$ for some $b \in R$. Now, $0 = a + ab + a^2b = a + a(b + ab) = a + ac$, where $c = b + ab$. Further, $0 = 0\tilde{a} = (a + ac)\tilde{c} = a\tilde{c} + ac\tilde{c}$ and $0 = a(c + \tilde{c} + c\tilde{c}) = ac + a\tilde{c} + ac\tilde{c}$. Thus $ac = 0 = a + ac$ and $a = 0$, a contradiction. $\square$

7.15 Corollary. *A ring R has non maximal ideal if and only if R is a radical ring such that $R^2 + pR = R$ for every prime number p.* $\square$

7.16 Example. (i) Let R be a radical ring such that $R^2 = R$ (see e.g. 9.5(ii), 9.6(ii), 9.7(ii)). Then R has no maximal ideal.

(ii) Let S be a zero multiplication ring whose additive group $S(+)$ is divisible. Again, S is a ring without maximal ideals.

(iii) Put $T = R \times S$. Then $0 \neq T^2 \neq T$ and the ring T has no maximal ideals.

7.17 Lemma. *Let $\mathscr{R}$ be a non-empty family of radical subrings of a radical ring R. If $S = \bigcap \mathscr{R} \neq 0$ then S is a subring of R and a radical ring.*

Proof. Obvious. $\square$

7.18. Remark. Let R be a radical ring and A a subset of R. We will say that R is *rd-generated* by A if $S = R$ whenever S is a radical subring of R with $A \nsubseteq S$. Notice that if R is finitely rd-generated then it is finitely id-generated.

7.19 Proposition. *The following conditions are equivalent for a ring R:*

(i) *R is a radical ring and no proper subring of R is a radical ring.*

(ii) *R is a simple radical ring.*

(iii) *R is a radical ring containing no proper subrings.*

(iv) *$R^2 = 0$ and $R(+) \simeq \mathbb{Z}_p(+)$ for a prime p.*

Proof. Easy (use 1.20 and 3.1). $\square$

7.20. Lemma. *The following conditions are equivalent for a ring R and $n \geq 2$:*
(i) *R is nilpotent of index n.*
(ii) $R^n = 0 \neq R^{n-1}$.
(iii) $(0 : R^{n-1}) = R \neq (0 : R^{n-2})$.
(iv) $(0 : R^i) \neq (0 : R^{i+1})$ *for every* $i = 1, 2, \ldots, n-2$ *and* $(0 : R^{n-1}) = (0 : R^n) = \\ = \ldots = R$.

Proof. Easy to check. □

7.21 Proposition. *Let R be a nilpotent ring and $\mathscr{A}$ be an abstract class of abelian groups closed under taking subgroups, factorgroups and extensions* (the latter means that an abelian group A is in $\mathscr{A}$, provided that it contains a subgroup B such that both B and A/B are in $\mathscr{A}$). *Then the additive group $R(+)$ belongs to $\mathscr{A}$ if and only if the same is true for the adjoint group $R(\circ)$.*

Proof. We proceed by induction on the nilpotence index $n \geq 2$ of R. If $n = 2$ then $R^2 = 0$, $R(+) = R(\circ)$ and there is nothing to show. Consequently, let $n \geq 3$, $I = (0 : R)$, $S = R/I$ and let $\pi : R \to S$ denote the natural projection. Then S is a ring nilpotent of index at most $n - 1$, $\pi : R(+) \to S(+)$ and $\pi : R(\circ) \to S(\circ)$ are projective group homomorphisms and $I(+) = I(\circ)$ is the joint kernel of these homomorphism. The rest is clear. □

7.22 Proposition. *Let R be a nilring and $\mathscr{A}$ be an abstract class of abelian groups closed under taking subgroups, factorgroups and extensions such that an abelian group A belongs to $\mathscr{A}$, provided that every finitely generated subgroup of A is in $\mathscr{A}$. Then the additive group $R(+)$ belongs to $\mathscr{A}$ if and only if the same is true for the adjoint group $R(\circ)$.*

Proof. Let M be a finite subset of R such that M contains at least one non-zero element and let B, C and S denote te subgroups and the subring of $R(+)$, $R(\circ)$ and R, respectively, generated by the set M. Clearly, $B \subseteq S$, $C \subseteq S$ and S is nilpotent. Now, if $R(+) \in \mathscr{A}$ then $S(+) \in \mathscr{A}$, $S(\circ) \in \mathscr{A}$ by 7.21 and we conclude that $R(\circ) \in \mathscr{A}$. Similarly the converse. □

7.23 Lemma. *Let R be a radical subring of a ring S with unit and let Q be a subring of S such that Q is a field and $1_S \in Q$. If $R_1 = R \cap Q \neq 0$ then R_1 is a subring of Q and R_1 is a radical domain.*

Proof. If $a \in R_1$ then $b = 1_S + a \in Q$ and $c = \tilde{a} \in R$. We have $0 = a + c + \\ + ac = a + bc$ and $bc = -a$. If $b = 0$ then $a = 0$ and $c = 0 \in R_1$. If $b \neq 0$ then $b^{-1} \in Q$ and $c = -ab^{-1} \in Q$. Thus $\tilde{a} = c \in R_1$. □

7.24 Lemma. *Let a field F be an algebraic extension of a field Q and let R be a radical subring of F. Then $R_1 = R \cap Q \neq 0$, R_1 is a subring of Q and R_1 is a radical domain.*

Proof. Since F is algebraic over Q, we have $R \cap Q \neq 0$ and 7.23 applies. □

8. Subrings of radical rings

8.1 Construction. Let R_1 be a subring of a ring S_1 with unit $1 = 1_{S_1}$ such that $1_{S_1} \notin R_1$. The set $A = 1 + R_1$ is a subsemigroup of the multiplicative semigroup $S_1(\cdot)$ and $0 \notin A$. Now, consider the corresponding ring of quotients $S = S_1A^{-1}$; we have $S = \{r/(1 + a)\} \mid r \in S_1, a \in A\}$ and $r/(1 + a) = s/(1 + b)$ iff $(r(1 + b) - - s(1 + a))(1 + c) = 0$ for some $c \in A$. Put also $R = R_1A^{-1} = \{a/(1 + b) \mid \mid a, b \in R_1\}$.

8.1.1 Lemma. *S is a ring with unit, R is a subring of S (or $R = 0$) and $1_S \notin R$.*

Proof. Easy to check. □

8.1.2 Lemma. (i) *The mapping $\varphi : S_1 \to S$, where $\varphi(r) = r/1$, is a ring homomorphism of S_1 into S and $\varphi(1_{S_1}) = 1_S$.*

(ii) $\operatorname{Ker}(\varphi) = \{r \in S_1 \mid r(1 + a) = 0$ *for some* $a \in R_1\} = \bigcup_{a\in R_1}(0 : 1 + a)_{S_1}$.

(iii) *φ is injective if and only if $(0 : 1 + a)_{S_1} = 0$ for every $a \in R_1$.*

(iv) *$\varphi \mid R_1$ is injective if and only if $ab \neq a$ for all $a, b \in R_1$, $a \neq 0$.*

(v) *$R \neq 0$ and only if $\varphi(R_1) \neq 0$ and if and only if there exists at least one $a_1 \in R_1$ such that $a_1 \neq a_1b$ for every $b \in R_1$.*

Proof. Easy to check. □

8.1.3. Lemma. *Let $a, b \in R_1$, $u = a/(1 + b)$ and $v = (-a)/(1 + a + b)$, $u, v \in R$. Then $u \circ v = u + v + uv = 0$.*

Proof. Easy to check. □

8.1.4 Lemma. *If $R \neq 0$ (see 8.1.2(v)) then R is a radical ring.*

Proof. The assertion follows from 8.1.3. □

8.1.5 Lemma. *If R_1 is a radical ring then $\varphi \mid R_1$ is injective and R is a radical ring.*

Proof. $\varphi \mid R_1$ is injective by 7.9 and 9.1.2(iv), and hence $R \neq 0$ (we have $\varphi(R_1) \subseteq R$). Then R is a radical ring by 8.1.4. □

8.1.6 Lemma. *If $R_1 \subseteq \mathcal{J}(S_1)$ then $A \subseteq S_1^*$ and $S_1 \simeq S$. Moreover, if R_1 is an ideal of S_1 then $\varphi \mid R_1 : R_1 \to R$ is a ring isomorphism.*

Proof. Easy to see. □

8.1.7 Lemma. *If R_1 is a domain without unit then $\varphi \mid R_1$ is injective and R is a radical domain.*

Proof. $\varphi \mid R_1$ is injective by 8.1.2(iv), and hence $R \neq 0$. By 8.1.4, R is a radical ring and it is easy to check that R is a domain. □

8.1.8 Lemma. *If R_1 has the unit element then $\varphi(R_1) = 0$.*

Proof. Obvious. $\square$

8.2 Proposition. *The following conditions are equivalent for a ring R:*

(i) *R is a subring of a radical ring.*

(ii) *$ab \neq a$ for all $a, b \in R$, $a \neq 0$.*

(iii) *The adjoint semigroup $R(\circ)$ is cancellative.*

Proof. (i) implies (ii) by 7.9, (ii) is equivalent to (iii) by 2.1(vi) and (vi) implies (i) by 8.1.2(iv) and 8.1.4. $\square$

8.3 Proposition. *Every domain without unit is a subring of a radical domain.*

Proof. See 8.1.7. $\square$

8.4 Example. The ring $2\mathbb{Z}$ of even integers is a finitely generated domain without unit, but it is not a radical domain.

9. Radical rings – examples

9.1 Example. (i) Every nil-ring is a radical ring. Consequently, every nilpotent ring and, in particular, every zero multiplication ring is a radical ring.

(ii) Let p be a prime and $\mathbb{Q}_p = \{\frac{m}{p^k} \mid m,\ k \in \mathbb{Z},\ k \geq 0\} \subseteq \mathbb{Q}$. Then $\mathbb{Q}_p(+)$ is a subgroup of $\mathbb{Q}(+)$ and if R is a zero multiplication ring with $R(+) \simeq \mathbb{Q}_p(+)$ then R is a radical ring and $R(+)$ is a torsionfree group of rank 1.

9.2 Example. (i) Let S be a subring of a field Q such that $Q = \{ab^{-1} \mid a, b \in S,\ b \neq 0\}$ (i.e., Q is a quotient field of S). Let R be a subring of Q such that $1 \notin R$ and $a(a+b)^{-1} \in R$ whenever $a, b \in S$, $b \neq 0$ and $ab^{-1} \in R$ (since $1 \notin R$, we have $a + b \neq 0$). Then $ab^{-1} - a(a+b)^{-1} - a^2(ab + b^2)^{-1} = 0$, and hence R is a radical ring.

(ii) Let S be a unique factorization domain with the unit element, not a field, and let $q \in S$ be an irreducible element. Denote by R the set of all $ab^{-1} \in Q$ such that $a, b \in S$, $a \in Sq$ and $b \in S \setminus Sq$. Then R is a subring of Q and R is a radical domain (see (i)). Moreover, $q \in R \setminus R^2$, and so $R \neq R^2$.

(iii) Choose $S = \mathbb{Z}$ and $Q = \mathbb{Q}$. Then $q \in \mathbb{Z}$ is any prime number and $R(+)$ is a torsionfree group of rank 1. Moreover, R is a radical domain, $R \neq R^2$, $(0 : R) = 0$, $R(\circ) \simeq \mathbb{Z}_2(+) \times \mathbb{Z}(+)^{(\omega)}$ for $q = 2$ and $R(\circ) \simeq \mathbb{Z}(+)^{(\omega)}$ for $q \geq 3$.

9.3 Example. (i) Every non-zero proper ideal of a local ring with unit is a radical ring.

(ii) Let F be a field and S the corresponding semigroup ring of the additive semigroup $\mathbb{Q}^+(+)$ of positive rationals over F (the addition on S will be denoted by $\oplus$ to avoid a confusion). Every non-zero element $a \in S$ can be written in a (normal) formal as $a = \alpha_0 r_0 \oplus \ldots \oplus \alpha_m r_m$, where $m \geq 0$, $\alpha_i \in F \setminus \{0\}, r_i \in \mathbb{Q}^+$ and $r_0 < r_1 < \ldots < r_m$. Using this, it follows easily that S is a domain and $P = \{a \in S \mid a = 0 \text{ or } a \neq 0, r_0 \neq 0_{\mathbb{Q}}\}$ is a prime ideal of S. Now, $R_1 = (S \setminus P)^{-1} S$ (the corresponding quotient ring) is a uniserial domain, not a field, and $R = (S \setminus P)^{-1} P$ is a unique maximal ideal of R_1. Clearly, R is a radical domain, $R^2 = R$ and $(0 : R) = 0$.

(iii) Let I be a non-zero proper principal ideal of the ring R_1 (see (ii)). Then $I \subseteq R$ and $IR \neq I$ (since $R = \mathcal{J}(R_1)$). Now, if $R_2 = R/IR$ the R_2 is a radical ring, $R_2^2 = R_2$ and $(0 : R_2) \neq 0$.

9.4 Example. Let $p \geq 2$ be a prime number and A a non-trivial commutative semigroup (denoted multiplicatively) containing the absorbing (alias zero) element 0 such that $a^p = 0$ for every $a \in 0$ for every $a \in A$ (such a semigroup will be called *p-zeropotent*). Denote by R the corresponding contracted semigroup ring of A over the p-element field $\mathbb{Z}_p$ of integers modulo p. Every non-zero element $r \in R$ can be expressed as a sum $r = k_1 a_1 + \ldots + k_n a_n$, where $n \geq 1$, $1 \leq k_i \leq p - 1$, and a_i are pair-wise different elements from $A \setminus \{0\}$. The ring R is of characteristic p, and hence $(r + s)^p = r^p + s^p$ for all $r, s \in R$. Using this, it follows easily that, in fact, $r^p = 0$ for every $r \in R$. In particular, R is a nil-ring, and hence a radical ring, too. Finally, notice that $R^2 = R$, provided that $A = \{ab \mid a, b \in A\}$.

9.5 Example. (i) Let $p \geq 2$ be a prime and F a free commutative semigroup (denoted multiplicatively) with the absorbing element 0 such that F is freely generated by an infinite countable set $\{a_1, a_2, \ldots\}$. Let ϱ be the congruence of F generated by the pairs $(a_i, a_{2i} a_{2i+1})$ and $(a_i^p, 0)$, $i \geq 1$. It is easy to check that $(a_j, a_k) \neq \varrho$ for $j \neq k$, and hence $A = F/\varrho$ is an infinite commutative p-zeropotent semigroup. Moreover, $A = \{ab \mid a,\ b \in A\}$.

(ii) Consider the radical ring R corresponding to A by 9.4. Then $R^2 = R$ and $r^p = 0 = pr$ for every $r \in R$.

9.6 Example. (i) Let $p \geq 2$ be a prime and A a non-trivial commutative p-zeropotent semigroup. Further, let B denote a commutative semigroup with absorbing element such that B is freely generated by the set $\{(m,a) \mid a \in A \setminus \{0\}, m \in \mathbb{Z},\ m \geq 1\}$ subject to the defining relations $(m,a)(m,b) = (m,ab)$ for $ab \neq 0$ and $(m,a)(m,b) = 0$ for $ab = 0$. Then $\alpha^p = 0$ for every $\alpha \in B$ and, if $\alpha \neq 0$, then α has a unique expression $\alpha = (m_1, a_1)(m_2, a_2) \ldots (m_k, a_k)$, $k \geq 1$, $a_1, \ldots a_k \in A \setminus \{0\}$, $1 \leq m_1 < m_2 < \ldots < m_k$, and we put $\partial(\alpha) = m_k$.

(ii) Let R be the radical ring corresponding to B by 9.4. Then $r^p = 0 = pr$ for every $r \in R$ and if $r \neq 0$ then $r = t_1 \alpha_1 + \ldots + t_m \alpha_m$, $m \geq 1$, $1 \leq t_i \leq \ \leq p - 1$, $\alpha_i \in B \setminus \{0\}$ pair-wise different, and if $n > \max(\partial(\alpha_i))$ then $(n, a) r \neq 0$ for every $a \in A \setminus \{0\}$. Consequently, $(0 : R) = 0$. Finally, if $A = \{ab \mid a, b \in A\}$ (see 9.5(i)) then $B = \{\alpha\beta \mid \alpha, \beta \in B\}$ and $R^2 = R$.

9.7 Example. (i) Let M be an uncountable set, $\mathscr{M}_c$ the set of infinite countable subsets of M and $\mathscr{M} = \mathscr{M}_c \cup \{M\}$.Define a multiplication on $\mathscr{M}$ by $IK = I \cup K$ if $I \cap K = \emptyset$ and $IK = M$ if $I \cap K \neq \emptyset$. Then $\mathscr{M}$ becomes a commutative 2-zeropotent semigroup and $\mathscr{M} = \{IK \mid I, K \in \mathscr{M}\}$.

(ii) Consider the radical ring R corresponding to $\mathscr{M}$ by 9.4. Then $R^2 = R$ and $r^2 = 0 = 2r$ for every $r \in R$. If $r \neq 0$ then $r = I_1 + \ldots + I_m$, where $m > 1$ and $I_1, \ldots I_m$ are pair-wise different countable subsets of M. Now, there is $I \in \mathscr{M}_c$ with $I \cap (I_1 \cup \ldots \cup I_m) = \emptyset$ and we have $I \cdot r = (I \cup I_1) + \; + \ldots + (I \cup I_m) \neq 0$. Thus $(0 : R) = 0$.

9.8 Example. Let $R = \{0,2,4,6\} \subseteq \mathbb{Z}_8$. Then $R = \mathscr{J}(\mathbb{Z}_8)$, R is a radical ring of characteristic 4, $R(+) \simeq \mathbb{Z}_4(\times)$ is a cyclic group and $R(\circ) \simeq \mathbb{Z}_2(+)^{(2)}$ is not cyclic. Moreover, $R(\circ) \simeq R_1(\circ)$, where R_1 is the zero multiplication ring defined on $\mathbb{Z}_2(+)^{(2)}$. Of course, the radical rings R and R_1 are not isomorphic, Similarly, $R(+) \simeq R_2(+)$, where R_2 is the zero multiplication ring defined on $\mathbb{Z}_4(+)$ and the radical rings R and R_2 are not isomorphic.

9.9 Example. (i) If p is a prime number and $n \geq 2$ then $R(p,n) = \mathscr{J}(\mathbb{Z}_{p^n})$ $(= \{0, p, 2p, \ldots, (p^{n-1} - 1)p\})$ is a radical ring, $R(p,n)(+) \simeq \mathbb{Z}_{p^{n-1}}(+) \simeq$ $\simeq R(p,n)(\circ)$ are cyclic groups for $p \geq 3$, $R(2,2)(+) \simeq \mathbb{Z}_2(+) \simeq R(2,2)(\circ)$, $R(2,n)(+) \simeq \mathbb{Z}_{2^{n-1}}(+)$ is cyclic and $R(2,n)(\circ) \simeq \mathbb{Z}_2(+) \times \mathbb{Z}_{2^{n-2}}(+)$ is not cyclic for $n \geq 3$. Moreover, the ring $R(p,n)$ is nilpotent of index n.

(ii) Let $p_2 < p_3 < p_4 < \ldots$ be the sequence of all primes and let R denote the (ring) direct sum of the rings $R(p_n, n)$, $n \geq 2$ (see (i)). Then R is an (infinite radical) nil-ring, R is not nilpotent, $R(+)$ is a reduced torsion group of Prüfer rank 1 and the same is true for $R(\circ)$.

9.10 Example. Let $T = \mathbb{Z}_2[x]$ (the polynomial ring in one indeterminate x over the field $\mathbb{Z}_2$ of integers modulo 2) and let $S = T[G]$ be the corresponding group ring of a two-element (multiplicative) group $G = \{1, \alpha\}$ over T. Clearly, S is a finitely generated ring (namely by the set $\{1, x, \alpha\}$) and $R = \mathscr{J}(S) =$ $= \{f + \alpha f \mid f \in T\}$ is a zero multiplication ring. Notice that $R(+) \simeq \mathbb{Z}_2(+)^{(\omega)}$ and R is not a finitely generated ring. The multiplicative group S^* is not finitely generated either.

9.11 Example. Let $S_1 = \mathbb{Z}[x]$ be the polynomial ring in one indeterminate x over the ring $\mathbb{Z}$ of integers, $R_1 = S_1 x$ and $T_1 = \mathbb{Q}(x)$. Put $F_1 = \{f/(1 + g) \mid f, g \in R_1\}$. Then F_1 is a subring of T_1 and F_1 is a radical ring; we have $\overline{f/(1 + g)} =$ $= -f/(1 + f + g)$ for all $f, g \in R_1$. Moreover, F_1 is rd-generated (see 7.1.5) by the one-element set $\{x\}$.

Indeed, let P be a radical subring of F_1 such that $x \in P$. To show that $P = F_1$, it is enough to check that $x/(1 + g) \in P$ for every $g \in R_1$ and this is done by induction on $m = \deg(g)$.

The situation is clear for $g = 0$, and so let $g \neq 0$. Then $m \geq 1$ and $g = h + nx^m$, $h \in R_1$, $\deg(h) < m$, $0 \neq n \in \mathbb{Z}$. Now, $x/(1 + h) \in P$ by induction and, since P is a radical ring, $\overline{x/(1 + h)} = -x/(1 + x + h) \in P$. Then, since P is a subring of F_1, $nx^m/(1 + x + h) \in P$ and $(nx^m - x)/(1 + x + h) \in P$. Furthermore, similarly, $(x - nx^m)/(1 + g) = (x - nx^m)/(1 + x + h + nx^m - x) \in P$. On the other hand, $x/(1 + h) \in P$ implies $nx^m/(1 + h) \in P$ and $-nx^m/(1 + g) = -nx^m/(1 + nx^m + h) \in P$. Thus both elements $(x - nx^m)/(1 + g)$ and $nx^m/(1 + g)$ are in P and we conclude that $x/(1 + g) \in P$, too.

9.12 Example. Let T be a ring with unit, $T[x]$ the ring of polynomials in one indeterminate x over T and $R = T[x]x/T[x]x^n$, $n \geq 2$. Then R is a ring nilpotent of index n and $R(+) \simeq T(+)^{(n-1)}$. If $\alpha = x + T[x]x^n \in R$, $m \geq 1$ and $\alpha_m = \alpha \circ \ldots \circ \alpha$ (m-times) then $\alpha_m = \sum_{i=1}^{k} \binom{m}{i} x^i + T[x]\, x^n$, $k = \min(m, n - 1)$. In particular, $\alpha_{n-1} \neq 0$ and $\alpha_n = n(x^{n-1} + x) + \sum_{i=2}^{n-2} \binom{n}{i} x^i + T[x]\, x^n$.

10. Finitely generated radical rings

10.1 Proposition. *Every finitely generated ring is a Hilbert ring.*

Proof. Since finitely generated rings are closed under factor-rings, it is enough to show that $\mathscr{J}(R) = \mathscr{N}(R)$ for every finitely generated ring R (see 4.8).

First, put $S = \mathbb{D}(R)$ (see 5.1). Then $R \simeq R^{\triangle}$, $\mathscr{J}(S) = \mathscr{J}(R^{\triangle})$ and $\mathscr{N}(S) = \mathscr{N}(R^{\triangle})$. Consequently, it suffices to show that $\mathscr{J}(S) = \mathscr{N}(S)$. But S is a finitely generated ring with unit, and so there is $n \geq 0$ such that S is a homomorphic image of the polynomial ring $T = \mathbb{Z}[x_1, \ldots, x_n]$ in n (commuting) indeterminates $x_1, \ldots, x_n$ over the ring $\mathbb{Z}$ of integers. Of course, $\mathbb{Z}$ is a Hilbert ring and this property is known to be preserved by polynomials. Thus T is a Hilbert ring and the same is true for S. □

10.2 Proposition. *Let R be a finitely generated ring. Then $\mathscr{J}(R)$ is nilpotent.*

Proof. By 10.1, $\mathscr{J}(R) = \mathscr{N}(R)$, and so $\mathscr{J}(R)$ is a nil-ring. We have $\mathscr{J}(R) \simeq \mathscr{J}(R^{\triangle})$, $R^{\triangle} \subseteq S = \mathbb{D}(R)$ (see 5.1). Since S is a finitely generated ring with unit, it is a noetherian ring, and therefore $\mathscr{N}(S) = \mathscr{N}(R^{\triangle}) = \mathscr{J}(R^{\triangle})$ is nilpotent. □

10.3 Lemma. *Let a ring R be generated by a non-empty set A. If $S = R^2 \neq 0$ then S is, as a ring, generated by the set $\{ab, abc \mid a, b, c \in A\}$. Consequently, if R is a finitely generated ring and $R^2 \neq 0$ then R^2 is a finitely generated ring.*

Proof. Easy. □

10.4 Proposition. *Every finitely generated radical ring is nilpotent.*

Proof. Let R be a finitely generated radical ring. By 10.1, R is a Hilbert ring, and so $\mathscr{N}(R) = \mathscr{J}(R) = R$. Thus R is a nil-ring and R is nilpotent by 1.12 (or 10.2). □

10.5 Theorem. *The following conditions are equivalent for a radical ring R:*
(i) *The ring R is finitely generated.*
(ii) *The additive group $R(+)$ of R is finitely generated.*
(iii) *The adjoint group $R(\circ)$ of R is finitely generated.*
Moreover, if these conditions are satisfied then R is nilpotent.

Proof. (i) implies (ii). By 10.3, R is nilpotent. Consequently, if A is a non-empty and finite set of elements generating R as a ring then the set $B = \{a_1a_2 \dots a_n \mid n \geq 1, a_i \in A\}$ is also finite. However, $R(+)$ is generated by B.

(i) implies (iii). By 10.3, $R^n = 0$ for some $n \geq 2$. If $n = 2$ then $R(+) = R(\circ)$ and $R(\circ)$ is finitely generated by the preceding part of the proof. If $n \geq 3$ then $S = R^2 \neq 0$, S is an ideal of R and a radical ring, S is a finitely generated ring (see 10.3), $S^{n-1} = 0$ and $S(\circ)$ is a subgroup of $R(\circ)$. Now, $S(\circ)$ is finitely generated (by induction on n) and $R(\circ)/S(\circ) \simeq (R/S)(\circ)$, where $(R/S)^2 = 0$. Consequently, both $S(\circ)$ and $R(\circ)/S(\circ)$ are finitely generated and it follows that $R(\circ)$ is finitely generated, too.

(ii) implies (i). This implication is trivial.

(iii) implies (i). If A is a set generating the adjoint group $R(\circ)$ the $A \cup \tilde{A}$ (where $a \circ \tilde{a} = 0$) generates the ring R. □

10.6 Remark. (i) $R = \mathscr{J}(\mathbb{Z}_8)$ is a radical ring, $R(+) \simeq \mathbb{Z}_4(+)$ is a cyclic group and $R(\circ) \simeq \mathbb{Z}_2(+)^{(2)}$ is not a cyclic group. Moreover, $R^2 \neq 0 = R^3$.

(ii) The ring S from 9.10 is a finitely generated ring with unit such that $\mathscr{J}(S)$ is not a finitely generated ring. In fact, $\mathscr{J}(S)^2 = 0$ and $\mathscr{J}(S)(+)$ is not finitely generated.

(iii) There exist finitely rd-generated (and hence finitely id-generated) radical domains (see 9.11 and 11.1.2). In particular, these rings are not nilpotent.

11. Free radical rings

11.1 Construction.. Let X be a non-epty set of indeterminates over $\mathbb{Z}$, $S_X = \mathbb{Z}[X]$ (the corresponding polynomial ring), $R_X = \sum_{x \in X} S_X x$ (the ideal of S_X generated by X), $T_X = \mathbb{Q}(X)$ (the quotient field of S_X) and $F_X = \{f/(1+g) \mid f, g \in R_X\} \subseteq T_X$.

11.1.1 Lemma. *F_X is a subring of T_X, $R_X \subseteq F_X$ and F_X is a radical domain. Moreover, $\widetilde{f/(1+g)} = -f/(1+f+g)$ for all $f, g \in R_X$.*

Proof. Easy (cf. 8.1.1, 8.1.3 and 8.1.4). □

11.1.2 Lemma. *The radical ring F_X is rd-generated* (see 7.1.8) *by the set X.*

Proof. Let P be a subring of F_X such that $X \subseteq P$ and P is a radical ring. We have to show that $P = F_X$.

First, put $A = P + \mathbb{Z} \cdot 1_T$. Then A is a subring of T_X, A contains the unit element, $P \subseteq A$ and, since P is a radical ring, we have $P \subseteq \mathscr{J}(A)$. Now, let $f, g \in R_X$. Clearly, $R_X \subseteq P$, $f, g \in P$, $g \in \mathscr{J}(A)$ and $1 + g \in A^*$. Consequently, $1/(1 + g) \in A$ and there are $a \in P$ and $n \in \mathbb{Z}$ such that $1/(1 + g) = a + n \cdot 1_T$. Thus $f/(1 + g) = fa + nf \in P$. □

11.1.3 Lemma. *Let R be a radical ring and $\varphi : X \to R$ a mapping. Then there exists a uniquely determined (ring) homomorphism $\xi : F_X \to R$ such that $\xi \mid X = \varphi$.*

Proof. Put $S = \mathbb{D}(R)$. Then there is a (uniquely defined) ring homomorphism $\psi : S_X \to S$ such that $\psi(x) = (0, \varphi(x)) \in R^\triangle$ (see 5.1) for every $x \in X$ and $\psi(1) = 1$. Further, since $1 + R^\triangle \subseteq S^*$, we can define a mapping $\varrho : F_X \to S$ by $\varrho(f/(1 + g)) = \psi(f)(1 + \psi(g))^{-1}$. Then $\psi(R_X) \subseteq R^\triangle$ and, since $R^\triangle$ is an ideal of S, we have $\varrho(F_X) \subseteq R^\triangle$. Clearly, ϱ is a ring homomorphism and $\varrho(x) = (0, \varphi(x))$ for every $x \in X$. Now, $\xi = \iota\varrho : F_X \to R$, $\iota : R^\triangle \to R$ being the natural isomorphism, is a ring homomorphism of F_X into R. Finally, if $\xi_1 : F_X \to R$ is a ring homomorphism such that $\xi_1 \mid X = \varphi$ then the set $A = \{a \in F_X \mid \xi(a) = \xi_1(a)\}$ contains X and, clearly, A is a radical subring of F_X. By 11.1.2, $A = F_X$, and hence $\xi_1 = \xi$. □

11.2 Proposition. *The radical domain F_X is a free radical ring freely rd-generated by the set X.*

Proof. See 11.1. □

11.3 Corollary. *Let R be a radical ring rd-generated by a non-empty set M. Then there exists an ideal I of the radical domain F_X, where* $\operatorname{card}(X) = \operatorname{card}(M)$, *such that R is isomorphic to the factor-ring F_X/I.* □

11.4 Remark. The radical domain F_1 from 9.11 is a free radical ring freely rd-generated by the one-element set $\{x\}$.

11.5 Remark. The class of radical rings (together with zero rings) may be viewed as a primitive class (or variety) of universal algebras. The corresponding signature contains two binary symbols ($+$ and $\cdot$), one unary symbol ($\tilde{}$) and the primitive class is given by the following equations: $\mathbf{x} + \mathbf{y} \doteq \mathbf{y} + \mathbf{x}$, $\mathbf{x} + (\mathbf{y} + \mathbf{z}) \doteq (\mathbf{x} + \mathbf{y}) + \mathbf{z}$, $\mathbf{xy} \doteq \mathbf{yx}$, $\mathbf{x}(\mathbf{yz}) \doteq (\mathbf{xy})\mathbf{z}$, $\mathbf{x}(\mathbf{y} + \mathbf{z}) \doteq \mathbf{xy} + \mathbf{xz}$, $\mathbf{x} \doteq \mathbf{x} + (\mathbf{y} + \tilde{\mathbf{y}} + \mathbf{y}\tilde{\mathbf{y}})$. Free algebras of this primitive class are constructed in 11.1.

12. Subdirectly irreducible radical rings

A ring A is said to be *subdirectly irreducible* if the set of non-zero ideals of R has the smallest element. If M is the smallest non-zero ideal of R then M is called *the monolith* (or *the heart*) of R and denoted by $M = \mathscr{M}(R)$.

12.1 Proposition. *Let R be a subdirectly irreducible radical ring and $M = \mathscr{M}(R)$. Then:*

(i) $M \subseteq (0:R)$ *and* $M^2 = 0$.

(ii) $M(+) \simeq \mathbb{Z}_p(+)$ *fo a prime p (in particular, M is finite).*

(iii) $M \subseteq \mathbb{Z}a$ *for every* $a \in (0:R)$, $a \neq 0$.

(iv) $M \subseteq Ra$ *for every* $a \in R \setminus (0:R)$.

(v) $(0:R) \subseteq T$, *where T is the torsion part of* $R(+)$.

(vi) $T(+)$ *is a p-group and* $(0:R)(+) \simeq \mathbb{Z}_{p^n}(+)$, $1 \leq n \leq \infty$.

Proof. (i) and (ii). See 7.14.

(iii) and (iv). Obvious.

(v) and (vi). Denote $I = (0:R)$. Then every subgroup of $I(+)$ is an ideal of R, and hence $I(+)$ is a subdirectly irreducible abelian group. Thus $I(+) \simeq \mathbb{Z}_{p^n}(+)$, $1 \leq n \leq \infty$, and $I \subseteq T$. Further, if q is a prime number then $J = \{a \in T \mid qa = 0\}$ is an ideal of R. Consequently, either $J = 0$ or $M \subseteq J$ and $q = p$. Thus $T(+)$ is a p-group. □

12.2 Proposition. *Let R be a radical ring and $a \in R$, $a \neq 0$. Then set $\mathscr{A}$ of ideals J such that $a \notin J$ is non-empty and upwards-inductive. If $K \in \mathscr{A}$ is maximal in $\mathscr{A}$ then $S = R/K$ is a subdirectly irreducible radical ring, $\mathscr{M}(S) = (K + Ra)/K$ if $Ra \nsubseteq K$ and $\mathscr{M}(S) = (K + \mathbb{Z}a)/K$ if $Ra \subseteq K$.*

Proof. Easy to check. □

12.3 Proposition. *Every radical ring R is isomorphic to s subring of the cartesian product of subdirectly irreducible factor-rings of R.*

Proof. For every $a \in R$, $a \neq 0$, choose an ideal K_a maximal with respect to $a \notin K_a$ (see 12.2). Then R/K_a are subdirectly irreducible radical rings, $\bigcap K_a = 0$ and R imbeds into $\prod R/K_a$. □

References

[1] Amberg, B. and Dickenscheid, O., *On the adjoint group of a radical ring*, Canad. Math. Bull. **38** (1995), 262–270.

[2] Amberg, B., Dickenscheid, O. and Sysak, Ya. P., *Subgroups of the adjoint group of a radical ring*, Canad. J. Math **59** (1988), 3–15.

[3] Amberg, B., Franciosi, S. and de Giovanni, F., *Products of Groups*, Oxford Mathematical Monographs, Clarendon Press, Oxford, 1992.

[4] Amberg, B. and P. Sysak, Ya. P., *Radical rings and their adjoint groups*, In: M. Curzio, F. de Giovanni (eds), Topics in Infinite Groups, Quaderni di Mat. **8** (2001), 21–44.

[5] Ault, J. C. and Watters, J. F., *Circle groups of nilpotent rings*, Amer. Mat. Monthly **80** (1973), 48–52.

[6] Dickenscheid, O., *On the adjoint group of some radical rings*, Glasgow Math. J. **39** (1997), 35–41.

[7] Dorroh, J. L., *Concerning adjunctions to algebras*, Bull. Amer. Math. Soc. **38** (1932), 85–88.

[8] HEATHERLY, H. E., *Adjoint groups and semigroups of rings*, Riv. Mat. Pura Appl. **6** (1990), 105 – 108.
[9] ———, *Adjoint groups of radical rings*, Riv. Mat. Univ. Parma (6) **2** (1999), 35 – 68.
[10] JACOBSON, N., *The radical and semi-simplicity for arbitrary rings*, Amer. J. Math. **67** (1945), 300 – 320.
[11] KALOUJNINE, L., *Zum Problem der Klassification der endlichen metabelschen p-Gruppen*, Wiss. Z. Humbold Univ. Berlin Math. Nat. Reihe **4** (1955), 1 – 7.
[12] KRUSE, R., L., *A note on the adjoint group of a finitely generated radical ring*, J. London Math. Soc. (2) **1** (1969), 743 – 744.
[13] MCCOY, N., *The Theory of Rings*, Chelsea Pub. Co., New York, 1973.
[14] WATTERS, F., *On the adjoint grup of a radical ring*, J. London Math. Soc. **43** (1968), 725 – 729.
[15] SHAN, YUJIANG, *Jacobson Radical Rings and their Adjoint Groups*, Ph. D. Thesis, University of Southwestern Louisiana, 1998.