Università degli Studi di Napoli Federico II
Dipartimento di Matematica e Applicazioni
"Renato Caccioppoli"

Local nearrings and products of groups

Candidate: Susanna Di Termini

Supervisor: Prof. Francesco de Giovanni

Thesis for the degree of Doctor of Philosophy at the University of Naples
Italy

XVIII cycle

Introduction

My thesis is divided into five chapters.

The first one focuses on some special factorized groups. A group G is called a factorized group if G can be written by the product of two subgroups A and B.

In the theory of factorized groups, triply factorized groups play an important role. A group G is called triply factorized by its subgroups A, B and M, if

$$G = AM = BM = AB,$$

where M is a normal subgroup of G and $A \cap M = B \cap M = \{1\}$. Many problems concerning with factorized groups can be reduced to triply factorized groups, (see [1]).

Triply factorized groups are also connected with radical rings in a natural way. A ring R is called radical if R forms a group R° under "the circle operation"

$$a \circ b = ab + a + b$$

for every a, $b \in R$. The radical ring R° operates on the additive group R^+ and it can be shown that the semidirect product $R^\circ \ltimes R^+$ is a group which is triply factorized by two subgroups A and B isomorphic to R° and a normal subgroup M isomorphic to R^+. Hence, in the triply factorized groups obtained in this way, the normal subgroup M is always abelian.

There is a result of Y. P. Sysak [32] such that there always exists a radical ring if

$$G = AM = BM = AB$$

is a triply factorized group with abelian subgroups A, B and M and $A \cap B = \{1\}$.

At the end of the first chapter a particular product of groups is investigated. More precisely groups having weakly c-normal subgroups are studied. A subgroup H is called weakly c-normal if there exists a subnormal subgroup K such that $G = HK$ and $H \cap K \leq Core_G(H)$. Finite groups having weakly c-normal subgroups are investigated in ([40] and [41]), where the authors

studied the influence of weakly c-normality of some subgroups on the structure of finite groups. Most of these results are collected in my thesis in order to have a general overview of this subject. In particular, they proved that G is solvable if and only if M is weakly c-normal in G for every maximal subgroup M in G (cmp. [40], Corollary 3.2).

In [7] infinite groups with many weakly c-normal subgroups are investigated. More precisely, the structure of weakly Ic-Dedekind groups are considered. A weakly Ic-Dedekind group is a group such that every infinite subgroup is weakly c-normal. It will be proved that if G is locally soluble weakly Ic-Dedekind group and $G/X(G)$ is periodic, then either G is a Černikov group or it is metabelian. Finally in [7], Theorem 10, the following result is proved:

Let G be a locally nilpotent weakly Ic-Dedekind group without elements of order 2. If $G/X(G)$ is periodic, then either G is a Černikov group or G is nilpotent of class at most 3.

The second chapter of the thesis is characterized by the investigation of a particular algebraic structure, namely nearrings.

Nearrings are a generalization of rings in the sense that addition does not need to be commutative and only one distributive law holds.

In this study, left nearrings are considered. Right nearrings are used by some authors (cmp. [27]) and all the results about left nearrings have always an analogue for right nearrings and vice versa.

Nearrings have an important role in the generalizing of the construction of triply factorized groups by using radical rings. A method to construct triply factorized groups $G = AM = BM = AB$ with non-abelian normal subgroup M using nearrings is described in [13].

An example of a nearring is given by the set of all mappings from a group G in G denoted by $M(G)$, where G is a group not necessarily abelian with the operation "+" of sum and with the neutral element 0. More precisely,

$$M(G) = \{\alpha : G \longrightarrow G\},$$

is a left nearring under the pointwise addition

$$g(\alpha + \beta) = g\alpha + g\beta$$

and the composition of mappings

$$g(\alpha\beta) = (g\alpha)\beta$$

for every $g \in G$ and α, $\beta \in M(G)$.

Some special structures of nearrings such as the zero-symmetric part R_0 and the constant part R_c of R are considered. In particular, it will be proved

that the additive group R^+ of R is the semidirect product of ${R_c}^+$ and ${R_0}^+$. Note that nearrings homomorphisms and factor of nearrings are defined in the usual way. As for rings, ideals of nearrings are exactly the kernel of nearrings homomorphisms. More precisely, I is called ideal in the nearring R if I^+ is a normal subgroup of R^+ and the following two properties hold:

- $RI \subseteq I$;
- $(r+i)s - rs \in I$ for all $i \in I$ and r, $s \in R$.

In this chapter some other relevant results about nearrings are collected, most of which are well-known and can be found for example in [24] and in [27].

In the third chapter the notion of monogenic R-module is introduced and an useful generalization of Jacobson radical for nearrings is presented. Furthermore, the notion of quasiregularity is investigated. The following definition of quasiregular element is given by Beidleman (cmp. [4]): an element r of a zero-symmetric nearring R is called quasiregular, if there exists $s \in R$ such that $(1-r)s = 1$

Meldrum [24] gives another definition of a quasiregular element: let R be a nearring, the element $z \in R$ is called "right quasiregular" if z is contained in the right ideal of R generated by

$$\{x - zx \mid x \in R\}.$$

It will be showed that if z is quasiregular in the sense of Beidleman, then z is right quasiregular in the sense of Meldrum [24].

Furthermore, there is a section devoted to the theory of nearfields. The structure of nearfields were studied before investigating on nearrings. A nearfield is a group respect with the addition and respect with multiplication.

At the beginning of the last century Dickson found an example for a finite nearfield. He showed that for a finite nearfield the additive group is abelian. During the first half of the last century Dickson developed the principles of the nearfields theory and then Zassenhaus [39] classified all the finite nearfields. In the subsection (3.2.1) nearfields above a Černikov multiplicative group are considered. In particular it will be proved that a nearfield above a Černikov multiplicative group is finite. An overview of the theory of nearfields can be found for instance in [35].

At the end of the chapter the definition and some properties of the prime rings are described. More precisely, the prime ring of a nearring R with identity is a commutative ring and in the finite case, it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

The last section of the chapter is devoted to the investigation of the construction subgroups. Using such subgroups, it is possible to construct triply factorized groups in a very similar way as in section (1.2). For a detailed description of the use of construction subgroups in the theory of triply factorized groups see [13].

The fourth chapter focuses on local nearrings. The study of such a structure was begun by Maxson [20]-[23] and continued by several other authors. The nearring R is called local if the set of elements of R, which have not right inverses, denoted as

$$L_R = \{k \in R \mid kR \neq R\}$$

is a R-subgroup of R. Some properties of the additive group R^+ and of subgroup L_R are described. In particular, if R is a finite nearring or it has a finite exponent, then R^+ is a p-group. Among the important results, there is one which plays a relevant role in the use of triply factorized groups: if R is a local nearring then L_R is a construction subgroup, in other terms $1 + L_R$ is a subgroup of the multiplicative group R^*. In [12] it was shown that if R is a local nearring with identity 1 then the set $1 + L_R$ acts on L_R by left multiplication, so that the semidirect product $L_R \rtimes (1 + L_R)$ is a group of the form $G = AB = AM = BM$ with a normal subgroup M and subgroups A and B such that M is isomorphic to L_R and A and B are isomorphic to $1 + L_R$. Thus, in many cases the study of local nearrings can be reduced to that of the triply factorized groups. This approach was partly used in [15] in order to investigate on local nearrings with abelian multiplicative group and explicitly applied in [2] and [33] with the aim to describe local nearrings with dihedral multiplicative and generalized quaternion groups respectively.

The structure of the multiplicative group associated to a local nearring is very important. It turns out that for a finite local nearring the multiplicative group R^* is the semidirect product of $L_R + 1$ and the group of units of R/L_R. Furthermore, it turns out that if R^* is a torsion group, then the additive group R^+ is also a periodic group.

In the last chapter two special classes of local nearrings are investigated. The first part of the chapter focuses on local nearrings having a dihedral multiplicative group. For a detailed account of these results see [2], and [13]. One of the most important results which describes the structure of such a local nearring in [2] is the following:

Let R be a local nearring whose multiplicative group R^* is dihedral and let L_R be the subgroup of all non-invertible elements of R. Then
(1) R is finite.

(2) The additive group R is either a 3-group of order at most 9 or a 2-group of order at most 32.
(3) The subgroup L_R is either an abelian group or a group at most 16 with derived subgroup of order 2. In particular, L_R has an abelian subgroup of index 2.

Actually, by a recent investigation made by Hubert, the following results hold.

There is no local nearring of order 32 whose multiplicative group is dihedral.

If R is a local nearring with dihedral group of units of even order, then $|R| \leq 16$.

In the section (5.2) local nearrings with generalized quaternion multiplicative group are investigated. A detailed account of these results is in [33]. The term "generalized quaternion group" can here be interpreted as either a finite generalized quaternion group

$$Q_{2^n} = \{a, b \mid a^{2^{n-1}} = b^4 = 1, a^{2^{n-2}} = (ab)^2 = b^2\},$$

with $n \geq 3$ or, up to isomorphism, a unique infinite locally quaternion group Q_{2^∞} in which every finite subset is contained in a subgroup isomorphic to Q_{2^n} for some $n \geq 3$. Note that these groups are 2-groups with locally cyclic subgroups of index 2, the following theorem proves that local nearrings above such multiplicative groups are finite.

Let R be a local nearring whose multiplicative group R^* has a locally cyclic 2-subgroup of finite index. Then R is finite.

One of the most important results of this section is the following theorem which describes in a detailed way the structure of a local nearring with a generalized multiplicative quaternion group.

Let R be a local nearring whose multiplicative group R^* is generalized quaternion. Then the following statements hold.

1) The group R^* is either quaternion of order 8 or generalized quaternion of order 16.

2) The additive group R^+ of R is abelian of one of types $(3,3)$, $(2,2,2,2)$, $(2,2,4)$, $(2,2,2,2,2)$ and $(2,2,2,4)$.

3) The subgroup L_R of all non-invertible elements of R is trivial if R^+ is of type $(3,3)$ and it is elementary abelian of index 2 in R^+ otherwise.

Conversely, for each abelian group of type listed in statement 2) there exists at least one R with additive group R^+ of this structure whose multiplicative group R^* is a generalized quaternion group.

Contents

Chapter 1

Products of groups

1.1 Factorized groups.

In the theory of factorized groups, triply factorized groups play an important role. Many problems concerning factorized groups can be reduced to triply factorized groups. For a detailed account of this subject see [1].

Definition 1.1.1 *A group is called* factorized (by A and B), if it can be written as a product $G = AB$ of two of its subgroups A and B.

If $G = AB$ is a factorized group and N is a normal subgroup of G, then the factor group $G/N = (AN/N)(BN/N)$ is also factorized. The following example shows that a subgroup S of G does not need to be factorized by a subgroup of A and a subgroup of B.

Example 1.1.2 *Let* $G = D_{12} = \langle x,\ y \mid x^2 = y^6 = 1,\ y^x = y^{-1} \rangle$ *be the dihedral group of order* 12. *Then* G *is factorized by* $A = \langle x \rangle$ *and* $B = \langle y^2,\ xy^3 \rangle$, *but the subgroup* $S = \langle y^3 \rangle$ *of* G *cannot be written as a product of a subgroup* A *and a subgroup of* B.

The following two lemmas give further elementary properties of factorized subgroups.

Lemma 1.1.3 *([1], Lemma* (1.1.2)*) Let the group* $G = AB$ *be the product of two subgroups* A *and* B. *Then the following properties hold.*
(*i*) *The intersection of arbitrarily many factorized subgroups of* G *is factorized.*
(*ii*) *The subgroup generated by arbitrarily many factorized normal subgroups of* G *is factorized.*
(*iii*) *If* N *is a normal subgroup of* G, *a subgroup* S/N *of the factor group*

$G/N = (AN/N)(BN/N)$ is factorized if and only if S is a factorized subgroup of G.

Proof. The proof of (i) is obvious.

(ii) Let $(S_i)_{i\in I}$ be a system of factorized normal subgroups of G, and put $S = \langle S_i \mid i \in I\rangle$. If $x \in S$, there exist finitely many indices $i_1 \ldots, i_t$ in I such that x belongs to

$$\begin{aligned} S_{i_1} \ldots S_{i_t} &= (A \cap S_{i_1})(B \cap S_{i_1})S_{i_2} \ldots S_{i_t} \\ &= (A \cap S_{i_1})S_{i_2}(B \cap S_{i_1})S_{i_3} \ldots S_{i_t} \\ &= (A \cap S_{i_1})(A \cap S_{i_2})(B \cap S_{i_2})(B \cap S_{i_1})S_{i_3} \ldots S_{i_t} = \\ &= \ldots \\ &= (A \cap S_{i_1}) \ldots (A \cap S_{i_t})(B \cap S_{i_t}) \ldots (B \cap S_{i_1}) \\ &\leq (A \cap S)(B \cap S). \end{aligned}$$

Hence $S = (A \cap S)(B \cap S)$, and clearly also $A \cap B$ is contained in S.

(iii) Let S be a factorized subgroup of G containing N. If $xN = abN$ is an element of S/N, with $x \in S$, $a \in A$, and $b \in B$, then $x = aby$, where y is in $N \leq S$. Hence $ab = xy^{-1}$ belongs to S, and so a is in S. Therefore S/N is a factorized subgroup of G/N.

Conversely, suppose that the subgroup S/N is factorized in G/N. Let $x = ab$ be an element of S, with $a \in A$ and $b \in B$. Since $xN = abN$, it follows that aN belongs to S/N. Hence a is in S and so S is factorized.

Lemma 1.1.4 *([1], Lemma 1.1.3) Let the group $G = AB$ be the product of two subgroups A and B. If a subgroup S of G is factorized, then $S = AS \cap BS$*

Proof. Consider an element x of $AS \cap BS$. Then $x = au = bv$, with $a \in A$, $b \in B$, and u, v in S. It follows that $a^{-1}b = uv^{-1}$ is in S, so that a belongs to S and hence also x is in S. Therefore $S = AS \cap BS$.

Definition 1.1.5 *A factorized group G is called triply factorized (by A, B, and M), if $G = A \ltimes M = B \ltimes M = AB$ for two subgroups A and B and a normal subgroup M of G.*

By Lemma (1.1.3), the intersection $X(S)$ of all factorized subgroups of $G = AB$ containing the subgroup S is the smallest factorized subgroup of G containing S. The subgroup $X(S)$ is called the factorizer of S in $G = AB$.

The following lemma shows that in the case of normal subgroup N of G, the factorizer $X(N)$ has a triple factorization.

Lemma 1.1.6 *([1], Lemma (1.1.4)) Let the group $G = AB$ be factorized by A and B and let N be a normal subgroup of G. Then the following statements hold:*
(1) $X(N) = AN \cap BN$
(2) $X(N) = (A \cap BN)N = (B \cap AN)N = (A \cap BN)(B \cap AN)$.

Example 1.1.7 *Let A, B, G, and S be as in Example (1.1.2). Then $S \trianglelefteq G$ and $X(S) = \langle x,\ y^3 \rangle$. In this case, $A \cap BS = A$ and $B \cap AS = \langle xy^3 \rangle$.*

If G is a group which has a triple factorization of the form $G = AB = AM = BM$, where A and B are subgroups of G and M is an abelian normal subgroup of G, then $C = (A \cap M)(B \cap M)$ is a normal subgroup of G. In this case,

$$G/C = (AC/C) \ltimes (MC/C) = (BC/C) \ltimes (MC/C) = (AC/C)(BC/C)$$

Remark 1.1.8 Note that in a triply factorized group $G = A \ltimes M = B \ltimes M = AB$ the subgroups A and B are complements of M and hence $A \cong B$. But A and B can only be conjugate if $A = B = G$.

1.2 Triply factorized groups and radical rings

This section is devoted to the connection of a triply factorized groups with radical rings.

Definition 1.2.1 *Let R be an associative ring. R is called a radical ring, if R coincides with its Jacobson radical $\mathcal{J}(R)$, i.e., if R forms a group under the circle operation*

$$a \circ b := a + b + ab$$

for all a, $b \in R$. Obviously, a radical ring does not contain an identity element.

The following construction, made by Ya. Sysak, is described in [1].

Let R be a radical ring, embedded in an arbitrary way into the ring R_1 with identity element. Then the radical ring is isomorphic to the subgroup $R + 1$ of the group of units of R_1.

Let U be a left ideal of R and $M = R/U$ be a left R-module. Then the group $A = R + 1$ operates on M via

$$(l + U)^{m+1} = (m + 1)^{-1}l + U$$

for all l, m in R. In the semidirect product $G = G(R) = A \ltimes M$,

$$B = \{((l+1)^{-1},\ l + U) |\ l \in R\}$$

is a complement of M with the property

$$G = A \ltimes M = B \ltimes M = AB,$$

i.e., G is a triply factorized group.

Note that for a triply factorized group

$$G = A \ltimes M = B \ltimes M = AB$$

there is always a radical ring R such that G can be constructed by R. The following theorem proved by Ya. Sysak, shows that this happens, if A, B and M are abelian and $A \cap B = 1$.

Proposition 1.2.2 *([1], Proposition 6.1.1) If $G = A \ltimes M = B \ltimes M = AB$ is a triply factorized group with abelian subgroups A, B and M, with $A \cap B = \{1\}$, then there exists a radical commutative ring R with $G \cong G(R)$.*

Remark 1.2.3 Since the group M in the above construction is the additive group of a R-module, it is always abelian. Note that, using the structure of nearrings, whose notion will be defined in the following chapter, it is possible to obtain triply factorized groups $G = A \rtimes M = B \rtimes M = AB$ with a possibly non-abelian subgroup M.

In the following two sections groups having weakly c-normal subgroups are investigated. The properties of such groups will be investigated in a detailed way both in the finite case and in the infinite case.

1.3 Some factorized groups

A subgroup H of a group G is said to be *permutably complemented* if there exists a subgroup K such that $G = HK$ and $H \cap K = \{1\}$. The structure of groups in which every subgroup is permutably complemented was completely described by Cernikova and Emaldi; for a detailed description of this subject see the monograph [31].

Let G be a group. A subgroup H of G is called *c-supplemented* if there exists a subgroup K of G such that $G = HK$ and $H \cap K$ is contained in the core H_G of H in G, in this case K is called a *c-supplement* of H in G. Finite groups in which all subgroups are c-supplemented have been considered in [3].

A subgroup of a group is called *weakly c-normal* if it has a c-supplement that is a subnormal subgroup of the group. In such a section the most important results about weakly c-normal subgroups of finite groups which have been recently studied in [40] are collected.

Definition 1.3.1 *A subgroup H of G is called weakly c-normal in G if there exists a subnormal subgroup K such that $G = HK$ and $H \cap K \subseteq H_G$.*

Definition 1.3.2 *A group G is called* weakly c-simple if G has no weakly c-normal subgroup except of the identity group $\{1\}$ and the whole group G.

Let π be a set of prime numbers and π' the complement of π in the set of all prime numbers. Consider now the following families of subgroups:

$$F_c = \{M \mid M \text{ maximal subgroup of } G, \text{ such that } |G : M| \text{ is composite}\}.$$

$$F^p = \{M \mid M \text{ maximal subgroup of } G,\ N_G(B) \leq M \text{ for a } B \in Sly_p(G)\}.$$

$F^s = \cup_{p \in \pi(G)} F^p$.
$F^{pc} = F^p \cap F_c$.
$F^{sc} = F^s \cap F_c$.
and define $S^s(G) = \cap\{M \mid M \in F^{sc}\}$ if F^{sc} is non-empty; otherwise
$S^s(G) = G$.
$S^p(G) = \cap\{M \mid M \in F^{pc}\}$ if F^{pc} is non-empty; otherwise
$S^p(G) = G$.

In the sequel some known results will be considered.

Lemma 1.3.3 *(cmp. [17], Lemma 2.1) Let G be a group, then the following statements hold.*
(1) *Let H be a subgroup of G. Then H is weakly c-normal in G if and only if there exists a subnormal subgroup N of G such that $G = HN$ and $H \cap N = H_G$.*
(2) *If H is normal in G, then H is weakly c-normal in G.*
(3) *G is weakly c-simple if and only if G is simple.*
(4) *If H is weakly c-normal in G and $H \leq M \leq G$, then H is weakly c-normal in M.*
(5) *Let K be a normal subgroup of G and $K \leq H$. Then H is weakly c-normal in G if and only if H/K is weakly c-normal in G/K.*
(6) *Let H be a π-subgroup of G and N a normal π'-subgroup of G. If H is weakly c-normal in G, then HN/N is weakly c-normal in G/N. Furthermore, if $N \leq N_G(H)$, then the converse also holds.*

Lemma 1.3.4 *[36] Let G be a finite group. Then G is supersolvable if and only if $G = S^s(G)$.*

Lemma 1.3.5 *([17], Corollary 3.2) A finite group G is solvable if and only if every maximal subgroup of G is weakly c-normal in G.*

Lemma 1.3.6 *([8], Theorem A; 14.3) If H is a subnormal subgroup of a group G, then $Soc(G) \leq N_G(H)$, where $Soc(G)$ is the socle of G, i.e., the product of all minimal normal subgroups of G.*

Lemma 1.3.7 *([28], 10.4.2) If a finite group G has a nilpotent maximal subgroup M of odd order, then G is solvable.*

Lemma 1.3.8 *([30], Theorem 1) Suppose that G is a finite insoluble group with a nilpotent maximal subgroup M. Let T be the unique Sylow 2-subgroup of M and U the unique 2-complement of M. Then U is normal in G, $Z(U) \leq Z(G)$, $G/Z(U) \cong G/U \times U/Z(U)$ and G/U is an insoluble group whose Sylow 2-subgroups are maximal subgroups. In particular, if $Z(G) = 1$ then M is a Sylow 2-subgroup of G.*

The following theorem is proved by Zhu, Guo, Zhang in ([41], Theorem 3.1).

Theorem 1.3.9 *Let G be a finite group. Then G is solvable if and only if M is weakly c-normal in G for every maximal subgroup M in F^{sc}.*

The previous result also holds in the case in which the maximal subgroups are c-normal and it is proved by Wang in [36].

Definition 1.3.10 *A subgroup H of G is called c-normal in G if there exists a normal subgroup K of G such that $G = HK$ and $H \cap K \leq H_G$.*

The notion of c-normality is introduced by Wang in [36], where the author studied the influence of such a property on the structure of finite groups.

1.4 Generalizations of c-Dedekind groups

In this section weakly c-normal subgroups of infinite groups are investigated. For a detailed description see [7].

A group is said to be a *c-Dedekind group* if all its subgroups are c-normal. It is well-known that the Frattini subgroup of a group with complemented

subgroup lattice is trivial, and this property suggests that for a c-Dedekind group G the subgroup $X(G)$, defined as the intersection of all maximal normal subgroups of G, must play an important role. In fact, it was proved in [19] that a group G such that $G/X(G)$ is periodic, is a c-Dedekind group if and only if all subgroups of $X(G)$ are normal in G.

Clearly, every c-normal subgroup is also a weakly c-normal subgroup, but arbitrary weakly c-normal subgroups do not need to be c-normal (see for instance [40], example 1).

Recall that, as quoted above, if G is any group $X(G)$ is the intersection of all normal subgroups of G that are also maximal subgroups.

Lemma 1.4.1 *Let G be a group in which all cyclic subgroups are weakly c-normal. Then all subgroups of $X(G)$ are normal in G.*

Proof. Let X be any cyclic subgroup of $X(G)$ and assume by contradiction, that X is not normal in G. Let Y be a subnormal c-supplement of X in G, so that $G = XY$ and $X \cap Y = X_G$. Since X is not normal in G, the subgroup Y must be properly contained in G and hence also $N = Y^G$ is a proper subgroup of G. Clearly $G = NX$ and $G/N \simeq X/X \cap N$ is a non-trivial cyclic group, so that there exists a maximal subgroup M/N of G/N. It follows that $X \leq X(G) \leq M$ and hence $G = XN = M$. This contradiction shows that all cyclic subgroups of $X(G)$ are normal in G and hence the Lemma is proved.

Corollary 1.4.2 *Let G be a group in which all cyclic subgroups are weakly c-normal, then the group $G/Z(X(G))$ is abelian. In particular, G is metabelian and hypercyclic.*

Proof. By Lemma (1.4.1), G acts as a group of power automorphisms on $X(G)$ and hence $G/C_G(X(G))$ is abelian. If follows that

$$G' \leq X(G) \cap C_G(X(G)) = Z(X(G))$$

and hence G'' is trivial. Moreover, all subgroups of G' are normal in G so that G is hypercyclic.

The following result proves, in particular, that any periodic group in which all subgroups are weakly c-normal is a c-Dedekind group.

Theorem 1.4.3 *Let G be a group in which all cyclic subgroups are weakly c-normal. If $G/X(G)$ is periodic, then G is a c-Dedekind group.*

Proof. By Lemma (1.4.1), all subgroups of $X(G)$ are normal in G so that the result follows from Theorem 3 of [19].

Using the same arguments as in [19] it can be also proved the following result.

Theorem 1.4.4 *Let G be a locally nilpotent group whose cyclic subgroups are weakly c-normal. If either G is not periodic or G is periodic and $2 \notin \pi(G)$, then G is nilpotent of class at most 3.*

Definition 1.4.5 *A group G is called Ic-Dedekind group if every infinite subgroup is weakly c-normal.*

Note that subgroups and quotients of weakly Ic-Dedekind groups are likewise weakly Ic-Dedekind groups.

Lemma 1.4.6 *Let G be a weakly Ic-Dedekind group and let x be an element of infinite order of $X(G)$. If y is any element of $X(G)$, then $\langle x, y\rangle$ is a normal subgroup of G.*

Proof. Arguing as in Lemma (1.4.1) it is possible to see that $\langle x\rangle$ is normal in G. Put $X = \langle x,\ y\rangle = \langle x\rangle\langle y\rangle$ and suppose that X is not a normal subgroup of G. Let Y be a subnormal subgroup of G such that $G = XY$ and $X \cap Y = X_G$. Since X is not normal in G, the subgroup Y is properly contained in G so also Y^G is a proper subgroup of G. As $G = XY^G$, the factor group G/Y^G is a non-trivial supersoluble so that G contains a maximal normal subgroup M containing Y^G. Thus $X \leq X(G) \leq M$ and $G = XY^G = M$. This contradiction proves that X is a normal subgroup of G.

Lemma 1.4.7 *Let G a weakly Ic-Dedekind group and let H be a locally finite subgroup of $X(G)$. Then either H is a Cernikov group or all subgroups of H are normal in G.*

Proof. Assume that H is not a Černikov group. Then H does not satisfy the minimal condition on abelian subgroups (see [34]), so that it contains an abelian subgroup with infinite socle and there exists in H a chain of subgroups

$$S_1 > S_2 > \cdots > S_n > \cdots > \bigcap_{n\in\mathbb{N}} S_n = \{1\}$$

where each S_i is the direct product of infinitely many cyclic groups of prime order. Let i be a positive integer such that S_i is not normal in G, and let L be a subnormal c-supplement of S_i in G. Then $G = S_iL = S_iL^G$ and L^G

is a proper subgroup of G. Since G/L^G is isomorphic to a quotient of S_i, it follows that there exists a maximal normal subgroup M of G containing L^G. Therefore $G = S_iL^G = M$, that is a contradiction. It follows that S_n is a normal subgroup of G for each positive integer n. Let x be any element of H and let k be a positive integer such that $S_k \cap \langle x\rangle = \{1\}$. As above, it is possible to prove that $\langle x\rangle S_i$ is a normal subgroup of G for every $i \geq k$, and hence also

$$\bigcap_{i\geq k}\langle x\rangle S_i = \langle x\rangle(\bigcap_{i\geq k} S_i) = \langle x\rangle$$

is a normal subgroup of G. It follows that all subgroups of H are normal in G.

Theorem 1.4.8 *Let G be a locally soluble weakly Ic-Dedekind group. Then either $X(G)$ is a Černikov group or all subgroups of $X(G)$ are normal in G.*

Proof. Let H be any subgroup of $X(G)$. Assume that H contains an element of infinite order x. Then by Lemma (1.4.6) $\langle y\rangle^G \leq \langle x,\ y\rangle$ for any element y of H; therefore H is normal in G in this case. On the other hand, if H is periodic, either H is a Černikov group or it is a normal subgroup of G by Lemma (1.4.7). It follows that $X(G)$ satisfies the minimal condition on non-normal subgroups and hence it is either a Černikov group or a Dedekind group (see [26]); in particular, if $X(G)$ does not satisfy the minimal condition, all subgroups of $X(G)$ are normal in G again by Lemma (1.4.6) and Lemma (1.4.7). The theorem is proved.

Corollary 1.4.9 *Let G be a locally soluble weakly Ic-Dedekind group. If $G/X(G)$ is periodic, then either $X(G)$ is a Černikov group or G is a c-Dedekind group.*

Proof. By Theorem (1.4.8), either $X(G)$ is a Černikov group or all subgroups of $X(G)$ are normal in G. Therefore the result follows immediately from Theorem 3 of [19].

Theorem 1.4.10 *Let G be a locally soluble weakly Ic-Dedekind group. If $G/X(G)$ is periodic, then either G is a Černikov group or it is metabelian.*

Proof. By ([19], Corollary 2) assume that G is not a c-Dedekind group, so that in particular, $X(G)$ is a Černikov group by Corollary (1.4.9). Thus G is soluble and periodic. Assume that G is not a Černikov group. Let a, b, c, d be elements of G and put $X = \langle a, b, c, d\rangle$. Then X induces a finite group of automorphisms on G and hence G must contain an abelian non-

Černikov X-invariant subgroup A (see [38]). If S is the socle of A, then $Y = \langle S,\ X\rangle = SX$ is an infinite residually finite weakly Ic-Dedekind group. Let N be any normal subgroup of finite index of Y. Clearly, N is infinite so that all subgroups of Y/N are weakly c-normal and hence $Y'' \leq N$ by Corollary (1.4.2). As Y is residually finite, it follows that Y'' is trivial. In particular, $[[a, b], [c, d]] = 1$ and hence G is metabelian.

By Theorem (1.4.4), any periodic locally nilpotent group in which all subgroups are weakly c-normal is nilpotent of class at most 3, provided that it does not contain elements of order 2; therefore the proof of Theorem (1.4.10) also shows that the following result holds.

Theorem 1.4.11 *Let G be a locally nilpotent weakly Ic-Dedekind group without elements of order 2. If $G/X(G)$ is periodic, then either G is a Černikov group or G is nilpotent of class at most 3.*

Chapter 2

Nearrings

2.1 Elementary properties of nearrings

This chapter deals with the theory of nearrings, most of the results can be found in Meldrum [24], Pilz [27], and Clay [6].

Definition 2.1.1 *A set R with two binary operations "$+$" and "$\cdot$" is called a left nearring, if the following conditions hold:*

(1) $(R, +)$ *is a group not necessarily abelian with neutral element* 0*;*

(2) $(R, \cdot)$ *is a semigroup;*

(3) the left distributive law holds, i.e.,

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

for all x, y, $z \in R$.

Remark 2.1.2 The group $(R, +)$ is often denoted as R^+.

As usual, instead of $x \cdot y$ will be written xy. If R contains an element 1 such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in R$, then R is called *nearring with identity.* A nearring with $xy = 0$ for all x, $y \in R$ is called a *zero symmetric nearring,* and a nearring is called *constant nearring, if $xy = y$ for all x, $y \in R$.* If, instead of the property (3), the right distributive holds, R is called *right nearring.* Right nearrings are used by some authors (e.g. Pilz [27]), and all results about left nearrings always have an analogue for right nearrings and vice versa.

Conventions 2.1.3 *Let R be a nearring, $r \in R$ and $n > 0$ a positive integer. Then $\underbrace{r + \cdots + r}_{n \text{ times}}$ in the sequel will always be written rn and never*

nr. Analogously, for negative integers m, rm will mean $-(r(-m))$. If the integral factors are written on the right, they can be considered as multiples of the identity element. Conversely, nr will mean $\underbrace{(1+\cdots+1)}_{n-times}r$, which is in general different from rn.

Note that because of left distributivity, in every nearring R the equation $(xy)n = x(yn)$ holds for all x, $y \in R$ and for all $n \in \mathbb{Z}$, even if R has not an identity element.

As for rings, it can be shown that a nearring with identity must be trivial if $1 = 0$. Hence, in the sequel "nearring with identity" will always imply $1 \neq 0$.

Example 2.1.4 *a) Let G be a not necessarily abelian additive group with neutral element 0. Then*

$$M(G) = \{\alpha : G \longrightarrow G\},$$

the set of all mappings from G in G, is a left nearring under pointwise addition

$$g(\alpha + \beta) = g\alpha + g\beta$$

and the composition of mappings

$$g(\alpha\beta) = (g\alpha)\beta).$$

b) The following subsets of $M(G)$ are also nearrings under these operations:

- $M_0(G) = \{\alpha : G \longrightarrow G \mid 0\alpha = 0\}$
- $M_c(G) = \{\alpha : G \longrightarrow G \mid \alpha = const\}$
- $M_c{}^0(G) = \{\alpha : G \longrightarrow G \mid \alpha|_{G-\{0\}} = const \text{ and } 0\alpha = 0\}$

Example 2.1.5 *Let R be a ring, and let $R[x]$ be the set of all polynomials in one "indeterminate" over R. Define addition in $R[x]$ in the usual way, and define composition "$\circ$" by $f \circ g = f(g)$, where f, $g \in R[x]$. Then $(R[x], +, \circ)$ is the right nearring of polynomials over R.*

Definition 2.1.6 *Let $(R, +, \cdot)$ be a nearring. Then a non-empty subset S of R is called a subnearring if $(S, +, \cdot)$ satisfies the axioms of definition (2.1.1), with the operations being induced by those in R.*

It is then immediate that $M_0(G)$ is a subnearring of $M(G)$. As in the case with subgroups and other familiar substructures, there is an easier criterion for a subset to be a subnearring than that given by the definition.

Lemma 2.1.7 *([24]) Let S be a subset of the nearring $(R, +, \cdot)$. Then S is a subnearring if and only if $(S, +)$ is a subgroup of $(R, +)$ and $(S, \cdot)$ is a subsemigroup of $(R, \cdot)$.*

Note that $(R[x], +, \circ)$ is a nearring whose additive group is commutative. This is also the case with $M(G)$ and $M_0(G)$ if G is abelian. This prompts the following definition.

Definition 2.1.8 *A nearring $(R, +, \cdot)$ is called abelian if $(R, +)$ is an abelian group and it is called commutative if $(R, \cdot)$ is a commutative semigroup.*

Remark 2.1.9 The following equalities hold in any nearrings as for rings:

a) $r0 = 0$ for every $r \in R$

b) $r(-s) = -(rs)$ for every r, $s \in R$.

Considering constant nearrings, it is easy to see that the following equations do not hold in nearrings in general:

a') $0r = 0$ for every $r \in R$

b') $(-r)s = -(rs)$ for every r, $s \in R$.

Definition 2.1.10 *Let R be a nearring.*

a) $R_0 = \{r \in R \mid 0r = 0\}$ *is called the zero-symmetric part of R.*

b) $R_c = \{r \in R \mid 0r = r\}$ *is called the constant part of R.*

c) $R_d = \{d \in R \mid (r + s)d = rd + sd \ \forall r,\ s \in R\}$. *An element d is called distributive element, if $d \in R_d$*

d) An element $d \in R$ is called antidistributiv, if $(r + s)d = sd + rd$ for every r, $s \in R$.

e) The nearring R is called constant, zero-symmetric, or distributive if $R = R_c$, $R = R_0$ or $R = R_d$ respectively.

f) R is called distributively generated (d.g.), if there is a subsemigroup $S \leq (R_d, \cdot)$, such that the additive group R^+ is generated by S. In this case, R is denoted by $R = (R, S)$.

g) If R is a nearring with identity, the group of units of R is denoted by R^*.

h) If R is a nearring with identity and $r \in R$, $o^+(r)$ is the additive order of $r \in R^+$. If $r \in R^*$, $o^*(r)$ is the multiplicative order of r.

Lemma 2.1.11 *Let R be a nearring and $r \in R$. If $-r$ is antidistributiv, then r is distributive.*

Proof. For all s, $t \in R$ the element $-r$ is antiditributiv $\iff (s+t)(-r) = t(-r)+s(-r) \iff -((s+t)r) = -(tr)-(sr) \iff sr+tr = (s+t)r \iff r$ is distributiv.

Lemma 2.1.12 *Let R be a nearring with identity whose additive group R^+ is abelian. Then the set D of all distributive elements of R is a subring of R whose multiplicative group D^* coincides with the intersection $D \cap R^*$.*

Proof. If d_1 and $d_2 \in D$ and $r, s \in R$, then $(r+s)(d_1-d_2) = (r+s)d_1-(r+s)d_2 = rd_1+sd_1-sd_2-rd_2 = (rd_1-rd_2)+(sd_1-sd_2) = r(d_1-d_2)+s(d_1-d_2)$. Therefore D is a subgroup of R^+ and simultaneously a subsemigroup of $(R,\cdot)$ containing the identity of R. Thus D is a subring of R whose multiplicative group D^* is clearly contained in $D \cap R^*$. On the other hand, if $d \in D \cap R^*$, then $(rd^{-1}+sd^{-1})d = (rd^{-1})d+(sd^{-1})d = r+s$ and so $(r+s)d^{-1} = rd^{-1}+sd^{-1}$. Hence $d^{-1} \in D$ and thus $D^* = D \cap R^*$, as desired.

The following result is concerning with distributive nearrings and it is proved by Weinert in [37].

Lemma 2.1.13 *If R is a distributive nearring, then*

$$R^2 = \left\{ \sum_{i=1}^{n} x_i y_i \mid \; n \in \mathbb{N}_0 \;\; x_i, \;\; y_i \in R \right\}$$

is a ring. In particular, a distributive nearring with identity element is a ring.

Proof. Since $R^2 \subseteq R$, it follows that R^2 is a distributive nearring, it is sufficient to prove that R^2 is abelian. Let a, b, c, $d \in R$. Then the following two equalities hold:

$$(a+b)(c+d) = a(c+d)+b(c+d) = ac+ad+bc+bd$$

and

$$(a+b)(c+d) = (a+b)c+(a+b)d = ac+bc+ad+bd.$$

Hence $ad+bc = bc+ad$ for all a, b, c, $d \in R$. This means that R^2 is abelian.

Corollary 2.1.14 (*a*) *Commutative nearrings are distributive.*
(*b*) *Distributive nearrings with identity element are rings.*
(*c*) *Commutative nearrings with identity element are rings.*

Proof. Let R be a commutative nearring, then $(r+s)t = t(r+s) = tr+ts = rt+st$ for all r, s, $t \in R$ and so R is distributiv. The condition (b) is proved by applying the previous lemma (2.1.13). The last condition is a consequence of the conditions (a) and (b).

The following theorem proved by Meldrum in ([24], Theorem 1.15) gives an important description of the structure of the additive group of a nearring.

Theorem 2.1.15 *Let R be a nearring. Then R_c is the unique maximal constant subnearring of R and R_0 is the unique maximal zero-symmetric subnearring of R. Moreover, $R^+ = {R_c}^+ \ltimes {R_0}^+$. In particular, if $r \in R$, then $r - 0r \in R_0$ and $0r \in R_c$.*

Corollary 2.1.16 *Let R be a nearring with identity 1. Then $1 \in R_0$ and hence $1 \cdot z \in R_0$ for all $z \in \mathbb{Z}$.*

The following result is proved by ([24], Lemma 1.12).

Lemma 2.1.17 *Let R be a nearring and $r \in R$ an element of the form $r = 0x$ for some $x \in R$. Then $r \in R_c$. On the other hand, all elements of R_c are of this form (since $y = 0y$, for $y \in R_c$).*

In nearrings with identity the structure of the group of units has an important role. It results that the multiplicative inverse of zero-symmetric elements are zero-symmetric as well.

Proposition 2.1.18 *Let R be a nearring with identity 1 and $r \in R^* \cap R_0$. Then $r^{-1} \in R_0$.*

Proof. Let $r^{-1} = r_0 + 0r^{-1}$ with $r_0 \in R_0$. Then, $1 = rr^{-1} = r(r_0 + 0r^{-1}) = rr_0 + 0r^{-1}$ and hence $-rr_0 + 1 = 0r^{-1}$. Since sums, products, and additive inverses of zero-symmetric elements are zero-symmetric, the left side of the last equation is contained in R_0, while the right side is contained in R_c by Lemma (2.1.17), and thus both must be 0. Hence, $0r^{-1} = 0$ and $r^{-1} \in R_0$.

The following lemma shows that the group of units of a nearring R is factorized by the group of units of the zero-symmetric part of R and the group $R_c + 1$.

Lemma 2.1.19 *Let R be a nearring with identity 1. Then $R_c + 1$ is a subgroup of R^* isomorphic to ${R_c}^+$ and $R^* = {R_0}^*(R_c + 1)$ with ${R_0}^* \cap (R_c + 1) = \{1\}$.*

Proof. The mapping $\sigma : {R_c}^+ \longrightarrow (R_c + 1)^*$ such that $x \mapsto -x+1$ is a group isomorphism. Moreover, if $r \in R^*$, by (2.1.15), there are elements $c \in R_c$ and $z \in R_0$ such that $r = c + z = z(c + 1)$. Since the intersection $R_0 \cap R_c = \{0\}$ and $1 \in R_0$, it follows that ${R_0}^* \cap (R_c + 1) = \{1\}$.

The following result is important for the study of the construction of triply factorized groups.

Proposition 2.1.20 *Let R be a nearring with identity element 1. Then R^* is isomorphic to a subgroup of $Aut(R^+)$, i.e, R^* operates faithfully on R^+.*

Proof. Consider $r \in R^*$ and the mapping $\sigma_r : R \longrightarrow R$ such that $x \mapsto rx$ for all $x \in R$. Since $(x + y)\sigma_r = r(x + y) = rx + ry = x\sigma_r + y\sigma_r$ for all x, $y \in R$, it follows that σ_r is an endomorphism of R^+. By its definition, the mapping results bijective, hence $\sigma_r \in Aut(R^+)$. Since $\sigma_r\sigma_s = \sigma_{sr}$ for all s, $r \in R^*$, the mapping $\sigma : R^* \longrightarrow Aut(R^+)$ with $r \mapsto \sigma_{r^{-1}}$ for all $r \in R^*$ is a group homomorphism. But if σ_r is the identity mapping, $rx = x$ for all $x \in R$, in particular for $x = 1$ and hence $r = 1$. It follows that σ is a monomorphism thus R^* is isomorphic to $Im(\sigma)$.

Theorem 2.1.21 *Let R be a nearring and let $r \in R$ have finite additive order. Then $o^+(xr) \mid o^+(r)$ for all $x \in R$.*

Proof. Let $n = o^+(r)$. Then $(xr) \cdot n = x(r \cdot n) = x0 = 0$. Hence, $o^+(xr) \mid o^+(r)$.

Corollary 2.1.22 *Let R be a nearring with identity. Then, $o^+(r) = exp(R^+)$ for all $r \in R^*$.*

Proof. Suppose that $exp(R^+) < \infty$ and $r \in R^*$. Then $o^+(r) \mid exp(R^+) = n$. Let s be an arbitrary element of R. Then $s \cdot o^+(r) = sr^{-1}r \cdot o^+(r) = sr^{-1}(r \cdot o^+(r)) = sr^{-1}0 = 0$, and hence $o^+(s) \mid o^+(r)$; thus, $o^+(r) = n$. By the same argument, $o^+(r)$ must be infinite, if the exponent of R^+ is infinite. Indeed if $o^+(r) = n < \infty$ for some $r \in R^*$, $s \cdot o^+(r) = 0$ for all $s \in R$.

2.2 Homomorphisms of nearrings

Homomorphisms are an important tool for the investigation of any algebraic structures. As in the case of the rings or groups, nearring homomorphisms can be used to embed nearrings into other nearrings and in this way it possible to have some information on the structure of the nearrings taken into consideration.

Definition 2.2.1 *Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be nearrings. The mapping α is called nearring homomorphism, if for all r_1, $r_2 \in R$ the following properties hold:*

$$(r_1 + r_2)\alpha = r_1\alpha + r_2\alpha,$$

$$(r_1 r_2)\alpha = (r_1\alpha)(r_2\alpha).$$

The terms kernel of a homomorphism, monomorphism, epimorphism, endomorphism and automorphism are defined as usual.

Lemma 2.2.2 *([24], Lemma 1.17) Let α be a homomorphism from the nearring R to the nearring S. Then*
(a) α is a group homomorphism from $(R,+)$ to $(S,+)$;
(b) α is a semigroup homomorphism from $(R,\cdot)$ to $(S,\cdot)$;
(c) $R\alpha$ is a subnearring of S.

Theorem 2.2.3 *Let R be a nearring and G be a group. Let U be a proper subgroup such that $U \cong R^+$. Then R can be embedded into $M(G)$, i.e., $\theta : R \longrightarrow M(G)$ is a monomorphism.*

Proof. Let α be the isomorphism $\alpha : R \longrightarrow U$ such that $r\alpha := u_r \in U$, for every $r \in R$. Let $r \in R$, and $\theta : R \longrightarrow M(G)$, define for every $g \in G$

$$g(r\theta) = \begin{cases} u_r & g \notin U \\ gu_r & g \in U \end{cases}$$

Show that θ is a nearring homomorphism. Let r_1, $r_2 \in R$. For every $g \in G$ it follows that

$$g((r_1 + r_2)\theta) = \begin{cases} u_{r_1} + u_{r_2} & g \notin U \\ g(u_{r_1} + u_{r_2}) & g \in U \end{cases}$$

$$= \begin{cases} g(r_1\theta) + g(r_2\theta) & g \notin U \\ gu_{r_1} + gu_{r_2} & g \in U \end{cases}$$

$$= \begin{cases} g(r_1\theta + r_2\theta) & g \notin U \\ g(r_1\theta) + g(r_2\theta) & g \in U \end{cases}$$

$$= g(r_1\theta + r_2\theta).$$

Then θ is a group homomorphism from R^+ to $M(G)^+$. Moreover

$$g((r_1\theta) \circ (r_2\theta)) = (g(r_1\theta))(r_2\theta)$$

$$= \begin{cases} u_{r_1}(r_2\theta) & g \notin U \\ g u_{r_1}(r_2\theta) & g \in U \end{cases}$$

$$= \begin{cases} u_{r_1} u_{r_2} & g \notin U \\ g u_{r_1} u_{r_2} & g \in U \end{cases}$$

$$= g((r_1 r_2)\theta)$$

for all $g \in G$. Thus θ is also a semigroup homomorphism from R^* to $(M(G), \cdot)$ and so it is a nearring homomorphism. If $r_1\theta = r_2\theta$, then $u_{r_1} = g(r_1\theta) = g(r_2\theta) = u_{r_2}$ for every $g \in U$. Since α is an isomorphism, it follows that θ is injective.

Theorem 2.2.4 *(a) Every nearring R can be embedded in a nearring with identity.*
(b) A zero-symmetric nearring R_0 can be embedded in a zero-symmetric nearring with identity.
(c) A constant nearring R_c can be embedded in a constant nearring with identity.

Proof. *(a)* Let G be an additive group with neutral element 0 and let U be a proper subgroup of G such that $U \cong R^+$. By the previous result (2.2.3), it follows the thesis.

(b) Let R_0 be a zero-symmetric nearring, which can be embedded in the nearring $M(G)$, where G is a group. Since $0 \in U$, it follows that $0(r\theta) = 0u_r = 0$ for all $r \in R_0$. Thus $r\theta \in M_0(G)$ for all $r \in R_0$. Thus R_0 can be embedded in a zero-symmetric nearring.

(c) If R_c is a constant nearring, then for every $g \in G$ and $r \in R_c$, it follows that

$$g(r\theta) = \begin{cases} u_r & g \notin U \\ g u_r & g \in U \end{cases}$$

$$= u_r$$

Thus $(R_c)\theta \subseteq M_c(G)$ and R_c can be embedded in the constant nearring $M_c(G)$.

2.3 Nearring modules

As in ring theory, it is possible to study modules over nearrings. The notion of such a structure is defined via the concept of representation.

Definition 2.3.1 *a) Let $(G,+)$ be a group and R be a nearring. The group G is called right R-module, if there is a nearring homomorphism $\omega : (R,+,\cdot) \longrightarrow (M(G),+,\circ)$. Such a homomorphism is called representation of R. A representation ω of R is called faithful, if $Ker(\omega) = \{0\}$.*

b) Let R be a nearring and G a R-module. Consider $Y \subseteq G$ the following set

$$\mathcal{U}_R(Y) = \{x \in R |\ Yx = 0\}$$

is called annihilator of Y. If ω is a representation of R, then ω is faithful, if and only if $\mathcal{U}_R(G) = Ker(\omega) = \{0\}$.

Remark 2.3.2 It is possible to define the notion of R-modules, which is equivalent to the previuos definition (2.3.1): let $(G,+)$ be a group with neutral element 0 and R be a nearring. Let $\mu : G \times R \longrightarrow G$, such that $(g,r) \mapsto gr$. Then, (G,μ) is called R-module, if the following properties hold for all $g \in G$, r, $s \in R$:

1) $g(r+s) = gr + gs$

2) $g(rs) = (gr)s$.

Example 2.3.3 *1. Every nearring R is a R-module, which is also denoted by R_R. It is often called regular R-module.*

2. Every additive group G is a $M(G)$-module as the identity application

$$id : M(G) \longrightarrow M(G)$$

is the representation of $M(G)$. Clearly G is also a faithful $M(G)$-module.

2.4 Ideals and special subgroups

In this section the ideals of nearrings are studied. As for rings, the ideals are defined as the kernels of homomorphisms. More precisely, an ideal is a normal subgroup of the additive group of a nearring R which is invariant with respect to the link multiplication with elements of R. Moreover it must fulfil the property according which for every $x \in I$, $(r+x)s - rs \in I$ for every r, $s \in R$.

Definition 2.4.1 *Let R be a nearring and G a R-module.*

a) A normal subgroup I of R^+ is called ideal of R, denoted $I \trianglelefteq R$, if

i) $RI \subseteq I$

ii) $(r+x)s - rs \in I$, $\forall r,\ s \in R$, $\forall x \in I$.

If I has only the property i), it is called left ideal (denoted $I \trianglelefteq_l R$), if I has only the property ii), it is called right ideal (denoted $I \trianglelefteq_r R$).

b) A normal subgroup N of G^+ is called R-ideal of G, (denoted $N \trianglelefteq_R G$), if the element $(g+n)r - nr$ is contained in N for all $g \in G$ for all $n \in N$ and for all $r \in R$. In particular, the right ideals of R are the R-ideals of the regular R-module R_R.

c) A subgroup $U \leqslant G^+$ is called R-submodule of G (denoted $U \leqslant_R G$), if $UR \subseteq U$.

Corollary 2.4.2 *([24], Corollary 2.32) Let R be a nearring and Y be a subset of the R-module G. Then $(0:Y) = \mathcal{U}_R(Y) \trianglelefteq_r R$ and $\mathcal{U}_R(G) \trianglelefteq R$.*

Definition 2.4.3 *Let R be a nearring, K an ideal of R. Let*

$$R/K := \{K + r;\ r \in R\}$$

be the set of cosets of K in R. Then $(R/K, +, \cdot)$ is called the quotient nearring of R over K, where $+$ and $\cdot$ are defined by

$$(K + r_1) + (K + r_2) := K + r_1 + r_2$$

and

$$(K + r_1) \cdot (K + r_2) := K + r_1 r_2$$

for all $r_1,\ r_2 \in R$.

Theorem 2.4.4 *([24], Theorem 1.24) Let R be a nearring, K be an ideal of R. Then the quotient nearring of R over K is a nearring.*

Definition 2.4.5 *Let R be a nearring and let K be an ideal of R. Then $\pi : R \longrightarrow R/K$ defined by $r\pi = K + r$ is called the natural homomorphism associated with K.*

Theorem 2.4.6 *Let R and S be nearrings and $\alpha : R \longrightarrow S$ a nearring homomorphism. Then $Kern\ \alpha$ is an ideal of R. Moreover every ideal I of R is the kernel of a nearring homomorphism.*

Proof. Since $\alpha : R^+ \longrightarrow S^+$ is a group homomorphism, $Kern\ \alpha$ is a normal subgroup of R^+. Let $k \in Kern\ \alpha$ and $r,\ s \in R$. Then the following equalities hold.

$$(rk)\alpha = (r\alpha)(k\alpha) = (r\alpha)0_s = 0_s$$

and

$$\begin{aligned}((r+k)s - rs)\alpha &= (r\alpha + k\alpha)(s\alpha) - (r\alpha)(s\alpha)\\ &= (r\alpha + 0_s)(s\alpha) - (r\alpha)(s\alpha) = 0_s.\end{aligned}$$

Thus rk and $(r+k)s - rs \in Kern\ \alpha$. This means that $Kern\ \alpha$ is an ideal of R.

Define $\nu : R \longrightarrow R/I$ such that $r\nu := I + r$. It is easy to prove that ν is a homomorphism with $Kern\ \alpha = I$.

As in the case of nearrings, the R-ideals are the kernel of R-homomorphism between R-modules.

Definition 2.4.7 *(a) A nearring is called simple, if R and $\{0\}$ are the only ideals of R. An R- module is called simple, if it has no trivial R-ideals (cmp. [27]).*
(b) An ideal $I \trianglelefteq R$ is called maximal ideal, if $I \neq R$ and $I \trianglelefteq J \triangleleft R$ implies that $J = I$. Maximal left, right ideals and R-ideals are defined analogously.

Example 2.4.8 *Let R be a nearring. Then the zero-symmetric part R_0 is a right ideal of R. By the theorem (2.1.15), ${R_0}^+ \trianglelefteq R^+$, thus it is sufficient to show that for all $z \in R_0$ and all $r,\ s \in R$ the element $(r+z)s - rs$ is zero-symmetric. But this is true, since $0((r+z)s - rs) = (0r + 0z)s - 0rs = 0rs - 0rs = 0$.*

Note that, as for rings, the sum of two nearring ideals is still an ideal.

Lemma 2.4.9 *a) The group-theoretical sum of two right ideals K and L is a right ideal.*

b) The group-theoretical sum of two left ideals K and L is a left ideal.

c) The group-theoretical sum of two ideals K and L is an ideal.

Proof. Since K and L are normal subgroups of R^+ in the three cases (a), (b) and (c) the sum $K + L$ is also a normal subgroup of R^+.

(a) Let $s,\ r \in R$, $k \in K$ and $l \in L$. Then

$$(r+k+l)s - rs = (r+k+l)s \underbrace{-rs + (r+k)s}_{\in K} - (r+k+l)s + \underbrace{(r+k+l)s - (r+k)s}_{\in L}$$

Note that $-rs + (r + k)s \in K$ since K is a normal subgroup of R and $(r+k)s+rs \in K$. Thus $(r+k+l)s-rs+(r+k)s-(r+k+l)s \in K$ and moreover $(r+k+l)s-(r+k)s \in L$ since $r+k \in R$. Then $(r+k+l)s-rs \in K+L$.

(b) Let $r \in R$, $k \in K$ and $l \in L$. Then $r(k+l) = rk+rl \in K+L$ and so $K+L$ is a link ideal of R.

The property (c) follows from (a) and (b).

As in the ring theory, nearrings with identity element always contain maximal ideals.

Lemma 2.4.10 *Let R be a nearring with identity element, $I \lhd R$ a proper ideal of R. Then there is a maximal ideal $M \lhd R$ such that $I \subseteq M$.*

Proof. Let

$$\mathcal{S} = \{L \lhd R \mid I \subseteq L\}.$$

Since $I \in \mathcal{S}$, $\mathcal{S} \neq \emptyset$, and $\mathcal{S}$ is partially ordered by inclusion. Now let η be a chain in $\mathcal{S}$, and let $J := \bigcup\{L \mid L \in \eta\}$. For $L \in \eta$, $1_R \notin L$ since $L \neq R$. Thus $1_R \notin J$ and so $J \neq R$. Moreover, since η is a chain in S, it is easy to check that $J \trianglelefteq R$. By Zorn's lemma, $\mathcal{S}$ contains a maximal element M.

The following theorem shows that the factor nearring R/I of a nearring R modulo an ideal I is zero-symmetric if the constant part R_c is contained in the ideal I.

Theorem 2.4.11 *Let R be a nearring and I an ideal of R with $R_c \subseteq I$. Then R/I is zero-symmetric nearring.*

Proof. Let $r \in R$. Then $I(r+I) = (0+I)(r+I) = 0r+I = I$, since $0r \in R_c \subseteq I$.

In the ring theory, left and right ideals are often introduced as subgroups of additive group of ring, which are invariant under left or right multiplication (or both) with arbitrary ring elements. In the theory of nearrings the R-invariant subgroups are important.

Definition 2.4.12 *Let R be a nearring and $H \leqslant R^+$ be a subgroup of the additive group R^+.*

a) H is called left R-subgroup of R (denoted $H \leqslant_l R$), if $RH \subseteq H$.

b) H is called right R-subgroup of R (denoted $H \leqslant_r R$), if $HR \subseteq H$.

c) If H is both a right and a left R-subgroup, it is called two-sided R-subgroup or (R,R)-subgroup of R.

In the sequel, the right R-subgroup are called briefly R-subgroups.

Example 2.4.13 *Let R be a nearring. Then the constant part R_c is an (R,R)-subgroup of R, since the following equalities hold $0rc = c = rc$ and $0cr = cr$ for $r \in R$ and $c \in R_c$. By the lemma (2.1.17), rc, $cr \in R_c$*

The following result shows that in the zero-symmetric nearrings the right ideals are right R-subgroups. From this point of view, zero-symmetric nearrings are a bit closer to rings than general nearrings.

Lemma 2.4.14 *([24], Lemma 1.35) Let R be a nearring. If I is a right ideal of R then $IR_0 \subseteq I$. In particular, if $R = R_0$ is a zero-symmetric nearring, every right ideal is a right R-subgroup, and every ideal is a (R,R)-subgroup of R.*

Lemma 2.4.15 *If R is a nearring with identity and B is a R-subgroup of R. Then*

$$(B : R) := \{r \in R \mid Rr \subseteq B\}$$

is the largest (R,R)-subgroup of R, which is contained in B.

Proof. $(B : R) \subseteq B$, since $r = 1r \in B$ for all $r \in (B : R)$. Note that $(B : R)$ is a (R,R)-subgroup of R, as the following equalities hold for all $r \in R$ and $b \in (B : R)$:

$$R(br) = (Rb)r \subseteq Br \subseteq B,$$

i.e., $br \in (B : R)$ and $(B : R)R \subseteq (B : R)$.

$$R(rb) = Rb \subseteq B,$$

i.e., $rb \in (B : R)$ and $R(B : R) \subseteq (B : R)$.

Let U be a proper (R,R)-subgroup of R in B. Since U is a link R-subgroup of R, for all the elements $u \in U$, $Ru \subseteq U \subset B$. Thus $u \in (B : R)$ and $U \subseteq (B : R)$. This means that $(B : R)$ is the largest (R,R)-subgroup in B.

Chapter 3

Nearrings and radical theory

3.1 Monogenic R-modules and modules of type ν

In ring theory the Jacobson radical $\mathcal{J}(R)$ of a ring R plays an important role (cmp. [9]). There are several different definitions of the Jacobson radical in ring theory. Unfortunately, these definitions lead to different concepts when generalized to nearrings. In the following, a few useful generalizations of Jacobson radical for nearrings are introduced. These are closely connected to quasiregularity for nearrings, as the usual quasiregualrity is connected to the Jacobson radical in ring theory.

Many notions which are collected in the following, can be found in [24]

Definition 3.1.1 *Let R be a nearring and G be an R-module. The R-module G is called monogenic, if there exists a $g \in G$ such that $gR = G$, in other terms $G = \{gr \mid r \in R\}$. An element $g \in G$ such that $G = gR$ is called a generator of G.*

Proposition 3.1.2 *Let G be a monogenic R-module and R be a nearring with identity, then $g1 = g$ for all $g \in G$.*

Proof. Let $h \in G$ be a generator of G, and let $g \in G$ an arbitrary element. Then there is an element $r \in R$ with $g = hr$. It follows that $g1 = (hr)1 = h(r1) = hr = g$.

Definition 3.1.3 *Let G be a monogenic R-module. Then*

- *G is an R-module of type 0, if G is simple, i.e., it has not non-trivial proper R-ideals;*

- *G is an R-module of type 1, if G is simple and for all $g \in G$, either $gR = G$ or $gR = \{0\}$;*
- *G is an R-module of type 2, if G has not non-trivial proper R-submodules.*

Note that R-modules of type 2 are also of type 1, and those of type 1 are also of type 0.

Lemma 3.1.4 *If R is a nearring with identity and G is an R-module of type 2, then $G = gR$ for all $g \in G - \{0\}$.*

Proof. For every $g \in G$, the set gR is a submodule of G, since for r, $s \in R$ the following properties hold $gr+gs = g(r+s) \in gR$ and $(gr)s = g(rs) \in gR$. Since G is of type 2, $gR = \{0\}$ or $gR = G$. But $g = g1 \in gR$, and hence, if $g \neq 0$, then $gR = G$.

Using R-modules of type ν, it possible to define the radicals $\mathcal{J}_\nu(R)$ for a zero-symmetric nearring R. Note that if R is a ring, these three radicals coincide with the Jacobson radical of R.

Definition 3.1.5 *Let R be a nearring. For $\nu \in \{0,\ 1,\ 2\}$ the ν-radical $\mathcal{J}_\nu(R)$ is*

$$\mathcal{J}_\nu(R) = \bigcap \{\mathcal{U}_R(G) \mid G \text{ is an } R - \text{module of type } \nu\}.$$

If there are no R-modules of type ν, then put $\mathcal{J}_\nu(R) = R$.

Remark 3.1.6 For zero-symmetric nearrings R, Beidleman ([4]) defines the radical $\mathcal{J}(R)$ as the intersection of all right ideals of R which are maximal as R-subgroups. Using the result (3.1.4), it is easy to see that $\mathcal{J}(R) = \mathcal{J}_2(R)$.

Definition 3.1.7 *([4]) Let R be a zero-symmetric nearring and B a right ideal of R. B is called modular, if B is maximal as R-subgroup.*

Definition 3.1.8 *Let R be a zero-symmetric nearring, put*

$$I := \{B \mid B \text{ is a modular right } R - \text{subgroup}\}.$$

Then the radical $\mathcal{J}(R) = \cap_{B \in I} B$. If $I = \emptyset$, then put $\mathcal{J}(R) = R$ and R is called radical nearring.

Theorem 3.1.9 *Let R be a zero-symmetric nearring, with $R \neq R\mathcal{J}(R)$, then the radical $\mathcal{J}(R)$ is an ideal.*

Proof. Since $\mathcal{J}(R)$ is a right ideal, it is sufficient to prove that $\mathcal{J}(R)$ is a link ideal. By contradiction suppose that $R\mathcal{J}(R) \not\subseteq \mathcal{J}(R)$. Then there exists a modular right ideal B, such that $R\mathcal{J}(R) \not\subseteq B$. Moreover $B \subset R\mathcal{J}(R) + B \subseteq R$. Since $\mathcal{J}(R)$ is a right ideal, $R\mathcal{J}(R)$ is a R-subgroup. By (2.4.9), $R\mathcal{J}(R)+B$ is a R-subgroup and it is equal to R since B is a maximal R-subgroup. Moreover for every $j \in \mathcal{J}(R)$ and for every $b \in B$ it follows that

$$(1+j)b - b \in \mathcal{J}(R) \subseteq R\mathcal{J}(R) = R - B.$$

This means that $(1+j)b - b = r - b'$ for an element $b' \in B$ and $r \in R$. Thus $(1+j)b = r - b' + b \in R - B = RJ(R)$. For $j = 0$, it follows that $b \in RJ(R)$ and so $B \subseteq RJ(R)$. Hence $R = RJ(R)$ which is a contradction.

3.1.1 Quasiregularity in nearrings

In the following some results about quasiregularity in the theory of nearrings are collected. The concept of quasiregularity defined in ring theory can be generalized to nearrings theory. The definition of quasiregularity seems to be more complicated in nearrings theory because of the lack of the right distributive law. For a detailed description of this topic see [4] and [24].

Definition 3.1.10 *[24] Let R be a nearring. The element $z \in R$ is said to be right quasiregular, if z is contained in the right ideal of R generated by $\{x - zx \mid x \in R\}$. A subset X of R is called quasiregular if every element of X is right quasiregular.*

If R is a zero-symmetric nearring with identity element 1, Beidleman [4] calls the element $z \in R$ right quasiregular, if there exists an element $r \in R$ such that $(1 - z)r = 1$. More precisely:

Definition 3.1.11 *Let R be a zero-symmetric nearring with identity. An element $r \in R$ is called quasiregular, if there exists an element $s \in R$ such that $(1 - r)s = 1$ and a subset is called quasiregular if every element is quasiregular.*

Remark 3.1.12 If z is quasiregular in the sense of Beidleman, then z is right quasiregular in the sense of Meldrum [24]. Indeed, let z be right quasiregular in the sense of Beidleman [4], $r \in R$ with $(1 - z)r = 1$, and let I be the right ideal generated by $\{x - zx \mid x \in R\}$. Then $1 - z \in I$, and since R is zero-symmetric, I is an R-subgroup of R by (2.4.14). Hence $z = 1 \cdot z = (1 - z)rz \in I$.

Note that the definitions of Beidleman [4], and Meldrum [24] are not equivalent, even for zero-symmetric nearrings with identity.

Theorem 3.1.13 *If B is a quasiregular R-subgroup of a zero-symmetric nearring R, then B is contained in the radical $\mathcal{J}(R)$ of R.*

Proof. Assume that $B \nsubseteq \mathcal{J}(R)$. Then there exists a modular right ideal B' such that $B \nsubseteq B'$. By ([4], lemma (1.2)), $R = B' + B$, since B' is a maximal R-subgroup. If $1 = b' + b$, where $b' \in B'$, $b \in B$, then $1 - b = b' \in B'$. Now B is quasiregular and so there is an element $r \in R$ such that $1 = (1 - b)r = b'r \in B'$, a contradiction. Hence, $B \subseteq \mathcal{J}(R)$.

Let R be a nearring and B a proper R-subgroup of R. Since R contains an identity element 1, it follows by Zorn's lemma that B is contained in a maximal R-subgroup. In particular, R contains a maximal R-subgroup. Therefore, the collection $\mathcal{L}$ of all maximal R-subgroups of R is non-empty.

Definition 3.1.14 *Let $\mathcal{L}$ be the collection of all maximal R-subgroups of R. Then the R-subgroup $A = \cap_{B \in L} B$ is called the radical-subgroup of R.*

Clearly, the radical-subgroup A of a nearring R is a R-subgroup of R. By its definition, it follows that $A \subseteq \mathcal{J}(R)$.

Theorem 3.1.15 *The radical-subgroup A of a nearring R is a quasiregular R-subgroup that contains all quasi-regular right ideals of R.*

Proof. Let a be an element of A. Show that $(1 - a)R = R$. For if $(1 - a)R$ is a proper R-subgroup, then $(1 - a)R$ is contained in a maximal R-subgroup B. Therefore, $1 = (1 - a) + a \in B$, a contradiction. Since $(1 - a)R = R$ there is an element $r \in R$ such that $(1 - a)r = 1$, and therefore A is quasi-regular R-subgroup.

Assume A' is non-zero quasi-regular right ideal of R. If A' is not contained in the radical-subgroup A, then there exists a maximal R-subgroup B such that A' is not contained in B. By ([4], Lemma (1.2)), $R = A' + B$, since B is a maximal R-subgroup. Let $1 = b + a'$, where $b \in B$, $a' \in A'$. Then, since A' is quasi-regular, there exists an element $r \in R$ such that $1 = (1 - a')r = br \in B$, a contradiction. Therefore, A' is contained in A.

Corollary 3.1.16 *([4], Corollary 2.3) The group sum of two quasi-regular right ideals of R is a quasi-regular right ideal.*

Corollary 3.1.17 *([4], Corollary 2.4) The radical $\mathcal{J}(R)$ of a nearring R is quasi-regular ideal if, and only if, $\mathcal{J}(R) = A$ where A is the radical-subgroup of R.*

Appealing (3.1.15), the following result holds:

Corollary 3.1.18 *([4], Corollary (2.5)) If A is the radical-subgroup of R, then $(A : R)$ is a quasi-regular two-sided R-subgroup that contains all the quasi-regular ideals of R.*

Corollary 3.1.19 *([4], Corollary 2.6) If $(A : R) = \{0\}$, then R contains no proper non-zero quasi-regular ideals.*

As for rings, it is possible to define nil and nilpotent subsets for nearrings, as well as nilpotent elements.

Definition 3.1.20 *Let R be a nearring. An element $x \in R$ is called nilpotent, if there is a positive integer n such that $x^n = 0$. A subset $X \subseteq R$ is called nil, if all elements of X are nilpotent. A subset $X \subseteq R$ is called nilpotent, if there is a positive integer n such that*

$$X^n = \{r_1 \cdot \cdots \cdot r_n \mid r_i \in X\} = \{0\}$$

By the previous definitions (3.1.20) it follows that every nilpotent subset of R is nil.

The following lemma is well-known in ring theory, and hold also for nearrings.

Lemma 3.1.21 *A nilpotent element of a nearring R is right quasiregular. In particular, a nil subset of R is quasiregular.*

Proof. Let $z \in R$ be a nilpotent element. Then there is a positive integer n with $z^n = 0$. Let K be the right ideal of R generated by $\{x - zx \mid x \in R\}$. Then for all $i \geq 1$ the element $z^i - zz^i = z^i - z^{i+1} \in K$. In particular, $z = z - z^n = \sum_{i=1}^{n}(z^i - z^{i+1}) \in K$. Hence z is right quasiregular.

The following definition will be useful in the proof of (3.1.24).

Definition 3.1.22 *Let R be a nearring and X, $Y \neq \emptyset$ X, $Y \subseteq R$. Then*

$$C_Y(X) := \{y \in Y \mid Xy \subseteq R_c\}$$

Theorem 3.1.23 *([24], Theorem 5.38) Let R be a zero-symmetric nearring with descending chain condition for R-subgroups. Then every quasiregular R-subgroup H of R is nilpotent.*

This may be generalized as follows:

Theorem 3.1.24 *Let R be a nearring with identity element which satisfies the descending chain condition for R-subgroups. Let H be an R-subgroup of R with $H+1 \subseteq R^*$. Then there is a positive integer n such that $H^n = H \cap R_c$.*

Proof. For $k \in \mathbb{N}$, let H_k be the R-subgroup of R generated by H^k. Then

$$H = H_1 \supseteq H_2 \supseteq \cdots H_{k-1} \supseteq H_k \supseteq H_{k+1} \cdots \supseteq$$

is a descending chain of R-subgroups. By the chain condition, there is a least positive integer n with $H_n = H_{n+1}$. First, it is clear that $H \cap R_c \subseteq H^k$ for all k, and hence $H_k \cap R_c = H \cap R_c$. Let $K = H_n$, show that $K = H \cap R_c$.

Assume that $K \neq H \cap R_c$. If K_2 is the R-subgroup generated by $\{k_1 k_2 \mid k_1,\ k_2 \in K\}$, then $K_2 \geq H_{2n} = H_n = K$. Hence $K_2 = K$. Now consider the set

$$\mathcal{S} = \{L \mid L \leq_r R,\ L \subseteq K,\ LK \neq H \cap R_c\}.$$

(Note that $H \cap R_c$ is always contained in XK for $X \subseteq R$). Since $K = K_2$ is the R-subgroup generated by K^2 and $K \neq H \cap R_c$, $K^2 \neq H \cap R_c$. Thus $K \in \mathcal{S}$. By the descending chain condition, $\mathcal{S}$ contains a minimal element M. Since $MK \neq H \cap R_c$, there is an element $m \in M$ with $mK \neq H \cap R_c$. It follows that mK is an R-subgroup of R contained in K. Now $(mK)K = H \cap R_c$ would mean that $mK^2 = H \cap R_c$. But then $K^2 \subseteq \mathcal{C}_R(m) \leq_r R$, and hence $\mathcal{C}_R(m) \supseteq K_2 = K$ (c. f. Definition (3.1.22)). This is a contradiction since $mK \neq H \cap R_c$, and thus $(mK)K \neq H \cap R_c$ and $mK \in \mathcal{S}$. Moreover, $mK \subseteq M$ and by the minimality of M, it follows that $mK = M$.

Let $x \in K$ with $mx = m$. Then $mxr = mr$ and hence $xr - r \in \mathcal{U}_R(m)$ for all $r \in R$. Since $H + 1 \subseteq R^*$, $-x + 1 \in \mathcal{U}_R(m) \cap R^*$. It follows

$$m = \underbrace{m(-x+1)}_{=0}(-x+1)^{-1} = 0(-x+1)^{-1} \in R_c.$$

Then $mk \in R_c$ for all $k \in K$ and thus $mK = H \cap R_c$, which is a contradiction. Hence $K = H \cap R_c$.

3.2 Nearfields

This chapter is devoted to the study of nearfields, an important class of nearrings. An overview of the theory of nearfields can be found in Waehling [35].

Definition 3.2.1 *A nearring F is called nearfield, if $F - \{0\}$ is a multiplicative group. A nearfield which is not a skew-field is called a proper nearfield.*

Example 3.2.2 *([35])*

- *Every skew-field and every field is a nearfield.*

- *Let $p \neq 2$ be a prime number and $\mathbb{F}_{p^2} = (F, +, \cdot)$ be the Galois field with p^2 elements. Consider the two binary operations the addition "+" defined in the usual way and the multiplication "$\circ$", defined as follows:*

$$y \circ z = \begin{cases} yz & \text{if there exists an element } x \text{ with } y = x^2 \\ yz^p & \text{otherwise} \end{cases}$$

$(F, +, \circ)$ forms a nearfield. For $p = 3$, $(F, +, \circ)$ is the smallest non-trivial nearfield.

Remark 3.2.3 Let x and y elements of F, with $xy = 0$ and $x \neq 0$. Then $y = x^{-1}xy = x^{-1}0 = 0$. If $y \neq 0$ then $x = 0$, which is a contradiction. Thus $y = 0$.

Corollary 3.2.4 *Let F be a nearfield. Then either $Char(F) = 0$ or $Char(F) = p$, with p a prime number.*

Theorem 3.2.5 *If F is a finite nearfield, then the additive group F^+ is abelian.*

Proof. Since F is a finite nearfield, then $Char(F) = p$, where p is a prime number. Thus $x \cdot p = x + \cdots + x = x(1 + \cdots + 1) = x(1 \cdot p) = 0$ for $x \in F$. This means that F^+ is a p-group. Let p^n be the order of F for some $n \in \mathbb{N}$ and K_1, $K_2 \cdots K_r$ be the conjugacy classes of the elements of F^+, which have at least two elements. Then $p^n = |Z(F^+)| + \sum_{i=1}^{r} |K_i|$, where clearly $|K_i| = |F^+ : C_{F^+}(x)|$ as K_i is the conjugacy class of $x \in F^+$. Then $p \mid |K_i|$ for every $i \in \{1, \cdots, r\}$. This means that $p \mid |Z(F^+)|$ and $Z(F^+) \neq \{0\}$. Hence there exists $a \in Z(F^+)$, $a \neq 0$. For x, $y \in F$, $y \neq 0$, $x + y = ya^{-1}(ay^{-1}x + a) = ya^{-1}(a + ay^{-1}x) = y + x$. This completes the proof.

Lemma 3.2.6 *Let R a nearfield. Then the set of all distributive elements of R is a division subring of R.*

Proof. It follows from (2.1.12) and (3.2.5).

Lemma 3.2.7 *Let F be a nearfield and let x, $y \in F$. Then the following equalities hold:*
(a) $x^2 = 1$ *if and only if* $x = 1$ *or* $x = -1$
(b) $(-1)x = x(-1)$
(c) $(-x)y = -xy = x(-y)$
(d) $-y - x = -x - y$.

Proof. (a) Let x be 1 or -1, then $x^2 = 1$. Suppose that $x^2 = 1$. It follows that

$$(-1)(1+1) = (-1) + (-1) = -(1+1) = (1+1)(-1).$$

Put $y := x - 1$ in the case $1 = -1$ and put $y := 1 + (-1 + x)2^{-1}$ in the case $2 = 1 + 1 \neq 0$.

If $1 = -1$, it follows that

$$xy = x(x-1) = x^2 - x = 1 - x = (1-x)(-1) = -(1-x) = x - 1 = y,$$

if $1 \neq -1$, then

$$\begin{aligned} xy &= x(1 + (-1+x)2^{-1}) \\ &= x + x(-1+x)2^{-1} = x + (-x+1)2^{-1} \\ &= 1 \underbrace{-1+x}_{=(-x+1)(-1)} + (-x+1)2^{-1} = 1 + (-x+1)(-1+2^{-1}) \\ &= 1 + (-x+1)(2^{-1}(-1)2 + 2^{-1}) \\ &= 1 + (-x+1)2^{-1}((-1)(1+1)+1) = 1 + (-x+1)2^{-1}((-1)+(-1)+1) \\ &= 1 + (-x+1)2^{-1}(-1) = 1 + (-x+1)(-1)2^{-1} = y \end{aligned}$$

In both cases if $y \neq 0$, it follows that $x = 1$ and if $y = 0$, in the first case $x = 1$ and in the second case $x = -1$.

(b) If $x = 0$ the thesis is proved. Suppose that $x \neq 0$, then $(x(-1)x^{-1})^2 = x(-1)x^{-1}x(-1)x^{-1} = 1$. Using the part (a), it follows that $x(-1)x^{-1} = -1$, i.e., $x(-1) = (-1)x$ or $x(-1)x^{-1} = 1$, i.e., $x(-1) = x$ and $-1 = 1$. Note that also in this case the equality $x(-1) = (-1)x$ holds.

(c) $(-x)y = (-x \cdot 1)y = x(-1)y =^{(b)} xy(-1) = -xy = x(-y)$.

(d) $-y - x = -(x+y) =^{(c)} (-1)(x+y) = (-1)x + (-1)y =^{(c)} -x - y$

Theorem 3.2.8 *If F is a nearfield, then the additive group F^+ is abelian.*

Proof. Let x, $y \in F$. By (3.2.7), $(-1)(-y-x) = (-1)(-x-y)$. Then $-(-y-x) = -(-x-y)$ and thus $x + y = y + x$.

3.2.1 Nearfields with periodic multiplicative groups.

In the following section nearfields above a Cernikov multiplicative group are studied. In particular, it will be proved that a nearfield above a Černikov multiplicative group is finite as well as a nearfield above a periodic multiplicative group of exponent p.

Lemma 3.2.9 *Let F be a nearfield and F^* be a periodic group. Then $Char(F) = p$ with p a prime number and F^+ is periodic.*

Proof. Since F has the identity element, consider the element $1+1 \in F$. If $1+1=0$ then $Char(F)=2$. Suppose that $1+1 \neq 0$, then $1+1 \in F^*$ and there exists $m \in \mathbb{N}$ such that $(1+1)^m = 1$. Thus $1 \cdot (2^m - 1) = 0$ and $Char(F) = p \neq 0$. This means that $pF = 0$ and F^+ is an elementary abelian p-group. In particular, F^+ is periodic.

Remark 3.2.10 Since every skew-field above a periodic multiplicative group is a field see [11], it follows easily the following result:

Lemma 3.2.11 *Let F be a nearfield and F^* be a periodic group. Then $K_F := \{a \in F \ / (x+y)a = xa + ya, \ \forall \ x, \ y \in F\}$ is a field.*

The proof of the following result can be found in [35].

Lemma 3.2.12 *Let F be an infinite nearfield, whose multiplicative group has a normal abelian subgroup of finite index n. Then $[F : K_F] \leq n!$.*

Definition 3.2.13 *Let G be a multiplicative group. Define*

$$\pi(G) = \{p \mid p \text{ a prime number}, \ x^p = 1, \ \text{for an element } x \in G - \{1\}\}$$

the set of all prime numbers which are the orders of the elements of G.

Lemma 3.2.14 *Let G be a Černikov group, then $|\pi(G)| < \infty$*

Proof. Since G is a Černikov group, there exists a normal abelian subgroup A of G with finite index, which is the direct product of n quasicyclic groups, $n \in \mathbb{N}$. It follows that $|\pi(A)| = n$. Let $g \in G - A$ an element of prime order, note that every element which belongs to the same coset has the same prime order. Since G has a finite number of cosets, it follows that $|\pi(G-A)| < \infty$. Thus $|\pi(G)| < \infty$.

The following result can be easily proved. For the sake of brevity the proof is omitted.

Lemma 3.2.15 *Let F be a nearfield with $Char(F) = p$, p a prime number and $F = \cup_{i=1}^{\infty} F_i$, where F_i is a finite subnearfield of F which belong to an ascending chain of F for every $i \in \mathbb{N}$. If F^* is infinite, then $\pi(F^*)$ is infinite.*

Corollary 3.2.16 *Let K be a field and K^* be a Černikov group. Then K is finite.*

Proof. Since K^* is a Černikov group, it is in particular a periodic group. Let $K = \cup_{i=1}^{\infty} K_i$ the union of the finite subfields K_i of an ascending chain of K^*. By (3.2.9), $Char(K) = p$ and by (3.2.14), it follows that $|\pi(K^*)| < \infty$. If $|K^*| = \infty$, then $|\pi(K^*)| = \infty$ by (3.2.15). This is a contradiction, thus K^* is finite and so K is finite.

Theorem 3.2.17 *Let F a nearfield and F^* is a Černikov multiplicative group. Then F is finite.*

Proof. Suppose F an infinite nearfield. By (3.2.12) $|F : K_F| < \infty$. Since F^* is a Černikov group, it is in particular a periodic group. Thus K_F is a field by (3.2.11) and so by the previous result (3.2.16) it is finite. Hence it follows that F is finite, which is a contradiction.

3.3 Prime rings

The prime field of a field is the subfield generated by the identity element. In general, it is not true that the subnearring generated by the identity element is a field but it turns out that such a structure is a commutative ring.

Definition 3.3.1 *Let R be a nearring with identity element 1. Then define $E_R := \langle 1 \rangle^+$. Furthermore, define $P_R = \{nm^{-1} \mid n \in E_R,\ m \in E_R \cap R^*\}$*

Definition 3.3.2 *Let R be a nearring with identity 1. Then P_R is called the prime ring of R.*

Lemma 3.3.3 *Let R be a nearring with identity 1. Then E_R and P_R are commutative rings.*

Proof. Let n, $m \in E_R$, i.e., there exist integers $\tilde{n}$, $\tilde{m}$ such that $n = 1 \cdot \tilde{n}$ and $m = 1 \cdot \tilde{m}$. If $\tilde{m} \geq 0$ then $nm = \underbrace{n + \cdots + n}_{\tilde{m} \text{ summands}} \in E_R$ and hence, if $\tilde{m} < 0$, then $nm = -(n(-m)) \in E_R$. Since $nm = (1 \cdot \tilde{n}) \cdot \tilde{m} = 1 \cdot (\tilde{n})(\tilde{m}) = 1 \cdot (\tilde{m})(\tilde{n}) = mn$, it is also clear that E_R is a commutative nearring with identity and hence a ring by (2.1.13).

It is clear that P_R is closed under multiplication and that $(P_R, \cdot)$ is a commutative semigroup. Thus it suffices to show that P_R is closed under addition. Let n, $x \in E_R$ and m, $y \in E_R \cap R^*$. Then it is not difficult to see that $nm^{-1} + xy^{-1} = (ny + mx)(my)^{-1}$. Hence P_R is a commutative nearring with identity and thus a ring by (2.1.13).

Lemma 3.3.4 *Let R be a nearring with identity 1 and $o^+(1) = n < \infty$. Then $E_R = P_R \cong \mathbb{Z}/n\mathbb{Z}$.*

Proof. It is clear that $E_R \cong \mathbb{Z}/n\mathbb{Z}$. Since an element of $\mathbb{Z}/n\mathbb{Z}$ which is not invertible is a zero-divisor, it cannot be invertible in R. Hence the inverses of invertible elements of E_R are contained in E_R and thus $E_R = P_R$.

Lemma 3.3.5 *([13], Lemma 4.3.4) Let R be a nearring with identity 1 and $o^+(1) = \infty$. Then $E_R \cong \mathbb{Z}$. There is a set π_R of primes such that an element $n \in E_R$ is invertible in R if and only if no prime $p \in \pi_R$ is a divisor of n. $P_R \cong \mathbb{Z}D^{-1}$, where $D = \mathbb{Z} - (\cup_{p\in\pi_R} p\mathbb{Z})$, i.e.,*

$$P_R \cong \{\frac{n}{m} \in \mathbb{Q} \mid \forall p \in \pi_R \ : \ p \nmid m\}.$$

Note that it is possible that π_R contains all prime numbers. In this case P_R is isomorphic to $\mathbb{Z}$.

Note that by (3.3.4) and by (3.3.5) P_R is always contained in R_0.

3.4 Construction subgroups

Definition 3.4.1 *Let R be a nearring with identity 1. Let $U \leq R^+$ such that $(U + 1) \leq R^*$. Then, U is called a construction subgroup of R.*

Proposition 3.4.2 *Let R be a nearring with identity and U be a construction subgroup of R. Then $(U + 1)U \subseteq U$.*

Proof. Let $A = U + 1 \leq R^*$. Since U is an additive group, for every a, $b \in A$, it follows that $a - b = a - 1 + 1 - b = (a - 1) - (b - 1) \in U$ since $a - 1$, $b - 1 \in U$. Now let u, $v \in U$ with $u = a - 1$ and $v = b - 1$ for suitable elements a, $b \in A$. Then $(u + 1)v = a(b - 1) = ab - a \in U$, since ab, $a \in A$.

Example 3.4.3 *(a) Let R be a nearring with identity. Then the trivial subgroup $\{0\}$ is a construction subgroup.*
(b) Let R be a nearring with identity 1. Then R_c is a construction subgroup of R, since $R_c + 1 \leq R^*$ by (2.1.19).
(c) Let p be a prime, $n \geq 1$ a positive integer, and $R = \mathbb{Z}/p^n\mathbb{Z}$. Then the subgroup pR of R is a construction subgroup of R.
(d) Let R be a ring with identity element. Then the Jacobson radical $\mathcal{J}(R)$ is a construction subgroup of R.

In the following, the structure of construction subgroups is investigated. In particular, for zero-symmetric nearrings some result are showed.

Proposition 3.4.4 *Let R be a zero-symmetric nearring with identity. If U is a construction subgroup, then U is quasiregular in the sense of Meldrum. If U is also an R-subgroup, U is contained in the radical $\mathcal{J}_2(R)$.*

Proof. Let U be a construction subgroup of the zero-symmetric nearring R, and let $x \in U$. Let I be the right ideal of R generated by $\{r - xr \mid r \in R\}$. Then $1 - x \in I$ and since $I^+ \trianglelefteq R^+$, also $-x + 1 \in I$. But since R is zero-symmetric and U is a construction subgroup, also $1 = (-x+1)(-x+1)^{-1} \in I$ by Lemma (2.4.14), and thus $I = R$. Hence $x \in I$ and so x is a right quasiregular element. The final part of the proposition follows immediately from Theorem (3.1.13).

The following theorem shows that every nearring with identity contains maximal construction subgroups.

Theorem 3.4.5 *Let R be a nearring with identity 1 and U be a construction subgroup of R. Then U is contained in a maximal construction subgroup. In particular, R contains maximal construction subgroups.*

Proof. Let $\mathcal{M}$ be the set of all construction subgroups of R which contain U. Since $U \in \mathcal{M}$, $\mathcal{M} \neq \emptyset$. Note that $\mathcal{M}$ is partially ordered by inclusion. Let $\mathcal{A}$ be the chain in $\mathcal{M}$ and let $V = \bigcup\{K \mid K \in \mathcal{A}\}$. Then V is a construction subgroup of R, since for $u, v \in V$ there is a group $K \in \mathcal{A}$ with $u, v \in K$, and hence $u-v \in K \subseteq V$, $u+1, v+1 \in R^*$ and $(u+1)(v+1)^{-1} \in K+1 \subseteq V+1$. By Zorn's Lemma, $\mathcal{M}$ contains a maximal element.

Lemma 3.4.6 *Let R be a zero-symmetric nearring with identity, $K \trianglelefteq_r R$ is quasiregular right ideal of R in the sense of Beidleman [4]. Then K is a construction subgroup.*

Proof. Since R is zero-symmetric, K is an R-subgroup. Since K is quasiregular in the sense of Beidleman ([4]), for every $k \in K$ the element $1-k$ is right invertible, and since K is a right ideal, $K + 1 = 1 + K$ and all the elements of $K + 1$ have a right inverse. Thus it is sufficient to show that these right inverses are contained in $K+1$ and that $K+1$ is closed under multiplication. First let $k \in K$ be an arbitrary element, $r \in R$ be the right quasi-inverse of $-k$, i.e., $(1 + k)r = 1$. Then $1 - (1 + k)r = 0$. Moreover, since K is a right ideal, $(1+k)r-r \in K$. This means that $1-(1+k)r+(1+k)r-r = 1-r \in K$ if and only if $r - 1 \in K$, and hence $r \in K + 1$. Now let $k.\ l \in K$. Then $(k + 1)(l + 1) = (k + 1)l + k + 1 = ((k + 1)l - l) + (l + k) + 1 \in K + 1$, and hence $K + 1$ is closed with respect to multiplication.

Lemma 3.4.7 *Let R be a nearring and U be a construction subgroup of R, and $I \trianglelefteq R$. Then $(U + I)/I$ is a construction subgroup of R/I.*

Proof. It is clear that $(U+I)/I$ is a subgroup of $(R/I)^+$. Now, let $u \in U$. Then there exists an element $v \in U$ such that $(u+1)(v+1) = 1$, and hence $((u+I)+(1+I))((v+I)(1+I)) = (u+1)(v+1)+I = 1+I$.

The following result shows that the sum of two construction subgroups can be a construction subgroup under special hypothesis.

Lemma 3.4.8 *Let R be a nearring with identity and let U and V be two construction subgroups with the additional property that $U+V = V+U$. If U and V are left R-subgroups, then $U+V$ is also a construction subgroup.*

Proof. Let U and V be left R-subgroups. Since $U+V = V+U$, it follows that $U+V$ is an additive group. Let u, $u' \in U$ and v, $v' \in V$, then

$$(u+v+1)(u'+v'+1) = \underbrace{\underbrace{(u+v+1)u'}_{\in U} + \underbrace{(u+v+1)v'}_{\in V} + u + v + 1}_{\in U+V}.$$

Moreover, since $RU \subseteq U$ and U and V are construction subgroups,

$$(v+1)^{-1}u + 1$$

is contained in $U+1$ and therefore

$$\begin{aligned}
&\big(((v+1)^{-1}u+1)^{-1}(v+1)^{-1}\big)(u+v+1)\\
&= ((v+1)^{-1}u+1)^{-1}\big((v+1)^{-1}(u+v+1)\big)\\
&= ((v+1)^{-1}u+1)^{-1}\big((v+1)^{-1}u+1\big)\\
&= 1,
\end{aligned}$$

in other words all the elements of $U+V+1$ are left invertible. But since $((v+1)^{-1}u+1)^{-1} \in U+1$ and $(v+1)^{-1} \in V+1$, it follows that $((v+1)^{-1}u+1)^{-1}(v+1)^{-1} \in U+V+1$. This means that $U+V+1$ is closed under multiplication and every element of $U+V+1$ is left invertible in $U+V+1$. Hence $U+V+1$ is a group under multiplication and thus $U+V$ is a construction subgroup.

The following result shows a relationship between the chain condition for subgroups of R^* and for construction subgroups of R.

Lemma 3.4.9 *Let R be a nearring with identity, and let R^* satisfy the ascending or descending chain condition on subgroups. Then R fulfils the ascending or descending chain condition for construction subgroups, respectively.*

Proof. Let R^* satisfy the ascending chain condition for subgroups. Furthermore, let $U_0 \leq U_1 \leq \cdots$ be an ascending chain of construction subgroups of R. Then $U_0+1 \leq U_1+1 \leq \cdots$ is an ascending chain of subgroups of R^* and hence there is an element $n \in \mathbb{N}$ with $U_n + 1 = U_m + 1$ for all $m \geq n$. Thus $U_n = U_m$ for $m \geq n$. The proof is similar for the descending chain condition.

By definition of construction subgroup, if U is a construction subgroup of a nearring R, then $U + 1$ is a subgroup of R^*. The following result shows that if U is also an ideal of R, then $U + 1$ is a normal subgroup of R^*.

Lemma 3.4.10 *Let R be a nearring with identity and U be a construction subgroup of R which is an ideal of R. Then $U + 1$ is normal in R^*.*

Proof. Since U is an ideal of R, the canonical epimorphism $\sigma : R \longrightarrow R/U$ can be restricted to the set R^*. Since σ is a nearring homomorphism, $\sigma|R^*$ is a group homomorphism $R^* \longrightarrow (R/U)^*$. Clearly, $U + 1$ is the kernel of $\sigma|R^*$, and hence $U + 1$ is normal in R^*.

Chapter 4

Local Nearrings

The study of local nearrings was begun by Maxson [20]-[23] and continued by several other authors. In particular, it was shown in [12] that if R is a local nearring with identity 1 and L_R is the subgroup of all non-invertible elements of R, then the set $1 + L_R$ is a subgroup of the multiplicative group R^* of R acting on L_R by left multiplication, so that the semidirect product $L_R \rtimes (1 + L_R)$ is a group of the form $G = AB = AM = BM$ with a normal subgroup M isomorphic to L_R and with subgroups A and B isomorphic to $1 + L_R$. Thus, in many cases the study of local nearrings can be reduced to that of groups of this form, so called triply factorized groups (cmp. Chapter 1). First, this approach was partly used in [15] where the author studied local nearrings with abelian multiplicative group and explicitly applied in [2] and in [33] where the investigation is concerned with local nearrings with dihedral multiplicative group and generalized quaternion group rispectively.

4.1 Basic properties of local nearrings

Local nearrings belong to a large class of nearrings containing non-trivial construction subgroups and hence are useful for the construction of triply factorized groups. They were first introduced by Maxson [20] as a generalization of local rings. In the following subsection some basic properties of local nearrings are described. In particular, the structure of additive group and the group of units of local nearrings are studied.

4.1.1 Structure of local nearrings

In the following, only nearrings R with identity 1 are considered. Most of the following results are proved in the case of zero-symmetric nearrings in [20].

Definition 4.1.1 *Let R be a nearring. The set of elements of R, which have not right inverses, will be denoted as L_R, i.e.,*

$$L_R = \{k \in R \mid kR \neq R\}$$

Definition 4.1.2 *The nearring R is called a local nearring, if L_R is an R-subgroup of R.*

Theorem 4.1.3 *([20], Theorem 2.2) Let R be a local nearring. Then the subgroup L_R is the unique maximal R-subgroup of R.*

The following theorem gives an important criterion for a nearring to be local.

Theorem 4.1.4 *([20], Theorem 2.3) The nearring R is local if and only if L_R is a subgroup of R^+.*

The next result shows that a local nearring R is the set theoretical union of the group R^* of units of R and the R-subgroup L_R. Thus every element of R is either a unit or contained in L_R.

Lemma 4.1.5 *Let R be a local nearring. Then the elements of L_R has no left inverses and the elements of $R - L_R$ are units.*

Proof. Assume that $l \in L_R$ has a left inverse r, i.e., $rl = 1$. Then $lr \in L_R$ and hence $1 - lr \notin L_R$. Therefore there exists an element $t \in R$ with $1 = (1 - lr)t$. This implies that $r = r(1 - lr)t = 0t$, and hence $1 = rl = 0tl \in R_c$. Since $1 \in R_0$, this yields that $1 = 0$ by Theorem (2.1.15) a contradiction. Thus, the elements of L_R have no left inverses.

Now let $r \in (R - L_R)$. Then there is an element $s \in R$ with $rs = 1$. By the above argument, $s \notin L_R$, and hence there is an element $t \in R$ such that $st = 1$. But then $r = r \cdot 1 = r(st) = (rs)t = t$. Hence, r is a unit and so $R^* = R - L_R$.

Corollary 4.1.6 *Let R be a local nearring, then L_R is a (R, R)-subgroup of R.*

The following two results show that there is a connection between local nearrings and triply factorized groups.

Proposition 4.1.7 *Let R be a local nearring. Then L_R is a construction subgroup of R.*

Proof. It is clear that $L_R + 1 \subseteq R^*$. Thus let k, $l \in L_R$. Then

$$(k+1)(l+1) = (k+1)l + k + 1 \in L_R + 1.$$

Moreover, let $l' = (l+1)^{-1}$. Then $1 = l'(l+1) = l'l + l'$ and hence $l' = -l'l + 1 \in L_R + 1$. Thus $L_R + 1$ is a group with respect to the multiplication.

Lemma 4.1.8 *([2], Lemma 3.12(2)) Let R be a local nearring with identity 1. Then the subgroup L_R is invariant under the action of R^* on R^+ by left multiplication and the semidirect product $G = L_R \rtimes (1 + L_R)$ has subgroups A and B isomorphic to $1 + L_R$ such that $G = AB = L_R \rtimes A = L_R \rtimes B$ and $A \cap B = 1$.*

Lemma 4.1.9 *Let R be a nearring. Then $R_c \subseteq L_R$.*

Proof. Assume that $x \in R_c$ is an invertible element. Then there is an element $y \in R$ with $1 = yx = x \in R_c$. By the corollary (2.1.16), $1 \in R_0$ and by the theorem (2.1.15), $R_c \cap R_0 = \{0\}$, a contradiction to $1 \neq 0$.

Corollary 4.1.10 *([13], 5.19) Let L_R be nil, then R is a zero-symmetric local nearring.*

The following result shows that a local nearring always contains a zero-symmetric local subnearring.

Proposition 4.1.11 *Let R be a local nearring. Then R_0 is also local. Moreover, $L_{R_0} = L_R \cap R_0$.*

Proof. If $l \in L_R \cap R_0$, then $l \in L_{R_0}$. Now let $l \in L_{R_0}$. Note that l cannot be a unit in R, since the inverses of zero-symmetric units are also zero-symmetric by Proposition (2.1.18). Hence $l \in L_R$ and thus $L_{R_0} = L_R \cap R_0$ is an additive group. By Theorem (4.1.4), R_0 is local.

It is well-known that for local rings R the group L_R is always an ideal of R which coincides with the Jacobson radical $\mathcal{J}(R)$. A similar result can be stated for local nearrings R, if $R \neq \mathcal{J}_2(R)$, but it seems to be still unknown whether a local nearring R with $R = \mathcal{J}_2(R)$ exists or not.

Lemma 4.1.12 *If R is a zero-symmetric local nearring, then L_R is a quasiregular R-subgroup of R and $L_R \subseteq \mathcal{J}_2(R)$.*

Proof. Since R is zero-symmetric, L_R is a quasiregular R-subgroup by (3.1.6) and hence it is contained in $\mathcal{J}_2(R)$ by (3.1.13).

Remark 4.1.13 (a) If R is a zero-symmetric local nearring with descending chain condition for R-subgroups, then L_R is nilpotent by (3.1.23).
(b) If R is local nearring with descending chain condition for R-subgroups then by (3.1.24), and (4.1.9) there exists $n \in \mathbb{N}_0$ with ${L_R}^n = R_c$.

As for rings it is possible to show that non-trivial factor nearrings of local nearrings are likewise local.

Lemma 4.1.14 *Let R be a local nearring and $I \lhd R$ a proper ideal of R. Then the factor nearring R/I is local.*

Proof. Since I is a proper ideal, $I \leq L_R$. Thus L_R/I is an additive subgroup of $(R/I)^+$. For $r \in R^*$, $(r+I)(r^{-1}+I) = 1+I$, and hence $r+I \in (R/I)^*$. Now let $l \in L_R$ and assume that there is an element $k+I \in R/I$ with $(l+I)(k+I) = 1+I$. This means that $lk-1 \in I$. But since $I \leq L_R$ and $lk-1 \notin L_R$, this is a contradiction. Hence, $L_{R/I} = L_R/I$ and R/I is local.

The following theorem gives a criterion for L_R to be an ideal of the local nearring R.

Lemma 4.1.15 *([20], Theorem 2.10) If R is zero-symmetric nearring with $\mathcal{J}_2(R) \neq R$, then R is local if and only if $L_R = \mathcal{J}_2(R)$. The subgroup L_R is an ideal of R if and only if $R \neq \mathcal{J}_2(R)$.*

Corollary 4.1.16 *([20], Corollaries 2.11 and 2.12) Let R be a local nearring with $L_R \trianglelefteq R$.*
(a) The factor nearring R/L_R is a nearfield. In particular, R/L_R is abelian.
(b) R is simple if and only if R is a nearfield.

4.1.2 The additive group R^+

Let R be a local nearring. If there is a positive integer n, such that $1 \cdot n \in L_R$, then R is said to satisfy *the Property $(\mathcal{P})$*.

Now, let $K = \{n \in \mathbb{N} \mid 1 \cdot n \in L_R\}$. Then K has a minimal element n_0. If n_0 is a composite number, say $n_0 = n_1 n_2$, with $1 < n_i < n_0$ for $i \in \{1,\ 2\}$, then $1 \cdot n_i \in R^* = R - L_R$ for $i \in \{1,\ 2\}$ and hence $1 \cdot n_0 = 1 \cdot (n_1 n_2) = (1 \cdot n_1)(1 \cdot n_2) \in R^*$, a contradiction. Thus n_0 is a prime number.

As consequence of that, R fulfils the Property $(\mathcal{P})$ if and only if there is a prime p with $1 \cdot p \in L_R$.

Proposition 4.1.17 *Let R be a local nearring satisfying the Property $(\mathcal{P})$, and let n, m be positive integers with $1 \cdot n$ and $1 \cdot m \in L_R$. If d is the greatest*

common divisor of n and m, then $1 \cdot d \in L_R$. In particular, the prime p with $1 \cdot p \in L_R$ is uniquely determined.

Proof. Since d is the greatest common divisor of n and m, there are integral numbers x and y with $d = nx + my$. But then $1 \cdot d = 1 \cdot (nx + my) = (1 \cdot n) \cdot x + (1 \cdot m) \cdot y \in L_R$. It is clear now that p must be a divisor of all $n \in \mathbb{N}$ with $1 \cdot n \in L_R$.

The following result shows that if L_R has finite exponent and is non-trivial, it follows that R satisfies the Property $(\mathcal{P})$.

Lemma 4.1.18 *Let R be a local nearring, and let ${L_R}^+$ have finite exponent. Then R is a nearfield or R satisfies the Property $(\mathcal{P})$.*

Proof. Assume that R is not a nearfield, i.e., $L_R \neq \{0\}$. Let $n = exp({L_R}^+)$ and assume that R does not satisfy the Property $(\mathcal{P})$. Then $1 \cdot n \in R^*$, i.e., there is an $x \in R$ with $(1 \cdot n)x = 1$. But then $l = l(1 \cdot n)x = (l \cdot n)x = 0x$ for all $l \in L_R$. By Corollary (2.1.16), $1 \cdot n$ is zero-symmetric, so that by Propostion (2.1.18), it follows that x is zero-symmetric. Thus, $l = 0x = 0$ for all $l \in L_R$, a contradiction to $L_R \neq \{0\}$. Hence $1 \cdot n \in L_R$ and R satisfies the Property $(\mathcal{P})$.

The next theorem and the subsequent corollary give some information about the structure of the additive group of a local nearring with certain finiteness conditions. In particular, it turns out that the additive group of a finite local nearring is always a p-group for some prime number p.

Theorem 4.1.19 *If R is a local nearring with descending chain condition for R-subgroups and with the Property $(\mathcal{P})$, then R^+ is a p-group for the prime p with $1 \cdot p \in L_R$.*

Proof. The proof for the zero-symmetric case can be found in Maxson ([20], Theorem 7.4). Here, the proof for the general case will be given.

Let p be the prime with $1 \cdot p \in L_R$ and consider the chain

$$L_R \supseteq (1 \cdot p)L_R \supseteq (1 \cdot p)^2 L_R \supseteq \cdots \supseteq (1 \cdot p)^{k-1} L_R \supseteq (1 \cdot p)^k L_R \supseteq \cdots .$$

Since rL_R is an R-subgroup of R for all $r \in R$, in the above chain, there exists some $k \in \mathbb{N}$ with $(1 \cdot p)^{k-1} L_R = (1 \cdot p)^k L_R$. This means that $(1 \cdot p)^k = (1 \cdot p)^k l_1$ for a suitable $l_1 \in L_R$, i.e., $(1 \cdot p)^k (1 - l_1) = 0$. Since $1 - l_1 \in R^*$, there is an element $x = (1 - l_1)^{-1}$. Then $(1 \cdot p)^k = (1 \cdot p)^k (1 - l_1)x = 0x$, which is a constant element by Lemma (2.1.17). By Corollary (2.1.16), $(1 \cdot p)^k = 1 \cdot p^k \in R_0$, i.e., $0x = (1 \cdot p)^k \in R_c \cap R_0 = \{0\}$. Hence $o^+(1) \mid p^k$, and by Corollary (2.1.22) R^+ is a p-group.

Corollary 4.1.20 *The additive group of a local nearring R, whose subgroup L_R is finite and non-trivial, is a p-group for a prime p. In particular, the additive group of a finite local nearring is always a p-group (even if L_R is trivial).*

Proof. Since L_R is the unique maximal R-subgroup of R, all proper subgroups of R lie in L_R. But since L_R is finite, R satisfies the descending chain condition on R-subgroups. By Lemma (4.1.18), R satisfies the Property $(\mathcal{P})$, and hence R^+ is a p-group by Theorem (4.1.19). If R is finite, R satisfies the Property $(\mathcal{P})$ as well as the descending chain condition for R-subgroups, even if L_R is trivial.

Corollary 4.1.21 *Let R be a local nearring. Then $|R^*|$ is odd, if and only if R is a finite nearfield of characteristic 2.*

Proof. If R is a finite nearfield of characteristic 2, it is clear that $|R^*|$ is odd.

Let $|R^*|$ be odd, in particular finite. Since $L_R + 1 \subseteq R^*$ and $|L_R + 1| = |L_R|$, L_R and hence R is finite. By Corollary (4.1.20), $|R| = p^n$ and $|L_R| = p^m$ for a prime p and non-negative integers n and m with $m < n$. This means that $|R^*| = p^n - p^m = p^m(p^{n-m} - 1) \equiv 1 \pmod 2$. Since the number $p^{n-m} - 1$ is odd, it follows that $p = 2$. But then p^m is odd only for $m = 0$, i.e., $|L_R| = 1$. Hence R is a nearfield.

The following result shows an useful connection between the nilpotency of L_R and the exponent of the additive group ${L_R}^+$.

Proposition 4.1.22 *Let R be a local nearring. If R^+ is a p-group for a prime p and ${L_R}^n = \{0\}$ for some $n \in \mathbb{N}$ then $exp({L_R}^+) \leq p^{n-1}$.*

Proof. Since $o^+(1) = p^l$ for some $l \in \mathbb{N}$. It follows that $0 = 1 \cdot p^l \in L_R$ and hence $p \in L_R$. Let $l \in L_R$ be an arbitrary element. Then $l \cdot p^{n-1} \in {L_R}^n = 0$ and hence $l \cdot p^{n-1} = 0$. Thus $exp({L_R}^+)$ divides p^{n-1}.

4.1.3 The structure of L_R

It seems to be unknown whether there is a local nearring R with the property that L_R is not an ideal of R or not. It is even not known if L_R has to be a normal subgroup of the additive group R^+. But it is in fact possible to determine some structural facts about local nearrings R in which L_R is not a normal subgroup of R^+.

Lemma 4.1.23 *Let R be a local nearring in which the additive subgroup ${L_R}^+$ is not normal in the additive group R^+. Then ${L_R}^+$ concides with its normalizer $N_{R^+}({L_R}^+)$.*

Proof. Since ${L_R}^+$ is not normal in R^+, there is an element $r \in R^*$ and an element $k \in L_R$ with $-r+k+r \notin L_R$. This means that $r^{-1}(-r+k+r) = -1+r^{-1}k+1 \in R^*$. Hence, for arbitrary $s \in R^*$, $-s+s(r^{-1}k)+s \notin L_R$. But $s(r^{-1}k) \in L_R$, hence $R^* \cap N_{R^+}({L_R}^+) = \emptyset$, and thus ${L_R}^+ = N_{R^+}({L_R}^+)$.

Theorem 4.1.24 *Let R be a local nearring with nil R-subgroup L_R. Then $L_R \trianglelefteq R$*

Proof. Let $l \in L_R$ and $r, s \in R$ and let n be the smallest integer with $l^n = 0$. Assume that the element $t = (r+l)s - rs$ does not belong to L_R. Then $l^{n-1}t = l^{n-1}(r+l)s - l^{n-1}rs = (l^{n-1}r + l^n)s - l^{n-1}rs = l^{n-1}rs - l^{n-1}rs = 0$. But if $t \in R^*$, multiplying with t^{-1}, from the right it follows that $l^{n-1} = 0$, contradicting the choice of n.

Thus, it suffices to show that ${L_R}^+ \trianglelefteq R^+$. But since $(r+l)s - rs \in L_R$ for all $r, s \in R$ and $l \in L_R$, with $r = -1$ and $s = 1$, it follows that $-1+l+1 \in L_R$. By Lemma (4.1.23), ${L_R}^+ \trianglelefteq R^+$.

Corollary 4.1.25 *Let R be a zero-symmetric local nearring with descending chain condition for R-subgroups. Then $L_R \trianglelefteq R$.*

Proof. L_R is quasiregular by Lemma (4.1.12), and hence nilpotent by Theorem (3.1.23). Thus, $L_R \trianglelefteq R$ by Theorem (4.1.24).

Lemma 4.1.26 *Let R be a local nearring.*
(a) If the group R^+ is not perfect, then ${L_R}^+ \trianglelefteq R^+$.
(b) If $L_R \trianglelefteq R$, then R^+ is not perfect.

Proof. *(a)* If R^+ is not perfect, $(R^+)'$ is a proper subgroup of R^+. Since $r[s,t] = [rs, rt]$ for all r, s, $t \in R$, $(R^+)'$ is a left R-subgroup of R, and hence is contained in L_R. This means that ${L_R}^+ \trianglelefteq R^+$.

(b) Now let $L_R \trianglelefteq R$. By Corollary (4.1.16), R/L_R is a nearfield. Hence, $R^+/{L_R}^+$ is an abelian group and thus $(R^+)' \subseteq L_R$. This means that R^+ is not perfect.

The following theorem shows that it is sufficient to investigate the zero-symmetric part of a local nearring to check if L_R is an ideal of R. Moreover, it is shown in (4.1.28), that in a finite local nearring R the R-subgroup L_R is always an ideal.

Theorem 4.1.27 *Let R be a local nearring. Then $L_R \trianglelefteq R$ if and only if $L_{R_0} \trianglelefteq R_0$.*

Proof. If $L_R \trianglelefteq R$, it is clear that $L_{R_0} \trianglelefteq R_0$. Consider the case $L_{R_0} \trianglelefteq R_0$. As in the proof of Theorem (4.1.24), it suffices to show that $t = (r+l)s - rs \in L_R$ for all r, $s \in R$ and all $l \in L_R$. Since $R^+ = R_0^+ \rtimes R_c^+$ the elements r, s and l can be uniquely written as $r = r_0 + r_c$, $s = s_0 + s_c$, and $l = l_0 + l_c$ with r_0, s_0, $l_0 \in R_0$ and r_c, s_c, $l_c \in R_c$.

Thus $t = (r+l)(s_0+s_c) - r(s_0+s_c) = (r+l)s_0 + s_c - s_c - rs_0 = (r+l)s_0 - rs_0$. Since L_R is a (R,R)-subgroup of R by Corollary (4.1.6), the element t is contained in L_R if $r \in L_R$ or $s \in L_R$. Hence it may be assumed that r, $s \in R^*$. Then $r^{-1}t = r^{-1}(r+l)s_0 - r^{-1}rs_0 = (1+r^{-1})s_0 - s_0$ and $r^{-1}t \in L_R$ if and only if $t \in L_R$. Thus it suffices to show that $t = (1+l)s - s \in L_R$ for all $s \in R_0{}^*$ and for all $l \in L_R$.

Now, $(1+l_0)^{-1}t = (1+l_0)^{-1}(1+l_0+l_c)s - (1+l_0)^{-1}s = (1+l_c)s - (1+l_0)^{-1}s = (1+l_c)s - s + s - (1+l_0)^{-1}s$. Since $L_{R_0} \trianglelefteq R_0$, $s - (1+l_0)^{-1}s \in L_{R_0} \leq L_R$, and hence $t \in L_R$ if and only if $(1+l_c)s - s \in L_R$. But if $(1+l_c)s - s \in R^*$, there is an element $x \in R^*$ with $1 = x((1+l_c)s - s) = (x+l_c)s - xs$. This means that $0 = 0 \cdot 1 = 0((x+l_c)s - xs) = (0x+l_c)s - 0xs$ and hence $(0x+l_c)s = 0xs$. Since s is invertible, $0x + l_c = 0x$ and hence $l_c = 0$. But this contradicts $(1+l_c)s - s \in R^*$. Hence $L_R \trianglelefteq R$.

Corollary 4.1.28 *If R is a finite local nearring, then L_R is an ideal of R.*

Proof. If R is zero-symmetric, then the subgroup L_R is nil (see [24], Theorem 5.38) and so L_R is an ideal of R by (4.1.24) and (4.1.6). The general case follows from Theorem (4.1.27).

Corollary 4.1.29 *Let R be a local nearring with descending chain condition for R-subgroups. Then*

$$L_R \trianglelefteq R.$$

Proof. By Corollary (4.1.25), $L_{R_0} \trianglelefteq R_0$. Hence by Theorem (4.1.27) $L_R \trianglelefteq R$.

Remark 4.1.30 It seems to be unknown, if there is a local nearring with $L_R \not\trianglelefteq R$, and hence it is unknown if it can happen that $L_R{}^+ \not\trianglelefteq R^+$. The result (4.1.28) shows, that such a local nearring must be infinite, if it exists. Moreover, if R is a local nearring with $L_R \not\trianglelefteq R$, then let I be a maximal ideal in R (by Lemma (2.4.10), such an ideal exists). Then R/I is a simple local nearring, and $L_{R/I} \not\trianglelefteq R/I$. Thus, if there is a local nearring with $L_R \not\trianglelefteq R$, then there also exists a simple local nearring with this property. Simple local nearrings are investigated in the following subsection.

The next result gives some information about the centralizer of L_R in a local nearring. In particular, if the group ${L_R}^+$ is not abelian, the centralizer $C_R(L_R)$ is contained in L_R.

Lemma 4.1.31 *Let R be a local nearring. If there is an element $r \in R^*$ such that $r \in C_{R^+}({L_R}^+)$, then $R^* \subseteq C_{R^+}({L_R}^+)$ and ${L_R}^+$ is abelian. Hence $L_R \leq Z(R^+)$.*

Proof. Let $r \in R^* \cap C_{R^+}({L_R}^+)$. Then $-r+l+r = l$ for all $l \in L_R$ and hence $r^{-1}l = r^{-1}(-r+l+r) = -1+r^{-1}+1$ for all $l \in L_R$. Hence, $1 \in C_{R^+}({L_R}^+)$ and thus $R^* \subseteq C_{R^+}({L_R}^+)$. Now, $l+k+1 = l+(k+1) = (k+1)+l = k+(1+l) = k+l+1$. Hence ${L_R}^+$ is abelian.

In the proposition (4.1.7), it was shown that in a local nearring R the group L_R is always a construction subgroup. The following lemma shows that in a local nearring R even every proper left R-subgroup is a construction subgroup.

Lemma 4.1.32 *Let R be a local nearring and U be a proper left R-subgroup of R. Then $U+1$ and $1+U$ are subgroups of R^*.*

Proof. It is clear that $U+1 \subseteq R^*$, since $U \subseteq L_R$. Let u, $v \in U$, $\tilde{u} = (u+1)^{-1} \in R^*$. Then

$$(u+1)(v+1) = \underbrace{(u+1)v+u}_{\in U}+1 \in U+1.$$

Moreover, $1 = \tilde{u}(u+1) = \tilde{u}u+\tilde{u}$, i.e., $\tilde{u} = -\tilde{u}u+1 \in U+1$. Similarly it follows that $1+U \leq R^*$.

Lemma 4.1.33 *Let R be a local nearring, $I \lhd R$ a proper ideal of R. Then $I+1 \trianglelefteq R^*$*

Proof. Since $I \lhd R$, I is a proper left R-subgroup of R and hence by Lemma (4.1.32), a construction subgroup of R. By Lemma (3.4.10), $I+1$ is a normal subgroup of R^*.

The following theorem shows that the converse of Lemma (4.1.33) holds for the construction subgroup L_R of a local nearring R. Moreover, this gives another criterion for L_R to be an ideal of R.

Theorem 4.1.34 *Let R be a local nearring. The subgroup L_R+1 is a normal subgroup of R^* if and only if $L_R \trianglelefteq R$.*

Proof. If $L_R \trianglelefteq R$ then $L_R + 1 \trianglelefteq R^*$ by Lemma (4.1.33).

On the other hand, if $L_R + 1 \trianglelefteq R^*$, for every $l \in L_R$ and every $r \in R^*$ there is an element $k_{l,\,r} \in L_R$ with $r^{-1}(l+1)r = k_{l,\,r} + 1$.

(1) Let $l \in L_R$. Then

$$\begin{aligned} k_{l,\,-1} + 1 = (-1)(l+1)(-1) = ((-1)l - 1)(-1) = 1 - (-1)l \\ \iff (-1)l = -1 - k_{l,\,-1} + 1 \\ \iff l = (-1)(-1 - k_{l,\,-1} + 1) = 1 - (-1)k_{l,\,-1} - 1 \\ \iff -1 + l + 1 = -(-1)k_{l,\,-1} \in L_R \end{aligned}$$

Hence $1 \in N_{R^+}(L_R{}^+)$. By Lemma (4.1.23), $L_R{}^+ \trianglelefteq R^+$.

(2) Let $l \in L_R$, r, $s \in R$. If $r \in L_R$ or $s \in L_R$, then $(l+r)s - rs \in L_R$. Thus it may be assumed that r, $s \in R^*$. Then

$$\begin{aligned} (l+r)s - rs = r(r^{-1}l + 1)r^{-1}rs - rs \\ = (k_{r^{-1}l,\,r^{-1}} + 1)rs - rs = rs(rs)^{-1}(k_{r^{-1}l,\,r^{-1}} + 1)rs - rs \\ = rs(k_{k_{r^{-1}l,\,r^{-1}},rs} + 1) - rs = rsk_{k_{r^{-1}l,\,r^{-1}},rs} + rs - rs \\ = rsk_{k_{r^{-1}l,\,r^{-1}},rs} \in L_R \end{aligned}$$

Corollary 4.1.35 *Let R be a finite local nearring. Then $L_R + 1 \in Syl_p(R^*)$ for some prime p. By Theorem (4.1.28), $L_R \triangleleft R$, so that $L_R + 1$ is normal in R^*. This is the only Sylow-p-subgroup of R^*, and every p-element of R^* must be an element of $L_R + 1$.*

Proof. If $|R| < \infty$, then $|R| = p^n$ and $|L_R| = p^m$ for a prime p and some non-negative integers n and m with $m < n$. Hence, $|R^*| = p^n - p^m = p^m(p^{n-m} - 1)$. Since $|L_R + 1| = |L_R| = p^m$, it follows that $L_R + 1 \in Syl_p(R^*)$.

Lemma 4.1.36 *([2], Lemma 3.6) Let R be a local nearring with $L_R{}^+ \trianglelefteq R^+$. Then*

$$N = L_R \cup N_{R^*}(1 + L_R)$$

is a local nearring with $L_N \trianglelefteq N$.

The following result shows that a local nearring with cyclic additive group is finite.

Theorem 4.1.37 *Let R be a local nearring with cyclic additive group. Then R is finite.*

Proof. Assume that R is infinite, i.e., $R^+ \cong \mathbb{Z}^+$. Then there is a non-negative integer k with $L_R = k\mathbb{Z}$. Let $E \neq 0$ be the identity element of R, which does not need to concide with the generator 1 of the additive group $\mathbb{Z}^+$. Without loss of generality $n > 0$, $n \in \mathbb{Z}$. For every $n \in R^*$ there is an element $x \in R^*$ with $E = xn \in n\mathbb{Z}$. Now if $k \neq 0$, let q be a prime number with $q \nmid k$; if $k = 0$, let q be an arbitrary prime number. Then $q^m \notin L_R$ for every $m \in \mathbb{N}$. Hence, $E \in q^m\mathbb{Z}$, which implies

$$E \in \bigcap_{m\in\mathbb{N}} q^m\mathbb{Z} = \{0\}.$$

This contradiction shows that $|R|$ is finite.

4.1.4 Simple local nearrings

If R is a local nearring, it seems to be unknown whether L_R is always an ideal of R or not. This subsection investigates the structure of a local nearring R, in which L_R is not an ideal of R.

Let R be such a local nearring. Since by Theorem (4.1.27), $L_R \trianglelefteq R$ if and only if $L_{R_0} \trianglelefteq R_0$, in the following R will be assumed zero-symmetric. By Corollary (4.1.25), R cannot satisfy the descending chain condition. Clearly, every proper (right) ideal of R is contained in L_R. Since R has an identity element, it contains maximal (right) ideals by Lemma (2.4.10). Since the sum of two (right) ideals is likewise a (right) ideal by Lemma (2.4.9) and the sum of two distinct maximal (right) ideals is the whole nearring, R can contain only one maximal (right) ideal. Furthermore, factor nearrings of local nearrings are local, so if I is the maximal ideal of R, the nearring R/I is simple local nearring which is not a nearfield. Obviously, $L_{R/I}$ is not an ideal of R/I.

Without loss of generality, in the following assume that R is simple.

Theorem 4.1.38 *R does not have non-trivial proper right ideals.*

Proof. Let $I \lhd_r R$ be a right ideal of R and assume that $I \neq \{0\}$. Then $G = R/I$ is a R-module with $I \leq \mathcal{U}_R(G) \trianglelefteq R$. Since $I \neq \{0\}$ and since R is simple, $\mathcal{U}_R(G) = R$, a contradiction to $1 \in R((I + 1) \cdot 1 = I + 1 \neq I)$.

Theorem 4.1.39 *R has no zero-divisors.*

Proof. Assume $kl = 0$ for k, $l \in R - \{0\}$. Then $\mathcal{U}_R(k) \trianglelefteq_r R$ and $0 \neq l \in \mathcal{U}_R(k)$. By (4.1.38), $\mathcal{U}_R(k) = R$, a contradiction to $k \cdot 1 = k \neq 0$.

In the following let $0 \neq l \in L_R$ be fixed and let $G = lR$. Then G is a monogenic R-module.

Theorem 4.1.40 *G is isomorphic to the regular R-module R_R*

Proof. The mapping $\alpha : R \longrightarrow G$ with $r\alpha = lr$ is a R-module isomorphism:

(1) α is a group homomorphism:

$$(r+s)\alpha = l(r+s) = lr + ls = r\alpha + s\alpha$$

(2) α is a R-module homomorphism:

$$(rs)\alpha = l(rs) = (lr)s = (r\alpha)s$$

(3) α is a monomorphism:

$$r\alpha = 0 \Leftrightarrow lr = 0 \Leftrightarrow r = 0$$

By the definition of G it is clear that α is surjective, so $G \cong_R R$.

Corollary 4.1.41 *G is a simple R-module*

Proof. By Theorem (4.1.40), G is isomorphic to R_R. If G has a proper non-trivial R-ideal, then so does R_R. But R-ideals of R are exactly the right ideals of R, and these do not exist in R by Theorem (4.1.38).

Thus G is a R-module of type 0. Since $\mathcal{J}_1(R) = \mathcal{J}_2(R) = R$, G cannot be of type 1 or type 2. Thus there is an element $g \in G$ with $0 < gR < G$. The results (4.1.40), (4.1.41) applied to gR, gives an infinite descending chain of R-submodules of G:

$$G = lR \supset l_1R \supset l_2R \supset \cdots$$

The nearring R can be embedded into the nearring $M_0(G)$ via

$$\alpha : R \longrightarrow M_0(G)$$

such that $r \mapsto \alpha_r$ with $(ls)\alpha_r = l(sr)$. Then α is a nearring monomorphism. Let $g \in G$, r, $s \in R$.

- $g\alpha_{r+s} = g(r+s) = gr + gs = g\alpha_r + g\alpha_s$, hence $\alpha_{r+s} = \alpha_r + \alpha_s$.
- $g\alpha_{rs} = g(rs) = (gr)s = g\alpha_r\alpha_s$, hence $\alpha_{rs} = \alpha_r\alpha_s$.
- Let $\alpha_r = \alpha_s$. Then, for all $t \in R$, $ltr = lt\alpha_r = lt\alpha_s = lts$, it follows $0 = ltr - lts = lt(r-s)$, i.e., $r = s$. Hence, α is injective.

Proposition 4.1.42 *α_r is surjective if and only if $r \in R^*$.*

Proof. Let α_r be surjective. Then there is a $g = ls \in G = lR$ with $g\alpha_r = l$, i.e., $lsr = l$. Then $0 = lsr - l = l(sr - 1)$ and by Theorem (4.1.39) $sr = 1$. Hence $r \in R^*$. The converse is trivial.

Remark 4.1.43 Since the elements of $L_R\alpha$ are not surjective, they have nontrivial annihilators in $M_0(G)$. Define β_l via

$$g\beta_l = \begin{cases} 0 & g \in Im(\alpha_l) \\ g & g \notin Im(\alpha_l) \end{cases}$$

Since α_l is not surjective, $\beta_l \neq 0$ and it is clear that $\alpha_l\beta_l = 0$.

4.1.5 Prime rings of local nearrings

In this subsection the structure of the prime rings of local nearrings will be investigated. It turns out that these prime rings are local.

Lemma 4.1.44 *Let R be a local nearring.*

(a) If $o^+(1) = m < \infty$, then the prime ring P_R is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$ for a prime p.

(b) If $o^+(1) = \infty$, then $P_R \cong \mathbb{Q}_p = \{\frac{n}{m} \in \mathbb{Q} \mid p \nmid m\}$, if there is a prime p with $1 \cdot p \in L_R$, and $P_R \cong \mathbb{Q}$, if there is no such a prime.
In particular, the prime ring of a local nearring is local.

(c) If $L_{P_R} = \{0\}$, then P_R is a field, since it is both a nearfield and a ring.

Proof. (a) By Lemma (3.3.4), $P_R \cong \mathbb{Z}/m\mathbb{Z}$. Since $o^+(1) < \infty$, R has the Property $(\mathcal{P})$, so that there is a prime p such that $1 \cdot p \in L_R \cap P_R$, i.e., $p \mid m$. But $L_R \cap P_R$ is a group with respect to the addition , and all elements of P_R which are not contained in L_R are invertible in P_R by Lemma (3.3.4). Hence P_R is local and thus m is a prime power.

(b) Consider the mapping $\sigma : P_R \longrightarrow \mathbb{Q}$ with $(1 \cdot n)(1 \cdot m)^{-1} \mapsto \frac{n}{m}$. It is easy to check that σ is a ring monomorphism. If there is a prime p with $1 \cdot p \in L_R$, then $1 \cdot m$ is invertible if and only if $p \nmid m$, i.e., $Im(\sigma) = \mathbb{Q}_p$. If there is no such a prime, σ is an epimorphism.

Since it is well known that $\mathbb{Q}_p$ is a local ring, it follows that P_R is always a local ring.

(c) This is obviuos.

Corollary 4.1.45 *If R^+ has finite exponent, then R^+ is a p-group for a prime p.*

Proof. R^+ has finite exponent if and only if $o^+(1) < \infty$. Hence, P_R is a finite local nearring, and by Theorem (4.1.19) ${P_R}^+$ is a p-group. Thus $o^+(1)$ is a power of p, and since $o^+(1) = exp(R^+)$, R^+ is a p-group.

The converse of Corollary (4.1.45) is also true. If R^+ is a p-group for some prime p, then there is a positive integer n such that $o^+(1) = p^n$. But by Corollary (2.1.22) it follows that $exp(R^+) = p^n < \infty$.

Lemma 4.1.46 *Let R be a local nearring with ${L_R}^+ \trianglelefteq R^+$. Then $P_R + L_R$ is also a local nearring.*

Proof. Let $N = L_R \cup N_{R^*}(L_R + 1)$. By Theorem (4.1.36), N is a subnearring of R and $L_R \trianglelefteq N$. Furthermore, since $1 \in N$, the prime ring P_R is contained in N. Hence $P_R + L_R \subseteq N$. Since $L_R \trianglelefteq N$ and P_R is a subnearring of N, by Lemma (2.4.9) $P_R + L_R$ is a subnearring of N with $L_R \trianglelefteq P_R + L_R$. Let $r = p + l \in (P_R + L_R) - L_R$. Then there exists $r^{-1} \in R$. Since r is invertible, p cannot be an element of L_R. Hence the inverse $p^{-1} \in P_R$ exists. Since $L_R \trianglelefteq R$, the element $rp^{-1} - 1 = (p + l)p^{-1} - pp^{-1} \in L_R$. Multiplying this with r^{-1} from the left, it follows that $p^{-1} - r^{-1} \in L_R$. Thus, $-r^{-1} = -p^{-1} + p^{-1} - r^{-1} \in P_R + L_R$, and so also $r^{-1} \in P_R + L_R$. This means that $P_R + L_R$ is local.

If a (not necessarily local) nearring R is used for the construction of triply factorized groups, only a construction subgroup U of R is considered. Hence it suffices to consider the subnearring of R generated by $U + 1$. Thus, if ${L_R}^+ \trianglelefteq R^+$, for the construction of triply factorized groups using local nearrings, it is possible to assume that $R = P_R + L_R$.

4.1.6 The multiplicative group R^*

In this subsection the structure of the group of units of a local nearring will be investigated. It turns out that for a finite local nearring this group can be described as a semidirect product of $L_R + 1$ and the group of units of a nearfield R/L_R. Furthermore, it will be showed that if the group of units of a local nearring R is a torsion group, also the additive group of R is periodic.

Lemma 4.1.47 *Let R be a local nearring with $L_R \trianglelefteq R$. Then $(R/L_R)^* \cong R^*/(1 + L_R)^*$.*

Proof. Clearly, the mapping $\alpha : (R/L_R)^* \longrightarrow R^*/(L_R + 1)^*$ with

$$(L_R + r)\alpha = (L_R + 1)r$$

is a group isomorphism.

Lemma 4.1.48 *Let R be a finite local nearring. Then*

$$R^* \cong (L_R + 1)^* \rtimes (R/L_R)^*.$$

Proof. Let $|R| = p^n$, p is a prime, $n \in \mathbb{N}$. Moreover, let $|L_R| = p^m$, $(0 < m < n)$. Then $|R^*| = p^n - p^m = p^m(p^{n-m} - 1)$. Since $p^m \nmid p^{n-m} - 1$, the group $L_R + 1$ has a complement B in R^* by the Schur- Zassenhaus Theorem (cmp. [29], Theorem 9.1.2). But since $B \cong R^*/(L_R + 1)^* \cong (R/L_R)^*$, it follows that $R^* \cong (L_R + 1)^* \rtimes (R/L_R)^*$.

The following result follows from ([35], Satz III.2.8).

Lemma 4.1.49 *Let R be a nearfield and D be the set of all distributive elements of R. If the multiplicative group R^* of R has an abelian subgroup of finite index. Then the additive group of D is a subgroup of finite index in R^+*

Lemma 4.1.50 *Let R be a local nearring.*
(a) If R^+ is a torsion group, then $exp(R^+) < \infty$.
(b) If R contains a non-trivial element of finite additive order, R has the Property $(\mathcal{P})$.
(c) If $|R : L_R| < \infty$, R has the Property $(\mathcal{P})$.
(d) If R^* is periodic, so is R^+.

Proof. (a) By Corollary (2.1.22), $exp(R^+) = o^+(1) < \infty$.

(b) Let $0 \neq r \in R$ with $n = o^+(r) < \infty$. Then $0 = rn$. This implies that $n \in L_R$. Hence R has the Property $(\mathcal{P})$.
(c) Consider the right cosets of L_R. Since $|R : L_R| < \infty$, there are positive integers $n < m$ with $L_R + n = L_R + m$. Hence $n - m \in L_R$. Thus R has the Property $(\mathcal{P})$.
(d) Let R^* be periodic. Assume that $exp(R^+) = \infty$. By Lemma (4.1.44), P_R is isomorphic either to $\mathbb{Q}$ or to $\mathbb{Q}_p$ for a prime p. Both rings $\mathbb{Q}$ and $\mathbb{Q}_p$ have non-periodic multiplicative groups, which contradicts $P_R^* \leq R^*$.

Theorem 4.1.51 *Let R be a local nearring which is not a nearfield, then $|R| \leq |L_R|^2$.*

Proof. By Corollary (2.4.2), for every $y \in R$, the annihilator $\mathcal{U}_R(y)$ is a right ideal of R. Since $1 \notin \mathcal{U}_R(y)$, this yields $\mathcal{U}_R(y) \leq L_R$. Now let $0 \neq l \in L_R$. Define $\lambda_l : R \longrightarrow lR$ by $x\lambda_l = lx$ for all $x \in R$. This is an R-endomorphism of the regular module R_R with $Ker(\lambda_l) = \mathcal{U}_R(l)$. Hence $R_R/\mathcal{U}_R(l) \cong_R Im(\lambda_l)$. Since $Im(\lambda_l) \subseteq lR \subseteq L_R$, $|R| = |R_R| = |Ker(\lambda_l)| \cdot |Im(\lambda_l) \leq |L_R| \cdot |L_R| = |L_R|^2$.

Corollary 4.1.52 *(a) Let R be a local nearring which is not a nearfield, with $|L_R| < \infty$. Then R is finite.*
(b) $|R| = |L_R|$ if and only if R is infinite.

Proof. *(a)* The proof of Theorem (4.1.51) shows that L_R is a finite subgroup of finite index of R^+. Hence R is finite.

(b) If R is infinite, also L_R is infinite by Theorem (4.1.51). In this case, $|R| \leq |L_R|^2 = |L_R|$. On the other hand, if R is finite, $|L_R| < |R|$ since $1 \notin L_R$.

By Malone ([18], Corollary 4) no generalized quaternion group can occur as the additive groups of nearrings with identity. The next corollary shows that also non-commutative dihedral groups cannot occur as additive groups of local nearrings.

Corollary 4.1.53 *Let $n \geq 3$ be an integer. Then there is no local nearring R with $R^+ \cong D_{2^n}$.*

Proof. The dihedral group D_{2^n} has exponent $2^{n-1} > 2$. Assume that R is a local nearring with $R^+ \cong D_{2^n}$. Then by Corollary (2.1.22) all elements of additive order 2 must be contained in L_R. But D_{2^n} is generated by two elements of order 2, and hence $L_R = R$, contradicting $1 \notin L_R$.

Chapter 5

Special local nearrings

5.1 Local nearrings with dihedral group

In this section local nearrings with dihedral multiplicative group are investigated. For a detailed account of these results see [2] and [13]. The first lemma on the structure of dihedral groups is well-known and will not be proved.

Lemma 5.1.1 *Let D be a dihedral group and $N \trianglelefteq D$. Then one of the following properties holds:*
(a) $|D : N| = 2$ and N is a dihedral group.
(b) $D = N$.
(c) N is a cyclic group.

Lemma 5.1.2 *([2], Lemma 3.10) Let R be a local nearring whose subgroup L_R has finite index in the additive group R^+ of R. Then L_R is a normal subgroup of R^+.*

Lemma 5.1.3 *If R is a nearfield with (non-trivial) dihedral multiplicative group, then $|R| = 3$ and hence $R \cong \mathbb{F}_3$.*

Proof. By Lemma (3.2.7) (a) the equation $x^2 = 1$ has only two solutions $x = 1$ and $x = -1$ in R. Hence $|R| < 4$, which means that $|R^*| = 2$. Thus $|R| = 3$, and so $R \cong \mathbb{F}_3$.

Lemma 5.1.4 *([2], Lemma 4.2) Let R be a local nearring. If the multiplicative subgroup $1 + L_R$ of the dihedral group R^* is cyclic, then L_R is finite.*

Theorem 5.1.5 *Let R be a local nearring whose multiplicative group R^* is dihedral. Then R is finite.*

Proof. If R^* is finite, then the subgroup L_R is also finite. Hence R is finite by (4.1.5). In particular, R^+ is a p-group for some prime p by Lemma (4.1.20). Thus to prove the theorem, it suffices to show that R^* is finite.

Suppose the contrary, and let R be a counterexample whose multiplicative group R^* is infinite dihedral. Then $L_R \neq 0$ by Lemma (5.1.3) and so L_R is infinite. Therefore $1 + L_R$ is an infinite dihedral subgroup of R^* by Lemma (5.1.4) and hence it has finite index in R^*. This implies that L_R has finite index in R^+ and thus L_R is normal in R^+ by Lemma (5.1.2).

Put $N = L_R \cup N_{R^*}(1 + L_R)$. Then N is a local subnearring of R by Lemma (4.1.36) and its multiplicative group $N^* = N_{R^*}(1+L_R)$ is also infinite dihedral. Moreover, since $1 + L_R$ is normal in N^*, the index of $1 + L_R$ in N^* is at most 2.

If $1+L_R = N^*$, then the factor group N^+/L_R is of order 2 and so $2\cdot 1 \in L_R$. If $2 \cdot 1 = 0$, then R^+ is a group of exponent 2 and thus abelian. But then the subgroup L_R must be finite because the semidirect product $L_R \rtimes (1 + L_R)$ is a soluble group factorized by two dihedral subgroups by (4.1.8) and so is polycyclic by ([1], Theorem 4.4.2). This contradiction shows that $2 \cdot 1 \neq 0$ and so -1 is an element of order 2 in R^*. Hence $C_{R^*}(-1) = \{1,\ -1\}$. Since -1 commutes with $3 \cdot 1$, this implies $3 \cdot 1 = -1$ and so $4 \cdot 1 = 0$.

Consider an element $a \in L_R$ such that $1+a$ is an element of infinite order in R^*. Then $(1+a)^{-1} = 1+b$ for some $b \in L_R$ and $(-1)(1+a) = (1+b)(-1)$. This gives $-1 + (-1)a = -b - 1$ and so $(-1)a = +1 - b - 1$. By symmetry, $(-1)b = 1 - a - 1$. Therefore $(-1)(a + b) = 1 - (a + b) - 1$ and hence $(-1)(1+a+b) = (1+a+b)(-1)$, so that either $1+a+b = 1$ or $1+a+b = -1$.

In the first case $b = -a$ and so $1 = (1+a)(1-a) = 1+a-(1+a)a$ which implies $(1+a)a = a$. But then $(1+a)^4 = 1+a+(1+a)a+(1+a)^2a+(1+a)^3a = 1 + 4a = 1$, contrary to the choice of a. Therefore $a + b = 2 \cdot 1$ and, by symmetry, $b + a = 2 \cdot 1$ so that $a + b = b + a$ and $2a = 2b$. Hence $a - b = -a + b$. On the other hand, $(-1)(a - b) = 1 - b + a - 1$ and so $(-1)(1 + a - b) = (1 - a + b)(-1)$. Thus $(-1)(1 + a - b) = (1 + a - b)(-1)$ which implies $1 + a - b = -1$. Therefore $b = a + 2 \cdot 1 = 2 \cdot 1 + a$. Show that in this case also $(1 + a)^4 = 1$ which contradicts the choice of a.

Indeed, since $1 = (1+a)(1+b) = 1+a+(1+a)b$, it follows that $a = (1+a)b$ and so $a = (1+a)(a+2\cdot 1) = (1+a)a+2(1+a)$. Hence $(1+a)a = 2(1+a)+a$ and thus $(1 + a)^2 = (1 + a) + (1 + a)a = 3(1 + a) + a = -(1 + a) + a$. Therefore $(1 + a) + (1 + a)^2 = a$ and so $(1 + a)^3 = -(1 + a)^2 + (1 + a)a = a + (1 + a) + 2(1 + a) + a = a + 3(1 + a) + a = -1 + a$.

Finally,

$$(1 + a)^4 = -(1 + a)^3 + (1 + a)^2a$$

$$= a + 1 + 2(1 + a)^2 + (1 + a)a$$

$$= a + 1 + 2(-(1+a) + a) + 2(1+a) + a$$
$$= a + 1 + a + 2 \cdot 1 + a + 1 + a + 1$$
$$= a + 3 \cdot 1 + 1 + a + 1 = 1.$$

Thus $1 + L_R \neq N^*$ so that $1 + L_R$ is the subgroup of index 2 in N^*. Therefore the factor group N^+/L_R is of order 3 and so $3 \cdot 1 \in L_R$. Hence $2 \cdot 1 \in R^*$ and -1 is an element of order 2 of R^* which commutes with $2 \cdot 1$. This implies that $2 \cdot 1 = -1$, and so $3 \cdot 1 = 0$. Therefore R^+ is a group of exponent 3 and hence soluble. As above, this means that the semidirect product $L_R \rtimes (1 + L_R)$ is a polycyclic group and hence L_R must be finite. This final contradiction completes the proof of the theorem.

Theorem 5.1.6 *Let R be a finite local nearring of odd order. If the multiplicative group R^* of R is dihedral, then either R is isomorphic to the Galois field $\mathbb{F}_3$ of order 3 or R^+ is an elementary abelian group of order 9.*

Proof. Note first that the subgroup L_R is an ideal of R by (4.1.28). As the factor nearring R/L_R is a nearfield whose multiplicative group is isomorphic to the factor group $R^*/(1 + L_R)$, which is dihedral, $R/L_R \cong \mathbb{F}_3$ by Lemma (5.1.3). Therefore $3 \cdot 1 \in L_R$ and hence R^+ is a 3-group by Lemma (4.1.20). Thus $1 + L_R$ is a normal 3-subgroup of R^* and so a cyclic group whose elements are inverted by (-1). In particular, $4 \cdot 1 = (-1)(4 \cdot 1)(-1) = (4 \cdot 1)^{-1}$ from which it follows that $16 \cdot 1 = 1$ and so $3 \cdot 1 = 0$. Therefore R^+ is a group of exponent 3. Next, the group $L_R \rtimes (1 + L_R)$ is the product of two cyclic 3-subgroups by Lemma (4.1.8), so that L_R is cyclic by ([32], Lemma 6). Hence the order of L_R is equal to 3 and so the group R^+ is elementary abelian of order 9.

5.1.1 Nearrings of even order

In this subsection local nearrings of even order will be studied. In [2] it was shown that a local nearring of even order has order at most 32, if its group of units is dihedral. Actually, an investigation in [13] of all possible additive groups of order 32 shows that there is no local nearring of order 32 whose multiplicative group is dihedral. Thus ([13], 8.3.11) improves the main result of [2].

Lemma 5.1.7 *Let R be a local nearring of order 2^{n+1} with dihedral multiplicative group. Then the factor nearring R/L_R is of order 2 and so $R^* = 1 + L_R$ is a group of order 2^n. Furthermore, the additive group R^+ of R has exponent at most 8.*

Proof. Since the factor nearring R/L_R is a nearfield of even order, it cannot be isomorphic to $\mathbb{F}_3$. Thus, by Lemma (5.1.3), $(R/L_R)^*$ cannot be dihedral and hence must be trivial. This means that $R/L_R \cong \mathbb{F}_2$ and so $|R : L_R| = 2$.

Let 2^l be the exponent of R^+. Then $P_R \cong \mathbb{Z}/2^l\mathbb{Z}$ by (3.3.4). Hence ${P_R}^* \cong C_2 \times C_{2^{l-2}}$ is an abelian subgroup of R^*. This means that $|{P_R}^*| \leq 4$, which is equivalent to $|P_R| \leq 8$. Thus $exp(R^+) \leq 8$.

Lemma 5.1.8 *([2], Lemma 5.4) Let R be a local nearring of even order with dihedral multiplicative group such that R^* operates faithfully on ${L_R}^+$. Then the following two statements hold:*
(1) *L_R is either a group of order 4 or a non-cyclic abelian group of order 8.*
(2) *R^+ is either a cyclic group of order 8 or a group with exponent at most 4.*

In particular, $|R| \leq 16$.

Corollary 5.1.9 *Let R be a local nearring of even order with dihedral multiplicative group such that R^* operates faithfully on ${L_R}^+$. Then $exp(R^+) \leq 4$.*

Proof. By Lemma (5.1.8) R^+ is either a cyclic group of order 8 or a group of exponent at most 4. But if R^+ is isomorphic to C_8, then $R \cong \mathbb{Z}_8/8\mathbb{Z}$ by Lemma (3.3.4). This is impossible since in this local nearring the operation of $L_R + 1$ on L_R is not faithful (it is not difficult to see that

$$Stab_{R^*}(L_R) =< -3 >^*$$

in this case).

Theorem 5.1.10 *([2], Theorem 5.7) Let R be a local nearring of 2^n with $n \geq 1$, and let R^* be dihedral. Then $2 \leq n \leq 5$ and ${L_R}^+$ is either an abelian group or a group of order 16 whose derived subgroup has order 2. In particular, L_R has an abelian subgroup of index 2.*

The following result plays an important role in the investigation of local nearrings having a dihedral multiplicative group. In [13], it is proved that there does not exist any local nearrings having a dihedral multiplicative group of order 32. For this study, all the groups of order 32 are considered, most of all cannot occur as R^+, since for example their exponent is larger than 8.

Theorem 5.1.11 *([13], Theorem 8.3.11) There is no local nearring of order 32 whose multiplicative group is dihedral.*

Corollary 5.1.12 *([13], Corollary 8.3.12) If R is a local nearring with dihedral group of units of even order, then $|R| \leq 16$.*

In the following the structure of finite triply factorized 2-groups $G = AB = AM = BM$ with dihedral subgroups A and B is determined.

The following result is useful for the proof of Lemma (5.1.14) and it is due to King see [16].

Lemma 5.1.13 *The centre of every non-abelian normal subgroup of a p-group H which is contained in $\phi(H)$ cannot be cyclic.*

Lemma 5.1.14 *([2], Lemma 5.6) Let H be a 2-group of the form $H = AK = BK = AB$ with two dihedral subgroups A and B and a normal subgroup K such that $A \cap B = A \cap K = B \cap K = 1$. Then the following statements hold:*

(1) *the Frattini subgroups $\phi(A)$ and $\phi(B)$ are permutable, so that their product $F = \phi(A)\phi(B)$ is a subgroup of H;*

(2) *$\phi(F) = \phi(A)^2\phi(B)^2$ is a normal subgroup of H;*

(3) *the intersection $F \cap K$ is a cyclic subgroup of index at most 4 in K except in the case in which K is of order 16 and $F \cap K$ is elementary abelian of order 4.*

5.2 Local nearrings with quaternion group

In this section local nearrings with generalized quaternion multiplicative group will be considered. For a detailed account of this topic see [33]. It turns out that the structure of such nearrings can be completely described. The term "generalized quaternion group" can here be interpreted as either a finite generalized quaternion group

$$Q_{2^n} = \{a, b \mid a^{2^{n-1}} = b^4 = 1, a^{2^{n-2}} = (ab)^2 = b^2\}$$

with $n \geq 3$ or, up to isomorphism, a unique infinite locally quaternion group Q_{2^∞} in which every finite subset is contained in a subgroup isomorphic to Q_{2^n} for some $n \geq 3$.

5.2.1 Some triply factorized groups

In this subsection triply factorized groups of the form $G = AB = AK = BK$ with subgroups A and B and a normal subgroup K such that $A \cap K = B \cap K = 1$ will be considered.

The first lemma of this subsection describes the periodic groups where the subgroups A and B have quasicyclic 2-subgroups of finite index.

Recall that an infinite periodic group is *quasicyclic* if it is abelian and all its proper subgroups are cyclic. It is precisely an infinite locally cyclic p-group for some prime p and so it has only one cyclic subgroup of order p^n for each positive integer n.

A group is *Chernikov* if it has a normal subgroup of finite index which is a direct product of finitely many quasicyclic subgroups. For a detailed account of the results concerning Chernikov groups and their finiteness conditions see the book [29].

Lemma 5.2.1 *Let G be a periodic group of the form $G = AB = AK = BK$ with two subgroups A and B each of which has a quasicyclic 2-subgroup of finite index and a normal subgroup K such that $A \cap K = B \cap K = 1$. Then the subgroup K is either finite or quasicyclic-by-finite.*

Proof. Since the subgroups A and B satisfy the minimal condition on subgroups, the group G satisfies the minimal condition on normal subgroups by ([1], Lemma 1.2.6) and thus its hypercentre $Z_\infty(G)$ is a Chernikov subgroup by a result of Baer (see for instance [29, Theorem 5.22]). Moreover, if G is a soluble-by-finite group, then G itself is Chernikov by ([1], Corollary 3.2.8). Hence, if A_0 and B_0 are quasicyclic subgroups of A and B, respectively, then the subgroup $H = \langle A_0, B_0 \rangle$ is abelian of finite index in G and clearly $H = A_0B_0 = (H \cap K)A_0 = (H \cap K)B_0$. Therefore the subgroup $H \cap K$ and so K is either finite or quasicyclic-by-finite, as desired. Show now that the group G must really be soluble-by-finite.

Suppose the contrary and choose a counterexample G such that the index of the quasicyclic subgroup A_0 in A is minimal. Since the hypercentre of G is Chernikov by proved above, it does not contain the subgroup K, so that the intersection $K_0 = K \cap Z_\infty(G)$ is a normal subgroup of G properly contained in K. Therefore the intersection $A_0K_0 \cap B_0K_0$ is also a normal subgroup of G because it is normal in AK_0 and BK_0 simultaneously. Thus, passing to the factor group $G/(A_0K_0 \cap B_0K_0)$, we may assume that $K \cap Z_\infty(G) = A_0 \cap B_0 = 1$. Indeed, if $x \in K$ and $[x, G] \leq A_0K_0 \cap B_0K_0$, then $[x, G] \leq (A_0K_0 \cap B_0K_0) \cap K = K_0 \leq Z_\infty(G)$ and hence $x \in K_0$. Note also that $A \neq A_0$ and so $B \neq B_0$ because otherwise the group G is abelian by ([1] Theorem 7.4.4).

As A_0 has only one involution a, it belongs to the centre of A and so the centralizer $C_K(a)$ is an A-invariant subgroup of K. Therefore the intersections $B_1 = AC_K(a) \cap B$ and $A_1 = A \cap B_1C_K(a)$ are subgroups such that $A_1B_1 = C_K(a)A_1 = C_K(a)B_1$ by [1, Lemma 1.1.4]. If $C_K(a)$ is finite, then the

subgroup K and so G is soluble-by-finite by a result of Shunkov [34], contrary to the assumption. Thus the centralizer $C_K(a)$ and hence the subgroups A_1 and B_1 are infinite. Hence $A_0 \leq A_1$ and $B_0 \leq B_1$, so that either the index of A_0 in A_1 is less than that of A_0 in A or $A_1 = A$ and so $B_1 = B$. However in the first case the subgroup $A_1B_1 = C_K(a)A_1 = C_K(a)B_1$ is soluble-by-finite by the choice of G and thus $C_K(a)$ is a quasicyclic-by-finite subgroup by proved above. Since the index of $C_K(a)$ in K is finite because it is equal to the index of A_1 in A, the subgroup K is quasicyclic-by-finite and so the group G is Chernikov, contrary to the assumption. Therefore $C_K(a) = K$ and, by the same arguments, $C_K(b) = K$ for the unique involution $b \in B_0$. Hence the subgroup $\langle a, b\rangle$ is central in G and has a non-trivial intersection with K because $A_0 \cap K = B_0 \cap K = A_0 \cap B_0 = 1$. On the other hand, by assumption $K \cap Z_\infty(G) = 1$, and this final contradiction completes the proof.

Repeating the arguments of the proof of the Lemma (5.1.14), it can be shown that statements 1) - 3) hold also for triply factorized 2-groups

$$G = AB = AK = BK$$

with generalized quaternion subgroups A and B. For the purpose of this section, it suffices to consider the case when the subgroup K is elementary abelian.

Lemma 5.2.2 *Let H be a 2-group of the form $H = AK = BK = AB$ with two generalized quaternion subgroups A and B and an elementary abelian normal subgroup K such that $A \cap B = A \cap K = B \cap K = 1$. Then the order of K is either 8 or 16.*

Proof. Let $F =< \Phi(A), \Phi(B) >$ be the subgroup of H generated by the Frattini subgroups $\Phi(A)$ and $\Phi(B)$. Show that in fact $F = \Phi(A)\Phi(B)$. As the Frattini subgroup $\Phi(H)$ contains F and it is contained in the subgroup $\Phi(A)K = \Phi(B)K$, it follows that

$$(^*) \qquad \Phi(H) = \Phi(A)(\Phi(H) \cap K) = \Phi(B)(\Phi(H) \cap K).$$

Clearly the index $[K : \Phi(H) \cap K]$ is either 2 or 4 because $[A : \Phi(A)] = [B : \Phi(B)] = 4$. In particular, if A and B are of order 8, then $\Phi(H)$ has order at most 8 and therefore the subgroup $\Phi(H)$ must be abelian by King's result [16] cited above. Hence in this case $F = \Phi(A)\Phi(B)$.

Suppose now that A and B are subgroups of order at least 16. Since elementary abelian groups of order 2^n with $n \geq 4$ have no automorphisms of order 2^{n-1}, the centralizers $C_A(K)$ and $C_B(K)$ are both non-trivial and so they contain the centers $Z(A)$ and $Z(B)$, respectively. Therefore $Z(A)Z(B)$ is a

central subgroup of H contained in F. Clearly the factor group $H/(Z(A)Z(B))$ satisfies the hypothesis of Lemma (5.1.14) because the factor groups $A/Z(A)$ and $B/Z(B)$ are dihedral. Hence $F/(Z(A)Z(B)) = (\Phi(A)\Phi(B))/(Z(A)Z(B))$ and thus $F = \Phi(A)\Phi(B)$.

It follows from (*) that $F = \Phi(A)\Phi(B) = \Phi(A)(F \cap K) = \Phi(B)(F \cap K)$, so that the index $|K : F \cap K|$ is equal to 4 because $|A : \Phi(A)| = |B : \Phi(B)| = 4$. On the other hand, since the Frattini subgroups $\Phi(A)$ and $\Phi(B)$ are cyclic, the order of $F \cap K$ does not exceed 4 by [32, Lemma 6]. As K is of order at least 16, this means that the order of $F \cap K$ must be equal to 4, so that K is of order 16.

It is clear that every locally cyclic p-group is either finite or quasicyclic. Furthermore, it follows from Lemma (4.1.7) that a local nearring is finite if and only if its multiplicative group is finite.

Theorem 5.2.3 *Let R be a local nearring whose multiplicative group R^* has a locally cyclic 2-subgroup of finite index. Then R is finite.*

Proof. Suppose the contrary and let R be a counterexample in which L_R is the subgroup of all non-invertible elements of R. Then R^* contains a quasicyclic 2-subgroup C of finite index and $1 + L_R$ is a subgroup of R^* by Lemma (4.1.7). Moreover, it follows that either $L_R = 0$ and so R is a nearfield or L_R is infinite and so the subgroup $1 + L_R$ contains C.

Assume first that R is an infinite nearfield and let D denote the set of all distributive elements of R. Then D is a division subring of R by Lemma (3.2.6) and thus the multiplicative group D^* of D is a subgroup of R^*. The subring D cannot be finite because otherwise R must also be finite by Lemma (4.1.49) which is not the case. Thus D^* is infinite and so C must be contained in D^*. Therefore there exists a maximal abelian subgroup P of D^* containing C, so that P has finite index in R^*. Clearly the set $P \cup \{0\}$ forms a maximal subfield F of D and for every element $a \in R$ the set aF is a subgroup of the additive group R^+ of R. Since R^* is a union of finitely many left cosets of P in R^*, there exist elements $a_1 = 1, a_2, \ldots, a_n$ of R^* such that $R^* = P \cup a_2P \cup \ldots a_nP$. Then $R^+ = F \cup a_2F \cup \cdots \cup a_nF$ and hence some of the subgroups $a_iF, 1 \leq i \leq n$ must have finite index in R^+ by a result of B. Neumann (see for instance ([1], Lemma 1.2.4). But then every subgroup a_iF is of finite index in R^+, so that for all $i \neq j$ the intersection $a_iF \cap a_jF$ is a subgroup of finite index in R^+. On the other hand, this intersection coincides with $\{0\}$ because $a_iP \cap a_jP = \emptyset$ and this implies that R is finite, contrary to the assumption.

Now let the subgroup L_R be infinite. Then the quasicyclic 2-subgroup C of finite index in R^* must be contained in $1 + L_R$. If $G = L_R \rtimes (1 + L_R)$ is a

semidirect product in which $1 + L_R$ acts on L_R by left multiplication, then G has two subgroups A and B isomorphic to $1 + L_R$ such that

$$G = AB = L_R \rtimes A = L_R \rtimes B$$

by Lemma (4.1.8). But then, on the one hand, the group R^+ and so its subgroup L_R is a p-group of finite exponent for some prime p by Lemma (4.1.50) and, on the other hand, the group G is periodic and hence its normal subgroup L_R is quasicyclic-by-finite by Lemma (5.2.1). This is a final contradiction which completes the proof.

Recall that an abelian p-group is said to be of type $(p^{n_1}, \ldots, p^{n_k})$ with positive integers $n_1, \ldots, n_k$ if it is the direct product of k cyclic groups of orders $p^{n_1}, \ldots, p^{n_k}$, respectively.

From here and up to the end of this section R will be a finite local nearring with identity 1 whose multiplicative group R^* is generalized quaternion and L_R will denote the subgroup of all non-invertible elements of R.

Theorem 5.2.4 *Let R be a local nearring whose multiplicative group R^* is generalized quaternion. Then the following statements hold.*

1) The group R^* is either quaternion of order 8 or generalized quaternion of order 16.

2) The additive group R^+ of R is abelian of one of types $(3,3)$, $(2,2,2,2)$, $(2,2,4)$, $(2,2,2,2,2)$ and $(2,2,2,4)$.

3) The subgroup L_R of all non-invertible elements of R is trivial if R^+ is of type $(3,3)$ and it is elementary abelian of index 2 in R^+ otherwise.

Conversely, for each abelian group of type listed in statement 2) there exists at least one R with additive group R^+ of this structure whose multiplicative group R^* is generalized quaternion.

Note that, up to isomorphism, there exists only one local nearring of order 9 with quaternion multiplicative group, namely non-commutative Dickson nearfield coupled to the Galois field of order 9 (see [35], Chapter IV, Part 1). Using some calculations made by means of a GAP-program based on the package "SONATA, version 2.3" of computer algebra system GAP 4.4, it can be shown that the number of non-isomorphic local nearrings R of order 16 with quaternion group R^* is divided in two halves: there exist 24 such nearrings with R^+ of type $(2,2,2,2)$ and as many with R^+ of type $(2,2,4)$. Two appropriate examples of these nearrings as well as that of such local nearrings of order 32 are given in the last section.

Proof. The proof is divided into several lemmas. Consider, first, the case when R is a nearfield. It turns out that, up to isomorphism, there exists only one nearfield with generalized quaternion multiplicative group.

Lemma 5.2.5 *If R is a nearfield, then its order is equal to 9 and so R^* is a quaternion group of order 8.*

Proof. As R^+ is a p-group of order p^n for some prime p and an integer $n \geq 2$ by Lemma (4.1.20), it holds $p^n = 2^q + 1$. A result of Zsigmondy (see for instance ([14], Theorem IX.8.3) shows now that this is possible only if $p = 3$ and $n = 2$, so that R is of order 9.

Lemma 5.2.6 *If the additive group R^+ of R is a 2-group, then its exponent does not exceed 4.*

Proof. Indeed, as the exponent of R^+ is finite by Lemma (4.1.50), it is equal to 2^l for some positive integer l. Therefore the subnearring P_R of R generated by 1 is isomorphic to the residue ring $\mathbb{Z}/2^l\mathbb{Z}$ by Lemma (3.3.4) and hence its multiplicative group ${P_R}^*$ is abelian of type $(2, 2^{l-2})$ for $l \geq 2$. On the other hand, ${P_R}^*$ is contained in R^*, so that it must be cyclic because so are the finite abelian subgroups of a generalized quaternion group. Thus $l \leq 2$, as desired.

Lemma 5.2.7 *Let R be a local nearring whose multiplicative group is generalized quaternion group, then either R is a nearfield or R^+ is a 2-group, $R^* = 1 + L_R$ and L_R is a subgroup of index 2 in R^+.*

Proof. As R^* is a group of order 2^q for some integer $q \geq 3$ and $1 + L_R$ is a subgroup of R^*, the order of $1 + L_R$ is equal to 2^s with $0 \leq s \leq q$. This means that L_R is of order 2^s and hence either R is a nearfield or $L_R \neq \{0\}$ and so $s \geq 1$. Since R^+ is a p-group for some prime p by Lemma (4.1.45) and Lemma (4.1.50), in the second case $p = 2$ and so R^+ is of order 2^n for some $n > q$. Taking into account that $R = L_R \cup R^*$, the following equality holds: $2^n = 2^s + 2^q = 2^s(1 + 2^{q-s})$ which implies that $q = s$ and $n = q + 1$. Thus $R^* = 1 + L_R$ and the subgroup L_R is of index 2 in R^+, as desired.

Lemma 5.2.8 *Let the multiplicative group R^* act on the additive group R^+ by left multiplication and let $G = R^+ \rtimes R^*$ be the semidirect product of R^+ by R^*. Then the subgroup L_R is normal in G and contained in the Frattini subgroup $\Phi(G)$ of G.*

Proof. Clearly without loss of generality we may assume that $L_R \neq 0$, so that it follows from Lemma (5.2.7) that R^+ is a finite 2-group. Therefore G is also such a group generated by its subgroup R^* and the element 1 of R^+. As R^* is generated by two elements, the group G is 3-generated and so the factor group $G/\Phi(G)$ is of order 8.

On the other hand, since L_R has index 2 in R^+ and $R^* = 1 + L_R$ by Lemma (5.2.7), the subgroup L_R is normal in G and the factor group G/L_R is the direct product of the cyclic group R^+/L_R of order 2 and a generalized quaternion group isomorphic to R^*. Thus, if $\Phi(R^*)$ is the Frattini subgroup of R^*, then the subgroup $H = L_R \rtimes \Phi(R^*)$ of G is also normal in G and the factor group G/H is elementary abelian of order 8. Therefore $\Phi(G) = H$ and so L_R is contained in $\Phi(G)$, as desired.

Corollary 5.2.9 *If the subgroup L_R is non-abelian, then the center of L_R is non-cyclic.*

Proof. Indeed, the group R^+ is a 2-group by Lemma (5.2.7) and so the semidirect product $G = R^+ \rtimes R^*$ is a 2-group in which L_R is a normal subgroup contained in its Frattini subgroup $\Phi(G)$ by Lemma (5.2.8).

Lemma 5.2.10 *The additive group R^+ of R is abelian and the subgroup L_R is elementary abelian.*

Proof. It follows from Lemma (5.2.5) that only the case $L_R \neq 0$ is necessary to consider. Then R^+ is a 2-group, $R^* = 1 + L_R$ and L_R is a subgroup of index 2 in R^+ by Lemma (5.2.7). In particular, the order of L_R is equal to 2^q for some integer $q \geq 3$ and the group R^* acts on L_R by left multiplication. Show first that this action cannot be faithful, i.e. the representation of R^* by automorphisms of L_R has a non-trivial kernel.

Indeed, otherwise L_R has an automorphism of order 2^{q-1} and therefore is either a non-cyclic abelian group of order 8 or a dihedral or generalized quaternion group by the result of Berkovich [5]. But if L_R is dihedral or generalized quaternion, then its center $Z(L_R)$ is cyclic, contrary to Corollary (5.2.9). Hence $q = 3$ and the subgroup L_R is abelian of types $(2, 2, 2)$ or $(2, 4)$. Since in both cases the automorphism group of L_R is dihedral of order 8, they are also excluded. Thus the kernel of the representation of R^* by automorphisms of L_R is non-trivial and so it contains the center $Z(R^*)$ of R^*.

Assume next that the additive group R^+ is not elementary abelian. Then R^+ is a group of exponent 4 by Lemma (5.2.6), so that $-1 \neq 1$. As $(-1)^2 = 1$ and so $\langle -1 \rangle = Z(R^*)$, it follows that $(-1)a = a$ for every $a \in L_R$. Furthermore, $(-1)(1+a) = (1+a)(-1)$ and hence $-1 + (-1)a = -a - 1$. Therefore

$-a = -1+a+1$ for every $a \in L_R$. Thus, if $b \in L_R$, then $-b = -1+b+1$ and $-(a+b) = -1+a+b+1$. As $-(a+b) = -b-a = (-1+b+1)+(-1+a+1) = -1+b+a+1$, this implies $a+b = b+a$ for any $a, b \in L_R$ and so L_R is abelian. Show that in fact L_R is an elementary abelian subgroup.

Suppose the contrary and let $M = \{a \cdot 2 \mid a \in L_R\}$. Then $1+M$ is a non-trivial subgroup of R^*. Indeed, as L_R is abelian, for every $a, b \in L_R$ it follows that $(1+a\cdot 2)(1+b\cdot 2) = 1+a\cdot 2+(1+a\cdot 2)b\cdot 2 = 1+a+(1+a\cdot 2)b+a+(1+a\cdot 2)b = 1+(a+(1+a\cdot 2)b)\cdot 2 \in 1+M$. Therefore $-1 \in 1+M$ because $\langle -1 \rangle$ is the only subgroup of order 2 in R^*. Hence $2 = a \cdot 2$ for some $a \in L_R$. On the other hand, multiplying the equality $-a = -1+a+1$ from the left on a, we have $-a^2 = -a+a^2+a = a^2$, so that $a^2 \cdot 2 = a^2 + a^2 = 0$. This implies that $2 = a \cdot 2 = a^2 \cdot 2 = 0$, contrary to the assumption.

Thus the subgroup L_R is elementary abelian and so $1+a = a+1$ for every $a \in L_R$. Since R^+ is generated by L_R and the element 1, this means that the group R^+ is abelian, as desired. □

Lemma 5.2.11 *If the local nearring R is of order 2^{q+1} with $q \geq 2$, then its additive group R^+ is abelian, the subgroup L_R is elementary abelian of index 2 in R^+ and either $q = 3$ or $q = 4$.*

Proof. It follows from Lemma (5.2.7) and Lemma (5.2.10) that $R^* = 1+L_R$, the group R^+ is abelian and the subgroup L_R is elementary abelian of index 2 in R^+. Furthermore, the semidirect product $G = L_R \rtimes 1+L_R$ in which $1+L_R$ acts on L_R by left multiplication is a group of the form $G = AB = L_R \rtimes A = L_R \rtimes B$ whose subgroups A and B are isomorphic to $1+L_R$ by Lemma (4.1.8). Therefore the order of L_R is equal to 8 or 16 by Lemma (5.2.2) and so $q = 3$ or $q = 4$.

As a conclusion, statements (1) - (3) of Theorem (5.2.4) are an immediate consequence of Lemma (5.2.5) and Lemma (5.2.11). Finally, the examples given below in the last section show that every abelian group satisfying statement (2) of the Theorem (5.2.4) is really the additive group of a local nearring with generalized quaternion multiplicative group.

5.2.2 Examples

Recall first the example of the non-commutative Dickson nearfield coupled to the Galois field F_9 of order 9.

Example 1. Define on the field $F_9 = F(+, \cdot)$ a new operation $*$ as follows: for all $a, b \in F$ put

$$a * b = \begin{cases} ab & \text{if} \quad a^4 = 1, \quad \text{and} \\ ab^3 & \text{otherwise.} \end{cases}$$

Then a simple calculation shows that $R = F(+, *)$ is a nearfield with quaternion multiplicative group.

The following two examples of local nearrings of order 16 were chosen by means of a GAP-program based on the package "SONATA, version 2.3" and now they can manually be verified.

Example 2. Let R be the nearring with identity 1 whose additive group R^+ is abelian of type $(2, 2, 2, 2)$ with generators $1, r_1, r_2, r_3$ and the semigroup $(R, \cdot)$ satisfies the relations:

$$\begin{array}{llll} (1+r_2)r_1 = r_1, & & (1+r_3)r_1 = r_1, & \\ (1+r_2)r_2 = r_1+r_2, & & (1+r_3)r_2 = r_2, & \\ (1+r_2)r_3 = r_1+r_3, & & (1+r_3)r_3 = r_1+r_3, & \\ r_2^2 = r_3^2 = r_1 \quad \text{and} & & r_1^2 = r_i r_j = 0 & \\ \text{for all} \quad i \neq j, \quad 1 \leq i, j \leq 3. & & & \end{array}$$

Then it is easy to see that the subgroup L of R^+ generated by the elements r_1, r_2, r_3 consists of non-invertible elements of R. Furthermore $(1+r_2)^2 = 1 + r_2 + (1+r_2)r_2 = 1 + r_2 + r_1 + r_2 = 1 + r_1$ and similarly $(1+r_3)^2 = 1 + r_1$. Next, $(1+r_1)^2 = 1 + r_1 + (1+r_2)^2 r_1 = 1 + r_1 + (1+r_2)r_1 = 1$ and $(1+r_2)(1+r_3)(1+r_2) = (1+r_2)(1+r_3+r_2) = 1+r_3$. Thus, if $a = 1+r_2$ and $b = 1+r_3$, then $a^4 = 1$, $a^2 = b^2$ and $b^{-1}ab = a^{-1}$. Therefore the multiplicative subgroup of R^* generated by the elements a, b is quaternion of order 8 and so must coincide with R^* because $L \cap R^* = \emptyset$ and L has the same order. Hence R^* is the quaternion group and $R = L \cup R^*$ is a local nearring with $L_R = L$.

Example 3. Let R be the nearring with identity 1 whose additive group R^+ is abelian of type $(2, 2, 4)$ with generators $r_1, r_2, 1$ and the semigroup $(R, \cdot)$ satisfies the relations:

$$\begin{array}{llll} (1+r_1)r_1 = 2+r_1, & & (1+r_2)r_1 = r_1, & \\ (1+r_1)r_2 = 2+r_2, & & (1+r_2)r_2 = 2+r_2, & \\ r_1 r_2 = 0, & & r_1^2 = r_2^2 = r_2 r_1 = 2, & \\ (r_1+r_2)r_1 = 0, & & (r_1+r_2)r_2 = 2, & \\ 2 \cdot r_1 = 2 \cdot r_2 & & = 0. & \end{array}$$

Then the subgroup L of R^+ generated by the elements $r_1, r_2, 2$ consists of the non-invertible elements of R and the multiplicative group R^* is quaternion of order 8 because it is generated by the elements $a = 1 + r_1$ and $b = 1 + r_2$ which satisfy the relations $a^2 = b^2 = -1$ and $b^{-1}ab = a^{-1}$. Thus $R = L \cup R^*$ is a local nearring with $L_R = L$.

The final two examples of local nearrings of order 32 arose from studying generalized quaternion groups of automorphisms of the abelian groups of type

$(2,2,2,2,2)$ and $(2,2,2,4)$. Most calculations were also made with computer algebra system GAP 4.4.

Example 4. Let R be the nearring with identity 1 whose additive group R^+ is abelian of type $(2,2,2,2,2)$ with generators $1, r_1, r_2, r_3, r_4$ and whose semigroup $(R,\cdot)$ satisfies the relations:

$$\begin{array}{rclrcl}
(1+r_1)r_1 & = & r_1+r_2+r_3+r_4, & (1+r_2)r_1 & = & r_1+r_2+r_3,\\
(1+r_1)r_2 & = & r_2+r_3, & (1+r_2)r_2 & = & r_2+r_4,\\
(1+r_1)r_3 & = & r_3+r_4, & (1+r_2)r_3 & = & r_3+r_4,\\
(1+r_1)r_4 & = & r_4, & (1+r_2)r_4 & = & r_4 \quad \text{and}\\
(r_i+r_j+r_k)r_l & = & (r_i+r_j+r_k+r_l)r_m & = 0 & & \text{for all}\\
1 & \leq & i,j,k,l,m \quad \leq 4. & & &
\end{array}$$

Clearly the subgroup L of R^+ generated by the elements r_1, r_2, r_3, r_4 is the set of all non-invertible elements of R and a rudimentary verification shows that the multiplicative group R^* is generated by the elements $a = 1+r_1$ and $b = 1+r_2$ satisfying the relations $a^8 = b^4 = 1$, $a^4 = b^2$ and $b^{-1}ab = a^{-1}$. Thus the group R^* is generalized quaternion of order 16 and $R = L \cup R^*$, so that R is a local nearring with $L_R = L$.

Example 5. Let R be the nearring with identity 1 whose additive group R^+ is abelian of type $(2,2,2,4)$ with generators r_1, r_2, r_3 and 1, with 1 of order 4 and let the semigroup $(R,\cdot)$ satisfies the relations:

$$\begin{array}{rclrcl}
(1+r_1)r_1 & = & 2+r_1+r_3, & (1+r_2)r_1 & = & 2+r_1,\\
(1+r_1)r_2 & = & r_2+r_3, & (1+r_2)r_2 & = & 2+r_2,\\
(1+r_1)r_3 & = & r_1+r_2+r_3, & (1+r_2)r_3 & = & 2+r_1+r_2+r_3
\end{array}$$

$$\begin{array}{rlcll}
\text{and} & (r_i+r_j)r_k & = & (r_i+r_j+r_k)r_l & = \\
 & (2+r_i+r_j)r_k & = & (2+r_i+r_j+r_k)r_l & = 0\\
\text{for all} & 1 \leq i,j,k,l \leq 3. & & &
\end{array}$$

Clearly the subgroup L of R^+ generated by the elements $r_1, r_2, r_3, 2$ coincides with the set of all non-invertible elements of R and it is easily verified that the multiplicative group R^* is generated by the elements $a = 1+r_1$ and $b = 1+r_2$ satisfying the relations $a^8 = b^4 = 1$, $a^4 = b^2$ and $b^{-1}ab = a^{-1}$. Therefore the group R^* is generalized quaternion of order 16 and hence $R = L \cup R^*$, so that R is a local nearring with $L_R = L$, as desired.

Bibliography

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

[2] B. Amberg, P. Hubert and Y. P. Sysak. *Local nearrings with dihedral multiplicative group*, J. Algebra, 273 (2004), 700-717.

[3] A. Ballester-Bolinches, Y. Wang and G. Xiuyun. *c-Supplemented subgroups of finite groups.* Glasgow Math. J. 42 (2000), 383 – 389.

[4] J. Beidleman. *Quasi-regularity in near-rings.* Math. Z., 89: 224-229, 1965.

[5] V. G. Berkovich. *Groups of order p^n that admit an automorphism of order p^{n-1}*, Algebra i Logika 9 (1970) 3-8 (in Russian).

[6] J. R. Clay. *Nearrings: geneses and applications.* Oxford Science Publications, 1992.

[7] F. De Mari, S. Di Termini. *Groups with weakly c-normal subgroups.* Accepted by the Journal Rendiconti dell'Istituto Lombardo.

[8] K. Doerk and T. O. Hawkes. *Finite soluble groups.* Walter de Gruyter, Berlin-New York, 1992.

[9] N. Jacobson. *Structure of rings.* American Mathematical Society. Colloquium Publications. Vol. 37., 1956.

[10] H. E. Heatherly, J. J. Malone. *Some near-ring embeddings.* Quart. J. Math. (Oxford)(2) 20 (1969), 81-85.

[11] I. N. Herstein. *Noncommutative Rings.* The Mathematical Association of America, Menasha, Wisconsin, 1968.

[12] P. Hubert. *Local nearrings and triply factorized groups*, Comm. Algebra, 32 (2004), 1229-1235.

[13] P. Hubert. *Nearrings and a construction of triply factorized groups*, Dissertation zur Erlangung des Grades "Doktor der Naturwissenschaften", Johannes Gutenberg Universitaet Mainz, 2005.

[14] B. Huppert and N. Blackburn. *Finite groups* II. Springer 1982.

[15] A. Gorodnik. *Local near-rings with commutative group of units*, Houston J. Math., 25 (1999), 223-234.

[16] B. M. King. *Normal subgroups of groups of prime-power order,* in : Proc. Second Internat. Conf. on the Theory of Groups (Australian Nat. Univ., Canberra, 1973), in Lecture Notes in Math. vol. 372, Springer, Berlin, 1974, pp. 401-408.

[17] Z. Lujin, G. Wenbin, K.P. Shum. *Weakly c-normal subgroups of finite groups and its properties* Comm. in Algebra, 30 (2002), 5505-5512.

[18] J. J. Malone. *Generalized quaternion groups and distributively generated near-rings.* Proc. Edinb. Math. Soc., II. Ser., 18: 235-238, 1973.

[19] E. Massarotti. *A note on generalized dedekind groups.* Rend. Acc. Sc. Fis. Mat. Napoli 68 (2001), 49–53.

[20] C. J. Maxson. *On local near-rings* Math. Z., 106, 197-205, 1968.

[21] C. J. Maxson. *Local near-rings of cardinality p^n.* Can. Math. Bull., 11: 555-561, 1968.

[22] C. J. Maxson. *On the construction of finite local near-rings.* I: *On non-cyclic abelian p-groups*, Q. J. Math., Oxf. II. Ser., 21, 1970, 449-457.

[23] C. J. Maxson. *On the construction of finite local near-rings.* II: *On non-abelian abelian p-groups*, Q. J. Math., Oxf. II. Ser., 22, 1971, 65-72.

[24] J. D. P. Meldrum. *Near-rings and their links with groups.* Pitman, London, 1985.

[25] W. Noebauer. *Ueber die Darstellung von universellen Algebren durch Funktionalgebren.* Publ. Math. Debrecen 10 (1963), 151-154.

[26] R. E. Phillips, J. S. Wilson. *On certain minimal conditions for infinite groups.* J. Algebra 51 (1978), 41–68.

[27] G. Pilz. *Near-rings. The theory and its applications.* North Holland, Amsterdam, 1977.

[28] D. J. S. Robinson. *A course in the Theory of groups*, Springer-Verlag, New York-Heidelberg-Berlin, 1982.

[29] D. J. S. Robinson. *Finiteness Conditions and Generalized Soluble Groups*, Springer, Berlin (1972).

[30] J. Rose. *On finite insolvable groups with nilpotent maximal subgroup*, J. Alegebra, 48 (1977), 182-196.

[31] R. Schimdt. *Subgroup lattice of groups*. de Gruyter, Berlin (1994).

[32] Y. P. Sysak. *Products of locally cyclic torsion-free groups*, Algebra i Logika 25 (6) (1986) 672-686.

[33] Y. P. Sysak, S. Di Termini. *Local nearrings with generalized quaternion multiplicative group*. Accepted by the Journal Ricerche di matematica.

[34] V. P. Šunkov. *Locally finite groups with a minimality condition for abelian subgroups*. Algebra and Logic 9 (1970), 350–370.

[35] H. Waehling. *Theorie der Fastkoerper*. Thales Verlag, Essen, 1987.

[36] Y. Wang. *c-Normality of groups and its properties*. J. Algebra, 78 (1996), 101-108.

[37] H. J. Weinert. *Ringe mit nichtkommutativer Addition*. I. 1975.

[38] D. I. Zaicev. *On solvable subgroups of locally solvable groups*, Soviet Math. Dokl. 15 (1974), 342–345.

[39] H. Zassenhaus. *Ueber endliche Fastkoerper*. Abhandlungen des Mathematischen Seminars Universitaet Hamburg 11, 187-220, 1936.

[40] K. Zhu, W. Guo and K. P. Shum. *Weakly c-normal subgroups of finite groups and their properties*. Comm. Algebra 30 (2002), 5505–5512.

[41] L. Zhu, W. Guo and X. Zhang. *On weakly c-normal subgroups of finite groups*. Proceedings of the International Conference on Algebra and its Application, 2002.